AVG Anti-Virus 2011

Podręcznik użytkownika

Wersja dokumentu 2011.21 (16.5.2011)

Spis treści

1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację systemu **AVG Anti-Virus 2011**.

Gratulujemy zakupu systemu AVG Anti-Virus 2011!

System **AVG Anti-Virus 2011** należy do linii uznanych i nagradzanych produktów AVG, które zapewniają użytkownikom spokój ducha, a ich komputerom — pełne bezpieczeństwo. Podobnie jak pozostałe produkty, system **AVG Anti-Virus 2011** zaprojektowano od podstaw pod kątem zapewnienia słynnego już poziomu ochrony w nowy, bardziej przyjazny dla użytkownika sposób. Nowy produkt **AVG Anti-Virus 2011** łączy ulepszony interfejs z agresywniejszym i szybszym skanowaniem. Dla wygody użytkownika zautomatyzowano najczęściej używane funkcje i dodano nowe, „inteligentne" opcje, które pozwalają precyzyjnie dostosować funkcje ochronne programu do swoich potrzeb. Koniec z poświęcaniem wydajności na rzecz ochrony!

System AVG zaprojektowano i zbudowano tak, by chronił użytkownika podczas pracy na komputerze i w sieci. Ciesz się pełną ochroną AVG.

Wszystkie produkty AVG zapewniają ochronę:

- odpowiednią do sposobu korzystania z komputera (w tym: bankowości i zakupów online, przeglądania stron WWW i przeszukiwania internetu, korzystania z komunikatorów internetowych, poczty e-mail i portali społecznościowych, a także pobierania plików;
- na tyle bezproblemową, że zaufało jej ponad 110 milionów osób na całym świecie, wspieraną przez globalną sieć wysoko wykwalifikowanych i doświadczonych specjalistów;
- wspieraną przez całodobową pomoc techniczną.

2. Wymagania instalacyjne AVG

2.1. Obsługiwane systemy operacyjne

System **AVG Anti-Virus 2011** służy do ochrony stacji roboczych działających pod następującymi systemami operacyjnymi:

- 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 także z nowszymi dodatkami SP dla niektórych systemów operacyjnych)

***Uwaga**: Składnik Identity Protection nie jest obsługiwany w systemie Windows XP x64. Można zainstalować na nim system AVG Anti-Virus 2011, ale bez składnika Identity Protection.*

2.2. Minimalne i zalecane wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG Anti-Virus 2011**:

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

Zalecane wymagania sprzętowe dla systemu **AVG Anti-Virus 2011**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB pamięci RAM.
- 1400 MB wolnego miejsca na dysku twardym (w celu instalacji),

3. Opcje instalacji systemu AVG

System AVG można zainstalować za pomocą instalatora znajdującego się na oryginalnym dysku CD lub pobranego z witryny AVG (http://www.avg.com/).

Przed rozpoczęciem instalacji systemu AVG zalecamy odwiedzenie naszej witryny (http://www.avg.com/) w celu sprawdzenia, czy jest dostępny nowy plik instalacyjny. Dzięki temu można mieć pewność, że instalowana jest najnowsza dostępna wersja systemu AVG Anti-Virus 2011.

Podczas samego procesu instalacji konieczne będzie podanie numeru licencji/sprzedaży. Należy więc przygotować go przed rozpoczęciem instalacji. Numer sprzedaży znajduje się na opakowaniu dysku CD. W przypadku zakupienia pakietu AVG przez internet, numer licencji dostarczany jest poprzez e-mail.

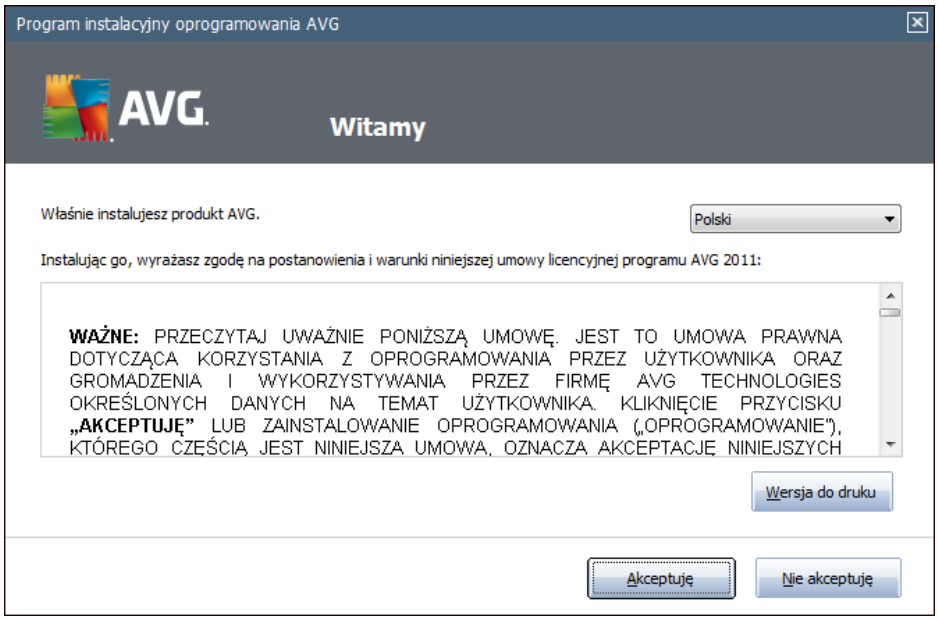
4. Proces instalacji systemu AVG

Do zainstalowania systemu **AVG Anti-Virus 2011** na komputerze konieczny jest najnowszy plik instalacyjny. Można znaleźć go na dysku CD będącym częścią dystrybucyjnej edycji programu — istnieje jednak ryzyko, że będzie on nieaktualny. Dlatego zaleca się pobranie najnowszego pliku instalacyjnego z internetu. Można go pobrać ze strony internetowej firmy AVG (http://www.avg.com/) w sekcji ***Pomoc techniczna / Pobierz.***

Instalacja to sekwencja okien dialogowych zawierających krótkie opisy poszczególnych etapów. Poniżej znajdują się objaśnienia każdego z nich:

4.1. Witamy

Proces instalacji rozpoczyna się od wyświetlenia okna dialogowego ***Witamy***. Można w nim wybrać język, który ma być używany podczas instalacji, oraz domyślny język interfejsu użytkownika AVG. W górnej sekcji okna dialogowego znajduje się menu rozwijane z listą dostępnych języków:



Uwaga: *W tym miejscu wybierany jest tylko język instalacji. Wybrany język zostanie zainstalowany jako domyślny język interfejsu użytkownika AVG, wraz z językiem angielskim (który jest instalowany automatycznie). Aby zainstalować inne, dodatkowe języki interfejsu użytkownika, należy je zdefiniować w jednym z kolejnych okien dialogowych — **Opcje niestandardowe**.*

Następnie wyświetlona zostanie pełna treść umowy licencyjnej AVG. Prosimy o jej uważne przeczytanie. Aby potwierdzić zapoznanie się z treścią umowy, zrozumienie jej i zaakceptowanie, kliknij przycisk ***Akceptuję***. Jeśli nie zgadzasz się z postanowieniami umowy licencyjnej, kliknij przycisk ***Odrzuć***. Instalacja zostanie natychmiast przerwana.

4.2. Aktywuj licencję AVG

W oknie dialogowym ***Aktywuj licencję*** użytkownik jest proszony o wprowadzenie numeru licencji w polu tekstowym.

Numer sprzedaży można znaleźć na opakowaniu dysku CD z oprogramowaniem **AVG Anti-Virus 2011**. Numer licencji jest wysyłany za pośrednictwem poczty e-mail po dokonaniu zakupu oprogramowania **AVG Anti-Virus 2011** online. Ważne jest dokładne wprowadzenie tego numeru. Jeśli numer jest dostępny w formie cyfrowej (*w wiadomości e-mail*), zaleca się skopiowanie go i wklejenie w odpowiednim polu.

Aby kontynuować instalację, kliknij przycisk ***Dalej***.

4.3. Wybierz typ instalacji

Okno dialogowe ***Wybierz typ instalacji*** umożliwia wybranie jednej z dwóch opcji instalacji: ***Instalacja szybka*** lub ***Instalacja niestandardowa***.

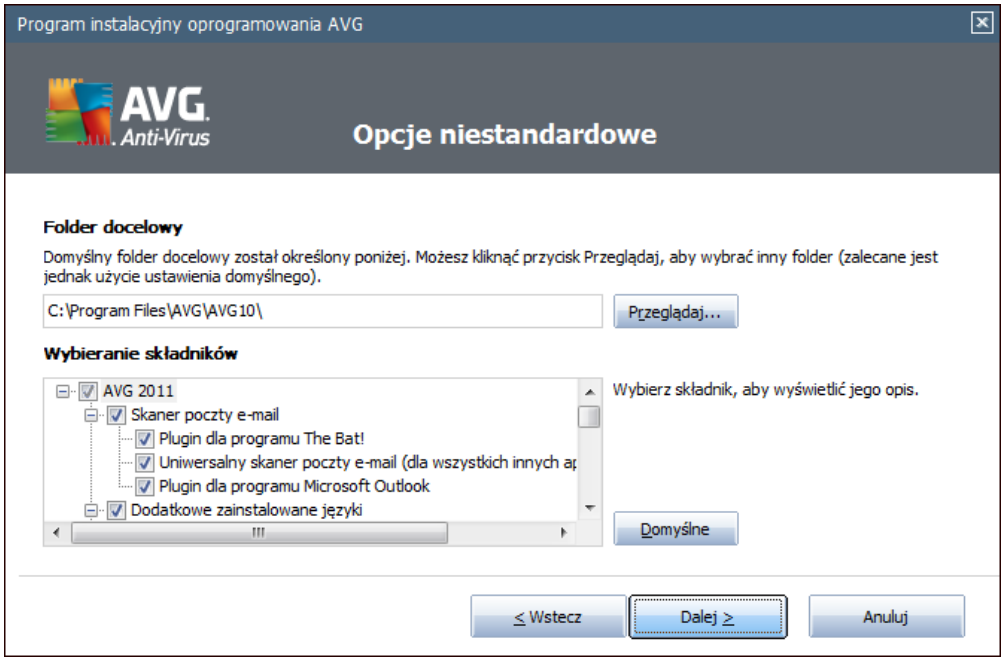
Większość użytkowników zdecydowanie powinna wybrać opcję ***Instalacja szybka***, która pozwala zainstalować system AVG w sposób całkowicie zautomatyzowany, z ustawieniami wstępnie zdefiniowanymi przez dostawcę oprogramowania AVG. Taka konfiguracja zapewnia maksymalne bezpieczeństwo oraz optymalne wykorzystanie zasobów. Jeśli w przyszłości zajdzie potrzeba zmiany konfiguracji, można będzie to zrobić bezpośrednio z poziomu interfejsu AVG. W przypadku wybrania opcji ***Szybka instalacja*** kliknij przycisk ***Dalej***, aby przejść do okna dialogowego ***Zainstaluj pasek narzędzi AVG Security Toolbar***.

Opcję ***Instalacja niestandardowa*** powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować systemu AVG z ustawieniami domyślnymi, (np. po to, aby dostosować go do specyficznych wymagań systemowych). W przypadku wybrania tej opcji kliknij przycisk ***Dalej***, aby przejść do okna ***Opcje niestandardowe***.

W prawej części tego okna dialogowego znajduje się pole wyboru dotyczące ***gadżetu AVG*** (*obsługiwanego w systemie Windows Vista/Windows 7*). Aby zainstalować gadżet, wystarczy zaznaczyć to pole. ***Gadżet AVG*** będzie wtedy dostępny z paska bocznego systemu Windows, umożliwiając bezpośredni dostęp do najważniejszych funkcji systemu **AVG Anti-Virus 2011**, tj. skanowania i aktualizacji.

4.4. Opcje niestandardowe

Okno dialogowe ***Opcje niestandardowe*** umożliwia skonfigurowanie dwóch parametrów instalacji:



Folder docelowy

W sekcji ***Folder docelowy*** można określić lokalizację, w której ma zostać zainstalowany system **AVG Anti-Virus 2011**. Domyślnie pakiet AVG jest instalowany w folderze Program Files na dysku C:. Aby zmienić tę lokalizację, kliknij przycisk ***Przeglądaj*** i w wyświetlonym oknie wybierz odpowiedni folder.

Wybór składników

Sekcja ***Wybór składników*** zawiera przegląd wszystkich możliwych do zainstalowania składników systemu **AVG Anti-Virus 2011**. Jeśli ustawienia domyślne nie są dla Ciebie odpowiednie, możesz dodać lub usunąć żądane składniki.

Wybierać można jednak tylko składniki należące do zakupionej edycji systemu AVG!

Po podświetleniu dowolnej pozycji na liście ***Wybór składników***, obok zostanie wyświetlony krótki opis odpowiedniego składnika. Szczegółowe informacje o funkcjach poszczególnych składników zawiera rozdział ***Przegląd składników***. Aby przywrócić domyślną konfigurację wstępnie ustawioną przez dostawcę oprogramowania, należy użyć przycisku ***Domyślne***.

Aby kontynuować, kliknij przycisk ***Dalej***.

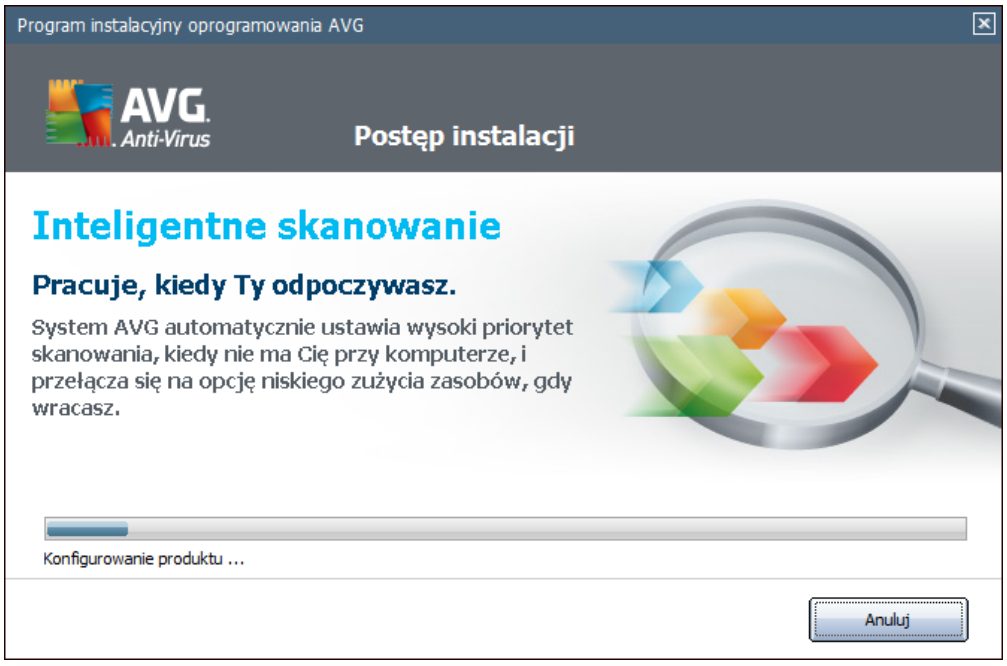
4.5. Zainstaluj pasek narzędzi AVG Security Toolbar

W oknie dialogowym ***Instalowanie paska narzędzi AVG Security Toolbar*** można zadecydować, czy ma zostać zainstalowany pasek narzędzi ***AVG Security Toolbar***. Jeśli domyślne ustawienia nie zostaną zmienione, składnik ten zostanie automatycznie zainstalowany w przeglądarce internetowej (*obecnie obsługiwane przeglądarki to Microsoft Internet Explorer w wersji 6.0 lub nowszej i Mozilla Firefox w wersji 3.0 lub nowszej*), aby zapewnić kompleksową ochronę podczas surfowania po internecie.

Możliwe jest również wybranie *AVG Secure Search (powered by Google)* jako wyszukiwarki domyślnej. Jeśli tak, należy pozostawić odpowiednie pole wyboru zaznaczone.

4.6. Postęp instalacji

Okno dialogowe ***Postęp instalacji*** zawiera jedynie informacje o postępie procesu instalacji i nie wymaga żadnych działań ze strony użytkownika:



Po zakończeniu instalacji nastąpi przekierowanie do następnego okna dialogowego.

4.7. Instalacja powiodła się

Wyświetlenie okna dialogowego ***Instalacja powiodła się*** potwierdza, że system **AVG Anti-Virus 2011** został w pełni zainstalowany i skonfigurowany.

Możesz podać w tym oknie swoje informacje kontaktowe, aby otrzymywać wszystkie aktualności dotyczące produktu. Poniżej formularza rejestracji znajdują się następujące dwie opcje:

- ***Tak, chcę otrzymywać za pośrednictwem poczty e-mail informacje o aktualizacjach zabezpieczeń i specjalnych ofertach firmy AVG*** — zaznaczenie tego pola oznacza, że chcesz być informowany o nowościach w dziedzinie zabezpieczeń internetowych oraz otrzymywać informacje o specjalnych ofertach firmy AVG, ulepszeniach i aktualizacjach produktów itd.

- ***Wyrażam zgodę na uczestnictwo w Programie udoskonalania produktów i bezpieczeństwa sieci AVG 2011*** — zaznaczenie tego pola oznacza wyrażenie zgody na uczestnictwo w Programie udoskonalania produktów (*szczegółowe informacje można znaleźć w rozdziale Zaawansowane ustawienia AVG / Program udoskonalania produktów*), w ramach którego zbierane są anonimowe informacje o wykrytych zagrożeniach w celu podnoszenia ogólnego poziomu bezpieczeństwa w internecie.

W celu ukończenia procesu instalacji konieczne jest ponowne uruchomienie komputera — można to zrobić natychmiast (wybierając opcję ***Uruchom ponownie teraz***) lub odłożyć na później (opcja ***Uruchom ponownie później***).

> ***Uwaga:*** *Jeśli używana jest licencja produktu biznesowego AVG, a wcześniej wybrano zainstalowanie składnika Administracja zdalna (patrz Opcje niestandardowe), okno dialogowe "Instalacja powiodła się" będzie wyglądało inaczej:*
>
> *Należy określić parametry bazy AVG DataCenter — podaj parametry połączenia z bazą AVG DataCenter (w formacie serwer:port). Jeśli nie masz tych informacji, możesz pozostawić to pole puste i dokonać konfiguracji później w oknie* ***Ustawienia zaawansowane / Administracja zdalna****. Szczegółowe informacje dotyczące Administracji zdalnej AVG można znaleźć w podręczniku użytkownika systemu AVG Business Edition; podręcznik ten można pobrać z witryny internetowej systemu AVG (http://www.avg.com/).*

5. Po instalacji

5.1. Rejestracja produktu

Po ukończeniu instalacji systemu **AVG Anti-Virus 2011** należy zarejestrować produkt online na stronie internetowej AVG (http://www.avg.com/) w sekcji ***Rejestracja*** (*postępując zgodnie z wyświetlanymi tam instrukcjami*). Rejestracja umożliwia pełny dostęp do konta użytkownika AVG, biuletynu aktualizacji AVG i innych usług oferowanych wyłącznie zarejestrowanym klientom.

5.2. Dostęp do interfejsu użytkownika

Dostęp do ***interfejsu użytkownika AVG*** można uzyskać na kilka sposobów:

- klikając dwukrotnie ***ikonę AVG na pasku zadań,***
- klikając dwukrotnie ikonę AVG na pulpicie,
- klikając dwukrotnie status znajdujący się w dolnej sekcji ***gadżetu AVG*** (*jeśli został zainstalowany — obsługiwany w systemach Windows Vista i Windows 7*),
- z poziomu menu ***Start/Programy/AVG 2011/Interfejs użytkownika AVG,***
- z poziomu ***paska narzędzi AVG Security Toolbar,*** za pomocą opcji ***Uruchom system AVG.***

5.3. Skanowanie całego komputera

Istnieje pewne ryzyko, że wirus dostał się do komputera przed zainstalowaniem systemu **AVG Anti-Virus 2011**. Z tego powodu należy uruchomić test ***Skan całego komputera***, aby upewnić się, że jest on w pełni bezpieczny.

Instrukcje dotyczące uruchamiania testu ***Skan całego komputera*** zawiera rozdział ***Skanowanie AVG***.

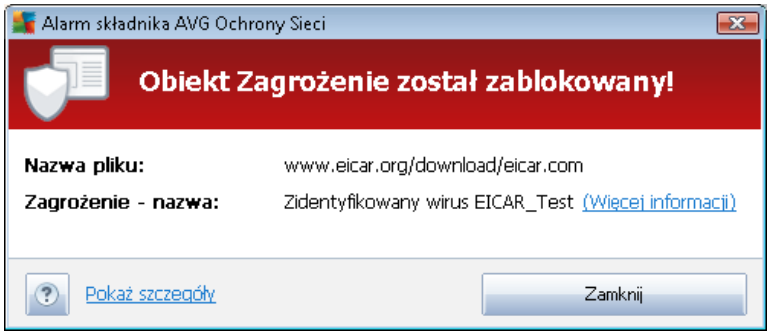
5.4. Test EICAR

Aby potwierdzić, że system **AVG Anti-Virus 2011** został zainstalowany poprawnie, można przeprowadzić test EICAR.

Test EICAR jest standardową i całkowicie bezpieczną metodą służącą do sprawdzania prawidłowości działania systemu antywirusowego. Można go bezpiecznie rozpowszechniać, ponieważ nie jest prawdziwym wirusem i nie zawiera żadnych fragmentów złośliwego kodu. Większość produktów rozpoznaje go jako wirusa (*chociaż zwykle zgłasza go pod jednoznaczną nazwą, np. „EICAR-AV-Test”*). Wirusa EICAR można pobrać z witryny stowarzyszenia EICAR, dostępnej pod adresem www.eicar.com. Można tam również znaleźć wszystkie niezbędne informacje na temat testu EICAR.

Spróbuj pobrać plik ***eicar.com*** i zapisać go na dysku twardym komputera. Natychmiast po

rozpoczęciu pobierania pliku testowego, składnik ***Ochrona Sieci*** zareaguje wyświetleniem ostrzeżenia. Pojawienie się komunikatu potwierdza, że oprogramowanie AVG jest prawidłowo zainstalowane na komputerze.



Ze strony internetowej http://www.eicar.com można również pobrać skompresowaną wersję „wirusa" EICAR (*w formie pliku eicar_com.zip*). ***Ochrona Sieci*** pozwoli pobrać ten plik i zapisać go na dysku, ale ***Ochrona rezydentna*** wykryje go już w chwili rozpakowywania. **Jeśli system AVG nie rozpozna pliku testowego EICAR jako wirusa, należy ponownie sprawdzić jego konfigurację!**

5.5. Konfiguracja domyślna systemu AVG

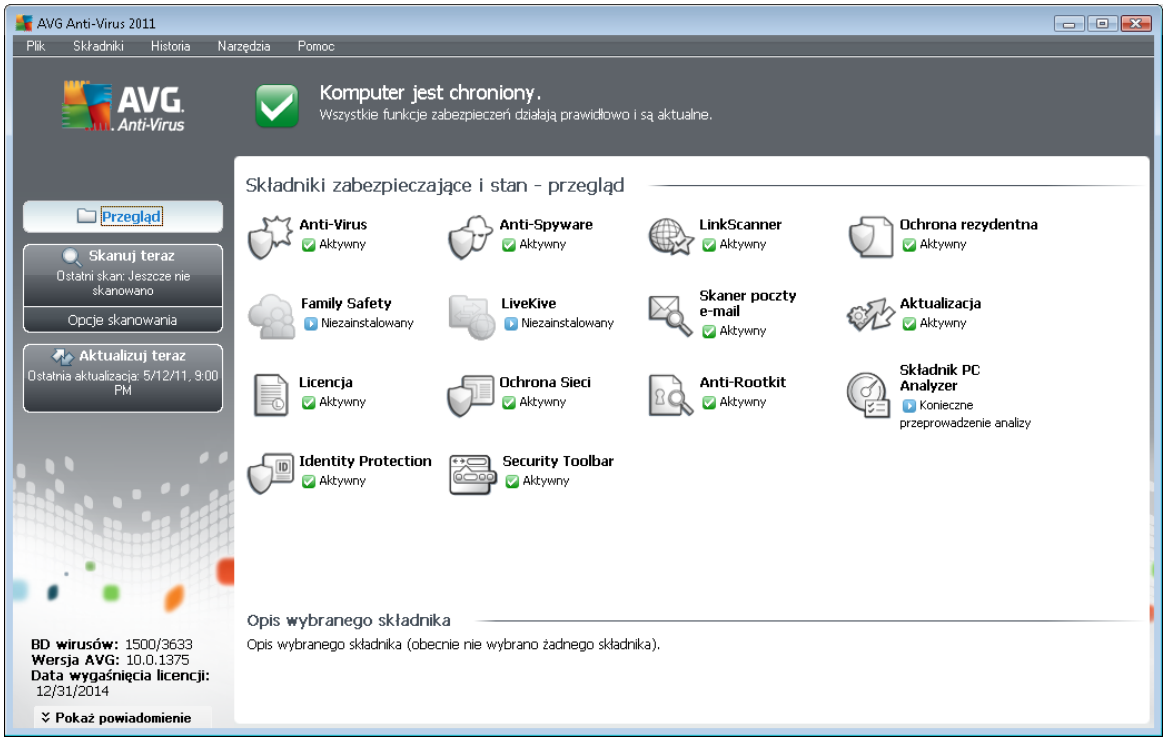
Konfiguracja domyślna (*ustawienia stosowane zaraz po instalacji*) systemu **AVG Anti-Virus 2011** jest wstępnie definiowana przez producenta i ma na celu zapewnienie optymalnej wydajności wszystkich składników oraz funkcji.

Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach! Wszelkie zmiany ustawień powinny być wprowadzane wyłącznie przez doświadczonych użytkowników.

Mniejsze zmiany ustawień ***składników AVG*** można wprowadzać bezpośrednio z ich interfejsu użytkownika. Jeśli konfiguracja systemu AVG powinna zostać lepiej dopasowana do potrzeb, należy użyć ***zaawansowanych ustawień AVG***, wybierając z menu systemowego pozycję ***Narzędzia/ Ustawienia zaawansowane*** i edytując opcje w otwartym oknie dialogowym ***AVG - Ustawienia zaawansowane***.

6. Interfejs użytkownika AVG

Otwarcie systemu **AVG Anti-Virus 2011** następuje w jego oknie głównym:



Okno główne jest podzielone na kilka sekcji:

- ***Menu główne*** *(górny wiersz okna)* to standardowe narzędzie nawigacyjne umożliwiające dostęp do wszystkich składników, usług i funkcji systemu AVG — szczegóły >>
- ***Informacje o stanie bezpieczeństwa*** *(prawa część górnej sekcji okna)* zawiera informacje dotyczące bieżącego stanu programu AVG — szczegóły >>
- ***Szybkie linki*** *(lewa kolumna)* umożliwiają uzyskanie szybkiego dostępu do najważniejszych i najczęściej używanych funkcji programu AVG — szczegóły >>
- ***Przegląd składników*** *(centralna część okna)* zawiera przegląd zainstalowanych składników programu AVG — szczegóły >>
- ***Statystyka*** *(lewa dolna sekcja okna)* zawiera najważniejsze dane statystyczne dotyczące działania programu — szczegóły >>
- ***Ikona na pasku zadań*** *(prawy dolny róg ekranu, na pasku systemowym)* sygnalizuje bieżący stan programu AVG — szczegóły >>
- ***Gadżet AVG*** *(pasek boczny obsługiwany w systemach Windows Vista i Windows 7)* umożliwia szybki dostęp do funkcji skanowania i aktualizacji systemu AVG — szczegóły >>

6.1. Menu systemowe

Menu systemowe to standardowa metoda nawigacji we wszystkich aplikacjach w systemie Windows. Jest położone poziomo w górnej części głównego okna systemu **AVG Anti-Virus 2011**. Menu systemowe zapewnia dostęp do poszczególnych składników AVG, funkcji i usług.

Menu systemowe jest podzielone na pięć sekcji:

6.1.1. Plik

- ***Zakończ*** — powoduje zamknięcie **AVG Anti-Virus 2011**interfejsu użytkownika. System AVG działa jednak w tle, a komputer jest nadal chroniony!

6.1.2. Składniki

Pozycja ***Składniki*** w menu głównym zawiera linki do wszystkich zainstalowanych składników AVG; kliknięcie któregoś z nich powoduje otwarcie domyślnego okna interfejsu odpowiedniego składnika:

- ***Przegląd systemu*** — pozwala przełączyć widok do domyślnego okna interfejsu użytkownika AVG, zawierającego przegląd zainstalowanych składników i informacje o ich stanie.
- ***Anti-Virus*** — zapewnia ochronę przed wirusami, które mogą zainfekować komputer — szczegóły >>
- ***Anti-Spyware*** — zapewnia ochronę przed oprogramowaniem szpiegującym i reklamowym — szczegóły >>
- ***LinkScanner*** — sprawdza wyniki wyszukiwania wyświetlane przez serwisy internetowe — szczegóły >>
- ***Skaner poczty e-mail*** — sprawdza wszystkie przychodzące i wychodzące wiadomości e-mail w poszukiwaniu wirusów — szczegóły >>
- ***Bezpieczeństwo rodziny*** — pozwala śledzić aktywność online Twoich dzieci i chronić je przed nieodpowiednią zawartością — szczegóły >>
- ***LiveKive*** — zapewnia automatyczne tworzenie internetowej kopii zapasowej Twoich danych — szczegóły >>
- ***Ochrona rezydentna*** — działa w tle; skanuje pliki przy ich kopiowaniu, otwieraniu i zapisywaniu — szczegóły >>
- ***Menedżer aktualizacji*** — kontroluje wszystkie aktualizacje systemu AVG — szczegóły >>
- ***Licencja*** — wyświetla numer, typ i datę wygaśnięcia licencji —szczegół >>
- ***Ochrona Sieci*** — skanuje wszystkie dane pobierane przez przeglądarkę internetową — szczegóły >>

- ***Anti-Rootkit*** — wykrywa programy i technologie próbujące ukryć w systemie szkodliwe oprogramowanie — szczegóły >>

- ***PC Analyzer*** — analizuje stan komputera — szczegóły >>

- ***Identity Protection*** — składnik chroniący przed złośliwym oprogramowaniem, wyspecjalizowany w zapobieganiu kradzieży cennych danych osobowych — szczegóły >>

- ***Pasek narzędzi Security Toolbar*** — pozwala korzystać z wybranych funkcji systemu AVG bezpośrednio z poziomu przeglądarki internetowej — szczegóły >>

- ***Administracja zdalna*** — składnik wyświetlany tylko w edycjach biznesowych systemu AVG, o ile został wybrany podczas instalacji.

6.1.3. Historia

- ***Wyniki skanowania*** — przełącza do interfejsu skanera AVG, konkretnie do okna dialogowego ***Przegląd wyników skanowania***

- ***Zagrożenia wykryte przez Ochronę rezydentną*** — otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez składnik ***Ochrona rezydentna***

- ***Zagrożenia wykryte przez Skaner poczty e-mail*** — otwiera okno dialogowe zawierające przegląd załączników e-mail uznanych za niebezpieczne przez składnik ***Skaner poczty e-mail***.

- ***Zagrożenia wykryte przez Ochronę Sieci*** — otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez składnik ***Ochrona Sieci***

- ***Przechowalnia wirusów*** — powoduje otwarcie interfejsu ***Przechowalni wirusów***, do której program AVG przenosi wszystkie niemożliwe do wyleczenia infekcje. W czasie tej kwarantanny zainfekowane pliki są izolowane i nie zagrażają bezpieczeństwu komputera, a jednocześnie istnieje możliwość ich naprawy w przyszłości.

- ***Dziennik historii zdarzeń*** — otwiera interfejs dziennika historii z przeglądem wszystkich zarejestrowanych **AVG Anti-Virus 2011akcji** .

6.1.4. Narzędzia

- ***Skanuj komputer*** — przełącza do interfejsu skanera systemu AVG i uruchamia skan całego komputera.

- ***Skanuj wybrany folder*** — przełącza do interfejsu skanera systemu AVG i umożliwia wskazanie plików oraz folderów, które mają zostać przeskanowane.

- ***Skanuj plik*** — umożliwia uruchomienie na żądanie testu pojedynczego pliku wybranego z drzewa katalogów.

- ***Aktualizuj*** — automatycznie uruchamia proces aktualizacji systemu **AVG Anti-Virus 2011.**

- ***Aktualizuj z katalogu*** — uruchamia proces aktualizacji korzystając z pliku

zlokalizowanego w określonym folderze na dysku lokalnym. Jednak ta opcja jest zalecana do użytku jedynie w sytuacjach awaryjnych, np. gdy nie ma połączenia z internetem (*komputer został zainfekowany i odłączony od internetu, komputer jest podłączony do sieci bez dostępu do internetu itp.*). W nowo otwartym oknie należy wskazać folder, w którym został wcześniej umieszczony plik aktualizacyjny i uruchomić proces.

- ***Ustawienia zaawansowane*** — otwiera okno dialogowe ***AVG — Ustawienia zaawansowane***, w którym można edytować konfigurację systemu**AVG Anti-Virus 2011** . Na ogół zaleca się zachowanie domyślnych ustawień zdefiniowanych przez producenta oprogramowania AVG.

6.1.5. Pomoc

- ***Spis treści*** — otwiera pliki pomocy systemu AVG.
- ***Uzyskaj pomoc online*** — otwiera witrynę firmy AVG (http://www.avg.com/) na stronie centrum pomocy technicznej dla klientów.
- ***Strona Mój AVG*** — otwiera witrynę systemu AVG (http://www.avg.com/).
- ***Informacje o wirusach i zagrożeniach*** — powoduje otwarcie ***Encyklopedii Wirusów*** online, w której znaleźć można szczegółowe informacje na temat znanych wirusów.
- ***Aktywuj ponownie*** — otwiera okno ***Aktywacja programu AVG*** zawierające dane wprowadzone na etapie ***personalizacja programu AVG*** (podczas procesu instalacji). W oknie tym można wprowadzić numer licencji w celu zastąpienia numeru sprzedaży (*użytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przykład podczas uaktualnienia do nowego produktu AVG*).
- ***Zarejestruj teraz*** — stanowi link do strony rejestracji w witrynie systemu AVG (http://www.avg.com/). Należy w niej wprowadzić swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysługuje bezpłatna pomoc techniczna.

Uwaga**: W przypadku korzystania z próbnej wersji systemu* **AVG Anti-Virus 2011, ostatnie dwie wyświetlone pozycje to* ***Kup teraz*** *i* ***Aktywuj***. *Umożliwiają one uaktualnienie programu do jego pełnej wersji. W przypadku systemu* **AVG Anti-Virus 2011** *zainstalowanego z numerem sprzedaży, te pozycje to* ***Zarejestruj*** *i* ***Aktywuj***. *Więcej informacji można znaleźć w sekcji Licencja niniejszej dokumentacji.*

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

6.2. Status bezpieczeństwa

Sekcja ***Informacje o stanie bezpieczeństwa*** znajduje się w górnej części Interfejsu użytkownika AVG. Znajdziesz tam informacje o bieżącym stanie bezpieczeństwa systemu **AVG Anti-Virus 2011** . W obszarze tym mogą być wyświetlane następujące ikony:

 — Zielona ikona oznacza, że system AVG jest w pełni funkcjonalny. Komputer jest całkowicie chroniony, bazy danych są aktualne, a wszystkie zainstalowane składniki działają prawidłowo.

 — Ikona pomarańczowa oznacza, że co najmniej jeden składnik jest nieprawidłowo skonfigurowany; należy sprawdzić jego właściwości i ustawienia. W systemie AVG nie wystąpił jednak żaden problem krytyczny, a użytkownik prawdopodobnie wyłączył tylko z jakiegoś powodu jeden lub więcej składników. System AVG nadal chroni komputer, należy jednak sprawdzić ustawienia składnika, który zgłasza problem. Jego nazwa jest wyświetlana w sekcji ***Informacje o stanie bezpieczeństwa***.

Ikona ta jest także wyświetlana, gdy z jakiegoś powodu stan błędu składników ma być ignorowany (*opcja „Ignoruj stan składnika" jest dostępna po kliknięciu prawym przyciskiem ikony odpowiedniego składnika w głównej sekcji okna AVG*). Użycie tej opcji może być wskazane w określonych sytuacjach, ale stanowczo zaleca się jak najszybsze ponowne wyłączenie opcji ***Ignoruj stan składnika***.

 — Czerwona ikona oznacza, że stan systemu AVG jest krytyczny! Jeden lub więcej składników nie działa, a system AVG nie może chronić komputera. Należy natychmiast usunąć zgłoszony problem. Jeśli nie jest to możliwe, należy skontaktować się z zespołem Pomocy technicznej AVG.

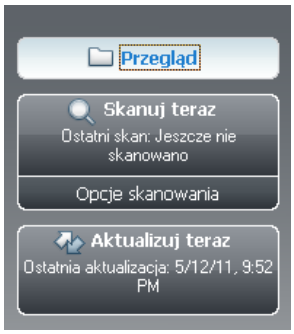
Jeśli system AVG nie działa w sposób optymalny, wyświetlony zostanie nowy przycisk o nazwie Napraw (lub Napraw wszystkie problemy, jeśli problem dotyczy więcej niż jednego składnika). Kliknięcie tego przycisku spowoduje uruchomienie automatycznego procesu sprawdzenia konfiguracji programu. Jest to prosty sposób na osiągnięcie optymalnej wydajności systemu AVG i maksymalnego poziomu bezpieczeństwa.

Stanowczo zaleca się reagowanie na zmiany ***Stanu bezpieczeństwa*** i natychmiastowe rozwiązywanie ewentualnych problemów. Brak reakcji naraża komputer na poważne zagrożenia!

Uwaga: *Dostęp do informacji o stanie systemu AVG zapewnia przez cały czas również ikona na pasku zadań.*

6.3. Szybkie linki

Szybkie linki *(z lewej strony interfejsu użytkownika AVG)* pozwalają natychmiast uzyskać dostęp do najważniejszych i najczęściej używanych funkcji systemu AVG:



- ***Przegląd*** — pozwala przełączać między bieżącym interfejsem systemu AVG a interfejsem domyślnym, zawierającym przegląd wszystkich zainstalowanych składników; zobacz rozdział ***Przegląd składników*** >>
- ***Skanuj teraz*** — domyślnie ten przycisk udostępnia informacje o ostatnim uruchomionym skanowaniu (*typ skanowania, data*). Można skorzystać z polecenia ***Skanuj teraz*** w celu ponownego uruchomienia takiego samego skanowania lub kliknąć link ***Opcje skanowania***, aby otworzyć interfejs skanowania AVG, w którym można uruchamiać skany, planować je lub edytować ich parametry — zobacz rozdział ***Skanowanie AVG*** >>
- ***Aktualizuj teraz*** — ten link udostępnia datę ostatniego uruchomienia procesu aktualizacji. Kliknij przycisk, aby natychmiast uruchomić proces aktualizacji systemu AVG — zobacz rozdział ***Aktualizacje AVG*** >>

Linki te są zawsze dostępne. Kliknięcie jednego z nich w celu uruchomienia określonego procesu powoduje wyświetlenie innego okna dialogowego, ale sama sekcja szybkich linków nie ulegnie zmianie. Uruchomiony proces zostanie dodatkowo przedstawiony w formie graficznej.

6.4. Przegląd składników

Sekcja ***Przegląd składników*** znajduje się w środkowej części interfejsu użytkownika systemu AVG. Obszar ten podzielony jest na dwie części:

- Przegląd wszystkich zainstalowanych składników (panel z odpowiednimi ikonami oraz informacjami o tym, czy dany składnik jest aktywny, czy nie)
- Opis wybranego składnika.

Sekcja **Przegląd składników** systemu ***AVG Anti-Virus 2011*** zawiera informacje o następujących składnikach:

- ***Anti-Virus*** — zapewnia ochronę przed wirusami, które mogą zainfekować komputer — szczegóły >>

- ***Anti-Spyware*** — zapewnia ochronę przed oprogramowaniem szpiegującym i reklamowym — szczegóły >>
- ***LinkScanner*** — sprawdza wyniki wyszukiwania wyświetlane przez serwisy internetowe — szczegóły >>
- ***Skaner poczty e-mail*** — sprawdza wszystkie przychodzące i wychodzące wiadomości e-mail w poszukiwaniu wirusów — szczegóły >>
- ***Ochrona rezydentna*** — działa w tle; skanuje pliki przy ich kopiowaniu, otwieraniu i zapisywaniu — szczegóły >>
- ***Bezpieczeństwo rodziny*** — pozwala śledzić aktywność online Twoich dzieci i chronić je przed nieodpowiednią zawartością — szczegóły >>
- ***LiveKive*** — zapewnia automatyczne tworzenie internetowej kopii zapasowej Twoich danych — szczegóły >>
- ***Menedżer aktualizacji*** — kontroluje wszystkie aktualizacje systemu AVG — szczegóły >>
- ***Licencja*** — wyświetla numer, typ i datę wygaśnięcia licencji —szczegół >>
- ***Ochrona Sieci*** — skanuje wszystkie dane pobierane przez przeglądarkę internetową — szczegóły >>
- ***Anti-Rootkit*** — wykrywa programy i technologie próbujące ukryć w systemie szkodliwe oprogramowanie — szczegóły >>
- ***PC Analyzer*** — analizuje stan komputera — szczegóły >>
- ***Identity Protection*** — składnik chroniący przed złośliwym oprogramowaniem, wyspecjalizowany w zapobieganiu kradzieży cennych danych osobowych — szczegóły >>
- ***Pasek narzędzi Security Toolbar*** — pozwala korzystać z wybranych funkcji systemu AVG bezpośrednio z poziomu przeglądarki internetowej — szczegóły >>
- ***Administracja zdalna*** — składnik wyświetlany tylko w edycjach biznesowych systemu AVG, o ile został wybrany podczas instalacji.

Pojedyncze kliknięcie ikony dowolnego składnika spowoduje podświetlenie go w sekcji przeglądu. Jednocześnie u dołu interfejsu użytkownika pojawia się opis funkcji wybranego składnika. Dwukrotne kliknięcie ikony powoduje otwarcie interfejsu konkretnego składnika (z jego opcjami i statystykami).

Kliknięcie prawym przyciskiem ikony składnika powoduje otwarcie menu kontekstowego. Można w nim nie tylko otworzyć graficzny interfejs składnika, ale także wybrać opcję ***ignorowania stanu składnika***. Opcję tę należy wybrać, jeśli stan błędu składnika jest znany, ale z pewnego powodu system AVG ma być nadal używany, a użytkownik nie ma być ostrzegany za pomocą ikony na pasku zadań.

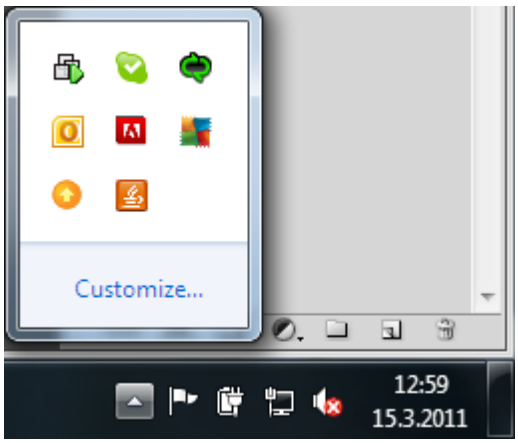
6.5. Statystyki

Obszar ***Statystyki*** znajduje się w lewym dolnym rogu ***Interfejsu użytkownika systemu AVG***. Sekcja ta zawiera szereg informacji o działaniu programu:

- ***BD wirusów*** — aktualnie używana wersja bazy wirusów.
- ***Wersja AVG*** — zainstalowana wersja systemu AVG *(numer w formacie 10.0.xxxx, gdzie 10.0. to wersja linii produktów, a xxxx — numer kompilacji).*
- ***Data wygaśnięcia licencji*** — data wygaśnięcia licencji systemu AVG.

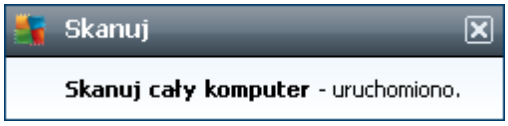
6.6. Ikona na pasku zadań

Ikona AVG (*na pasku zadań systemu Windows*) wskazuje obecny stan systemu **AVG Anti-Virus 2011**. Ikona ta jest zawsze widoczna, niezależnie od tego, czy Interfejs użytkownika AVG jest otwarty, czy też nie:



Jeśli , ***ikona na pasku zadań*** jest kolorowa, wszystkie składniki systemu AVG są aktywne i w pełni funkcjonalne. Może ona być kolorowa także wtedy, gdy system AVG zasygnalizował błędy, ale użytkownik akceptuje je i celowo ***ignoruje stan składników***. Ikona z wykrzyknikiem wskazuje problem (*nieaktywny składnik, stan błędu itp.*). W takim przypadku należy dwukrotnie kliknąć ***ikonę AVG***, aby otworzyć Interfejs użytkownika i sprawdzić stan składników.

Ikona na pasku zadań informuje również o bieżących aktywnościach systemu AVG i możliwych zmianach jego stanu (*np. automatyczne uruchomienie zaplanowanego skanowania lub aktualizacji, zmianę stanu składnika, wystąpienie błędu, ...*) dzięki wyskakującym okienkom wyświetlanym nad ikoną AVG:



Dwukrotne kliknięcie ***ikony na pasku zadań*** pozwala także szybko, w dowolnym momencie uzyskać dostęp do Interfejsu użytkownika systemu AVG. Kliknięcie ***ikony na pasku zadań***

prawym przyciskiem myszy otwiera menu kontekstowe zawierające następujące opcje:

- ***Otwórz Interfejs użytkownika AVG*** — otwiera Interfejs użytkownika.
- ***Skany*** — kliknij, aby otworzyć menu kontekstowe składnika
- ***Uruchom program PC Analyzer*** — kliknij, aby uruchomić składnik PC Analyzer.
- ***Uruchomione skany*** — ten element jest wyświetlany tylko w przypadku, gdy na komputerze jest aktualnie uruchomione skanowanie. Istnieje możliwość ustawienia priorytetu uruchomionego skanu, zatrzymania skanowania lub wstrzymania go. Ponadto dostępne są następujące akcje: *Ustaw priorytet dla wszystkich skanów, Wstrzymaj wszystkie skanowania* lub *Zatrzymaj wszystkie skanowania*.
- ***Aktualizuj teraz*** — uruchamia natychmiastową aktualizację.
- ***Pomoc*** — otwiera plik pomocy na stronie startowej.

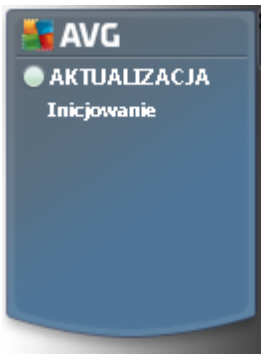
6.7. Gadżet AVG

Gadżet AVG jest wyświetlany na pulpicie systemu Windows (*pasku bocznym*). Ta aplikacja jest obecna tylko w systemach operacyjnych Windows Vista i Windows 7. ***Gadżet AVG*** oferuje natychmiastowy dostęp do najważniejszych funkcji systemu **AVG Anti-Virus 2011** , tj. skanowania i aktualizacji:

Gadżet AVG udostępnia następujące opcje szybkiego dostępu:

- ***Skanuj teraz*** — kliknięcie łącza ***Skanuj teraz*** umożliwia bezpośrednie uruchomienie ***skanu całego komputera*****.** Postęp procesu skanowania można obserwować w interfejsie użytkownika gadżetu. Krótki przegląd statystyk zawiera informacje o liczbie przeskanowanych obiektów, oraz wykrytych i wyleczonych zagrożeń. Proces skanowania można zawsze wstrzymać lub zatrzymać podczas wykonywania. Szczegółowe dane związane z wynikami skanowania można znaleźć w oknie dialogowym ***Przegląd wyników skanowania*****;** okno to można otworzyć za pomocą dostępnej z poziomu gadżetu opcji ***Pokaż szczegóły*** (wyniki odpowiedniego skanowania będą dostępne w sekcji ***Skany gadżetu na pasku bocznym***).

- ***Aktualizuj teraz*** — kliknięcie łącza ***Aktualizuj teraz*** umożliwia uruchomienie aktualizacji systemu AVG bezpośrednio z poziomu gadżetu:



- ***Link do serwisu Twitter*** — otwiera nowe okno interfejsu ***gadżetu AVG***, zawierające przegląd najnowszych informacji systemu AVG opublikowanych w serwisie Twitter. Kliknij link ***Wyświetl wszystkie informacje AVG na Twitterze***, aby otworzyć nowe okno, w którym nastąpi przekierowanie bezpośrednio na stronę WWW serwisu Twitter poświęconą aktualnościom dotyczącym systemu AVG:

- ***Link do serwisu Facebook*** — powoduje otwarcie przeglądarki internetowej z wyświetloną stroną ***społeczności AVG***.

- ***LinkedIn*** — ta opcja jest dostępna jedynie podczas instalacji sieciowej (*tj. w przypadku*

instalowania systemu AVG przy użyciu jednej z licencji biznesowych), a jej wybranie powoduje otwarcie przeglądarki internetowej na stronie internetowej ***społeczności AVG SMB*** w sieci LinkedIn.

- ***PC Analyzer***  — otwiera interfejs składnika ***PC Analyzer***.
- ***Pole wyszukiwania*** — wprowadzenie słowa kluczowego powoduje natychmiastowe zwrócenie wyników w nowo otwartym oknie domyślnej przeglądarki internetowej.

7. Składniki AVG

7.1. Anti-Virus

7.1.1. Zasady działania składnika Anti-Virus

Silnik skanujący programu antywirusowego skanuje wszystkie pliki i wykonywane na nich operacje (otwieranie, zamykanie itd.) w poszukiwaniu znanych wirusów. Każdy wykryty wirus jest blokowany (aby nie mógł wykonywać żadnych szkodliwych działań), a następnie usuwany lub izolowany. Większość programów antywirusowych korzysta także z analizy heurystycznej — pliki są skanowane w poszukiwaniu charakterystycznych cech wirusów - tak zwanych sygnatur. Oznacza to, że skaner antywirusowy może wykryć nowe, nieznane dotąd wirusy, jeśli posiadają one pewne popularne właściwości.

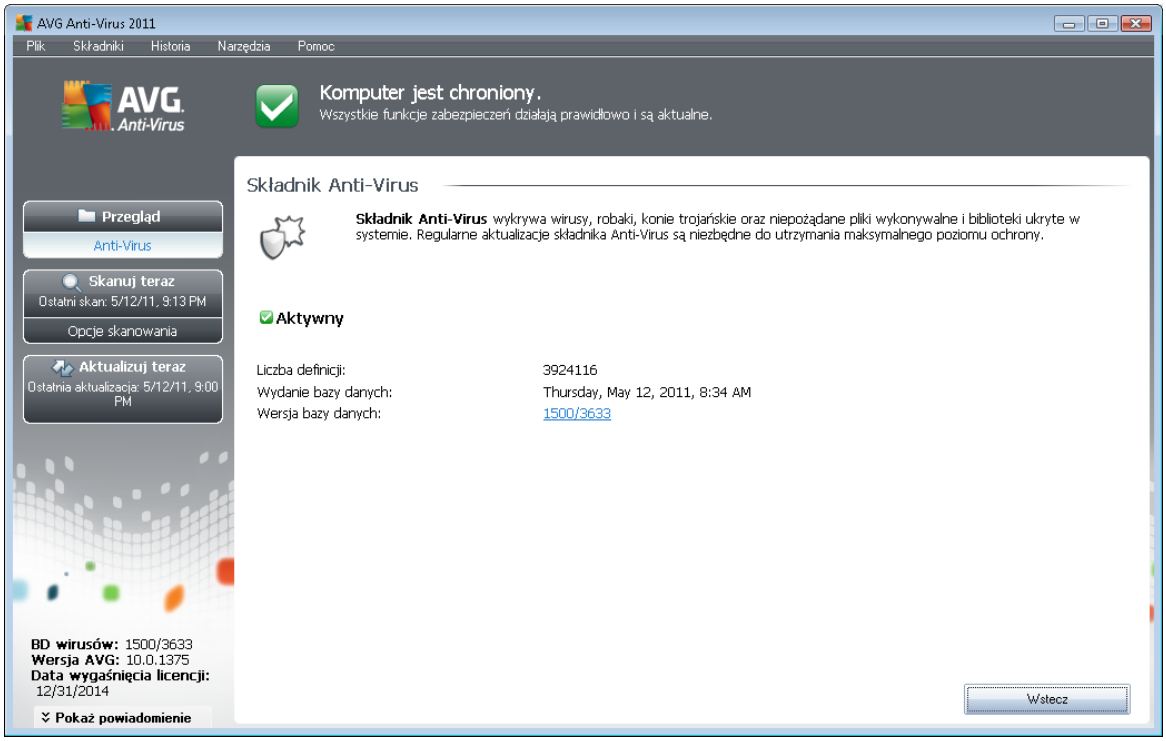
Ważną zaletą ochrony antywirusowej jest fakt, że nie pozwala ona na uruchomienie żadnych znanych wirusów na komputerze!

Korzystanie z tylko jednej technologii nie zapewnia stuprocentowej skuteczności wykrywania wirusów, dlatego składnik ***Anti-Virus*** wykorzystuje jednocześnie kilka metod:

- Skanowanie — wyszukiwanie ciągów bajtów typowych dla danego wirusa.
- Analiza heurystyczna — dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej.
- Wykrywanie generyczne — wykrywanie instrukcji typowych dla danego wirusa lub grupy wirusów.

Program AVG jest również w stanie analizować i wykrywać wykonywalne aplikacje i biblioteki DLL, które mogą być potencjalne niepożądane w Twoim systemie. Takie zagrożenia (różne rodzaje oprogramowania szpiegującego, reklamowego itp.) nazywane są również potencjalnie niechcianymi programami. Ponadto program AVG skanuje rejestr systemu w poszukiwaniu podejrzanych wpisów, a także monitoruje tymczasowe pliki internetowe i śledzące pliki cookie. Umożliwia to traktowanie wszystkich potencjalnie szkodliwych obiektów w taki sam sposób jak innych infekcji.

7.1.2. Interfejs składnika Anti-Virus



Interfejs składnika ***Anti-Virus*** zawiera krótki opis jego funkcji, informację o bieżącym stanie (Składnik *Anti-Virus jest aktywny.*), a także krótki przegląd statystyk:

- ***Liczba definicji*** — liczba wirusów zdefiniowanych w najnowszej wersji bazy danych.
- ***Wydanie bazy danych*** — data i godzina ostatniej aktualizacji bazy danych wirusów.
- ***Wersja bazy danych*** — numer aktualnie zainstalowanej wersji bazy wirusów; numer ten jest zwiększany przy każdej jej aktualizacji.

Interfejs tego składnika zawiera tylko jeden przycisk (***Wstecz***) — kliknięcie go spowoduje powrót do domyślnego interfejsu użytkownika systemu AVG (*przeglądu składników*).

7.2. Anti-Spyware

7.2.1. Zasady działania składnika Anti-Spyware

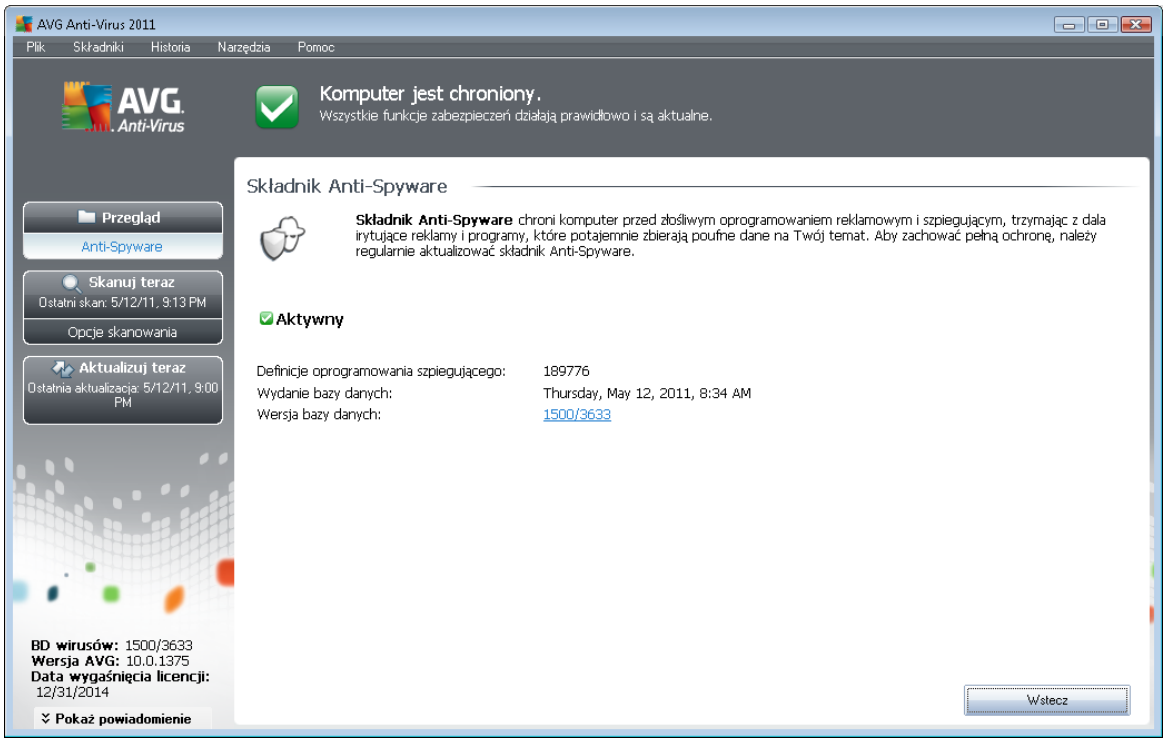
Oprogramowanie szpiegujące (spyware) jest zazwyczaj definiowane jako pewien rodzaj szkodliwego oprogramowania, które gromadzi informacje z komputera użytkownika bez jego wiedzy i pozwolenia. Niektóre aplikacje szpiegujące mogą być instalowane przez użytkownika celowo, mimo że często zawierają one reklamy, wyskakujące okna i inne denerwujące elementy.

Obecnie źródłem większości infekcji są potencjalnie niebezpieczne witryny internetowe.

Powszechne są również inne metody rozprzestrzeniania, na przykład poprzez pocztę e-mail lub za pomocą robaków i wirusów. Najskuteczniejszą ochroną jest stosowanie stale pracującego w tle składnika ***Anti-Spyware***, który działa jak ochrona rezydentna i skanuje aplikacje w tle podczas ich uruchamiania.

Istnieje jednak ryzyko, że szkodliwe oprogramowanie znalazło się na komputerze przed zainstalowaniem systemu **AVG Anti-Virus 2011** lub że użytkownik zaniedbał jego aktualizacje, nie korzystając z aktualnych baz wirusów i nowych wersji programu. Z tego powodu AVG umożliwia pełne przeskanowanie komputera pod kątem obecności oprogramowania szpiegującego (za pomocą interfejsu skanera). Wykrywa ono również uśpione lub nieaktywne szkodliwe oprogramowanie, które zostało pobrane, ale jeszcze nie aktywowane.

7.2.2. Interfejs składnika Anti-Spyware



Interfejs składnika ***Anti-Spyware*** zawiera krótki opis jego funkcji, informację o bieżącym stanie oraz statystyki:

- ***Definicje oprogramowania szpiegującego*** — liczba sygnatur programów typu spyware zdefiniowanych w najnowszej wersji bazy danych.
- ***Wydanie bazy danych*** — data i godzina ostatniej aktualizacji bazy danych oprogramowania szpiegującego.
- ***Wersja bazy danych*** — numer ostatniej wersji bazy danych oprogramowania szpiegującego; numer ten rośnie przy każdej aktualizacji bazy wirusów.

Interfejs tego składnika zawiera tylko jeden przycisk (***Wstecz***) — kliknięcie go spowoduje powrót do domyślnego interfejsu użytkownika systemu AVG (*przeglądu składników*).

7.3. LinkScanner

7.3.1. Zasady działania technologii LinkScanner

Składnik ***LinkScanner*** zapewnia ochronę przed rosnącą liczbą zagrożeń internetowych. Zagrożenia te mogę być ukryte na stronie internetowej każdego typu (od stron rządowych przez witryny dużych i znanych marek, a kończąc na stronach małych firm). Rzadko kiedy pozostają tam dłużej niż 24 godziny. Składnik ***LinkScanner*** zapewnia nadzwyczaj skuteczną ochronę, skanując wszystkie linki znajdujące się na każdej przeglądanej stronie. Robi to dokładnie wtedy, gdy ma to największe znaczenie — zanim zdecydujesz się je kliknąć.

