AVG Anti-Virus 2012

Podręcznik użytkownika

Wersja dokumentu 2012.03 (29.11.2011)

Spis treści

1. Wprowadzenie 6

2. Wymagania instalacyjne AVG 7

2.1 Obsługiwane systemy operacyjne 7
2.2 Minimalne i zalecane wymagania sprzętowe 7

3. Proces instalacji systemu AVG 8

3.1 Witamy 8
3.2 Aktywuj licencję 10
3.3 Wybierz typ instalacji 11
3.4 Opcje niestandardowe 12
3.5 Zainstaluj pasek narzędzi AVG Security Toolbar 13
3.6 Postęp instalacji 14
3.7 Instalacja powiodła się 15

4. Po instalacji 17

4.1 Rejestracja produktu 17
4.2 Dostęp do interfejsu użytkownika 17
4.3 Skanowanie całego komputera 17
4.4 Test EICAR 17
4.5 Konfiguracja domyślna systemu AVG 18

5. Interfejs użytkownika AVG 19

5.1 Menu systemowe 20
5.1.1 Plik 20
5.1.2 Składniki 20
5.1.3 Historia 20
5.1.4 Narzędzia 20
5.1.5 Pomoc 20
5.1.6 Pomoc techniczna 20
5.2 Status bezpieczeństwa 27
5.3 Szybkie linki 28
5.4 Przegląd składników 29
5.5 Ikona na pasku zadań 30
5.6 Gadżet AVG 32

6. Składniki AVG 34

6.1 Anti-Virus 34
6.1.1 Silnik skanujący 34
6.1.2 Ochrona rezydentna 34
6.1.3 Ochrona przed oprogramowaniem szpiegującym 34
6.1.4 Interfejs składnika Anti-Virus 34
6.1.5 Przypadki wykrycia przez Ochronę Rezydentną 34
6.2 LinkScanner 40
6.2.1 Interfejs składnika LinkScanner 40
6.2.2 Zagrożenia wykryte przez funkcję Search-Shield 40
6.2.3 Zagrożenia wykryte przez funkcję Surf-Shield 40
6.2.4 Zagrożenia wykryte przez Ochronę Sieci 40
6.3 Ochrona poczty e-mail 46
6.3.1 Skaner poczty e-mail 46
6.3.2 Anti-Spam 46
6.3.3 Interfejs ochrony poczty e-mail 46
6.3.4 Zagrożenia wykryte przez Skaner poczty e-mail 46
6.4 Anti-Rootkit 50
6.4.1 Interfejs składnika Anti-Rootkit 50
6.5 PC Analyzer 52
6.6 Identity Protection 54
6.6.1 Interfejs składnika AVG Identity Protection 54
6.7 Administracja zdalna 57

7. Moje aplikacje 58

7.1 LiveKive 58
7.2 Bezpieczeństwo rodziny 59
7.3 PC Tuneup 59

8. Pasek narzędzi AVG Security Toolbar 61

9. Zaawansowane ustawienia AVG 63

9.1 Wygląd 63
9.2 Dźwięki 66
9.3 Tymczasowo wyłącz ochronę AVG 67
9.4 Anti-Virus 68
9.4.1 Ochrona rezydentna 68
9.4.2 Serwer pamięci podręcznej 68
9.5 Ochrona poczty e-mail 74
9.5.1 Skaner poczty 74

9.6 LinkScanner 83
9.6.1 Ustawienia LinkScannera 83
9.6.2 Ochrona Sieci 83
9.7 Skany 86
9.7.1 Skan całego komputera 86
9.7.2 Skan rozszerzenia powłoki 86
9.7.3 Skan określonych plików lub folderów 86
9.7.4 Skanowanie urządzeń wymiennych 86
9.8 Zaplanowane zadania 92
9.8.1 Skan zaplanowany 92
9.8.2 Harmonogram aktualizacji definicji 92
9.8.3 Harmonogram aktualizacji programu 92
9.9 Aktualizacja 102
9.9.1 Proxy 102
9.9.2 Połączenie telefoniczne 102
9.9.3 URL 102
9.9.4 Zarządzaj 102
9.10 Anti-Rootkit 109
9.10.1 Wyjątki 109
9.11 AVG Identity Protection 110
9.11.1 Ustawienia składnika Identity Protection 110
9.11.2 Lista dozwolonych 110
9.12 Potencjalnie niechciane programy 114
9.13 Przechowalnia wirusów 117
9.14 Program udoskonalania produktów 117
9.15 Ignoruj błędny status 120
9.16 Administracja zdalna 121

10. Skanowanie AVG 123

10.1 Interfejs skanowania 123
10.2 Wstępnie zdefiniowane testy 124
10.2.1 Skan całego komputera 124
10.2.2 Skan określonych plików lub folderów 124
10.2.3 Skan Anti-Rootkit 124
10.3 Skan z poziomu eksploratora systemu Windows 134
10.4 Skan z poziomu wiersza poleceń 135
10.4.1 Parametry skanowania z wiersza poleceń 135
10.5 Planowanie skanowania 137

10.5.1 Ustawienia harmonogramu *137*
10.5.2 Jak skanować? *137*
10.5.3 Co skanować? *137*
10.6 Przegląd wyników skanowania 147
10.7 Szczegóły wyników skanowania 148
10.7.1 Karta Przegląd wyników *148*
10.7.2 Karta Infekcje *148*
10.7.3 Karta Oprogramowanie szpiegujące *148*
10.7.4 Karta Ostrzeżenia *148*
10.7.5 Karta Rootkity *148*
10.7.6 Karta Informacje *148*
10.8 Przechowalnia wirusów 155

11. Aktualizacje AVG 158

11.1 Uruchomienie aktualizacji 158
11.2 Postęp aktualizacji 158
11.3 Poziomy aktualizacji 159

12. Dziennik historii 160

13. FAQ i pomoc techniczna 162

1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację systemu **AVG Anti-Virus 2012**.

AVG Anti-Virus 2012 zapewnia ochronę w czasie rzeczywistym przed najbardziej zaawansowanymi współczesnymi zagrożeniami. Bezpiecznie korzystaj z czatów, pobieraj i wymieniaj pliki bez ryzyka oraz graj i oglądaj filmy w spokoju:

- Bezpiecznie pobieraj i udostępniaj pliki oraz wysyłaj wiadomości dzięki składnikowi Ochrona Sieci AVG™
- Bezpieczeństwo w sieciach społecznościowych dzięki Ochronie sieci społecznościowych AVG
- Przeglądanie i przeszukiwanie stron internetowych bez ryzyka dzięki ochronie w czasie rzeczywistym zapewnianej przez składnik LinkScanner®

2. Wymagania instalacyjne AVG

2.1. Obsługiwane systemy operacyjne

System **AVG Anti-Virus 2012** 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 2012, ale bez składnika Identity Protection.*

2.2. Minimalne i zalecane wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG Anti-Virus 2012**:

- Procesor Intel Pentium 1,5 GHz
- 512 MB pamięci RAM.
- 950 MB wolnego miejsca na dysku (na potrzeby instalacji)

Zalecane wymagania sprzętowe dla systemu **AVG Anti-Virus 2012**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB pamięci RAM.
- 1350 MB wolnego miejsca na dysku (na potrzeby instalacji)

3. Proces instalacji systemu AVG

Skąd pobrać plik instalacyjny

Do zainstalowania systemu **AVG Anti-Virus 2012** na komputerze konieczny jest najnowszy plik instalacyjny. Aby upewnić się, że instalujesz najnowszą dostępną wersję **AVG Anti-Virus 2012**, zalecamy pobranie pliku instalacyjnego bezpośrednio z witryny AVG (http://www.avg.com/). Sekcja ***Centrum Pomocy technicznej / Pobierz*** zawiera pełen zestaw plików instalacyjnych dla wszystkich edycji AVG.

Jeśli nie jesteś pewien, którego pliku potrzebujesz, użyj funkcji ***Wybierz produkt*** znajdującej się u dołu strony. Po udzieleniu odpowiedzi na trzy proste pytania, dowiesz się, czego dokładnie szukasz. Kliknij przycisk ***Kontynuuj***, aby przejść do listy potrzebnych Ci plików.

Jak przebiega proces instalacji?

Po pobraniu i zapisaniu instalatora na dysku, można uruchomić proces instalacji. Instalacja składa się z kilku łatwych w zrozumieniu ekranów. Każdy z nich opisuje krótko, czego dotyczy. Poniżej znajdują się ich szczegółowe opisy:

3.1. Witamy

Proces instalacji rozpoczyna okno ***Witamy w instalatorze AVG:***

Wybierz język instalacji

W tym oknie możesz wybrać język, który ma być używany podczas instalacji. W prawej części okno znajduje się menu z dostępnymi językami. Wybierz żądany język, a proces instalacji będzie w

nim kontynuowany.

Uwaga: W tym momencie wybierany jest jedynie język instalatora. System AVG Anti-Virus 2012 zostanie zainstalowany z obsługą wskazanego języka (oraz dodatkowo języka angielskiego, który dostępny jest domyślnie). Możliwa jest jednak instalacja dodatkowych języków i używanie systemu AVG Anti-Virus 2012 w dowolnym z nich. Jeden z kolejnych ekranów - Opcje niestandardowe - pozwala na wybór zestawu alternatywnych języków.

Umowa licencyjna

Ekran ***Witamy w instalatorze AVG*** wyświetla również pełną 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.

Polityka prywatności AVG

Oprócz umowy licencyjnej możliwe jest również przejrzenie treści polityki prywatności firmy AVG. W lewym dolnym rogu tego okna znajduje się link ***Polityka prywatności AVG***. Kliknięcie go przeniesie Cię na stronę AVG (http://www.avg.com/), zawierającą pełen tekst polityki prywatności AVG.

Przyciski kontrolne

W pierwszym oknie instalatora dostępne są tylko dwa przyciski:

- ***Akceptuj*** - potwierdza przeczytanie, zrozumienie i akceptację postanowień umowy licencyjnej. Instalacja będzie kontynuowana.
- ***Odrzuć*** - powoduje odrzucenie umowy licencyjnej. Instalacje zostanie natychmiast zakończona. System **AVG Anti-Virus 2012** nie będzie zainstalowany!

3.2. Aktywuj licencję

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

Gdzie znaleźć numer licencji

Numer sprzedaży można znaleźć na opakowaniu dysku CD z oprogramowaniem **AVG Anti-Virus 2012**. Numer licencji jest wysyłany za pośrednictwem poczty e-mail po dokonaniu zakupu oprogramowania **AVG Anti-Virus 2012** 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.

Jak użyć metody Kopiuj/Wklej

Użycie metody ***Kopiuj/Wklej*** przy wpisywaniu numeru licencji systemu **AVG Anti-Virus 2012** pozwala uniknąć błędów przy tradycyjnym przepisywaniu. Wykonaj następujące kroki:

- Otwórz wiadomość e-mail zawierającą Twój numer licencji.
- Przytrzymaj wciśnięty lewy przycisk myszy, przeciągając go od początku do końca numeru licencji. Numer powinien zostać podświetlony.
- Przytrzymaj ***Ctrl*** i naciśnij klawisz ***C***. Spowoduje to skopiowanie numeru.
- Umieść kursor w miejscu, w którym chcesz wkleić skopiowany tekst.
- Przytrzymaj ***Ctrl*** i naciśnij klawisz ***V***. Spowoduje to wklejenie numeru w żądanym polu.

Przyciski kontrolne

Tak jak w przypadku wielu okien instalatora, dostępne są trzy przyciski kontrolne:

- ***Wstecz*** - powoduje powrót do poprzedniego okna dialogowego.
- ***Dalej*** - kontynuuje instalację, przechodząc do kolejnego kroku.
- ***Anuluj*** - kończy natychmiastowo proces instalacji; System **AVG Anti-Virus 2012** nie zostanie zainstalowany!

3.3. Wybierz typ instalacji

Typy 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 Anti-Virus 2012** w sposób całkowicie zautomatyzowany, z ustawieniami wstępnie zdefiniowanymi przez dostawcę oprogramowania. Taka konfiguracja zapewnia maksymalne bezpieczeństwo oraz optymalne wykorzystanie zasobów. Jeśli w przyszłości zajdzie potrzeba zmiany konfiguracji, można będzie to zrobić bezpośrednio z poziomu aplikacji **AVG Anti-Virus 2012**. 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 Anti-Virus 2012** 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.

Instalacja gadżetu AVG

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 2012**, tj. skanowania i aktualizacji.

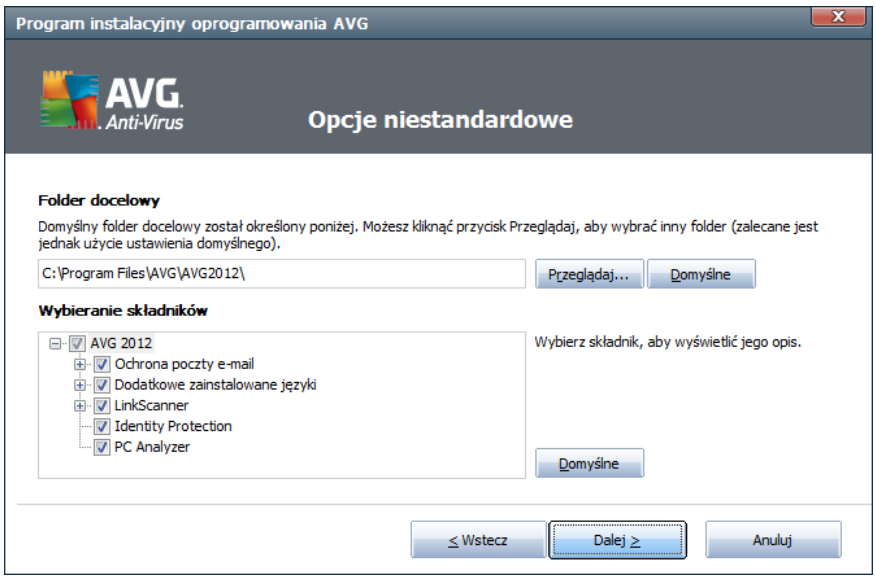
Przyciski kontrolne

Tak jak w przypadku wielu okien instalatora, dostępne są trzy przyciski kontrolne:

- ***Wstecz*** - powoduje powrót do poprzedniego okna dialogowego.
- ***Dalej*** - kontynuuje instalację, przechodząc do kolejnego kroku.
- ***Anuluj*** - kończy natychmiastowo proces instalacji; System **AVG Anti-Virus 2012** nie zostanie zainstalowany!

3.4. 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 2012**. Domyślnie system **AVG Anti-Virus 2012** zostanie zainstalowany 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 2012**. 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***.

Przyciski kontrolne

Tak jak w przypadku wielu okien instalatora, dostępne są trzy przyciski kontrolne:

- ***Wstecz*** - powoduje powrót do poprzedniego okna dialogowego.
- ***Dalej*** - kontynuuje instalację, przechodząc do kolejnego kroku.
- ***Anuluj*** - kończy natychmiastowo proces instalacji; System **AVG Anti-Virus 2012** nie zostanie zainstalowany!

3.5. Zainstaluj pasek narzędzi AVG Security Toolbar

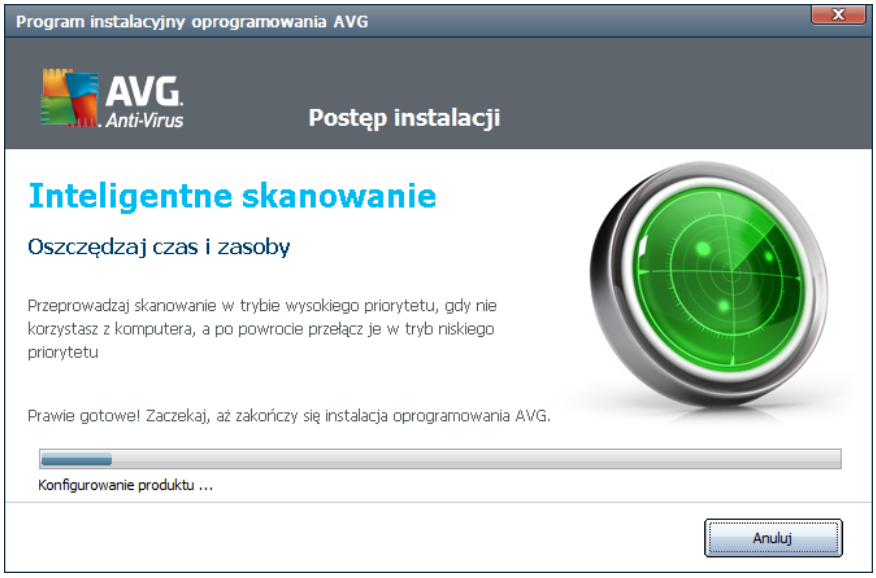
W oknie dialogowym ***Instalowanie paska narzędzi AVG Security Toolbar*** można zadecydować, czy ma zostać zainstalowany pasek narzędzi AVG Security Toolbar. Jeśli domyślne ustawienia nie zostaną zmienione, składnik ten zostanie automatycznie zainstalowany w przeglądarce internetowej

(*obecnie obsługiwane przeglądarki to Microsoft Internet Explorer w wersji 6.0 lub nowszej i Mozilla Firefox w wersji 3.0 lub nowszej*), aby zapewnić Ci 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.

3.6. Postęp instalacji

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



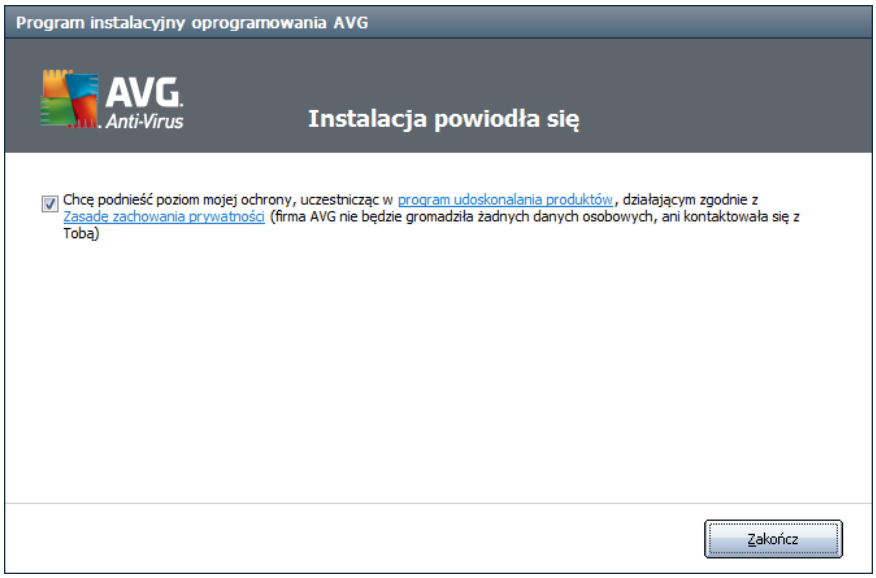
Po zakończeniu instalacji nastąpi przekierowanie do następnego okna dialogowego.

Przyciski kontrolne

W tym oknie dostępny jest tylko jeden przycisk - ***Anuluj***. Powinien być używany tylko w przypadku konieczności zatrzymania procesu instalacji. Prosimy pamiętać, że wówczas system **AVG Anti-Virus 2012** nie zostanie zainstalowany!

3.7. Instalacja powiodła się

Wyświetlenie okna dialogowego ***Instalacja powiodła się*** potwierdza, że system **AVG Anti-Virus 2012** został w pełni zainstalowany i skonfigurowany:



Program udoskonalania produktów

To okno pozwala zdecydować, czy chcesz brać udział w Programie udoskonalania produktów (*Szczegóły znajdują się w rozdziale Zaawansowane ustawienia AVG / Program udoskonalania produktów AVG*), który pozwala nam zbierać anonimowe informacje o wykrytych zagrożeniach, podnosząc dzięki temu ogólny poziom bezpieczeństwa w internecie. Jeśli zgadzasz się na warunki programu, pozostaw pole ***Wyrażam zgodę na uczestnictwo w Programie udoskonalania produktów...*** zaznaczone *(wartość domyślna)*.

Instalacja licencji biznesowych

Jeśli posiadasz biznesową licencję AVG, a w jednym z poprzednich okien zdecydowałeś się na instalację Administracji zdalnej *(patrz rozdział Opcje niestandardowe)*, końcowy ekran instalacji będzie miał następujący interfejs:

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/).

zapoznaj się z rozdziałem Przegląd składników. Aby przywrócić domyślną konfigurację wstępnie ustawioną przez dostawcę oprogramowania, należy użyć przycisku ***Domyślne***.

Przyciski kontrolne

W tym oknie dostępne są następujące przyciski kontrolne:

- ***Zakończ*** - Kliknij ten przycisk, by zakończyć proces instalacji i w pełni cieszyć się ochroną **AVG Anti-Virus 2012**.

4. Po instalacji

4.1. Rejestracja produktu

Po ukończeniu instalacji **AVG Anti-Virus 2012** zalecamy rejestrację naszego produktu na stronie internetowej AVG (http://www.avg.com/). Rejestracja umożliwia pełny dostęp do konta użytkownika AVG, biuletynu aktualizacji AVG i innych usług oferowanych wyłącznie zarejestrowanym klientom.

Na stronę rejestracji najprościej jest przejść z poziomu interfejsu użytkownika systemu **AVG Anti-Virus 2012**. Wystarczy w tym celu wybrać z głównego menu Pomoc / Zarejestruj teraz. Zostaniesz wówczas przeniesiony na stronę ***Rejestracja*** (http://www.avg.com/). Tam znajdziesz dalsze wskazówki.

4.2. 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 2012/Interfejs użytkownika AVG,***

4.3. Skanowanie całego komputera

Istnieje pewne ryzyko, że wirus dostał się do komputera przed zainstalowaniem systemu **AVG Anti-Virus 2012**. Z tego powodu należy uruchomić test Skan całego komputera, aby upewnić się, że jest on w pełni bezpieczny.

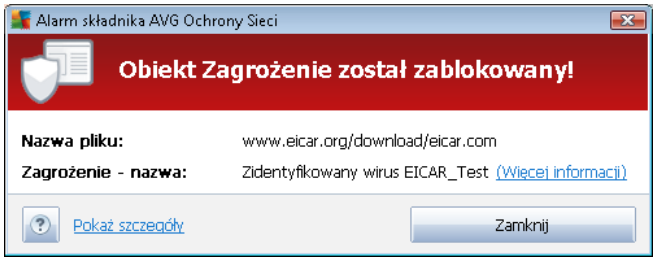
Instrukcje dotyczące uruchamiania testu Skan całego komputera zawiera rozdział Skanowanie AVG .

4.4. Test EICAR

Aby potwierdzić, że system **AVG Anti-Virus 2012** 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, Ochrona Sieci (*działająca w ramach składnika Link Scanner*) 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 (*część technologii Anti-Virus*) wykryje go już w chwili rozpakowywania.

Jeśli system AVG nie rozpozna pliku testowego EICAR jako wirusa, należy ponownie sprawdzić jego konfigurację!

4.5. Konfiguracja domyślna systemu AVG

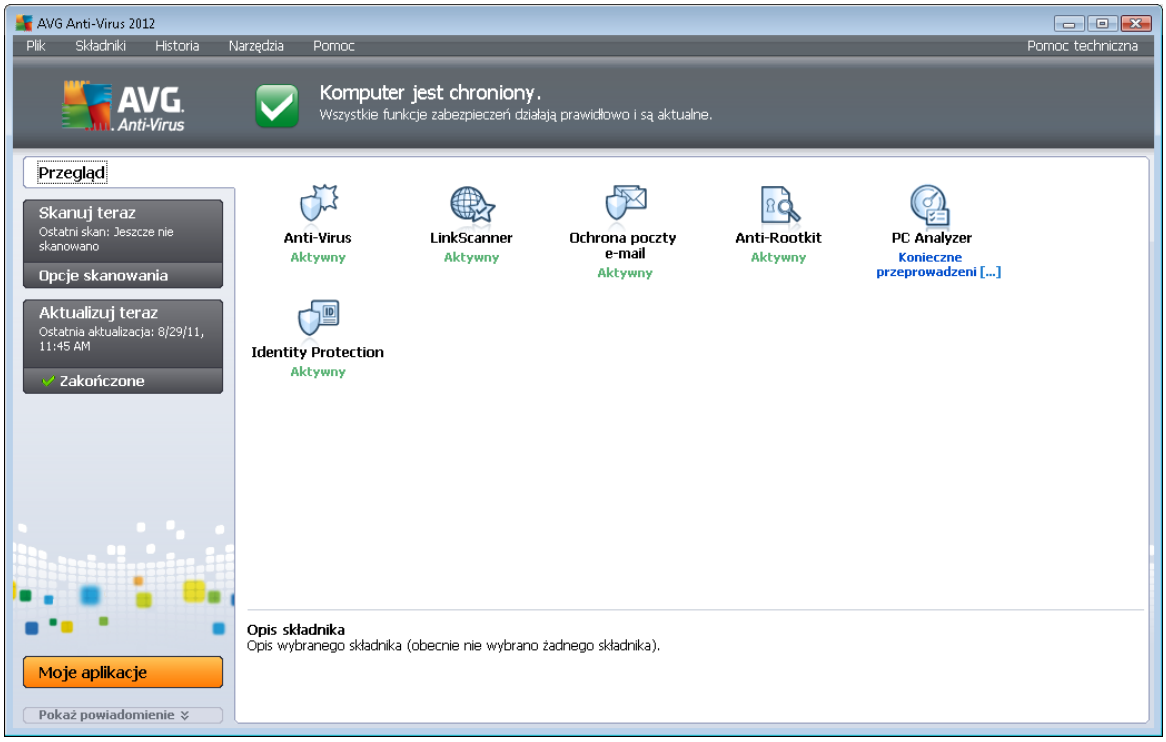
Konfiguracja domyślna (*ustawienia stosowane zaraz po instalacji*) systemu **AVG Anti-Virus 2012** jest wstępnie definiowana przez producenta i ma na celu zapewnienie optymalnej wydajności wszystkich składników oraz funkcji.

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.

5. Interfejs użytkownika AVG

Otwarcie systemu **AVG Anti-Virus 2012** powoduje wyświetlenie jego okna głównego:



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 Anti-Virus 2012** - szczegóły >>
- ***Informacje o stanie bezpieczeństwa*** *(prawa część górnej sekcji okna)* zawiera informacje dotyczące bieżącego stanu systemu **AVG Anti-Virus 2012** - szczegóły >>
- ***Szybkie linki*** *(lewa kolumna)* umożliwiają uzyskanie szybkiego dostępu najważniejszych i najczęściej używanych funkcji systemu **AVG Anti-Virus 2012** - szczegóły >>
- ***Moje aplikacje*** *(lewa dolna sekcja okna)* otwiera przegląd dodatkowych aplikacji przeznaczonych dla **AVG Anti-Virus 2012**: LiveKive, Bezpieczeństwo rodziny i PC Tuneup
- ***Przegląd składników*** *(centralna część okna)* zawiera przegląd zainstalowanych komponentów **AVG Anti-Virus 2012** - szczegóły >>
- ***Ikona na pasku zadań*** *(prawy dolny róg ekranu, na pasku systemowym)* sygnalizuje bieżący stan systemu **AVG Anti-Virus 2012** - szczegóły >>
- ***Gadżet AVG*** *(pasek boczny obsługiwany w systemach Windows Vista i Windows 7)* umożliwia szybki dostęp do funkcji skanowania i aktualizacji **AVG Anti-Virus 2012** - szczegóły >>

5.1. 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 2012**. Menu systemowe zapewnia dostęp do poszczególnych składników AVG, funkcji i usług.

Menu systemowe jest podzielone na pięć sekcji:

5.1.1. Plik

- ***Zakończ*** - powoduje zamknięcie **AVG Anti-Virus 2012**interfejsu użytkownika. System AVG działa jednak w tle, a komputer jest nadal chroniony!

5.1.2. 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 dialogowego interfejsu użytkownika systemu AVG, zawierającego przegląd zainstalowanych składników i informacje o ich stanie.
- ***Anti-Virus*** wykrywa wirusy, oprogramowanie szpiegujące, robaki internetowe, konie trojańskie, podejrzane pliki wykonywalne i biblioteki, a także chroni przed niebezpiecznymi programami reklamowymi - szczegóły >>
- ***Link Scanner*** chroni Cię przed zagrożeniami internetowymi w czasie gdy przeglądasz strony WWW - szczegóły >>
- ***Ochrona poczty e-mail*** sprawdza przychodzące wiadomości e-mail w poszukiwaniu spamu, wirusów, prób phishingu i innych zagrożeń - szczegóły >>
- ***Anti-Rootkit*** skanuje system w poszukiwaniu groźnych rootkitów, ukrytych pod postacią aplikacji, sterowników i bibliotek - szczegóły >>
- ***PC Analyzer*** - analizuje stan komputera - szczegóły >>
- ***Identity Protection*** chroni Twoje dane przed nieznanymi jeszcze zagrożeniami - 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.

5.1.3. 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 zawierające przegląd załączników uznanych przez Ochronę poczty e-mail za niebezpieczne
- Zagrożenia wykryte przez Ochronę Sieci - otwiera okno zawierające przegląd zagrożeń wykrytych przez Ochronę Sieci (część technologii LinkScanner)
- 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 2012akcji** .

5.1.4. 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 2012**.
- ***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 2012. Na ogół zaleca się zachowanie domyślnych ustawień zdefiniowanych przez producenta oprogramowania AVG.

5.1.5. 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.

- ***AVG - Twoje WWW*** - powoduje otwarcie strony internetowej AVG (http://www.avg.com/)

- ***Informacje o wirusach i zagrożeniach*** - otwiera Encyklopedię Wirusów online, w której znaleźć można szczegółowe informacje na temat znanych wirusów.

- ***Aktywuj ponownie*** - otwiera okno ***Aktywacja programu AVG*** zawierające dane wprowadzone na etapie personalizacji 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*** - jest linkiem do strony rejestracyjnej AVG (http://www.avg.com/). Należy tam podać 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 2012, ostatnie dwie pozycje to* ***Kup teraz*** *i* ***Aktywuj***. *Umożliwiają one uaktualnienie programu do jego pełnej wersji. W przypadku systemu* **AVG Anti-Virus 2012** *zainstalowanego z numerem sprzedaży, te pozycje to* ***Zarejestruj*** *i* ***Aktywuj***.

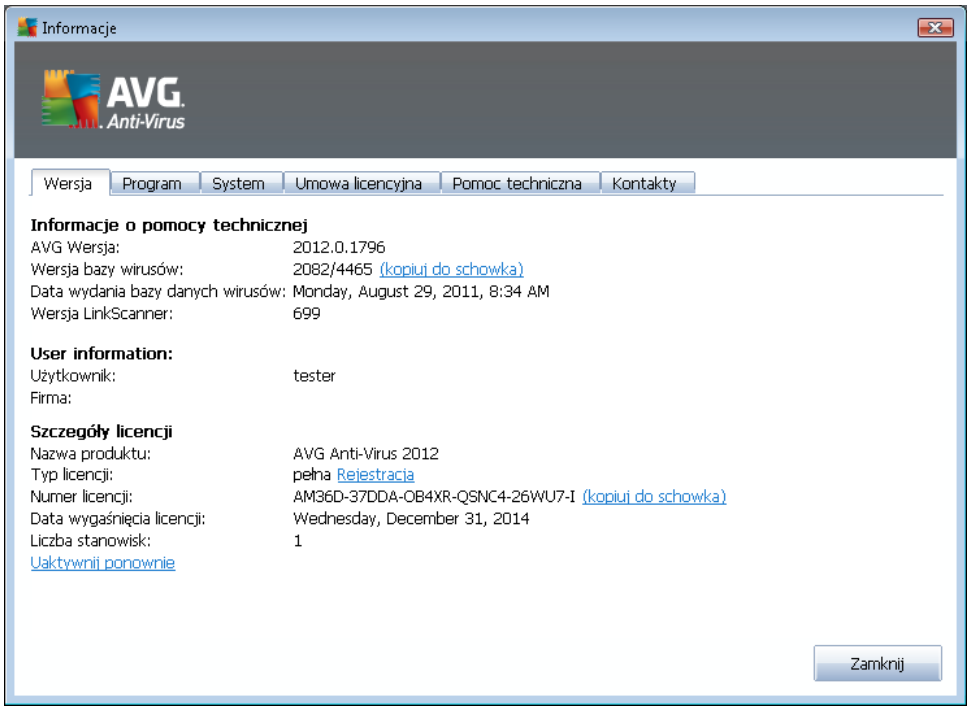
- ***AVG - informacje*** - otwiera okno dialogowe ***Informacje***. Okno to składa się z pięciu kart zawierających informacje na temat nazwy programu, wersji silnika antywirusowego i jego bazy danych, systemu, umowy licencyjnej oraz danych kontaktowych firmy ***AVG Technologies CZ***.

5.1.6. Pomoc techniczna

Link ***Pomoc techniczna*** otwiera nowe okno ***Informacje***, które zawiera szczegóły pomocne przy poszukiwaniu pomocy. Okno to wyświetla podstawowe informacje o zainstalowanym systemie AVG (*wersja programu i bazy danych*) oraz posiadanej licencji, a także zestaw przydatnych linków pomocy technicznej.

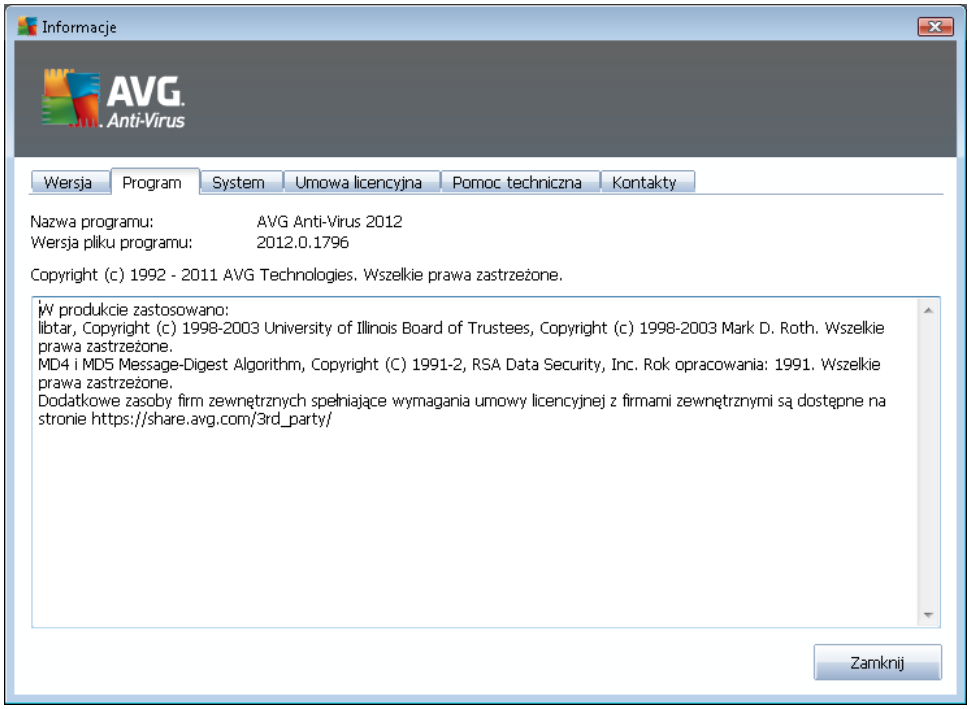
Okno ***Informacje*** podzielone jest na sześć kart:

Karta ***Wersja*** podzielona jest na trzy obszary:

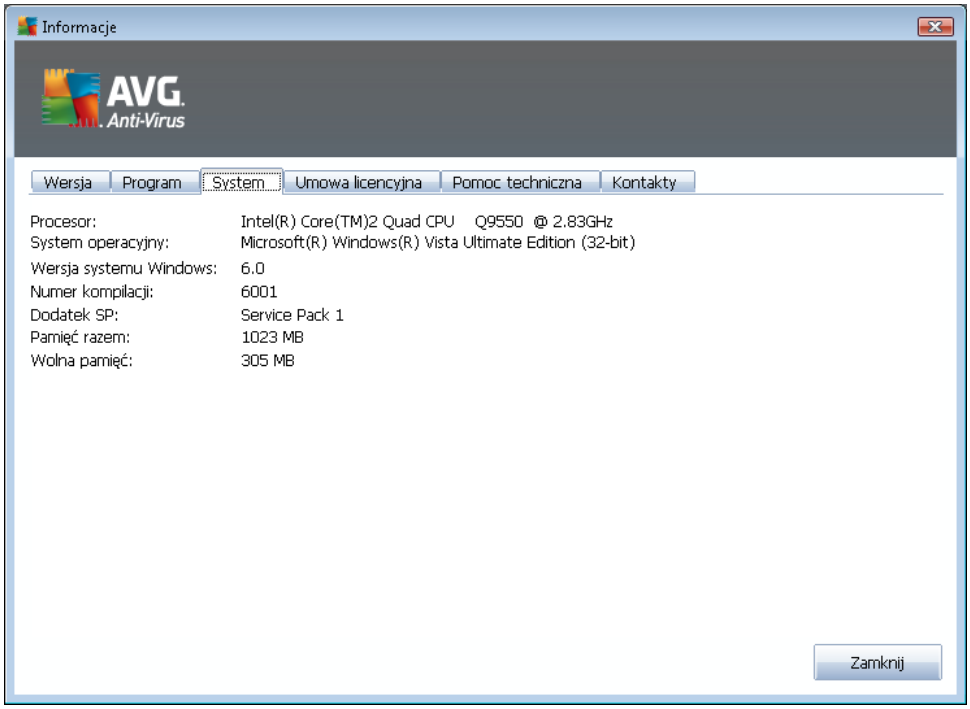


- ***Informacje o pomocy technicznej*** - Dostarcza informacji o wersjach: systemu **AVG Anti-Virus 2012**, bazy wirusów, bazy danych składnika Anti-Spam oraz składnika LinkScanner.
- ***Informacje o użytkowniku*** - Zawiera dane zarejestrowanego użytkownika i firmy.
- ***Szczegóły licencji*** - Podaje informacje o posiadanej licencji *(nazwę produktu, typ licencji, jej numer i datę wygaśnięcia oraz ilość stanowisk*). W tej samej sekcji znajduje się również link ***Rejestracja***, który pozwala zarejestrować produkt **AVG Anti-Virus 2012** w trybie online; Rejestracja daje możliwość pełnego korzystania z Pomocy technicznej AVG. Link ***Uaktywnij ponownie*** otwiera okno ***Aktywuj AVG***: wprowadzenie w nim nowego numeru licencji umożliwia zastąpienie numeru handlowego *(używanego podczas instalacji AVG Anti-Virus 2012)*, lub zmianę licencji *(np. przy uaktualnieniu do bogatszej wersji systemu AVG).*

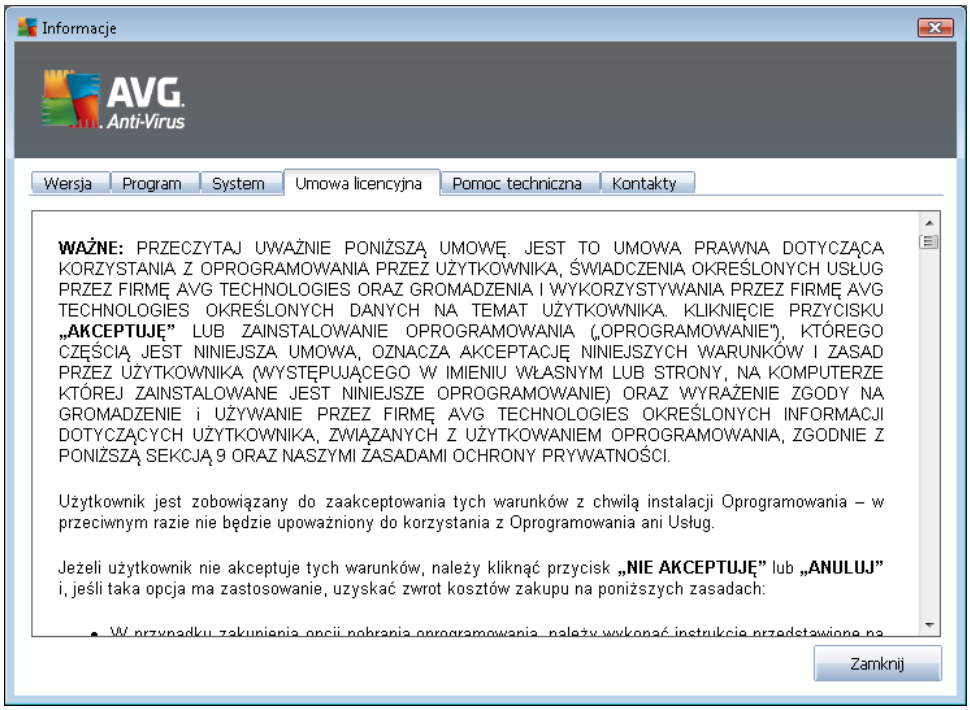
Na karcie ***Program*** możesz znaleźć informacje o wersji programu **AVG Anti-Virus 2012** oraz o użytych bibliotekach innych producentów:



Karta ***System*** wyświetla listę parametrów Twojego systemu *(typ procesora, wersja systemu operacyjnego, numer wydania, zainstalowane dodatki Service Pack, rozmiar całkowitej i dostępnej pamięci)*:

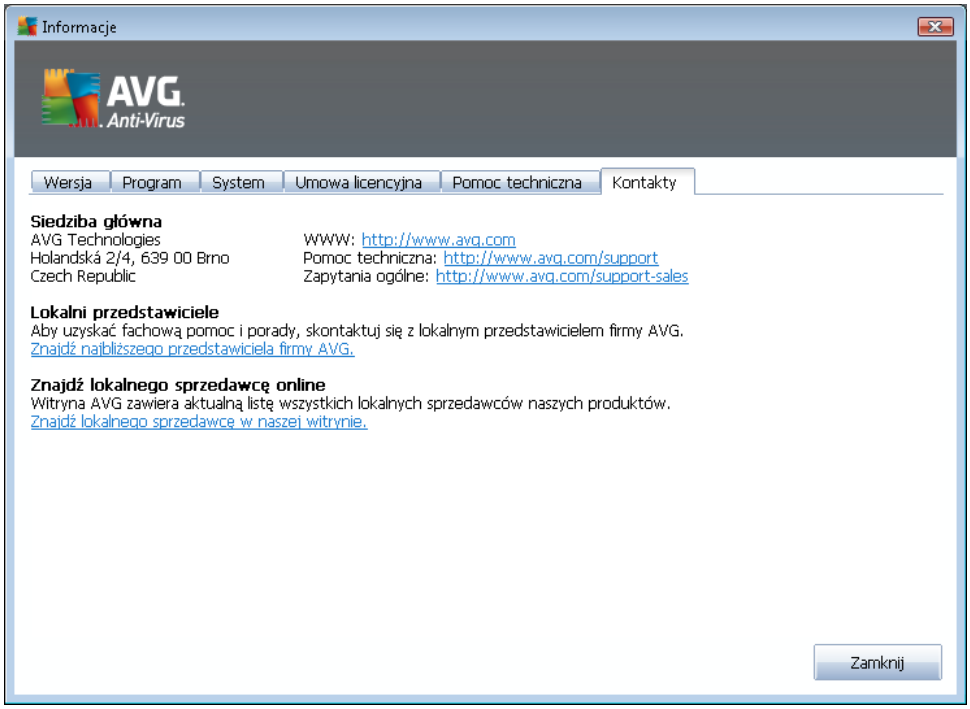


Karta ***Umowa licencyjna*** zawiera pełną treść umowy licencyjnej zawartej z firmą AVG Technologies:



Karta ***Pomoc techniczna*** przedstawia użytkownikowi wszystkie sposoby kontaktu z zespołem Pomocy technicznej AVG. Wyświetla także linki do witryny AVG (http://www.avg.com/), forum i FAQ. Niżej znajdują się również informacje przydatne przy uzyskiwaniu pomocy:

Karta ***Kontakt*** zawiera listę kontaktów do firmy AVG Technologies oraz jej lokalnych przedstawicieli i resellerów:



5.2. Status bezpieczeństwa

Obszar ***Informacje o stanie bezpieczeństwa*** znajduje się w górnej części głównego okna **AVG Anti-Virus 2012**. Znajdziesz tam informacje o bieżącym stanie bezpieczeństwa systemu **AVG Anti-Virus 2012**. W obszarze tym mogą być wyświetlane następujące ikony:

- Zielona ikona wskazuje, że system ***AVG Anti-Virus 2012 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 Anti-Virus 2012** nie wystąpił jednak żaden błąd krytyczny, a użytkownik prawdopodobnie wyłączył z jakiegoś powodu jeden lub więcej składników. Wciąż jesteś chroniony!. należy jednak sprawdzić ustawienia składnika, który zgłasza problem. Jego nazwa jest wyświetlana w sekcji ***Informacje o stanie bezpieczeństwa***.

