

AVG 9 Internet Security

Podrecznik uzytkownika

Wersja dokumentu 90.6 (14.9.2009)

Copyright AVG Technologies CZ, s.r.o. Wszelkie prawa zastrzezone.
Wszystkie pozostale znaki towarowe sa wlasnoscia ich wlasncieli.

W produkcie zastosowano algorytm MD5 Message-Digest Algorithm firmy RSA Data Security, Inc. utworzony w roku 1991, Copyright (C) 1991-2, RSA Data Security, Inc.

W produkcie wykorzystywany jest kod z biblioteki C-SaCzech. Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

W produkcie zastosowano biblioteki do kompresji zlib, Copyright (c) 1995-2002 Jean-loup Gailly i Mark Adler. Ten produkt wykorzystuje biblioteki do kompresji libbzip2. Copyright (c) 1996-2002 Julian R. Seward.

Spis treści

1. Wprowadzenie	8
2. Wymagania instalacyjne AVG	9
2.1 Obsługiwane systemy operacyjne	9
2.2 Minimalne wymagania sprzętowe	9
3. Opcje instalacji systemu AVG	10
4. AVG Download Manager	11
4.1 Wybór języka	11
4.2 Test połączenia	12
4.3 Ustawienia proxy	13
4.4 Wybór typu licencji	14
4.5 Pobieranie plików instalacyjnych	15
5. Proces instalacji systemu AVG	16
5.1 Uruchamianie instalacji	16
5.2 Umowa licencyjna	17
5.3 Sprawdzanie stanu systemu	17
5.4 Wybieranie typu instalacji	18
5.5 Uaktywnienie licencji AVG	18
5.6 Instalacja niestandardowa — Folder docelowy	20
5.7 Instalacja niestandardowa — Wybór składników	21
5.8 AVG DataCenter	22
5.9 Pasek narzędzi AVG Security Toolbar	23
5.10 Instalowanie systemu AVG	24
5.11 Zaplanowanie regularnych skanów i aktualizacji	25
5.12 Wybór typu komputera	25
5.13 Architektura sieciowa komputera	26
5.14 Konfiguracja ochrony systemu AVG została ukończona	27
6. Po instalacji	28
6.1 Rejestracja produktu	28
6.2 Dostęp do Interfejsu użytkownika	28
6.3 Skanowanie całego komputera	28
6.4 Test Eicar	28

6.5 Konfiguracja domyślna AVG	29
7. Interfejs użytkownika AVG	30
7.1 Menu systemowe	31
7.1.1 Plik	31
7.1.2 Składniki	31
7.1.3 Historia	31
7.1.4 Narzędzia	31
7.1.5 Pomoc	31
7.2 Status bezpieczeństwa	34
7.3 Linki	35
7.4 Przegląd składników	36
7.5 Statystyki	37
7.6 Ikona na pasku zadań	37
8. Składniki AVG	39
8.1 Anti-Virus	39
8.1.1 Zasady działania składnika Anti-Virus	39
8.1.2 Interfejs składnika Anti-Virus	39
8.2 Anti-Spyware	41
8.2.1 Zasady działania składnika Anti-Spyware	41
8.2.2 Interfejs składnika Anti-Spyware	41
8.3 Anti-Spam	43
8.3.1 Zasady działania składnika Anti-Spam	43
8.3.2 Interfejs składnika Anti-Spam	43
8.4 Anti-Rootkit	45
8.4.1 Zasady działania składnika Anti-Rootkit	45
8.4.2 Interfejs składnika Anti-Rootkit	45
8.5 Narzędzia systemowe	47
8.5.1 Procesy	47
8.5.2 Połączenia sieciowe	47
8.5.3 Autostart	47
8.5.4 Rozszerzenia przeglądarki	47
8.5.5 Przeglądarka LSP	47
8.6 Zapora	54
8.6.1 Zasady działania Zapory	54
8.6.2 Profile Zapory	54
8.6.3 Interfejs Zapory	54

8.7 Skaner poczty e-mail	59
8.7.1 Zasady działania Skanera poczty e-mail	59
8.7.2 Interfejs Skanera poczty e-mail	59
8.7.3 Zagrozenia wykryte przez Skaner poczty e-mail	59
8.8 Skladnik ID Protection	63
8.8.1 Podstawy działania ID Protection	63
8.8.2 Interfejs skladnika ID Protection	63
8.9 Licencja	66
8.10 LinkScanner	67
8.10.1 Zasady działania technologii LinkScanner	67
8.10.2 Interfejs LinkScanner	67
8.10.3 AVG Search-Shield	67
8.10.4 AVG Active Surf-Shield	67
8.11 Ochrona sieci WWW	70
8.11.1 Zasady działania skladnika Ochrona sieci WWW	70
8.11.2 Interfejs skladnika Ochrona sieci WWW	70
8.11.3 Zagrozenia wykryte przez Ochrone sieci WWW	70
8.12 Ochrona rezydentna	76
8.12.1 Zasady działania Ochrony rezydentnej	76
8.12.2 Interfejs skladnika Ochrona rezydentna	76
8.12.3 Zagrozenia wykryte przez Ochrone rezydentna	76
8.13 Menedzer aktualizacji	81
8.13.1 Zasady działania Menedzera aktualizacji	81
8.13.2 Interfejs Menedzera aktualizacji	81
8.14 Pasek narzedzi AVG Security Toolbar	84
8.14.1 Interfejs paska narzedzi AVG Security Toolbar	84
8.14.2 Opcje Paska narzedzi AVG Security Toolbar	84

9. Zaawansowane ustawienia AVG 91

9.1 Wyglad	91
9.2 Dzwieki	93
9.3 Ignoruj bledny stan skladników	95
9.4 AVG Identity Protection	96
9.4.1 Ustawienia skladnika Identity Protection	96
9.4.2 Lista dozwolonych	96
9.5 Przechowalnia wirusów	100
9.6 Wyjatki PNP	101
9.7 Anti-Spam	103

9.7.1 Ustawienia	103
9.7.2 Wydajność	103
9.7.3 RBL	103
9.7.4 Biała lista	103
9.7.5 Czarna lista	103
9.7.6 Ustawienia zaawansowane	103
9.8 Ochrona sieci WWW	115
9.8.1 Ochrona WWW	115
9.8.2 Komunikatory internetowe	115
9.9 LinkScanner	119
9.10 Skany	120
9.10.1 Skan całego komputera	120
9.10.2 Skan rozszerzenia powłoki	120
9.10.3 Skan określonych plików lub folderów	120
9.10.4 Skan urządzeń wymiennych	120
9.11 Zaplanowane zadania	127
9.11.1 Skan zaplanowany	127
9.11.2 Harmonogram aktualizacji bazy wirusów	127
9.11.3 Harmonogram aktualizacji programu	127
9.11.4 Harmonogram aktualizacji składnika Anti-Spam	127
9.12 Skaner poczty e-mail	139
9.12.1 Certyfikacja	139
9.12.2 Filtrowanie poczty	139
9.12.3 Dzienniki i Wyniki	139
9.12.4 Serwery	139
9.13 Ochrona rezydentna	147
9.13.1 Ustawienia zaawansowane	147
9.13.2 Wykluczenia katalogów	147
9.13.3 Wykluczone pliki	147
9.14 Anti-Rootkit	152
9.15 Aktualizacja	153
9.15.1 Proxy	153
9.15.2 Połączenie telefoniczne	153
9.15.3 URL	153
9.15.4 Zarządzaj	153
9.16 Administracja zdalna	160
10. Ustawienia Zapory	162

10.1 Ogólne	162
10.2 Bezpieczeństwo	163
10.3 Profile kart sieciowych i obszarów	164
10.4 Dzienniki	165
10.5 Profile	167
10.5.1 Informacje o profilu	167
10.5.2 Zdefiniowane sieci	167
10.5.3 Aplikacje	167
10.5.4 Usługi systemowe	167
11. Skanowanie AVG	179
11.1 Interfejs skanowania	179
11.2 Wstępnie zdefiniowane testy	180
11.2.1 Skan całego komputera	180
11.2.2 Skan określonych plików lub folderów	180
11.2.3 Skan Anti-Rootkit	180
11.3 Skan z poziomu eksploratora systemu Windows	190
11.4 Skan z poziomu wiersza poleceń	191
11.4.1 Parametry skanowania z wiersza poleceń	191
11.5 Planowanie skanowania	194
11.5.1 Ustawienia harmonogramu	194
11.5.2 Jak skanować?	194
11.5.3 Co skanować?	194
11.6 Przegląd wyników skanowania	204
11.7 Szczegóły wyników skanowania	205
11.7.1 Karta "Przegląd wyników"	205
11.7.2 Karta "Infekcje"	205
11.7.3 Karta "Oprogramowanie szpiegujące"	205
11.7.4 Karta "Ostrzeżenia"	205
11.7.5 Karta "Rootkity"	205
11.7.6 Karta "Informacje"	205
11.8 Przechowywanie wirusów	214
12. Aktualizacje AVG	216
12.1 Poziomy aktualizacji	216
12.2 Typy aktualizacji	216
12.3 Proces aktualizacji	217
13. Historia zdarzeń	218

14. FAQ i pomoc techniczna	220
---	------------

1. Wprowadzenie

Ten podręcznik użytkownika zawiera dokumentację systemu **AVG 9 Internet Security**.

Gratulujemy zakupu produktu AVG 9 Internet Security!

AVG 9 Internet Security należy do linii uznanych i nagradzanych produktów AVG, które zapewniają użytkownikom spokój ducha, a ich komputerom — pełne bezpieczeństwo. Podobnie jak pozostałe produkty AVG, **AVG 9 Internet Security** zaprojektowano od podstaw pod kątem zapewnienia słynnego już poziomu ochrony, w nowy, bardziej przyjazny dla użytkownika sposób.

Najnowszy produkt **AVG 9 Internet Security** zyskał poprawiony interfejs oraz bardziej agresywny i szybszy silnik skanujący. Dla wygody użytkownika zautomatyzowano najczęściej używane funkcje i dodano nowe, „inteligentne” opcje, które pozwalają precyzyjnie dostosować funkcje ochronne programu do swoich potrzeb. Koniec z poświęcaniem wydajności na rzecz ochrony!

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

2. Wymagania instalacyjne AVG

2.1. Obsługiwane systemy operacyjne

AVG 9 Internet Security jest przeznaczony do ochrony stacji roboczych z następującymi systemami operacyjnymi:

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

(a także z nowszymi dodatkami service pack dla niektórych systemów operacyjnych)

Uwaga: Składnik [*ID Protection*](#) nie jest obsługiwany przez systemy Windows 2000 i XP x64. Na tych systemach operacyjnych można zainstalować system AVG 9 Internet Security tylko bez składnika IDP.

2.2. Minimalne wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG 9 Internet Security** są następujące:

- Procesor Intel Pentium 1,2 GHz
- 250 MB wolnego miejsca na dysku twardym (na potrzeby instalacji),
- 256 MB pamięci RAM.

3. Opcje instalacji systemu AVG

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

Przed rozpoczęciem instalacji systemu AVG zalecamy odwiedzenie naszej witryny (<http://www.avg.com/>) w celu sprawdzenia, czy jest dostępny nowy plik instalacyjny. W ten sposób zyskasz pewność, że zostanie zainstalowana najnowsza wersja systemu AVG 9 Internet Security.

Zalecamy także wypróbowanie nowego narzędzia — [AVG Download Manager](#) pomoże Ci wybrać odpowiedni plik instalacyjny!

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

4. AVG Download Manager

AVG Download Manager to proste narzędzie pomagające wybrać odpowiedni plik instalacyjny dla danego produktu AVG. Na podstawie wprowadzonych przez użytkownika informacji, menedżer wybierze odpowiedni produkt, typ licencji, zestaw składników i język. Na koniec **AVG Download Manager** pobierze odpowiednie pliki i rozpocznie [proces instalacji](#).

Ostrzeżenie: Program AVG Download Manager nie jest odpowiedni do pobierania wersji sieciowych oraz SBS i obsługuje tylko następujące systemy operacyjne: Windows 2000 (SP4 + pakiet zbiorczy SRP), Windows XP (SP2 i nowsze), Windows Vista (wszystkie wersje).

AVG Download Manager jest dostępny do pobrania z witryny systemu AVG (<http://www.avg.com/>). Poniżej znajduje się krótki opis wszystkich kroków, przez które przeprowadzi Cię **AVG Download Manager**:

4.1. Wybór języka



AVG Download Manager pozwoli w pierwszym kroku wybrać język instalacji. Należy pamiętać, że wybór ten dotyczy tylko procesu instalacji; po jej zakończeniu język programu będzie można zmienić bezpośrednio w jego ustawieniach. Aby kontynuować, kliknij przycisk **Dalej**.

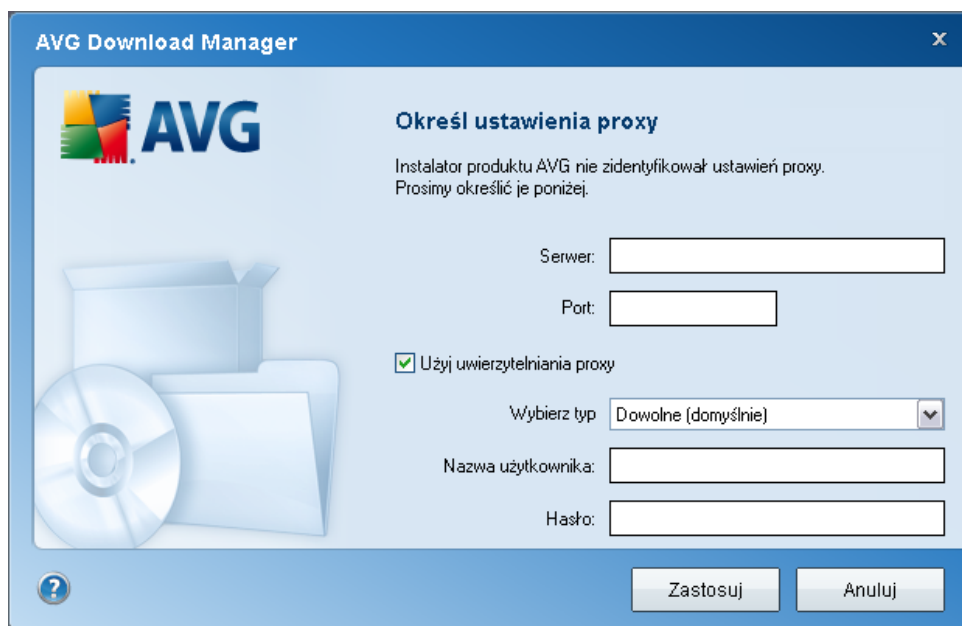
4.2. Test połączenia

W następnym kroku **AVG Download Manager** próbuje nawiązać łączność z serwerem aktualizacyjnym. Przejście dalej nie będzie możliwe, dopóki **AVG Download Manager** nie zakończy testu połączenia.

- Jeśli test wykaze brak łączności, należy upewnić się, że komputer jest faktycznie połączony z internetem. Aby ponowić próbę, kliknij przycisk **Powtórz**

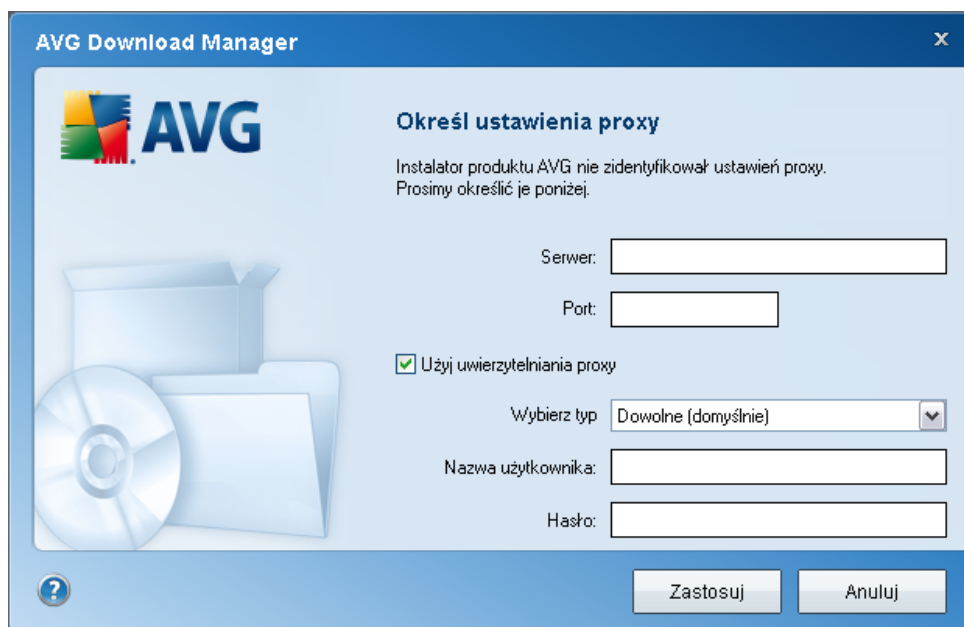


- Jeśli używasz serwera proxy, kliknij przycisk **Ustawienia proxy** i podaj [wymagane szczegóły](#):



- Jeśli test wypadł pomyślnie, kliknij przycisk **Dalej**, aby kontynuować.

4.3. Ustawienia proxy



Jeśli **AVG Download Manager** nie może zidentyfikować ustawień proxy, trzeba określić je ręcznie. Podaj następujące informacje:

- **Serwer** — prawidłowa nazwa lub adres IP serwera proxy.
- **Port** — odpowiedni numer portu.
- **Użyj uwierzytelniania proxy** — zaznacz to pole, jeśli Twój serwer proxy wymaga uwierzytelniania.
- **Wybierz typ uwierzytelniania** — wybierz z listy rozwijanej typ uwierzytelniania. Stanowczo zalecamy, aby zachować wartość domyślną (*serwer sam podaje swoje wymagania*). Doświadczeni użytkownicy mogą jednak wybrać opcję "Podstawowe" (*wymagane przez niektóre serwery*) lub "NTLM" (*wymagane przez wszystkie serwery ISA*). Następnie podaj prawidłową **Nazwę użytkownika** i **Hasło** (opcjonalnie).

Po potwierdzeniu ustawień (za pomocą przycisku **Zastosuj**), **AVG Download Manager** automatycznie przejdzie do następnego kroku.

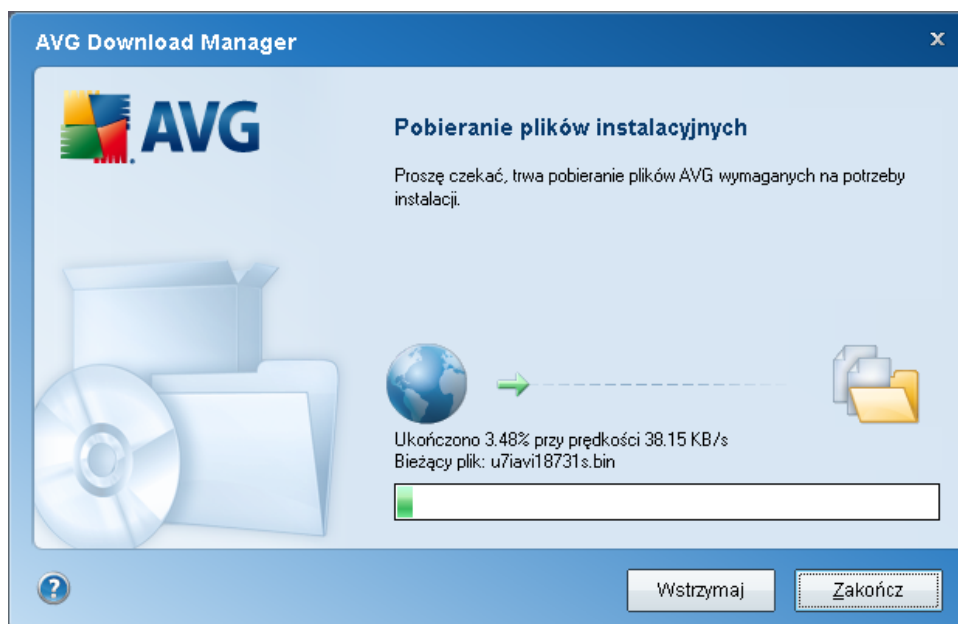
4.4. Wybór typu licencji



W tym kroku należy wybrać typ licencji produktu, który ma zostać pobrany. Dostępne typy to:

- **Wersja pełna** — tj. **AVG Anti-Virus**, **AVG Anti-Virus plus Firewall** lub **AVG Internet Security**.
- **Wersja próbna** — daje możliwość wypróbowania wszystkich funkcji wersji pełnej przez okres 30 dni.
- **Wersja bezpłatna** — oferuje bezpłatną ochronę użytkownikom prywatnym. Posiada jednak pewne ograniczenia. Wersja bezpłatna zapewnia tylko niektóre funkcje oferowane przez wersję komercyjną.

4.5. Pobieranie plików instalacyjnych



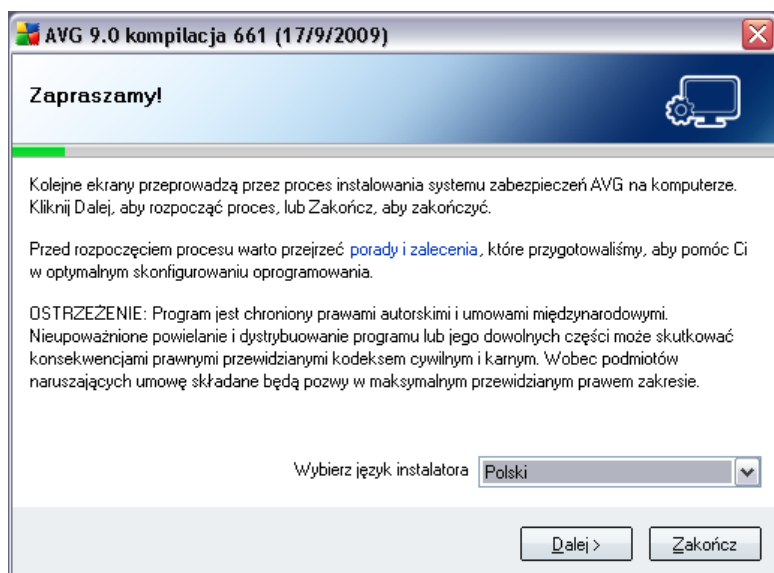
Wszystkie informacje, których **AVG Download Manager** potrzebuje do pobrania pakietów instalacyjnych i uruchomienia instalacji, zostały już podane. Można rozpocząć [instalację systemu AVG](#).

5. Proces instalacji systemu AVG

Aby zainstalować na komputerze system **AVG 9 Internet Security**, należy najpierw uzyskać dostęp do najnowszego instalatora programu. Można znaleźć go na dysku CD będącym częścią dystrybucyjnej edycji programu - istnieje jednak w tym wypadku ryzyko, że będzie on nieaktualny. Dlatego zaleca się pobranie najnowszego pliku instalacyjnego z internetu. Dostępny jest on na oficjalnej stronie AVG (<http://www.avg.com/>), w sekcji **Pobierz**. Można również użyć nowego narzędzia **AVG Download Manager**, które pomaga wybrać odpowiedni pakiet instalacyjny i automatycznie uruchamia proces instalacji.

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

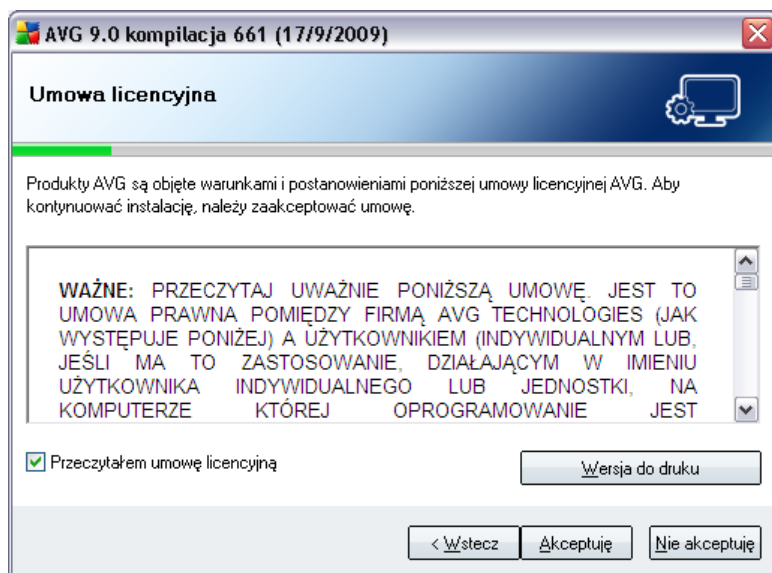
5.1. Uruchamianie instalacji



Proces instalacji rozpoczyna okno **Witamy w instalatorze AVG**. Można w nim wskazać język, który ma być używany podczas instalacji. W dolnej części okna znajdziesz menu **Wybierz język instalatora**. Kliknij przycisk **Dalej**, aby potwierdzić wybór i przejść do kolejnego ekranu.

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

5.2. Umowa licencyjna



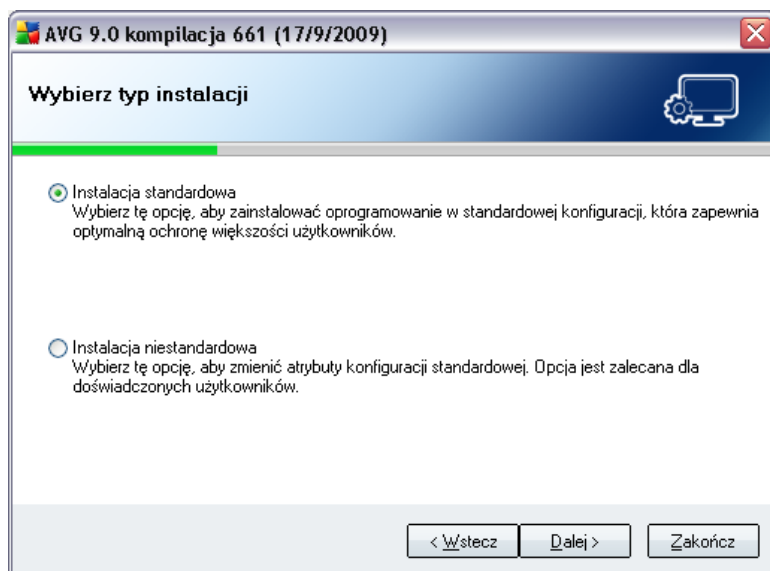
Okno dialogowe **Umowa licencyjna** zawiera pełną treść umowy licencyjnej AVG. Przeczytaj ją uważnie i potwierdź jej akceptację, zaznaczając pole **Przeczytałem warunki umowy licencyjnej** i wciskając przycisk **Dalej**.

Jeśli nie zgadzasz się na postanowienia umowy, kliknij przycisk **Nie akceptuję**; instalacja zostanie natychmiast przerwana.

5.3. Sprawdzanie stanu systemu

Po potwierdzeniu umowy licencyjnej nastąpi przekierowanie do okna **Sprawdzanie stanu systemu**. W oknie tym nie trzeba wykonywać żadnych czynności; system jest sprawdzany przed rozpoczęciem instalacji AVG. Należy poczekać na ukończenie procesu; przejście do kolejnego okna nastąpi automatycznie.

5.4. Wybieranie typu instalacji



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

Większość użytkowników zdecydowanie powinna wybrać opcję **instalacji standardowej**, która pozwala zainstalować system AVG w całkowicie zautomatyzowany sposób, z ustawieniami zdefiniowanymi przez dostawcę oprogramowania AVG. Taka konfiguracja zapewnia maksymalne bezpieczeństwo oraz optymalne wykorzystanie zasobów. Jeśli w przyszłości zajdzie potrzeba zmiany konfiguracji, można będzie to zrobić bezpośrednio z poziomu interfejsu AVG.

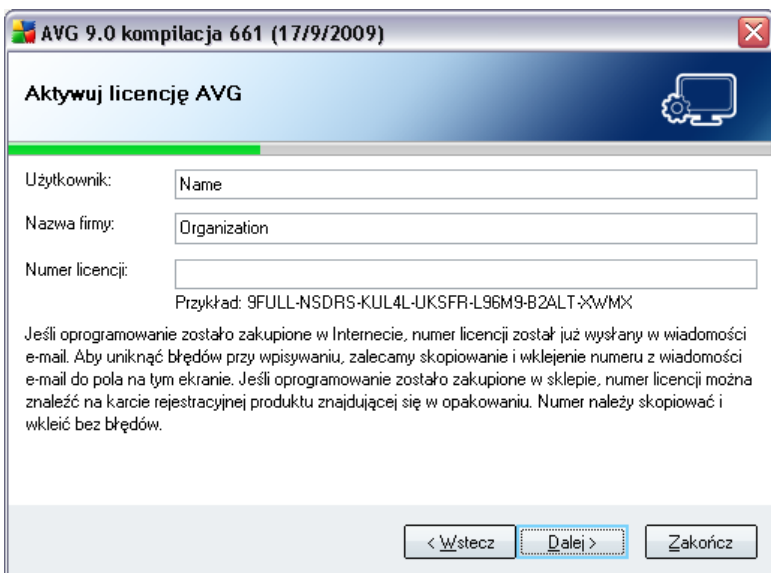
Instalacje niestandardowa powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować programu AVG z domyślnymi ustawieniami, np. na komputerach o specyficznej konfiguracji sprzętowej.

5.5. Uaktywnienie licencji AVG

W oknie dialogowym **Aktywacja licencji AVG** należy wprowadzić swoje dane rejestracyjne. W polu **Nazwa użytkownika** wpisz swoje imię i nazwisko, a w polu **Nazwa firmy** — nazwę organizacji.

Następnie wprowadz numer licencji (lub numer sprzedaży) w polu tekstowym **Numer licencji**. Numer sprzedaży znajduje się na opakowaniu dysku CD z oprogramowaniem **AVG 9 Internet Security**. Numer licencji jest wysyłany poprzez

e-mail po zakupieniu oprogramowania **AVG 9 Internet Security** online. Ważne jest dokładne wprowadzenie wspomnianego numeru. Jeśli numer jest dostępny w formie cyfrowej (w wiadomości e-mail), zaleca się skopiowanie go i wklejenie w odpowiednim polu.



AVG 9.0 kompilacja 661 (17/9/2009)

Aktywuj licencję AVG

Użytkownik:

Nazwa firmy:

Numer licencji:

Przykład: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX

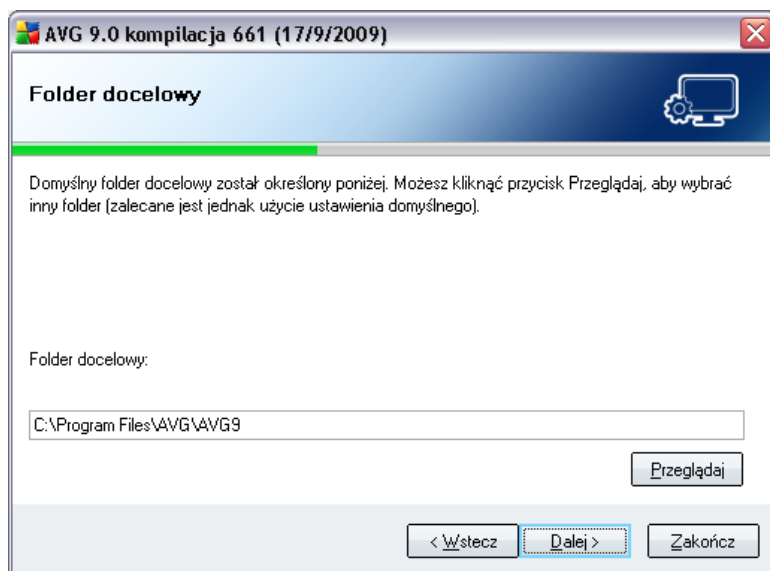
Jeśli oprogramowanie zostało zakupione w Internecie, numer licencji został już wysłany w wiadomości e-mail. Aby uniknąć błędów przy wpisywaniu, zalecamy skopiowanie i wklejenie numeru z wiadomości e-mail do pola na tym ekranie. Jeśli oprogramowanie zostało zakupione w sklepie, numer licencji można znaleźć na karcie rejestracyjnej produktu znajdującej się w opakowaniu. Numer należy skopiować i wkleić bez błędów.

< Wstecz **Dalej >** Zakończ

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

Jeśli w poprzednim kroku została wybrana instalacja standardowa, nastąpi przekierowanie bezpośrednio do okna **Pasek narzędzi AVG Security Toolbar**. Jeśli została wybrana instalacja niestandardowa, zostanie wyświetlone okno **Folder docelowy**.

5.6. Instalacja niestandardowa — Folder docelowy

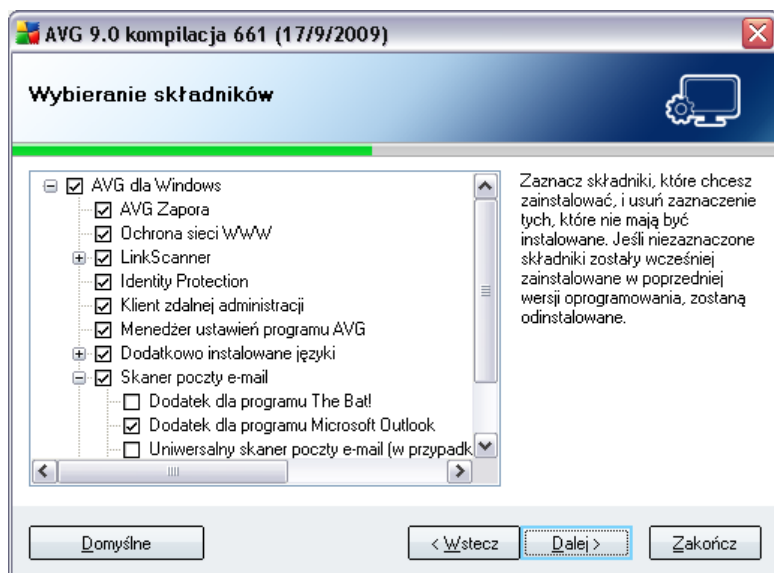


Okno dialogowe **Folder docelowy** pozwala określić lokalizację dla plików **AVG 9 Internet Security**. Domyślnie pakiet AVG jest instalowany w folderze "Program Files" na dysku C:. Jeśli wybrany folder nie istnieje, zostanie wyświetlone nowe okno dialogowe z pytaniem o zgodę na jego utworzenie.

Aby zmienić tę lokalizację, kliknij przycisk **Przeglądaj** i w wyświetlonym oknie wybierz odpowiedni folder.

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

5.7. Instalacja niestandardowa – Wybór składników



Okno dialogowe **Wybór składników** zawiera przegląd wszystkich składników **AVG 9 Internet Security**, które można zainstalować. Jeśli ustawienia domyślne nie są dla Ciebie odpowiednie, możesz dodać lub usunąć zadane składniki.

Wybierac można jednak tylko składniki należące do zakupionej edycji systemu AVG. Tylko one będą widoczne w niniejszym oknie dialogowym!

• Wybór języka

Na tej samej liście można także zdefiniować język (lub języki) instalowanego systemu AVG. Należy w tym celu zaznaczyć opcję **Dodatkowe zainstalowane języki** i wybrać je z odpowiedniego menu.

• Pluginy skanera poczty e-mail

Wybranie pozycji **Skaner poczty e-mail** pozwala wskazać pluginy, które mają zostać zainstalowane w celu zapewnienia ochrony poczty elektronicznej. Domyślnie instalowany jest **Plugin dla programu Microsoft Outlook**. Jeśli zakupiona licencja uwzględnia składnik **Anti-Spam**, jego instalacja nastąpi automatycznie. Inną opcją jest **Dodatek dla programu The Bat!** W przypadku korzystania z innego klienta poczty e-mail (*MS Exchange, Qualcomm Eudora, ...*) należy wybrać **Uniwersalny skaner poczty e-mail**, który chroni wiadomości e-mail niezależnie od używanego programu pocztowego.

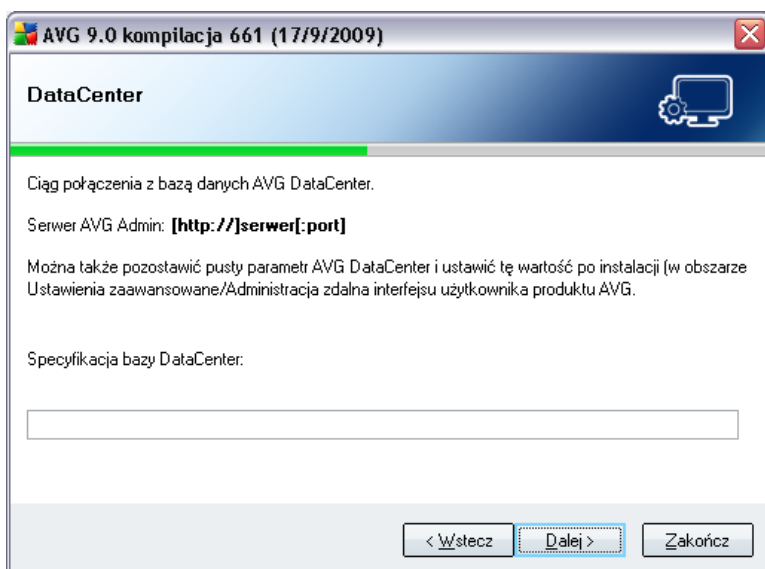
- **Administracja zdalna**

Jeśli planujesz korzystać z Administracji zdalnej AVG, zaznacz także odpowiednią pozycję na liście.

Aby kontynuować, kliknij przycisk **Dalej**.

5.8. AVG DataCenter

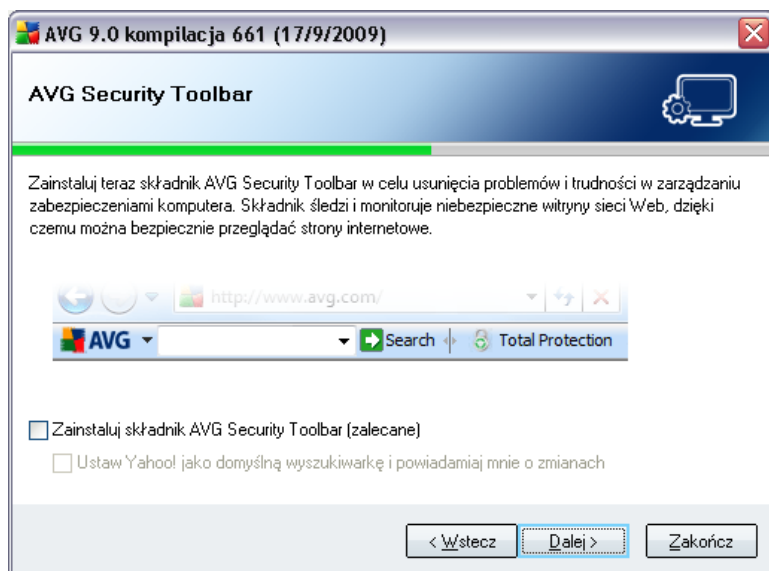
Jeśli w poprzednim oknie dialogowym (**Instalacja niestandardowa – Wybór składników**) zaznaczono do instalacji składnik **Administracja zdalna**, należy określić parametry **AVG DataCenter**:



W polu tekstowym **specyfikacji AVG DataCenter** podaj łańcuch znaków połączenia z **AVG DataCenter** (w formacie *serwer:port*). Jeśli nie masz tych informacji, możesz pozostawić pole puste i dokonać konfiguracji później, w oknie dialogowym [**Ustawienia zaawansowane / Administracja zdalna**](#).

Uwaga: Szczegółowe informacje dotyczące zdalnej administracji systemu AVG można znaleźć w podręczniku użytkownika systemu AVG Network Edition, który można pobrać ze strony internetowej systemu AVG (<http://www.avg.com/>).

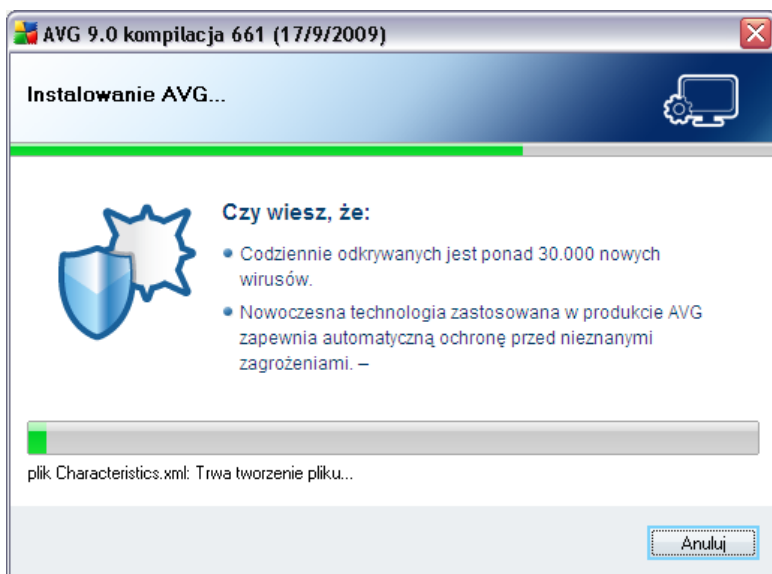
5.9. Pasek narzędzi AVG Security Toolbar



W oknie dialogowym **Pasek narzędzi AVG Security Toolbar** należy zdecydować, czy ma zostać zainstalowany **Pasek narzędzi AVG Security Toolbar** (weryfikacja wyników wyszukiwania zwracanych przez obsługiwane wyszukiwarki internetowe). Jeśli domyślne ustawienia nie zostały zmienione, składnik ten zostanie automatycznie zainstalowany w przeglądarce internetowej, aby zapewnić kompleksową ochronę podczas przeglądania internetu.

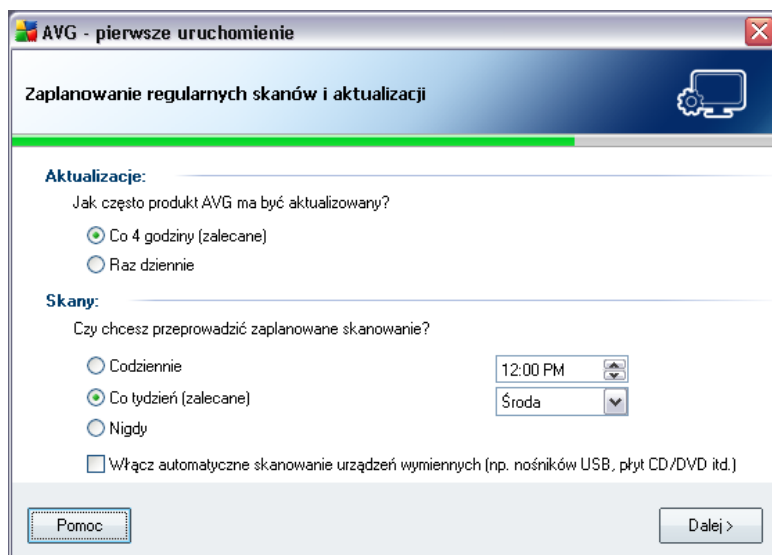
5.10. Instalowanie systemu AVG

Okno dialogowe **Instalowanie systemu AVG** zawiera informacje o postępie instalacji i nie wymaga działań ze strony użytkownika:



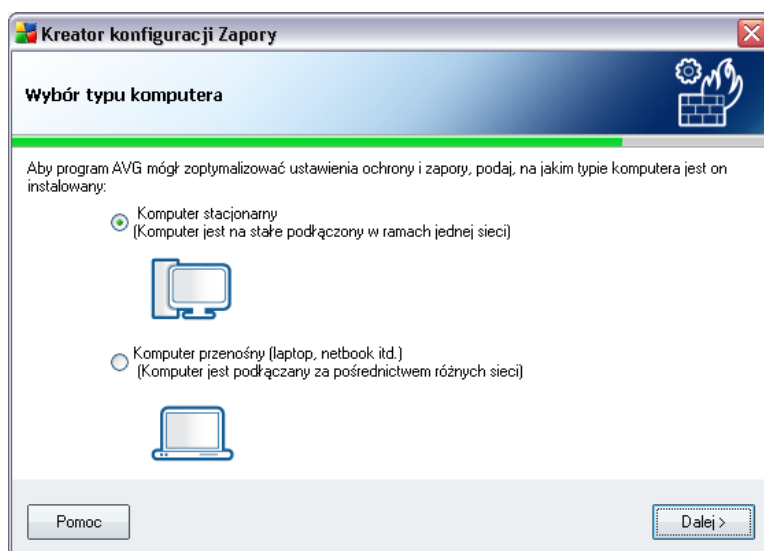
Po zakończeniu instalacji automatycznie nastąpi przekierowanie do następnego okna dialogowego.

5.11. Zaplanowanie regularnych skanów i aktualizacji



W oknie dialogowym **Planowanie cyklicznych skanów i aktualizacji** określa się częstotliwość sprawdzania dostępności nowych plików aktualizacji i zdefiniowanie czasu, w którym należy uruchomić [skan zaplanowany](#). Zaleca się zachowanie wartości domyślnych. Aby kontynuować, kliknij przycisk **Dalej**.

5.12. Wybór typu komputera



W tym oknie dialogowym, **Kreator konfiguracji składowa Zapora** zapyta o rodzaj używanego komputera. Na przykład: notebook łączący się z internetem z wielu różnych lokalizacji (*lotniska, pokoje hotelowe itp.*) wymaga bardziej rygorystycznych reguł zabezpieczeń niż komputer pracujący w domenie (*siec firmowa itp.*). Na podstawie wybranego sposobu użytkowania komputera dobrany zostanie poziom bezpieczeństwa domyślnych reguł **Zapory**.

Dostępne są tu dwie opcje:

- **Komputer stacjonarny**
- **Komputer przenośny**

Wybór należy potwierdzić kliknięciem przycisku **Dalej**, co spowoduje przejście do następnego okna dialogowego.

5.13. Architektura sieciowa komputera



W tym oknie, **Kreator konfiguracji Zapory** wyświetla pytanie o sposób podłączenia komputera do internetu. Domyślne reguły **Zapory** zostaną dopasowane do poziomu zabezpieczeń zapewnianych przez wybrany rodzaj połączenia.

Dostępne są tu trzy opcje:

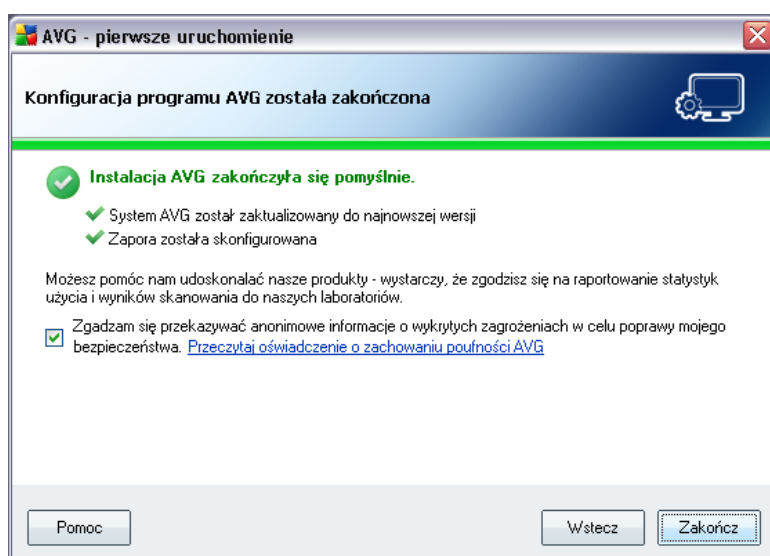
- **Bezpośrednie połączenie z internetem**

- **Niewielka sieć domowa**
- **Komputer jest przypisany do domeny**

Wskaz, który typ połączenia internetowego jest najbardziej zbliżony do Twojego.

Wybór należy potwierdzić kliknięciem przycisku **Dalej**, co spowoduje przejście do następnego okna dialogowego.

5.14. Konfiguracja ochrony systemu AVG została ukończona



Konfiguracja **AVG 9 Internet Security** zakończyła się pomyślnie.

W tym oknie dialogowym należy wskazać, czy informacje o znalezionych zagrożeniach i szkodliwych witrynach mają być anonimowo przesyłane do laboratorium wirusów AVG. Jeśli tak, należy zaznaczyć pole wyboru **Zgadzam się dostarczać ANONIMOWE informacje o wykrytych zagrożeniach, aby podnieść swój poziom ochrony**.

Na koniec należy wcisnąć przycisk **Zakończ**. Rozpoczęcie pracy z systemem AVG może wymagać ponownego uruchomienia komputera.

6. Po instalacji

6.1. Rejestracja produktu

Po ukończeniu instalacji systemu **AVG 9 Internet Security** należy zarejestrować produkt online na stronie internetowej AVG (<http://www.avg.com/>), w sekcji **Rejestracja** (postępując zgodnie z wyświetlanymi tam instrukcjami). Rejestracja umożliwia pełny dostęp do konta użytkownika AVG, biuletynu aktualizacji AVG i innych usług oferowanych wyłącznie zarejestrowanym klientom.

6.2. 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,
- z poziomu menu **Start/Programy/AVG 9.0/Interfejs użytkownika AVG**.

6.3. Skanowanie całego komputera

Istnieje ryzyko, że Twój komputer został zainfekowany jeszcze przed zainstalowaniem systemu **AVG 9 Internet Security**. 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](#).

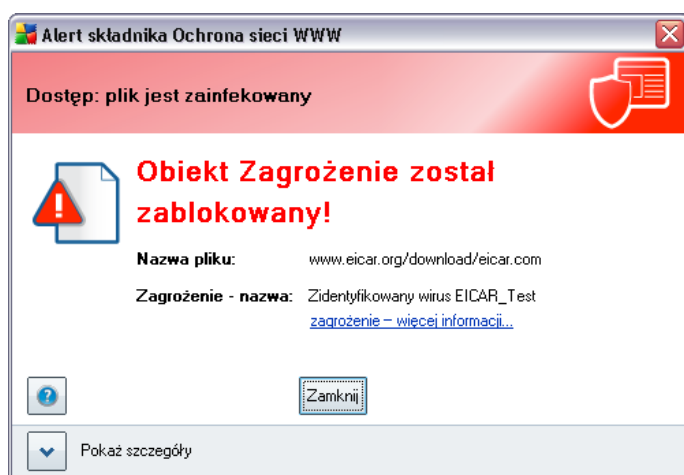
6.4. Test Eicar

W celu potwierdzenia poprawności instalacji systemu **AVG 9 Internet Security**, można wykonać test EICAR.

Test EICAR jest standardowa i całkowicie bezpieczna metoda służąca 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 (choć 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, składnik [Ochrona sieci WWW](#) zareaguje wyświetleniem ostrzeżenia. Pojawienie się komunikatu [Ochrony sieci WWW](#) potwierdza, że oprogramowanie AVG jest prawidłowo zainstalowane na komputerze.



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

6.5. Konfiguracja domyślna AVG

Konfiguracja domyślna (*ustawienia stosowane zaraz po zainstalowaniu*) pakietu **AVG 9 Internet Security**, wstępnie zdefiniowana przez dostawcę oprogramowania, ma na celu zapewnienie optymalnej wydajności wszystkich składników i funkcji.

Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach! Wszelkie zmiany 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 [Zaawansowane ustawienia AVG](#).

7. Interfejs użytkownika AVG

AVG 9 Internet Security otwórz w głównym oknie



Główne okno Interfejsu Użytkownika AVG jest podzielone na kilka sekcji:

- **Menu główne** (górny wiersz okna) to standardowe narzędzie nawigacyjne umożliwiające dostęp do wszystkich składników, usług i funkcji programu AVG — [szczegóły >>](#)
- **Informacje o stanie bezpieczeństwa** (prawa część górnej sekcji okna) zawiera informacje dotyczące bieżącego stanu programu AVG — [szczegóły >>](#)
- **Linki** (lewa kolumna) umożliwia uzyskanie szybkiego dostępu najważniejszych

i najczęściej używanych funkcji programu AVG — [szczegóły >>](#)

- **Przegląd składników** (centralna część okna) zawiera przegląd zainstalowanych komponentów programu AVG — [szczegóły >>](#)
- **Statystyka** (lewa dolna sekcja okna) zawiera najważniejsze dane statystyczne dotyczące działania programu — [szczegóły >>](#)
- **Ikona na pasku zadań** (prawy dolny róg ekranu, na pasku systemowym) sygnalizuje bieżący stan programu AVG — [szczegóły >>](#)

7.1. Menu systemowe

Menu systemowe to standardowa metoda nawigacji we wszystkich aplikacjach w systemie Windows. Znajduje się ono na samej górze interfejsu użytkownika **AVG 9 Internet Security**. Menu systemowe zapewnia dostęp do poszczególnych składników AVG, funkcji i usług.

Menu systemowe jest podzielone na pięć sekcji:

7.1.1. Plik

- **Zakończ** — powoduje zamknięcie interfejsu użytkownika **AVG 9 Internet Security**. System AVG działa jednak w tle, a komputer jest nadal chroniony!

7.1.2. Składniki

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

- **Przegląd systemu** — pozwala przełączyć widok do domyślnego okna Interfejsu użytkownika AVG, zawierającego [przegląd zainstalowanych składników](#).
- **Anti-Virus** — otwiera domyślne okno interfejsu składnika [Anti-Virus](#).
- **Anti-Rootkit** — otwiera domyślne okno interfejsu składnika [Anti-Rootkit](#).
- **Anti-Spyware** — otwiera domyślne okno interfejsu składnika [Anti-Spyware](#).
- **Zapora** — otwiera domyślne okno interfejsu składnika [Zapora](#).
- **LinkScanner** — otwiera domyślne okno interfejsu składnika [LinkScanner](#).

- **Narzędzia systemowe** — otwiera domyślne okno interfejsu składnika [Narzędzia systemowe](#).
- **Anti-Spam** — otwiera domyślne okno interfejsu składnika [Anti-Spam](#).
- **Skaner poczty e-mail** — otwiera domyślne okno interfejsu składnika [Skaner poczty e-mail](#).
- **ID Protection** — otwiera domyślne okno interfejsu składnika [ID Protection](#).
- **Licencja** — otwiera domyślne okno interfejsu składnika [Licencja](#).
- **Ochrona sieci WWW** — otwiera domyślne okno interfejsu składnika [Ochrona sieci WWW](#).
- **Ochrona rezydentna** — otwiera domyślne okno interfejsu składnika [Ochrona rezydentna](#).
- **Menedżer aktualizacji** — otwiera domyślne okno interfejsu składnika [Menedżer aktualizacji](#).

7.1.3. Historia

- [Wyniki skanowania](#) — powoduje przełączenie do interfejsu skanera AVG, konkretnie do okna dialogowego [Przegląd wyników skanowania](#).
- [Zagrożenia wykryte przez Ochronę Rezydentną](#) — powoduje otwarcie okna dialogowego zawierającego przegląd zagrożeń wykrytych przez [Ochronę Rezydentną](#).
- [Zagrożenie wykryte przez Skaner poczty e-mail](#) — powoduje otwarcie okna zawierającego przegląd załączników e-mail uznanych za niebezpieczne przez [Skaner poczty e-mail](#).
- [Zagrożenia wykryte przez Ochronę sieci WWW](#) — powoduje otwarcie okna dialogowego zawierającego przegląd zagrożeń wykrytych przez [Ochronę sieci WWW](#).
- [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](#) — powoduje otwarcie interfejsu dziennika historii

z przeglądem wszystkich zarejestrowanych akcji **AVG 9 Internet Security** .

- **Zapora** — powoduje otwarcie karty **Dzienniki** (dostępnej również w Konfiguracji Zapory), która zawiera szczegółowy przegląd wszystkich działań tego składnika

7.1.4. Narzędzia

- **Skanuj komputer** — przelacza do [Interfejsu skanera AVG](#) i uruchamia skanowanie całego komputera.
- **Skanuj wybrany folder** — przelacza do [Interfejsu skanera AVG](#) i umożliwia zdefiniowanie (w ramach struktury katalogów i dysków) plików oraz folderów, które mają być przeskanowane.
- **Skanuj plik** — umożliwia uruchomienie na zadanie testu pojedynczego, wskazanego pliku.
- **Aktualizuj** — automatycznie uruchamia proces aktualizacji. **AVG 9 Internet Security**
- **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 **AVG 9 Internet Security** . Na ogół zaleca się zachowanie domyślnych ustawień zdefiniowanych przez producenta oprogramowania AVG.
- **Ustawienia Zapory** — otwiera okno zaawansowanej konfiguracji składnika **Zapora AVG**.

7.1.5. Pomoc

- **Spis treści** — otwiera pliki pomocy systemu AVG.
- **Uzyskaj pomoc online** — otwiera witrynę firmy AVG (<http://www.avg.com/>) na stronie centrum pomocy technicznej dla klientów.
- **Strona Mój AVG** — otwiera witrynę systemu AVG (<http://www.avg.com/>).

- **Informacje o wirusach i zagrożeniach** — powoduje otwarcie [Encyklopedii Wirusów](#) online, w której znaleźć można szczegółowe informacje na temat znanych zagrożeń.
- **Aktywuj ponownie** — otwiera okno **Aktywacja programu AVG** zawierające dane wprowadzone na etapie [personalizacja programu AVG](#) (podczas instalacji). W oknie tym można wprowadzić numer licencji w celu zastąpienia numeru sprzedaży (użytego do zainstalowania programu AVG) lub starego numeru licencji (na przykład podczas uaktualnienia do nowego produktu AVG).
- **Zarejestruj teraz** — jest linkiem do strony rejestracji w witrynie systemu AVG (<http://www.avg.com/>). Należy tam podać swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysługuje bezpłatna pomoc techniczna.
- **AVG — informacje** — powoduje otwarcie okna **Informacje** zawierającego pięć kart, z których można odczytać nazwę programu, wersję silnika antywirusowego i jego bazy danych, informacje o systemie, umowę licencyjną oraz informacje kontaktowe dotyczące firmy **AVG Technologies CZ**.

7.2. Status bezpieczeństwa

Sekcja **Informacje o stanie bezpieczeństwa** znajduje się w górnej części Interfejsu użytkownika AVG. Znajdziesz tam informacje o bieżącym stanie bezpieczeństwa systemu **AVG 9 Internet Security**. W obszarze tym mogą być wyświetlane następujące ikony:



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



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

Ikona jest także wyświetlana, gdy z jakiegoś powodu [stan błędu składników ma](#)

[być ignorowany](#) (opcja "Ignoruj stan składnika" jest dostępna po kliknięciu prawym przyciskiem ikony odpowiedniego składnika w głównej sekcji okna AVG). Użycie tej opcji może być wskazane w określonych sytuacjach, ale stanowczo zaleca się jak najszybsze ponowne wyłączenie opcji **Ignoruj stan składnika**.



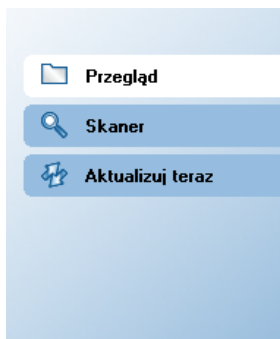
Ikona czerwona oznacza, że stan systemu AVG jest krytyczny! Jeden lub więcej składników nie działa, a system AVG nie może chronić komputera. Należy natychmiast usunąć zgłoszony problem. Jeśli nie jest to możliwe, należy skontaktować się z zespołem [Pomocy Technicznej AVG](#).

Stanowczo zaleca się reagowanie na zmiany **Statusu Bezpieczeństwa** i natychmiastowe rozwiązywanie ewentualnych problemów. Brak reakcji narazi komputer na poważne zagrożenia!