Technologia składnika ***LinkScanner*** składa się z dwóch funkcji: ***Search-Shield*** i ***Surf-Shield***:

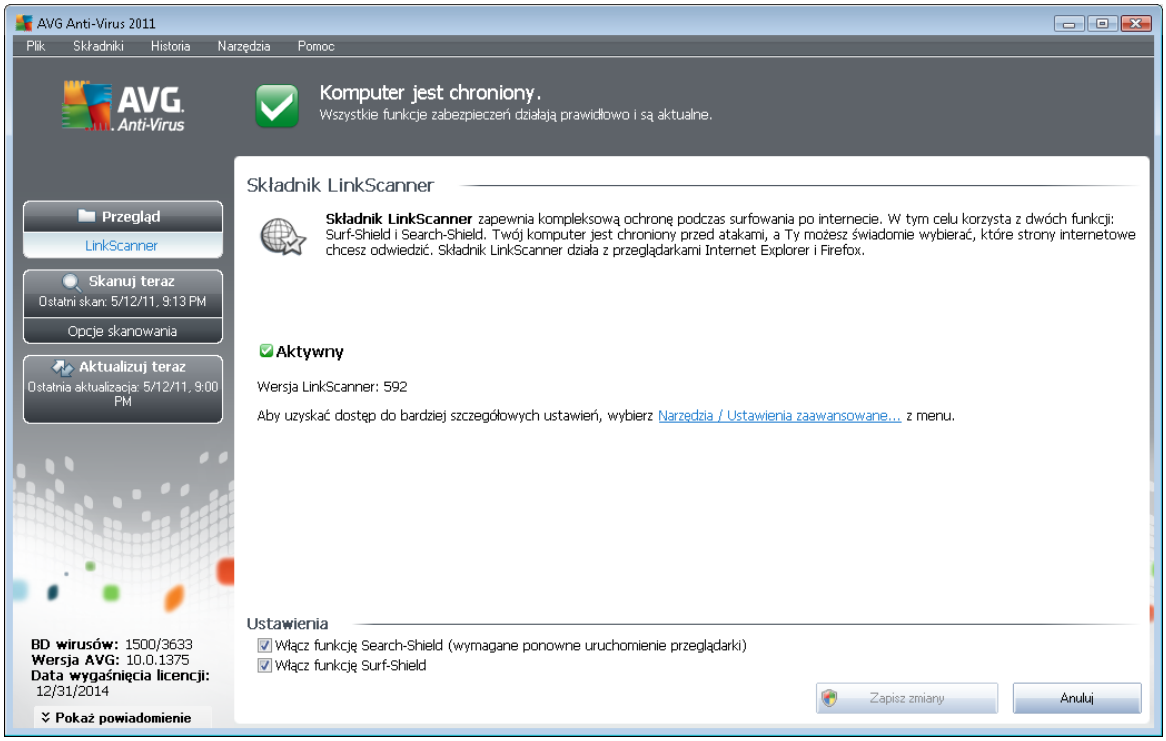
- Φυνκχφα ***Search-Shield*** wykorzystuje listę witryn internetowych (*adresów URL*), które zostały uznane za niebezpieczne. Na podstawie tej listy sprawdzane są wszystkie wyniki wyszukiwania zwracane przez serwisy Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg i SlashDot. Następnie obok każdego z nich wyświetlana jest odpowiednia ikona klasyfikacji bezpieczeństwa (*w przypadku wyników wyszukiwania serwisu Yahoo wyświetlana jest tylko ikona informująca o niebezpiecznej witrynie*).

- ***Funkcja Surf-Shield***skanuje zawartość odwiedzanych witryn internetowych bez względu na ich adres. Nawet jeśli jakaś witryna nie zostanie wykryta przez funkcję***Search-Shield*** (*np. gdy utworzono nową szkodliwą witrynę WWW lub witryna wcześniej uznana za nieszkodliwą zawiera aktualnie niebezpieczny kod*), przy próbie jej odwiedzenia przeprowadzone zostanie skanowanie, a w razie podejrzeń — zostanie ona zablokowana przez funkcję ***Surf-Shield***.

Uwaga: *Składnik LinkScanner nie jest przeznaczony dla platform serwerowych!*

7.3.2. Interfejs LinkScanner

Interfejs składnika ***LinkScanner*** zawiera krótki opis jego funkcji oraz informacje na temat bieżącego stanu. Ponadto można tam znaleźć informacje o numerze wersji najnowszej bazy danych ***LinkScanner*** (*Wersja składnika LinkScanner*).



Ustawienia składnika LinkScanner

W dolnej części okna dialogowego możliwa jest edycja następujących opcji:

- ***Włącz funkcję Search-Shield*** (*opcje domyślnie włączona*) — skanuje wszystkie łącza pojawiające się w wynikach wyszukiwania zwracanych przez serwisy Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg oraz SlashDot, a następnie obok każdego z nich wyświetla klasyfikację bezpieczeństwa.

- ***Włącz funkcję Surf-Shield*** (*domyślnie włączona*) — aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (*w czasie rzeczywistym*). Znane złośliwe witryny i ich niebezpieczna zawartość blokowane są już w momencie otwarcia ich przez użytkownika za pomocą przeglądarki (*lub jakiejkolwiek innej aplikacji korzystającej z protokołu HTTP*).

7.3.3. Search-Shield

Podczas przeszukiwania internetu z włączoną funkcją ***Search-Shield*** wszystkie wyniki zwracane przez najbardziej popularne wyszukiwarki internetowe, (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg i SlashDot*) są sprawdzane pod kątem niebezpiecznych i podejrzanych łączy. Sprawdzając linki i oznaczając odpowiednio te, które okazały się niebezpieczne, składnik ***AVG LinkScanner*** ostrzega przed przejściem do podejrzanej witryny. Dzięki temu można mieć pewność, że odwiedzane strony internetowe nie stanowią zagrożenia.

Obok ocenianego aktualnie wyniku wyszukiwania wyświetlany jest symbol informujący o trwającym skanowaniu łącza. Po zakończeniu skanowania wyświetlana jest ikona informująca o jego wynikach:

 Strona, do której prowadzi link jest bezpieczna (*ta ikona nie będzie wyświetlana dla bezpiecznych wyników wyszukiwania zwróconych przez serwis Yahoo! JP*).

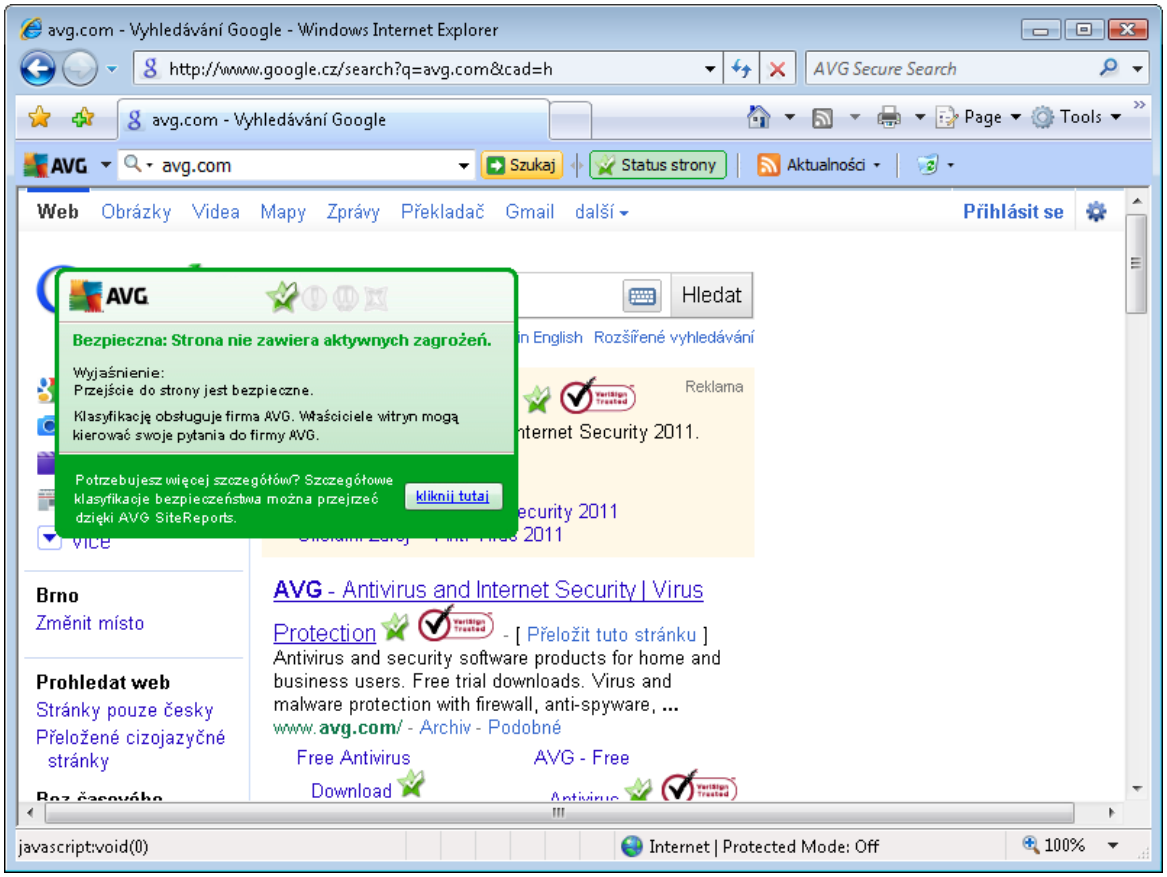
 Strona, do której prowadzi łącze, nie zawiera zagrożeń, ale jest podejrzana (*wątpliwości budzi jej pochodzenie lub przeznaczenie, więc nie zaleca się dokonywania na niej zakupów itp.*).

 Strona, do której prowadzi link, jest bezpieczna, ale zawiera linki do potencjalnie niebezpiecznych stron (lub podejrzany kod, który jednak nie stanowi bezpośredniego zagrożenia).

 Strona, do której prowadzi link, zawiera aktywne zagrożenia! Dla bezpieczeństwa użytkownika dostęp do tej strony zostanie zablokowany.

 Strona, do której prowadzi link, nie jest dostępna i nie udało się jej przeskanować.

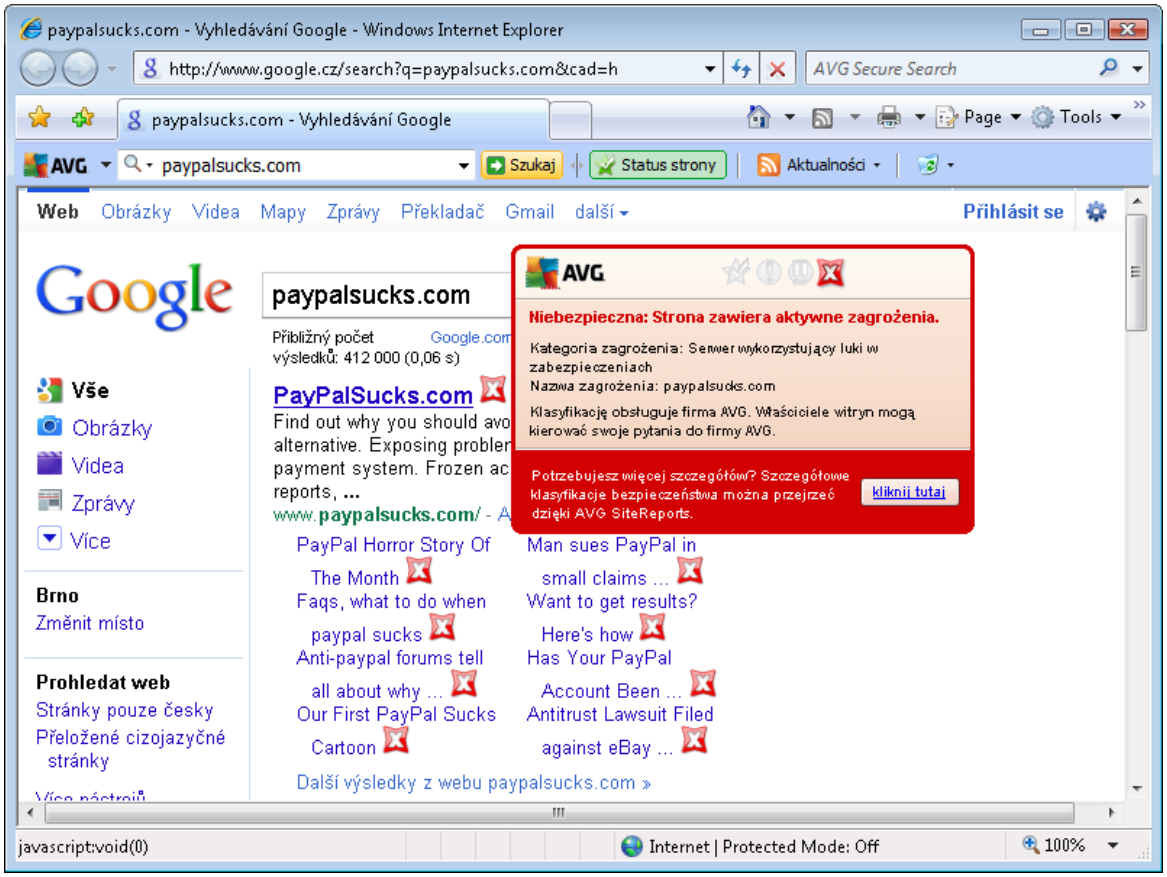
Umieszczenie kursora na wybranej ikonie wyników sprawdzania powoduje wyświetlenie szczegółowych informacji o danym łączu. Informacje te obejmują szczegóły zagrożenia (*o ile są one dostępne*):



7.3.4. Surf-Shield

Ta zaawansowana funkcja ochrony blokuje szkodliwą zawartość dowolnej otwieranej witryny internetowej, zapobiegając pobraniu jej na dysk twardy. Gdy jest ona włączona, kliknięcie jakiegokolwiek linku lub wpisanie adresu URL prowadzącego do niebezpiecznej witryny spowoduje automatyczne zablokowanie strony, dzięki czemu komputer nie zostanie nieświadomie zainfekowany. Należy pamiętać, że nawet samo wyświetlenie niebezpiecznej witryny internetowej może zainfekować komputer. Dlatego też, gdy zostanie wywołana strona zawierająca kod wykorzystujący luki zabezpieczeń lub inne poważne zagrożenia, składnik ***AVG Link Scanner*** nie pozwoli na jej wyświetlenia w przeglądarce.

Jeśli kiedykolwiek trafisz na szkodliwą stronę internetową, ***składnik Link Scanner*** wyświetli w przeglądarce ostrzeżenie podobne do tego:



Odwiedzanie takiej witryny jest bardzo ryzykowne i należy tego unikać!

7.4. Ochrona rezydentna

7.4.1. Zasady działania składnika Ochrona rezydentna

Składnik ***Ochrona rezydentna*** zapewnia stałą ochronę komputera. Skanuje on każdy otwierany, zapisywany lub kopiowany plik, a także chroni obszary systemowe komputera. Po wykryciu wirusa w przetwarzanym pliku ***Ochrona rezydentna*** zatrzymuje aktualnie wykonywane operacje i uniemożliwia uaktywnienie zagrożenia. Użytkownik zwykle nie zauważa działania tej ochrony, ponieważ funkcjonuje ona „w tle" i wyświetla powiadomienia tylko w przypadku, gdy wykryje zagrożenie. Domyślną reakcją ***Ochrony rezydentnej*** jest zablokowanie dostępu do niebezpiecznego pliku. Składnik ***Ochrona rezydentna*** jest ładowany do pamięci komputera podczas uruchamiania systemu.

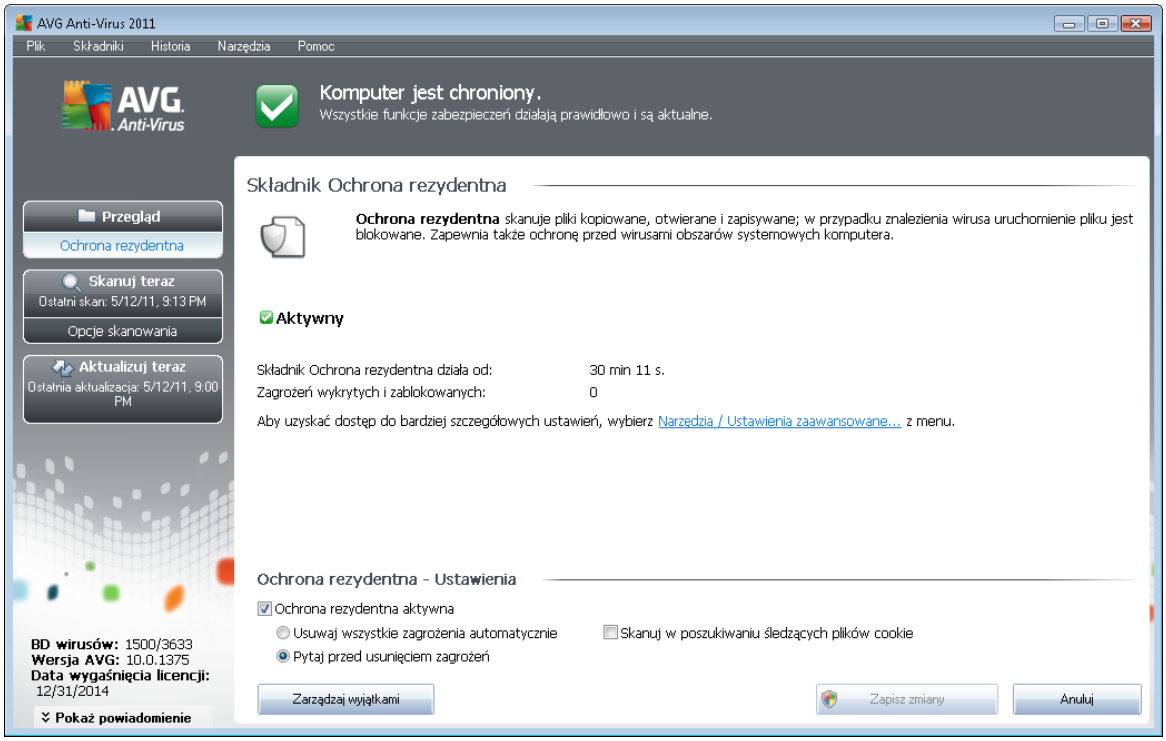
Wykonuje ona następujące zadania:

- skanuje w poszukiwaniu określonych typów potencjalnych zagrożeń,
- skanuje nośniki wymienne (*pamięci flash itp.*),

- skanuje pliki o określonych rozszerzeniach lub bez rozszerzenia,
- zezwala na określone wyjątki — pliki lub foldery, które nigdy nie mają być skanowane.

Ostrzeżenie: Ochrona rezydentna ładowana jest do pamięci komputera podczas uruchamiania systemu i musi pozostać włączona przez cały czas!

7.4.2. Interfejs składnika Ochrona rezydentna



Interfejs składnika ***Ochrona rezydentna*** zawiera informacje o funkcjach ***Ochrony rezydentnej***, i jej stanie, a także dane statystyczne:

- ***Ochrona rezydenta jest aktywna od*** — określa czas, jaki upłynął od ostatniego uruchomienia składnika.
- ***Zagrożenia wykryte i zablokowane*** — liczba wykrytych infekcji, do których uruchomienia/otwarcia nie dopuszczono (*w razie potrzeby, np. w celach statystycznych, ta wartość może zostać zresetowana*).

Ustawienia Ochrony rezydentnej

W dolnej części okna dialogowego znajduje się sekcja o nazwie ***Ustawienia Ochrony rezydentnej***, w której można edytować niektóre jej podstawowe funkcje (*szczegółowa konfiguracja, podobnie jak w wypadku innych składników, dostępna jest z poziomu menu Narzędzia/Ustawienia zaawansowane*).

Pole ***Ochrona rezydentna aktywna*** umożliwia łatwe włączanie/wyłączanie Ochrony rezydentnej. Domyślnie funkcja ta jest włączona. Gdy Ochrona rezydentna jest włączona, można określić w jaki sposób ma reagować na wykryte infekcje:

- automatycznie (***Usuwaj wszystkie zagrożenia automatycznie***)
- lub tylko za zgodą użytkownika (***Pytaj przed usunięciem zagrożeń***).

Wybór ten nie ma wpływu na poziom bezpieczeństwa — umożliwia on jedynie podjęcie każdorazowej decyzji o usunięciu lub pozostawieniu wykrytych infekcji.

W obu przypadkach można określić, czy pliki mają być ***skanowane w poszukiwaniu śledzących plików cookie***. W konkretnych przypadkach można włączyć tę opcję, aby osiągnąć najwyższy poziom ochrony, ale domyślnie jest ona wyłączona. (*pliki cookie to dane tekstowe wysyłane przez serwer do przeglądarki, która przy następnych odwiedzinach na danej stronie udostępni je serwerowi w celach identyfikacyjnych. Pliki cookie są używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencji dotyczących wyglądu witryny lub zawartości koszyka w sklepach internetowych*).

Uwaga: Dostawca oprogramowania AVG *skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego* ***Narzędzia / Ustawienia zaawansowane*** *i skorzystać z interfejsu Zaawansowane ustawienia AVG*.

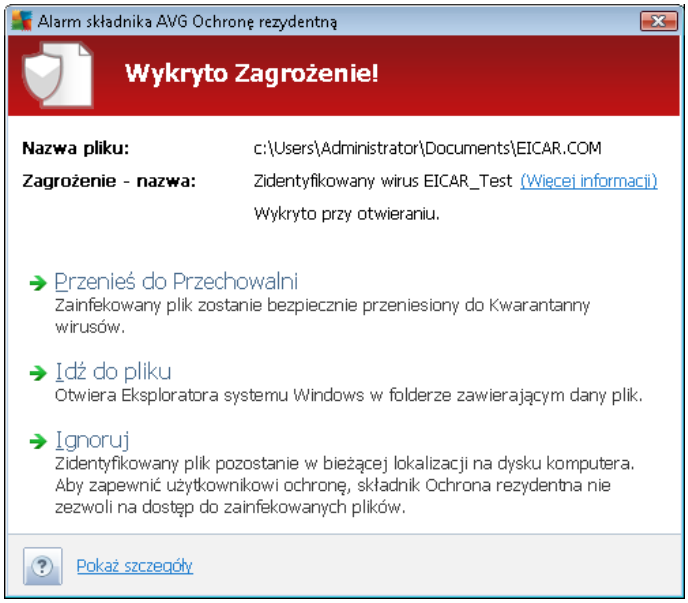
Przyciski kontrolne

W interfejsie składnika ***Ochrona rezydentna*** dostępne są następujące przyciski kontrolne:

- ***Zarządzaj wyjątkami*** — otwiera okno dialogowe ***Ochrona rezydentna — wykluczone obiekty***, w którym można zdefiniować foldery i pliki pomijane podczas skanowania przez składnik ***Ochrona rezydentna***.
- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- ***Anuluj*** — kliknięcie tego przycisku spowoduje powrót do domyślnego okna ***interfejsu użytkownika systemu AVG*** (*przegląd składników*).

7.4.3. Zagrożenia wykryte przez Ochronę rezydentną

Ochrona rezydentna to składnik służący do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego ostrzeżenia:



W tym oknie dialogowym będą wyświetlane ostrzeżenia dotyczące pliku wykrytego i oznaczonego jako zainfekowany (*Nazwa pliku*), nazwa rozpoznanej infekcji (*Nazwa zagrożenia*) i link do ***Encyklopedii wirusów***, w której można znaleźć szczegółowe informacje, jeśli są dostępne (*Więcej informacji*).

Następnie można zadecydować, jaka akcja ma zostać wykonana. Dostępne są następujące opcje.

Uwaga: w pewnych przypadkach nie wszystkie opcje są dostępne (zależy to od rodzaju zainfekowanego pliku oraz jego lokalizacji).

- ***Usuń zagrożenie jako użytkownik uprzywilejowany*** — to pole należy zaznaczyć w przypadku podejrzenia, że obecnie zalogowany użytkownik nie posiada wystarczających uprawnień do usunięcia danego pliku. Użytkownicy uprzywilejowani mają rozszerzone uprawnienia dostępu; zaznaczenie wspomnianego pola może być konieczne do pomyślnego usunięcia pliku w przypadku, gdy jest on zlokalizowany np. w folderze systemowym.

- ***Wylecz*** — ten przycisk jest wyświetlany tylko w przypadku, gdy wykrytą infekcję można wyleczyć. Zagrożenie jest wówczas usuwane z pliku, który zostanie przywrócony do pierwotnego stanu. Jeśli sam plik jest wirusem, ta funkcja umożliwia usunięcie go (*zostanie on przeniesiony do* ***Przechowalni wirusów***).

- ***Przenieś do Przechowalni*** — wirus zostanie przeniesiony do ***Przechowalni wirusów AVG***

- ***Przejdź do pliku*** — pozwala przejść do lokalizacji podejrzanego obiektu (*w nowym oknie Eksploratora Windows*)

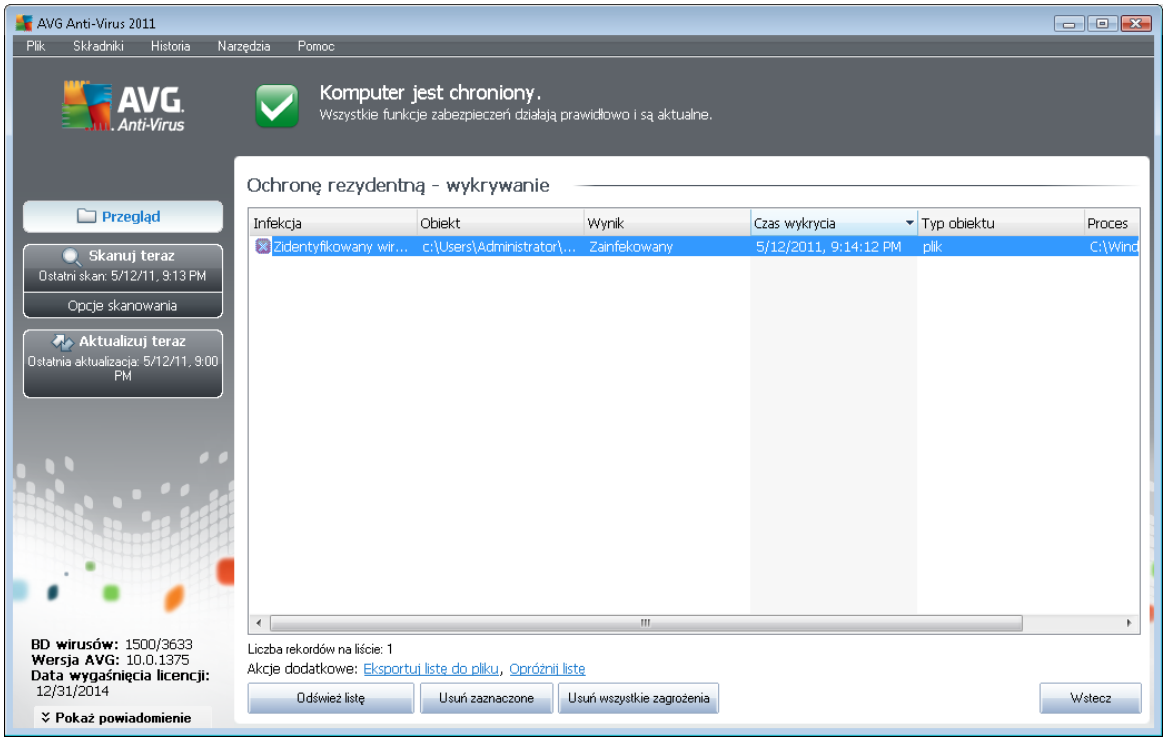
- ***Ignoruj*** — tej opcji NIE należy używać bez uzasadnionego powodu!

Uwaga: *Może się zdarzyć, że rozmiar wykrytego obiektu przekracza limit wolnego miejsca w Przechowalni wirusów. W takiej sytuacji w przypadku próby przeniesienia zainfekowanego obiektu*

do Przechowalni wirusów zostanie wyświetlony komunikat informujący o problemie. Istnieje jednak możliwość zmiany rozmiaru Przechowalni wirusów. Można to zrobić, określając dostępny procent rzeczywistego rozmiaru dysku twardego. Aby zwiększyć rozmiar Przechowalni wirusów, należy przejść do okna dialogowego Przechowalnia wirusów w sekcji Zaawansowane ustawienia AVG (rozmiaru Przechowalni wirusów).

W dolnej części tego okna dialogowego znajduje się link ***Pokaż szczegóły*** — kliknięcie go spowoduje otwarcie okna zawierającego szczegółowe informacje dotyczące procesu, który uruchomił infekcję.

Przegląd wszystkich zagrożeń wykrytych przez składnik ***Ochrona rezydentna*** można znaleźć w oknie dialogowym ***Zagrożenia wykryte przez Ochronę rezydentną*** dostępnym poprzez menu ***Historia / Zagrożenia wykryte przez Ochronę rezydentną***:



Okno ***Zagrożenia wykryte przez Ochronę rezydentną*** zawiera przegląd obiektów wykrytych i uznanych przez ten ***składnik*** za niebezpieczne (które następnie wyleczono lub przeniesiono do ***Przechowalni wirusów***). Podawane są tam następujące informacje:

- ***Infekcja***— opis (ewentualnie nazwa) wykrytego zagrożenia.
- ***Obiekt*** — lokalizacja obiektu.
- ***Wynik*** — działanie podjęte w związku z wykryciem.
- ***Czas wykrycia*** — data i godzina wykrycia obiektu.
- ***Typ obiektu*** — typ wykrytego obiektu.

- ***Proces*** — akcja wykonana w celu wywołania potencjalnie niebezpiecznego obiektu (co umożliwiło jego wykrycie).

U dołu okna znajdują się informacje na temat łącznej liczby wykrytych infekcji. Ponadto, można wyeksportować całą listę obiektów do pliku, (***Eksportuj listę do pliku***) lub usunąć wszystkie jej pozycje (***Opróżnij listę***). Przycisk ***Odśwież listę*** pozwala zaktualizować listę obiektów wykrytych przez ***Ochronę rezydentną***. Przycisk ***Wstecz*** przełącza z powrotem do domyślnego okna ***interfejsu użytkownika AVG*** *(przeglądu składników)*.

7.5. Bezpieczeństwo rodziny

Funkcja ***AVG Bezpieczeństwo rodziny*** pozwala chronić dzieci przed nieodpowiednią zawartością stron internetowych i wynikami wyszukiwania oraz umożliwia tworzenie raportów dotyczących ich aktywności online. Możesz ustawić odpowiedni poziom ochrony dla każdego dziecka i monitorować je oddzielnie przy użyciu unikatowych kont.

Składnik ten jest aktywny tylko wtedy, gdy na danym komputerze zainstalowany jest produkt ***AVG Bezpieczeństwo rodziny***. Jeśli produkt ***AVG Bezpieczeństwo rodziny*** nie jest zainstalowany, kliknij odpowiednią ikonę w interfejsie użytkownika systemu **AVG Anti-Virus 2011**. Nastąpi przekierowanie na stronę internetową produktu, na której można znaleźć wszystkie wymagane informacje.

7.6. AVG LiveKive

Program AVG LiveKive automatycznie tworzy kopie zapasowe wszystkich Twoich plików, zdjęć i muzyki w jednym bezpiecznym miejscu, pozwalając Ci dzielić się nimi z rodziną i przyjaciółmi oraz korzystać z nich na urządzeniach takich jak iPhone lub działających na systemie Android.

Składnik ten jest aktywny tylko wtedy, gdy na danym komputerze zainstalowany jest produkt ***AVG LiveKive***. Jeśli produkt ***AVG LiveKive*** nie jest zainstalowany, kliknij odpowiednią ikonę w interfejsie użytkownika systemu **AVG Anti-Virus 2011** . Nastąpi przekierowanie na stronę internetową produktu, na której można znaleźć wszystkie wymagane informacje.

7.7. Skaner poczty e-mail

Poczta e-mail to od dawna częste źródło wirusów i koni trojańskich. Wyłudzenia danych i spam powodują, że stała się ona jeszcze większym zagrożeniem. Darmowe konta pocztowe są szczególnie narażone na otrzymywanie szkodliwych wiadomości e-mail, *gdyż rzadko korzystają z technologii antyspamowych*, a domowi użytkownicy najczęściej używają właśnie takich kont. Dodatkowo odwiedzają oni nieznane witryny i wpisują w formularzach dane osobowe (*takie jak adres e-mail*), co powoduje, że w jeszcze większym stopniu narażają się na ataki za pośrednictwem poczty e-mail. Firmy używają na ogół komercyjnych kont pocztowych, które w celu ograniczenia ryzyka korzystają z filtrów antyspamowych i innych środków bezpieczeństwa.

7.7.1. Zasady działania Skanera poczty e-mail

Uniwersalny skaner poczty e-mail automatycznie skanuje przychodzące/wychodzące wiadomości e-mail. Można go używać z klientami poczty e-mail, które nie mają własnych pluginów AVG (*ale nie tylko*). Składnik ten jest przeznaczony głównie do użytku z aplikacjami takimi jak Outlook Express, Mozilla, Incredimail itp.

Podczas instalacji systemu AVG tworzone są automatyczne serwery kontrolujące pocztę e-mail: jeden do sprawdzania wiadomości przychodzących, drugi do wychodzących. Przy ich pomocy wiadomości e-mail są automatycznie sprawdzane na portach 110 i 25 (*standardowe porty wysyłania/ odbierania poczty e-mail*).

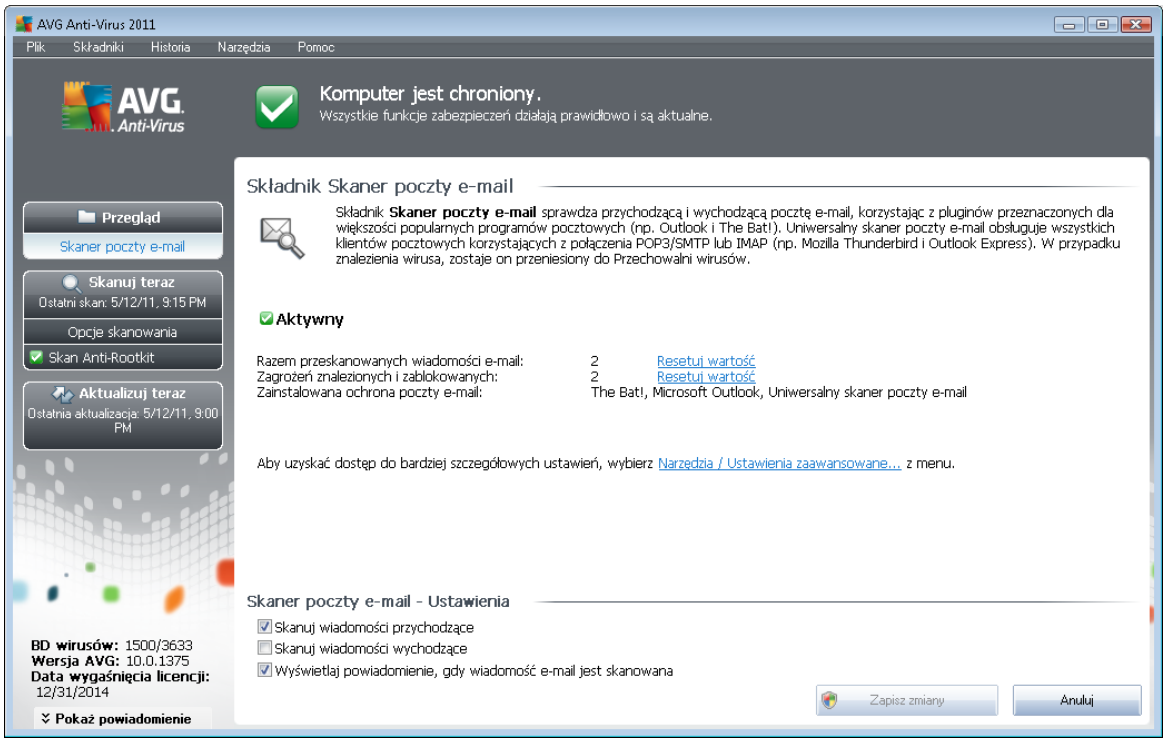
Skaner poczty e-mail pośredniczy między programem pocztowym a zewnętrznymi serwerami pocztowymi.

- ***Poczta przychodząca:*** Podczas otrzymywania wiadomości z serwera ***Skaner poczty e-mail*** sprawdza ją w poszukiwaniu wirusów, usuwa zainfekowane załączniki i dołącza certyfikat. Wykryte wirusy są natychmiast poddawane kwarantannie w ***Przechowalni wirusów***. Wiadomość jest później przekazywana do programu pocztowego.

- ***Poczta wychodząca:*** Wiadomość jest wysyłana z programu pocztowego do składnika Skaner poczty e-mail, gdzie jest sprawdzana wraz z załącznikami w poszukiwaniu wirusów. Następnie wiadomość jest wysyłana do serwera SMTP (*skanowanie wychodzących wiadomości e-mail jest domyślnie wyłączone i można je skonfigurować ręcznie*).

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

7.7.2. Interfejs Skanera poczty e-mail



Okno dialogowe składnika ***Skaner poczty e-mail*** zawiera krótki opis funkcji tego składnika, informacje o jego bieżącym stanie oraz następujące statystyki:

- ***Razem przeskanowanych wiadomości e-mail*** — liczba wiadomości e-mail przeskanowanych od czasu ostatniego uruchomienia składnika ***Skaner poczty e-mail*** (*w*

razie potrzeby ta wartość może zostać zresetowana, np. dla celów statystycznych — Resetuj wartość)

- ***Zagrożeń znalezionych i zablokowanych*** — liczba zainfekowanych wiadomości wykrytych od czasu ostatniego uruchomienia ***Skanera poczty e-mail***.
- ***Zainstalowany plugin poczty e-mail*** — informacje o pluginie odpowiednim dla Twojego domyślnego klienta poczty

Skanera poczty e-mail - Ustawienia

W dolnej części okna znajduje się sekcja ***Skaner poczty e-mail - Ustawienia*** , w której można skonfigurować podstawowe funkcje składnika:

- ***Skanuj wiadomości przychodzące*** — pozycję tę należy zaznaczyć, aby wszystkie wiadomości e-mail przychodzące na dane konto pocztowe były skanowane w poszukiwaniu wirusów. Domyślnie ta opcja jest włączona i nie zaleca się zmian w tych ustawieniach!
- ***Skanuj wiadomości wychodzące*** — zaznaczenie tej opcji pozwala określić, czy powinny być skanowane wszystkie wiadomości e-mail wysyłane z konta pocztowego. Opcja ta jest domyślnie wyłączona.
- ***Wyświetlaj powiadomienie, gdy wiadomość e-mail jest skanowana*** — tę pozycję należy zaznaczyć, jeśli nad ikoną AVG na pasku zadań ma być wyświetlane odpowiednie okno powiadomienia w chwili, gdy ***Skaner poczty e-mail*** skanuje wiadomość. Domyślnie ta opcja jest włączona i nie zaleca się zmian w tych ustawieniach!

Dostęp do zaawansowanej konfiguracji składnika ***Skaner poczty e-mail*** można uzyskać z poziomu menu ***Narzędzia / Ustawienia zaawansowane***. Wszelkie zmiany w konfiguracji powinny być wprowadzane wyłącznie przez doświadczonych użytkowników.

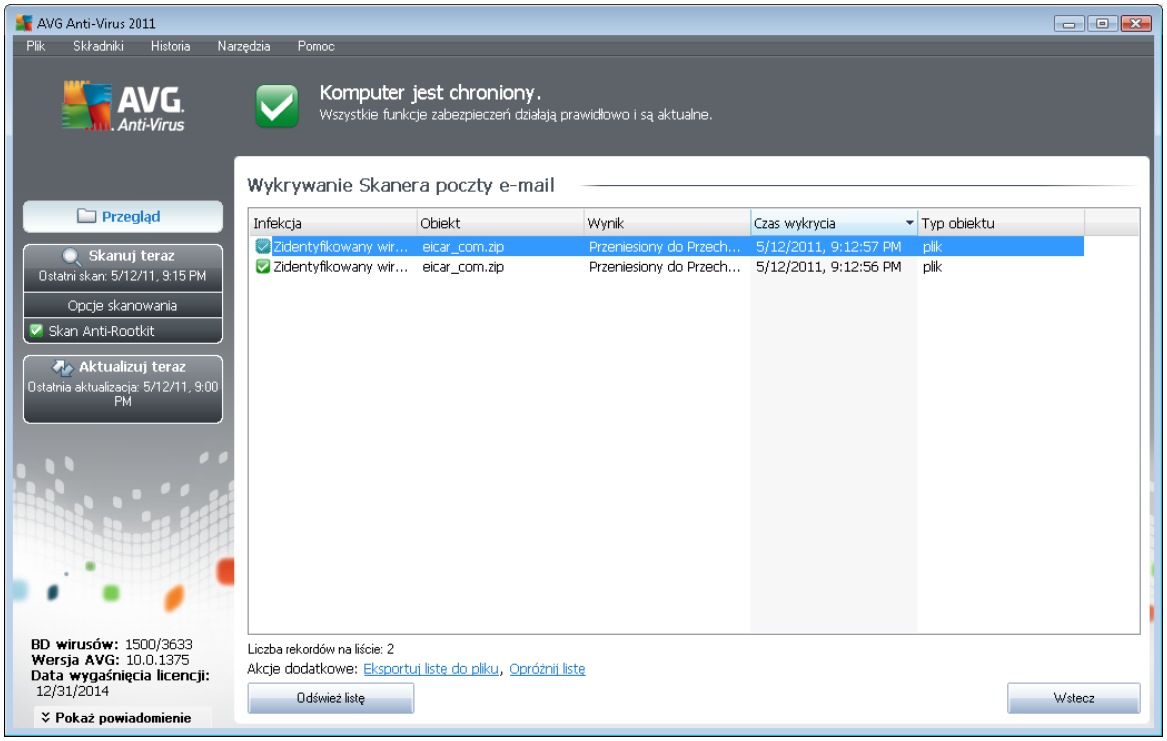
Uwaga: *Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego* ***Narzędzia / Ustawienia zaawansowane*** *i skorzystać z interfejsu Zaawansowane ustawienia AVG.*

Przyciski kontrolne

W interfejsie ***Skanera poczty e-mail*** dostępne są następujące przyciski kontrolne:

- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- ***Anuluj*** — kliknięcie tego przycisku spowoduje powrót do domyślnego okna ***interfejsu użytkownika systemu AVG*** (*przegląd składników*).

7.7.3. Zagrożenia wykryte przez Skaner poczty e-mail



W oknie dialogowym ***Zagrożenia wykryte przez Skaner poczty e-mail*** *(dostępnym po wybraniu odpowiedniej opcji z menu Historia*) wyświetlana jest lista wszystkich obiektów wykrytych przez składnik ***Skaner poczty e-mail***. Podawane są tam następujące informacje:

- ***Infekcja***— opis (ewentualnie nazwa) wykrytego zagrożenia.
- ***Obiekt*** — lokalizacja obiektu.
- ***Wynik*** — działanie podjęte w związku z wykryciem.
- ***Czas wykrycia*** — data i godzina wykrycia podejrzanego obiektu.
- ***Typ obiektu*** — typ wykrytego obiektu.

U dołu okna znajdują się informacje na temat łącznej liczby wykrytych infekcji. Ponadto, można wyeksportować całą listę obiektów do pliku, (***Eksportuj listę do pliku***) lub usunąć wszystkie jej pozycje (***Opróżnij listę***).

Przyciski kontrolne

W interfejsie składnika ***Skaner poczty e-mail*** dostępne są następujące przyciski sterujące:

- ***Odśwież listę*** — aktualizuje listę wykrytych zagrożeń.
- ***Wstecz*** — powoduje przejście z powrotem do poprzednio wyświetlanego okna

dialogowego.

7.8. Menedżer aktualizacji

7.8.1. Zasady działania Menedżera aktualizacji

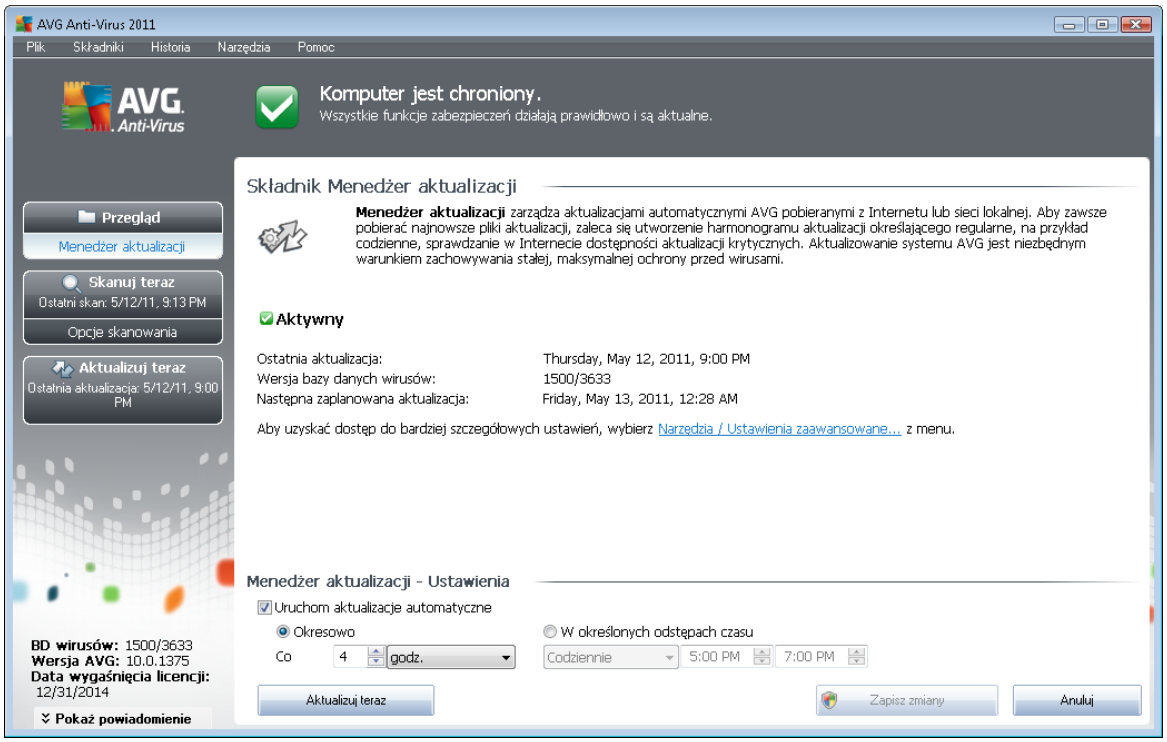
Żadne oprogramowanie zabezpieczające nie może zapewnić realnej ochrony przed różnymi typami zagrożeń bez regularnych aktualizacji. Twórcy wirusów nieustannie szukają nowych luk w programach i systemach operacyjnych, które mogliby wykorzystać. Nowe wirusy, szkodliwe oprogramowanie i metody ataków pojawiają się każdego dnia. Z tego powodu dostawcy oprogramowania na bieżąco wydają aktualizacje i poprawki zabezpieczeń, które mają usuwać wykryte luki.

Regularne aktualizacje systemu AVG są kluczowe dla Twojego bezpieczeństwa!

Pomaga w tym składnik ***Menedżer aktualizacji***. Za jego pomocą można zaplanować automatyczne pobieranie aktualizacji (z internetu lub sieci lokalnej). Jeśli jest to możliwe, definicje wirusów należy pobierać codziennie. Mniej istotne aktualizacje programu można pobierać co tydzień.

Uwaga: *Więcej informacji na temat typów i poziomów aktualizacji zawiera rozdział Aktualizacje systemu AVG.*

7.8.2. Interfejs Menedżera aktualizacji



Interfejs składnika ***Menedżer aktualizacji*** zawiera informacje o jego funkcjach i bieżącym stanie, a

także następujące statystyki:

- ***Ostatnia aktualizacja***data i godzina przeprowadzenia ostatniej aktualizacji baza danych.
- ***Wersja bazy danych wirusów*** — numer wersji aktualnie zainstalowanej bazy wirusów; numer ten jest zwiększany przy każdej aktualizacji bazy danych.
- ***Następna zaplanowana aktualizacja*** — data i godzina następnej zaplanowanej aktualizacji.

Menedżer aktualizacji - Ustawienia

W dolnej części okna dialogowego znajduje się sekcja ***ustawień Menedżera aktualizacji***, w której można wprowadzać zmiany reguł uruchamiania procesu aktualizacji. Można określić tam, czy pliki aktualizacyjne mają być pobierane automatycznie (***Uruchom aktualizacje automatyczne***), czy tylko na żądanie. Opcja ***Uruchom aktualizacje automatyczne*** jest włączona i zaleca się pozostawienie jej w tym stanie. Regularne pobieranie najnowszych aktualizacji ma kluczowe znaczenie dla prawidłowego funkcjonowania każdego oprogramowania zabezpieczającego!

Ponadto, można określić, kiedy aktualizacje mają być uruchamiane:

- ***Okresowo*** — należy zdefiniować interwał aktualizacji.
- ***W określonych odstępach czasu*** — należy określić dokładny czas uruchomienia aktualizacji.

Domyślny interwał aktualizacji to 4 godziny. Stanowczo nie zaleca się zmiany tych opcji bez uzasadnionej przyczyny!

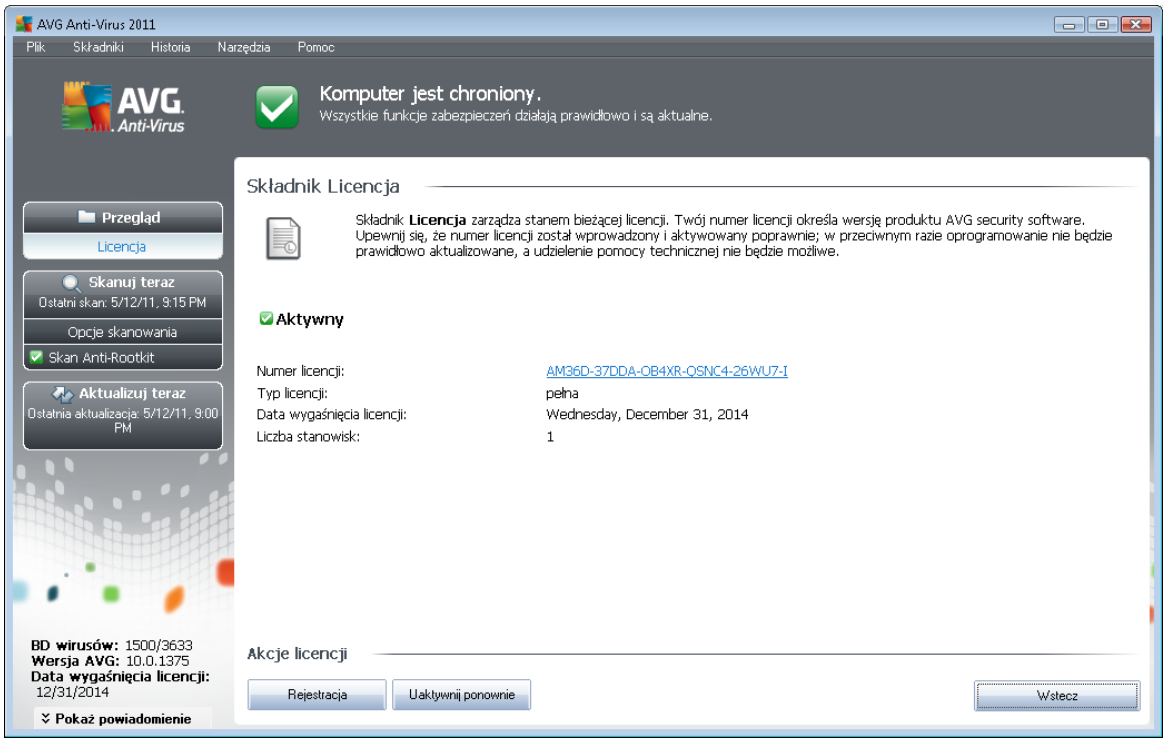
Uwaga: Dostawca oprogramowania AVG *skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego* ***Narzędzia / Ustawienia zaawansowane*** *i skorzystać z interfejsu Zaawansowane ustawienia AVG.*

Przyciski kontrolne

W interfejsie składnika ***Menedżer aktualizacji*** dostępne są następujące przyciski kontrolne:

- ***Aktualizuj teraz*** — kliknięcie przycisku uruchamia natychmiastową aktualizację na żądanie.
- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- ***Anuluj*** — kliknięcie tego przycisku spowoduje powrót do domyślnego okna ***interfejsu użytkownika systemu AVG*** (*przegląd składników*).

7.9. Licencja



Interfejs składnika ***Licencja*** zawiera krótki opis jego funkcji, informację o jego bieżącym stanie oraz następujące informacje:

- ***Numer licencji*** — skrócona forma numeru licencji (*ze względów bezpieczeństwa ostatnie cztery symbole są pominięte*). Jeżeli kiedykolwiek będziesz proszony o podanie swojego numeru licencji, użyj go w tej samej formie. Dlatego też zdecydowanie zalecamy korzystanie z metody Kopiuj/Wklej w przypadku jakiejkolwiek manipulacji numerem licencji.

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

- ***Data wygaśnięcia licencji*** — data określająca okres ważności licencji. Aby móc korzystać z systemu **AVG Anti-Virus 2011** po tej dacie, należy odnowić licencję. Licencję można odnowić online za pośrednictwem witryny firmy AVG.

- ***Liczba stanowisk*** — liczba stacji roboczych, na których można zainstalować system **AVG Anti-Virus 2011**.

Przyciski kontrolne

- ***Zarejestruj*** — łączy się ze stroną rejestracji w witrynie internetowej systemu AVG (http://www.avg.com/). Należy tam podać swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysługuje bezpłatna pomoc techniczna.

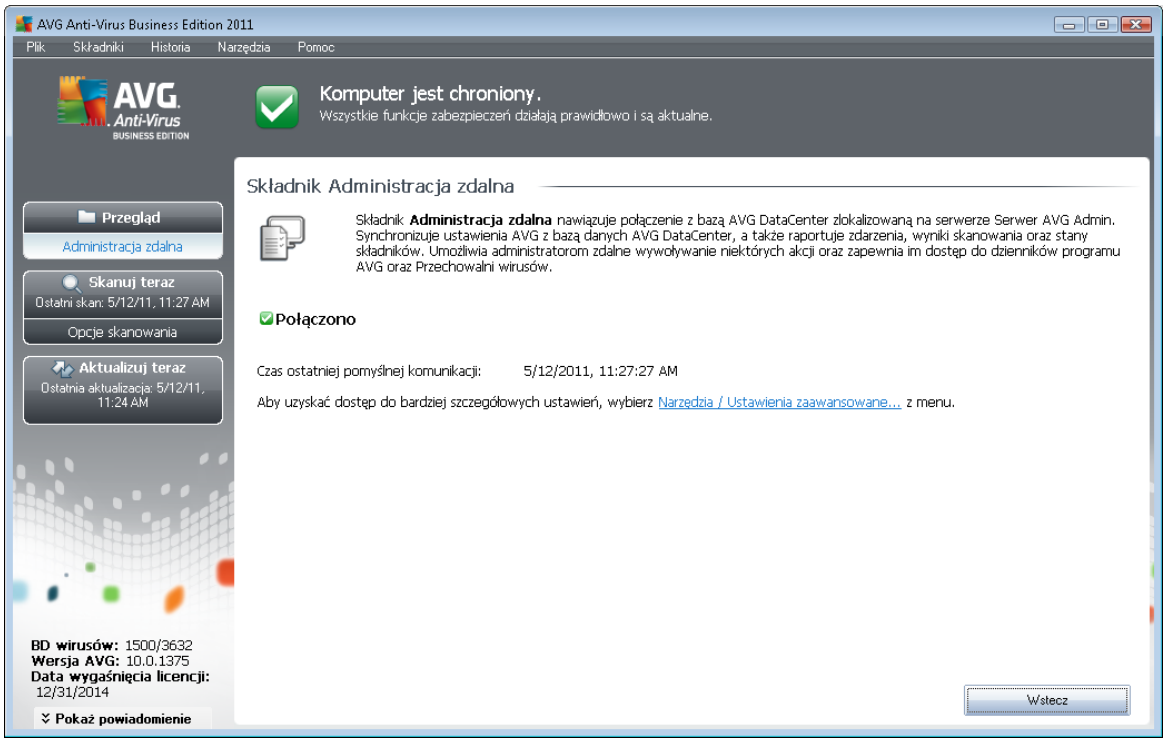
- ***Uaktywnij ponownie*** — otwiera okno dialogowe ***Aktywacja programu AVG*** zawierające

dane wprowadzone na etapie ***Personalizacji programu AVG*** podczas Instalacji. W oknie tym można wprowadzić numer licencji w celu zastąpienia numeru sprzedaży (*użytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przykład podczas uaktualnienia do nowego produktu AVG*).

Uwaga: W przypadku korzystania z próbnej wersji systemu *AVG Anti-Virus 2011* **dostępne przyciski to** *Kup teraz* ***i*** *Aktywuj. Umożliwiają one uaktualnienie programu do jego pełnej wersji. W przypadku systemu* **AVG Anti-Virus 2011** *zainstalowanego przy użyciu numeru sprzedaży, te przyciski to* ***Zarejestruj*** *i* ***Aktywuj***.

- ***Wstecz*** — kliknięcie tego przycisku powoduje powrót do domyślnego ***interfejsu użytkownika systemu AVG*** *(przeglądu składników)*.

7.10. Administracja zdalna



Składnik ***Administracja zdalna*** jest wyświetlany w interfejsie użytkownika systemu **AVG Anti-Virus 2011** tylko w przypadku, gdy została zainstalowana wersja biznesowa produktu AVG (*zobacz składnik* ***Licencja***). W oknie dialogowym składnika ***Administracja zdalna*** można znaleźć informacje o tym, czy składnik jest aktywny i połączony z serwerem. Wszystkie ustawienia składnika ***Administracja zdalna*** muszą zostać skonfigurowane w obszarze ***Ustawienia zaawansowane / Administracja zdalna***.

Szczegółowy opis opcji i funkcji Administracji zdalnej w systemie AVG można znaleźć dokumentacji poświęconej wyłącznie temu zagadnieniu. Dokumentacja ta jest dostępna na stronie internetowej AVG (www.avg.com), w sekcji ***Centrum pomocy technicznej / Pobierz dokumentację***.

Przyciski kontrolne

- ***Wstecz*** — kliknięcie tego przycisku powoduje powrót do domyślnego interfejsu użytkownika systemu AVG (*przeglądu składników*).

7.11. Ochrona Sieci

7.11.1. Zasady działania składnika Ochrona Sieci

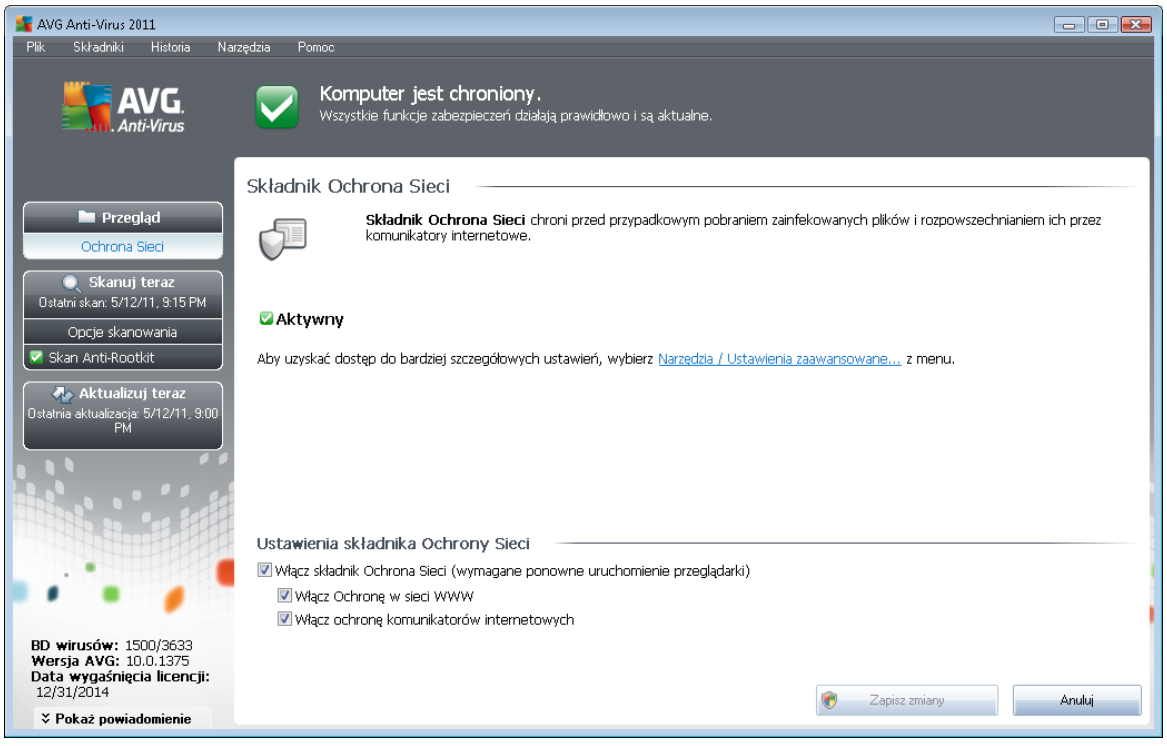
Ochrona Sieci to rodzaj programu rezydentnego, zapewniającego ochronę w czasie rzeczywistym. Składnik ten skanuje zawartość odwiedzanych stron internetowych (*oraz znajdujących się na nich plików*), jeszcze zanim zostaną załadowane przez przeglądarkę lub pobrane na dysk twardy.

