

AVG 9 Anti-Virus

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

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

W produkcji 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	6
2. Wymagania instalacyjne AVG	7
2.1 Obsługiwane systemy operacyjne	7
2.2 Minimalne wymagania sprzętowe	7
3. Opcje instalacji systemu AVG	8
4. AVG Download Manager	9
4.1 Wybór języka	9
4.2 Test połączenia	10
4.3 Ustawienia proxy	11
4.4 Wybór typu licencji	12
4.5 Pobieranie plików instalacyjnych	13
5. Proces instalacji systemu AVG	14
5.1 Uruchamianie instalacji	14
5.2 Umowa licencyjna	15
5.3 Sprawdzanie stanu systemu	15
5.4 Wybieranie typu instalacji	16
5.5 Uaktywnienie licencji AVG	16
5.6 Instalacja niestandardowa — Folder docelowy	18
5.7 Instalacja niestandardowa — Wybór składników	19
5.8 AVG DataCenter	20
5.9 Pasek narzędzi AVG Security Toolbar	21
5.10 Instalowanie systemu AVG	22
5.11 Zaplanowanie regularnych skanów i aktualizacji	23
5.12 Konfiguracja ochrony systemu AVG została ukonczona	23
6. Po instalacji	25
6.1 Rejestracja produktu	25
6.2 Dostęp do Interfejsu użytkownika	25
6.3 Skanowanie całego komputera	25
6.4 Test Eicar	25
6.5 Konfiguracja domyślna AVG	26
7. Interfejs użytkownika AVG	27

7.1 Menu systemowe	28
7.1.1 Plik	28
7.1.2 Składniki	28
7.1.3 Historia	28
7.1.4 Narzędzia	28
7.1.5 Pomoc	28
7.2 Status bezpieczeństwa	31
7.3 Linki	32
7.4 Przegląd składników	32
7.5 Statystyki	33
7.6 Ikona na pasku zadań	34
8. Składniki AVG	35
8.1 Anti-Virus	35
8.1.1 Zasady działania składnika Anti-Virus	35
8.1.2 Interfejs składnika Anti-Virus	35
8.2 Anti-Spyware	37
8.2.1 Zasady działania składnika Anti-Spyware	37
8.2.2 Interfejs składnika Anti-Spyware	37
8.3 Licencja	39
8.4 LinkScanner	40
8.4.1 Zasady działania technologii LinkScanner	40
8.4.2 Interfejs LinkScanner	40
8.4.3 AVG Search-Shield	40
8.4.4 AVG Active Surf-Shield	40
8.5 Ochrona sieci WWW	43
8.5.1 Zasady działania składnika Ochrona sieci WWW	43
8.5.2 Interfejs składnika Ochrona sieci WWW	43
8.5.3 Zagrożenia wykryte przez Ochronę sieci WWW	43
8.6 Ochrona rezydentna	49
8.6.1 Zasady działania Ochrony rezydentnej	49
8.6.2 Interfejs składnika Ochrona rezydentna	49
8.6.3 Zagrożenia wykryte przez Ochronę rezydentna	49
8.7 Menedżer aktualizacji	54
8.7.1 Zasady działania Menedżera aktualizacji	54
8.7.2 Interfejs Menedżera aktualizacji	54
8.8 Pasek narzędzi AVG Security Toolbar	57
8.8.1 Interfejs paska narzędzi AVG Security Toolbar	57

8.8.2 Opcje Paska narzedzi AVG Security Toolbar	57
9. Zaawansowane ustawienia AVG	64
9.1 Wyglad	64
9.2 Dzwieki	66
9.3 Ignoruj bledny stan skladnikow	68
9.4 Przechowalnia wirusow	69
9.5 Wyjatki PNP	70
9.6 Ochrona sieci WWW	72
9.6.1 Ochrona WWW	72
9.6.2 Komunikatory internetowe	72
9.7 LinkScanner	76
9.8 Skany	77
9.8.1 Skan calego komputera	77
9.8.2 Skan rozszerzenia powloki	77
9.8.3 Skan okreslonych plikow lub folderow	77
9.8.4 Skan urzadzen wymiennych	77
9.9 Zaplanowane zadania	84
9.9.1 Skan zaplanowany	84
9.9.2 Harmonogram aktualizacji bazy wirusow	84
9.9.3 Harmonogram aktualizacji programu	84
9.10 Skaner poczty e-mail	94
9.10.1 Certyfikacja	94
9.10.2 Filtrowanie poczty	94
9.10.3 Dzienniki i Wyniki	94
9.10.4 Serwery	94
9.11 Ochrona rezydentna	102
9.11.1 Ustawienia zaawansowane	102
9.11.2 Wykluczenia katalogow	102
9.11.3 Wykluczone pliki	102
9.12 Aktualizacja	107
9.12.1 Proxy	107
9.12.2 Polaczenie telefoniczne	107
9.12.3 URL	107
9.12.4 Zarzadzaj	107
10. Skanowanie AVG	114
10.1 Interfejs skanowania	114

10.2	Wstępnie zdefiniowane testy	115
10.2.1	<i>Skan całego komputera</i>	115
10.2.2	<i>Skan określonych plików lub folderów</i>	115
10.3	Skan z poziomu eksploratora systemu Windows	123
10.4	Skan z poziomu wiersza poleceń	124
10.4.1	<i>Parametry skanowania z wiersza poleceń</i>	124
10.5	Planowanie skanowania	127
10.5.1	<i>Ustawienia harmonogramu</i>	127
10.5.2	<i>Jak skanować?</i>	127
10.5.3	<i>Co skanować?</i>	127
10.6	Przegląd wyników skanowania	136
10.7	Szczegóły wyników skanowania	138
10.7.1	<i>Karta "Przegląd wyników"</i>	138
10.7.2	<i>Karta "Infekcje"</i>	138
10.7.3	<i>Karta "Oprogramowanie szpiegujące"</i>	138
10.7.4	<i>Karta "Ostrzeżenia"</i>	138
10.7.5	<i>Karta "Informacje"</i>	138
10.8	Przechowalnia wirusów	146
11.	Aktualizacje AVG	148
11.1	Poziomy aktualizacji	148
11.2	Typy aktualizacji	148
11.3	Proces aktualizacji	148
12.	Historia zdarzeń	150
13.	FAQ i pomoc techniczna	152

1. Wprowadzenie

Ten podręcznik użytkownika zawiera dokumentację systemu **AVG 9 Anti-Virus**.

Gratulujemy zakupu produktu AVG 9 Anti-Virus!

AVG 9 Anti-Virus 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 Anti-Virus** zaprojektowano od podstaw pod kątem zapewnienia słynnego już poziomu ochrony, w nowy, bardziej przyjazny dla użytkownika sposób.

Najnowszy produkt **AVG 9 Anti-Virus** 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 Anti-Virus 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)

2.2. Minimalne wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG 9 Anti-Virus** 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 Anti-Virus.

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 zakupienia 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

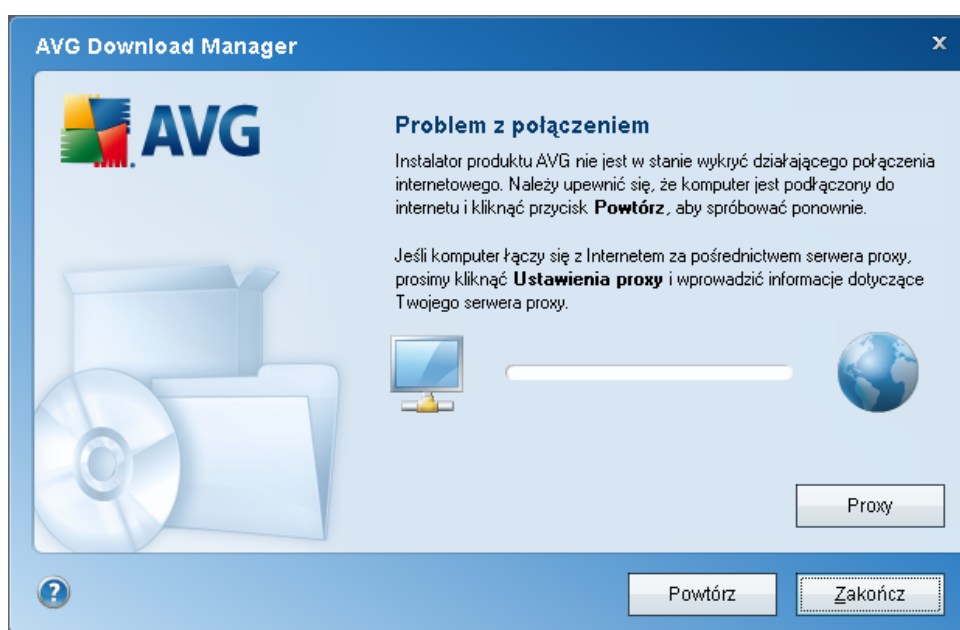


AVG Download Manager pozwoli w pierwszym kroku wybrać język instalacji. Należy pamiętać, że wybór ten dotyczy tylko procesu instalacji; po jej zakończeniu język programu będzie można zmienić bezpośrednio w jego ustawieniach. Aby kontynuować, kliknij przycisk **Dalej**.

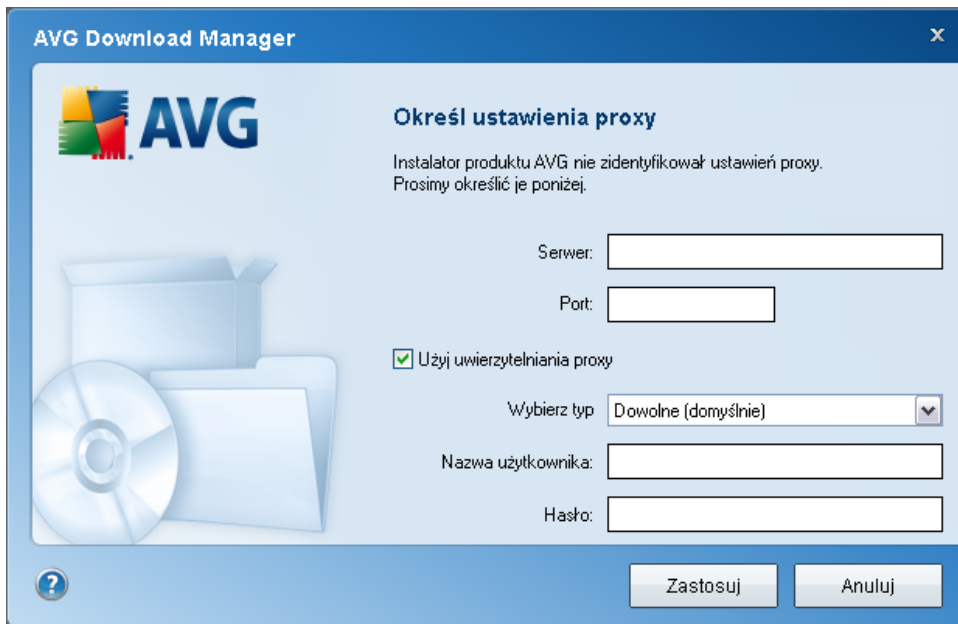
4.2. Test połączenia

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**

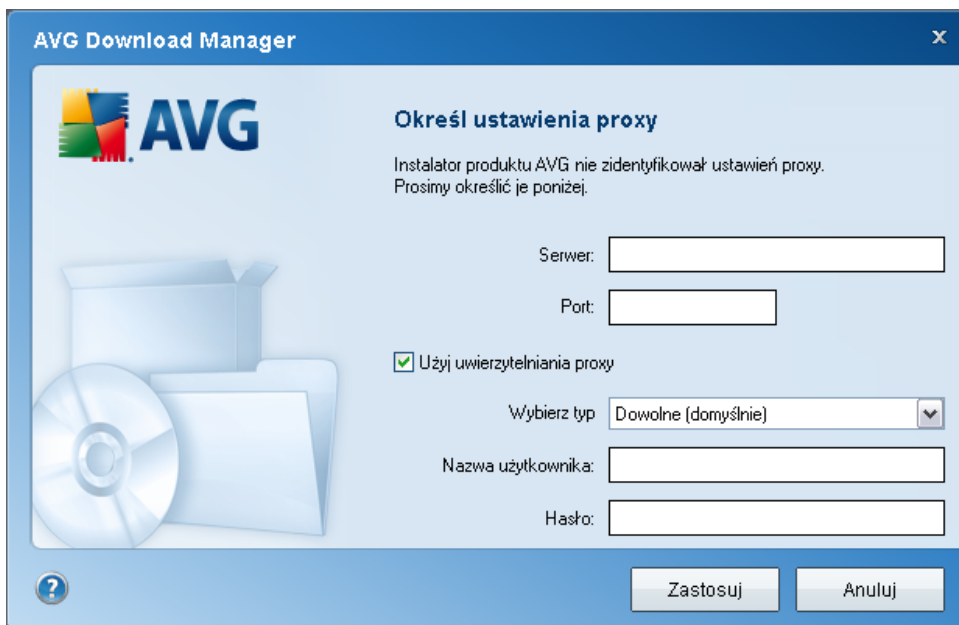


- Jeśli używasz serwera proxy, kliknij przycisk **Ustawienia proxy** i podaj [wymagane szczegóły](#):



- 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.

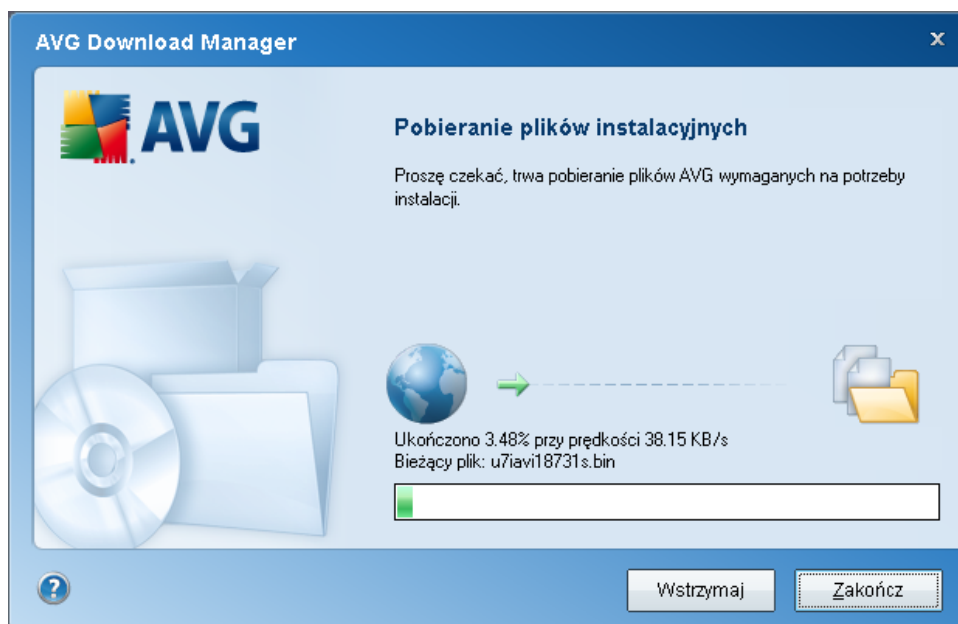
4.4. Wybór typu licencji



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



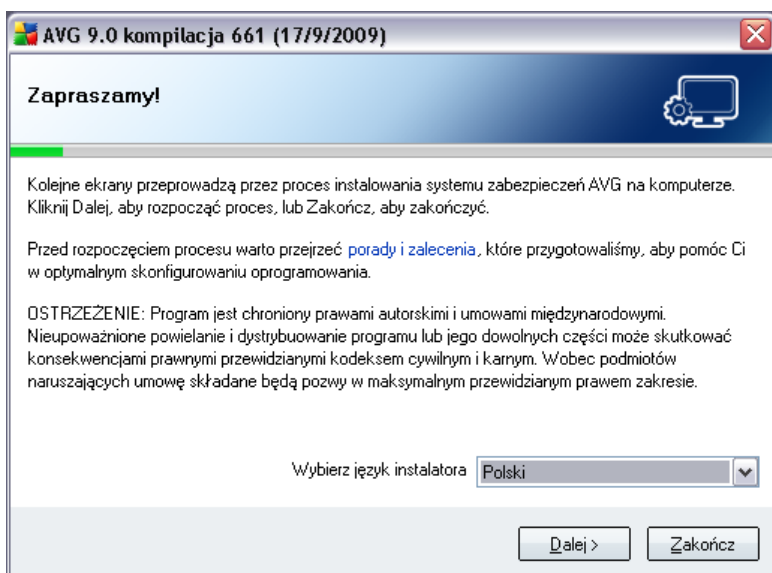
Wszystkie informacje, których **AVG Download Manager** potrzebuje do pobrania pakietów instalacyjnych i uruchomienia instalacji, zostały już podane. Można rozpocząć [instalację systemu AVG](#).