Pomarańczowa ikona pojawia się również wtedy, gdy z jakiegoś powodu zdecydowałeś się ignorować błędny stan któregoś ze składników. Opcja ***ignorowania stanu składnika*** dostępna jest po wywołaniu menu kontekstowego (*za pomocą prawego przycisku myszy*) nad

ikoną odpowiedniego składnika w przeglądzie składników systemu **AVG Anti-Virus 2012**. Zaznaczając tę opcję potwierdzasz, że zdajesz sobie sprawę z błędnego stanu składnika, ale z pewnych powodów chcesz pozostawić system **AVG Anti-Virus 2012** w tym stanie, bez powiadomień wyświetlanych przez ikonę na pasku zadań. W pewnych sytuacjach użycie tej opcji może być pomocne, jednak nie należy jej nadużywać.

 - Czerwona ikona wskazuje na krytyczny stan systemu ***AVG Anti-Virus 2012***! Co najmniej jeden składnik nie działa poprawnie, a system **AVG Anti-Virus 2012** nie może chronić Twojego komputera. Należy natychmiast usunąć zgłoszony problem. Jeśli nie jest to możliwe, należy skontaktować się z zespołem Pomocy technicznej AVG.

Jeżeli system AVG Anti-Virus 2012 wykryje, że nie działa z optymalną wydajnością, obok informacji o stanie pojawi się przycisk "Napraw" (lub "Napraw wszystkie", jeśli problem dotyczy kilku składników). Kliknięcie tego przycisku spowoduje uruchomienie automatycznego procesu sprawdzenia konfiguracji programu. Jest to prosty sposób na osiągnięcie optymalnej wydajności systemu AVG Anti-Virus 2012 oraz maksymalnego poziomu bezpieczeństwa.

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

Uwaga: *Informacje o stanie systemu AVG Anti-Virus 2012 można również uzyskać w dowolnym momencie z poziomu ikony na pasku zadań.*

5.3. Szybkie linki

Szybkie linki znajdują się po lewej stronie interfejsu użytkownika **AVG Anti-Virus 2012**. Pozwalają one uzyskać natychmiastowy dostęp do najważniejszych i najczęściej używanych funkcji aplikacji, czyli skanowania i aktualizacji. Szybkie linki dostępne są z poziomu dowolnego okna interfejsu:

Szybkie linki podzielone są na trzy sekcje:

- ***Przegląd*** - Użyj tego linku, aby z dowolnego okna AVG przejść natychmiast do przeglądu wszystkich zainstalowanych składników. *(Szczegóły można znaleźć w rozdziale Przegląd składników)*

- ***Skanuj teraz*** - Domyślnie przycisk ten wyświetla informację o ostatnio przeprowadzonym teście *(np. typ skanu, data uruchomienia)*. Kliknij ***Skanuj teraz***, aby ponownie rozpocząć ten sam test. Jeśli chcesz uruchomić inny skan, kliknij link ***Opcje skanowania***. Otworzysz

w ten sposób Interfejs skanera AVG, który pozwala uruchamiać, planować i edytować testy. *(Szczegóły można znaleźć w rozdziale Skanowanie AVG)*

- ***Aktualizuj teraz*** - Link ten wyświetla datę i czas uruchomienia ostatniej aktualizacji. Możesz użyć tego przycisku, aby natychmiast uruchomić proces aktualizacji. *(Szczegóły można znaleźć w rozdziale Aktualizacje AVG)*

Szybkie linki są zawsze widoczne w Interfejsie użytkownika AVG. Kliknięcie jednego z nich w celu uruchomienia określonego procesu powoduje wyświetlenie innego okna dialogowego, ale sama sekcja linków nie ulegnie zmianie. Ponadto, postęp każdego uruchomionego procesu widoczny jest w sekcji nawigacyjnej **AVG Anti-Virus 2012**, abyś miał nad nim pełną kontrolę.

5.4. Przegląd składników

Sekcja Przegląd składników

Obszar ***Przeglądu składników*** znajduje się w centralnej części interfejsu użytkownika systemu **AVG Anti-Virus 2012** . Obszar ten podzielony jest na dwie części:

- ***Przegląd wszystkich zainstalowanych składników*** składający się z paneli reprezentujących poszczególne składniki. Każdy panel posiada ikonę odpowiedniego składnika oraz informację, czy jest on w danym momencie aktywny.
- ***Opis składnika*** widoczny jest w dolnej części okna. Wyjaśnia on w kilku słowach podstawowe funkcje składnika. Podaje również informacje o jego bieżącym stanie.

Lista zainstalowanych składników

Sekcja **Przegląd składników** systemu ***AVG Anti-Virus 2012*** zawiera informacje o następujących składnikach:

- ***Anti-Virus*** wykrywa wirusy, oprogramowanie szpiegujące, robaki internetowe, konie trojańskie, podejrzane pliki wykonywalne i biblioteki, a także chroni przed niebezpiecznymi programami reklamowymi - szczegóły >>
- ***Link Scanner*** chroni Cię przed zagrożeniami internetowymi w czasie gdy przeglądasz strony WWW - szczegóły >>
- ***Ochrona poczty e-mail*** sprawdza przychodzące wiadomości e-mail w poszukiwaniu spamu, wirusów, prób phishingu i innych zagrożeń - szczegóły >>
- ***Anti-Rootkit*** skanuje system w poszukiwaniu groźnych rootkitów, ukrytych pod postacią aplikacji, sterowników i bibliotek - szczegóły >>
- ***PC Analyzer*** - analizuje stan komputera - szczegóły >>
- ***Identity Protection*** chroni Twoje dane przed nieznanymi jeszcze zagrożeniami - szczegóły

>>

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

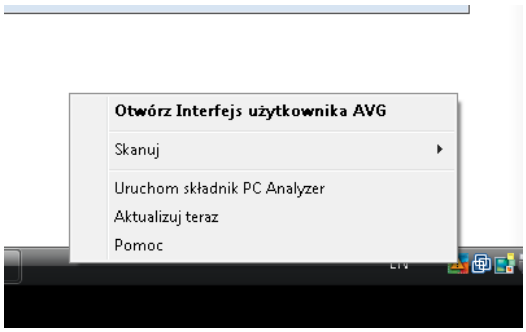
- ***Administracja zdalna*** - składnik wyświetlany tylko w edycjach biznesowych systemu AVG, o ile został wybrany podczas instalacji.

Dostępne akcje

- ***Umieść kursor nad ikoną dowolnego składnika***, aby go zaznaczyć. W dolnej części interfejsu użytkownika zostanie wówczas wyświetlony opis jego podstawowych funkcji.
- ***Pojedyncze kliknięcie ikony składnika*** spowoduje przejście do jego interfejsu, zawierającego szereg statystyk.
- ***Kliknięcie ikony składnika prawym przyciskiem*** otworzy menu kontekstowe z następującymi opcjami:
  - ***Otwórz*** - Otwiera interfejs konkretnego składnika *(podobnie jak w przypadku pojedynczego kliknięcia jego ikony)*.
  - ***Ignoruj stan tego składnika*** - Zaznaczając tę opcję potwierdzasz, że błędny stan składnika jest Ci znany, lecz z pewnych powodów chcesz pozostawić system AVG w tym stanie, bez powiadomień wyświetlanych przez ikonę na pasku zadań.
  - ***Otwórz ustawienia zaawansowane ...*** - Ta opcja dostępna jest tylko przy niektórych składnikach - tych, które posiadają ustawienia zaawansowane.

5.5. Ikona na pasku zadań

Ikona AVG *(na pasku zadań systemu Windows, w prawym dolnym rogu ekranu)* wyświetla bieżący stan systemu **AVG Anti-Virus 2012**. Ikona ta jest zawsze widoczna, niezależnie od tego, czy Interfejs użytkownika **AVG Anti-Virus 2012** jest otwarty czy zamknięty:



Ikona AVG na pasku zadań

- Jeśli ikona na pasku zadań jest kolorowa i nie zawiera żadnych dodatków, oznacza to,

że wszystkie składniki systemu **AVG Anti-Virus 2012** 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. *(Korzystając z opcji ignorowania stanu składników potwierdzasz, że wiesz o nieprawidłowym stanie systemu, ale z pewnych powodów nie chcesz przywrócić go do normalnego działania.)*

- Ikona z wykrzyknikiem oznacza, że pewien składnik *(lub kilka z nich)* jest w stanie błędu. Prosimy o baczne obserwowanie takich sytuacji oraz o podjęcie próby przywrócenia poprawnej konfiguracji odpowiednich składników. W tym celu wystarczy kliknąć dwukrotnie ikonę, co spowoduje otwarcie interfejsu użytkownika AVG. Szczegóły na temat błędnego stanu systemu można znaleźć w sekcji Informacje o stanie bezpieczeństwa.

- Kolorowej ikonie na pasku zadań może również towarzyszyć wirujący promień światła. Taki wygląd ikony oznacza, że właśnie uruchomiono proces aktualizacji.

- Kolorowa ikona z białą strzałką oznacza, że przeprowadzany jest jeden ze skanów **AVG Anti-Virus 2012**.

Informacje ikony na pasku zadań

Ikona AVG na pasku zadań informuje również użytkownika **AVG Anti-Virus 2012** o bieżącej aktywności systemu lub o zmianach w jego konfiguracji (*np. automatyczne uruchomienie aktualizacji lub zaplanowanego skanu, zmiana stanu składnika, wystąpienie błędu, ...*) dzięki okienkom wyświetlanym nad ikoną:

Akcje dostępne z poziomu ikony na pasku zadań

Ikona AVG na pasku zadań może być używana jako szybki sposób na uruchomienie interfejsu użytkownika **AVG Anti-Virus 2012** (wystarczy dwukrotne kliknięcie). Kliknięcie ikony prawym przyciskiem myszy otwiera menu kontekstowe zawierające następujące opcje:

- ***Otwórz interfejs użytkownika AVG*** - Otwiera interfejs użytkownika systemu **AVG Anti-Virus 2012**.

- ***Skanuj*** - Otwiera menu kontekstowe zawierające predefiniowane skany (*Skan całego komputera*, *Skan określonych plików lub folderów*, *skan Anti-Rootkit*) i umożliwia natychmiastowe uruchomienie dowolnego z nich. .

- ***Uruchom PC Analyzer*** - Uruchamia 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.

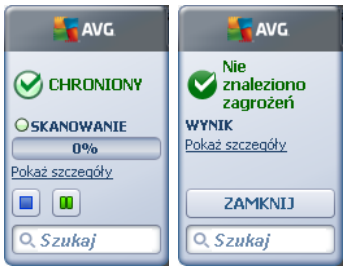
5.6. Gadżet AVG

Gadżet AVG jest wyświetlany na pulpicie systemu Windows w (*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 2012**, tj. skanowania i aktualizacji:

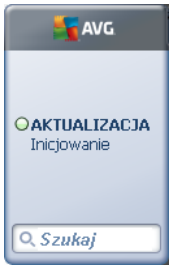
Szybki dostęp do skanowania i aktualizacji

W razie potrzeby ***Gadżet AVG*** umożliwi Ci natychmiastowe uruchomienie testu lub aktualizacji:

- ***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 linku ***Aktualizuj teraz*****AVG Anti-Virus 2012** umożliwia uruchomienie aktualizacji systemu bezpośrednio z poziomu gadżetu:



Dostęp do sieci społecznościowych

Gadżet AVG daje również szybki dostęp do najpopularniejszych sieci społecznościowych. Odpowiednie przyciski przeniosą Cię do społeczności AVG na Twitterze, portalu Facebook i LinkedIn:

- ***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 ***społeczności AVG SMB*** w sieci LinkedIn.

Inne funkcje dostępne z poziomu gadżetu

- ***PC Analyzer*** - otwiera interfejs składnika PC Analyzer.

- ***Pole wyszukiwania*** - wprowadzenie słowa kluczowego powoduje natychmiastowe zwrócenie wyników w nowo otwartym oknie domyślnej przeglądarki internetowej.

6. Składniki AVG

6.1. Anti-Virus

Składnik ***Anti-Virus*** jest rdzeniem całego systemu **AVG Anti-Virus 2012** i łączy w sobie szereg funkcji niezbędnych w każdym programie antywirusowym:

- Silnik skanujący
- Ochronę rezydentną
- Ochronę przed oprogramowaniem szpiegującym

6.1.1. Silnik skanujący

Silnik skanujący, który jest rdzeniem składnika ***Anti-Virus*** aktywnie skanuje wszystkie pliki i operacje dyskowe *(otwieranie/zamykanie plików, itd.)* w poszukiwaniu znanych wirusów. Wszelkie wykryte infekcje zostaną zablokowane, a następnie wyleczone lub przeniesione do Przechowalni wirusów.

System AVG Anti-Virus 2012 gwarantuje, że na komputerze nie będzie działał żaden znany wirus!

Metody wykrywania

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. ***Anti-Virus*** korzysta z następujących metod detekcji:

- Skanowanie - wyszukiwanie ciągów bajtów typowych dla danego wirusa.
- *Analiza heurystyczna* - dynamiczna emulacja instrukcji skanowanego obiektu w środowisku wirtualnego komputera
- Wykrywanie generyczne - wykrywanie instrukcji typowych dla danego wirusa lub grupy wirusów.

Korzystanie z tylko jednej technologii nie zapewnia stuprocentowej skuteczności wykrywania wirusów, dlatego składnik ***Anti-Virus*** wykorzystuje jednocześnie kilka metod. **AVG Anti-Virus 2012** jest w stanie analizować i wykrywać aplikacje i biblioteki DLL, które mogą być potencjalnie niepożądane w Twoim systemie. Takie zagrożenia (różne rodzaje oprogramowania szpiegującego, reklamowego itp.) nazywane są również Potencjalnie Niechcianymi Programami. . Ponadto, **AVG Anti-Virus 2012** skanuje rejestr systemu Windows pod kątem podejrzanych wpisów, a także tymczasowe pliki internetowe i szpiegujące pliki cookie. Wszystkie te zagrożenia mogą być traktowane równie poważnie, jak pozostałe infekcje.

AVG Anti-Virus 2012 zapewnia Twojemu komputerowi nieprzerwaną ochronę!

6.1.2. Ochrona rezydentna

System AVG Anti-Virus 2012 jest w stanie zapewnić Ci stałą ochronę dzięki tzw. Ochronie rezydentnej. Składnik ***Anti-Virus*** skanuje każdy plik *(o określonym rozszerzeniu lub bez rozszerzenia)* w trakcie jego otwierania, zapisywania lub kopiowania. Chroni dzięki temu obszary systemowe komputera oraz urządzenia wymienne (*dyski flash itp.*). Po wykryciu wirusa w analizowanym pliku Ochrona rezydentna zatrzymuje aktualnie wykonywane operacje i uniemożliwia uaktywnienie zagrożenia. Zazwyczaj użytkownik nie będzie w stanie zauważyć tego procesu, ponieważ odbywa się on w tle. Powiadomienia wyświetlane są tylko w wypadku wykrycia zagrożenia. Automatycznie następuje również zablokowanie dostępu do pliku oraz usunięcie wirusa.

Ochrona rezydentna ładowana jest do pamięci komputera podczas rozruchu systemu i aby zachować skuteczność musi pozostać włączona przez cały czas!

6.1.3. Ochrona przed oprogramowaniem szpiegującym

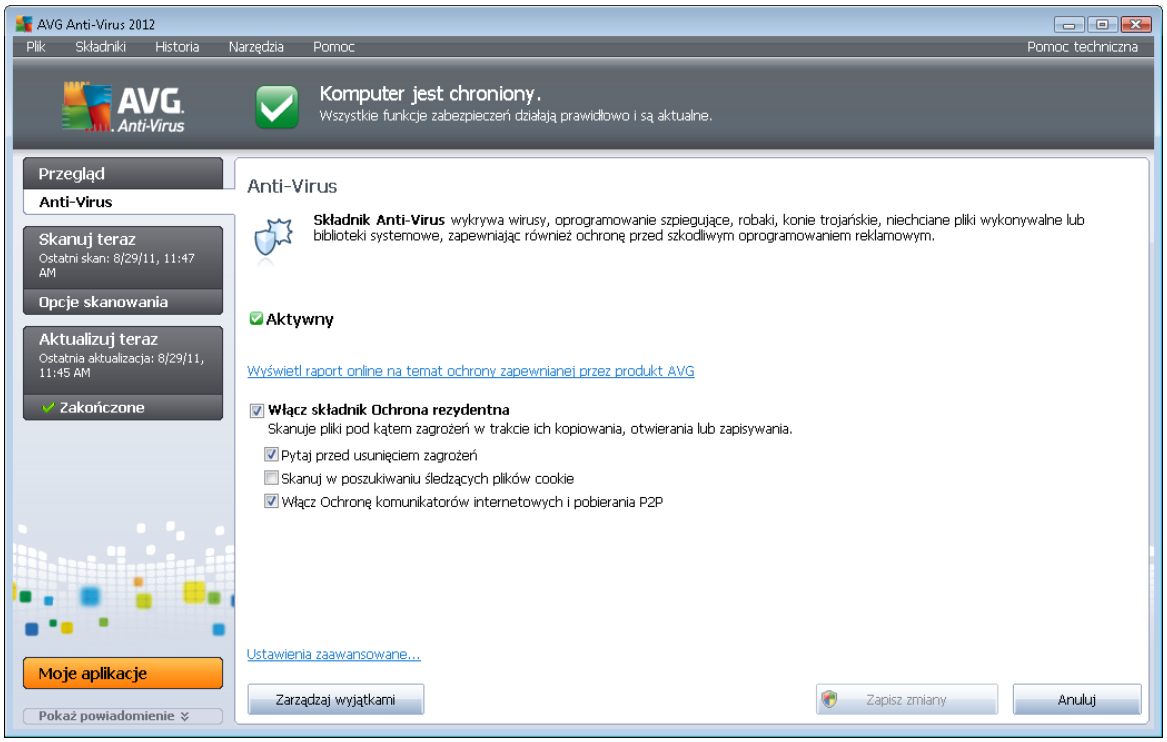
Anti-Spyware stanowi bazę danych oprogramowania szpiegującego, która umożliwia identyfikację znanych wszystkich znanych zagrożeń tego typu. Eksperci firmy AVG zajmujący się oprogramowaniem szpiegującym dokładają wszelkich starań, aby jak najszybciej identyfikować i opisywać najnowsze sygnatury oprogramowania szpiegującego, a następnie dodają ich definicje do naszej bazy danych. Nowe definicje są pobierane jako aktualizacje, więc użytkownicy są zawsze niezawodnie chronieni nawet przed najnowszymi typami oprogramowania szpiegującego. ***Anti-Spyware*** pozwala na pełne przeskanowanie komputera pod kątem oprogramowania szpiegującego. Wykrywa również uśpione lub nieaktywne szkodliwe oprogramowanie, które zostało pobrane, ale jeszcze nie aktywowane.

Czym jest oprogramowanie szpiegujące?

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 celowo i często zawierają reklamy, wyskakujące okna i inne nieprzyjemne 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.

6.1.4. Interfejs składnika Anti-Virus

Interfejs składnika ***Anti-Virus*** podaje najważniejsze informacje o jego funkcjach, aktualnym stanie *(Aktywny)*, a także zawiera podstawowe opcje konfiguracyjne:



Konfiguracja

To okno dialogowe udostępnia najważniejsze elementy konfiguracyjne składnika ***Anti-Virus***. Poniżej znajduje się ich krótki opis:

- ***Wyświetl raport online na temat ochrony zapewnianej przez produkt AVG*** - Link ten przeniesie Cię na jedną ze stron AVG (http://www.avg.com/). Znajdziesz na niej statystyczne podsumowanie wszystkich działań systemu **AVG Anti-Virus 2012** prowadzonych na Twoim komputerze w ostatnim okresie, oraz od momentu instalacji.

- ***Włącz Ochronę rezydentną*** - Opcja ta pozwala na łatwe włączenie/wyłączenie Ochrony rezydentnej. Ochrona rezydentna to składnik służący do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. W przypadku wykrycia jakiegokolwiek zagrożenia, zostaniesz natychmiast powiadomiony. Funkcja ta domyślnie jest włączona i stanowczo zalecamy jej zachowanie! Sekcja poświęcona Ochronie rezydentnej pozwala także zdecydować o akcji podejmowanej po wykryciu infekcji:

  - ***Automatycznie usuwaj zagrożenia*** / ***Pytaj przed usunięciem zagrożeń*** - Należy wybrać jedną z tych opcji. Wybór ten nie ma wpływu na poziom bezpieczeństwa - umożliwia on jedynie podjęcie każdorazowej decyzji o usunięciu lub pozostawieniu wykrytych infekcji.

- ***Skanuj w poszukiwaniu śledzących plików cookie*** - W obu przypadkach można określić, czy pliki mają być skanowane w poszukiwaniu śledzących plików cookie. *(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 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.)* W konkretnych przypadkach można włączyć tę opcję, aby osiągnąć najwyższy poziom ochrony, ale domyślnie jest ona wyłączona.

- ***Włącz ochronę komunikatorów internetowych*** - Zaznacz to pole, jeśli chcesz mieć pewność, że wiadomości przesyłane przy użyciu komunikatorów internetowych (*np. ICQ, MSN Messenger, ...*) nie zawierają wirusów.

- ***Ustawienia zaawansowane***... - Kliknięcie tego linku spowoduje przejście do konkretnego okna Ustawień zaawansowanych systemu **AVG Anti-Virus 2012**. Możliwa będzie dzięki temu szczegółowa edycja konfiguracji składnika. Przypominamy jednak, domyślna konfiguracja wszystkich składników **AVG Anti-Virus 2012** zapewnia optymalną wydajność i najwyższy stopień ochrony. Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach!

Przyciski kontrolne

We wspomnianym oknie znajdują się następujące przyciski kontrolne:

- ***Zarządzaj wyjątkami*** - Otwiera nowe okno Ochrona rezydentna - Wyjątki. Można dojść do niego również z poziomu menu głównego, poprzez Ustawienia zaawansowane / Anti-Virus / Ochrona rezydentna / Wyjątki *(więcej informacji na ten temat znajduje się w odpowiednim rozdziale pomocy)*. Okno to pozwala zdefiniować pliki i foldery, które mają być wykluczone ze skanowania Ochrony rezydentnej. 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 katalogu *(lub 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.

- ***Zapisz zmiany*** - Zapisuje wszystkie zmiany w konfiguracji składnika dokonane w tym oknie, a następnie powraca do głównego okna interfejsu użytkownika systemu **AVG Anti-Virus 2012** (*przeglądu składników*).

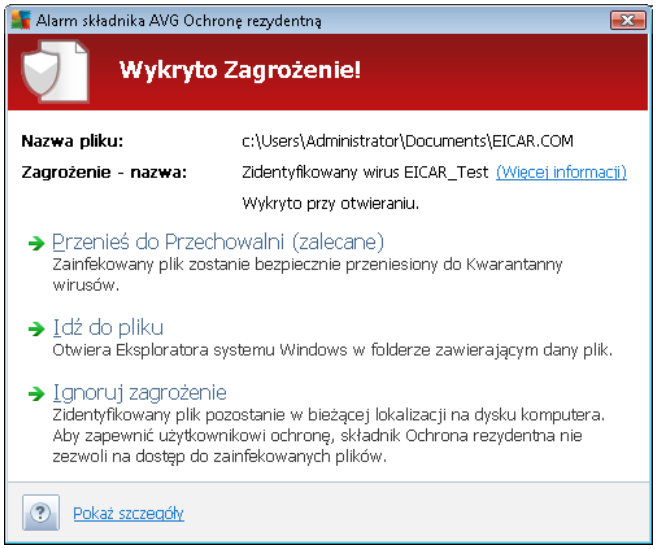
- ***Anuluj*** - Cofa wszystkie zmiany wprowadzone w tym oknie dialogowym. Konfiguracja nie zostanie zapisana. Nastąpi powrót do głównego okna interfejsu użytkownika systemu **AVG**

Anti-Virus 2012 (*przeglądu składników*).

6.1.5. Przypadki wykrycia przez Ochronę Rezydentną

Wykryto zagrożenie!

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. Dostępnych jest kilka opcji. ***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

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

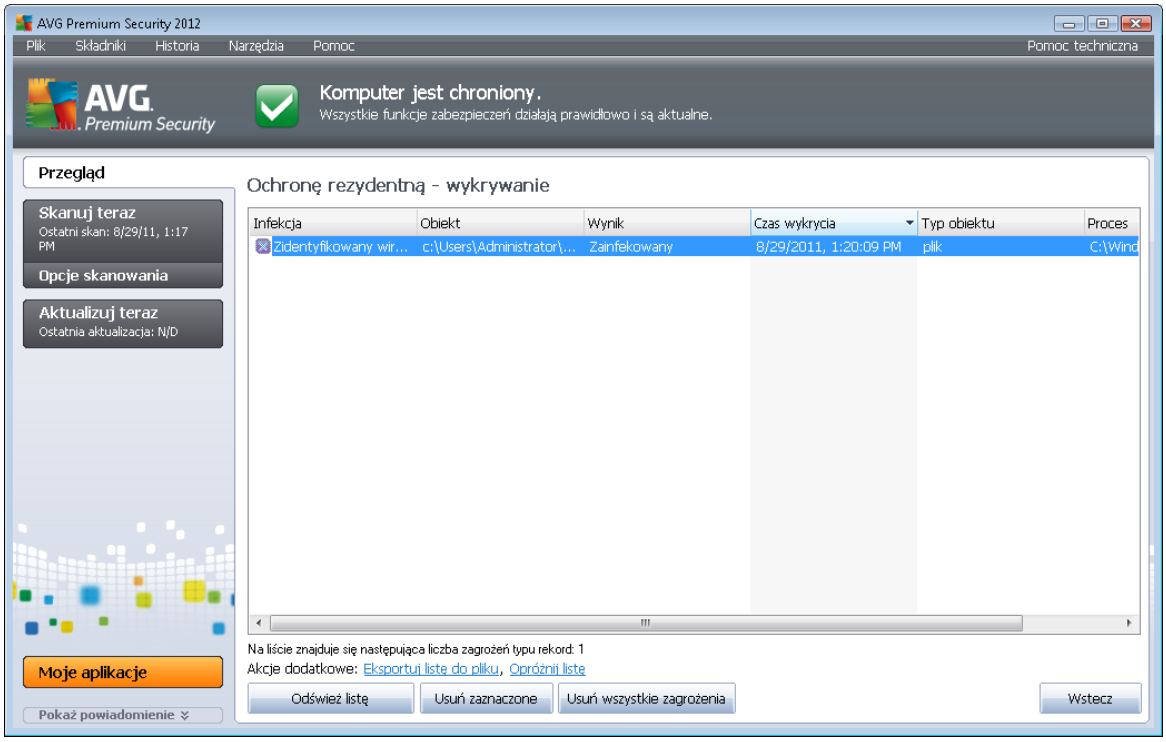
- ***Ignoruj*** - tej opcji NIE należy używać bez uzasadnionego powodu!

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 zagrożeń wykrytych przez Ochronę rezydentną

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*** przenosi z powrotem do domyślnego okna interfejsu użytkownika AVG (*przeglądu składników*).

6.2. 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.

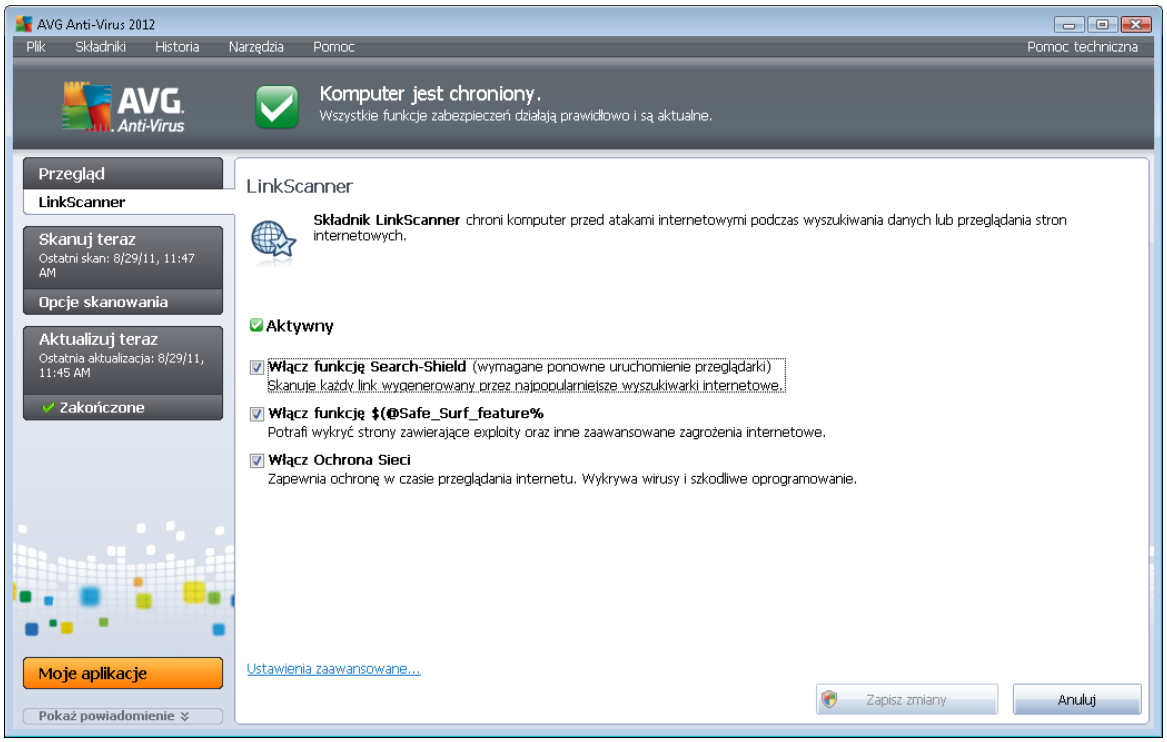
Składnik LinkScanner nie jest przeznaczony dla platform serwerowych!

Technologia składnika ***LinkScanner*** składa się z dwóch funkcji:

- Funkcja Search-Shield wykorzystuje listę witryn internetowych (adresów URL), które zostały uznane za niebezpieczne. Wszystkie wyniki wyszukiwania serwisów Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, and Seznam są sprawdzane na podstawie tej listy, a następnie obok każdego z nich wyświetlana jest odpowiednia ikona klasyfikacji bezpieczeństwa (*w przypadku wyników wyszukiwania serwisu Yahoo! wyświetlane są tylko ewentualne ikony informujące o niebezpieczeństwie*).
- 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.
- Ochrona Sieci zapewnia ochronę czasu rzeczywistego podczas przeglądania internetu. Skanuje zawartość odwiedzanych stron (włączając w to udostępnione na nich pliki) jeszcze zanim zostaną wyświetlone w przeglądarce czy pobrane na dysk. Ochrona Sieci wykrywa wirusy i oprogramowanie szpiegujące oraz natychmiast zatrzymuje ich pobieranie, by nie przedostały się na Twój komputer.

6.2.1. Interfejs składnika LinkScanner

Interfejs składnika LinkScanner zawiera krótki opis jego funkcji oraz informację o bieżącym stanie *(Aktywny)*:



W dolnej części okna dialogowego możesz skonfigurować podstawowe parametry tego składnika:

- ***Włącz funkcję Search-Shield*** - (*domyślnie włączona*): Odznaczenie tego pola spowoduje wyłączenie funkcji Search-Shield.
- ***Włącz funkcję Surf-Shield*** - (*domyślnie włączona*): Aktywna (*działająca w czasie rzeczywistym*) ochrona przed zainfekowanymi stronami WWW. 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*).
- ***Włącz Ochronę Sieci*** - (*domyślnie włączona*): Skanowanie w czasie rzeczywistym, obejmujące wirusy i oprogramowanie szpiegujące spotykane na odwiedzanych stronach WWW. Po wykryciu przez Ochronę Sieci jakiegokolwiek zagrożenia, pobieranie pliku zostaje zatrzymane, by zapobiec infekcji.

6.2.2. Zagrożenia wykryte przez funkcję 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 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*).

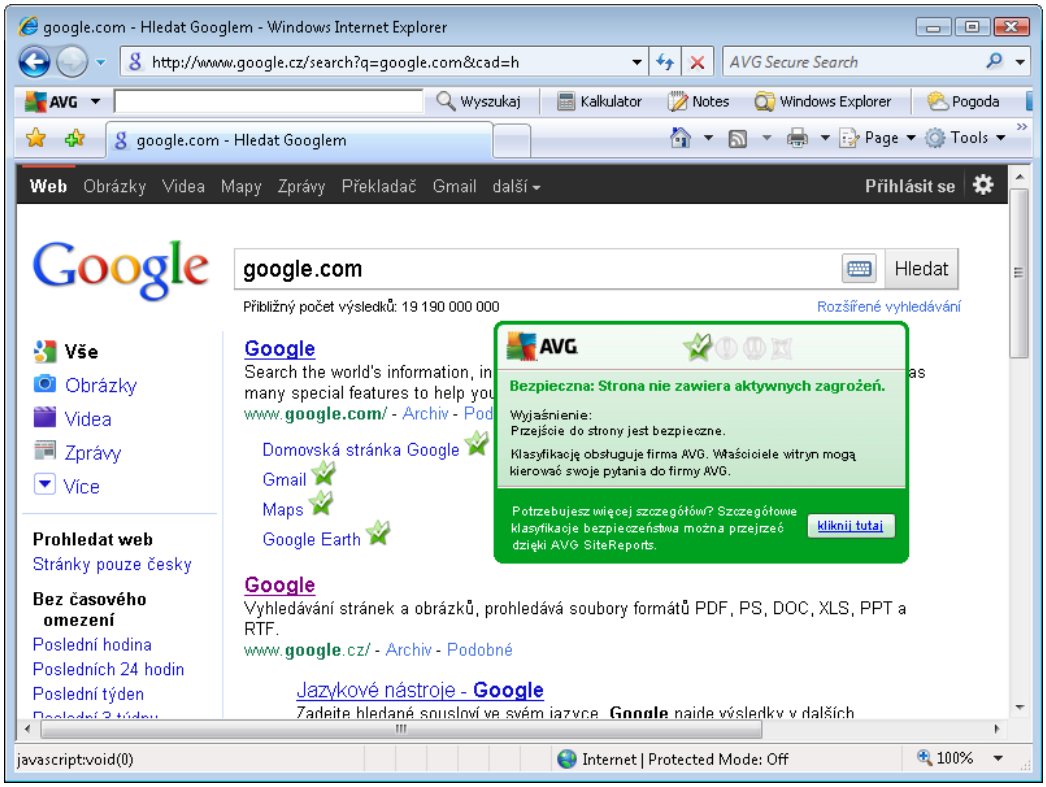
 Strona, do której prowadzi łącze, nie zawiera zagrożeń, ale jest podejrzana (*wątpliwości budzi jej pochodzenie lub przeznaczenie, więc nie zaleca się dokonywania na niej zakupów itp.*).

 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.

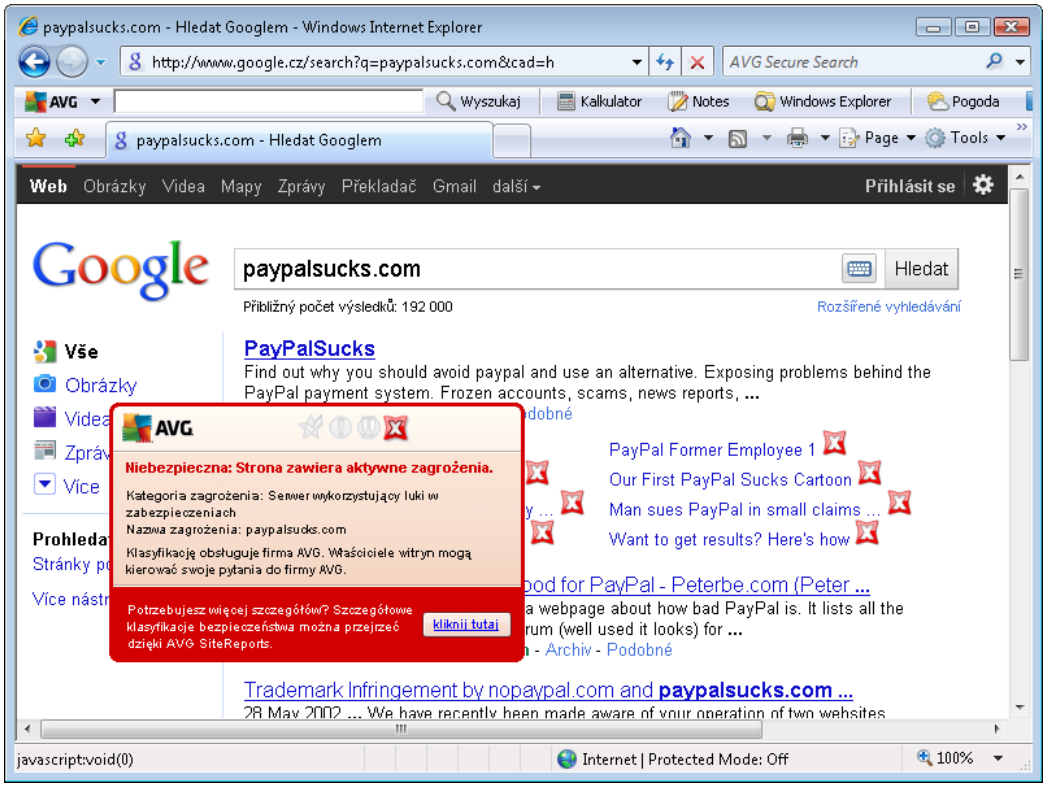
Umieszczenie kursora na wybranej ikonie wyników sprawdzania powoduje wyświetlenie szczegółowych informacji o danym łączu. Informacje te obejmują szczegóły zagrożenia (*o ile są one dostępne*):



6.2.3. Zagrożenia wykryte przez funkcję 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 Link Scanner nie pozwoli na jej wyświetlenia w przeglądarce.

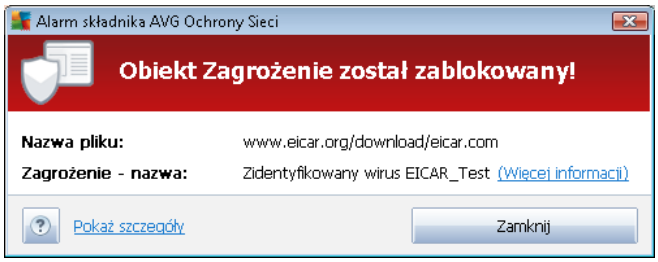
Jeśli kiedykolwiek trafisz na szkodliwą stronę internetową, składnik Link Scanner wyświetli w przeglądarce ostrzeżenie podobne do tego:



Odwiedzanie takiej witryny jest bardzo ryzykowne i należy tego unikać!

6.2.4. 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:

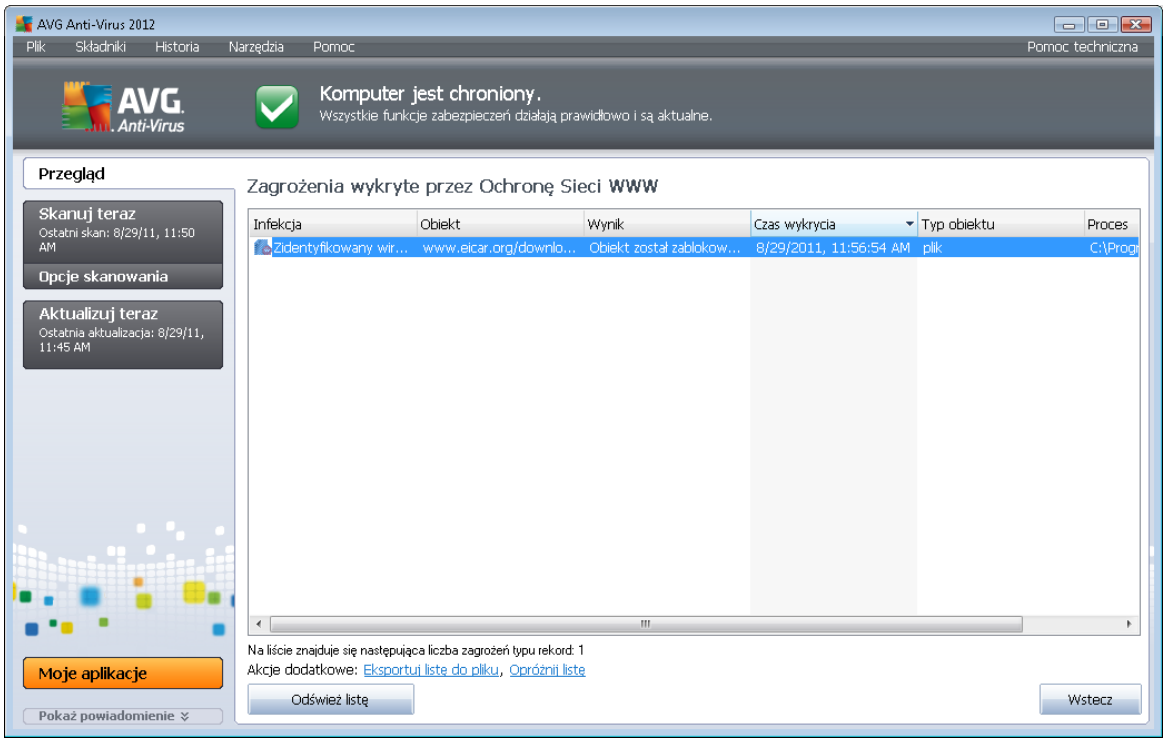


W tym oknie dialogowym będą wyświetlane ostrzeżenia dotyczące pliku wykrytego i oznaczonego jako zainfekowany (*Nazwa pliku*), nazwa rozpoznanej infekcji (*Nazwa zagrożenia*) i link do Encyklopedii wirusów, w której można znaleźć szczegółowe informacje, jeśli są dostępne (*Więcej informacji*). W oknie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

Przyciski kontrolne

- ***Odśwież listę*** - pozwala zaktualizować listę obiektów wykrytych przez składnik ***Ochrona Sieci***

- ***Wstecz*** - przełącza z powrotem do domyślnego interfejsu użytkownika systemu AVG *(przeglądu składników)*

6.3. Ochrona 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.

Składnik ***Ochrona poczty e-mail*** jest odpowiedzialny za skanowanie wszystkich wiadomości e-mail, zarówno wysyłanych, jak i otrzymywanych. Każdy wirus wykryty w wiadomości jest natychmiast przenoszony do Przechowalni. Skaner poczty może odfiltrowywać określone typy załączników i dodawać do wiadomości tekst certyfikujący brak infekcji. ***Ochrona poczty e-mail*** składa się z dwóch głównych funkcji:

- Skaner poczty e-mail

- Anti-Spam

6.3.1. Skaner 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 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).