Ochrona Sieci wykrywa strony zawierające niebezpieczny kod javascript i blokuje ich ładowanie. Ponadto, identyfikuje szkodliwe oprogramowanie zawarte na stronach WWW i w razie podejrzeń zatrzymuje pobieranie, aby nie dopuścić do infekcji komputera.

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

7.11.2. Interfejs składnika Ochrona Sieci

Interfejs składnika ***Ochrona Sieci*** opisuje działanie tego rodzaju ochrony. Ponadto można tu znaleźć informacje o bieżącym stanie składnika. W dolnej części okna dialogowego widoczne są podstawowe opcje tego składnika:



Ustawienia składnika Ochrona Sieci

Najistotniejsza opcja umożliwia natychmiastowe włączenie lub wyłączenie składnika ***Ochrona Sieci*** (można to zrobić, zaznaczając lub usuwając zaznaczenie pola ***Włącz Ochronę Sieci***). Opcja ta jest domyślnie włączona, a składnik ***Ochrona Sieci*** aktywny. Jednak jeśli nie istnieją ważne powody do zmiany tego ustawienia, zaleca się pozostawienie składnika aktywnego. Jeśli to pole jest zaznaczone, a składnik ***Ochrona Sieci*** jest włączony, na dwóch kolejnych kartach znajdują się dalsze opcje:

- ***Włącz Ochronę WWW*** — potwierdza, że ***Ochrona Sieci*** ma skanować zawartość stron WWW.
- ***Włącz ochronę komunikatorów internetowych*** — zaznacz tę pozycję, jeśli składnik ***Ochrona Sieci*** ma monitorować wymianę plików prowadzoną za pośrednictwem komunikatorów internetowych (*np. ICQ, MSN Messenger itp.*) pod kątem obecności wirusów.

Uwaga: Dostawca oprogramowania AVG *skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego* ***Narzędzia / Ustawienia zaawansowane*** *i skorzystać z interfejsu Zaawansowane ustawienia AVG*.

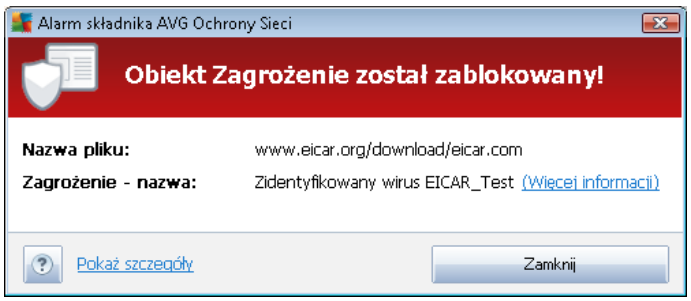
Przyciski kontrolne

W interfejsie składnika ***Ochrona rezydentna*** dostępne są następujące przyciski kontrolne:

- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- ***Anuluj*** — kliknięcie tego przycisku spowoduje powrót do domyślnego okna ***interfejsu użytkownika AVG*** (*przeglądu składników*).

7.11.3. Zagrożenia wykryte przez Ochronę Sieci

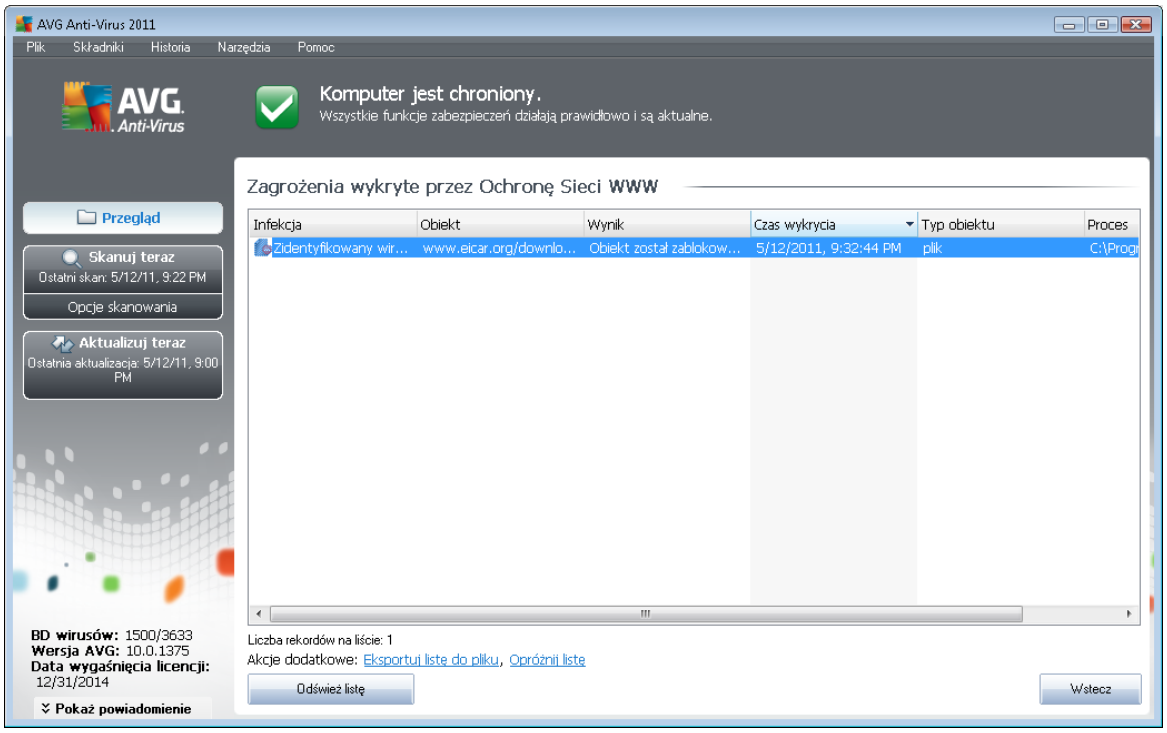
Ochrona Sieci skanuje zawartość odwiedzanych stron internetowych (oraz znajdujących się na nich plików) jeszcze zanim zostaną wyświetlone w przeglądarce lub pobrane na dysk twardy. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego okna:



W tym oknie dialogowym będą wyświetlane ostrzeżenia dotyczące pliku wykrytego i oznaczonego jako zainfekowany (*Nazwa pliku*), nazwa rozpoznanej infekcji (*Nazwa zagrożenia*) i link do ***Encyklopedii wirusów***, w której można znaleźć szczegółowe informacje, jeśli są dostępne (*Więcej informacji*). W oknie dialogowym dostępne są następujące przyciski:

- ***Pokaż szczegóły*** — kliknięcie przycisku ***Pokaż szczegóły*** spowoduje otwarcie nowego okna dialogowego, w którym można znaleźć informacje o procesie uruchomionym podczas wykrycia infekcji (np. jego identyfikator).
- ***Zamknij*** — kliknięcie tego przycisku spowoduje zamknięcie okna ostrzeżenia.

Podejrzana strona nie zostanie otwarta, a wykryty obiekt zostanie zapisany na liście ***zagrożeń wykrytych przez Ochronę Sieci*** (ten przegląd wykrytych zagrożeń jest dostępny z menu systemowego po wybraniu opcji ***Historia / Zagrożenia wykryte przez Ochronę Sieci***.



Podawane są tam następujące informacje:

- ***Infekcja***— opis (*ewentualnie nazwa*) wykrytego zagrożenia.
- ***Obiekt*** — źródło obiektu (*strona WWW*)
- ***Wynik*** — działanie podjęte w związku z wykryciem.
- ***Czas wykrycia*** — data i godzina wykrycia i zablokowania zagrożenia
- ***Typ obiektu*** — typ wykrytego obiektu.
- ***Proces*** — akcja wykonana w celu wywołania potencjalnie niebezpiecznego obiektu (co

umożliwiło jego wykrycie).

U dołu okna znajdują się informacje na temat łącznej liczby wykrytych infekcji. Ponadto, można wyeksportować całą listę obiektów do pliku, (***Eksportuj listę do pliku***) lub usunąć wszystkie jej pozycje (***Opróżnij listę***). Przycisk ***Odśwież listę*** pozwala zaktualizować listę obiektów wykrytych przez składnik ***Ochrona Sieci***. Przycisk ***Wstecz*** przełącza z powrotem do domyślnego okna ***interfejsu użytkownika AVG*** *(przeglądu składników)*.

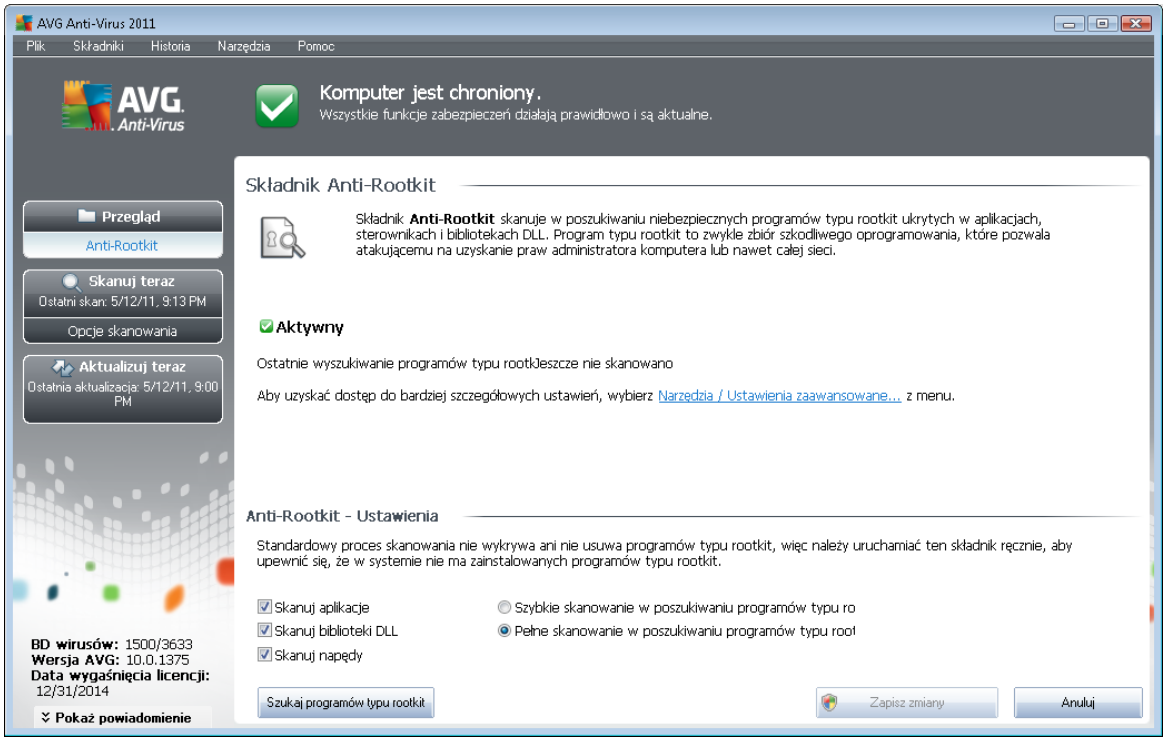
7.12. Anti-Rootkit

Program typu rootkit to aplikacja zaprojektowana w celu przejęcia całkowitej kontroli nad systemem komputerowym bez zgody jego właścicieli czy upoważnionych administratorów. Bezpośredni dostęp do sprzętu jest rzadko wymagany, ponieważ programy typu rootkit w pełni zdalnie kontrolują system operacyjny komputera. Zwykle ukrywają one swoją obecność poprzez przejęcie kontroli nad standardowymi mechanizmami bezpieczeństwa systemu operacyjnego. Wiele z nich jest jednocześnie końmi trojańskimi, które dodatkowo starają się przekonać użytkowników, że ich systemy są bezpieczne. Techniki stosowane przez programy typu rootkit to m.in. ukrywanie uruchomionych procesów przed programami monitorującymi oraz ukrywanie plików lub danych przed samym systemem operacyjnym.

7.12.1. Zasady działania składnika Anti-Rootkit

AVG Anti-Rootkit to specjalistyczne narzędzie do wykrywania i skutecznego usuwania niebezpiecznych programów typu rootkit, wykorzystujących technologie, które mogą kamuflować obecność innego szkodliwego oprogramowania na komputerze. Składnik ***AVG Anti-Rootkit*** umożliwia wykrywanie programów typu rootkit na podstawie wstępnie zdefiniowanego zestawu reguł. Należy zwrócić uwagę na fakt, że wykrywane są wszystkie programy typu rootkit (*nie tylko te szkodliwe*). Jeśli składnik ***AVG Anti-Rootkit*** wykrywa program typu rootkit, nie znaczy to jeszcze, że ten program jest szkodliwy. Niekiedy programy typu rootkit są używane jako sterowniki lub jako komponenty innych, pożytecznych aplikacji.

7.12.2. Interfejs składnika Anti-Rootkit



Interfejs użytkownika składnika ***Anti-Rootkit*** udostępnia krótki opis funkcji tego składnika, informacje o jego bieżącym stanie oraz o ostatnim uruchomionym teście ***Anti-Rootkit***. W oknie dialogowym ***Anti-Rootkit*** dostępny jest również link ***Narzędzia / Ustawienia zaawansowane***. Za jego pomocą można uzyskać dostęp do zaawansowanej konfiguracji składnika ***Anti-Rootkit***.

Uwaga: *Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany ustawień powinny być wprowadzane wyłącznie przez doświadczonych użytkowników.*

Anti-Rootkit — Ustawienia

W dolnej części okna znajduje się sekcja ***ustawień składnika Anti-Rootkit***, w której skonfigurować można podstawowe funkcje skanowania w poszukiwaniu programów typu rootkit. W pierwszej kolejności należy zaznaczyć odpowiednie pola wyboru, aby określić obiekty, które mają być skanowane:

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

Następnie należy wybrać tryb skanowania w poszukiwaniu programu typu rootkit:

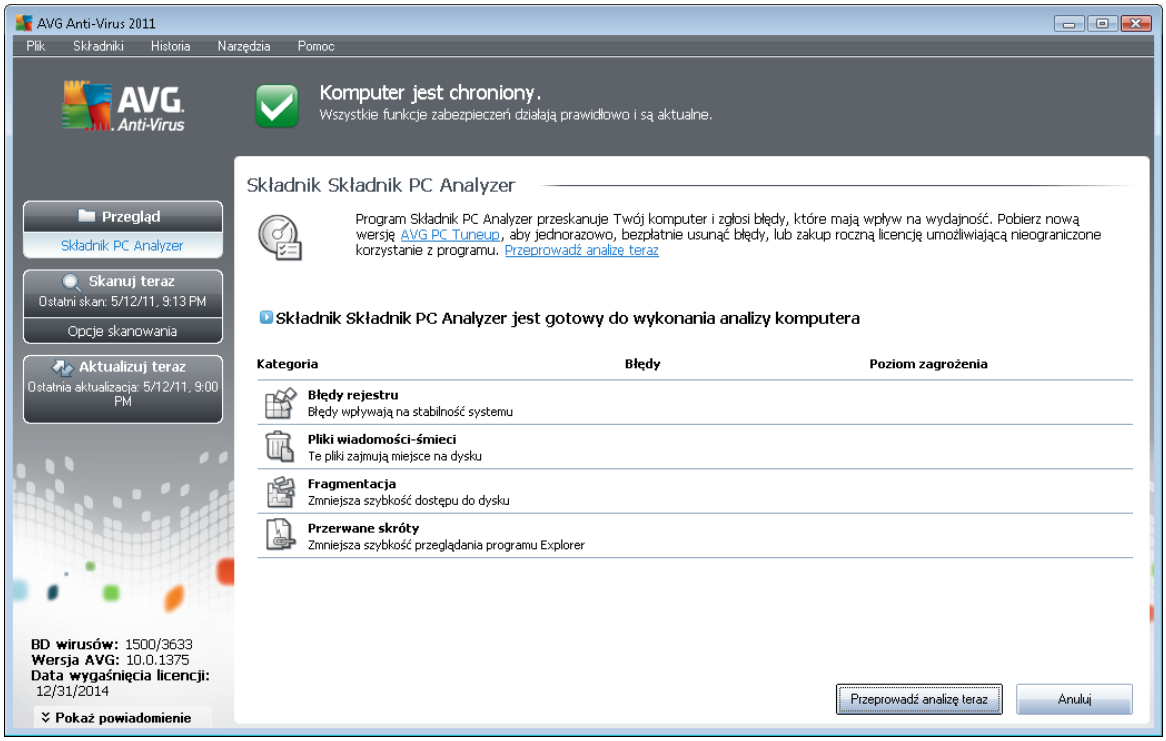
- ***Szybkie skanowanie w poszukiwaniu programów typu rootkit*** — skanuje wszystkie uruchomione procesy, załadowane sterowniki i folder systemowy (*zazwyczaj c:\Windows*)
- ***Pełne skanowanie w poszukiwaniu programów typu rootkit*** — skanuje wszystkie uruchomione procesy, załadowane sterowniki i folder systemowy (*zazwyczaj c:\Windows*) oraz wszystkie dyski lokalne (*w tym dyski flash, ale bez uwzględnienia napędów dyskietek/ płyt CD*)

Przyciski kontrolne

- ***Szukaj programów typu rootkit*** — ponieważ skanowanie w poszukiwaniu programów typu rootkit nie jest częścią testu ***Skan całego komputera***, można je uruchomić bezpośrednio z interfejsu składnika ***Anti-Rootkit***, klikając ten przycisk.
- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisać wszystkie zmiany wprowadzone w danym oknie i powrócić do domyślnego ***interfejsu użytkownika AVG*** (*przeglądu składników*).
- ***Anuluj*** — kliknięcie tego przycisku pozwala powrócić do domyślnego ***interfejsu użytkownika AVG*** (*przeglądu składników*) bez zapisywania wprowadzonych zmian.

7.13. PC Analyzer

Składnik ***PC Analyzer*** skanuje komputer pod kątem problemów systemowych i zapewnia przejrzysty przegląd czynników, które mogą pogarszać ogólną wydajność komputera. W interfejsie użytkownika tego składnika jest wyświetlany wykres podzielony na cztery wiersze, odpowiadające następującym kategoriom: Błędy rejestru, Pliki-śmieci, Fragmentacja i Błędne skróty:



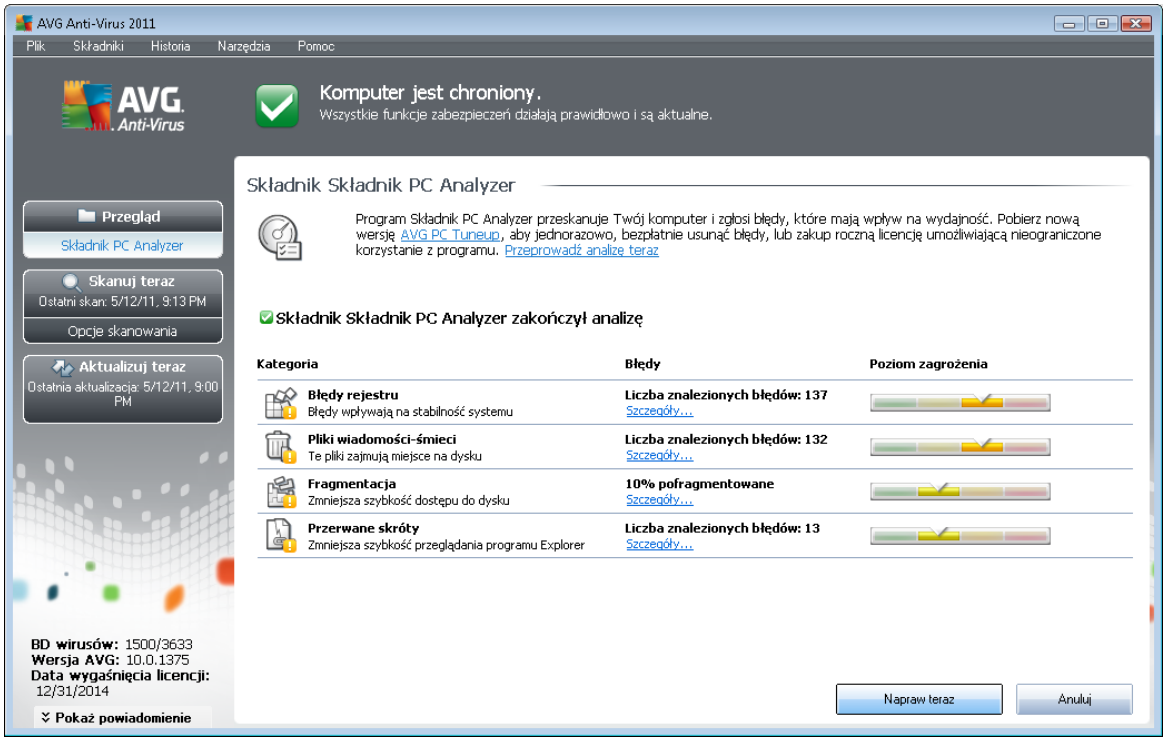
- ***Błędy rejestru*** — podaje informację o liczbie błędów w rejestrze systemu Windows. Naprawa rejestru wymaga zaawansowanej wiedzy, dlatego nie jest zalecane przeprowadzanie jej samodzielnie.

- ***Pliki-śmieci*** — informuje o liczbie niepotrzebnych plików. Zazwyczaj są to różnego rodzaju pliki tymczasowe oraz pliki znajdujące się w Koszu.

- ***Fragmentacja*** — umożliwia obliczenie procentowego stopnia fragmentacji danych na dysku twardym (po upływie dłuższego czasu wiele plików może być rozproszonych w różnych miejscach dysku fizycznego). W celu naprawienia tego problemu można użyć narzędzia do defragmentacji.

- ***Błędne skróty*** — powiadamia o niedziałających skrótach prowadzących do nieistniejących lokalizacji itd.

Aby uruchomić analizę systemu, kliknij przycisk ***Analizuj teraz***. Postęp analizy oraz jej wyniki będzie można obserwować bezpośrednio na wykresie:



W podglądzie wyników wyświetlana będzie liczba wykrytych problemów systemowych (pozycja ***Błędy***) z podziałem na odpowiednie kategorie sprawdzane podczas analizy. Wyniki analizy będą również wyświetlane w postaci graficznej na osi w kolumnie ***Poziom zagrożenia***.

Przyciski kontrolne

- ***Analizuj teraz*** (*wyświetlany przed uruchomieniem analizy*) — kliknięcie tego przycisku umożliwia uruchomienie natychmiastowej analizy komputera.
- ***Napraw teraz*** (*wyświetlany po zakończeniu analizy*) — kliknięcie tego przycisku umożliwia przejście do witryny AVG (http://www.avg.com/) na stronę udostępniającą szczegółowe i aktualne informacje dotyczące składnika ***PC Analyzer***.
- ***Anuluj*** — kliknięcie tego przycisku umożliwia zatrzymanie uruchomionej analizy lub powrót do domyślnego interfejsu użytkownika systemu AVG (*przeglądu składników*) po zakończeniu analizy.

7.14. Składnik ID Protection

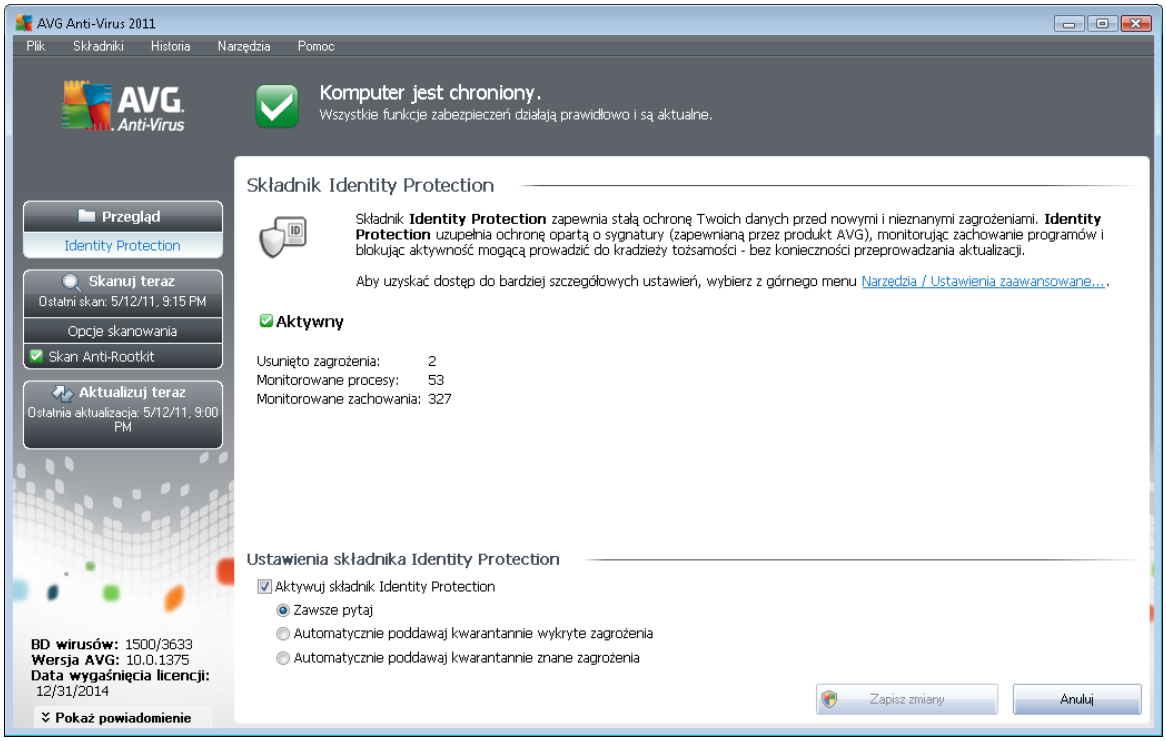
AVG Identity Protection to program chroniący przed szkodliwym oprogramowaniem; jego głównym zadaniem jest zapobieganie kradzieżom haseł, rachunków bankowych, numerów kart kredytowych i innych cennych danych przez oprogramowanie typu *malware*. Gwarantuje on, że wszystkie programy uruchomione na komputerze działają prawidłowo. ***AVG Identity Protection*** wykrywa i blokuje podejrzane zachowanie (dzięki stałemu nadzorowi), a także chroni komputer przed nowym szkodliwym oprogramowaniem.

7.14.1. Podstawy działania ID Protection

Składnik AVG Identity Protection służy do ochrony przed szkodliwym oprogramowaniem, zapewniając ochronę przed wszystkimi jego rodzajami (*jak np. programami szpiegującymi, botami, kradzieżami tożsamości itp.*), używając technologii behawioralnych. Ponieważ szkodliwe oprogramowanie jest coraz bardziej zaawansowane i przybiera postać zwykłych programów, które mogą jednak narazić komputer na zdalny atak w celu kradzieży tożsamości, składnik ***AVG Identity Protection*** zapewnia ochronę przed wszystkimi podejrzanymi aplikacjami. Aplikacja dopełnia ochronę zapewnianą przez składnik ***AVG Anti-Virus***, który zabezpiecza przed znanymi wirusami, korzystając z mechanizmu skanowania i analizy sygnatur.

Stanowczo zalecamy zainstalowanie zarówno składnika AVG Anti-Virus, jak i AVG Identity Protection. Razem zapewniają one kompleksową ochronę komputera.

7.14.2. Interfejs składnika ID Protection



Interfejs składnika ***Identity Protection*** zawiera krótki opis jego podstawowych funkcji, informacje o stanie oraz podstawowe dane statystyczne:

- ***Usunięte szkodliwe oprogramowanie*** — zawiera liczbę aplikacji wykrytych jako szkodliwe oprogramowanie (a następnie usuniętych)
- ***Monitorowane procesy*** — liczba obecnie uruchomionych aplikacji, które są monitorowane przez składnik IDP
- ***Monitorowane zachowania*** — liczba określonych czynności uruchomionych w monitorowanych aplikacjach

Ustawienia składnika Identity Protection

W dolnej części okna dialogowego znajduje się sekcja ***Ustawienia składnika Identity Protection***, w której można skonfigurować jego podstawowe funkcje:

- ***Aktywuj składnik Identity Protection*** (*opcja domyślnie włączona*) — należy zaznaczyć to pole, aby aktywować składnik Identity Protection i otworzyć dalsze opcje.

W pewnych przypadkach składnik ***Identity Protection*** może zgłosić, że plik pochodzący z zaufanego źródła jest podejrzany lub niebezpieczny. Ponieważ składnik ***Identity Protection*** wykrywa zagrożenia na podstawie zachowania, takie zdarzenie ma zazwyczaj miejsce, gdy jakiś program próbuje przechwytywać sekwencje klawiszy, instalować inne programy lub gdy na komputerze instalowany jest nowy sterownik. Dlatego też należy wybrać jedną z poniższych opcji, aby określić zachowanie składnika ***Identity Protection*** w przypadku wykrycia podejrzanej aktywności:

  - ***Zawsze monituj*** — jeśli aplikacja zostanie wykryta jako szkodliwe oprogramowanie, użytkownik zostanie zapytany, czy ma ona zostać zablokowana (*ta opcja jest domyślnie włączona i zaleca się niezmienianie tego bez ważnego powodu*)
  - ***Automatycznie poddawaj kwarantannie wykryte zagrożenia*** — wszystkie aplikacje uznane za szkodliwe będą automatycznie blokowane
  - ***Automatycznie poddawaj kwarantannie znane zagrożenia*** — tylko aplikacje, które z całą pewnością zostały wykryte jako szkodliwe oprogramowanie, będą blokowane

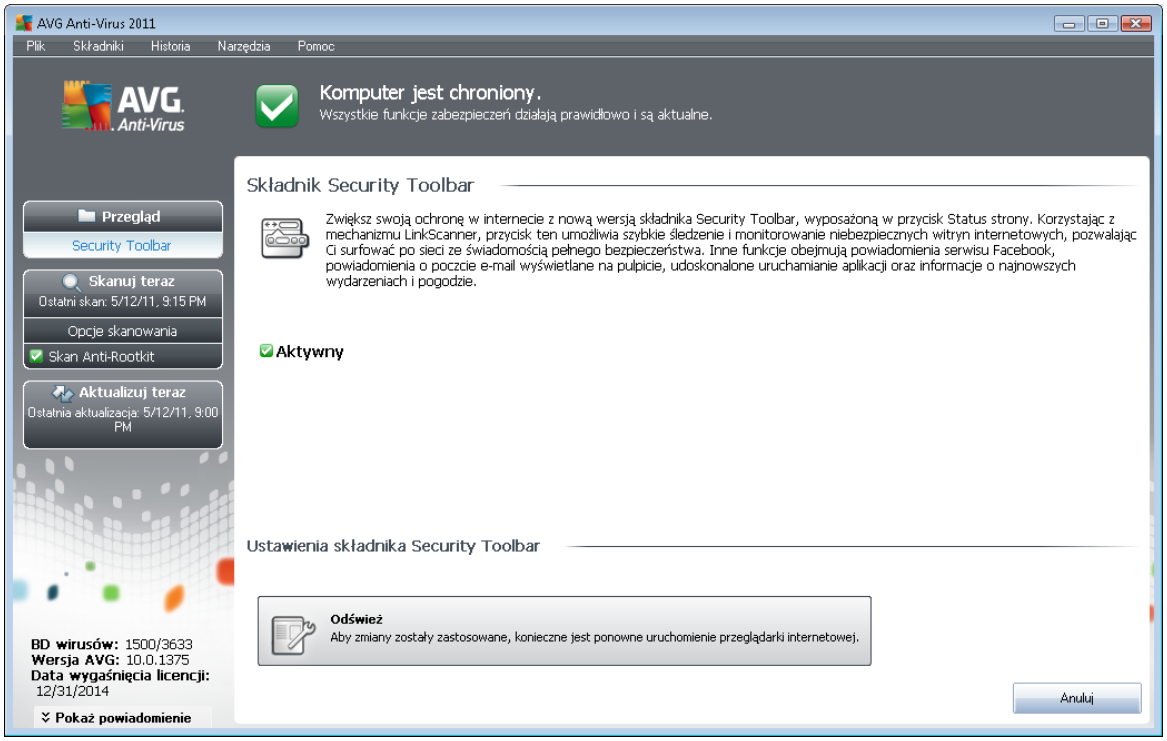
Przyciski kontrolne

W interfejsie składnika ***Identity Protection*** są dostępne następujące przyciski sterujące:

- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- ***Anuluj*** — kliknięcie tego przycisku spowoduje powrót do domyślnego okna ***interfejsu użytkownika systemu AVG*** (*przegląd składników*).

7.15. Pasek narzędzi zabezpieczeń

Pasek narzędzi Security Toolbar jest opcjonalnym paskiem narzędzi przeglądarki internetowej, który oferuje udoskonaloną ochronę AVG oraz różne inne funkcje i narzędzia przydatne podczas przeglądania zasobów internetu. Obecnie pasek narzędzi***Security Toolbar*** jest obsługiwany przez przeglądarki Internet Explorer (*w wersji 6.0 lub nowszej)* i Mozilla Firefox *(w wersji 3.0 lub nowszej*):



Z paska narzędzi ***Security Toolbar*** w oknie przeglądarki internetowej można uzyskać bezpośredni dostęp do wszystkich ***jego*** opcji.

8. Pasek narzędzi AVG Security Toolbar

AVG Security Toolbar to nowe narzędzie współpracujące ze składnikiem ***LinkScanner.*** Pasek narzędzi ***AVG Security Toolbar*** może służyć do sterowania funkcjami składnika ***LinkScanner.***

Jeśli podczas instalacji systemu **AVG Anti-Virus 2011** zostanie wybrana również instalacja paska narzędzi, zostanie on automatycznie dodany do przeglądarki (*Internet Explorer 6.0 lub nowsza, Mozilla Firefox 3.0 lub nowsza*). W tym momencie nie są obsługiwane inne przeglądarki internetowe.

Uwaga: *W przypadku korzystania z alternatywnej przeglądarki internetowej (np. Avant Browser) mogą wystąpić nieoczekiwane zachowania.*

8.1. Interfejs paska narzędzi AVG Security Toolbar

Pasek narzędzi ***AVG Security Toolbar*** współpracuje z przeglądarkami ***MS Internet Explorer*** (*w wersji 6.0 lub nowszej*) i ***Mozilla Firefox*** (*w wersji 3.0 lub nowszej*). Po podjęciu decyzji o zainstalowaniu paska narzędzi ***AVG Security Toolbar*** (*pytanie to padło podczas procesu instalacji systemu AVG*), zostanie on umieszczony pod paskiem adresu w oknie przeglądarki:

AVG Security Toolbar składa się z następujących elementów:

8.1.1. Przycisk logo AVG

Ten przycisk pozwala uzyskać dostęp do głównych elementów paska narzędzi. Kliknięcie przycisku logo spowoduje przejście do witryny systemu AVG. Kliknięcie strzałki obok ikony AVG powoduje otwarcie menu z następującymi opcjami:

- ***Informacje o pasku narzędzi*** — link do strony głównej składnika ***AVG Security Toolbar***, zawierającej szczegółowe informacje o działaniu paska narzędzi.
- ***Uruchom AVG*** — powoduje otwarcie interfejsu użytkownika systemu **AVG Anti-Virus 2011**.
- ***System AVG — informacje*** — otwiera menu kontekstowe z linkami prowadzącymi do ważnych informacji o bezpieczeństwie i systemie **AVG Anti-Virus 2011**:
  - *Informacje o zagrożeniach* — otwiera witrynę internetową AVG na stronie zawierającej najważniejsze dane dotyczące najistotniejszych zagrożeń, zalecenia dotyczące usuwania wirusów, informacje o aktualizacjach systemu AVG, oraz bazę wirusów.
  - *Nowości AVG* — otwiera stronę internetową zawierającą najnowsze informacje prasowe dotyczące systemu AVG.
  - *Obecny poziom zagrożenia* — otwiera stronę internetową laboratorium wirusów,

która zawiera graficzną reprezentację obecnego poziomu zagrożeń w sieci.

- *Laboratoria AVG Threat Labs* — otwiera stronę WWW AVG, na której można wyszukać określone zagrożenia na podstawie ich nazw i uzyskać szczegółowe informacje o każdym z nich.

- ***Opcje*** — powoduje otwarcie okna dialogowego, w którym można modyfikować ustawienia paska narzędzi ***AVG Security Toolbar*** — patrz rozdział ***Opcje paska narzędzi AVG Security Toolbar***

- ***Usuń historię*** — pozwala użyć paska narzędzi ***AVG Security Toolbar*** w celu usunięcia całej historii (albo osobno historii wyszukiwania, historii przeglądarki, historii pobierania lub plików cookie).

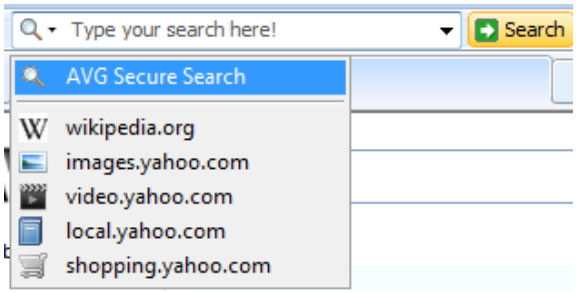
- ***Aktualizacja*** — pozwala sprawdzić dostępność nowych aktualizacji ***paska narzędzi AVG Security Toolbar***

- ***Pomoc*** — pozwala znaleźć odpowiednie pliki pomocy, skontaktować się z pomocą techniczną AVG, wysłać opinię dotyczącą produktu lub wyświetlić szczegóły dotyczące bieżącej wersji paska narzędzi.

8.1.2. Pole wyszukiwarki AVG Secure Search (powered by Google)

Pole wyszukiwarki ***AVG Secure Search (powered by Google)*** to łatwy i bezpieczny sposób na przeszukiwanie sieci za pomocą serwisu AVG Secure Search (powered by Google). Wprowadź słowo lub wyrażenie w polu wyszukiwania i kliknij przycisk ***Wyszukaj*** lub naciśnij klawisz ***Enter*** , aby rozpocząć bezpośrednie wyszukiwanie za pomocą serwisu AVG Secure Search (powered by Google) — niezależnie od tego, jaką stronę w danej chwili odwiedzasz. Wspomniane pole zawiera także historię poprzednich wyszukiwań. Wyszukiwania uruchamiane z poziomu tego pola są analizowane przez funkcje ***AVG Search-Shield***.

Pole wyszukiwarki można również przełączyć w tryb Wikipedii lub innych usług:



8.1.3. Status strony

Ten przycisk Paska narzędzi AVG wyświetla ocenę aktualnie wyświetlanej strony WWW na podstawie kryteriów funkcji ***AVG Surf-Shield***.

- — Strona, do której prowadzi link, jest bezpieczna

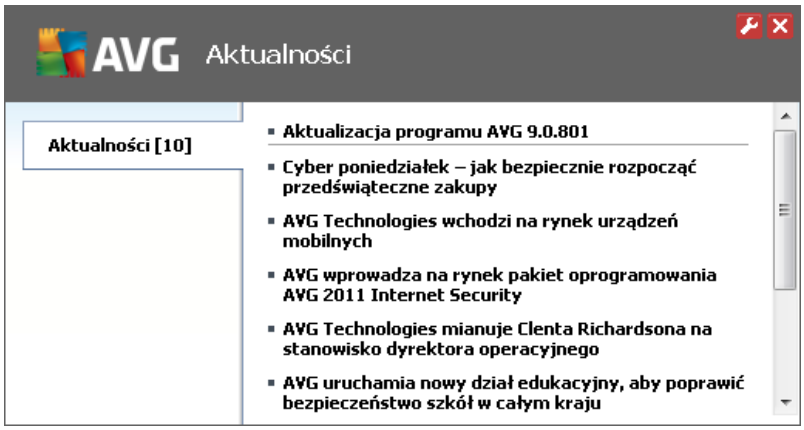
- — strona jest podejrzana.

- — Strona zawiera linki do niebezpiecznych stron.
- — Strona, do której prowadzi link, zawiera aktywne zagrożenia! Dla bezpieczeństwa użytkownika dostęp do tej strony zostanie zablokowany.
- — Strona nie jest dostępna i nie udało się jej przeskanować.

Kliknij ten przycisk, aby otworzyć panel zawierający szczegółowe informacje dotyczące określonej strony internetowej.

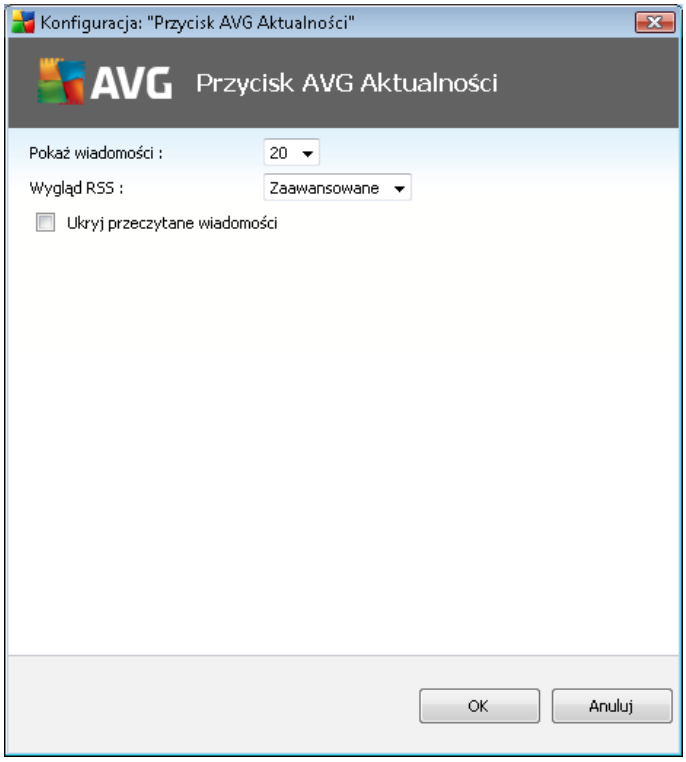
8.1.4. Aktualności AVG

Ten przycisk paska narzędzi ***AVG Security Toolbar*** umożliwia otwarcie i przeglądanie najnowszych ***informacji prasowych*** dotyczących systemu AVG, w tym artykułów i publikacji firmy AVG:



W prawym górnym rogu wyświetlane są dwa czerwone przyciski kontrolne:

- — ten przycisk otwiera okno dialogowe, w którym można określić parametry przycisku ***Aktualności AVG*** znajdującego się na pasku ***AVG Security Toolbar***:

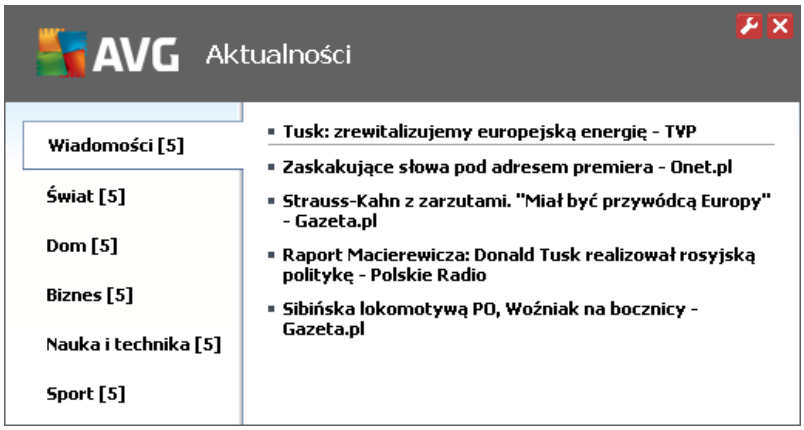


- o ***Pokaż wiadomości*** — określ liczbę wiadomości, która może być jednocześnie wyświetlania.
- o ***Wygląd RSS*** — wybierz tryb Zaawansowany lub Podstawowy bieżącego widoku przeglądu aktualności (*domyślnie wybrany jest tryb zaawansowany — patrz powyżej*).
- o ***Ukryj przeczytane wiadomości*** — zaznacz tę pozycję, aby przeczytane wiadomości były na bieżąco zastępowane przez nowe.

- — kliknięcie tego przycisku spowoduje zamknięcie otwartego przeglądu aktualności.

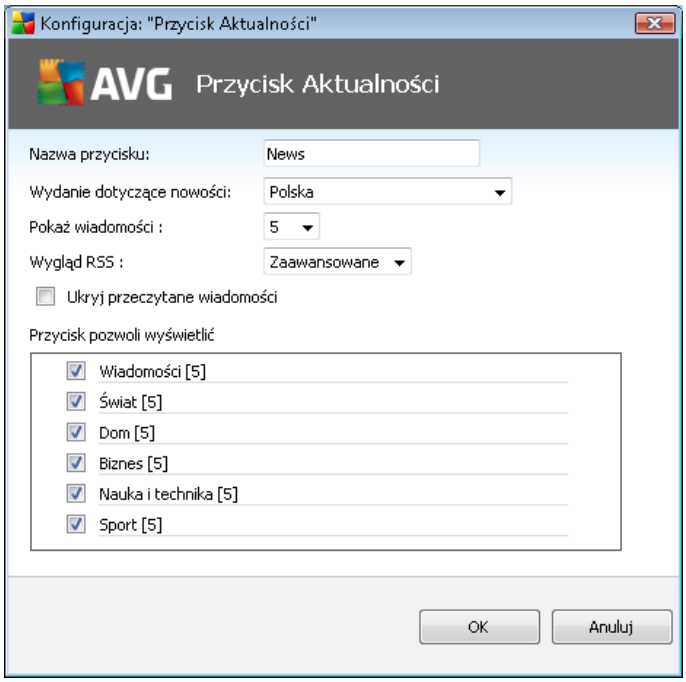
8.1.5. Aktualności

Bezpośrednio z poziomu paska narzędzi ***AVG Security Toolbar*** ten przycisk otwiera przegląd najnowszych aktualności z wybranych mediów, podzielony na kilka sekcji:



W prawym górnym rogu wyświetlane są dwa czerwone przyciski kontrolne:

- — ten przycisk otwiera okno dialogowe, w którym można określić parametry przycisku ***Aktualności*** znajdującego się na pasku ***AVG Security Toolbar***:



- ***Nazwa przycisku*** — można zmienić nazwę przycisku wyświetlaną na pasku narzędzi ***AVG Security Toolbar.***

- ***Wydanie dotyczące nowości*** — wybierz kraj z listy, aby wyświetlać aktualności z wybranego regionu.
- ***Pokaż wiadomości*** — określ liczbę wiadomości, która może być jednocześnie wyświetlania.

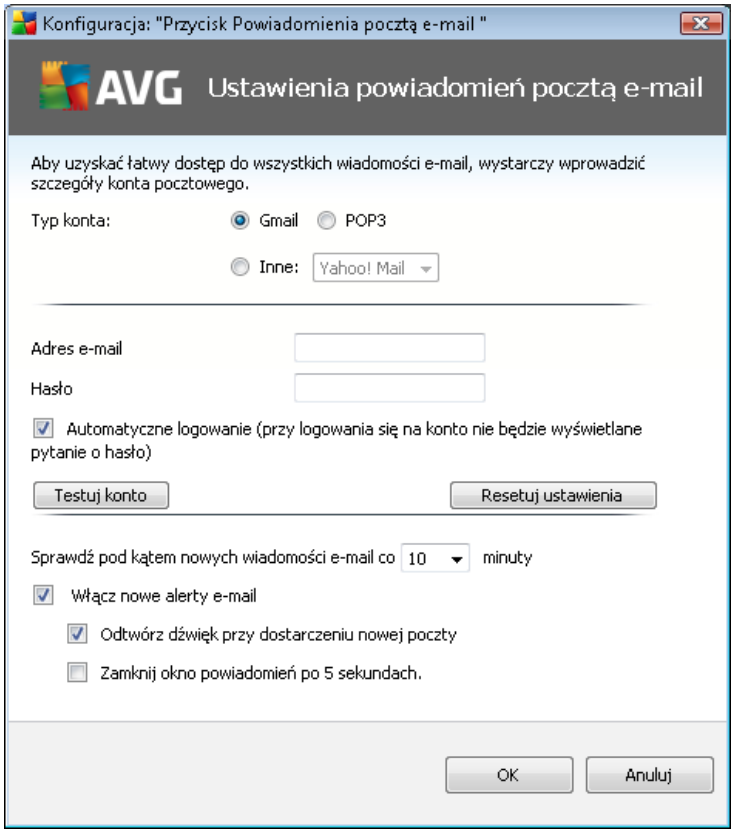
- o ***Wygląd RSS*** — przełącz między opcją Podstawowy/Zaawansowany, aby wybrać wygląd przeglądu aktualności (***domyślnie ustawiony jest przegląd zaawansowany; patrz wyżej***).
- o ***Ukryj przeczytane wiadomości*** — zaznacz tę pozycję, aby przeczytane wiadomości nie były już wyświetlane w przeglądzie aktualności i były zastępowane nowymi.
- o ***Przycisk pozwoli wyświetlić*** — w tym polu można określić, jakiego rodzaju wiadomości mają być wyświetlane w przeglądzie aktualności paska narzędzi ***AVG Security Toolbar***.
  - — kliknięcie tego przycisku spowoduje zamknięcie otwartego przeglądu aktualności.

8.1.6. Usuń historię

Ten przycisk umożliwia usunięcie historii przeglądarki, podobnie jak opcja ***logo AVG -> Usuń historię***.

8.1.7. Powiadomienia e-mail

Przycisk ***Powiadomienia e-mail*** umożliwia aktywowanie na pasku narzędzi ***AVG Security Toolbar*** ***powiadomień o nowej poczcie.*** Kliknięcie tego przycisku otwiera okno dialogowe, w którym można zdefiniować parametry konta e-mail oraz reguł wyświetlania wiadomości e-mail. Postępuj zgodnie z instrukcjami wyświetlanymi w oknie dialogowym:



- ***Typ konta*** — określ typ protokołu używany przez konto poczty e-mail. Można wybrać spośród następujących typów: *Gmail*, *POP3* lub wybrać nazwę serwera z menu rozwijanego *Inne* (*obecnie tej opcji można używać dla kont Yahoo! JP Mail lub Hotmail*). Jeśli nie masz pewności, jakiego typu serwera pocztowego używa dane konto, spróbuj znaleźć informacje otrzymane od dostawcy poczty e-mail lub dostawcy usług

internetowych.

- ***Logowanie*** — w poniższej sekcji podaj swój dokładny *adres e-mail* i *hasło*. Pozostaw opcję *Automatyczne logowanie* zaznaczoną, aby nie wprowadzać tych danych za każdym razem.
- ***Sprawdź konto*** — ten przycisk pozwala sprawdzić wprowadzone dane.
- ***Resetuj ustawienia*** — pozawala na szybkie usunięcie danych wprowadzonych powyżej.
- ***Sprawdzaj nowe wiadomości co ... min.*** — zdefiniuj interwał sprawdzania skrzynki pocztowej (*wartość z przedziału 5–120 minut*) i określ sposób informowania o nadejściu nowych wiadomości e-mail.
- ***Włącz alerty nowych wiadomości*** — odznaczenie tego pola spowoduje wyłączenie wizualnych powiadomień o otrzymaniu nowych wiadomości e-mail.
    - ***Odtwórz dźwięk przy dostarczeniu nowej poczty*** — odznaczenie tego pola spowoduje wyłączenie dźwiękowych powiadomień o nowych wiadomościach e-mail.
    - ***Zamknij okno powiadomień po 5 sekundach*** — zaznacz to pole, aby po 5 sekundach automatycznie zamknąć powiadomienie o nowej wiadomości e-mail.

8.1.8. Informacje o pogodzie

Przycisk ***Pogoda*** służy do wyświetlania informacji o aktualnej temperaturze (*dane aktualizowane co 3-6–godzin*) w wybranym miejscu, bezpośrednio z poziomu interfejsu paska narzędzi ***AVG Security Toolbar***. Kliknięcie przycisku spowoduje otwarcie nowego panelu zawierającego szczegółowe informacje o pogodzie:

Poniżej opisane są jego opcje:

- ***Zmień lokalizację*** — kliknij link ***Zmień lokalizację***, aby wyświetlić okno dialogowe

Szukaj lokalizacji. Podaj nazwę żądanej lokalizacji w polu tekstowym i potwierdź wybór, klikając przycisk ***Szukaj***. Jeśli na liście wyników znajdziesz wiele lokalizacji o tej samej nazwie, wybierz położenie, którego szukasz. Na koniec zostanie ponownie wyświetlony panel zawierający informacje o pogodzie dla wybranej lokalizacji.

- ***Przelicznik skali Fahrenheita/Celsjusza***— w prawym górnym rogu panelu informacyjnego można wybrać skalę Fahrenheita lub Celsjusza. Informacje na pasku narzędzi będą podawane w wybranej przez Ciebie skali.

- ***Pełna prognoza*** — jeśli potrzebujesz pełnych i szczegółowych informacji o prognozie pogody, kliknij link ***Pełna prognoza***, który przekieruje Cię do profesjonalnego serwisu pogodowego.

8.1.9. Facebook

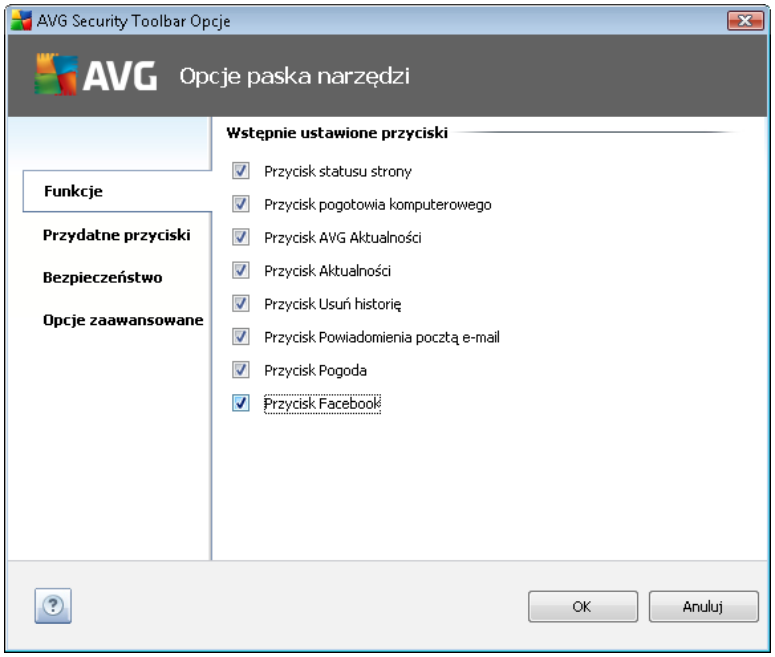
Przycisk ***Facebook*** umożliwia łączenie się z siecią społecznościową Facebook bezpośrednio z paska narzędzi ***AVG Security Toolbar***. Po kliknięciu przycisku zostanie wyświetlone zaproszenie do logowania. Kliknij ponownie, aby otworzyć okno dialogowe ***Logowanie w serwisie Facebook***. Podaj swoje dane i kliknij przycisk ***Połącz***. Jeśli jeszcze nie masz konta w serwisie Facebook, możesz utworzyć je używając linku ***Rejestracja w serwisie Facebook***.

Po przejściu przez proces rejestracji w serwisie Facebook zostanie wyświetlone zapytanie o zezwolenie na korzystanie z aplikacji ***AVG Social Extension*** (Rozszerzenie AVG dla sieci społecznościowych). Działanie tej aplikacji jest niezbędne dla paska narzędzi, aby możliwe było połączenie z serwisem Facebook, dlatego zalecane jest zezwolenie na jej działanie. Połączenie z serwisem Facebook zostanie wtedy uaktywnione i przycisk ***Facebook*** na pasku narzędzi ***AVG Security Toolbar*** będzie oferował standardowe opcje menu Facebook.

8.2. Opcje Paska narzędzi AVG Security Toolbar

Opcje konfiguracji wszystkich parametrów ***Paska narzędzi AVG Security Toolbar*** dostępne są bezpośrednio z poziomu panelu ***AVG Security Toolbar***. Interfejs edycji dostępny jest po wybraniu opcji *AVG / Opcje* z menu paska. Jego otwarcie następuje w nowym oknie dialogowym (***Opcje paska narzędzi***), które jest podzielone na cztery sekcje:

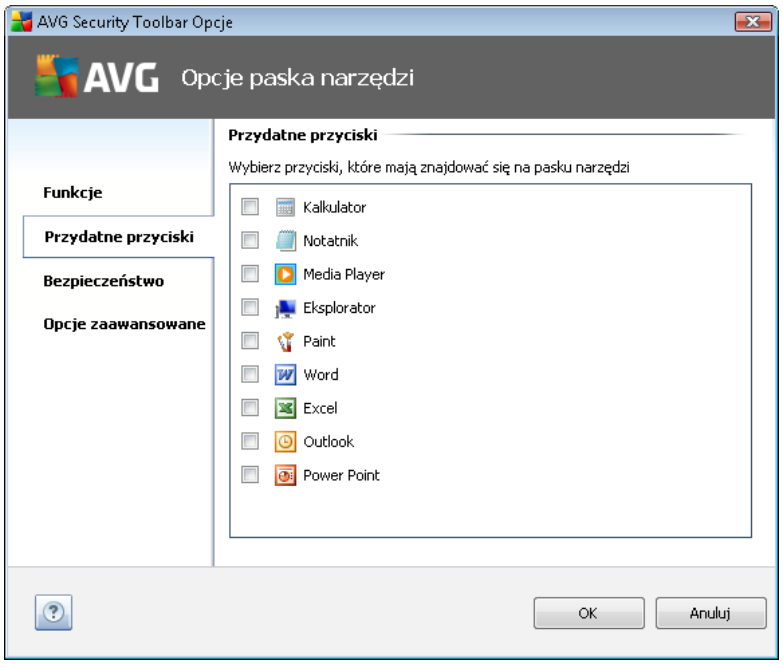
8.2.1. Karta Ogólne



Na tej karcie możliwe jest określenie, które przyciski kontrolne mają być wyświetlane / ukryte na panelu ***Paska narzędzi AVG Security Toolbar***. Należy w tym celu zaznaczyć wszystkie przyciski, które mają być wyświetlane. Poniżej znajduje się opis funkcji wszystkich przycisków paska narzędzi:

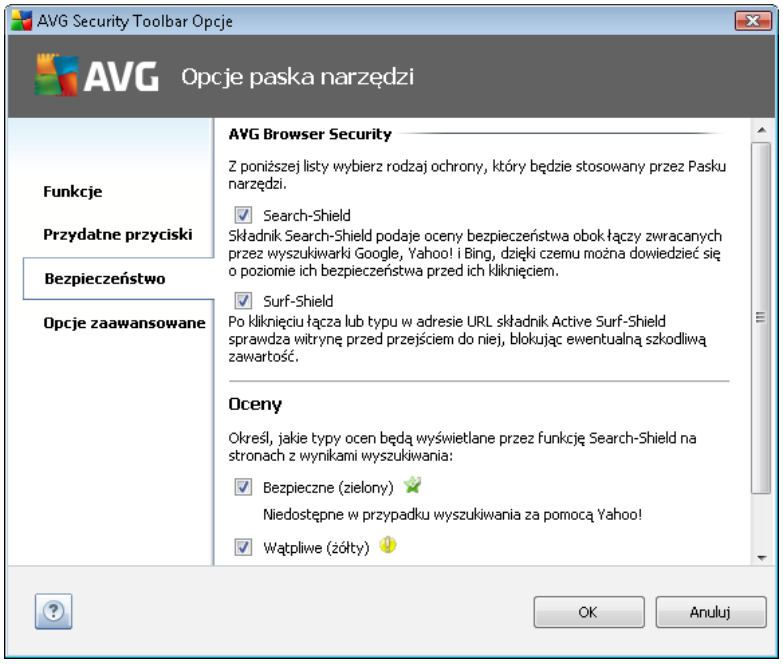
- ***Przycisk Status strony —*** ten przycisk pozwala wyświetlić informacje o statusie aktualnie otwartej strony w obszarze paska narzędzi ***AVG Security Toolbar.***
- ***Nowości AVG*** — otwiera stronę internetową zawierającą najnowsze informacje prasowe dotyczące systemu AVG.
- ***Wiadomości*** — udostępnia strukturalny przegląd bieżących wiadomości z codziennej prasy.
- ***Przycisk Usuń historię*** — przycisk ten pozwala usunąć całą historię, lub tylko historię wyszukiwania, przeglądania i pobierania (a także ciasteczka) bezpośrednio z poziomu panelu Paska narzędzi AVG Security Toolbar.
- ***Przycisk Powiadomienia e-mail*** — ten przycisk umożliwia wyświetlanie nowo otrzymanych wiadomości e-mail w obszarze Paska ***AVG Security Toolbar***.
- ***Przycisk Pogoda*** — ten przycisk umożliwia bezpośredni dostęp do informacji o stanie pogody w wybranej lokalizacji.
- ***Przycisk serwisu Facebook*** — ten przycisk umożliwia bezpośrednie połączenie z siecią społecznościową Facebook.