5. Proces instalacji systemu AVG

Aby zainstalować na komputerze system **AVG 9 Anti-Virus**, 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:

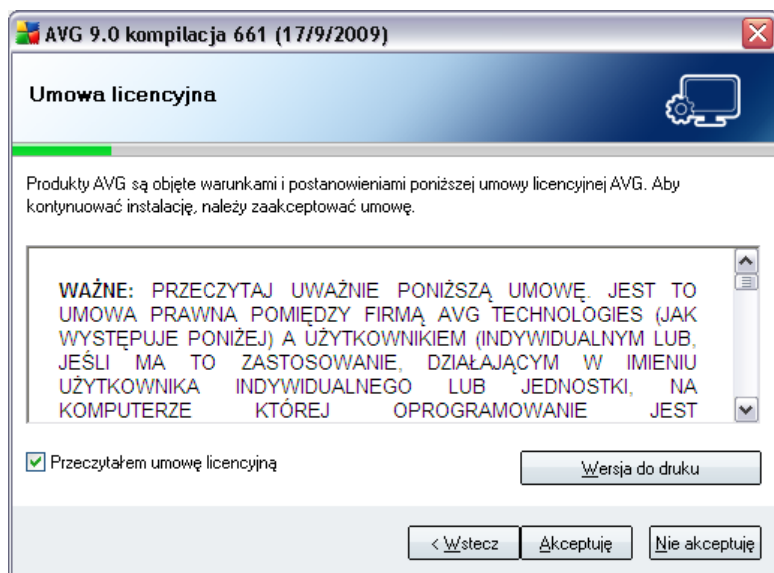
5.1. Uruchamianie instalacji



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



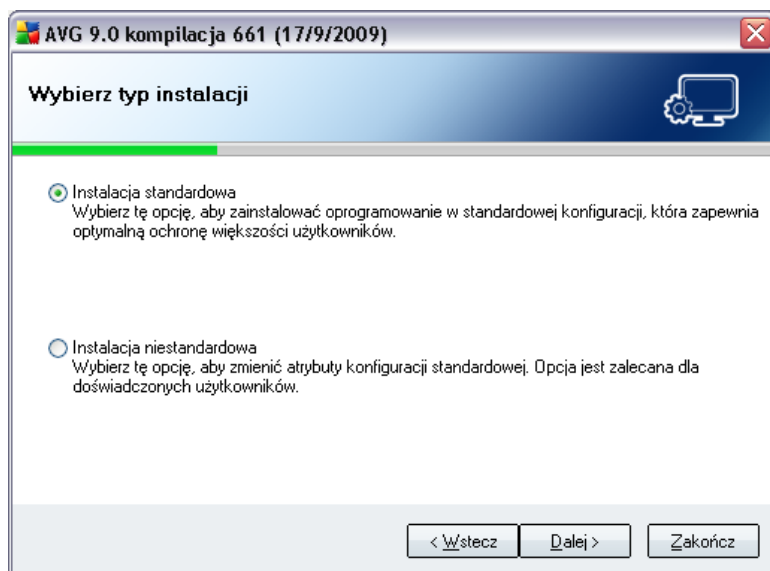
Okno dialogowe **Umowa licencyjna** zawiera pełną treść umowy licencyjnej AVG. Przeczytaj ją uważnie i potwierdź jej akceptację, zaznaczając pole **Przeczytałem warunki umowy licencyjnej** i wciskając przycisk **Dalej**.

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.

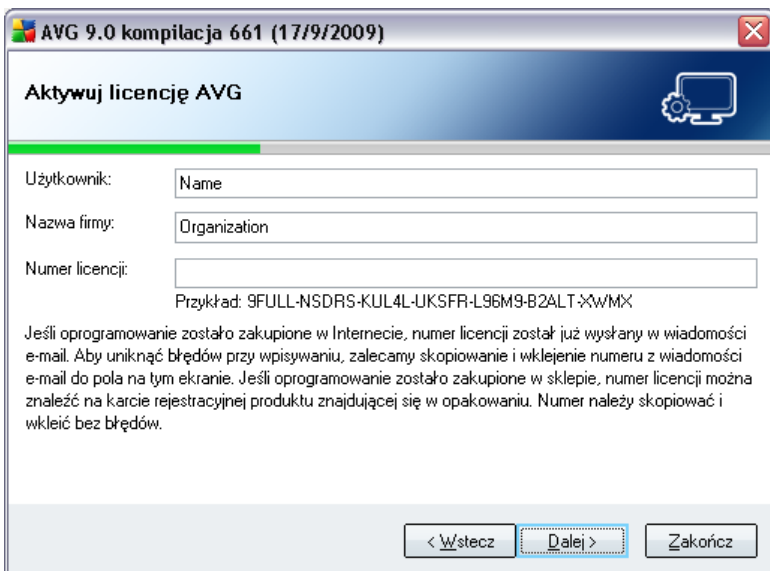
Instalacje niestandardowa powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować programu AVG z domyślnymi ustawieniami, np. na komputerach o specyficznej konfiguracji sprzętowej.

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 Anti-Virus**. Numer licencji jest wysyłany poprzez e-mail

po zakupieniu oprogramowania **AVG 9 Anti-Virus** 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.

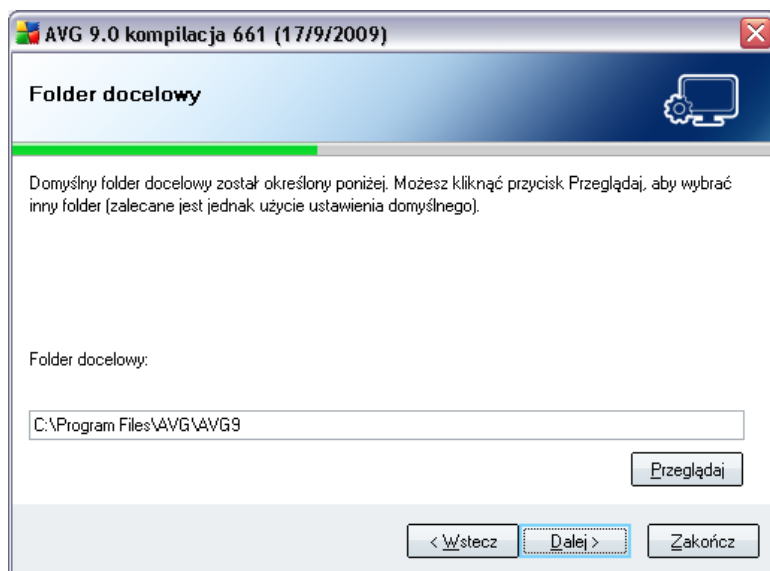


The screenshot shows a window titled "AVG 9.0 kompilacja 661 (17/9/2009)". The main heading is "Aktywuj licencję AVG". There are three input fields: "Użytkownik:" with "Name" as a placeholder, "Nazwa firmy:" with "Organization" as a placeholder, and "Numer licencji:". Below the license number field is an example: "Przykład: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XXWMX". A paragraph of text explains that if the software was purchased online, the license number is in an email, and if purchased in a store, it's on the product card. At the bottom, there are three buttons: "< Wstecz", "Dalej >", and "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

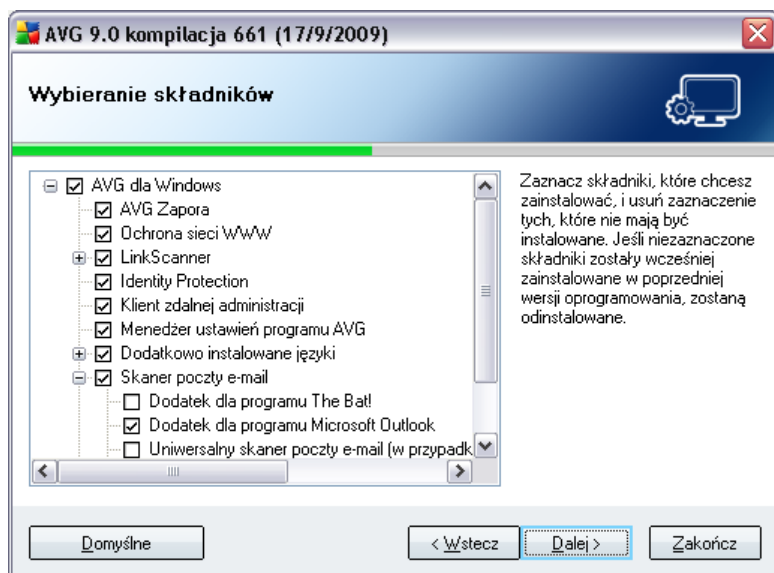


Okno dialogowe **Folder docelowy** pozwala określić lokalizację dla plików **AVG 9 Anti-Virus**. Domyślnie pakiet AVG jest instalowany w folderze "Program Files" na dysku C:. Jeśli wybrany folder nie istnieje, zostanie wyświetlone nowe okno dialogowe z pytaniem o zgodę na jego utworzenie.

Aby zmienić tę lokalizację, kliknij przycisk **Przełączaj** 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 Anti-Virus**, 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 **Dodatkowo 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**. 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.

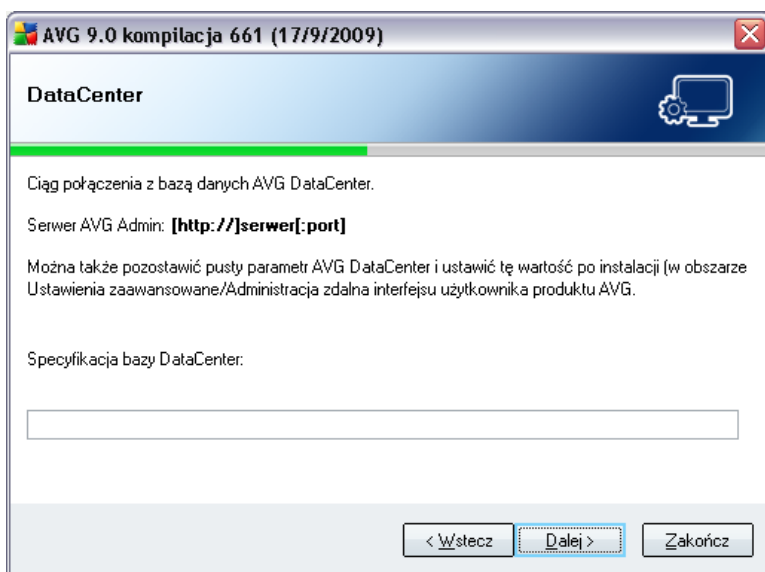
- **Administracja zdalna**

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

Aby kontynuować, kliknij przycisk **Dalej**.

5.8. AVG DataCenter

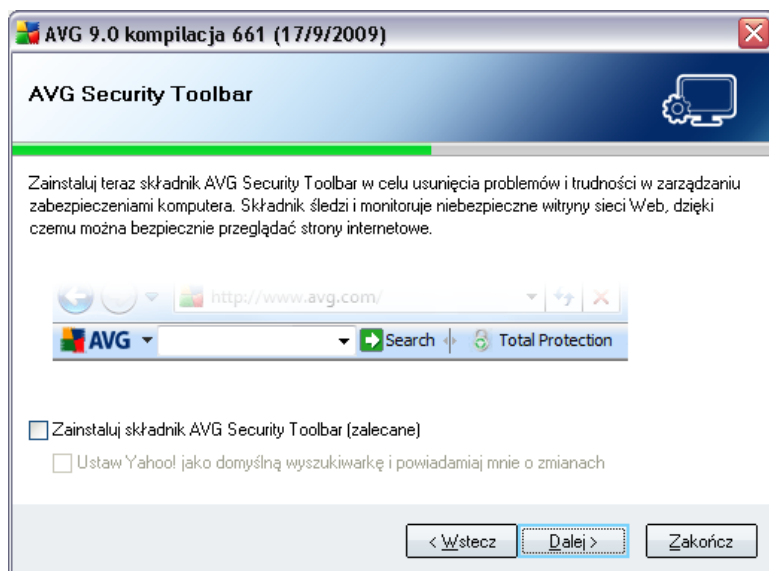
Jeśli w poprzednim oknie dialogowym (**Instalacja niestandardowa – Wybór składników**) zaznaczono do instalacji składnik **Administracja zdalna**, należy określić parametry **AVG DataCenter**:



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/>).

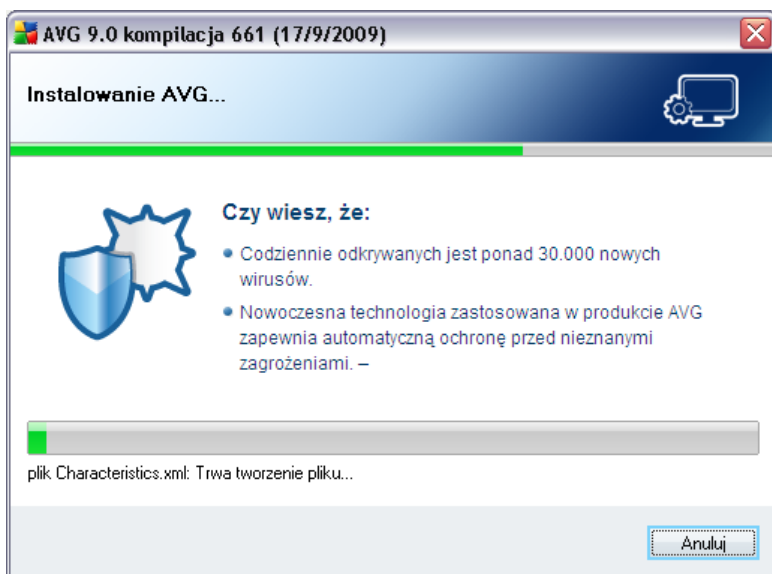
5.9. Pasek narzędzi AVG Security Toolbar



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.