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

6.3.2. Anti-Spam

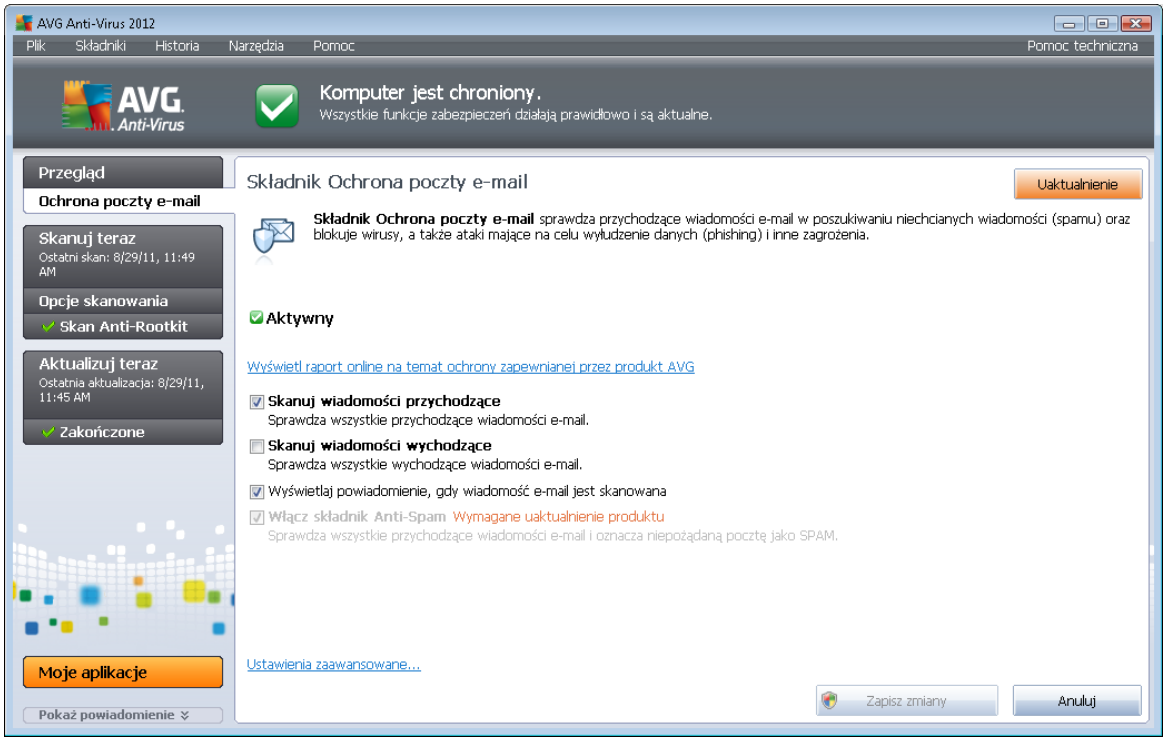
Jak działa składnik Anti-Spam?

Składnik Anti-Spam sprawdza wszystkie przychodzące wiadomości e-mail i oznacza te niepożądane jako SPAM. ***Składnik Anti-Spam*** może modyfikować temat wiadomości e-mail (*wykrytej jako SPAM*), dodając do niego specjalny ciąg tekstowy. Dzięki temu możliwe jest łatwe filtrowanie wiadomości e-mail w programie pocztowym. ***Składnik Anti-Spam*** podczas przetwarzania każdej wiadomości wykorzystuje kilka metod analizy, oferując maksymalnie skuteczną ochronę przeciwko niepożądanym wiadomościom e-mail. Składnik ***Anti-Spam*** do wykrywania spamu korzysta z regularnie aktualizowanej bazy danych. Można także użyć serwerów RBL (*publicznych baz adresów znanych nadawców spamu*) lub ręcznie dodać adresy do białej listy (*wiadomości pochodzące z tych adresów nie są nigdy oznaczane jako spam*) lub czarnej listy (*wiadomości pochodzące z tych adresów są zawsze oznaczane jako spam*).

Czym jest spam?

Mianem spamu określa się niepożądaną pocztę e-mail (głównie reklamy produktów lub usług, które są hurtowo rozsyłane do wielkiej liczby odbiorców jednocześnie, zapełniając ich skrzynki pocztowe). Spamem nie jest korespondencja seryjna rozsyłana do odbiorców po wyrażeniu przez nich zgody. Spam jest nie tylko irytujący, ale może być również źródłem oszustw, wirusów i obraźliwych treści.

6.3.3. Interfejs ochrony poczty e-mail



Interfejs składnika ***Skaner poczty e-mail*** zawiera krótki opis jego funkcji i informację o stanie *(Aktywny).* Użyj linku ***Wyświetl raport online na temat ochrony zapewnianej przez produkt AVG*** aby przejrzeć dokładne statystyki aktywności i detekcji **AVG Anti-Virus 2012** na poświęconej temu stronie AVG (http://www.avg.com/).

Podstawowe ustawienia ochrony poczty e-mail

W oknie ***Ochrona poczty e-mail*** możesz skonfigurować podstawowe funkcje tego składnika:

- ***Skanuj wiadomości przychodzące*** *(domyślnie włączona)* - zaznacz to pole, aby wszystkie wiadomości e-mail przychodzące na dane konto pocztowe były skanowane w poszukiwaniu wirusów.
- ***Skanuj wiadomości wychodzące*** *(domyślnie wyłączone)* - zaznacz to pole, aby skanowane były wszystkie wiadomości wysyłane z Twojego konta e-mail.
- ***Wyświetlaj powiadomienie, gdy wiadomość e-mail jest skanowana*** *(domyślnie włączona)* - zaznacz to pole, jeśli chcesz, aby nad ikoną AVG (na pasku zadań) wyświetlane było odpowiednie powiadomienie w chwili, gdy Skaner poczty e-mail skanuje wiadomość.

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.

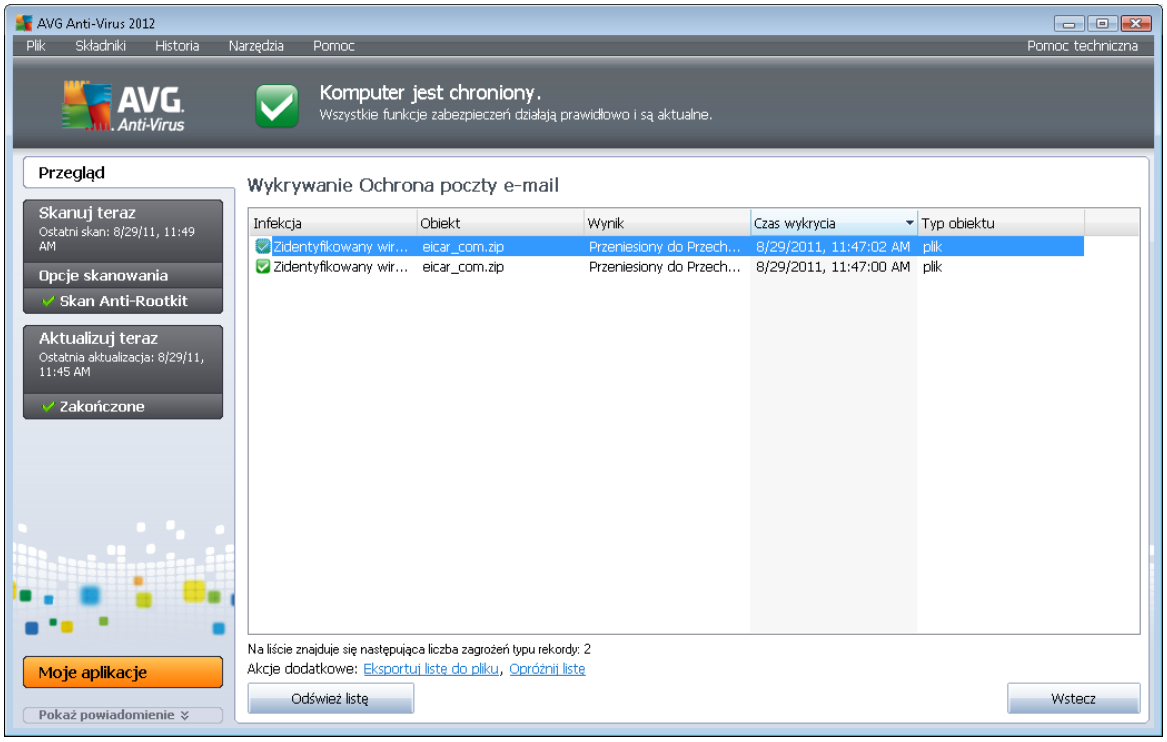
Pozycja ***Włącz składnik Anti-Spam*** pozwala aktywować filtrowanie niechcianych wiadomości trafiających do Twojej skrzynki pocztowej. Jednak składnik Anti-Spam nie wchodzi w skład produktu **AVG Anti-Virus 2012**. Jest on dostępny w bogatszych edycjach systemu AVG. ***Więcej informacji o możliwości uaktualnienia systemu AVG znajduje się na naszej stronie internetowej (http://www.avg.com/).***

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 powoduje powrót do domyślnego okna Interfejsu użytkownika AVG (*przeglądu składników*)

6.3.4. Zagrożenia wykryte przez Skaner poczty e-mail



W oknie dialogowym ***Zagrożenia wykryte przez Ochronę poczty e-mail*** *(dostępnym po wybraniu odpowiedniej opcji z menu Historia*) wyświetlana jest lista wszystkich obiektów wykrytych przez składnik Ochrona 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.

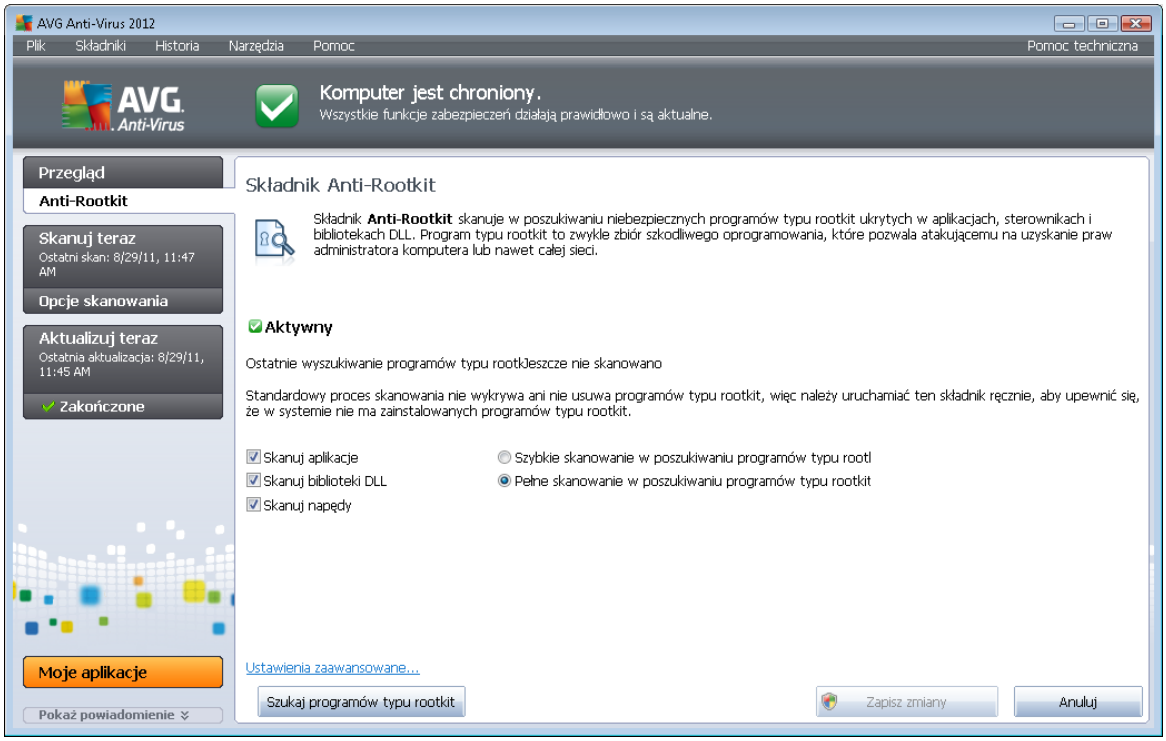
6.4. Anti-Rootkit

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 ***Anti-Rootkit*** umożliwia wykrywanie programów typu rootkit na podstawie wstępnie zdefiniowanego zestawu reguł. Przypominamy, że wykryte zostaną wszystkie rootkity *(nie tylko te szkodliwe)*. Jeśli składnik ***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.

Czym jest program typu 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.

6.4.1. Interfejs składnika Anti-Rootkit



Interfejs składnika ***Anti-Rootkit*** zawiera krótki opis jego funkcji, informuje o aktualnym stanie *(Aktywny)*, oraz o dacie ostatniego uruchomienia skanu ***Anti-Rootkit*** (***Ostatnie wyszukiwanie programów typu 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***.

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.

Podstawowe ustawienia Anti-Rootkit

W dolnej części okna znajduje się sekcja umożliwiająca skonfigurowanie podstawowych funkcji skanowania pod kątem rootkitów. 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

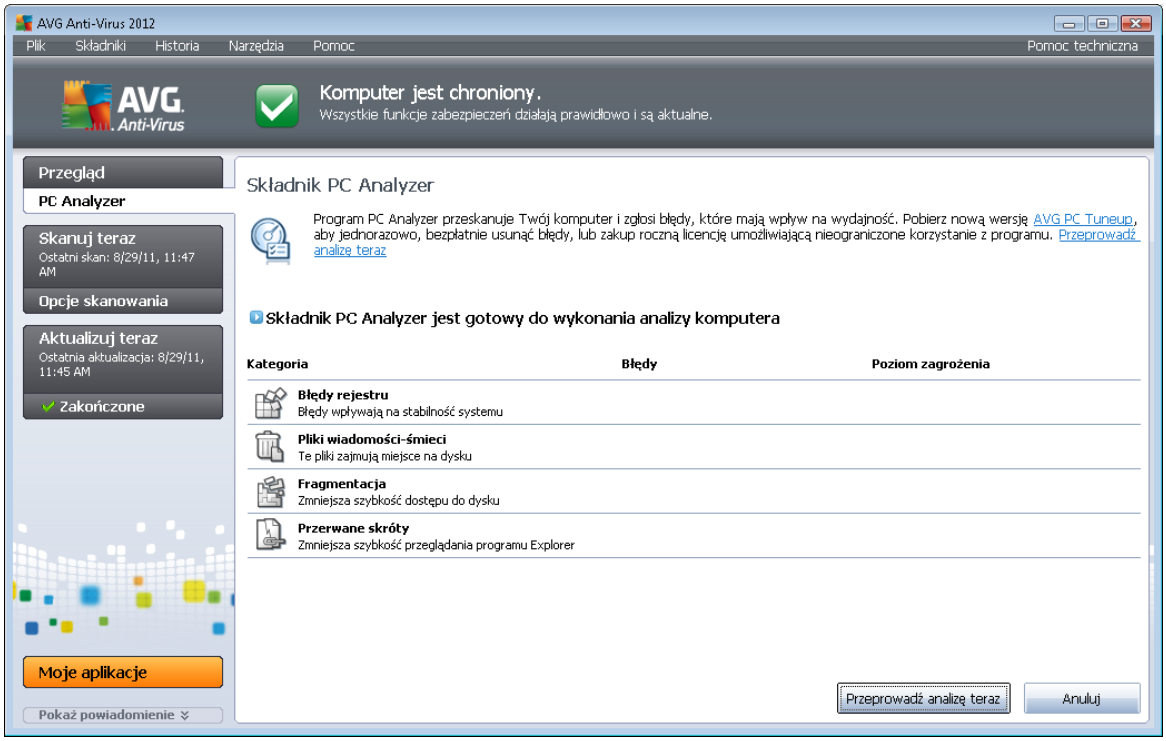
- ***Szukaj programów typu rootkit*** - ponieważ to skanowanie nie jest częścią testu Skan całego komputera, można je uruchomić bezpośrednio z Interfejsu składnika ***Anti-Rootkit***, klikając ten przycisk.

- ***Zapisz zmiany*** - kliknięcie tego przycisku pozwala zapisać wszystkie zmiany wprowadzone w danym oknie i powrócić do domyślnego okna interfejsu użytkownika AVG (*przeglądu składników*).

- ***Anuluj*** - kliknięcie tego przycisku pozwala powrócić do domyślnego okna interfejsu użytkownika AVG (*przeglądu składników*) bez zapisywania wprowadzonych zmian.

6.5. 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:



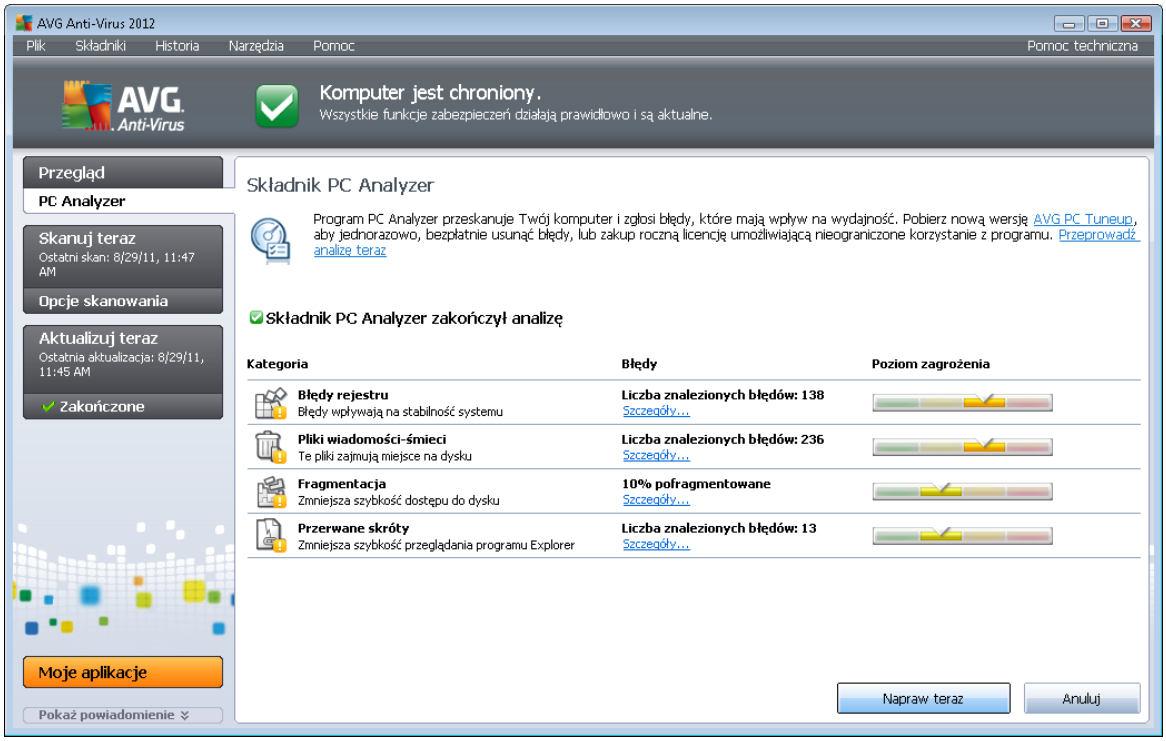
- ***Błędy rejestru*** - podaje informację o liczbie błędów w rejestrze systemu Windows. Naprawa rejestru wymaga zaawansowanej wiedzy, dlatego nie jest zalecane przeprowadzanie jej samodzielnie.

- ***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 ulec rozproszeniu po różnych sektorach 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*** - użyj tego przycisku by zakończyć bieżącą analizę lub powrócić do domyślnego okna AVG (*Przeglądu składników*) po jej zakończeniu

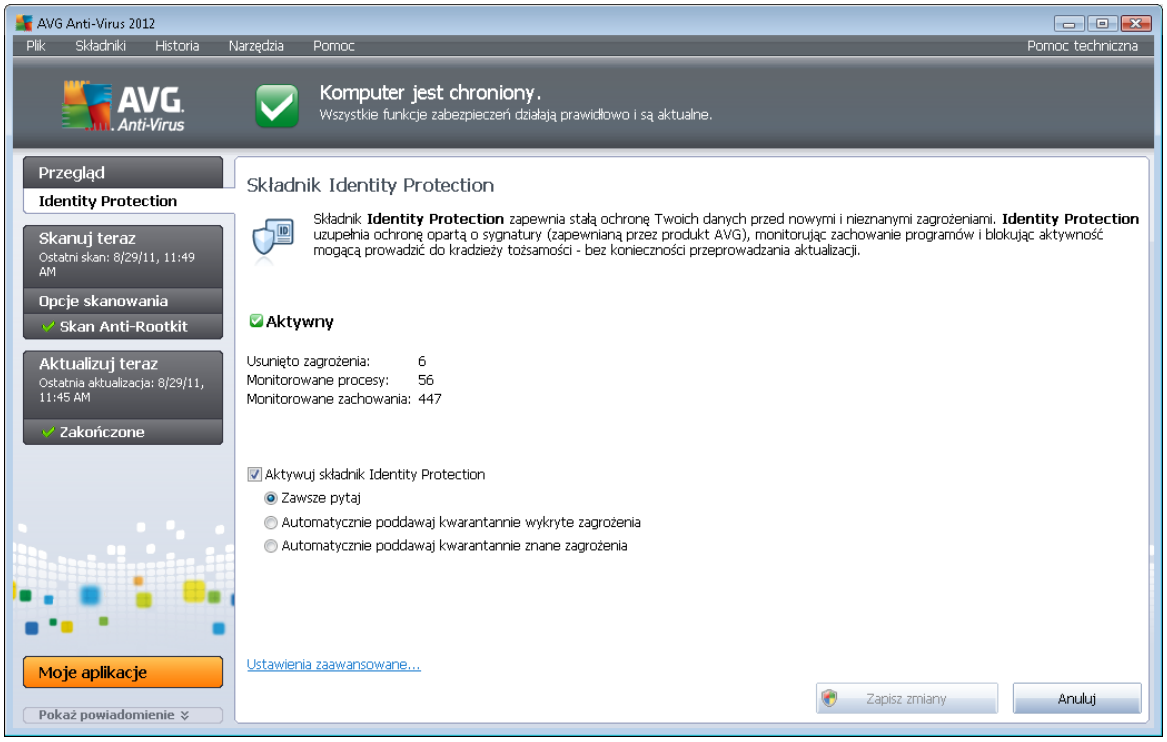
6.6. Identity Protection

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

Składnik ***Identity Protection*** zapewnia komputerowi ochronę w czasie rzeczywistym przeciw nowym, a nawet nieznanym zagrożeniom. Monitoruje wszystkie procesy *(w tym ukryte)* i rozpoznaje ponad 285 różnych wzorców zachowań, dzięki czemu może ustalić, czy w systemie dzieje się coś szkodliwego. Z tego względu może wykrywać zagrożenia, które nie zostały jeszcze opisane w bazie danych wirusów. Gdy w komputerze pojawi się nieznany kod programu, jest on natychmiast obserwowany i monitorowany pod kątem szkodliwego zachowania. Jeśli dany plik zostanie uznany za szkodliwy, składnik ***Identity Protection*** przeniesie jego kod do Kwarantanny i cofnie wszelkie zmiany wprowadzone w systemie *(ingerencje w inne programy, zmiany w rejestrze, operacje otwarcia portów itd.).* Nie ma potrzeby przeprowadzania skanów w celu zapewnienia ochrony. Technologia ma charakter wysoce proaktywny, wymaga rzadkich aktualizacji i zapewnia stałą ochronę.

Identity Protection doskonale uzupełnia ochronę zapewnianą przez Anti-Virus. Zdecydowanie zalecamy zainstalowanie obydwu produktów, aby zapewnić pełną ochronę komputera!

6.6.1. Interfejs składnika AVG Identity Protection



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

- ***Usunięte zagrożenia*** - podaje 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

Podstawowe ustawienia AVG Identity Protection

W dolnej części okna dialogowego możesz skonfigurować podstawowe funkcje tego składnika:

- ***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:

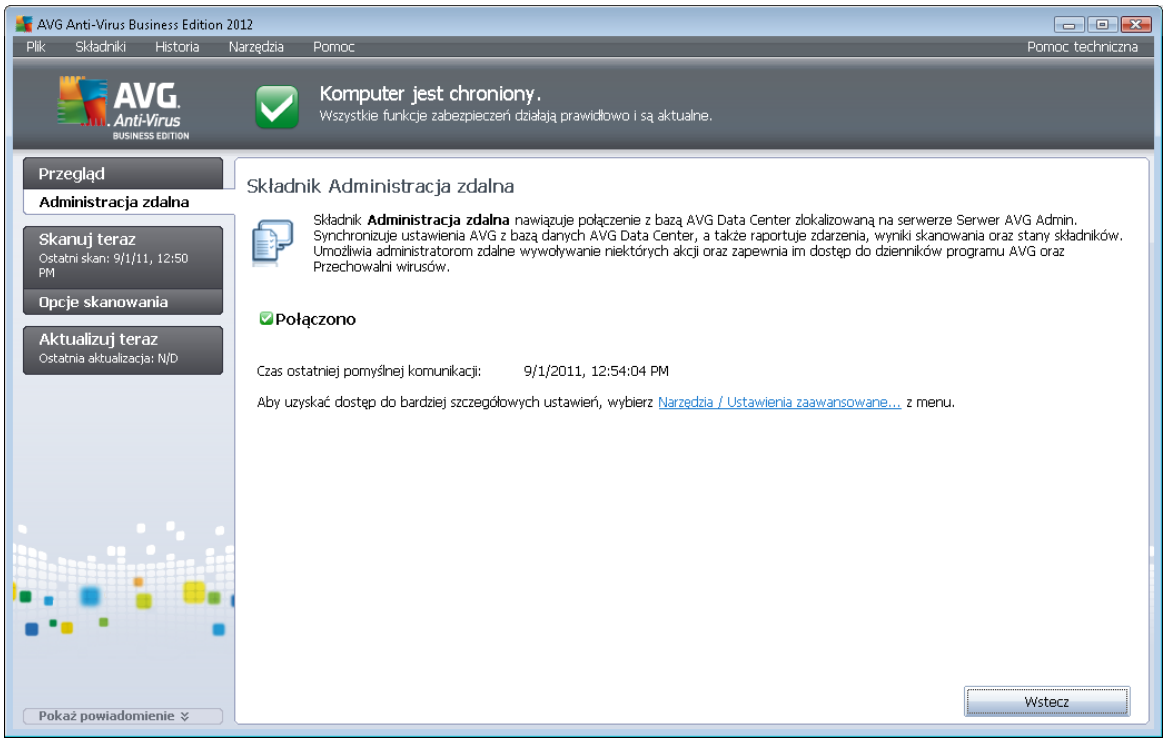
  - ***Zawsze monituj*** - jeśli aplikacja zostanie wykryta jako szkodliwe oprogramowanie, użytkownik zostanie zapytany, czy ma ona zostać zablokowana (*ta opcja jest domyślnie włączona i zaleca się niezmienianie tego bez ważnego powodu*)
  - ***Automatycznie poddawaj kwarantannie wykryte zagrożenia*** - 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 powoduje powrót do domyślnego okna Interfejsu użytkownika AVG (*przeglądu składników*)

6.7. Administracja zdalna



Składnik ***Administracja zdalna*** wyświetlany jest w interfejsie użytkownika **AVG Anti-Virus 2012** tylko w przypadku wersji Business Edition *(szczegóły posiadanej licencji można znaleźć na karcie Wersja w oknie Informacje otwieranym z poziomu głównego menu Pomoc)*. W oknie 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***.

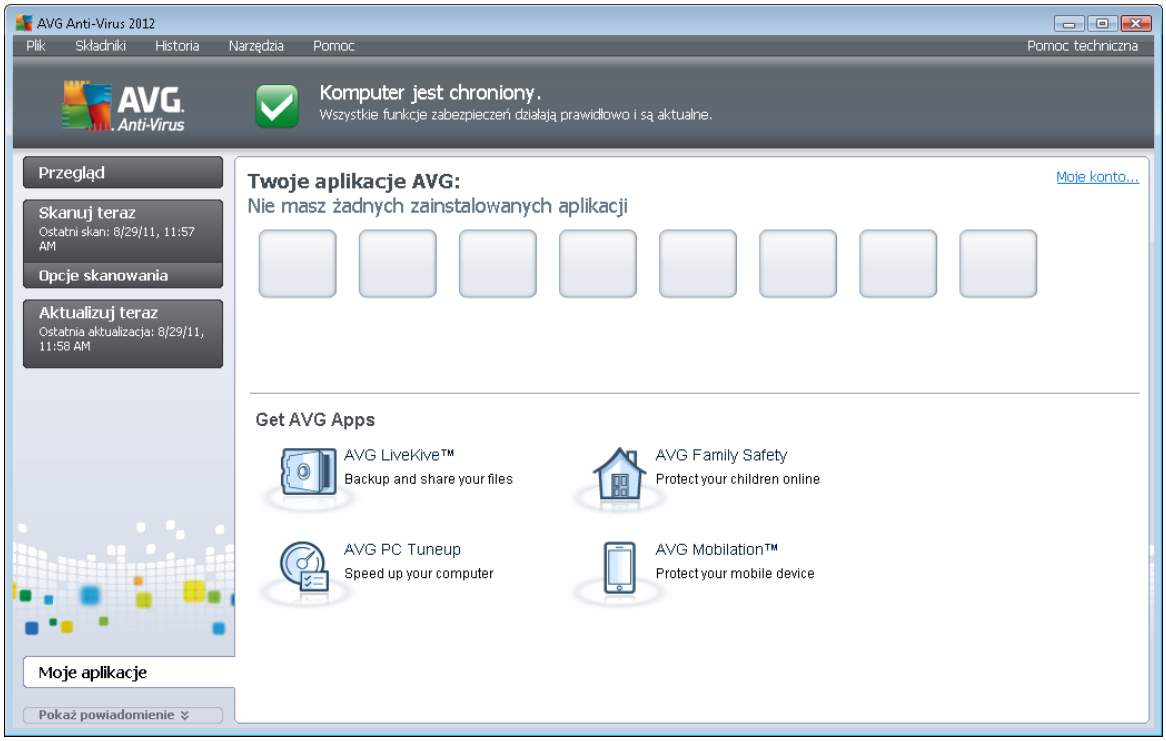
Szczegółowy opis opcji i funkcji Administracji zdalnej w systemie AVG można znaleźć dokumentacji poświęconej wyłącznie temu zagadnieniu. Wspomnianą dokumentację można pobrać ze strony internetowej AVG (http://www.avg.com/), z sekcji ***Centrum pomocy technicznej / Pobierz / Dokumentacja***.

Przyciski kontrolne

- ***Wstecz*** - kliknięcie tego przycisku powoduje powrót do głównego okna interfejsu użytkownika AVG (*przeglądu składników*).

7. Moje aplikacje

Aplikacje LiveKive, Family Safety i PC Tuneup dostępne są jako autonomiczne produkty, które mogą uzupełniać Twoją instalację systemu **AVG Anti-Virus 2012**. Okno ***Twoje aplikacje AVG*** *(dostępne po kliknięciu przycisku Moje aplikacje w głównym oknie AVG)* wyświetla przegląd aplikacji, które już zostały, lub mogą zostać zainstalowane:



7.1. LiveKive

LiveKive ma w założeniu tworzyć kopie zapasowe ważnych danych na naszych bezpiecznych serwerach. ***Program 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 typu iPhone i Android. ***LiveKive*** to przede wszystkim:

- Środek bezpieczeństwa w przypadku uszkodzenia komputera i/lub dysku twardego
- Dostęp do danych z dowolnego urządzenia podłączonego do internetu
- Ułatwiona organizacja danych
- Współdzielenie danych z upoważnionymi osobami

Więcej informacji oraz link umożliwiający pobranie tego składnika można znaleźć na poświęconej mu stronie AVG. Aby to zrobić, wystarczy użyć linku LiveKive, w oknie Moje aplikacje.

7.2. Bezpieczeństwo rodziny

Funkcja ***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.

Więcej informacji oraz link umożliwiający pobranie tego składnika można znaleźć na poświęconej mu stronie AVG. Aby to zrobić, wystarczy użyć linku Bezpieczeństwo rodziny, w oknie Moje aplikacje.

7.3. PC Tuneup

PC Tuneup jest zaawansowanym narzędziem analizującym stan systemu pod kątem zwiększenia wydajności Twojego komputera. ***PC Tuneup*** zawiera w swoim pakiecie:

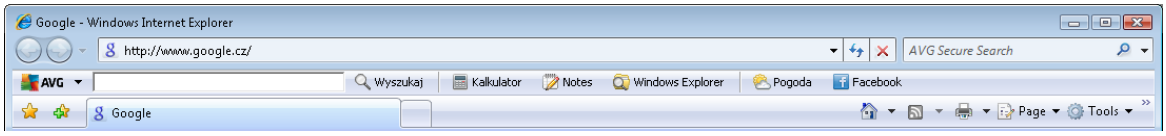
- Disk Cleaner - usuwa niepotrzebne pliki, które spowalniają działanie komputera.
- Disk Defrag - defragmentuje dyski i optymalizuje system plików.
- Registry Cleaner - naprawia błędy rejestru, zwiększając stabilność komputera.
- Registry Defrag - kompaktuje rejestr, zwalniając cenną pamięć.
- Disk Doctor - wyszukuje i naprawia uszkodzone sektory, utracone klastry oraz błędy katalogów.
- Internet Optimizer - dostosowuje uniwersalne ustawienia systemowe do konkretnego typu łącza internetowego.
- Track Eraser - usuwa historię komputera i przeglądarki internetowej.
- Disk Wiper - czyści wolną przestrzeń dyskową, uniemożliwiając odzyskanie poufnych danych przechowywanych w przeszłości.
- File Shredder - trwale usuwa wskazane pliki na dysku lub pamięci USB.
- File Recovery - potrafi przywrócić przypadkowo usunięte pliki z dysków twardych, pamięci USB i innych urządzeń.
- Duplicate File Finder - pomaga znaleźć i usunąć powielone pliki, które marnują przestrzeń dyskową.
- Services Manager - wyłącza niepotrzebne usługi, które spowalniają działanie komputera.
- Startup Manager - pozwala użytkownikowi zarządzać programami, które uruchamiają się automatycznie przy starcie systemu.
- Uninstall Manager - pomaga całkowicie odinstalować oprogramowanie, którego nie używasz.

- Tweak Manager - udostępnia setki opcji i ustawień, które zazwyczaj w systemie Windows są ukryte.
- Task Manager - wyświetla wszystkie działające procesy, usługi i otwarte pliki.
- Disk Explorer - wyświetla pliki zajmujące najwięcej miejsca na dysku twardym.
- System Information - dostarcza szczegółowych informacji o zainstalowanym sprzęcie i oprogramowaniu.

Więcej informacji oraz link umożliwiający pobranie tego składnika można znaleźć na poświęconej mu stronie AVG. Aby to zrobić, wystarczy użyć linku PC Tuneup, w oknie Moje aplikacje.

8. Pasek narzędzi AVG Security Toolbar

AVG Security Toolbar to narzędzie ściśle współpracujące ze składnikiem LinkScanner. Jego zadaniem jest zapewnienie maksymalnego bezpieczeństwa podczas przeglądania internetu. Proces instalacji systemu **AVG Anti-Virus 2012** pozwala Ci zdecydować, czy chcesz zainstalować ***AVG Security Toolbar***. ***AVG Security Toolbar*** dostępny jest bezpośrednio z poziomu przeglądarki internetowej. Obecnie obsługiwane przeglądarki to: Internet Explorer (*wersja 6.0 i nowsze*), oraz Mozilla Firefox (*wersja 3.0 i nowsze*). Nie gwarantujemy działania naszego paska narzędzi w innych przeglądarkach *(jeżeli używasz jednej z alternatywnych przeglądarek, np. Avant Browser, może wystąpić jej nieprzewidziane zachowanie)*.



AVG Security Toolbar składa się z następujących elementów:

- ***Logo AVG*** wraz z menu rozwijanym:
  - ***Użyj AVG Secure Search*** - Pozwala na wyszukiwanie z poziomu paska ***AVG Security Toolbar*** przy użyciu mechanizmu ***AVG Secure Search*** . Wszystkie wyniki wyszukiwania będą na bieżąco sprawdzane przez funkcję Search-Shield, abyś mógł poczuć się absolutnie bezpiecznie.
  - ***Obecny poziom zagrożenia*** - otwiera stronę internetową laboratorium wirusów, która zawiera graficzną reprezentację obecnego poziomu zagrożeń w sieci.
  - ***Laboratoria AVG Threat Labs*** - Otwiera ***Raport*** dostępny na stronach AVG (http://www.avg.com/), który zawiera szczegółowe informacje o konkretnych zagrożeniach (wg ich nazw).
  - ***Pomoc paska narzędzi*** - Otwiera podręcznik online opisujący wszystkie funkcje paska ***AVG Security Toolbar***.
  - ***Prześlij opinię o produkcie*** - Otwiera formularz internetowy, który pozwoli Ci wyrazić swoją opinię o ***AVG Security Toolbar***.
  - ***Informacje...*** - Otwiera okno zawierające szczegóły dotyczące zainstalowanej wersji paska ***AVG Security Toolbar***.
- ***Pole wyszukiwania*** - Szukaj informacji przy użyciu paska ***AVG Security Toolbar***, aby mieć pewność, że wszystkie wyświetlone wyniki są w stu procentach bezpieczne. Wprowadź słowo lub frazę i kliknij przycisk ***Szukaj*** *(lub użyj klawisza Enter)*. Wszystkie wyniki wyszukiwania będą na bieżąco sprawdzane przez funkcję Search-Shield *(część technologii LinkScanner)*.
- Skróty umożliwiające szybki dostęp do aplikacji takich jak: ***Kalkulator***, ***Notatnik***, ***Eksplorator Windows***
- ***Pogoda*** - Przycisk otwierający nowe okno, które zawiera informacje o bieżącej pogodzie (w

miejscu Twojego pobytu), oraz prognozie na najbliższe 2 dni. Informacje te są na bieżąco aktualizowane (co 3-6 godzin). Okno pogody umożliwia również ręczną zmianę bieżącej lokalizacji oraz wybór między stopniami Celsjusza a Fahrenheita.

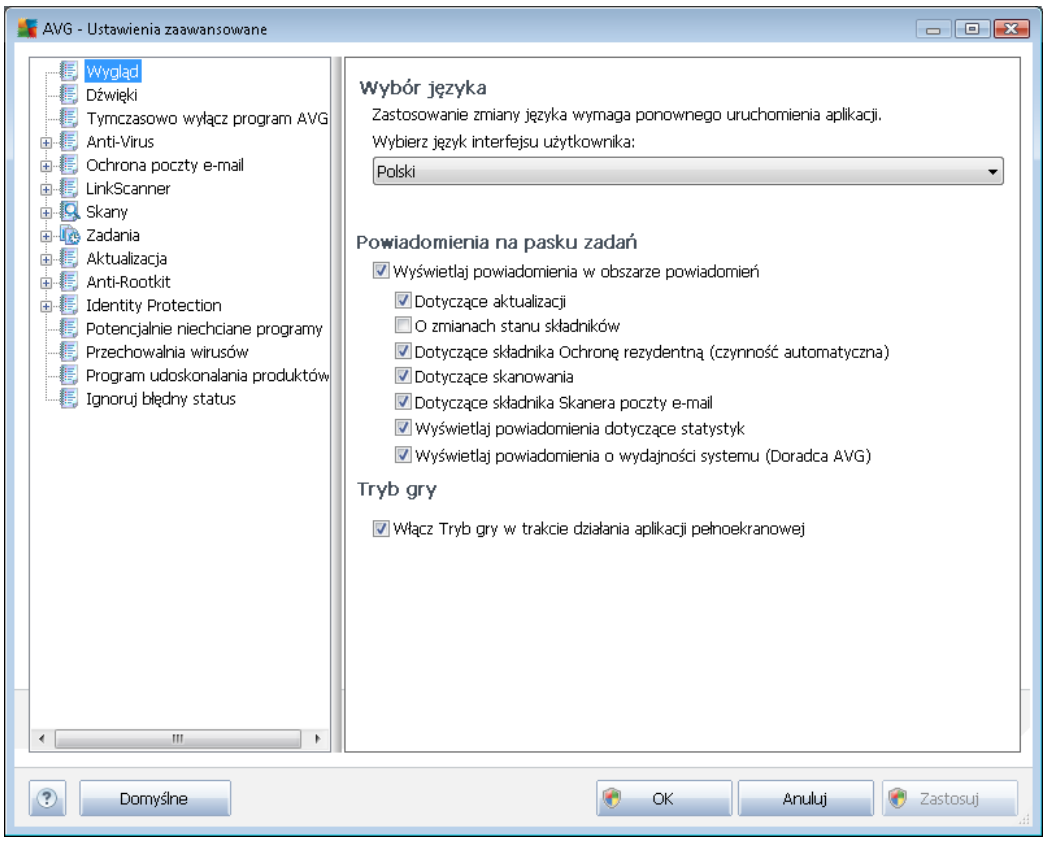
- ***Facebook*** - Przycisk pozwalający na bezpośrednie połączenie z portalem Facebook z poziomu paska ***AVG Security Toolbar*** *zachowanie.*

9. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG Anti-Virus 2012** 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 nawigacji, ***Wygląd***, odnosi się do ogólnych ustawień interfejsu użytkownika **AVG Anti-Virus 2012** oraz kilku podstawowych opcji sterujących zachowaniem aplikacji:

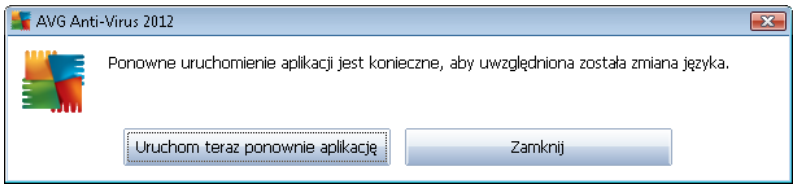


Wybór języka

W sekcji ***Wybór języka*** z rozwijanego menu można wybrać język aplikacji. Wybrany język będzie używany w całym interfejsie użytkownika **AVG Anti-Virus 2012**. Menu rozwijane zawiera tylko języki wybrane podczas instalacji (*patrz rozdział Opcje niestandardowe*) i język angielski (*instalowany domyślnie*). Przełączenie aplikacji **AVG Anti-Virus 2012** na inny język wymaga ponownego uruchomienia interfejsu użytkownika. Wykonaj następujące kroki:

- Wybierz żądany język z menu rozwijanego

- Potwierdź wybór, klikając przycisk ***Zastosuj*** button *(prawy dolny róg okna)*
- Kliknij przycisk ***OK***, aby potwierdzić.
- Pojawi się wówczas komunikat informujący o konieczności restartu aplikacji **AVG Anti-Virus 2012**
- Kliknij przycisk ***Uruchom aplikację ponownie***, aby zgodzić się na restart i poczekać kilka sekund na zastosowanie zmian:



Powiadomienia na pasku zadań

W tym obszarze można wyłączyć wyświetlane w dymkach powiadomienia dotyczące stanu aplikacji **AVG Anti-Virus 2012**. Domyślnie wszystkie powiadomienia są wyświetlane. Stanowczo nie zaleca się zmiany tego ustawienia bez uzasadnionej przyczyny! Powiadomienia informują m.in. o rozpoczęciu testu lub aktualizacji, oraz o zmianie stanu któregokolwiek ze składników **AVG Anti-Virus 2012**. Z reguły warto zwracać na nie uwagę.