8.2.2. Karta Użyteczne przyciski



Karta ***Użyteczne przyciski*** umożliwia wybór aplikacji z listy i wyświetlanie ich ikon w interfejsie paska narzędzi. Ikona służy wówczas jako szybkie łącze umożliwiające natychmiastowe uruchomienie odpowiedniej aplikacji.

8.2.3. Karta Bezpieczeństwo



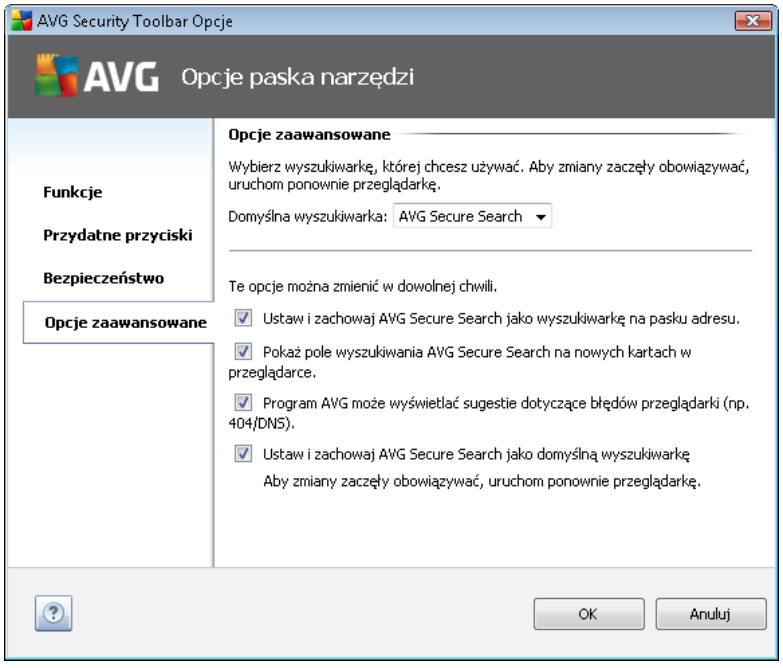
Karta ***Bezpieczeństwo*** jest podzielona na dwie sekcje (***Bezpieczeństwo przeglądarki*** i ***Oceny***), w

których można zaznaczyć określone pola, aby skonfigurować następujące funkcje:

- ***AVG Browser Security*** — tę pozycję należy zaznaczyć, aby aktywować składniki ***Search-Shield*** i ***Surf-Shield***
- ***Oceny*** — należy wybrać symbole graficzne, które mają być używane przy klasyfikacji wyników wyszukiwania przez funkcję ***Search-Shield***:
  - strona jest bezpieczna
  - strona jest podejrzana
  - strona zawiera linki do niebezpiecznych witryn
  - strona zawiera aktywne zagrożenia
  - strona nie jest dostępna i nie można jej przeskanować

Należy zaznaczyć odpowiednią opcję, aby potwierdzić, że informacje o określonym poziomie zagrożenia mają być wyświetlane. Nie można jednak wyłączyć wyświetlania czerwonego symbolu przypisanego stronom zawierającym realne zagrożenie. ***Jeśli nie istnieje ważny powód, żeby modyfikować domyślną konfigurację zdefiniowaną przez twórców programu, stanowczo zaleca się jej zachowanie.***

8.2.4. Karta Opcje zaawansowane



Na karcie ***Opcje zaawansowane*** należy najpierw określić, która wyszukiwarka ma być używana

jako domyślna. Możesz wybrać wyszukiwarkę *AVG Secure Search (powered by Google), Baidu, WebHledani*, *Yandex i Yahoo! JP*. Po zmianie domyślnej wyszukiwarki należy ponownie uruchomić przeglądarkę internetową, aby zmiany zostały zachowane.

Następnie można aktywować lub wyłączyć szczegółowe ustawienia paska narzędzi ***AVG Security Toolbar*** *(podane opcje dotyczą domyślnych ustawień przeglądarki AVG Secure Search (powered by Google))*:

- ***Ustaw i zachowaj AVG Secure Search (powered by Google) jako domyślną wyszukiwarkę używaną na pasku adresu*** — jeśli ta opcja jest zaznaczona, możliwe jest automatycznie wyszukiwanie stron przy użyciu serwisu Google (bezpośrednio na pasku adresu przeglądarki internetowej).

- ***Zezwalaj systemowi AVG na sugestie dotyczące błędów nawigacji przeglądarki (404/ DNS)*** — jeśli podczas przeglądania sieci zostanie wybrana strona nieistniejąca lub niedostępna (błąd 404), automatycznie zostanie zaproponowany przegląd alternatywnych stron o podobnej tematyce.

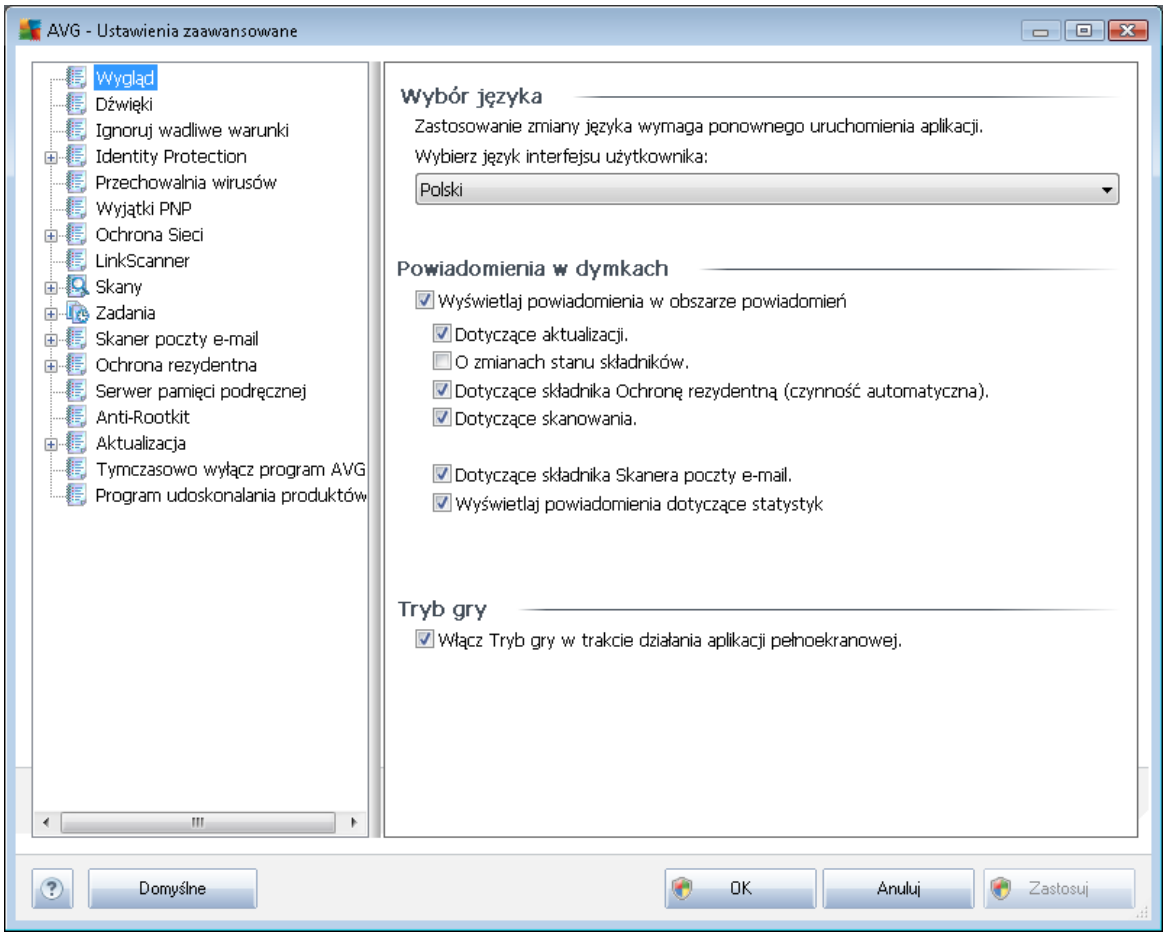
- ***Ustaw i zachowaj AVG Secure Search (powered by Google) jako domyślną wyszukiwarkę*** — Google jest domyślną wyszukiwarką internetową ***Paska narzędzi AVG Security Toolbar***, a aktywowanie tej opcji powoduje, że staje się również domyślną wyszukiwarką przeglądarki internetowej.

9. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG Anti-Virus 2011** zostają otwarte w nowym oknie o nazwie ***AVG - Ustawienia zaawansowane***. Okno to podzielone jest na dwa obszary: lewy zawiera drzewo nawigacyjne, a prawy — opcje konfiguracji programu. Wybranie składnika, którego (*lub części którego*) konfiguracja ma zostać zmieniona, powoduje przejście do odpowiedniego okna z prawej strony.

9.1. Wygląd

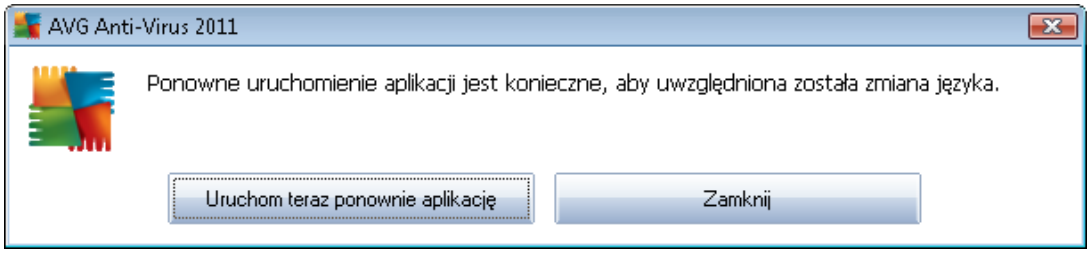
Pierwszy element w drzewie nawigacyjnym, ***Wygląd***, odnosi się do ogólnych ustawień interfejsu użytkownika systemu AVG oraz kilku podstawowych opcji sterujących zachowaniem aplikacji:



Wybór języka

W sekcji ***Wybór języka*** można wybrać żądany język z listy rozwijanej; język ten będzie używany w całym interfejsie użytkownika systemu AVG. Menu rozwijane zawiera tylko języki wybrane podczas instalacji (*patrz rozdział Opcje niestandardowe*) i język angielski (*instalowany domyślnie*). Przełączenie aplikacji na inny język wymaga ponownego uruchomienia interfejsu użytkownika. W tym celu należy wykonać następujące kroki:

- Wybierz żądany język aplikacji i potwierdź wybór, klikając przycisk ***Zastosuj*** (widoczny w prawym dolnym rogu).
- Wciśnij przycisk ***OK***, aby potwierdzić.
- W nowym oknie dialogowym pojawi się informacja, że zmiana języka interfejsu systemu AVG wymaga ponownego uruchomienia programu:



Powiadomienia w dymkach

W tym obszarze można wyłączyć wyświetlane w dymkach powiadomienia dotyczące stanu aplikacji. Domyślnie wszystkie powiadomienia są wyświetlane i nie zaleca się zmiany tych ustawień. Zwykle informują one o zmianach stanu składników AVG i w żadnym wypadku nie wolno ich ignorować!

Jeśli jednak z jakiegoś powodu powiadomienia te nie mają być wcale wyświetlane lub mają dotyczyć tylko określonych składników AVG, można zdefiniować własne preferencje, zaznaczając lub odznaczając odpowiednie opcji:

- ***Wyświetlaj powiadomienia w obszarze powiadomień*** — pole jest domyślnie zaznaczone (*opcja włączona*), a powiadomienia są wyświetlane. Usunięcie zaznaczenia opcji powoduje całkowite wyłączenie wyświetlania powiadomień w dymkach. Po włączeniu tej opcji można bardziej szczegółowo określić, jakie powiadomienia mają być wyświetlane:
  - ***Wyświetlaj w obszarze powiadomień komunikaty dotyczące aktualizacji*** — należy określić, czy mają być wyświetlane informacje dotyczące rozpoczęcia, postępu i zakończenia aktualizacji systemu AVG;
  - ***Wyświetlaj powiadomienia o zmianach stanu składników*** — należy określić, czy mają być wyświetlane informacje dotyczące aktywności lub nieaktywności składników bądź możliwych problemów ich dotyczących. W przypadku zgłaszania stanu błędu składnika, opcja ta określa funkcję informacyjną ikony na pasku zadań (zmiany koloru), która wskazuje na problemy z dowolnym składnikiem systemu AVG;
  - ***Wyświetlaj w obszarze powiadomień na pasku zadań komunikaty dotyczące składnika Ochrona rezydentna (akcja automatyczna) — należy określić, czy informacje dotyczące procesów zapisywania, kopiowania i*** otwierania plików mają być wyświetlane (*ta konfiguracja jest dostępna tylko, jeśli włączona jest opcja automatycznego leczenia Ochrony rezydentnej*);

- ***Wyświetlaj w obszarze powiadomień komunikaty dotyczące skanowania*** — należy określić, czy mają być wyświetlane informacje dotyczące automatycznego rozpoczęcia, postępu i zakończenia zaplanowanego skanowania;

- ***Wyświetlaj w obszarze powiadomień komunikaty dotyczące składnika Skaner poczty e-mail*** — należy określić, czy mają być wyświetlane informacje dotyczące skanowania wszystkich przychodzących i wychodzących wiadomości e-mail.

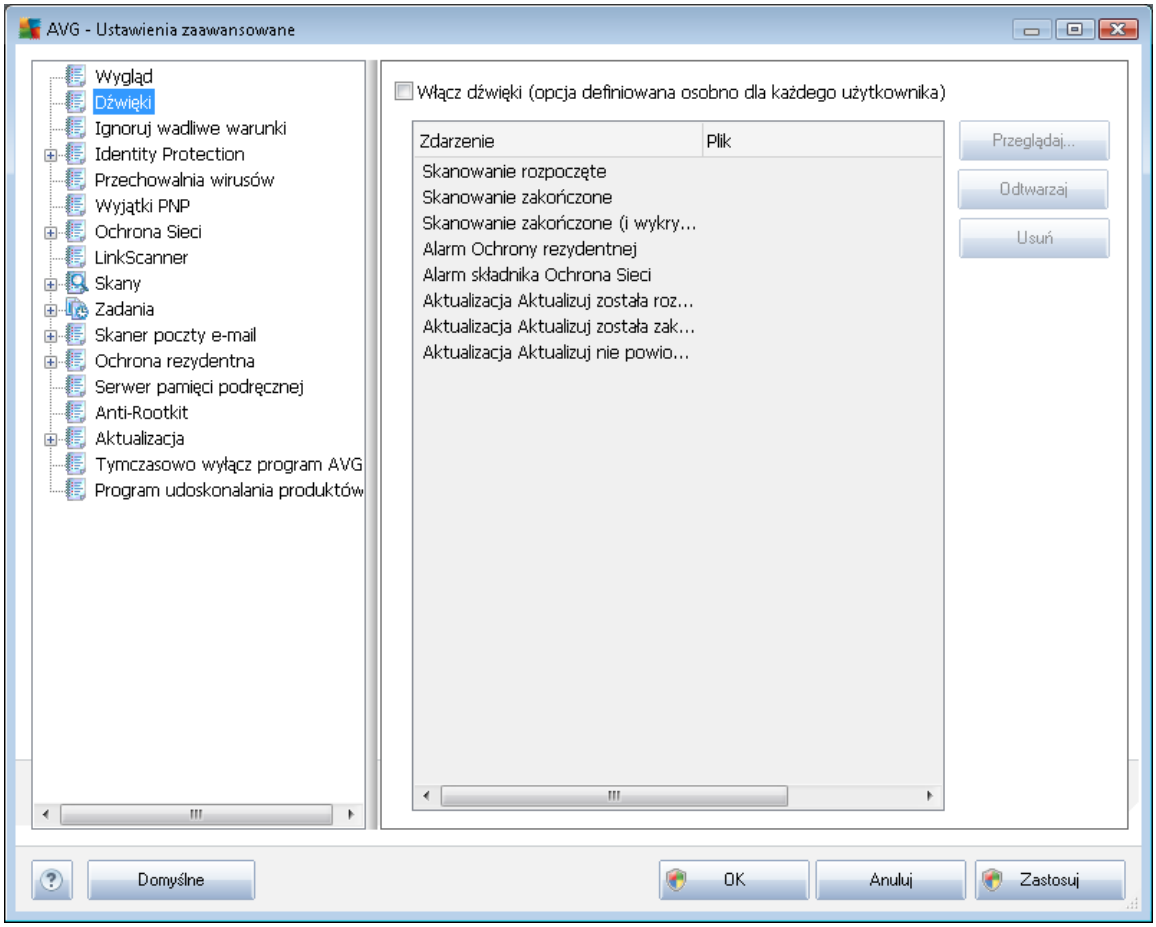
- ***Wyświetlaj powiadomienia dotyczące statystyk*** — pozostaw tę opcję włączoną, aby zezwolić na wyświetlanie na pasku zadań powiadomień dotyczących statystyk.

Tryb gry

Ta funkcja jest przeznaczona dla aplikacji pełnoekranowych, w działaniu których mogłyby przeszkadzać (*np. minimalizować lub zakłócać wyświetlanie grafiki*) powiadomienia systemu AVG (*wyświetlane np. w chwili uruchomienia zaplanowanego skanowania*). Aby tego uniknąć, należy pozostawić pole wyboru ***Włącz tryb gry w trakcie działania aplikacji pełnoekranowej*** zaznaczone (*ustawienie domyślne*).

9.2. Dźwięki

W oknie dialogowym ***Dźwięki*** można określić, czy system AVG ma informować o określonych czynnościach za pomocą dźwięków. Jeśli tak, należy zaznaczyć pole wyboru ***Włącz efekty dźwiękowe*** (*domyślnie wyłączone*), aby włączyć listę czynności systemu AVG:

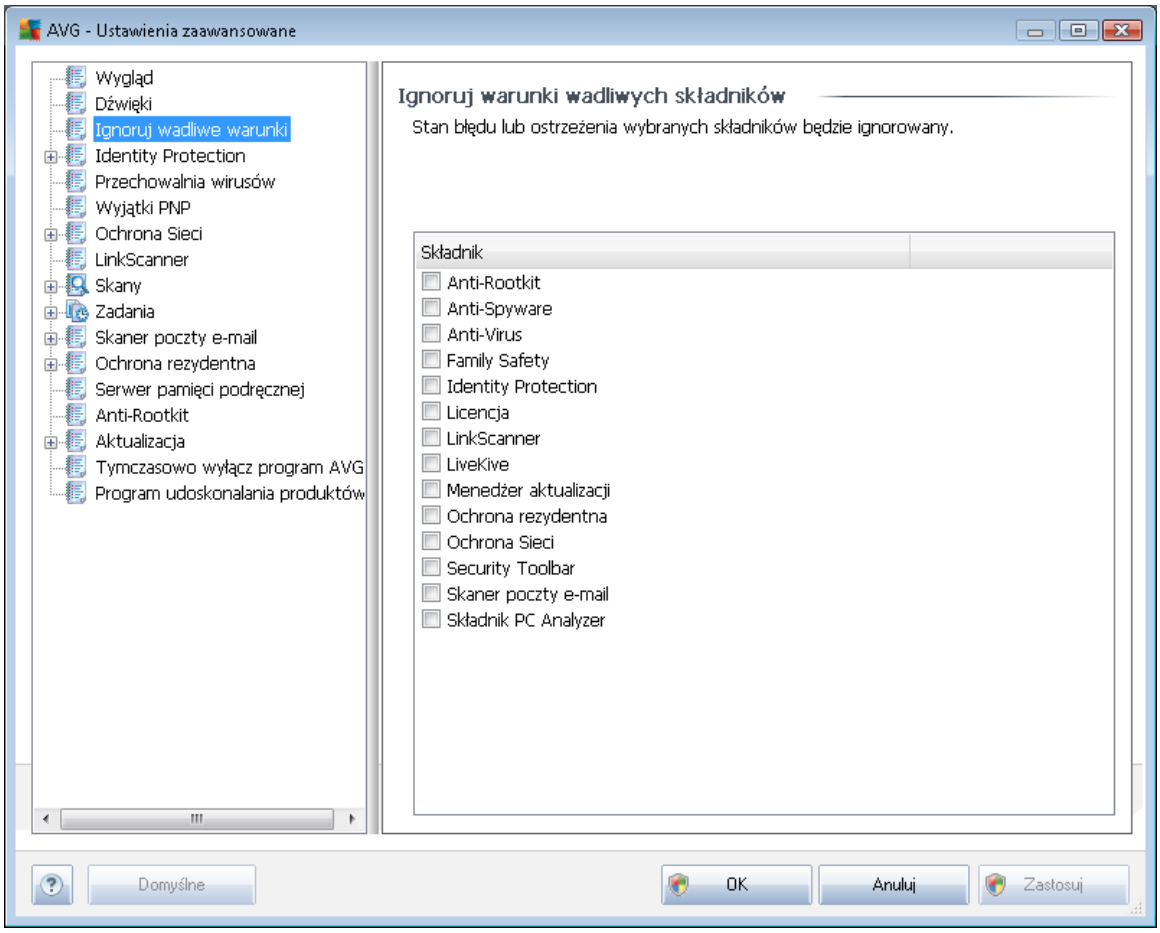


Następnie należy wybrać odpowiednie zdarzenie z listy i wskazać plik dźwiękowy, który ma zostać do niego przypisany (***Przeglądaj***). Aby odtworzyć wybrany dźwięk, należy zaznaczyć go na liście i nacisnąć przycisk ***Odtwórz***. Aby usunąć dźwięk przypisany do określonego zdarzenia, należy użyć przycisku ***Usuń***.

Uwaga: *Obsługiwane są tylko pliki *.wav!*

9.3. Ignoruj błędny stan składników

W oknie dialogowym ***Ignoruj błędny stan składników*** można wskazać składniki, które mają być pomijane w powiadomieniach o błędnym stanie:



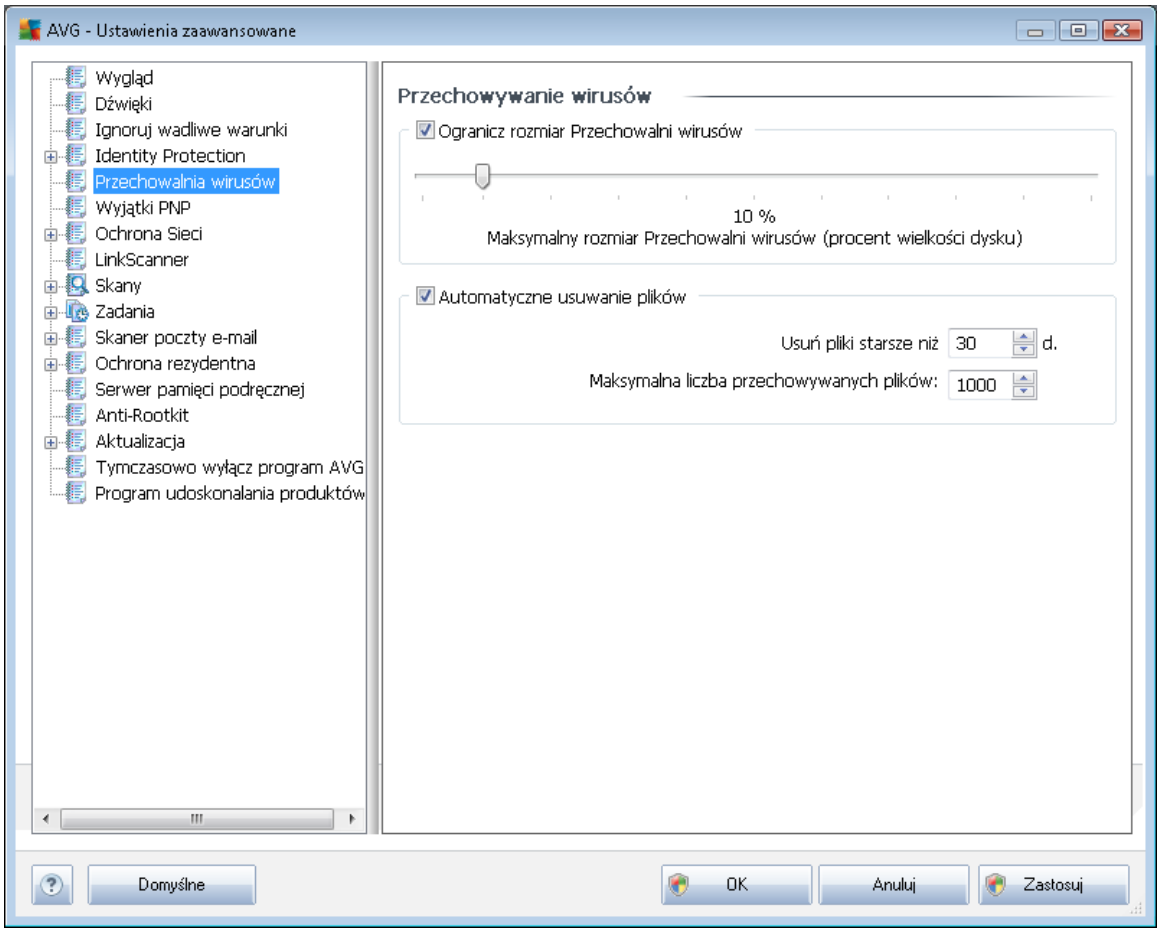
Domyślnie żaden składnik nie jest zaznaczony. Oznacza to, że jeśli dowolny składnik znajdzie się w stanie błędu, natychmiast wygenerowane zostanie powiadomienie:

- ***ikona na pasku zadań*** — gdy wszystkie składniki systemu AVG działają prawidłowo, wyświetlana ikona jest czterokolorowa; w przypadku błędu wyświetlany jest żółty wykrzyknik;
- tekstowy opis problemu jest widoczny w sekcji ***Informacje o stanie bezpieczeństwa*** okna głównego AVG.

Może wystąpić sytuacja, w której składnik powinien zostać tymczasowo wyłączony (*nie jest to zalecane; wszystkie składniki powinny być zawsze włączone i działać w trybie domyślnym, ale niekiedy może być wymagane odstępstwo od tej reguły*). W takim przypadku ikona na pasku zadań automatycznie informuje o stanie błędu składnika. W takiej sytuacji nie ma jednak faktycznego błędu, ponieważ wyłączenie składnika było celowe, a ryzyko z tym związane jest znane. Ponadto, gdy ikona jest szara, nie może już informować o ewentualnych realnych błędach.

W takim przypadku należy w powyższym oknie dialogowym zaznaczyć składniki, które mogą być w stanie błędu (*lub wyłączone*) bez wyświetlania odpowiednich powiadomień. Opcja ***ignorowania stanu składników*** jest także dostępna dla określonych składników bezpośrednio w sekcji przeglądu składników okna głównego systemu AVG.

9.4. Przechowalnia wirusów



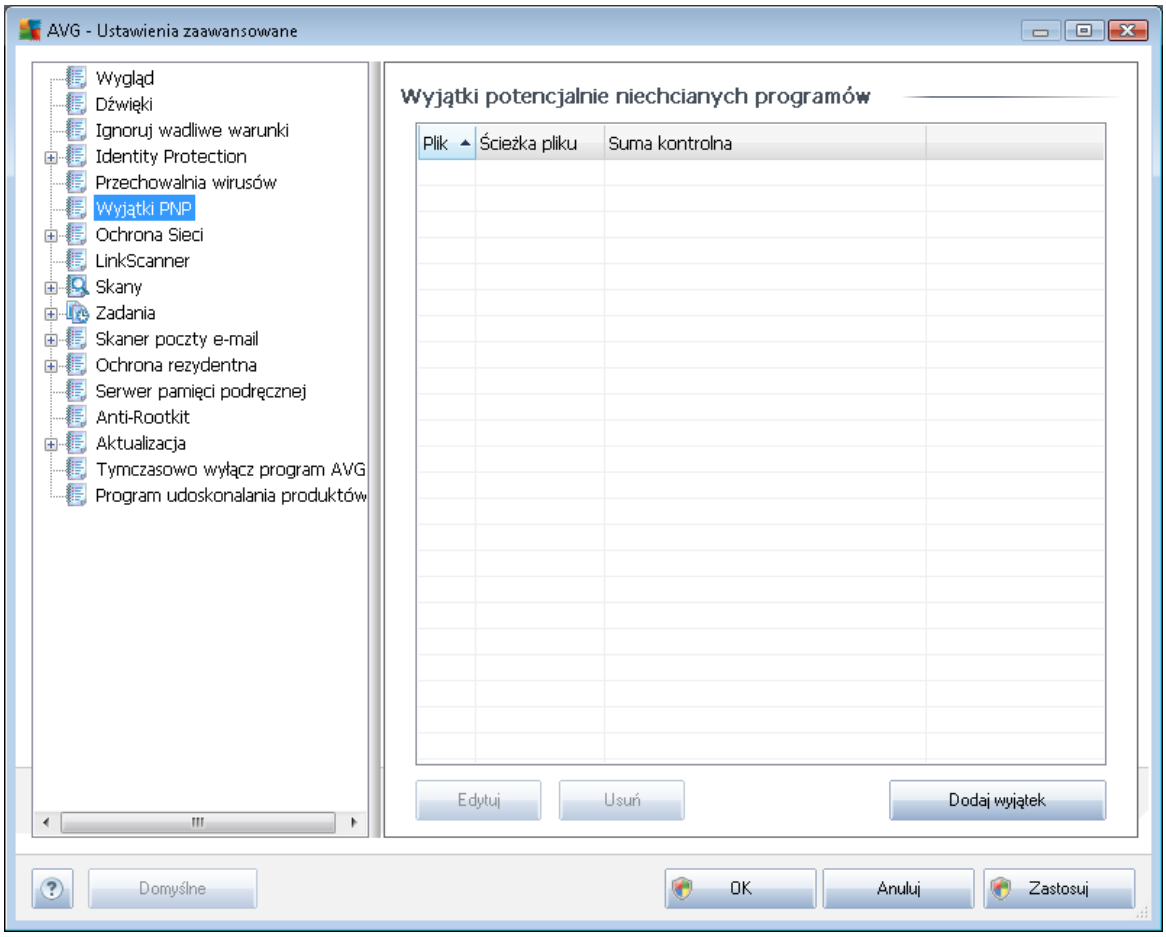
W oknie ***Przechowalnia wirusów*** można zdefiniować kilka parametrów dotyczących administrowania obiektami znajdującymi się w ***Przechowalni***:

- ***Ogranicz rozmiar Przechowalni wirusów*** — za pomocą suwaka należy określić maksymalny rozmiar ***Przechowalni wirusów***. Rozmiar jest określany w stosunku do rozmiaru dysku lokalnego.

- ***Automatyczne usuwanie plików*** — w tym obszarze można zdefiniować maksymalny okres przetrzymywania obiektów w ***Przechowalni wirusów*** (***Usuń pliki starsze niż ... dni***) oraz maksymalną liczbę plików, które mogą znajdować się w ***Przechowalni*** (***Maksymalna liczba przechowywanych plików***).

9.5. Wyjątki PNP

System **AVG Anti-Virus 2011** potrafi analizować i wykrywać pliki wykonywalne i biblioteki DLL, których obecność w systemie operacyjnym może być niepożądana. W niektórych przypadkach użytkownik może chcieć zachować na komputerze określone potencjalnie niechciane programy (*jeśli zostały zainstalowane celowo*). Niektóre aplikacje, zwłaszcza bezpłatne, zawierają oprogramowanie reklamowe. Może ono zostać wykryte i zgłoszone przez system AVG jako ***potencjalnie niechciany program***. Jeśli chcesz zachować taki program na komputerze, możesz zdefiniować go jako wyjątek potencjalnie niechcianych programów:



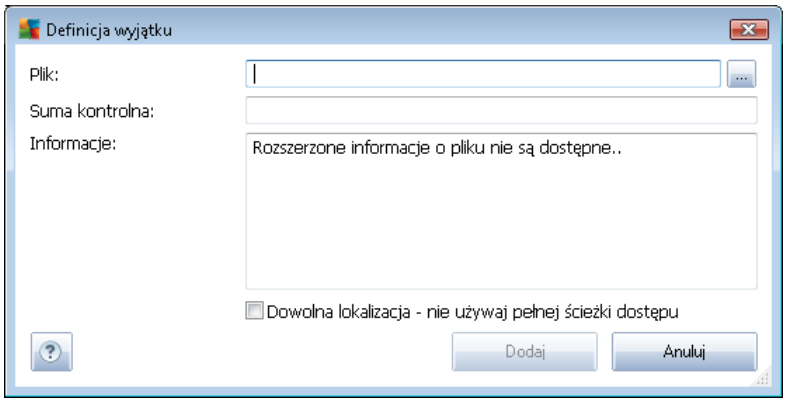
Okno ***Wyjątki potencjalnie niechcianych programów*** zawiera listę już zdefiniowanych i aktualnie obowiązujących wyjątków potencjalnie niechcianych programów. Listę tę można edytować, usuwać istniejące pozycje lub dodawać nowe wyjątki. Dla każdego wyjątku na liście dostępne są następujące informacje:

- ***Plik*** — zawiera nazwę odpowiedniej aplikacji.
- ***Ścieżka pliku*** — wyświetla ścieżkę dostępu do aplikacji.
- ***Suma kontrolna*** — wyświetla unikatową „sygnaturę” wybranego pliku. Suma ta jest generowanym automatycznie ciągiem znaków, który pozwala systemowi AVG

jednoznacznie odróżniać wybrany plik od innych. Jest ona generowana i wyświetlana po pomyślnym dodaniu pliku.

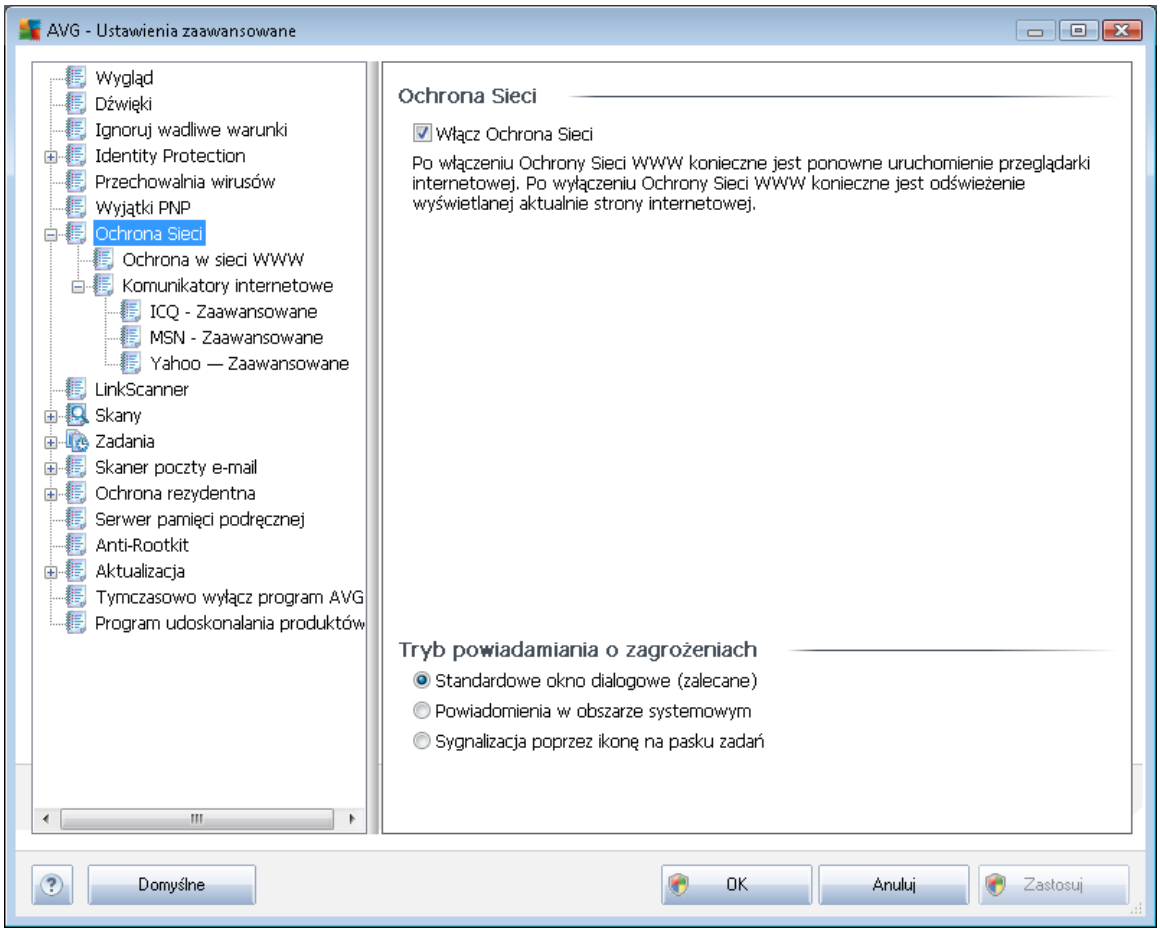
Przyciski kontrolne

- ***Edytuj*** — otwiera okno edycji (*identyczne jak okno definiowania nowego wyjątku, patrz niżej*), w którym można zmienić parametry istniejącego wyjątku.
- ***Usuń*** — usuwa wybrany element z listy wyjątków.
- ***Dodaj wyjątek*** — otwiera okno edycji, w którym można zdefiniować parametry nowego wyjątku:



  - **Plik** — należy podać pełną ścieżkę do pliku, który ma być oznaczony jako wyjątek.
  - ***Suma kontrolna*** — wyświetla unikatową „sygnaturę” wybranego pliku. Suma ta jest generowanym automatycznie ciągiem znaków, który pozwala systemowi AVG jednoznacznie odróżniać wybrany plik od innych. Jest ona generowana i wyświetlana po pomyślnym dodaniu pliku.
  - ***Informacje o pliku*** — wyświetla wszelkie dodatkowe dostępne informacje na temat pliku (*licencja/wersja itp.*).
  - ***Dowolna lokalizacja — nie używaj pełnej ścieżki dostępu*** — jeśli plik ma być zdefiniowany jako wyjątek jedynie dla konkretnej lokalizacji, wówczas należy pozostawić to pole niezaznaczone. Jeśli to pole zostanie zaznaczone, określony plik będzie traktowany jako wyjątek bez względu na to, gdzie się znajduje (*mimo to konieczne jest jednak wprowadzenie pełnej ścieżki do konkretnego pliku, ponieważ plik ten będzie używany jako unikalny przykład na wypadek, gdyby w systemie znajdowały się dwa pliki o tej samej nazwie*).

9.6. Ochrona Sieci



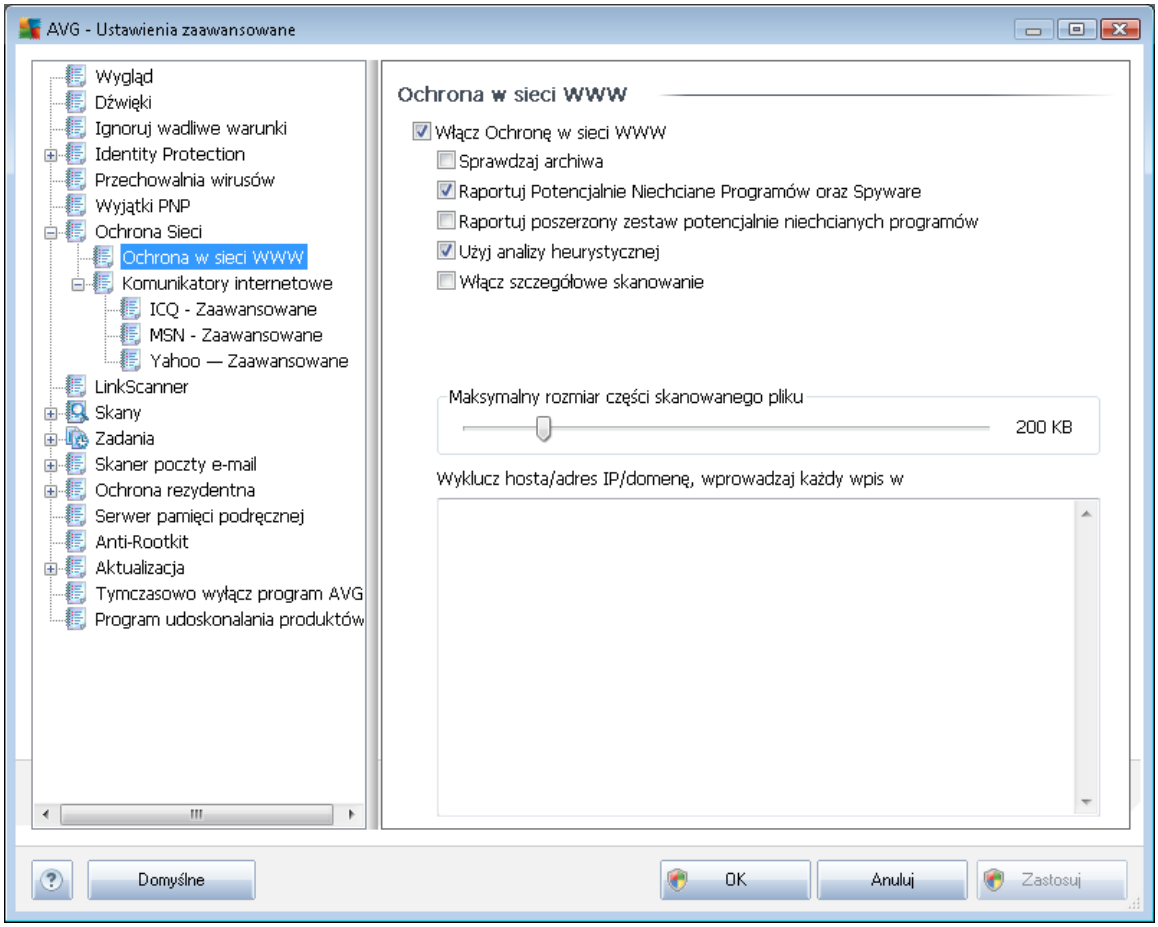
W oknie dialogowym ***Ochrona Sieci*** można włączyć lub wyłączyć cały składnik ***Ochrona Sieci*** za pomocą opcji ***Włącz Ochronę Sieci*** (*domyślnie jest ona włączona*). Szczegółowe ustawienia tego składnika dostępne są w kolejnych oknach dialogowych dostępnych z poziomu drzewa nawigacyjnego:

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

Tryb powiadamiania o zagrożeniach

W dolnej części okna można wybrać sposób informowania o wykrytych zagrożeniach: za pomocą zwykłych okien dialogowych, powiadomień w dymkach lub ikony na pasku zadań.

9.6.1. Ochrona WWW



W oknie dialogowym ***Ochrona w sieci WWW*** można edytować konfigurację dotyczącą skanowania zawartości witryn internetowych. Interfejs pozwala modyfikować następujące ustawienia:

- ***Włącz Ochronę w sieci WWW*** — potwierdza, że składnik ***Ochrona Sieci*** ma skanować zawartość stron WWW. Jeśli ta opcja jest aktywna (*domyślnie*), można włączyć lub wyłączyć następujące funkcje:

  - ***Sprawdzaj archiwa*** — (*domyślnie wyłączone*) — skanowanie ma obejmować także archiwa zawarte na wyświetlanych stronach WWW.

  - ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje włączenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

  - ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość

oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

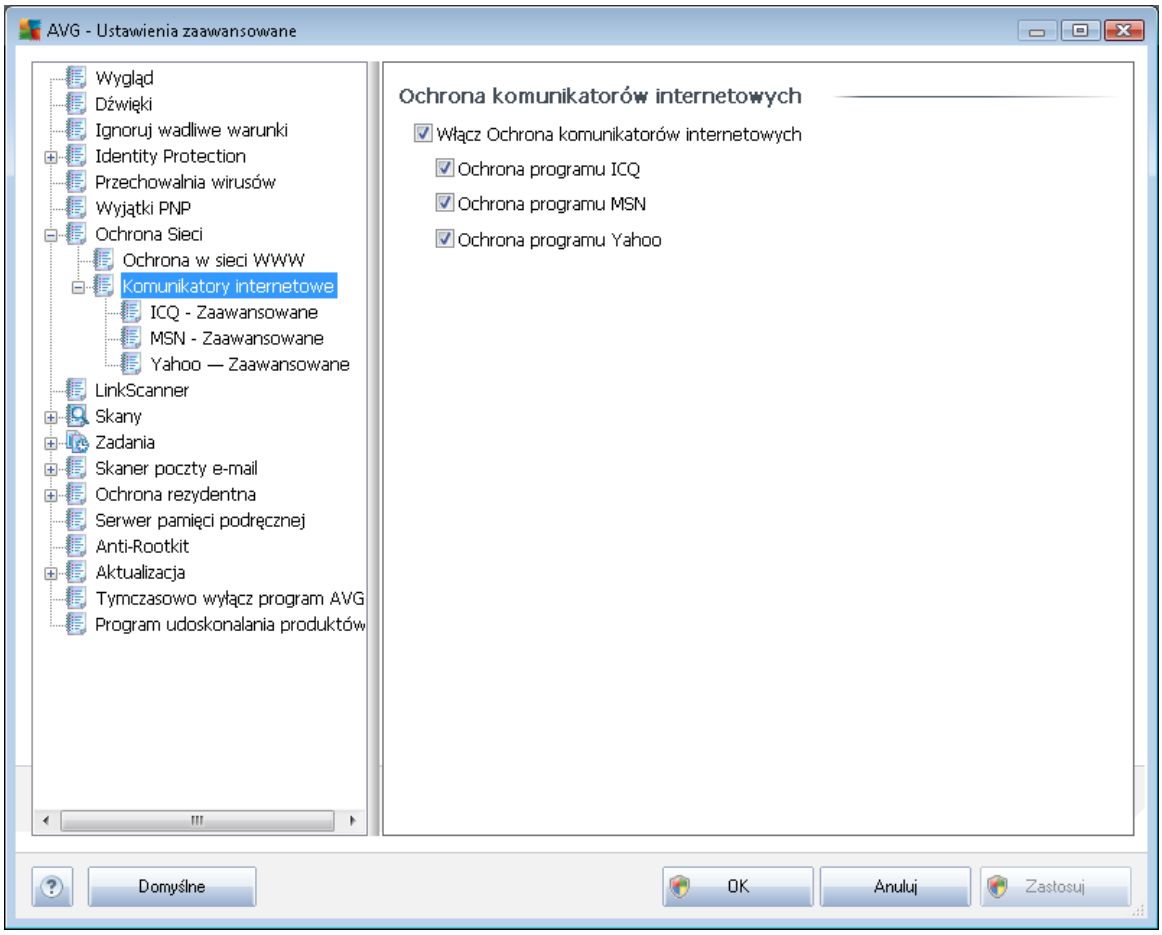
- ***Użyj heurystyki*** — (*opcja domyślnie włączona*) — skanowanie zawartości wyświetlanych stron ma wykorzystywać analizę heurystyczną (*dynamiczną emulację instrukcji skanowanego obiektu w wirtualnym środowisku*).

- ***Włącz szczegółowe skanowanie*** (*domyślnie wyłączone*) — w określonych sytuacjach (*gdy zachodzi podejrzenie, że komputer jest zainfekowany*) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będą one skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

- ***Maksymalny rozmiar części skanowanego pliku*** — jeśli wyświetlana strona zawiera pliki, można skanować ich zawartość jeszcze przed pobraniem na dysk twardy. Ponieważ jednak skanowanie obszernych plików zajmuje dłuższy czas, otwieranie stron WWW może zostać znacznie spowolnione. Za pomocą tego suwaka można określić maksymalny rozmiar plików, które mają być skanowane przez składnik ***Ochrona Sieci*** . Nawet jeśli pobierany plik jest większy od wybranego limitu i nie zostanie przeskanowany przez Ochronę Sieci, nie zmniejsza to Twojego bezpieczeństwa: jeśli plik jest zainfekowany, ***Ochrona rezydentna*** natychmiast to wykryje.

- ***Wyklucz hosta/adres IP/domenę*** — w polu tym można wpisać dokładną nazwę serwera (*host, adres IP, adres IP z maską, adres URL*) lub domenę, która ma być pomijana przy skanowaniu przez składnik ***Ochrona Sieci***. Wykluczać należy tylko hosty, co do których istnieje absolutna pewność, że nie stanowią zagrożenia.

9.6.2. Komunikatory internetowe

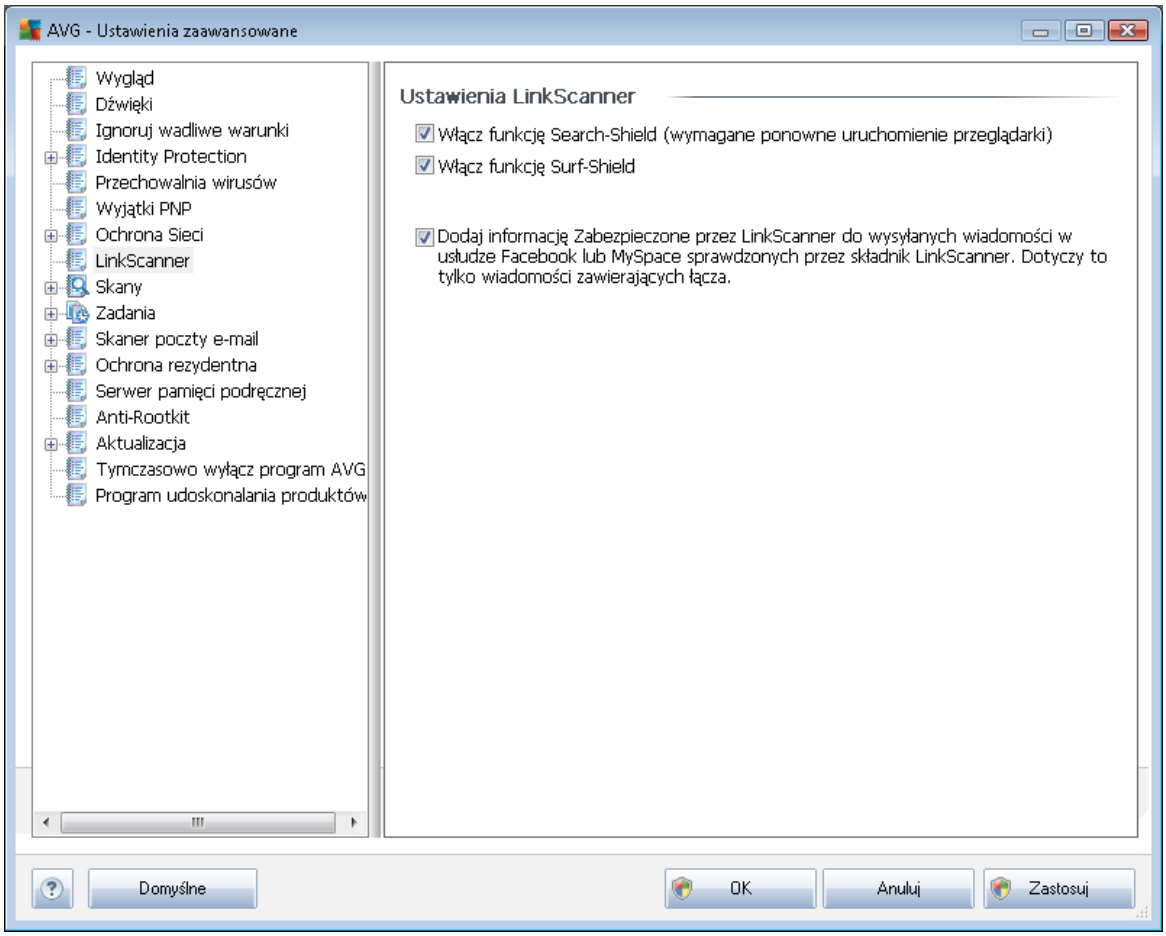


W oknie dialogowym ***Ochrona komunikatorów internetowych*** można edytować ustawienia składnika ***Ochrona Sieci***, dotyczące skanowania plików wymienianych za pośrednictwem komunikatorów internetowych. Obecnie obsługiwane są trzy komunikatory: ***ICQ***, ***MSN*** i ***Yahoo*** — jeśli składnik ***Ochrona Sieci*** ma sprawdzać, czy komunikacja danego typu jest bezpieczna, należy zaznaczyć odpowiednie pole wyboru.

Aby szczegółowo określić zaufane i blokowane kontakty, należy przejść do odpowiedniego okna dialogowego (***ICQ — Zaawansowane***, ***MSN — Zaawansowane lub Yahoo — Zaawansowane***) i stworzyć ***białą listę*** (*listę użytkowników, którzy będą mogli przesyłać wiadomości*) oraz ***czarną listę*** (*użytkowników, którzy mają być blokowani*).

9.7. LinkScanner

Okno dialogowe ***Ustawienia składnika LinkScanner*** umożliwia włączenie/wyłączenie podstawowych funkcji składnika ***LinkScanner***:



- ***Włącz funkcję Search-Shield*** (*opcje domyślnie włączona*) — skanuje wszystkie łącza pojawiające się w wynikach wyszukiwania zwracanych przez serwisy Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg oraz SlashDot, a następnie obok każdego z nich wyświetla klasyfikację bezpieczeństwa.

- ***Włącz funkcję Surf-Shield*** (*domyślnie włączona*) — aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (*w czasie rzeczywistym*). Znane złośliwe witryny i ich niebezpieczna zawartość blokowane są już w momencie otwarcia ich przez użytkownika za pomocą przeglądarki (*lub jakiejkolwiek innej aplikacji korzystającej z protokołu HTTP*).

- ***Dodaj informację „Ochronę zapewnia AVG LinkScanner”*** — zaznacz to pole, aby ***LinkScanner*** certyfikował linki wysyłane poprzez serwis Facebook lub MySpace.

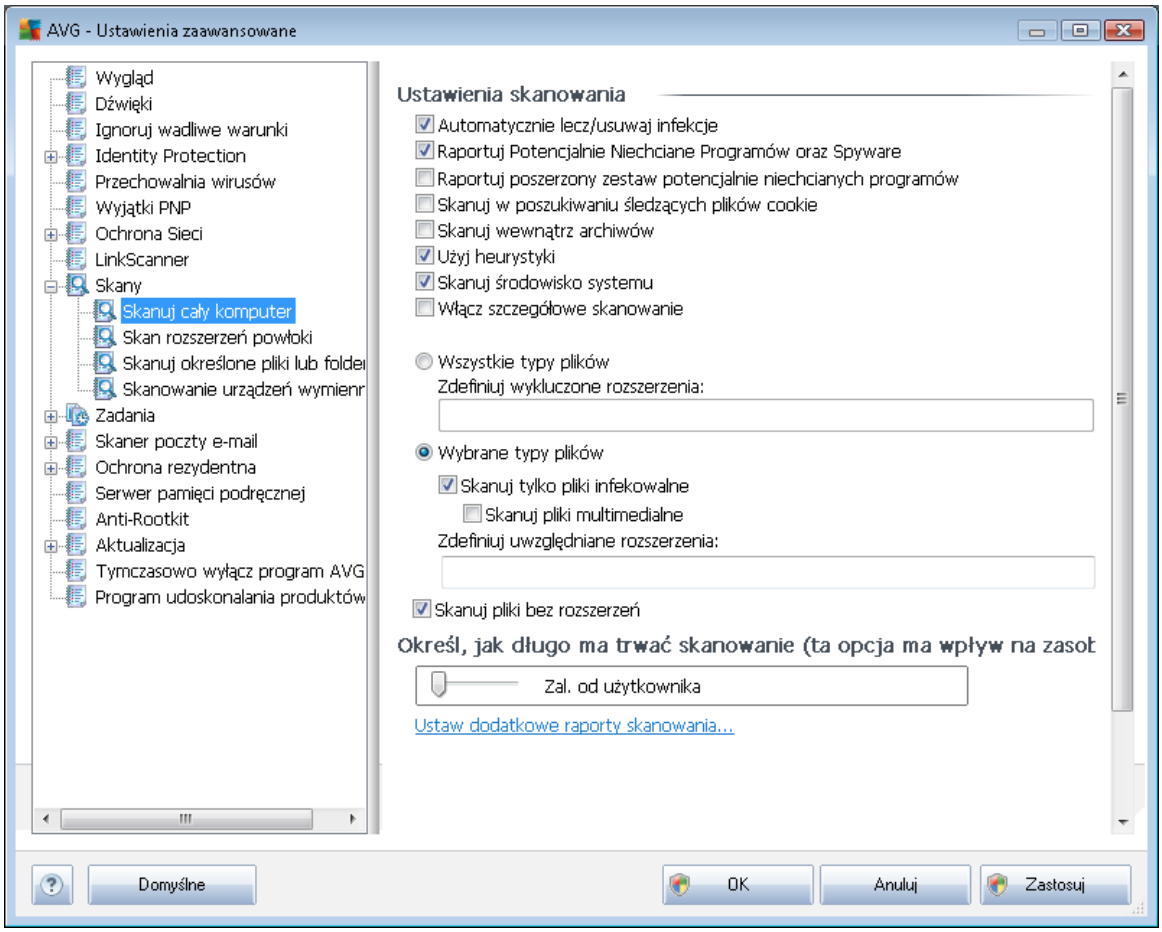
9.8. Skany

Zaawansowane ustawienia skanowania są podzielone na cztery kategorie odnoszące się do określonych typów testów:

- ***Skan całego komputera*** — standardowe, zdefiniowane wstępnie skanowanie całego komputera.
- ***Skan rozszerzenia powłoki*** — skanowanie wybranych obiektów bezpośrednio z interfejsu Eksploratora Windows.
- ***Skan określonych plików lub folderów*** — standardowe, wstępnie zdefiniowane skanowanie określonych obszarów komputera.
- ***Skan urządzeń wymiennych*** — skanowanie urządzeń wymiennych podłączonych do komputera.

9.8.1. Skan całego komputera

Opcja ***Skan całego komputera*** umożliwia edycję parametrów jednego z testów zdefiniowanych wstępnie przez dostawcę oprogramowania, tj. testu ***Skan całego komputera***:



Ustawienia skanowania

Sekcja ***Ustawienia skanowania*** zawiera listę parametrów silnika skanującego:

- ***Automatycznie lecz/usuwaj infekcje*** (*opcja domyślnie włączona*) — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do***Przechowalni wirusów***.

- ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje włączenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

- ***Skanuj w poszukiwaniu śledzących plików cookie*** (*domyślnie wyłączone*) — ten parametr składnika Anti-Spyware określa, czy wykrywane mają być pliki cookie (*używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** (*domyślnie wyłączone*) — parametr ten określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- ***Użyj heurystyki*** (*domyślnie włączone*) — analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) jest jedną z metod wykrywania wirusów w czasie skanowania.

- ***Skanuj środowisko systemu*** (*domyślnie włączone*) — skanowanie obejmie także obszary systemowe komputera.