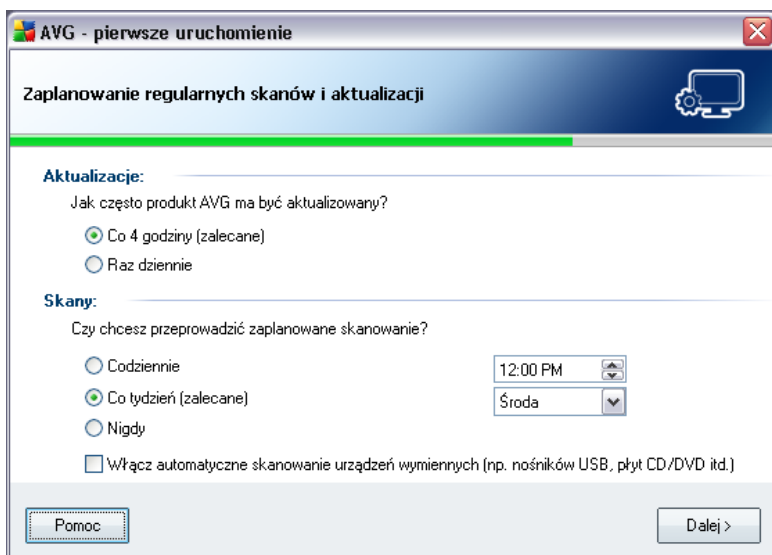
5.10. Instalowanie systemu AVG

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



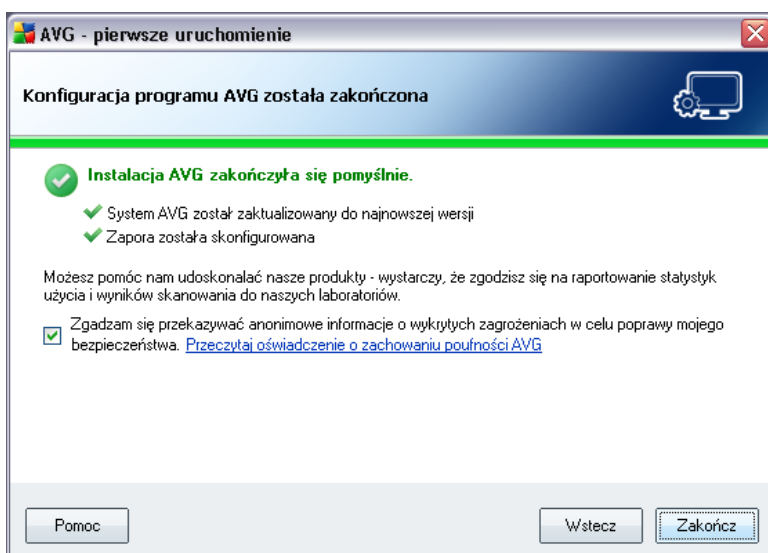
Po zakończeniu instalacji automatycznie nastąpi przekierowanie do następnego okna dialogowego.

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. Konfiguracja ochrony systemu AVG została ukończona



Konfiguracja **AVG 9 Anti-Virus** zakonczyła sie pomyslnie.

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

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

6. Po instalacji

6.1. Rejestracja produktu

Po ukończeniu instalacji systemu **AVG 9 Anti-Virus** 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 Anti-Virus**. 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](#).

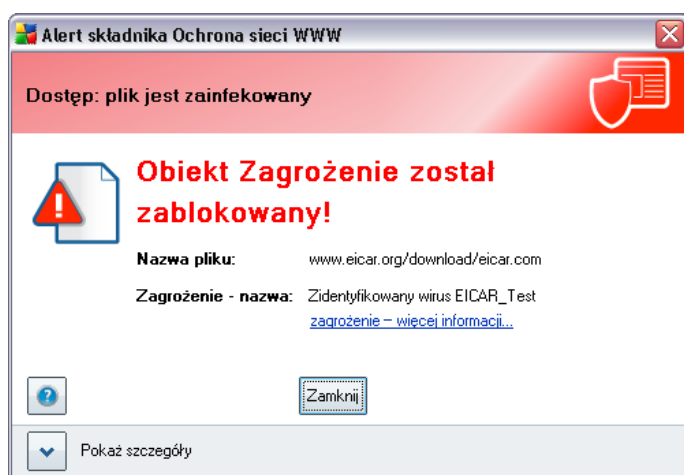
6.4. Test Eicar

W celu potwierdzenia poprawności instalacji systemu **AVG 9 Anti-Virus**, można wykonać test EICAR.

Test EICAR jest standardową i całkowicie bezpieczną metodą służącą do sprawdzania prawidłowości działania systemu antywirusowego. Można go bezpiecznie rozpowszechniać, ponieważ nie jest prawdziwym wirusem i nie zawiera żadnych fragmentów złośliwego kodu. Większość produktów rozpoznaje go jako wirusa (choć zwykle zgłasza go pod jednoznaczna nazwa, 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

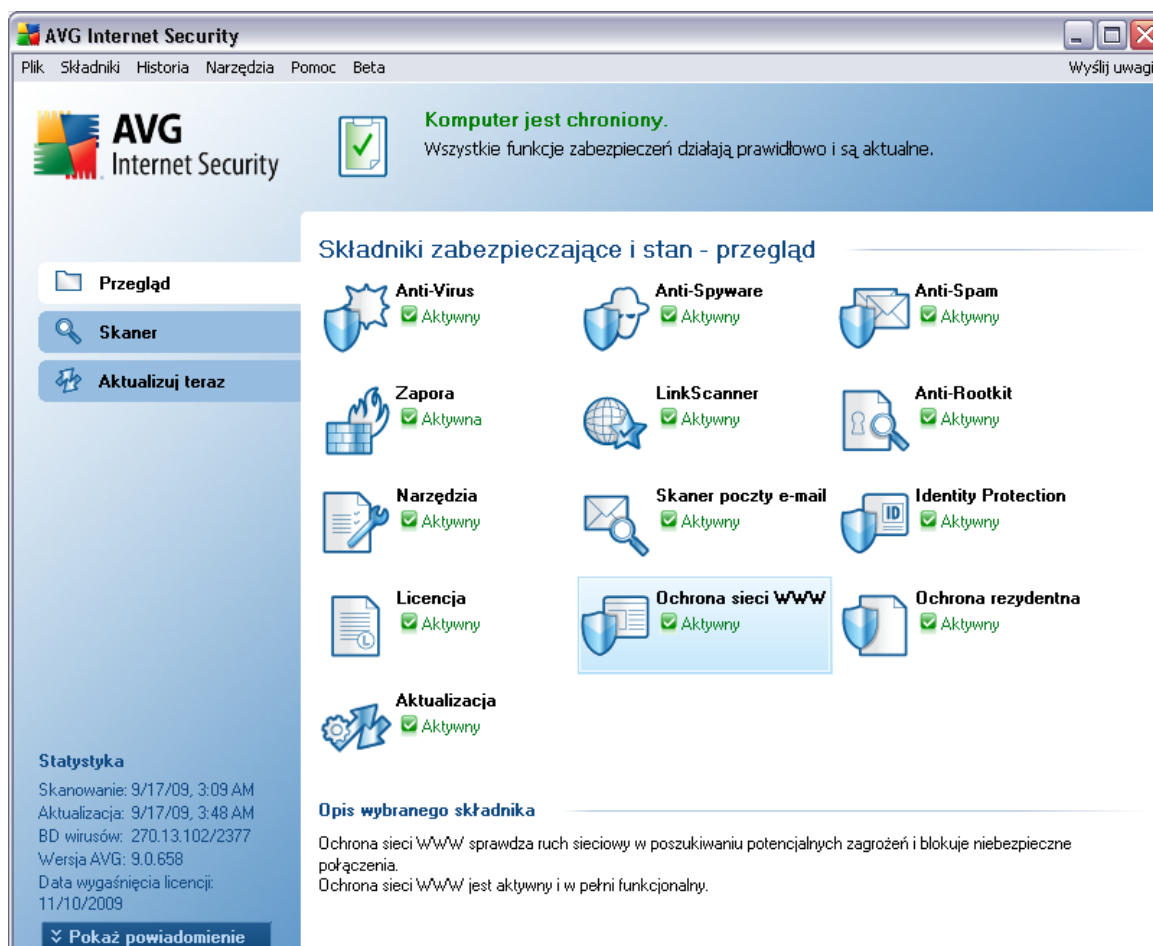
Konfiguracja domyślna (*ustawienia stosowane zaraz po zainstalowaniu*) pakietu **AVG 9 Anti-Virus**, wstępnie zdefiniowana przez dostawcę oprogramowania, ma na celu zapewnienie optymalnej wydajności wszystkich składników i funkcji.

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 Anti-Virus otwórz w głównym oknie



Główne okno Interfejsu Użytkownika AVG jest podzielone na kilka sekcji:

- **Menu główne** (górną 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 Anti-Virus**. 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 Anti-Virus**. 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-Spyware** — otwiera domyślne okno interfejsu składnika **Anti-Spyware**.
- **LinkScanner** — otwiera domyślne okno interfejsu składnika **LinkScanner**.
- **Skaner poczty e-mail** — otwiera domyślne okno interfejsu składnika **Skaner poczty e-mail**.

- **Licencja** — otwiera domyslne okno interfejsu skladnika [Licencja](#).
- **Ochrona sieci WWW** — otwiera domyslne okno interfejsu skladnika [Ochrona sieci WWW](#).
- **Ochrona rezydentna** — otwiera domyslne okno interfejsu skladnika [Ochrona rezydentna](#).
- **Menedzer aktualizacji** — otwiera domyslne okno interfejsu skladnika [Menedzer aktualizacji](#).

7.1.3. Historia

- **Wyniki skanowania** — powoduje przelaczenie do interfejsu skanera AVG, konkretnie do okna dialogowego [Przegląd wyników skanowania](#).
- **Zagrożenia wykryte przez Ochrone Rezydentna** — powoduje otwarcie okna dialogowego zawierajacego przeglad zagrozen wykrytych przez [Ochrone Rezydentna](#).
- **Zagrożenie wykryte przez Skaner poczty e-mail** — powoduje otwarcie okna zawierajacego przeglad załączników e-mail uznanych za niebezpieczne przez [Skaner poczty e-mail](#).
- **Zagrożenia wykryte przez Ochrone sieci WWW** — powoduje otwarcie okna dialogowego zawierajacego przeglad zagrozen wykrytych przez [Ochrone 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 sa izolowane i nie zagrazaja bezpieczenstwu komputera, a jednoczesnie istnieje mozliwosc ich naprawy w przyszlosci.
- **Dziennik historii zdarzen** — powoduje otwarcie interfejsu dziennika historii z przegladem wszystkich zarejestrowanych akcji **AVG 9 Anti-Virus** .

7.1.4. Narzedzia

- **Skanuj komputer** — przelacza do [Interfejsu skanera AVG](#) i uruchamia skanowanie calego komputera.
- **Skanuj wybrany folder** — przelacza do [Interfejsu skanera AVG](#) i umożliwia zdefiniowanie (w ramach struktury katalogów i dysków) plików oraz folderów, które maja byc przeskanowane.

- **Skanuj plik** — umożliwia uruchomienie na zadanie testu pojedynczego, wskazanego pliku.
- **Aktualizuj** — automatycznie uruchamia proces aktualizacji. **AVG 9 Anti-Virus**
- **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 Anti-Virus**. Na ogół zaleca się zachowanie domyślnych ustawień zdefiniowanych przez producenta oprogramowania 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, przysługujące bezpłatną pomoc techniczną.
- **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, umowe 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 Anti-Virus**. 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**.



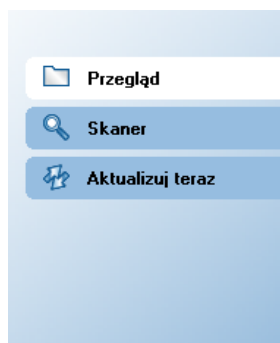
Ikona czerwona oznacza, że stan systemu AVG jest krytyczny! Jeden lub więcej składników nie działa, a system AVG nie może chronić komputera. Należy natychmiast usunąć zgłoszony problem. Jeśli nie jest to możliwe, należy skontaktować się z zespołem [Pomocy Technicznej AVG](#).

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 Anti-Virus** 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 >>](#)
- **LinkScanner** — sprawdza wyniki wyszukiwania wyświetlane przez serwisy internetowe — [szczegóły >>](#)
- **Skaner poczty e-mail** — sprawdza wszystkie przychodzące i wychodzące wiadomości e-mail w poszukiwaniu wirusów — [szczegóły >>](#)
- **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.

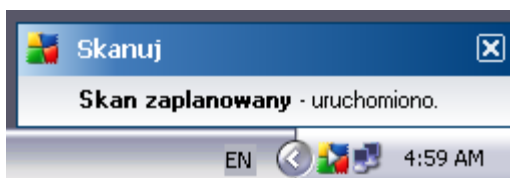
7.6. Ikona na pasku zadań

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

Jeśli  **ikona na pasku zadań** jest kolorowa, oznacza to, że wszystkie składniki systemu AVG są aktywne i w pełni funkcjonalne. Może ona być kolorowa także wtedy, gdy system AVG zasygnalizował błędy, ale użytkownik akceptuje je i celowo [ignoruje stan składników](#).

Ikona szara ze znakiem wykrzyknika  oznacza problem (nieaktywny składnik, stan błędu itd.). W takim przypadku należy dwukrotnie kliknąć **ikone na pasku zadań**, aby otworzyć Interfejs użytkownika i skorygować stan składników.

Ikona na pasku zadań dostarcza także szczegółowych informacji na temat bieżących działań systemu AVG i możliwych zmian w programie (np. uruchomienia automatycznego lub zaplanowanego skanowania lub aktualizacji, zmiany stanu składnika, błędu itp.) w wyskakującym okienku:



Dwukrotne kliknięcie **ikony na pasku zadań** pozwala także szybko, w dowolnym momencie uzyskać dostęp do Interfejsu użytkownika systemu AVG. Kliknięcie **ikony na pasku zadań** prawym przyciskiem myszy otwiera menu kontekstowe zawierające następujące opcje:

- **Otwórz Interfejs użytkownika AVG** — otwiera [Interfejs użytkownika](#).
- **Aktualizuj** — uruchamia natychmiastową [aktualizację](#)

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.

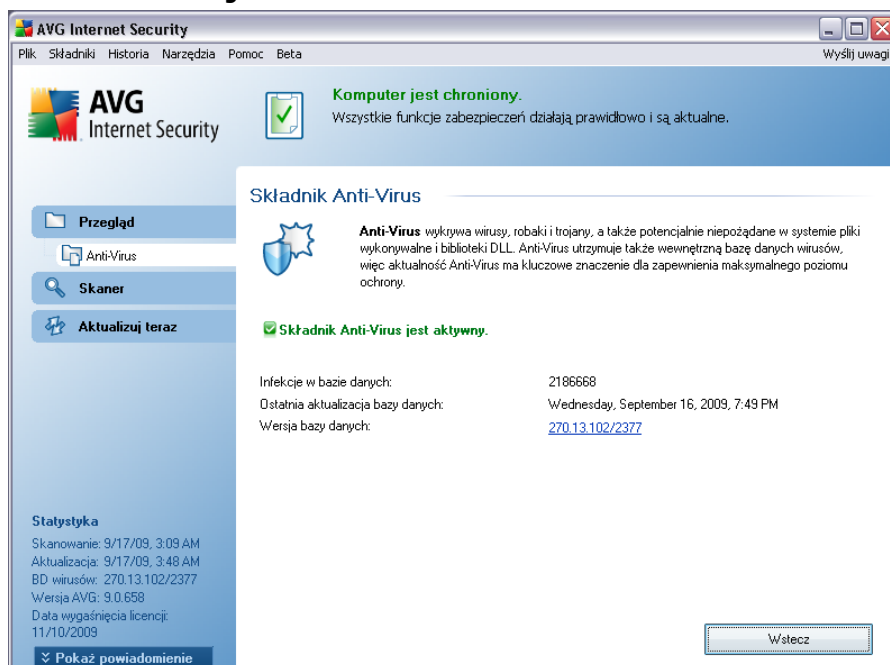
Ważną zaletą ochrony antywirusowej jest fakt, że nie pozwala ona na uruchomienie żadnych znanych wirusów na komputerze!