Jeśli jednak z jakiegoś powodu zdecydujesz, że nie chcesz być w ten sposób informowany, lub że interesują Cię tylko niektóre powiadomienia *(związane z konkretnym składnikiem AVG Anti-Virus 2012)*, możesz zdefiniować swoje preferencje poprzez zaznaczenie odpowiednich pól:

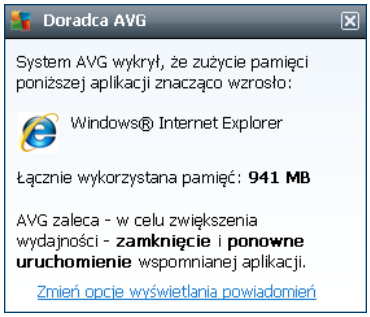
- ***Wyświetlaj powiadomienia w obszarze powiadomień*** *(domyślnie włączone)* - będą wyświetlane wszystkie powiadomienia. Odznaczenie tej opcji powoduje całkowite wyłączenie wszystkich powiadomień. Po włączeniu tej opcji można bardziej szczegółowo określić, jakie powiadomienia mają być wyświetlane:
  - ***Wyświetlaj w obszarze powiadomień komunikaty dotyczące aktualizacji*** *(domyślnie włączone)* - wyświetlane będą powiadomienia dotyczące uruchomienia, postępu i zakończenia aktualizacji systemu **AVG Anti-Virus 2012**.
  - ***Wyświetlaj powiadomienia o zmianach stanu składników*** *(domyślnie wyłączone)* - wyświetlane będą powiadomienia o włączeniu/wyłączeniu, oraz o ewentualnych problemach dotyczących składników. W przypadku zgłoszenia błędnego stanu składnika, funkcja ta zareaguje zmieniając kolory ikony na pasku zadań, co będzie wskazywało na problemy z którymś ze składników systemu **AVG Anti-Virus 2012**.
  - ***Wyświetlaj w obszarze powiadomień komunikaty dotyczące Ochrony rezydentnej (akcja automatyczna)*** *(domyślnie włączone)* - wyświetlane będą informacje dotyczące zapisywania, kopiowania i otwierania plików (*ta konfiguracja jest dostępna tylko, jeśli włączona jest opcja automatycznego leczenia Ochrony rezydentnej*).

- ***Wyświetlaj w obszarze powiadomień komunikaty dotyczące skanowania*** *(domyślnie włączone)* - wyświetlane będą informacje dotyczące automatycznego rozpoczęcia, postępu i zakończenia zaplanowanego skanowania.

- ***Wyświetlaj powiadomienia dotyczące Skanera poczty e-mail*** *(domyślnie włączone)* - Wyświetlane będą informacje o skanowaniu wszystkich wiadomości przychodzących i wychodzących.

- ***Wyświetlaj powiadomienia dotyczące statystyk*** *(domyślnie włączone)* - pozostaw to pole zaznaczone, aby być regularnie powiadamianym o dotychczasowych statystykach bezpieczeństwa.

- ***Wyświetlaj powiadomienia Doradcy AVG*** *(domyślnie włączone)* - **Doradca AVG** monitoruje obsługiwane przeglądarki internetowe *(Internet Explorer, Chrome, Firefox, Opera i Safari)* i informuje Cię, jeżeli zużyją nadmierną ilość pamięci. W takiej sytuacji wydajność komputera może znaczącą spaść, a najskuteczniejszym sposobem na jej przywrócenie jest restart przeglądarki. Pozostaw pole ***Wyświetlaj powiadomienia Doradcy AVG*** zaznaczone, by być stale informowanym.

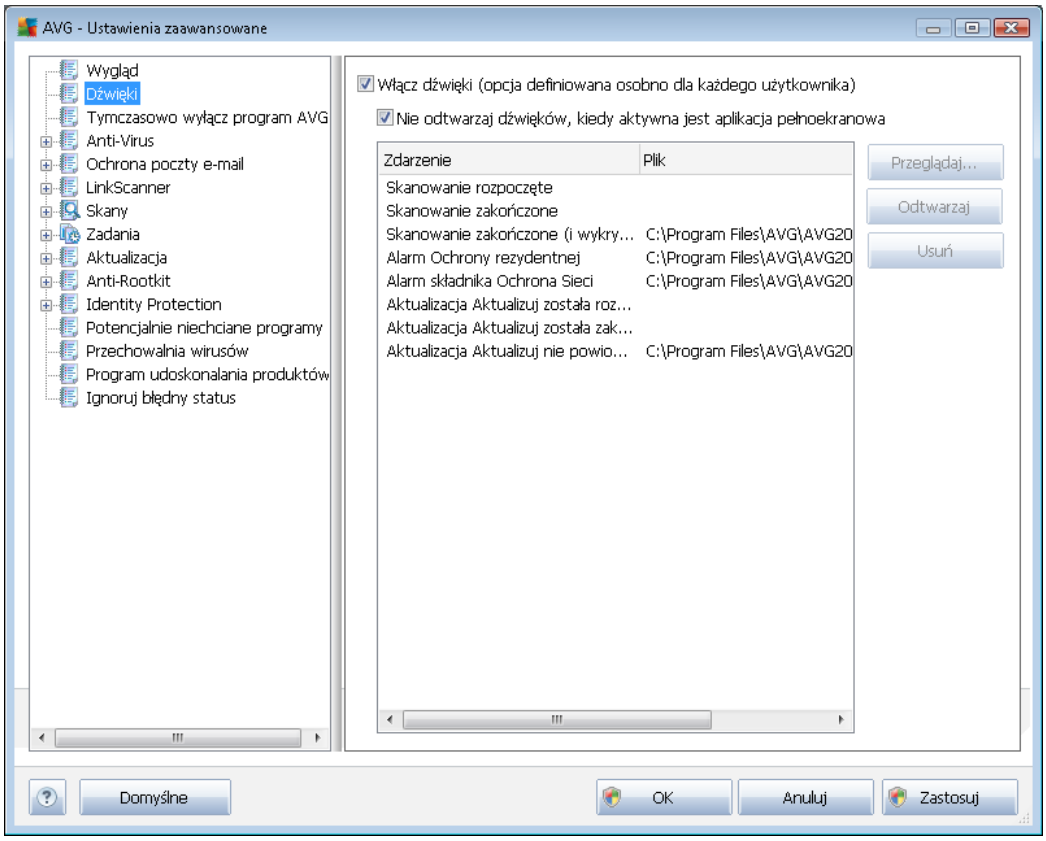


Tryb gry

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 Anti-Virus 2012** ma informować o określonych czynnościach za pomocą dźwięków:



Ustawienia obowiązują wyłącznie dla bieżącego konta użytkownika, co oznacza, że każdy użytkownik komputera może mieć własne ustawienia dźwięków. Jeżeli zgadzasz się na powiadomienia dźwiękowa, pozostaw pole ***Włącz dźwięki*** zaznaczone (*domyślnie ta opcja jest aktywna*). Możesz również zaznaczyć pole ***Nie odtwarzaj dźwięków w trakcie działania aplikacji pełnoekranowej***, by wyłączyć dźwięki wtedy, gdy mogłyby przeszkadzać *(więcej informacji znajduje się w sekcji Tryb Gry, w rozdziale Ustawienia zaawansowane / Wygląd niniejszej dokumentacji)*.

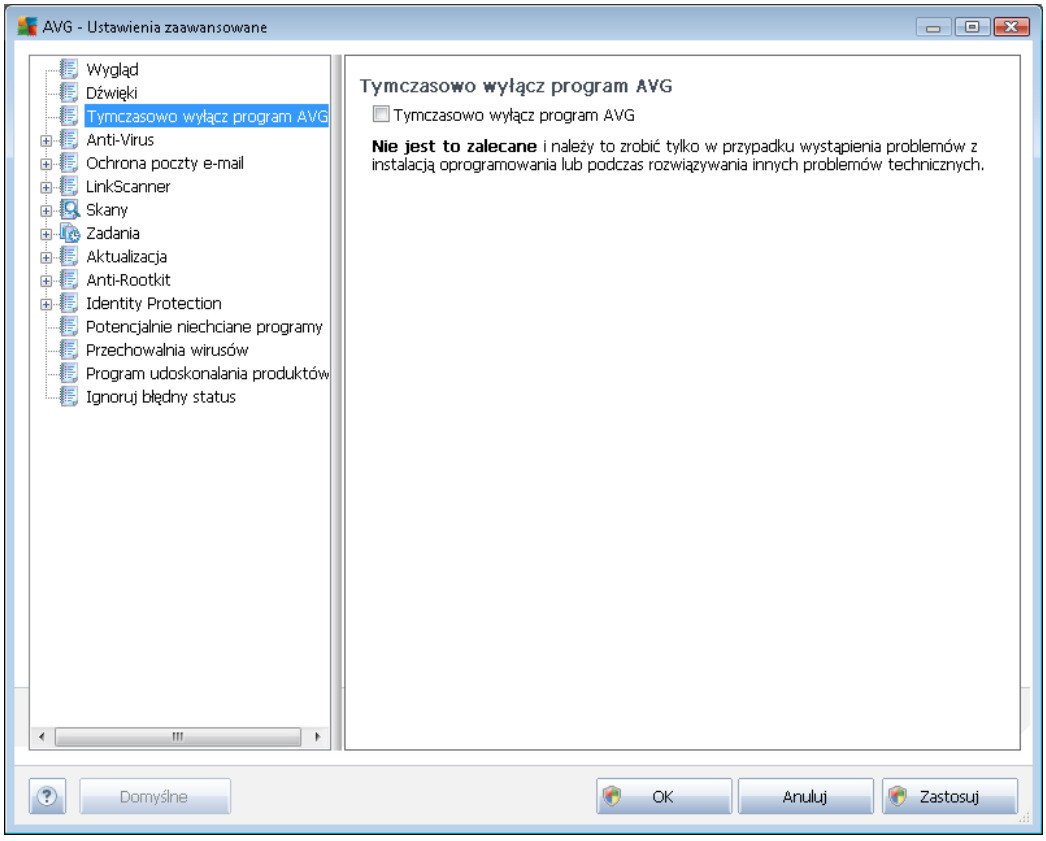
Przyciski kontrolne

- ***Przeglądaj*** - Po wybraniu konkretnego zdarzenia z listy, użyj przycisku ***Przeglądaj***, aby wskazać żądany plik dźwiękowy. *(Przypominamy, że obecnie obsługiwane są tylko pliki *.wav!)*
- ***Odtwórz*** - Aby odsłuchać wybranego dźwięku, wskaż na liście żądane zdarzenie i kliknij przycisk ***Odtwórz***.
- ***Usuń*** - Użyj przycisku ***Usuń***, aby usunąć dźwięk przypisany do danego zdarzenia.

9.3. Tymczasowo wyłącz ochronę AVG

W oknie dialogowym ***Tymczasowo wyłącz ochronę AVG*** można wyłączyć całą ochronę zapewnianą przez system **AVG Anti-Virus 2012**.

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



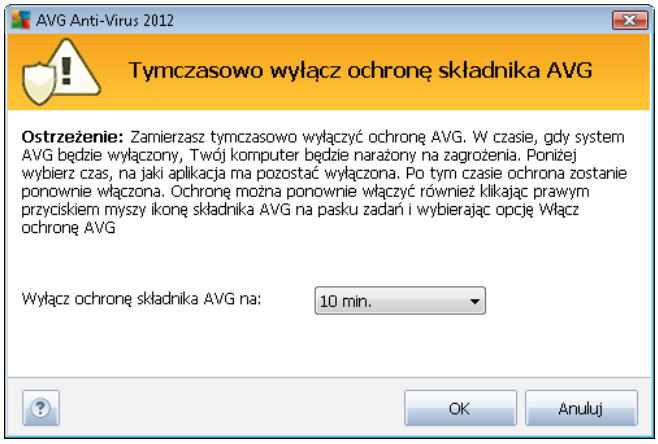
W większości przypadków ***nie jest konieczne*** wyłączanie systemu **AVG Anti-Virus 2012** przed instalowaniem nowego oprogramowania lub sterowników, nawet jeśli instalator lub kreator sugeruje uprzednie zamknięcie działających programów i aplikacji. Jeżeli jednak napotkasz problemy przy instalacji, spróbuj najpierw wyłączyć Ochronę rezydentną (pole *Włącz Ochronę rezydentną*) first. Jeśli jednak tymczasowe wyłączenie systemu **AVG Anti-Virus 2012** jest konieczne, należy go włączyć ponownie gdy tylko będzie to możliwe. Jeśli oprogramowanie antywirusowe jest wyłączone, komputer podłączony do internetu jest narażony na ataki, przed którymi nie będzie chroniony.

Jak wyłaczyć ochronę AVG

- Zaznacz pole ***Tymczasowo wyłącz ochronę AVG***, a następnie potwierdź swoją decyzję, klikając przycisk ***Zastosuj***

- Określ w nowo otwartym oknie ***Tymczasowo wyłącz ochronę AVG*** na jak długo chcesz wyłączyć system **AVG Anti-Virus 2012**. Domyślnie ochrona pozostanie nieaktywna przez 10 minut, co powinno wystarczyć na wykonanie przeciętnego zadania, np. instalację

nowego oprogramowania itp. Należy pamiętać, że wstępny limit czasu, który można ustawić, to 15 minut i wartość ta nie może zostać zmieniona z przyczyn bezpieczeństwa. Po upłynięciu określonego czasu, wszystkie składniki zostaną ponownie aktywowane.

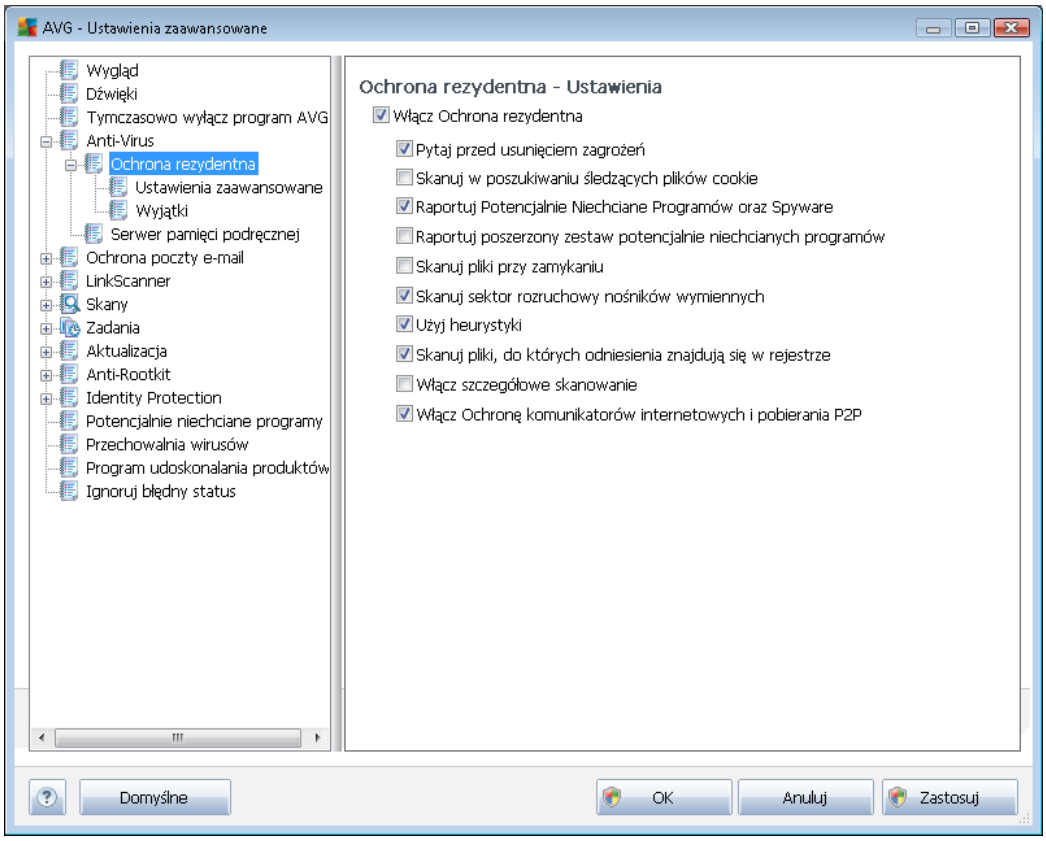


9.4. Anti-Virus

Wprowadź w tym miejscu temat.

9.4.1. Ochrona rezydentna

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*).

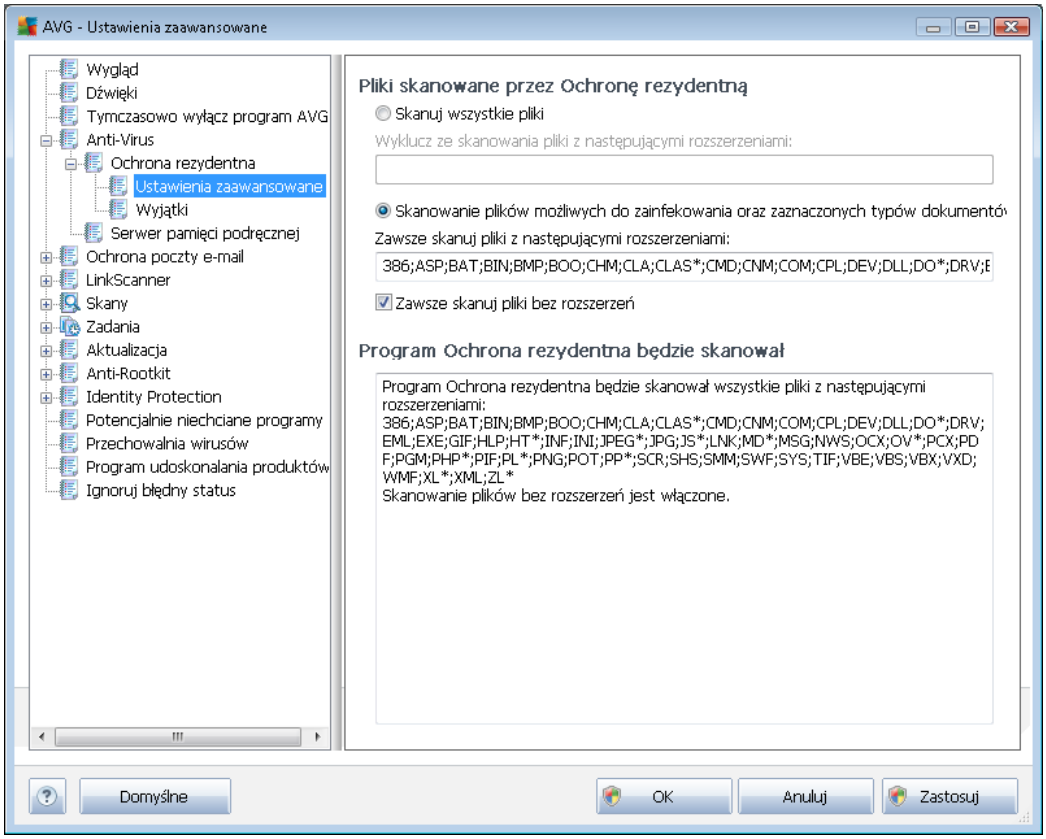
- ***Usuwaj wszystkie zagrożenia automatycznie*** (*opcja domyślnie wyłączona*) - każda wykryta infekcja będzie automatycznie leczona. Wszystkie infekcje, których nie uda się wyleczyć, będą usuwane.

- ***Skanuj pliki wymienione 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.

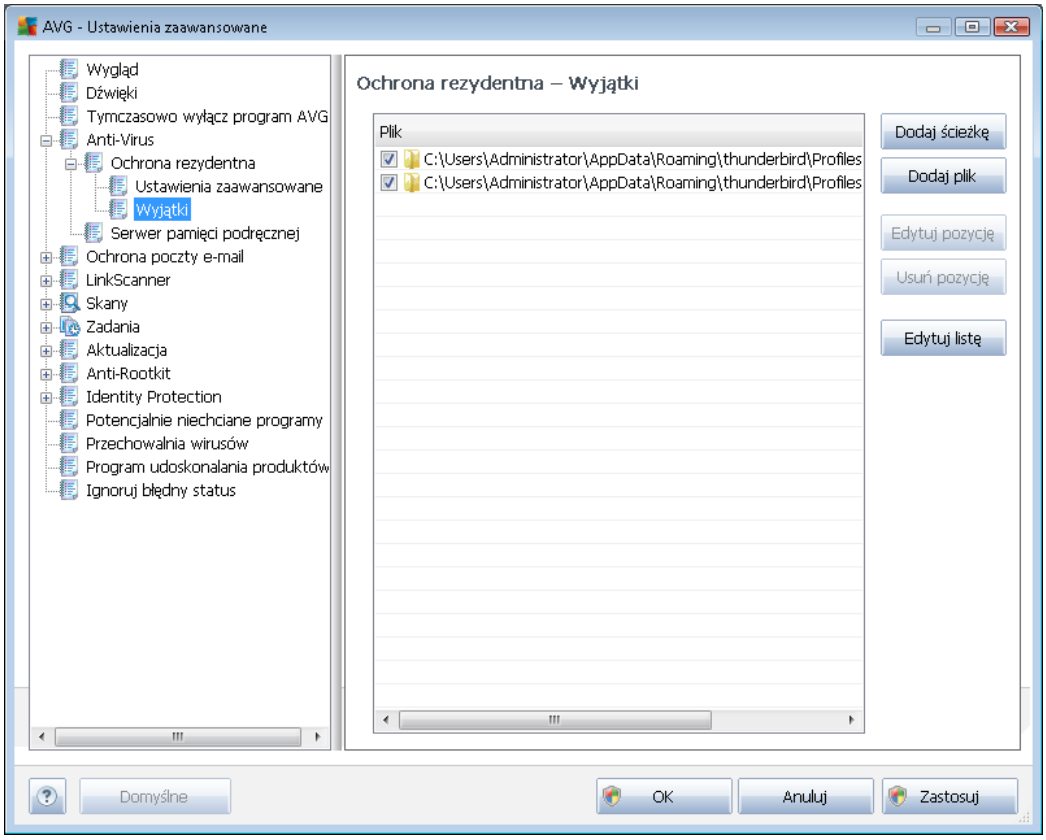
- ***Włącz Ochronę komunikatorów internetowych i pobierania P2P*** (*opcja domyślnie włączona*) - Zaznacz to pole, aby zapewnić ochronę komunikatorów internetowych (*np. ICQ, MSN Messenger, ...*) i programów P2P .

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



Zaznacz odpowiednie pole, w zależności od tego, czy chcesz skanować ***wszystkie pliki*** czy ***tylko pliki infekowalne i niektóre typy dokumentów***. Jeśli wybrałeś drugą opcję, 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***.



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!

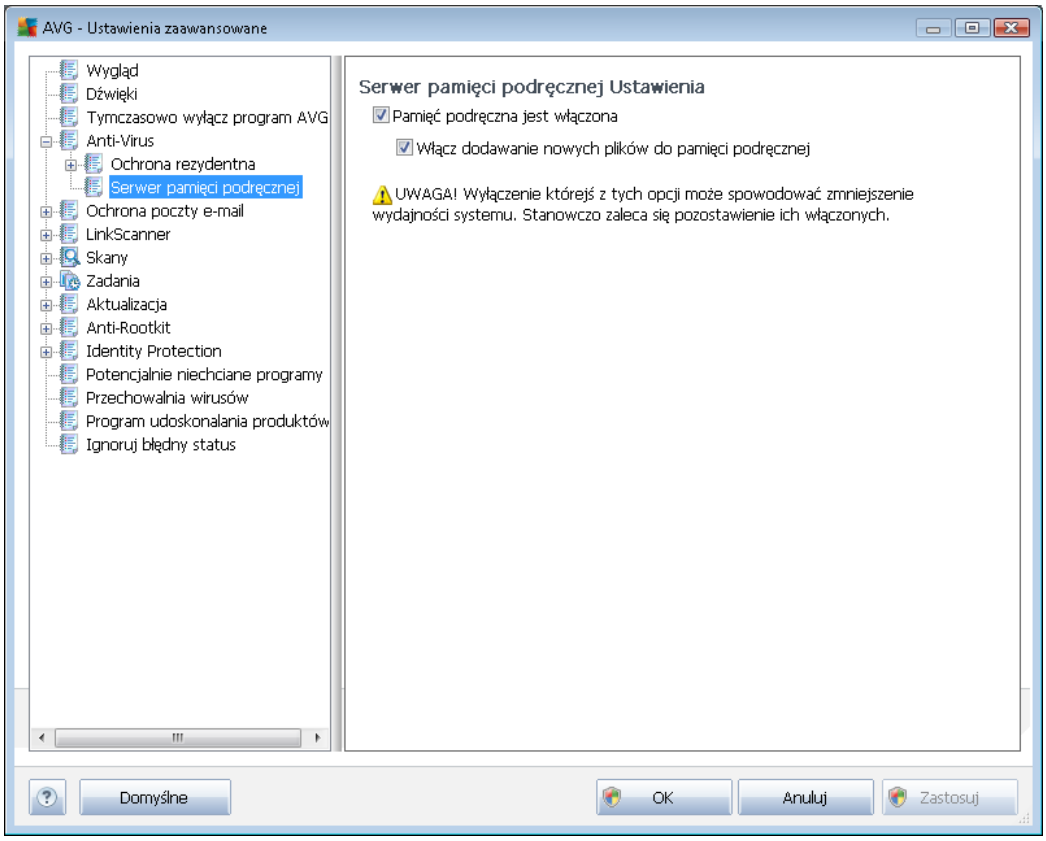
Przyciski kontrolne

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.
- ***Edytuj listę*** - umożliwia edycję listy wyjątków w nowym oknie, które zawiera standardowe pole tekstowe.

9.4.2. Serwer pamięci podręcznej

Okno ***Ustawienia serwera pamięci podręcznej*** odnosi się do procesu serwera pamięci podręcznej, który ma za zadanie przyspieszenie wszystkich testów **AVG Anti-Virus 2012**:



Zbiera on i przechowuje informacje o zaufanych plikach (*tych, które zostały podpisane cyfrowo przez znane źródło*). Pliki takie są automatycznie uznawane za bezpieczne, więc nie muszą być powtórnie skanowanie i mogą zostać pominięte.

Okno ***Ustawienia serwera pamięci podręcznej*** zawiera następujące 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.

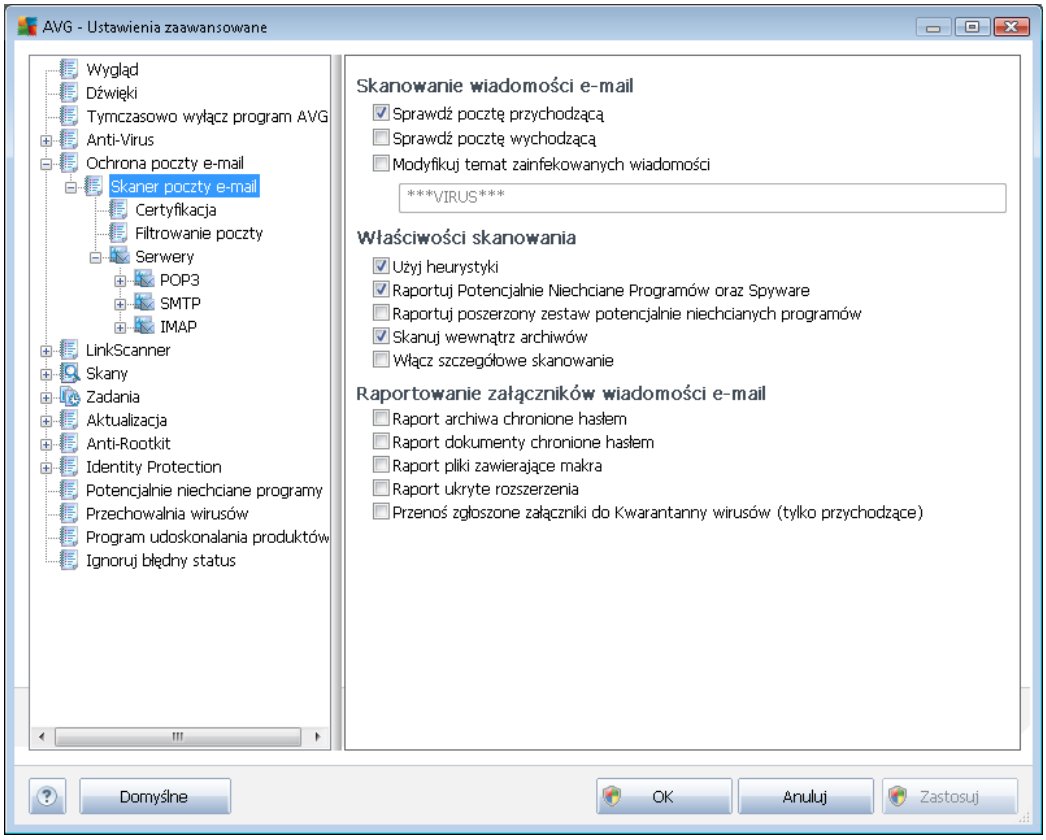
Jeśli nie posiadasz ku temu ważnego powodu, stanowczo odradzamy wyłączanie serwera pamięci podręcznej! Unikniesz dzięki temu znacznego obniżenia wydajności systemu.

9.5. Ochrona poczty e-mail

W sekcji ***Ochrona poczty e-mail*** możesz edytować konfigurację składników Skaner poczty e-mail oraz Anti-Spam:

9.5.1. Skaner poczty

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.

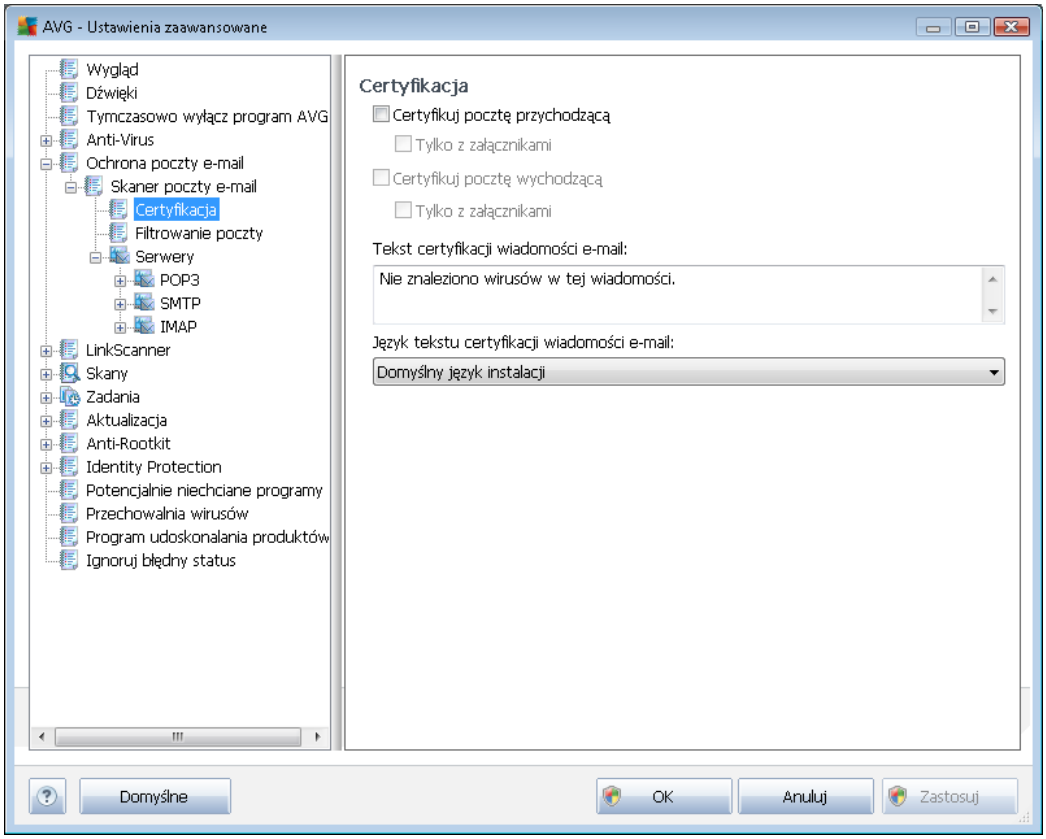
- ***Raportuj dokumenty chronione hasłem*** - dokumentów chronionych hasłem nie można skanować w poszukiwaniu wirusów. Należy zaznaczyć to pole wyboru, aby system AVG zgłaszał je jako potencjalnie niebezpieczne.

- ***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.

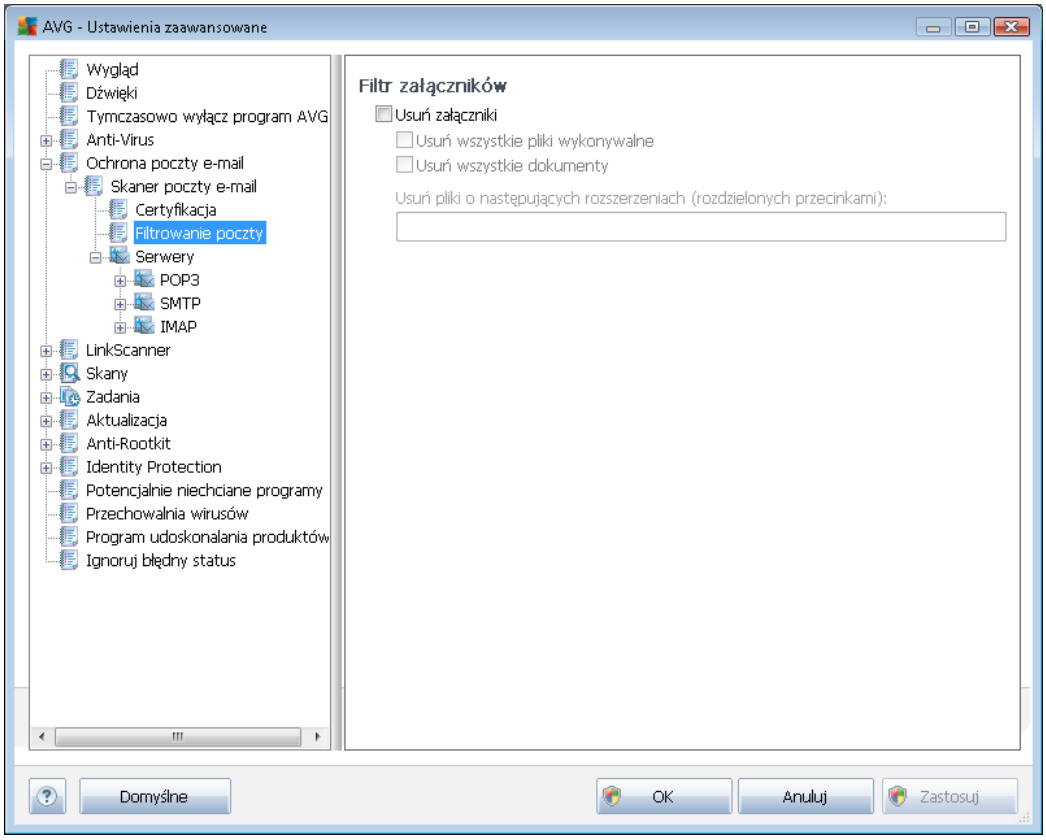
- ***Przenoś raportowane załączniki do Przechowalni wirusów*** - możesz skonfigurować system AVG tak, aby powiadamiał Cię poprzez e-mail o wykrytych archiwach i dokumentach zabezpieczonych hasłem, plikach zawierających makra lub ukrytych rozszerzeniach, które zostaną wykryte w załącznikach skanowanych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

W oknie ***Certyfikacja*** znajdują się opcje pozwalające włączyć lub wyłączyć ***Certyfikację poczty przychodzącej*** i ***wychodzącej***. Zaznaczenie parametru ***Tylko z załącznikami*** sprawi, że certyfikowane będą jedynie wiadomości zawierające załączniki:



Domyślnie, tekst certyfikacji stwierdza po prostu, że *Nie znaleziono wirusów w tej wiadomości.* Treść tą można jednak łatwo zmienić, korzystając z pola ***Tekst certyfikacji wiadomości e-mail***. Sekcja ***Język tekstu certyfikacji wiadomości e-mail*** pozwala na zmianę języka automatycznie generowanej części certyfikacji (*Nie znaleziono wirusów w tej wiadomości*).

Uwaga: *We wskazanym języku będzie wyświetlany jedynie domyślny tekst certyfikacji. Część zdefiniowana przez użytkownika nie zostanie automatycznie przetłumaczona!*



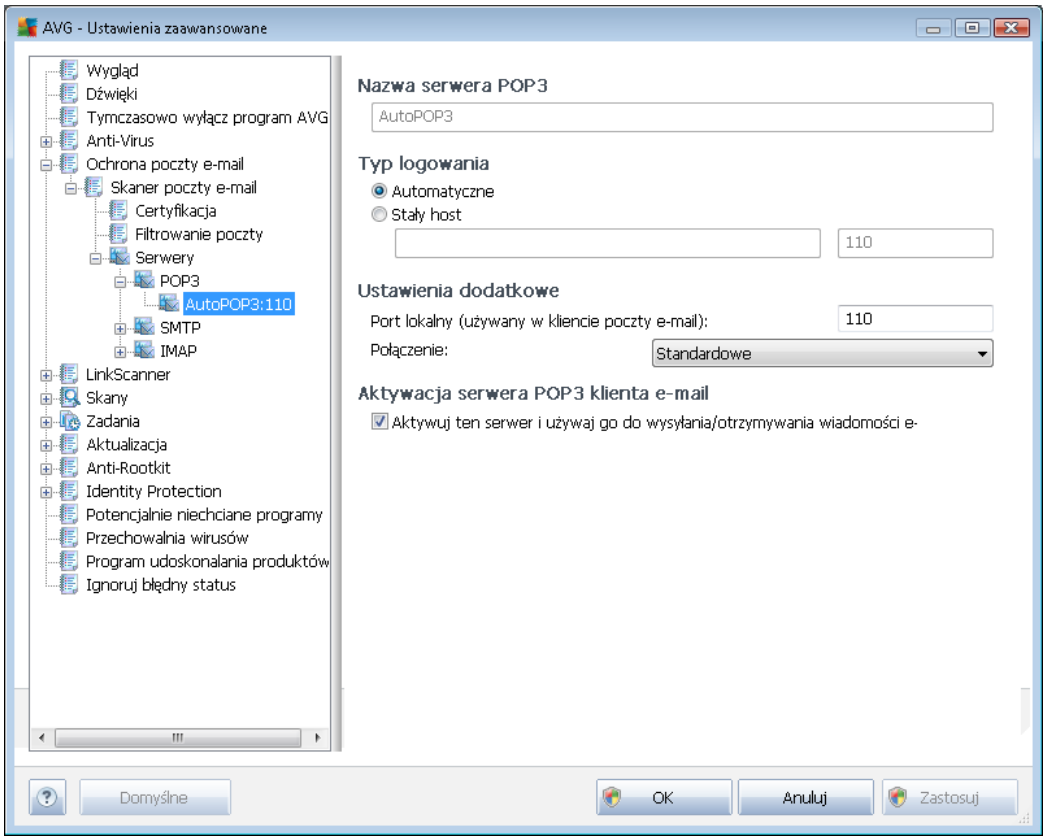
W oknie ***Filtr załączników*** można ustawiać parametry skanowania załączników e-mail. Opcja ***Usuń załączniki*** jest domyślnie wyłączona. Jeśli zostanie włączona, wszystkie załączniki wiadomości zidentyfikowane jako zainfekowane lub potencjalnie niebezpieczne, będą automatycznie usuwane. Aby określić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

W sekcji ***Serwery*** edytować można parametry serwerów Skanera poczty e-mail:

- Serwer POP3
- Serwer SMTP
- Serwer IMAP

Dodanie nowe serwera poczty wychodzącej lub przychodzącej możliwe jest za pomocą przycisku ***Dodaj nowy serwer***.

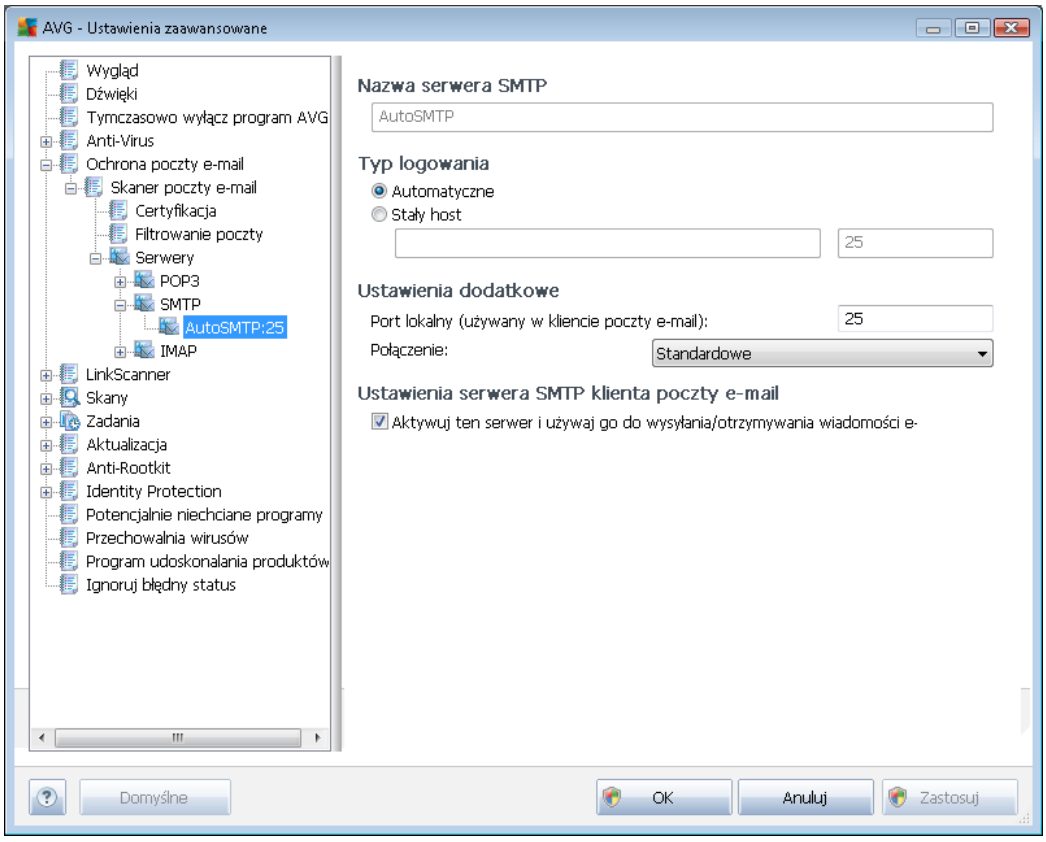


W tym oknie dialogowym (*dostępnym z menu **Serwery / POP3***) można zdefiniować nowy Skaner poczty e-mail serwer poczty przychodzącej, korzystający z protokołu POP3:

- ***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.