- ***Włącz szczegółowe skanowanie*** (*domyślnie wyłączone*) — w określonych sytuacjach (*gdy zachodzi podejrzenie, że komputer jest zainfekowany*) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będą one skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

Następnie należy zdecydować, czy skanowane mają być

- ***wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików (*po zapisaniu przecinki zostają zamienione na średniki*), które mają być pomijane;

- ***wybrane typy plików*** — skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe niewykonywalne*), z uwzględnieniem multimediów (*plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowanie skróci się jeszcze bardziej, ponieważ takie pliku często są duże i niezbyt podatne na infekcje*). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

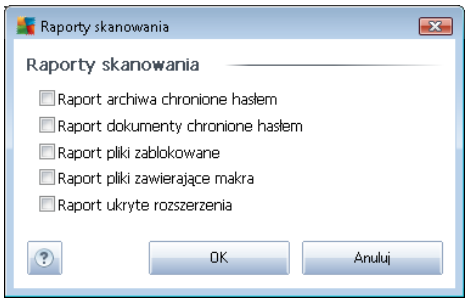
- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

Określ, jak długo ma trwać skanowanie

W obszarze ***Określ, jak długo ma trwać skanowanie*** można określić żądaną szybkość skanowania, która zależna jest od poziomu wykorzystania zasobów systemowych. Domyślna wartość tej opcji to poziom *Zależny od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Jeśli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowolnić działanie innych procesów i aplikacji (*opcji tej można śmiało używać wtedy, gdy komputer jest włączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

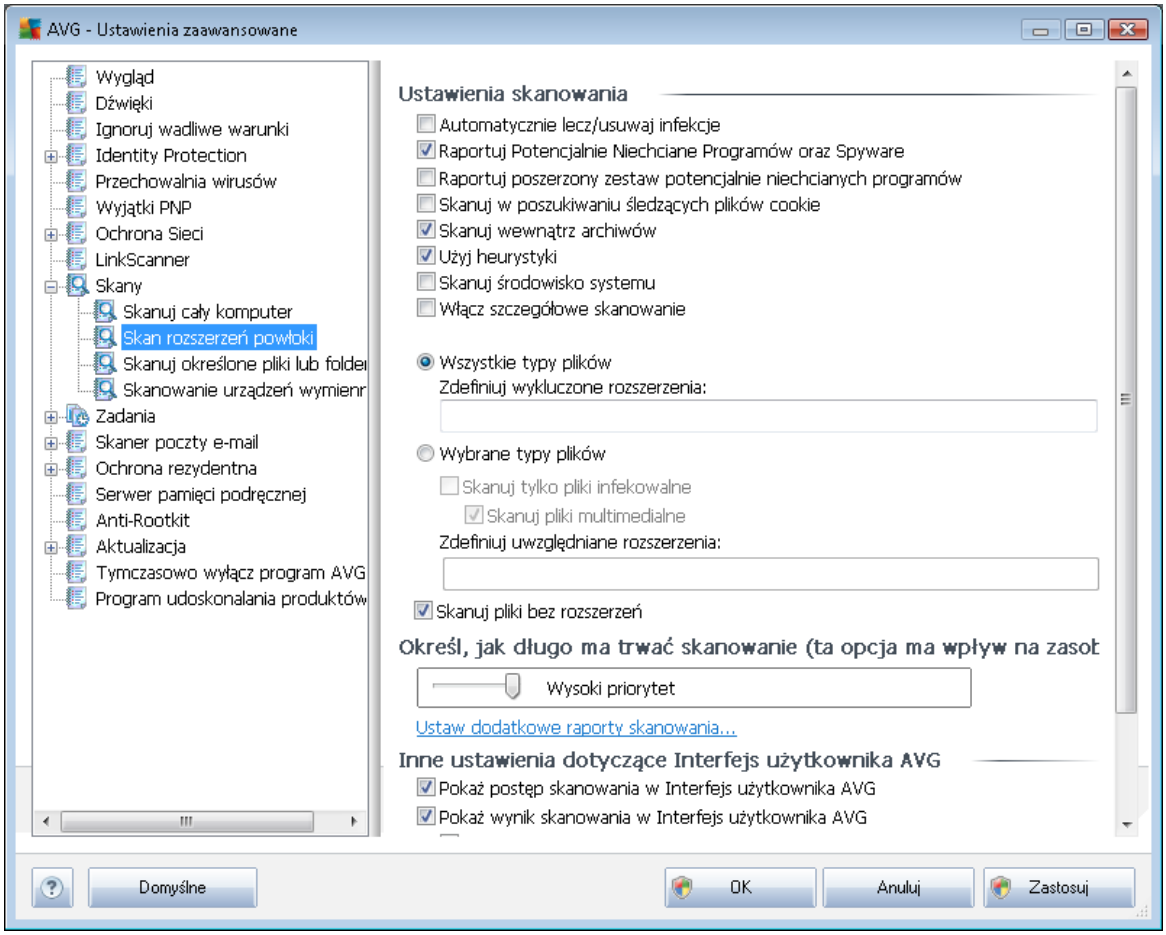
Ustaw dodatkowe raporty skanowania...

Kliknięcie linku ***Ustaw dodatkowe raporty skanowania...*** powoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym można określić szczegółowość raportów, zaznaczając żądane elementy:



9.8.2. Skan rozszerzenia powłoki

Analogicznie do testu ***Skan całego komputera***, test ***Skan rozszerzenia powłoki*** także oferuje szereg opcji umożliwiających edycję parametrów domyślnych. W tym przypadku konfiguracja odnosi się do skanowania określonych obiektów bezpośrednio z interfejsu Eksploratora Windows (*rozszerzenie powłoki*); zobacz rozdział ***Skanowanie z poziomu Eksploratora Windows***:



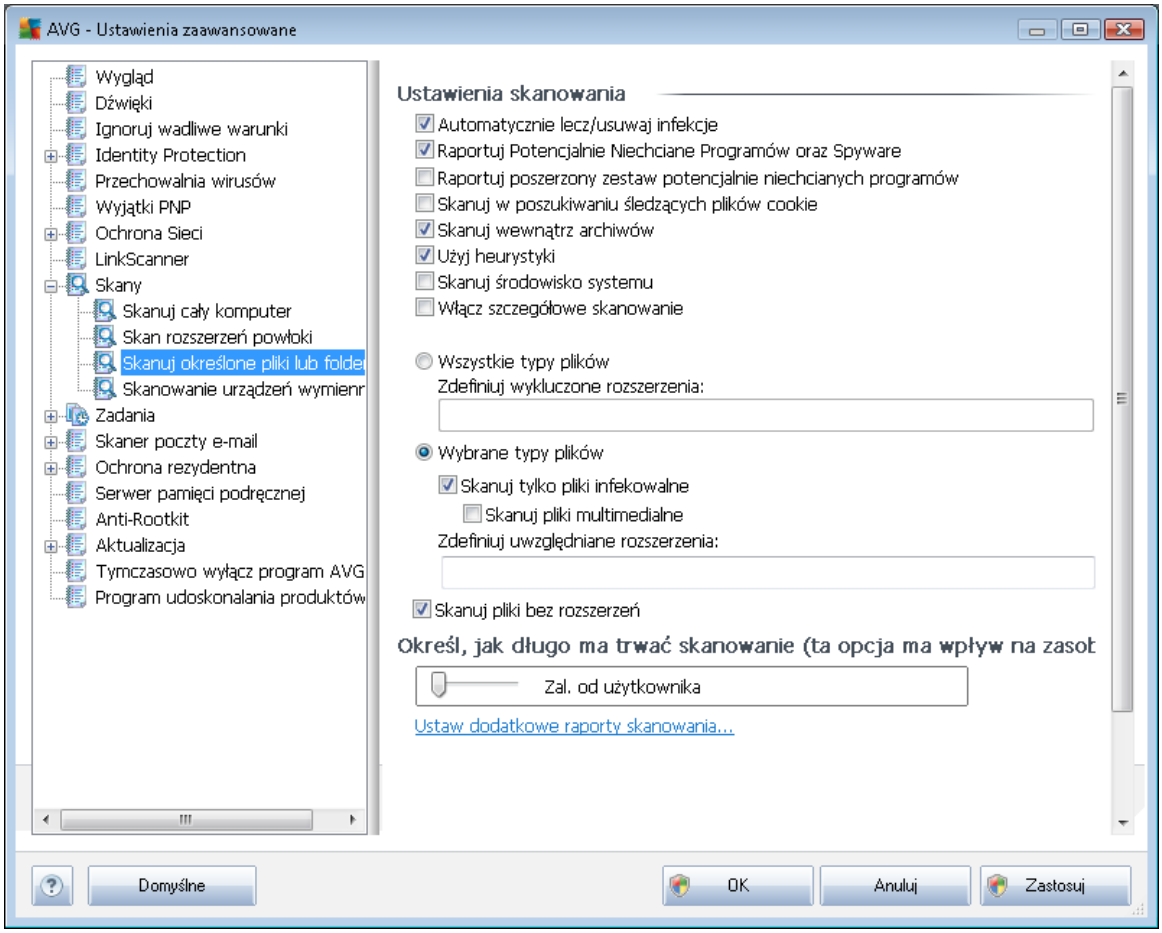
Lista parametrów jest identyczna jak dla testu ***Skan całego komputera***. Jednak ustawienia domyślne obu skanów różnią się (*np. skan całego komputera nie sprawdza archiwów, lecz skanuje środowisko systemowe, podczas gdy Skan rozszerzenia powłoki — odwrotnie*).

Uwaga: *Opis poszczególnych parametrów zawiera rozdział* ***Zaawansowane ustawienia AVG / Skany / Skan całego komputera***.

Podobnie do okna dialogowego ***Skan całego komputera,*** okno dialogowe ***Skan rozszerzenia powłoki*** również zawiera sekcję o nazwie ***Inne ustawienia...***, w której można określić, czy informacje o postępie i wynikach skanowania mają być dostępne z poziomu interfejsu użytkownika systemu AVG. Możliwa jest również taka konfiguracja, przy której wyniki skanowania będą prezentowane tylko w razie wykrycia infekcji.

9.8.3. Skan określonych plików lub folderów

Okno konfiguracji ***Skanu określonych plików lub folderów*** jest identyczne jak w przypadku testu ***Skan całego komputera***. Wszystkie opcje konfiguracyjne są takie same, jednak ustawienia domyślne dla ***skanu całego komputera*** są bardziej rygorystyczne:

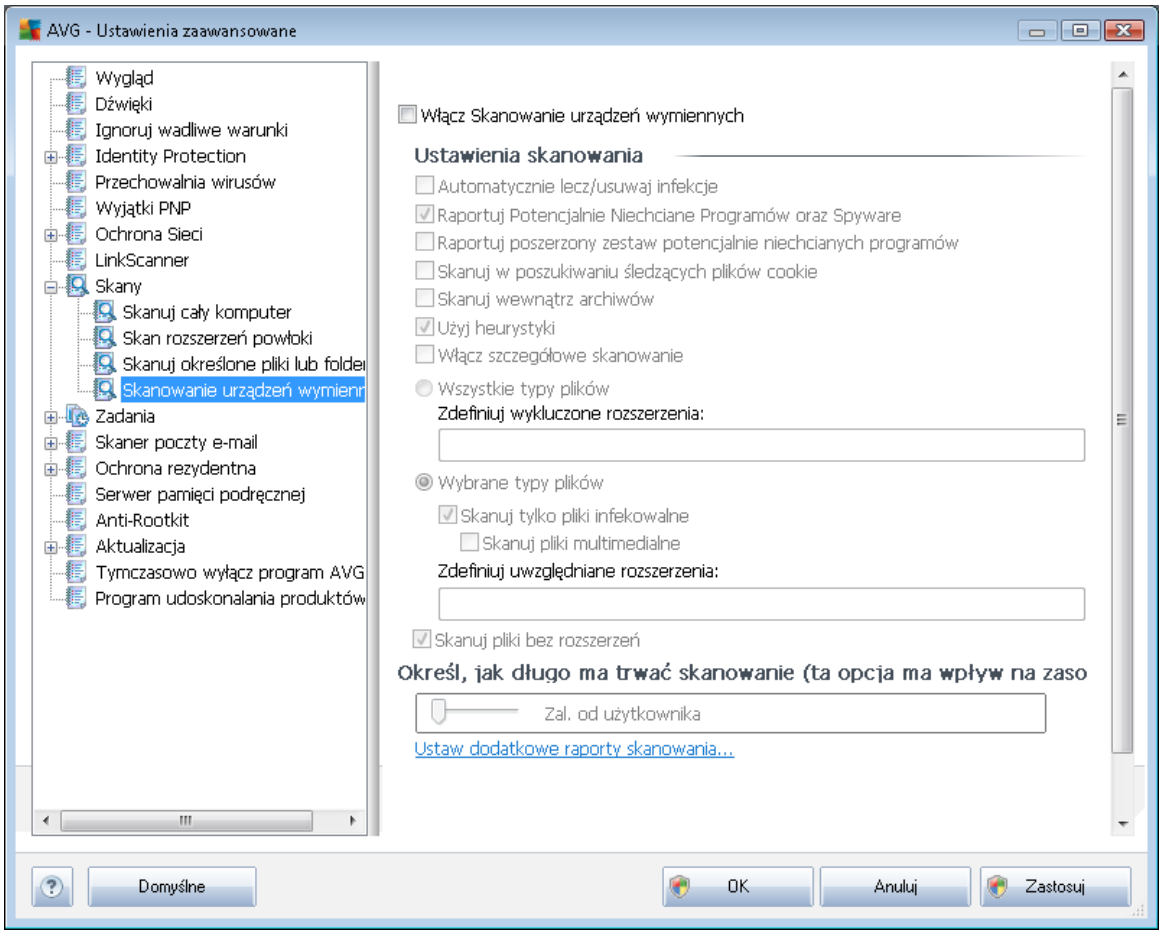


Wszystkie parametry ustawiane w tym oknie dialogowym odnoszą się tylko do obszarów wybranych do ***skanowania określonych plików lub folderów***!

Uwaga: *Opisy poszczególnych parametrów zawiera rozdział* ***Zaawansowane ustawienia AVG / Skany / Skan całego komputera***.

9.8.4. Skan urządzeń wymiennych

Okno konfiguracji ***Skanu urządzeń wymiennych*** jest również bardzo podobne do okna dialogowego ***Skan całego komputera***:



Skan urządzeń wymiennych jest uruchamiany automatycznie po podłączeniu do komputera dowolnego urządzenia wymiennego. Domyślnie jest on wyłączony. Skanowanie urządzeń wymiennych w poszukiwaniu potencjalnych zagrożeń jest jednak bardzo ważne, ponieważ są one częstym źródłem infekcji. Jeśli skanowanie ma być uruchamiane automatycznie, należy zaznaczyć opcję ***Włącz skanowanie urządzeń wymiennych***.

Uwaga: *Opisy poszczególnych parametrów zawiera rozdział* ***Zaawansowane ustawienia AVG / Skany / Skan całego komputera***.

9.9. Zaplanowane zadania

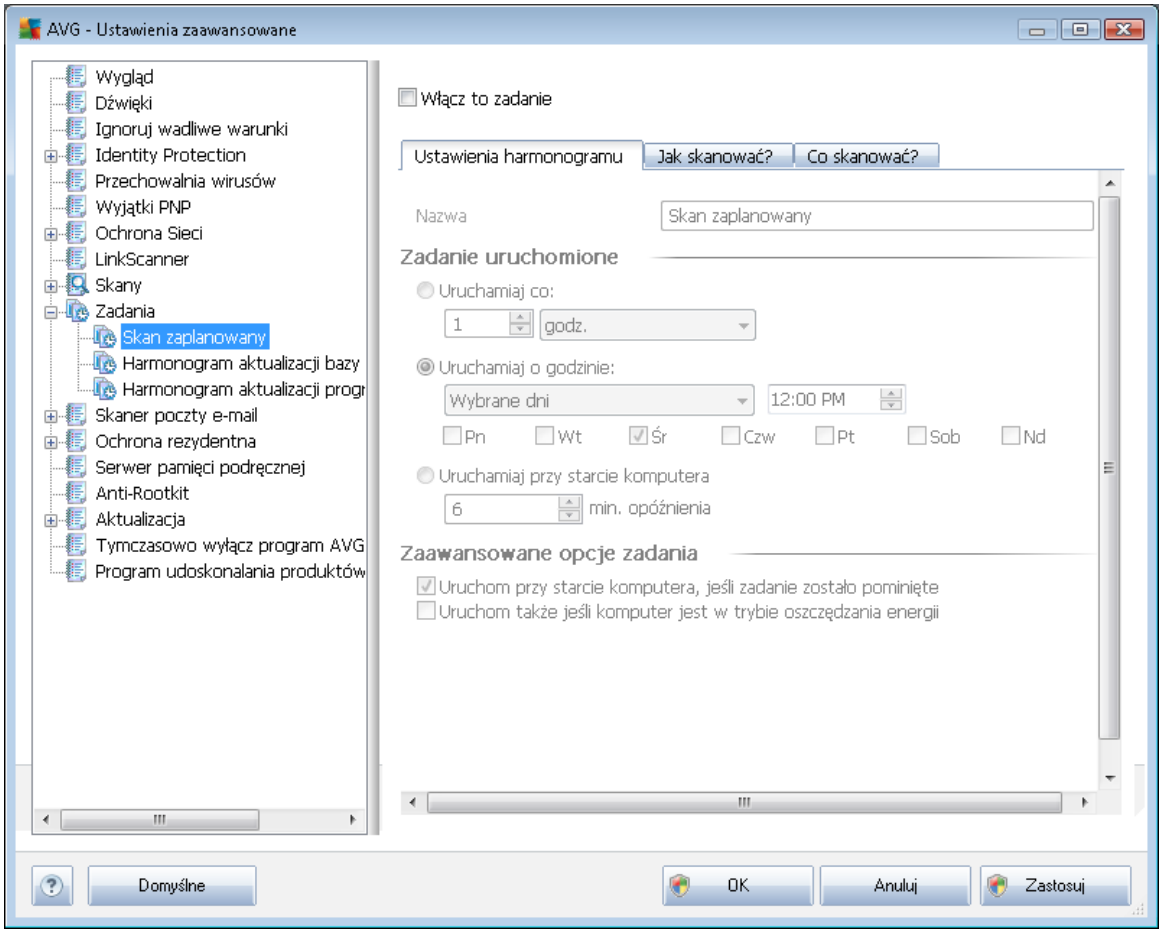
W oknie ***Zadania*** można edytować domyślne ustawienia następujących pozycji:

- Skan zaplanowany
- Harmonogram aktualizacji bazy wirusów

- Harmonogram aktualizacji programu

9.9.1. Skan zaplanowany

Parametry zaplanowanego skanu można edytować (*albo utworzyć nowy harmonogram*) na trzech kartach. Na każdej karcie można zaznaczyć pole ***Włącz to zadanie*** lub usunąć jego zaznaczenie, aby tymczasowo wyłączyć zaplanowany test lub włączyć go ponownie, gdy zajdzie taka potrzeba:



W polu tekstowym ***Nazwa*** (*wyłączone dla harmonogramów domyślnych*) wyświetlana jest nazwa przypisana do danego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (*aby dodać harmonogram, należy kliknąć prawym przyciskiem myszy element* ***Skan zaplanowany*** *w drzewie nawigacji po lewej*) można określić własną nazwę, a wspomniane pole tekstowe jest edytowalne. Należy używać krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości.

Przykład: *Nazwy takie jak „Nowy skan" lub „Mój skan" nie są odpowiednie, ponieważ nie informują o tym, co jest przedmiotem skanowania. Przykładem dobrej opisowej nazwy jest „Skan obszarów systemowych". Ponadto, nie ma potrzeby określać w nazwie skanowania, czy skanowany jest cały komputer, czy tylko jego wybrane obszary — własne testy użytkownika są zawsze specyficznym skanowaniem określonych plików lub folderów.*

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

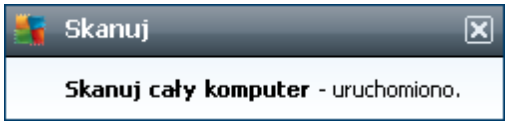
Zadanie uruchomione

W tym miejscu można określić, jak często ma być uruchamiane nowe skanowanie. Uruchamianie skanowania może być powtarzane w określonych odstępach czasu (***Uruchamiaj co***) lub w zadanych momentach (***Uruchamiaj o określonej godzinie***), a także na skutek wystąpienia określonego zdarzenia (***akcja powiązana z uruchomieniem komputera***).

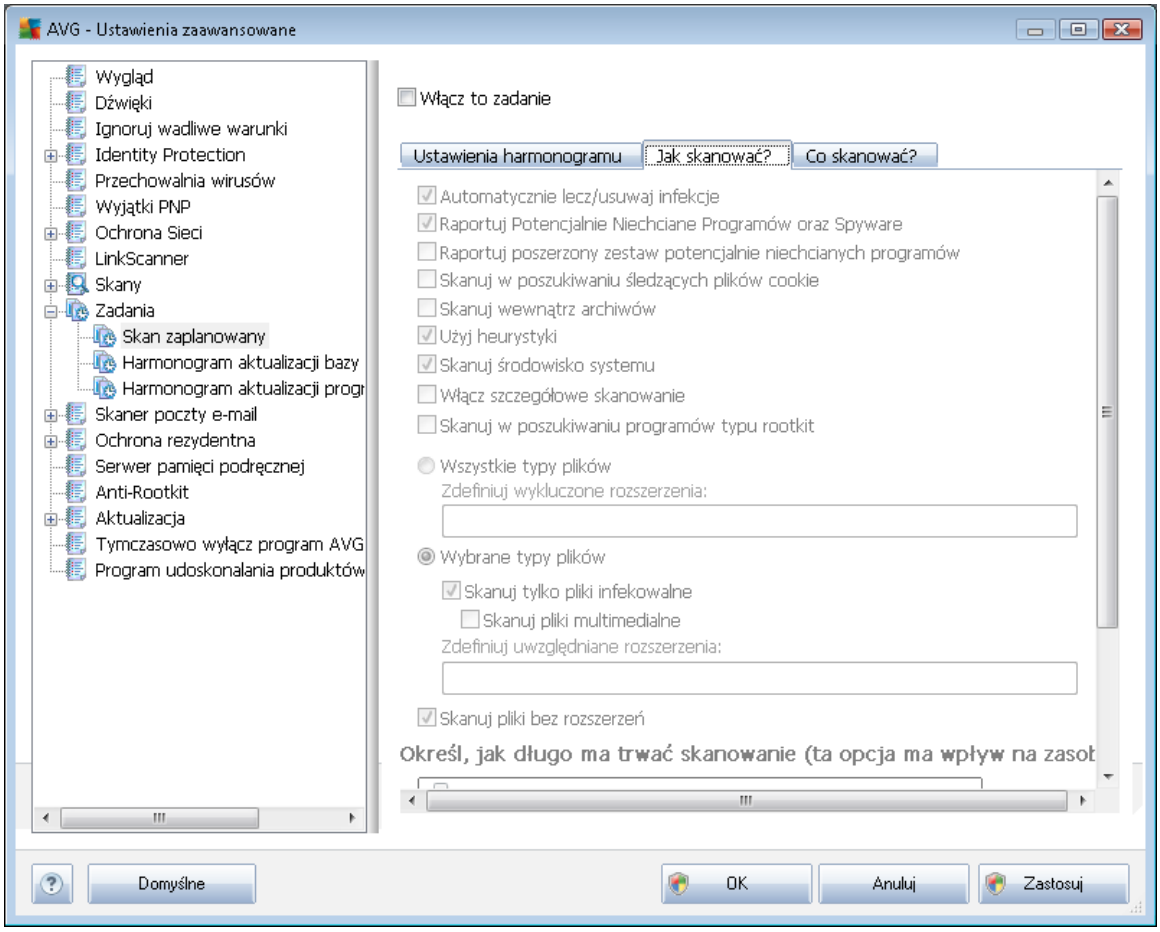
Zaawansowane opcje harmonogramu

Ta sekcja umożliwia zdefiniowanie warunków uruchamiania skanowania w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

Po rozpoczęciu zaplanowanego skanu, nad ikoną AVG na pasku zadań wyświetlone zostanie odpowiednie powiadomienie:



Następnie pojawi się nowa ikona AVG na pasku zadań (*kolorowa, z białą strzałką — jak powyżej*), która informuje o uruchomieniu zaplanowanego skanowania. Kliknięcie ikony uruchomionego skanowania AVG prawym przyciskiem myszy pozwala wyświetlić menu kontekstowe, za pomocą którego można wstrzymać lub zatrzymać skanowanie, a także zmienić jego priorytet:



Karta ***Jak skanować?*** zawiera listę parametrów testu, które można włączyć lub wyłączyć. Domyślnie większość funkcji jest włączona, a odpowiadające im ustawienia są stosowane podczas skanowania. Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachowując wstępnie zdefiniowaną konfigurację:

- ***Automatycznie lecz/usuwaj infekcje*** *(opcja domyślnie włączona)* — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do***Przechowalni wirusów***.

- ***Raportuj potencjalnie niechciane programy i spyware*** *(opcja domyślnie włączona)* — zaznaczenie tego pola powoduje włączenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a także wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość

oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

- ***Skanuj w poszukiwaniu śledzących plików cookie*** (*opcja domyślnie wyłączona*) — ten parametr składnika ***Anti-Spyware*** określa, czy wykrywane mają być pliki cookie (*używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** (*opcje domyślnie wyłączona*) — parametr określa, że skanowanie ma obejmować wszystkie pliki, nawet te znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- ***Użyj heurystyki*** (*opcja domyślnie włączona*) — analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) będzie jedną z metod wykrywania wirusów w czasie skanowania.

- ***Skanuj środowisko systemu*** (*opcja domyślnie włączona*) — skanowanie obejmie także obszary systemowe komputera.

- ***Włącz szczegółowe skanowanie*** (*domyślnie wyłączone*) — w określonych sytuacjach (*gdy zachodzi podejrzenie, że komputer jest zainfekowany*) można zaznaczyć tę opcję, aby aktywować algorytmy bardziej dokładnego skanowania, które w celu uzyskania absolutnej pewności będą skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

- ***Skanuj w poszukiwaniu programów typu rootkit*** (*opcja domyślnie wyłączona*) — zaznaczenie tej pozycji pozwala włączyć wykrywanie programów typu rootkit do operacji skanowania całego komputera. Test Anti-Rootkit można także uruchomić niezależnie, dzięki interfejsowi składnika ***Anti-Rootkit***

Następnie należy zdecydować, czy skanowane mają być

- ***wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików (*po zapisaniu przecinki zostają zamienione na średniki*), które mają być pomijane;

- ***wybrane typy plików*** — skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe i niewykonywalne*), z uwzględnieniem multimediów (*plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże i niezbyt podatne na infekcje*). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

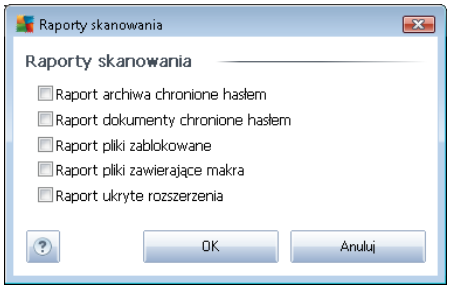
- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

Określ, jak długo ma trwać skanowanie

W obszarze ***Określ, jak długo ma trwać skanowanie*** można określić żądaną szybkość skanowania, w zależności od wykorzystania zasobów systemowych. Domyślna wartość tej opcji to poziom *Zależny od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Jeśli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowolnić działanie innych procesów i aplikacji (*opcji tej można śmiało używać, gdy komputer jest włączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

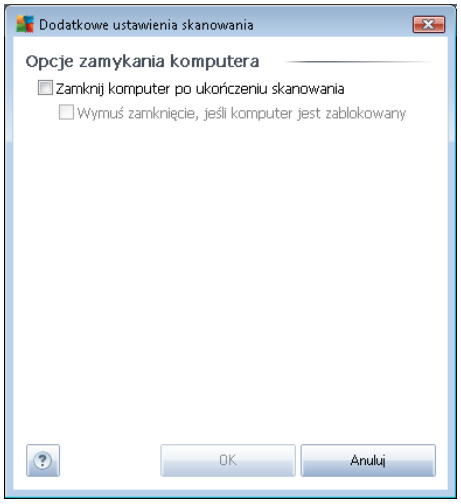
Ustaw dodatkowe raporty skanowania

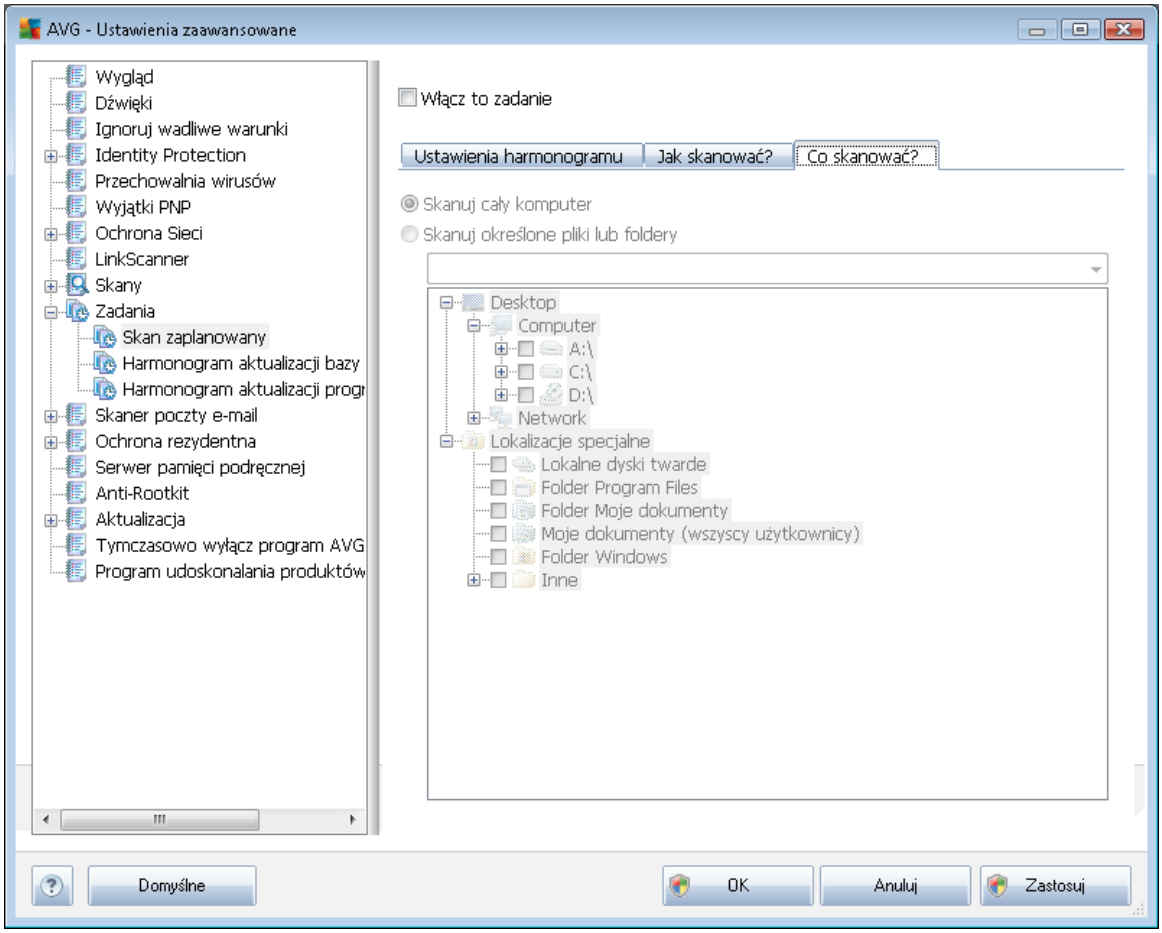
Kliknięcie linku ***Ustaw dodatkowe raporty skanowania...*** spowoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym można określić szczegółowość raportów, zaznaczając żądane elementy:



Dodatkowe ustawienia skanowania

Dodatkowe ustawienia skanowania — ten link pozwala otworzyć nowe okno dialogowe ***Opcje zamykania komputera***, w którym można określić, czy komputer ma być zamykany automatycznie po zakończeniu procesu skanowania. Wybranie opcji (***Zamknij komputer po ukończeniu skanowania***) spowoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet wtedy, gdy w danej chwili jest on zablokowany (***Wymuś zamknięcie, jeśli komputer jest zablokowany***).



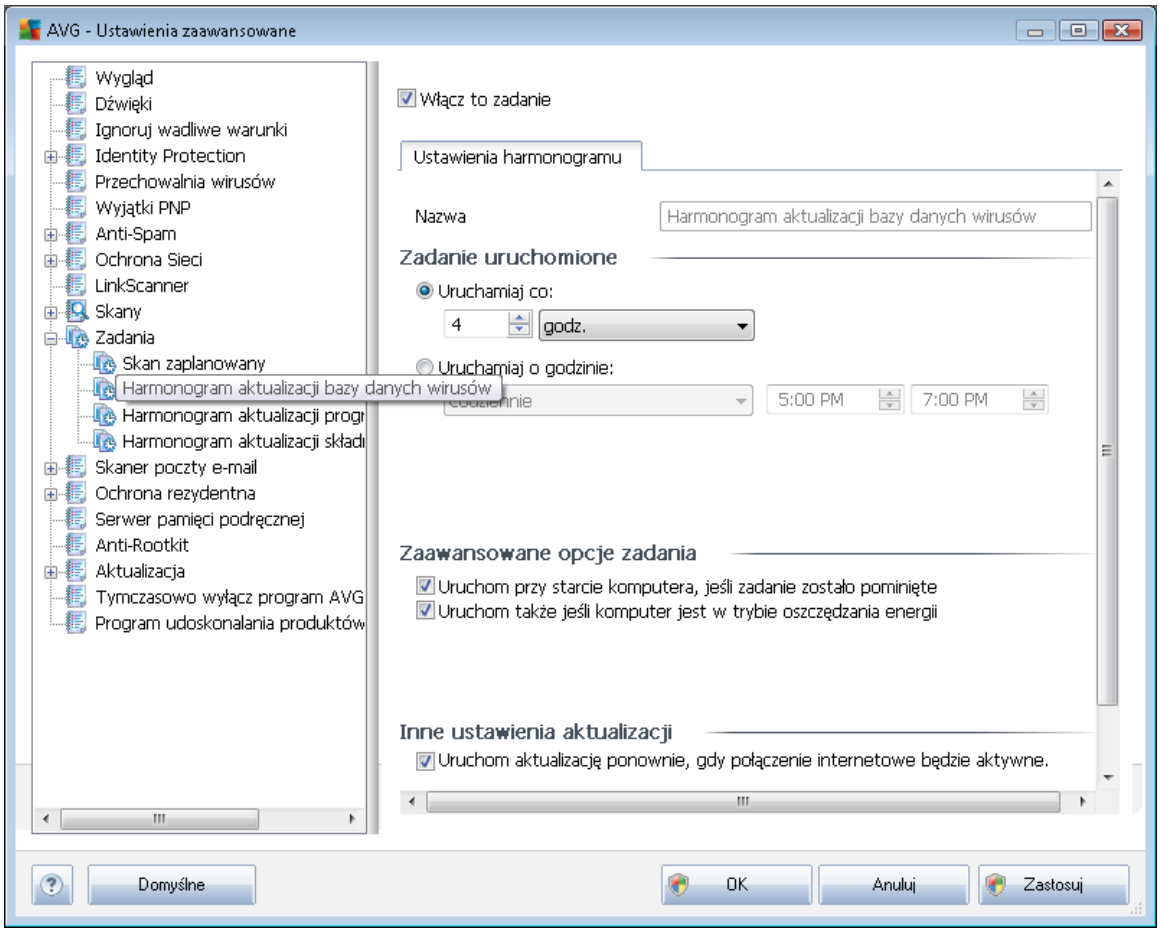


Na karcie ***Co skanować?*** można określić, czy planowane jest skanowanie całego komputera, czy skanowanie określonych plików lub folderów. W przypadku skanowania określonych plików lub folderów, w dolnej części okna dialogowego aktywowane jest drzewo katalogów, w którym można

wybrać obiekty do przeskanowania.

9.9.2. Harmonogram aktualizacji bazy wirusów

Jeśli ***jest to naprawdę konieczne***, tymczasowo można dezaktywować zaplanowaną aktualizację bazy wirusów, usuwając zaznaczenie pola ***Włącz to zadanie*** i zaznaczając je ponownie później:



Podstawowe opcje harmonogramu aktualizacji bazy wirusów dostępne są w składniku ***Menedżer aktualizacji***. W niniejszym oknie można ustawić szczegółowe parametry harmonogramu. W polu tekstowym ***Nazwa*** (*wyłączone dla harmonogramów domyślnych*) jest wyświetlana nazwa przypisana do tego harmonogramu przez producenta programu.

Zadanie uruchomione

W tej sekcji należy określić interwał dla planowanych aktualizacji bazy danych wirusów. Można zaplanować uruchamianie aktualizacji stale co pewien czas (***Uruchom co ...***) lub definiując określoną datę i godzinę (***Uruchom o określonej godzinie ...***).

Zaawansowane opcje harmonogramu

Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji bazy wirusów w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

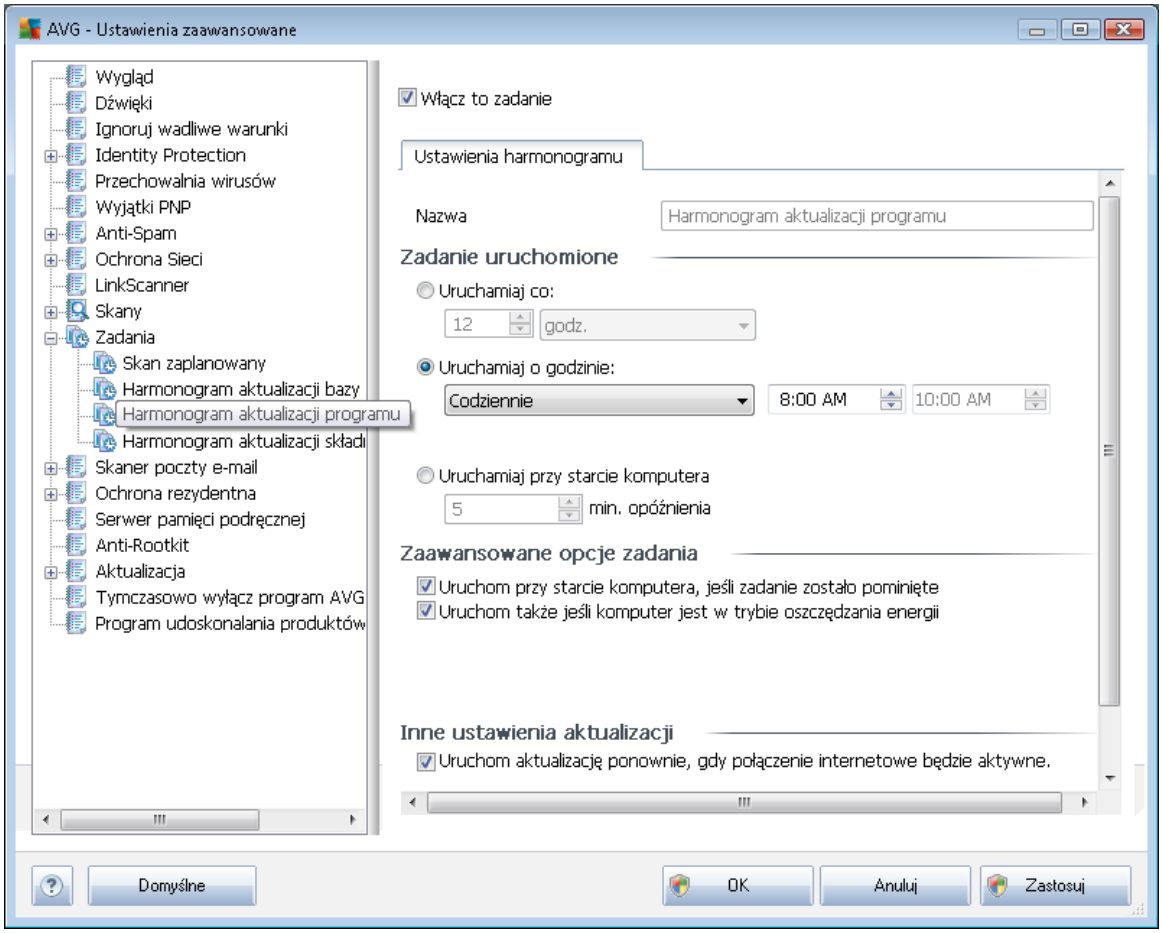
Inne ustawienia aktualizacji

Na koniec należy zaznaczyć pole wyboru ***Uruchom aktualizację natychmiast po nawiązaniu połączenia z internetem***, aby upewnić się, że jeśli połączenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie się, po ponownym połączeniu z internetem aktualizacja zostanie rozpoczęta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o określonej godzinie, nad ikoną AVG na pasku systemowym wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wygląd***).

9.9.3. Harmonogram aktualizacji programu

Jeśli ***jest to naprawdę konieczne***, tymczasowo można dezaktywować zaplanowaną aktualizację programu, usuwając zaznaczenie pola ***Włącz to zadanie*** i zaznaczając je ponownie później:



W polu tekstowym ***Nazwa*** (*nieaktywne dla harmonogramów domyślnych*) wyświetlana jest nazwa

przypisana do tego harmonogramu przez producenta programu.

Zadanie uruchomione

W tym miejscu należy określić interwał dla nowo zaplanowanych aktualizacji programu. Uruchamianie aktualizacji może być powtarzane w określonych odstępach czasu (***Uruchamiaj co***) lub w zadanych momentach (***Uruchamiaj o określonej godzinie***), a także na skutek wystąpienia określonego zdarzenia (***akcja powiązana z uruchomieniem komputera***).

Zaawansowane opcje harmonogramu

Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji programu w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

Inne ustawienia aktualizacji

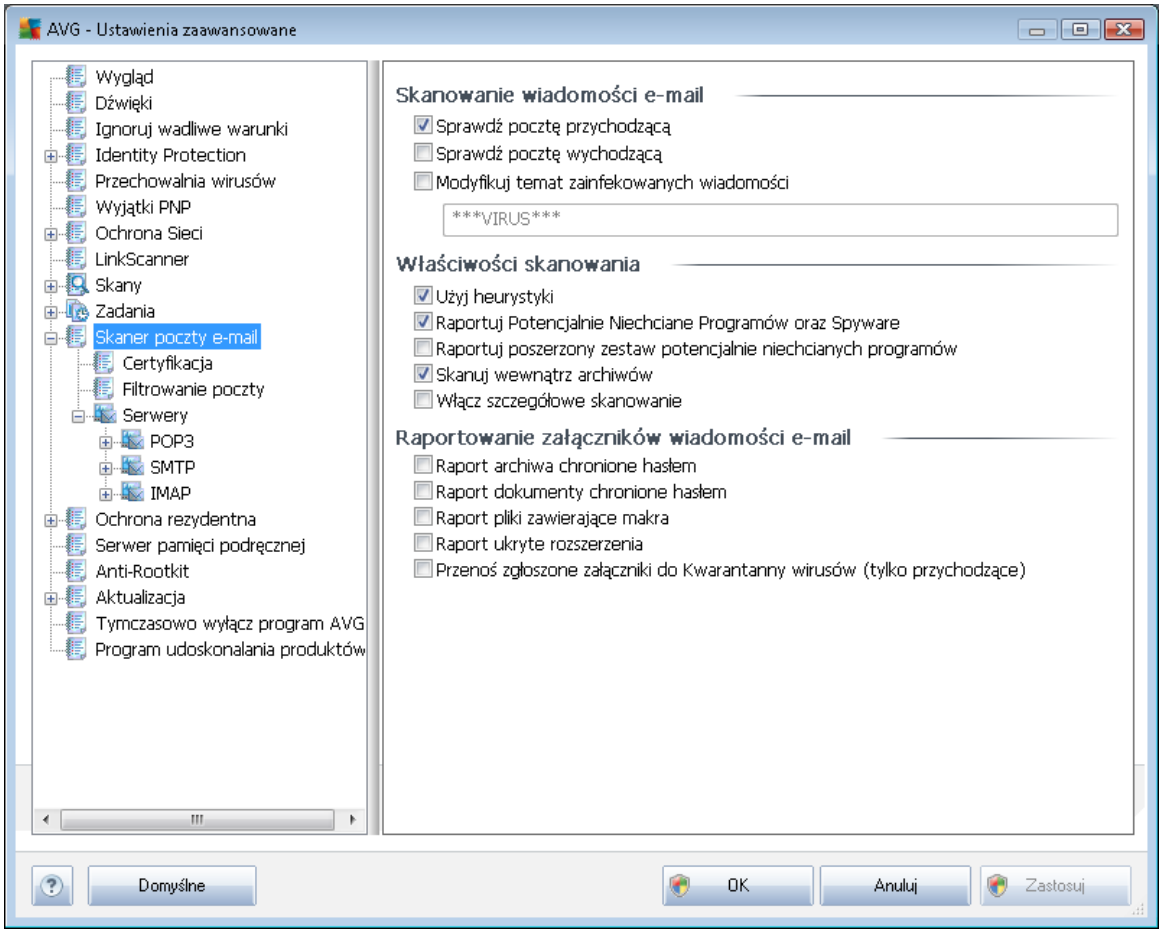
Na koniec należy zaznaczyć pole wyboru ***Uruchom aktualizację natychmiast po nawiązaniu połączenia z internetem***, aby upewnić się, że jeśli połączenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie się, po ponownym połączeniu z internetem aktualizacja zostanie rozpoczęta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o określonej godzinie, nad ikoną AVG na pasku systemowym wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wygląd***).

Uwaga: *Jeśli zaplanowane skanowanie i zaplanowana aktualizacja nałożą się, proces aktualizacji będzie miał pierwszeństwo i skanowanie zostanie przerwane.*

9.10. Skaner poczty e-mail

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



Skanowanie wiadomości e-mail

W tej sekcji można określić następujące, podstawowe ustawienia dla przychodzących i wychodzących wiadomości e-mail:

- ***Sprawdzaj pocztę przychodzącą*** (*domyślnie włączone*) — zaznacz lub odznacz to pole, aby włączyć/wyłączyć opcję skanowania wszystkich wiadomości e-mail dostarczanych do klienta poczty e-mail.

- ***Sprawdzaj pocztę wychodzącą*** (*domyślnie wyłączone*) — zaznacz lub odznacz to pole, aby włączyć/wyłączyć opcję skanowania wszystkich wiadomości e-mail wysyłanych z klienta poczty e-mail.

- ***Modyfikuj temat zainfekowanych wiadomości*** (*domyślnie wyłączone*)) — jeśli chcesz otrzymywać ostrzeżenia o tym, że przeskanowana wiadomość e-mail została wykryta jako zainfekowana, zaznacz to pole i wprowadź żądany tekst w polu tekstowym. Ten tekst będzie dodawany do tematu każdej wykrytej zainfekowanej wiadomości e-mail, aby ułatwić

ich identyfikowanie i filtrowanie. Wartość domyślna to ***WIRUS***; zaleca się jej zachowanie.

Właściwości skanowania

W tej sekcji można określić sposób skanowania wiadomości e-mail:

- ***Użyj analizy heurystycznej*** (*domyślnie włączone*) — zaznaczenie tego pola umożliwia korzystanie z analizy heurystycznej podczas skanowania wiadomości e-mail. Gdy ta opcja jest włączona, możliwe jest filtrowanie załączników nie tylko według ich rozszerzenia, ale również na podstawie ich właściwej zawartości. Opcje filtrów mogą zostać dostosowane w oknie ***Filtrowanie poczty***.

- ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje aktywowanie silnika ***Anti-Spyware*** i skanowanie w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

- ***Skanuj wewnątrz archiwów*** (*domyślnie włączone*) — zaznaczenie tego pola umożliwia skanowanie zawartości archiwów dołączonych do wiadomości e-mail.

- ***Włącz szczegółowe skanowanie*** (*domyślnie wyłączone*) — w określonych sytuacjach (*np. gdy zachodzi podejrzenie, że komputer jest zainfekowany przez wirus lub exploit*) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będą one skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

Raportowanie załączników wiadomości

W tej sekcji można skonfigurować dodatkowe raporty dotyczące potencjalnie niebezpiecznych lub podejrzanych plików. Należy zwrócić uwagę na fakt, że Skaner poczty e-mail nie wyświetla zazwyczaj żadnych komunikatów z ostrzeżeniem, a jedynie dodaje na końcu wiadomości tekst certyfikacji. Historię działań tego składnika można przejrzeć w oknie Zagrożenia wykryte przez Skaner poczty e-mail:

- ***Raportuj archiwa chronione hasłem*** — archiwów (*ZIP, RAR itp.*) chronionych hasłem nie można skanować w poszukiwaniu wirusów. Należy zaznaczyć to pole wyboru, aby system AVG zgłaszał je jako potencjalnie niebezpieczne.

- ***Raportuj dokumenty chronione hasłem*** — dokumentów chronionych hasłem nie można skanować w poszukiwaniu wirusów. Należy zaznaczyć to pole wyboru, aby system AVG zgłaszał je jako potencjalnie niebezpieczne.

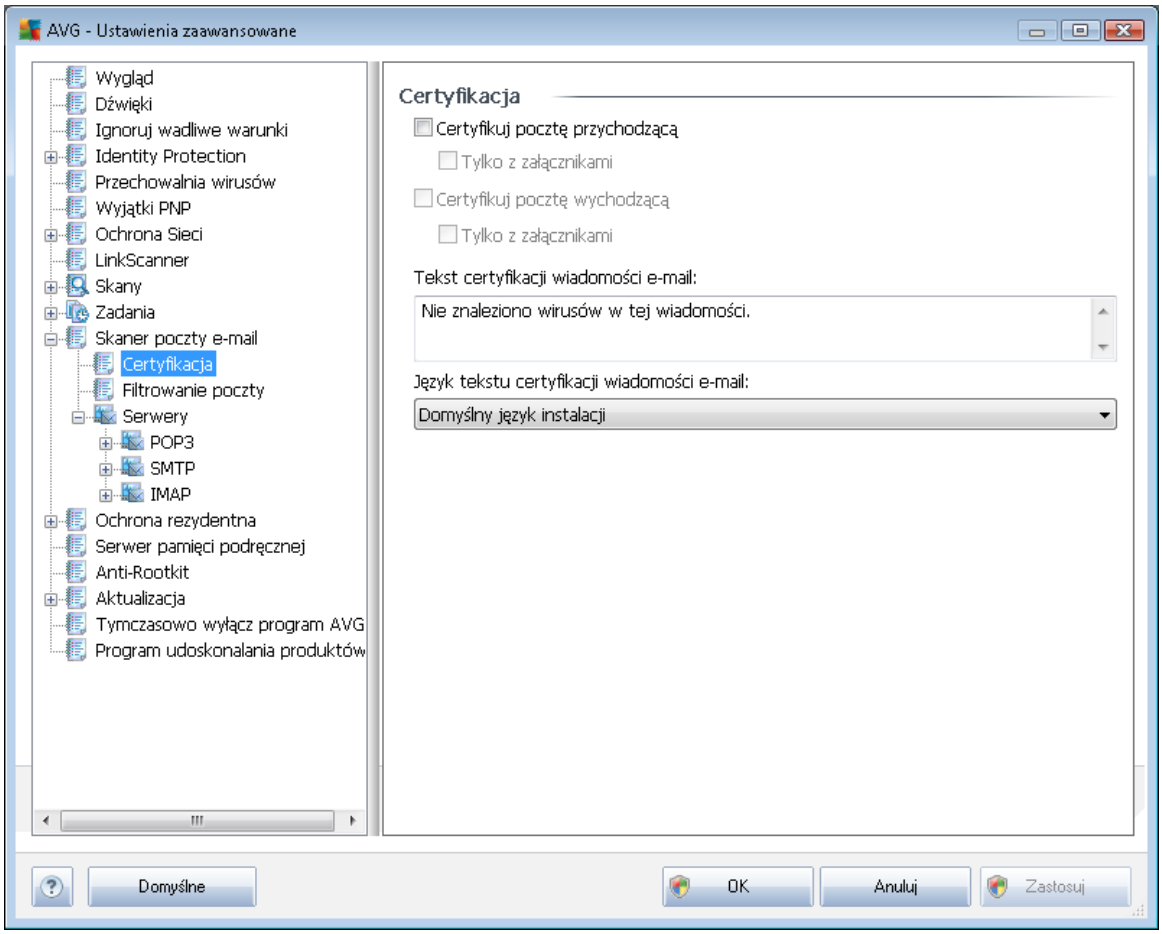
- ***Raportuj pliki zawierające makra*** — makro to predefiniowana sekwencja kroków mająca ułatwiać wykonywanie określonych czynności (*szeroko znane są na przykład makra programu MS Word*). Makra mogą być potencjalnie niebezpieczne — warto zaznaczyć to pole, aby mieć pewność, że pliki zawierające makra będą raportowane jako podejrzane.

- ***Raportuj ukryte rozszerzenia*** — ukryte rozszerzenia mogą maskować podejrzane pliki wykonywalne (np. plik.txt.exe) jako niegroźne pliki tekstowe (np. plik.txt). Należy zaznaczyć to pole wyboru, aby zgłaszać je jako potencjalnie niebezpieczne.

- ***Przenoś raportowane załączniki do Przechowalni wirusów*** — możesz skonfigurować system AVG tak, aby powiadamiał Cię poprzez e-mail o wykrytych archiwach i dokumentach zabezpieczonych hasłem, plikach zawierających makra lub ukrytych rozszerzeniach, które zostaną wykryte w załącznikach skanowanych wiadomości. Należy także określić, czy w przypadku wykrycia takiej wiadomości podczas skanowania zainfekowany obiekt ma zostać przeniesiony do ***Przechowalni wirusów***.

9.10.1. Certyfikacja

W oknie dialogowym ***Ceryfikacja*** można określić tekst i język certyfikacji dla poczty przychodzącej i wychodzącej:



Tekst certyfikacji składa się z dwóch części: części użytkownika i części systemowej — w poniższym przykładzie pierwszy wiersz reprezentuje część użytkownika, a pozostała część jest generowana automatycznie przez system:

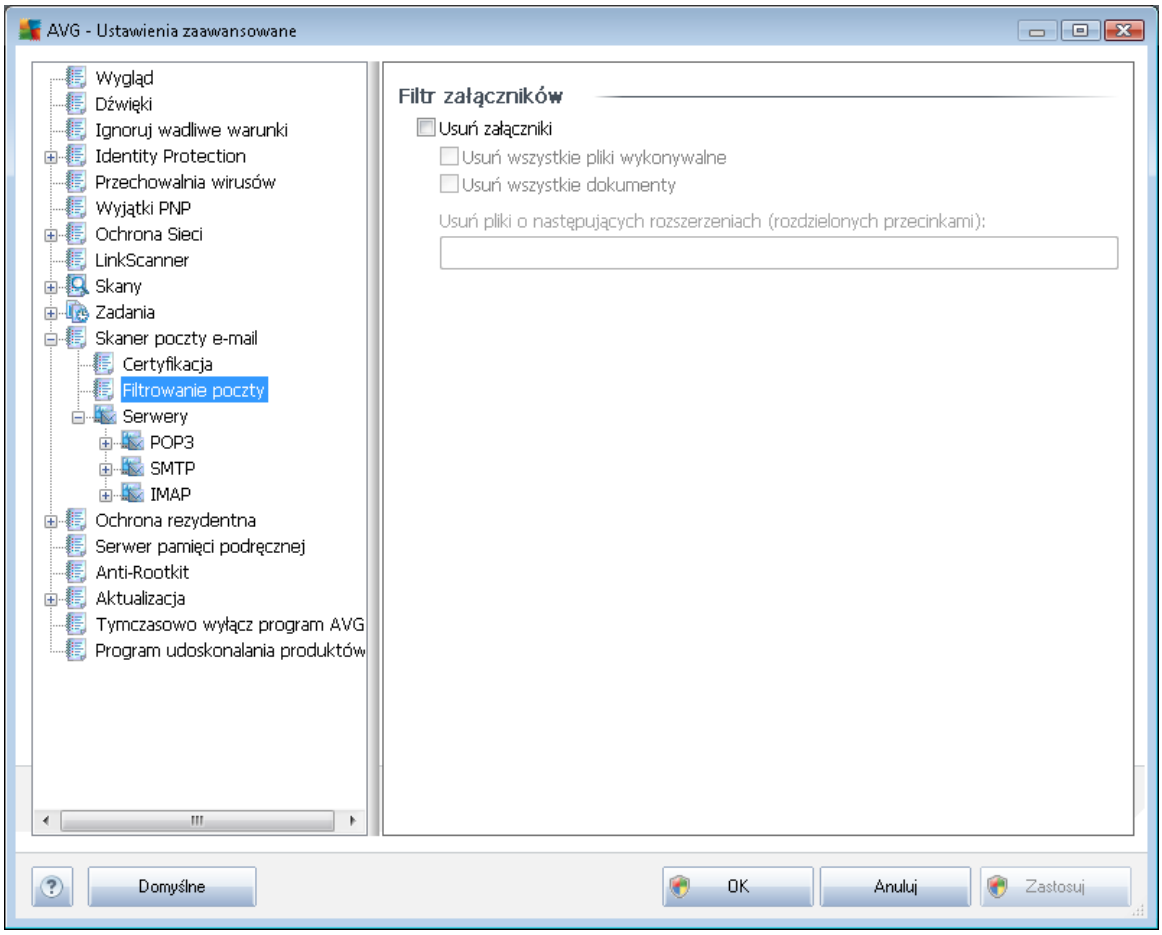
Nie znaleziono wirusów w tej wiadomości.

Sprawdzone przez system AVG.

Wersja: x.y.zz / Baza danych: xx.y.z — Data wydania: 12/9/2010

Jeśli zdecydujesz się korzystać z certyfikacji, w tym samym oknie będziesz mógł zdefiniować treść części użytkownika (***Tekst certyfikacji wiadomości e-mail***) i wybrać język, który ma być używany dla automatycznie generowanej części systemowej (***Język tekstu certyfikacji wiadomości e-mail***).

9.10.2. Filtrowanie poczty

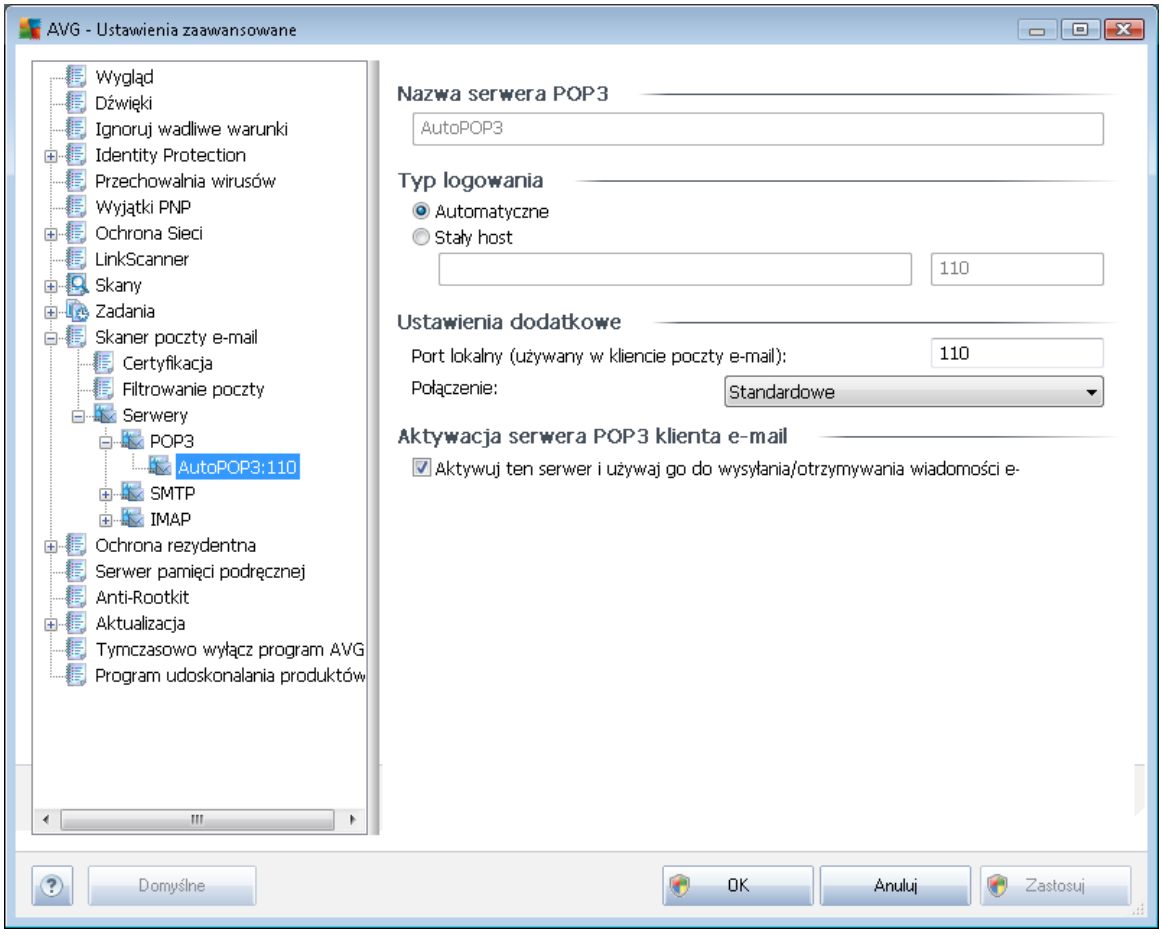


W oknie ***Filtr załączników*** można ustawiać parametry skanowania załączników e-mail. Opcja ***Usuń załączniki*** jest domyślnie wyłączona. Jeśli zostanie włączona, wszystkie załączniki wiadomości zidentyfikowane jako zainfekowane lub potencjalnie niebezpieczne, będą automatycznie usuwane. Aby określić typy załączników, które mają być usuwane, należy zaznaczyć odpowiednią opcję:

- ***Usuń wszystkie pliki wykonywalne*** — usunięte będą wszystkie pliki *.exe.
- ***Usuń wszystkie dokumenty*** — usunięte zostaną wszystkie pliki *.doc, *.docx, *.xls, *.xlsx.
- ***Usuń pliki o następujących rozszerzeniach oddzielonych przecinkami*** — usunięte będą wszystkie pliki o zdefiniowanych rozszerzeniach.