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

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

Program AVG jest również w stanie analizować i wykrywać wykonywalne aplikacje i biblioteki DLL, które mogą być 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 składnika Anti-Virus



Interfejs składnika **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 składnika 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

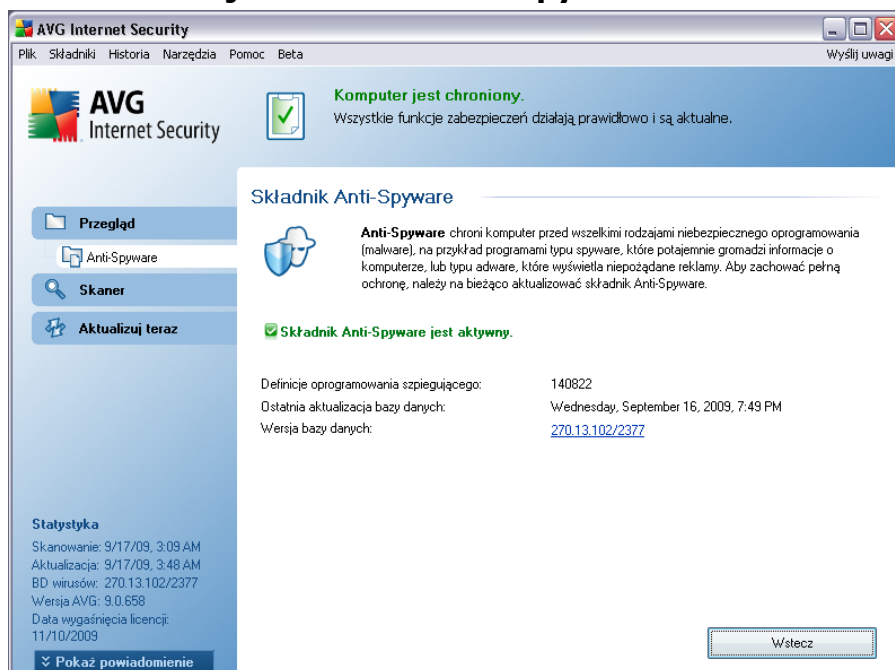
8.2.1. Zasady działania składnika Anti-Spyware

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. Najskuteczniejszą ochroną 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 Anti-Virus**, 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 uspięcone lub nie stwarza zagrożenia, czyli takie, które zostało pobrane, ale nie aktywowane.

8.2.2. Interfejs składowika Anti-Spyware



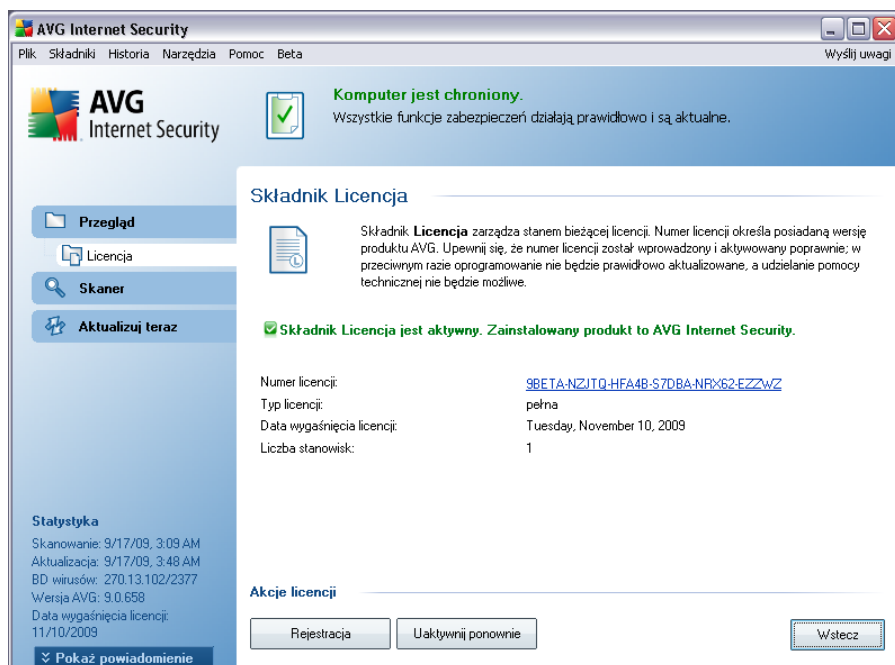
Interfejs składowika **Anti-Spyware** zawiera krótki opis jego funkcji, informacje o bieżącym stanie (Składowik *Anti-Spyware* jest aktywny.), oraz statystyki :

- **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 składowików).

Uwaga: Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składowiki 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. Licencja



Okno dialogowe składnika **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 Anti-Virus** po tej dacie, należy odnowić licencje. [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 Anti-Virus**.

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).

8.4. LinkScanner

8.4.1. 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**:

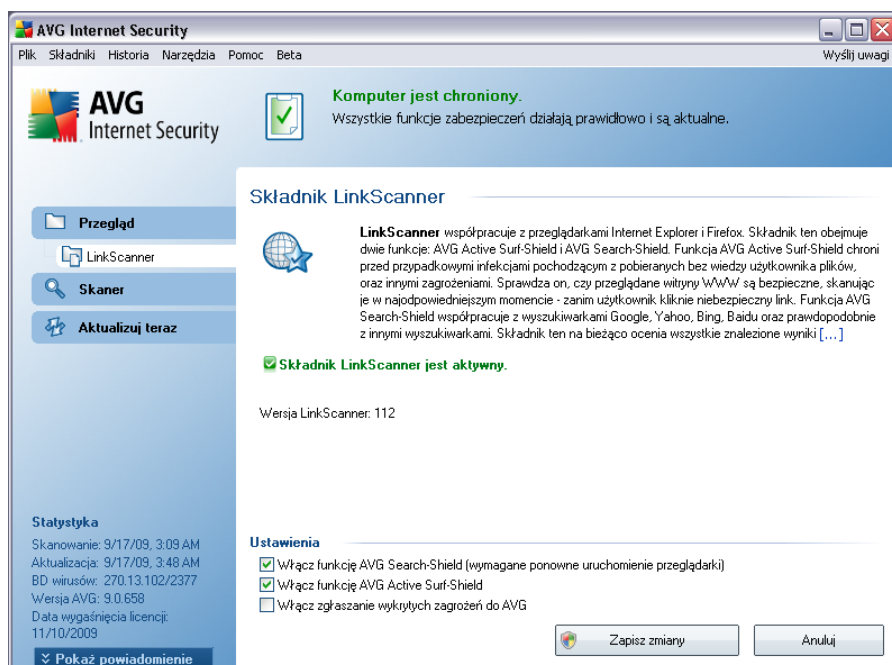
- **Składnik AVG Search Shield** zawiera listę witryn sieci Web (*adresów URL*), które uznane zostały za niebezpieczne. Wszystkie wyniki wyszukiwania otrzymane za pomocą wyszukiwarek Google, Yahoo!, MSN lub Baidu są sprawdzane na podstawie tej listy, a następnie otrzymują ikony werdyktu (w przypadku 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 utworzona nowa szkodliwa witryna sieci Web lub witryna wcześniej uznana za nieszkodliwa 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!

8.4.2. 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** — (*domyślnie 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** — (*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** — 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.


8.4.3. AVG Search-Shield


Podczas wyszukiwania w Internecie funkcja z włączona funkcja **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](#)**!).

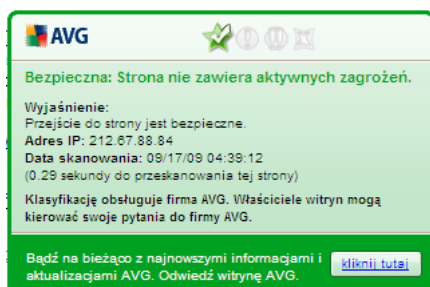
 Strona, do której prowadzi łącze, nie zawiera zagrożeń, ale jest podejrzana (wątpliwości budzi jej pochodzenie lub przeznaczenie, więc nie zaleca się dokonywania na niej zakupów itp.).

 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.

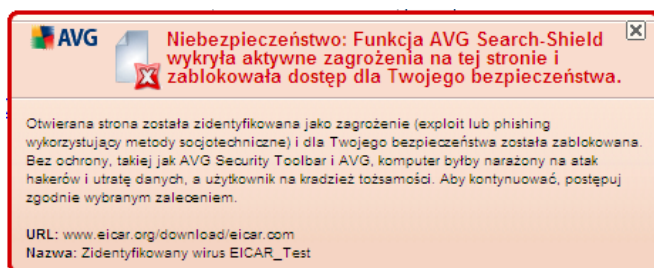
Umieszczenie kursora na wybranej ikonie wyników sprawdzania powoduje wyświetlenie szczegółowych informacji o danym łączu. Informacje te obejmują dodatkowe szczegóły dotyczące zagrożenia (jeśli są dostępne), adres IP łącza oraz czas przeskanowania strony przez AVG:



8.4.4. 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 wyświetlenie 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!

8.5. Ochrona sieci WWW

8.5.1. Zasady działania składnika 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!*

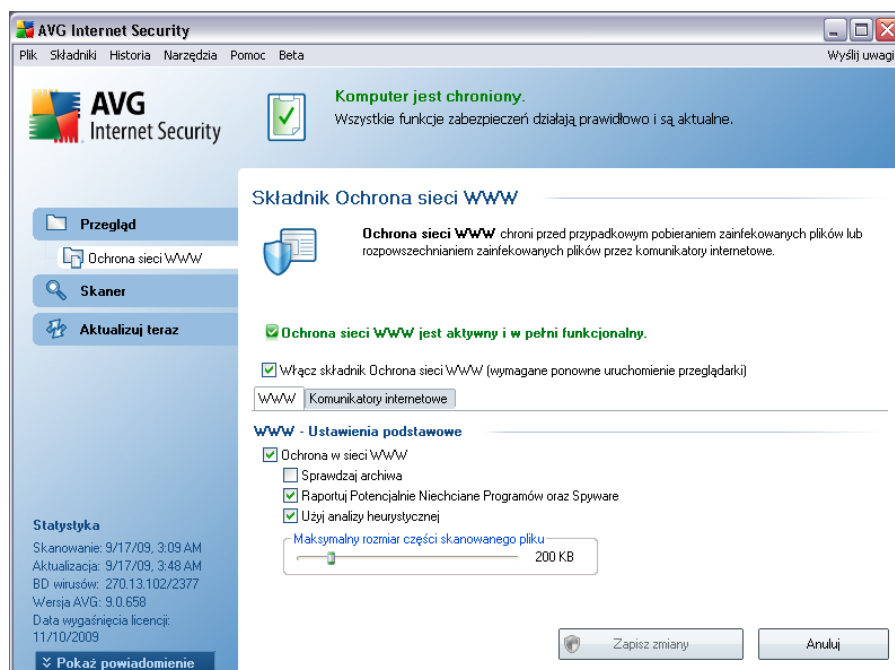
8.5.2. Interfejs składnika Ochrona sieci WWW

Interfejs składnika **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 składnika

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

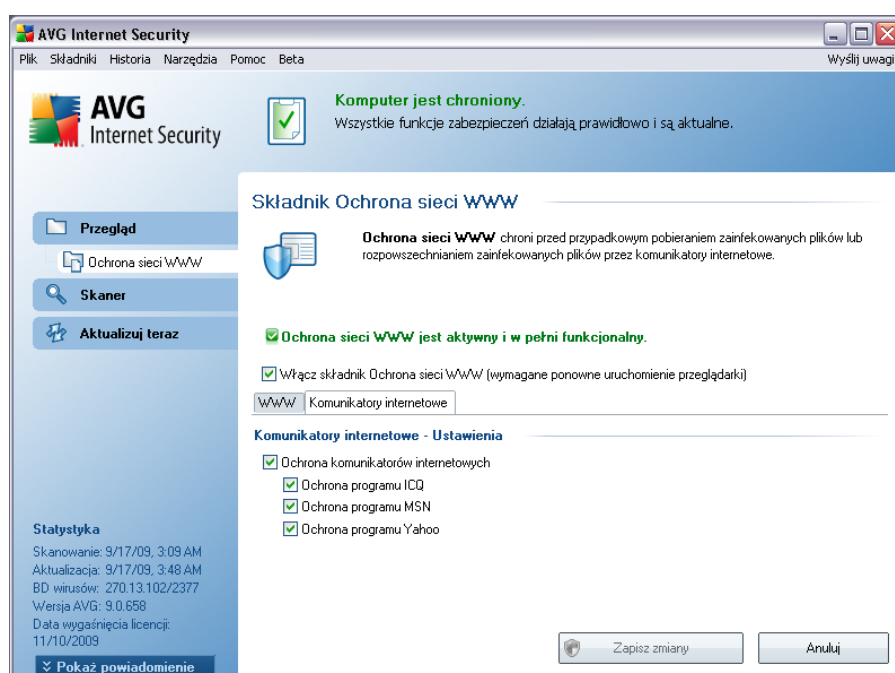
- **WWW** — karta odpowiadająca za skanowanie zawartości witryny internetowych. Interfejs pozwala modyfikować następujące ustawienia:



- **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 składnika 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.).



- 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 **AVGAVG 9 Anti-Virus** 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](#).