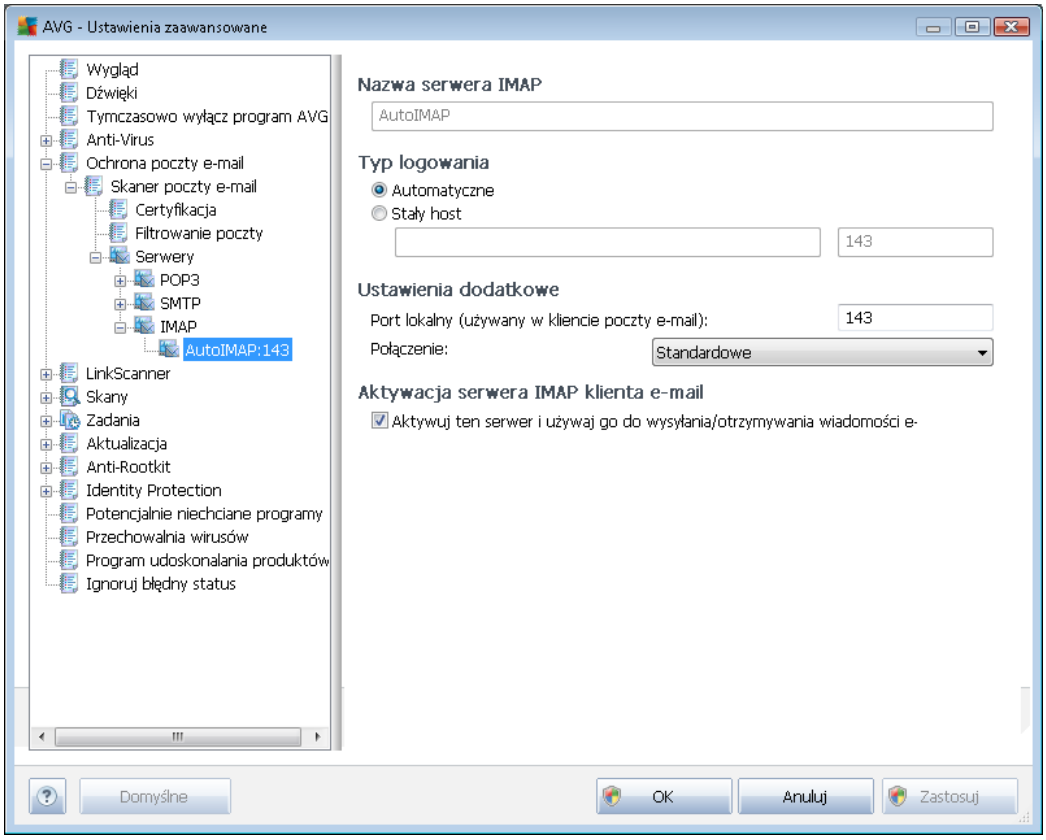
- ***Ustawienia dodatkowe*** - pozwalają zdefiniować bardziej szczegółowe parametry:
    - ***Port lokalny*** - określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w kliencie poczty jako port docelowy serwera POP3.
    - ***Połączenie*** - z menu rozwijanego należy wybrać 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.

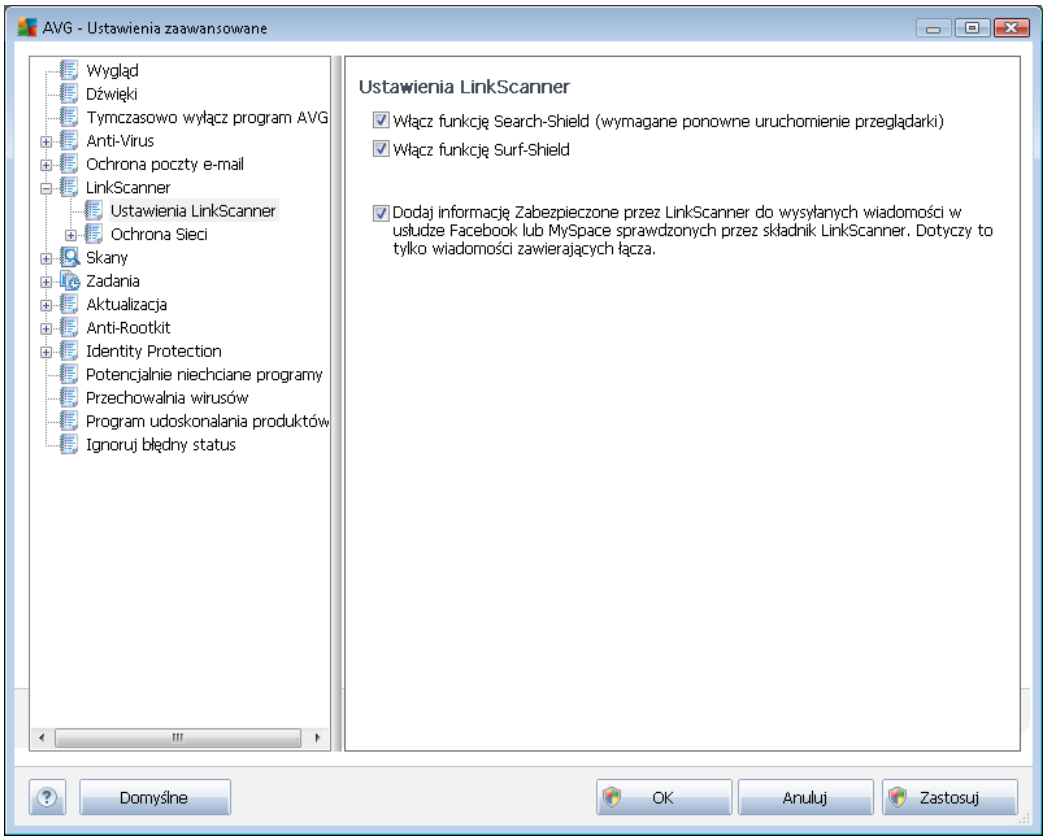
- ***Połączenie*** - z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślne SSL*). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko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

- ***Aktywacja serwera IMAP klienta poczty e-mail*** - zaznacz to pole, aby włączyć określony powyżej serwer IMAP.

9.6. LinkScanner

9.6.1. Ustawienia LinkScannera

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

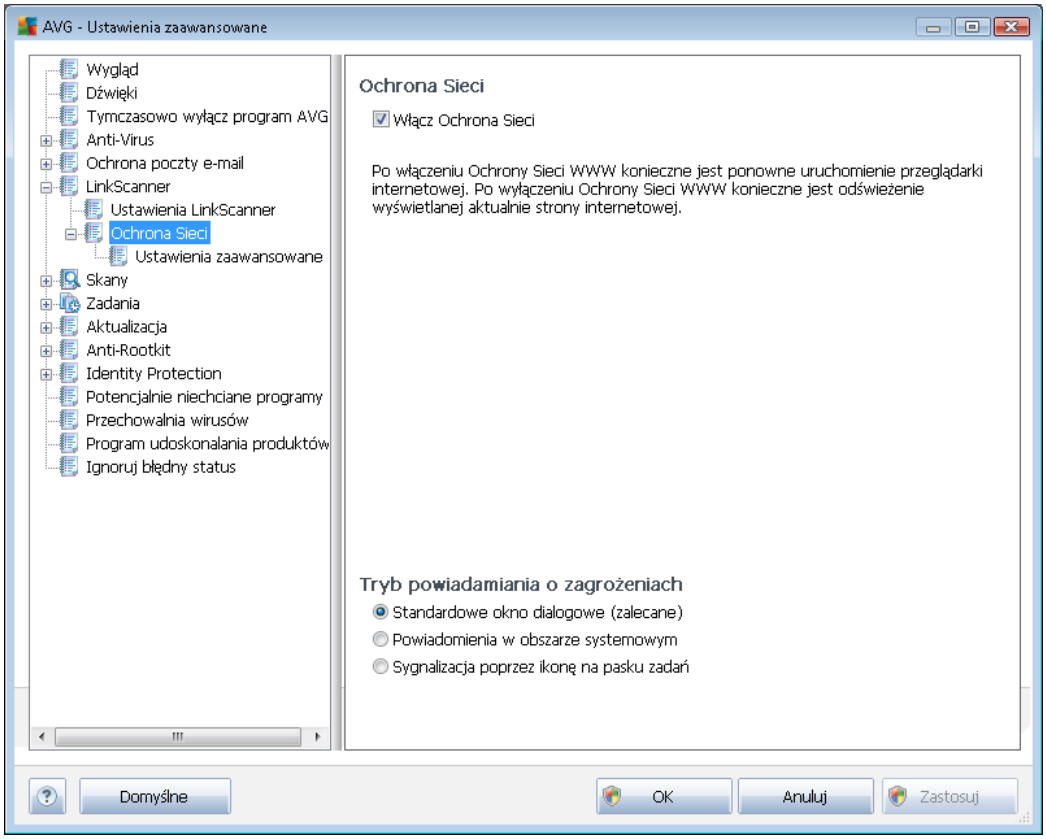


- ***Włącz funkcję Search-Shield*** (*opcja domyślnie włączona*) - skanuje wszystkie linki pojawiające się w wynikach wyszukiwania zwracanych przez serwisy Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg oraz SlashDot, a następnie obok każdego 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 'Zabezpieczone przez LinkScanner' ...*** - (*domyślnie włączone*): zaznacz to pole, jeśli chcesz dołączyć informację o skanie przeprowadzonym przez składnik LinkScanner do każdej wiadomości zawierającej linki, wysłanej za pośrednictwem sieci społecznościowych Facebook i MySpace.

9.6.2. Ochrona Sieci



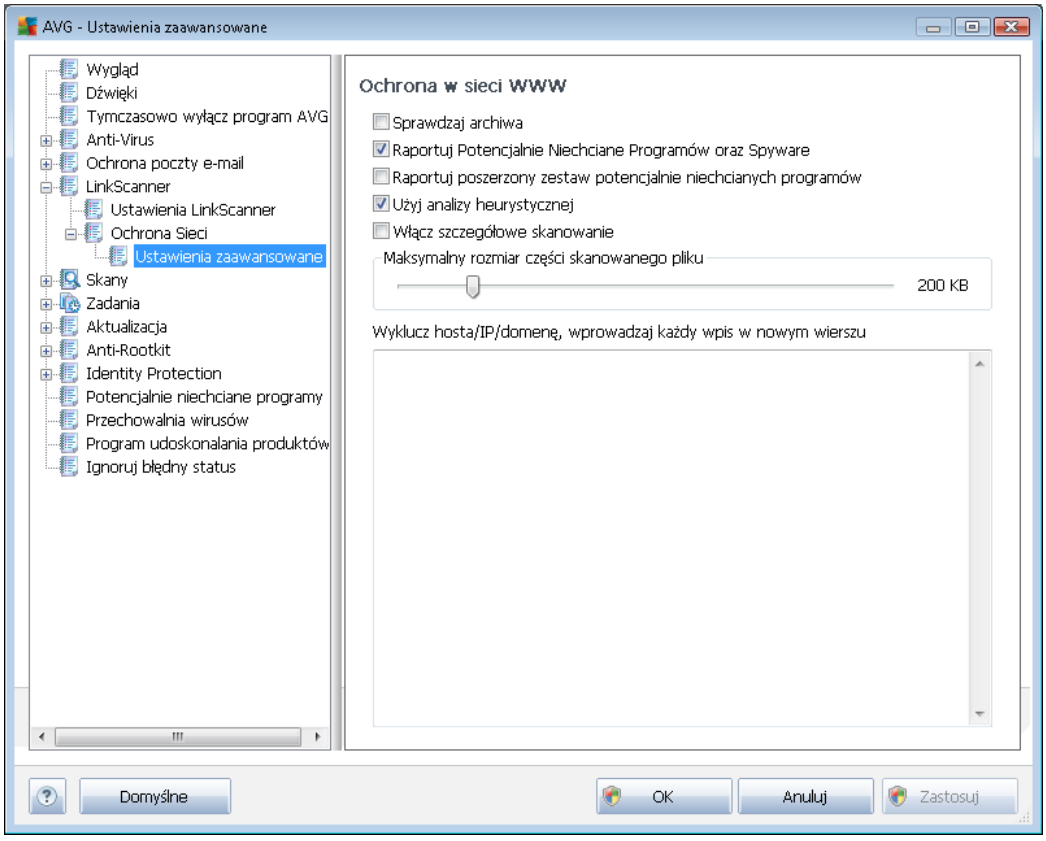
Okno ***Ochrona Sieci*** zawiera następujące opcje:

- ***Włącz Ochronę Sieci*** *(domyślnie włączona)* - Włącza/wyłącza wszystkie usługi składnika ***Ochrona Sieci***. Zaawansowane ustawienia ***Ochrony Sieci*** znajdują się w kolejnym oknie, nazwanym Web Protection.

- ***Włącz AVG Accelerator*** *(domyślnie włączony)* - Włącza/wyłącza ***AVG Accelerator*** - usługę umożliwiającą płynniejsze odtwarzanie filmów online i łatwiejsze pobieranie dodatkowych plików.

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.



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 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.

- ***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.

9.7. 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.

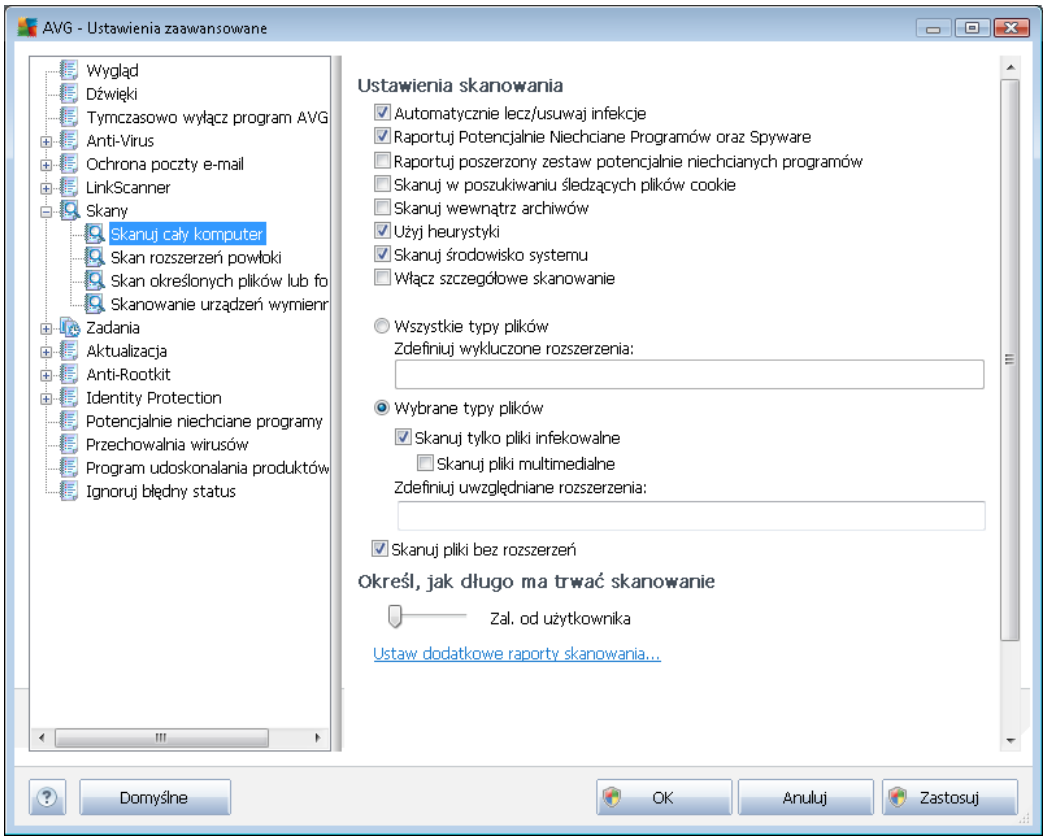
- ***Skan określonych plików lub folderów*** - standardowe, zdefiniowane wstępnie skanowanie wskazanych obszarów komputera

- ***Skan urządzeń wymiennych*** - skanowanie urządzeń wymiennych podłączonych do

komputera.

9.7.1. 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 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 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.

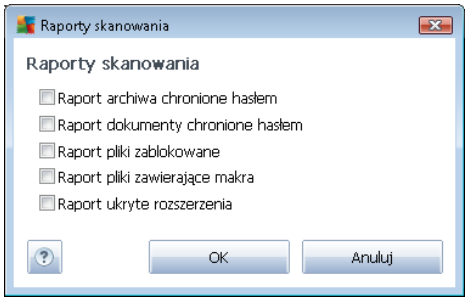
- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** - ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

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.

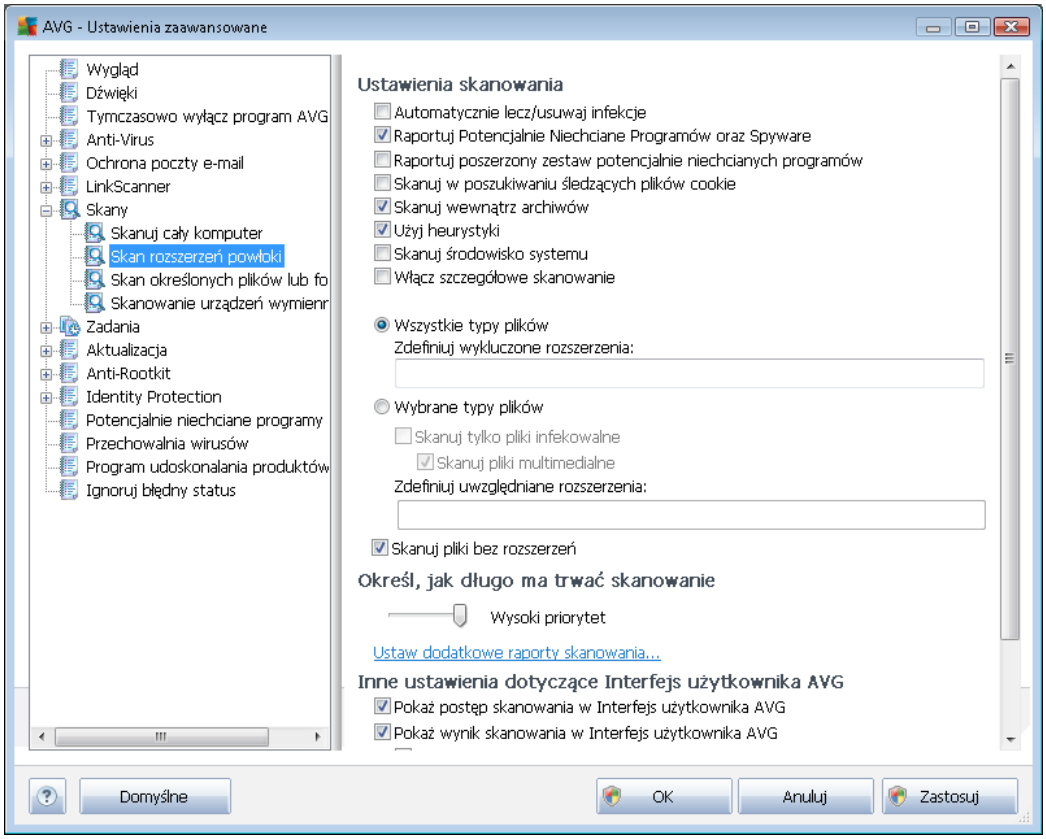
Ustaw dodatkowe raporty skanowania...

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



9.7.2. 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:



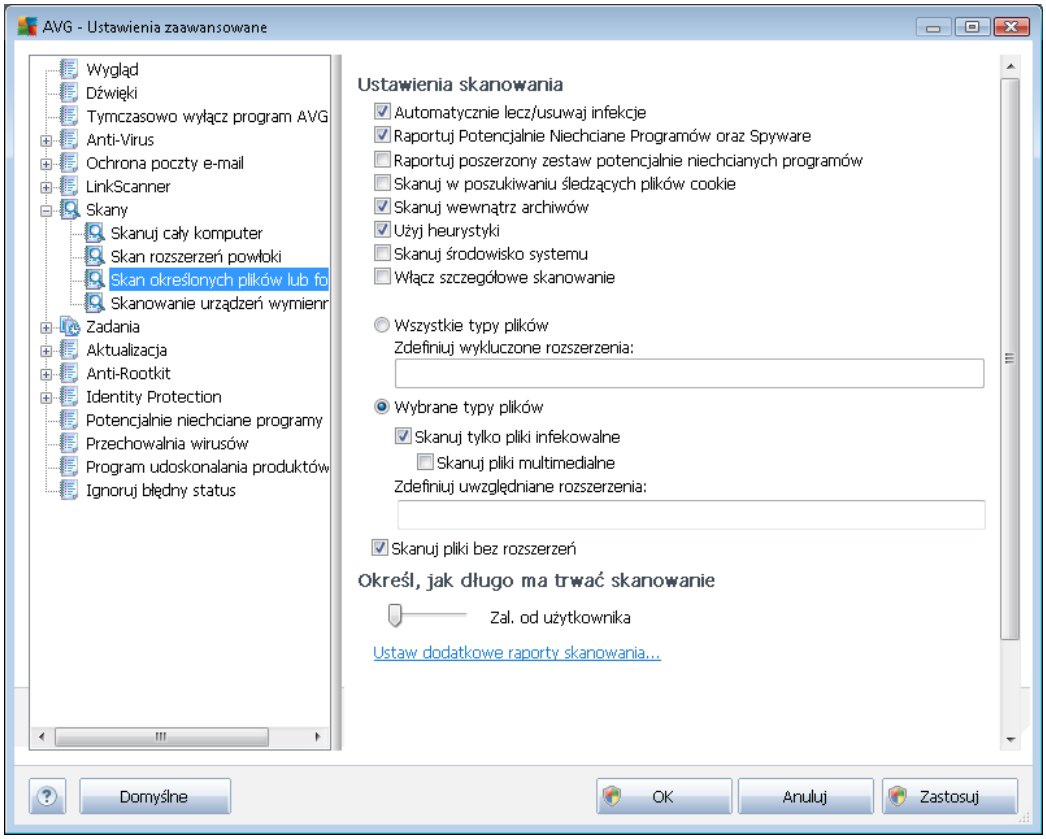
Lista parametrów jest identyczna jak dla testu Skan całego komputera. Jednak ustawienia domyślne obu skanów różnią się (*np. skan całego komputera nie sprawdza archiwów, lecz skanuje środowisko systemowe, podczas gdy Skan rozszerzenia powłoki - odwrotnie*).

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

Podobnie jak w przypadku Skanu całego komputera, okno dialogowe ***Skanu 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.

9.7.3. 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:

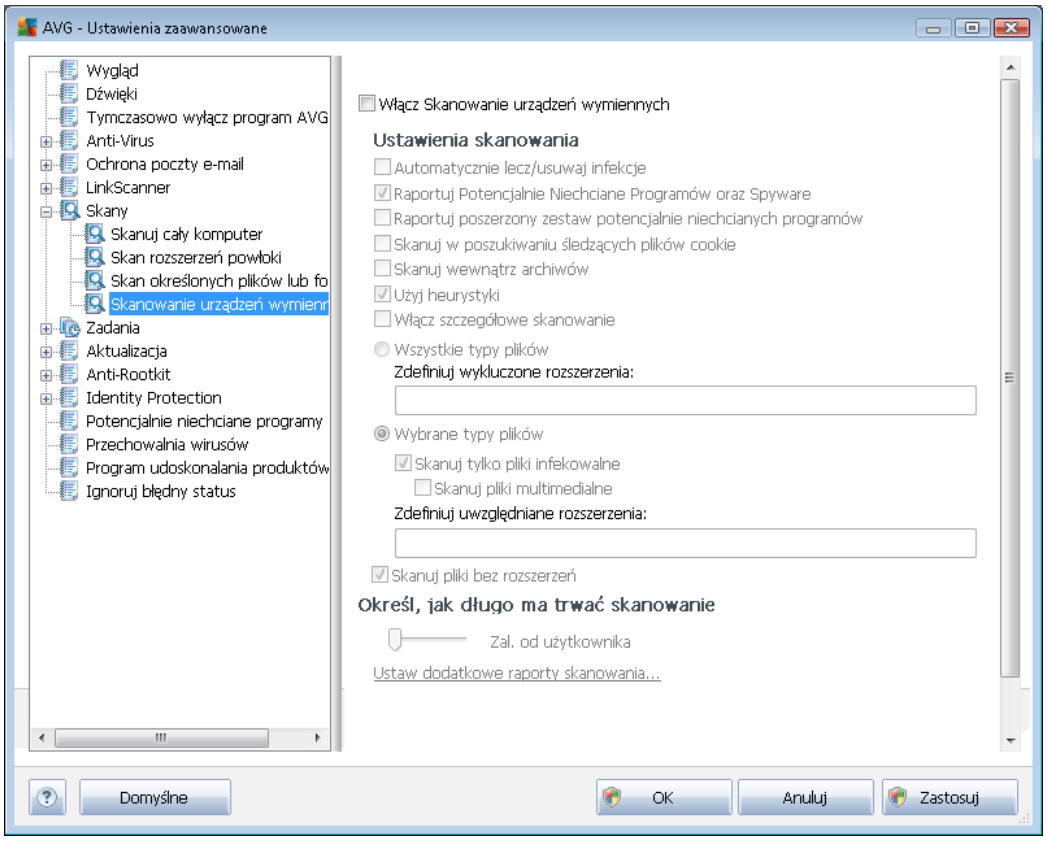


Wszystkie parametry ustawiane w tym oknie dialogowym odnoszą się tylko do obszarów wybranych do skanowania określonych plików lub folderów!

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

9.7.4. Skanowanie 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.*

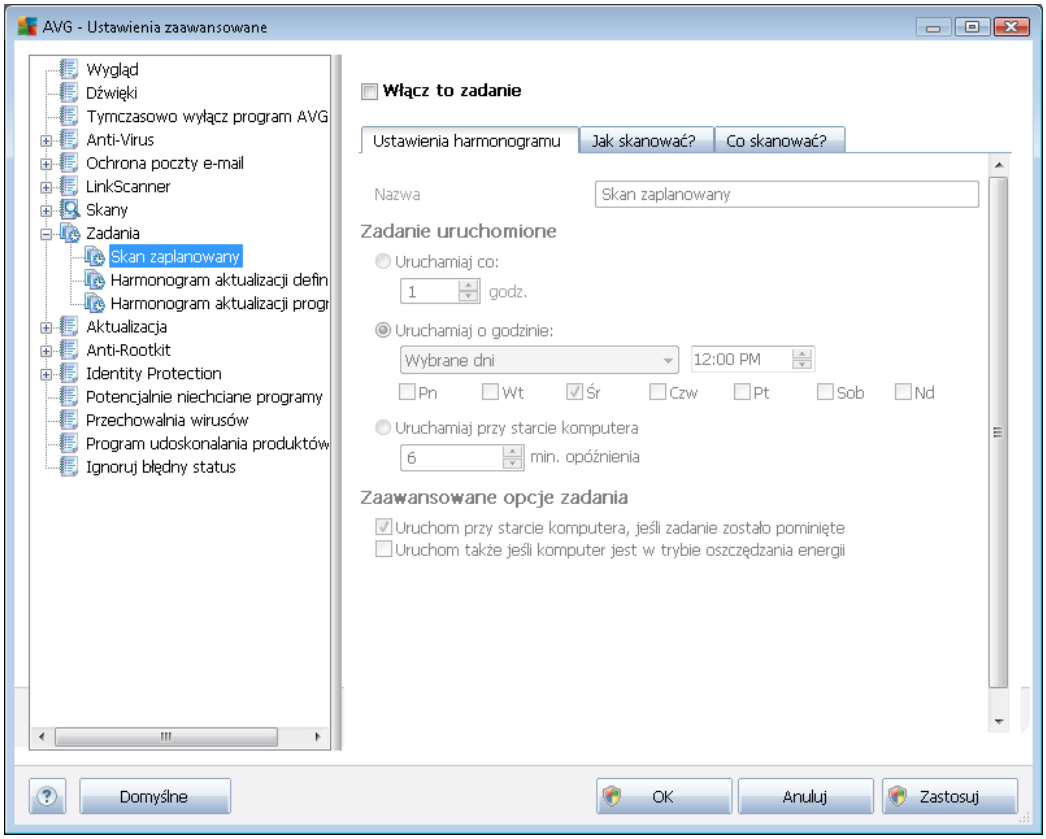
9.8. Zaplanowane zadania

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

- Skan zaplanowany
- Harmonogram aktualizacji definicji
- Harmonogram aktualizacji programu

9.8.1. Skan zaplanowany

Parametry zaplanowanego skanu można edytować (*podobnie jak przy tworzeniu nowego harmonogramu*) na trzech kartach. Na każdej karcie można zaznaczyć/odznaczyć pole ***Włącz to zadanie***, 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:

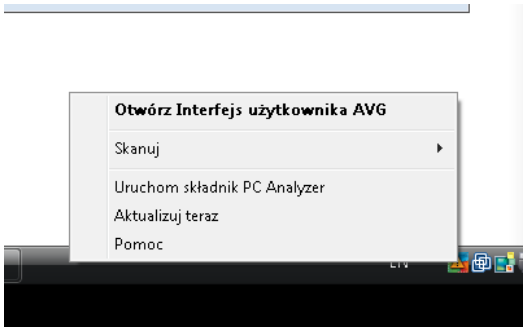
Zadanie uruchomione

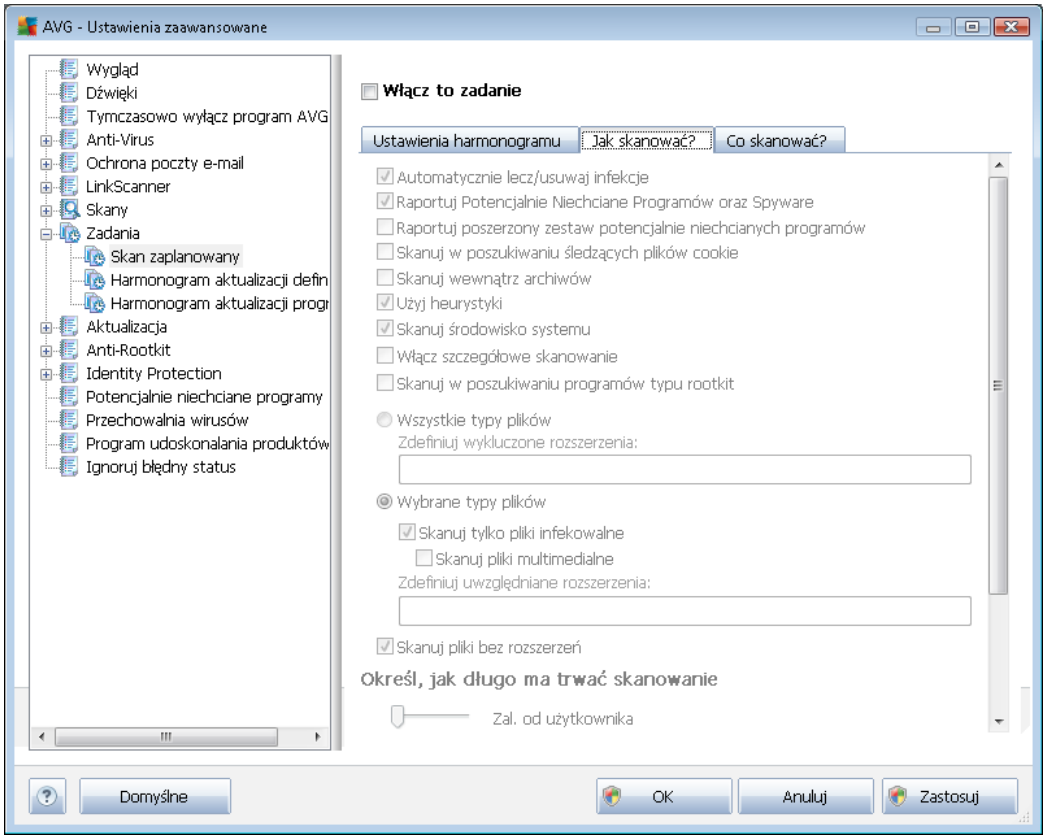
W tym miejscu można określić, jak często ma być uruchamiane nowe skanowanie. Uruchamianie skanowania może być powtarzane w określonych odstępach czasu (***Uruchamiaj co...***) lub w zadanych momentach (***Uruchamiaj o określonej godzinie...***), a także na skutek wystąpienia określonego zdarzenia (***Akcja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

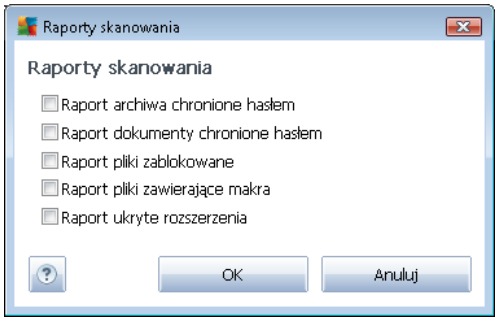
- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** - ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

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.

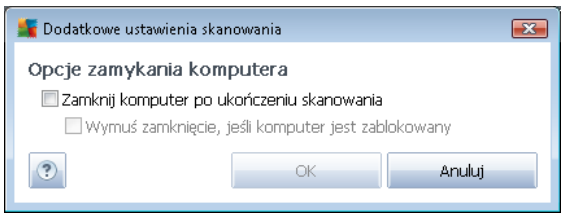
Ustaw dodatkowe raporty skanowania

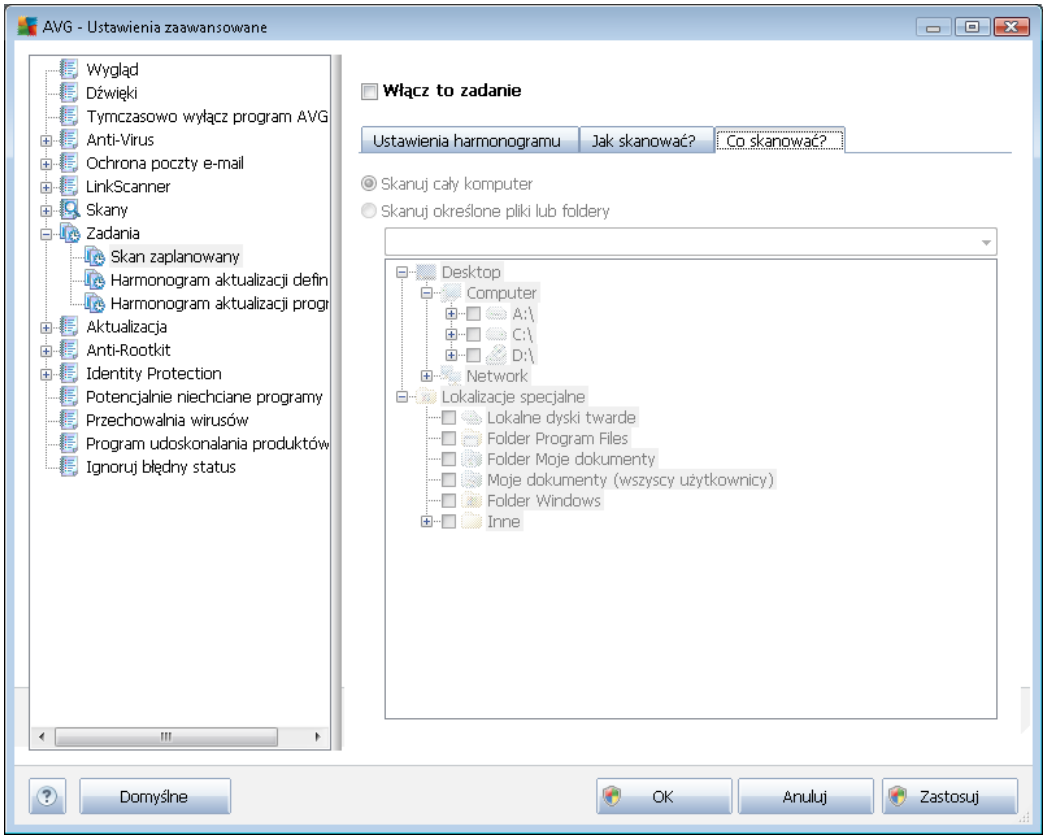
Kliknięcie linku ***Ustaw dodatkowe raporty skanowania...*** spowoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym można określić szczegółowość raportów, zaznaczając żądane elementy:



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***).

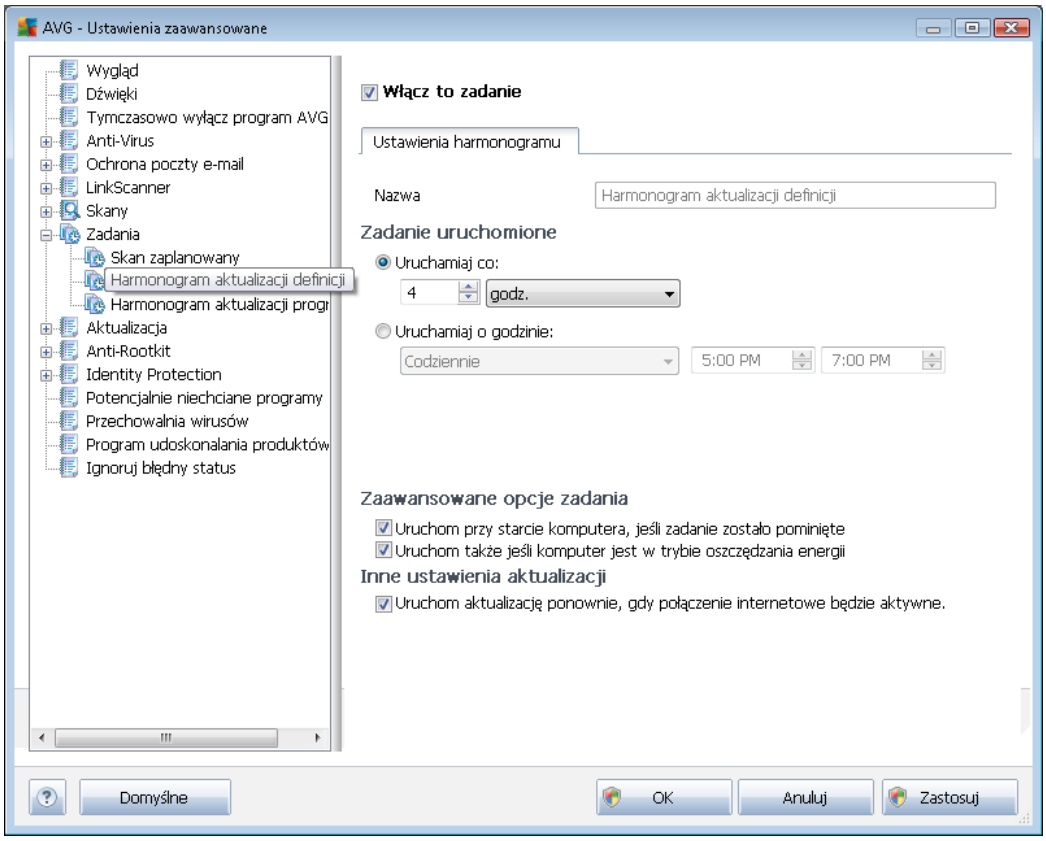




Na karcie ***Co skanować?*** można określić, czy planowane jest skanowanie całego komputera, czy skanowanie określonych plików lub folderów. W przypadku skanowania określonych plików lub folderów, w dolnej części okna dialogowego aktywowane jest drzewo katalogów, w którym można wybrać obiekty do przeskanowania.

9.8.2. Harmonogram aktualizacji definicji

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



W tym oknie dialogowym można ustawić szczegółowe parametry harmonogramu aktualizacji. W polu tekstowym ***Nazwa*** (*nieaktywne 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

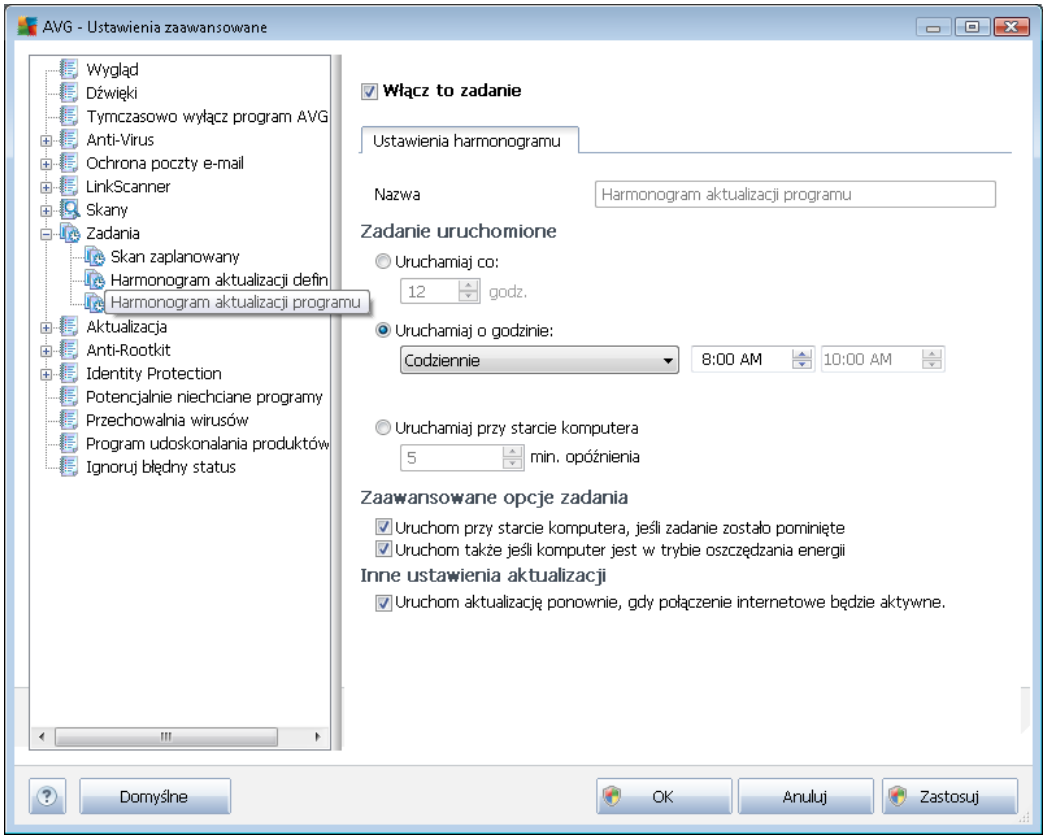
Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji programu w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

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*).