9.10.3. Serwery

W sekcji ***Serwery*** edytować można parametry wirtualnych serwerów ***Skanera poczty e-mail*** lub zdefiniować nowy (klikając przycisk ***Dodaj nowy serwer***).



W tym oknie dialogowym (*dostępnym z menu* ***Serwery / POP3***) można zdefiniować nowy ***Skaner poczty e-mail*** serwer poczty przychodzącej, korzystający z protokołu POP3:

- ***Nazwa serwera PO3*** — w tym polu można podać nazwę nowo dodanego serwera (*aby dodać serwer POP3, kliknij prawym przyciskiem myszy pozycję POP3 w menu nawigacyjnym po lewej stronie*). W przypadku automatycznie utworzonego serwera AutoPOP3 to pole jest nieaktywne.

- ***Typ logowania*** — definiuje metodę określania serwera pocztowego dla wiadomości przychodzących:

  - ***Automatycznie*** — logowanie jest przeprowadzane automatycznie zgodnie z ustawieniami klienta poczty e-mail.

  - ***Stały host*** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Login użytkownika pozostaje niezmieniony. Jako nazwy można użyć nazwy domeny (*np. pop.domena.com*) lub adresu IP (*np. 123.45.67.89*)). Jeśli serwer pocztowy używa niestandardowego portu, można podać go po dwukropku, zaraz za nazwą serwera (*np. pop.domena.com:8200*). Standardowym portem protokołu POP3 jest

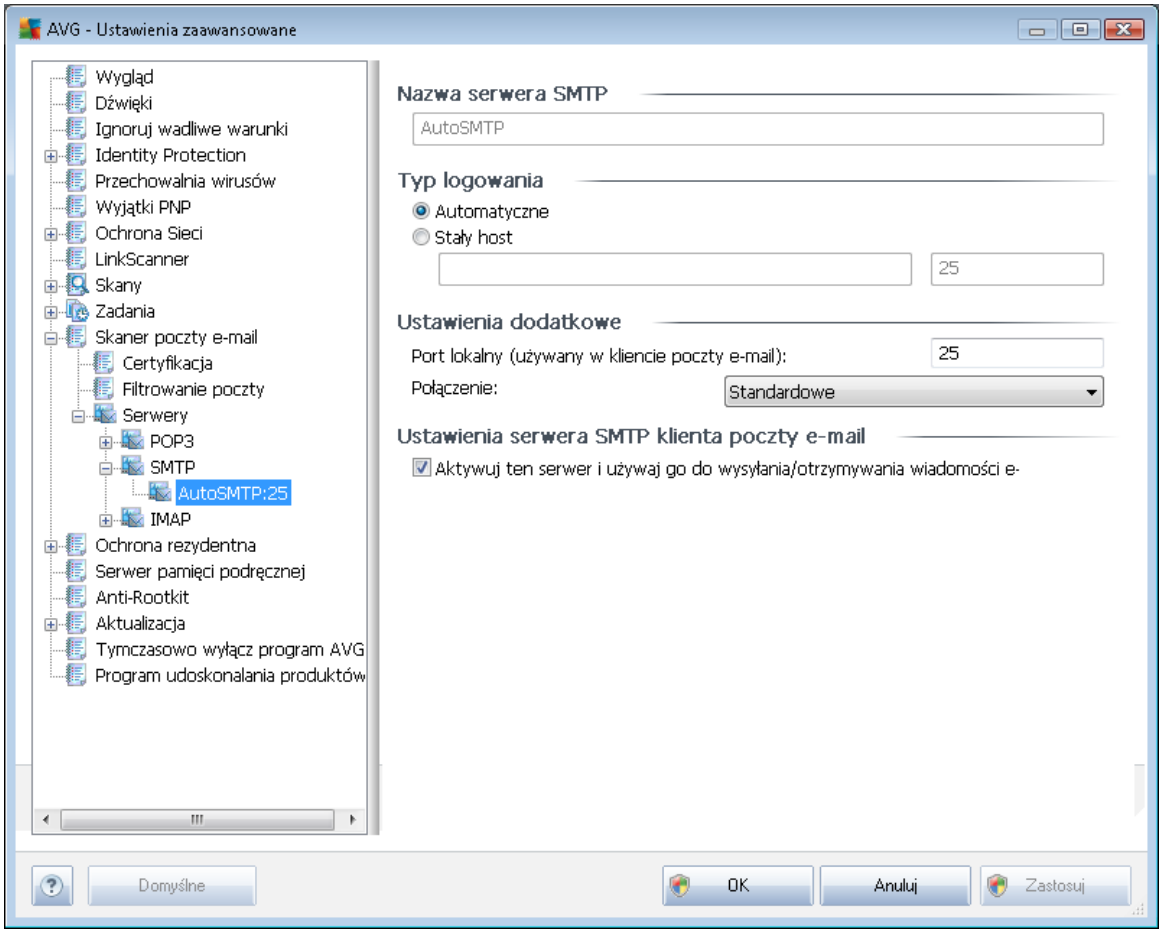
110.

- ***Ustawienia dodatkowe*** — pozwalają zdefiniować bardziej szczegółowe parametry:

  - ***Port lokalny*** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w kliencie poczty jako port docelowy serwera POP3.

  - ***Połączenie*** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślne SSL*). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.

- ***Aktywacja serwera POP 3 klienta poczty e-mail*** — opcję tę należy zaznaczyć, aby aktywować określony serwer POP3.

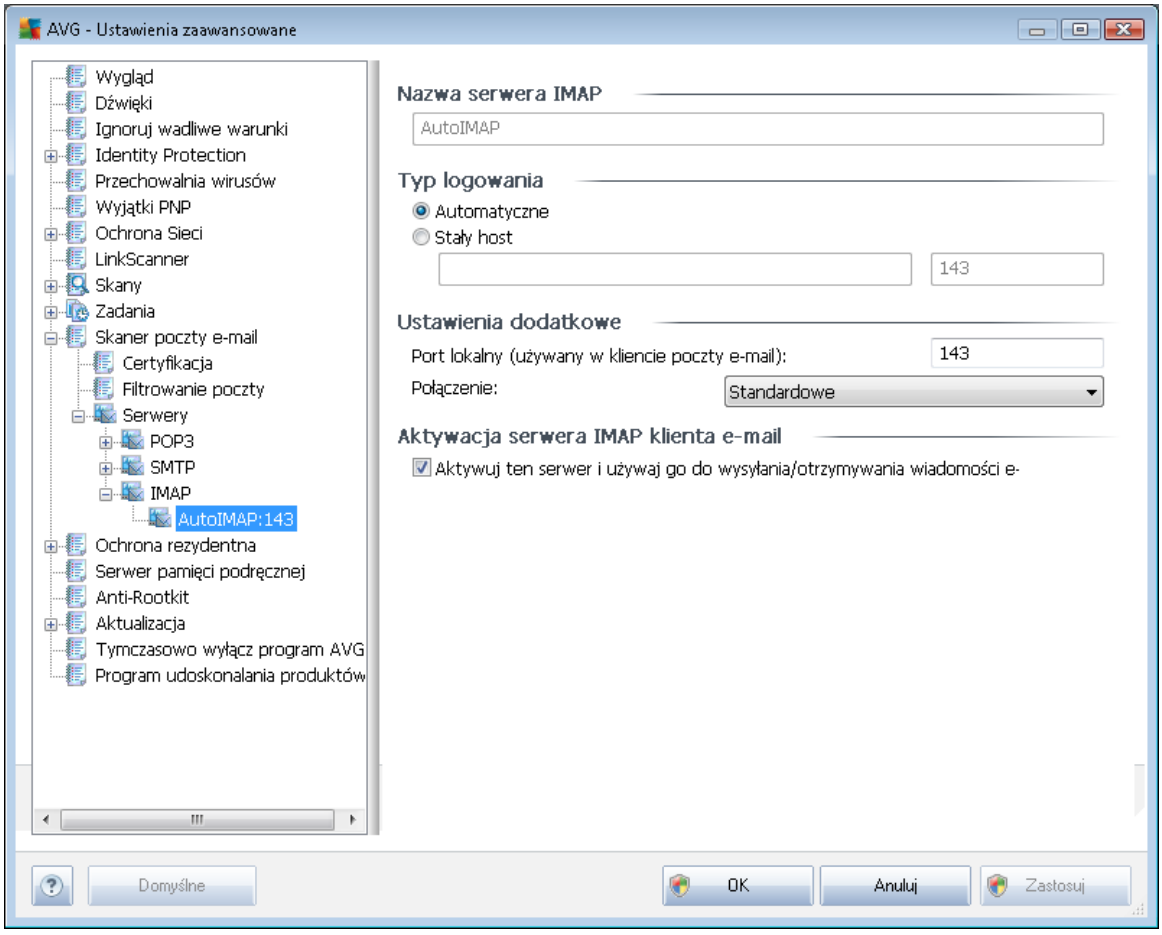


W tym oknie dialogowym (*dostępnym z menu* ***Serwery / SMTP***) można skonfigurować nowy ***Skaner poczty e-mail*** serwer poczty wychodzącej, korzystający z protokołu SMTP:

- ***Nazwa serwera SMTP*** — w tym polu można podać nazwę nowo dodanego serwera (*aby*

dodać serwer SMTP, kliknij prawym przyciskiem myszy pozycję SMTP w menu nawigacyjnym po lewej stronie). W przypadku automatycznie utworzonego serwera AutoSMTP to pole jest nieaktywne.

- ***Typ logowania*** — definiuje metodę określania serwera pocztowego dla wiadomości wychodzących:
    - ***Automatyczne*** — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail
    - ***Stały host*** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Można użyć nazwy domeny (*np. smtp.domena.com*) lub adresu IP (*np. 123.45.67.89)*). Jeśli serwer pocztowy używa niestandardowego portu, można podać go po dwukropku za nazwą serwera (*np. smtp.domena.com:8200*). Standardowym portem protokołu SMTP jest port 25.
- ***Ustawienia dodatkowe*** — pozwalają zdefiniować bardziej szczegółowe parametry:
    - ***Port lokalny*** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port komunikacji SMTP.
    - ***Połączenie*** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślne SSL*). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
- ***Aktywacja serwera SMTP*** — zaznacz to pole, aby włączyć określony powyżej serwer SMTP.



W tym oknie dialogowym (dostępnym z menu ***Serwery / IMAP***) można skonfigurować nowy ***Skaner poczty e-mail*** serwer poczty przychodzącej, korzystający z protokołu IMAP:

- ***Nazwa serwera IMAP*** — w tym polu można podać nazwę nowo dodanego serwera (*aby dodać serwer IMAP, kliknij prawym przyciskiem myszy pozycję IMAP w menu nawigacyjnym po lewej stronie*). W przypadku automatycznie utworzonego serwera AutoIMAP to pole jest nieaktywne.

- ***Typ logowania*** — definiuje metodę określania serwera pocztowego dla poczty wychodzącej:

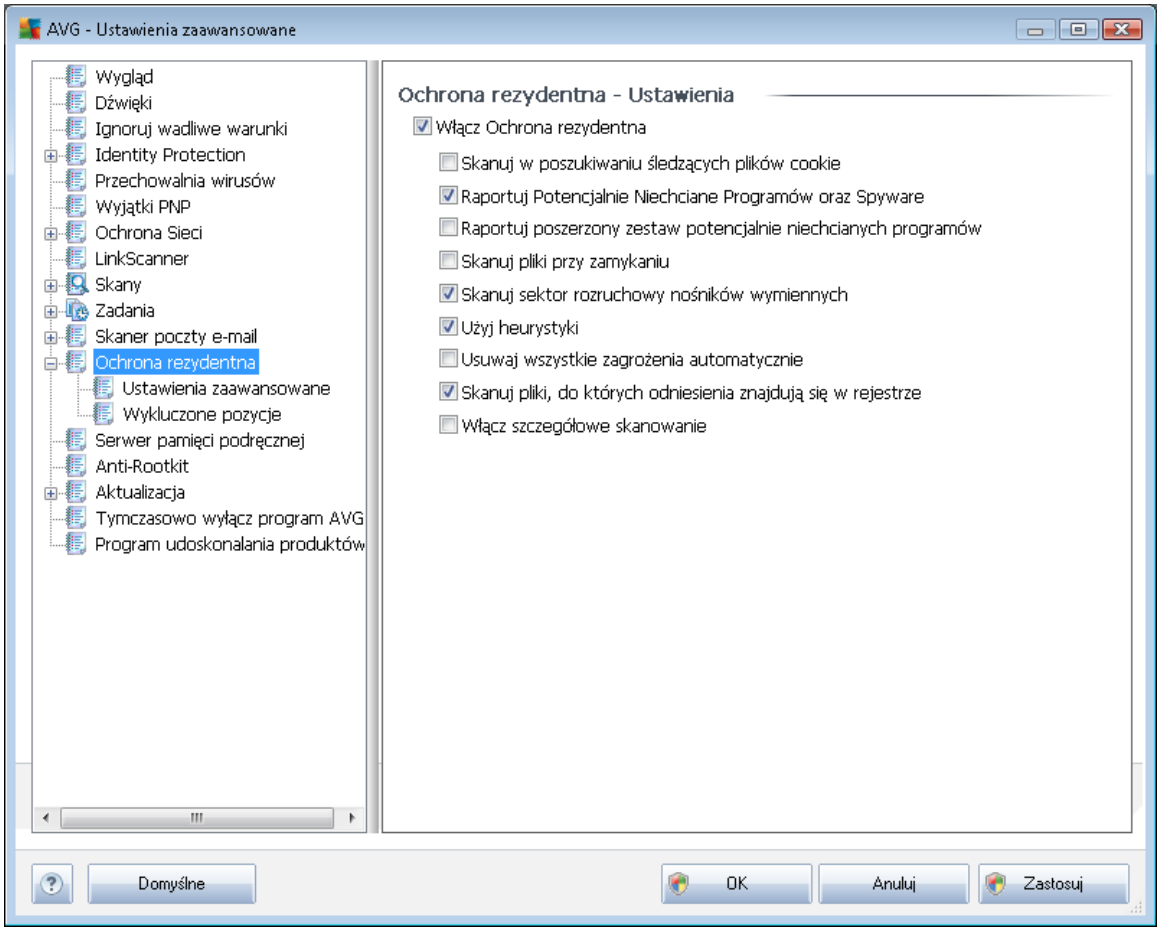
    - ***Automatyczne*** — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail

    - ***Stały host*** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Można użyć nazwy domeny (*np. smtp.domena.com*) lub adresu IP (*np. 123.45.67.89*)). Jeśli serwer pocztowy używa niestandardowego portu, można podać go po dwukropku za nazwą serwera (*np. imap.domena.com:8200*). Standardowym portem protokołu IMAP jest port 143.

- ***Ustawienia dodatkowe*** — pozwalają zdefiniować bardziej szczegółowe parametry:
    - ***Port lokalny*** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port do komunikacji IMAP.
    - ***Połączenie*** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślne SSL*). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
- ***Aktywacja serwera IMAP klienta poczty e-mail*** — zaznacz to pole, aby włączyć określony powyżej serwer IMAP.

9.11. Ochrona rezydentna

Składnik ***Ochrona Rezydentna*** zapewnia aktywną ochronę plików i folderów przed wirusami, oprogramowaniem szpiegującym i innymi zagrożeniami.



W oknie ***Ustawienia Ochrony rezydentnej*** można całkowicie włączyć lub wyłączyć ***Ochronę Rezydentną***, zaznaczając lub odznaczając pole ***Włącz Ochronę Rezydentną*** (*opcja ta jest domyślnie włączona*). Ponadto, można aktywować tylko wybrane funkcje składnika ***Ochrona***

rezydentna:

- ***Skanuj w poszukiwaniu śledzących plików cookie*** (*opcja domyślnie wyłączona*) — parametr ten określa, czy w czasie skanowania mają być wykrywane pliki cookie. (*Pliki cookie w protokole HTTP są używane do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencje dotyczące wyglądu witryny lub zawartość koszyka w sklepach internetowych*.)

- ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje włączenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

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

- ***Skanuj sektor rozruchowy nośników wymiennych***(*opcja domyślnie włączona*).

- ***Użyj heurystyki*** (*opcja domyślnie włączona*) — przy skanowaniu będzie używana analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej*).

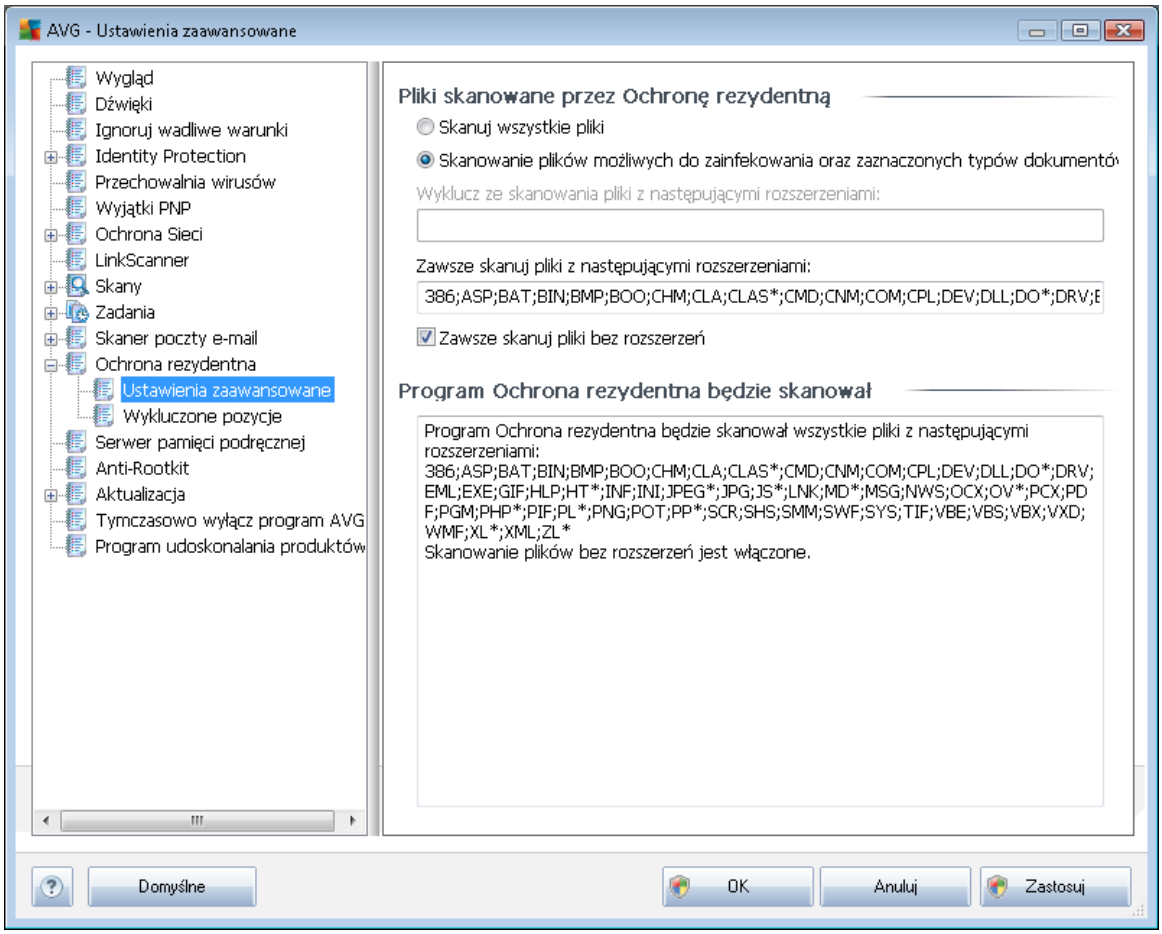
- ***Usuwaj wszystkie zagrożenia automatycznie*** (*opcja domyślnie wyłączona*) — każda wykryta infekcja będzie automatycznie leczona. Wszystkie infekcje, których nie uda się wyleczyć, będą usuwane.

- ***Skanuj pliki, do których odniesienia znajdują się w rejestrze*** (*opcja domyślnie włączona*) — ten parametr określa, że system AVG będzie skanować wszystkie pliki wykonywalne dodane do rejestru w sekcji autostartu.

- ***Włącz szczegółowe skanowanie*** (*opcja domyślnie wyłączona*) — w określonych sytuacjach (*w stanie wyjątkowej konieczności*) można zaznaczyć tę opcję, aby aktywować algorytmy bardziej szczegółowego skanowania, które będą dogłębnie sprawdzać wszystkie obiekty mogące stwarzać zagrożenie. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

9.11.1. Ustawienia zaawansowane

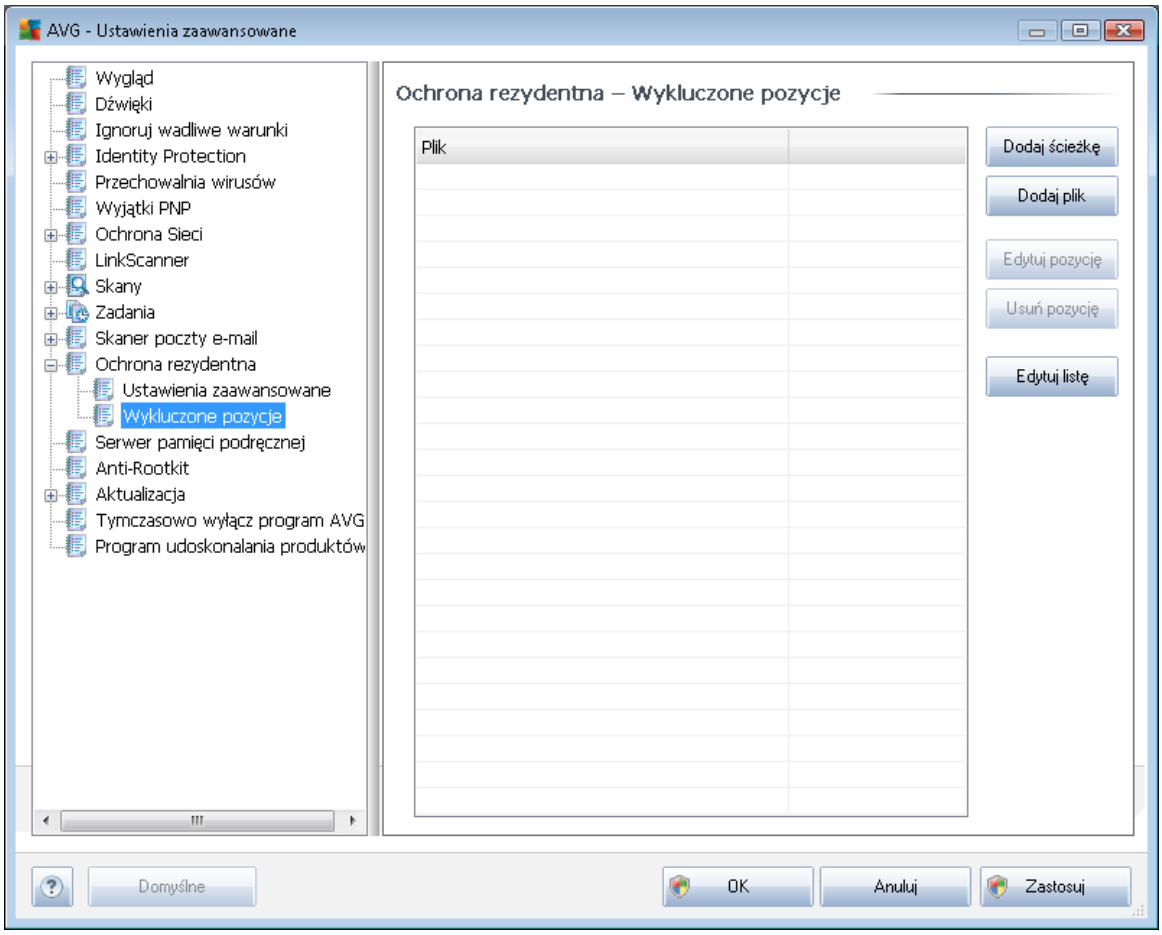
W oknie ***Pliki skanowane przez Ochronę Rezydentną*** można określić, które pliki mają być skanowane (*według ich rozszerzeń*):



Zdecyduj, czy chcesz skanować tylko pliki infekowalne - jeśli tak, będziesz mógł określić listę rozszerzeń plików, które mają być wykluczone ze skanowania, oraz listę tych, które mają być zawsze skanowane.

Znajdująca się poniżej sekcja o nazwie ***Ochrona rezydentna będzie skanować*** podsumowuje bieżące ustawienia składnika ***Ochrona rezydentna***.

9.11.2. Wykluczone obiekty



Okno dialogowe ***Ochrona rezydentna — wykluczone obiekty*** pozwala definiować foldery, które mają być wykluczone ze skanowania przez ***Ochronę rezydentną***.

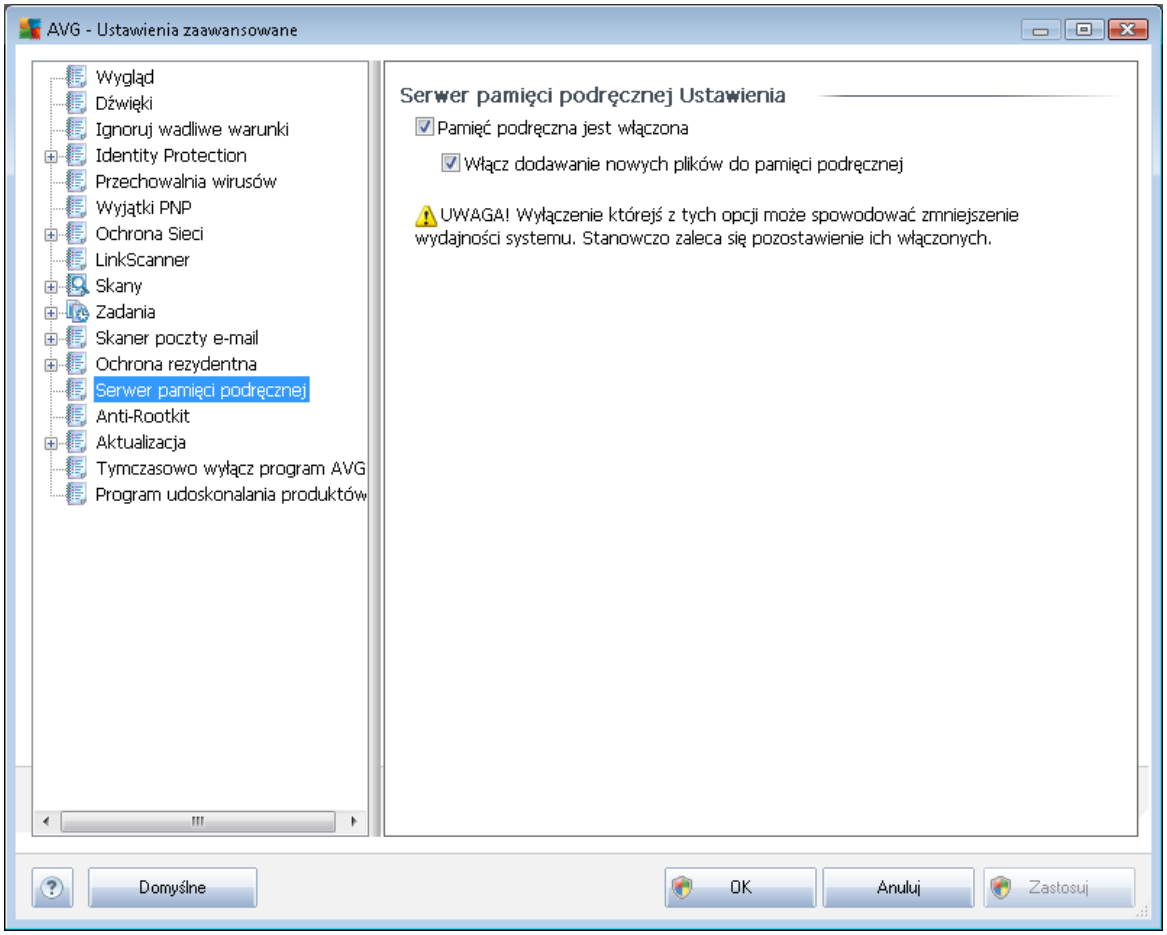
Jeśli nie jest to koniecznie, zdecydowanie zalecamy nie wykluczać żadnych obiektów ze skanowania!

W bieżącym oknie dostępne są następujące przyciski kontrolne:

- ***Dodaj ścieżkę*** — umożliwia określenie katalogów, które mają zostać wykluczone ze skanowania, przez wybranie ich kolejno w drzewie nawigacyjnym dysku lokalnego.
- ***Dodaj plik*** — umożliwia określenie plików, które mają zostać wykluczone ze skanowania, przez wybranie ich kolejno w drzewie nawigacyjnym dysku lokalnego.
- ***Edytuj pozycję*** — umożliwia edycję ścieżki dostępu do wybranego pliku lub folderu.
- ***Usuń pozycję*** — umożliwia usunięcie z listy ścieżki do wybranej pozycji.

9.12. Serwer pamięci podręcznej

Funkcja ***Serwer pamięci podręcznej*** to tak naprawdę proces mający na celu przyspieszenie skanowania (*skanowania na żądanie, zaplanowanego skanowania całego komputera oraz skanowania składnika Ochrona rezydentna*). Zbiera on i zachowuje informacje na temat bezpiecznych plików (*takich jak pliki systemowe z podpisem cyfrowym itp.*) — pliki te są wówczas uważane za bezpieczne i pomijane podczas skanowania.



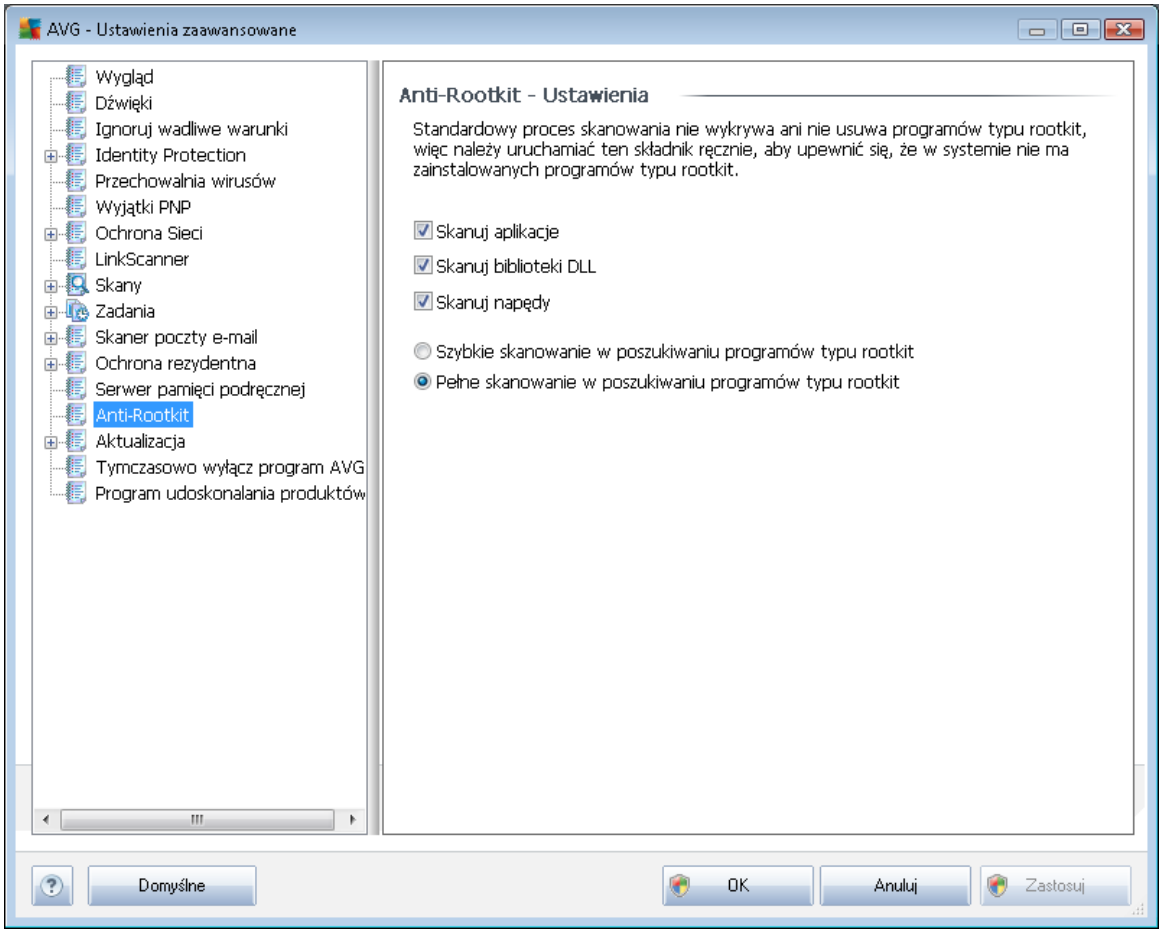
Okno dialogowe ustawień zawiera dwie opcje:

- ***Włączona pamięć podręczna*** (*opcja domyślnie włączona*) — odznaczenie tego pola powoduje wyłączenie funkcji ***Serwer pamięci podręcznej*** i opróżnienie pamięci podręcznej. Należy pamiętać, że skanowanie może spowolnić działanie komputera i zmniejszyć jego ogólną wydajność, ponieważ każdy używany plik będzie skanowany w poszukiwaniu wirusów i oprogramowania szpiegującego.

- ***Włącz dodawanie nowych plików do pamięci podręcznej*** (*opcja domyślnie włączona*) — odznaczenie tego pola umożliwia wyłączenie funkcji dodawania kolejnych plików do pamięci podręcznej. Wszystkie pliki zapisane w pamięci podręcznej są w niej przechowywane dopóki funkcja nie zostanie zupełnie wyłączona lub do czasu kolejnej aktualizacji bazy wirusów.

9.13. Anti-Rootkit

W tym oknie dialogowym można edytować konfigurację składnika ***Anti-Rootkit***:



Wszystkie funkcje składnika ***Anti-Rootkit***dostępne w tym oknie dialogowym można także edytować bezpośrednio w ***interfejsie składnika Anti-Rootkit***.

Zaznacz odpowiednie pola wyboru, aby określić obiekty, które mają być skanowane:

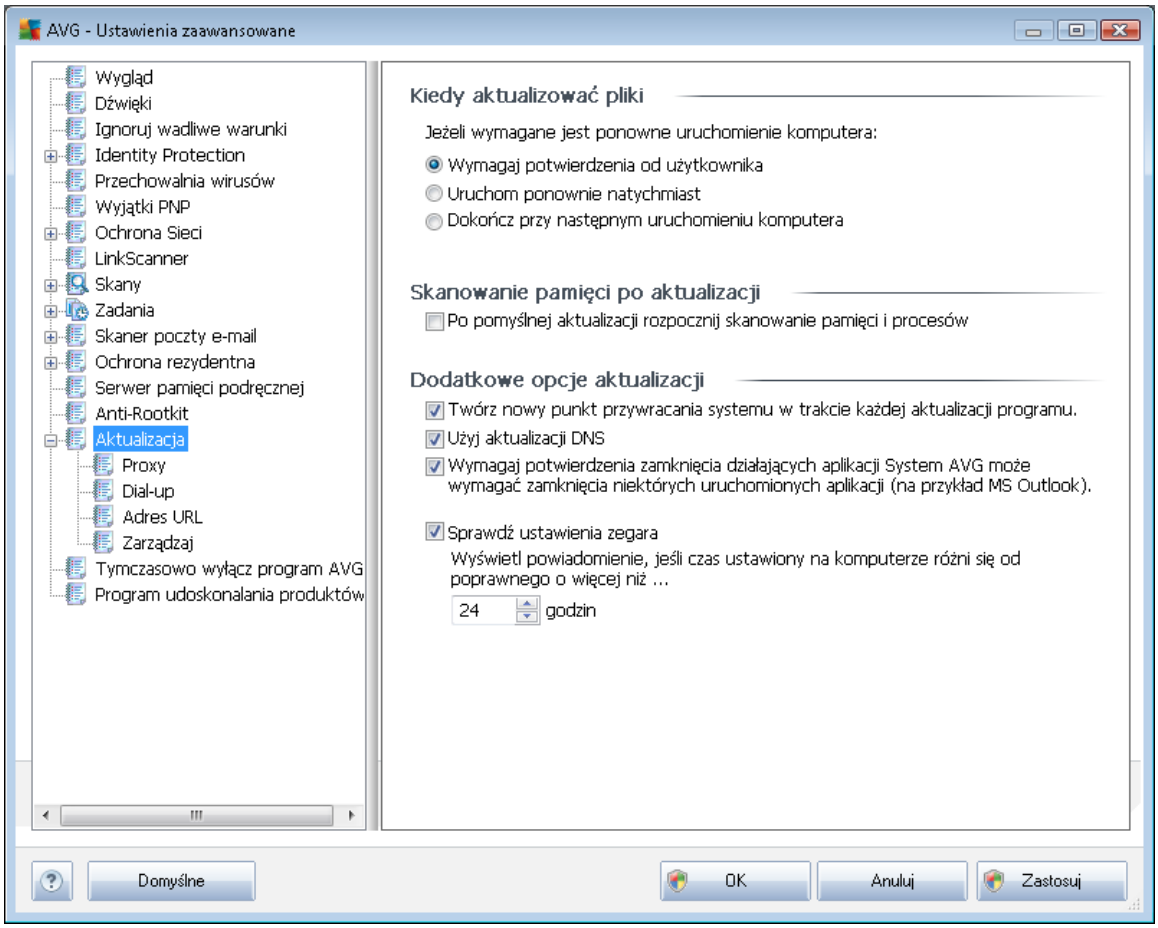
- ***Skanuj aplikacje***
- ***Skanuj biblioteki DLL***
- ***Skanuj sterowniki***

Następnie należy wybrać tryb skanowania w poszukiwaniu programu typu rootkit:

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

uruchomione procesy, załadowane sterowniki i folder systemowy (*zazwyczaj c:\Windows*) oraz wszystkie dyski lokalne (*w tym dyski flash, ale bez uwzględnienia napędów dyskietek/ płyt CD*)

9.14. Aktualizacja



Kliknięcie pozycji ***Aktualizacja*** otwiera nowe okno dialogowe, w którym można określić ogólne parametry aktualizacji AVG:

Kiedy aktualizować pliki

W tej sekcji dostępne są trzy opcje, których można użyć, gdy proces aktualizacji będzie wymagać ponownego uruchomienia komputera. Dokończenie aktualizacji może zostać zaplanowane na kolejne uruchomienie komputera albo można od razu uruchomić komputer ponownie:

- ***Wymagaj potwierdzenia od użytkownika*** *(opcja domyślna)*— przed zakończeniem aktualizacji system zapyta użytkownika o pozwolenie na ponowne uruchomienie komputera.
- ***Uruchom ponownie natychmiast*** — komputer zostanie automatycznie uruchomiony

ponownie zaraz po zakończeniu procesu aktualizacji — potwierdzenie ze strony użytkownika nie jest wymagane.

- ***Dokończ przy następnym uruchomieniu komputera*** — dokończenie procesu aktualizacji zostanie odłożone do czasu kolejnego uruchomienia komputera. Należy pamiętać, że tę opcję należy zaznaczyć wyłącznie, jeśli komputer jest regularnie uruchamiany ponownie (co najmniej raz dziennie)!

Skanowanie pamięci po aktualizacji

Pole to należy zaznaczyć, jeśli po każdej pomyślnej aktualizacji system ma uruchamiać skanowanie pamięci. Pobrana aktualizacja mogła zawierać nowe definicje wirusów, które mogą zostać zastosowane podczas takiego skanowania.

Dodatkowe opcje aktualizacji

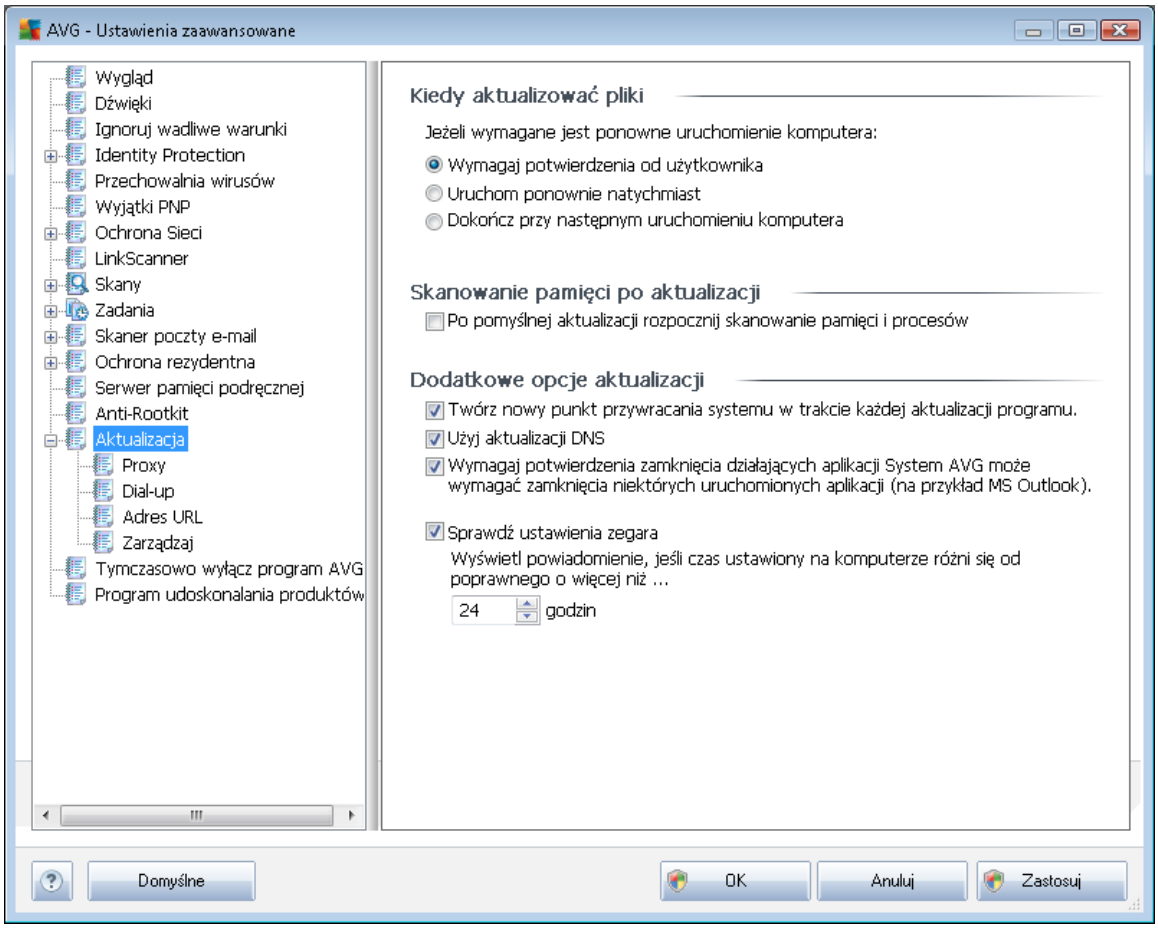
- ***Twórz nowy punkt przywracania systemu po każdej aktualizacji programu*** — przed każdym uruchomieniem aktualizacji systemu AVG tworzony będzie punkt przywracania systemu. Przy jego użyciu możliwe będzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Aby przywrócić system, należy wybrać kolejno: Start / Wszystkie programy / Akcesoria / Narzędzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoświadczonym użytkownikom! Aby korzystać z tej funkcji, pole wyboru musi pozostać zaznaczone.

- ***Użyj aktualizacji DNS*** (*opcja domyślnie włączona*) — gdy to pole jest zaznaczone, przy uruchamianiu aktualizacji system **AVG Anti-Virus 2011** wyszukuje informacje o najnowszej wersji bazy wirusów i programu na serwerze DNS. Następnie pobierane i instalowane są jedynie niewielkie pliki aktualizacyjne. Dzięki temu łączna ilość pobieranych danych jest minimalizowana, a proces aktualizacji przebiega szybciej.

  - ***Wymagaj potwierdzenia zamknięcia działających aplikacji*** (*domyślnie włączona*) — daje pewność, że żadne działające aplikacje nie zostaną zamknięte bez potwierdzenia ze strony użytkownika, jeśli do zakończenia aktualizacji będzie wymagane ponowne uruchomienie komputera.

  - ***Sprawdź ustawienia zegara*** — zaznacz to pole jeśli chcesz, aby program AVG wyświetlił powiadomienie, gdy różnica między właściwym a lokalnym czasem komputera przekroczy określoną wartość.

9.14.1. Proxy



Serwer proxy jest samodzielnym serwerem lub uruchomioną na komputerze usługą gwarantującą bezpieczniejsze połączenie internetowe. Zgodnie z określonymi w Twojej sieci zasadami, połączenie internetowe może odbywać się bezpośrednio lub poprzez serwer proxy. Można także zezwolić na korzystanie z obu opcji jednocześnie. Dlatego też w oknie ***Ustawienia aktualizacji — Proxy*** należy najpierw wybrać jedną z dostępnych opcji:

- ***Używaj proxy***
- ***Nie używaj serwera proxy*** — ustawienia domyślne
- ***Spróbuj połączyć przy użyciu proxy, a w razie niepowodzenia połącz bezpośrednio***

W przypadku wybrania opcji użycia serwera proxy należy podać dalsze informacje. Ustawienia serwera mogą zostać skonfigurowane ręcznie lub automatycznie.

Konfiguracja ręczna

W przypadku wybrania konfiguracji ręcznej (zaznaczenie *opcji* ***Ręcznie*** *aktywuje odpowiednią*

sekcję) należy podać następujące informacje:

- ***Serwer*** — określ adres IP lub nazwę serwera
- ***Port*** — określ numer portu umożliwiającego dostęp do internetu (*domyślnie jest to port 3128, ale może być ustawiony inaczej; w przypadku wątpliwości należy skontaktować się z administratorem sieci*).

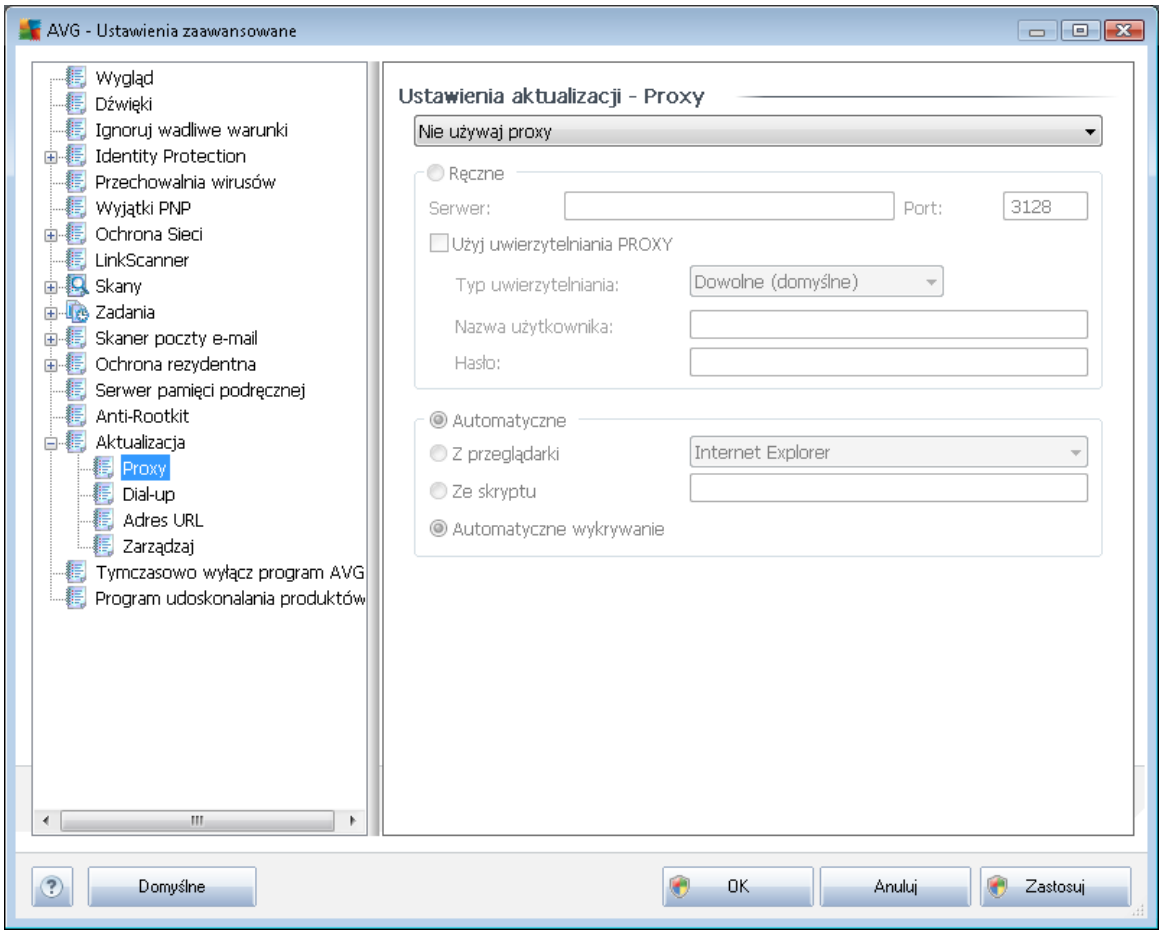
Zdarza się, że na serwerze proxy dla każdego użytkownika skonfigurowane są odrębne reguły. Jeśli serwer proxy jest skonfigurowany w ten sposób, należy zaznaczyć opcję ***Użyj uwierzytelniania PROXY***, aby serwer weryfikował nazwę użytkownika i hasło przed nawiązaniem połączenia.

Konfiguracja automatyczna

W przypadku wybrania konfiguracji automatycznej (*zaznaczenie opcji **Automatycznie** aktywuje odpowiedni obszar okna dialogowego*) należy wskazać, skąd ma zostać pobrana konfiguracja proxy:

- ***Z przeglądarki*** — konfiguracja zostanie odczytana z domyślnej przeglądarki internetowej.
- ***Ze skryptu*** — konfiguracja zostanie odczytana z pobranego skryptu zawierającego funkcję zwracającą adres serwera proxy.
- ***Automatyczne wykrywanie*** — konfiguracja zostanie wykryta automatycznie bezpośrednio na serwerze proxy.

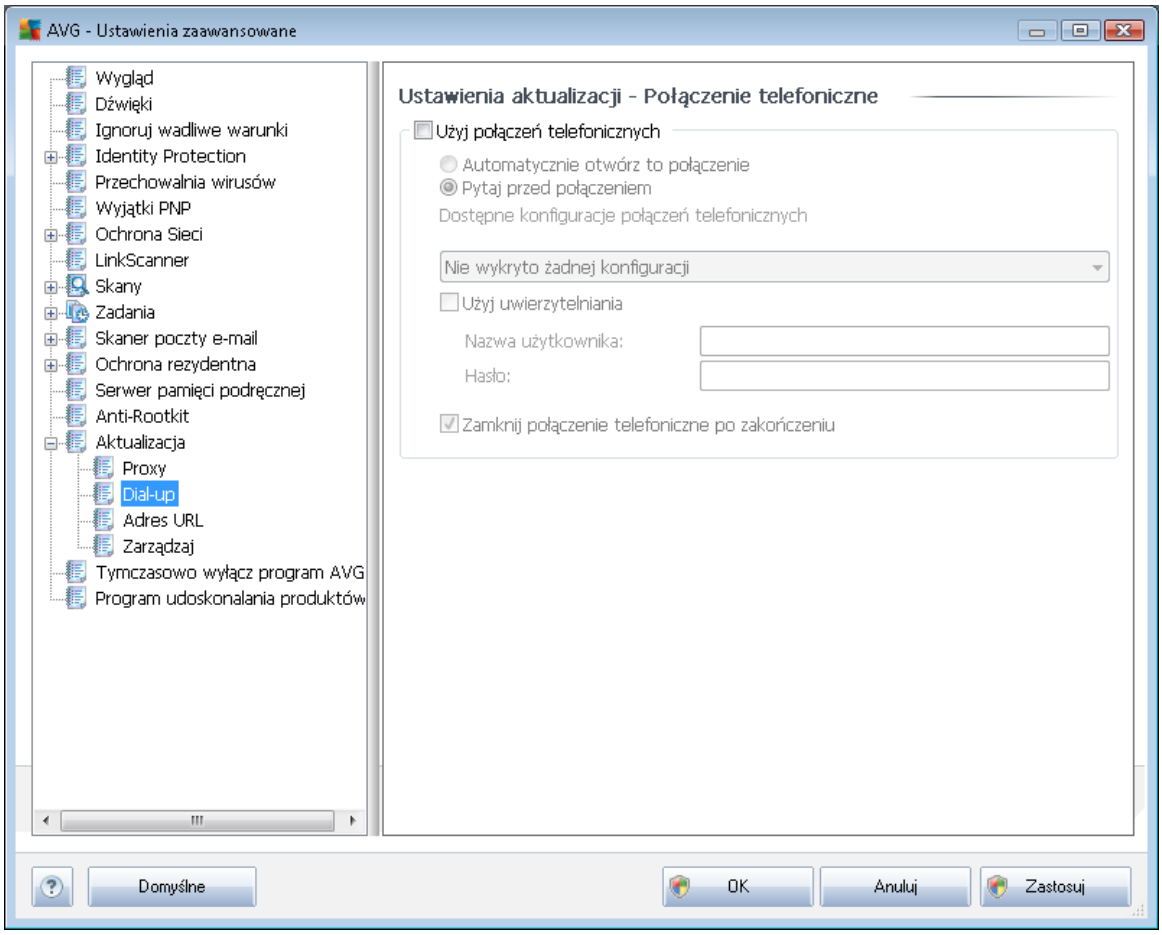
9.14.2. Połączenie telefoniczne



Wszystkie opcjonalne parametry podawane w oknie ***Ustawienia aktualizacji — Połączenie telefoniczne*** odnoszą się do połączenia dial-up z internetem. Pola tego okna pozostają nieaktywne aż do zaznaczenia opcji ***Użyj połączeń telefonicznych.***

Należy określić, czy połączenie z internetem zostanie nawiązane automatycznie (***Automatycznie otwórz to połączenie***), czy też realizację połączenia należy zawsze potwierdzać ręcznie (***Pytaj przed połączeniem***). W przypadku łączenia automatycznego należy także określić, czy połączenie ma być zamykane natychmiast po zakończeniu aktualizacji (***Zamknij połączenie telefoniczne po zakończeniu***).

9.14.3. URL

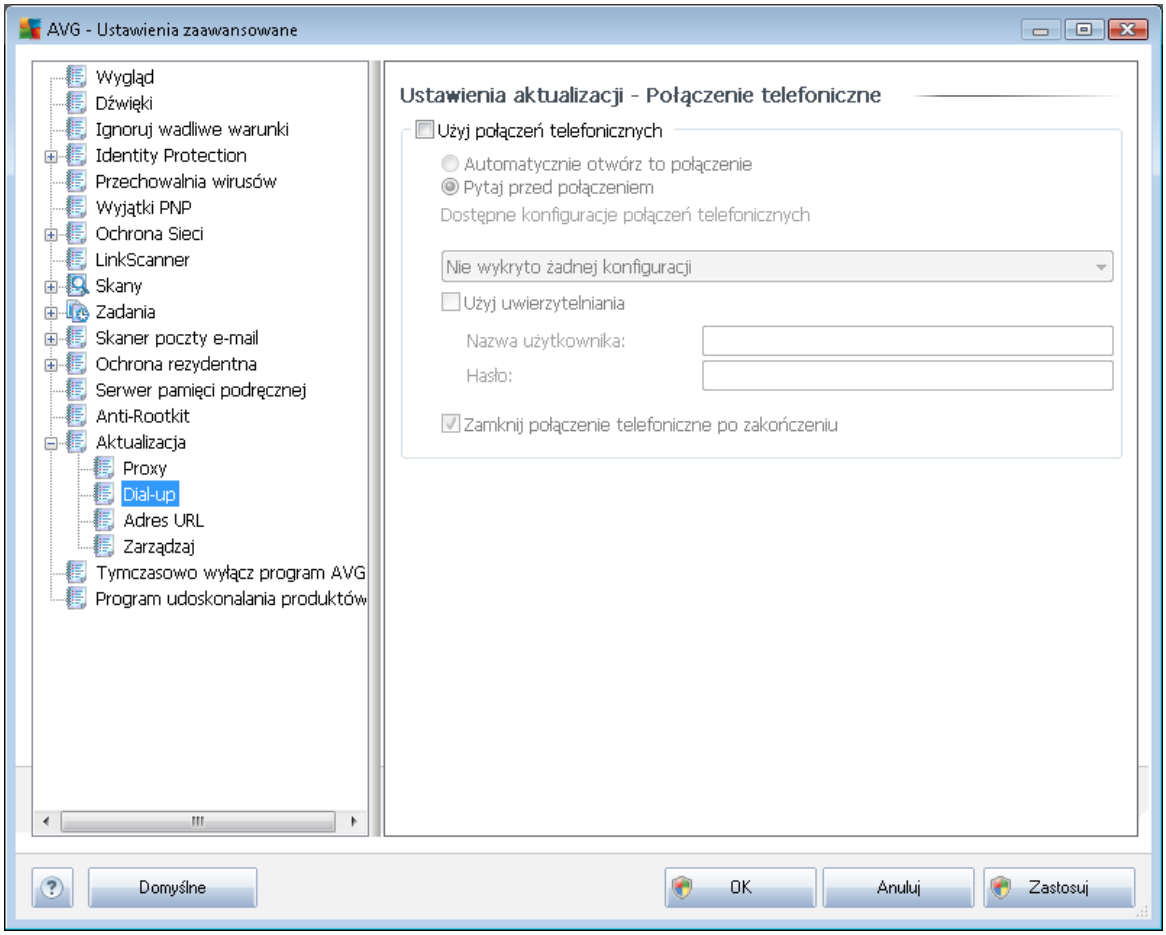


W oknie ***URL*** znajduje się lista adresów internetowych, z których można pobierać pliki aktualizacyjne. Listę i jej elementy można modyfikować za pomocą następujących przycisków kontrolnych:

- ***Dodaj***— powoduje otwarcie okna dialogowego umożliwiającego określenie nowego adresu URL, który zostanie dodany do listy.
- ***Edytuj*** — powoduje otwarcie okna dialogowego umożliwiającego edycję parametrów wybranego adresu URL.
- ***Usuń***— powoduje usunięcie wybranego adresu z listy.
- ***W górę***— przenosi wybrany adres URL o jedną pozycję w górę.
- ***W dół*** — przenosi wybrany adres URL o jedną pozycję w dół.