Uwaga: Dostęp do informacji o stanie systemu AVG zapewnia przez cały czas również [ikona na pasku zadań](#).

7.3. Linki

Szybkie linki (z lewej strony [interfejsu użytkownika AVG](#)) pozwala natychmiast uzyskiwać dostęp do najważniejszych i najczęściej używanych funkcji systemu AVG:



- **Przegląd** — pozwala przełączać między bieżącym interfejsem AVG i interfejsem domyślnym, zawierającym przegląd wszystkich zainstalowanych składników (zobacz rozdział [Przegląd składników >>](#))
- **Skaner** — otwiera interfejs skanera AVG, w którym można uruchamiać testy, planować skany i edytować ich parametry (zobacz rozdział [Testy AVG >>](#))
- **Aktualizuj teraz** — otwiera odpowiedni interfejs i uruchamia proces aktualizacji systemu AVG (zobacz rozdział [Aktualizacje AVG >>](#))

Linki te są dostępne przez cały czas. Kliknięcie jednego z nich w celu uruchomienia określonego procesu powoduje wyświetlenie innego okna dialogowego, ale sama sekcja linków nie ulegnie zmianie. Ponadto, działający proces został dodatkowo przedstawiony w formie graficznej — *zobacz ilustracja 2*).

7.4. Przegląd składników

Sekcja **Przegląd składników** znajduje się w środkowej części [Interfejsu użytkownika AVG](#). Obszar ten podzielony jest na dwie części:

- Przegląd wszystkich zainstalowanych składników (panel z odpowiednimi ikonami oraz informacjami o stanie komponentów)
- Opis wybranego składnika.

W systemie **AVG 9 Internet Security** sekcja **Przegląd składników** zawiera informacje o następujących składnikach:

- **Anti-Virus** — zapewnia ochronę przed wirusami, które mogą zainfekować komputer — [szczegóły >>](#)
- **Anti-Spyware** — skanuje uruchamiane aplikacje w tle — [szczegóły >>](#)
- **Anti-Spam** — sprawdza wszystkie przychodzące wiadomości e-mail i oznacza niepożądaną pocztę jako SPAM — [szczegóły >>](#)
- **Zapora** — kontroluje wymianę danych z innymi komputerami w internecie lub sieci lokalnej — [szczegóły >>](#)
- **LinkScanner** — sprawdza wyniki wyszukiwania wyświetlane przez serwisy internetowe — [szczegóły >>](#)
- **Anti-Rootkit** — wykrywa programy i technologie próbujące ukryć w systemie szkodliwe oprogramowanie — [szczegóły >>](#)
- **Narzędzia systemowe** oferuje szczegółowe podsumowanie środowiska AVG — [szczegóły >>](#)
- **Skaner poczty e-mail** — sprawdza wszystkie przychodzące i wychodzące wiadomości e-mail w poszukiwaniu wirusów — [szczegóły >>](#)
- **ID Protection** — składnik chroniący przed złośliwym oprogramowaniem wyspecjalizowany w zapobieganiu kradzieży cennych danych osobistych — [szczegóły >>](#)

- **Licencja** — zawiera pełną treść umowy licencyjnej AVG — [szczegóły >>](#)
- **Ochrona sieci WWW** — skanuje wszystkie dane pobierane przez przeglądarkę WWW — [szczegóły >>](#)
- **Ochrona rezydentna** — działa w tle; skanuje pliki przy ich kopiowaniu, otwieraniu i zapisywaniu — [szczegóły >>](#)
- **Menedżer aktualizacji** — kontroluje wszystkie aktualizacje systemu AVG — [szczegóły >>](#)

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

Kliknięcie prawym przyciskiem ikony składnika powoduje otwarcie menu kontekstowego: można w nim nie tylko otworzyć interfejs składnika, ale także wybrać opcję **ignorowania stanu składnika**. Opcję tę należy wybrać, jeśli [stan błędu składnika](#) jest znany, ale z dowolnego powodu system AVG ma być nadal używany, a [ikona na pasku zadań](#) nie ma być wyszarzona jako ostrzeżenie.

7.5. Statystyki

Obszar **Statystyki** znajduje się w lewym dolnym rogu [Interfejsu użytkownika AVG](#). Sekcja ta zawiera szereg informacji o działaniu programu:

- **Skanowanie** — data ostatniego przeprowadzonego testu.
- **Aktualizacja** — data ostatniej aktualizacji.
- **BD wirusów** — aktualnie używana wersja bazy wirusów.
- **Wersja AVG** — zainstalowana wersja systemu AVG (*numer w formacie 8.0.xx, gdzie 8.0 to wersja linii produktów, a xx — numer kompilacji*).
- **Data wygasnięcia licencji** — data wygasnięcia licencji systemu AVG.

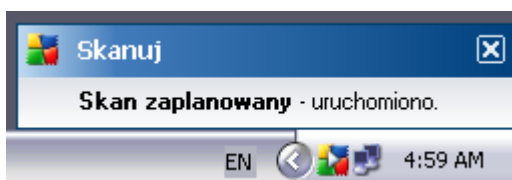
7.6. Ikona na pasku zadań

Ikona AVG na pasku zadań (systemu Windows) informuje o bieżącym stanie programu **AVG 9 Internet Security**. Ikona ta jest zawsze widoczna, niezależnie od tego, czy Interfejs użytkownika AVG jest otwarty, czy też nie.

Jesli  **ikona na pasku zadan** jest kolorowa, oznacza to, ze wszystkie skladniki systemu AVG sa aktywne i w pelni funkcjonalne. Moze ona byc kolorowa takze wtedy, gdy system AVG zasygnalizowal bledy, ale uzytkownik akceptuje je i celowo [ignoruje stan skladnikow](#).

Ikona szara ze znakiem wykrzyknika  oznacza problem (nieaktywny skladnik, stan bledu itd.). W takim przypadku nalezy dwukrotnie kliknac **ikone na pasku zadan**, aby otworzyc Interfejs uzytkownika i skorygowac stan skladnikow.

Ikona na pasku zadan dostarcza takze szczegolowych informacji na temat biezacych dzialan systemu AVG i mozliwych zmian w programie (np. uruchomienia automatycznego lub zaplanowanego skanowania lub aktualizacji, przełączenia profilu Zapory, zmiany stanu skladnika, bledu itp.) w wyskakujacym okienku:



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

- **Otwórz Interfejs uzytkownika AVG** — otwiera [Interfejs uzytkownika](#).
- **Aktualizuj** — uruchamia natychmiastowa [aktualizacje](#)

8. Składniki AVG

8.1. Anti-Virus

8.1.1. Zasady działania składnika Anti-Virus

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

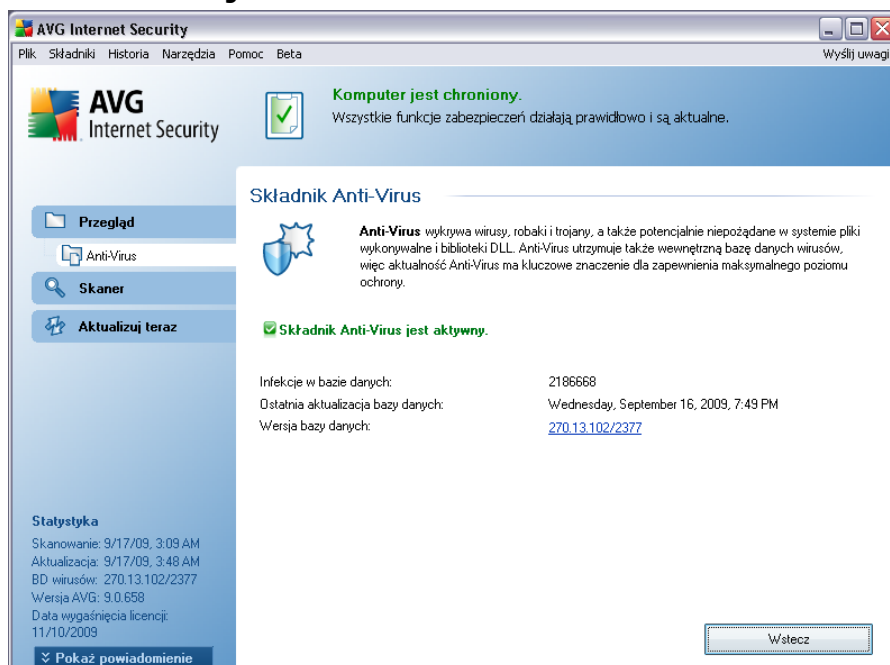
Ważna zaleta ochrony antywirusowej jest fakt, że nie pozwala ona na uruchomienie żadnych znanych wirusów na komputerze!

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

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

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

8.1.2. Interfejs składowika Anti-Virus



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

- **Infekcje w bazie danych** — liczba wirusów zdefiniowanych w najnowszej wersji bazy danych.
- **Ostatnia aktualizacja bazy danych** — data i godzina ostatniej aktualizacji bazy wirusów.
- **Wersja bazy danych** — numer ostatniej wersji bazy danych; zwiększany jest przy każdej jej aktualizacji.

Interfejs tego składowika zawiera tylko jeden przycisk (**Wstecz**) — kliknięcie go powoduje powrót do domyślnego [Interfejsu użytkownika AVG](#) (przeglądu składników).

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

8.2. Anti-Spyware

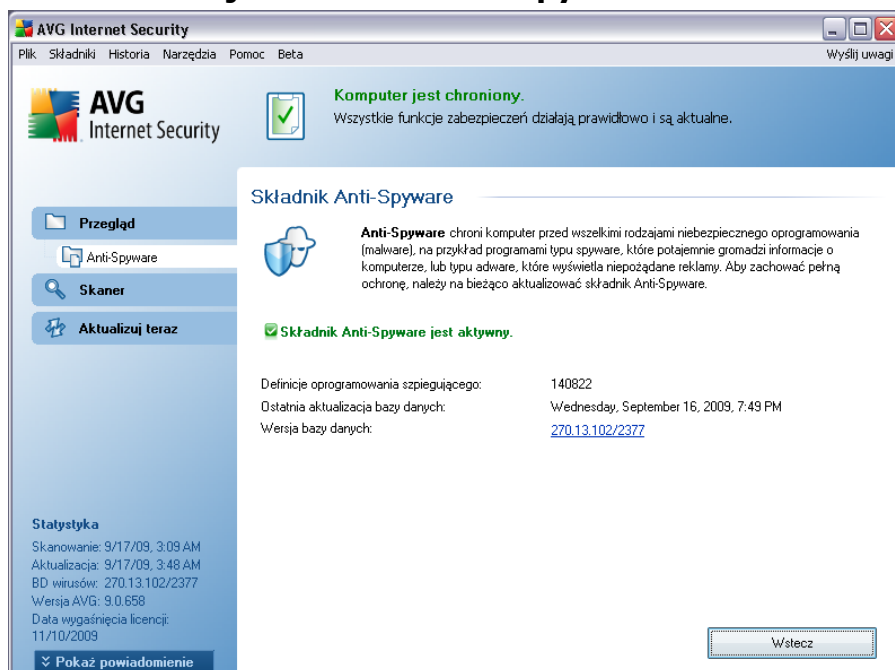
8.2.1. Zasady działania składnika Anti-Spyware

Oprogramowanie szpiegujące (spyware) jest zazwyczaj definiowane jako pewien rodzaj szkodliwego oprogramowania, które gromadzi informacje z komputera użytkownika bez jego wiedzy i pozwolenia. Niektóre aplikacje szpiegujące mogą być instalowane 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 e-mail lub w efekcie działalności robaków i wirusów. Najskuteczniejsza ochrona jest stosowanie stale pracującego w tle składnika **Anti-Spyware**, który działa jak ochrona rezydentna i skanuje aplikacje podczas ich uruchamiania.

Istnieje jednak ryzyko, że szkodliwe oprogramowanie znalazło się na komputerze przed zainstalowaniem pakietu **AVG 9 Internet Security**, lub że użytkownik zaniedbał jego aktualizację, nie korzystając z aktualnych baz wirusów [i nowych wersji programu](#). Z tego powodu AVG umożliwia pełne przeskanowanie komputera pod kątem obecności oprogramowania szpiegującego (za pomocą interfejsu skanera). Wykrywa on również szkodliwe oprogramowanie, które jest uspijone lub nie stwarza zagrożenia, czyli takie, które zostało pobrane, ale nie aktywowane.

8.2.2. Interfejs składowika Anti-Spyware



Interfejs składowika **Anti-Spyware** zawiera krótki opis jego funkcji, informacje o bieżącym stanie (Składnik *Anti-Spyware* jest aktywny.), oraz statystyki :

- **Definicje oprogramowania szpiegującego** — liczba sygnatur programów typu spyware zdefiniowanych w najnowszej wersji bazy danych.
- **Ostatnia aktualizacja bazy danych** — data i godzina ostatniej aktualizacji.
- **Wersja bazy danych** — numer ostatniej wersji bazy danych; zwiększany jest on przy każdej aktualizacji.

Interfejs tego składowika zawiera tylko jeden przycisk (**Wstecz**) — kliknięcie go powoduje powrót do domyślnego [Interfejsu użytkownika AVG](#) (przeglądu składników).

Uwaga: Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfiguracje 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](#).

8.3. Anti-Spam

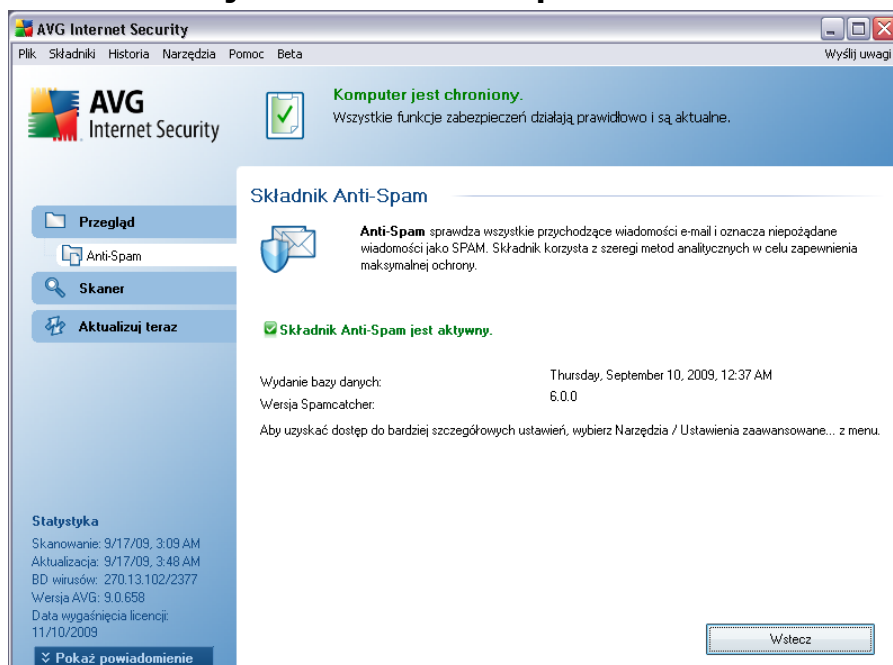
Mianem „spam” określa się niechciana pocztę e-mail (głównie reklamy produktów lub usług, które są hurtowo rozsyłane do wielkiej liczby odbiorców jednocześnie, zapelniając ich skrzynki pocztowe). Spamem nie jest korespondencja seryjna rozsyłana do odbiorców po wyrażeniu przez nich zgody. Spam jest nie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

8.3.1. Zasady działania składowika Anti-Spam

Składnik AVG Anti-Spam sprawdza wszystkie przychodzące wiadomości e-mail i oznacza te niepożądane jako SPAM. **Składnik AVG 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 AVG Anti-Spam podczas przetwarzania każdej wiadomości wykorzystuje kilka metod analizy, oferując maksymalnie skuteczną ochronę przeciwko niepożądanym wiadomościom e-mail. Składowik **AVG Anti-Spam** do wykrywania spamu korzysta z regularnie aktualizowanej bazy danych. Można także użyć [zdefiniowanych serwerów RBL](#) (*publicznych baz adresów znanych nadawców spamu*) lub ręcznie dodać adresy do [białej listy](#) (*nigdy nieoznaczanej jako spam*) lub [czarnej listy](#) (*zawsze oznaczanej jako spam*).

8.3.2. Interfejs składnika Anti-Spam



Okno dialogowe składnika **Anti-Spam** zawiera krótki opis jego funkcji, informacje o bieżącym stanie (Składnik *Anti-Spam* jest aktywny.) oraz następujące statystyki:

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

Interfejs tego składnika zawiera tylko jeden przycisk (**Wstecz**) — kliknięcie go powoduje powrót do domyślnego [Interfejsu użytkownika systemu AVG](#) (przeglądu składników).

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

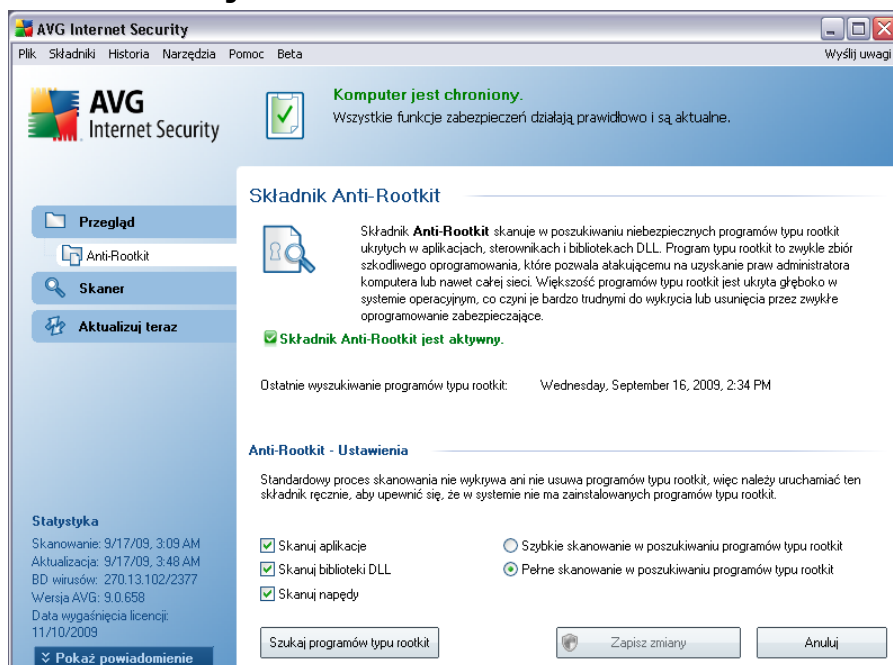
8.4. Anti-Rootkit

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 myląc lub unikając standardowych mechanizmów bezpieczeństwa systemu operacyjnego. Wiele z nich jest jednocześnie koniami trojańskimi, które dodatkowo starają się przekonać użytkowników, że ich systemy są bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorującymi) oraz plików lub danych przed samym systemem operacyjnym.

8.4.1. Zasady działania składnika Anti-Rootkit

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

8.4.2. Interfejs składowika Anti-Rootkit



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

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

- **Skanuj aplikacje**
- **Skanuj biblioteki DLL**
- **Skanuj napędy**

Następnie należy wybrać tryb skanowania rootkitów:

- **Szybkie skanowanie w poszukiwaniu programów typu rootkit** — skanowany jest tylko folder systemowy (zwykle C:\Windows).
- **Pełne skanowanie w poszukiwaniu programów typu rootkit** —

skanowane są wszystkie dostępne dyski, oprócz A: i B:.

Dostępne przyciski sterujące to:

- **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** — pozwala zapisać wszystkie zmiany wprowadzone w danym oknie i powrócić do domyślnego [Interfejsu użytkownika AVG](#) (przeglądu składników).
- **Anuluj** — pozwala powrócić do domyślnego [Interfejsu użytkownika AVG](#) (przeglądu składników) bez zapisywania wprowadzonych zmian.

8.5. Narzędzia systemowe

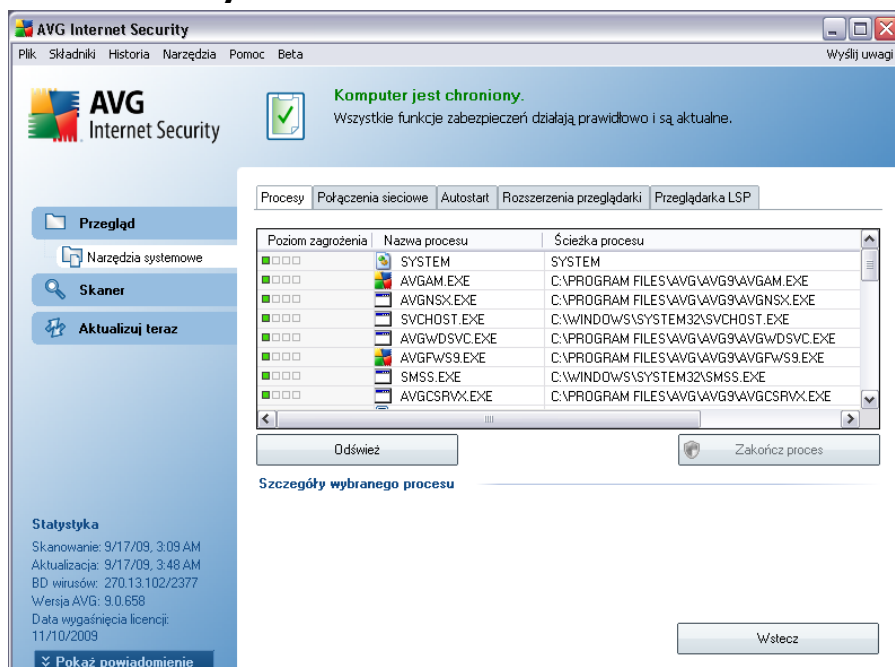
Składnik Narzędzia systemowe odnosi się do narzędzi umożliwiających uzyskanie szczegółowego podsumowania środowiska pracy **AVG 9 Internet Security**.

Wyswietlany jest tam przegląd:

- [Procesy](#) — lista procesów (czyli działających aplikacji) aktualnie aktywnych na komputerze.
- [Połączenia sieciowe](#) — lista aktualnie aktywnych połączeń
- [Autostart](#) — lista wszystkich aplikacji uruchamianych podczas startu systemu Windows
- [Rozszerzenia przeglądarki](#) — lista pluginów, tzn. aplikacji zainstalowanych w przeglądarce internetowej.
- [Przeglądarka LSP](#) — lista dostawców usług warstwowych (LSP)

Niektóre listy można też edytować, ale powinni to robić wyłącznie bardzo doświadczeni użytkownicy!

8.5.1. Procesy



Okno **Procesy** zawiera listę procesów (czyli *działających aplikacji*) aktualnie aktywnych na komputerze. Lista ta podzielona jest na następujące kolumny:

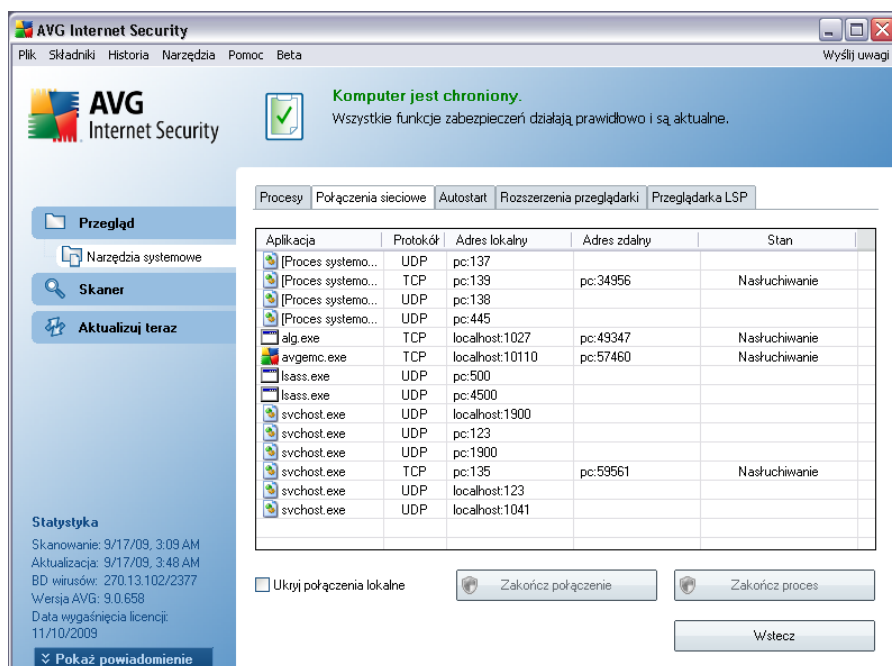
- **Poziom ryzyka** — graficzna reprezentacja ryzyka stwarzanego przez określone procesy, przedstawiana na czterostopniowej skali od najmniej istotnego (■ ■ ■ ■) do krytycznego (■ ■ ■ ■).
- **Nazwa procesu** — nazwa działającego procesu.
- **Ścieżka** — fizyczna ścieżka do uruchomionego pliku.
- **Okno** — jeśli to możliwe, podaje nazwę okna aplikacji.
- **Internet** — wskazuje, czy działający proces łączy się także z internetem (*Tak/Nie*).
- **Usługa** — wskazuje, czy działający proces jest usługą (*Tak/Nie*).
- **PID** — numer identyfikacyjny procesu - unikatowy, wewnętrzny numer procesu w systemie Windows.

Przyciski kontrolne

W interfejsie **narzędzi systemowych** dostępne są następujące przyciski sterujące:

- **Odśwież** — aktualizuje listę procesów zgodnie z obecnym stanem.
- **Zakończ procesy** — można wybrać jedną lub kilka aplikacji i zakończyć je, klikając ten przycisk. **Stanowczo zaleca się, aby nie zamykać żadnych procesów, jeśli nie ma absolutnej pewności, że stanowią one rzeczywiste zagrożenie!**
- **Wstecz** — przełącza z powrotem do domyślnego **Interfejsu użytkownika systemu AVG** (przeglądu składników).

8.5.2. Połączenia sieciowe



Okno **Połączenia sieciowe** zawiera listę aktywnych połączeń. Lista ta podzielona jest na następujące kolumny:

- **Aplikacja** — nazwa aplikacji nawiązującej połączenie. Ta informacja dostępna jest wyłącznie w systemie Windows XP.

- **Protokół** — protokół transmisyjny używany do połączenia:
 - o TCP — protokół współpracujący z protokołem IP (Internet Protocol) przy transmisji danych w internecie.
 - o UDP — protokół alternatywny do TCP.
- **Adres lokalny** — używany adres IP komputera lokalnego (i numer portu).
- **Adres zdalny** — Adres IP komputera zdalnego (i numer portu). Jeśli jest to możliwe, znaleziona zostanie również nazwa hosta komputera zdalnego.
- **Stan** — określa najbardziej prawdopodobny stan połączenia (*Połączony, Serwer powinien zamknąć, Nasłuchiwanie, Ukończono zamykanie aktywne, Zamykanie pasywne, Zamykanie aktywne*).

Aby stworzyć listę tylko zewnętrznych połączeń, należy zaznaczyć pole wyboru **Ukryj połączenia lokalne** w dolnej sekcji okna dialogowego.

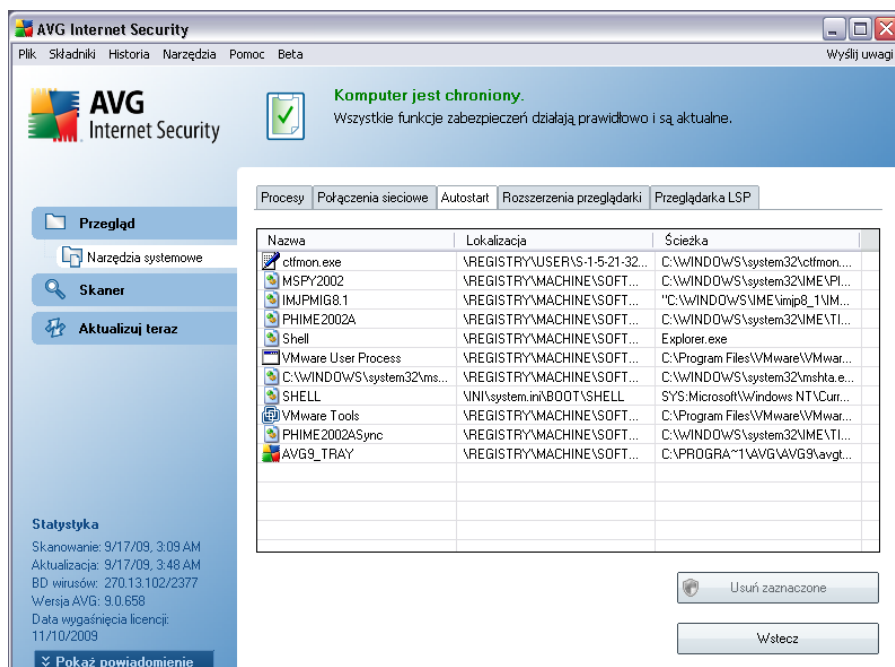
Przyciski kontrolne

Dostępne przyciski sterujące to:

- **Zakończ połączenie** — zamyka wybrane połączenia.
- **Zakończ proces** — zamyka jedną lub kilka aplikacji używających połączeń wybranych z listy (*ten przycisk dostępny jest jedynie w systemie Windows XP*).
- **Wstecz** — wraca do domyślnego [Interfejsu użytkownika AVG](#) (przeglądu składników).

Uwaga: Czasami możliwe jest kończenie tylko tych aplikacji, które są w stanie "Połączony". Stanowczo zaleca się, aby nie zamykać żadnych połączeń, jeśli nie ma absolutnej pewności, że stanowią one rzeczywiste zagrożenie!

8.5.3. Autostart

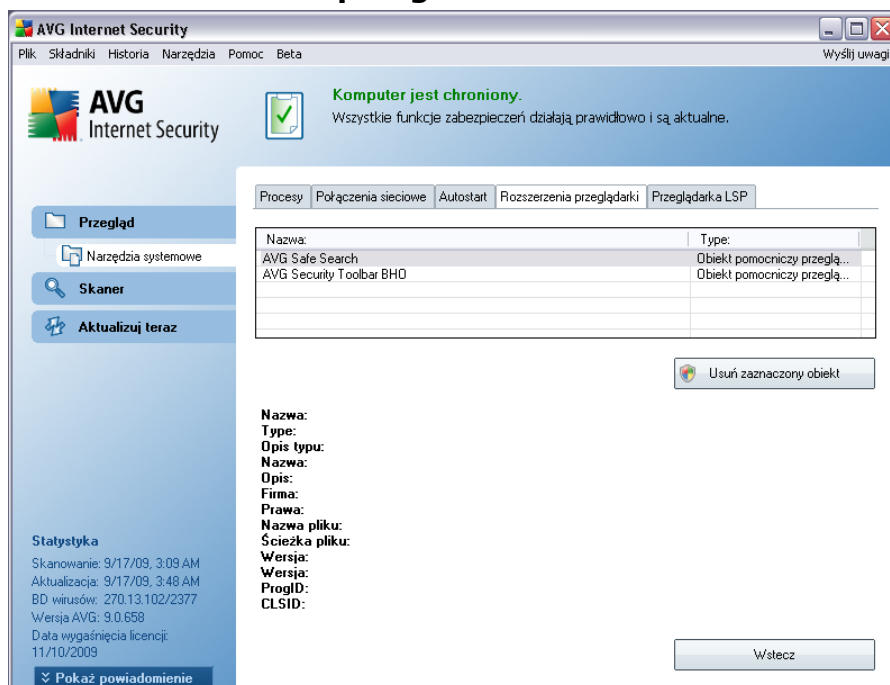


Okno **Autostart** zawiera listę wszystkich aplikacji uruchamianych w czasie rozruchu systemu Windows. Bardzo często szkodliwe aplikacje dodają się automatycznie do listy autostartu zlokalizowanej w rejestrze.

Mozna usunąć jeden lub więcej wpisów, zaznaczając je i klikając przycisk **Usuń zaznaczone elementy**. Przycisk **Wstecz** przełącza z powrotem do domyślnego okna **Interfejsu użytkownika AVG** (przeglądu składników).

Zaleca się, aby nie usuwać żadnych aplikacji z tej listy, jeśli nie ma absolutnej pewności, że stanowią one rzeczywiste zagrożenie!

8.5.4. Rozszerzenia przeglądarki



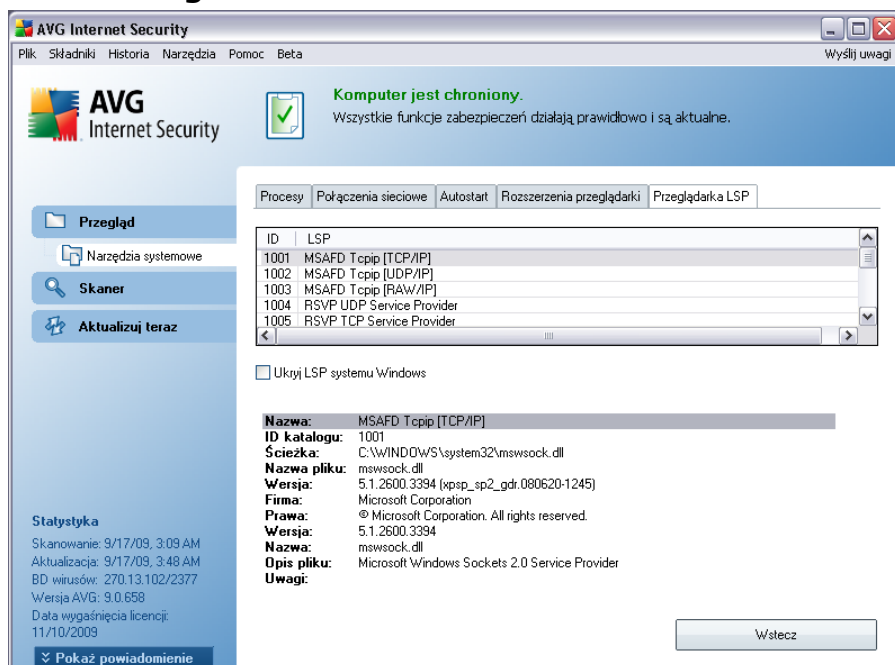
Okno **Rozszerzenia przeglądarki** zawiera listę pluginów, tj. aplikacji zintegrowanych z przeglądarką internetową. Lista ta może zawierać zarówno użyteczne dodatki, jak i potencjalnie szkodliwe programy. Kliknij obiekt z listy, aby otrzymać szczegółowe informacje o wybranym pluginie. Zostaną one wyświetlone w dolnej sekcji okna dialogowego.

Przyciski kontrolne

Na karcie **Rozszerzenia przeglądarki** dostępne są następujące przyciski kontrolne:

- **Usun zaznaczone obiekty** — usuwa plugin w danej chwili zaznaczony na liście. **Stanowczo zaleca się, aby nie usuwać z listy żadnych pluginów, jeśli nie ma absolutnej pewności, że stanowią one rzeczywiste zagrożenie!**
- **Wstecz** — przełącza z powrotem do domyślnego [Interfejsu użytkownika systemu AVG](#) (przeglądu składników)

8.5.5. Przeglądarka LSP



Okno **Przeglądarka LSP** zawiera pełną listę dostawców usług warstwowych (LSP).

Dostawca usług warstwowych (LSP) jest sterownikiem systemowym odpowiedzialnym za usługi sieciowe systemu operacyjnego Windows. Ma on dostęp do wszystkich danych przychodzących i wychodzących z komputera, a także może je modyfikować. Niektóre sterowniki LSP są niezbędne, aby system Windows mógł łączyć się z innymi komputerami (w tym również z internetem). Jednak pewne szkodliwe aplikacje potrafią zarejestrować się w systemie jako LSP, uzyskując w ten sposób dostęp do wszystkich transmitowanych danych. Dlatego też przegląd ten może być pomocny w sprawdzaniu wszystkich możliwych zagrożeń związanych z LSP.

W pewnych okolicznościach możliwa jest także naprawa uszkodzonych sterowników LSP (*np. gdy plik został usunięty, ale pozostały wpisy w rejestrze*). Gdy zostanie wykryty sterownik LSP kwalifikujący się do naprawy, zostanie wyświetlony przycisk umożliwiający jej dokonanie.

Aby uwzględnić na liście sterowniki LSP należące bezpośrednio do systemu Windows, odznacz pole **Ukryj sterowniki LSP systemu Windows**. Przycisk **Wstecz** przełącza z powrotem do domyślnego okna **Interfejsu użytkownika systemu AVG** (przeglądu składników).

8.6. Zapora

Zapora internetowa to system, który wymusza stosowanie zasad kontroli dostępu między dwoma lub większą liczbą sieci, blokując lub umożliwiając przepływ danych. Zapora składa się z zestawu regul, które sterują komunikacją na każdym indywidualnym porcie sieciowym, chroniąc w ten sposób sieć lokalną przed atakami, których źródło znajduje się na zewnątrz (zazwyczaj w internecie). Komunikacja jest oceniana (w oparciu o zdefiniowane reguły), a następnie akceptowana lub blokowana. Jeśli zapora wykryje próbę ataku, blokuje ją i nie pozwala intruzowi przejąć kontroli nad komputerem.

Konfiguracja Zapory pozwala blokować lub dopuszczać komunikację wewnętrzną lub zewnętrzną (zarówno wychodzącą, jak i przychodzącą) na konkretnych portach i dla zdefiniowanych programów. Zapora może np. akceptować tylko ruch WWW, z którego korzysta program Microsoft Internet Explorer. Próba transmisji danych WWW przez jakąkolwiek inną przeglądarkę będzie w takim przypadku blokowana.

Zapora chroni również Twoje dane osobowe - nikt nie uzyska ich z Twojego komputera bez wyrażonej zgody. Decyduje też o tym, jak wymieniane są dane z innymi komputerami w sieci lokalnej lub internecie. Zapora w środowisku komercyjnym chroni również pojedyncze komputery przed atakami przeprowadzanymi z wnętrza tej samej sieci.

Sugestia: Generalnie nie zaleca się używania więcej niż jednej zapory internetowej na tym samym komputerze. Zainstalowanie dodatkowych zapór nie zwiększy bezpieczeństwa komputera. Zwiększy się natomiast prawdopodobieństwo, że wystąpią konflikty między tymi dwiema aplikacjami. Dlatego też zalecamy używanie tylko jednej zapory i wyłączenie wszystkich innych. Pozwala to wyeliminować ryzyko konfliktów i wszelkich problemów z tym związanych.

8.6.1. Zasady działania Zapory

W systemie AVG **Zapora** kontroluje cały ruch na każdym porcie sieciowym komputera. Na podstawie zdefiniowanych reguł **Zapora** ocenia uruchomione aplikacje (chcące nawiązać połączenie z siecią lokalną lub internetem) oraz programy usiłujące z zewnątrz połączyć się z Twoim komputerem. **Zapora** dopuszcza lub blokuje komunikację tych aplikacji na określonych portach sieciowych. Domyślnie, jeśli aplikacja jest nieznana (tj. nie posiada zdefiniowanych reguł **Zapory**), wyświetlone będzie pytanie, czy jej komunikacja ma zostać zaakceptowana.

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

Zapora może wykonać następujące czynności:

- Automatycznie zablokować lub zezwolić na komunikację znanych [aplikacji](#), albo poprosić użytkownika o potwierdzenie
- Korzystać z kompletnych [profilu](#) zawierających wstępnie zdefiniowane reguły (zgodnie z Twoimi potrzebami)
- Prowadzić [archiwum](#) wszystkich zdefiniowanych profili i ustawień
- [Automatycznie przełączać profile](#) przy łączeniu się z różnymi sieciami lub przy używaniu różnych kart sieciowych

8.6.2. Profile Zapory

[Zapora](#) umożliwia definiowanie określonych reguł bezpieczeństwa w oparciu o środowisko i tryb pracy komputera. Każda z opcji wymaga innego poziomu zabezpieczeń, a ich dostosowywanie odbywa się za pomocą odpowiednich profili. Krótko mówiąc, [profil Zapory](#) to określona konfiguracja tego [składnika](#). Dostępna jest pewna liczba wstępnie zdefiniowanych profili.

Dostępne profile

- **Odblokuj wszystko** to systemowy profil [Zapora](#), wstępnie skonfigurowany przez producenta; jest zawsze dostępny. Gdy profil ten jest aktywny, cała komunikacja sieciowa jest akceptowana, bez stosowania jakichkolwiek reguł zabezpieczeń - tak, jakby składnik [Zapora](#) był wyłączony (*tj. wszystkie programy mogą wymieniać dane, ale pakiety wciąż obsługiwane są przez sterownik filtra AVG - aby tego uniknąć, całkowicie wyłącz Zaporę*). Tego profilu systemowego nie można powielić ani usunąć, a jego ustawień nie da się modyfikować.
- **Blokuj wszystko** to systemowy profil [Zapory](#) wstępnie skonfigurowany przez producenta; jest zawsze dostępny. Gdy zostanie on aktywowany, wszystkie próby komunikacji z siecią będą blokowane. Komputer nie będzie ani dostępny z sieci zewnętrznej, ani nie będzie mógł się z nią połączyć. Tego profilu systemowego nie można powielić ani usunąć, a jego ustawień nie da się modyfikować.
- **Profile niestandardowe:**
 - o **Komputer przenośny** — odpowiedni dla typowych komputerów stacjonarnych połączonych bezpośrednio z internetem lub dla notebooków łączących się z internetem poza bezpieczną siecią firmową. Opcje te należy wybrać, jeśli łączysz się z siecią w domu, w małej sieci

firmowej (bez centralnej administracji). Opcje te należy wybrać również podczas podróżowania z notebookiem i łączenia się z siecią z nieznanych i potencjalnie niebezpiecznych miejsc (*kawiarnie internetowe, pokoje hotelowe itp.*). Zostaną w tym wypadku utworzone bardziej restrykcyjne reguły, ponieważ zakłada się, że komputer taki nie ma zapewnionej żadnej dodatkowej ochrony, dlatego też wymaga maksymalnej troski o bezpieczeństwo.

- o **Komputer w domenie** — odpowiedni dla komputerów pracujących w sieci lokalnej, np. w szkołach lub sieci firmowej. Zakłada się, że wspomniana sieć chroniona jest przy użyciu pewnych dodatkowych środków, więc poziom bezpieczeństwa może być niższy niż dla pojedynczego komputera.
- o **Sieć w domu lub małym biurze** — odpowiedni dla komputerów w mniejszej sieci, np. w domu lub w małej firmie (zazwyczaj tylko kilka komputerów połączonych ze sobą, bez „centralnego” administratora).

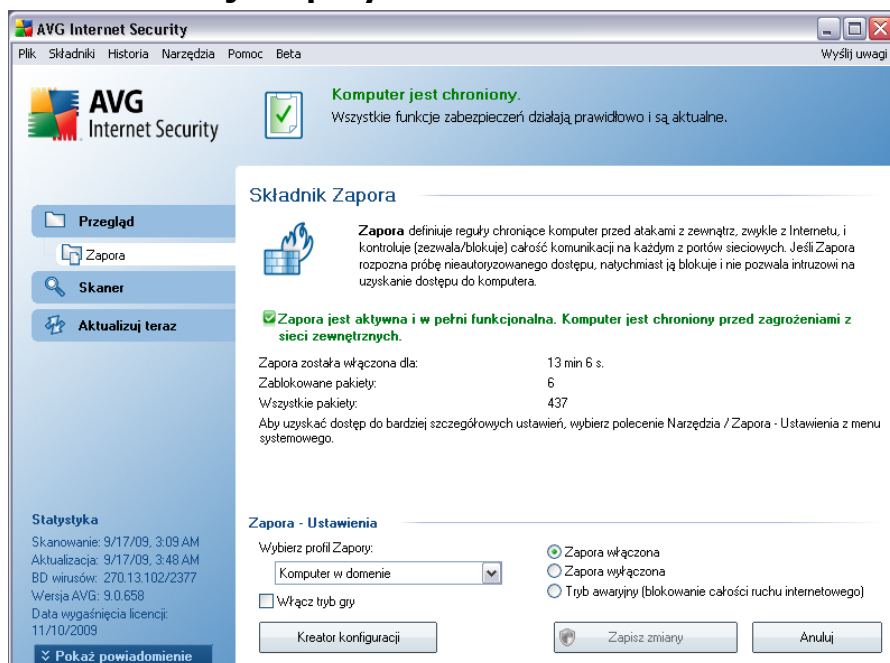
Przelaczanie profili

Funkcja przełączania profili umożliwia składnikowi [Zapora](#) automatyczne przełączenie się na zdefiniowany wcześniej profil w przypadku użycia określonej karty sieciowej lub połączenia z określonym typem sieci. Jeśli do obszaru sieciowego nie został jeszcze przypisany żaden profil, przy najbliższym połączeniu z tym obszarem [Zapora](#) wyświetli okno dialogowe z prośbą o przypisanie profilu.

Profile można tworzyć dla dowolnych interfejsów sieciowych lub obszarów. Ich dalsze ustawienia dostępne są w oknie [Profile kart sieciowych i obszarów](#), w którym można również w razie potrzeby wyłączyć te funkcje (*w takim przypadku dla każdego rodzaju połączenia będzie używany profil domyślny*).

Zazwyczaj funkcja ta będzie przydatna dla użytkowników korzystających z notebooka i różnych typów połączeń. W przypadku komputera stacjonarnego korzystającego tylko z jednego typu połączenia (*tj. kablowego połączenia z internetem*) funkcja przełączania profili prawdopodobnie nigdy nie będzie używana.

8.6.3. Interfejs Zapory



Interfejs składnika **Zapora** udostępnia niektóre podstawowe informacje na temat funkcji oraz krótkie omówienie statystyk **Zapory**:

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

Podstawowa konfiguracja składnika

- **Wybierz profil Zapory** — z menu rozwijanego wybierz jeden ze zdefiniowanych profili — dwa profile są dostępne przez cały czas (*domyslnie profile o nazwach **Odblokuj wszystko** oraz **Blokuj wszystko***). Inne profile zostały dodane wcześniej w wyniku edycji ustawień w oknie [Profil](#) w [Ustawieniach Zapory](#).

- **Wlacz tryb gry** — Zaznaczenie tego pola daje pewnosc, ze podczas dzialania aplikacji pelnoekranowych (gier, prezentacji programu PowerPoint itp.), **Zapora AVG** nie bedzie wyswietlala okien dialogowych z pytaniami, czy komunikacja dla nieznanej aplikacji ma zostac odblokowana. Jesli w tym czasie nowa aplikacja spróbuje polaczyc sie z siecia, **Zapora** automatycznie odblokuje lub zablokuje te próbe (zgodnie z ustawieniami biezacego profilu).
- **Stan Zapory:**
 - o **Zapora włączona** — należy zaznaczyć te opcje, aby zezwalac na komunikacje wszystkim aplikacjom, którym w zbiorze regul zdefiniowanych dla wybranego profilu **Zapory** przypisano akcje „pozwól”.
 - o **Zapora wyłączona** — ta opcja całkowicie wylacza **Zapora**. Ruch sieciowy nie bedzie blokowany ani monitorowany!
 - o **Tryb awaryjny (blokowanie calosci ruchu internetowego)** — należy zaznaczyć te opcje, aby blokowac caly ruch na wszystkich portach. **Zapora** wciaz dziala, lecz komunikacja z siecia jest zablokowana.

Uwaga: Dostawca oprogramowania AVG skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylaczenie przez doswiadczonych uzytkownikow. Jesli konieczna jest zmiana konfiguracji Zapory AVG, nalezy wybrac z menu glownego **Plik / Ustawienia Zapory** i skorzystac z interfejsu **Ustawienia Zapory**.

Przyciski kontrolne

- **Kreator konfiguracji** — przycisk ten pozwala przejsc do okna **Wybór typu komputera** (uzywanego podczas instalacji), w którym mozna skonfigurowac dzialanie **Zapory**.
- **Zapisz zmiany** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- **Anuluj** — klikniecie tego przycisku powoduje powrót do domyslnego okna **Interfejsu uzytkownika AVG** (przeglądu składników).

8.7. Skaner poczty e-mail

Poczta e-mail to od dawna częste źródło wirusów i koni trojańskich. Wyludzenia 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.

8.7.1. Zasady działania Skanera poczty e-mail

Składnik **Skaner poczty e-mail** automatycznie skanuje pocztę przychodzącą i wychodzącą. Można z niego korzystać przy programach pocztowych, dla których nie powstały pluginy AVG (*np. Outlook Express, Mozilla, Incredimail itd.*).

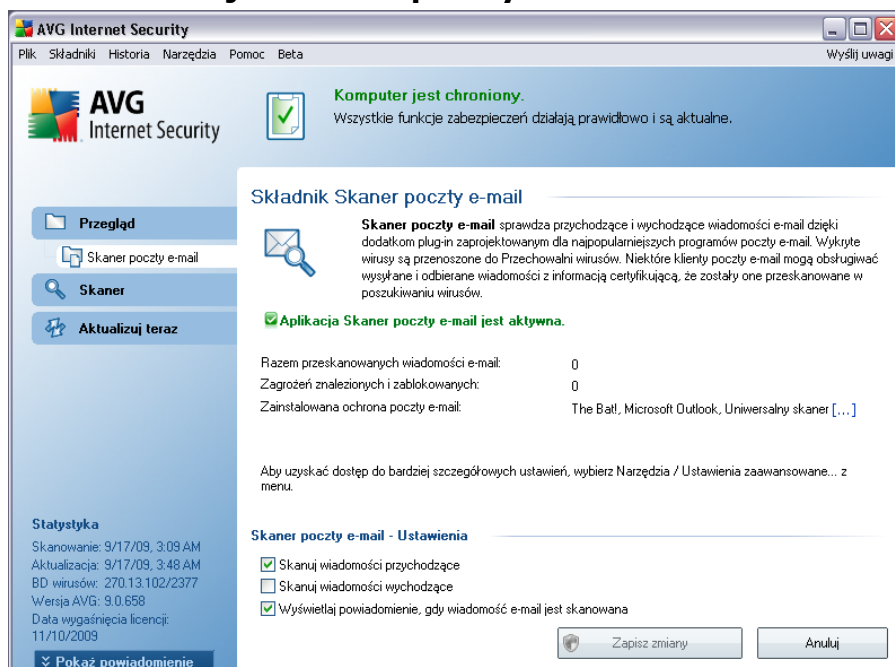
Podczas [instalacji](#) systemu AVG tworzone są automatyczne serwery kontrolujące pocztę e-mail: jeden do sprawdzania wiadomości przychodzących, drugi do wychodzących. Przy pomocy tych serwerów wiadomości e-mail są automatycznie sprawdzane na portach 110 i 25 (*standardowe porty dla wysyłania/odbierania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

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

- **Poczta przychodząca:** Podczas otrzymywania wiadomości z serwera, **Skaner poczty e-mail** sprawdza ją w poszukiwaniu wirusów, usuwa zainfekowane załączniki i dołącza certyfikat. Wykryte wirusy są natychmiast poddawane kwarantannie w [Przechowalni wirusów](#). Wiadomość jest później przekazywana do programu pocztowego.
- **Poczta wychodząca:** Wiadomość jest wysyłana z programu pocztowego do składnika Skaner poczty e-mail, gdzie jest sprawdzana wraz z załącznikami w poszukiwaniu wirusów. Następnie wiadomość jest wysyłana do serwera SMTP (*skanowanie wychodzących wiadomości e-mail jest domyślnie wyłączone i można je skonfigurować ręcznie*).

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

8.7.2. Interfejs Skanera poczty e-mail



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

- **Razem przeskanowanych wiadomości e-mail** — liczba wiadomości przeskanowanych od czasu ostatniego uruchomienia **Skanera poczty e-mail** (w razie potrzeby, np. dla celów statystycznych, wartość tę można wyzerować)
- **Zagrożeń znalezionych i zablokowanych** — liczba zainfekowanych wiadomości wykrytych od czasu ostatniego uruchomienia **Skanera poczty e-mail**.
- **Zainstalowany plugin poczty e-mail** — informacje o pluginie odpowiednim dla Twojego domyślnego klienta poczty

Podstawowa konfiguracja składowika

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

- **Skanuj wiadomości przychodzące** — pozycje te należy zaznaczyć, aby

wszystkie wiadomości e-mail przychodzące na dane konto pocztowe były skanowane w poszukiwaniu wirusów. Domyslnie ta opcja jest włączona i nie zaleca się zmian w tych ustawieniach!

- **Skanuj wiadomości wychodzące** — zaznaczenie tej opcji pozwala określić, czy powinny być skanowane wszystkie wiadomości e-mail wysyłane z konta pocztowego. Opcja ta jest domyslnie wyłączona.
- **Wyswietlaj ikone powiadomienia podczas skanowania wiadomości e-mail** — pozwala określić, czy składowik [Skaner poczty e-mail](#) ma podczas swojej pracy wyświetlać powiadomienia o aktualnie wykonywanym zadaniu (*łączenie z serwerem, pobieranie wiadomości, skanowanie wiadomości, ...*). Ta opcja jest aktywna i nie można jej edytować.

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

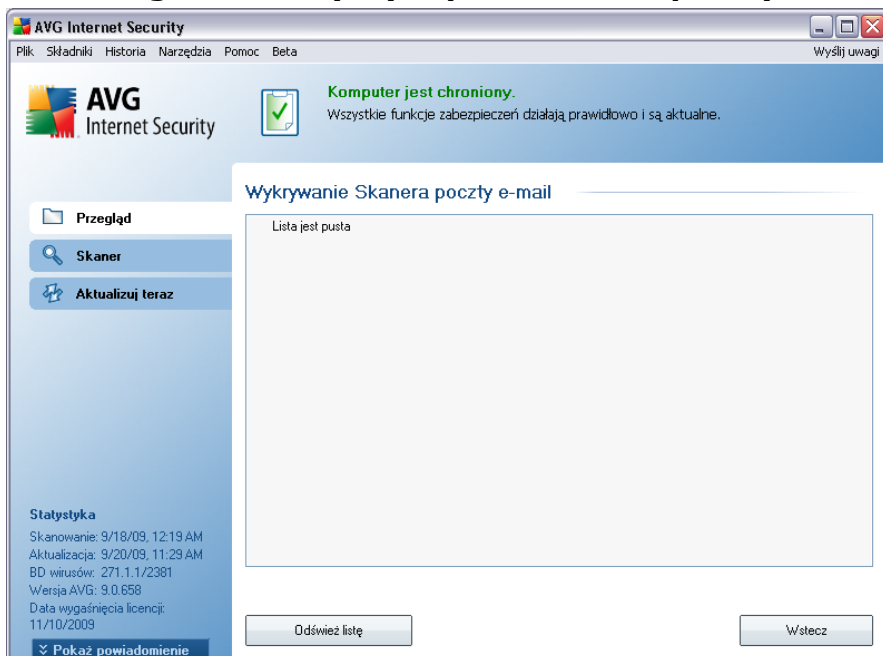
Uwaga: Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składowiki pod kątem optymalnej wydajności. Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana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

Przyciski kontrolne

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

- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- **Anuluj** — kliknięcie tego przycisku powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składowików).

8.7.3. Zagrozenia wykryte przez Skaner poczty e-mail



W oknie **Zagrozenia wykryte przez Skaner poczty e-mail** (dostępnym poprzez menu *Historia*) wyświetlana jest lista wszystkich obiektów znalezionych przez składnik **Skaner poczty e-mail**. Podawane są tam następujące informacje:

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

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

Przyciski kontrolne

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

- **Odśwież listę** — aktualizuje listę wykrytych zagrożeń.
- **Wstecz** — przełącza z powrotem do domyślnego [Interfejsu użytkownika systemu AVG](#) (przeglądu składowików).

8.8. Składowik ID Protection

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

8.8.1. Podstawy działania ID Protection

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

Stanowczo zalecamy zainstalowanie zarówno składowika [AVG Anti-Virus](#), jak i AVG Identity Protection. Razem zapewniają one kompleksową ochronę komputera.

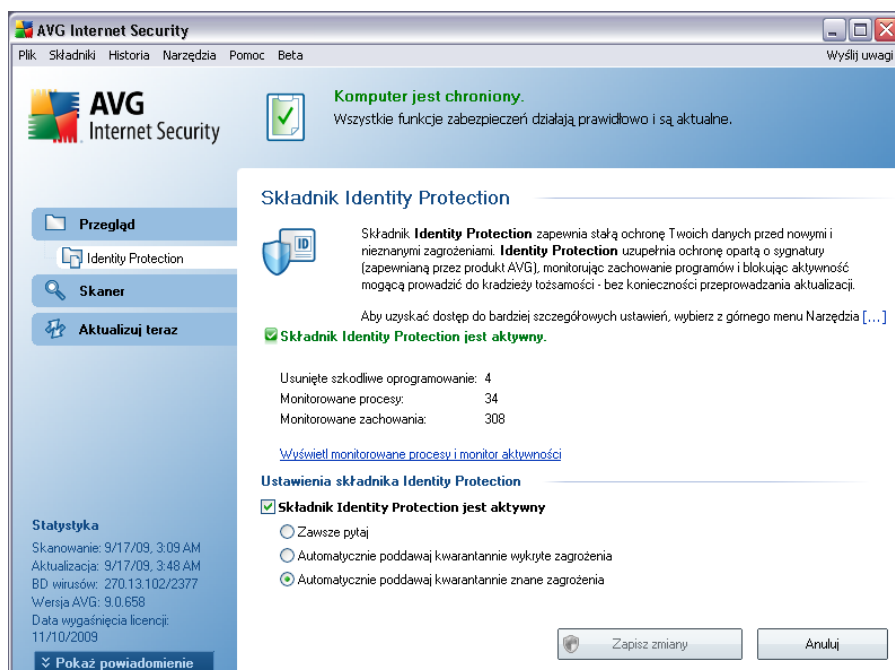
8.8.2. Interfejs składowika ID Protection

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

- **Usunięte szkodliwe oprogramowanie** — zawiera liczbę aplikacji wykrytych jako szkodliwe oprogramowanie (a następnie usuniętych)
- **Monitorowane procesy** — liczba obecnie uruchomionych aplikacji, które są

monitorowane przez składnik IDP

- **Monitorowane zachowania** — liczba określonych czynności uruchomionych w monitorowanych aplikacjach



Podstawowa konfiguracja składnika

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

- **Składnik Identity Protection jest aktywny** — (domyslnie włączone) należy zaznaczyć to pole, aby aktywować składnik IDP i otworzyć dalsze opcje edycji.

W pewnych przypadkach program **Identity Protection** może zgłosić, że plik pochodzący z zaufanego źródła jest podejrzany lub niebezpieczny. Ponieważ program **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:

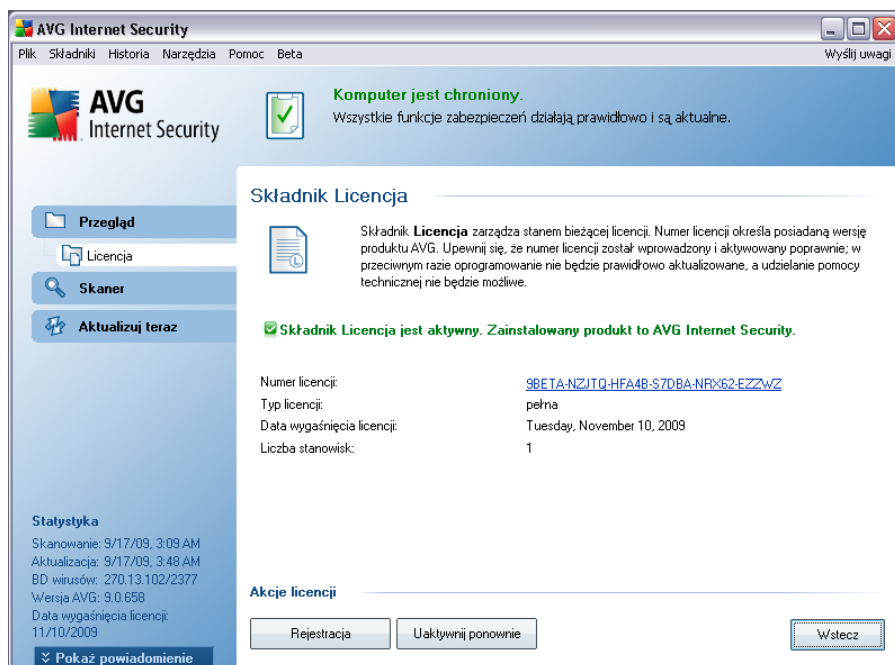
- o **Zawsze pytaj** — jeśli aplikacja zostanie wykryta jako szkodliwe oprogramowanie, użytkownik zostanie zapytany, czy powinna zostać zablokowana
- o **Automatycznie poddawaj kwarantannie wykryte zagrożenia** — wszystkie aplikacje uznane za szkodliwe będą automatycznie blokowane
- o **Automatycznie poddawaj kwarantannie znane zagrożenia** — tylko te aplikacje, które zostają wykryte jako szkodliwe oprogramowanie ze stuprocentową pewnością, będą blokowane (*ta opcja jest domyślnie włączona i nie zaleca się zmieniania tego stanu rzeczy bez ważnego powodu*)

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).