9.8.3. Harmonogram aktualizacji programu

Jeśli ***jest to naprawdę konieczne***, tymczasowo można dezaktywować zaplanowaną aktualizację programu, odznaczając pole ***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.

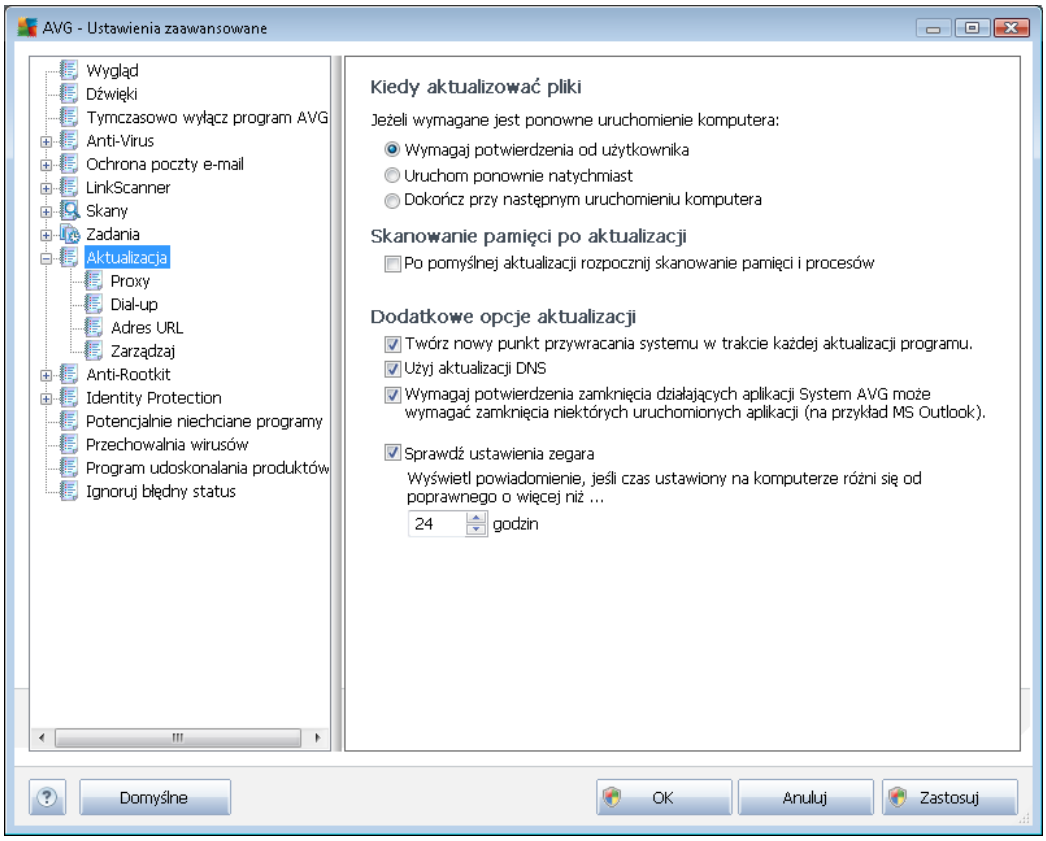
Inne ustawienia aktualizacji

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 systemu 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.*

9.9. 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 wymaga restartu komputera, który można od razu wykonać:

- ***Wymagaj potwierdzenia od użytkownika*** *(domyślnie)* - przed zakończeniem aktualizacji system zapyta użytkownika o pozwolenie na restart komputera.
- ***Uruchom ponownie natychmiast*** - komputer zostanie automatycznie zrestartowany zaraz po zakończeniu aktualizacji - potwierdzenie ze strony użytkownika nie jest wymagane
- ***Dokończ przy następnym uruchomieniu komputera*** - aktualizacja zostanie automatycznie odłożona i ukończona przy najbliższym restarcie systemu. 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

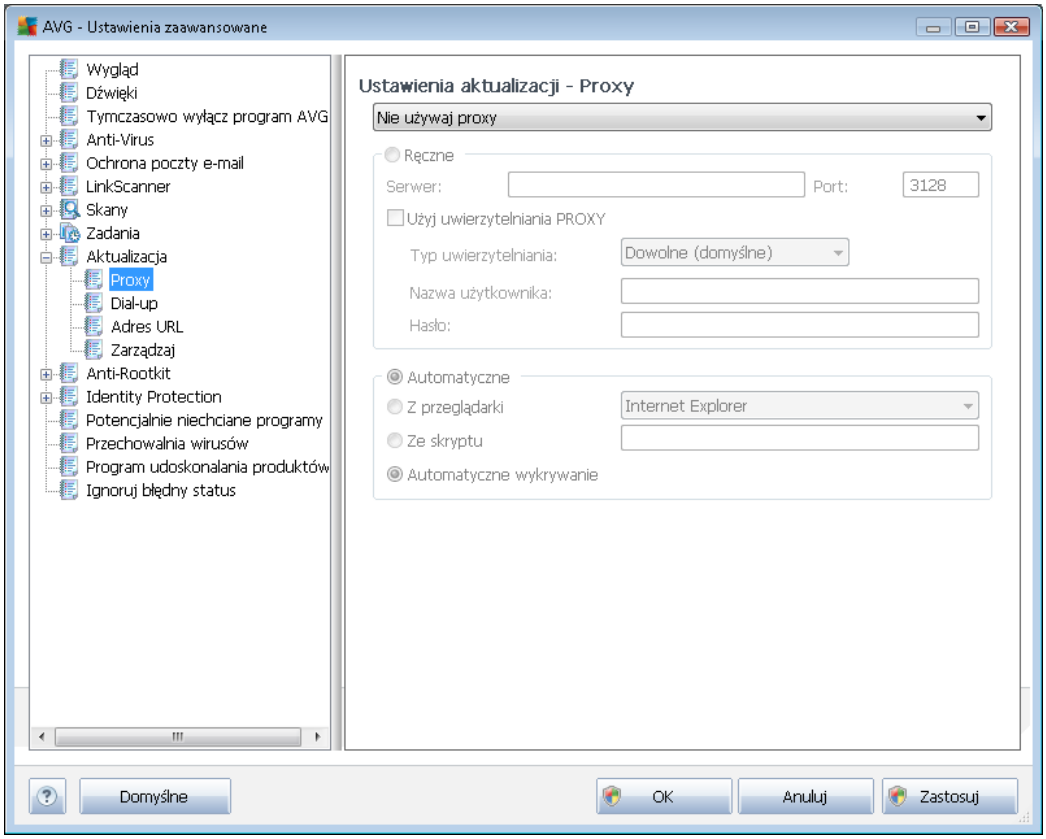
- ***Twórz nowy punkt przywracania systemu po każdej aktualizacji programu*** - przed każdym uruchomieniem aktualizacji systemu AVG tworzony będzie punkt przywracania systemu. Przy jego użyciu możliwe będzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). 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 2012** 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.

9.9.1. 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 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.

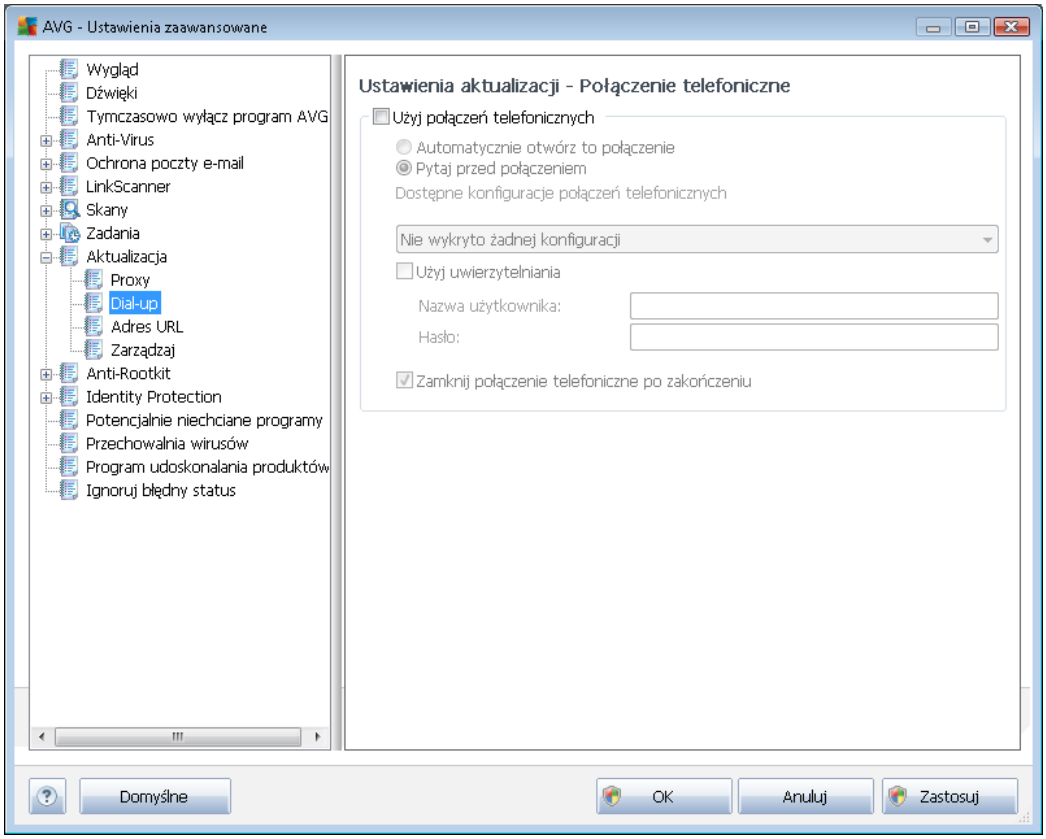
Konfiguracja automatyczna

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.

9.9.2. Połączenie telefoniczne

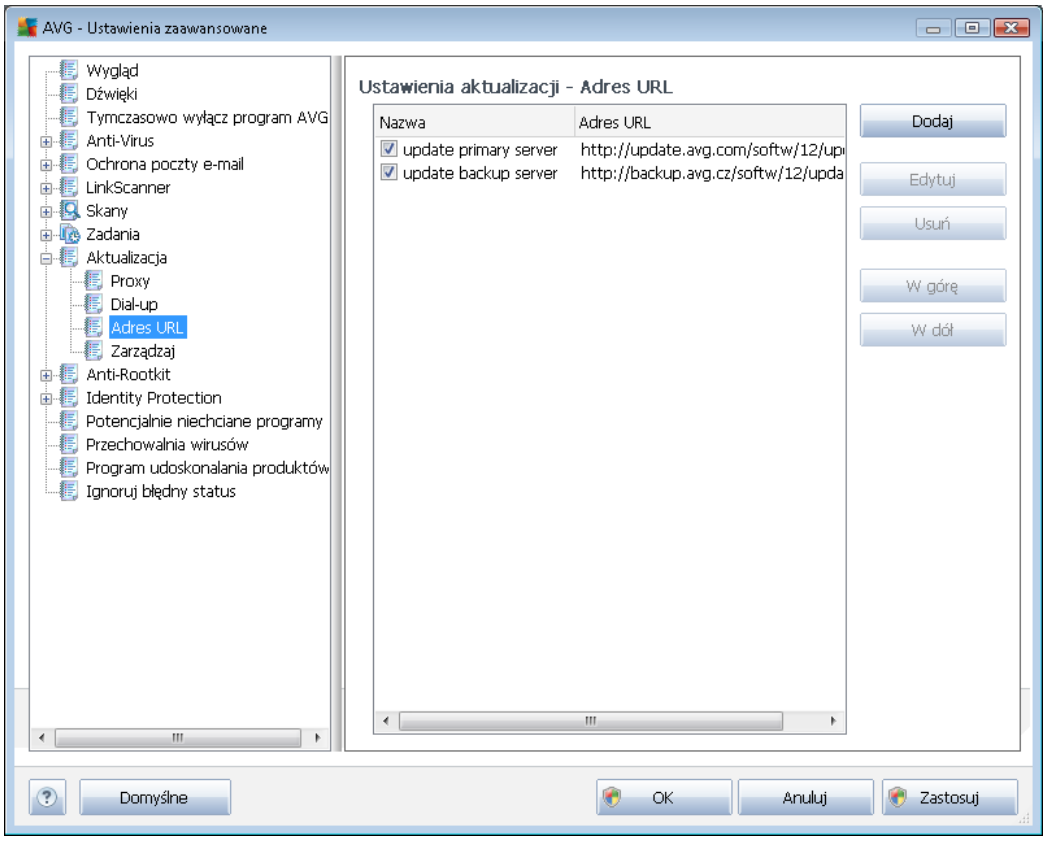
Wszystkie opcjonalne parametry podawane w oknie ***Ustawienia aktualizacji - Połączenie telefoniczne*** odnoszą się do połączenia dial-up z internetem. Pola tego okna pozostają nieaktywne aż do zaznaczenia opcji ***Użyj połączeń telefonicznych:***



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***).

9.9.3. URL

W oknie ***URL*** znajduje się lista adresów internetowych, z których będą pobierane pliki aktualizacyjne.



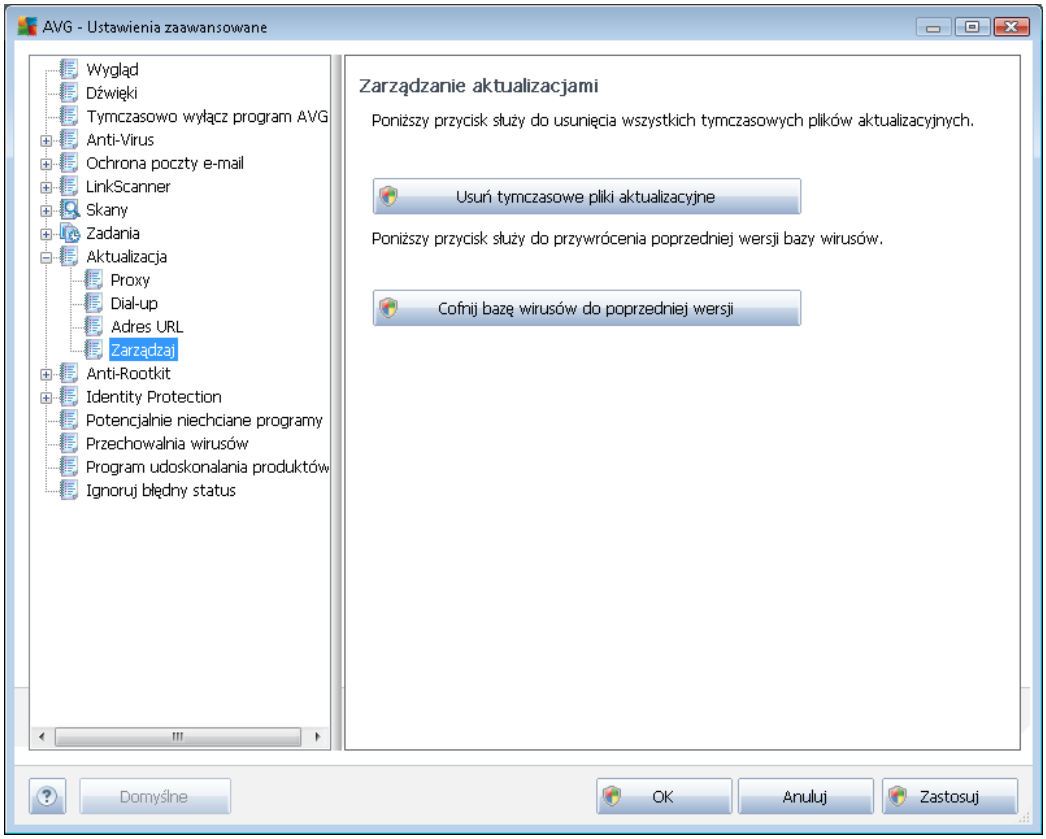
Przyciski kontrolne

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.

9.9.4. Zarządzaj

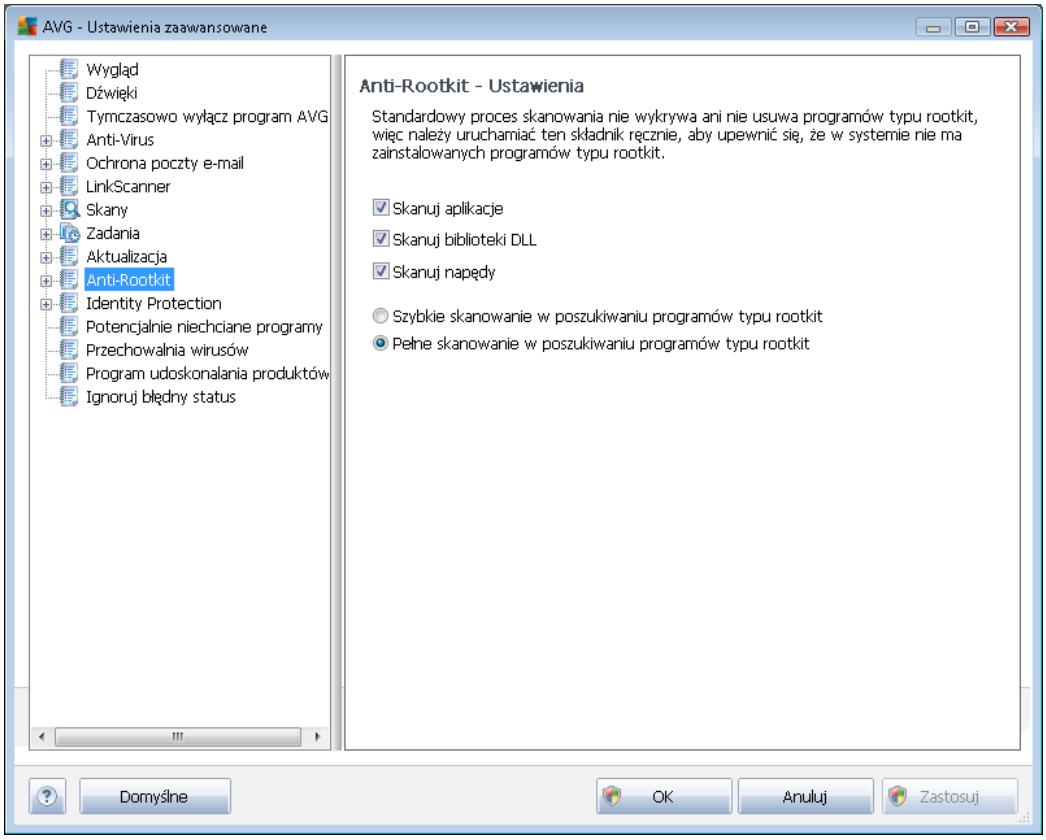
Okno ***Zarządzaj aktualizacjami*** udostępnia dwie funkcje:



- ***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*)

9.10. 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 jego interfejsie.

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

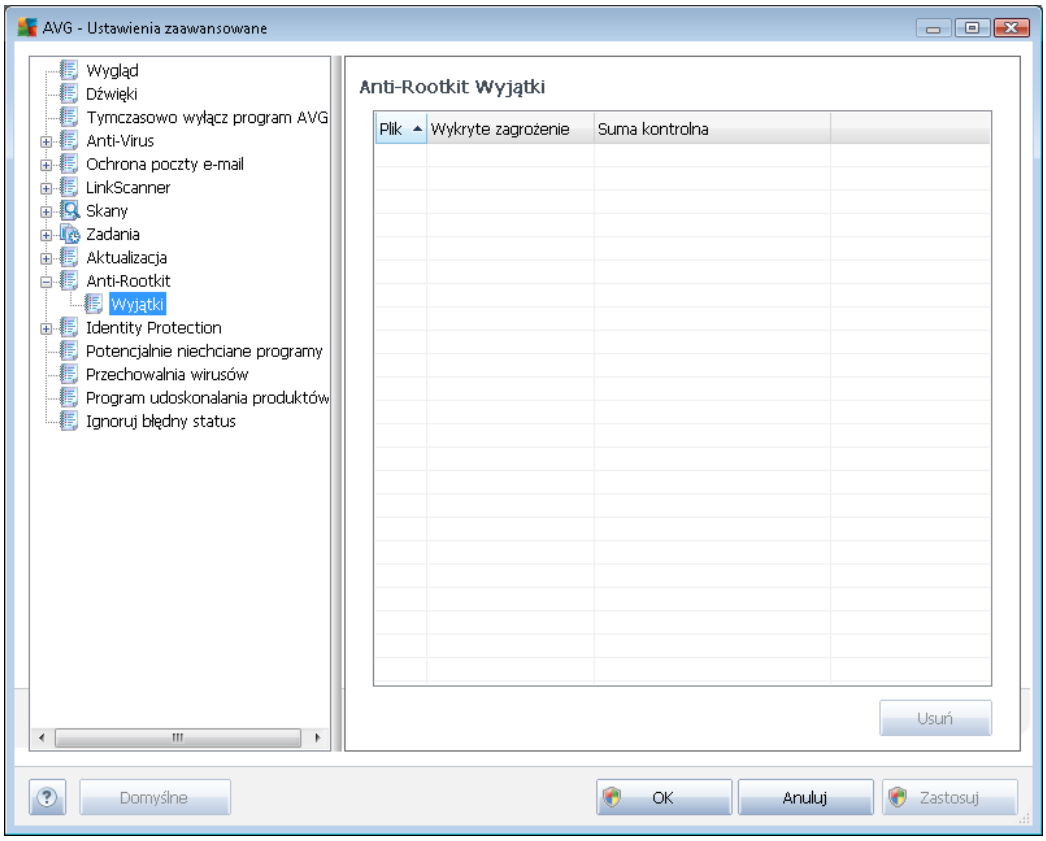
- ***Skanuj aplikacje***
- ***Skanuj biblioteki DLL***
- ***Skanuj sterowniki***

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*)

9.10.1. Wyjątki

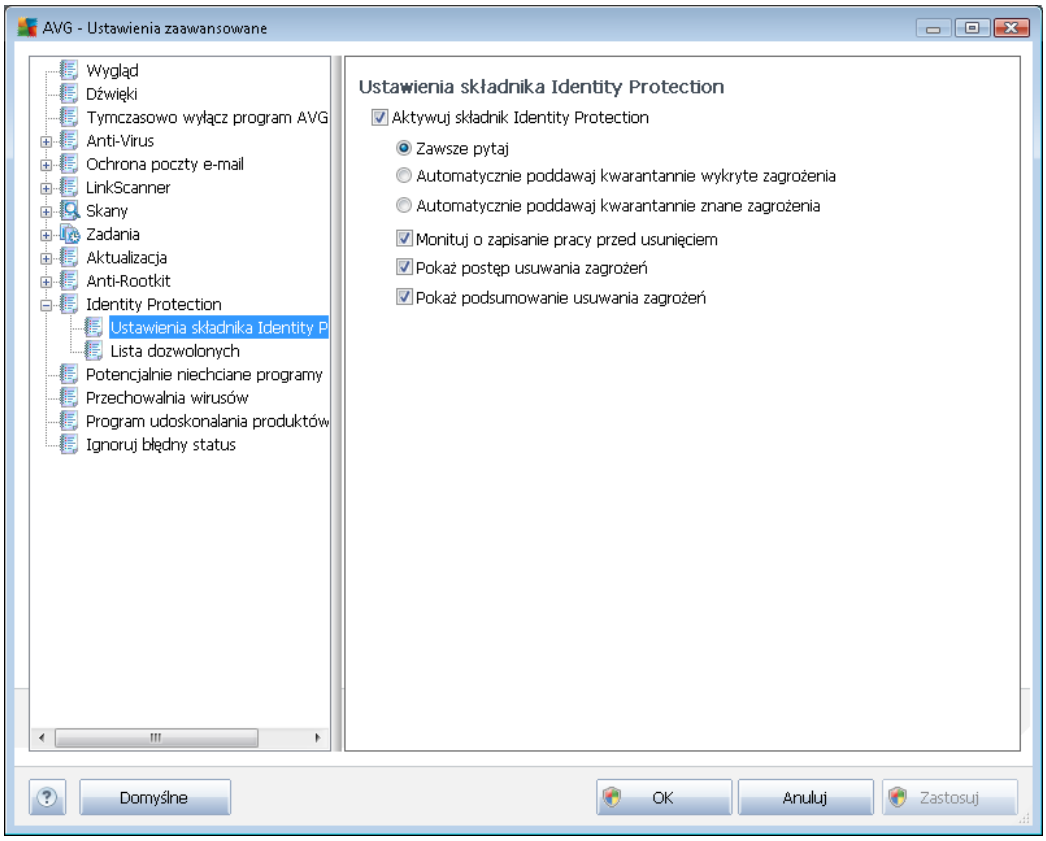
Okno ***Wyjątki Anti-Rootkit*** pozwala na zdefiniowanie plików *(np. pewnych sterowników wykrywanych błędnie jako roootkity)*, które mają być wykluczone ze skanowania:



9.11. AVG Identity Protection

9.11.1. Ustawienia składnika Identity Protection

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



Aktywuj składnik Identity Protection (*opcja domyślnie włączona*) - można odznaczyć to pole, aby wyłączyć składnik Identity Protection.

Stanowczo odradza się wyłączanie tej funkcji bez uzasadnionej przyczyny!

Jeśli składnik Identity Protection jest aktywny, można określić jego zachowanie w przypadku wykrycia zagrożenia:

- ***Zawsze monituj*** (*opcja domyślnie włączona*) - w przypadku wykrycia zagrożenia użytkownik zostanie zapytany, czy dany proces ma zostać poddany kwarantannie. Dzięki temu aplikacje, które mają pozostać uruchomione, nie zostaną usunięte.
- ***Automatycznie poddawaj kwarantannie wykryte zagrożenia*** - zaznacz to pole, aby wszystkie wykryte zagrożenia były natychmiast przenoszone w bezpieczne miejsce (do Przechowalni wirusów). Jeśli ustawienia domyślne zostaną zachowane, w przypadku wykrycia zagrożenia użytkownik zostanie zapytany, czy dany proces ma zostać przeniesiony do kwarantanny. Dzięki temu aplikacje, które mają pozostać uruchomione, nie zostaną usunięte.
- ***Automatycznie poddawaj kwarantannie znane zagrożenia*** - tylko znane zagrożenia

będą automatycznie poddawane kwarantannie (przenoszone do Przechowalni wirusów).

Następnie do wybranych pozycji można opcjonalnie przypisać dodatkowe funkcje składnika Identity Protection:

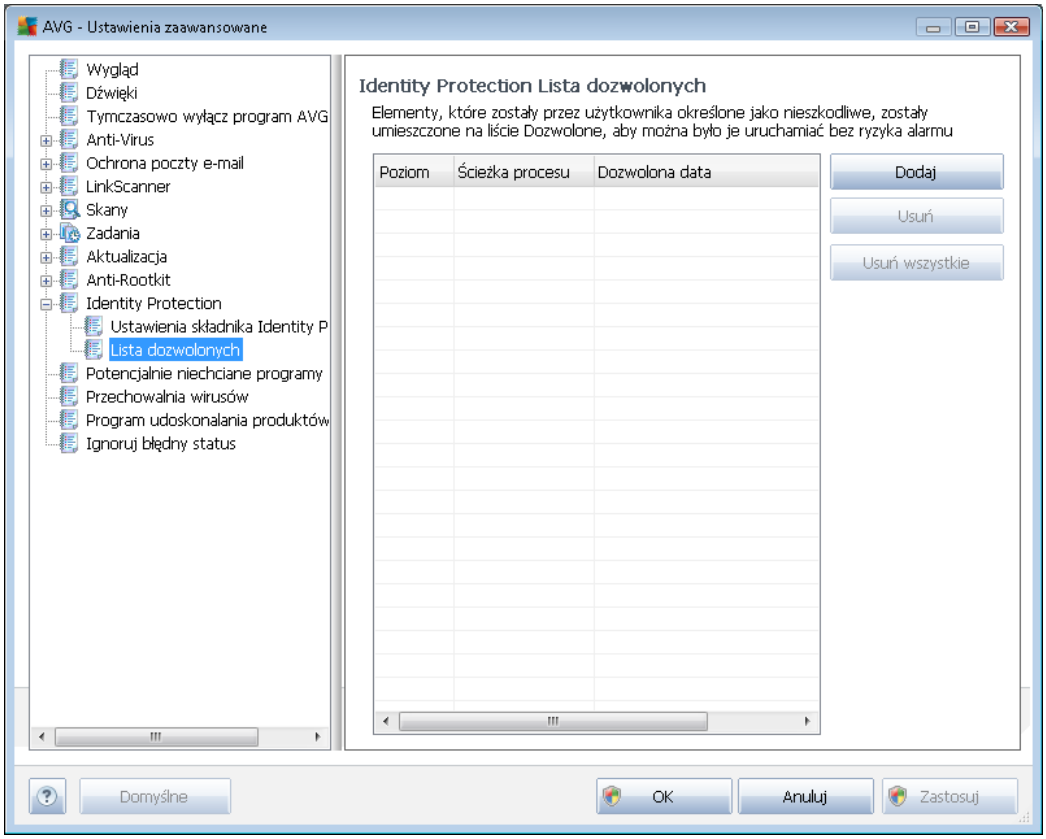
- ***Monituj o zapisanie pracy przed usunięciem*** (*opcja domyślnie wyłączona*) - zaznaczenie tej pozycji aktywuje ostrzeżenia przed przeniesieniem do Przechowalni aplikacji wykrytej jako potencjalnie szkodliwe oprogramowanie. Jeśli aplikacja jest w danym momencie używana, praca może zostać utracona - należy ją więc najpierw zapisać. Domyślnie ta opcja jest włączona i stanowczo zalecamy niewyłączanie jej.

- ***Pokaż postęp usuwania szkodliwego oprogramowania*** - (*domyślnie włączone*) - jeśli ta opcja jest włączona, wykrycie potencjalnie szkodliwego oprogramowania spowoduje otwarcie okna dialogowego wyświetlającego postęp przenoszenia szkodliwego oprogramowania do kwarantanny.

- ***Pokaż końcowe szczegóły usuwania szkodliwego oprogramowania*** (*opcja domyślnie włączona*) - jeśli ta opcja jest włączona, składnik ***Identity Protection*** wyświetla szczegółowe informacje o każdym obiekcie przeniesionym do Przechowalni (*poziom zagrożenia, lokalizacja itp.*).

9.11.2. Lista dozwolonych

Jeśli znajdujące się w oknie dialogowym ***Ustawienia składnika Identity Protection*** pole wyboru ***Automatycznie przenoś wykryte zagrożenia do kwarantanny*** pozostało niezaznaczone, system będzie pytał o potwierdzenie usunięcia każdego potencjalnie szkodliwego oprogramowania, które wykryje. Jeśli taki podejrzany program (*wykryty na podstawie zachowania*) zostanie uznany za bezpieczny, nastąpi dodanie go do listy ***Dozwolone*** i nie będzie on ponownie zgłaszany jako potencjalnie niebezpieczny:



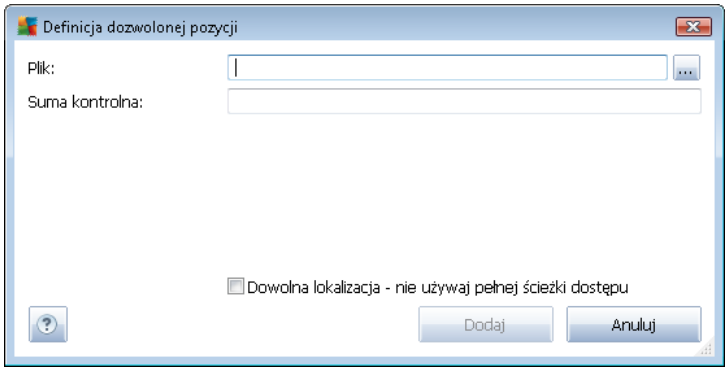
Lista ***Dozwolone*** zawiera następujące informacje o każdej aplikacji:

- ***Poziom*** - graficzna reprezentacja ryzyka stwarzanego przez określone procesy, przedstawiana na czterostopniowej skali od najmniej istotnego (■□□□) do krytycznego (■■■■)
- ***Ścieżka procesu*** - ścieżka dostępu do lokalizacji pliku wykonywalnego aplikacji (*procesu*)
- ***Data zezwolenia*** - data ręcznego określenia aplikacji jako bezpiecznej

Przyciski kontrolne

W oknie dialogowym ***Identity Protection - lista Dozwolone*** dostępne są następujące przyciski kontrolne:

- ***Dodaj*** - naciśnij ten przycisk, aby dodać nową aplikację do listy programów dozwolonych. Zostanie wyświetlone poniższe okno dialogowe:

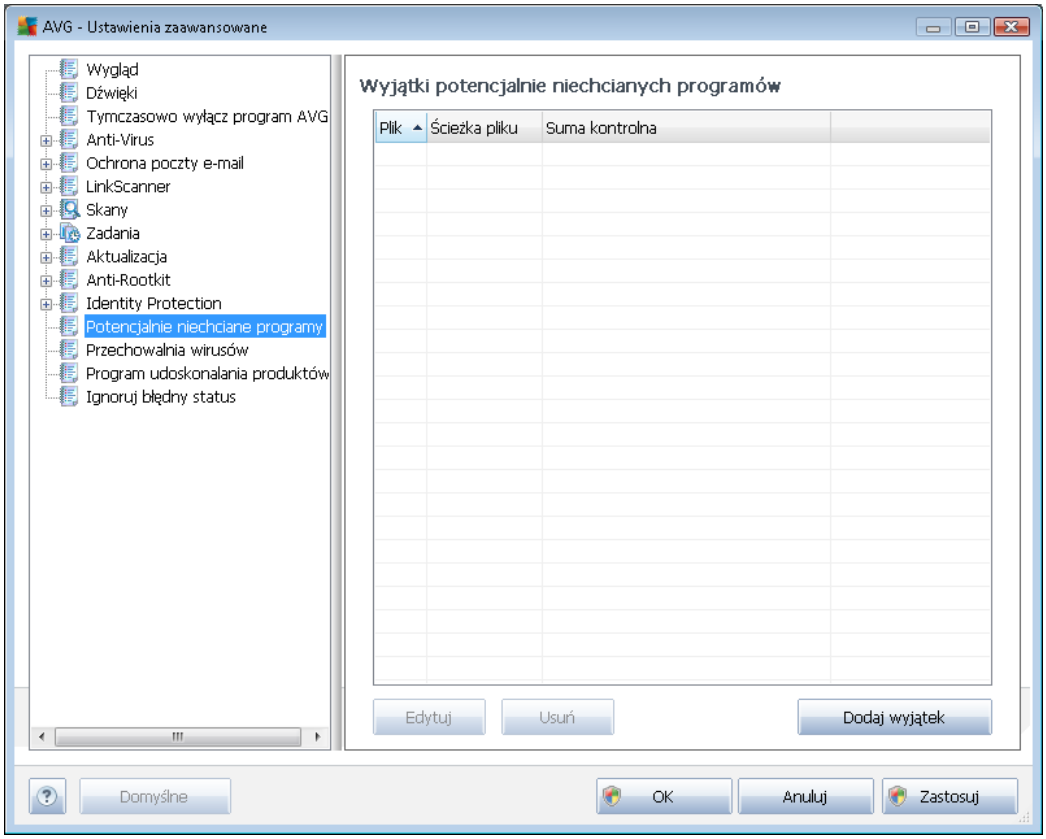


- ***Plik*** - należy podać pełną ścieżkę dostępu do pliku (*aplikacji*), który ma zostać oznaczony jako wyjątek
- ***Suma kontrolna*** - wyświetla unikatową „sygnaturę" wybranego pliku. Suma ta jest generowanym automatycznie ciągiem znaków, który pozwala systemowi AVG jednoznacznie odróżniać wybrany plik od innych. Jest ona generowana i wyświetlana po pomyślnym dodaniu pliku.
- ***Dowolna lokalizacja - nie używaj pełnej ścieżki dostępu*** - jeśli plik ma zostać zdefiniowany jako wyjątek jedynie dla konkretnej lokalizacji, wówczas należy pozostawić to pole wyboru niezaznaczone.

- ***Usuń*** - wciśnij ten przycisk, aby usunąć z listy zaznaczone aplikacje.
- ***Usuń wszystkie*** - wciśnij ten przycisk, aby usunąć wszystkie aplikacje z listy.

9.12. Potencjalnie niechciane programy

System **AVG Anti-Virus 2012** 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 jako *potencjalnie niechciany program*. Jeśli chcesz zachować taki program na komputerze, możesz zdefiniować go jako wyjątek potencjalnie niechcianych programów:

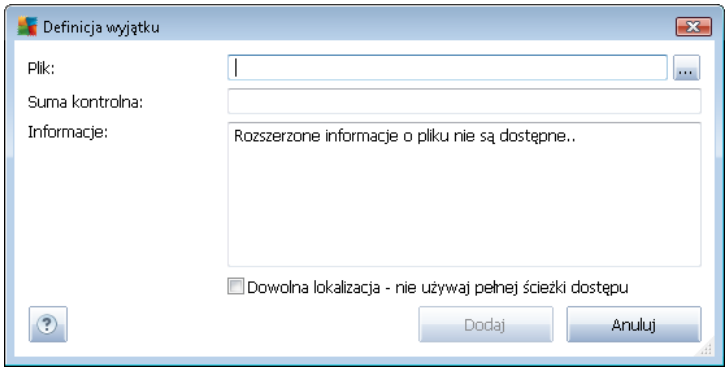


Okno ***Wyjątki potencjalnie niechcianych programów*** zawiera listę już zdefiniowanych i aktualnie obowiązujących wyjątków potencjalnie niechcianych programów. Listę tę można edytować, usuwać istniejące pozycje lub dodawać nowe wyjątki. Dla każdego wyjątku na liście dostępne są następujące informacje:

- ***Plik*** - podaje dokładną nazwę apikacji
- ***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.

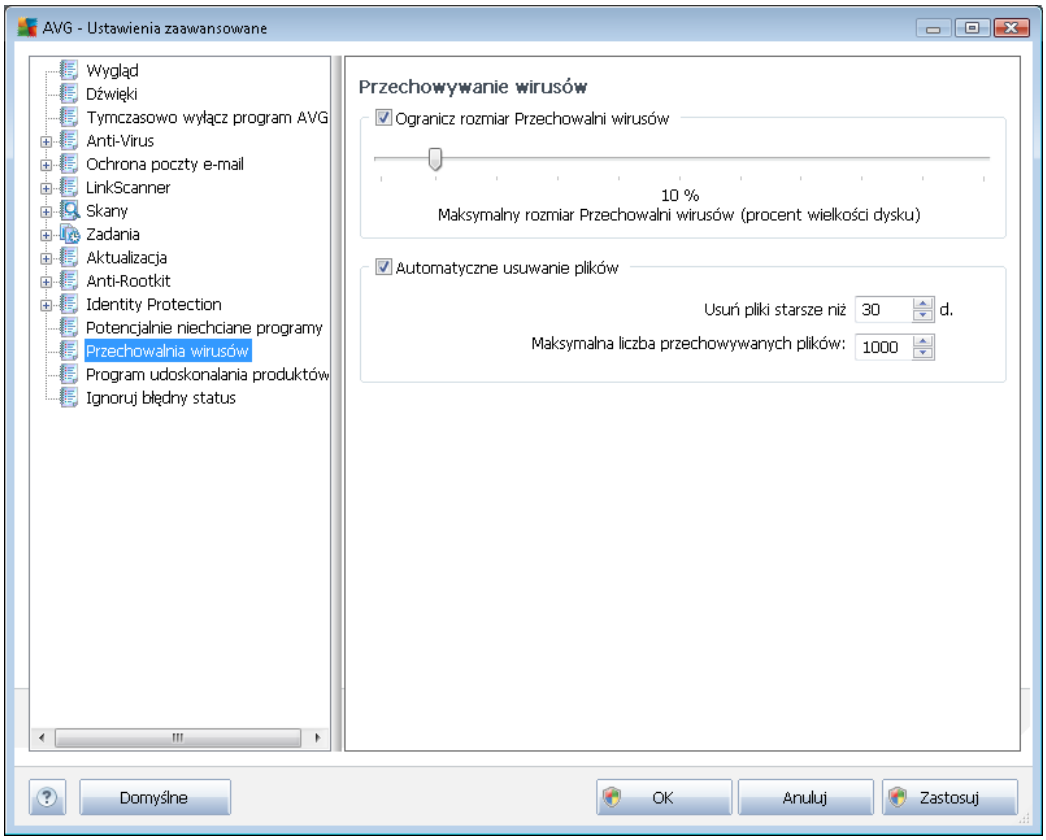
Przyciski kontrolne

- ***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 będzie używany jako unikalny przykład na wypadek, gdyby w systemie znajdowały się dwa pliki o tej samej nazwie)*.

9.13. 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.

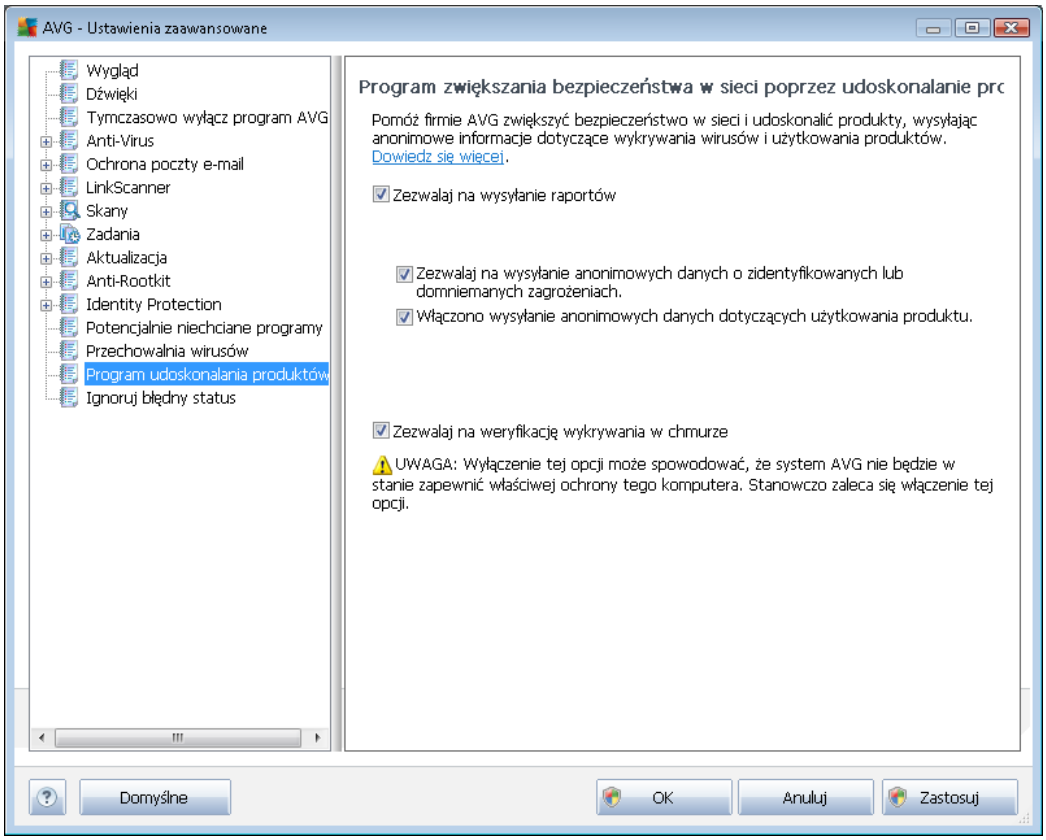
- ***Automatyczne usuwanie plików*** - w tym obszarze można zdefiniować maksymalny okres przetrzymywania obiektów w Przechowalni wirusów (***Usuń pliki starsze niż ... dni***) oraz maksymalną liczbę plików, które mogą znajdować się w Przechowalni (***Maksymalna liczba przechowywanych plików***).