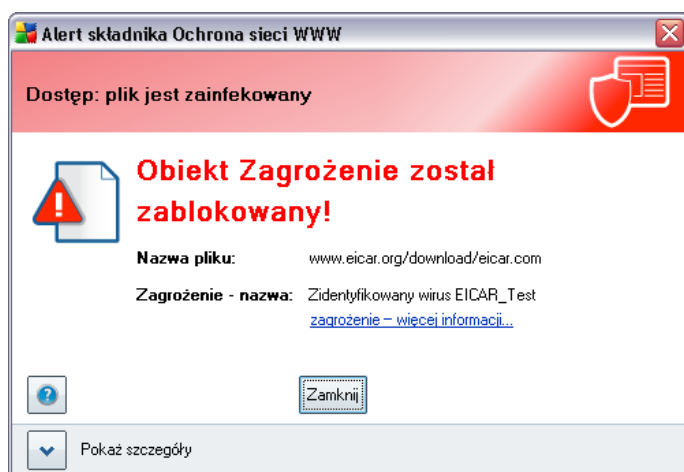
Dostępne przyciski

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

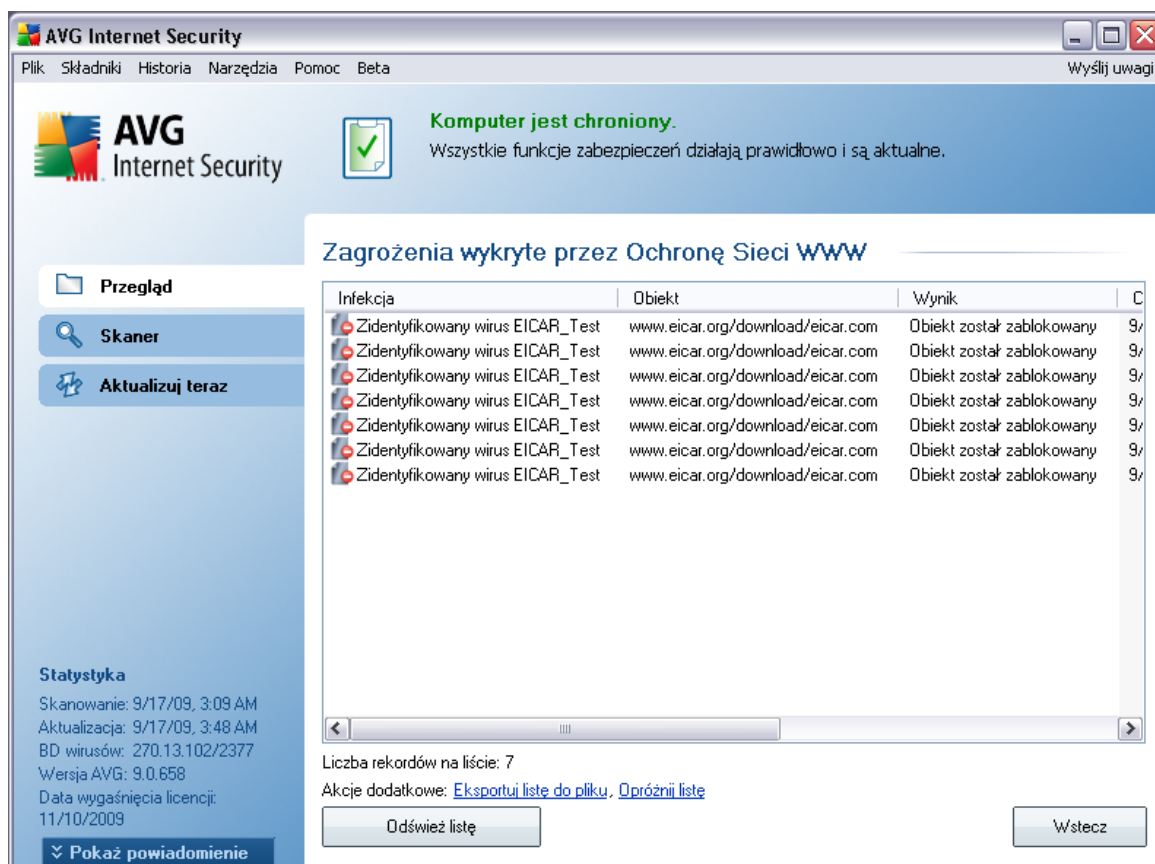
- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- **Anuluj** — powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składników).

8.5.3. 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 usunac wszystkie jej pozycje (**Opróznij liste**). Przycisk **Odswiez liste** pozwala zaktualizowac liste obiektów wykrytych przez skladnik **Ochrona sieci WWW**. Przycisk **Wstecz** przelacza z powrotem do domyslnego okna **Interfejsu uzytkownika AVG** (przegladu skladników).

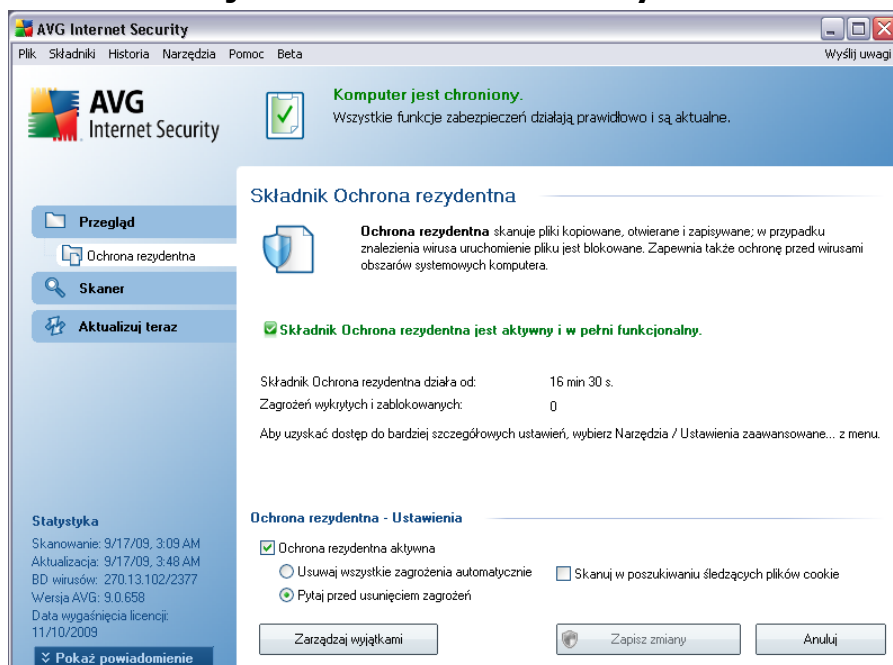
8.6. Ochrona rezydentna

8.6.1. Zasady dzialania Ochrony rezydentnej

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

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

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

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

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](#).

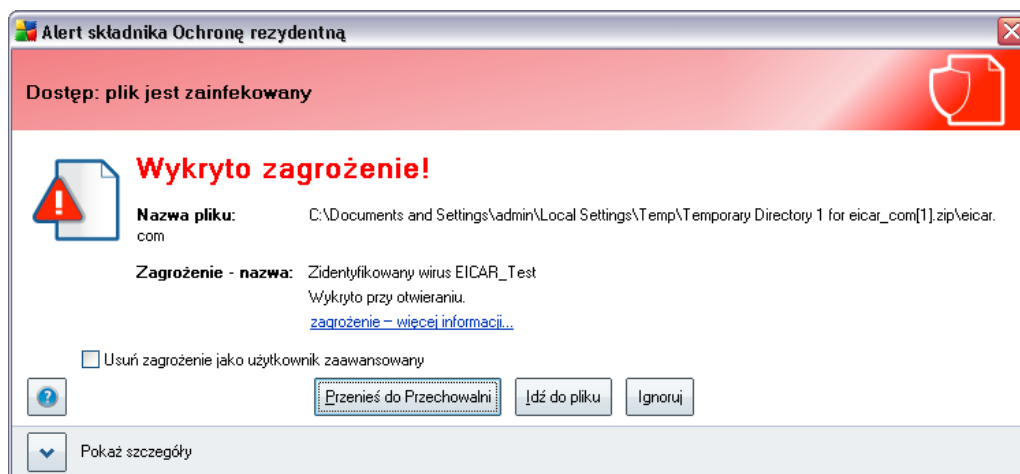
Dostepne przyciski

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).

8.6.3. Zagrożenia wykryte przez Ochronę rezydentną

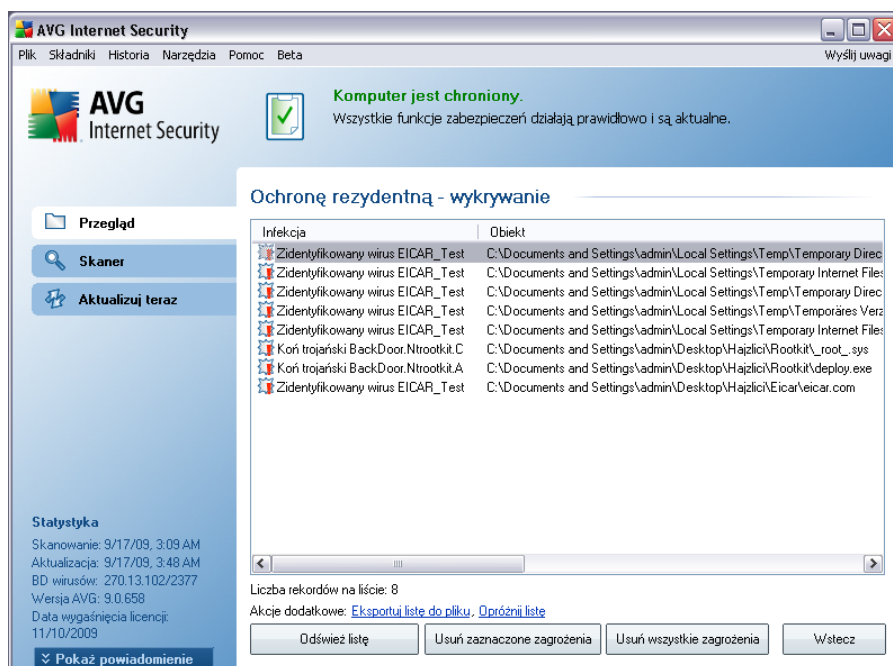
Ochrona rezydentna to składnik służący do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego ostrzeżenia:



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).
- **Przenieś do Przechowalni** — wirus zostanie przeniesiony do [Przechowalni wirusów AVG](#)
- **Przejdź do pliku** — pozwala przejść do lokalizacji podejrzanego obiektu (w *nowym oknie Eksploratora Windows*)
- **Ignoruj** — tej opcji NIE należy używać bez uzasadnionego powodu!

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



Okno **Zagrożenia wykryte przez Ochronę rezydentną** zawiera przegląd obiektów wykrytych i uznanych przez ten **składnik** za niebezpieczne (które następnie wyleczono lub przeniesiono do **Przechowalni wirusów**). 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** przelacza z powrotem do domyślnego **Interfejsu użytkownika**

[AVG](#) (przeglądu składników).

8.7. 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 mogłyby 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 usunąć 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.

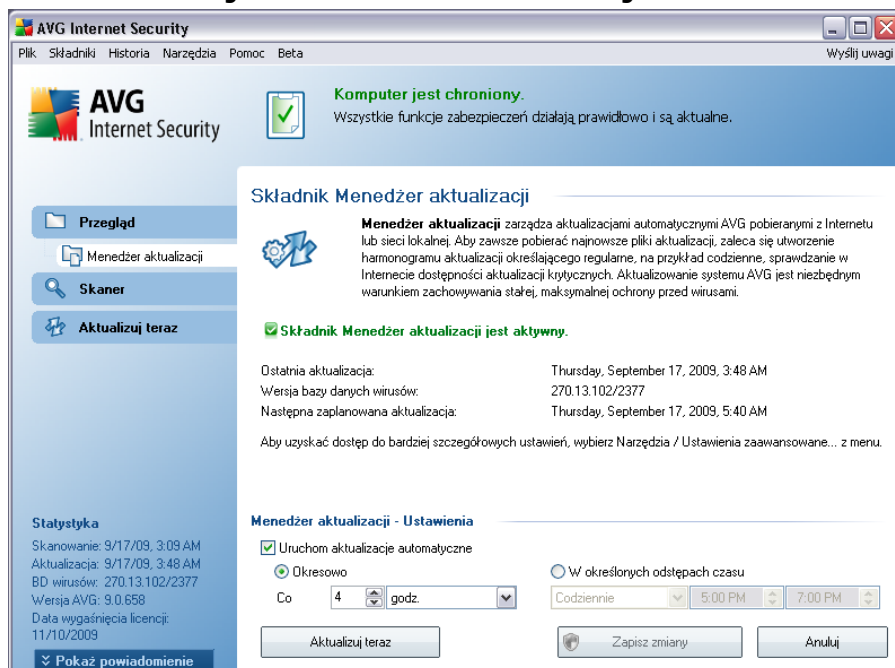
Uwaga: Program AVG Download Manager nie jest odpowiedni do pobierania wersji sieciowych oraz SBS i obsługuje tylko następujące systemy operacyjne: Windows 2000 (SP4 + pakiet zbiorczy SRP), Windows XP (SP2 i nowsze), Windows Vista (wszystkie wersje).

8.7.1. 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](#).

8.7.2. Interfejs Menedzera aktualizacji



Interfejs składowca **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:

- **Okresowo** — należy zdefiniować interwał aktualizacji.
- **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).

8.8. 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 Anti-Virus** 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 Anti-Virus**, jeśli nowe aktualizacje są dostępne.

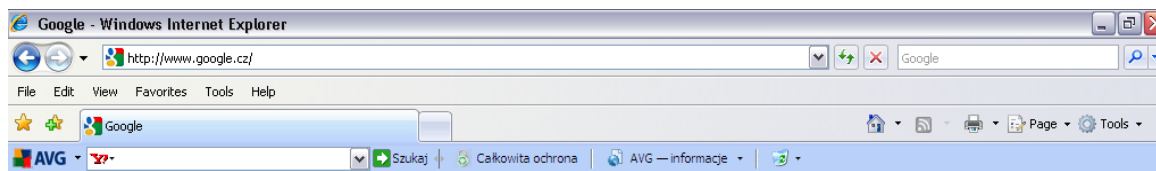
Uwaga: W przypadku korzystania z alternatywnej przeglądarki internetowej (np. *Avant Browser*) mogą wystąpić nieoczekiwane zachowania.

8.8.1. 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:



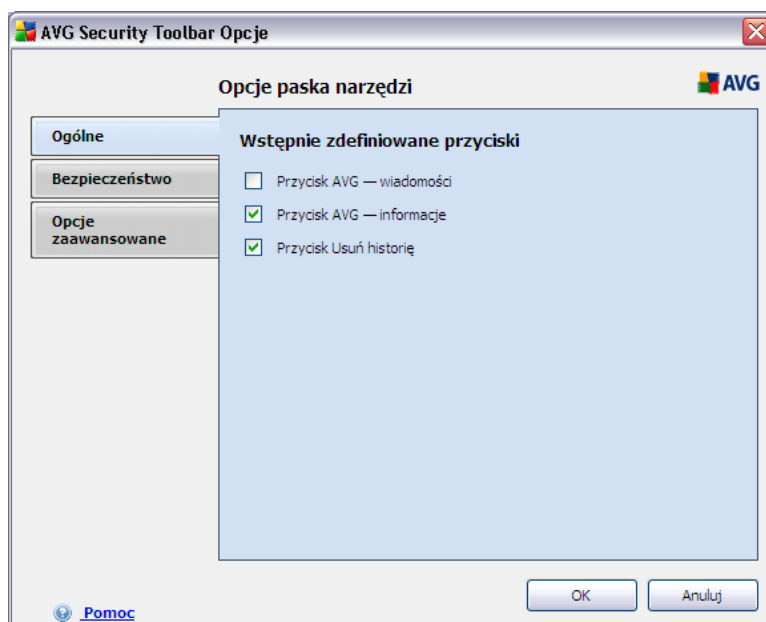
AVG Security Toolbar składa się z następujących elementów:

- **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:
 - **Informacje o pasku narzędzi** — link do strony głównej **AVG Security Toolbar**, zawierającej szczegółowe informacje o działaniu paska.
 - **Uruchom AVG 9.0** — powoduje otwarcie interfejsu użytkownika systemu [AVG](#)
 - **Opcje** — powoduje otwarcie okna dialogowego, w którym można określać ustawienia paska narzędzi **AVG Security Toolbar** — patrz rozdział [Opcje paska narzędzi AVG Security Toolbar](#)
 - **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.
 - **Aktualizacja** — pozwala sprawdzić dostępność nowych aktualizacji **dotyczących Paska narzędzi AVG**
 - **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/>).