8.9. Licencja



Okno dialogowe składowika **Licencja** zawiera krótki opis jego funkcji, informacje o jego bieżącym stanie (Składnik Licencja *jest aktywny.*), a także następujące informacje:

- **Numer licencji** — dokładny numer licencji. Jeżeli kiedykolwiek będziesz proszony o podanie swojego numeru licencji, użyj go w tej samej formie. Dlatego też zdecydowanie zalecamy korzystanie z metody kopiuj-wklej w przypadku jakiegokolwiek manipulacji numerem licencji.
- **Typ licencji** — określa typ zainstalowanego produktu.
- **Data wygaśnięcia licencji** — data określająca okres ważności licencji. Aby korzystać z systemu **AVG 9 Internet Security** po tej dacie, należy odnowić licencję. [Licencje można odnowić online](http://www.avg.com/) za pośrednictwem witryny firmy AVG (<http://www.avg.com/>).
- **Liczba stanowisk** — liczba stacji roboczych, na których można zainstalować system **AVG 9 Internet Security**.

Przyciski kontrolne

- **Zarejestruj** — łączy się ze stroną rejestracji w witrynie systemu AVG (<http://www.avg.com/>). Należy tam podać swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysługuje bezpłatna pomoc techniczna.
- **Uaktywnij ponownie** — otwiera okno dialogowe **Aktywacja programu AVG** zawierające dane wprowadzone na etapie **Personalizacji programu AVG** podczas **Instalacji**. W oknie tym można wprowadzić numer licencji w celu zastąpienia numeru sprzedaży (*użytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przykład podczas uaktualnienia do nowego produktu AVG*).
- **Wstecz** — kliknięcie tego przycisku powoduje powrót do domyślnego **Interfejsu użytkownika systemu AVG** (przeglądu składników).

8.10. LinkScanner

8.10.1. Zasady działania technologii LinkScanner

Składnik **LinkScanner®** zapewnia darmową ochronę przed witrynami internetowymi, które zdolne są do instalowania na komputerze szkodliwego oprogramowania za pośrednictwem przeglądarki internetowej lub jej pluginów. Technologia składnika **LinkScanner** składa się z dwóch funkcji: **AVG Search-Shield** i **AVG Active Surf-Shield**:

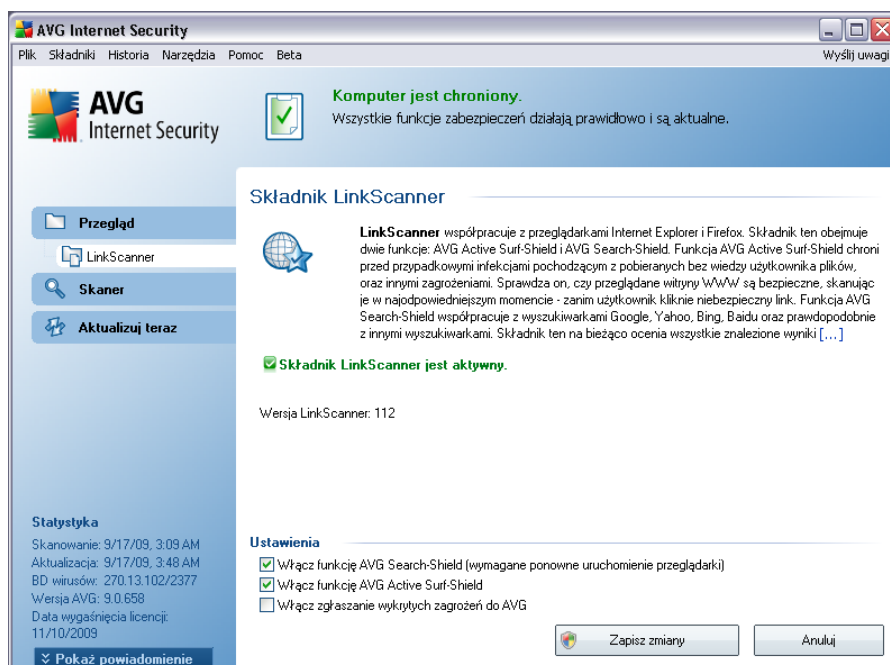
- **Składnik AVG Search Shield** zawiera listę witryn sieci Web (*adresów URL*), które uznane zostały za niebezpieczne. Wszystkie wyniki wyszukiwania otrzymane za pomocą wyszukiwarek Google, Yahoo!, MSN lub Baidu są sprawdzane na podstawie tej listy, a następnie otrzymują ikony werdyktu (w przypadku wyników wyszukiwania Yahoo! wyświetlane są tylko ikony „niebezpieczna witryna”). Jeśli bezpośrednio w przeglądarce wprowadzony zostanie jakikolwiek adres, kliknięty zostanie link na stronie WWW lub np. w wiadomości e-mail, AVG automatycznie go przeskanuje i — w razie potrzeby — adres zostanie zablokowany.
- **Składnik AVG Active Surf-Shield** skanuje zawartość odwiedzanych witryn internetowych bez względu na ich adres. Nawet jeśli jakaś witryna nie zostanie wykryta przez składnik **AVG Search Shield** (np. gdy utworzono nową szkodliwą witrynę sieci Web lub witryna wcześniej uznana za nieszkodliwą zawiera aktualnie niebezpieczny kod), przy próbie jej odwiedzenia zostanie ona przeskanowana (a w razie podejrzenia zablokowana) przez składnik **AVG Active Surf-Shield**.

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

8.10.2. Interfejs LinkScanner

Składnik **LinkScanner** składa się z dwóch funkcji, które można włączyć lub wyłączyć w jego interfejsie :

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



W dolnej części okna dialogowego możliwa jest edycja następujących opcji:

- **Włącz funkcję AVG Search-Shield** — (*domyslnie włączona*): Skanuje wszystkie linki pojawiające się w wynikach wyszukiwania serwisów Google, Yahoo! oraz MSN, a następnie obok każdego z nich wyświetla klasyfikację bezpieczeństwa.
- **Włącz funkcję AVG Active Surf-Shield** — (*domyslnie 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 jakiegokolwiek innej aplikacji korzystającej z protokołu HTTP).

- **Włącz zgłaszanie wykrytych zagrożeń do firmy AVG** — należy zaznaczyć to pole, aby włączyć raportowanie exploitów oraz niebezpiecznych witryn znalezionych przy użyciu funkcji **Safe Surf** lub **Safe Search**. Informacje te są przekazywane do naszej bazy danych.

8.10.3. AVG Search-Shield

Podczas wyszukiwania w Internecie funkcja z włączoną funkcją **Ochrona wyszukiwania systemu AVG** wszystkie wyniki najbardziej popularnych wyszukiwarek internetowych, np. Yahoo!, Google, MSN itd., są oceniane pod kątem obecności niebezpiecznej lub podejrzanej zawartości. Sprawdzając te łącza i oznaczając niebezpieczne, [pasek narzędzi zabezpieczeń systemu AVG](#) ostrzega przed przejściem na niebezpieczną lub podejrzaną stronę. W ten sposób można poruszać się tylko po bezpiecznych witrynach WWW.

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

 Strona, do której prowadzi łącze, jest bezpieczna (w wyszukiwarce Yahoo! ta ikona nie jest wyświetlana na [pasku narzędzi zabezpieczeń systemu AVG](#)!).

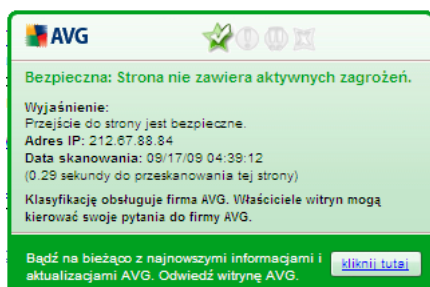
 Strona, do której prowadzi łącze, nie zawiera zagrożeń, ale jest podejrzana (wątpliwości budzi jej pochodzenie lub przeznaczenie, więc nie zaleca się dokonywania na niej zakupów itp.).

 Strona, do której prowadzi łącze, jest bezpieczna, ale zawiera łącza 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 łącze, nie jest dostępna i nie udało się jej przeskanować.

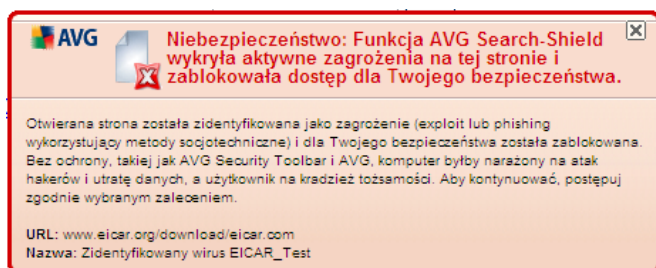
Umieszczenie kursora na wybranej ikonie wyników sprawdzania powoduje wyświetlenie szczegółowych informacji o danym łączu. Informacje te obejmują dodatkowe szczegóły dotyczące zagrożenia (jeśli są dostępne), adres IP łącza oraz czas przeskanowania strony przez AVG:



8.10.4. AVG Active Surf-Shield

Ta zaawansowana funkcja ochrony blokuje szkodliwa zawartość dowolnej otwieranej witryny internetowej, zapobiegając pobraniu jej na komputer. Gdy funkcja ta jest włączona, kliknięcie linku lub wpisanie adresu URL prowadzącego do niebezpiecznej witryny powoduje automatycznie zablokowanie jej otwarcia, dzięki czemu komputer nie zostanie nieswiadomie 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, [pasek narzędzi AVG Security Toolbar](#) nie pozwoli na jej wyświetlenia w przeglądarce.

Jeśli kiedykolwiek trafisz na szkodliwą stronę internetową, [pasek narzędzi AVG Security Toolbar](#) wyświetli w przeglądarce ostrzeżenie podobne do tego:



Odwiedzanie takiej witryny jest bardzo ryzykowne i należy tego unikać!

8.11. Ochrona sieci WWW

8.11.1. Zasady działania składowa Ochrona sieci WWW

Ochrona sieci WWW to rodzaj programu rezydentnego, zapewniającego ochronę w czasie rzeczywistym. Skanuje on zawartość odwiedzanych stron internetowych (oraz znajdujących się na nich plików) jeszcze zanim zostaną wyświetlone w przeglądarce

lub pobrane na dysk twardy.

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

Uwaga: *Ochrona sieci WWW nie jest przeznaczona dla platform serwerowych!*

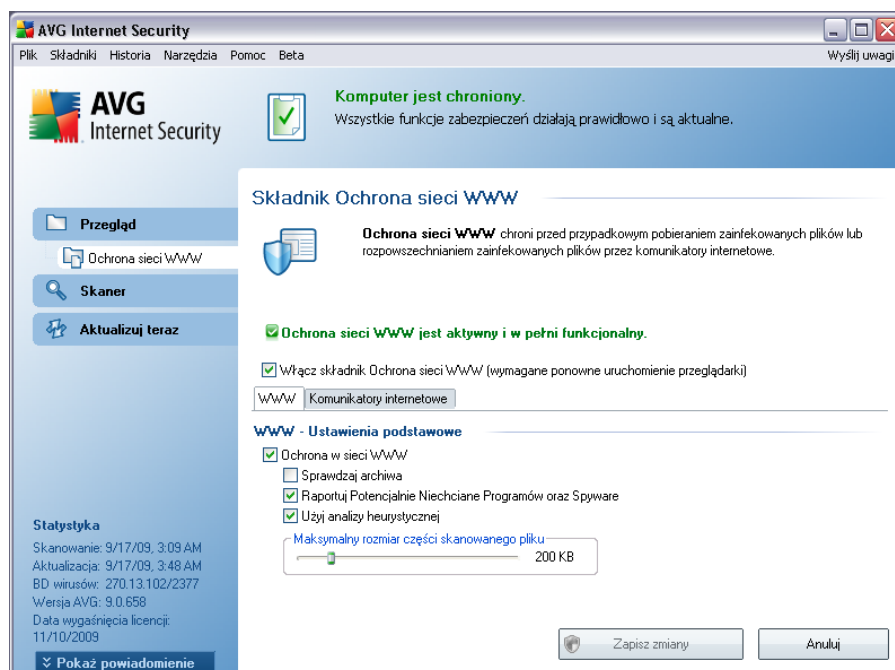
8.11.2. Interfejs składowika Ochrona sieci WWW

Interfejs składowika **Ochrona sieci WWW** opisuje działanie tego rodzaju ochrony. Znajdują się tam informacje na temat bieżącego stanu (*Składnik Ochrona sieci WWW jest aktywny i w pełni funkcjonalny.*). W dolnej części okna widoczne są podstawowe opcje Ochrony sieci WWW.

Podstawowa konfiguracja składowika

Najistotniejsza opcja umożliwia natychmiastowe włączenie lub wyłączenie składowika **Ochrona sieci WWW** (pole **Włącz Ochronę sieci WWW**). Pole to jest domyślnie zaznaczone, a składowik **Ochrona sieci WWW** aktywny. Jednak jeśli nie istnieją ważne powody do zmiany tego ustawienia, zaleca się pozostawienie składowika aktywnego. Jeśli to pole jest zaznaczone (składowik **Ochrona sieci WWW** działa), na dwóch kolejnych kartach znajdują się dalsze opcje konfiguracji.

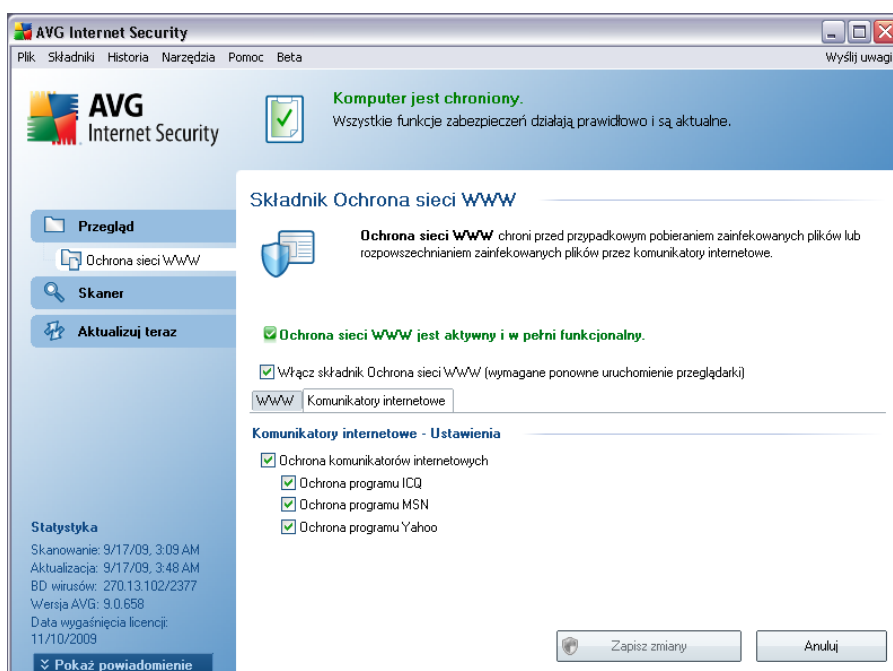
- **WWW** — karta odpowiadająca za skanowanie zawartości witryny internetowych. Interfejs pozwala modyfikować następujące ustawienia:



- o **Ochrona w sieci WWW** — potwierdza, że składnik **Ochrona sieci WWW** ma skanować zawartość stron internetowych. Jeśli ta opcja jest aktywna (*domyślnie*), można włączyć lub wyłączyć następujące funkcje:
 - **Skanuj wewnątrz archiwów** — skanowanie ma obejmować także archiwa dostępne na odwiedzanych stronach WWW.
 - **Raportuj potencjalnie niechciane programy** — skanowanie ma obejmować potencjalnie niechciane programy (*pliki wykonywalne, które mogą być programami szpiegującymi lub reklamowymi*) obecne na wyświetlanych stronach WWW.
 - **Użyj analizy heurystycznej** — skanowanie zawartości wyświetlanych stron ma wykorzystywać metody analizy heurystycznej (*dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej*) — zobacz rozdział [Zasady działania składu Anti-Virus](#).
 - **Maksymalny rozmiar skanowanych plików** — jeśli wyświetlana strona zawiera pliki, można skanować ich zawartość jeszcze przed pobraniem na twardy dysk. 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 WWW**. Nawet jeśli pobierany plik jest większy od wybranego limitu i nie zostanie przeskanowany przez **Ochronę sieci WWW**, nie zmniejsza to Twojego bezpieczeństwa: jeśli plik jest zainfekowany, składnik **Ochrona rezydentna** natychmiast to wykryje.

- **Komunikatory internetowe** — karta umożliwiająca edycję ustawień monitorowania komunikatorów internetowych (np. ICQ, MSN Messenger, Yahoo itp.).



- o Ochrona komunikatorów internetowych — zaznacz to pole, jeśli chcesz, aby Ochrona sieci WWW zapewniała bezpieczeństwo komunikacji online. O ile opcja ta jest zaznaczona, można dodatkowo określić, które komunikatory internetowe mają być kontrolowane — aktualnie program **AVG 9 Internet Security** obsługuje aplikacje ICQ, MSN oraz Yahoo.

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

zaawansowane i skorzystać z interfejsu [Zaawansowane ustawienia AVG](#).

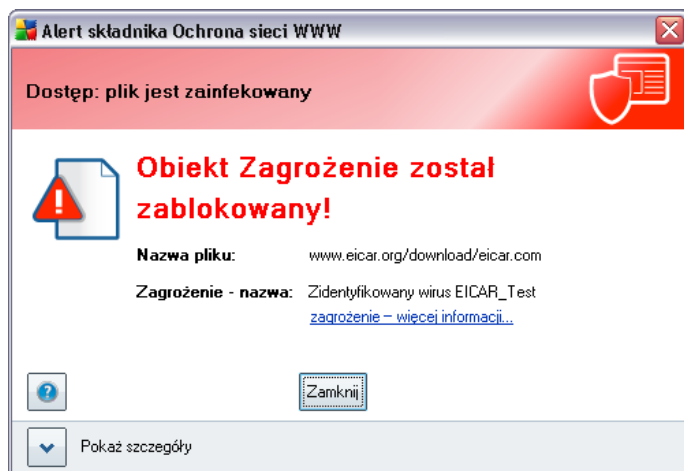
Dostępne przyciski

W interfejsie składnika **Ochrona sieci WWW** dostępne są następujące przyciski kontrolne:

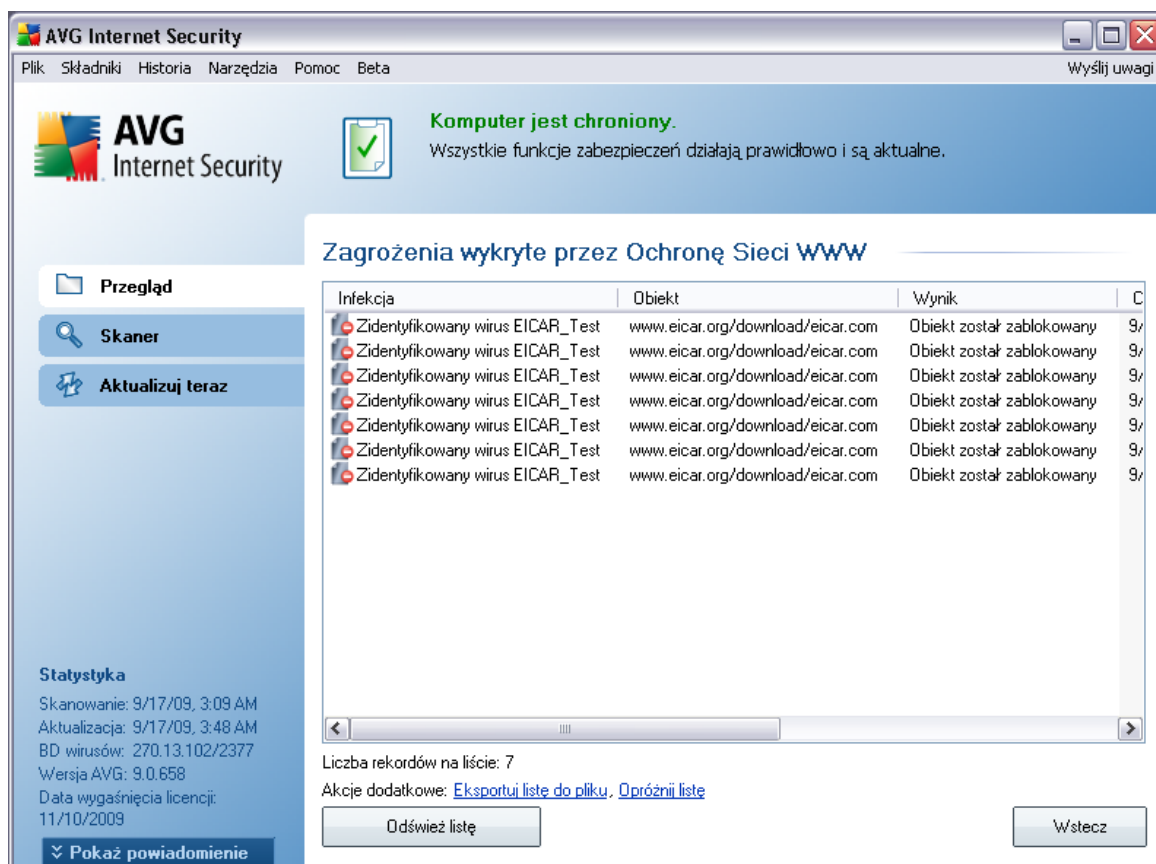
- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- **Anuluj** — powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składników).

8.11.3. Zagrożenia wykryte przez Ochronę sieci WWW

Ochrona sieci WWW 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:



Podjęta strona nie zostanie otwarta, a wykryty obiekt zostanie zapisany na liście **zagrożeń wykrytych przez Ochronę sieci WWW** (ten przegląd wykrytych zagrożeń jest dostępny poprzez menu systemowe [Historia / Zagrożenia wykryte przez Ochronę sieci WWW](#)).



Podawane są tam następujące informacje:

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

U dołu okna znajdują się informacje na temat łącznej liczby wykrytych infekcji. Ponadto, można wyeksportować całą listę obiektów do pliku, (**Eksportuj listę do**

pliku) lub usunąć wszystkie jej pozycje (**Opróżnij listę**). Przycisk **Odśwież listę** pozwala zaktualizować listę obiektów wykrytych przez składnik **Ochrona sieci WWW**. Przycisk **Wstecz** przełącza z powrotem do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składników).

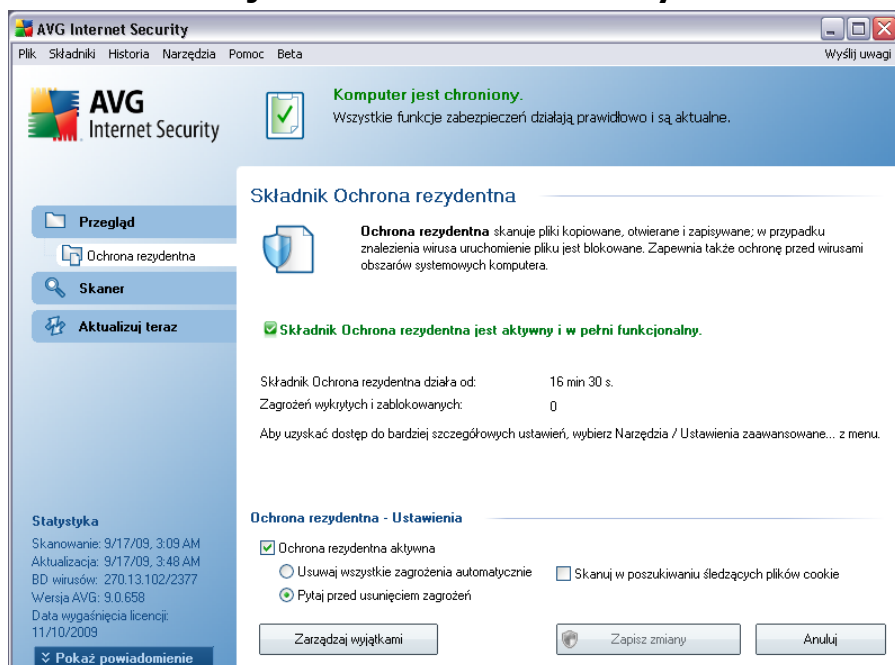
8.12. Ochrona rezydentna

8.12.1. Zasady działania Ochrony rezydentnej

Składnik **Ochrona rezydentna** zapewnia stałą ochronę komputera. Ochrona rezydentna skanuje każdy otwierany, zapisywany i kopiowany plik, a także chroni obszary systemowe komputera. Po wykryciu wirusa w przetwarzanym pliku, **Ochrona rezydentna** zatrzymuje aktualnie wykonywane operacje i uniemożliwia uaktywnienie się wirusa. Użytkownik zwykle nie zauważa działania tego składnika, ponieważ funkcjonuje ona „w tle” i wyświetla powiadomienia tylko w przypadku, gdy wykryje zagrożenie. Domyślna reakcja **Ochrony rezydentnej** jest zablokowanie dostępu do niebezpiecznego pliku. Składnik **Ochrona rezydentna** jest ładowany do pamięci komputera podczas uruchamiania systemu.

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

8.12.2. Interfejs składowika Ochrona rezydentna



Oprócz przeglądu najważniejszych statystyk oraz informacji na temat stanu składowika (*składowik Ochrona rezydentna jest aktywny i w pełni funkcjonalny*), interfejs **Ochrony rezydentnej** oferuje także kilka elementarnych opcji konfiguracyjnych. Wyświetlane są następujące statystyki:

- **Ochrona Rezydenta działa od** — określa czas, jaki upłynął od ostatniego uruchomienia składowika.
- **Zagrożeń wykrytych i zablokowanych** — liczba wykrytych infekcji, do których uruchomienia nie dopuszczono (*w razie potrzeby, np. dla celów statystycznych, wartość tę można wyzerować*)

Podstawowa konfiguracja składowika

W dolnej części okna dialogowego znajduje się sekcja o nazwie **Ochrona rezydentna - Ustawienia**, w której można edytować niektóre podstawowe funkcje (*szczegółowa konfiguracja, podobnie jak w wypadku innych składowików, dostępna jest za pośrednictwem menu Narzędzia / Ustawienia zaawansowane*).

Pole **Ochrona rezydentna aktywna** umożliwia łatwe włączanie/wyłączanie Ochrony

rezydentnej. Domyslnie funkcja ta jest wlaczona. Gdy Ochrona rezydentna jest wlaczona, mozna okreslic w jaki sposob ma reagowac na wykryte infekcje:

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

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

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

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

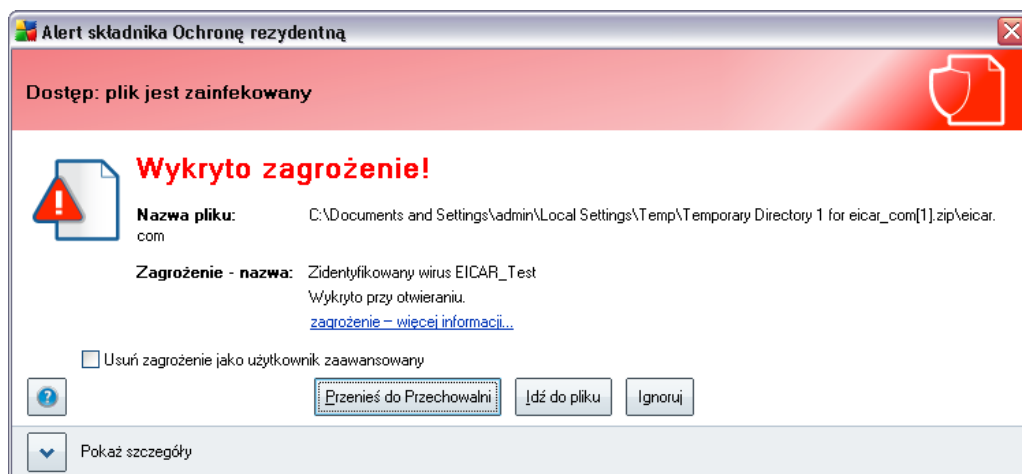
Dostepne przyciski

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

- **Zarządzaj wyjątkami** - otwiera okno dialogowe [Ochrona rezydentna — Wykluczone katalogi](#), w którym mozna zdefiniowac foldery ignorowane przez skladnik [Ochrona rezydentna](#).
- **Zapisz zmiany** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- **Anuluj** — klikniecie tego przycisku powoduje powrót do domyslnego okna [Interfejsu uzytkownika AVG](#) (przegladu skladnikow).

8.12.3. Zagrozenia wykryte przez Ochrone rezydentna

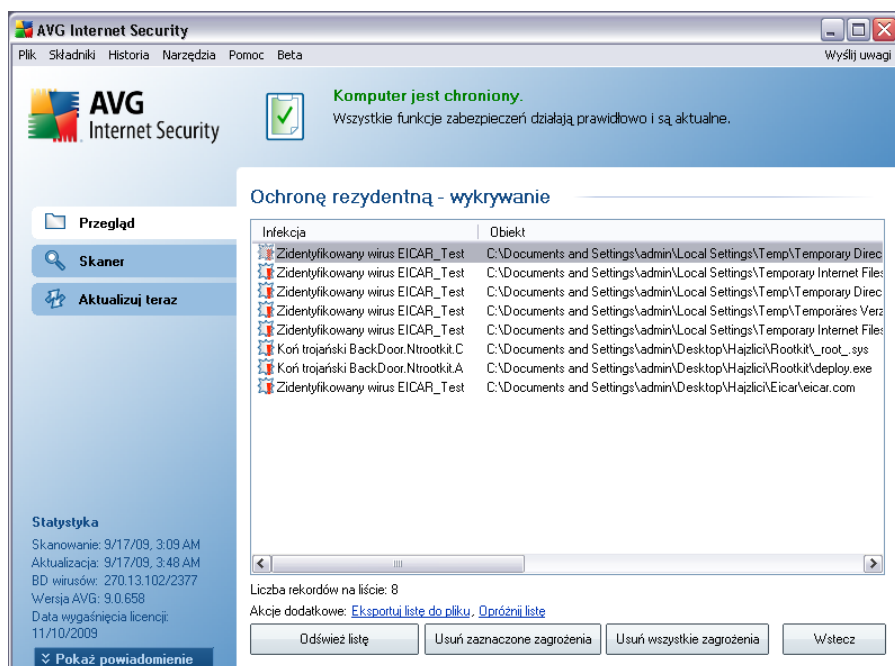
Ochrona rezydentna to składowy służy do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego ostrzeżenia:



Okno to zawiera informacje dotyczące wykrytej infekcji i pozwala wybrać czynność, która ma zostać wykonana:

- **Wylecz** — jeśli możliwe jest wyleczenie pliku, system AVG zrobi to automatycznie (opcja zalecana).
- **Przenies do Przechowalni** — wirus zostanie przeniesiony do [Przechowalni wirusów AVG](#)
- **Przejdź do pliku** — pozwala przejść do lokalizacji podejrzanego obiektu (w nowym oknie Eksploratora Windows)
- **Ignoruj** — tej opcji NIE należy używać bez uzasadnionego powodu!

Przegląd wszystkich zagrożeń wykrytych przez składowy [Ochrona rezydentna](#) można znaleźć w oknie dialogowym **Zagrozenia wykryte przez Ochrone rezydentna** dostępnym poprzez menu [Historia / Zagrozenia wykryte przez Ochrone rezydentna](#):



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](#)). Dla każdego wykrytego obiektu podawane są następujące informacje:

- **Infekcja** — opis (ewentualnie nazwa) wykrytego obiektu.
- **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 **Odswież listę** pozwala zaktualizować listę obiektów wykrytych przez **Ochronę rezydentną**. Przycisk **Wstecz** przełącza z powrotem do domyślnego [Interfejsu użytkownika](#)

[AVG](#) (przeglądu składników).

8.13. Menedżer aktualizacji

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

Regularne aktualizacje systemu AVG są kluczowe dla Twojego bezpieczeństwa!

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

Uwaga: Więcej informacji na temat typów i poziomów aktualizacji zawiera rozdział [Aktualizacje AVG](#).

AVG Download Manager jest prostym menedżerem, za pomocą którego można łatwo administrować pobieraniem produktów AVG. Na podstawie dokonanych wyborów menedżer dostosuje do Twoich potrzeb określony produkt, typ licencji i język. Główną zaletą tego narzędzia jest możliwość zarządzania pobieraniem produktów AVG zgodnie z potrzebami użytkownika. Dodatkowo zyskujesz pewność, że pobrany zostanie najnowszy instalator AVG, dzięki czemu zainstalowany program będzie w pełni aktualny.

AVG Download Manager

- zawsze pobiera najnowszy plik instalacyjny,
- redukuje wielkość pobieranego pliku,
- pozwala wznowić pobieranie przerwane z dowolnej przyczyny,
- współpracuje ze wszystkimi edycjami systemu AVG dla użytku prywatnego.

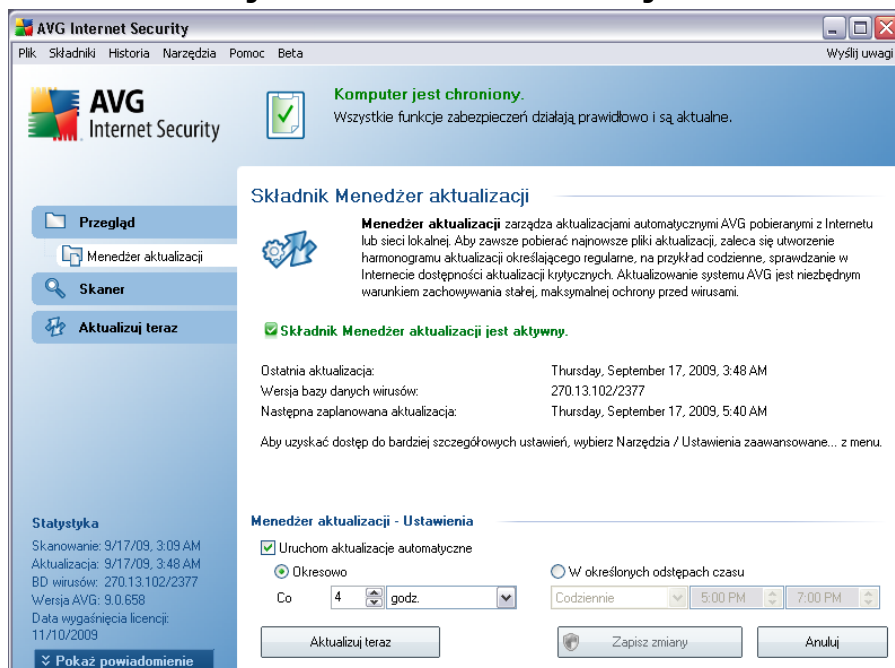
Uwaga: Program AVG Download Manager nie jest odpowiedni do pobierania wersji sieciowych oraz SBS i obsługuje tylko następujące systemy operacyjne: Windows 2000 (SP4 + pakiet zbiorczy SRP), Windows XP (SP2 i nowsze), Windows Vista (wszystkie wersje).

8.13.1. Zasady działania Menedzera aktualizacji

AVG Download Manager działa w następujący sposób:

- Po pierwsze, należy pobrać sam program **AVG Download Manager**. Po uruchomieniu program **AVG Download Manager** monitoruje o wybranie języka instalacji.
- Następnie **AVG Download Manager** spróbuje ustawić testowe połączenie internetowe. Jeśli test połączenia zakończy się pomyślnie, można będzie wybrać wersję programu AVG, która ma zostać zainstalowana (*pełna, próbna lub bezpłatna*).
- Po wybraniu wersji programu AVG należy wskazać produkt, który ma zostać zainstalowany.
- Na koniec pobierane są wszystkie wymagane pliki instalacyjne. **AVG Download Manager** jest zamykany i uruchomiona zostaje [instalacja programu AVG](#).

8.13.2. Interfejs Menedzera aktualizacji



Interfejs składowika **Menedżer aktualizacji** zawiera informacje o jego funkcjach i

bieżącym stanie (Składnik *Menedżer aktualizacji jest aktywny.*), a także istotne statystyki:

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

Podstawowa konfiguracja składnika

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

Ponadto, można określić, kiedy aktualizacje mają być uruchamiane:

- o **Okresowo** — należy zdefiniować interwał aktualizacji.
- o **O określonej godzinie** — należy zdefiniować dokładną datę i godzinę.

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

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

Przyciski kontrolne

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

- **Aktualizuj teraz** — kliknięcie przycisku uruchamia [natychmiastowa aktualizacje](#) na zadanie.
- **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).

8.14. Pasek narzędzi AVG Security Toolbar

Pasek narzędzi AVG Security Toolbar to nowy plugin współpracujący ze składnikiem [Link Scanner](#), który sprawdza wyniki zwracane przez obsługiwane wyszukiwarki internetowe (*Yahoo!*, *Google*, *MSN*, *Baidu*).

Jeśli w czasie instalacji systemu **AVG 9 Internet Security** zostanie wybrana instalacja paska narzędzi, automatycznie nastąpi jego dodanie do przeglądarki internetowej.

Pasek narzędzi AVG Security Toolbar służy do kontrolowania funkcji składnika [Link Scanner](#) i dostosowywania jego zachowania. Umożliwia również aktualizowanie systemu **AVG 9 Internet Security**, jeśli nowe aktualizacje są dostępne.

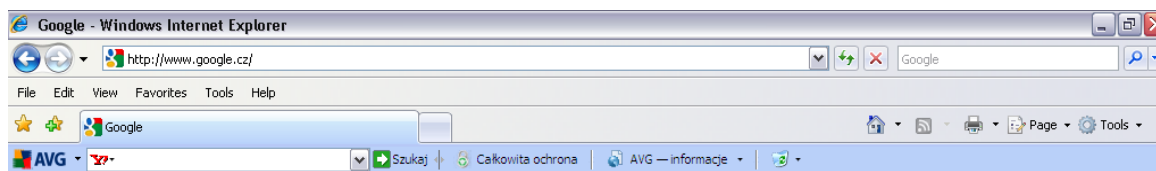
Uwaga: W przypadku korzystania z alternatywnej przeglądarki internetowej (np. *Avant Browser*) mogą wystąpić nieoczekiwane zachowania.

8.14.1. Interfejs paska narzędzi AVG Security Toolbar

Pasek narzędzi AVG Security Toolbar jest zgodny z przeglądarkami **MS Internet Explorer** (wersja 6.0 lub nowsza) i **Mozilla Firefox** (wersja 1.5 lub nowsza).

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

Po podjęciu decyzji o zainstalowaniu paska narzędzi **AVG Security Toolbar** (w czasie [instalacji systemu AVG](#) pojawiło się pytanie o zainstalowanie tego składnika), pasek umieszczany jest pod paskiem adresu w oknie przeglądarki:



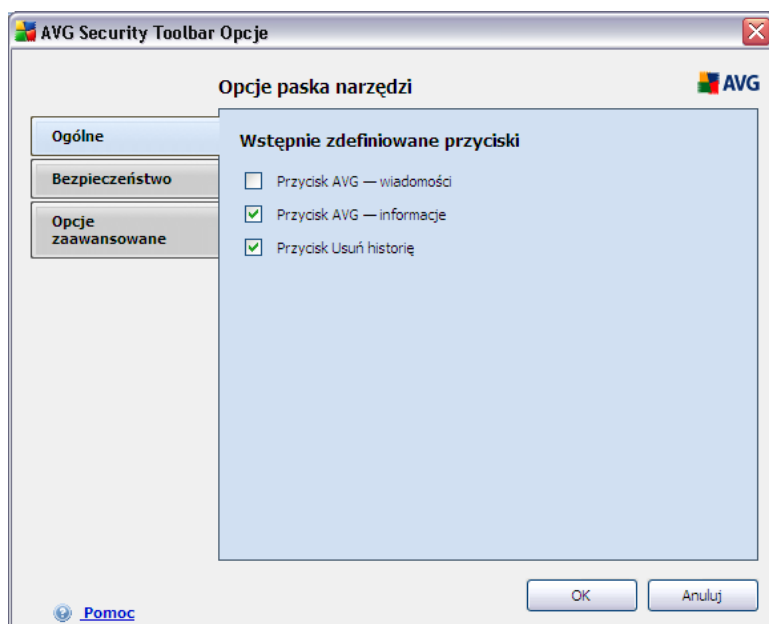
AVG Security Toolbar składa się z następujących elementów:

- **Przycisk logo AVG** — pozwala uzyskać dostęp do głównych elementów paska narzędzi. Kliknięcie go spowoduje przejście do witryny systemu AVG (<http://www.avg.com/>). Kliknięcie strzałki obok ikony AVG powoduje otwarcie menu z następującymi pozycjami:
 - o **Informacje o pasku narzędzi** — link do strony głównej **AVG Security Toolbar**, zawierającej szczegółowe informacje o działaniu paska.
 - o **Uruchom AVG 9.0** — powoduje otwarcie interfejsu użytkownika systemu [AVG](#)
 - o **Opcje** — powoduje otwarcie okna dialogowego, w którym można określać ustawienia paska narzędzi **AVG Security Toolbar** — patrz rozdział [Opcje paska narzędzi AVG Security Toolbar](#)
 - o **Usun historie** — daje dostęp do poleceń: *Usun cała historie*, *Usun historie wyszukiwania*, *Usun historie przeglądania*, *Usun historie pobierania* i *Usun pliki cookie* w Pasku narzędzi AVG Security Toolbar.
 - o **Aktualizacja** — pozwala sprawdzić dostępność nowych aktualizacji **dotyczących Paska narzędzi AVG**
 - o **Pomoc** — pomaga znaleźć odpowiednie pliki Pomocy, skontaktować się z [Pomocą Techniczną AVG](#) lub wyświetlić szczegóły dotyczące bieżącej wersji AVG Security Toolbar.
- **Yahoo! (pole wyszukiwarki)** — proste i bezpieczne przeszukiwanie sieci przy użyciu wyszukiwarki Yahoo! Wprowadzając wyraz lub frazę w tym polu i naciskając przycisk **Szukaj**, można rozpocząć wyszukiwanie przy użyciu serwisu Yahoo! — niezależnie od tego, jaka strona jest obecnie wyświetlana. Wspomniane pole zawiera także historie poprzednich wyszukiwań. Wszystkie wyniki wyszukiwania zostaną oczywiście sprawdzone za pomocą funkcji [AVG Search-Shield](#).
- **Przycisk AVG Active Surf-Shield** — pozwala włączyć lub wyłączyć funkcję [AVG Active Surf-Shield](#).
- **Przycisk AVG Search-Shield** — przycisk pozwala włączyć lub wyłączyć funkcję [AVG Search-Shield](#).
- **Przycisk Informacje o programie AVG** — zawiera linki do ważnych informacji dotyczących bezpieczeństwa, znajdujących się w witrynie AVG (<http://www.avg.com/>).

8.14.2. Opcje Paska narzędzi AVG Security Toolbar

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

- **Ogólne**



Na tej karcie możliwe jest określenie, które przyciski mają być wyświetlane / ukryte na panelu **Paska narzędzi AVG Security Toolbar**:

- o **Przycisk Nowosci AVG** — ta opcja pozwala wyświetlić przycisk **Nowosci AVG**. Kliknięcie tego przycisku na panelu **Paska narzędzi AVG Security Toolbar** otwiera rozwijane menu z linkami do aktualnych informacji prasowych o systemie AVG.
- o **Przycisk Informacje AVG** — przycisk **Informacje AVG** otwiera menu z następującymi opcjami:
 - **Informacje o pasku narzędzi** — otwiera stronę produktu **AVG Security Toolbar**, która zawiera szczegółowe informacje na jego temat

- *O zagrożeniach* — otwiera stronę internetową laboratorium wirusów firmy AVG, która zawiera informacje o najnowszych zagrożeniach, zaleceniach dotyczących usuwania wirusów, listę najczęściej zadawanych pytań itp.
 - *Nowości AVG* — otwiera stronę internetową zawierającą najnowsze informacje prasowe dotyczące systemu AVG
 - *Obecny poziom zagrożenia* — otwiera stronę internetową laboratorium wirusów, która zawiera graficzną reprezentację obecnego poziomu zagrożenia w sieci
 - *Encyklopedia wirusów* — otwiera stronę encyklopedii wirusów, w której można wyszukać określone wirusy na podstawie ich nazw i uzyskać szczegółowe informacje na ich temat
- o **Przycisk Usun historie** — przycisk ten pozwala *usunąć całą historię*, lub *usunąć historię wyszukiwania, przeglądania i pobierania* lub tylko *usunąć ciasteczki* bezpośrednio z panelu **Paska narzędzi AVG Security Toolbar**.

• **Bezpieczeństwo**



Karta **Bezpieczeństwo** jest podzielona na dwie sekcje (**Bezpieczeństwo**

przeglądarki i Oceny), w których można zaznaczyć określone pola, aby skonfigurować następujące funkcje:

- o **Bezpieczeństwo przeglądarki** — te pozycje należy zaznaczyć, aby aktywować lub wyłączyć [funkcje AVG Search-Shield](#) i/lub [funkcje AVG Surf-Shield](#)
- o **Oceny** — należy wybrać symbole graficzne, które mają być używane przy klasyfikacji wyników wyszukiwania przez funkcję [AVG Search-Shield](#) :

-  strona jest bezpieczna
-  strona jest podejrzana
-  strona zawiera linki do niebezpiecznych stron
-  strona zawiera aktywne zagrożenia
-  strona nie jest dostępna i nie można jej przeskanować

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

- **Opcje zaawansowane**



Na karcie **Opcje zaawansowane** można aktywować lub wyłączyć dalsze szczegółowe ustawienia **Paska narzędzi AVG Security Toolbar**:

- o **Ustaw i zachowaj Yahoo! jako domyślną wyszukiwarke używaną na pasku adresu** — (domyślnie włączone) — jeśli ta opcja jest zaznaczona, możliwe jest wyszukiwanie stron bezpośrednio w pasku adresu przeglądarki internetowej, przy użyciu Yahoo!
- o **Pokaż pole wyszukiwarki Yahoo! na nowych kartach** — (domyślnie włączone) — zaznaczenie tej opcji powoduje wyświetlanie pola wyszukiwarki Yahoo! na każdej nowo otwartej karcie przeglądarki internetowej.
- o **Zezwalaj systemowi AVG na sugestie dotyczące błędów nawigacji przeglądarki (404/DNS)** — (domyślnie włączone) — jeśli podczas przeglądania sieci zostanie wybrana strona nieistniejąca lub niedostępna (błąd 404), **Pasek narzędzi AVG** automatycznie zaproponuje przegląd alternatywnych stron o podobnej tematyce.
- o **Ustaw i zachowaj Yahoo! jako domyślną wyszukiwarke** — (domyślnie wyłączona) — Yahoo! jest domyślną wyszukiwarką internetową **Paska narzędzi AVG Security Toolbar**, a aktywowanie tej opcji powoduje, że staje się również domyślną wyszukiwarką przeglądarki internetowej.

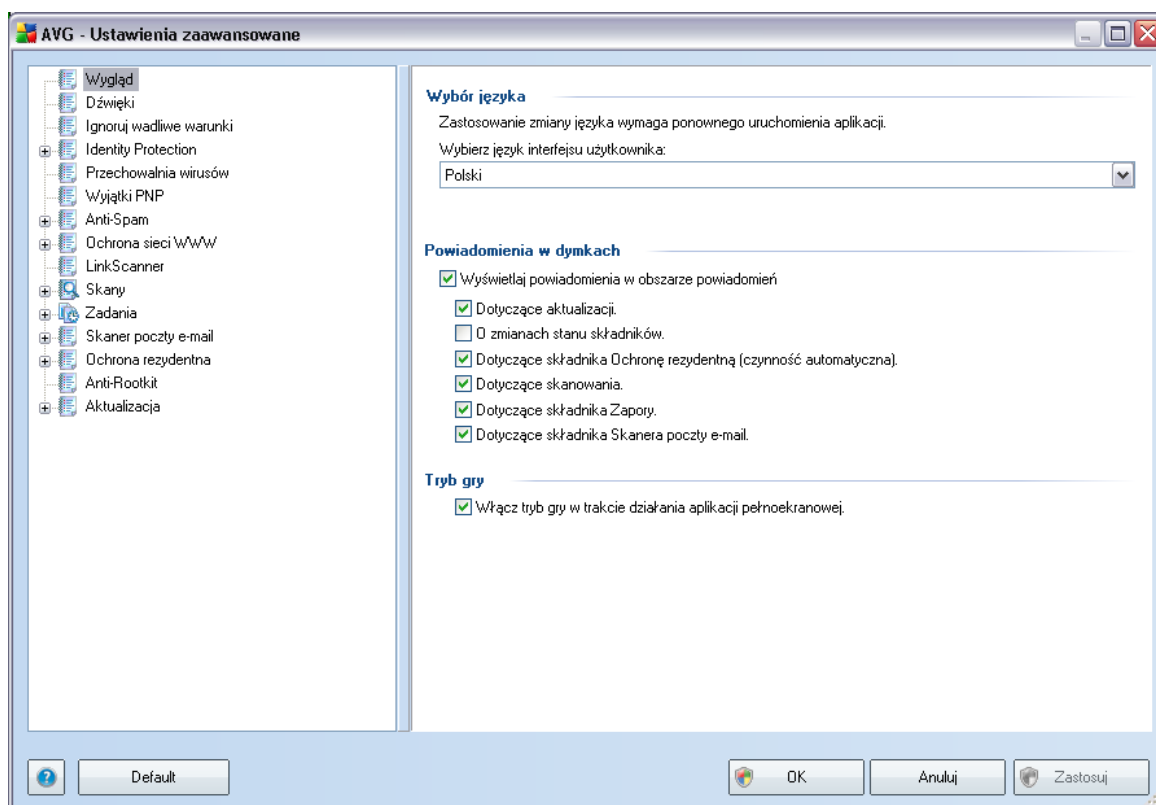
- o **Ponownie wyświetlaj Pasek narzędzi AVG Security Toolbar, jeśli został ukryty (po tygodniu)** — (domyślnie włączone) — ta opcja jest domyślnie aktywna i w przypadku przypadkowego ukrycia **Paska narzędzi AVG Security Toolbar** zostanie on ponownie wyświetlony po upływie tygodnia.

9. Zaawansowane ustawienia AVG

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

9.1. Wygląd

Pierwszy element w drzewie nawigacyjnym, **Wygląd**, odnosi się do ogólnych ustawień [Interfejsu użytkownika AVG](#) oraz kilku podstawowych opcji sterujących zachowaniem aplikacji:

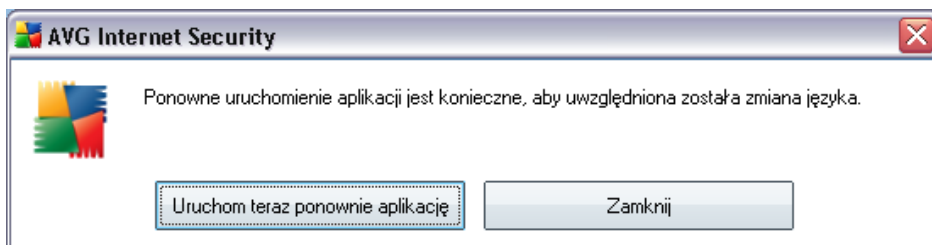


Wybór języka

W sekcji **Wybór języka** można wybrać zadany język z listy rozwijanej; język ten

bedzie uzywany w calym [interfejsie uzytkownika AVG](#). Menu rozwijane zawiera tylko jezyki wybrane podczas [instalacji](#) (zobacz rozdzial [Instalacja niestandardowa – Wybieranie skladnikow](#)). Przelaczenie aplikacji na inny jezyk wymaga ponownego uruchomienia interfejsu uzytkownika. W tym celu nalezy wykonac nastepujace kroki:

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



Powiadomienia w dymkach

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

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

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

okreslic, czy maja byc wyswietlane informacje dotyczace aktywnosci lub nieaktywnosci skladnikow badz mozliwych problemow ich dotyczacych. W przypadku zgloszania stanu bledu skladnika, opcja ta okresla funkcje informacyjna [ikony na pasku zadani](#) (zmiany koloru), która wskazuje na problemy z dowolnym skladnikiem systemu AVG;

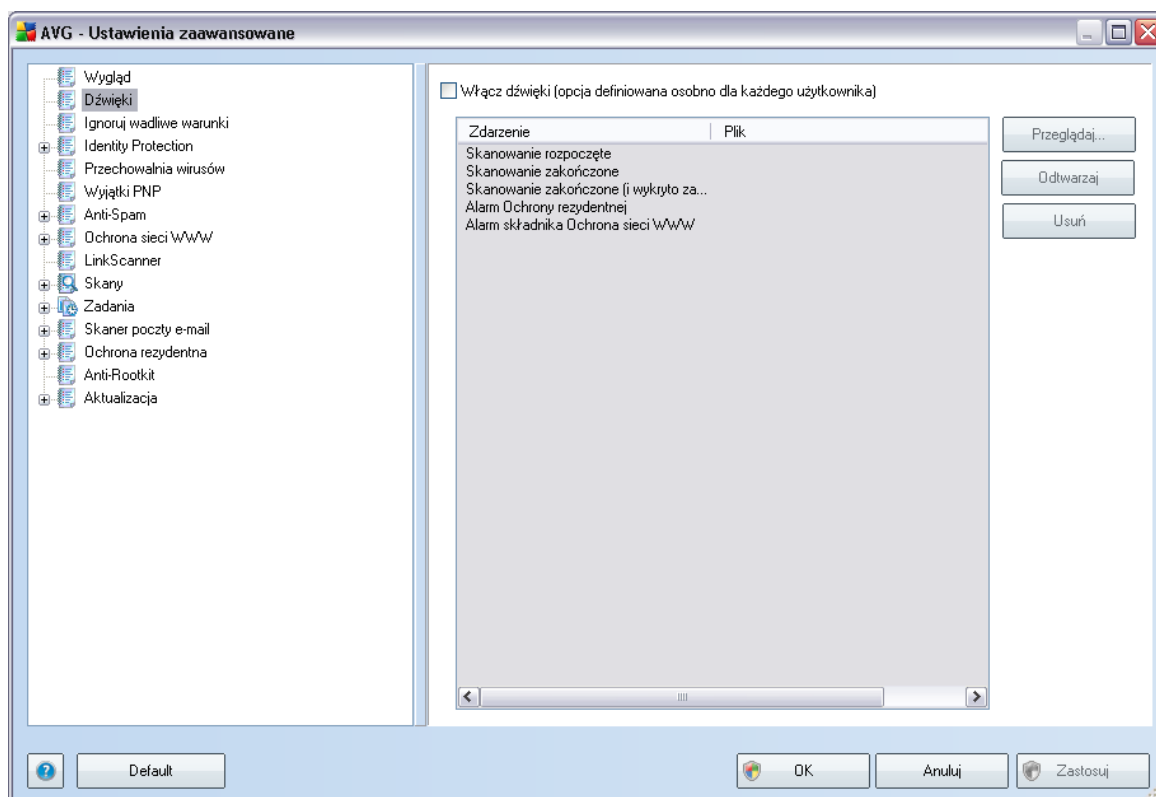
- o **Wyswietlaj w obszarze powiadomien komunikaty dotyczace skladnika [Ochrona rezydentna](#)** — należy okreslic, czy informacje dotyczace zapisywania, kopiowania i otwierania plikow maja byc wyswietlane, czy pomijane;
- o **Wyswietlaj w obszarze powiadomien komunikaty dotyczace [skanowania](#)** — należy okreslic, czy maja byc wyswietlane informacje dotyczace automatycznego rozpoczecia, postepu i zakonczenia zaplanowanego skanowania;
- o **Wyswietlaj komunikaty w obszarze powiadomien dotyczace [Zapory](#)** — należy okreslic, czy maja byc wyswietlane informacje dotyczace stanu i procesow Zapory, np. ostrzezenia o wlaczeniu/ wylaczeniu skladnika, mozliwym blokowaniu ruchu sieciowego itp.;
- o **Wyswietlaj komunikaty w obszarze powiadomien dotyczace skladnika [Skaner poczty e-mail](#)** — należy okreslic, czy maja byc wyswietlane informacje dotyczace skanowania wszystkich przychodzacych i wychodzacych wiadomosci e-mail.

Tryb gry

Ta funkcja systemu AVG przeznaczona jest dla programow dzialajacych w trybie pelnoekranowym, które do komunikacji uzywaja internetu. Ewentualne okna dialogowe systemu AVG moglyby zaklócac ich dzialanie (*np. powodowac ich minimalizacje lub zniekszaltcac obraz*). Aby tego uniknac, należy pozostawic pole wyboru **Wlacz tryb gry w trakcie dzialania aplikacji pelnoekranowej** zaznaczone (*ustawienie domyslne*).

9.2. Dzwieki

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

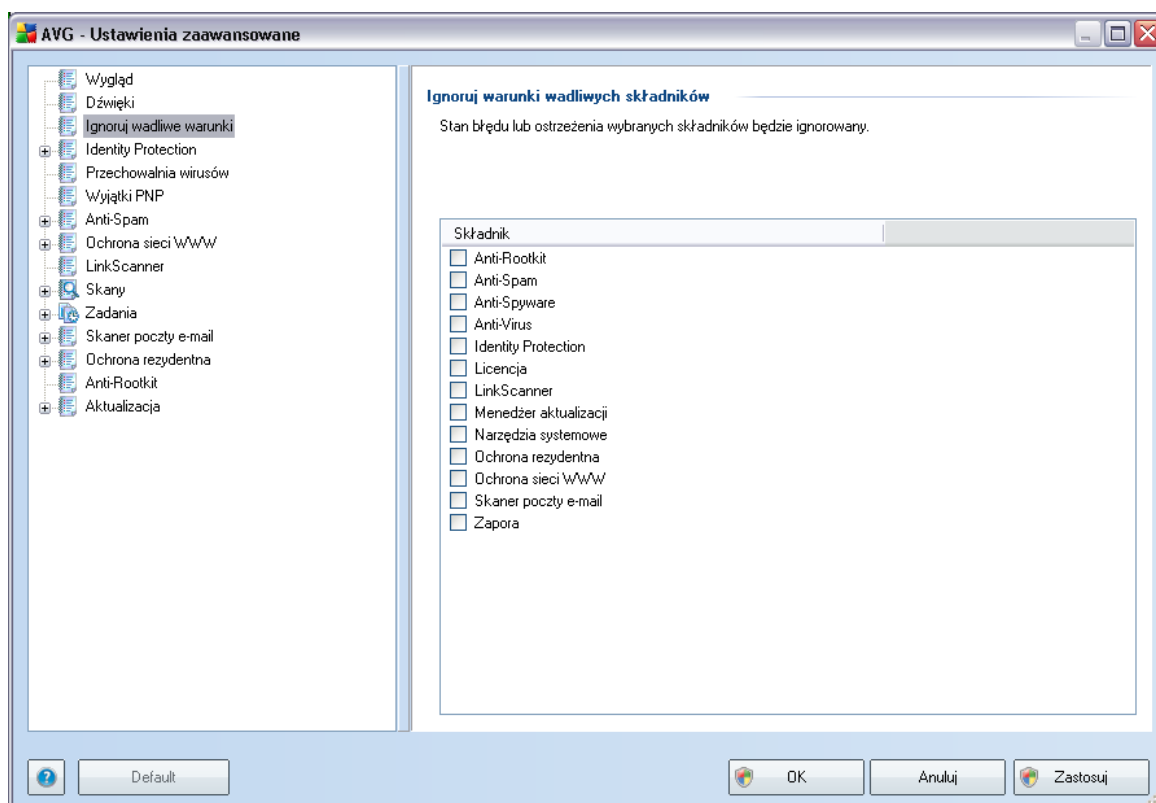


Następnie należy wybrać odpowiednie zdarzenie z listy i wskazać plik dźwiękowy, który ma zostać do niego przypisany (**Przeglądaj**). Aby odtworzyć wybrany dźwięk, należy zaznaczyć go na liście i nacisnąć przycisk **Odtwórz**. Aby usunąć dźwięk przypisany do określonego zdarzenia, należy użyć przycisku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

Uwaga: Obsługiwane są tylko pliki *.wav!