9.14. Program udoskonalania produktów

Okno ***Programu udoskonalania produktów*** zaprasza do udziału w programie AVG, który ma na celu podniesienie ogólnego poziomu bezpieczeństwa w internecie. Zaznaczenie opcji ***Zezwalaj na wysyłanie raportów*** spowoduje włączenie funkcji raportowania wykrytych zagrożeniach firmie AVG. Pomoże nam to w gromadzeniu aktualnych informacji o najnowszych wirusach. Wiedza ta jest konieczna, jeśli mamy im przeciwdziałać.

Wysyłanie raportów odbywa się automatycznie, zatem nie powoduje żadnych niedogodności. Co więcej, raporty nie zawierają żadnych poufnych danych. Zgłaszanie wykrytych zagrożeń jest

opcjonalne - prosimy jednak o pozostawienie tej opcji włączonej. Pozwala ona na udoskonalenie ochrony zapewnianej Tobie i innym użytkownikom 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:

- ***Wirus*** to 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*** są podkategorią wirusów i - w przeciwieństwie do swoich tradycyjnych kuzynów - nie potrzebują „nosicieli", do których musiałyby się dołączać; robaki rozsyłają się same na wiele komputerów (zwykle w wiadomościach e-mail), w efekcie mogą spowodować przeładowanie 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.

- ***Również 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.

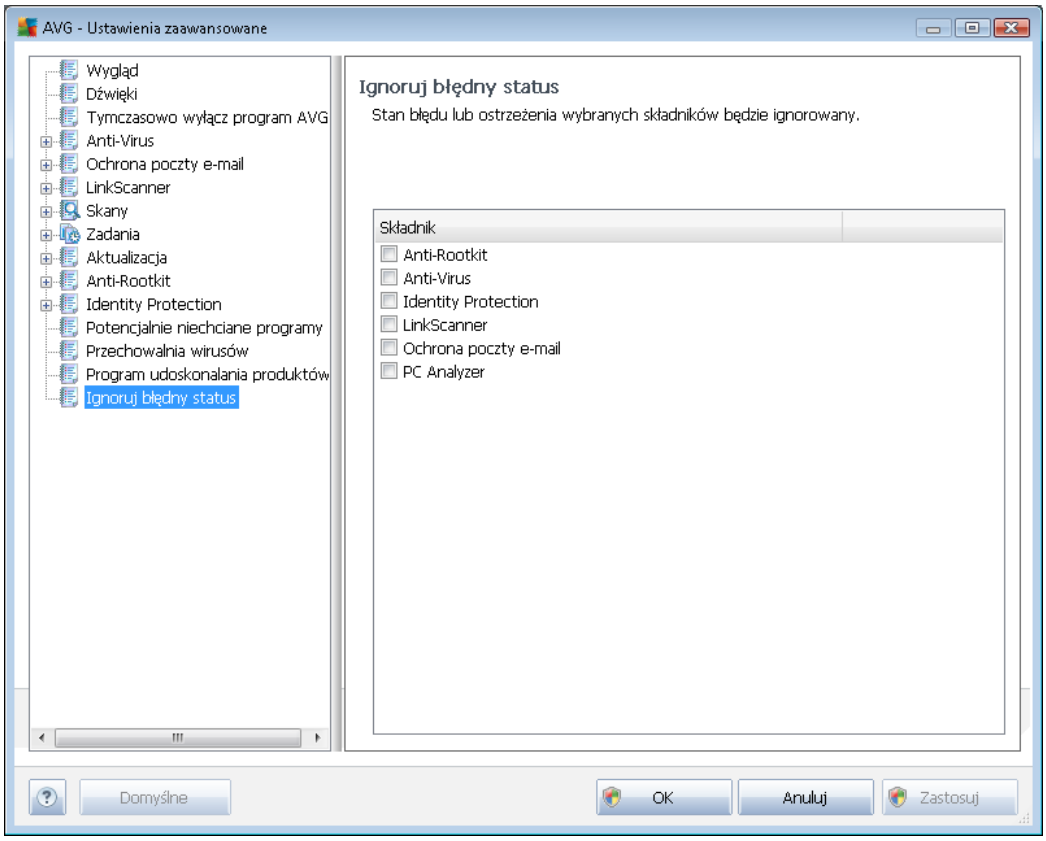
- ***Fałszywy alarm*** to masowo wysyłana wiadomość e-mail zawierająca informacje o wyimaginowanym zagrożeniu. Wiele z opisanych powyżej zagrożeń rozprzestrzenia się za pośrednictwem wiadomości e-mail zwanych fałszywkami.

- ***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 Anti-Virus 2012 zawiera szereg wyspecjalizowanych składników. Szczegółowe informacje o ich funkcjach zawiera rozdział Przegląd składników.

9.15. Ignoruj błędny status

W oknie dialogowym ***Ignoruj wadliwe warunki*** można wskazać składniki, które mają być pomijane w powiadomieniach o stanie systemu AVG:



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.

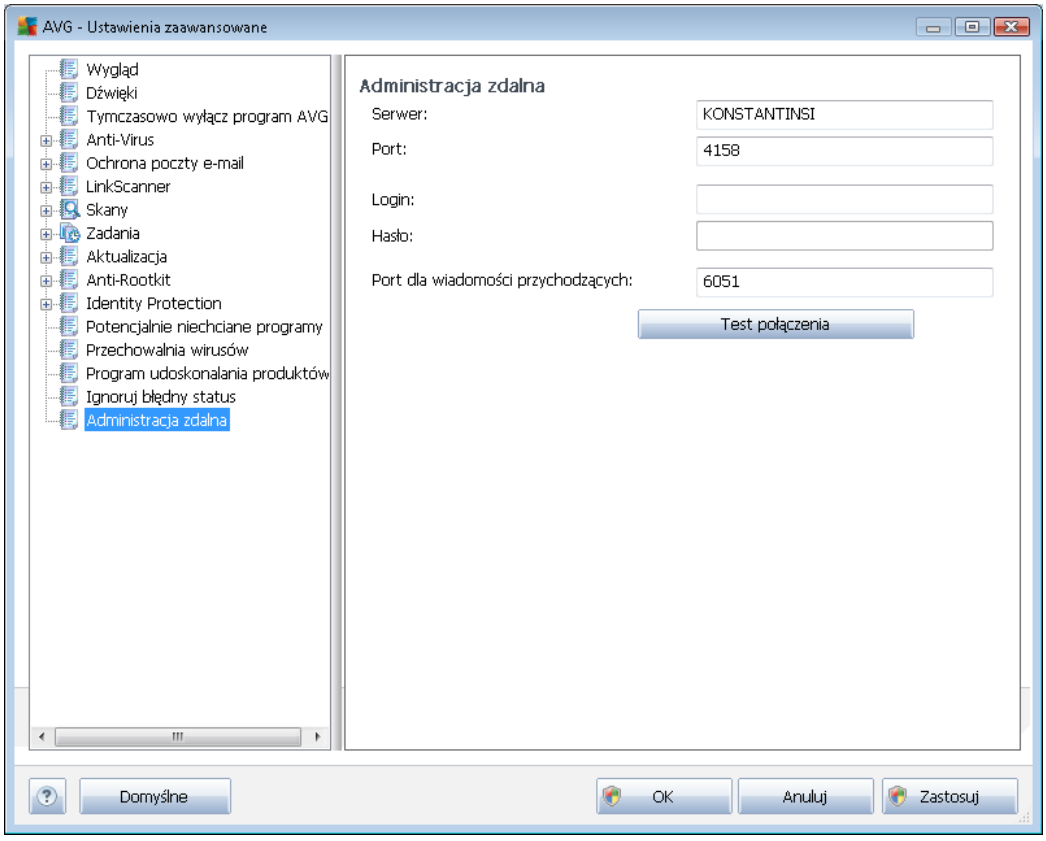
Może wystąpić sytuacja, w której składnik powinien zostać tymczasowo wyłączony (*nie jest to zalecane; wszystkie składniki powinny być zawsze włączone i działać w trybie domyślnym, ale niekiedy może być wymagane odstępstwo od tej reguły*). W takim przypadku ikona na pasku zadań automatycznie informuje 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 składnika jest także dostępna bezpośrednio w sekcji przeglądu składników okna głównego AVG.

9.16. Administracja zdalna

Pozycja ***Administracja zdalna*** i odpowiadające jej okno dialogowe będzie dostępne tylko jeśli zainstalowałeś system **AVG Anti-Virus 2012** przy użyciu jednej z biznesowych licencji AVG, potwierdzając w trakcie tego procesu chęć instalacji składnika ***Administracja zdalna***. Szczegółowy opis instalacji i konfiguracji Administracji zdalnej można znaleźć w dokumentacji AVG Business Edition, dostępnej pod adresem http://www.avg.com/, w sekcji Centrum pomocy technicznej / Pobierz.



Ustawienia składnika ***Administracja zdalna*** określają sposób łączenia się stacji roboczej AVG z systemem administracji zdalnej. Jeśli dana stacja ma łączyć się ze zdalnym serwerem administracyjnym, należy określić następujące parametry:

- ***Serwer*** - nazwa (lub adres IP) serwera, na którym zainstalowano oprogramowanie AVG Admin Server.
- ***Port*** - numer portu, przez który klient AVG komunikuje się z serwerem AVG Admin Server (*za domyślny uważany jest port 4158 - jeśli ma być używany, nie trzeba go wprowadzać*).
- ***Login*** - jeśli używana jest opcja bezpiecznej komunikacji między klientem AVG i oprogramowaniem AVG Admin Server, należy podać nazwę użytkownika.

- ***Hasło*** - wymagane, jeśli podano login.
- ***Port dla wiadomości przychodzących*** - numer portu, na którym klient AVG odbiera wiadomości od serwera AVG Admin Server.

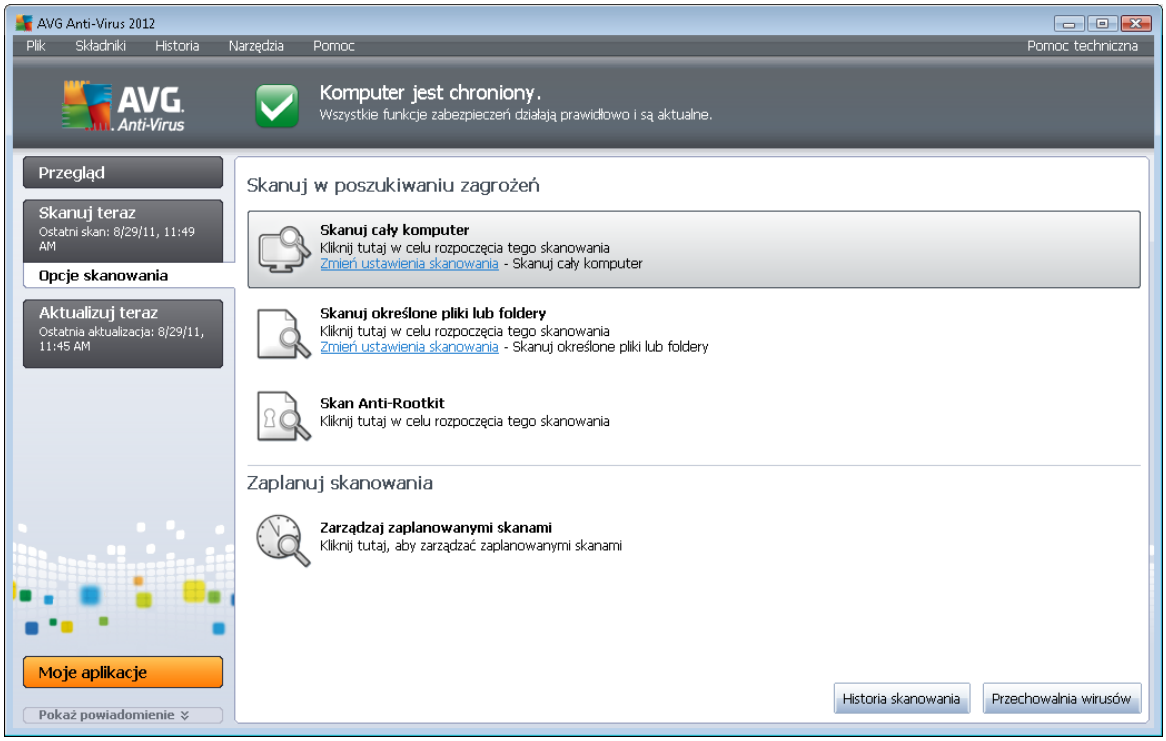
Przyciski kontrolne

Przycisk ***Testuj połączenie*** pozwala sprawdzić, czy wszystkie powyższe dane są prawidłowe i zapewnią pomyślne połączenie z bazą danych DataCenter.

10. Skanowanie AVG

Domyślnie system **AVG Anti-Virus 2012** nie uruchamia żadnych testów, ponieważ po przeprowadzeniu wstępnego skanu ochronę potrafią zapewnić rezydentne składniki **AVG Anti-Virus 2012**, które przez cały czas czuwają, by złośliwe oprogramowanie nie miało szans przedostania się na Twój komputer. Oczywiście wciąż możesz zaplanować skanowanie w regularnych odstępach czasu lub uruchamiać je ręcznie w zależności od potrzeb.

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 2012** 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.

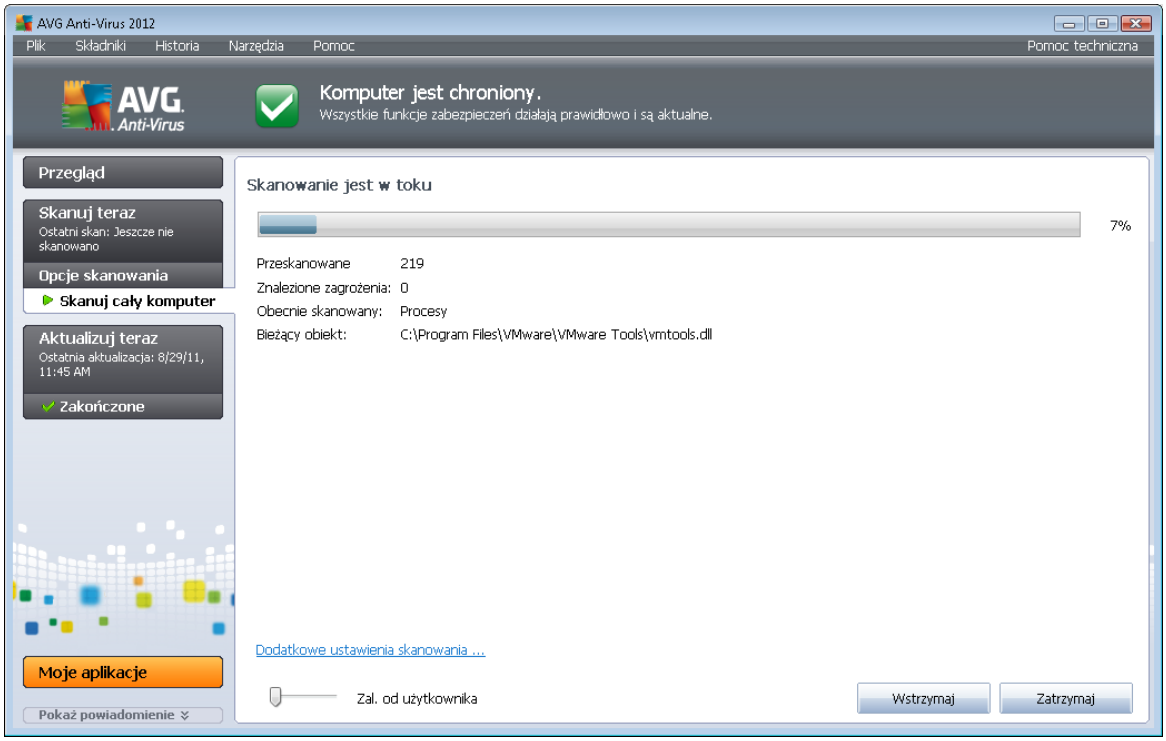
W systemie **AVG Anti-Virus 2012** dostępne są następujące typy skanowania zdefiniowane wstępnie przez producenta:

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.

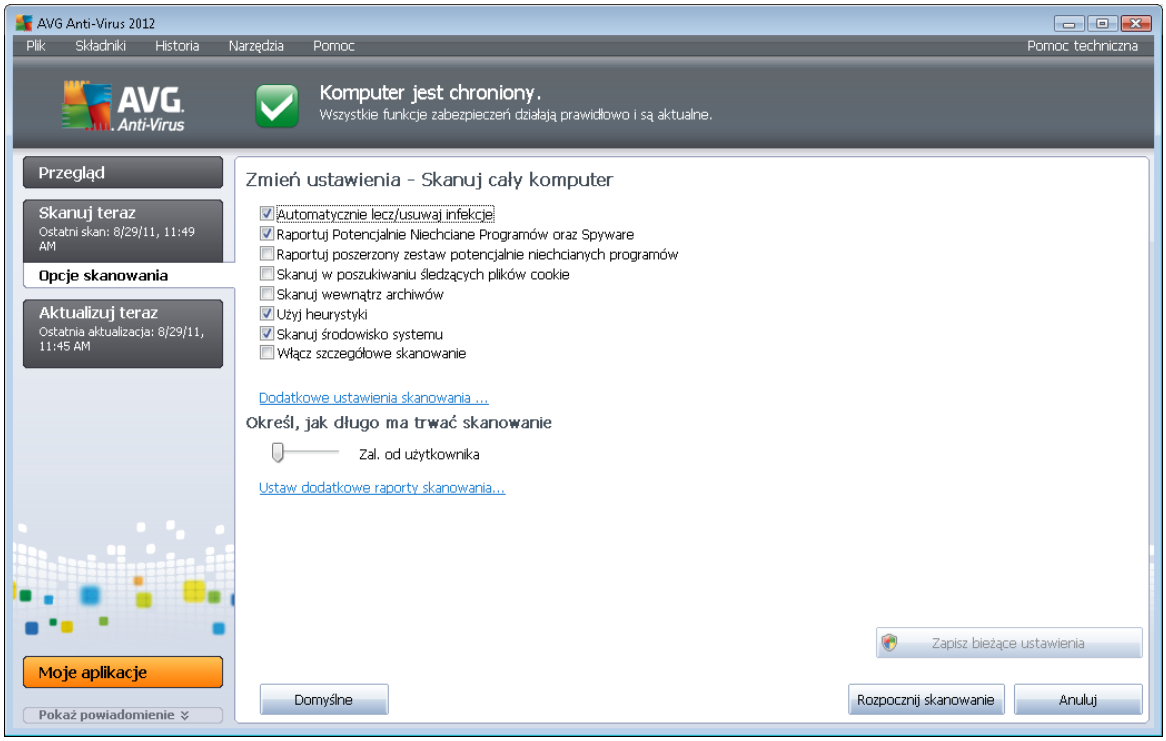
Uruchamianie skanowania

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.

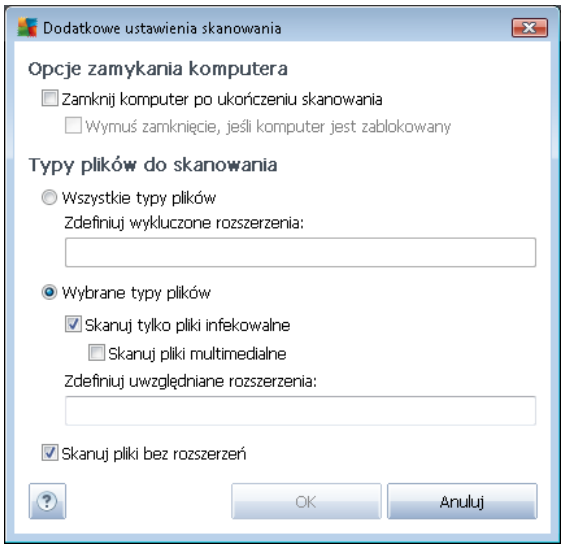
    - ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) - zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą 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***).
- ***Typy plików do skanowania*** - należy zdecydować, które z poniższych elementów mają być skanowane:

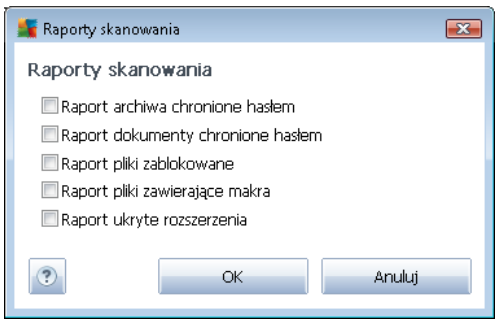
- ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być skanowane;

- ***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

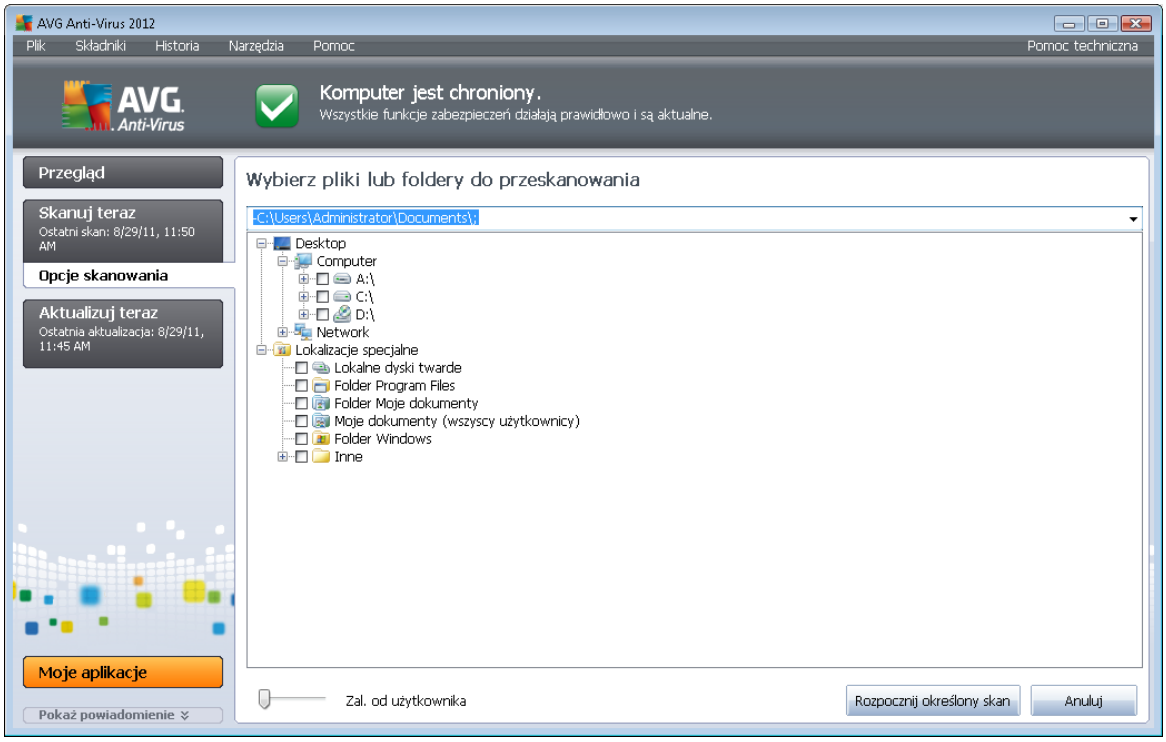
Skan określonych plików lub folderów - skanowane są tylko wskazane obszary komputera (wybrane foldery, a także dyski twarde, pamięci flash, CD itd.). Postępowanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu całego komputera: każdy znaleziony wirus jest leczony lub przenoszony do 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.

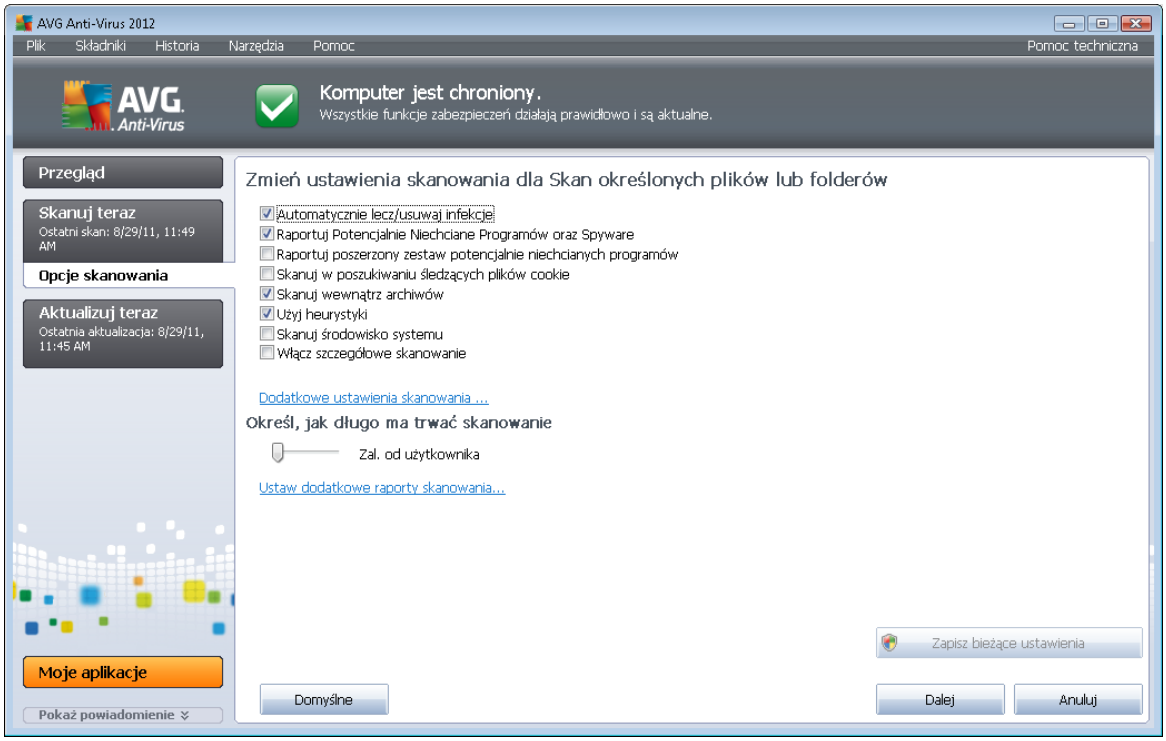
Można także przeskanować wybrany folder, wykluczając jednocześnie ze skanowania wszystkie jego podfoldery: należy wprowadzić znak minus „-” przed jego nazwą w wygenerowanej ścieżce (*patrz ilustracja*). Aby wykluczyć cały folder ze skanowania, należy użyć parametru „!”.

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.

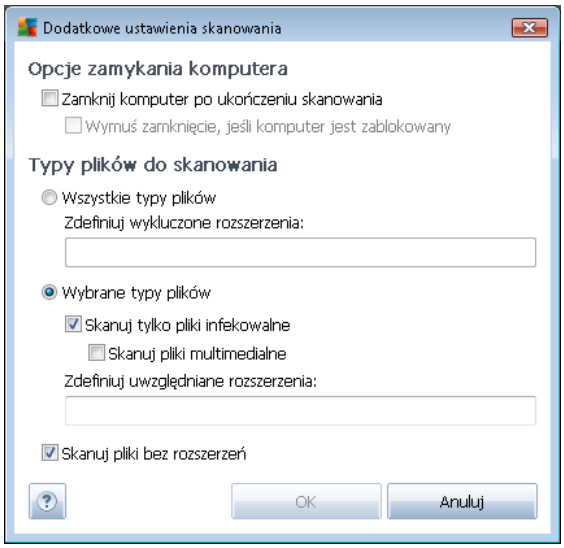
    - ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) - zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą 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***).
- ***Typy plików do skanowania*** - należy zdecydować, które z poniższych elementów mają być skanowane:

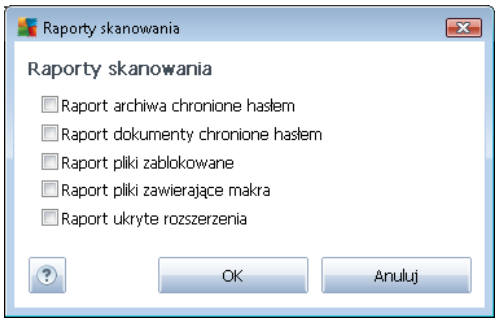
- ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być skanowane;

- ***Wybrane typy plików*** - skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe 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).*

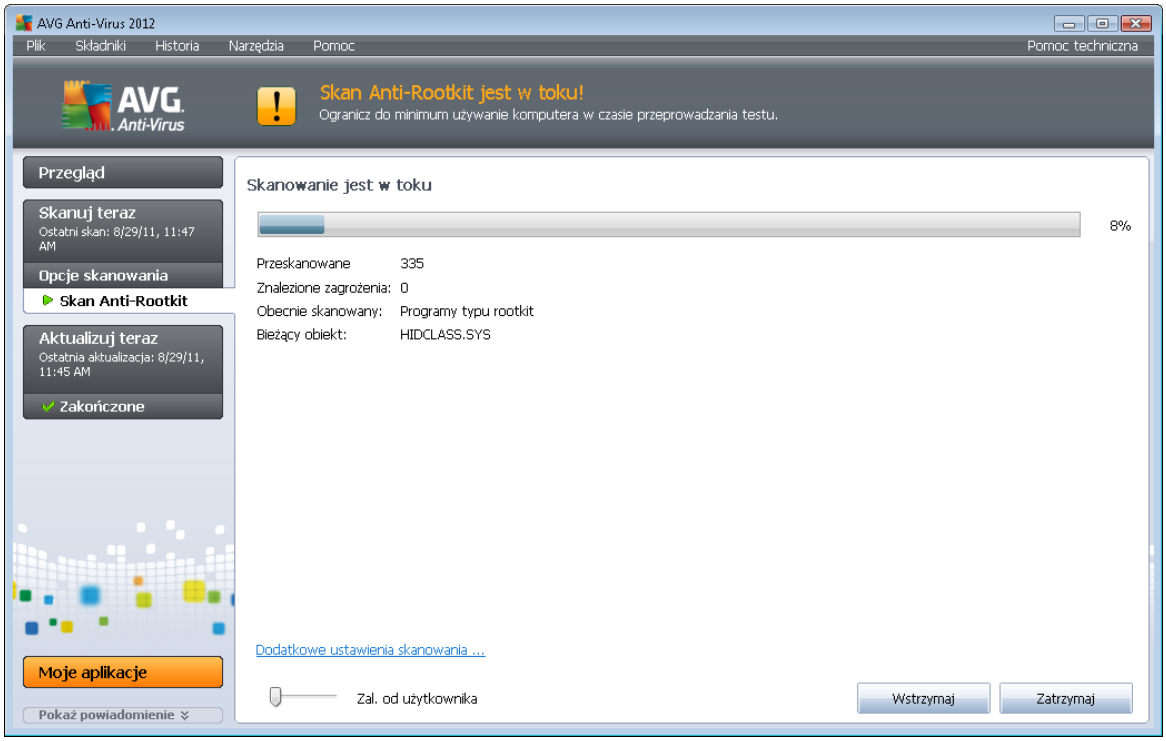
10.2.3. Skan Anti-Rootkit

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***).

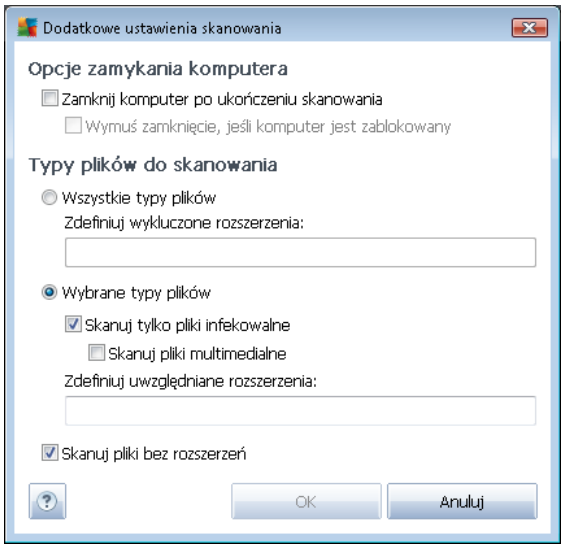


Edycja konfiguracji skanowania

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):

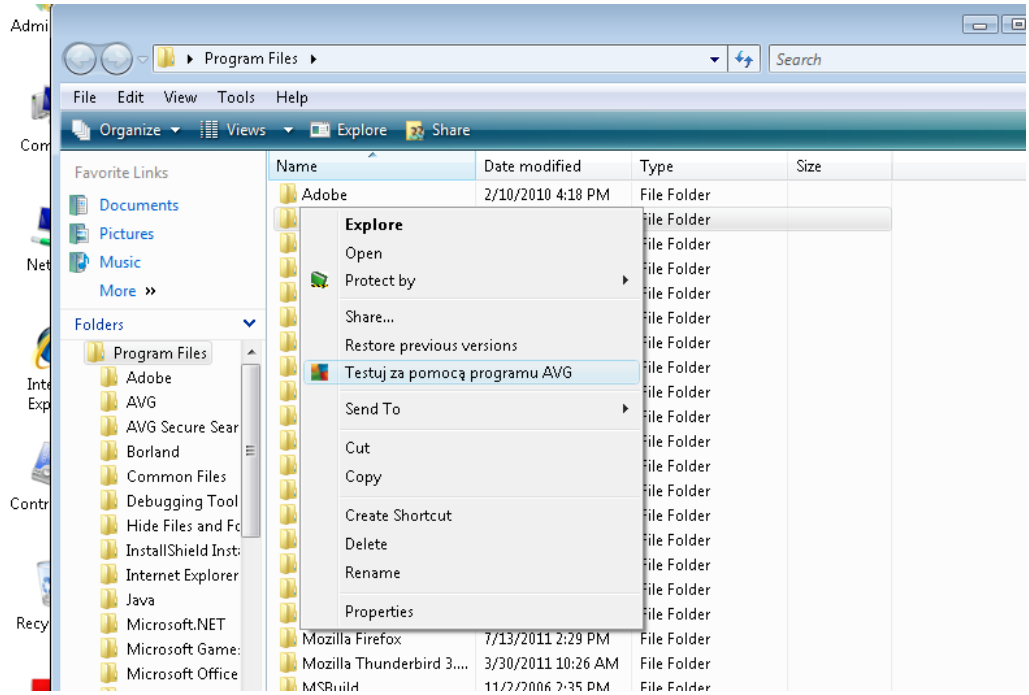
- ***Skanowanie automatyczne*** - za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślna wartość tej opcji to poziom *Zależny od użytkownika, co oznacza automatycznie dobrane wykorzystanie zasobów.* Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie 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 2012** 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 programie Eksplorator Windows zaznacz plik *(lub folder)*, który chcesz sprawdzić
- Kliknij go prawym przyciskiem myszy, aby wyświetlić menu kontekstowe.
- Wybierz polecenie ***Testuj za pomocą programu***, aby system AVG przeskanował dany obiekt **AVG Anti-Virus 2012**

10.4. Skan z poziomu wiersza poleceń

System **AVG Anti-Virus 2012** 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

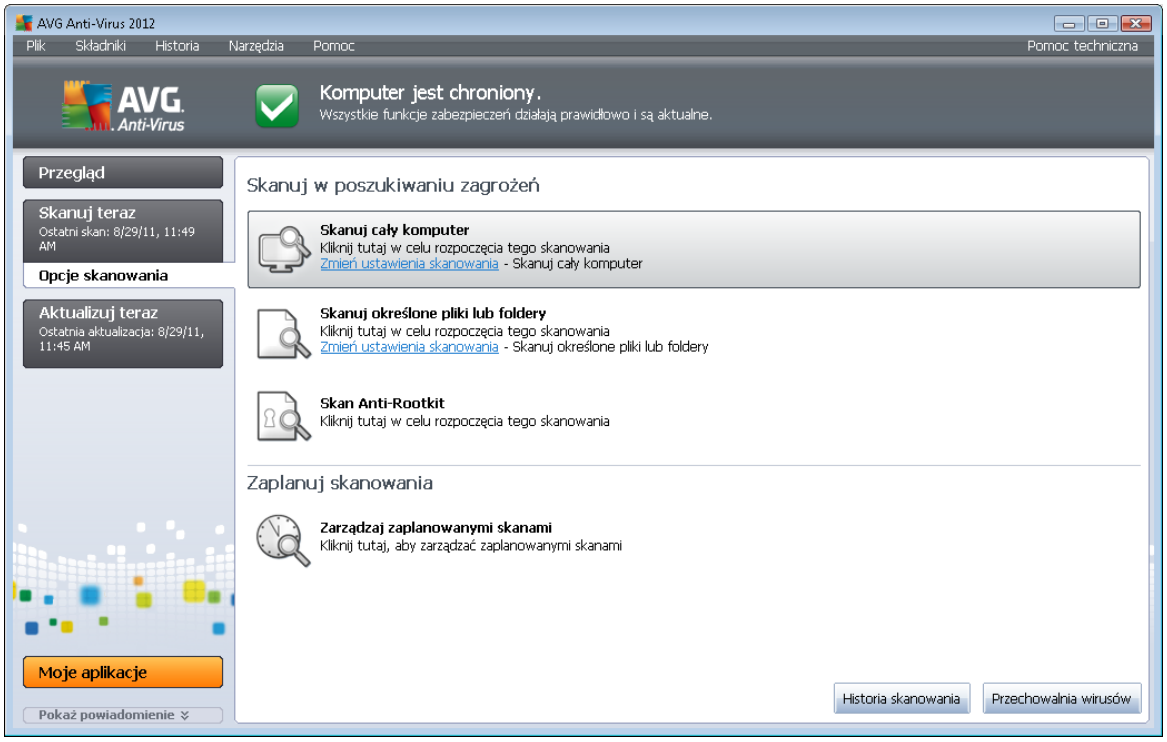
10.5. Planowanie skanowania

System **AVG Anti-Virus 2012** 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

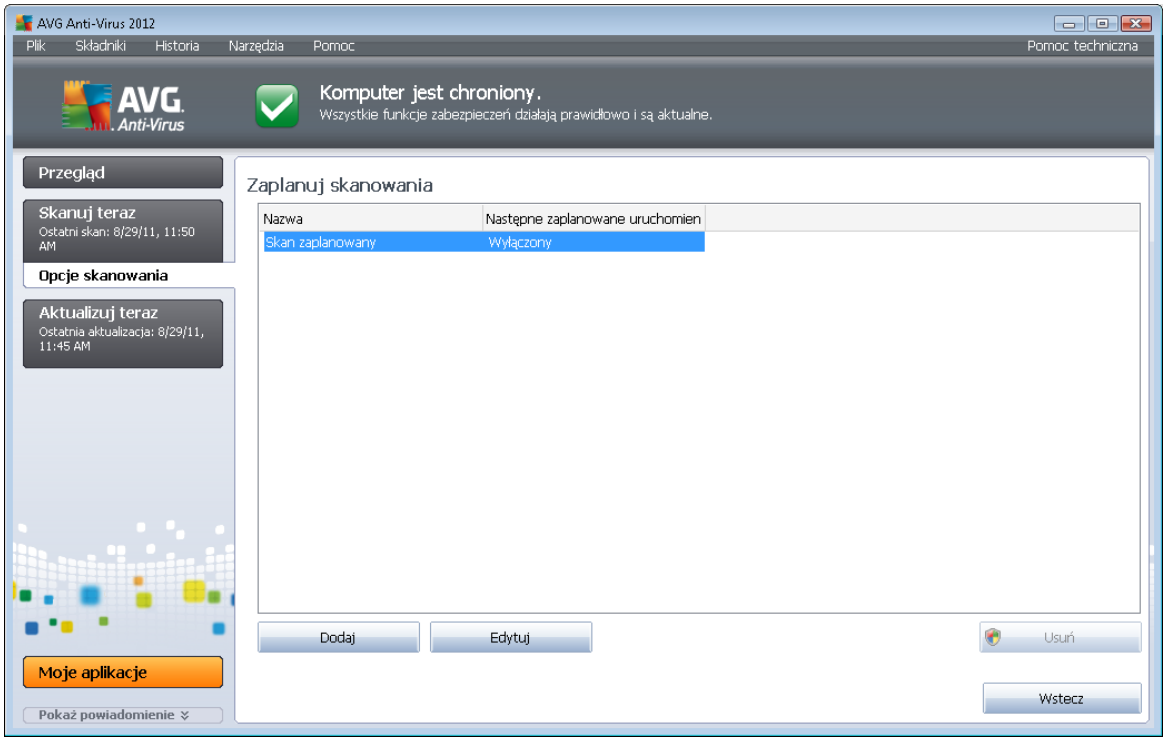
możliwe, należy skanować komputer codziennie - zgodnie z domyślną konfiguracją harmonogramu skanowania. Jeśli komputer działa 24 godziny na dobę, można zaplanować skanowanie poza czasem pracy. Jeśli komputer jest czasami wyłączany, pominięte z tego powodu skany uruchamiane są po ponownym włączeniu komputera.