8.8.2. Opcje Paska narzędzi AVG Security Toolbar

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

- **Ogólne**



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

- **Przycisk Nowości AVG** — ta opcja pozwala wyświetlić przycisk **Nowości AVG**. Kliknięcie tego przycisku na panelu **Paska narzędzi AVG Security Toolbar** otwiera rozwijane menu z linkami do aktualnych informacji prasowych o systemie AVG.
- **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
- **Przycisk Usun historie** — przycisk ten pozwala *usunąć całą historię*, lub *usunąć historię wyszukiwania, przeglądania i pobierania* lub tylko *usunąć ciasteczka* 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:

- **Bezpieczeństwo przeglądarki** — te pozycje należy zaznaczyć, aby aktywować lub wyłączyć **funkcje AVG Search-Shield** i/lub **funkcje AVG Surf-Shield**
- **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 szczególne ustawienia **Paska narzędzi AVG Security Toolbar**:

- **Ustaw i zachowaj Yahoo! jako domyślną wyszukiwarkę używaną na pasku adresu** — (domyślnie włączone) — jeśli ta opcja jest zaznaczona, możliwe jest wyszukiwanie stron bezpośrednio w pasku adresu przeglądarki internetowej, przy użyciu Yahoo!
- **Pokaż pole wyszukiwarki Yahoo! na nowych kartach** — (domyślnie włączone) — zaznaczenie tej opcji powoduje wyświetlanie pola wyszukiwarki Yahoo! na każdej nowo otwartej karcie przeglądarki internetowej.
- **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.
- **Ustaw i zachowaj Yahoo! jako domyślną wyszukiwarkę** — (domyślnie wyłączone) — Yahoo! jest domyślną wyszukiwarką internetową **Paska narzędzi AVG Security Toolbar**, a aktywowanie tej opcji powoduje, że staje się również domyślną wyszukiwarką przeglądarki internetowej.

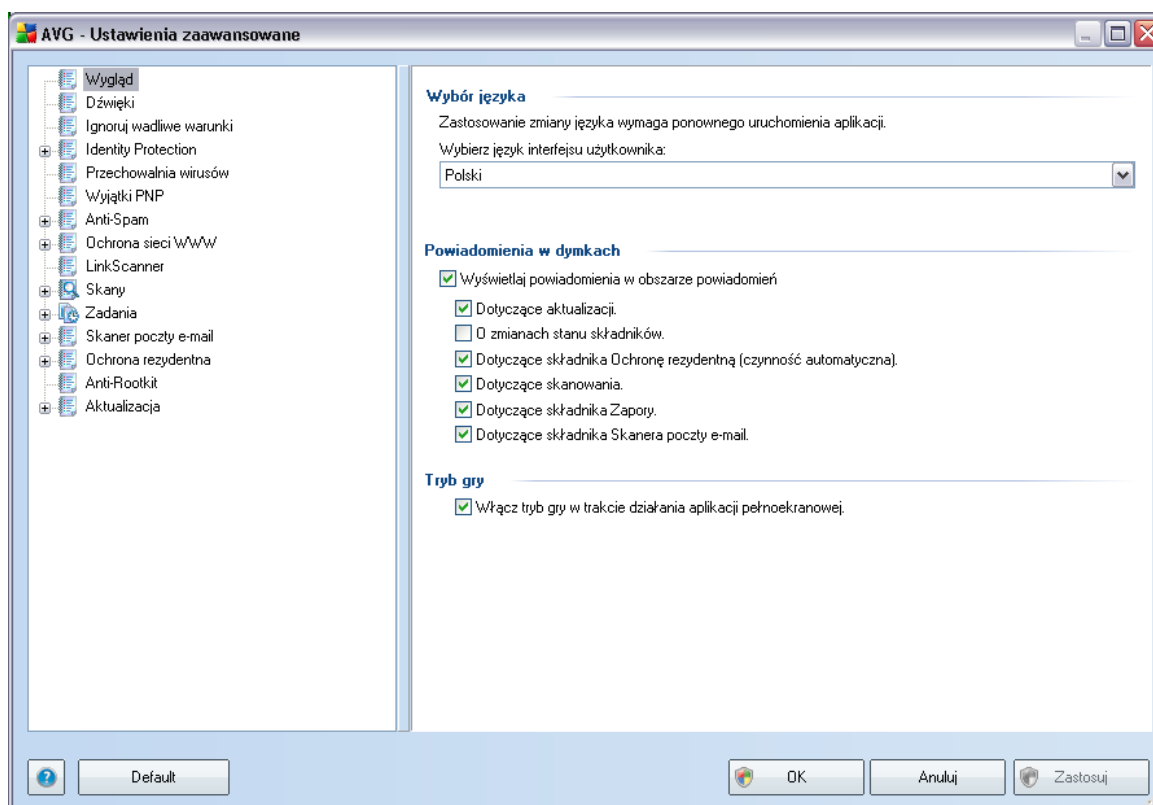
- **Ponownie wyświetlaj Pasek narzędzi AVG Security Toolbar, jeśli został ukryty (po tygodniu)** — (domyślnie włączone) — ta opcja jest domyślnie aktywna i w przypadku przypadkowego ukrycia **Paska narzędzi AVG Security Toolbar** zostanie on ponownie wyświetlony po upływie tygodnia.

9. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG 9 Anti-Virus** 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 składowki, 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:

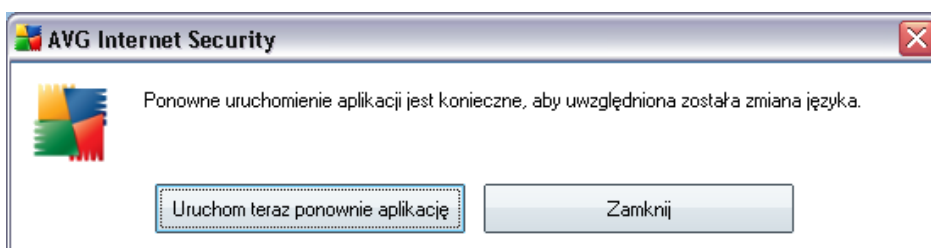


Wybór języka

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:
 - **Wyswietlaj w obszarze powiadomien komunikaty dotyczace aktualizacji** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace rozpozecia, postepu i zakonczenia aktualizacji systemu AVG;
 - **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 zgloszenia stanu bledu skladnika, opcja ta okresla funkcje informacyjna [ikony na pasku zadani](#) (zmiany koloru), ktora wskazuje na problemy z dowolnym skladnikiem systemu AVG;

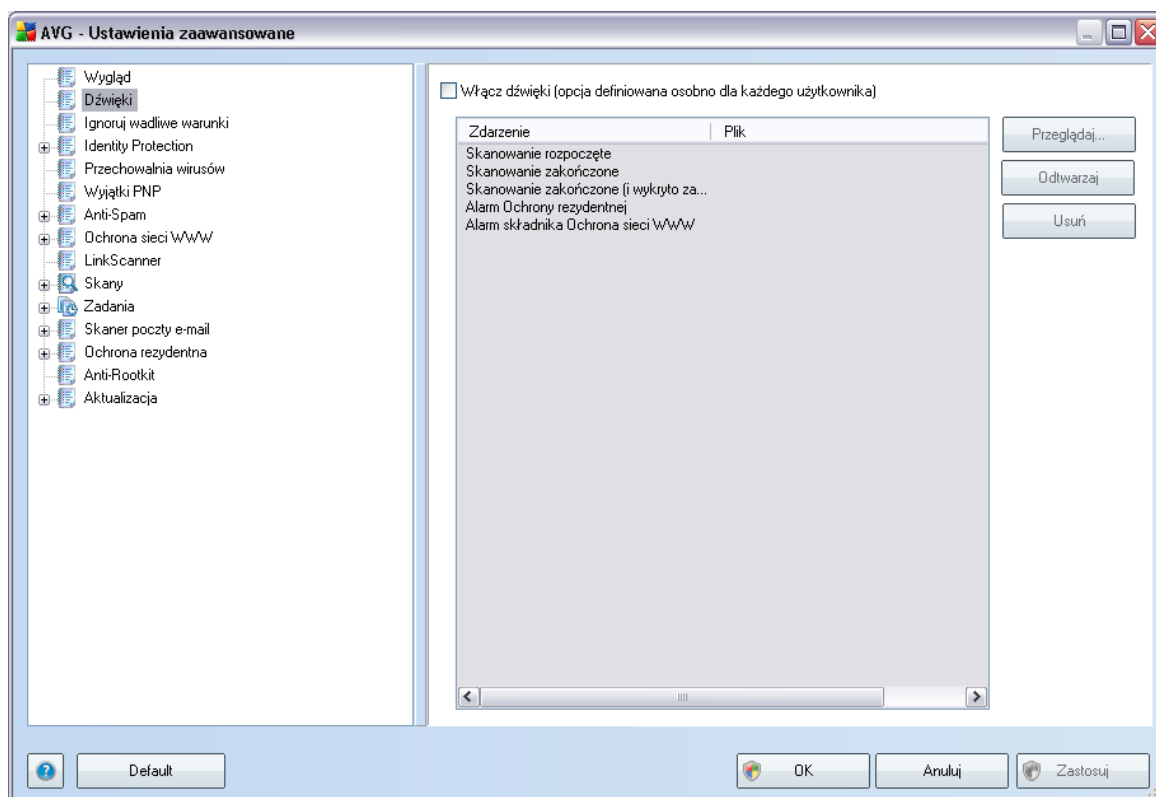
- **Wyswietlaj w obszarze powiadomien komunikaty dotyczace skladnika [Ochrona rezydentna](#)** — nalezy okreslic, czy informacje dotyczace zapisywania, kopiowania i otwierania plikow maja byc wyswietlane, czy pomijane;
- **Wyswietlaj w obszarze powiadomien komunikaty dotyczace [skanowania](#)** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace automatycznego rozpoczecia, postepu i zakonczenia zaplanowanego skanowania;
- **Wyswietlaj komunikaty w obszarze powiadomien dotyczace skladnika [Skaner poczty e-mail](#)** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace skanowania wszystkich przychodzacych i wychodzacych wiadomosci e-mail.

Tryb gry

Ta funkcja systemu AVG przeznaczona jest dla programow dzialajacych w trybie pelnoekranowym, ktore do komunikacji uzywaja internetu. Ewentualne okna dialogowe systemu AVG mogleby zaklócac ich dzialanie (*np. powodowac ich minimalizacje lub zniekszaltcac obraz*). Aby tego uniknac, nalezy 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, nalezy zaznaczyc pole wyboru **Wlacz efekty dzwiekowe** (*domyslnie wylaczone*), aby wlaczyc liste czynnosci systemu AVG:

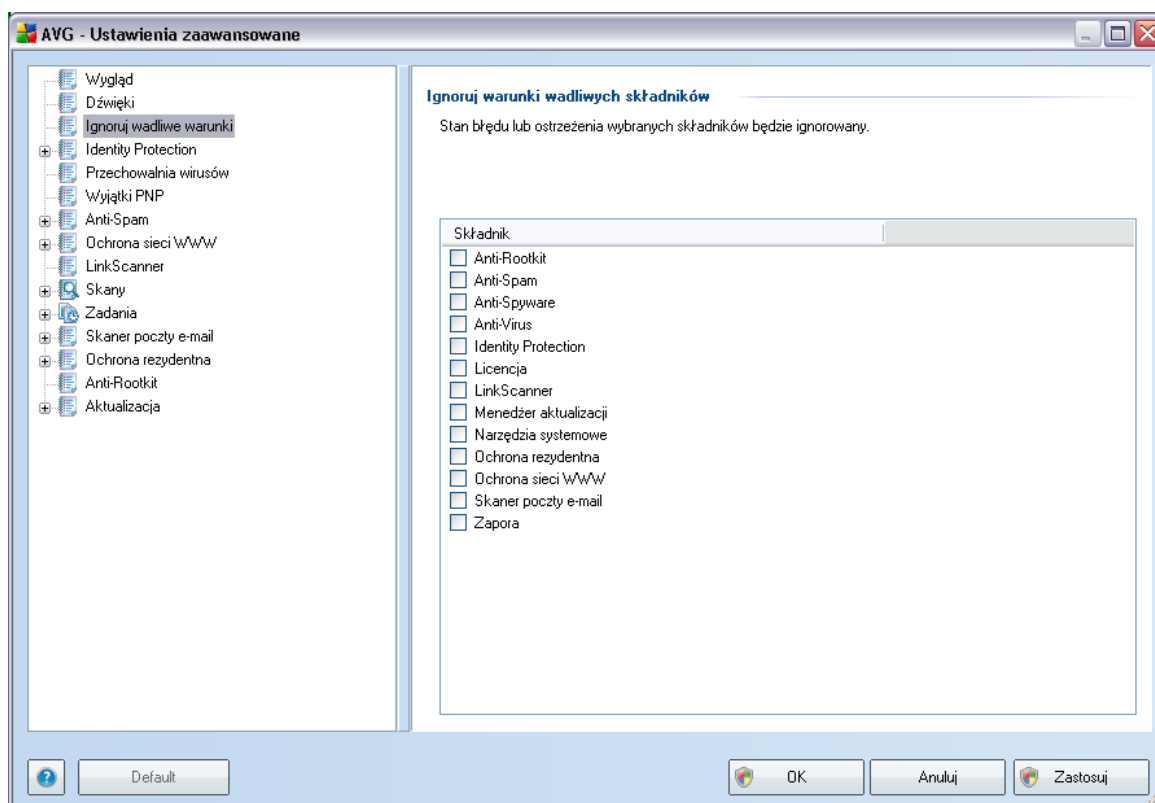


Następnie należy wybrać odpowiednie zdarzenie z listy i wskazać plik dźwiękowy, który ma zostać do niego przypisany (**Przełączaj**). Aby odtworzyć wybrany dźwięk, należy zaznaczyć go na liście i nacisnąć przycisk **Odtwórz**. Aby usunąć dźwięk przypisany do określonego zdarzenia, należy użyć przycisku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

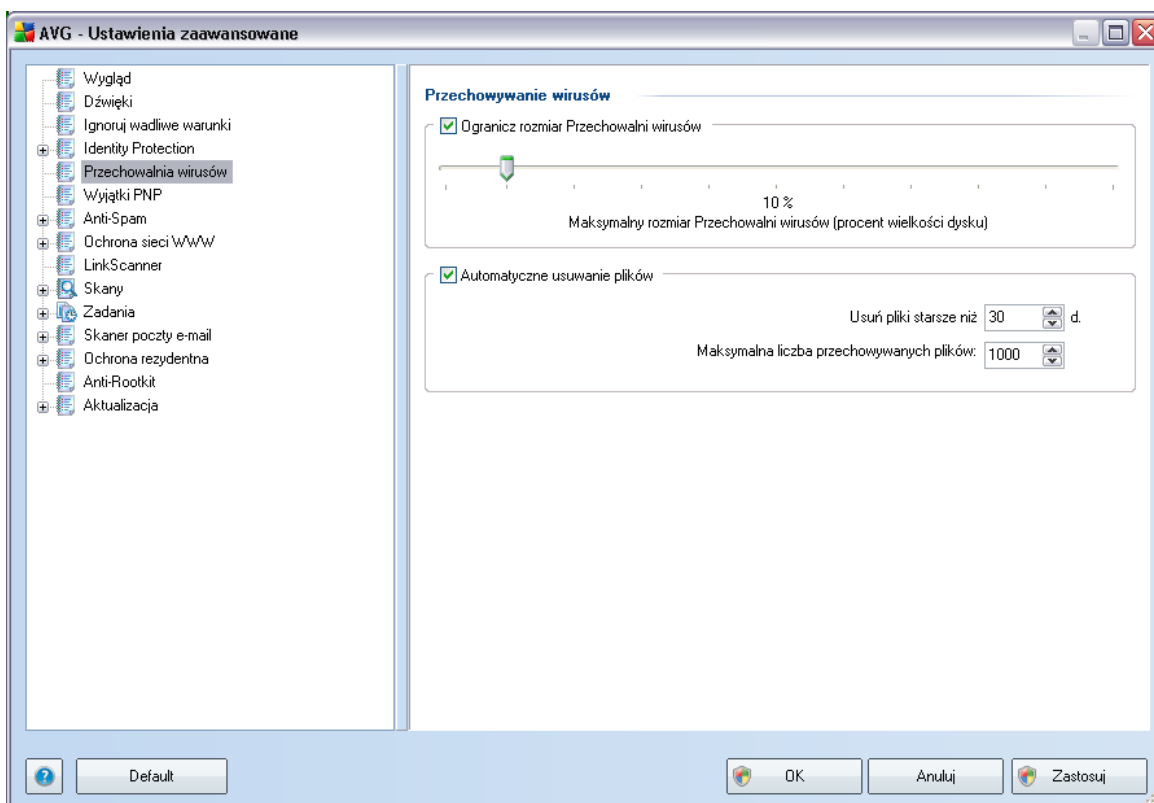
- **ikona na pasku zadan** — gdy wszystkie skladniki systemu AVG dzialaja prawidlowo, wyswietlana ikona jest czterokolorowa; w przypadku bledu wyswietlany jest zolty wykrzyknik,
- tekstowy opis problemu jest widoczny w sekcji **Informacje o stanie bezpieczenstwa** okna glownego AVG