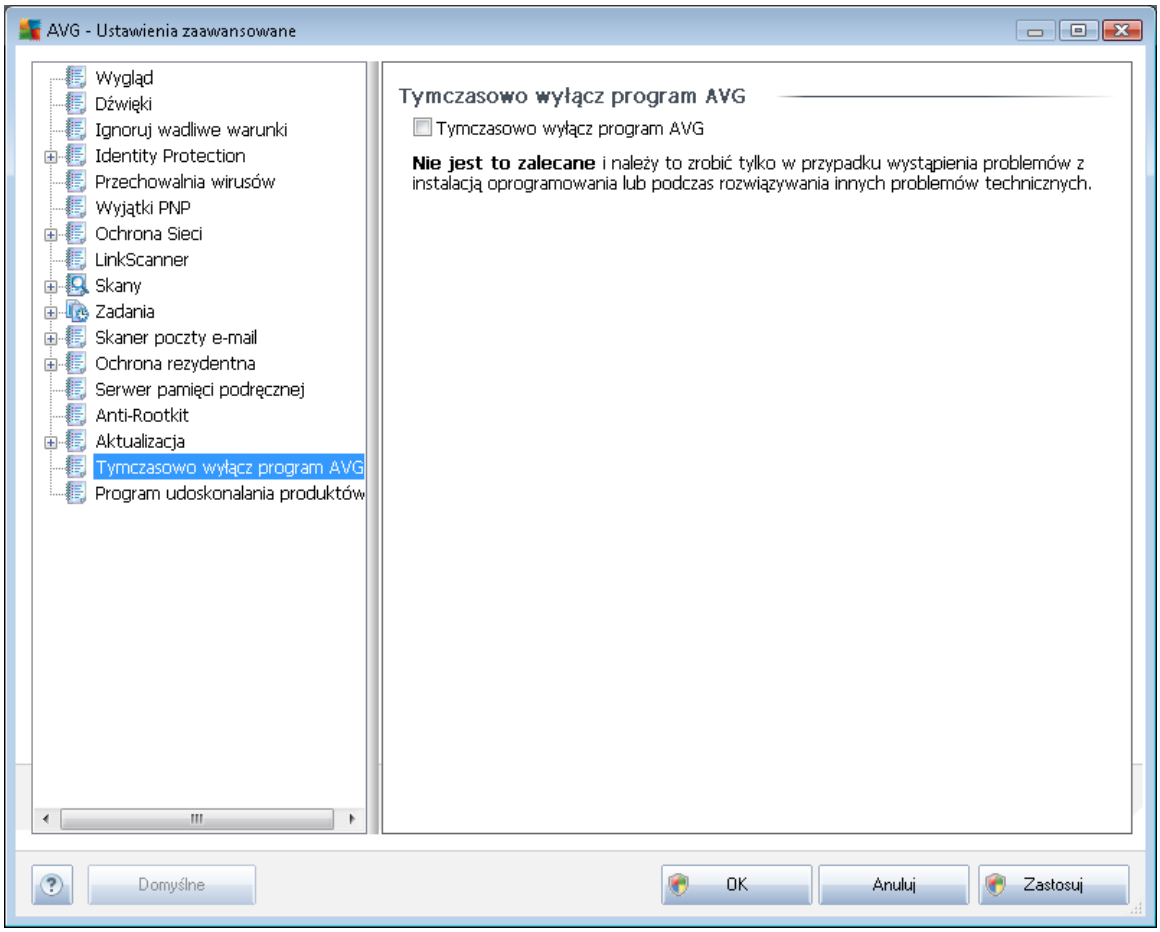
9.14.4. Zarządzaj

Okno dialogowe ***Zarządzaj*** zawiera dwa przyciski:



- ***Usuń tymczasowe pliki aktualizacyjne*** — pozwala usunąć z dysku twardego wszystkie zbędne pliki aktualizacyjne (*są one domyślnie przechowywane przez 30 dni*)
- ***Cofnij bazę wirusów do poprzedniej wersji*** — pozwala usunąć z dysku twardego ostatnią wersję bazy wirusów i przywrócić ją do poprzedniego stanu (*nowa baza będzie częścią najbliższej aktualizacji*)

9.15. Tymczasowo wyłącz ochronę AVG



W oknie dialogowym ***Tymczasowo wyłącz ochronę AVG*** można wyłączyć całą ochronę zapewnianą przez system **AVG Anti-Virus 2011**.

Pamiętaj, że tej opcji nie powinno się używać, chyba że jest to absolutnie konieczne!

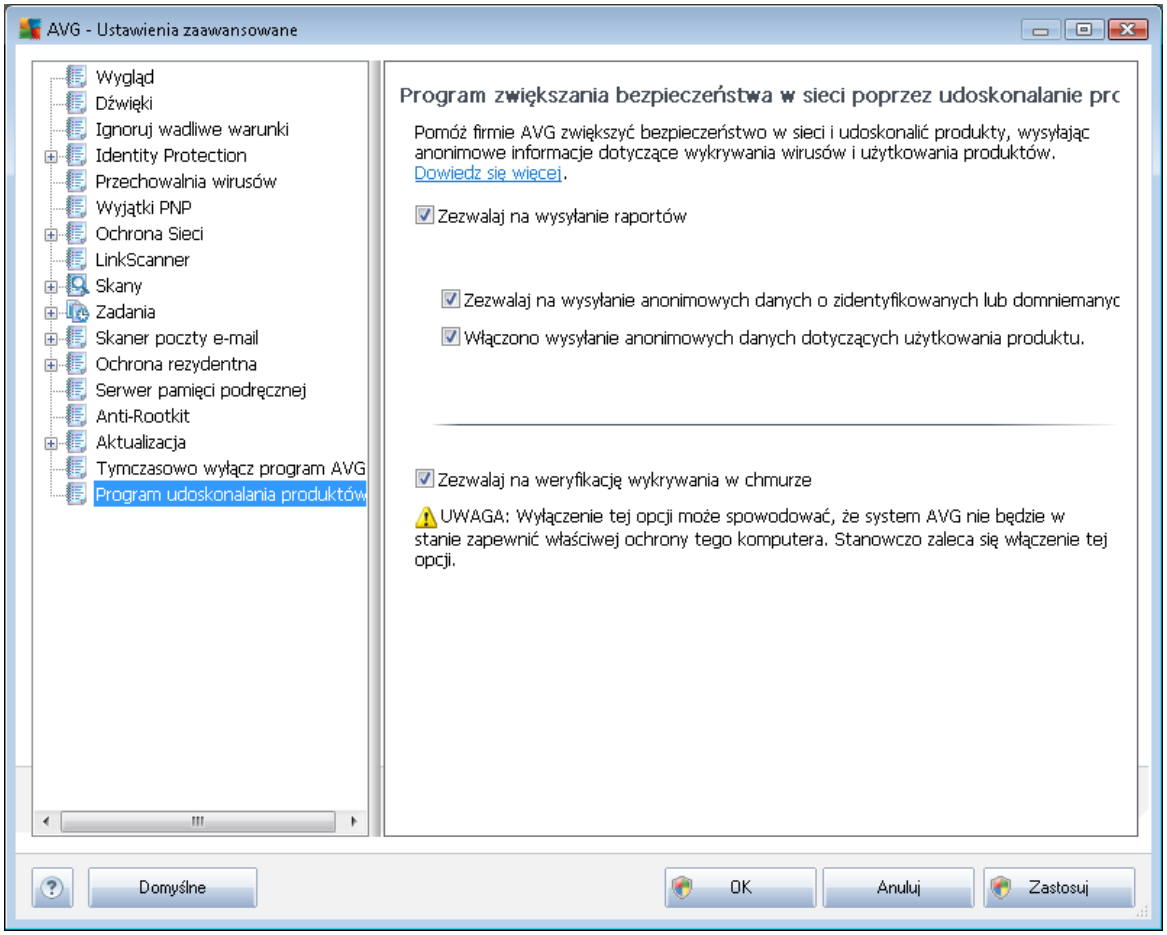
W większości przypadków ***nie jest konieczne*** wyłączanie systemu AVG przed instalowaniem nowego oprogramowania lub sterowników, nawet jeśli instalator lub kreator sugeruje uprzednie zamknięcie działających programów i aplikacji. Jeśli podczas instalacji rzeczywiście wystąpią problemy, spróbuj najpierw wyłączyć jedynie ***Ochronę rezydentną***. Jeśli zachodzi konieczność tymczasowego wyłączenia całego systemu AVG, należy włączyć go ponownie tak szybko, jak to tylko możliwe. Jeśli oprogramowanie antywirusowe jest wyłączone, komputer podłączony do internetu jest narażony na ataki, przed którymi nie będzie chroniony.

9.16. Program udoskonalania produktów

W oknie dialogowym ***Program udoskonalania produktów i bezpieczeństwa sieci AVG*** wyświetlane jest zaproszenie do uczestnictwa w procesie udoskonalania produktów firmy AVG oraz pomagania nam w podnoszeniu ogólnego poziomu bezpieczeństwa internetu. Zaznaczenie opcji ***Zezwalaj na wysyłanie raportów*** spowoduje włączenie funkcji wysyłania raportów o wykrytych

zagrożeniach do firmy AVG. Pomoże nam to w gromadzeniu aktualnych informacji o najnowszych wirusach. Wiedza ta jest konieczna, jeśli mamy im przeciwdziałać.

Zgłaszanie witryn obsługiwane jest automatycznie, więc nie powoduje żadnych niedogodności. Raporty nie zawierają także żadnych poufnych danych. Zgłaszanie wykrytych zagrożeń jest opcjonalne. Prosimy jednak o włączenie tej funkcji, gdyż ułatwia nam ona podnoszenie poziomu ochrony wszystkich użytkowników produktów AVG.



Obecnie istnieje znacznie więcej zagrożeń niż zwykłe wirusy. Autorzy szkodliwych programów i niebezpiecznych witryn internetowych są niezwykle kreatywni, więc nowe rodzaje zagrożeń pojawiają się bardzo często. Zdecydowana większość rozprzestrzenia się samodzielnie poprzez internet. Najpopularniejsze zagrożenia to:

- ***Wirusy*** — szkodliwy kod, który tworzy własne kopie i rozprzestrzenia się, często pozostając niezauważonym do czasu, gdy wyrządzi szkody. Niektóre wirusy stanowią poważne zagrożenie (usuwają lub celowo zmieniają napotkane pliki), a inne mają pozornie nieszkodliwe działanie (np. odtwarzają fragment utworu muzycznego). Wszystkie wirusy są jednak niebezpieczne ze względu na swoją podstawową cechę — możliwość mnożenia się. Nawet prosty wirus może w jednej chwili zająć całą pamięć komputera i spowodować awarię systemu.

- ***Robaki*** — podkategoria wirusów, które — w przeciwieństwie do swoich tradycyjnych kuzynów — nie potrzebują „nosicieli”; robaki rozsyłają się same na wiele komputerów (zwykle w wiadomościach e-mail), a w efekcie mogą spowodować nadmierne obciążenie serwerów pocztowych i systemów sieciowych.

- ***Oprogramowanie szpiegujące*** — zazwyczaj definiowane jako kategoria szkodliwego oprogramowania (*szkodliwe oprogramowanie = oprogramowanie zawierające niebezpieczny kod) obejmująca programy — zazwyczaj konie trojańskie — których celem jest kradzież osobistych informacji (haseł, numerów kart kredytowych) lub przeniknięcie do struktury komputera i umożliwienie atakującemu przejęcie nad nim kontroli (to wszystko oczywiście bez wiedzy lub zgody właściciela komputera*).

- ***Potencjalnie niechciane programy*** — rodzaj oprogramowania szpiegującego, które może - ale niekoniecznie musi - być niebezpieczne dla komputera. Specyficznym przykładem PNP jest oprogramowanie reklamowe, przeznaczone do emitowania reklam, zazwyczaj w postaci wyświetlania wyskakujących okienek; irytujące, ale w zasadzie nieszkodliwe.

- P ſωνιε↵ ***śledzące pliki cookie*** mogą być uznawane za oprogramowanie szpiegujące. Te małe pliki (przechowywane w przeglądarce internetowej i wysyłane do macierzystej witryny przy jej kolejnym odwiedzeniu) mogą zawierać historię przeglądania i tym podobne informacje.

- ***Exploity*** — szkodliwe programy wykorzystujące luki w systemie operacyjnym, przeglądarce internetowej lub innym programie.

- ***Phishing*** — próba zdobycia poufnych informacji poprzez podszywanie się pod wiarygodną i znaną organizację. Zazwyczaj kontakt z potencjalnymi ofiarami następuje przy użyciu masowo wysyłanych wiadomości e-mail zawierających np. prośbę o uaktualnienie szczegółów rachunku bankowego. Aby to zrobić, odbiorcy są proszeni o kliknięcie łącza prowadzącego do fałszywej strony internetowej udającej witrynę banku.

- ***Fałszywy alarm*** to masowo wysyłana wiadomość e-mail zawierająca informacje o wyimaginowanym zagrożeniu. Wiele z opisanych powyżej zagrożeń rozprzestrzenia się za pośrednictwem wiadomości e-mail zwanych fałszywkami.

- ***Istnieją także szkodliwe witryny sieci Web*** instalujące na komputerze złośliwe oprogramowanie, oraz podobnie działające zainfekowane strony WWW, które padły ofiarą hakerów wykorzystujących je do rozprzestrzeniania wirusów.

Aby zapewnić ochronę przed wszystkimi wymienionymi rodzajami zagrożeń, system AVG zawiera całą gamę wyspecjalizowanych składników:

- ***Anti-Virus***, aby chronić komputer przed wirusami;

- ***Anti-Spyware***, aby chronić komputer przed oprogramowaniem szpiegującym;

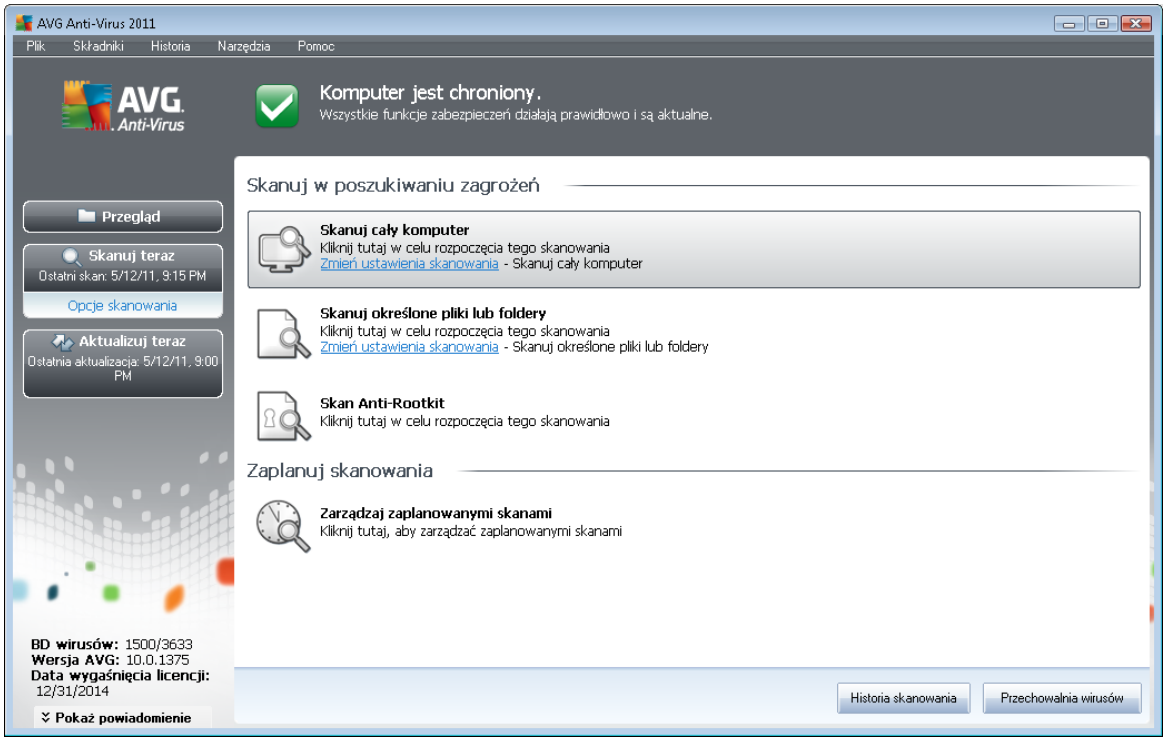
- ***Ochrona Sieci***, aby chronić Cię zarówno przed wirusami, jak i oprogramowaniem szpiegującym podczas przeglądania internetu;

- ***LinkScanner***, aby chronić komputer przed pozostałymi zagrożeniami online wymienionymi w tym rozdziale.

10. Skanowanie AVG

Skanowanie jest podstawowym elementem funkcjonowania systemu **AVG Anti-Virus 2011**. Możliwe jest uruchamianie testów na żądanie lub planowanie ich okresowego przeprowadzania o odpowiednich porach.

10.1. Interfejs skanowania



Interfejs skanera AVG jest dostępny za pomocą szybkiego łącza ***Opcje skanowania***. Kliknięcie go otwiera okno ***Skanuj w poszukiwaniu zagrożeń***. Okno to zawiera następujące elementy:

- przegląd wstępnie zdefiniowanych testów — trzy typy testów (zdefiniowane przez dostawcę oprogramowania) są gotowe do użycia na żądanie lub według utworzonego harmonogramu:
  - ***Skan całego komputera***
  - ***Skan określonych plików lub folderów***
  - ***Skan Anti-rootkit***
- Planowanie testów — w tym obszarze można definiować nowe testy i tworzyć nowe harmonogramy w zależności od potrzeb.

Przyciski kontrolne

Interfejs skanera zawiera następujące przyciski kontrolne:

- ***Historia skanowania*** — wyświetla okno dialogowe ***Przegląd wyników skanowania***, które zawiera pełną historię testów.

- ***Przechowalnia wirusów*** — otwiera nowe okno z zawartością ***Przechowalni wirusów***, w której izolowane są wykryte infekcje.

10.2. Wstępnie zdefiniowane testy

Jedną z głównych funkcji systemu **AVG Anti-Virus 2011** jest skanowanie na żądanie. Testy na żądanie służą do skanowania konkretnych obszarów komputera, gdy użytkownik podejrzewa obecność wirusa. Stanowczo zaleca się jednak wykonywanie tych testów regularnie, nawet w przypadku, gdy nie ma takich podejrzeń.

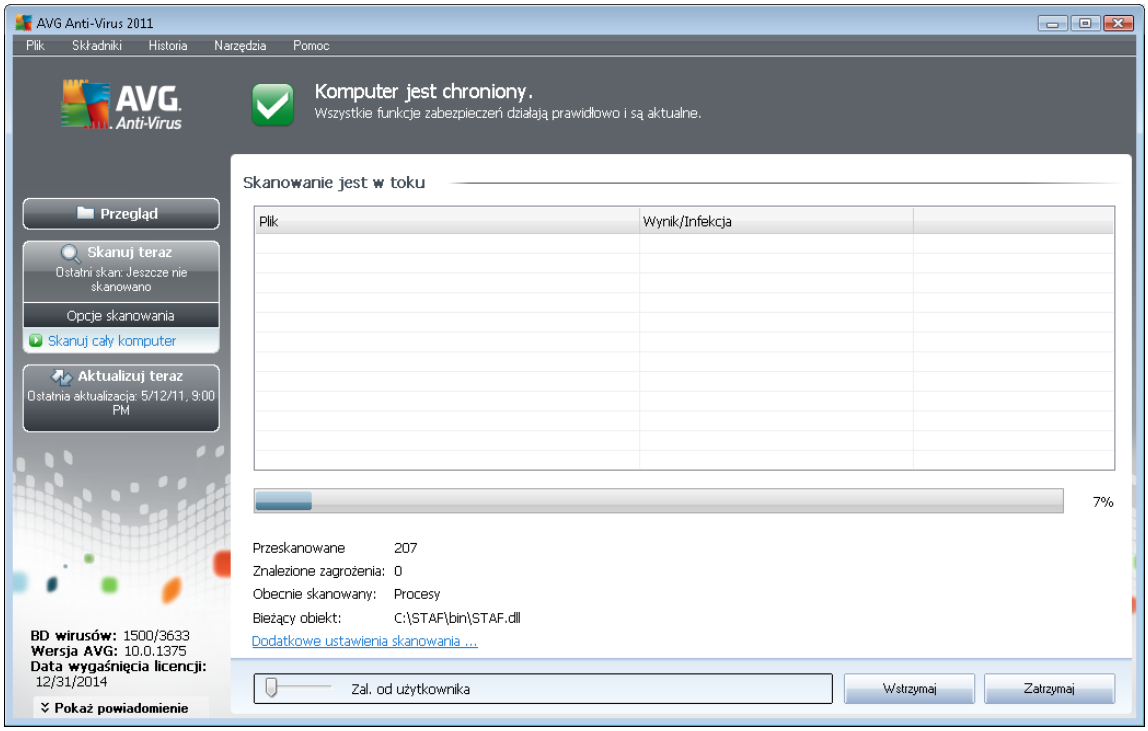
W systemie **AVG Anti-Virus 2011** dostępne są następujące typy skanowania zdefiniowane wstępnie przez producenta:

10.2.1. Skan całego komputera

Skan całego komputera — skanuje cały komputer w poszukiwaniu możliwych infekcji i/lub potencjalnie niechcianych programów. Test ten obejmuje wszystkie dyski twarde komputera. Wykryte infekcje są leczone lub przenoszone do ***Przechowalni wirusów***. Skanowanie całego komputera powinno być regularnie przeprowadzane co najmniej raz na tydzień.

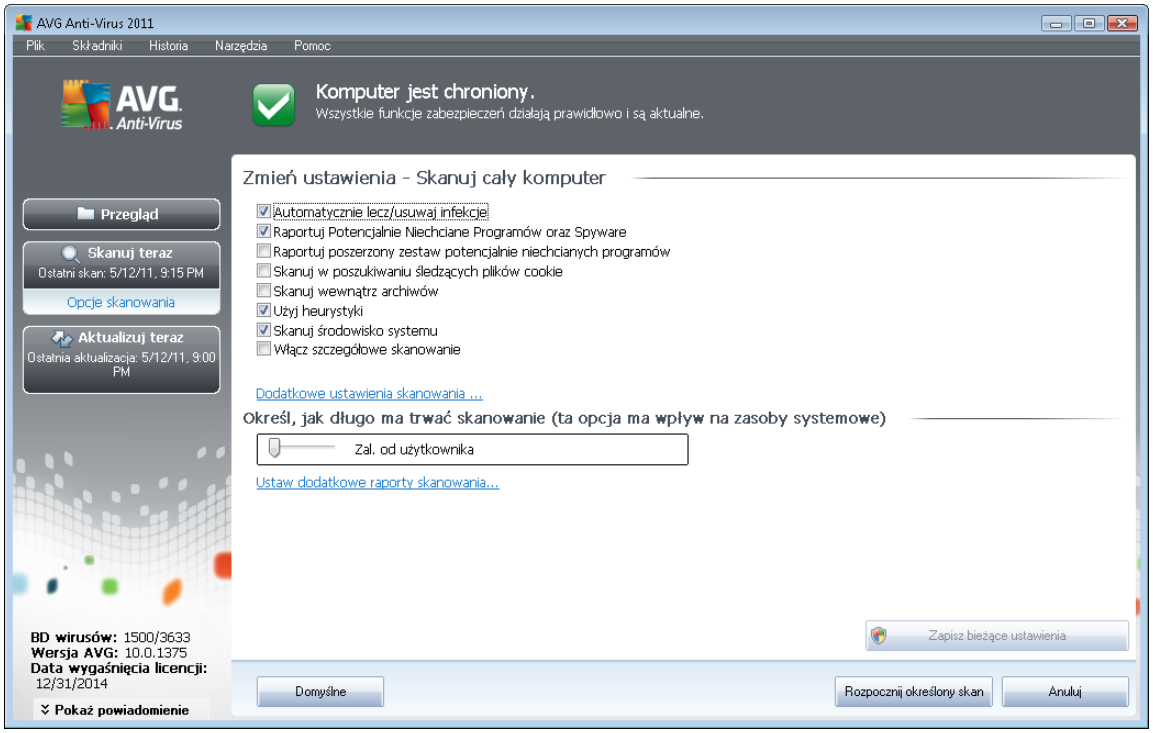
Uruchamianie skanowania

Skan całego komputera może zostać uruchomiony bezpośrednio z poziomu interfejsu skanera poprzez kliknięcie ikony skanowania. Dla tego skanowania nie można określać dalszych ustawień; jest ono uruchamiane natychmiast w oknie dialogowym ***Skanowanie w toku***. (*patrz ilustracja*). W razie potrzeby skanowanie można tymczasowo przerwać (***Wstrzymaj***) lub anulować (***Zatrzymaj***).



Edycja konfiguracji skanowania

Wstępnie zdefiniowane domyślne ustawienia testu ***Skan całego komputera*** można edytować. W tym celu należy kliknąć łącze ***Zmień ustawienia skanowania***, aby przejść do okna dialogowego ***Zmień ustawienia skanowania dla skanu całego komputera*** *(opcja dostępna z interfejsu skanowania za pośrednictwem łącza Zmień ustawienia skanowania dla testu Skan całego komputera)*. ***Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!***



- ***Parametry skanowania*** — na liście parametrów skanowania można włączać/wyłączać określone parametry w zależności od potrzeb:

    - ***Automatycznie lecz/usuwaj infekcje*** (*opcja domyślnie włączona*) — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do***Przechowalni wirusów***.

    - ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje aktywowanie silnika ***Anti-Spyware*** i skanowanie w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

    - ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

    - ***Skanuj w poszukiwaniu śledzących plików cookie*** (*domyślnie wyłączone*) — ten parametr składnika ***Anti-Spyware*** określa, czy wykrywane mają być pliki cookie (*używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania*

określonych informacji o użytkownikach — np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych).

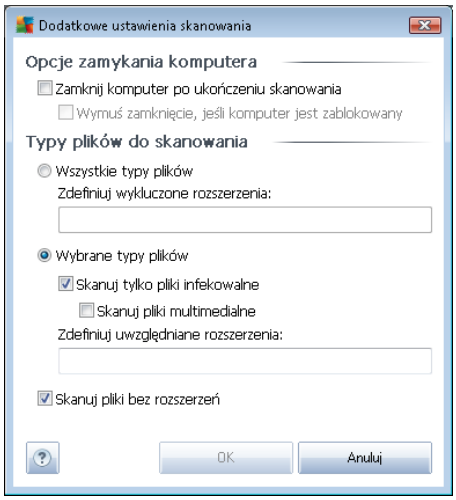
- **Skanuj wewnątrz archiwów** (*opcja domyślnie wyłączona*) — parametr ten określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- **Użyj heurystyki** (*opcja domyślnie włączona*) — analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) będzie jedną z metod wykrywania wirusów w czasie skanowania.

- **Skanuj środowisko systemu** (*opcja domyślnie włączona*) — skanowanie obejmie także obszary systemowe komputera.

- **Włącz szczegółowe skanowanie** (*domyślnie wyłączone*) — w określonych sytuacjach (*gdy zachodzi podejrzenie, że komputer jest zainfekowany*) można zaznaczyć tę opcję, aby aktywować algorytmy bardziej dokładnego skanowania, które w celu uzyskania absolutnej pewności będą skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

- ***Dodatkowe ustawienia skanowania*** — łącze do okna dialogowego ***Dodatkowe ustawienia skanowania***, w którym można określić następujące parametry:



- **Opcje wyłączania komputera** — określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukończeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, gdy jest zablokowany (***Wymuś zamknięcie, jeśli komputer jest zablokowany***).

- ***Zdefiniuj typy plików do skanowania*** — należy zdecydować, które z poniższych elementów mają być skanowane:

  - ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być

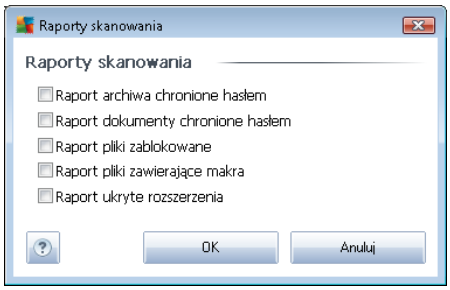
skanowane;

- ***Wybrane typy plików*** — skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje*). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

- ***Określ, jak długo ma trwać skanowanie*** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślna wartość tej opcji to poziom *Zależny od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas jego trwania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer jest tymczasowo nieużywany*).

- ***Ustaw dodatkowe raporty skanowania*** — ten link pozwala otworzyć nowe okno dialogowe ***Raporty skanowania***, w którym można określić raportowane elementy lub zdarzenia:



Ostrzeżenie: *Ustawienia te są identyczne jak domyślne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale* ***Skanowanie AVG / Planowanie skanowania / Jak skanować****. Jeśli jednak domyślna konfiguracja testu* ***Skan całego komputera*** *zostanie zmieniona, nowe ustawienia można zapisać jako konfigurację domyślną, aby były używane we wszystkich przyszłych skanach całego komputera.*

10.2.2. Skan określonych plików lub folderów

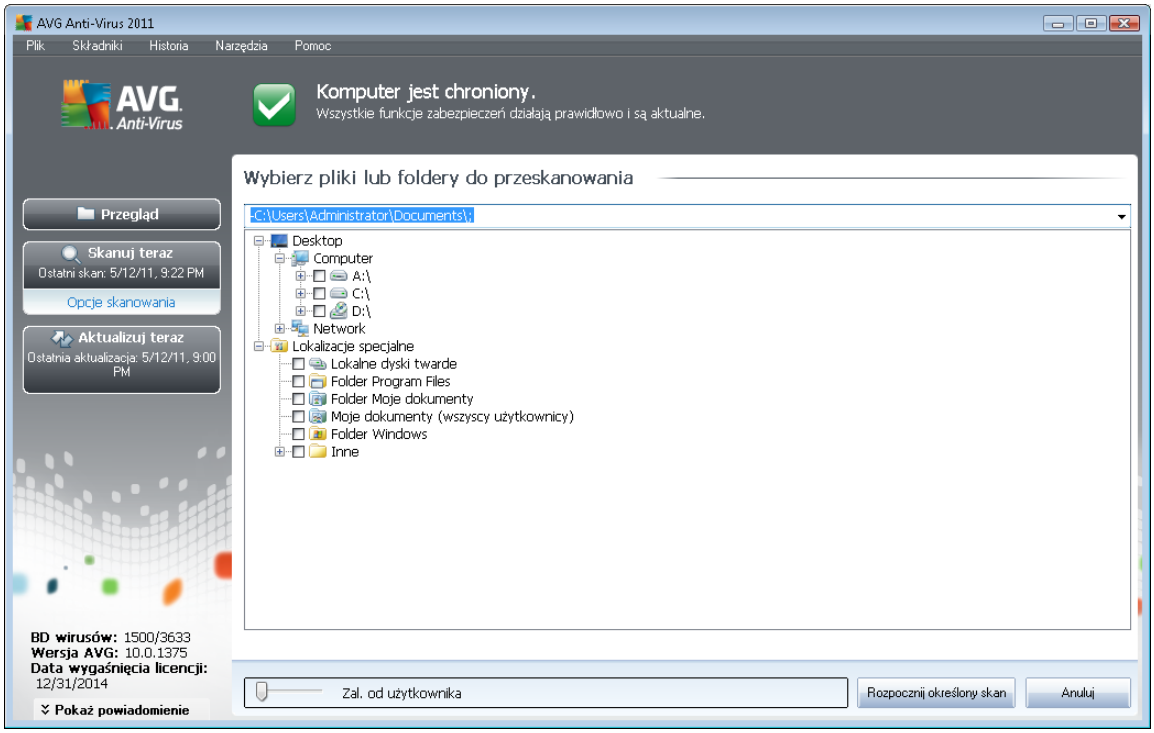
Skan określonych plików lub folderów — skanowane są tylko wskazane obszary komputera (wybrane foldery, a także dyski twarde, pamięci flash, CD itd.).). Postępowanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu całego komputera: każdy znaleziony wirus jest leczony lub przenoszony do ***Przechowalni***. Skanowanie określonych plików lub folderów może posłużyć do utworzenia własnych testów i planowania ich zgodnie z konkretnymi potrzebami.

Uruchamianie skanowania

Skanowanie określonych plików lub folderów można uruchomić bezpośrednio z poziomu interfejsu skanera, klikając ikonę testu. Wyświetlone zostanie nowe okno dialogowe ***Wybierz pliki lub foldery do przeskanowania***. W drzewie katalogów należy wybrać te, które mają zostać przeskanowane. Ścieżki do wszystkich wybranych folderów zostaną wygenerowane automatycznie i wyświetlone w polu tekstowym w górnej części okna dialogowego.

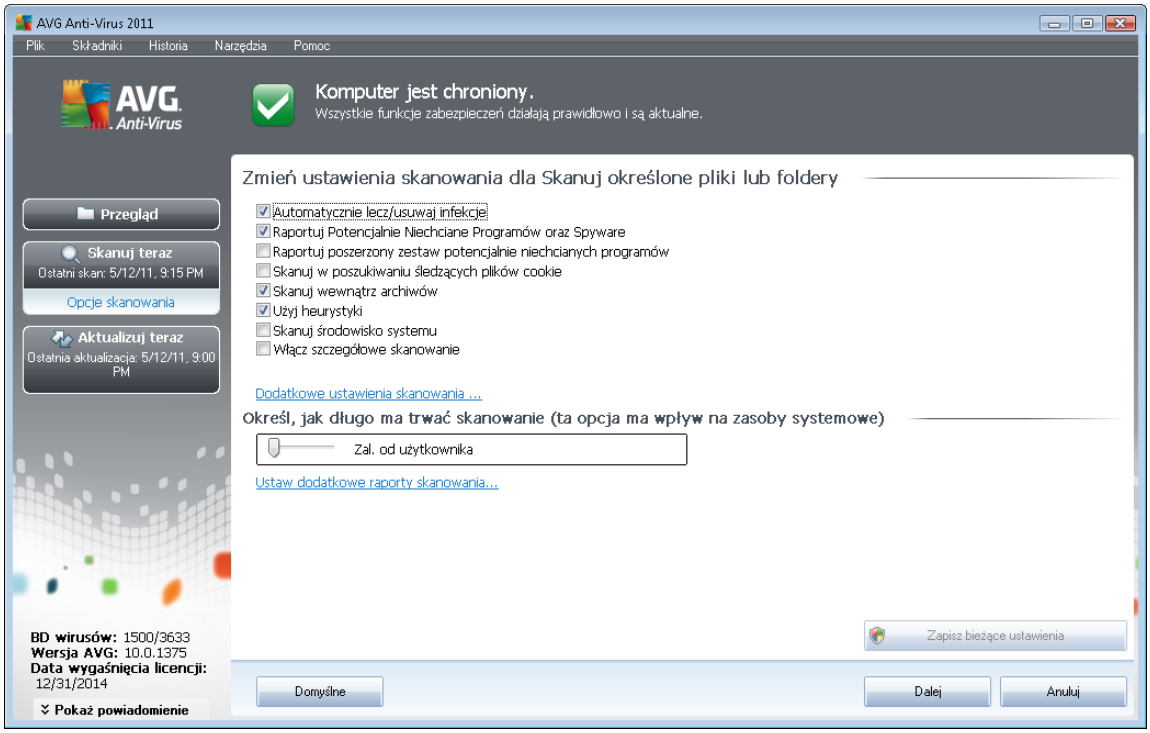
Można także przeskanować wybrany folder, wykluczając jednocześnie ze skanowania wszystkie jego podfoldery: należy wprowadzić znak minus „-” przed jego nazwą w wygenerowanej ścieżce (*patrz ilustracja*). Aby wykluczyć cały folder ze skanowania, należy użyć parametru „!”.

Na koniec, aby uruchomić skanowanie, należy kliknąć przycisk ***Rozpocznij skanowanie***; proces skanowania jest w zasadzie taki sam jak skan całego komputera.



Edycja konfiguracji skanowania

Wstępne, domyślne ustawienia testu ***Skan określonych plików lub folderów*** można łatwo edytować. Kliknięcie linku ***Zmień ustawienia skanowania*** powoduje otwarcie okna dialogowego umożliwiającego ***zmianę ustawień dla skanu określonych plików lub folderów***. ***Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!***



- ***Parametry skanowania*** — na liście parametrów skanowania można włączać/wyłączać określone parametry w zależności od potrzeb:

    - ***Automatycznie lecz/usuwaj infekcje*** (*opcja domyślnie włączona*) — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do***Przechowalni wirusów***.

    - ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje aktywowanie silnika ***Anti-Spyware*** i skanowanie w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

    - ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

    - ***Skanuj w poszukiwaniu śledzących plików cookie*** (*domyślnie wyłączone*) — ten parametr składnika ***Anti-Spyware*** określa, czy wykrywane mają być pliki cookie *(używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania*

określonych informacji o użytkownikach — np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych).

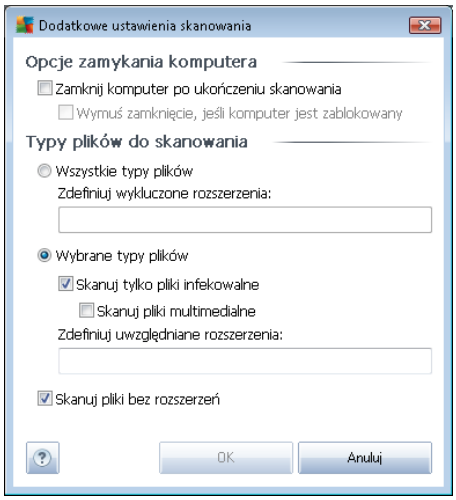
- **Skanuj wewnątrz archiwów** (*domyślnie włączone*) — parametr ten określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- **Użyj heurystyki** (*domyślnie wyłączone*) — analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) jest jedną z metod wykrywania wirusów w czasie skanowania.

- **Skanuj środowisko systemu** (*domyślnie wyłączone*) — skanowanie obejmie także obszary systemowe komputera.

- **Włącz szczegółowe skanowanie** (*domyślnie wyłączone*) — w określonych sytuacjach (*gdy zachodzi podejrzenie, że komputer jest zainfekowany*) można zaznaczyć tę opcję, aby aktywować algorytmy bardziej dokładnego skanowania, które w celu uzyskania absolutnej pewności będą skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

- **Dodatkowe ustawienia skanowania** — link do okna dialogowego **Dodatkowe ustawienia skanowania**, w którym można określić następujące parametry:



- **Opcje wyłączania komputera** — określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukończeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, gdy jest zablokowany (***Wymuś zamknięcie, jeśli komputer jest zablokowany***).

- **Zdefiniuj typy plików do skanowania** — następnie należy zdecydować, czy skanowane mają być:

  - ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być

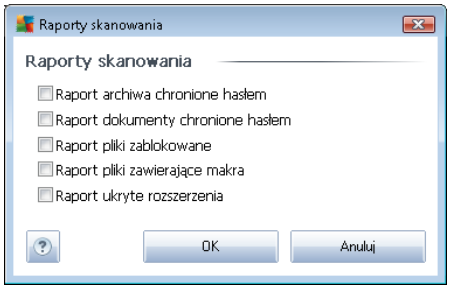
skanowane;

- ***Wybrane typy plików*** — skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe niewykonywalne*), z uwzględnieniem multimediów (*plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje*). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

- ***Priorytet procesu skanowania*** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślna wartość tej opcji to poziom *Zależny od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas jego trwania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer jest tymczasowo nieużywany*).

- ***Ustaw dodatkowe raporty skanowania*** — ten link pozwala otworzyć nowe okno dialogowe ***Raporty skanowania***, w którym można określić raportowane elementy lub zdarzenia:



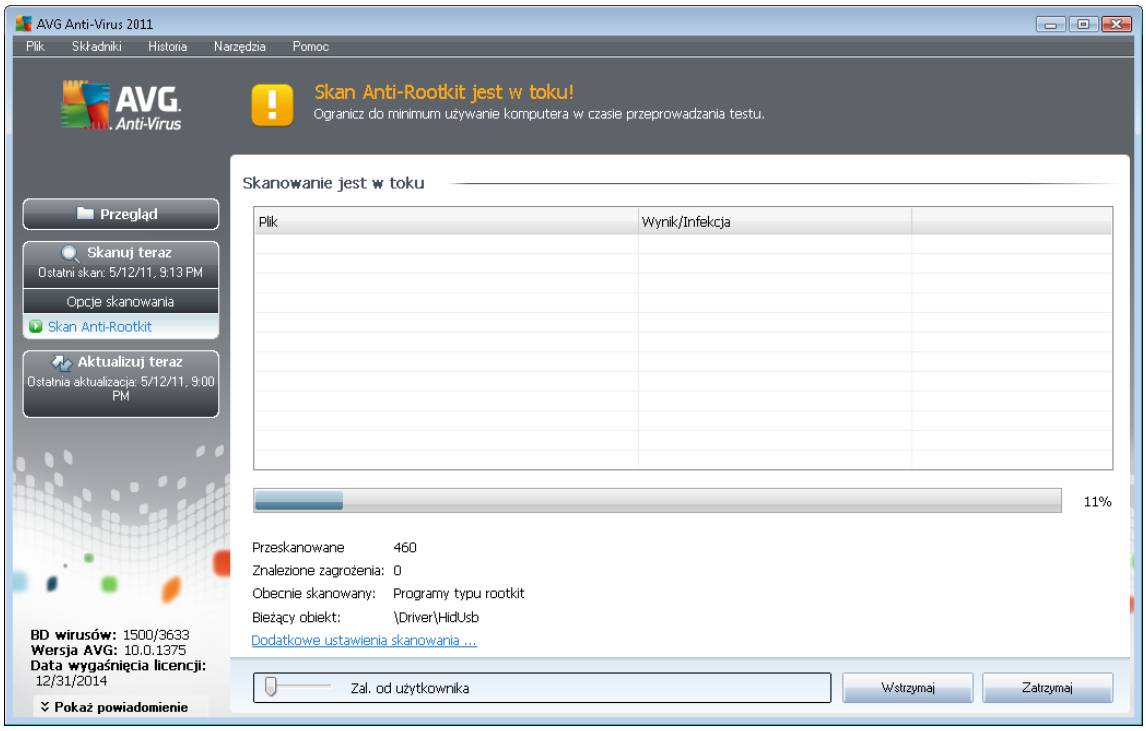
Ostrzeżenie: *Ustawienia te są identyczne jak domyślne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale* ***Skanowanie AVG / Planowanie skanowania / Jak skanować****. Jeśli jednak domyślna konfiguracja testu* ***Skan określonych plików lub folderów*** *zostanie zmieniona, nowe ustawienia będzie można zapisać jako konfigurację domyślną, która będzie używana we wszystkich zdefiniowanych w przyszłości skanach określonych plików lub folderów. Stanie się ona również szablonem dla wszystkich nowych skanów zaplanowanych (wszystkie testy użytkownika oparte są na bieżącej konfiguracji skanu określonych plików lub folderów).*

10.2.3. Skan Anti-Rootkit

Skan Anti-Rootkit przeszukuje komputer w poszukiwaniu obecnych na nim programów typu rootkit (*aplikacji oraz technologii, które mogą maskować działanie szkodliwego oprogramowania na tym komputerze*). Wykrycie programu typu rootkit nie jest równoznaczne z tym, że komputer jest zainfekowany. W niektórych przypadkach pewne sterowniki lub elementy zwykłych aplikacji mogą omyłkowo zostać zaklasyfikowane jako programy typu rootkit.

Uruchamianie skanowania

Skan Anti-Rootkit może zostać uruchomiony bezpośrednio z poziomu interfejsu skanera poprzez kliknięcie ikony odpowiedniego skanu. Dla tego typu skanowania nie można określać dalszych ustawień; jest ono uruchamiane od razu w oknie dialogowym ***Skanowanie w toku***. (*patrz ilustracja*). W razie potrzeby skanowanie można tymczasowo przerwać (***Wstrzymaj***) lub anulować (***Zatrzymaj***).



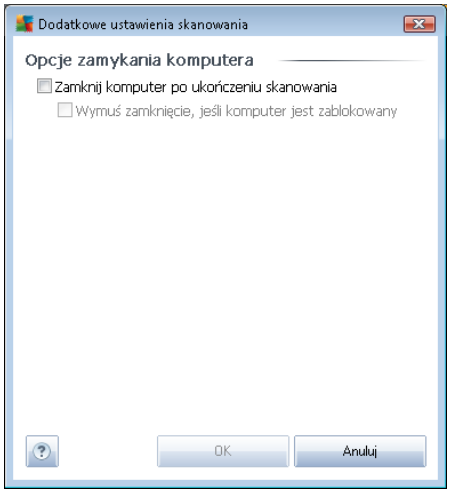
Edycja konfiguracji skanowania

Skan Anti-Rootkit jest zawsze uruchamiany z ustawieniami domyślnymi, a edycja parametrów skanowania jest dostępna tylko w oknie dialogowym ***Zaawansowane ustawienia systemu AVG / składnik Anti-Rootkit***. W interfejsie skanowania dostępne są następujące opcje (ale tylko wtedy, kiedy skanowanie jest w toku):

- ***Skanowanie automatyczne*** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślna wartość tej opcji to poziom *Zależny od użytkownika, co oznacza automatycznie dobrane wykorzystanie zasobów.* Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas jego trwania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer jest tymczasowo nieużywany*).

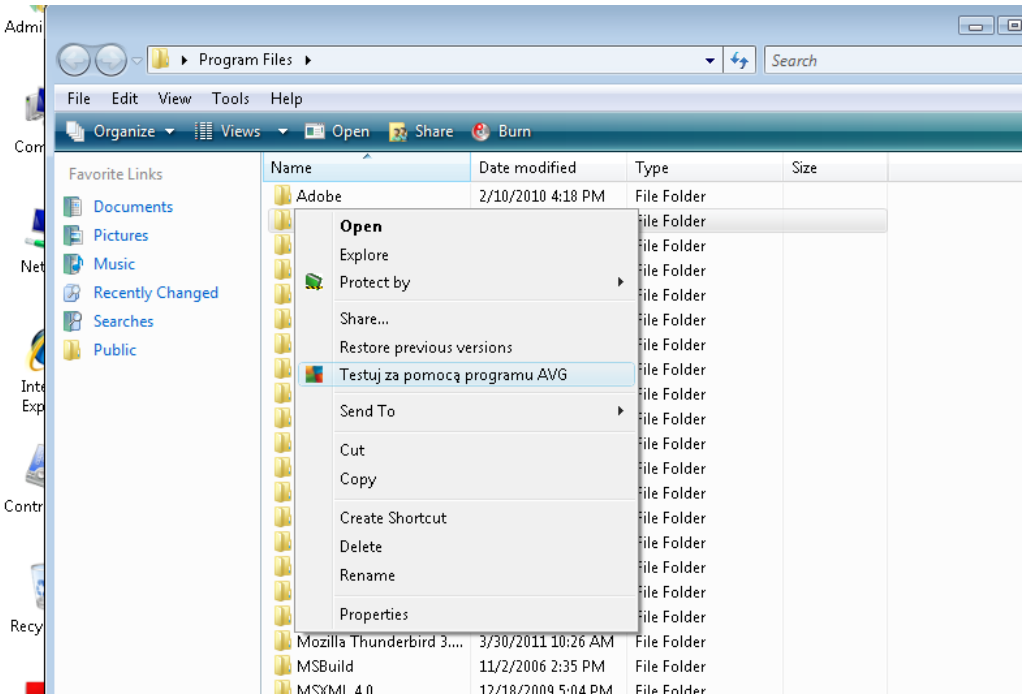
- ***Dodatkowe ustawienia skanowania*** — link ten umożliwia otwarcie okna dialogowego ***dodatkowych ustawień skanowania***, w którym dostępne są opcje automatycznego

wyłączenia komputera po przeprowadzonym ***skanowaniu AntiRootkit: Zamknij komputer po zakończeniu skanowania*** *oraz* ***Wymuś zamknięcie, jeśli komputer jest zablokowany***.



10.3. Skan z poziomu eksploratora systemu Windows

Oprócz wstępnie zdefiniowanych skanów obejmujących cały komputer lub wybrane obszary, system **AVG Anti-Virus 2011** oferuje także możliwość skanowania określonych obiektów bezpośrednio z interfejsu Eksploratora Windows. Jeśli nie ma pewności co do zawartości pliku, który ma zostać otwarty, można przeskanować go „na żądanie". W tym celu należy wykonać następujące kroki:



- W Eksploratorze Windows zaznacz plik (lub folder), który chcesz sprawdzić.
- Kliknij go prawym przyciskiem myszy, aby wyświetlić menu kontekstowe.
- Wybierz polecenie ***Testuj za pomocą programu AVG***, aby system AVG przeskanował dany obiekt.

10.4. Skan z poziomu wiersza poleceń

System **AVG Anti-Virus 2011** posiada opcję uruchamiania skanowania z poziomu wiersza poleceń. Opcji tej można używać na przykład na serwerach lub przy tworzeniu skryptu wsadowego, który ma być uruchamiany po każdym rozruchu komputera. Uruchamiając skanowanie z wiersza poleceń, można używać większości parametrów dostępnych w graficznym interfejsie użytkownika systemu AVG.

Aby uruchomić skanowanie z poziomu wiersza poleceń, należy użyć następującego polecenia w folderze, w którym zainstalowano system AVG:

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

Składnia polecenia

Składnia polecenia jest następująca:

- ***avgscanx /parametr*** ... np. ***avgscanx /comp*** w celu przeskanowania całego komputera
- ***avgscanx /parametr /parametr*** .. — jeśli używanych jest wiele parametrów, należy wpisać je w jednym wierszu, rozdzielając spacjami i ukośnikami
- jeśli parametry wymagają podania określonych wartości, (np. parametr ***/scan*** wymaga informacji o wybranych do przeskanowania obszarach komputera — należy wskazać dokładną ścieżkę), należy je rozdzielać przecinkami, na przykład: ***avgscanx /scan=C:\,D:***

Parametry skanowania

Aby wyświetlić pełny przegląd dostępnych parametrów, należy wpisać odpowiednie polecenie oraz parametr /? lub /HELP (np. ***avgscanx /?***). Jedynym wymaganym parametrem jest /SCAN, który pozwala określić, jakie obszary komputera mają być skanowane. Bardziej szczegółowe informacje na temat opcji zawiera przegląd parametrów wiersza poleceń.

Aby uruchomić skanowanie, należy nacisnąć klawisz ***Enter***. Skanowanie można zatrzymać, naciskając kombinację klawiszy ***Ctrl+C*** lub ***Ctrl+Pause***.

Skanowanie z poziomu wiersza poleceń uruchamiane za pomocą interfejsu graficznego

Gdy komputer działa w trybie awaryjnym, skanowanie z poziomu wiersza poleceń można również uruchomić za pomocą interfejsu graficznego użytkownika. Skanowanie zostanie uruchomione z wiersza poleceń, a okno dialogowe ***Kompozytor wiersza poleceń*** umożliwi jedynie określenie większości parametrów skanowania w wygodnym interfejsie graficznym.

Ponieważ okno to jest dostępne tylko w trybie awaryjnym, jego szczegółowy opis można znaleźć w pliku pomocy dostępnym bezpośrednio z tego okna.

10.4.1. Parametry skanowania z wiersza poleceń

Poniżej przedstawiono listę wszystkich parametrów dostępnych dla skanowania z wiersza poleceń:

- ***/SCAN*** Skanuj określone pliki lub foldery /SCAN=ścieżka;ścieżka (np. /SCAN=C:\;D:\)
- ***/COMP*** Skan całego komputera
- ***/HEUR*** Użyj analizy heurystycznej
- ***/EXCLUDE*** Wyklucz ze skanowania ścieżkę lub pliki
- ***/@*** Plik polecenia /nazwa pliku/
- ***/EXT*** Skanuj te rozszerzenia /na przykład EXT=EXE,DLL/
- ***/NOEXT*** Nie skanuj tych rozszerzeń /na przykład NOEXT=JPG/
- ***/ARC*** Skanuj archiwa
- ***/CLEAN*** Lecz automatycznie
- ***/TRASH*** Przenieś zainfekowane pliki do Przechowalni wirusów
- ***/QT*** Szybki test
- ***/MACROW*** Raportuj pliki zawierające makra
- ***/PWDW*** Raportuj pliki chronione hasłem
- ***/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*** Włącz sprawdzanie MBR/sektora rozruchowego

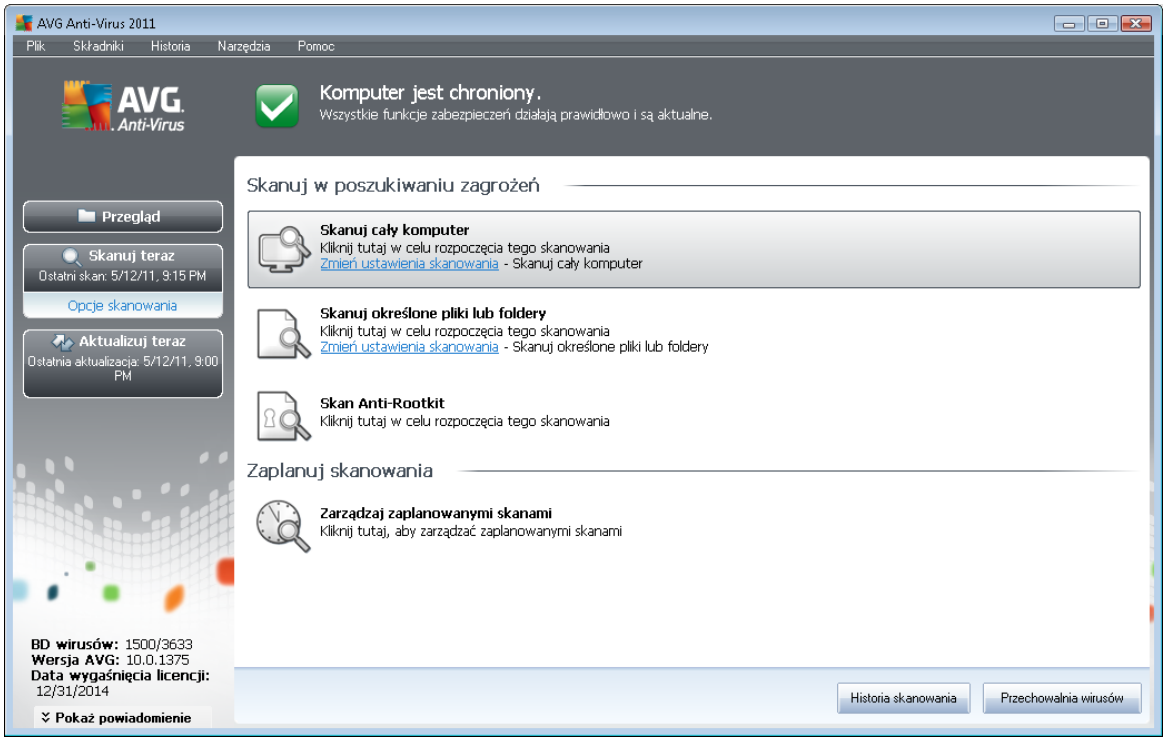
- ***/PROC*** Skanuj aktywne procesy
- ***/PUP*** Raportuj potencjalnie niechciane programy
- ***/REG*** Skanuj rejestr
- ***/COO*** Skanuj pliki cookie
- ***/?*** Wyświetl pomoc na ten temat
- ***/HELP*** Wyświetl pomoc na ten temat
- ***/PRIORITY*** Ustaw priorytet skanowania /Niski, Automatyczny, Wysoki/ (zobacz Ustawienia zaawansowane/ Skany)
- ***/SHUTDOWN*** Zamknij komputer po ukończeniu skanowania
- ***/FORCESHUTDOWN*** Wymuś zamknięcie komputera po ukończeniu skanowania
- ***/ADS*** Skanuj alternatywne strumienie danych (tylko NTFS)
- ***/ARCBOMBSW*** Raportuj wielokrotnie spakowane archiwa

10.5. Planowanie skanowania

System **AVG Anti-Virus 2011** pozwala uruchamiać skanowanie na żądanie (na przykład gdy podejrzewa się infekcję komputera) lub zgodnie z założonym harmonogramem. Stanowczo zaleca się korzystać z harmonogramu: ten sposób daje pewność, że komputer jest chroniony przed infekcjami i zwalnia użytkownika z obowiązku pamiętania o regularnych testach.

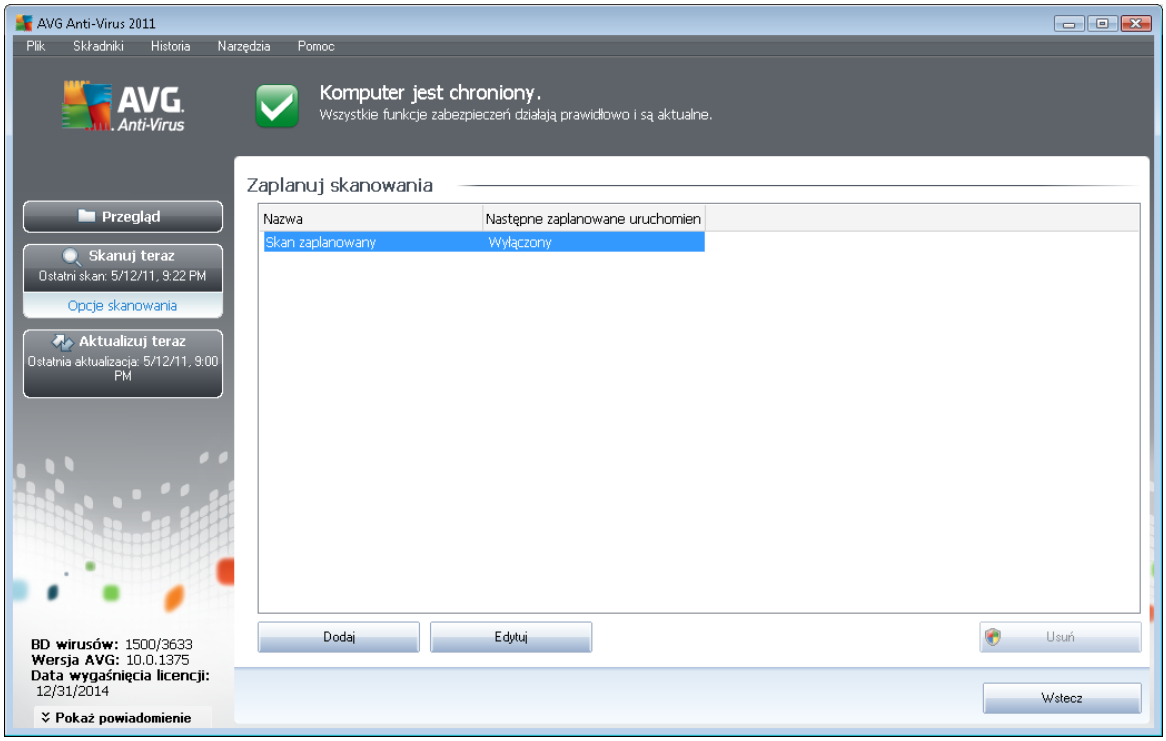
Skan całego komputera należy uruchamiać regularnie co najmniej raz na tydzień. Jeśli jest to możliwe, należy skanować komputer codziennie — zgodnie z domyślną konfiguracją harmonogramu skanowania. Jeśli komputer działa 24 godziny na dobę, można zaplanować skanowanie poza czasem pracy. Jeśli komputer jest czasami wyłączany, pominięte z tego powodu skany uruchamiane są po ponownym włączeniu komputera.

Aby utworzyć nowe harmonogramy, skorzystaj z przycisku znajdującego się w dolnej części interfejsu skanera AVG, w sekcji ***Zaplanuj skanowania***:



Zaplanuj skanowania

Kliknij ikonę w sekcji ***Zaplanuj skanowania***, aby otworzyć nowe okno dialogowe ***planowania skanowania***, które zawiera listę wszystkich zaplanowanych testów:

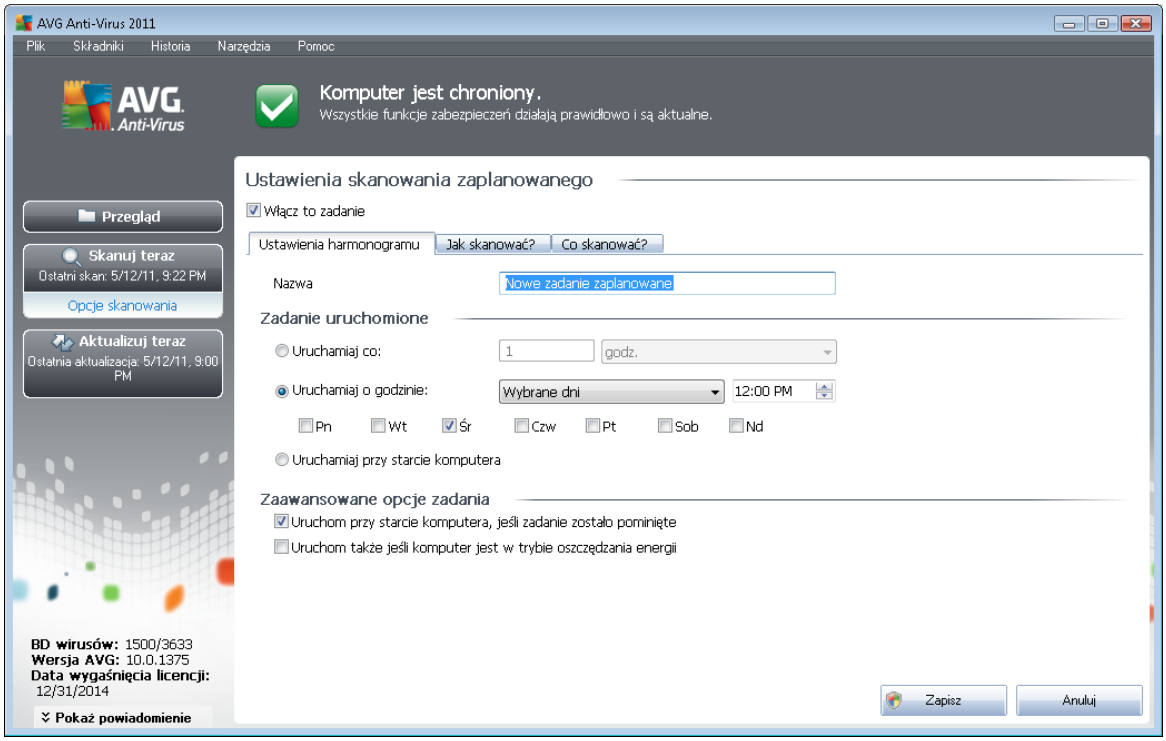


Zawartość okna można edytować, używając następujących przycisków:

- ***Dodaj*** — otwiera okno ***Ustawienia skanowania zaplanowanego***, a w nim kartę ***Ustawienia harmonogramu***. W oknie tym można określić parametry definiowanego testu.
- ***Edytuj*** — jest aktywny tylko, jeśli wybrano istniejący test na liście zaplanowanych testów. W takim przypadku kliknięcie przycisku powoduje przejście do okna dialogowego ***Ustawienia skanowania zaplanowanego***, na kartę ***Ustawienia harmonogramu***. Parametry wybranego testu są już określone i można je edytować.
- ***Usuń*** — jest aktywny tylko, jeśli wybrano istniejący test na liście zaplanowanych skanów. Kliknięcie przycisku spowoduje usunięcie wybranej pozycji z listy. Usuwać można jedynie testy zdefiniowane przez użytkownika; nie można usunąć predefiniowanego ***Zaplanowanego skanu całego komputera*** z ustawieniami domyślnymi.
- ***Wstecz*** — pozwala wrócić do interfejsu skanera AVG

10.5.1. Ustawienia harmonogramu

Aby zaplanować nowy test i uruchamiać go regularnie, należy przejść do okna dialogowego ***Ustawienia zaplanowanego testu*** (*klikając przycisk* ***Dodaj harmonogram skanowania*** *w oknie dialogowym* ***Planowanie skanowania***). Okno dialogowe jest podzielone na trzy karty: ***Ustawienia harmonogramu*** — *zobacz ilustracja poniżej(karta otwierana domyślnie),* ***Jak skanować*** i ***Co skanować***.