9.3. Ignoruj bledny stan skladników

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



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

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

Moze wystapic sytuacja, w której skladnik powinien zostac tymczasowo wylaczony (*nie jest to zalecane; wszystkie skladniki powinny byc zawsze wlaczone i dzialac w trybie domyslnym, ale niekiedy moze byc wymagane odstepstwo od tej reguly*). W

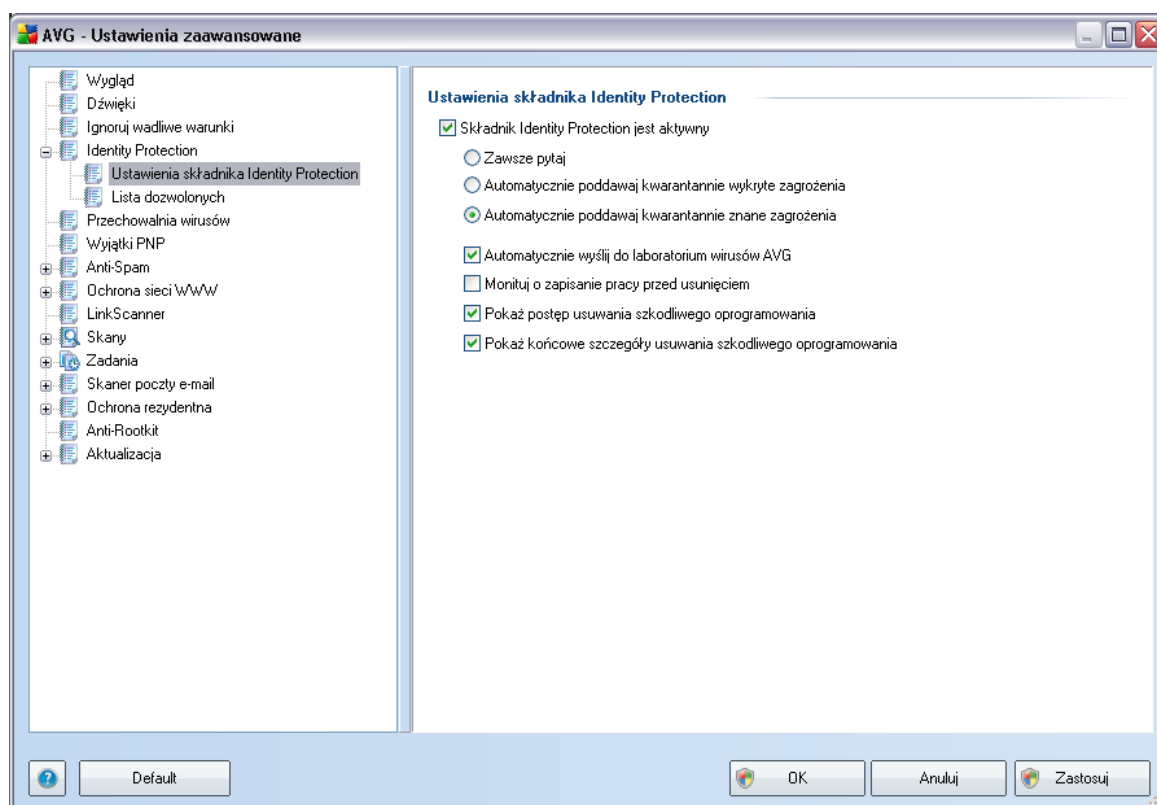
takim przypadku ikona na pasku zadań automatycznie informuje o stanie błędu składnika. W takiej sytuacji nie ma jednak faktycznego błędu, ponieważ wyłączenie składnika było celowe, a ryzyko z tym związane jest znane. Ponadto, gdy ikona jest szara, nie może już informować o ewentualnych realnych błędach.

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 dla określonych składników bezpośrednio w sekcji [przeglądu składników okna głównego AVG](#).

9.4. AVG Identity Protection

9.4.1. Ustawienia składnika Identity Protection

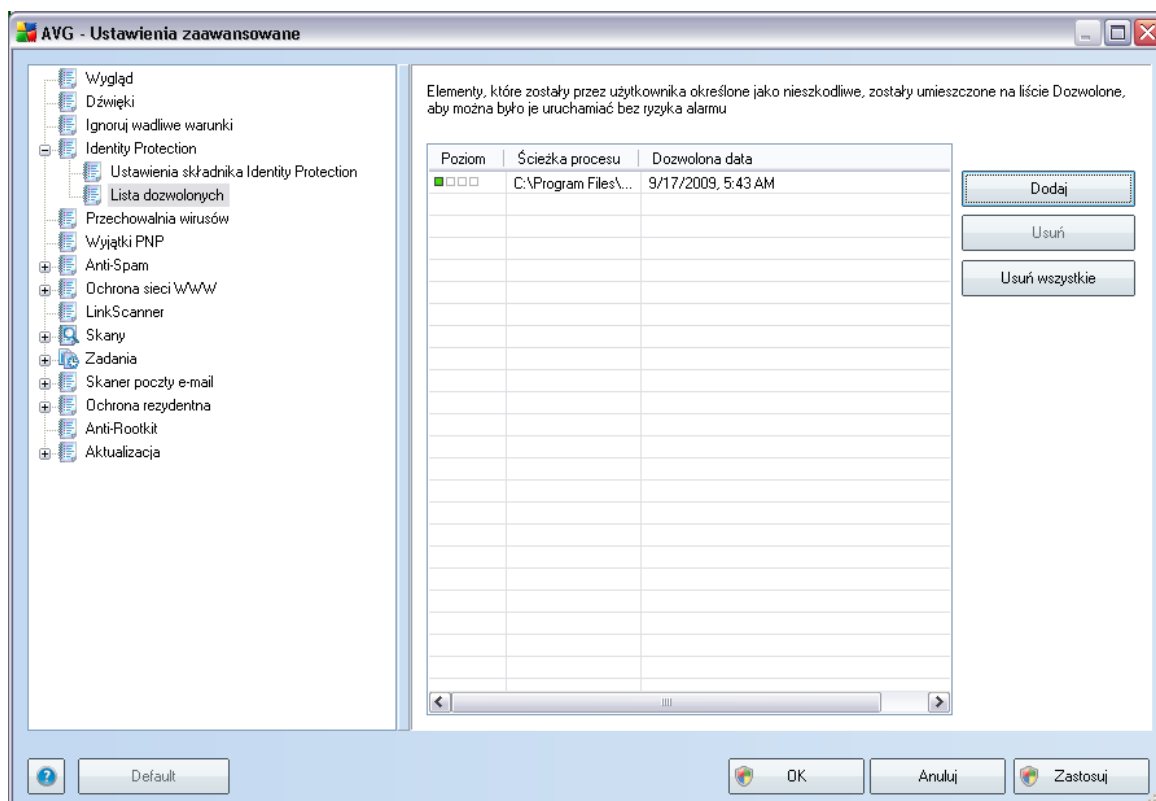
Okno dialogowe [Ustawienia Identity Protection](#) umożliwia włączenie/wyłączenie podstawowych funkcji składnika [Identity Protection](#):



- **Automatycznie poddawaj kwarantannie wykryte zagrożenia** — (domyślnie wyłączone) — należy zaznaczyć to pole wyboru, aby określić, że wszystkie wykryte zagrożenia będą natychmiast przenoszone w bezpieczne miejsce (do [Przechowalnię 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 przesyłaj do laboratoriów firmy AVG** — (domyślnie włączone) — zaleca się zachowanie tego ustawienia, aby uzupełnić bazy danych o złośliwej aktywności w sieci. Pomoże nam to identyfikować nowe zagrożenia.

9.4.2. Lista dozwolonych

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



Lista programów dozwolonych zawiera następujące informacje o każdej aplikacji:

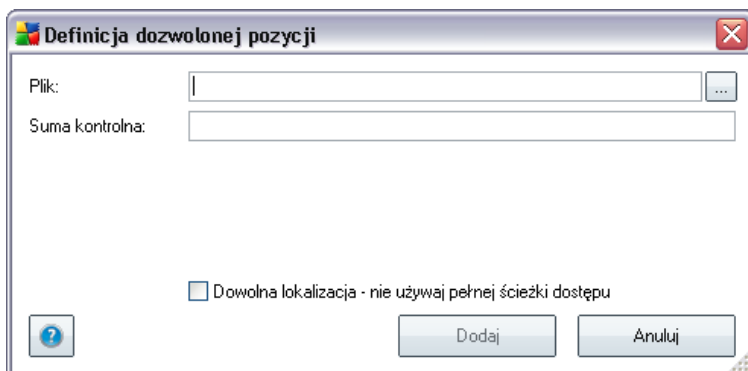
- **Poziom** — graficzna reprezentacja ryzyka stwarzanego przez określone procesy, przedstawiana na czterostopniowej skali od najmniej istotnego (■□□□) do krytycznego (■■■■)
- **Ścieżka procesu** — ścieżka dostępu do lokalizacji pliku wykonywalnego aplikacji (*procesu*)
- **Data dozwolenia** — data ręcznego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

Przyciski kontrolne

W oknie dialogowym **Lista dozwolonych** dostępne są następujące przyciski kontrolne:

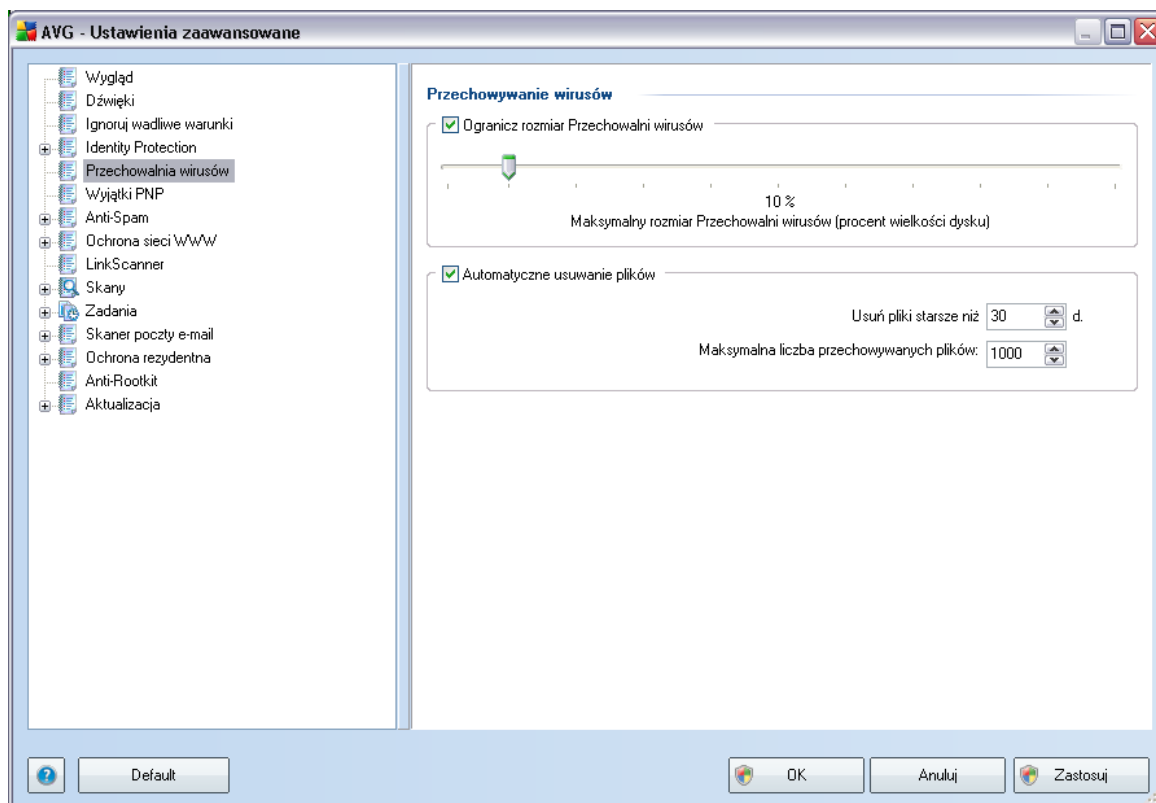
- **Dodaj** — naciśnij ten przycisk, aby dodać nową aplikację do listy programów

dozwolonych. Zostanie wyświetlone poniższe okno dialogowe:



- o **Plik** — należy podać pełną ścieżkę dostępu do pliku (*aplikacji*), który ma zostać oznaczony jako wyjątek
 - o **Suma kontrolna** — wyświetla unikatową „sygnaturę” wybranego pliku. Suma ta jest generowanym automatycznie ciągiem znaków, który pozwala programowi AVG jednoznacznie odróżnić wybrany plik od innych. Jest ona generowana i wyświetlana po pomyslnym dodaniu pliku.
 - o **Dowolna lokalizacja** — nie używaj pełnej ścieżki dostępu — jeśli plik ma zostać zdefiniowany jako wyjątek jedynie dla konkretnej lokalizacji, wówczas należy pozostawić to pole niezaznaczone.
- **Usun** — wciśnij ten przycisk, aby usunąć z listy zaznaczone aplikacje.
 - **Usun wszystkie** — wciśnij ten przycisk, aby usunąć wszystkie aplikacje z listy.

9.5. Przechowalnia wirusów

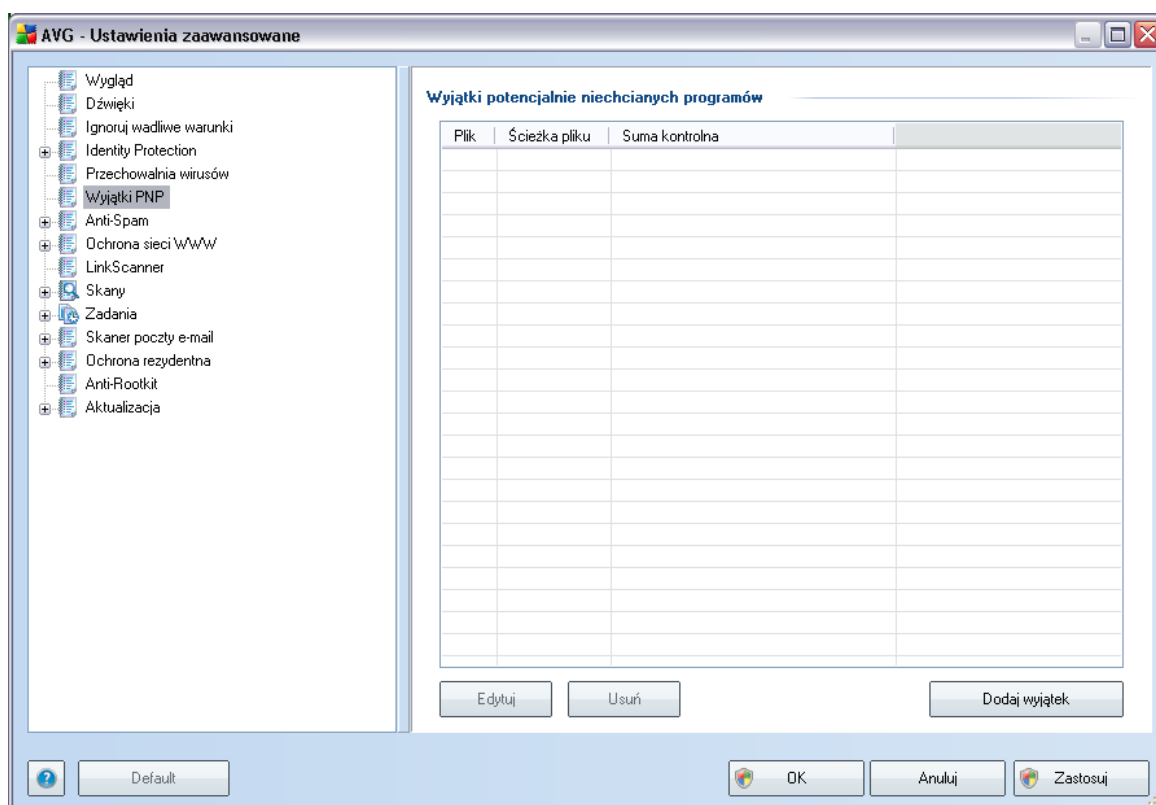


W oknie **Przechowalnia wirusów** można zdefiniować kilka parametrów dotyczących administrowania obiektami znajdującymi się w **Przechowalni**:

- **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**).

9.6. Wyjątki PNP

AVG 9 Internet Security potrafi analizować i wykrywać pliki wykonywalne oraz biblioteki DLL, których obecność w systemie operacyjnym może być niepożądana. W niektórych przypadkach użytkownik może chcieć zachować na komputerze określone potencjalnie niechciane programy (*jeśli zostały zainstalowane celowo*). Niektóre aplikacje, zwłaszcza bezpłatne, zawierają oprogramowanie reklamowe. Może ono zostać wykryte i zgłoszone przez system AVG jako **potencjalnie niechciany program**. Jeśli chcesz zachować taki program na komputerze, możesz zdefiniować go jako wyjątek potencjalnie niechcianych programów:



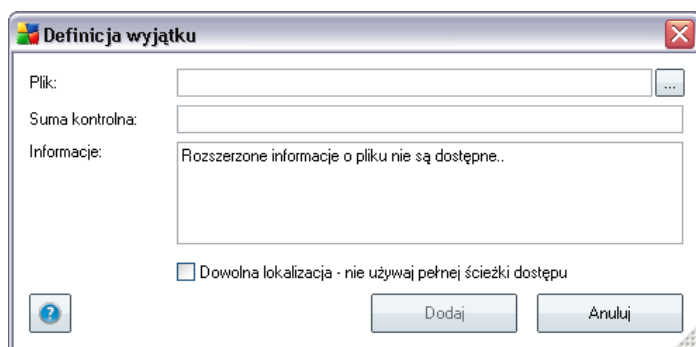
Okno **Wyjątki potencjalnie niechcianych programów** zawiera listę już zdefiniowanych i aktualnie obowiązujących wyjątków potencjalnie niechcianych programów. Listę tę można edytować, usuwać istniejące pozycje lub dodawać nowe wyjątki. Dla każdego wyjątku na liście dostępne są następujące informacje:

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

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

Przyciski kontrolne

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

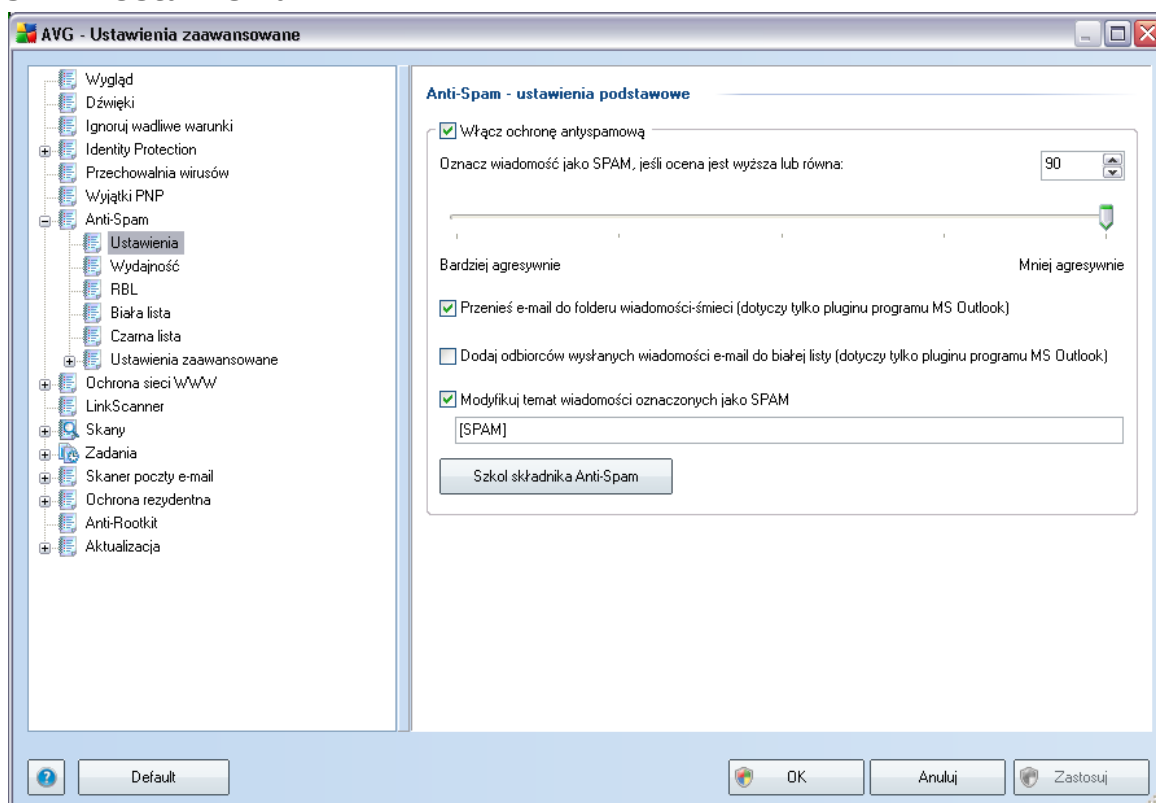


- o **Plik** — należy podac pelna sciezke do pliku, który ma byc oznaczony jako wyjątek.
- o **Suma kontrolna** — wyswietla unikatowa „signature” wybranego pliku. Suma ta jest generowanym automatycznie ciagiem znaków, który pozwala programowi AVG jednoznacznie odróżniac wybrany plik od innych. Jest ona generowana i wyswietlana po pomyslnym dodaniu pliku.
- o **Informacje o pliku** — wyswietla wszelkie dodatkowe dostepne informacje na temat pliku (*licencja/wersja itp.*).
- o **Dowolna lokalizacja — nie używaj pełnej ścieżki dostępu** — jesli

plik ma być zdefiniowany jako wyjątek jedynie dla konkretnej lokalizacji, wówczas należy pozostawić to pole niezaznaczone.

9.7. Anti-Spam

9.7.1. Ustawienia



W oknie **Podstawowe ustawienia składowa Anti-Spam** można zaznaczyć pole **Włącz ochronę antyspamową**, aby włączyć/wyłączyć skanowanie wiadomości e-mail. Ta opcja jest domyślnie włączona i jak zwykle nie zaleca się zmiany jej konfiguracji bez ważnego powodu.

W tym samym oknie można także wybrać mniej lub bardziej agresywne metody oceny. Filtr **Anti-Spam** przypisuje każdej wiadomości ocenę (*tj. wskaźnik informujący, jak bardzo jej treść przypomina SPAM*) na podstawie kilku dynamicznych technik skanowania. Wartość opcji **Oznacz wiadomość jako spam, jeśli ocena jest**

wyższa niż można dostosować, wpisując odpowiednią liczbę (od 0 do 100) bądź przesuwając suwak w lewo lub w prawo (tylko od 50 do 90).

Zwykle zaleca się stosowanie progu z przedziału od 50 do 90, a jeśli nie ma pewności co do właściwego ustawienia — równego 90. Poniżej przedstawiono opis progów oceny:

- **Wartosc 90–99** — większość przychodzących wiadomości e-mail jest normalnie dostarczana (bez oznaczania jako [spam](#)). [Spam](#), który łatwo zidentyfikować, jest [odfiltrowywany](#), ale znaczna jego część może nadal trafiać do Twojej skrzynki odbiorczej.
- **Wartosc 80–89** — wiadomości e-mail, które stanowią potencjalny [spam](#), są poprawnie odfiltrowywane. Niektóre z poządanych wiadomości (niebędących spamem) mogą zostać błędnie zablokowane.
- **Wartosc 60–79** — umiarkowanie agresywna konfiguracja. Wiadomości e-mail, które mogą stanowić [spam](#), są poprawnie odfiltrowywane. Poządane wiadomości (niebędące spamem) mogą zostać błędnie zablokowane.
- **Wartosc 1–59** — bardzo agresywna konfiguracja. Poządane wiadomości e-mail są odfiltrowywane w równym stopniu, jak wiadomości stanowiące [spam](#). Nie zalecamy stosowania tego progu podczas normalnej pracy.
- **Wartosc 0** — w tym trybie dostarczane są tylko wiadomości od nadawców z [białej listy](#). Wszystkie pozostałe wiadomości e-mail są uznawane za [spam](#). **Nie zalecamy stosowania tego progu podczas normalnej pracy.**

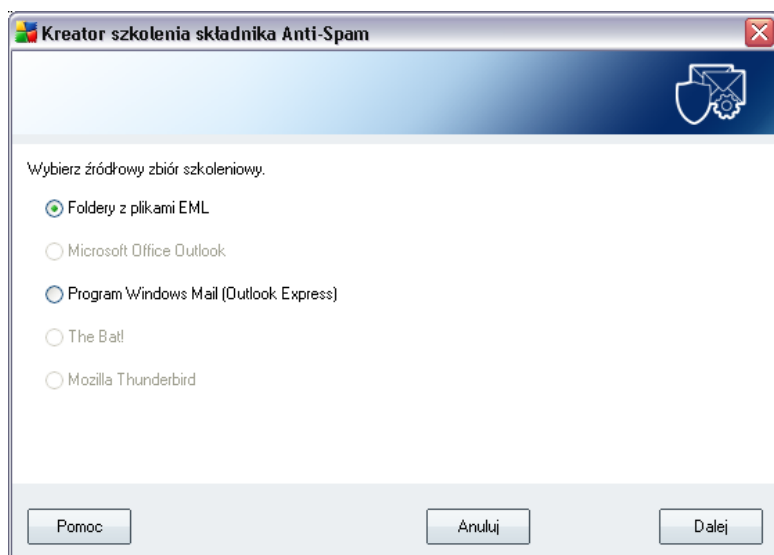
W oknie **Podstawowe ustawienia składowika Anti-Spam** można dokładniej zdefiniować sposób traktowania [spamu](#) wykrytego w wiadomościach e-mail:

- **Przenies wiadomość do folderu wiadomości-smieci** — jeśli opcja jest zaznaczona, wykryty spam będzie automatycznie przenoszony do wskazanego folderu wiadomości-smieci w kliencie poczty.
- **Dodaj odbiorców wysłanych wiadomości e-mail do [białej listy](#)** — zaznacz to pole, aby potwierdzić, że masz zaufanie do odbiorców wysłanych przez Ciebie wiadomości e-mail, a więc poczta przychodząca z ich kont ma zawsze być dostarczana.
- **Zmodyfikuj temat wiadomości oznaczonych jako spam** — jeśli opcja ta jest zaznaczona, wszystkie wykryte wiadomości zawierające [spam](#) będą oznaczane (w temacie) wskazaną frazą lub znakiem; zadany tekst można wpisać w polu znajdującym się poniżej.

Przyciski kontrolne

Przycisk "Rozpocznij szkolenie składnika Anti-Spam" pozwala uruchomić **Kreator szkolenia składnika Anti-Spam** opisany szczegółowo w [następnym rozdziale](#).

Pierwsze okno dialogowe **Kreatora Szkolenia składnika Anti-spam** wyświetla monit o wybranie źródła wiadomości e-mail, które mają być użyte w tym. Na ogół używa się do tego celu niechcianych wiadomości reklamowych, oraz e-maili błędnie oznaczonych jako spam.



Oto dostępne opcje:

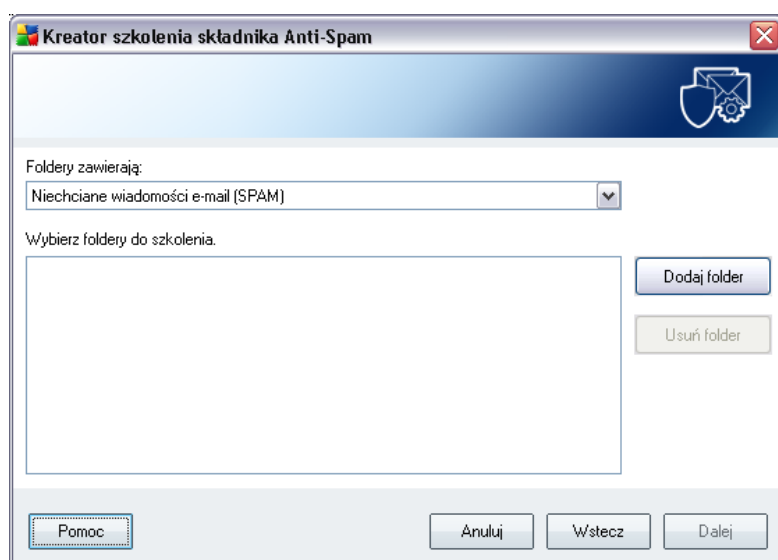
- **Konkretny klient poczty e-mail**— jeśli używasz jednego z wymienionych klientów poczty e-mail (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), po prostu wskaz go na wyświetlonej liście.
- **Folder z plikami EML** — jeśli jest używany jakikolwiek inny program pocztowy, należy zgromadzić wszystkie wiadomości w jednym folderze (w formacie .eml) lub upewnić się, że znasz lokalizację folderu, w którym program pocztowy domyślnie przechowuje wiadomości. Następnie należy zaznaczyć opcję **Folder z plikami EML**, oraz wskazać odpowiedni folder w następnym kroku.

Aby proces szkolenia był prostszy i przebiegał szybciej, warto już wcześniej tak posortować e-maile, aby folder używany w szkoleniu zawierał jedynie wiadomości szkoleniowe (albo spam, albo ham). Nie jest to jednak konieczne, gdyż wiadomości można przefiltrować ręcznie w późniejszym czasie.

Aby kontynuować, zaznacz odpowiednią opcję i kliknij przycisk **Dalej**.

Okno wyświetlane w tym kroku zależy od poprzedniego wyboru.

Foldery z plikami EML



W oknie tym należy wybrać folder z wiadomościami, które mają zostać użyte do szkolenia. Kliknij przycisk **Dodaj folder**, aby zlokalizować folder z plikami .eml (zapisanymi wiadomościami e-mail). Wybrany folder zostanie wyświetlony w bieżącym oknie.

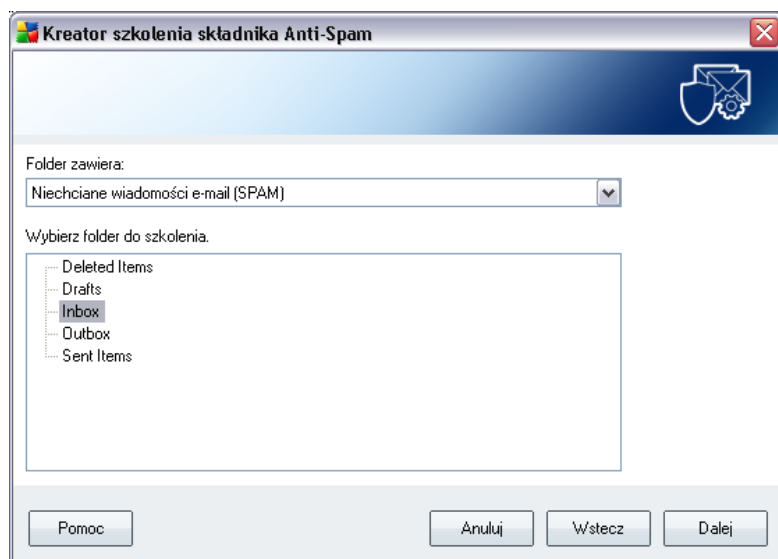
Z menu rozwijanego **Foldery zawierają** wybierz jedną z dwóch opcji — czy folder zawiera pożądane wiadomości (*HAM*), czy niechciane reklamy (*SPAM*). Należy pamiętać, że w następnym kroku będzie możliwa szczegółowa selekcja plików, więc folder nie musi zawierać tylko szkoleniowych wiadomości e-mail. Można też usunąć z listy niechciane foldery, klikając przycisk **Usuń folder**.

Po zakończeniu ustawień należy kliknąć przycisk **Dalej** i przejść do [Opcji filtrowania](#)

[wiadomości](#).

Określony klient poczty e-mail

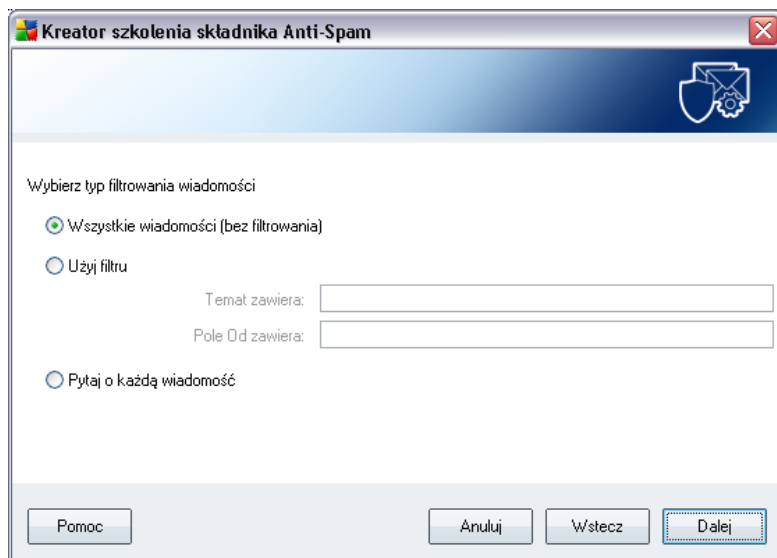
Po potwierdzeniu jednej z opcji pojawi się nowe okno dialogowe.



Uwaga: W wypadku programu Microsoft Office Outlook pojawi się najpierw monit proszący o wybranie profilu programu MS Office Outlook.

Z menu rozwijanego **Foldery zawierają** wybierz jedną z dwóch opcji — czy folder zawiera pożądaną wiadomość (**HAM**), czy niechciane reklamy (**SPAM**). Należy pamiętać, że w następnym kroku będzie możliwa szczegółowa selekcja plików, więc folder nie musi zawierać tylko szkoleniowych wiadomości e-mail. W głównej części okna pojawi się drzewo nawigacyjne wybranego klienta poczty e-mail. Zlokalizuj zadany folder i podświetl go za pomocą myszy.

Po skończeniu należy kliknąć przycisk **Dalej** i przejść do [Opcji filtrowania wiadomości](#).



W tym oknie można ustawić filtrowanie wiadomości e-mail.

Jeśli wybrany folder zawiera jedynie wiadomości, które mają być użyte w szkoleniu, należy zaznaczyć opcję **Wszystkie wiadomości (bez filtrowania)**.

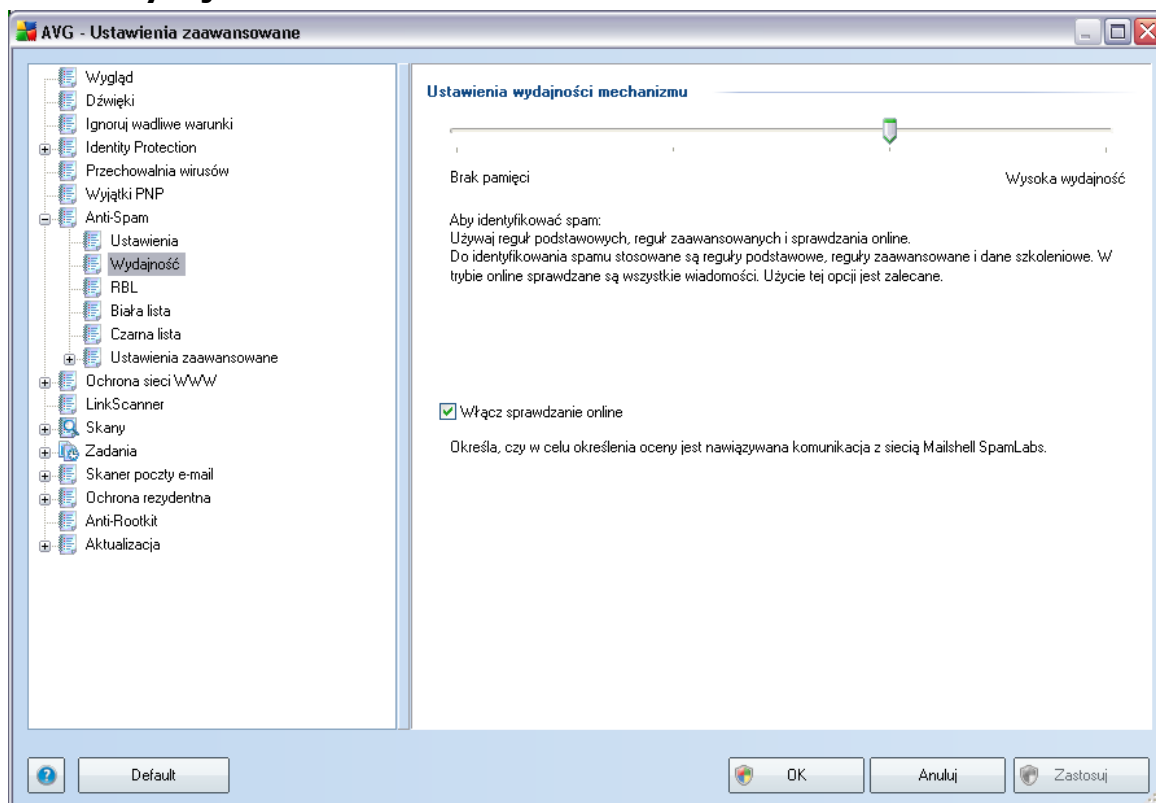
Jeśli nie ma pewności co do charakteru wiadomości znajdujących się w folderze i kreator powinien pytać o każdą z nich (dając możliwość określenia, czy ma zostać użyta w szkoleniu), należy wybrać opcję **Pytaj o każdą wiadomość**.

Aby zastosować bardziej zaawansowane filtrowanie, należy wybrać opcję **Użyj filtru**. Można będzie wówczas podać wyraz (*nazwę*), część wyrazu lub frazę, która ma być wyszukiwana w tematach i/lub adresach nadawców wiadomości. Wszystkie wiadomości dokładnie spełniające kryteria wyszukiwania zostaną użyte do szkolenia, bez dalszych monitów.

Uwaga!: W przypadku wypełnienia obu pól tekstowych zostaną użyte także adresy spełniające tylko jeden z dwóch warunków!

Gdy już zdecydujesz się na jedną z opcji, kliknij przycisk **Dalej**. Kolejne okno dialogowe ma charakter informacyjny i sygnalizuje, że kreator jest gotowy do przetwarzania wiadomości. Aby rozpocząć szkolenie, należy ponownie kliknąć przycisk **Dalej**. Szkolenie rozpocznie się zgodnie z wybranymi wcześniej parametrami.

9.7.2. Wydajność



Okno **Ustawienia wydajności mechanizmu** (otwierane po kliknięciu pozycji **Wydajność** w lewym panelu nawigacyjnym) daje dostęp do ustawień wydajności składowika **Anti-Spam**. Przesuwając suwak, można dostosować wydajność skanowania, przełączając się między trybami **Brak pamięci** i **Wysoka wydajność**.

- **Brak pamięci** — w czasie skanowania w poszukiwaniu [spamu](#) nie będą stosowane żadne reguły. Do identyfikacji będą używane tylko dane szkoleniowe. Ten tryb nie jest zalecany do częstego stosowania - chyba że konfiguracja sprzętowa komputera jest bardzo słaba.
- **Wysoka wydajność** — wymaga dużej ilości pamięci. W czasie skanowania w poszukiwaniu [spamu](#) stosowane będą następujące funkcje: pamięć podręczna dla reguł i definicji [spamu](#), reguły podstawowe i zaawansowane, adresy IP spamatorów i inne bazy danych.

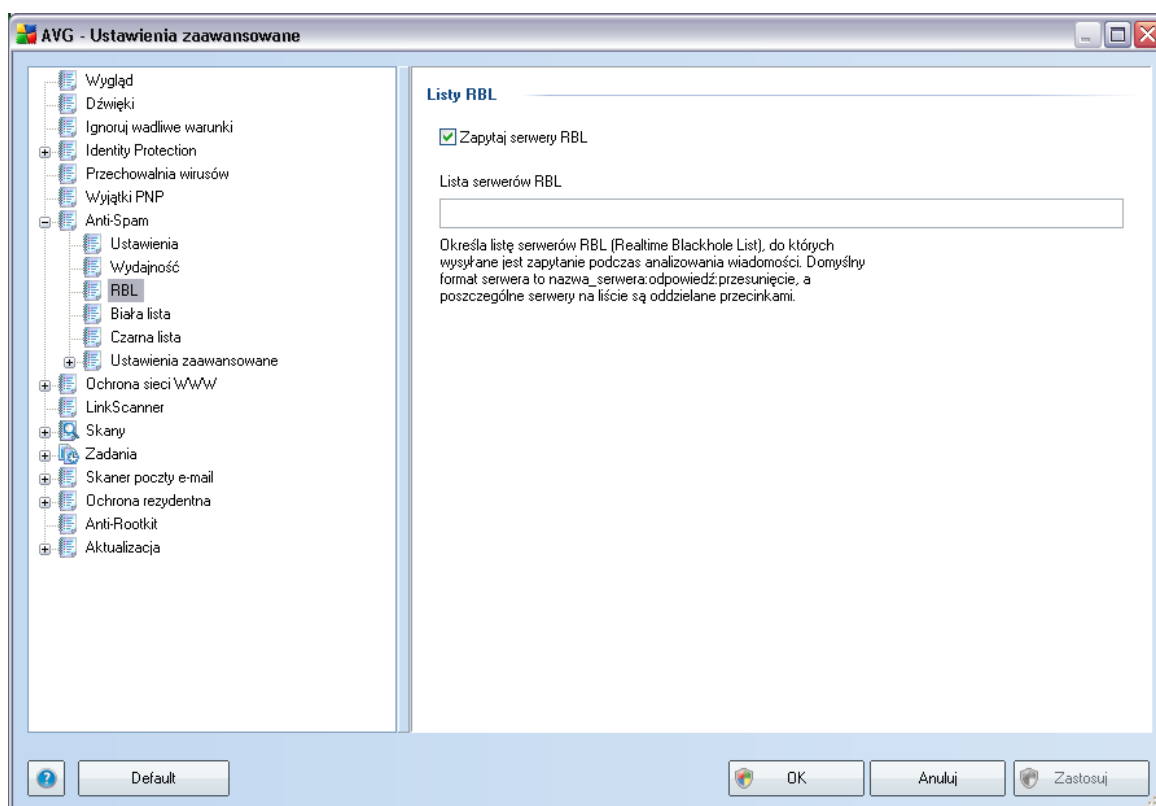
Opcja **Włącz sprawdzanie online** jest domyślnie włączona. Pozwala ona skuteczniej wykrywać [spam](#) dzięki komunikacji z serwerami [Mailshell](#): skanowane dane są

porównywane z bazami danych online firmy [Mailshell](#).

Zwykle zaleca się zachowanie ustawień domyślnych i zmienianie ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny być wprowadzane wyłącznie przez zaawansowanych użytkowników, którzy doskonale wiedzą, co robią!

9.7.3. RBL

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



W oknie tym można włączyć/wyłączyć funkcję **Zapytaj serwery RBL**.

Serwer RBL (*Realtime Blackhole List*) to specjalny serwer DNS z obszerną bazą danych znanych nadawców spamu. Jeżeli funkcja ta jest włączona, wszystkie wiadomości e-mail zostaną sprawdzone przy użyciu bazy serwera RBL i oznaczone jako [spam](#), w przypadku gdy okaże się identyczne z którymkolwiek wzorem w bazie danych. Bazy danych serwerów RBL zawierają zawsze aktualne sygnatury spamu, co zapewnia najskuteczniejsze i najdokładniejsze wykrywanie [niechcianych wiadomości](#).

Funkcja ta jest szczególnie przydatna dla użytkowników otrzymujących duże ilości spamu, który zazwyczaj nie jest wykrywany przez silnik [AVG Anti-Spam](#).

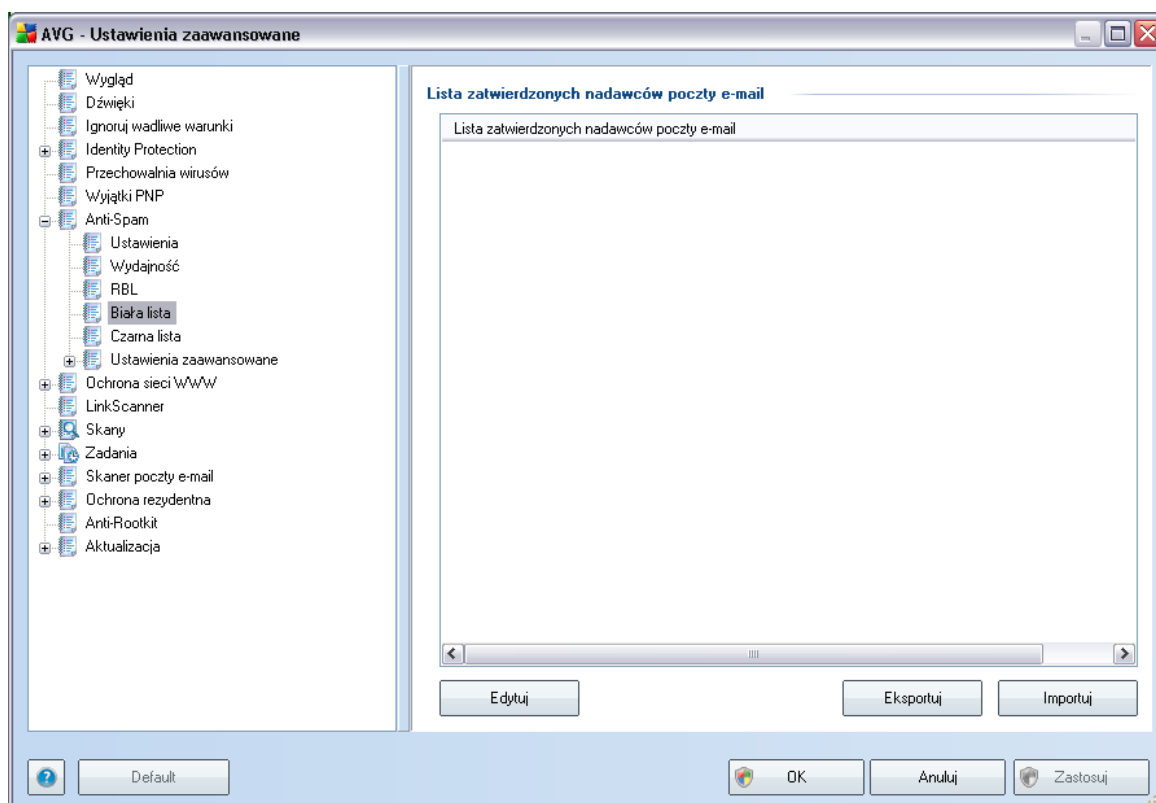
Lista serwerów RBL pozwala określić lokalizacje wybranych serwerów RBL.

Uwaga: Włączenie tej funkcji może w niektórych systemach i konfiguracjach spowolnić proces odbierania poczty e-mail, ponieważ każda wiadomość musi być zweryfikowana przy użyciu bazy danych serwera RBL.

Do serwera nie są wysyłane żadne dane osobiste!

9.7.4. Biała lista

Kliknięcie elementu **Biała lista** pozwala otworzyć okno dialogowe **Lista zatwierdzonych nadawców poczty e-mail** zawierające listę akceptowanych adresów nadawców i nazw domen, z których wysyłane wiadomości nigdy nie są oznaczane jako [spam](#).



W interfejsie tym można utworzyć listę nadawców, którzy nigdy nie wysyłają

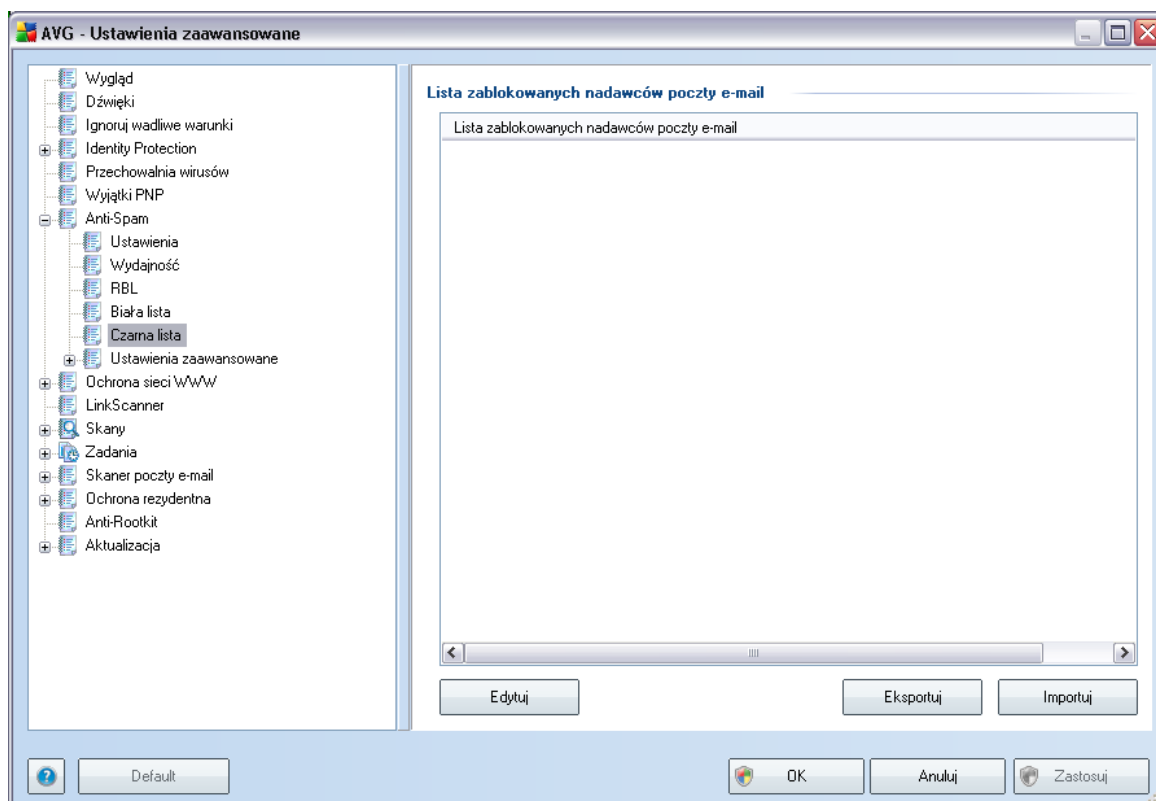
niepozadanych wiadomości ([spamu](#)). Można także utworzyć listę nazw całych domen (np. *avg.com*), które nie wysyłają spamu.

Po przygotowaniu listy adresów i domen, jej elementy można wprowadzić pojedynczo lub zaimportować wszystkie na raz. Dostępne są następujące przyciski kontrolne:

- **Edytuj** — przycisk ten służy do otwarcia okna dialogowego, w którym można ręcznie wprowadzić listę adresów (*również za pomocą metody kopiuj-wklej*). Każdą pozycję (*nadawce lub nazwę domeny*) należy wprowadzić w osobnym wierszu.
- **Eksportuj** — jeżeli z jakiegoś powodu chcesz wyeksportować wpisy, można użyć przycisku Eksportuj. Wszystkie wpisy zostaną zapisane w zwykłym pliku tekstowym.
- **Importuj** — jeżeli posiadasz plik tekstowy z adresami e-mail lub nazwami domen, można go zaimportować za pomocą tego przycisku. Wprowadzany plik musi być w zwykłym formacie tekstowym i zawierać każdy element (*adres lub nazwę domeny*) w osobnym wierszu.

9.7.5. Czarna lista

Kliknięcie pozycji **Czarna lista** pozwala otworzyć globalną listę zablokowanych adresów indywidualnych nadawców i domen, z których wiadomości zawsze są oznaczane jako [spam](#).



W interfejsie tym można utworzyć listę nadawców, którzy wysyłają lub prawdopodobnie będą wysyłali niepożądane wiadomości ([spam](#)). Można także utworzyć listę pełnych nazw domen (np. *spammingcompany.com*), z których otrzymujesz (lub spodziewasz się otrzymywać) spam. Wszystkie wiadomości e-mail wysłane z tych adresów/domen będą identyfikowane jako spam.

Jeśli sporządziłeś już listę adresów i domen, możesz wprowadzić jej elementy pojedynczo lub importować wszystkie na raz. Dostępne są następujące przyciski kontrolne:

- **Edytuj** — przycisk ten otwiera okno dialogowe, w którym można ręcznie wprowadzić listę adresów (również za pomocą metody *kopiuj-wklej*). Każdy element (*nadawce lub nazwe domeny*) należy wprowadzić w osobnym wierszu.
- **Eksportuj** — jeżeli z jakiegos powodu chcesz wyeksportować wpisy, można użyć przycisku Eksportuj. Wszystkie wpisy zostaną zapisane w zwykłym pliku tekstowym.

- **Importuj** — jeżeli posiadasz plik tekstowy z adresami e-mail lub nazwami domen, można go zaimportować za pomocą tego przycisku. Wprowadzany plik musi być w zwykłym formacie tekstowym i zawierać każdy element (*adres lub nazwę domeny*) w osobnym wierszu.

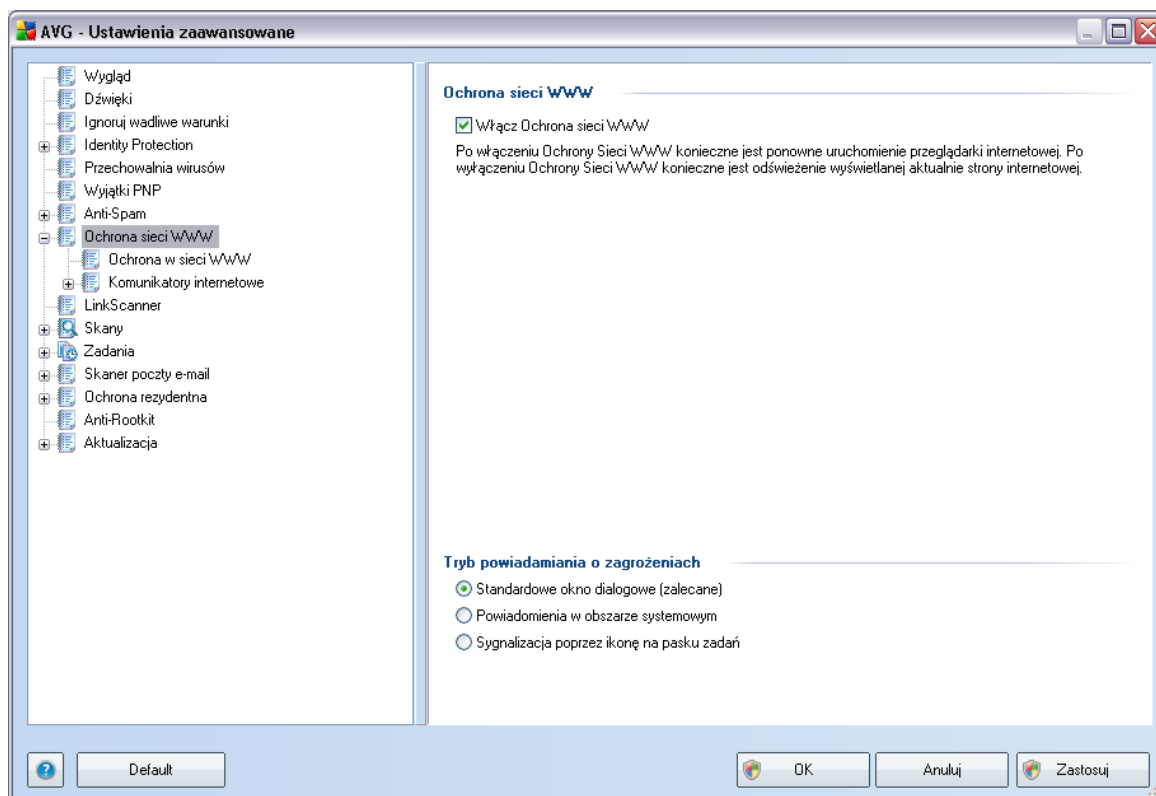
9.7.6. Ustawienia zaawansowane

Zwykle zaleca się zachowanie ustawień domyślnych i zmienianie ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny być wprowadzane wyłącznie przez zaawansowanych użytkowników, którzy doskonale wiedzą, co robią!

Aby mimo wszystko zmienić konfigurację składnika [Anti-Spam](#) na bardzo zaawansowanym poziomie, należy postępować zgodnie z instrukcjami wyświetlanymi w interfejsie użytkownika. Okna dialogowe najczęściej odpowiadają tylko jednej funkcji, której opis jest zawsze dostępny w tym samym oknie:

- **Pamięć podreczna** — sygnatury, reputacja domen, LegitRepute.
- **Szkolenie** — szkolenie dotyczące słów, historia ocen, offset oceny, maksymalna liczba wpisów, próg automatycznego szkolenia, waga, bufor zapisu.
- **Filtry** — lista języków, lista krajów, akceptowane adresy IP, zablokowane adresy IP, zablokowane kraje, zablokowane zestawy znaków, fałszywi nadawcy.
- **RBL** — serwery RBL, trafienia wielokrotne, próg, limit czasu, maksymalna liczba adresów IP.
- **Połączenie internetowe** — limit czasu.