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. Przechowalnia wirusów



W oknie **Przechowalnia wirusów** można zdefiniować kilka parametrów dotyczących administrowania obiektami znajdującymi się w [Przechowalni](#):

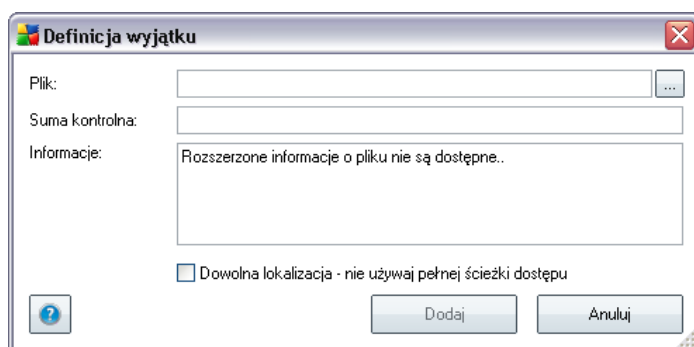
- **Ogranicz rozmiar Przechowalni wirusów** — za pomocą suwaka należy określić maksymalny rozmiar [Przechowalni wirusów](#). Rozmiar jest

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

- **Plik** — zawiera nazwe odpowiedniej aplikacji.
- **Sciezka pliku** — wyswietla sciezke dostepu do aplikacji.
- **Suma kontrolna** — wyswietla unikatowa „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 wyjatku (patrz nizej)*), w którym mozna zmienic parametry istniejacego wyjatku.
- **Usun** — usuwa wybrany element z listy wyjatków.
- **Dodaj wyjatek** — otwiera okno edycji, w którym mozna zdefiniowac parametry nowego wyjatku:

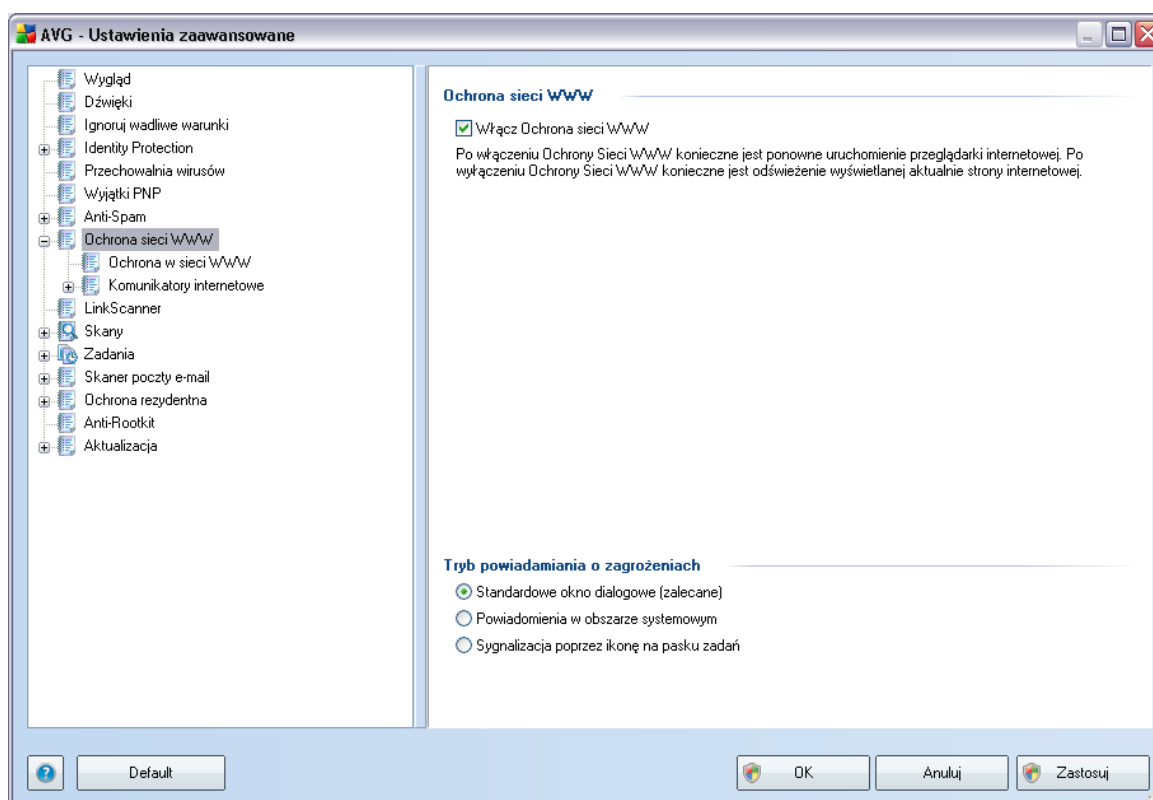


- **Plik** — nalezy podac pelna sciezke do pliku, który ma byc oznaczony jako wyjatek.
- **Suma kontrolna** — wyswietla unikatowa „signature” wybranego pliku. Suma ta jest generowanym automatycznie ciagiem znaków, który pozwala programowi AVG jednoznacznie odróżniac wybrany plik od innych. Jest ona generowana i wyswietlana po pomyslnym dodaniu

pliku.

- **Informacje o pliku** — wyświetla wszelkie dodatkowe dostępne informacje na temat pliku (*licencja/wersja itp.*).
- **Dowolna lokalizacja — nie używaj pełnej ścieżki dostępu** — jeśli plik ma być zdefiniowany jako wyjątek jedynie dla konkretnej lokalizacji, wówczas należy pozostawić to pole niezaznaczone.

9.6. 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:

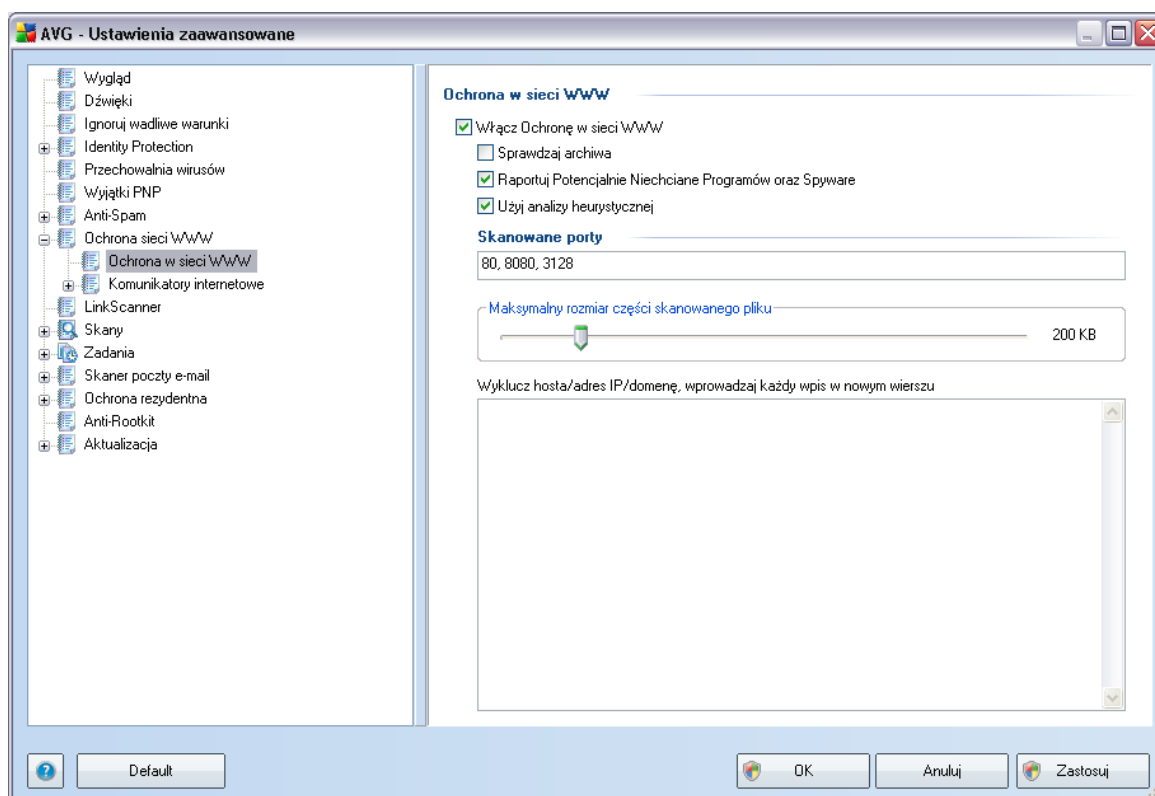
- **Ochrona WWW**

- [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.

9.6.1. Ochrona WWW

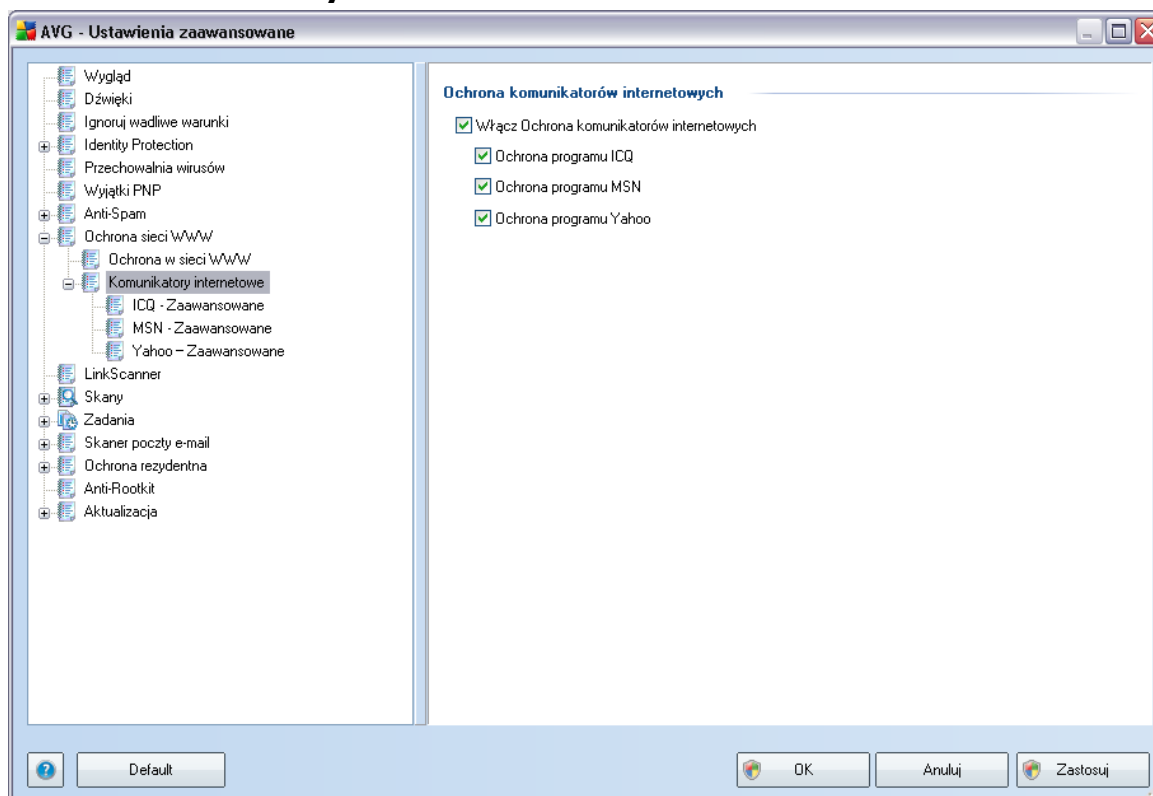


W oknie dialogowym **Ochrona w sieci WWW** można edytować konfigurację dotyczącą skanowania zawartości witryn internetowych. Interfejs edycji pozwala konfigurować następujące opcje:

- **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:

- **Skanuj wewnątrz archiwów** — skanowanie ma obejmować także archiwa zawarte na wyświetlanych stronach WWW.
- **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](#).
- **Użyj heurystyki** — skanowanie zawartości wyświetlanych stron ma wykorzystywać [analizę heurystyczną](#) (*dynamiczna emulacja instrukcji skanowanego obiektu w wirtualnym środowisku*).
- **Skanowane porty** — to pole zawiera listę standardowych numerów portów http. Jeśli konfiguracja komputera różni się od standardowej, można zmienić numery portów zgodnie z potrzebami.
- **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.
- **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.

9.6.2. Komunikatory internetowe

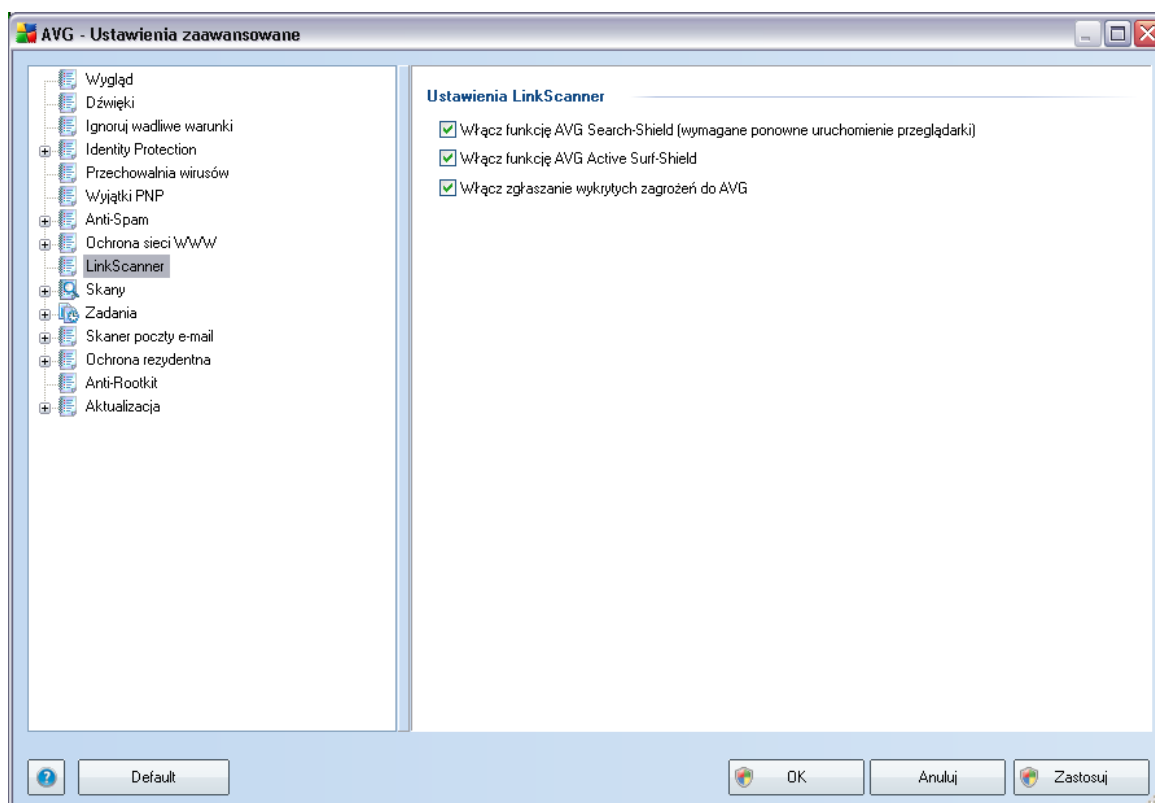


W oknie dialogowym **Ochrona komunikatorów internetowych** można edytować ustawienia składnika **Ochrona sieci WWW** dotyczące monitorowania plików przesyłanych za pośrednictwem komunikatorów. Obecnie obsługiwane są trzy komunikatory: **ICQ**, **MSN** i **Yahoo** — jeśli składnik **Ochrona sieci WWW** 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).