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 ***Planowanie skanowania***, aby otworzyć nowe okno dialogowe ***planowanie skanowania***, które zawiera listę wszystkich zaplanowanych testów:

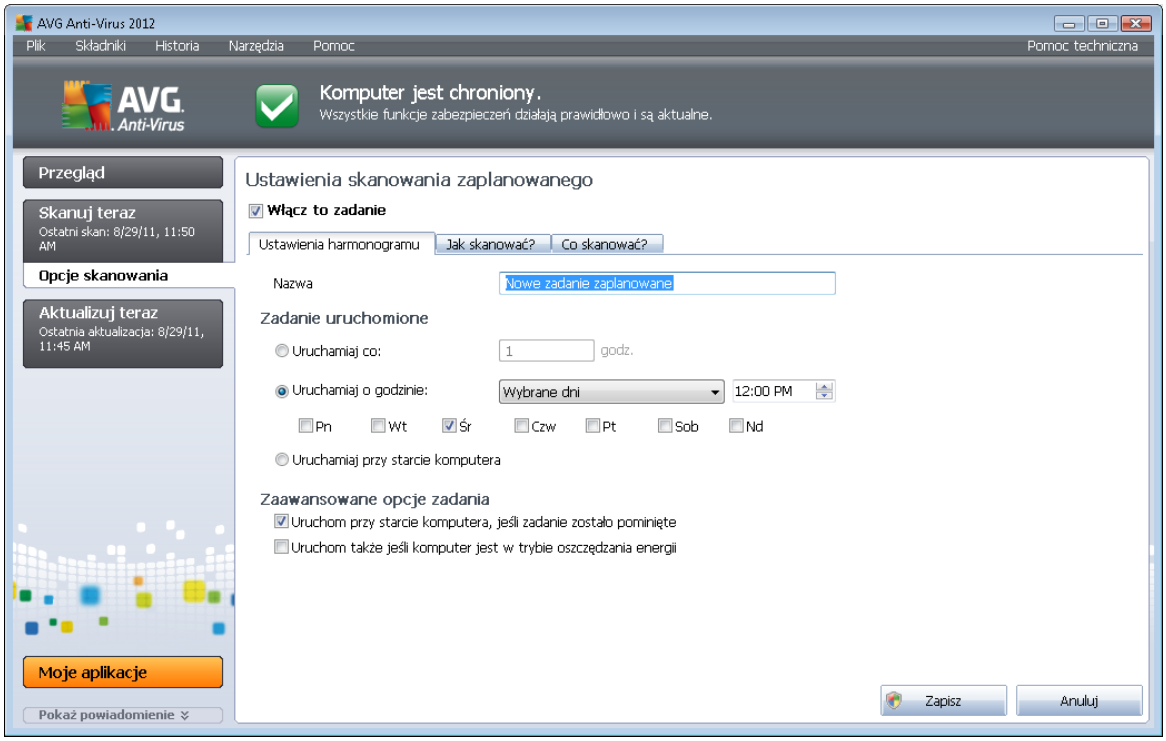


Zawartość okna można edytować, używając następujących przycisków:

- ***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***). To okno dialogowe podzielone jest 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

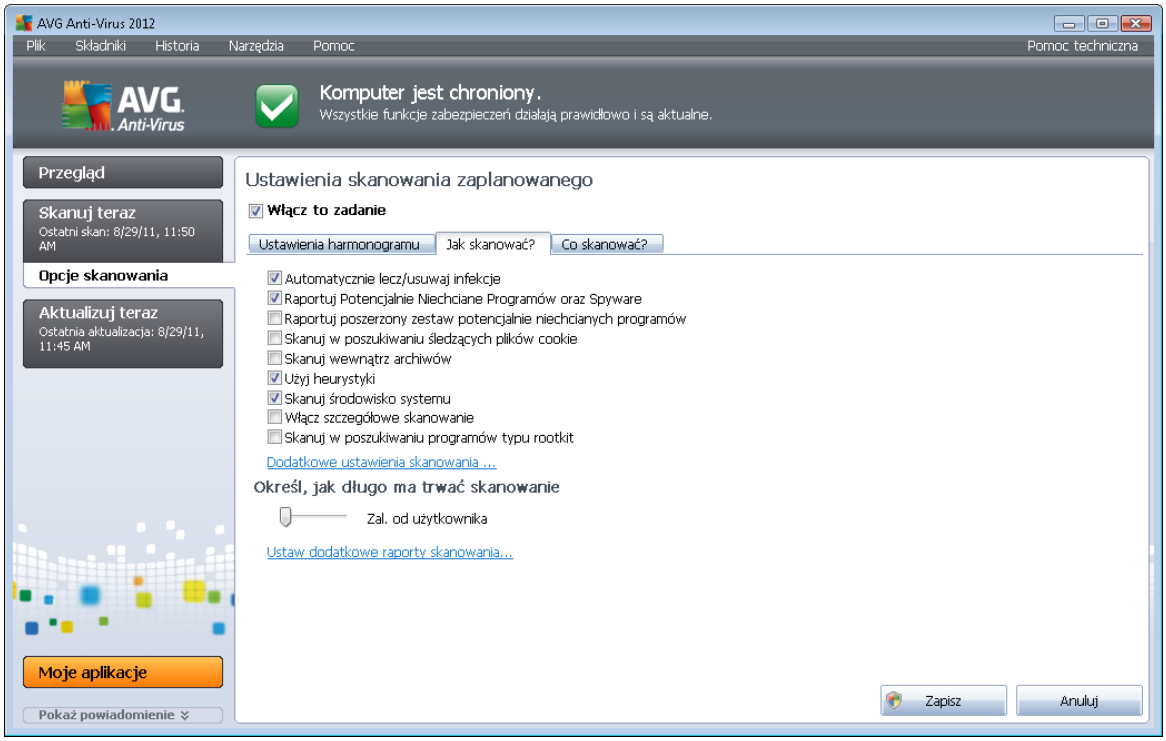
Na wszystkich trzech kartach okna dialogowego ***Konfiguracja skanu zaplanowanego*** (*Ustawienia*

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 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.

10.5.2. 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.

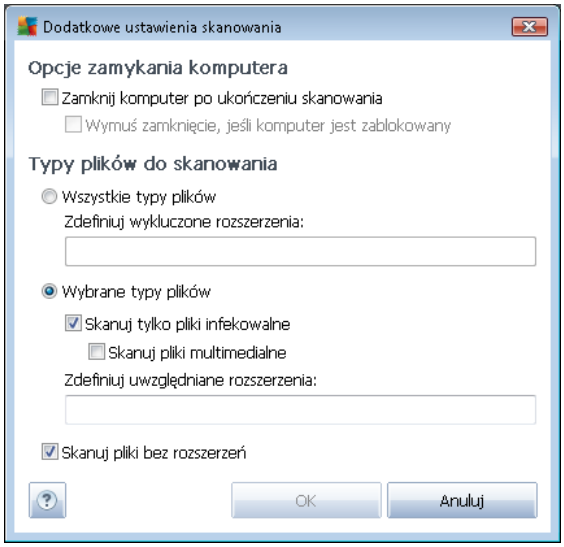
- ***Skanuj środowisko systemu*** (*opcja domyślnie włączona*) - skanowanie obejmie także obszary systemowe komputera.

- ***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.

- ***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 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***).

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

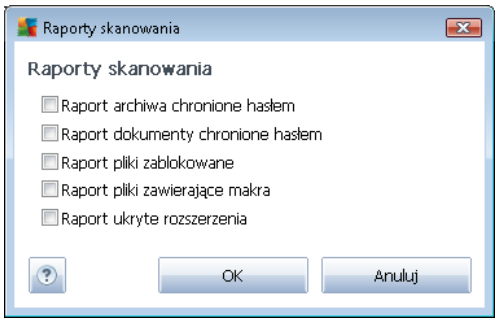
  - ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być skanowane;

  - ***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:



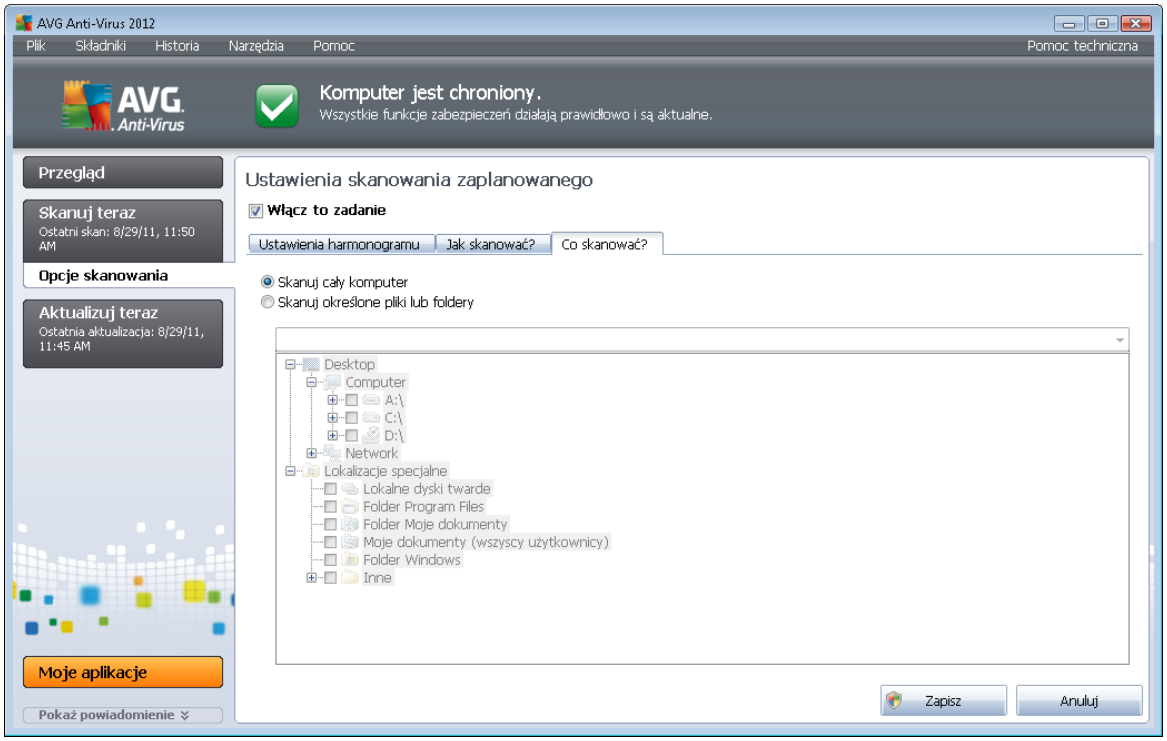
Przyciski kontrolne

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 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.

10.5.3. 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\

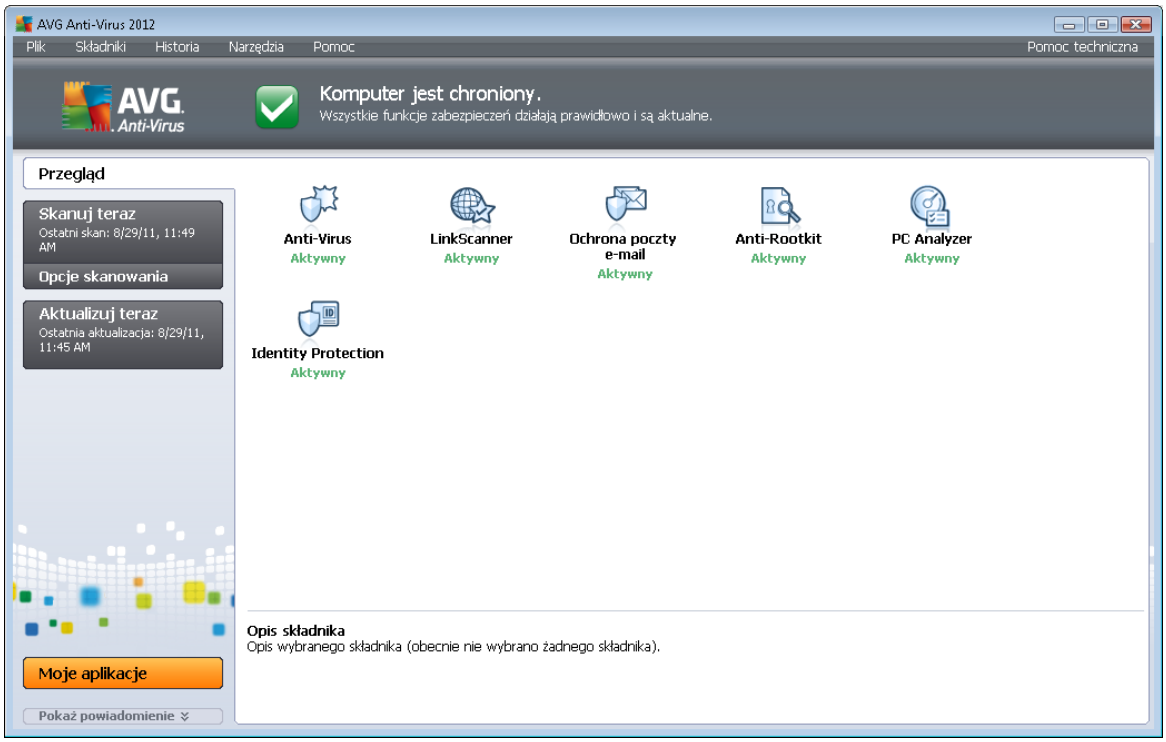
- ***Moje dokumenty (wszyscy użytkownicy)***
  - *dla systemu Win XP*: C:\Documents and Settings\All Users\Documents\
  - *dla systemu Windows Vista/7*: C:\Users\Public\Documents\
- ***Folder Windows*** - C:\Windows\
- ***Inne***
  - *Dysk systemowy* - dysk twardy, na którym zainstalowany jest system 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

Na wszystkich trzech kartach okna ***Ustawienia skanu zaplanowanego*** *(Ustawienia harmonogramu, Jak skanować i Co skanować)*:

- ***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.

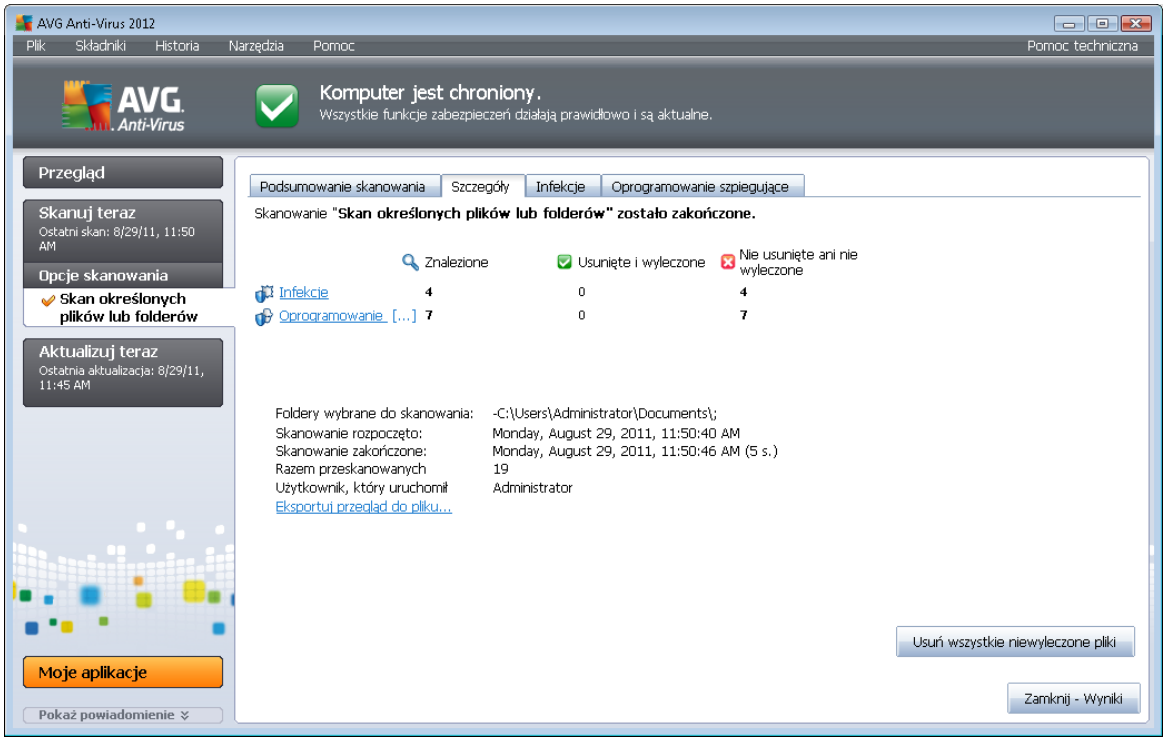
10.7. Szczegóły wyników skanowania

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. Ponadto, znajdziesz tu 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:

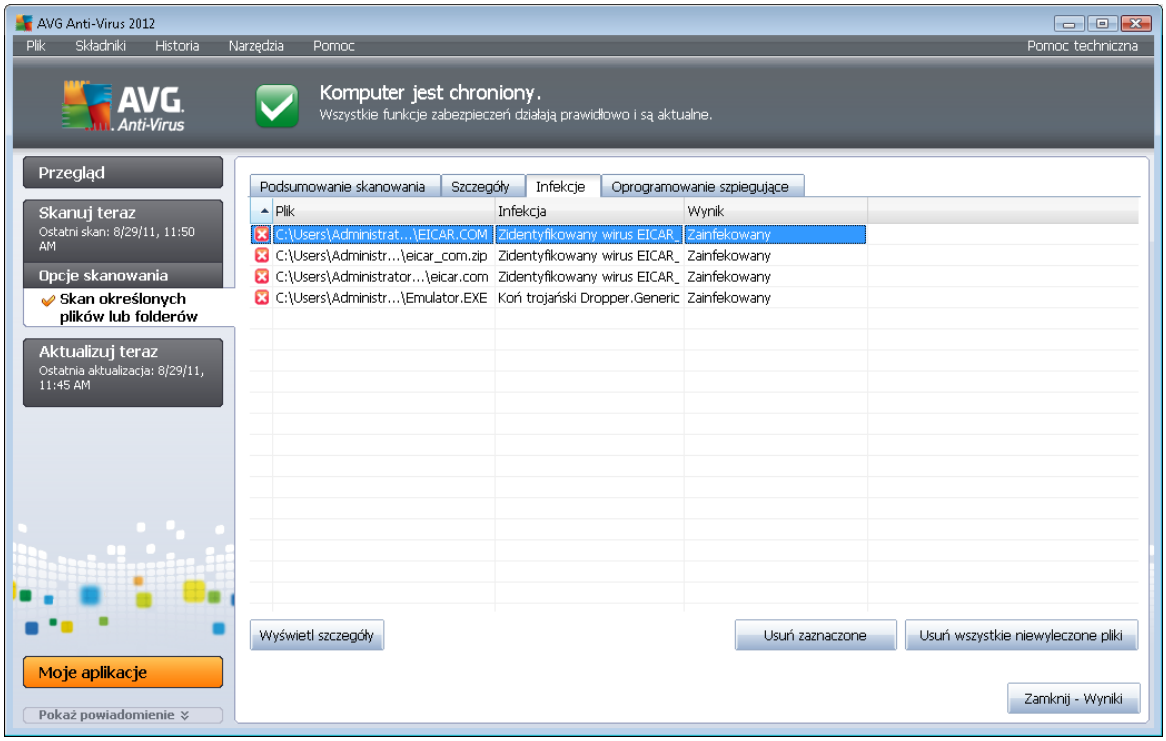
- wykryte infekcje wirusowe / oprogramowanie szpiegujące
- usunięte infekcje wirusowe / oprogramowanie szpiegujące
- liczbie infekcji wirusowych/programów szpiegujących, których nie udało się usunąć ani wyleczyć.

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*

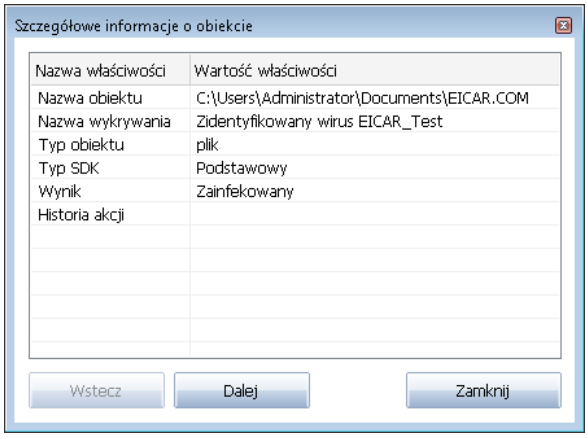
oknie Wyjątki i PNP)

- ***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:

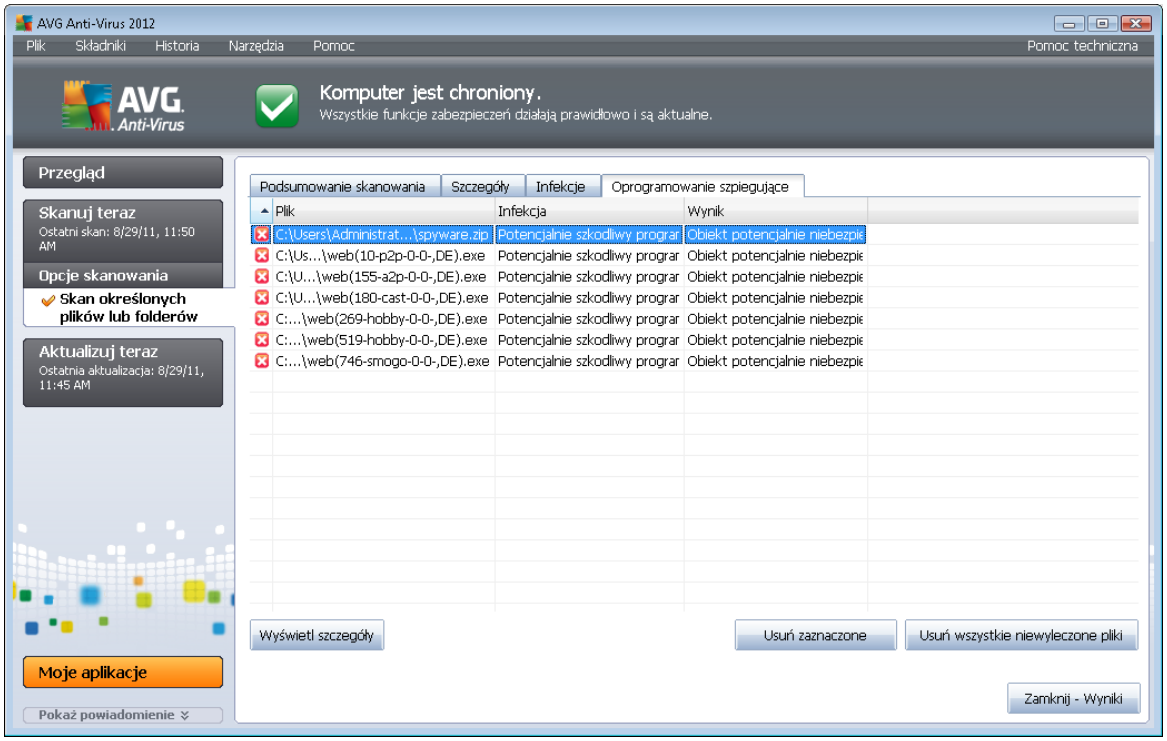
- ***Wyświetl szczegóły*** - otwiera nowe okno dialogowe ze ***szczegółowymi informacjami o obiekcie***:



  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:

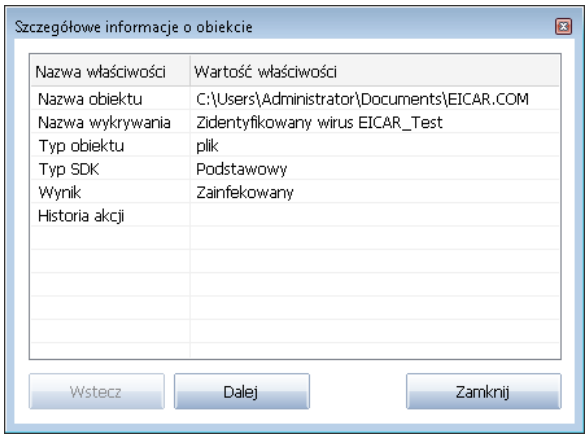
- ***Plik*** - pełna ścieżka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** - nazwa wykrytego oprogramowania szpiegującego (*szczegółowe informacje na temat wirusów zawiera Encyklopedia wirusów dostępna online*
- ***Wynik*** - określa bieżący stan obiektu, który wykryto podczas skanowania:
    - ***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 Anti-Virus 2012** 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. **AVG Anti-Virus 2012** Jeśli system zgłasza obecność ukrytego pliku, który wydaje się 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. Skan **AVG** jest w stanie wykryć pliki, które mogą nie być zainfekowane, ale są podejrzane. Zgłaszane będą one jako Ostrzeżenie 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 system **AVG Anti-Virus 2012** (*ani generalnie przez żaden inny program chroniący przed szkodliwym oprogramowaniem*).

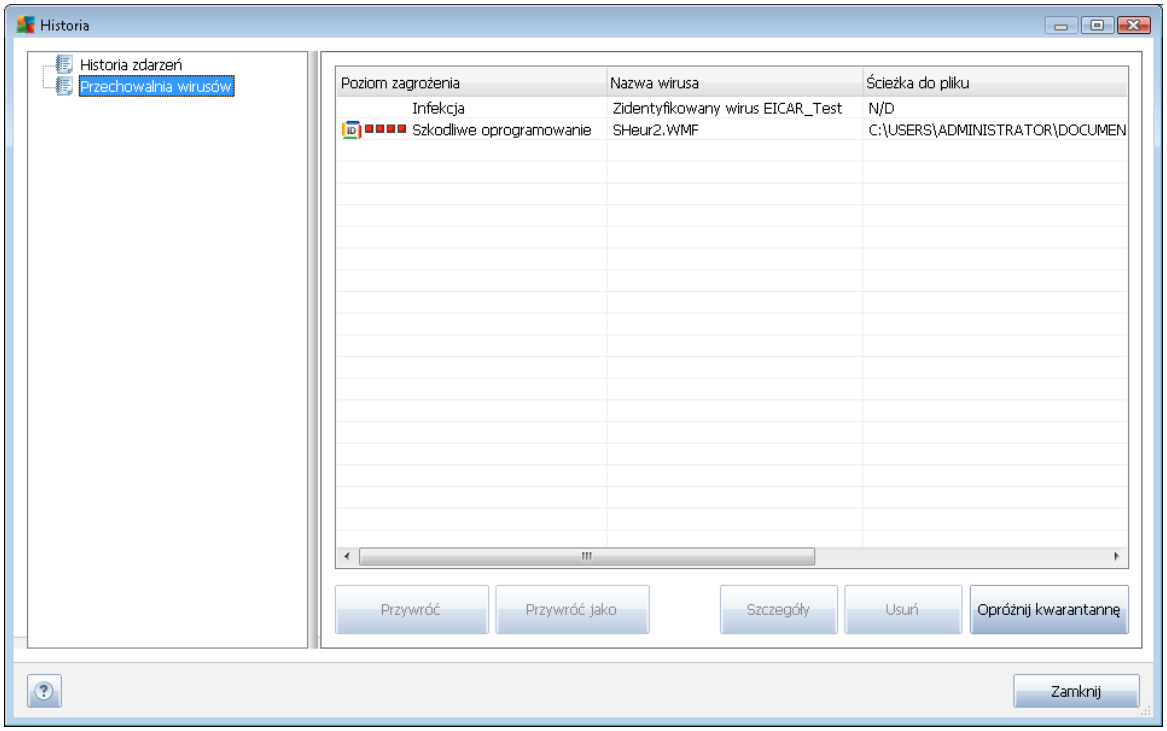
- ***Dokument zawierający makra*** - zgłoszone dokumenty zawierają makra, które mogą być szkodliwe.

- ***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 Anti-Virus 2012** 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 zgłasza tę niezgodność. **AVG Anti-Virus 2012** 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 Anti-Virus 2012**. 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.

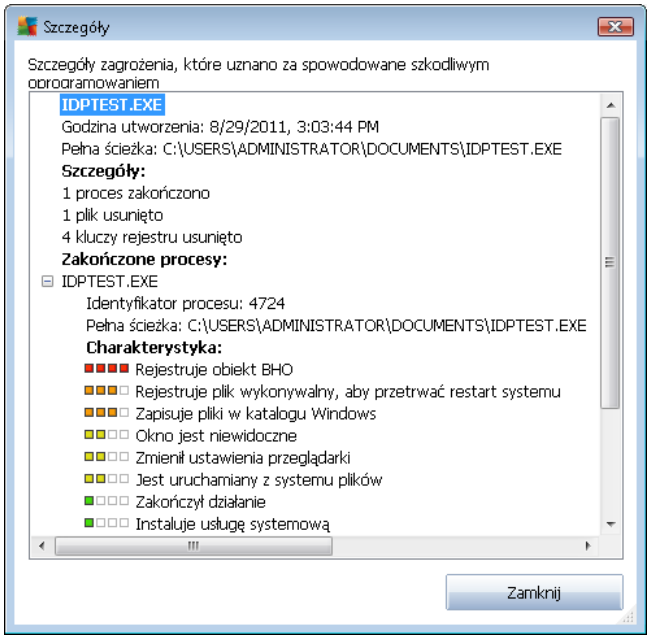
Interfejs ***Przechowalni wirusów*** jest otwierany w nowym oknie i zawiera przegląd informacji o izolowanych, zainfekowanych obiektach:

- ***Zagrożenie*** - jeśli w systemie został zainstalowany składnik Identity Protection**AVG Anti-Virus 2012**, 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

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.

Biorąc pod uwagę ilość nowo powstających zagrożeń internetowych oraz prędkość z jaką się rozprzestrzeniają, regularna aktualizacja systemu **AVG Anti-Virus 2012** jest absolutnie niezbędna. Najlepszym rozwiązaniem jest w tym wypadku pozostawienie domyślnych ustawień automatycznej aktualizacji. Przypominamy, że jeśli baza wirusów lokalnego systemu **AVG Anti-Virus 2012** jest nieaktualna, wykrycie najnowszych zagrożeń może być niemożliwe!

Regularne aktualizacje systemu AVG są kluczowe dla Twojego bezpieczeństwa! Jeśli jest to możliwe, definicje wirusów należy pobierać codziennie. Mniej istotne aktualizacje programu można pobierać co tydzień.

11.1. Uruchomienie aktualizacji

Aby zapewnić maksymalną dostępną ochronę, produkt **AVG Anti-Virus 2012** domyślnie sprawdza dostępność nowych aktualizacji co 4 godziny. Aktualizacje sytemu AVG nie są publikowane zgodnie z jakimkolwiek harmonogramem - powstają jako reakcja na pojawiające się zagrożenia. Sprawdzanie dostępności aktualizacji jest kluczowym czynnikiem zapewniającym skuteczność bazy wirusów.

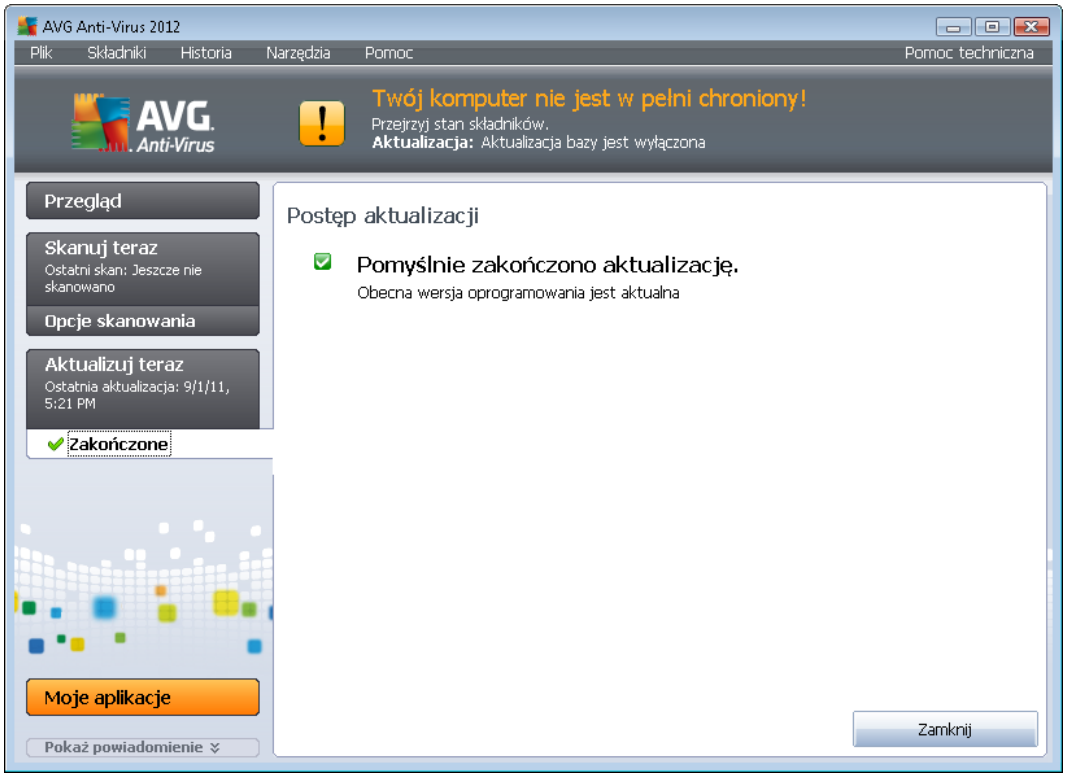
Jeżeli chcesz zmniejszyć ilość uruchamianych procesów aktualizacji, możesz ustalić swój własny harmonogram. Stanowczo zalecamy jednak uruchamianie aktualizacji minimum raz dziennie! Wspomniana konfiguracja dostępna jest w sekcji Ustawienia zaawansowane / Harmonogramy, na następujących ekranach:

- Harmonogram aktualizacji definicji
- Harmonogram aktualizacji programu

Jeżeli chcesz natychmiastowo sprawdzić dostępność nowych definicji, użyj szybkiego linku Aktualizuj teraz. Jest on widoczny przez cały czas w głównym oknie interfejsu użytkownika.

11.2. Postęp aktualizacji

Po uruchomieniu tego procesu program AVG sprawdza, czy dostępne są nowe pliki aktualizacyjne. Jeśli tak, system **AVG Anti-Virus 2012** rozpocznie ich pobieranie i sam uruchomi 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 każdą aktualizacją programu głównego AVG tworzony jest punkt przywracania systemu. W przypadku niepowodzenia aktualizacji i awarii systemu operacyjnego, można odtworzyć pierwotną konfigurację systemu, używając tego punktu. Aby użyć tej opcji, należy wybrać kolejno: Start / Wszystkie Programy / Akcesoria / Narzędzia systemowe / Przywracanie systemu. Zalecane tylko doświadczonym użytkownikom!*

11.3. Poziomy aktualizacji

AVG Anti-Virus 2012 oferuje dwa poziomy aktualizacji:

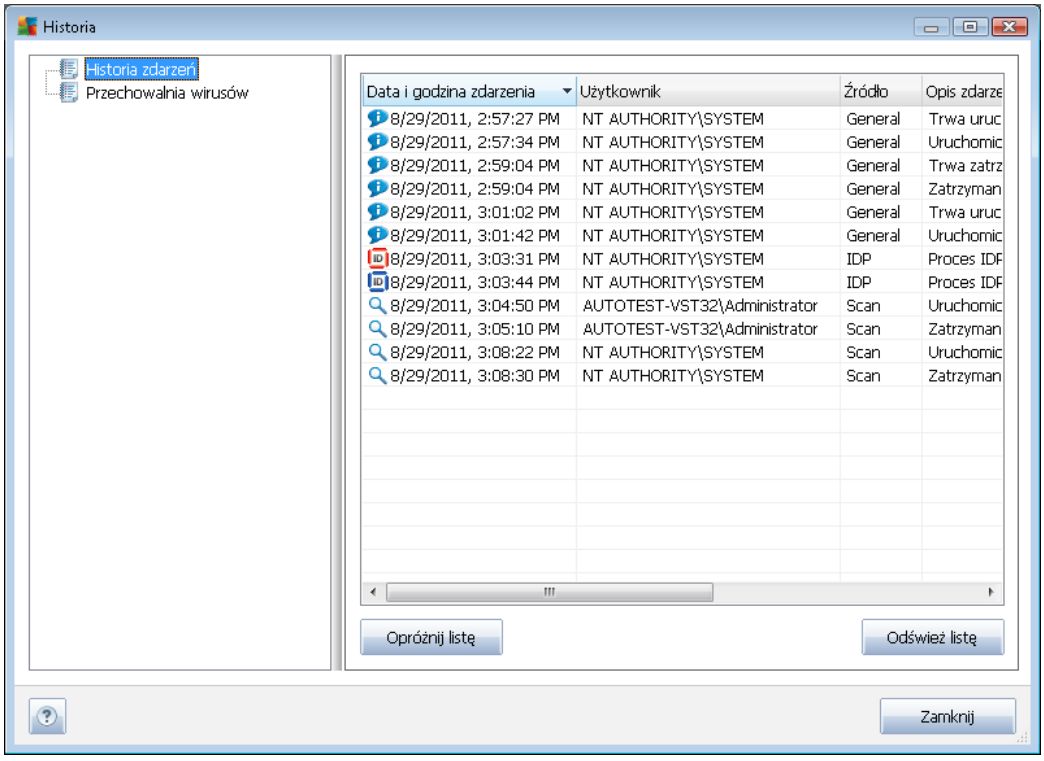
- ***Aktualizacja definicji*** zawiera uzupełnienia niezbędne do zapewnienia niezawodnej ochrony antywirusowej. Na ogół nie zawiera modyfikacji programu i aktualizuje tylko bazę definicji. Ta aktualizacja powinna zostać zastosowana, gdy tylko będzie dostępna.
- ***Aktualizacja programu*** zawiera różne zmiany w programie głównym, oraz poprawki i udoskonalenia.

Podczas planowania aktualizacji można zdefiniować jej parametry dla każdego z poziomów:

- Harmonogram aktualizacji definicji
- Harmonogram aktualizacji programu

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

12. Dziennik historii



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 2012**. ***Historia*** zawiera rekordy następujących typów zdarzeń:

- Informacje o aktualizacjach oprogramowania AVG;
- Informacje o rozpoczęciu lub zakończeniu skanów (*również tych zaplanowanych*)
- Informacje dotyczące wykrytych wirusów (*zarówno przez Ochronę rezydentną jak i zwykłe skanowanie*), wraz z ich lokalizacją
- Inne ważne zdarzenia.

Dla każdego zdarzenia wyświetlane są następujące informacje:

- ***Data i godzina zdarzenia*** określa dokładną datę i czas wystąpienia zdarzenia
- ***Użytkownik*** states the name of the user currently logged in at the time of the event occurrence
- ***Źródło*** podaje nazwę składnika lub innej części systemu AVG, która wywołała zdarzenie
- ***Opis zdarzenia*** - przedstawia krótkie podsumowanie zdarzenia.

Przyciski kontrolne

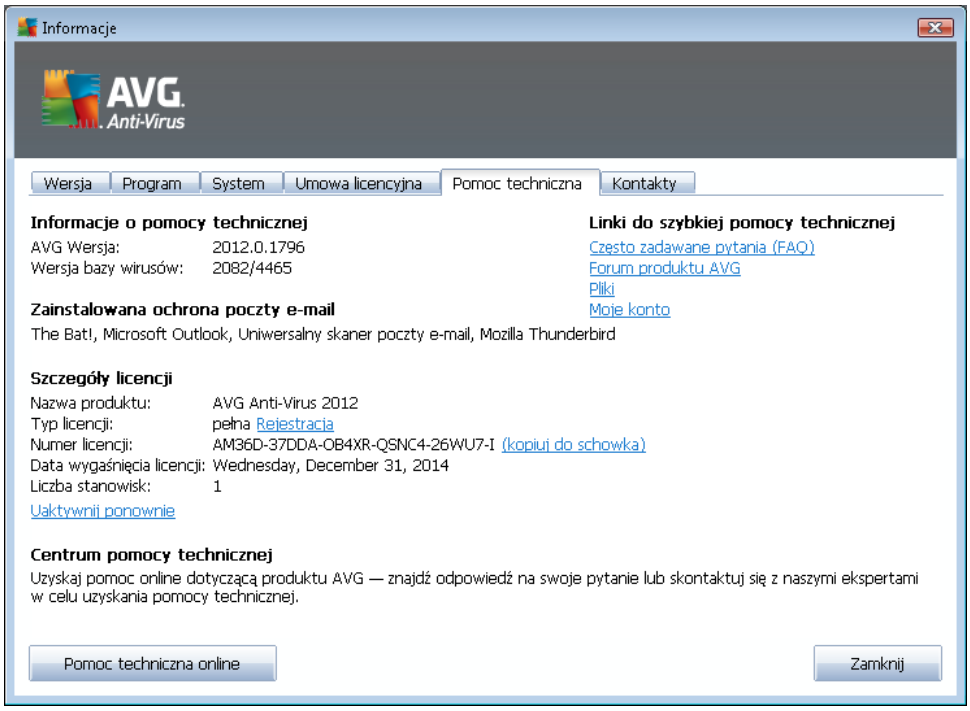
- ***Opróżnij listę*** - powoduje usunięcie wszystkich wpisów z listy
- ***Odśwież listę*** - powoduje odświeżenie całej listy

13. FAQ i pomoc techniczna

Jeżeli masz jakiekolwiek pytania natury technicznej lub handlowej (dotyczące produktów **AVG Anti-Virus 2012**), istnieje kilka sposobów uzyskania pomocy. Wybierz jedną z poniższych opcji:

- ***Skontaktuj się z Pomocą techniczną***: Możesz skontaktować się z zespołem Pomocy technicznej bezpośrednio z poziomu aplikacji AVG. Wybierz z głównego menu ***Pomoc / Uzyskaj pomoc online***, aby przejść do formularza online, który pozwoli Ci skontaktować się z nami - 24 godziny na dobę, 7 dni w tygodniu. Twój numer licencji zostanie wypełniony automatycznie. Więcej informacji znajdziesz na wspomnianej wyżej stronie internetowej.

- ***Pomoc techniczna (link w menu głównym)***: Menu aplikacji AVG (*w górnej części interfejsu użytkownika*) zawiera link ***Pomoc techniczna***, który otwiera nowe okno, zawierające wszystkie dane potrzebne przy poszukiwaniu pomocy. Znajdują się tam podstawowe informacje o zainstalowanym systemie AVG (*wersja programu i bazy wirusów*), szczegóły licencji oraz lista przydatnych linków:



- ***Rozwiązywanie problemów przy użyciu plików pomocy***: Pliki pomocy systemu **AVG Anti-Virus 2012** wzbogaciły się teraz o nową sekcję - ***Rozwiązywanie problemów***. Zawiera ona listę najczęściej występujących sytuacji, w których użytkownik może poszukiwać pomocy. Wybierz sytuację, która najlepiej opisuje Twój problem, aby otworzyć okno ze szczegółowymi instrukcjami jego rozwiązania.

- ***Centrum Pomocy technicznej na stronie AVG***: Możesz również poszukać rozwiązania problemu na stronie AVG (http://www.avg.com/). W sekcji ***Pomoc techniczna*** znajdziesz uporządkowaną strukturę tematów opisujących kwestie handlowe i techniczne.

- ***Często zadawane pytania***: Na stronie AVG (http://www.avg.com/) opublikowana jest również obszerna sekcja często zadawanych pytań. Można się do niej dostać poprzez

menu ***Centrum Pomocy technicznej / FAQ***. Wszystkie pytania podzielone są w czytelny sposób na sekcje: handlową, techniczną i na temat wirusów.

- ***Informacje o wirusach i zagrożeniach***: Jedna z części naszej witryny internetowej (http://www.avg.com/) poświęcona jest w całości kwestii wirusów. Z menu wybierz ***Centrum Pomocy technicznej / Informacje o wirusach i zagrożeniach***, aby przejść na stronę internetową zawierającą uporządkowane logicznie informacje o zagrożeniach online. Znajdziesz tam również instrukcje dotyczące usuwania wirusów i oprogramowania szpiegującego, a także porady dotyczące bezpieczeństwa.

- ***Forum dyskusyjne***: Możesz także skorzystać z forum użytkowników systemu AVG, zlokalizowanego pod adresem http://forums.avg.com.