9.8. Ochrona sieci WWW



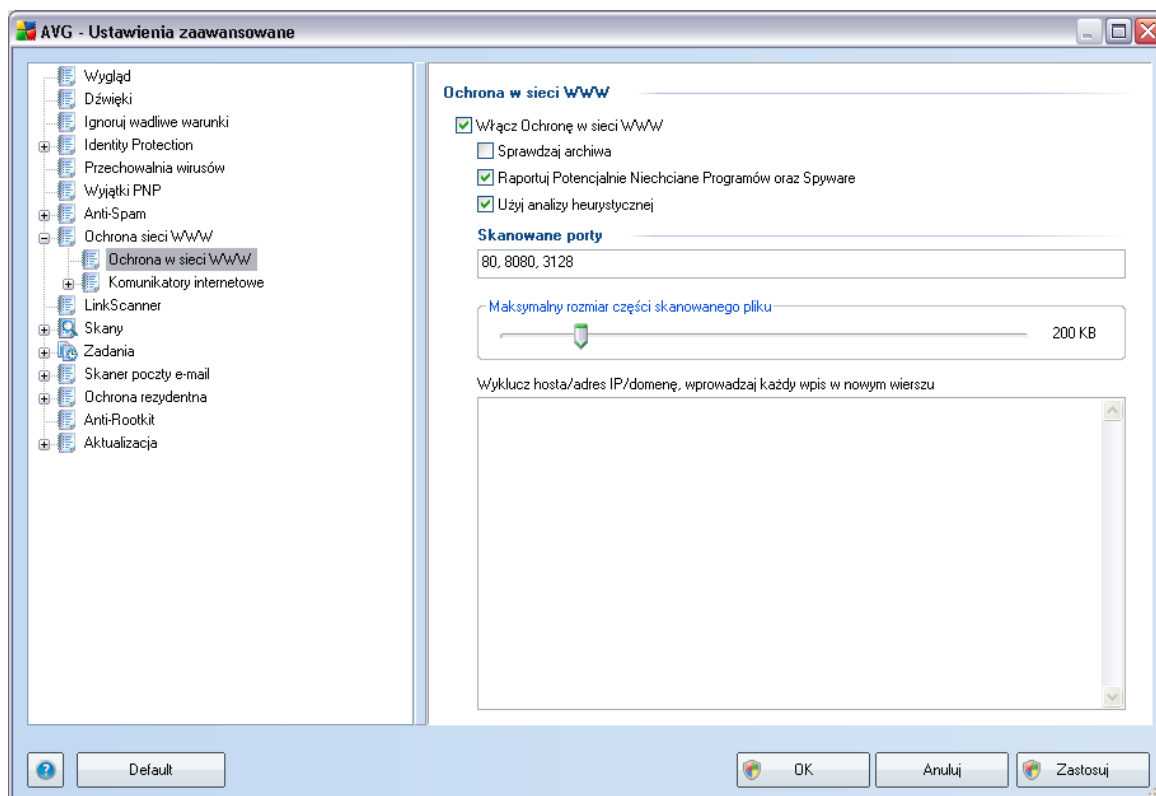
W oknie dialogowym **Ochrona w sieci WWW** można włączyć lub wyłączyć cały składnik **Ochrona sieci WWW** za pomocą opcji **Włącz ochronę sieci WWW** (domyślnie włączona). Szczegółowe ustawienia tego składnika dostępne są w kolejnych oknach dialogowych dostępnych z poziomu drzewa nawigacyjnego:

- [**Ochrona WWW**](#)
- [**Komunikatory internetowe**](#)

Tryb powiadamiania o zagrożeniach

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

9.8.1. Ochrona WWW

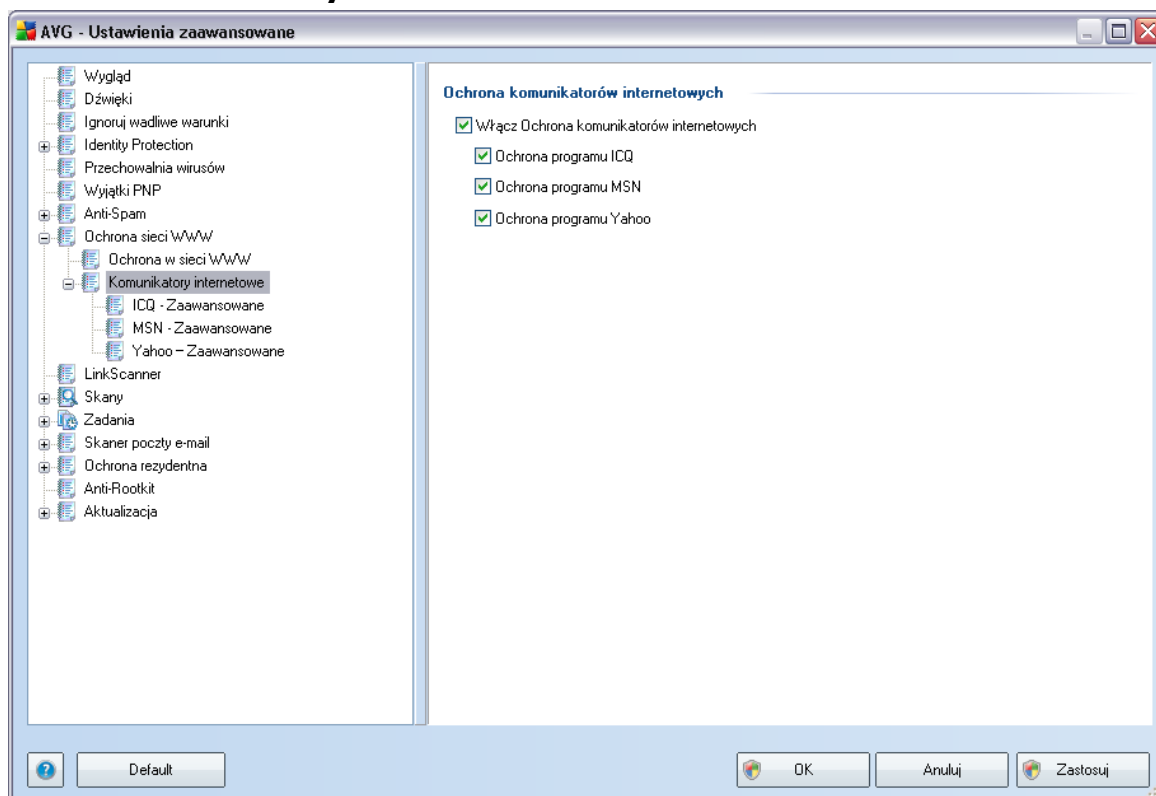


W oknie dialogowym **Ochrona w sieci WWW** można edytować konfigurację dotyczącą skanowania zawartości witryn internetowych. Interfejs edycji pozwala konfigurować następujące opcje:

- **Włącz Ochronę w sieci WWW** — potwierdza, że składnik **Ochrona sieci WWW** ma skanować zawartość stron WWW. Jeśli ta opcja jest włączona (domyślnie), można włączyć lub wyłączyć następujące elementy:
 - o **Skanuj wewnątrz archiwów** — skanowanie ma obejmować także archiwa zawarte na wyświetlanych stronach WWW.
 - o **Zgłaszaj potencjalnie niechciane programy i oprogramowanie szpiegujące** — skanowanie ma obejmować potencjalnie niechciane programy (*pliki wykonywalne, które mogą być programami szpiegującymi lub reklamowymi*) zawarte na wyświetlanych stronach WWW oraz [oprogramowanie szpiegujące](#).

- o **Użyj heurystyki** — skanowanie zawartości wyświetlanych stron ma wykorzystywać [analizę heurystyczną](#) (*dynamiczna emulacja instrukcji skanowanego obiektu w wirtualnym środowisku*).
- o **Skanowane porty** — to pole zawiera listę standardowych numerów portów http. Jeśli konfiguracja komputera różni się od standardowej, można zmienić numery portów zgodnie z potrzebami.
- o **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 WWW](#). Nawet jeśli pobierany plik jest większy od wybranego limitu i nie zostanie przeskanowany przez składnik Ochrona sieci WWW, ochrona jest nadal aktywna: jeśli plik jest zainfekowany, składnik [Ochrona rezydentna](#) natychmiast to wykryje.
- o **Wyklucz hosta/adres IP/domene** — w polu można wpisać dokładną nazwę serwera (*host, adres IP, adres IP z maską lub adres URL*) lub domene, które nie powinny być skanowane przez składnik [Ochrona sieci WWW](#). Wykluczać należy tylko hosty, co do których istnieje absolutna pewność, że nie stanowią zagrożenia.

9.8.2. Komunikatory internetowe

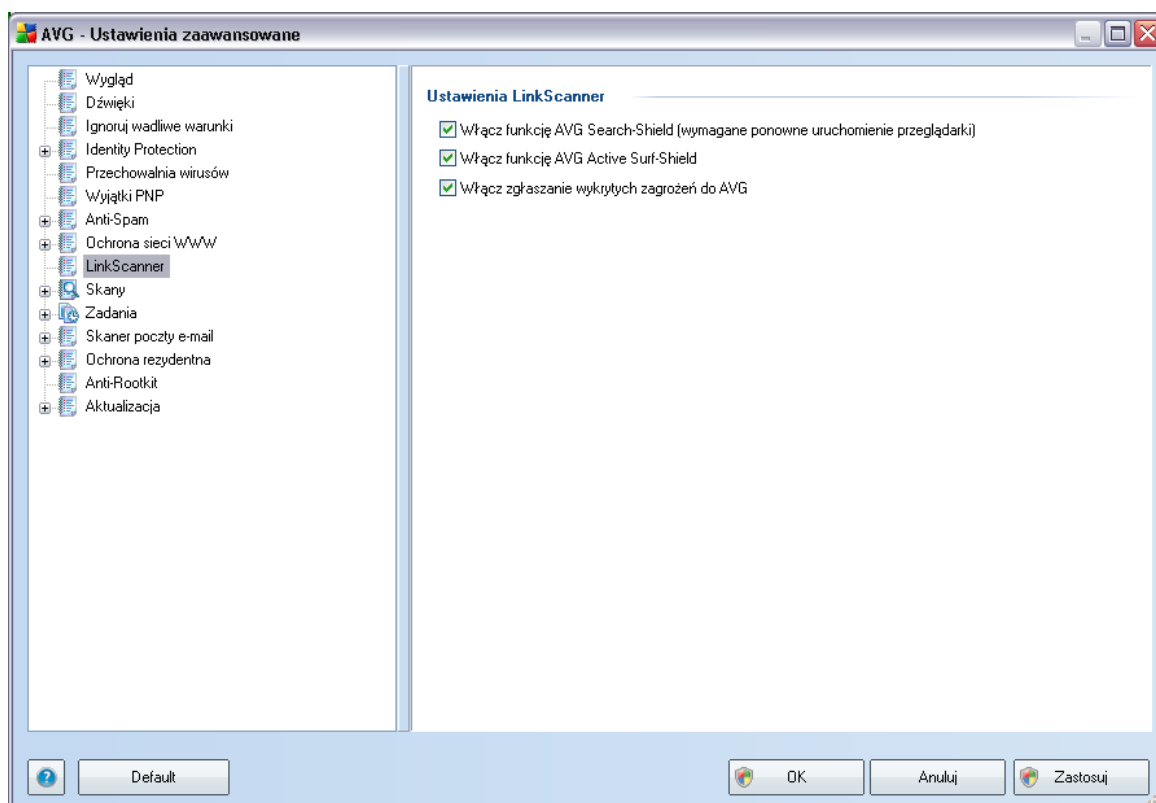


W oknie dialogowym **Ochrona komunikatorów internetowych** można edytować ustawienia składnika **Ochrona sieci WWW** dotyczące monitorowania plików przesyłanych za pośrednictwem komunikatorów. Obecnie obsługiwane są trzy komunikatory: **ICQ**, **MSN** i **Yahoo** — jeśli składnik **Ochrona sieci WWW**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

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

9.9. LinkScanner

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



- **Włącz funkcję AVG Search-Shield** — (domyślnie włączona): Skanuje wszystkie linki pojawiające się w wynikach wyszukiwania serwisów Google, Yahoo!, MSN oraz Baidu, a następnie obok każdego z nich wyświetla ikonę klasyfikacji bezpieczeństwa.
- **Włącz funkcję AVG Active 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 jakiegokolwiek innej aplikacji korzystającej z protokołu HTTP).
- **Włącz zgłaszanie wykrytych zagrożeń do firmy AVG** — (domyślnie włączone): należy zaznaczyć to pole, aby włączyć raportowanie exploitów oraz

niebezpiecznych witryn znalezionych przy użyciu funkcji **AVG Active Surf-Shield** lub **AVG Search-Shield**. Informacje te są przekazywane do naszej bazy danych.

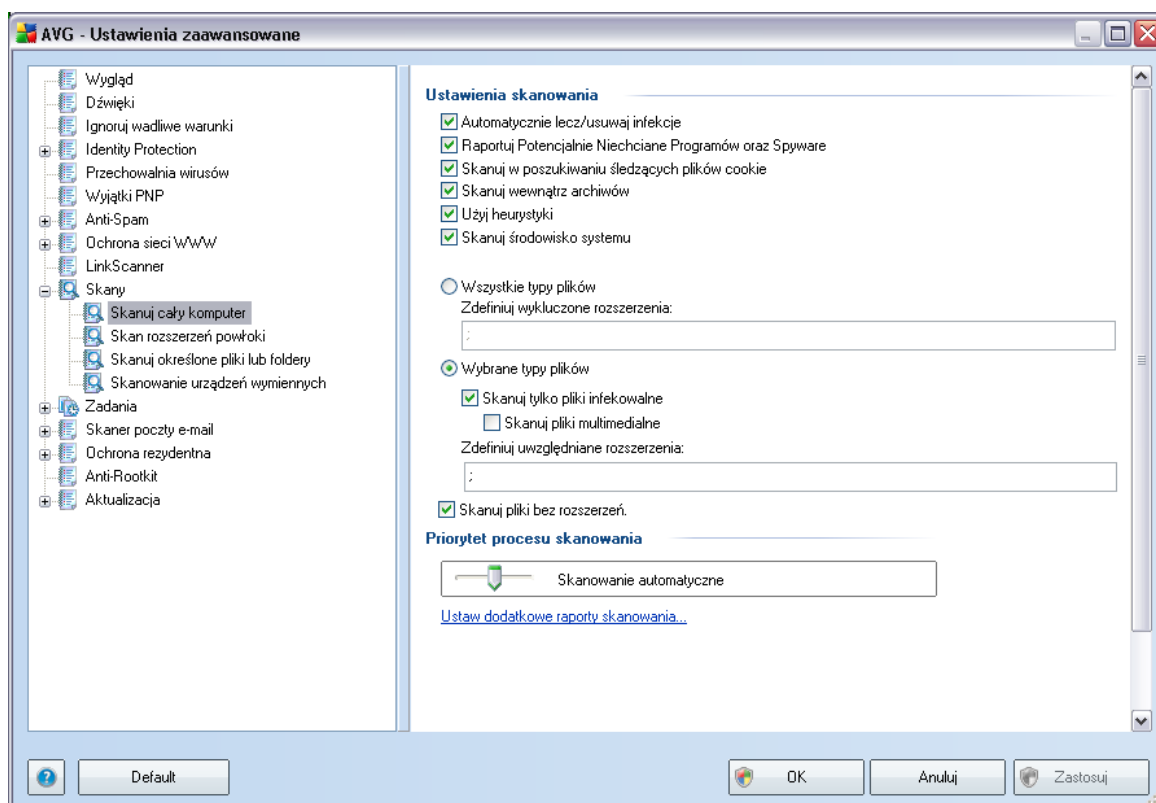
9.10. Skany

Zaawansowane ustawienia skanowania podzielone są na trzy kategorie odnoszące się do określonych typów testów zdefiniowanych przez producenta AVG:

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

9.10.1. Skan całego komputera

Opcja **Skan całego komputera** umożliwia edycję parametrów jednego ze wstępnie zdefiniowanych testów ([Skanu całego komputera](#)):



Ustawienia skanowania

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

- **Automatycznie lecz/usuwać infekcje** — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe 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. Zalecana metoda jest przeniesienie zainfekowanego pliku do [Przechowalni wirusów](#).
- **Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujące** — parametr ten kontroluje funkcje składnika [Anti-Virus](#), które

pozwalają wykrywać potencjalnie niechciane programy (pliki wykonywalne mogące działać jak oprogramowanie szpiegujące lub reklamowe), a następnie blokować je lub usuwać.

- **Skanuj w poszukiwaniu sledzacych plików cookie** — ten parametr składownika Anti-Spyware określa, że skanowanie ma wykrywać pliki cookie (pliki cookie są w protokole HTTP używane do uwierzytelniania, sledzenia i przechowywania określonych informacji o użytkownikach, na przykład preferencji wyglądu witryny czy zawartości koszyków w sklepach internetowych).
- **Skanuj wewnątrz archiwów** — parametr ten określa, czy skanowanie ma obejmować wszystkie pliki — nawet te znajdujące się wewnątrz niektórych typów archiwów, np. ZIP, RAR itd.
- **Użyj heurystyki** — analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny) jest jedną z metod wykrywania wirusów w czasie rzeczywistym.
- **Skanuj środowisko systemu** — skanowanie obejmie także obszary systemowe komputera.

Następnie należy zdecydować, czy skanowane mają być

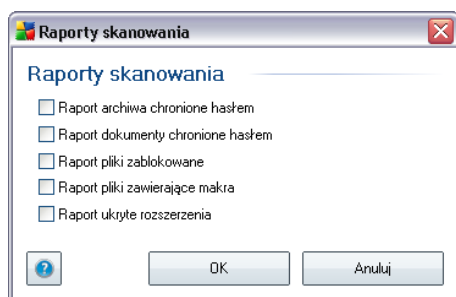
- **Wszystkie typy plików** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, który nie powinny być skanowane; LUB
- **Wybrane typy plików** — skanowane będą tylko pliki infekowalne (pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe i niewykonywalne), z uwzględnieniem multimediów (plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowanie skróci się jeszcze bardziej, ponieważ takie pliki często są duże, a nie są podatne na infekcję). 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

W sekcji **Priorytet procesu skanowania** można szczegółowo określić zadane prędkości skanowania, w zależności od wykorzystania zasobów systemowych. Domyślnie wartość tej opcji jest na średnim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jeśli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowolnić działanie innych procesów i aplikacji (*opcji można śmiało używać wtedy, gdy komputer jest włączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

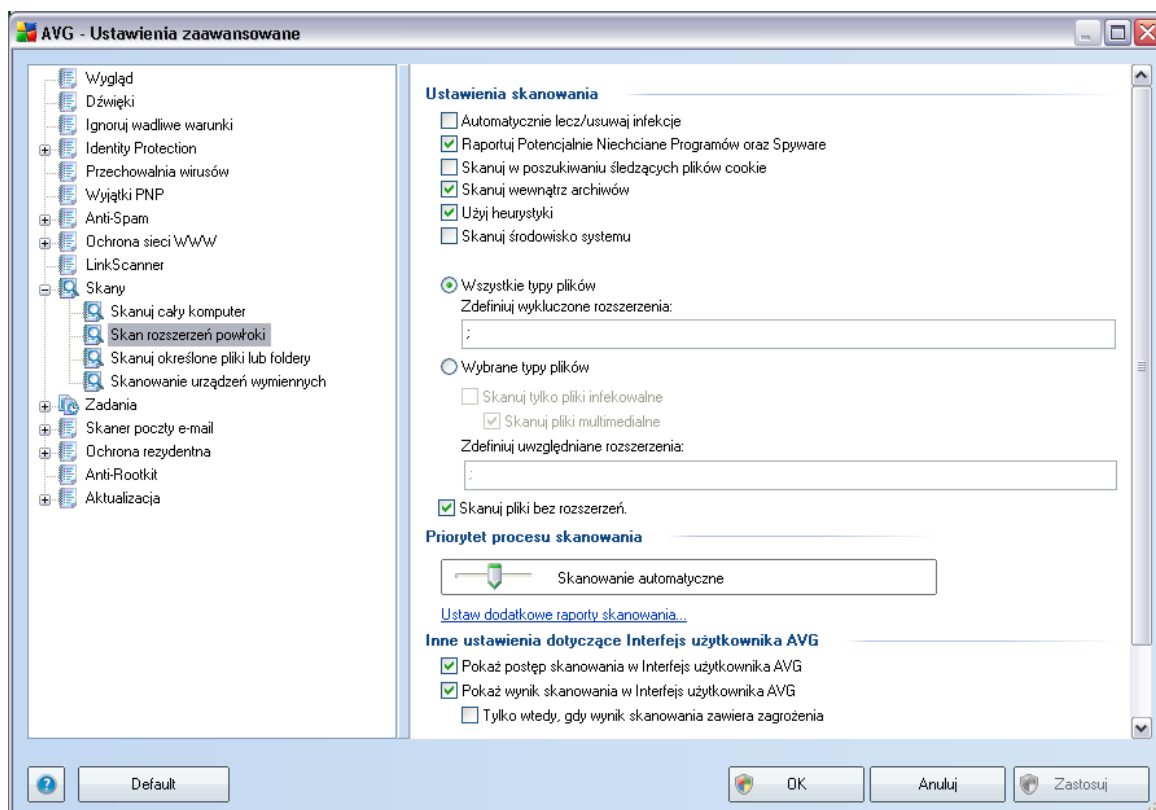
Ustaw dodatkowe raporty skanowania...

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



9.10.2. Skan rozszerzenia powłoki

Analogicznie do [Skanu całego komputera](#), test **Skan rozszerzenia powłoki** także oferuje szereg opcji silnika skanującego, zdefiniowanych wstępnie przez dostawcę oprogramowania AVG. W tym przypadku konfiguracja odnosi się do [skanowania określonych obiektów bezpośrednio z interfejsu Eksploratora Windows](#) (*rozszerzenie powłoki*); zobacz rozdział [Skanowanie z poziomu Eksploratora Windows](#):

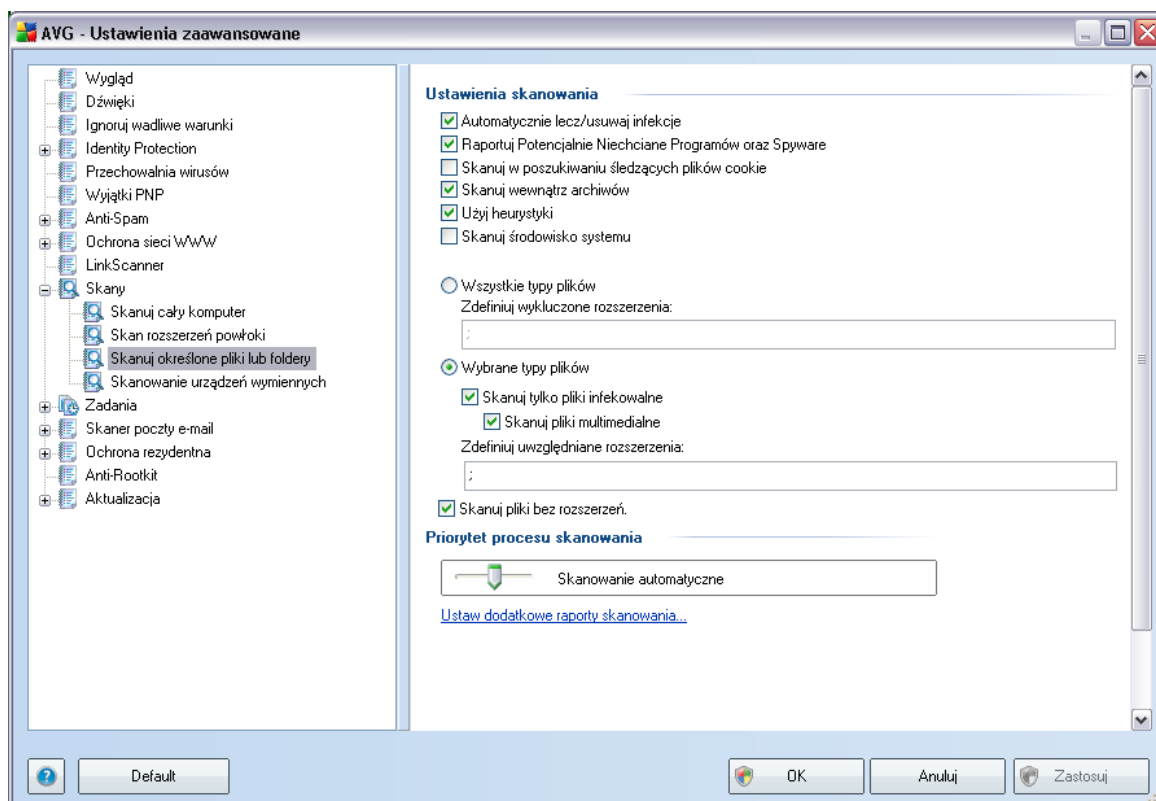


Lista parametrów jest identyczna jak dla testu [Skan całego komputera](#). Ustawienia domyślne są jednak inne: większość opcji **Skanu całego komputera** jest aktywna, natomiast w przypadku testu **Skan rozszerzeń powłoki** ([Skanowanie z poziomu Eksploratora Windows](#)) wybrane są tylko najistotniejsze parametry.

Uwaga: Opis poszczególnych parametrów można znaleźć w rozdziale [Zaawansowane ustawienia AVG / Skany / Skan całego komputera](#).

9.10.3. Skan określonych plików lub folderów

Interfejs edycji testu **Skan określonych plików lub folderów** jest identyczny jak w przypadku [Skanu całego komputera](#). Wszystkie opcje konfiguracyjne są takie same, jednak ustawienia domyślne dla [Skanu całego komputera](#) są bardziej rygorystyczne:

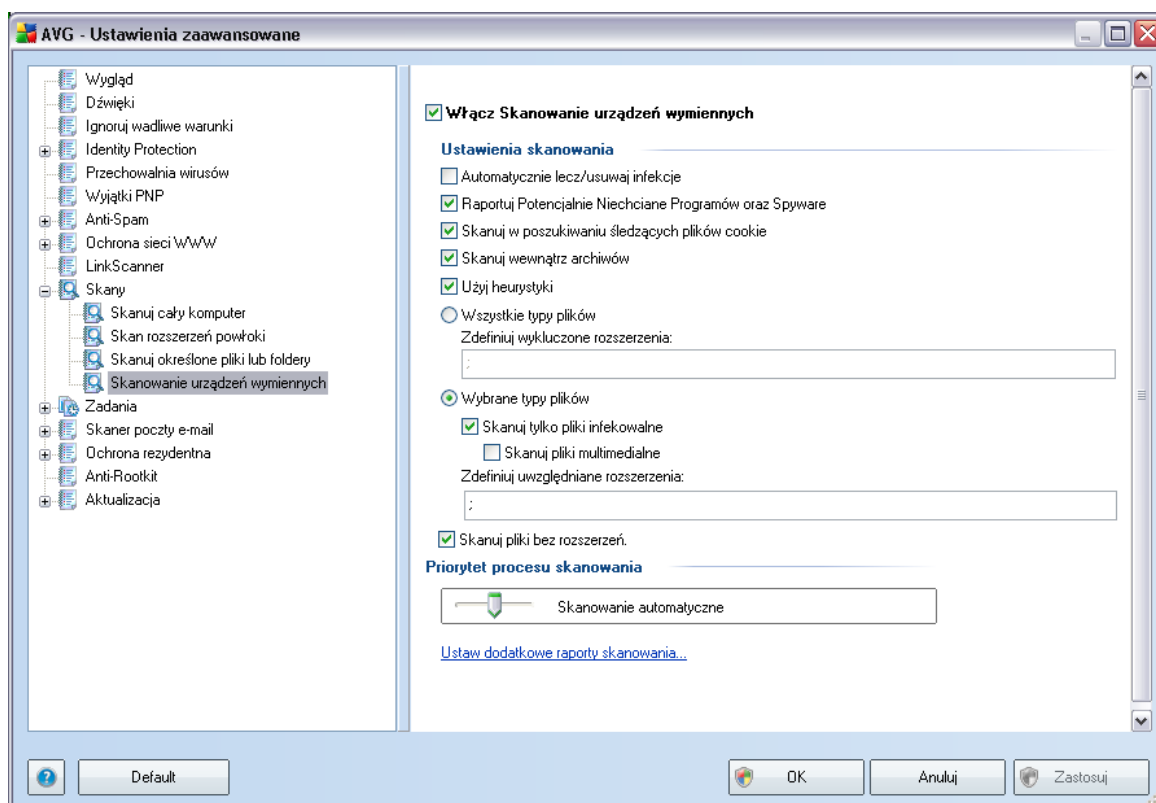


Wszystkie parametry ustawiane w tym oknie dialogowym odnoszą się tylko do obszarów wybranych do **skanowania określonych plików lub folderów**! Zaznaczenie opcji ***Skanuj w poszukiwaniu programów typu rootkit*** w tym oknie konfiguracyjnym oznacza, że wykonane zostanie tylko szybkie wyszukiwanie programów typu rootkit, czyli skanowanie w poszukiwaniu programów typu rootkit wyłącznie w wybranych obszarach.

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

9.10.4. Skan urządzeń wymiennych

Okno z opcjami **Skanu urządzeń wymiennych** jest także bardzo podobne do okna [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 skan ma być uruchamiany automatycznie, należy zaznaczyć opcję **Włącz skanowanie urządzeń wymiennych**.

Uwaga: Opis poszczególnych parametrów zawiera rozdział [Zaawansowane ustawienia AVG / Skany / Skan całego komputera](#).

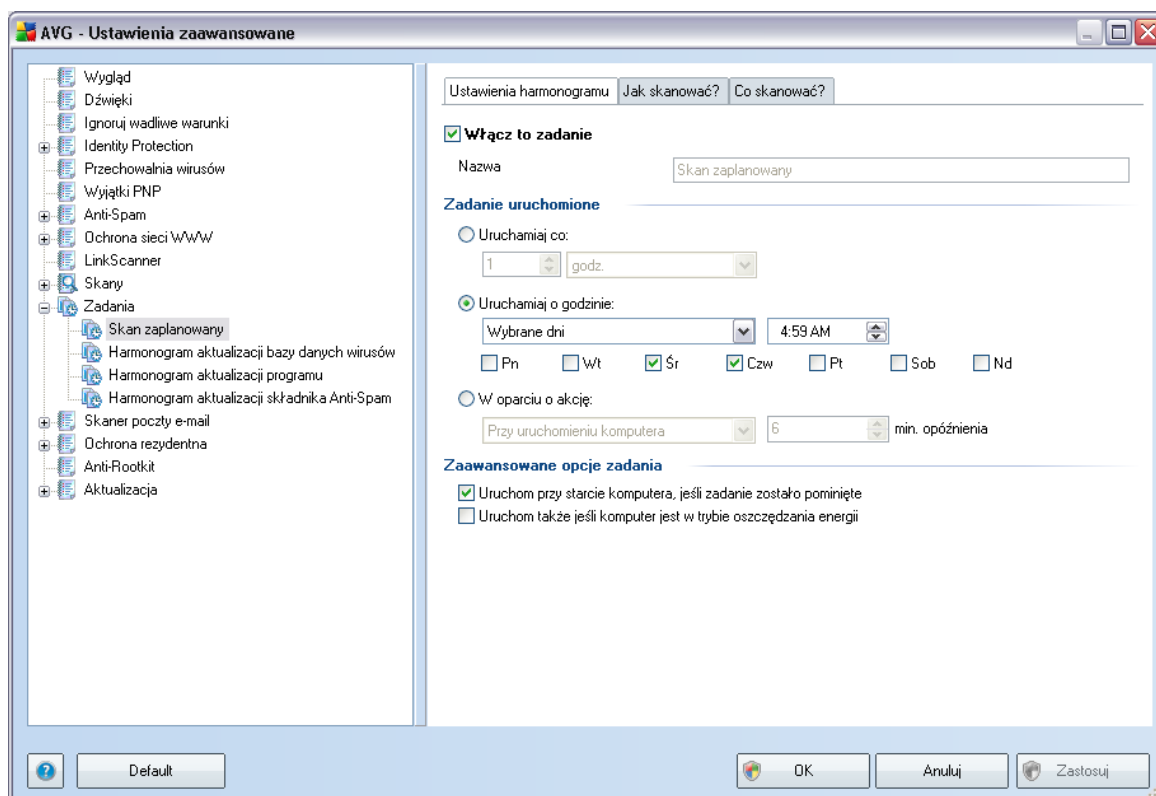
9.11. Zaplanowane zadania

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

- [Skan zaplanowany](#)
- [Harmonogram aktualizacji bazy danych wirusów](#)
- [Harmonogram aktualizacji programu](#)
- [Harmonogram aktualizacji składnika Anti-Spam](#)

9.11.1. Skan zaplanowany

Parametry skanowania zaplanowanego można edytować (*albo utworzyć nowy harmonogram*) na trzech kartach:



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

W polu tekstowym **Nazwa** (wylaczone dla harmonogramów domyslnych) jest wyświetlana nazwa przypisana do tego 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**).

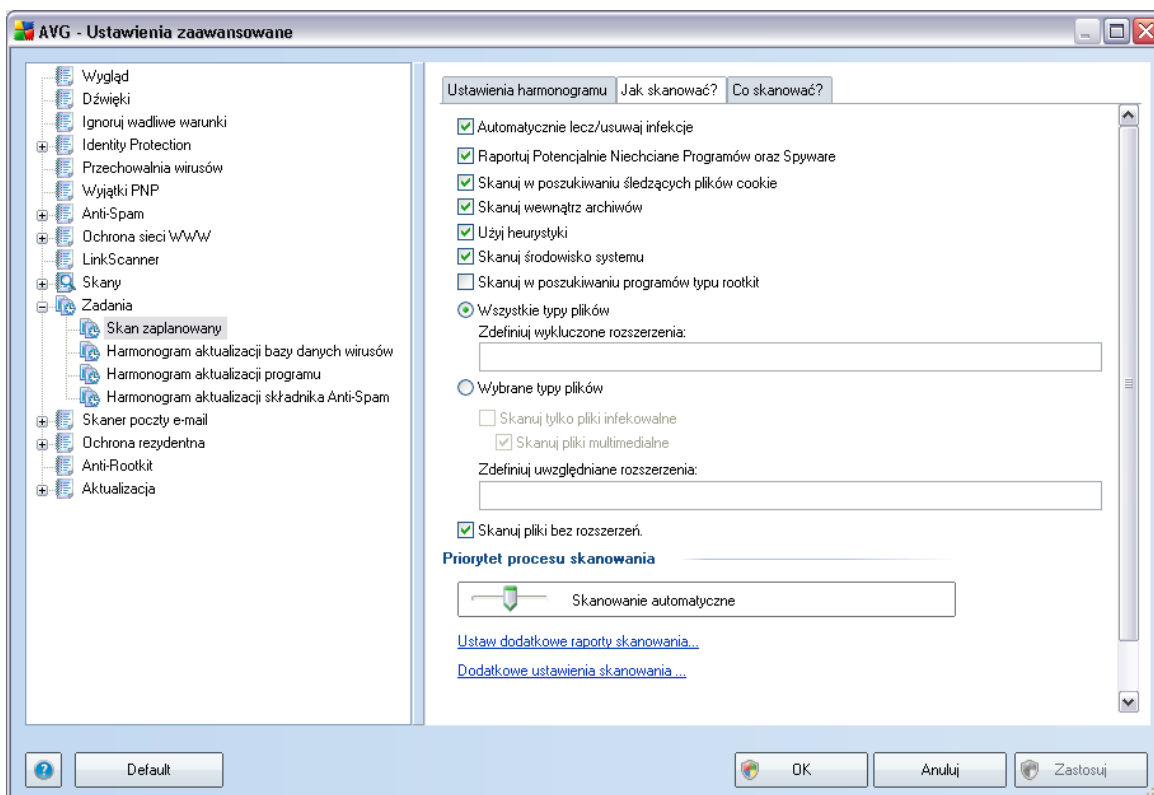
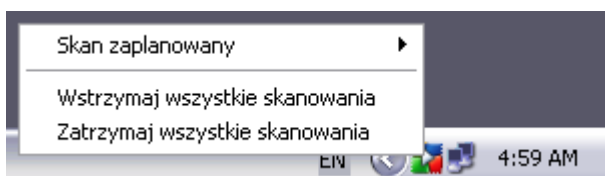
Zaawansowane opcje harmonogramu

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 tam nowa [ikona AVG](#) (kolorowa, z białą strzałką — jak powyżej), która informuje o uruchomieniu skanowania. Kliknięcie jej prawym przyciskiem myszy pozwala wyświetlić menu kontekstowe, dzięki któremu można wstrzymać lub anulować skanowanie:



Karta **Jak skanować?** zawiera listę parametrów testu, które można włączyć lub wyłączyć. Domyslnie 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/usuwa infekcje** — (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. Zalecana czynność jest przeniesienie zainfekowanego pliku do [Przechowalni wirusów](#).
- **Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujące** — (domyślnie włączona) parametr ten kontroluje funkcje składowa [Anti-Virus](#), które pozwalają [wykrywać potencjalnie niechciane programy](#) (pliki wykonywalne mogące działać jak oprogramowanie szpiegujące lub reklamowe), a następnie blokować je lub usuwać.
- **Skanuj w poszukiwaniu sledzających plików cookie** — (domyślnie włączona) ten parametr składowa [Anti-Spyware](#) określa, czy wykrywane mają być pliki cookie (używane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania określonych informacji o użytkownikach — np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych).
- **Skanuj wewnątrz archiwów** — (domyślnie włączona) parametr ten określa, czy skanowanie ma obejmować wszystkie pliki, nawet te znajdujące się wewnątrz niektórych typów archiwów, np. ZIP, RAR itd.
- **Użyj heurystyki** — (domyślnie włączona) analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny) jest jedną z metod wykrywania wirusów w czasie rzeczywistym.
- **Skanuj środowisko systemu** — (domyślnie włączona) skanowanie obejmie także obszary systemowe komputera.
- **Skanuj w poszukiwaniu programów typu rootkit** — zaznaczenie tej pozycji pozwala dołączyć wykrywanie programów typu rootkit do operacji skanowania całego komputera. Test Anti-Rootkit można także uruchomić niezależnie, dzięki interfejsowi składowa [Anti-Rootkit](#)

Następnie należy zdecydować, czy skanowane mają być

- **Wszystkie typy plików** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, który nie powinny być skanowane; LUB
- **Wybrane typy plików** — skanowane będą 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 skanowanie skróci się

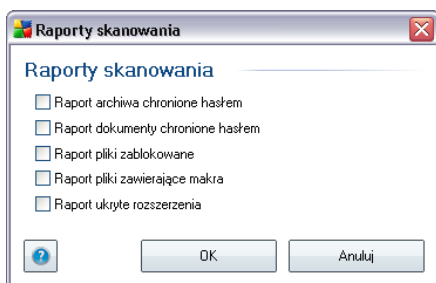
jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

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

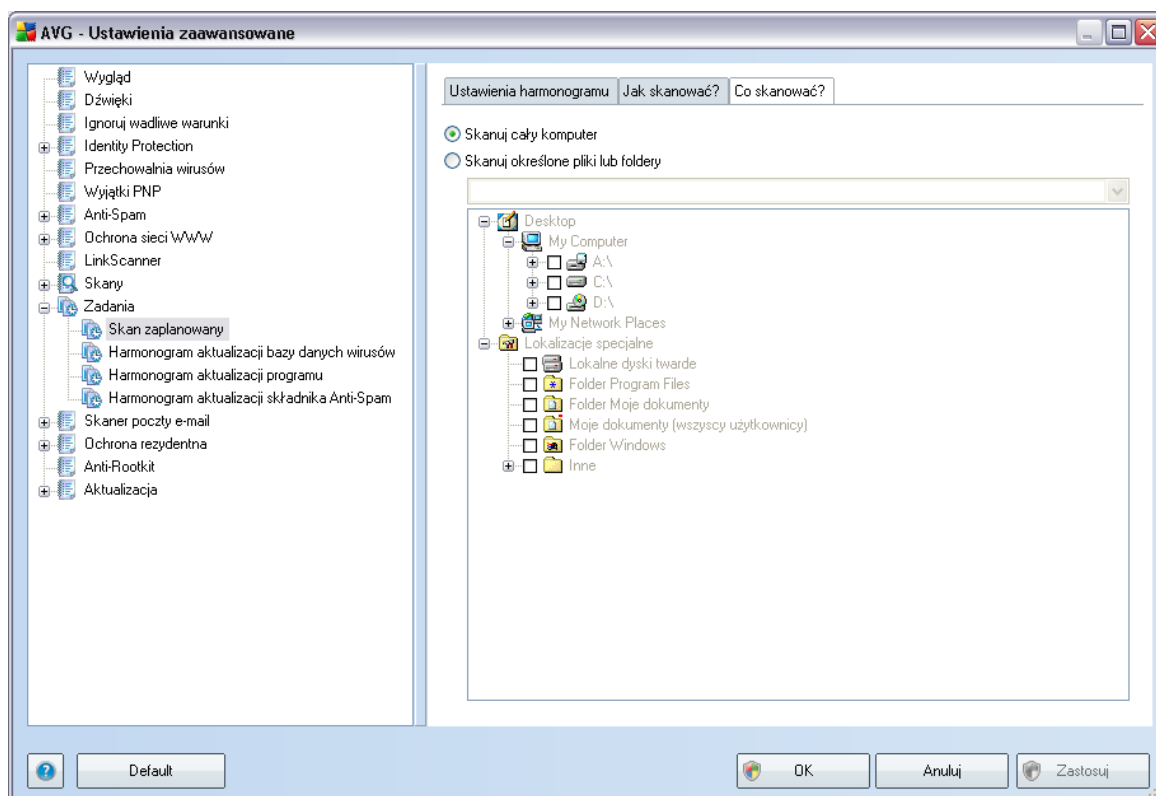
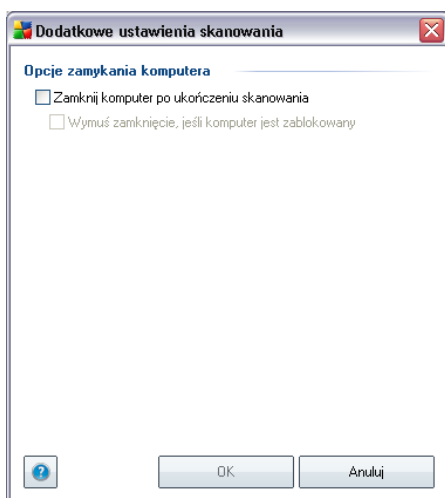
Priorytet procesu skanowania

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

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



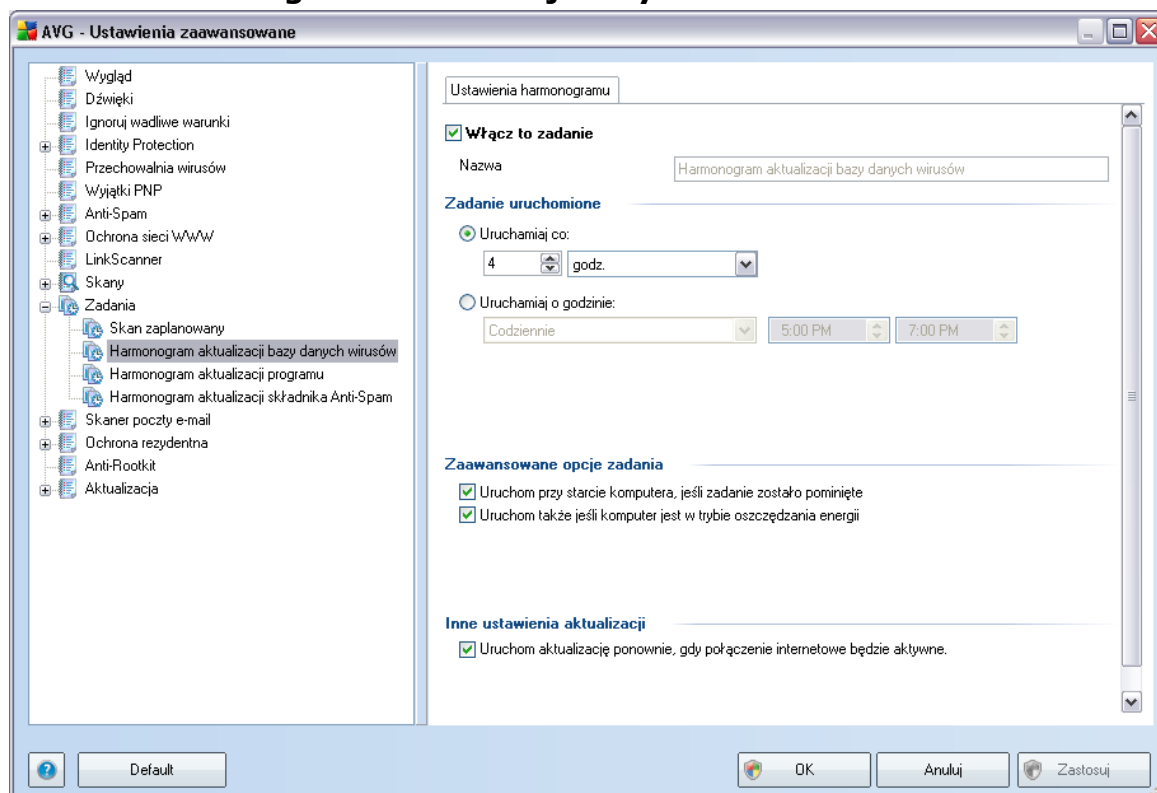
Dodatkowe ustawienia skanowania — link ten pozwala otworzyc nowe okno dialogowe **Opcje zamykania komputera**, w którym mozna okreslic, czy komputer ma byc zamykany automatycznie po zakonczeniu procesu skanowania. Wybranie pierwszej opcji (**Zamknij komputer po ukonczeniu skanowania**) powoduje aktywowanie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

9.11.2. Harmonogram aktualizacji bazy wirusów



Na karcie **Ustawienia harmonogramu** można odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć zaplanowaną aktualizację bazy wirusów i włączyć ją ponownie dopiero gdy zajdzie taka potrzeba.

Podstawowe opcje harmonogramu aktualizacji bazy wirusów dostępne są w składniku [Menedżer aktualizacji](#). W niniejszym oknie można ustawić szczegółowe parametry harmonogramu:

W polu tekstowym **Nazwa** (wylaczone dla harmonogramów domyslnych) jest wyświetlana nazwa przypisana do tego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (aby dodać harmonogram, należy kliknąć prawym przyciskiem myszy element **Harmonogram aktualizacji bazy wirusów** w

drzewie nawigacji po lewej) można określić własną nazwę, a wspomniane pole tekstowe jest edytowalne. Warto używać jak najkrótszych, opisowych nazw harmonogramów, aby potem móc je łatwo identyfikować.

Zadanie uruchomione

W tej sekcji należy określić interwał dla planowanych aktualizacji bazy danych wirusów. Aktualizacja może być powtarzana 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 harmonogramu

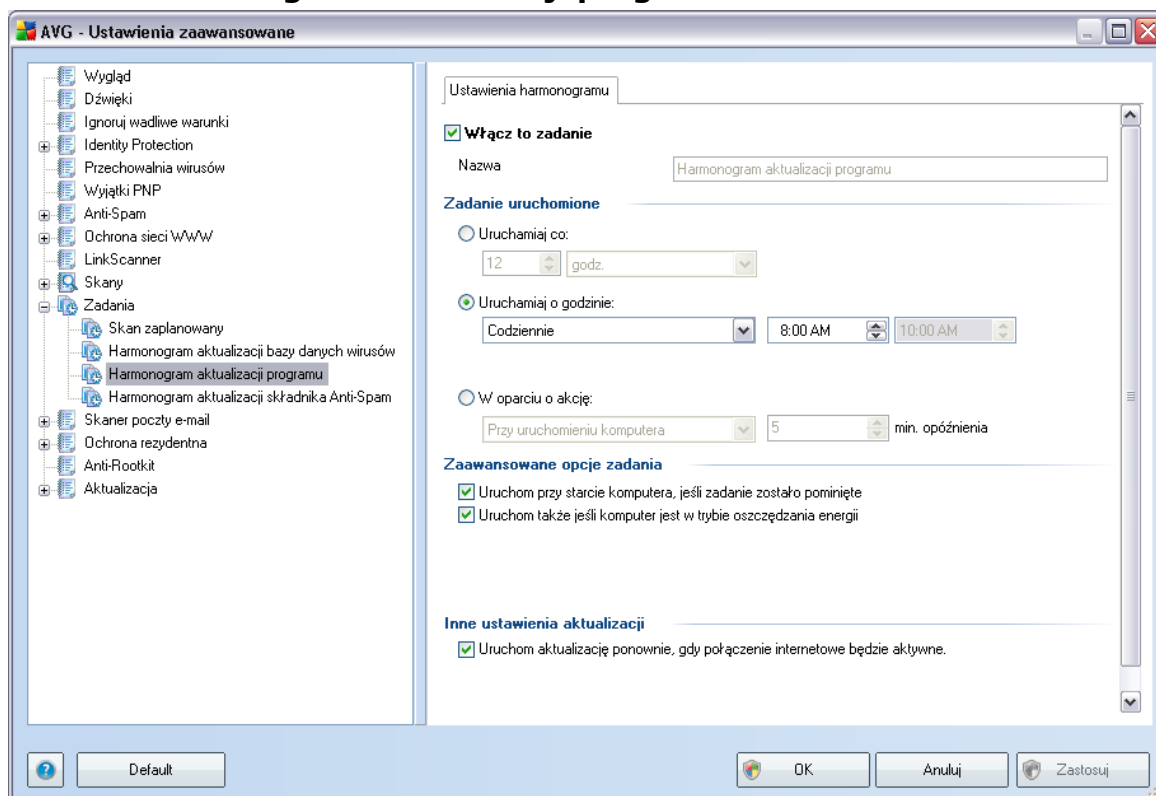
Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji bazy wirusów w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

Inne ustawienia aktualizacji

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

Po rozpoczęciu zaplanowanej aktualizacji nad [ikoną AVG na pasku zadań](#) wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji [Ustawienia zaawansowane/Wygląd](#)*).

9.11.3. Harmonogram aktualizacji programu



Na karcie **Ustawienia harmonogramu** można odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć zaplanowaną aktualizację programu i włączyć ją ponownie dopiero gdy zajdzie taka potrzeba.

W polu tekstowym **Nazwa** (wylaczone dla harmonogramów domyślnych) wyświetlana jest nazwa przypisana do tego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (aby dodać harmonogram, należy kliknąć prawym przyciskiem myszy element **Harmonogram aktualizacji programu** w drzewie nawigacji po lewej) można określić własną nazwę, a wspomniane pole tekstowe jest edytowalne. Warto używać jak najkrótszych, opisowych nazw harmonogramów, aby potem móc je łatwo identyfikować.

Zadanie uruchomione

W tym miejscu należy określić interwał dla nowo zaplanowanych aktualizacji programu. Aktualizacja może być powtarzana w określonych odstępach czasu (

Uruchamiaj co) lub o zadanej godzinie (**Uruchamiaj o określonej godzinie**), a także na skutek wystąpienia zdefiniowanego zdarzenia (**W oparciu o akcje, np. uruchomienie komputera**).

Zaawansowane opcje harmonogramu

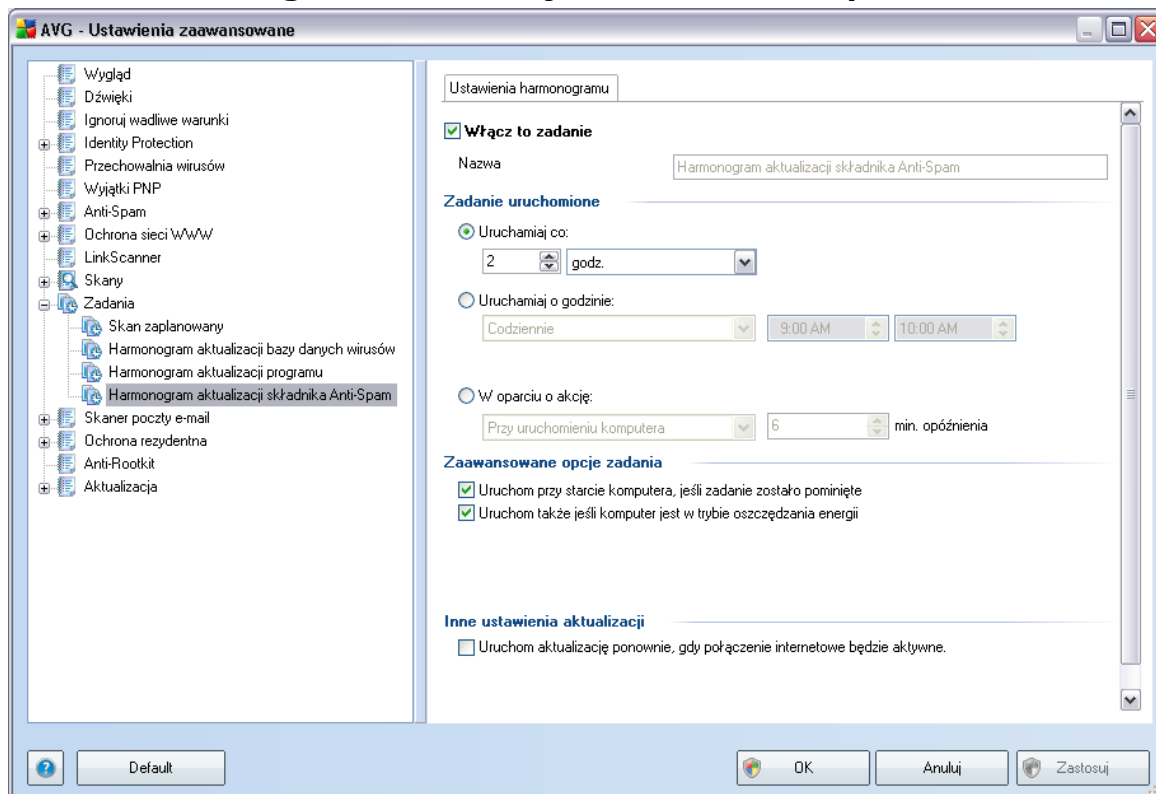
Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji programu w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

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 rozpoczęciu zaplanowanej aktualizacji nad [ikoną AVG na pasku zadań](#) wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji [Ustawienia zaawansowane/Wygląd](#)*).

9.11.4. Harmonogram aktualizacji składnika Anti-Spam



Na karcie **Ustawienia harmonogramu** można odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć zaplanowaną aktualizację składnika **Anti-Spam** i włączyć ją ponownie dopiero gdy zajdzie taka potrzeba.

Podstawowe opcje planowania aktualizacji składnika **Anti-Spam** opisano w interfejsie **Menedżera aktualizacji**. W niniejszym oknie można ustawić szczegółowe parametry harmonogramu:

W polu tekstowym **Nazwa** (wylaczone dla harmonogramów domyślnych) wyświetlana jest nazwa przypisana do tego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (aby dodać harmonogram, należy kliknąć prawym przyciskiem myszy element **Harmonogram aktualizacji składnika Anti-Spam** w drzewie nawigacji po lewej) można określić własną nazwę, a wspomniane pole tekstowe jest edytowalne. Warto używać jak najkrótszych, opisowych nazw harmonogramów, aby potem móc je łatwo identyfikować.

Zadanie uruchomione

W tym miejscu należy określić interwały aktualizacji składnika [Anti-Spam](#). Aktualizacja składnika [Anti-Spam](#) może być powtarzana w określonych odstępach czasu (**Uruchamiaj co**) lub o zadanej godzinie (**Uruchamiaj o określonej godzinie**), a także na skutek wystąpienia zdefiniowanego zdarzenia (**W oparciu o akcje, np. uruchomienie komputera**).

Zaawansowane opcje harmonogramu

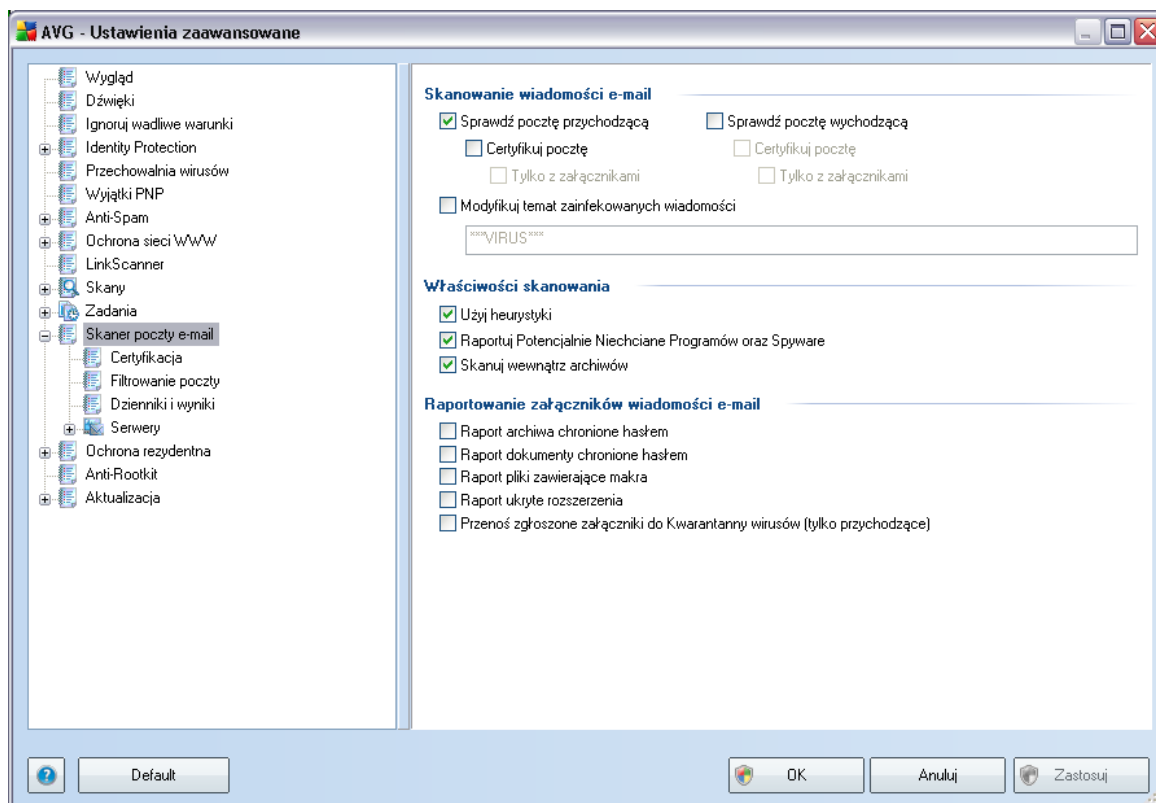
Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji składnika [Anti-Spam](#) w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

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 rozpoczęciu zaplanowanego skanowania, nad [ikona AVG na pasku zadań](#) wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji [Ustawienia zaawansowane/Wygląd](#)*).