Na karcie ***Ustawienia harmonogramu*** można zaznaczyć pole ***Włącz to zadanie***, aby tymczasowo wyłączyć zaplanowany test lub włączyć go ponownie, gdy zajdzie taka potrzeba.

Następnie należy nazwać nowo tworzony skan. Nazwę można wpisać w polu tekstowym obok etykiety ***Nazwa.*** Należy używać krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości.

Przykład: *Nazwy takie jak „Nowy skan” lub „Mój skan” nie są odpowiednie, ponieważ nie informują o tym, co jest przedmiotem skanowania. Przykładem dobrej opisowej nazwy jest „Skan obszarów systemowych”. Ponadto, nie ma potrzeby określać w nazwie skanowania, czy skanowany jest cały komputer, czy tylko jego wybrane obszary — własne testy użytkownika są zawsze specyficznym skanowaniem określonych plików lub folderów.*

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

- ***Zadanie uruchomione*** — należy określić interwał przeprowadzanych testów. Skanowanie może być powtarzane w określonych odstępach czasu (***Uruchamiaj co***) lub o zadanej godzinie (***Uruchamiaj o określonej godzinie***), a także na skutek wystąpienia zdefiniowanego zdarzenia (***W oparciu o akcję, np. uruchomienie komputera***).

- ***Zaawansowane opcje zadania*** — ta sekcja umożliwia zdefiniowanie warunków skanowania w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

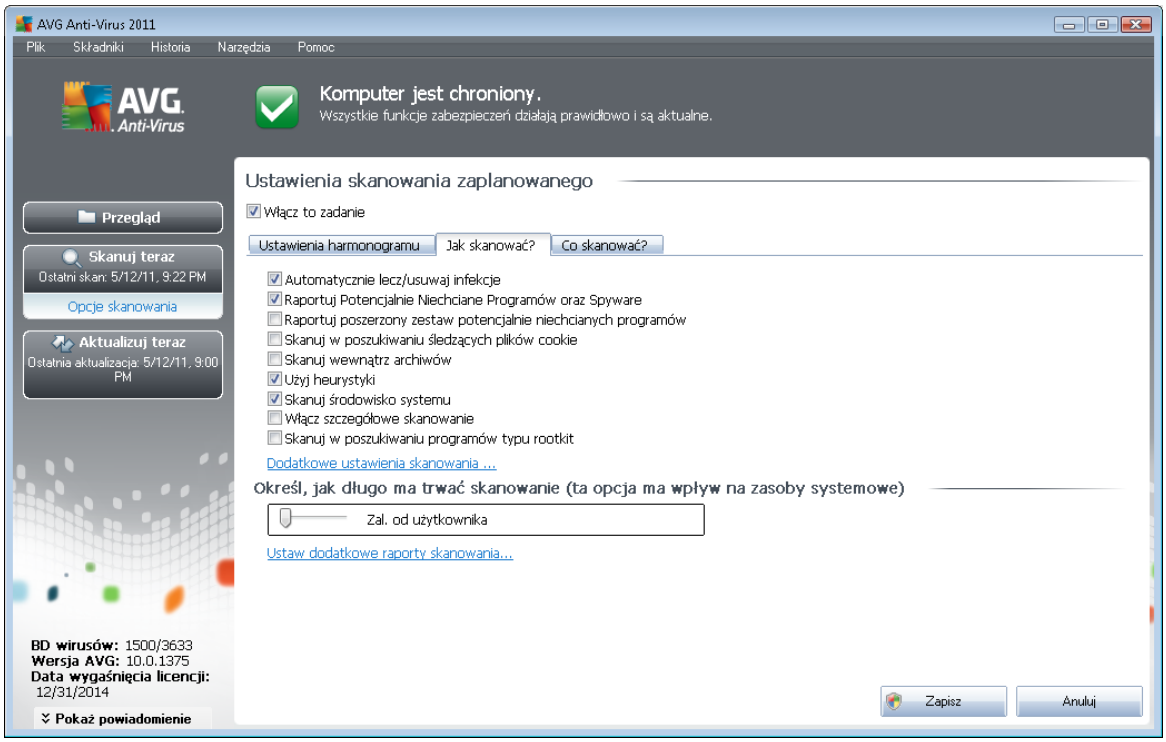
Przyciski kontrolne konfiguracji harmonogramu

Na wszystkich trzech kartach okna dialogowego ***Ustawienia zaplanowanego skanowania*** (***Ustawienia harmonogramu***, ***Jak skanować*** i ***Co skanować***) dostępne są dwa przyciski kontrolne. Działanie tych przycisków jest identyczne na każdej karcie:

- ***Zapisz*** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyślnego okna Interfejsu użytkownika AVG. Oznacza to, że aby zapisać nowe parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.

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

10.5.2. Jak skanować?



Karta ***Jak skanować?*** zawiera listę parametrów testu, które można włączyć lub wyłączyć. Domyślnie większość funkcji jest włączona, a odpowiadające im ustawienia są stosowane podczas skanowania. Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachowując wstępnie zdefiniowaną konfigurację:

- ***Automatycznie lecz/usuwaj infekcje*** (*opcja domyślnie włączona*) — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowanego pliku nie można wyleczyć, lub jeśli opcja ta zostanie wyłączona, system powiadomi o wykryciu wirusa i zapyta o sposób reakcji na infekcję. Zalecaną czynnością jest przeniesienie zainfekowanego pliku do ***Przechowalni wirusów***.

- ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje włączenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów).

Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji, gdyż znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

- ***Skanuj w poszukiwaniu śledzących plików cookie*** (*opcja domyślnie wyłączona*) — ten parametr składnika ***Anti-Spyware*** określa, czy wykrywane mają być pliki cookie *(używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** (*opcja domyślnie wyłączona*) — parametr ten określa, czy skanowanie ma obejmować pliki znajdujące się wewnątrz niektórych typów archiwów, np. ZIP, RAR itd.

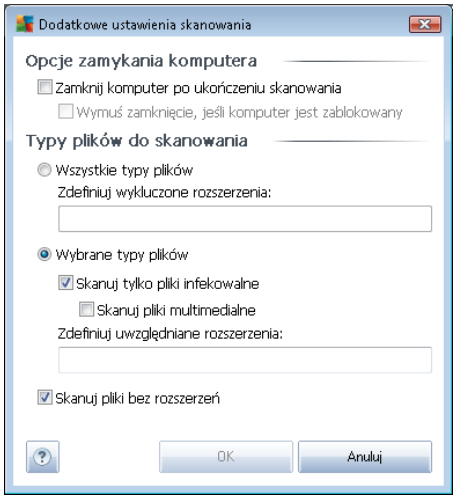
- ***Użyj heurystyki*** (*opcja domyślnie włączona*) — analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) będzie jedną z metod wykrywania wirusów w czasie skanowania.

- ***Skanuj środowisko systemu*** (*opcja domyślnie włączona*) — skanowanie obejmie także obszary systemowe komputera.

- ***Włącz szczegółowe skanowanie*** (*domyślnie wyłączone*) — w określonych sytuacjach (*gdy zachodzi podejrzenie, że komputer jest zainfekowany*) można zaznaczyć tę opcję, aby aktywować algorytmy bardziej dokładnego skanowania, które w celu uzyskania absolutnej pewności będą skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

Następnie można zmienić konfigurację skanowania zgodnie z poniższym opisem:

- ***Dodatkowe ustawienia skanowania*** — link do okna dialogowego ***Dodatkowe ustawienia skanowania***, w którym można określić następujące parametry:



- ***Opcje wyłączania komputera*** — określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukończeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, gdy jest zablokowany (***Wymuś zamknięcie, jeśli komputer jest zablokowany***).

- ***Zdefiniuj typy plików do skanowania*** — należy zdecydować, które z poniższych elementów mają być skanowane:

  - ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być skanowane;

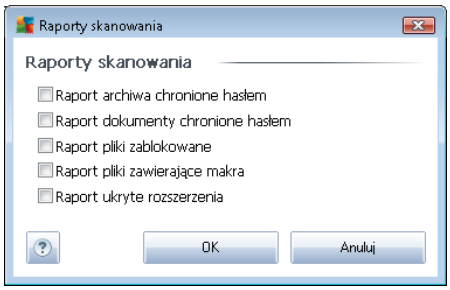
  - ***Wybrane typy plików*** — skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje*). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

  - Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

- ***Określ, jak długo ma trwać skanowanie*** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślna wartość tej opcji to poziom *Zależny od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas jego trwania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer jest tymczasowo nieużywany*).

- ***Ustaw dodatkowe raporty skanowania*** — ten link pozwala otworzyć nowe okno

dialogowe ***Raporty skanowania***, w którym można określić raportowane elementy lub zdarzenia:



Uwaga: *Domyślnie konfiguracja jest ustawiona pod kątem optymalnej wydajności. Konfigurację skanowania należy zmieniać tylko w uzasadnionych sytuacjach. Stanowczo zaleca się stosowanie wstępnie zdefiniowanych ustawień. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Więcej opcji dostępne jest w oknie* ***Ustawienia zaawansowane****, (* ***Menu główne/Plik/Ustawienia zaawansowane****).*

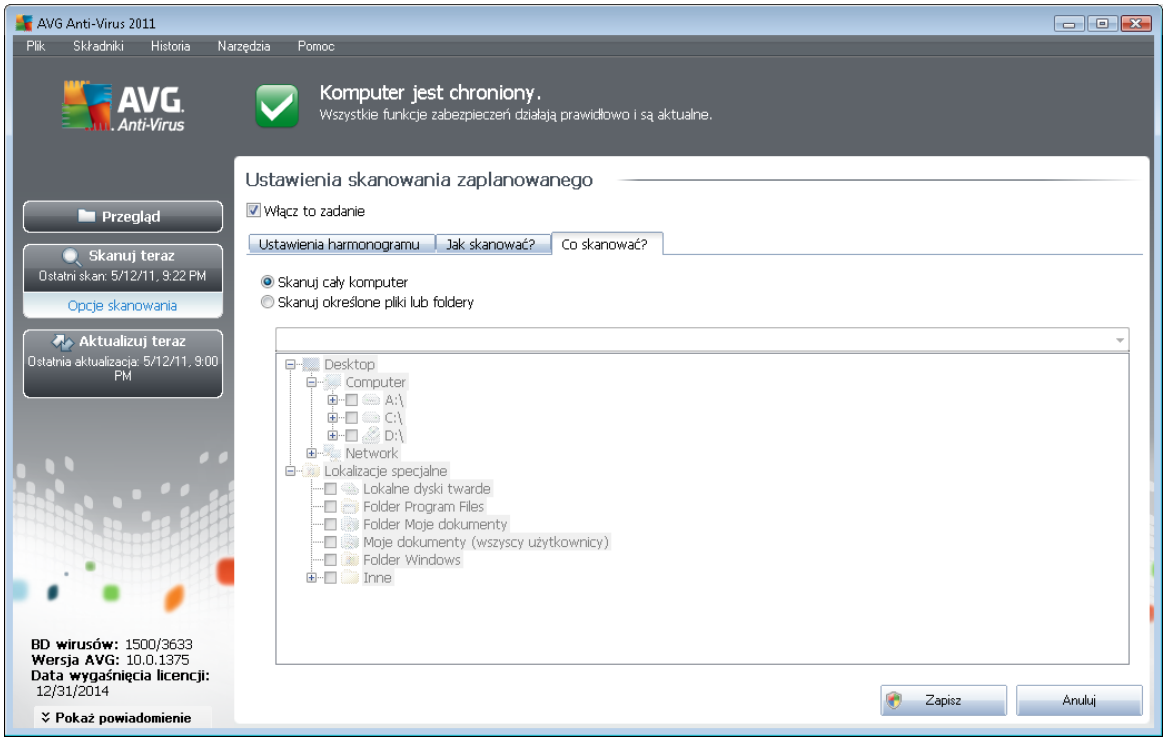
Przyciski kontrolne

Na wszystkich trzech kartach okna dialogowego ***Konfiguracja skanu zaplanowanego*** (***Ustawienia harmonogramu***, ***Jak skanować?*** i ***Co skanować?***) dostępne są dwa przyciski kontrolne. Ich działanie na każdej karcie jest takie samo:

- ***Zapisz*** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyślnego okna Interfejsu użytkownika AVG. Oznacza to, że aby zapisać nowe parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.

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

10.5.3. Co skanować?



Na karcie ***Co skanować?*** można określić, czy planowane jest skanowanie całego komputera, czy skanowanie określonych plików lub folderów.

Jeśli zostanie wybrane skanowanie określonych plików lub folderów, w dolnej części tego okna dialogowego zostanie aktywowane drzewo katalogów, które umożliwi wybranie folderów do skanowania (*rozwijaj pozycje, klikając znak plusa, dopóki nie znajdziesz folderu, który ma zostać przeskanowany*). Zaznaczając więcej pól, można wybrać kilka folderów. Wybrane foldery zostaną wyświetlone w polu tekstowym u góry okna dialogowego, a historia wybranych skanów będzie przechowywana w rozwijanym menu do późniejszego użytku. Opcjonalnie można wprowadzić ręcznie pełną ścieżkę dostępu wybranego folderu (*w przypadku kilku ścieżek należy je rozdzielić średnikiem bez dodatkowej spacji*).

Drzewo katalogów zawiera również gałąź ***Lokalizacje specjalne***. Poniżej znajduje się lista tych lokalizacji; będą one skanowane, jeśli zostanie obok nich zaznaczone odpowiednie pole wyboru:

- ***Lokalne dyski twarde*** — wszystkie dyski twarde na tym komputerze
- ***Folder Program Files***
    - C:\Program Files\
    - *w wersji 64-bitowej* C:\Program Files (x86)
- ***Folder Moje dokumenty***

- *dla systemu Win XP:* C:\Documents and Settings\Default User\Moje dokumenty\
- *dla systemu Windows Vista/7*: C:\Users\user\Documents\

- ***Moje dokumenty (wszyscy użytkownicy)***
  - *dla systemu Win XP*: C:\Documents and Settings\All Users\Documents\
  - *dla systemu Windows Vista/7*: C:\Users\Public\Documents\

- ***Folder Windows*** — C:\Windows\

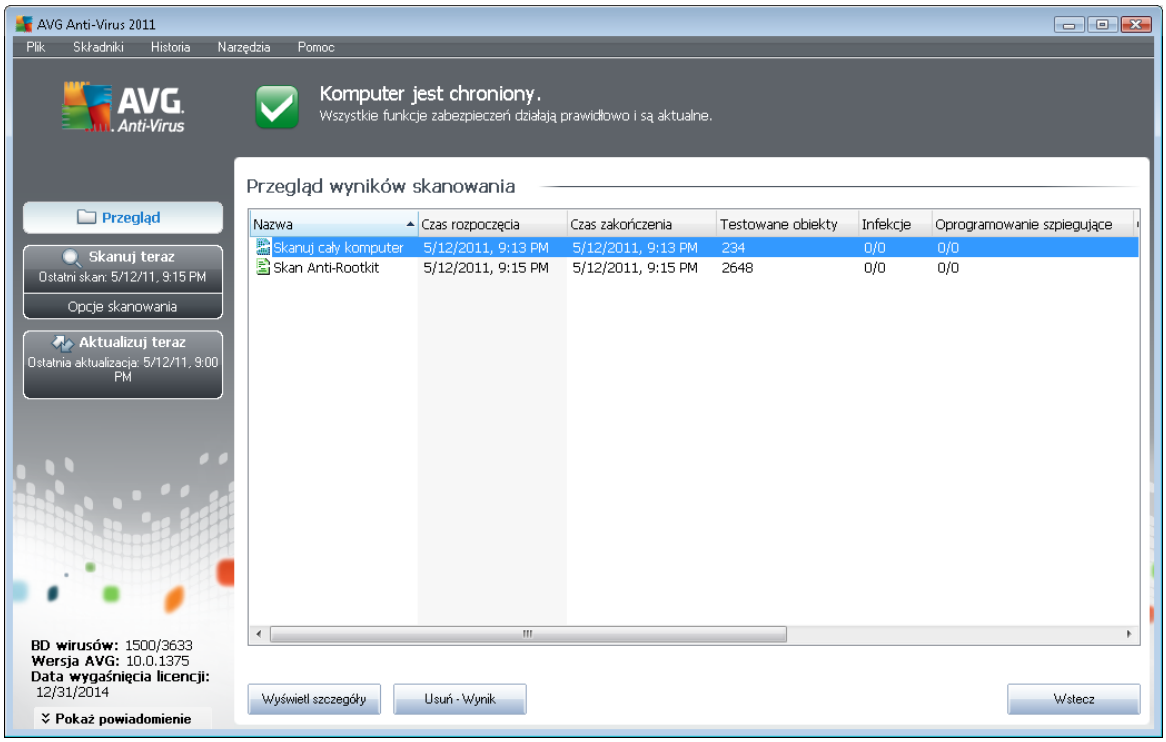
- ***Inne***
  - *Dysk systemowy* — dysk twardy, na którym zainstalowany jest system operacyjny (zazwyczaj C:)
  - *Folder systemowy* - C:\Windows\System32\
  - *Folder plików tymczasowych* — C:\Documents and Settings\User\Local\ (*Windows XP*) lub C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Folder tymczasowych plików internetowych* — C:\Documents and Settings\User\Ustawienia lokalne\Temporary Internet Files\ (*Windows XP*) lub C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Przyciski kontrolne konfiguracji harmonogramu

Na wszystkich trzech kartach okna z ***konfiguracją skanu zaplanowanego*** (***Ustawienia harmonogramu***, ***Jak skanować?*** i ***Co skanować?***) dostępne są dwa przyciski kontrolne. Ich działanie na każdej karcie jest takie same:

- ***Zapisz*** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyślnego okna interfejsu użytkownika systemu AVG. Oznacza to, że aby zapisać nowe parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.
- ***Anuluj*** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyślnego okna Interfejsu użytkownika AVG.

10.6. Przegląd wyników skanowania



Dostęp do okna ***Przegląd wyników skanowania*** możliwy jest z poziomu Interfejsu skanera AVG, przez kliknięcie przycisku ***Historia skanowania***. Okno to zawiera listę wszystkich wcześniejszych testów oraz informacje o ich wynikach:

- ***Nazwa*** — oznaczenie skanowania; może to być nazwa jednego ze wstępnie zdefiniowanych skanów lub nazwa nadana przez użytkownika jego skanowi zaplanowanemu. Każdej nazwie towarzyszy ikona określająca wynik skanowania:

  — zielona oznacza, że nie wykryto żadnych infekcji;

  — niebieska ikona oznacza, że wykryto infekcję, ale zainfekowany obiekt został automatycznie usunięty.

  — czerwona oznacza, że wykryto infekcję i nie udało się jej usunąć.

  Każda z ikon może być widoczna w całości lub „przerwana” — jeśli ikona jest cała, skanowanie zostało prawidłowo ukończone; w przeciwnym razie skanowanie zostało anulowane lub przerwane.

  Uwaga: *Szczegółowe informacje na temat każdego testu zawiera okno* ***Wyniki skanowania*** *dostępne po kliknięciu przycisku* ***Wyświetl szczegóły*** *(w dolnej części okna).*

- ***Czas rozpoczęcia*** — data i godzina uruchomienia testu.

- ***Czas zakończenia*** — data i godzina zakończenia skanowania.
- ***Przetestowano obiektów*** — liczba obiektów sprawdzonych podczas skanowania.
- ***Infekcje*** — liczba infekcji wirusowych, które zostały wykryte/usunięte.
- ***Oprogramowanie szpiegujące*** — liczba programów szpiegujących, które zostały wykryte/usunięte.
- ***Ostrzeżenia*** — liczba wykrytych podejrzanych obiektów
- ***Programy typu rootkit*** — liczba wykrytych programów typu rootkit
- ***Informacji w dzienniku skanowania*** — informacje dotyczące przebiegu i wyniku skanowania (zwykle o jego zakończeniu lub przerwaniu).

Przyciski kontrolne

Przyciski kontrolne dostępne w oknie ***Przegląd wyników skanowania*** to:

- ***Wyświetl szczegóły*** — kliknięcie tego przycisku powoduje przełączenie się do okna dialogowego ***Wyniki skanowania***, w którym można przejrzeć szczegółowe dane dotyczące wybranego skanowania.
- ***Usuń wynik*** — kliknięcie tego przycisku powoduje usunięcie wybranej pozycji z przeglądu wyników skanowania.
- ***Wstecz*** — otwiera ponownie domyślne okno Interfejsu skanera AVG.

10.7. Szczegóły wyników skanowania

Po wybraniu w oknie ***Przegląd wyników skanowania*** któregoś z testów, można kliknąć przycisk ***Wyświetl szczegóły***, aby przejść do okna ***Wyniki skanowania***, które zawiera dodatkowe informacje o jego przebiegu.

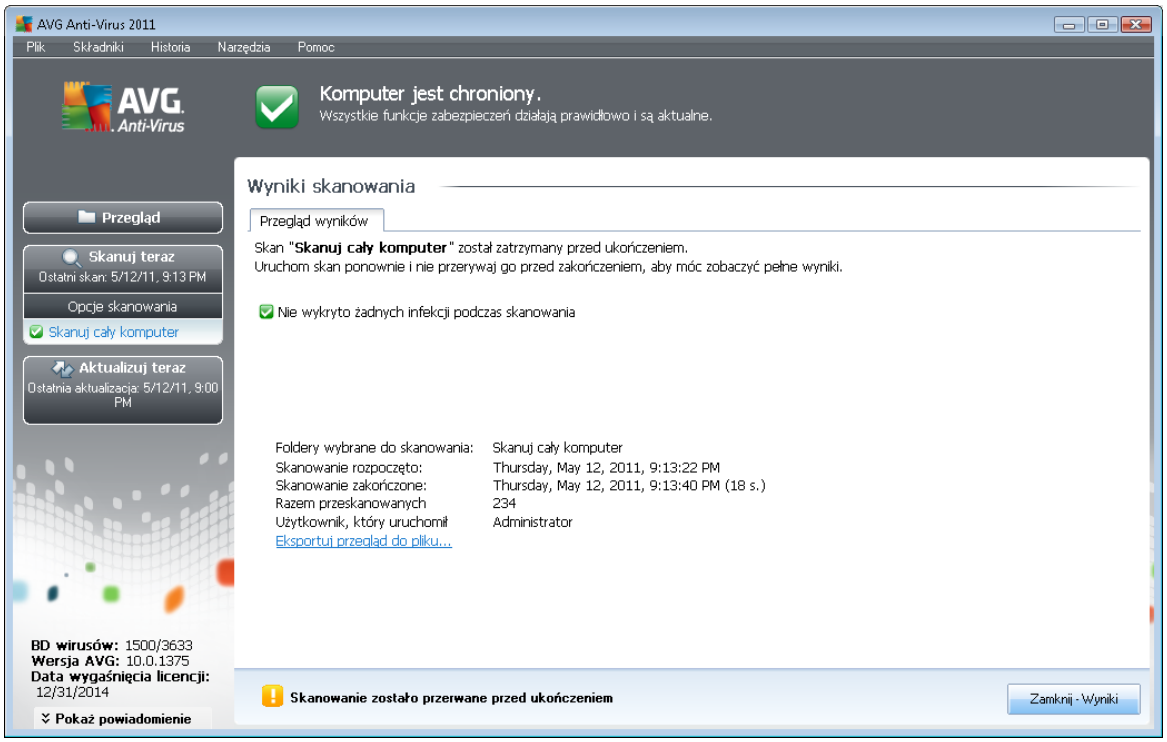
Okno to podzielone jest na kilka kart:

- ***Przegląd wyników*** — karta jest zawsze wyświetlana; zawiera statystyki dotyczące przebiegu skanowania.
- ***Infekcje*** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto co najmniej jedną infekcję wirusową.
- ***Oprogramowanie szpiegujące*** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto oprogramowanie szpiegujące.
- ***Ostrzeżenia*** — ta karta jest wyświetlana m.in. wówczas, gdy podczas skanowania wykryto pliki cookie.
- ***Programy typu rootkit*** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto

programy typu rootkit.

- ***Informacje*** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto potencjalne zagrożenia, których nie można było zakwalifikować do powyższych kategorii; dla każdego znalezionego obiektu wyświetlany jest komunikat ostrzegawczy. Dodatkowo, są tu wyświetlane informacje o obiektach, które nie mogły zostać przeskanowane (np. archiwa chronione hasłem).

10.7.1. Karta Przegląd wyników



Na karcie ***Wyniki skanowania*** można znaleźć szczegółowe statystyki oraz informacje o:

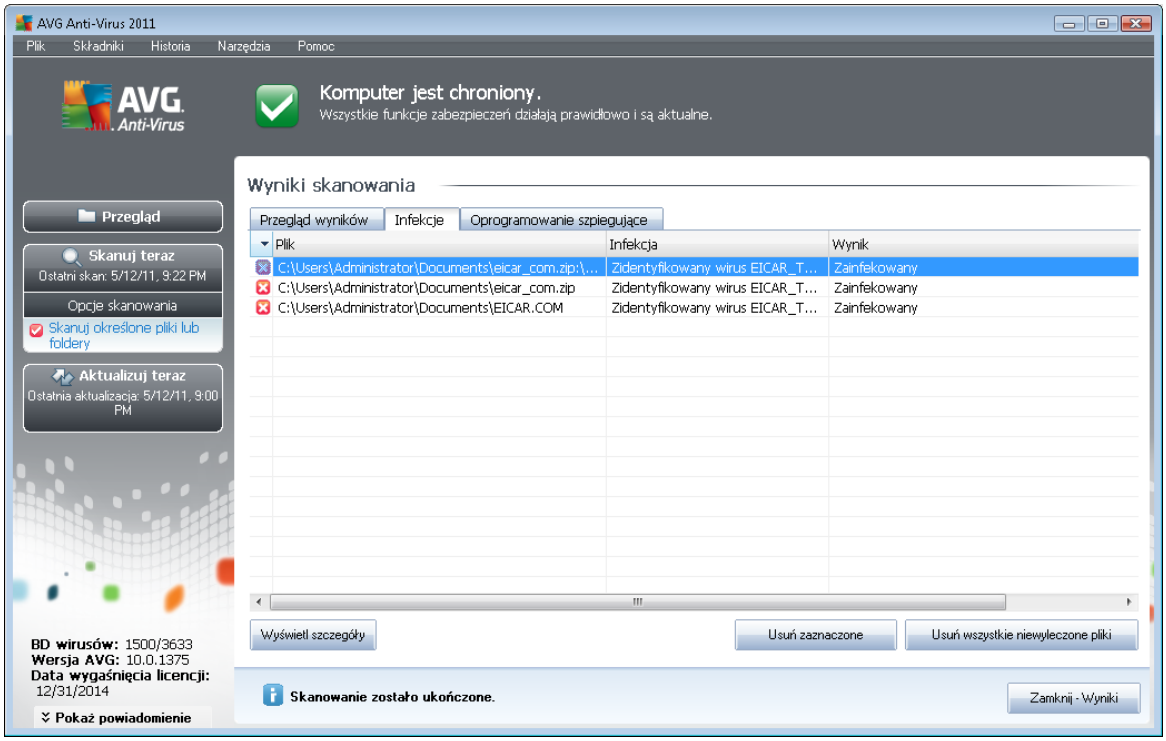
- wykrytych infekcjach wirusowych/programach szpiegujących
- usuniętychinfekcjach wirusowych/programach szpiegujących
- liczbie infekcji wirusowych/programów szpiegujących, których nie udało się usunąć ani wyleczyć.

Ponadto, znajdują się tu informacje o dacie i dokładnej godzinie uruchomienia testu, łącznej liczbie przeskanowanych obiektów, czasie trwania oraz liczbie napotkanych błędów.

Przyciski kontrolne

Okno to zawiera tylko jeden przycisk kontrolny. Kliknięcie przycisku ***Zamknij wyniki*** powoduje powrót do ***Przeglądu wyników skanowania***.

10.7.2. Karta Infekcje



Karta ***Infekcje*** jest wyświetlana w oknie dialogowym ***Wyniki skanowania*** tylko, jeśli podczas skanowania wykryto wirusa. Karta jest podzielona na trzy obszary, które zawierają następujące informacje:

- ***Plik*** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** — nazwa wykrytego wirusa (*szczegółowe informacje na temat wirusów zawiera Encyklopedia Wirusów dostępna online*).
- ***Wynik*** — określa bieżący stan zainfekowanego obiektu, który wykryto podczas skanowania:
    - ***Zainfekowany*** — zainfekowany obiekt został wykryty i pozostawiony w oryginalnej lokalizacji (*np. jeśli wyłączono opcję automatycznego leczenia w szczegółowych ustawieniach skanowania).*
    - ***Wyleczony*** — zainfekowany obiekt został automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
    - ***Przeniesiony do Przechowalni*** — zainfekowany obiekt został przeniesiony do ***Przechowalni wirusów***.
    - ***Usunięty*** — zainfekowany obiekt został usunięty.
    - ***Dodany do listy wyjątków PNP*** — znaleziony obiekt został uznany za wyjątek i

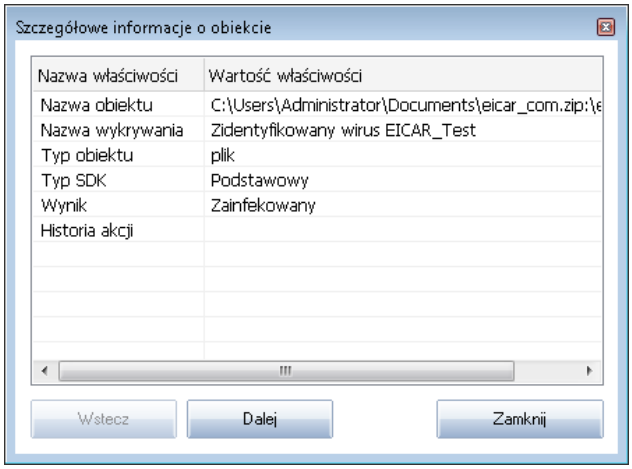
dodany do listy wyjątków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie* ***Wyjątki PNP***).

- **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanować.
- **Obiekt potencjalnie niebezpieczny** — obiekt został uznany za potencjalnie niebezpieczny, ale nie zainfekowany (*może na przykład zawierać makra*); informacje tę należy traktować wyłącznie jako ostrzeżenie.
- **Wymagany restart systemu** — aby całkowicie usunąć zainfekowany obiekt, należy ponownie uruchomić komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

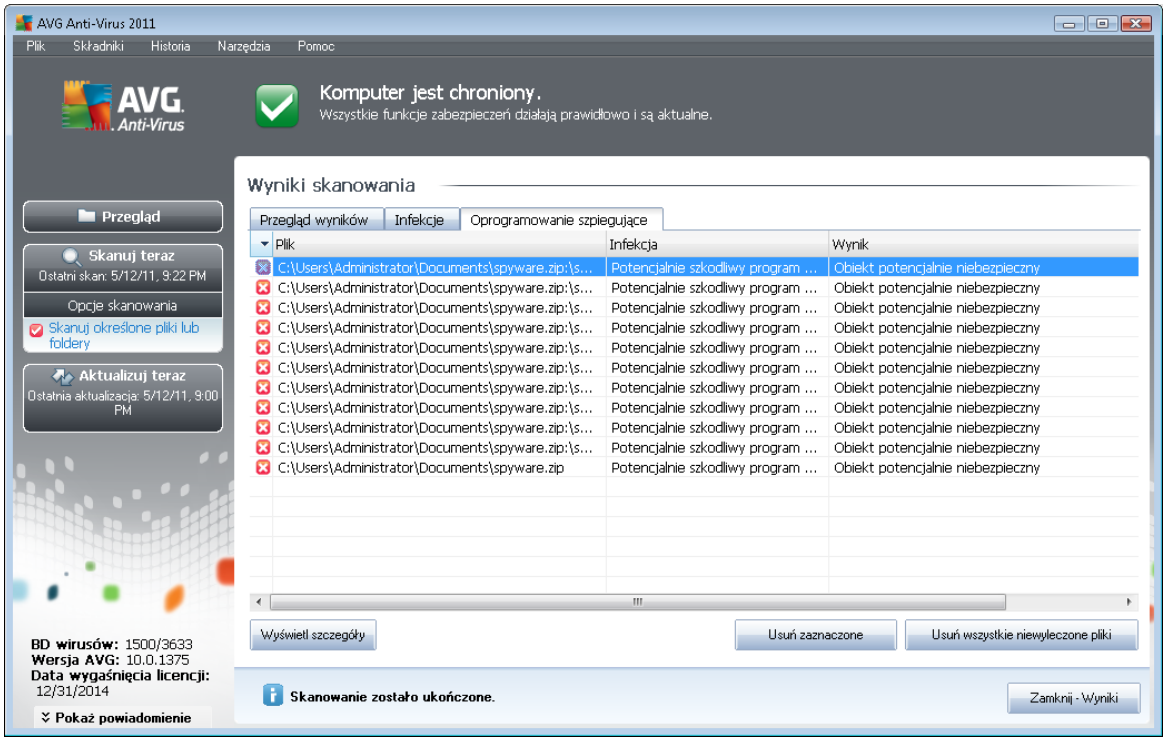
- ***Wyświetl szczegóły*** — otwiera nowe okno dialogowe ze ***szczegółowymi informacjami o obiekcie***:



  W tym oknie dialogowym można znaleźć szczegółowe informacje o wykrytym zainfekowanym obiekcie (*takie jak nazwa i położenie zainfekowanego obiektu, typ obiektu, typ SDK, wynik detekcji oraz historia akcji związanych z wykrytym obiektem*). Za pomocą przycisków ***Wstecz*** / ***Dalej*** można wyświetlać informacje o znalezionych obiektach. Przycisk ***Zamknij*** zamyka okno.

- ***Usuń wybrane*** — pozwala przenieść wybrane obiekty do ***Przechowalni wirusów.***
- ***Usuń wszystkie niewyleczone*** — pozwala usunąć wszystkie znalezione obiekty, których nie można wyleczyć ani przenieść do ***Przechowalni wirusów.***
- ***Zamknij wyniki*** — powoduje zamknięcie szczegółowych wyników i powrót do okna ***Przegląd wyników skanowania***.

10.7.3. Karta Oprogramowanie szpiegujące



Karta ***Oprogramowanie szpiegujące*** jest wyświetlana w oknie dialogowym ***Wyniki skanowania*** tylko, jeśli podczas skanowania wykryto oprogramowanie szpiegujące. Karta jest podzielona na trzy obszary, które zawierają następujące informacje:

- ***Plik*** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** — nazwa wykrytego oprogramowania szpiegującego (*szczegółowe informacje na temat wirusów zawiera* ***Encyklopedia wirusów*** *dostępna online*).
- ***Wynik*** — określa bieżący stan obiektu, który wykryto podczas skanowania:
    - ***Zainfekowany*** — zainfekowany obiekt został wykryty i pozostawiony w oryginalnej lokalizacji (np. jeśli wyłączono opcję automatycznego leczenia w szczegółowych ustawieniach skanowania).
    - ***Wyleczony*** — zainfekowany obiekt został automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
    - ***Przeniesiony do Przechowalni*** — zainfekowany obiekt został przeniesiony do ***Przechowalni wirusów***.
    - ***Usunięty*** — zainfekowany obiekt został usunięty.
    - ***Dodany do listy wyjątków PNP*** — znaleziony obiekt został uznany za wyjątek i dodany do listy wyjątków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w*

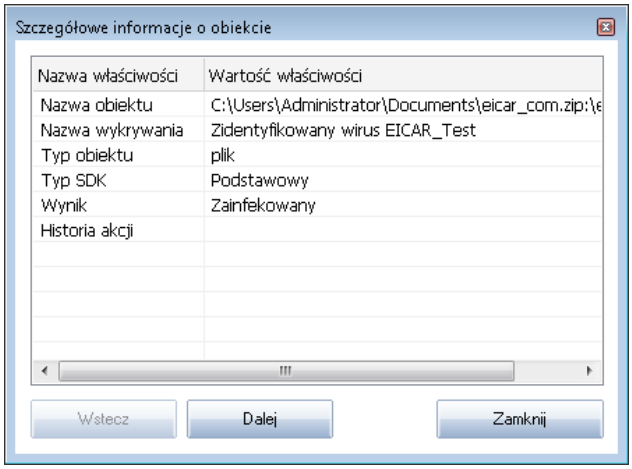
oknie ***Wyjątki PNP****).*

- **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanować.
- **Obiekt potencjalnie niebezpieczny** — obiekt został uznany za potencjalnie niebezpieczny, ale nie zainfekowany (może np. zawierać makra); informacja ta jest wyłącznie ostrzeżeniem.
- **Wymagany restart systemu** — aby całkowicie usunąć zainfekowany obiekt, należy ponownie uruchomić komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

- ***Wyświetl szczegóły*** — otwiera nowe okno dialogowe ze ***szczegółowymi informacjami o obiekcie***:



W tym oknie dialogowym można znaleźć szczegółowe informacje o wykrytym zainfekowanym obiekcie (*takie jak nazwa i położenie zainfekowanego obiektu, typ obiektu, typ SDK, wynik detekcji oraz historia akcji związanych z wykrytym obiektem*). Za pomocą przycisków ***Wstecz*** / ***Dalej*** można wyświetlać informacje o znalezionych obiektach. Przycisk ***Zamknij*** zamyka okno.

- ***Usuń wybrane*** — pozwala przenieść wybrane obiekty do ***Przechowalni wirusów.***
- ***Usuń wszystkie niewyleczone*** — pozwala usunąć wszystkie znalezione obiekty, których nie można wyleczyć ani przenieść do ***Przechowalni wirusów.***
- ***Zamknij wyniki*** — powoduje zamknięcie szczegółowych wyników i powrót do okna ***Przegląd wyników skanowania***.

10.7.4. Karta Ostrzeżenia

Karta ***Ostrzeżenia*** zawiera informacje o „podejrzanych" obiektach (*zwykle plikach*) wykrytych podczas skanowania. Gdy ***Ochrona Rezydentna*** wykryje takie pliki, zazwyczaj blokuje do nich dostęp. Typowe przykłady obiektów tego typu to: ukryte pliki, cookies, podejrzane klucze rejestru, zabezpieczone hasłem archiwa i dokumenty itp. Pliki te nie stanowią żadnego bezpośredniego zagrożenia dla bezpieczeństwa komputera i użytkownika. Informacje o nich przydatne są jednak w wypadku wykrycia na komputerze oprogramowania reklamowego lub szpiegującego. Jeśli podczas testu AVG pojawiły się tylko ostrzeżenia, nie jest konieczne podejmowanie jakichkolwiek działań.

Oto krótki opis najbardziej popularnych obiektów tego typu:

- ***Pliki ukryte*** Pliki ukryte są domyślnie niewidoczne dla użytkownika w systemie Windows. Niektóre wirusy mogą próbować uniknąć wykrycia przez wykorzystanie tej właściwości. Jeśli system AVG zgłasza obecność ukrytego pliku, który może być szkodliwy, można przenieść go do ***Przechowalni wirusów AVG***.

- ***Pliki cookie*** Pliki cookie to pliki tekstowe wykorzystywane przez strony internetowe do przechowywania informacji właściwych dla danego użytkownika. Są one później używane do ładowania witryn internetowych dostosowanych do wymagań użytkownika, itp.

- ***Podejrzane klucze rejestru*** Niektóre szkodliwe oprogramowanie przechowuje informacje w rejestrze systemu Windows, aby uruchamiać się podczas ładowania systemu lub rozszerzyć zakres swojego działania.

10.7.5. Karta Rootkity

Karta ***Programy typu rootkit*** zawiera informacje o programach typu rootkit wykrytych podczas skanowania (jeśli został uruchomiony ***skan Anti-Rootkit***).

Program typu rootkit to wirus zaprojektowany w celu przejęcia całkowitej kontroli nad systemem komputerowym bez zgody jego właścicieli czy upoważnionych administratorów. Bezpośredni dostęp do sprzętu jest rzadko wymagany, ponieważ programy typu rootkit w pełni zdalnie kontrolują system operacyjny komputera. Zwykle ukrywają one swoją obecność poprzez przejęcie kontroli nad standardowymi mechanizmami bezpieczeństwa systemu operacyjnego. Wiele z nich jest jednocześnie końmi trojańskimi, które dodatkowo starają się przekonać użytkowników, że ich systemy są bezpieczne. Techniki stosowane przez programy typu rootkit to m.in. ukrywanie uruchomionych procesów przed programami monitorującymi oraz ukrywanie plików lub danych przed samym systemem operacyjnym.

Struktura tej karty jest w zasadzie taka sama jak kart ***Infekcje*** i ***Oprogramowanie szpiegujące***.

10.7.6. Karta Informacje

Karta ***Informacje*** zawiera dane dotyczące znalezionych obiektów, których nie można zakwalifikować jako infekcje, oprogramowanie szpiegujące itp. Obiektów tych nie można w stu procentach uznać za niebezpieczne, ale często wymagają one uwagi użytkownika. Skaner AVG jest w stanie wykryć pliki, które mogą nie być zainfekowane, ale są podejrzane. Zgłaszane będą one jako ***lub*** Informacja.

Informacje o zagrożeniu mogą być zgłaszane z jednego z następujących powodów:

- ***Plik kompresowany w czasie rzeczywistym*** - Plik został skompresowany przy użyciu jednego z mniej popularnych programów kompresujących w czasie wykonania, co może wskazywać na próbę uniemożliwienia skanowania takiego pliku. Nie każde zgłoszenie takiego pliku oznacza obecność wirusa.

- ***Plik rekurencyjnie kompresowany w czasie rzeczywistym*** - Podobny do powyższego, ale rzadziej spotykany wśród zwykłego oprogramowania. Takie pliki są podejrzane i należy rozważyć ich usunięcie lub przesłanie do analizy.

- ***Archiwum lub dokument chroniony hasłem*** - Pliki chronione hasłem nie mogą być skanowane przez program AVG (*ani generalnie przez żaden inny program chroniący przed szkodliwym oprogramowaniem*).

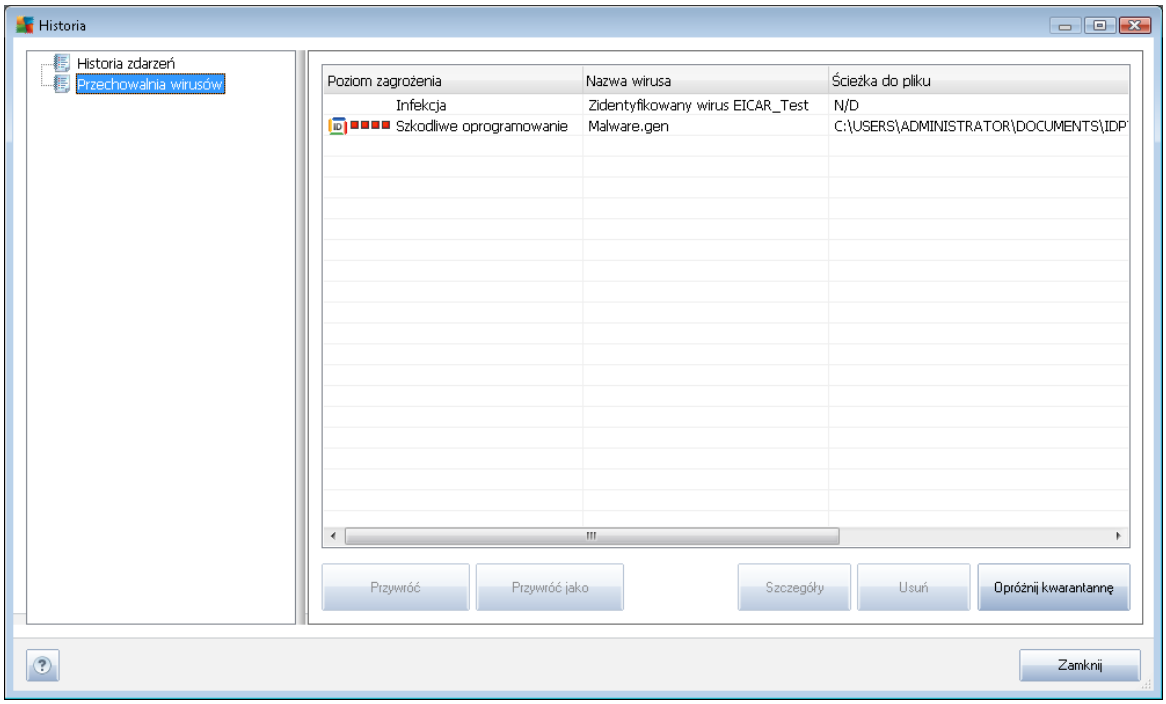
- ***Dokument zawierający makra*** — zgłoszone dokumenty zawierają makra, które mogą być szkodliwe.

- ***Ukryte rozszerzenie*** — pliki z ukrytymi rozszerzeniami mogą udawać np. obrazy, podczas gdy w rzeczywistości są plikami wykonywalnymi (*np. "obrazek.jpg.exe"*). Drugie rozszerzenie jest w systemie Windows domyślnie niewidoczne. Program AVG zgłasza takie pliki, aby zapobiec ich przypadkowemu uruchomieniu.

- ***Niewłaściwa ścieżka do pliku*** — jeżeli jakiś ważny plik systemowy jest uruchamiany z innej ścieżki niż domyślna (*np. plik "winlogon.exe" jest uruchamiany z folderu innego niż Windows*), system AVG zgłasza tę niezgodność. W niektórych przypadkach wirusy używają nazw standardowych procesów systemowych, aby ich obecność w systemie była trudniejsza do wychwycenia przez użytkownika.

- ***Plik zablokowany*** — raportowany plik jest zablokowany, dlatego nie może zostać przeskanowany przez system AVG. Oznacza to zazwyczaj, że dany plik jest stale używany przez system (*np. plik wymiany*).

10.8. Przechowalnia wirusów



Przechowalnia wirusów to bezpieczne środowisko przeznaczone do zarządzania podejrzanymi/zainfekowanymi obiektami, które zostały wykryte podczas testów przeprowadzanych przez program AVG. Po wykryciu zainfekowanego obiektu podczas skanowania (w przypadku, gdy program AVG nie jest w stanie automatycznie go wyleczyć), użytkownik zostanie poproszony o dokonanie wyboru reakcji na to zagrożenie. Zalecanym rozwiązaniem jest przeniesienie obiektu do ***Przechowalni wirusów***, skąd można będzie podjąć dalsze działanie związane z analizą, wyleczeniem lub usunięciem pliku. Głównym zadaniem ***Przechowalni*** jest przechowywanie wszelkich usuniętych plików przez określony czas, aby możliwe było upewnienie się, że nie były one potrzebne. Jeśli brak pliku powoduje problemy, można go wysłać wraz z pytaniem do analizy lub przywrócić do pierwotnej lokalizacji.

Interfejs ***Przechowalni wirusów*** jest otwierany w nowym oknie i zawiera przegląd informacji o izolowanych, zainfekowanych obiektach:

- ***Zagrożenie*** — jeśli w systemie ***został zainstalowany składnik*** Identity Protection**AVG Anti-Virus 2011**, w tej sekcji wyświetlana będzie graficzna identyfikacja poziomu zagrożenia odpowiednich obiektów — od "nieistotne" (■□□□) do "bardzo niebezpieczne" (■■■■); dostępne będą również informacje na temat typu infekcji (*zgodnie z ich poziomem zainfekowania — wszystkie obiekty na liście mogą być zainfekowane faktycznie lub potencjalnie*).

- ***Nazwa wirusa*** — nazwa wykrytej infekcji pochodząca z ***Encyklopedii wirusów*** (online).

- ***Ścieżka do pliku*** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego pliku.

- ***Pierwotna nazwa obiektu*** — wszystkie wykryte obiekty na liście posiadają standardowe

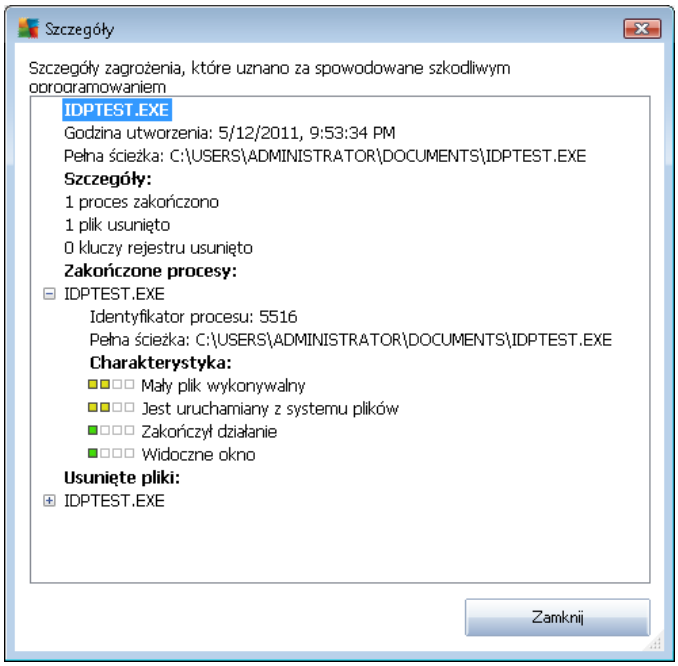
nazwy określane przez program AVG w trakcie skanowania. W przypadku gdy obiekt miał określoną nazwę, która jest znana (*np. nazwa załącznika wiadomości e-mail, która nie odpowiada faktycznej zawartości załącznika*), jest ona podawana w tej kolumnie.

- ***Data zachowania*** — data i godzina wykrycia podejrzanego pliku i przeniesienia go do ***Przechowalni.***

Przyciski kontrolne

Interfejs ***Przechowalni wirusów*** zawiera następujące przyciski kontrolne:

- ***Przywróć*** — przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- ***Przywróć jako*** — przenosi zainfekowany plik do wybranego folderu
- ***Szczegóły*** — ten przycisk może być używany tylko dla zagrożeń wykrytych przez składnik ***Identity Protection***. Jego kliknięcie wyświetla porównawczy przegląd szczegółów zagrożeń (*zainfekowane pliki/procesy, charakterystyka procesów itp.*). Należy zawrócić uwagę na fakt, że dla wszystkich pozycji innych niż wykryte przez składnik IDP ten przycisk pozostanie szary i nieaktywny!



- ***Usuń*** — nieodwracalnie usuwa zainfekowany plik z ***Przechowalni***.
- ***Opróżnij kwarantannę*** — usuwa bezpowrotnie całą zawartość ***kwarantanny***. Usunięcie plików z ***Przechowalni wirusów***oznacza całkowite i nieodwracalne usunięcie ich z dysku (*nie są one przenoszone do kosza*).

11. Aktualizacje AVG

Zapewnienie aktualności programu AVG jest niezbędne, ponieważ tylko w ten sposób wszystkie nowo pojawiające się wirusy będą wykrywane we właściwym czasie.

Aktualizacje systemu AVG nie są publikowane zgodnie z jakimkolwiek harmonogramem — powstają jako reakcja na pojawiające się zagrożenia. Dlatego też zalecamy sprawdzanie dostępności aktualizacji przynajmniej raz dziennie. Tylko w ten sposób można zapewnić ciągłą aktualność systemu **AVG Anti-Virus 2011**.

11.1. Poziomy aktualizacji

Program AVG oferuje dwa poziomy aktualizacji:

- ***Aktualizacja definicji*** zawiera uzupełnienia niezbędne do zapewnienia niezawodnej ochrony antywirusowej. Na ogół nie zawiera modyfikacji programu i aktualizuje tylko bazę definicji. Ta aktualizacja powinna zostać zastosowana, gdy tylko będzie dostępna.

- ***Aktualizacja programu*** zawiera różne zmiany w programie głównym, oraz poprawki i udoskonalenia.

Podczas planowania aktualizacji można wybrać poziom priorytetu aktualizacji, które mają zostać pobrane i zastosowane.

Uwaga: *Jeśli zaplanowane skanowanie i zaplanowana aktualizacja nałożą się, proces aktualizacji będzie miał pierwszeństwo i skanowanie zostanie przerwane.*

11.2. Typy aktualizacji

Można wyróżnić dwa typy aktualizacji:

- ***Aktualizacja na żądanie*** — natychmiastowa aktualizacja oprogramowania AVG, której można dokonać w dowolnym momencie, w razie wystąpienia takiej konieczności.

- ***Aktualizacja zaplanowana*** — system AVG umożliwia przygotowanie harmonogramu aktualizacji. Aktualizacja zaplanowana wykonywana jest zgodnie z zadanym harmonogramem. Gdy dostępne są nowe pliki aktualizacyjne, system AVG pobiera je bezpośrednio z internetu lub katalogu sieciowego. W przypadku braku nowych aktualizacji nie zostają dokonane żadne zmiany.

11.3. Proces aktualizacji

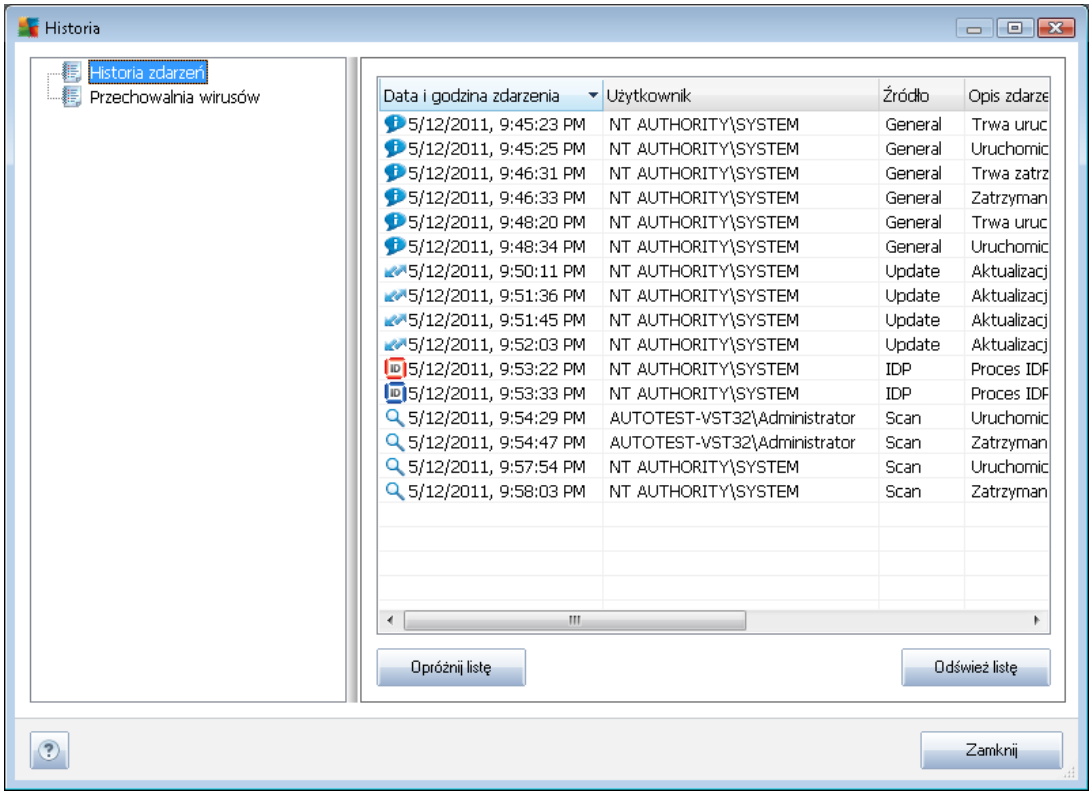
Proces aktualizacji można uruchomić natychmiast, gdy jest ona potrzebna, klikając szybki link ***Aktualizuj teraz***. Link ten jest zawsze dostępny w głównym oknie interfejsu użytkownika AVG. Mimo to, zaleca się regularne aktualizowanie systemu, zgodnie z harmonogramem, który można edytować za pomocą Menedżera aktualizacji.

Po uruchomieniu tego procesu program AVG sprawdza, czy dostępne są nowe pliki aktualizacyjne. Jeśli tak, system pobiera je i uruchamia właściwy proces aktualizacji. W tym czasie otwierany jest interfejs ***Aktualizacja***, w którym można śledzić przedstawiony graficznie postęp aktualizacji oraz przeglądać szereg parametrów (*rozmiar pliku aktualizacji, ilość odebranych danych, szybkość*

pobierania, czas pobierania itd., ...).

***Uwaga**: Przed zaktualizowaniem programu AVG tworzony jest punkt odtwarzania systemu. Przy jego użyciu możliwe będzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Funkcja ta jest dostępna po kolejnym wybraniu opcji: Start / Wszystkie programy / Akcesoria / Narzędzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoświadczonym użytkownikom!*

12. Historia zdarzeń



Dostęp do okna dialogowego ***Historia*** można uzyskać z menu systemowego, za pomocą opcji ***Historia/Dziennik historii zdarzeń***. Okno to zawiera podsumowanie najważniejszych wydarzeń, które wystąpiły w czasie pracy systemu **AVG Anti-Virus 2011**. ***Historia*** zawiera rekordy następujących typów zdarzeń:

- Informacje o aktualizacjach oprogramowania AVG;
- Uruchomienie, zakończenie lub wstrzymanie skanowania (*także automatycznego*);
- Zdarzenia powiązane z wykryciem wirusa (*przez Ochronę rezydentną lub podczas zwykłego skanowania*), wraz ze wskazaniem położenia zainfekowanego pliku;
- Inne ważne zdarzenia.

Dla każdego zdarzenia wyświetlane są następujące informacje:

- ***Data i godzina zdarzenia*** — określa dokładną datę i czas wystąpienia zdarzenia.
- ***Użytkownik*** — określa, kto zainicjował zdarzenie.
- ***Źródło*** — podaje nazwę składnika lub innej części systemu AVG, która wywołała zdarzenie.

- ***Opis zdarzenia*** — przedstawia krótkie podsumowanie zdarzenia.

Przyciski kontrolne

- ***Opróżnij listę*** — powoduje usunięcie wszystkich wpisów z listy zdarzeń.
- ***Odśwież listę*** — powoduje odświeżenie zawartości listy zdarzeń.

13. FAQ i pomoc techniczna

W przypadku jakichkolwiek problemów z oprogramowaniem AVG (w kwestiach handlowych lub technicznych) należy skorzystać z sekcji ***FAQ*** witryny systemu AVG (http://www.avg.com/).

Jeśli pomoc ta okaże się niewystarczająca, zalecamy kontakt z działem pomocy technicznej za pośrednictwem poczty e-mail. Zachęcamy do skorzystania z formularza kontaktowego, dostępnego po wybraniu polecenia menu systemowego ***Pomoc/Uzyskaj pomoc online***.