9.12. Skaner poczty e-mail

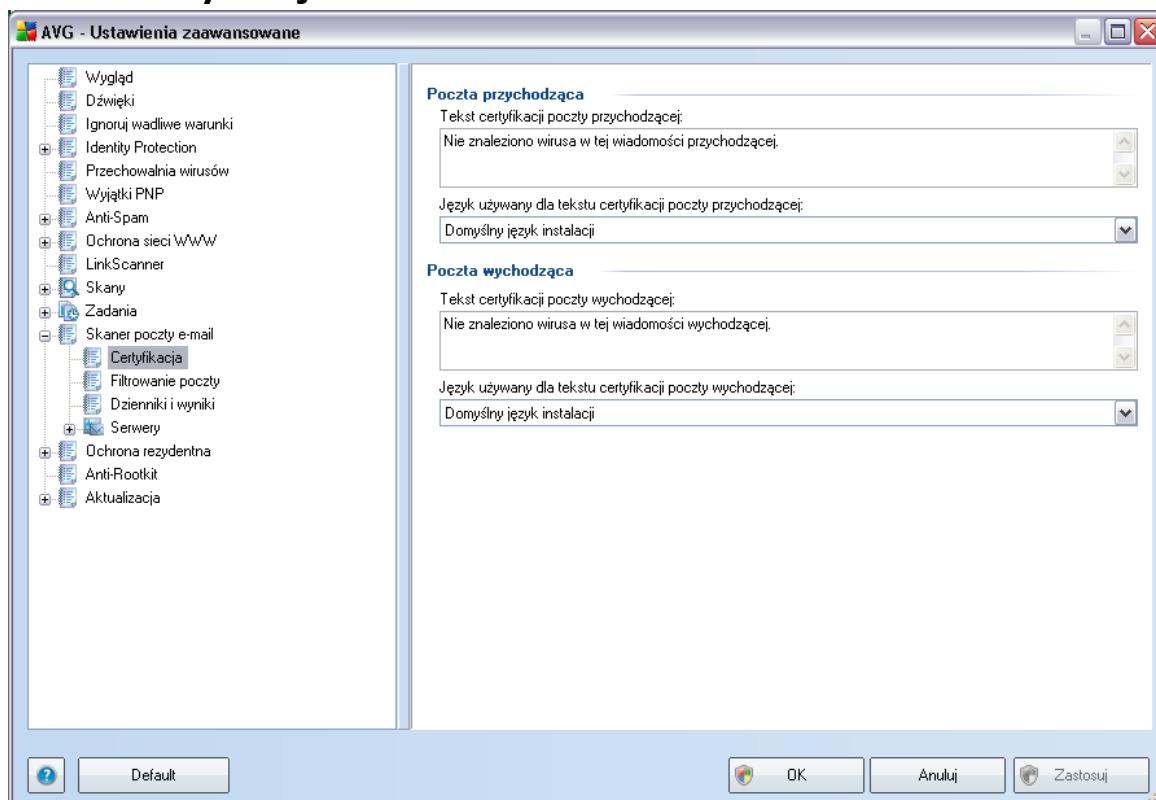


Okno **Skaner poczty e-mail** podzielone jest na trzy sekcje:

- **Skanowanie poczty e-mail** — w sekcji tej można określić, czy mają być skanowane wiadomości przychodzące i wychodzące, a także czy certyfikacja ma obejmować wszystkie wiadomości, czy tylko te z załącznikami (certyfikacja *nie jest dostępna w formacie HTML/RTF*). Ponadto, można określić, czy program AVG ma modyfikować temat wiadomości potencjalnie zawierających wirusy. W tym celu należy zaznaczyć pole **Modyfikuj temat zainfekowanych wiadomości** i ewentualnie zmienić tekst w polu obok (domyslnie jest to *****WIRUS*****).
- **Właściwości skanowania** — należy określić, czy podczas skanowania ma być stosowana [analiza heurystyczna](#) (**Użyj heurystyki**), czy system ma szukać [potencjalnie niechcianych programów](#) (**Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujące**), a także czy skanowane mają być archiwa (**Skanuj wewnątrz archiwów**).

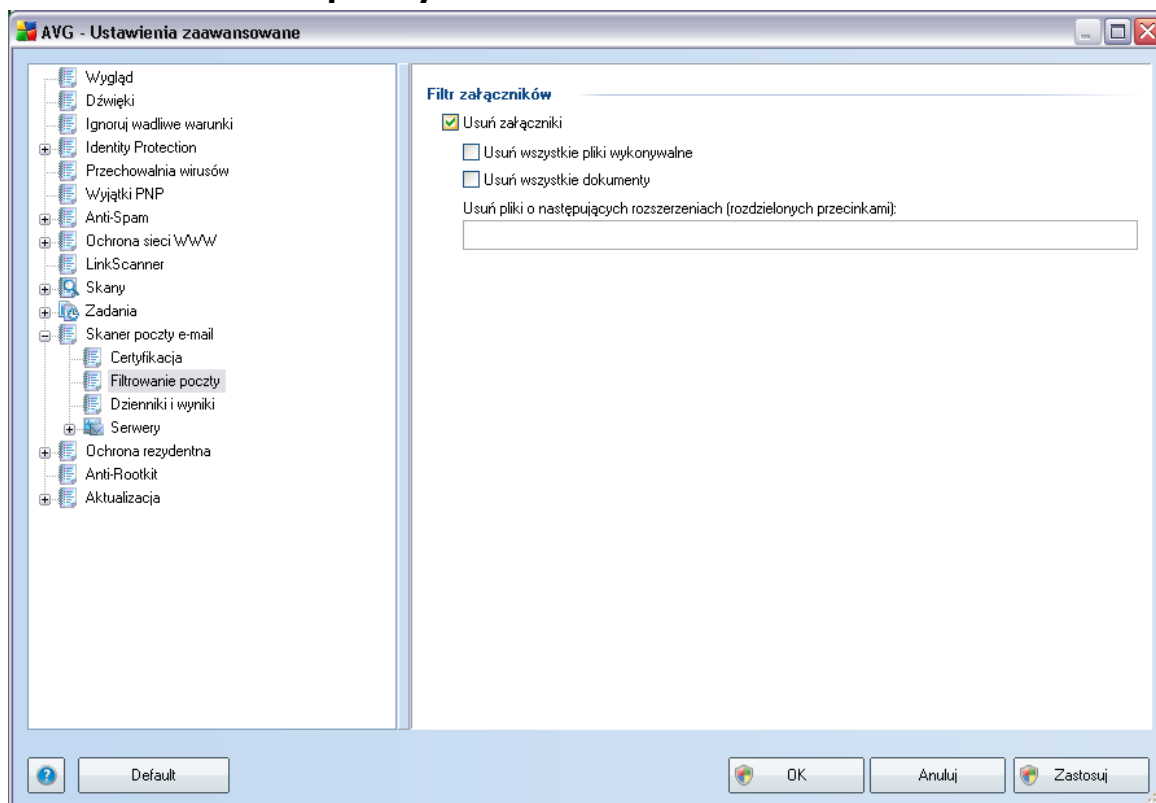
- **Raportowanie załączników e-mail** — należy określić, czy system ma powiadamiać pocztą e-mail o archiwach zabezpieczonych hasłem, dokumentach zabezpieczonych hasłem, plikach zawierających makra i/lub plikach o ukrytych rozszerzeniach, które zostaną wykryte jako załączniki do skanowanych wiadomości e-mail. Należy także określić, czy w przypadku wykrycia takiej wiadomości podczas skanowania zainfekowany obiekt ma zostać przeniesiony do [Przechowalni wirusów](#).

9.12.1. Certyfikacja



W oknie **Certyfikacja** można szczegółowo określić treść certyfikatu oraz jego język. Ustawienia te należy wprowadzić osobno dla **wiadomości przychodzących** i **wychodzących**.

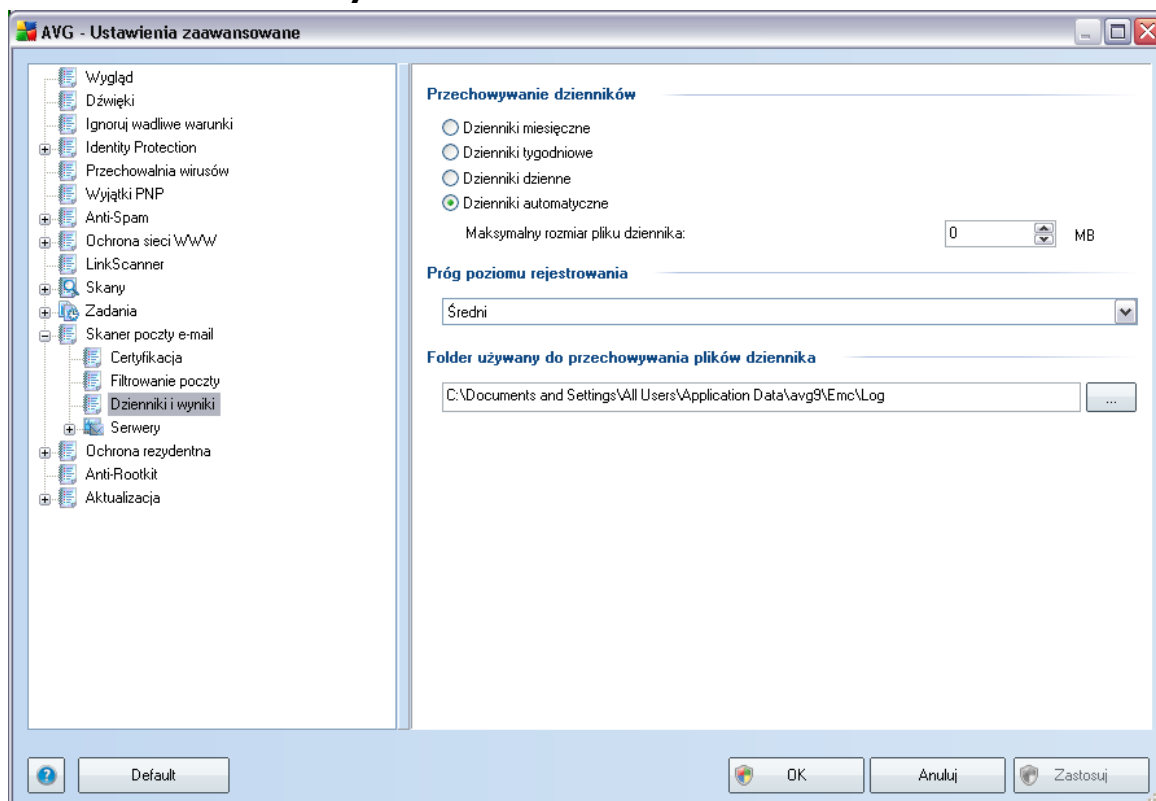
9.12.2. Filtrowanie poczty



W oknie **Filtr załączników** można ustawiać parametry skanowania załączników e-mail. Opcja **Usun 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:

- **Usun wszystkie pliki wykonywalne** — usuwane będą wszystkie pliki *.exe.
- **Usun wszystkie dokumenty** — usuwane będą wszystkie pliki *.doc.
- **Usun pliki o następujących rozszerzeniach oddzielonych przecinkami** — usuwane będą wszystkie pliki o zdefiniowanych rozszerzeniach.

9.12.3. Dzienniki i Wyniki

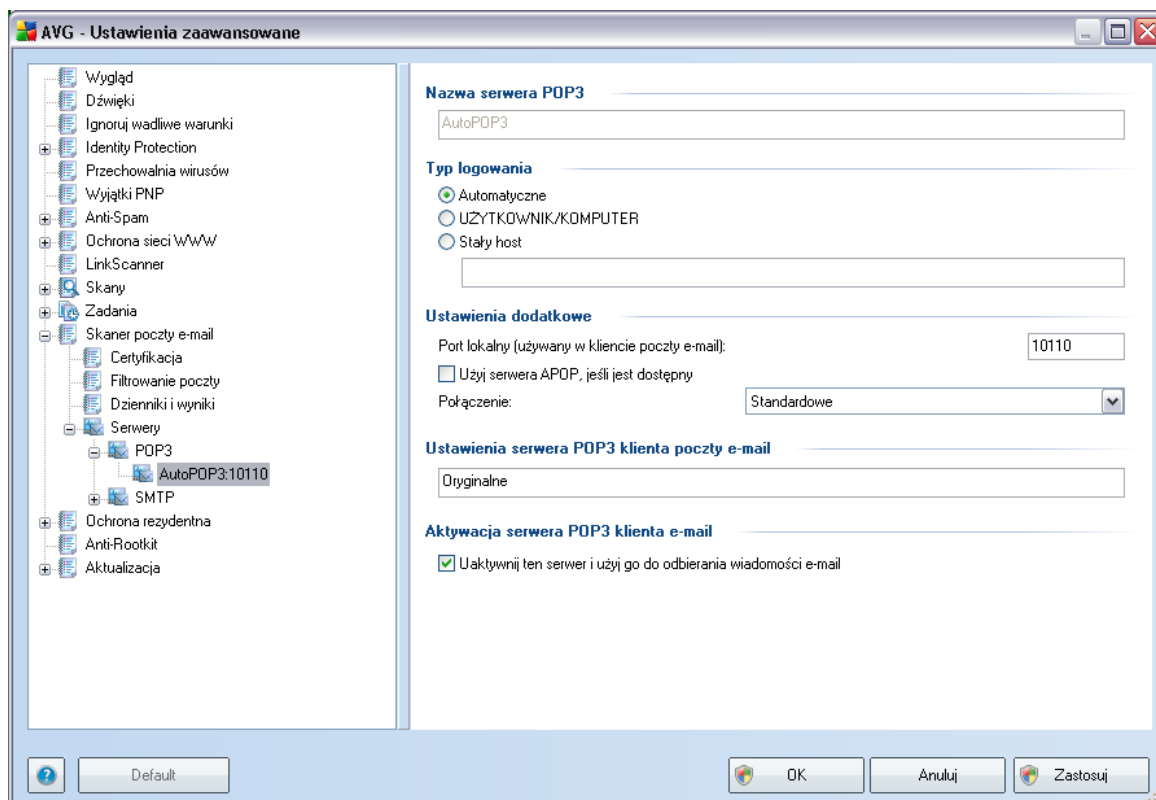


W oknie **Dzienniki i wyniki** można określić parametry przechowywania wyników skanowania poczty e-mail. Okno to podzielone jest na dwa obszary:

- **Przechowywanie dzienników** — pozwala zdecydować, czy informacje o skanowaniu poczty e-mail mają być rejestrowane codziennie, co tydzień, co miesiąc itd.; można tu także określić maksymalny rozmiar pliku dziennika (w MB).
- **Próg poziomu rejestrowania** — domyślnie ustawiony jest poziom średni; można wybrać niższy (*rejestrowanie podstawowych informacji o połączeniu*) lub wyższy (*rejestrowanie całego ruchu*).
- **Folder używany do przechowywania plików dziennika** — pozwala określić, gdzie mają znajdować się pliki dziennika.

9.12.4. Serwery

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

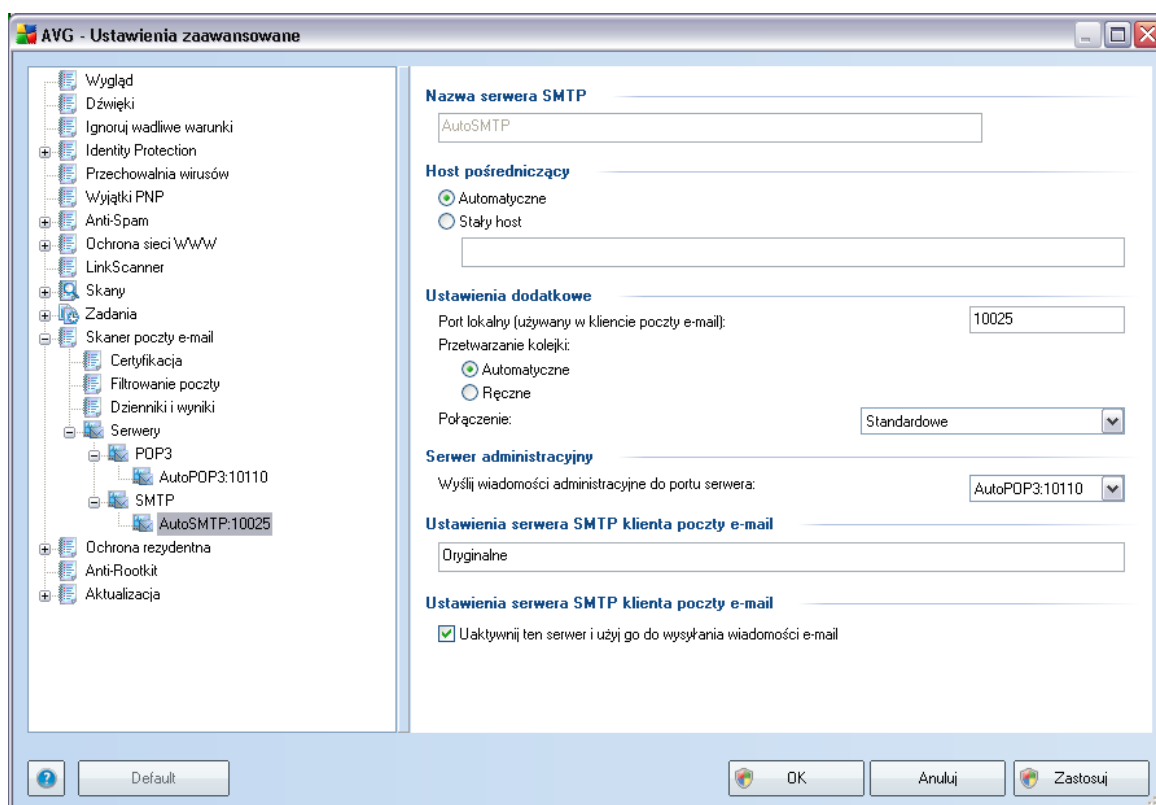


W tym oknie dialogowym (dostępnym z menu **Serwery / POP3**) można zdefiniować (na potrzeby [Skanera poczty e-mail](#)) nowy serwer poczty przychodzącej, korzystający z protokołu POP3:

- **Nazwa serwera POP3** — należy wpisać nazwę serwera lub zachować domyślną nazwę AutoPOP3.
- **Typ logowania** — definiuje metodę określania serwera pocztowego dla wiadomości przychodzących:
 - o **Automatycznie** — logowanie jest przeprowadzane automatycznie zgodnie z ustawieniami klienta poczty e-mail.

- o **UZYTKOWNIK/KOMPUTER** — najprostsza i najczęściej używana metoda ustalania docelowego serwera pocztowego jest metoda proxy. Stosując tę metodę, jako część loginu użytkownika należy podać jego nazwę lub adres (lub także port), oddzielając ją znakiem /. Na przykład dla konta użytkownik1 na serwerze pop.domena.com z numerem portu 8200 należy stosować login użytkownik1/pop.domena.com:8200.
- o **Staly 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 niezmienny. Jako nazwy można użyć nazwy domeny (na przykład pop.acme.com) lub adresu IP (na przykład 123.45.67.89). Jeśli serwer pocztowy używa niestandardowego portu, można określić go po dwukropku zaraz za nazwą serwera (na przykład pop.domena.com:8200). Standardowym portem protokołu POP3 jest 110.
- **Ustawienia dodatkowe** — pozwalają zdefiniować bardziej szczegółowe parametry:
 - o **Port lokalny** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w kliencie poczty jako port docelowy serwera POP3.
 - o **Użyj serwera APOP, jeśli jest dostępny** — opcja ta zapewnia bezpieczniejsze logowanie na serwerze pocztowym. Gwarantuje to, że [Skaner poczty e-mail](#) będzie używał alternatywnej metody przekazywania hasła użytkownika, polegającej na wysyłaniu go w formie zaszyfrowanej, która korzysta ze zmiennego klucza nadesłanego przez serwer. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
 - o **Polaczenie** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (zwykle/SSL/domyslnie 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.
- **W obszarze Aktywacja serwera POP3 klienta e-mail** znajdują się informacje dotyczące poprawnych ustawień klienta poczty e-mail (tak, aby wszystkie wiadomości przechodziły przez [Skaner poczty e-mail](#)). Informacje te stanowią podsumowanie odpowiednich parametrów określonych w całej konfiguracji AVG.

- **Aktywacja serwera POP 3 klienta poczty e-mail** — opcje te należy zaznaczyć/odznaczyć, aby aktywować/wyłączyć określony serwer POP3.



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

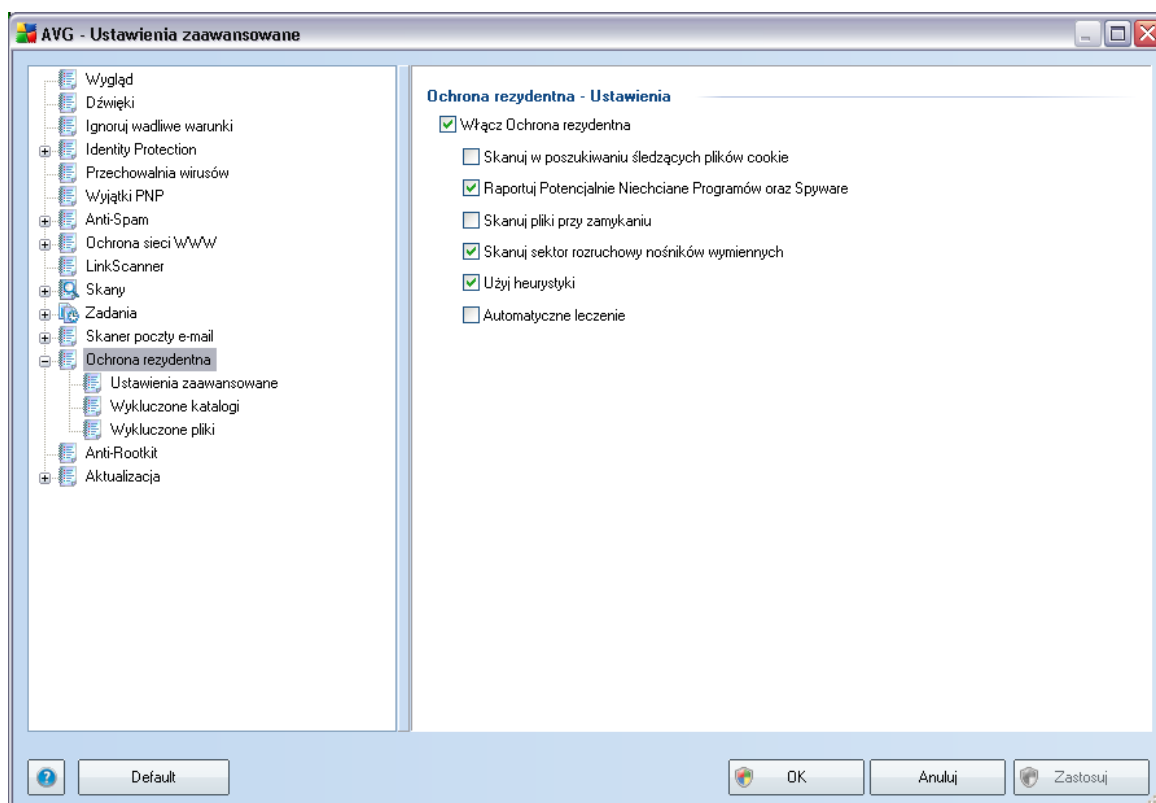
- **Nazwa serwera SMTP** — należy podać nazwę serwera lub zachować domyślną (AutoSMTP).
- **Host pośredniczący** — definiuje metodę określania serwera pocztowego dla wiadomości wychodzących:
 - o **Automatyczne** — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail
 - o **Staly host** — po wybraniu tej opcji program będzie zawsze korzystał z

serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Jako nazwy można użyć domeny (na przykład smtp.domena.com) lub adresu IP (na przykład 123.45.67.89). Jeśli serwer pocztowy używa niestandardowego portu, można określić go po dwukropku zaraz za nazwą serwera (np. smtp.acme.com:8200). Standardowym portem protokołu SMTP jest port 25.

- **Ustawienia dodatkowe** — pozwalają zdefiniować bardziej szczegółowe parametry:
 - o **Port lokalny** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port komunikacji SMTP.
 - o **Przetwarzanie kolejki** — określa zachowanie [skanera poczty e-mail](#) podczas przetwarzania wymaganych dotyczących wysyłania wiadomości e-mail:
 - Automatycznie — poczta wychodząca jest natychmiast dostarczana (wysyłana) do docelowego serwera pocztowego.
 - Ręczne — wiadomości są umieszczane w kolejce wiadomości wychodzących i wysyłane w późniejszym terminie.
 - o **Polaczenie** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (zwykle/SSL/domyslnie 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.
- **Serwer administracyjny** — zawiera numer portu serwera używanego do zwrotnego dostarczania raportów administracyjnych. Takie wiadomości są generowane, kiedy np. serwer docelowy jest niedostępny lub odrzuca wiadomość wychodzącą.
- **W sekcji** Ustawienia serwera SMTP klienta poczty e-mail znajdują się zalecenia dotyczące takiej konfiguracji klienta poczty, która umożliwi wysyłanie wiadomości do aktualnie modyfikowanego serwera. Informacje te stanowią podsumowanie odpowiednich parametrów określonych w całej konfiguracji AVG.

9.13. Ochrona rezydentna

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



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

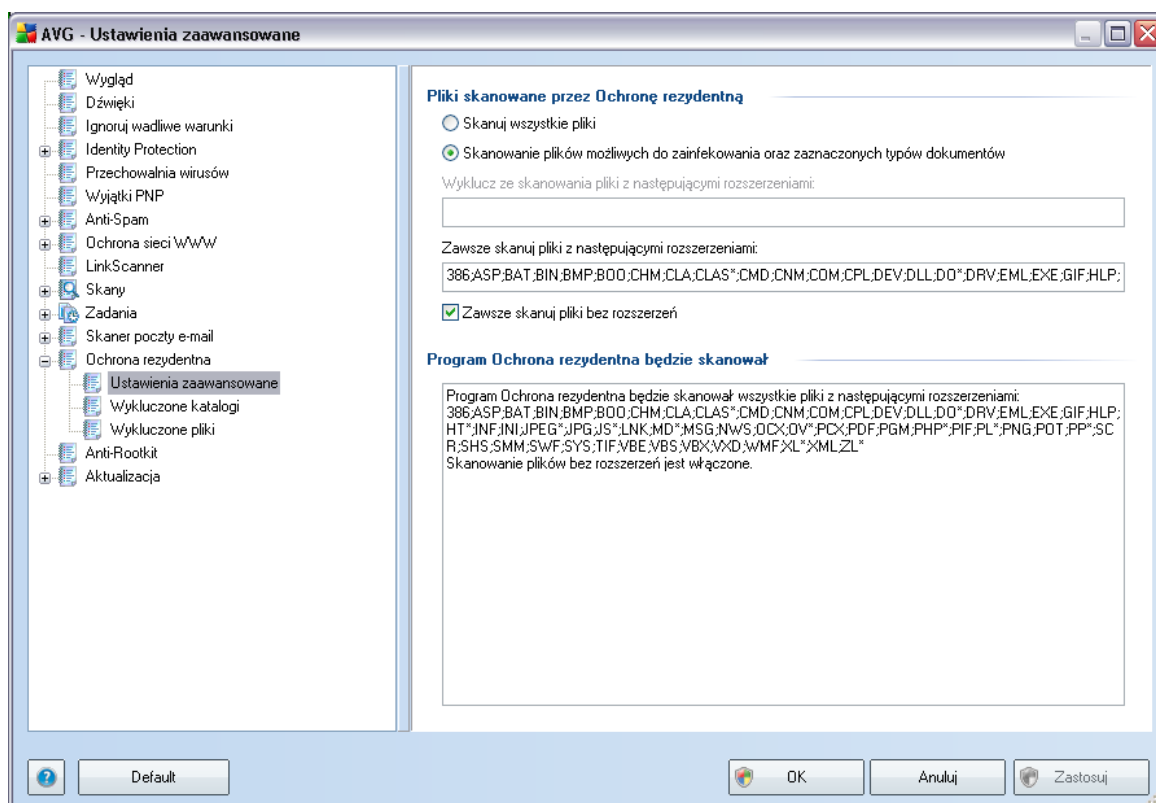
- **Skanuj w poszukiwaniu śledzących plików cookie** — parametr ten określa, czy w czasie skanowania mają być wykrywane pliki cookie. (Pliki cookie w protokole HTTP są używane do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencje dotyczące wyglądu witryny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

potencjalnie niechcianych programów (plików wykonywalnych, które mogą być oprogramowaniem szpiegującym lub reklamowym).

- **Skanuj pliki przy zamykaniu** — 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** — (domyślnie włączona)
- **Użyj heurystyki** — (domyślnie włączona) do wykrywania będzie używana heurystyka (dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej).
- **Automatyczne leczenie** — każda wykryta infekcja będzie automatycznie leczona (o ile jest to możliwe).

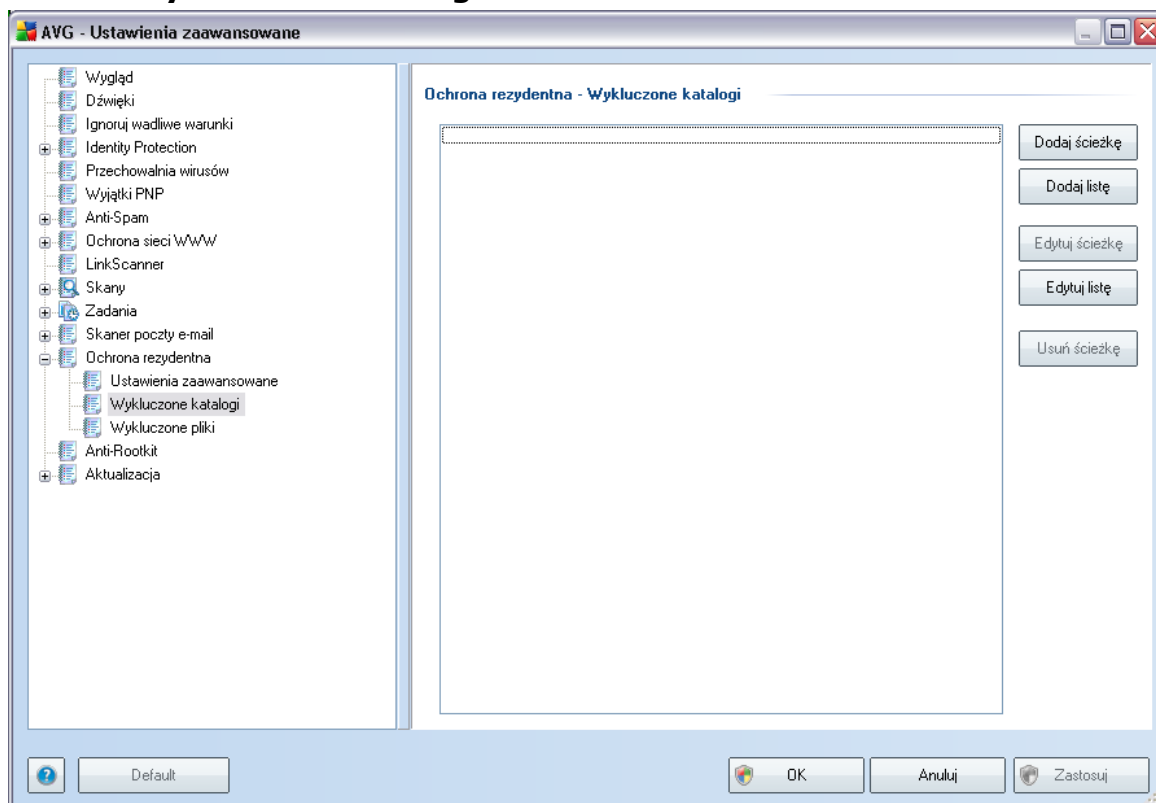
9.13.1. Ustawienia zaawansowane

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



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

9.13.2. Wykluczenia katalogów



Okno **Ochrona rezydentna — Wykluczone katalogi** pozwala definiować foldery, które mają być wykluczone ze skanowania przez [Ochronę Rezydentną](#).

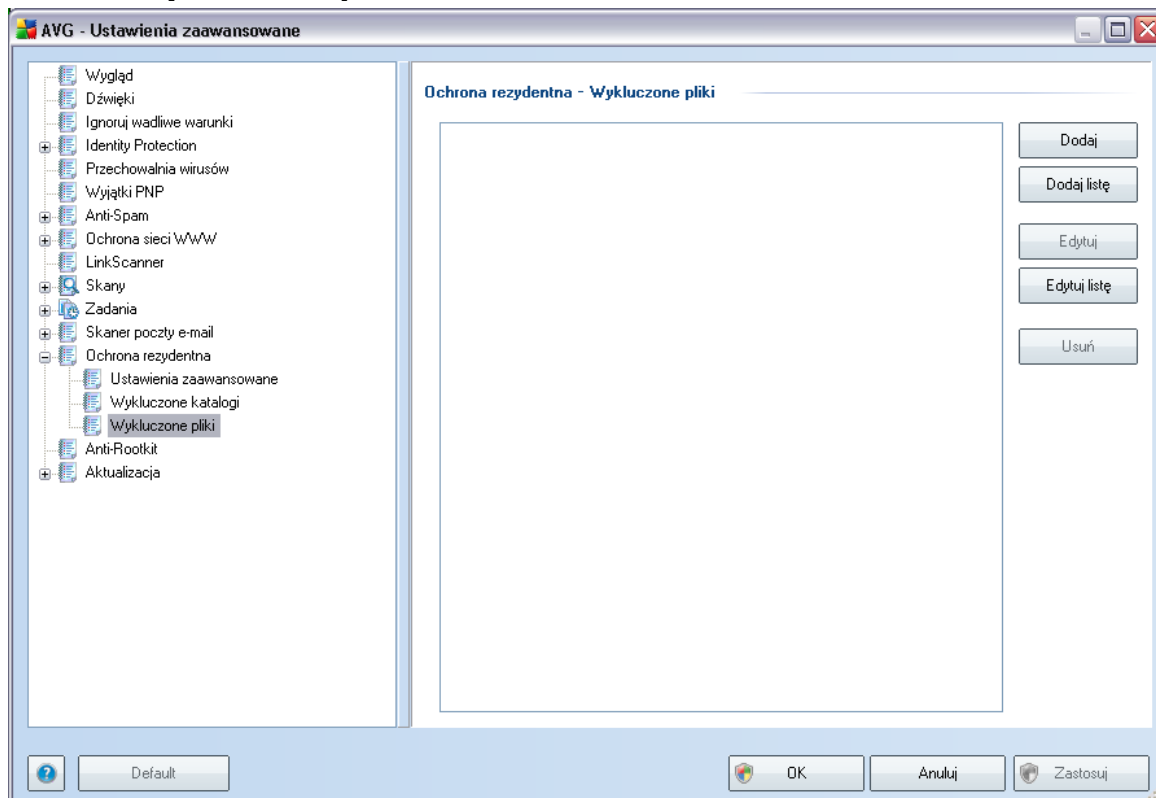
Jesli nie jest to konieczne, zdecydowanie zalecamy nie wykluczać żadnych katalogów ze skanowania!

W bieżącym oknie dostępne są następujące przyciski kontrolne:

- **Dodaj ścieżkę** — umożliwia określenie folderów, które mają zostać wykluczone ze skanowania, przez wybranie ich kolejno w drzewie obrazującym strukturę katalogów.
- **Dodaj listę** — umożliwia podanie listy katalogów, które zostaną wykluczone ze skanowania przez [Ochronę Rezydentną](#).
- **Edytuj ścieżkę** — umożliwia edycję ścieżki do wybranego folderu.

- **Edytuj listę** — umożliwia edycje listy folderów.
- **Usun ścieżkę** — umożliwia usunięcie z listy wybranego folderu.

9.13.3. Wykluczone pliki



Okno dialogowe **Ochrona rezydentna — wykluczone pliki** zachowuje się w taki sam sposób co poprzednio opisane okno **Ochrona rezydentna — wykluczone katalogi**, ale zamiast folderów można w nim określić pliki, które mają zostać wykluczone ze skanowania przez **Ochronę rezydentną**.

Jesli nie jest to konieczne, zdecydowanie zalecamy nie wylaczac zadnych katalogow ze skanowania!

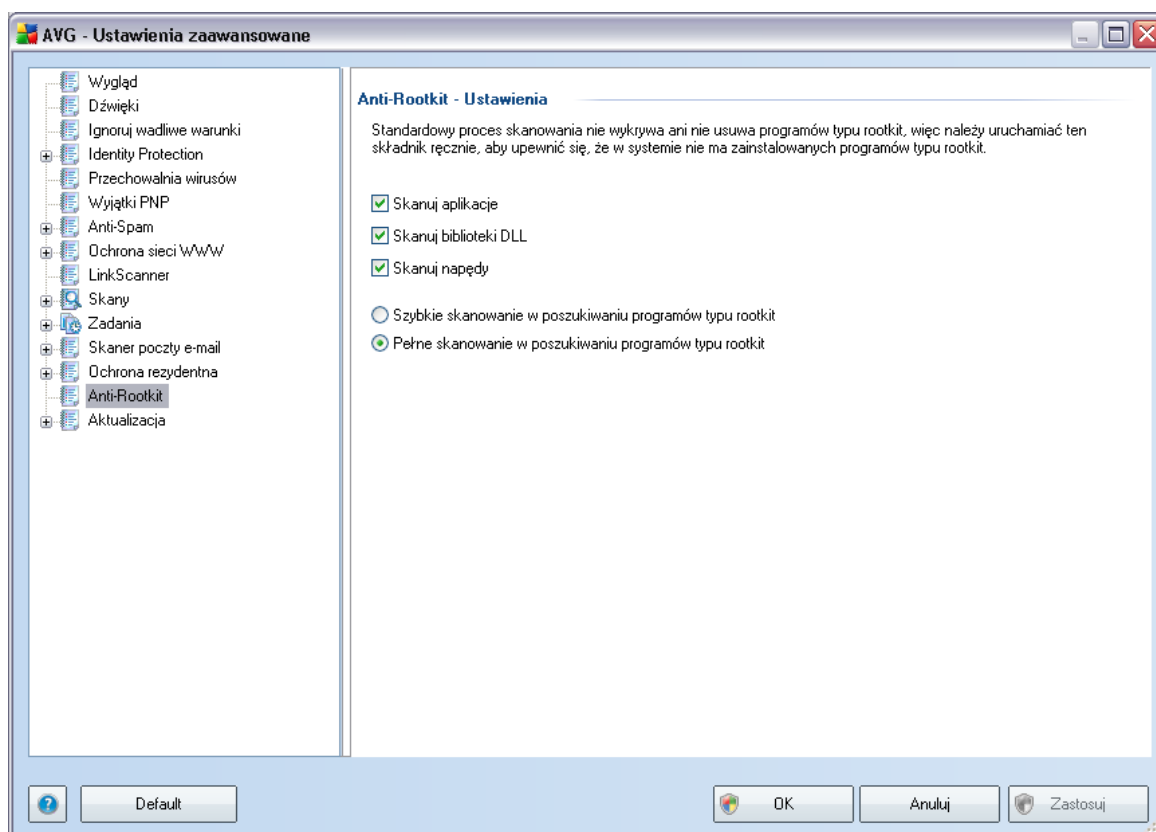
W bieżącym oknie dostępne są następujące przyciski kontrolne:

- **Dodaj ścieżkę** — umożliwia określenie katalogów, które mają zostać wykluczone ze skanowania, przez wybranie ich kolejno w drzewie nawigacyjnym dysku lokalnego.

- **Dodaj liste** — umożliwia podanie listy katalogów, które zostaną wykluczone ze skanowania przez [Ochronę Rezydentną](#).
- **Edytuj** — umożliwia edycję określonej ścieżki dostępu do wybranego folderu.
- **Edytuj liste** — umożliwia edycję listy folderów.
- **Usun** — umożliwia usunięcie z listy ścieżki dostępu do wybranego folderu.

9.14. Anti-Rootkit

W tym oknie dialogowym można edytować konfigurację składnika [Anti-Rootkit](#):



Wszystkie funkcje składnika [Anti-Rootkit](#) dostępne w tym oknie dialogowym można także edytować bezpośrednio w [interfejsie składnika Anti-Rootkit](#).

Należy zaznaczyć odpowiednie pola wyboru, aby określić obiekty, które mają być

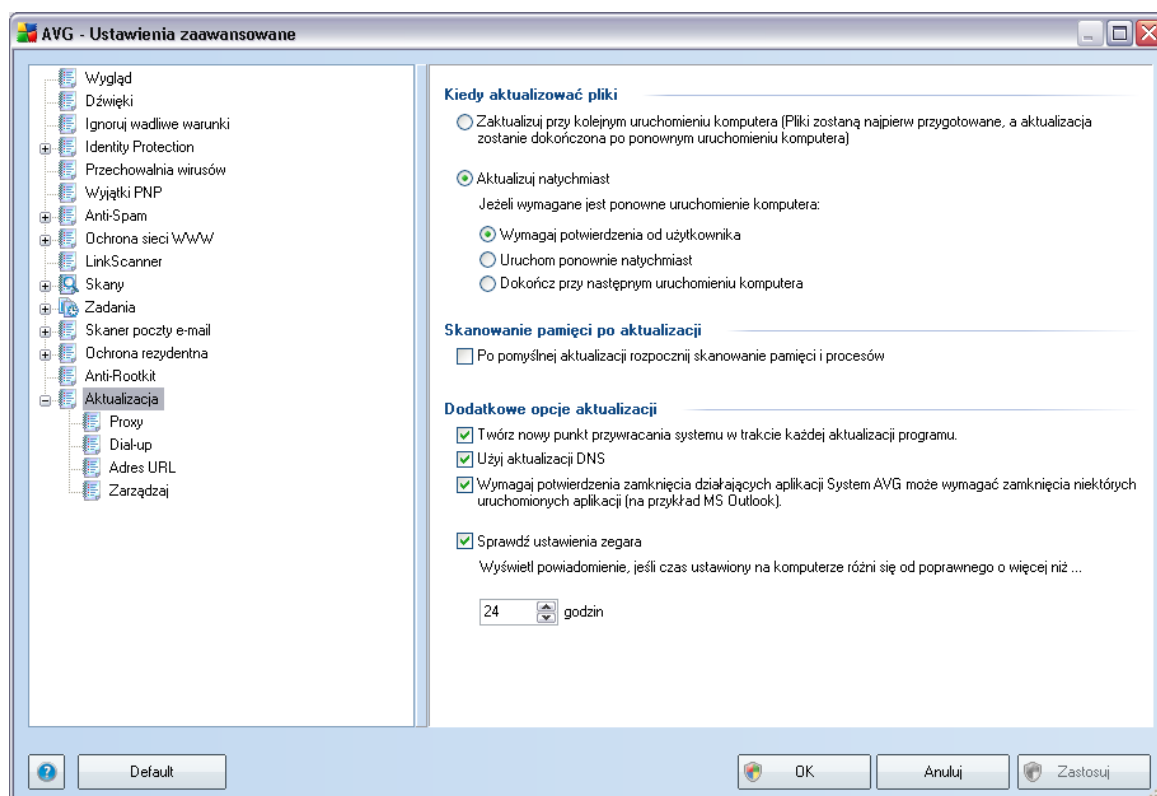
skanowane:

- **Skanuj aplikacje**
- **Skanuj biblioteki DLL**
- **Skanuj napedy**

Następnie należy wybrać tryb skanowania rootkitów:

- **Szybkie skanowanie w poszukiwaniu programów typu rootkit** — skanowany jest tylko folder systemowy (zwykle *c:\Windows*).
- **Pełne skanowanie w poszukiwaniu programów typu rootkit** — skanowane są wszystkie dostępne dyski, oprócz A: i B:.

9.15. Aktualizacja



Kliknięcie pozycji **Aktualizacja** otwiera nowe okno dialogowe, w którym można

okreslic ogólne parametry [aktualizacji AVG](#):

Kiedy aktualizować pliki

W tej sekcji można wybrać jedną z dwóch metod: zaplanowanie [aktualizacji](#) na najbliższy restart komputera lub uruchomienie [aktualizacji](#) natychmiast. Domyślnie wybrana jest opcja natychmiastowa, ponieważ zapewnia ona maksymalny poziom bezpieczeństwa. Zaplanowanie aktualizacji na kolejne uruchomienie komputera zaleca się tylko w przypadku, gdy komputer jest regularnie restartowany (co najmniej raz dziennie).

Przy pozostawieniu konfiguracji domyślnej (natychmiastowe uruchomienie), można określić warunki ewentualnego restartu komputera:

- **Wymagaj potwierdzenia od użytkownika** — 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** — zakończenie [aktualizacji](#) zostanie odłożone do najbliższego restartu komputera. Należy pamiętać, że opcja ta jest zalecana tylko w przypadku, gdy komputer jest regularnie uruchamiany (co najmniej raz dziennie).

Skanowanie pamięci po aktualizacji

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

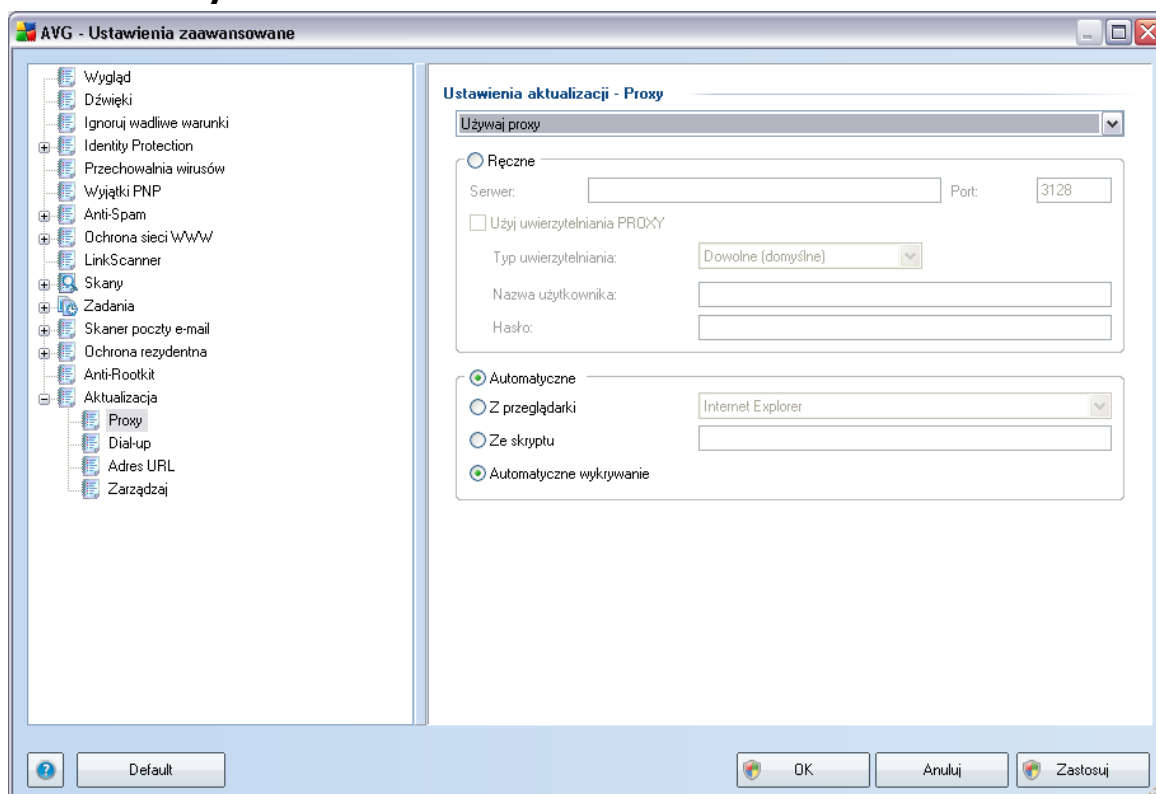
Dodatkowe opcje aktualizacji

- **Utwórz 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 niedoswiadczonego użytkownika! Na wszelki wypadek doradzamy pozostawić to pole zaznaczone.

- **Użyj aktualizacji DNS** — zaznacz to pole, aby potwierdzić, że chcesz używać metody wykrywania nowych aktualizacji, która ogranicza ilość danych przesyłanych między serwerem aktualizacyjnym a klientem AVG.
- **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 określona wartość.

9.15.1. Proxy



Serwer proxy jest samodzielnym serwerem lub uruchomiona na komputerze usługa

gwarantująca bezpieczniejsze połączenie internetowe. Zgodnie z określonymi w Twojej sieci zasadami, połączenie internetowe może odbywać się bezpośrednio lub poprzez serwer proxy. Można także zezwolic 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**
- **Spróbuj połączyć przy użyciu proxy, w razie niepowodzenia połącz bezpośrednio** (ustawienie domyślne)

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 **Recznie** aktywuje odpowiednią sekcję*) należy podać następujące informacje:

- **Serwer** — adres IP lub nazwa serwera.
- **Port** — numer portu umożliwiającego dostęp do internetu (*domyslnie 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

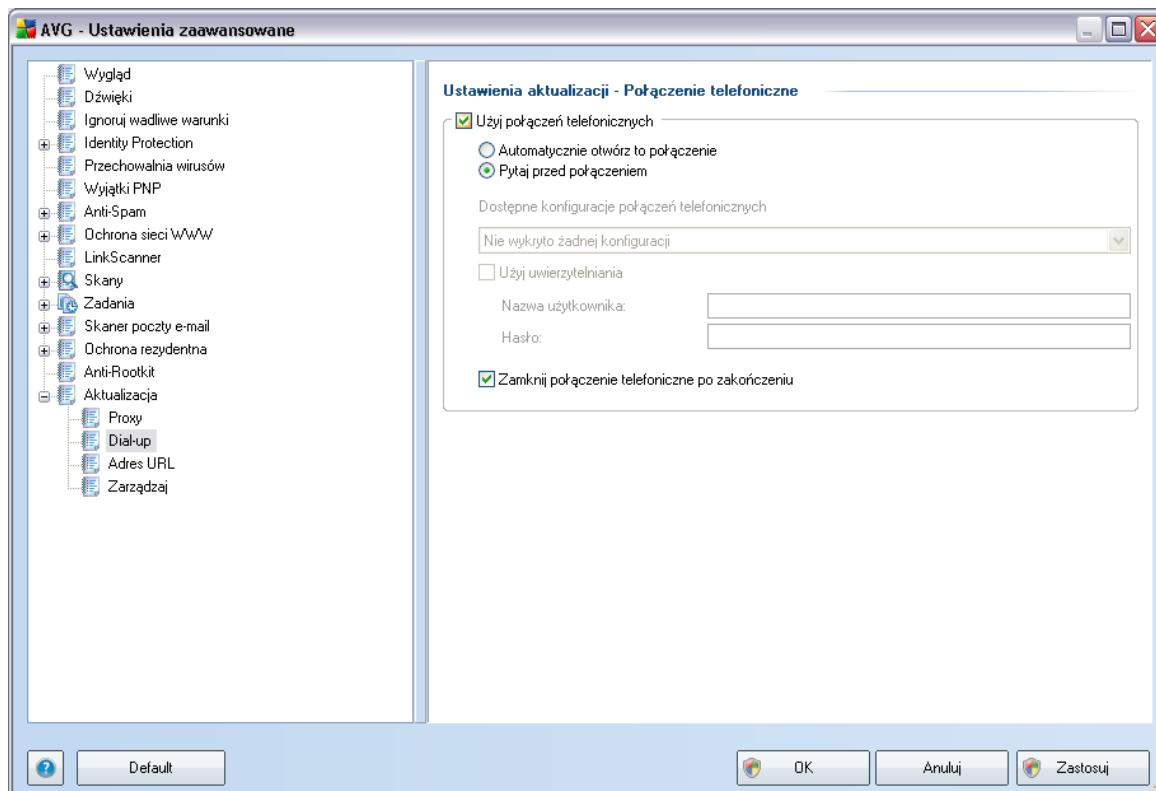
W przypadku wybrania konfiguracji automatycznej (zaznaczenie *opcji **Automatycznie** aktywuje odpowiednią sekcję*) należy wskazać, skąd ma zostać pobrana konfiguracja proxy:

- **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.

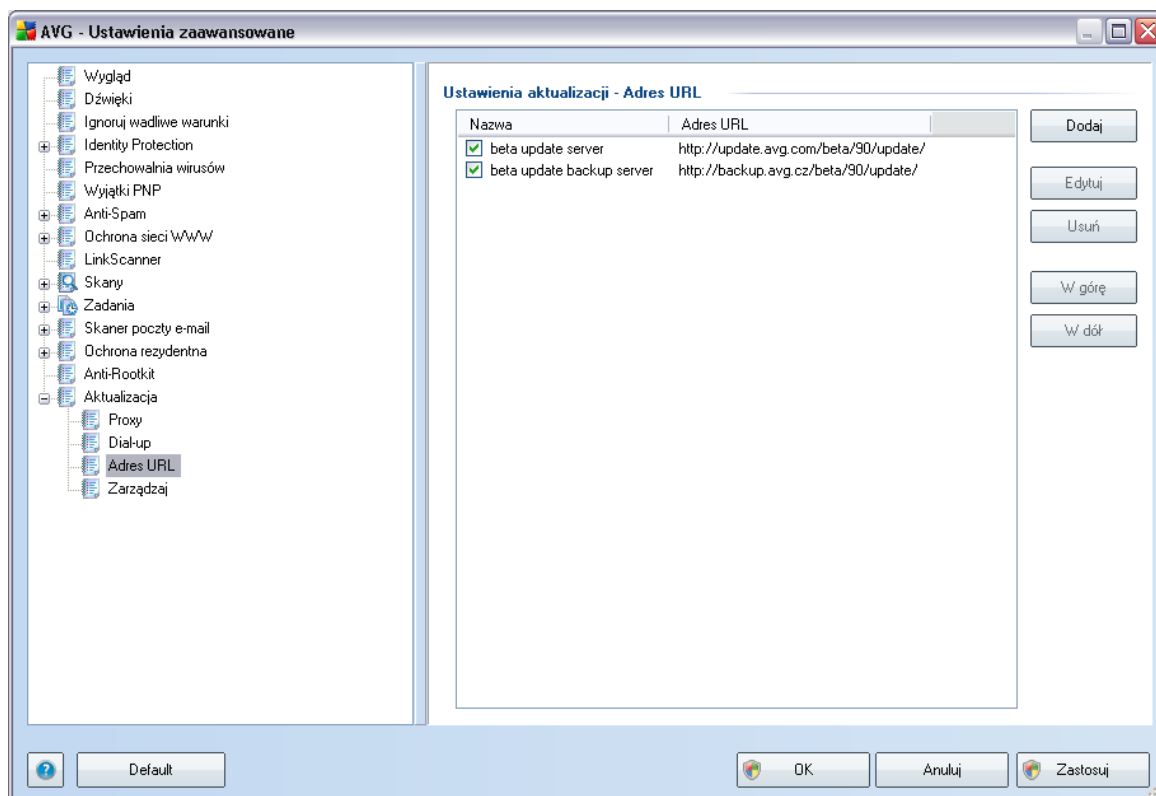
9.15.2. Połączenie telefoniczne



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**).

9.15.3. URL

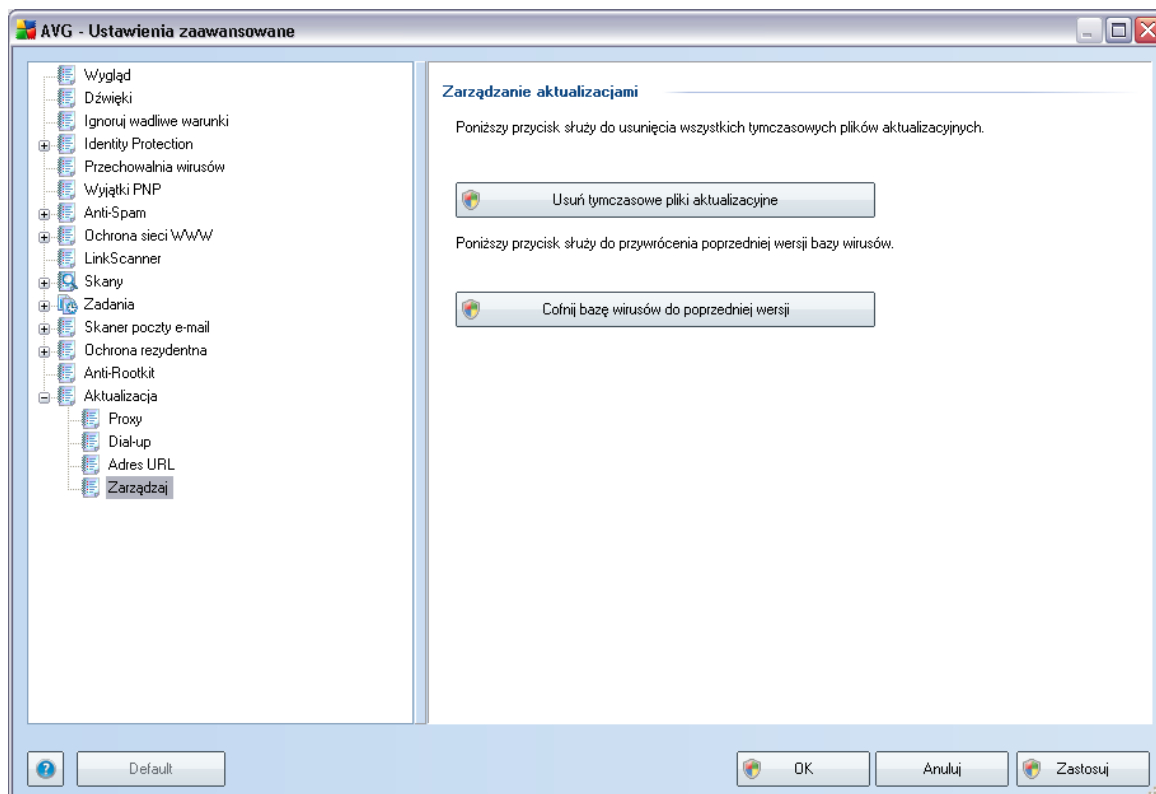


W oknie **URL** znajduje się lista adresów internetowych, z których można pobierać pliki aktualizacyjne. Listę i jej elementy można modyfikować za pomocą następujących przycisków kontrolnych:

- **Dodaj** — powoduje otwarcie okna dialogowego umożliwiającego określenie nowego adresu URL, który zostanie dodany do listy.
- **Edytuj** — powoduje otwarcie okna dialogowego umożliwiającego edycję parametrów wybranego adresu URL.
- **Usun** — 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.

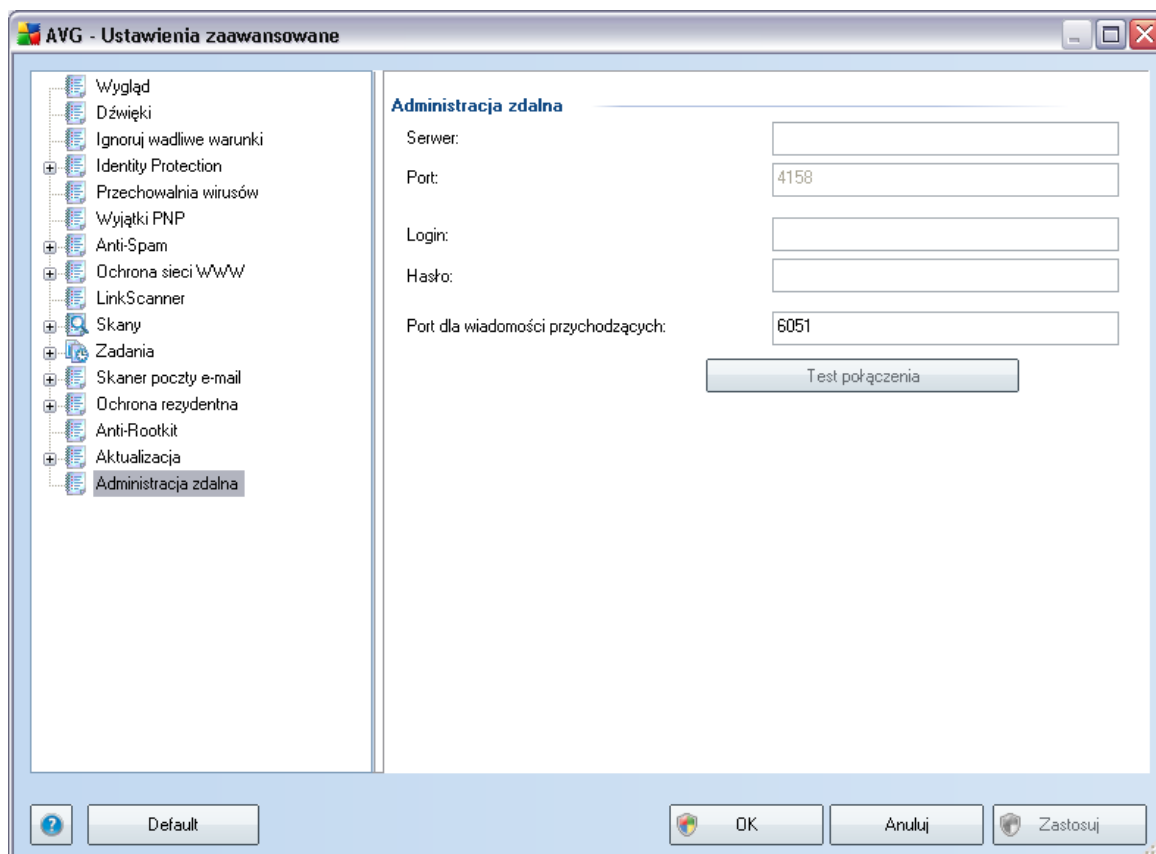
9.15.4. Zarządzaj

Okno dialogowe **Zarządzaj** zawiera dwa przyciski:



- **Usun tymczasowe pliki aktualizacyjne** — pozwala usunąć z dysku twardego wszystkie zbędne pliki aktualizacyjne (*sa one domyslnie 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*)

9.16. Administracja zdalna



Ustawienia **Administracji zdalnej** 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 a programem AVG Admin Server, należy podać w tym miejscu nazwę użytkownika. ...

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

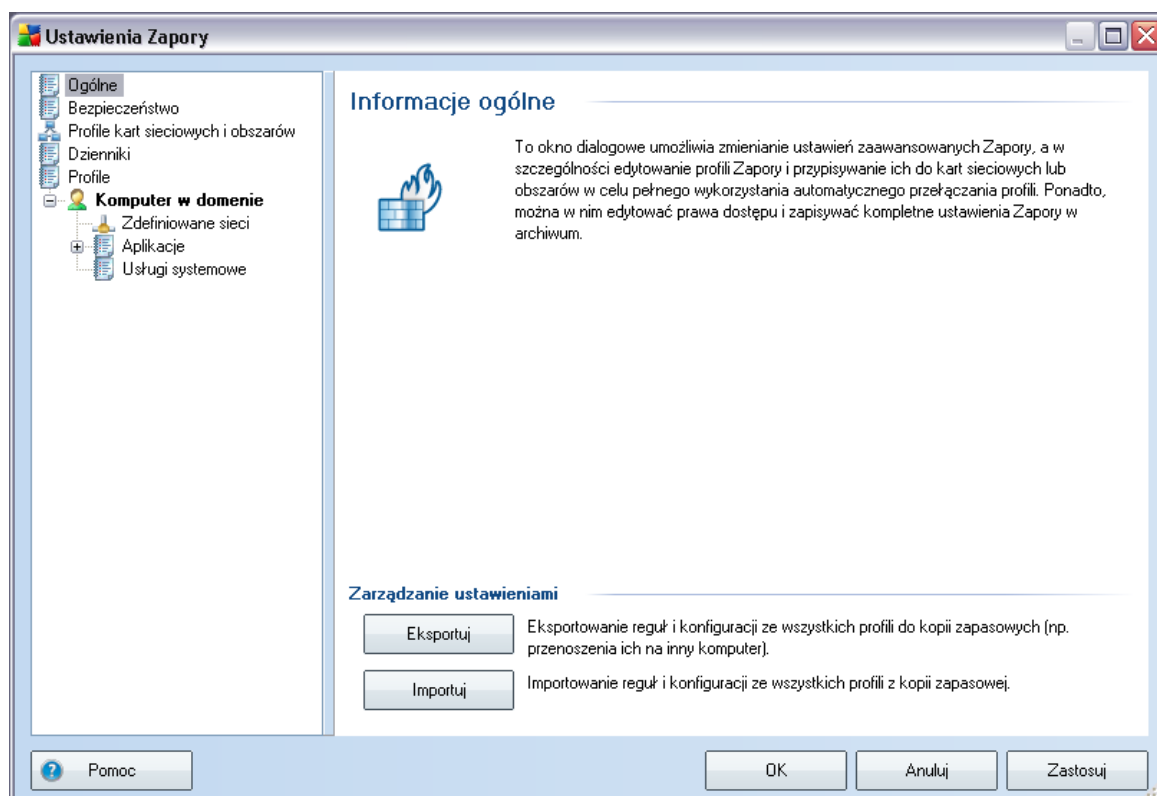
Przycisk **Testuj połączenie** pozwala sprawdzić, czy wszystkie powyższe dane są prawidłowe i zapewnia pomyślne połączenie z bazą danych DataCenter.

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

10. Ustawienia Zapory

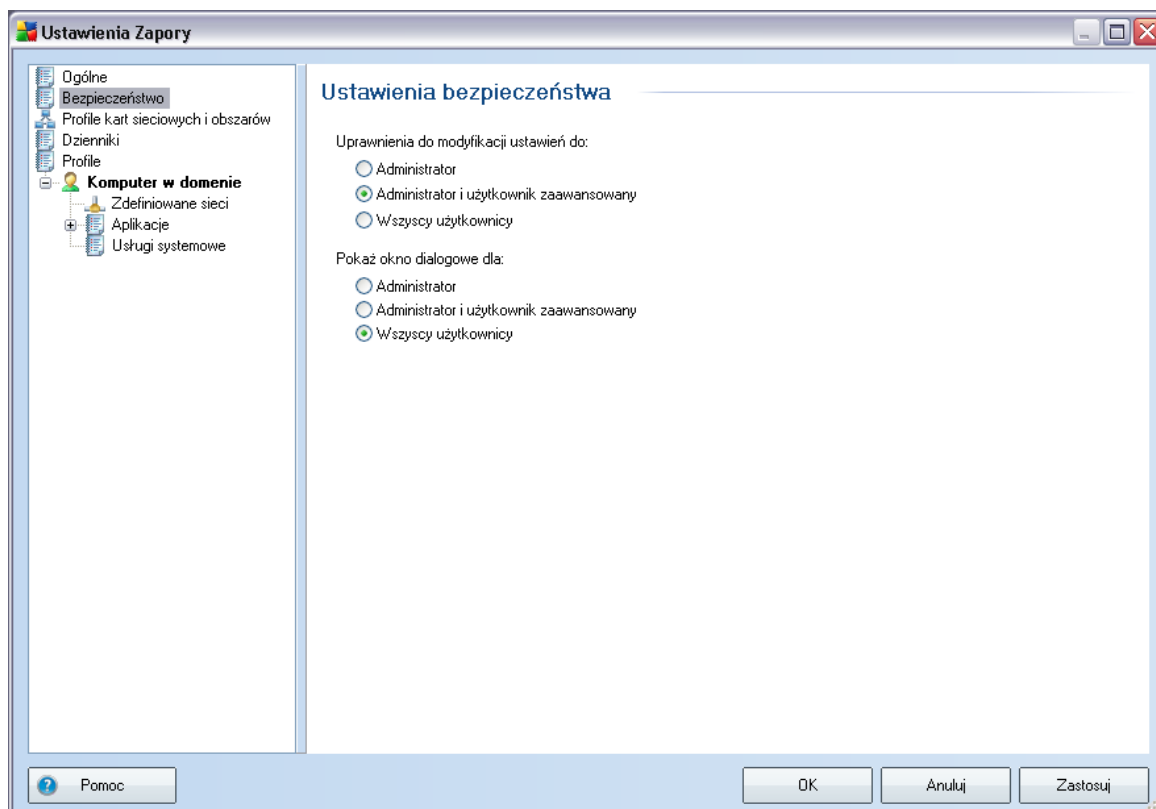
Konfiguracja **Zapory** otwierana jest w nowym oknie, gdzie w kilku sekcjach można określić nawet najbardziej zaawansowane parametry tego składnika. **Jednakże edycja zaawansowanej konfiguracji powinna być dokonywana jedynie przez ekspertów i doświadczonych użytkowników.**

10.1. Ogólne



W oknie **Informacje ogólne** można **wyeksportować / zaimportować konfiguracje** Zapory, tzn. wyeksportować zdefiniowane reguły i ustawienia **Zapory** do pliku kopii zapasowej lub też zaimportować do programu cały plik tego typu.

10.2. Bezpieczeństwo



W oknie **Ustawienia bezpieczeństwa** można zdefiniować ogólne reguły zachowania **Zapory** niezależnie od wybranego profilu:

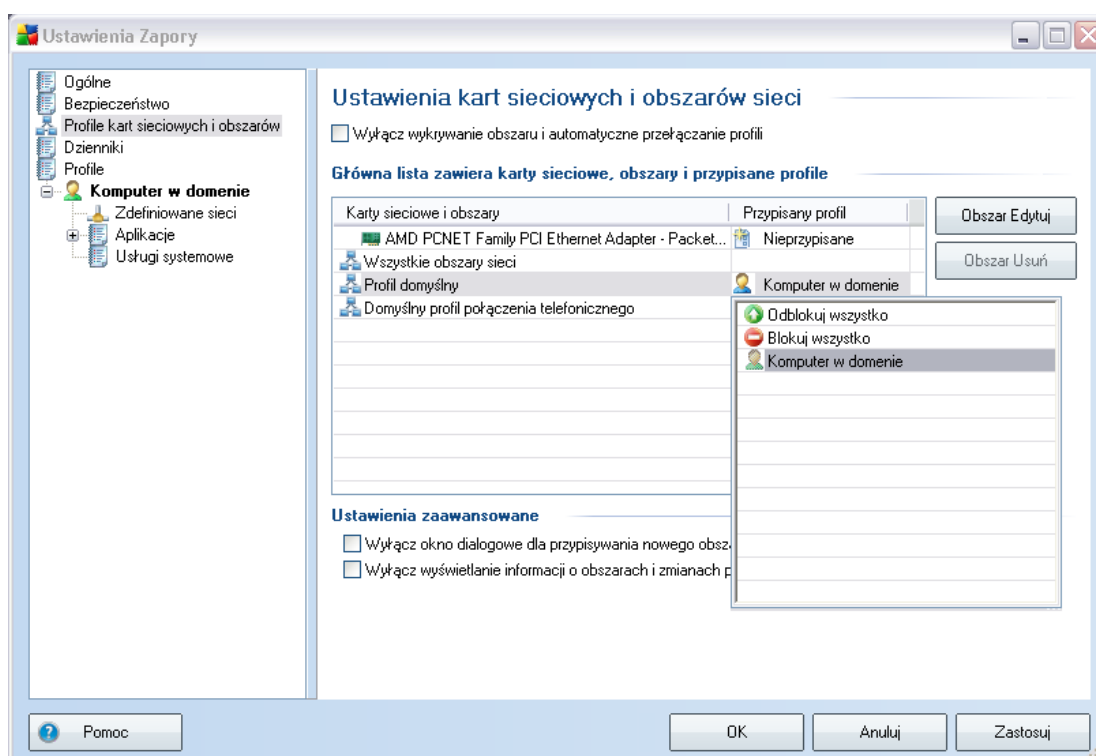
- **Pozwól modyfikować ustawienia:** — należy określić, kto może zmieniać konfigurację składnika **Zapora**.
- **Pokaż okno dialogowe:** — należy określić, komu można wyświetlać okna potwierdzeń Zapory (*okna dialogowe z prośbą o podjęcie decyzji w sytuacji nieobjętej żadną regułą **Zapory***).

W obu wypadkach można przypisać konkretne uprawnienie jednej z następujących grup użytkowników:

- o **Administratorom** — posiadają oni całkowitą kontrolę nad komputerem i możliwość przydzielania użytkownikom do grup z określonymi uprawnieniami.

- o **Administratorom i użytkownikom uprzywilejowanym** — administrator może przydzielić dowolnego użytkownika do uprzywilejowanej grupy (*Użytkownicy uprzywilejowani*) oraz określić jej członków.
- o **Wszyscy użytkownicy** — pozostali użytkownicy (nie przydzieleni do żadnej konkretnej grupy).

10.3. Profile kart sieciowych i obszarów



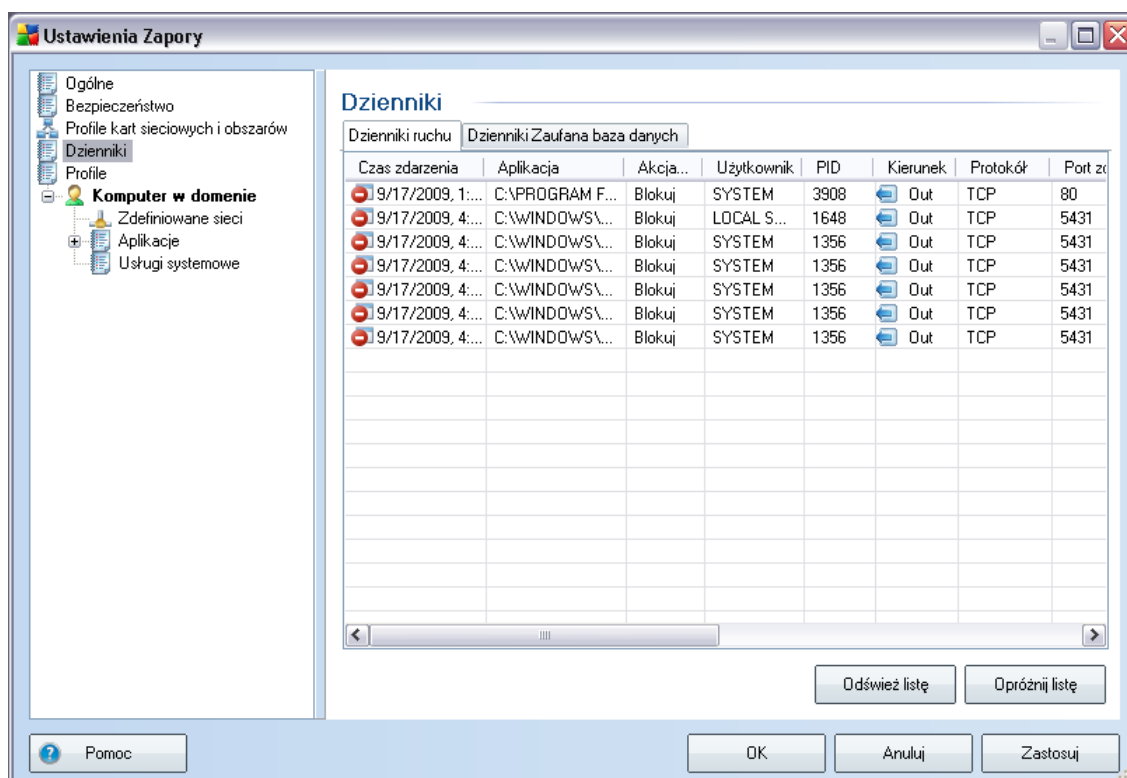
W oknie **Ustawienia kart sieciowych i obszarów** można edytować ustawienia związane z przypisywaniem zdefiniowanych profili do konkretnych kart i sieci.

- **Wyłącz wykrywanie obszaru i automatyczne przełączanie profili** — do każdej karty sieciowej (lub zdefiniowanej sieci) można przypisać jeden z profili Zapory. Jeśli nie chcesz tworzyć własnych, konkretnych profili, używany będzie jeden wspólny profil zdefiniowany na podstawie [typu komputera](#) i [sposobu połączenia z internetem](#) określonych podczas [procesu instalacji](#). Jeśli jednak postanowisz różnicować profile i przypisać je do konkretnych kart i obszarów, a następnie — z jakiegos powodu — zechcesz tymczasowo zmienić

to przypisanie, zaznacz opcje **Wylacz wykrywanie obszaru i automatyczne przełączanie profili**.

- **Lista kart sieciowych, obszarów i przypisanych profili** — na tej liście można znaleźć przegląd wykrytych kart i obszarów. Do każdego z nich można przypisać określony profil z menu zdefiniowanych profili. Aby otworzyć to menu, kliknij odpowiedni element na liście kart sieciowych i wybierz profil.
- **Ustawienia zaawansowane** — zaznaczenie odpowiednich opcji spowoduje wyłączenie komunikatów informacyjnych.

10.4. Dzienniki



Okno dialogowe **Dzienniki** umożliwia przegląd listy wszystkich działań podjętych przez **Zapora** oraz związanych z nią wydarzeń wraz ze szczegółowym opisem odpowiednich parametrów (*godzina zdarzenia, nazwa aplikacji, odpowiednia akcja dziennika, nazwa użytkownika, PID, kierunek komunikacji, typ protokołu, numery zdalnych i lokalnych portów itp.*) na dwóch następujących kartach:

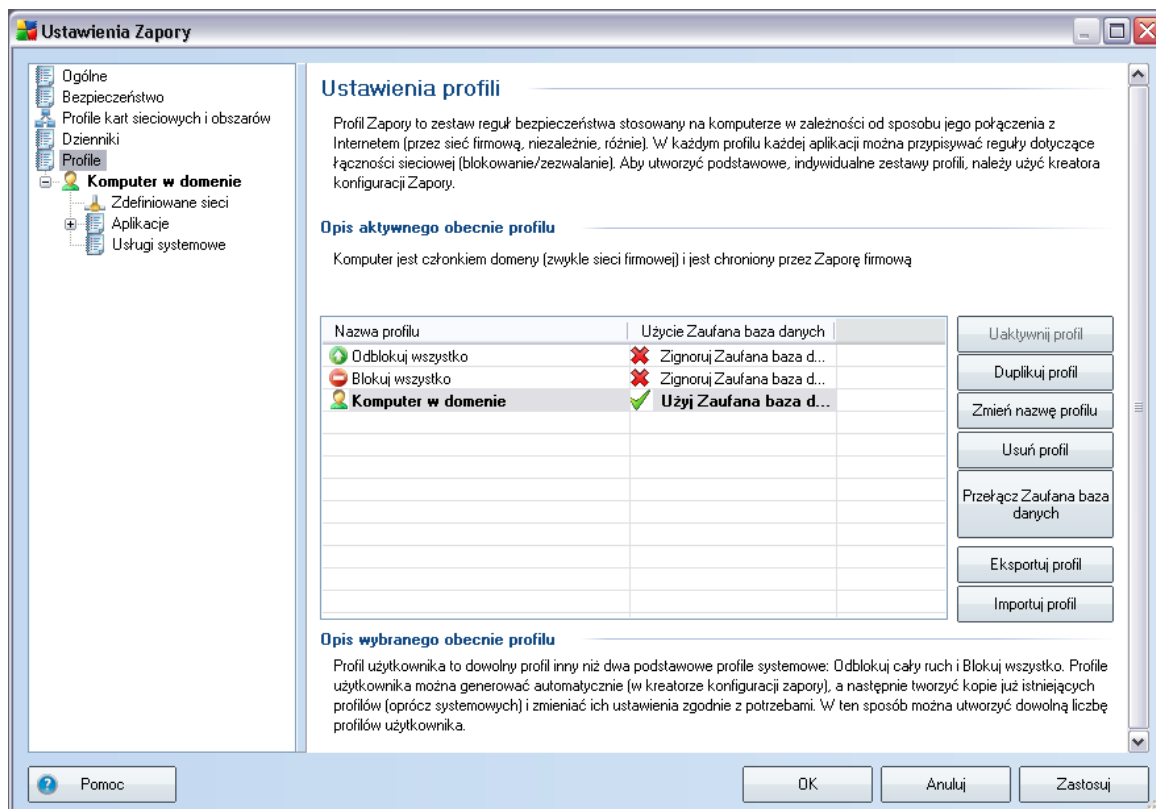
- **Dzienniki sieciowe** — zawiera informacje o aktywności wszystkich aplikacji, które próbowały połączyć się z siecią.
- **Dzienniki Trusted Database** — *Trusted Database* to wewnętrzna baza danych systemu AVG zbierająca informacje na temat certyfikowanych i zaufanych aplikacji, dla których komunikacja w trybie online jest zawsze dozwolona. Za pierwszym razem, kiedy nowa aplikacja próbuje się połączyć z siecią (np. gdy jeszcze nie została utworzona reguła zapory dla tej aplikacji), konieczna jest decyzja, czy zezwolic na komunikację sieciową. Najpierw system AVG przeszukuje bazę *Trusted Database*. Jeśli aplikacja znajduje się na liście, dostęp do sieci zostanie jej automatycznie umożliwiony. Dopiero wtedy, gdy w naszej bazie danych nie ma żadnych informacji na temat tej aplikacji, zostanie wyświetlone oddzielne okno dialogowe z pytaniem, czy dostęp do sieci powinien zostać odblokowany.

Przyciski kontrolne

- **Pomoc** — otwiera okno dialogowe z powiązаныmi tematami pomocy.
- **Odśwież listę** — wszystkie zarejestrowane parametry można uporządkować według wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) — wystarczy kliknąć odpowiedni nagłówek kolumny. Należy użyć przycisku **Odśwież listę**, aby zaktualizować aktualnie wyświetlane informacje.
- **Opróżnij listę** — pozwala usunąć wszystkie wpisy.

10.5. Profile

W oknie dialogowym **Ustawienia profilu** można znaleźć listę dostępnych profili.



Wszystkie [profile](#) (prócz systemowych) mogą być edytowane w tym oknie dialogowym przy użyciu następujących przycisków kontrolnych:

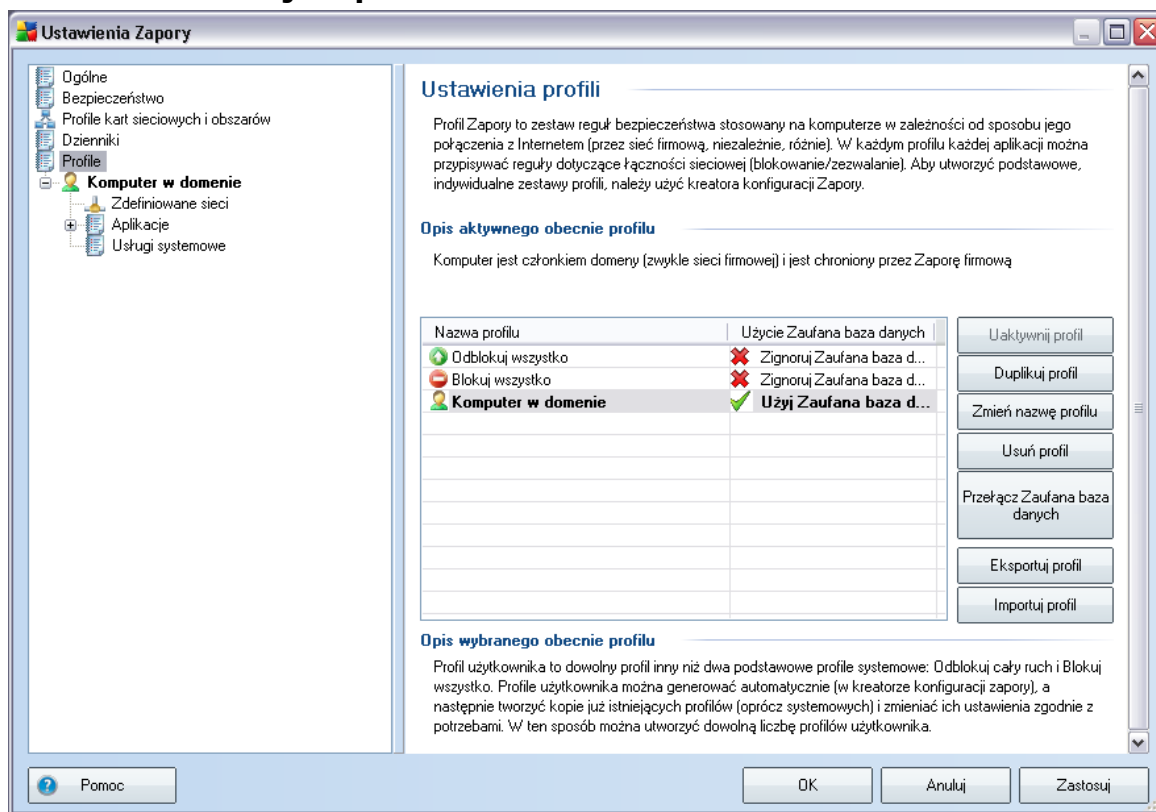
- **Uaktywnij profil** — przycisk ten ustawia wybrany profil jako aktywny, co oznacza, że konfiguracja wybranego profilu będzie używana przez **Zapora** do sterowania ruchem w sieci.
- **Duplikuj profil** — tworzy kopie wybranego profilu. Później będzie można przeprowadzić edycje i zmienić nazwę kopii, aby utworzyć nowy profil na podstawie istniejącego.
- **Zmień nazwę profilu** — umożliwia zdefiniowanie nowej nazwy dla wybranego profilu.

- **Usun profil** — usuwa wybrany profil z listy.
- **Włącz/wyłącz Trusted Database** — umożliwia danemu profilowi korzystanie z bazy *Trusted Database* (*Trusted Database to wewnętrzna baza danych AVG, zbierająca informacje na temat certyfikowanych i zaufanych aplikacji, którym bez obaw można zezwolic na połączenie z internetem.*)
- **Eksportuj profil** — zapisuje konfigurację wybranego profilu w pliku, którego będzie można użyć w przyszłości.
- **Importuj profil** — konfiguruje ustawienia wybranego profilu na podstawie danych zapisanych w pliku konfiguracyjnym.
- **Pomoc** — otwiera okno dialogowe z powiązaniem tematu pomocy.

W dolnej części okna dialogowego można znaleźć opis profilu wybranego z powyższej listy.

Menu nawigacyjne znajdujące się po lewej stronie zmienia odzwierciedla listę profili wyświetloną w oknie **Profile**. Każdy zdefiniowany profil tworzy jedną gałąź należącą do grupy **Profile**. Konkretnie profile można edytować w kolejnych oknach dialogowych (*identycznych dla wszystkich profili*).

10.5.1. Informacje o profilu



Okno dialogowe **Informacje o profilu** to pierwsze z okien sekcji, w której można edytować konfigurację wybranego profilu w osobnych oknach dialogowych dotyczących jego określonych parametrów.

- **Użyj dla tego profilu bazy Trusted Database** — (domyślnie włączone) te opcje należy zaznaczyć, aby aktywować bazy *Trusted Database* (czyli wewnętrzna baza danych systemu AVG zbierająca informacje o zaufanych i certyfikowanych aplikacjach korzystających z komunikacji online). Jeśli dla danej aplikacji nie ma jeszcze określonych reguł, konieczne jest sprawdzenie, czy aplikacja może uzyskać dostęp do sieci. System AVG przeszukuje najpierw bazy *Trusted Database* i jeżeli dana aplikacja jest na liście, zostanie uznana za bezpieczną i będzie jej umożliwiona komunikacja poprzez sieć. W innym przypadku zostanie wyświetlone zapytanie, czy dana aplikacja powinna uzyskać dostęp do internetu) dla określonego profilu.
- **Włącz obsługę sieci maszyn wirtualnych** — (domyślnie wyłączona) zaznaczenie tej pozycji pozwala maszynom wirtualnym VMware łączyć się

bezpośrednio z sieci.

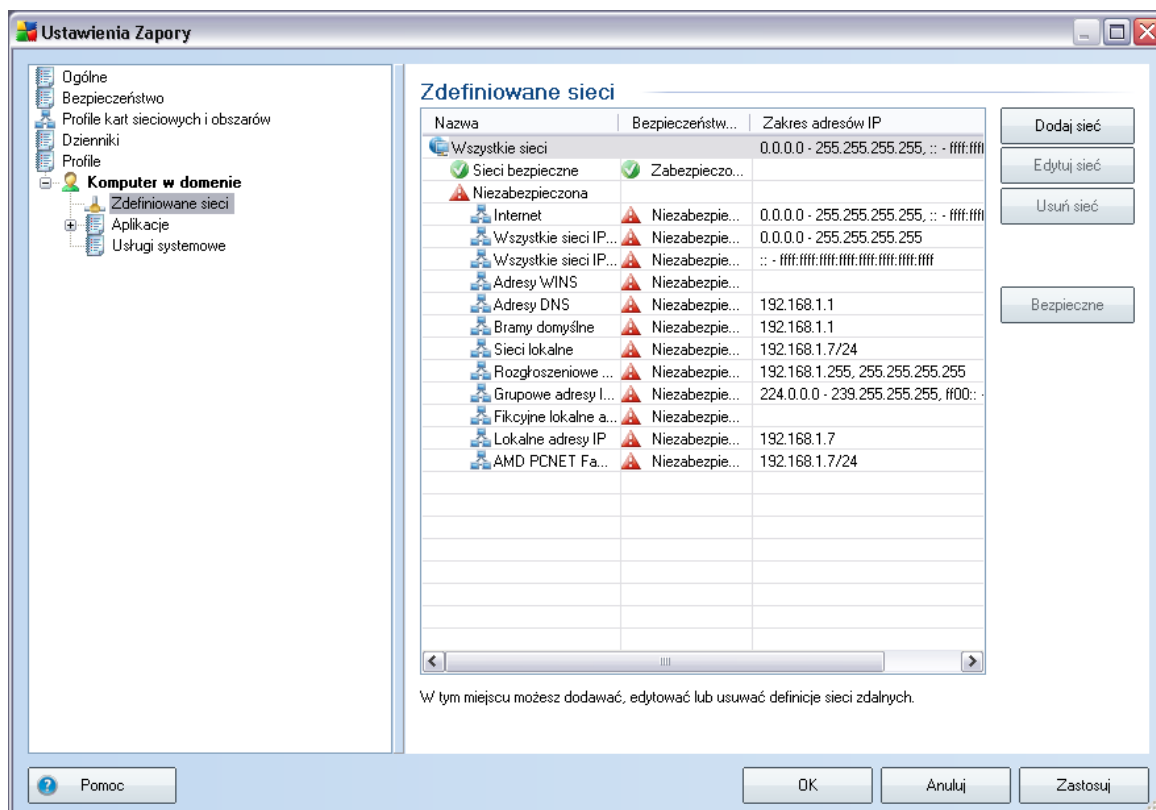
- **Użyj analizy behawioralnej przy ocenie ruchu sieciowego** — (domyślnie włączone) zaznaczenie tej opcji pozwala [Zaporze](#) na korzystanie z funkcji składnika [LinkScanner](#) podczas oceniania aplikacji — [LinkScanner](#) umożliwia stwierdzenie, czy aplikacja wykazuje jakiegokolwiek podejrzane zachowania, czy też można jej zaufać i zezwolic na komunikację online.

Ustawienia trybu gry

W sekcji **Ustawienia trybu gry** można określić czy komunikaty [Zapory](#) mają być wyświetlane nawet podczas działania aplikacji pełnoekranowych (*sa to na ogół gry, ale dotyczy to również wszelkich innych aplikacji, takich jak np. prezentacje PPT*). Komunikaty informacyjne mogą być w pewnym stopniu irytujące.

Jeśli zostanie zaznaczona opcja **Wyłącz powiadomienia Zapory w czasie gry**, z menu rozwijanego znajdującego się poniżej należy wybrać akcję, która ma podjąć Zaporę, gdy nowa aplikacja spróbuje nawiązać połączenie z siecią (*aby nie wyświetlać komunikatu z pytaniem o dostęp*). Wszystkie takie aplikacje mogą być odblokowane lub zablokowane.

10.5.2. Zdefiniowane sieci

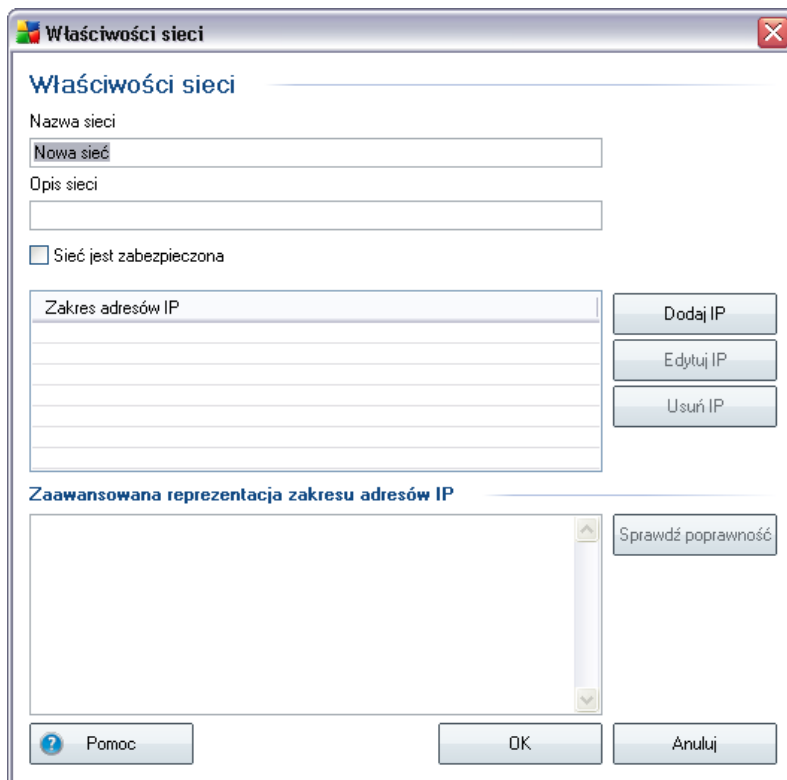


Okno **Zdefiniowane sieci** zawiera listę wszystkich sieci, z którymi połączony jest Twój komputer. Dla każdej wykrytej sieci wyświetlane są następujące informacje:

- **Sieci** — lista nazw wszystkich sieci, do których podłączony jest komputer.
- **Bezpieczeństwo sieci** — domyślnie wszystkie sieci uważane są za niebezpieczne i tylko w przypadku pewności, że dana sieć (i odpowiednia karta sieciowa) jest godna zaufania, można przypisać jej takie ustawienie (w tym celu należy kliknąć na liście pozycję odpowiadającą tej sieci i wybrać z menu kontekstowego opcję *Zabezpieczona*, bądź kliknąć przycisk *Bezpieczne*). Wszystkie bezpieczne karty sieciowe i odpowiadające im sieci zostaną wzięte pod uwagę przy przyznawaniu dostępu aplikacjom, dla których zastosowano regułę **Pozwól bezpiecznym**
- **Zakres adresów IP** — każda sieć zostanie automatycznie wykryta i określona w formie zakresu adresów IP

Przyciski kontrolne

- **Dodaj sieć** — otwiera okno **Właściwości sieci**, w którym można edytować parametry nowo zdefiniowanej sieci.

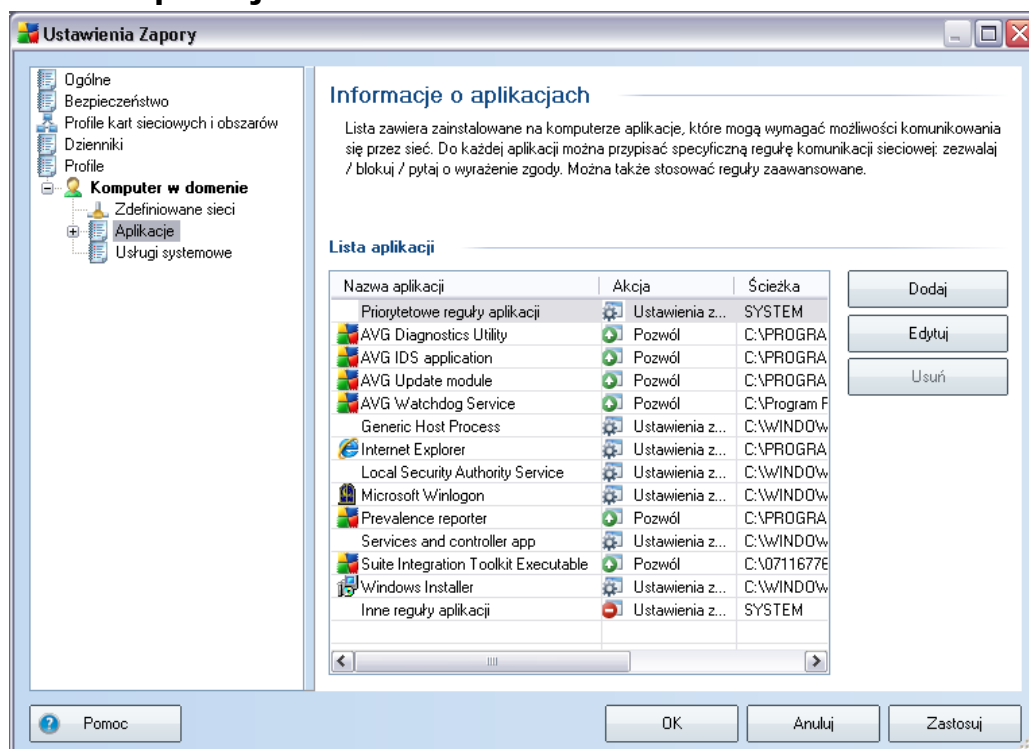


Należy wówczas określić **Nazwę sieci**, podać **Opis sieci** i zdecydować, czy jest zabezpieczona. Adres sieci może być określony ręcznie w odrębnym oknie dialogowym otwieranym za pomocą przycisku **Dodaj adres IP** (można też użyć przycisków **Edytuj adres IP/Usuń adres IP**). W oknie tym należy określić sieć, podając zakres adresów IP lub maskę.

W wypadku dużej liczby sieci, które mają być zdefiniowane jako części nowo utworzonej sieci, można użyć opcji **Zaawansowana reprezentacja zakresu adresów IP**: należy w tym celu wpisać listę wszystkich sieci do odpowiedniego pola tekstowego (*obsługiwane są wszystkie standardowe formaty*) i kliknąć przycisk **Sprawdź**, aby upewnić się, że format został rozpoznany. Następnie należy kliknąć przycisk **OK**, aby potwierdzić i zapisać dane.

- **Edytuj siec** — powoduje otwarcie okna dialogowego **Wlasciowosci sieci** (patrz wyzej). w którym można edytować parametry zdefiniowanej sieci (okno to jest identyczne jak podczas dodawania nowej sieci. Zobacz opis w poprzednim akapicie).
- **Usun siec** — usuwa wybrana siec z listy sieci.
- **Oznacz jako zabezpieczona** — domyslnie wszystkie sieci uważane są za niebezpieczne i tylko w przypadku pewności, że dana siec (i odpowiednia karta sieciowa) jest godna zaufania, można przypisać jej takie ustawienie.
- **Pomoc** — otwiera okno dialogowe z powiazanym tematem pomocy.

10.5.3. Aplikacje

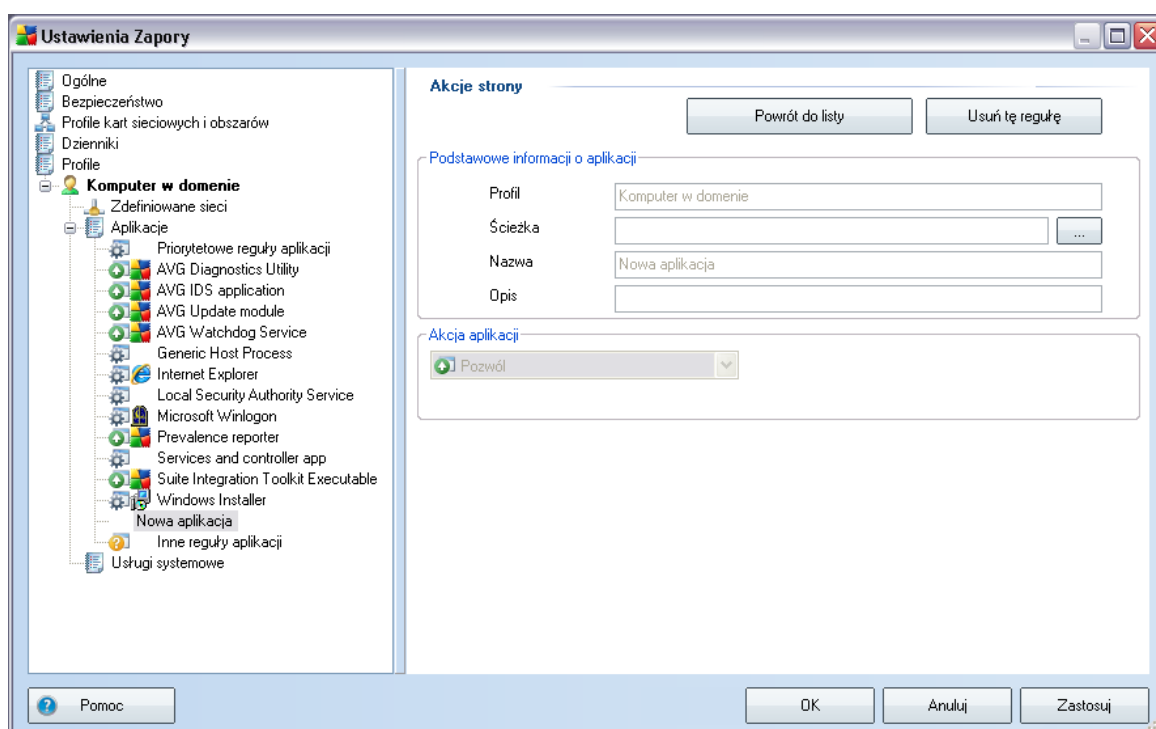


W oknie dialogowym **Informacje o aplikacjach** można znaleźć przegląd wszystkich aplikacji komunikujących się przez siec. Listę można edytować przy użyciu następujących przycisków kontrolnych:

- **Dodaj** — otwiera okno służące [do definiowania nowego zbioru reguł aplikacji.](#)

- **Edytuj** — otwiera okno służące do [edytowania istniejącego zbioru reguł aplikacji](#).
- **Usun** — usuwa wybrany zbiór reguł z listy.
- **Pomoc** — otwiera okno dialogowe z powiązonym tematem pomocy.

Okno dialogowe służące do dodania nowej reguły aplikacji otwierane jest za pomocą przycisku **Dodaj** w sekcji **Aplikacje** (w **ustawieniach Zapory**):



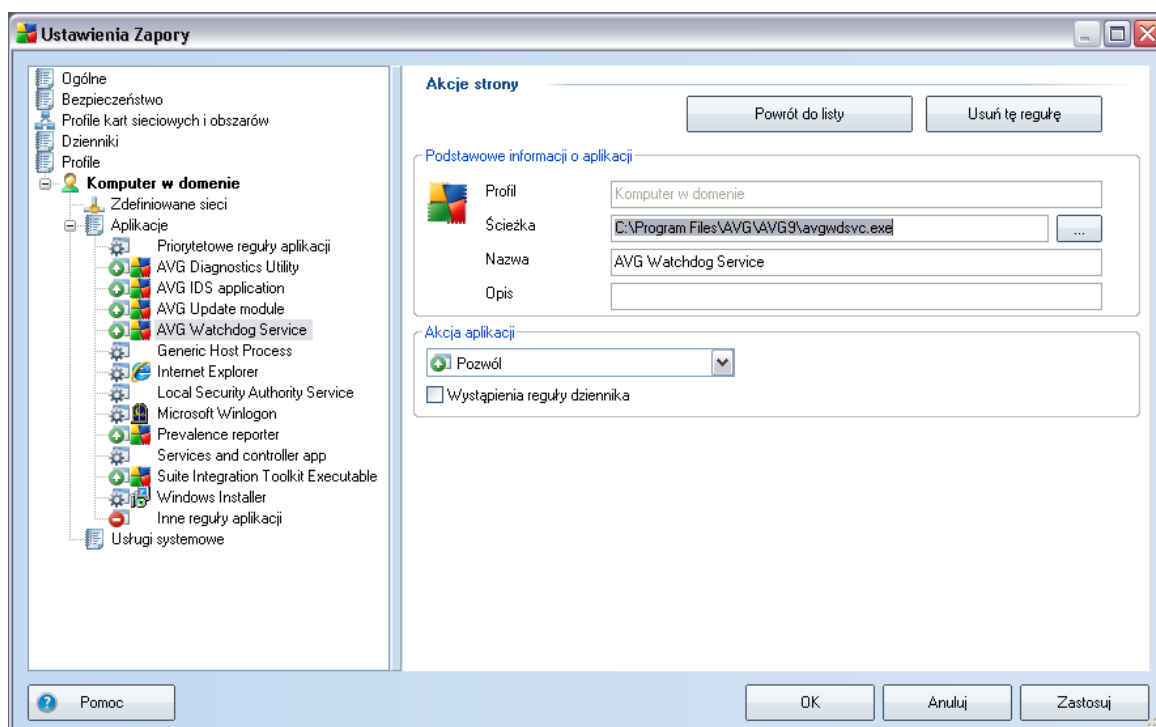
W oknie tym można zdefiniować:

- **Podstawowe informacje o aplikacji** — nazwa aplikacji, jej krótki opis i lokalizacja na dysku.
- **Akcja aplikacji** — z menu rozwijanego można wybrać regułę, która ma być stosowana do danej aplikacji.
 - **Ustawienia zaawansowane** — opcja ta umożliwia szczegółową edycję zbioru reguł obecnych w dolnej części okna dialogowego. *Opis tej sekcji*

znajduje sie w rozdziale [Edycja aplikacji](#).

- **Pozwól** — wszelkie próby nawiązania komunikacji przez tą aplikację będą dozwolone.
- **Pozwól bezpiecznym** — aplikacja będzie mogła komunikować się wyłącznie z bezpiecznymi sieciami (np. połączenia z chronioną siecią firmową będą dozwolone, natomiast komunikacja z internetem - zablokowana). Omówienie i opis bezpiecznych sieci znajduje się w oknie [Sieci](#).
- **Pytaj** — jeśli aplikacja podejmie próbę komunikacji przez sieć, zostanie wyświetlony monit pytający użytkownika o zgodę.
- **Blokuj** — wszelkie próby komunikacji podejmowane przez aplikację będą zablockowane.

Okno dialogowe do definiowania zbioru reguł aplikacji otwiera się za pomocą przycisku **Edytuj** w oknie dialogowym [Aplikacje](#) w [ustawieniach składowika Firewall](#):

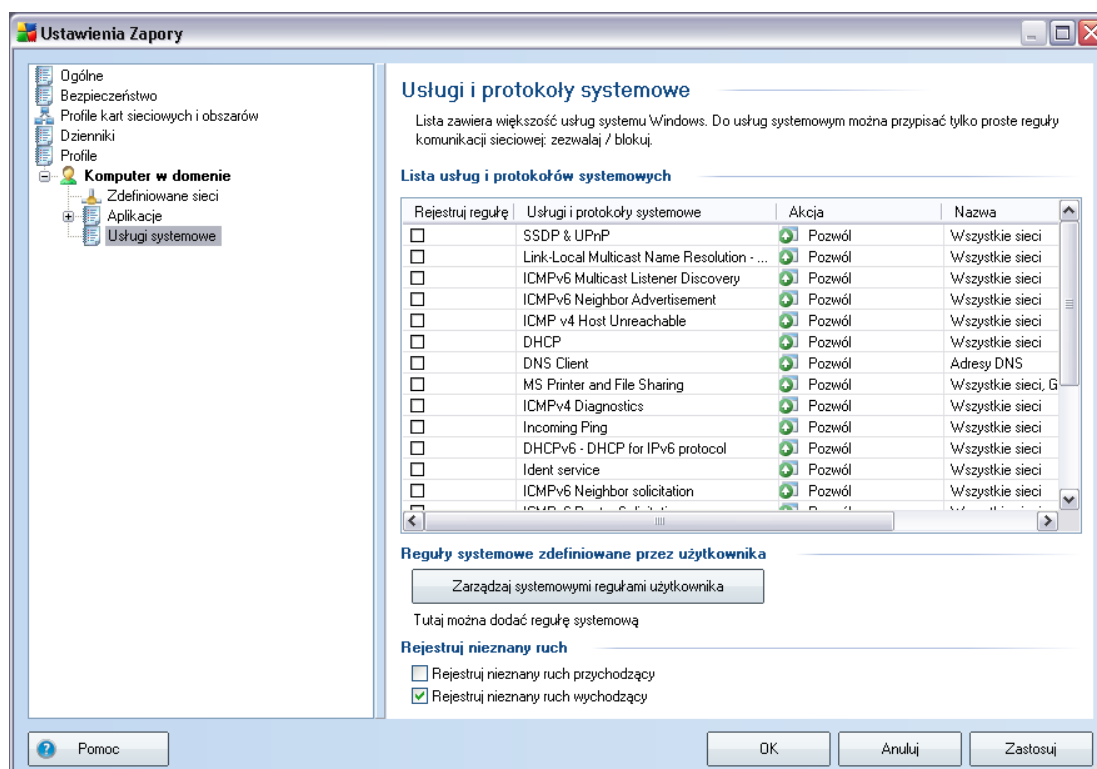


W oknie tym można edytować wszystkie parametry istniejącej aplikacji:

- **Podstawowe informacje o aplikacji** — nazwa aplikacji, jej krótki opis i lokalizacja na dysku.
- **Akcja aplikacji** — z menu rozwijanego można wybrać regułę, która ma być stosowana do danej aplikacji.
 - **Ustawienia zaawansowane** — opcja ta umożliwia szczegółową edycję reguły w dolnej części okna.
 - **Pozwól** — wszelkie próby nawiązania komunikacji przez tę aplikację będą dozwolone.
 - **Pozwól bezpiecznym** — aplikacja będzie mogła komunikować się wyłącznie z bezpiecznymi sieciami (*np. połączenia z chronioną siecią firmową będą dozwolone, natomiast komunikacja z internetem - zablokowana*). Omówienie i opis bezpiecznych sieci znajduje się w oknie [Sieci](#).
 - **Pytaj** — jeśli aplikacja podejmie próbę komunikacji przez sieć, zostanie wyświetlony monit pytający użytkownika o zgodę.
 - **Blokuj** — wszelkie próby komunikacji podejmowane przez aplikację będą zablokowane.
- **Rejestruj stosowanie reguły** — należy zaznaczyć tę opcję, jeśli wszystkie akcje [Zapory](#) podejmowane w związku z daną aplikacją mają być rejestrowane w dzienniku. Wspomniane wpisy dziennika można znaleźć w oknie [Dzienniki](#)

10.5.4. Usługi systemowe

Wszelkie zmiany w konfiguracji usług i protokołów systemowych powinny być wprowadzane JEDYNIEM przez doświadczonych użytkowników.



Okno **Usługi i protokoły systemowe** zawiera przegląd usług i protokołów systemowych komunikujących się poprzez sieć. Poniżej znajdują się dwie opcje: należy je zaznaczyć, jeżeli chcesz, aby rejestrowano cały nieznaną ruch w obu kierunkach (*przychodzącym i wychodzącym*).

Przyciski kontrolne

- **Dodaj/Edytuj** — oba przyciski otwierają to samo okno, w którym można edytować parametry usługi systemowej. Przycisk **Dodaj** otwiera puste okno dialogowe w trybie podstawowym (*bez sekcji ustawień zaawansowanych, która można otworzyć, wybierając zaawansowane ustawienia akcji aplikacji*). Przycisk **Edytuj** otwiera to samo okno dialogowe wypełnione danymi dotyczącymi wybranej usługi systemowej.

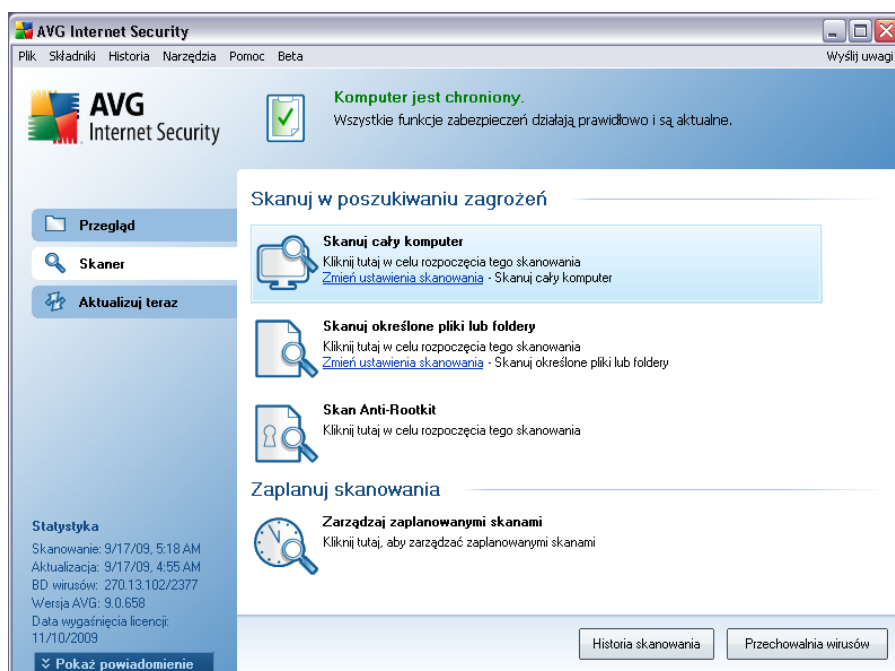
Wszelkie zmiany w konfiguracji usług i protokołów systemowych powinny

*byc wprowadzane **JEDYNIE** przez doświadczonych użytkowników.*

11. Skanowanie AVG

Skanowanie plików to podstawowa funkcja systemu **AVG 9 Internet Security**. Możliwe jest uruchamianie testów na zadanie lub [planowanie ich okresowego przeprowadzania](#) o odpowiednich porach.

11.1. Interfejs skanowania



Interfejs skanera AVG dostępny jest za pośrednictwem linku [Skaner](#). 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 zadanie lub według utworzonego harmonogramu:
 - o [Skan całego komputera](#)
 - o [Skan określonych plików lub folderów](#)
 - o [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.
- **Przechowywanie wirusów** — otwiera nowe okno z zawartością [Przechowywanie wirusów](#), w której izolowane są wykryte infekcje.

11.2. Wstępnie zdefiniowane testy

Jedną z głównych funkcji aplikacji **AVG 9 Internet Security** jest skanowanie na zadanie. Testy na zadanie 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.

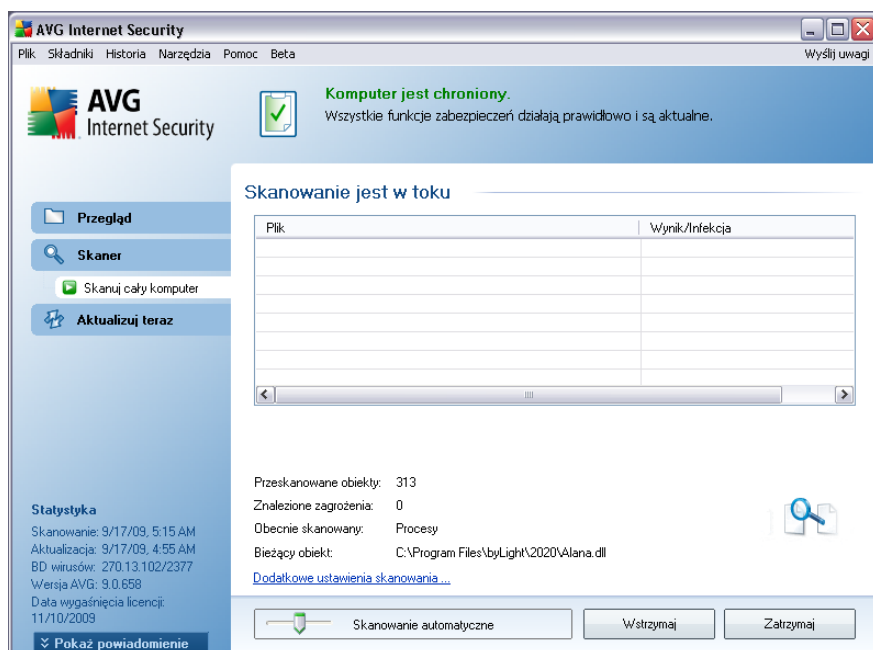
System **AVG 9 Internet Security** oferuje dwa typy skanowania zdefiniowane wstępnie przez AVG:

11.2.1. Skan całego komputera

Skanuj cały komputer — 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 [Przechowywanie wirusów](#). Skanowanie całego komputera powinno być regularnie przeprowadzane co najmniej raz na tydzień.

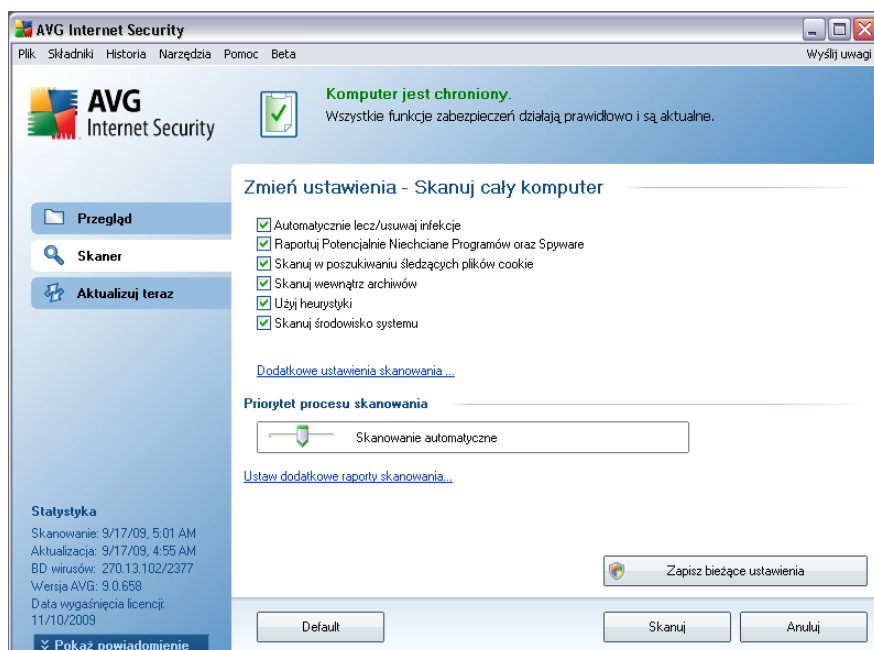
Uruchamianie skanowania

Skanowanie całego komputera można uruchomić bezpośrednio z poziomu [interfejsu skanera](#), klikając ikonę odpowiedniego testu. 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**).

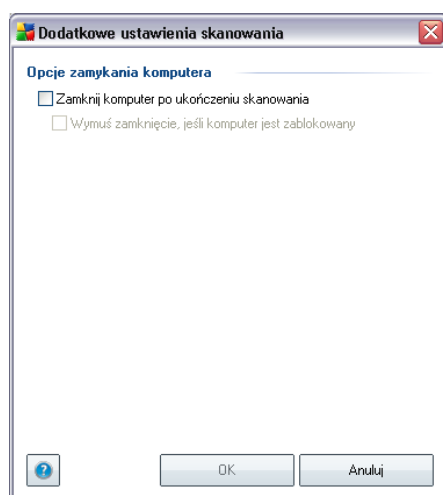


Edycja konfiguracji skanowania

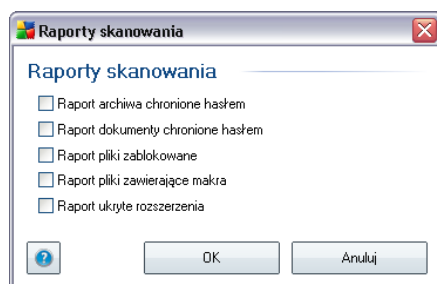
Zdefiniowane wstępne ustawienia domyślne testu **Skan całego komputera** można edytować. Kliknięcie linku **Zmień ustawienia skanowania** powoduje otwarcie okna dialogowego **Zmień ustawienia skanu całego komputera**. **Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!**



- **Parametry skanowania** — na liście parametrów skanowania można włączyć/wyłączyć określone parametry w zależności od potrzeb. Większość parametrów jest domyślnie włączona i automatycznie używana podczas skanowania.
- **Dodatkowe ustawienia skanowania** — link do okna dialogowego **Dodatkowe ustawienia skanowania**, w którym można określić następujące parametry:



- o **Opcje wyłączenia komputera** — określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie pierwszej opcji (**Zamknij komputer po ukończeniu skanowania**) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet wtedy, gdy jest zablokowany (**Wymus zamknięcie, jeśli komputer jest zablokowany**).
- o **Zdefiniuj typy plików do skanowania** — należy zdecydować, które z poniższych elementów mają być skanowane:
 - **Wszystkie typy plików** z opcja zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, który nie powinny być skanowane; LUB
 - **Wybrane typy plików** — skanowane będą 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 zostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliki 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. Domyślnie ustawiony jest priorytet średni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkość skanowania, jak i wykorzystanie zasobów systemowych. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).
- **Ustaw dodatkowe raporty skanowania** — link ten pozwala otworzyć nowe okno dialogowe **Raporty skanowania**, w którym można określić elementy lub zdarzenia, które mają być zgłaszane:



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.

11.2.2. Skan określonych plików lub folderów

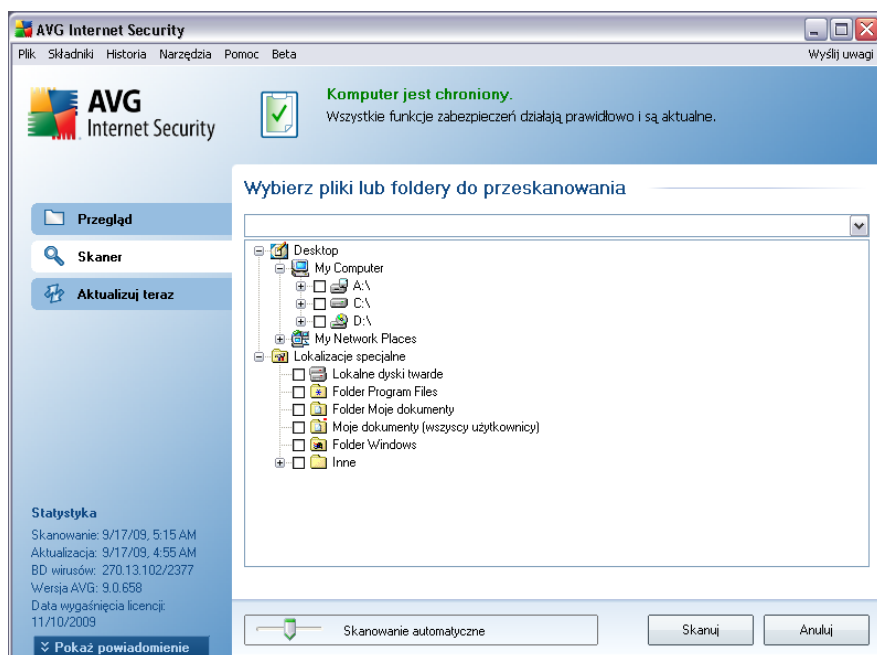
Skan określonych plików lub folderów — skanowane są tylko wskazane obszary komputera (wybrane foldery, a także dyski twarde, pamięci flash, CD itd.). Postępowanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu całego komputera: każdy znaleziony wirus jest leczony lub przenoszony do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

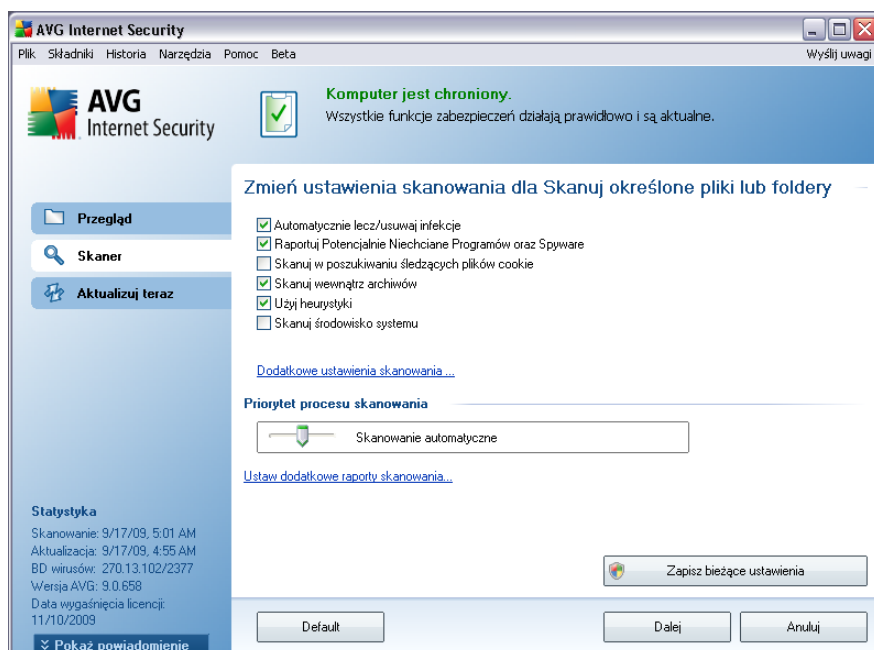
Mozna także przeskanować wybrany folder, wykluczając jednocześnie ze skanowania wszystkie jego podfoldery: należy wprowadzić znak minus „-” przed jego nazwą w wygenerowanej ścieżce (*patrz ilustracja*). Aby wykluczyć cały folder ze skanowania, należy użyć parametru „!”.

Na koniec, aby uruchomić skanowanie, należy nacisnąć przycisk **Rozpocznij skanowanie**; proces skanowania jest w zasadzie taki sam jak [skanowanie całego komputera](#).

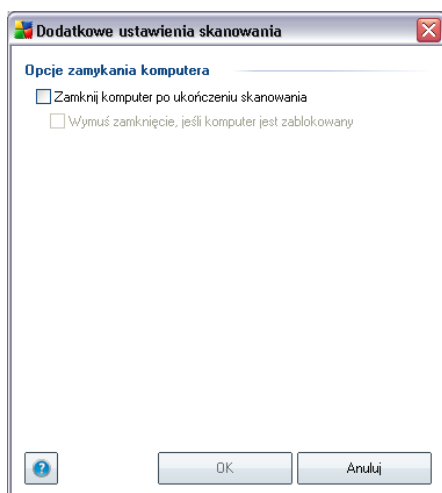


Edycja konfiguracji skanowania

Zdefiniowane wstępne ustawienia domyślne testu ***Skan określonych plików lub folderów*** można edytować. Kliknięcie linku ***Zmien ustawienia skanowania*** powoduje otwarcie okna dialogowego ***zmiany ustawień dla skanowania 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 (szczegółowy opis tych ustawień zawiera rozdział [Zaawansowane ustawienia AVG / Skany / Skanowanie określonych plików lub folderów](#)).
- **Dodatkowe ustawienia skanowania** — link do okna dialogowego "Dodatkowe ustawienia skanowania", w którym można określić następujące parametry:



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

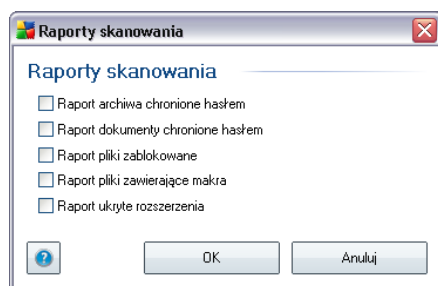
- o **Zdefiniuj typy plików do skanowania** — następnie należy zdecydować, czy skanowane mają być:

- **Wszystkie typy plików** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, który nie powinny być skanowane; LUB
- **Wybrane typy plików** — skanowane będą 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 skanowanie skróci się jeszcze bardziej, ponieważ takie pliki często są duże, a nie są podatne na infekcję*). 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. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkość skanowania, jak i wykorzystanie zasobów systemowych. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatna, gdy komputer jest w czasie skanowania używany, a czas trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).

- Ustaw dodatkowe raporty skanowania** — łącze pozwala otworzyć nowe okno dialogowe **Raporty skanowania**, w którym można określić, co ma być zgłaszane:



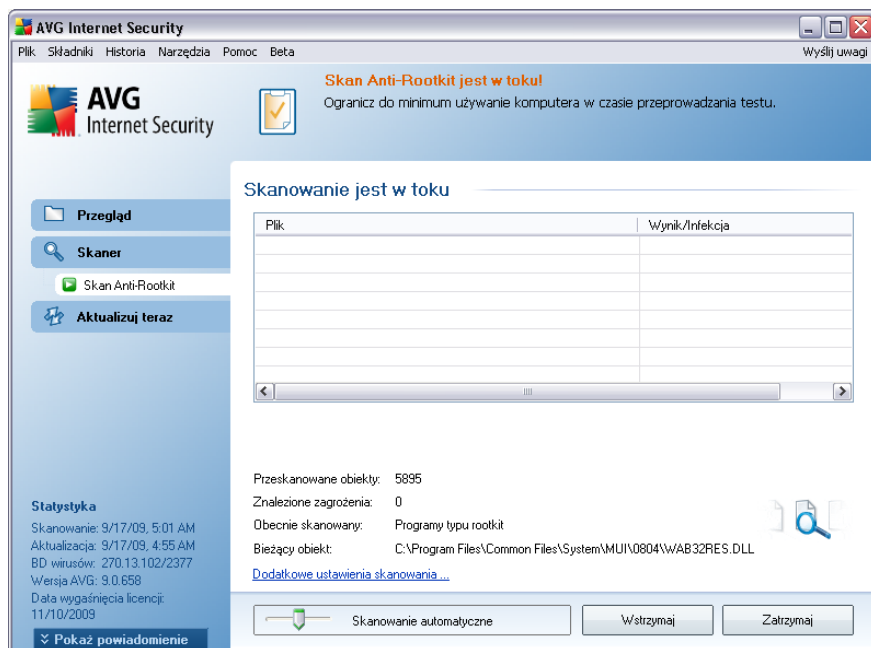
Ostrzeżenie: Ustawienia te są identyczne jak domyślne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale [Skanowanie AVG / Planowanie skanowania / Jak skanować](#). Jeśli jednak domyślna konfiguracja testu **Skan określonych plików lub folderów** zostanie zmieniona, nowe ustawienia będzie 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](#)).

11.2.3. 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 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**).

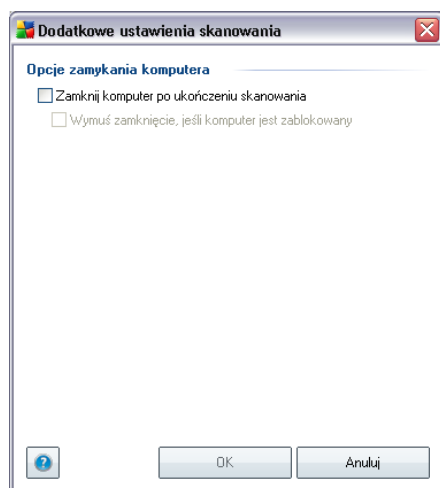


Edycja konfiguracji skanowania

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](#). Z poziomu [interfejsu skanera](#) dostępne są tylko następujące opcje konfiguracji:

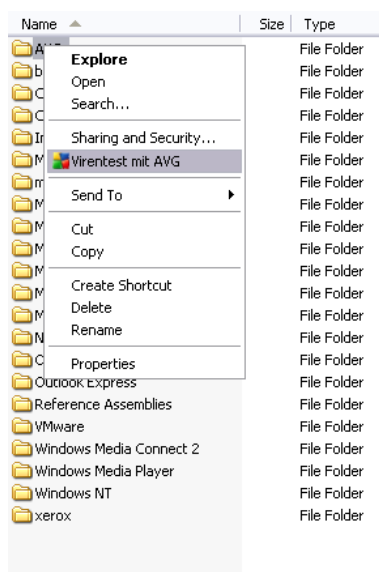
- **Skanowanie automatyczne** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślnie ustawiony jest priorytet średni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkość skanowania, jak i wykorzystanie zasobów systemowych. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatna, gdy komputer jest w czasie skanowania używany, a czas trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).

- **Dodatkowe ustawienia skanowania** — link ten umożliwia otwarcie nowego okna dialogowego **dodatkowych ustawień skanowania**, w którym dostępne są opcje **Zamknij komputer po zakończeniu skanowania** oraz **Wymus zamknięcie, jeśli komputer jest zablokowany**:



11.3. Skan z poziomu eksploratora systemu Windows

Oprócz wstępnie zdefiniowanych testów obejmujących cały komputer lub wybrane obszary, system **AVG 9 Internet Security** 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 zadanie”. W tym celu należy wykonać następujące kroki:



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

11.4. Skan z poziomu wiersza poleceń

AVG 9 Internet Security oferuje możliwość uruchamiania skanowania z wiersza poleceń. Opcji tej można używać na przykład na serwerach lub w czasie tworzenia skryptu wsadowego, który ma być uruchamiany po restarcie komputera. Uruchamiając skanowanie z wiersza poleceń, można używać większości parametrów dostępnych w graficznym interfejsie użytkownika AVG.

Aby uruchomić skanowanie z wiersza poleceń, należy wykonać następujące polecenie w folderze, w którym zainstalowano 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 określonej wartości, (np. parametr **/scan** wymaga informacji o wybranych do przeskanowania obszarach komputera — należy mu wskazać dokładną ścieżkę), wartości należy 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 wymagany 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 wiersza polecenia uruchamiane za pomocą interfejsu graficznego

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

Ponieważ okno to jest dostępne tylko w trybie awaryjnym, jego szczegółowy opis zawiera plik pomocy dostępny bezpośrednio ze wspomnianego okna.

11.4.1. Parametry skanowania z wiersza polecen

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

- **/SCAN** [Skanuj okreslone pliki lub foldery](#) /SCAN=sciezka;sciezka
(np. /SCAN=C:\;D:\)
- **/COMP** [Skanuj caly komputer](#)
- **/HEUR** [Uzyj analizy heurystycznej](#)
- **/EXCLUDE** Nie skanuj sciezki lub plikow
- **/@** Plik polecenia /nazwa pliku/
- **/EXT** Skanuj te rozszerzenia /na przyklad EXT=EXE,DLL/
- **/NOEXT** Nie skanuj tych rozszerzen /na przyklad NOEXT=JPG/
- **/ARC** Sprawdzaj archiwa
- **/CLEAN** Usuwarz automatycznie
- **/TRASH** [Przenies zainfekowane pliki do Przechowalni wirusow](#)
- **/QT** Szybki test
- **/MACROW** Raportuj pliki zawierajace makra
- **/PWDW** Raportuj pliki chronione haslem
- **/IGNLOCKED** Ignoruj pliki zablockowane
- **/REPORT** Raportuj do pliku /nazwa pliku/
- **/REPAPPEND** Dopisz do pliku raportu
- **/REPOK** Raportuj niezainfekowane pliki jako OK
- **/NOBREAK** Nie zezwalaj na przerwanie klawiszami CTRL-BREAK
- **/BOOT** Wlacz sprawdzanie MBR/sektora rozruchowego
- **/PROC** Skanuj aktywne procesy

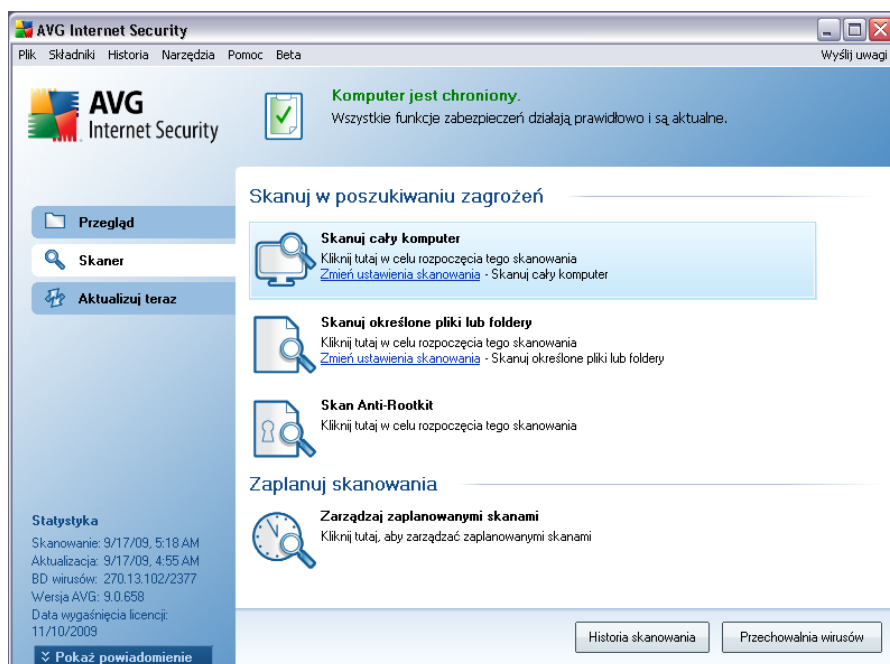
- **/PUP** Raportuj [potencjalnie niechciane programy](#)
- **/REG** Skanuj Rejestr
- **/COO** Skanuj pliki cookie
- **/?** Wyświetl pomoc na ten temat
- **/HELP** Wyświetl pomoc na ten temat
- **/PRIORITY** Ustaw priorytet skanowania /Niski, Auto, Wysoki/
(zobacz [Ustawienia zaawansowane / Skany](#))
- **/SHUTDOWN** Zamknij komputer po ukończeniu skanowania
- **/FORCESHUTDOWN** Wymus zamknięcie komputera po ukończeniu skanowania
- **/ADS** Skanuj alternatywne strumienie danych (tylko NTFS)

11.5. Planowanie skanowania

System **AVG 9 Internet Security** pozwala uruchomić skanowanie na zadanie użytkownika (np. 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.

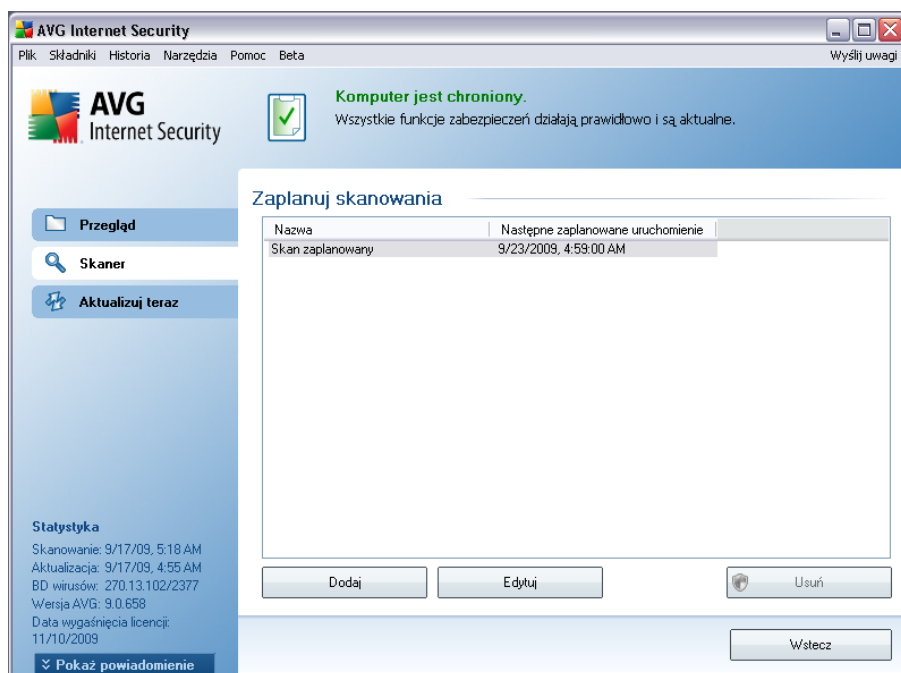
[Skan całego komputera](#) należy uruchamiać regularnie co najmniej raz na tydzień. Jeśli jest to możliwe, należy skanować komputer codziennie — zgodnie z domyślną konfiguracją harmonogramu skanowania. Jeśli komputer działa 24 godziny na dobę, można zaplanować skanowanie poza czasem pracy. Jeśli komputer 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**:



Planowanie skanowania

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

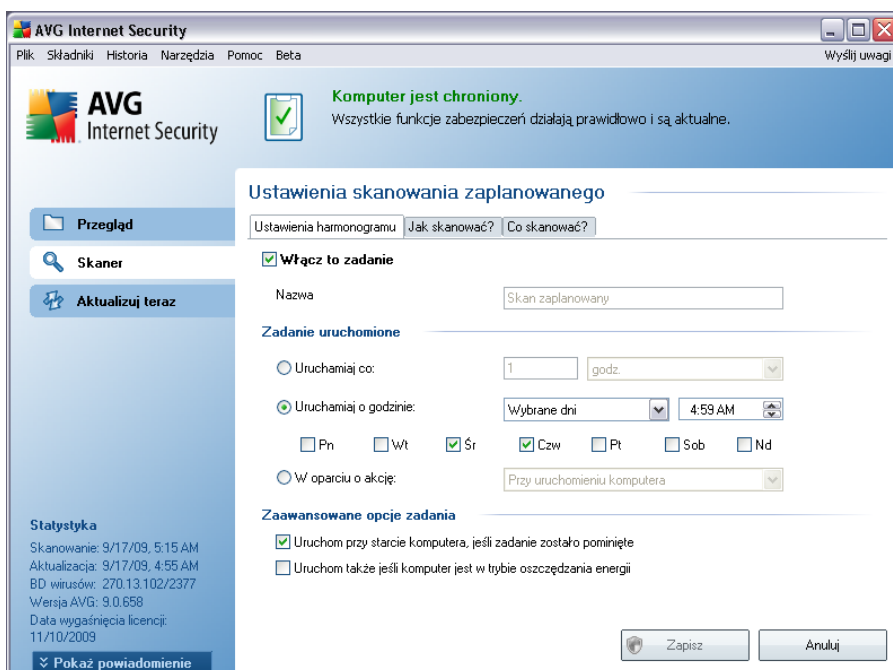


Zawartość okna można edytować, używając następujących przycisków:

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

11.5.1. 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 **planowania skanowania**). Okno to podzielone jest na trzy karty: **Ustawienia harmonogramu** — zobacz ilustracja poniżej (karta otwierana domyślnie), [Jak skanować?](#) i [Co skanować?](#).



Na karcie **Ustawienia harmonogramu** można zaznaczyć/odznaczyć 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 okreslać 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:

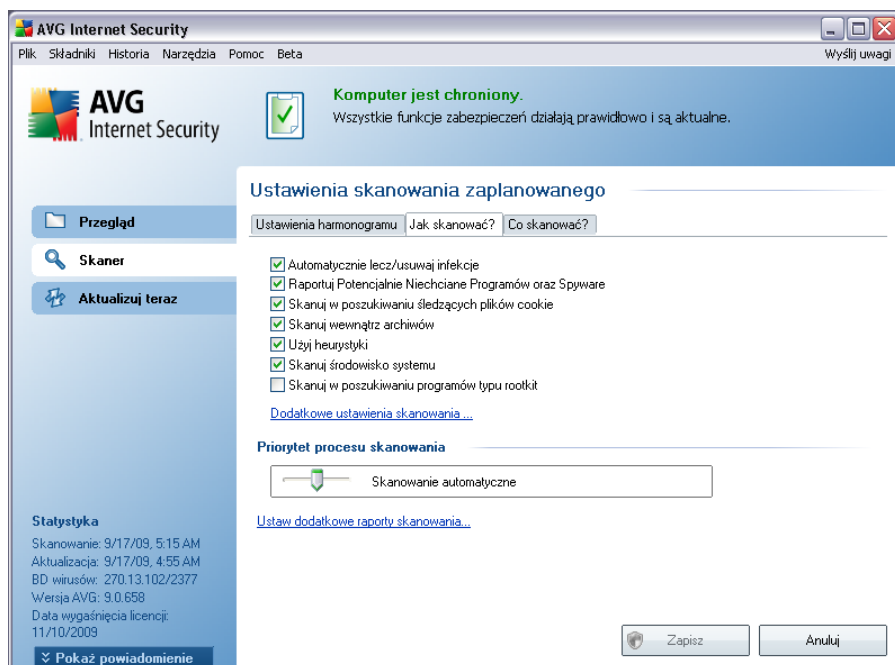
- **Zadanie uruchomione** — należy określić interwał przeprowadzanych testów. Skanowanie może być powtarzane w określonych odstępach czasu (**Uruchamiaj co**) lub o zadanej godzinie (**Uruchamiaj o określonej godzinie**), a także na skutek wystąpienia zdefiniowanego zdarzenia (**W oparciu o akcje, np. 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 zakładkach okna z **ustawieniami skanów zaplanowanych** (**Ustawienia harmonogramu**, [**Jak skanować?**](#) i [**Co skanować?**](#)) dostępne są dwa przyciski kontrolne. Ich działanie jest takie samo na każdej zakładce:

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

11.5.2. 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:

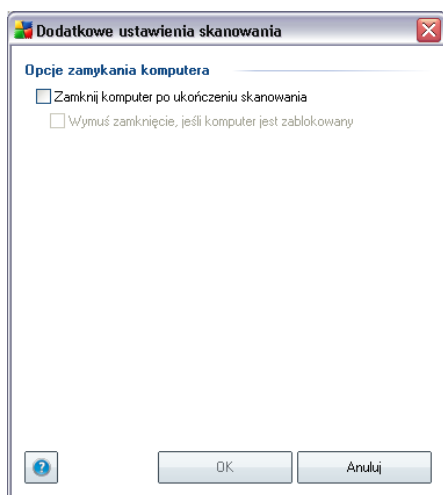
- **Automatycznie lecz/usuwać infekcje** — (domyślnie włączona) jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowanego pliku nie można wyleczyć, lub jeśli opcja ta zostanie wyłączona, system powiadomi o wykryciu wirusa i zapyta o sposób reakcji na infekcję. Zalecana czynnością jest przeniesienie zainfekowanego pliku do [Przechowalni wirusów](#).
- **Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujące** — (domyślnie włączone) ten parametr kontroluje funkcje składnika [Anti-Virus](#), które pozwalają [wykrywać potencjalnie niechciane programy](#) (pliki wykonywalne mogące się uruchamiać jako oprogramowanie szpiegujące lub reklamowe), a następnie blokować je lub usuwać.
- **Skanuj w poszukiwaniu śledzących plików cookie** — (domyślnie włączone) 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 włączona) parametr ten określa, czy skanowanie ma obejmować pliki znajdujące się wewnątrz niektórych typów archiwów, np. ZIP, RAR itd.
- **Użyj heurystyki** — (domyślnie włączona) analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny) jest jedną z metod wykrywania wirusów w czasie rzeczywistym.
- **Skanuj środowisko systemu** — (domyślnie włączona) skanowanie obejmie także obszary systemowe komputera.
- **Skanuj w poszukiwaniu programów typu rootkit** — zaznaczenie tej pozycji pozwala dołączyć 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 ten otwiera nowe okno dialogowe **Dodatkowe ustawienia skanowania**, w którym można określić następujące parametry:

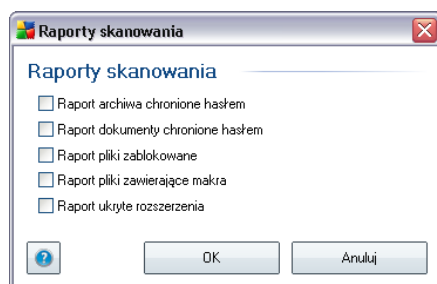


- o **Opcje wyłączenia komputera** — określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie

pierwszej opcji (**Zamknij komputer po ukonczeniu skanowania**) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, jeśli jest zablokowany (**Wymus zamknięcie, jeśli komputer jest zablokowany**).

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

- **Wszystkie typy plików** z opcja zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, który nie powinny być skanowane; LUB
 - **Wybrane typy plików** — skanowane będą 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 zostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliki 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. Domyślnie ustawiony jest priorytet średni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkość skanowania, jak i wykorzystanie zasobów systemowych. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).
 - **Ustaw dodatkowe raporty skanowania** — link ten pozwala otworzyć nowe okno dialogowe **Raporty skanowania**, w którym można określić elementy lub zdarzenia, które mają być zgłaszane:



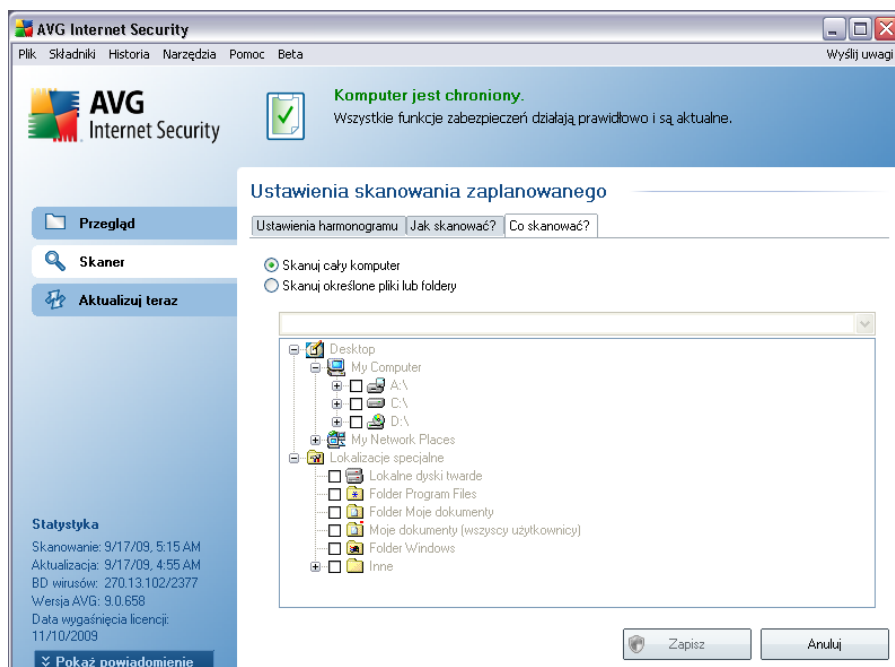
Uwaga: Domyslnie konfiguracja jest ustawiona pod kątem optymalnej wydajności. Konfiguracje skanowania należy zmieniać tylko w uzasadnionych sytuacjach. Stanowczo zaleca się stosowanie wstępnie zdefiniowanych ustawień. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników.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

Przyciski kontrolne

Na wszystkich trzech kartach okna z **konfiguracją 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 [domyslnego okna Interfejsu użytkownika AVG](#). Oznacza to, że aby zapisać nowe parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.
- **Anuluj** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do [Interfejsu użytkownika AVG](#).

11.5.3. Co skanowac?



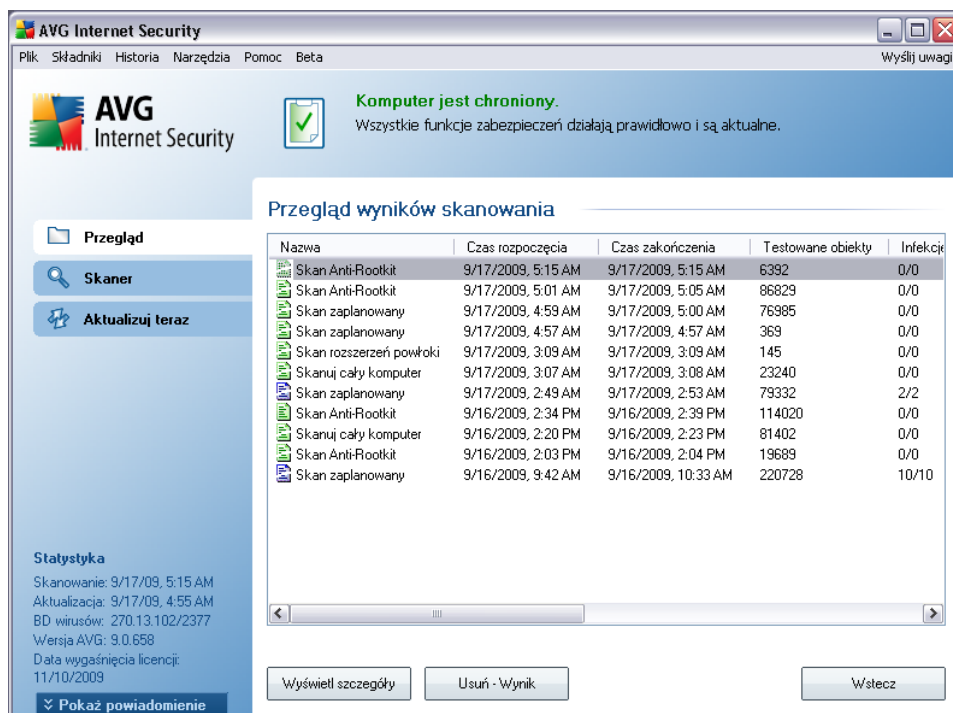
Na karcie **Co skanowac?** można określić, czy planowane jest [skanowanie całego komputera](#), czy [skanowanie określonych plików lub folderów](#). W przypadku skanowania określonych plików lub folderów, w dolnej części okna dialogowego aktywowane jest drzewo katalogów, w którym można wybrać obszar skanowania.

Przyciski kontrolne konfiguracji harmonogramu

Na wszystkich trzech zakładkach okna z **ustawieniami skanów zaplanowanych** ([Ustawienia harmonogramu](#), [Jak skanowac?](#) i [Co skanowac?](#)) dostępne są dwa przyciski kontrolne. Działanie tych przycisków jest takie samo na każdej zakładce:

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

11.6. 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 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 ukończony; w przeciwnym razie skanowanie zostało anulowane lub przerwane.

Uwaga: Szczegółowe informacje na temat każdego testu zawiera okno **Wyniki skanowania** dostępne po kliknięciu przycisku **Wyswietl 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.
- **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:

- **Wyswietl szczegóły** — przycisk jest aktywny tylko, jeśli w sekcji znajdującej się powyżej wybrano któryś z testów; kliknięcie go otwiera okno **Wyniki skanowania**, w którym można przejrzeć szczegółowe informacje o wybranym skanowaniu.
- **Usun wynik** — przycisk jest aktywny tylko, jeśli w sekcji znajdującej się powyżej wybrano któryś z testów; kliknięcie go powoduje usunięcie wybranej pozycji z przeglądu wyników skanowania.
- **Wstecz** — otwiera ponownie domyślne okno [Interfejsu skanera AVG](#).

11.7. Szczegóły wyników skanowania

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

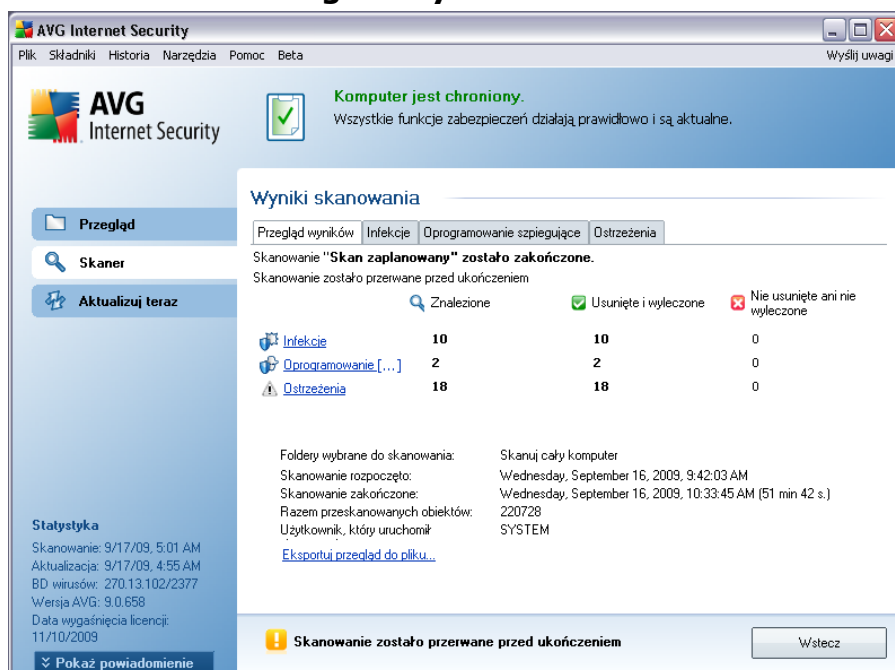
Okno to podzielone jest na kilka kart:

- **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** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto obiekty, których nie można było przeskanować.
- **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 znalezionej obiekty karta zawiera komunikat ostrzegawczy.

11.7.1. Karta "Przegląd wyników"



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

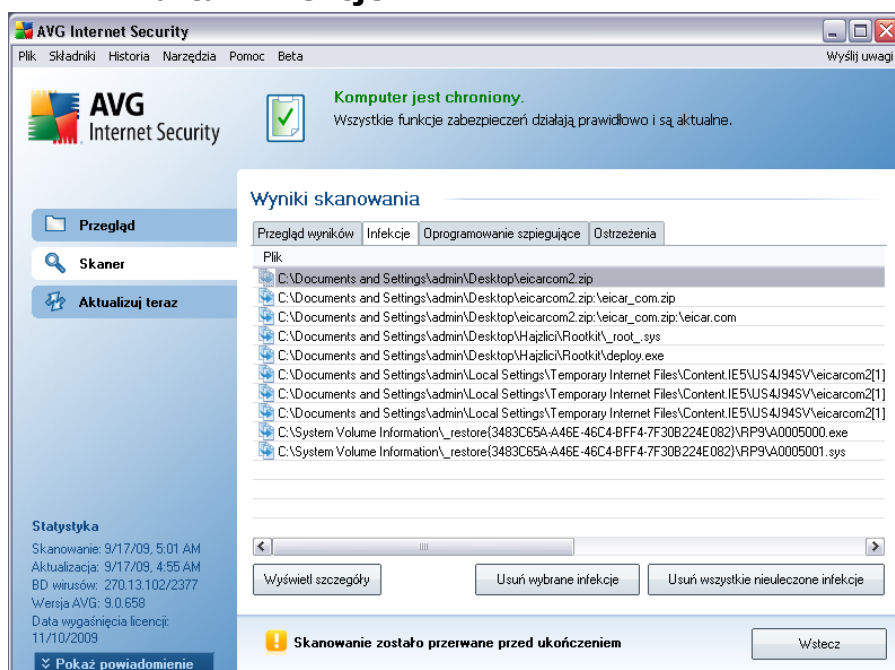
- wykrytych [infekcjach wirusowych/programach szpiegujących](#)
- usuniętych [infekcjach wirusowych/programach szpiegujących](#)
- liczbie [infekcji wirusowych/programów szpiegujących](#), których nie udało się usunąć ani wyleczyć.

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

Przyciski kontrolne

Okno to zawiera tylko jeden przycisk kontrolny. Kliknięcie przycisku **Zamknij wyniki** powoduje powrót do [Przeglądu wyników skanowania](#).

11.7.2. Karta "Infekcje"



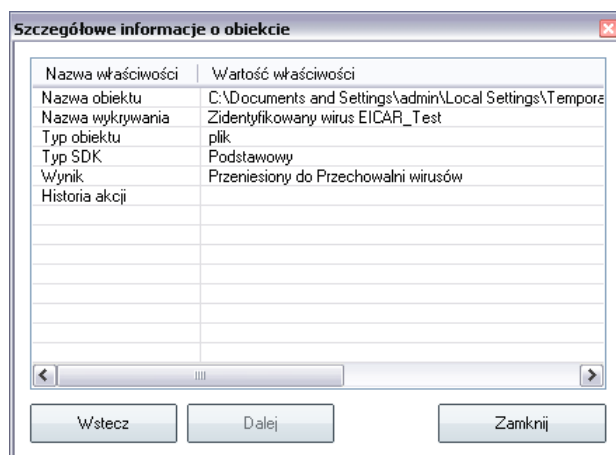
Karta **Infekcje** jest wyświetlana w oknie dialogowym **Wyniki skanowania** tylko, jeśli podczas skanowania wykryto [wirusa](#). Karta jest podzielona na trzy obszary, które zawierają następujące informacje:

- **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:
 - o **Zainfekowany** — zainfekowany obiekt został wykryty i pozostawiony w oryginalnej lokalizacji (np. jeśli [wylaczono opcje automatycznego leczenia](#) w szczegółowych ustawieniach skanowania).
 - o **Wyleczony** — zainfekowany obiekt został automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
 - o **Przeniesiony do Przechowalni** — zainfekowany obiekt został przeniesiony do [Przechowalni wirusów](#).
 - o **Usunięty** — zainfekowany obiekt został usunięty.
 - o **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](#)).
 - o **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanować.
 - o **Obiekt potencjalnie niebezpieczny** — obiekt został uznany za potencjalnie niebezpieczny, ale nie zainfekowany (może na przykład zawierać makra); informacje te należy traktować wyłącznie jako ostrzeżenie.
 - o **Wymagany restart systemu** — aby całkowicie usunąć zainfekowany obiekt, należy ponownie uruchomić komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

- **Wyświetl szczegóły** — otwiera nowe okno ze **szczegółowymi informacjami o wyniku testu**:



Mozna w nim znaleźć informacje o lokalizacji wykrytego pliku (**Nazwa właściwości**). Przyciski **Wstecz** i **Dalej** służą do nawigacji między pozycjami listy. Przycisk **Zamknij** zamyka okno.

- **Usun wybrane infekcje** — pozwala przenieść wybrane obiekty do [Przechowalni wirusów](#).
- **Usun wszystkie niewyleczone pliki** — 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](#).

11.7.3. 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:
 - o **Zainfekowany** — zainfekowany obiekt został wykryty i pozostawiony w oryginalnej lokalizacji (np. jeśli [wylaczono opcje automatycznego](#)

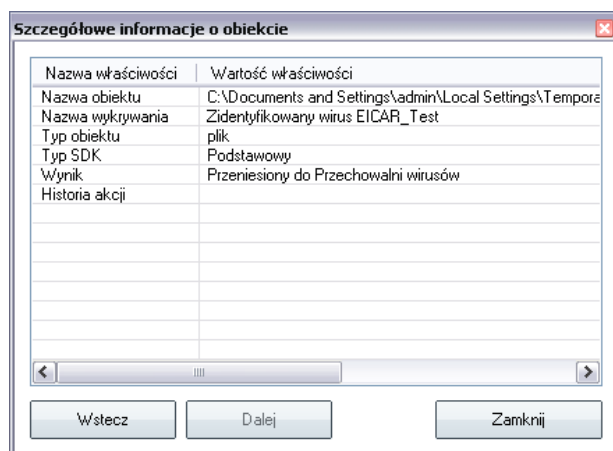
[leczenia](#) w szczegółowych ustawieniach skanowania).

- o **Wyleczony** — zainfekowany obiekt został automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
- o **Przeniesiony do Przechowalni** — zainfekowany obiekt został przeniesiony do [Przechowalni wirusów](#).
- o **Usunięty** — zainfekowany obiekt został usunięty.
- o **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](#)*).
- o **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanować.
- o **Obiekt potencjalnie niebezpieczny** — obiekt został uznany za potencjalnie niebezpieczny, ale nie zainfekowany (może np. zawierać makra); informacja ta jest wyłącznie ostrzeżeniem.
- o **Wymagany restart systemu** — aby całkowicie usunąć zainfekowany obiekt, należy ponownie uruchomić komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

- **Wyswietl szczegóły** — otwiera nowe okno ze **szczegółowymi informacjami o wyniku testu**:

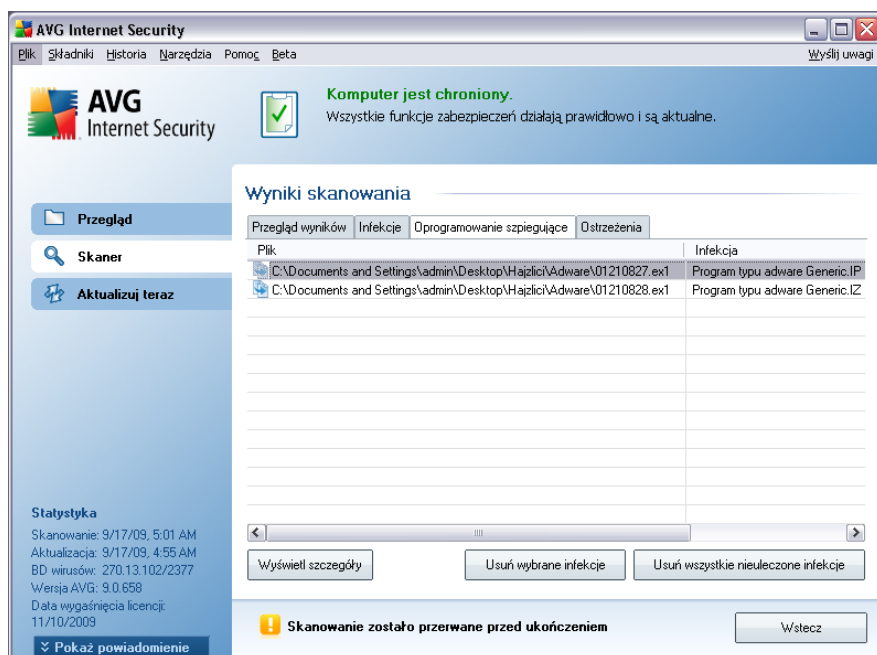


Mozna w nim znaleźć informacje o lokalizacji wykrytego pliku (**Nazwa właściwości**). Przyciski **Wstecz** i **Dalej** służą do nawigacji między pozycjami listy. Przycisk **Zamknij** zamyka okno.

- **Usun wybrane infekcje** — pozwala przenieść wybrane obiekty do [Przechowalni wirusów](#).
- **Usun wszystkie niewyleczone pliki** — 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](#).

11.7.4. Karta "Ostrzeżenia"

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



Oto krótki opis najbardziej popularnych obiektów tego typu:

- **Pliki ukryte** Pliki ukryte są domyślnie niewidoczne dla użytkownika w systemie Windows. Niektóre wirusy mogą próbować uniknąć wykrycia przez wykorzystanie tej właściwości. Jeśli system AVG zgłasza obecność ukrytego pliku, który może być szkodliwy, można przenieść go do [Przechowalni wirusów AVG](#).
- **Pliki cookie** Pliki cookie to pliki tekstowe wykorzystywane przez strony internetowe do przechowywania informacji właściwych dla danego użytkownika. Są one później używane do ładowania witryn internetowych dostosowanych do wymagań użytkownika, itp.
- **Podejrzane klucze rejestru** Niektóre szkodliwe oprogramowanie przechowuje informacje w rejestrze systemu Windows, aby uruchamiać się podczas ładowania systemu lub rozszerzyć zakres swojego działania.

11.7.5. Karta "Rootkity"

Karta **Rootkity** zawiera informacje na temat rootkitów wykrytych podczas skanowania, jeśli uruchomiono [Skanowanie Anti-rootkit](#) lub dodano tę opcję ręcznie do konfiguracji [Skan całego komputera](#) (opcja jest domyślnie wyłączona).

[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 myląc lub unikając standardowych mechanizmów bezpieczeństwa systemu operacyjnego. Wiele z nich jest jednocześnie koniami trojańskimi, które dodatkowo starają się przekonać użytkowników, że ich systemy są bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorującymi) oraz plików lub danych przed samym systemem operacyjnym.

Struktura tej karty jest w zasadzie taka sama jak kart [Infekcje](#) i [Oprogramowanie szpiegujące](#).

11.7.6. Karta "Informacje"

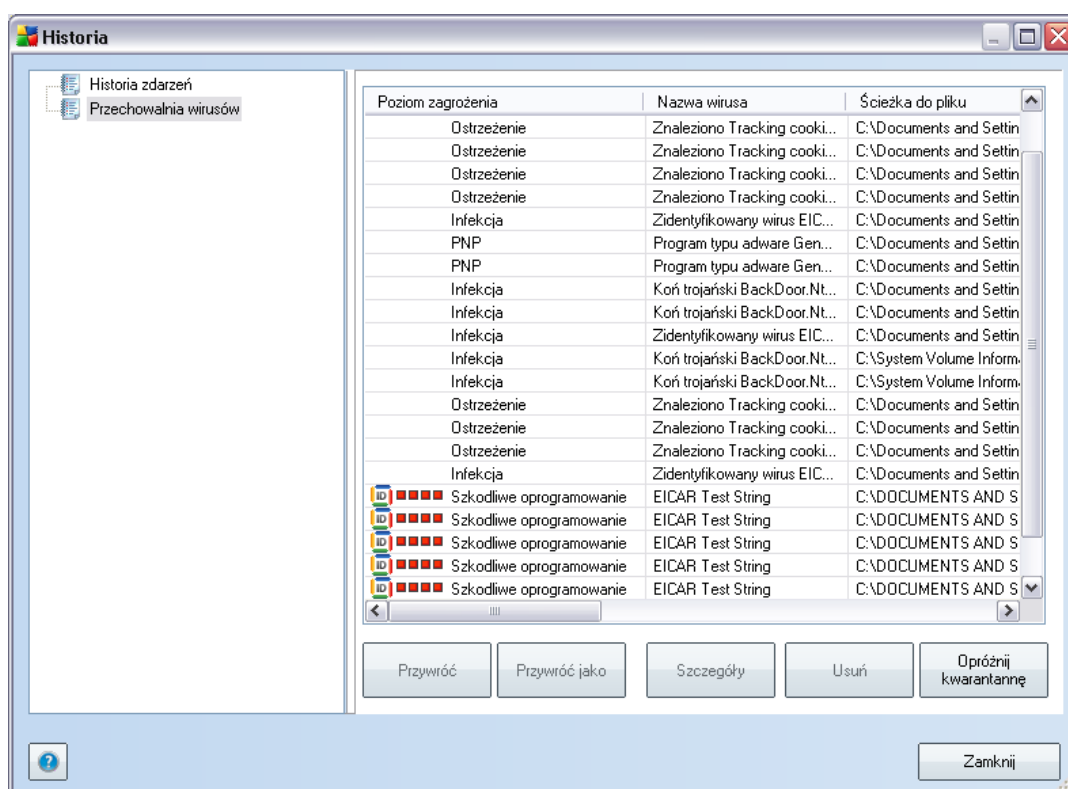
Karta **Informacje** zawiera dane dotyczące znalezionych obiektów, których nie można zakwalifikować jako infekcje, oprogramowanie szpiegujące itp. Obiektów tych nie można w stu procentach uznać za niebezpieczne, ale często wymagają one uwagi użytkownika. Skaner AVG jest w stanie wykryć pliki, które mogą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

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

- **Plik kompresowany w czasie rzeczywistym** - Plik został skompresowany przy użyciu jednego z mniej popularnych programów kompresujących w czasie wykonania, co może wskazywać na próbę uniemożliwienia skanowania takiego pliku. Nie każde zgłoszenie takiego pliku oznacza obecność wirusa.
- **Plik rekurencyjnie kompresowany w czasie rzeczywistym** - Podobny do powyższego, ale rzadziej spotykany wśród zwykłego oprogramowania. Takie pliki są podejrzane i należy rozważyć ich usunięcie lub przesłanie do analizy.
- **Archiwum lub dokument chroniony hasłem** - Pliki chronione hasłem nie mogą być skanowane przez program AVG (*ani generalnie przez żaden inny program chroniący przed szkodliwym oprogramowaniem*).
- **Dokument zawierający makra** — zgłoszone dokumenty zawierają makra, które mogą być szkodliwe.
- **Ukryte rozszerzenie** — pliki z ukrytymi rozszerzeniami mogą udawać np. obrazy, podczas gdy w rzeczywistości są plikami wykonywalnymi (np. "obrazek.jpg.exe"). Drugie rozszerzenie jest w systemie Windows domyślnie niewidoczne. Program AVG zgłasza takie pliki, aby zapobiec ich przypadkowemu uruchomieniu.

- **Niewlasciwa sciezka do pliku** — jeżeli jakiś ważny plik systemowy jest uruchamiany z innej ścieżki niż domyślna (np. plik "winlogon.exe" jest uruchamiany z folderu innego niż Windows), system AVG zgłasza tę niezgodność. W niektórych przypadkach wirusy używają nazw standardowych procesów systemowych, aby ich obecność w systemie była trudniejsza do wychwycenia przez użytkownika.
- **Plik zablokowany** — raportowany plik jest zablokowany, dlatego nie może zostać przeskanowany przez system AVG. Oznacza to zazwyczaj, że dany plik jest stale używany przez system (np. plik wymiany).

11.8. Przechowalnia wirusów



Przechowalnia wirusów to bezpieczne środowisko przeznaczone do zarządzania podejrzanymi/zainfekowanymi obiektami, które zostały wykryte podczas testów przeprowadzonych przez AVG. Po wykryciu zainfekowanego obiektu podczas skanowania (w przypadku, gdy AVG nie jest w stanie automatycznie go wyleczyć), użytkownik zostanie poproszony o wybranie reakcji na to zagrożenie. Zalecanym rozwiązaniem jest przeniesienie obiektu do **Przechowalni wirusów**, skąd można

bedzie podjac dalsze dzialanie zwiazane z analiza, wyleczeniem lub usuniecie pliku.

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

- **Zagrozenie** — zawiera graficzna reprezentacje poziomu znalezionego zagrozenia w czterostopniowej skali — od "nieistotne" (■□□□) do "bardzo niebezpieczne" (■■■■)
- **Typ infekcji** — klasyfikuje obiekty wedlug poziomu infekcji (*wszystkie obiekty na liscie sa prawdopodobnie lub na pewno zainfekowane*).
- **Nazwa wirusa** — nazwa wykrytej infekcji pochodzaca z [Encyklopedii wirusów](#) (online).
- **Sciezka do pliku** — pelna sciezka do oryginalnej lokalizacji zainfekowanego pliku.
- **Pierwotna nazwa obiektu** — wszystkie wykryte obiekty na liscie zostaly oznaczone standardowymi nazwami okreslanymi przez AVG w trakcie skanowania. W przypadku gdy obiekt mial okreslona nazwe, która jest znana (*np. nazwa zalacznika wiadomosci e-mail, która nie odpowiada faktycznej zawartosci zalacznika*), jest ona podawana w tej kolumnie.
- **Data zachowania** — data i godzina wykrycia podejrzanego pliku i przeniesienia go do **Przechowalni**.

Przyciski kontrolne

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

- **Przywróc** — przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- **Przywróc jako** — jesli zainfekowany obiekt ma zostac przeniesiony poza **Przechowalnie**, do okreslonego folderu, ten przycisk pozwala zapisac obiekt z nazwa inna niz pierwotna. Jesli nazwa pierwotna nie jest znana, uzyta zostanie nazwa standardowa.
- **Usun** — usuwa bezpowrotnie zainfekowany plik z **Przechowalni wirusów**.
- **Opróżnij przechowalnie** — usuwa bezpowrotnie cala zawartosc **Przechowalni wirusów**.

12. Aktualizacje AVG

Zapewnienie aktualności programu AVG jest niezbędne, ponieważ tylko w ten sposób wszystkie nowo pojawiające się wirusy będą wykrywane we właściwym czasie. Aktualizacje programu AVG nie są publikowane zgodnie z jakimkolwiek harmonogramem - powstają jako reakcja na pojawiające się zagrożenia. Dlatego też zalecamy sprawdzanie dostępności aktualizacji przynajmniej raz dziennie. Sprawdzanie co 4 godziny gwarantuje, że baza danych wirusów będzie aktualna także w ciągu dnia.

12.1. Poziomy aktualizacji

Program AVG oferuje dwa poziomy aktualizacji:

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

Podczas [planowania aktualizacji](#) można wybrać poziom priorytetu aktualizacji, które mają zostać pobrane i zastosowane.

12.2. Typy aktualizacji

Można wyróżnić dwa typy aktualizacji:

- **Aktualizacja na zadanie** — natychmiastowa aktualizacja oprogramowania AVG, której można dokonać w dowolnym momencie, w razie wystąpienia takiej konieczności.
- **Aktualizacja zaplanowana** — system AVG umożliwia przygotowanie [harmonogramu aktualizacji](#). Aktualizacja zaplanowana jest wykonywana regularnie, zgodnie z ustawioną konfiguracją. Gdy dostępne są nowe pliki aktualizacyjne, AVG pobiera je bezpośrednio z internetu lub katalogu sieciowego. W przypadku braku nowych aktualizacji proces ten kończy się, nie dokonując żadnych zmian.

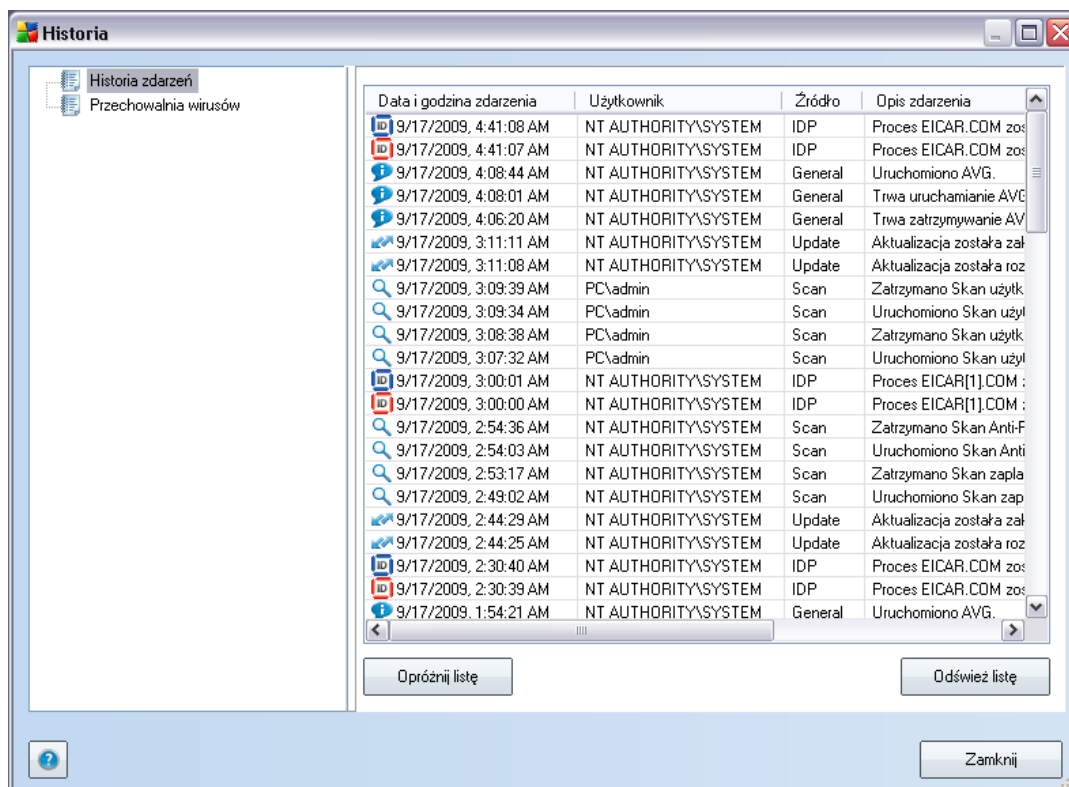
12.3. Proces aktualizacji

Aktualizacje można uruchamiać na zadanie, gdy są potrzebne, klikając link [Aktualizuj teraz](#). Link ten jest zawsze dostępny w głównym oknie [interfejsu użytkownika AVG](#). Mimo to, zaleca się regularne aktualizowanie systemu, zgodnie z harmonogramem, który można edytować za pomocą [Menedżera aktualizacji](#).

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

Uwaga: *Przed zaktualizowaniem programu AVG tworzony jest punkt odtwarzania 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 / Odtwarzanie systemu. Zalecane tylko doświadczonym użytkownikom!*

13. Historia zdarzen



Do interfejsu **Historii zdarzen** można dostać się poprzez [menu główne Historia/ Dziennik historii zdarzen](#). Okno to zawiera podsumowanie najważniejszych wydarzeń, które wystąpiły w czasie pracy systemu **AVG 9 Internet Security**. **Dziennik historii zdarzen** zawiera rekordy odpowiadające następującym typom zdarzeń:

- Informacje o aktualizacjach oprogramowania AVG;
- Uruchomienie, zakończenie lub wstrzymanie testu (łącznie z testami wykonywanymi automatycznie);
- Zdarzenia powiązane z wykryciem wirusa (przez [Ochronę Rezydentną](#) lub [podczas zwykłego skanowania](#)), wraz ze wskazaniem lokalizacji zainfekowanego pliku;
- Inne ważne zdarzenia.

Przyciski kontrolne

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

14. FAQ i pomoc techniczna

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

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