9.7. LinkScanner

Okno dialogowe **Ustawienia składnika LinkScanner** umożliwia włączenie/ wylączenie 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.

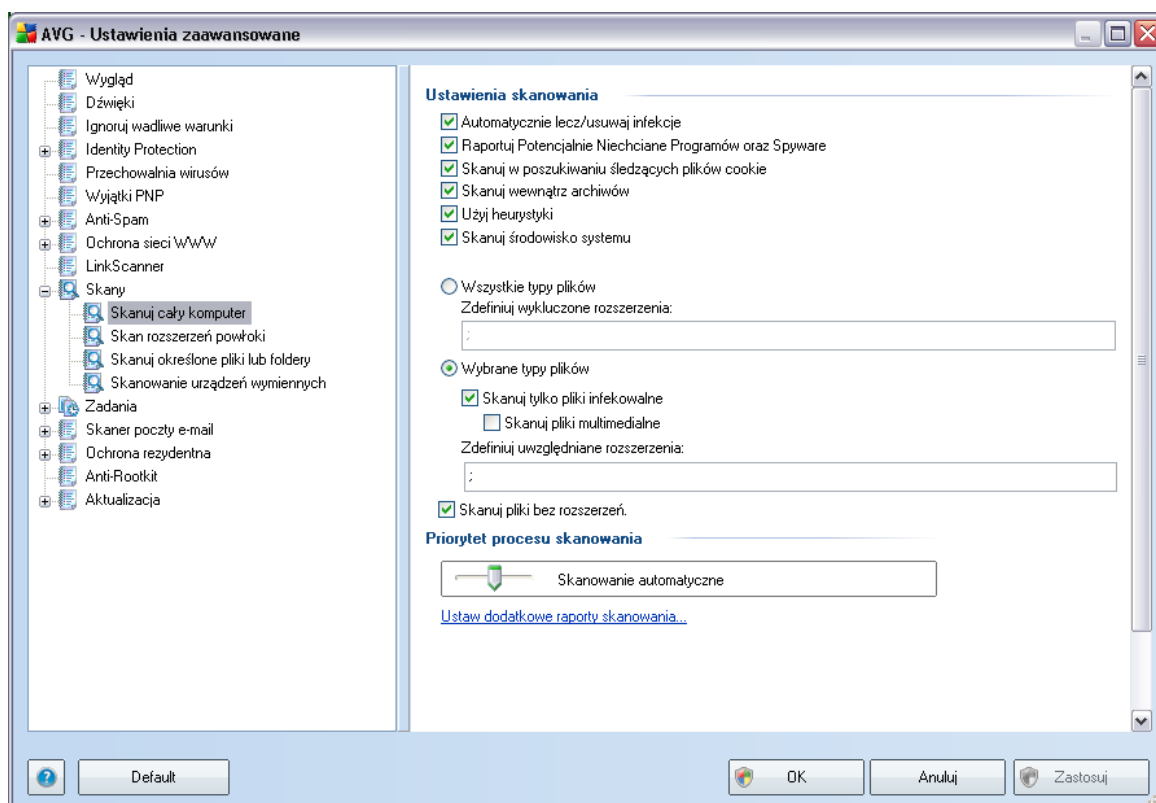
9.8. Skany

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

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

9.8.1. 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/usuwaj 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 składnika [Anti-Spyware](#) określa, że skanowanie ma wykrywać pliki cookie (pliki cookie są w protokole HTTP używane do uwierzytelniania, śledzenia 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

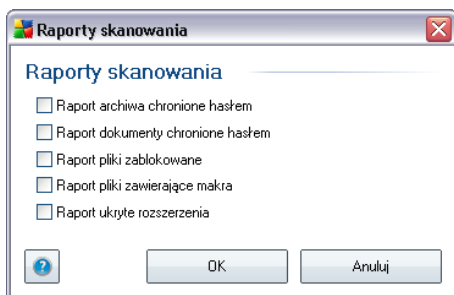
- **Wszystkie typy plików** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, który nie powinny być skanowane; LUB
- **Wybrane typy plików** — skanowane będą tylko pliki infekowalne (pliki, które nie mogą zostać zainfekowane, nie będą skanowane, 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 niezmięnie 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 zadana prędkość 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.

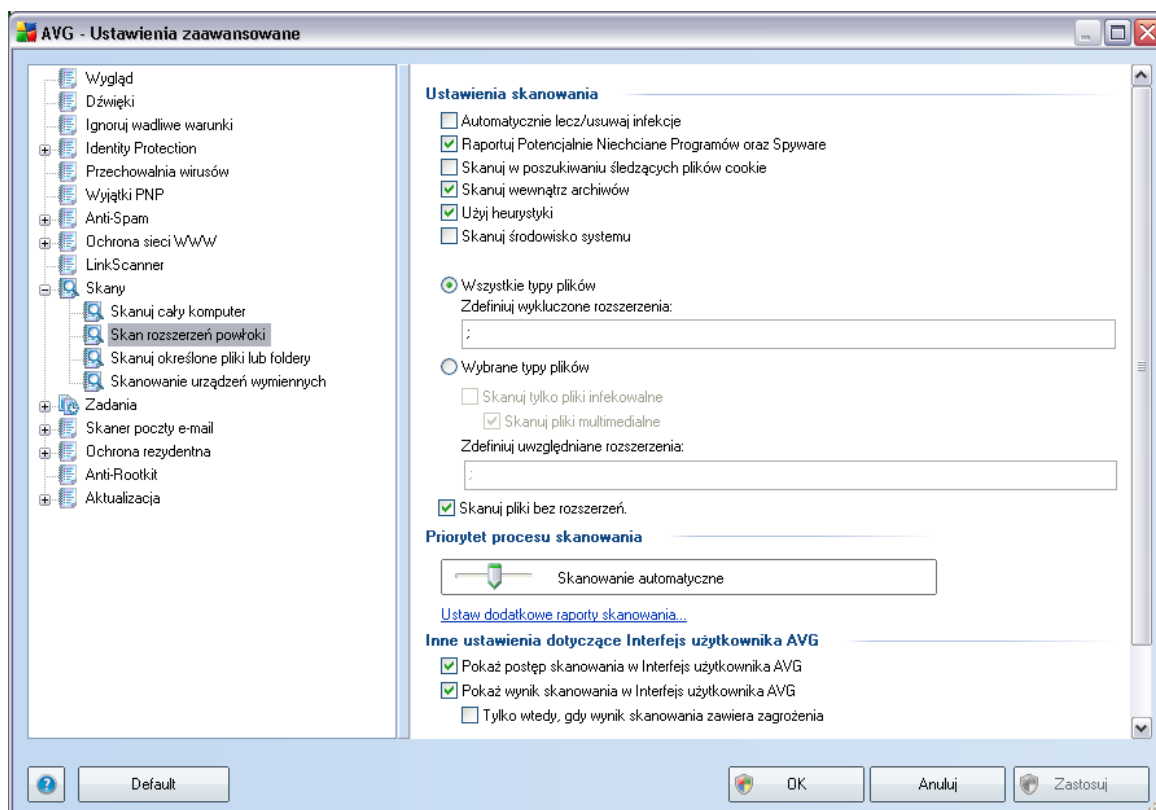
Ustaw dodatkowe raporty skanowania...

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



9.8.2. 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](#):

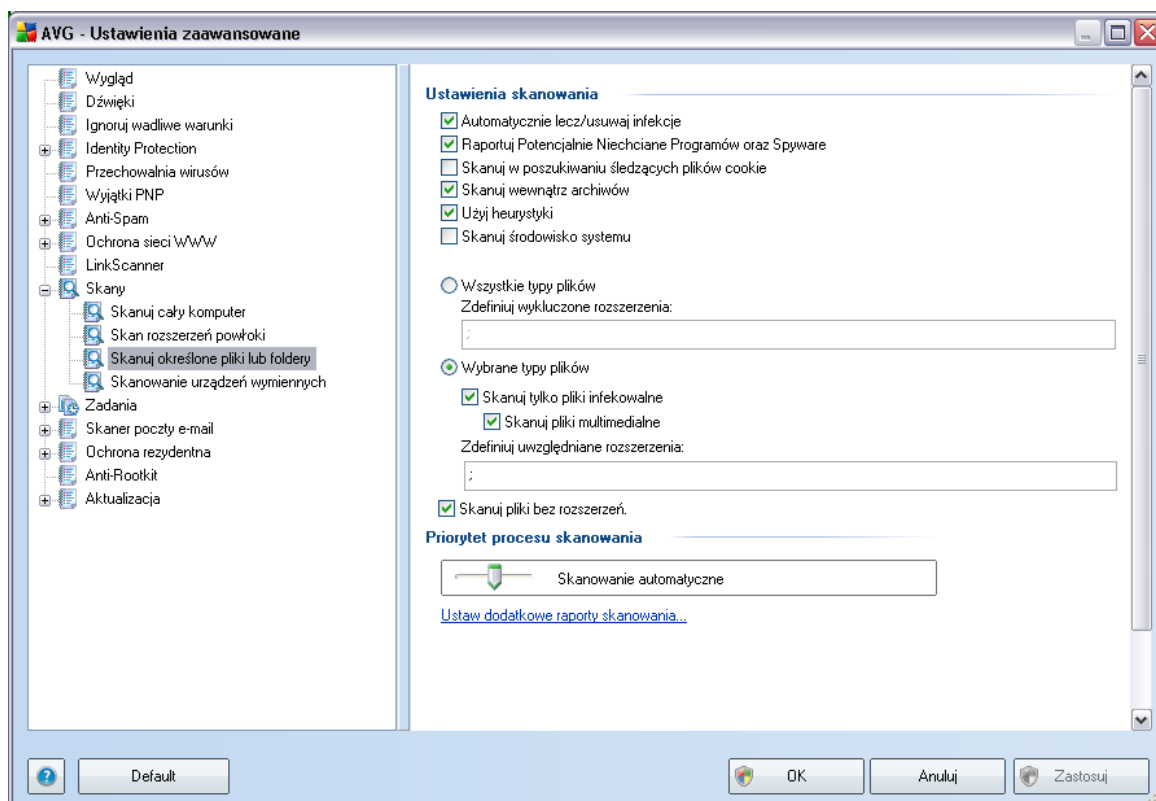


Lista parametrów jest identyczna jak dla testu [Skan całego komputera](#). Ustawienia domyślne są jednak inne: większość opcji [Skanu całego komputera](#) jest aktywna, natomiast w przypadku testu [Skan rozszerzenia powłoki \(Skanowanie z poziomu Eksploratora Windows\)](#) wybrane są tylko najistotniejsze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

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

9.8.3. 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:

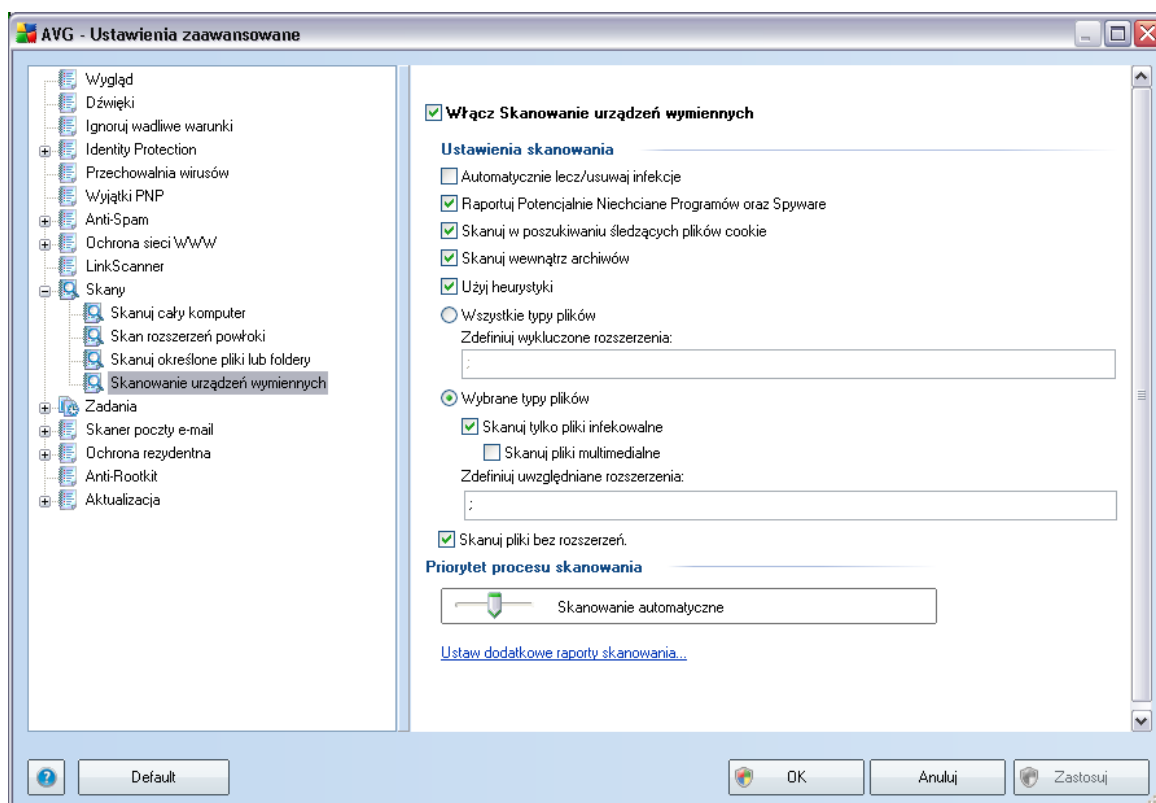


Wszystkie parametry ustawiane w tym oknie dialogowym odnoszą się tylko do obszarów wybranych do **skanowania określonych plików lub folderów!** Zaznaczenie opcji ***Skanuj w poszukiwaniu programów typu rootkit*** w tym oknie konfiguracyjnym oznacza, że wykonane zostanie tylko szybkie wyszukiwanie programów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

9.8.4. 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](#).

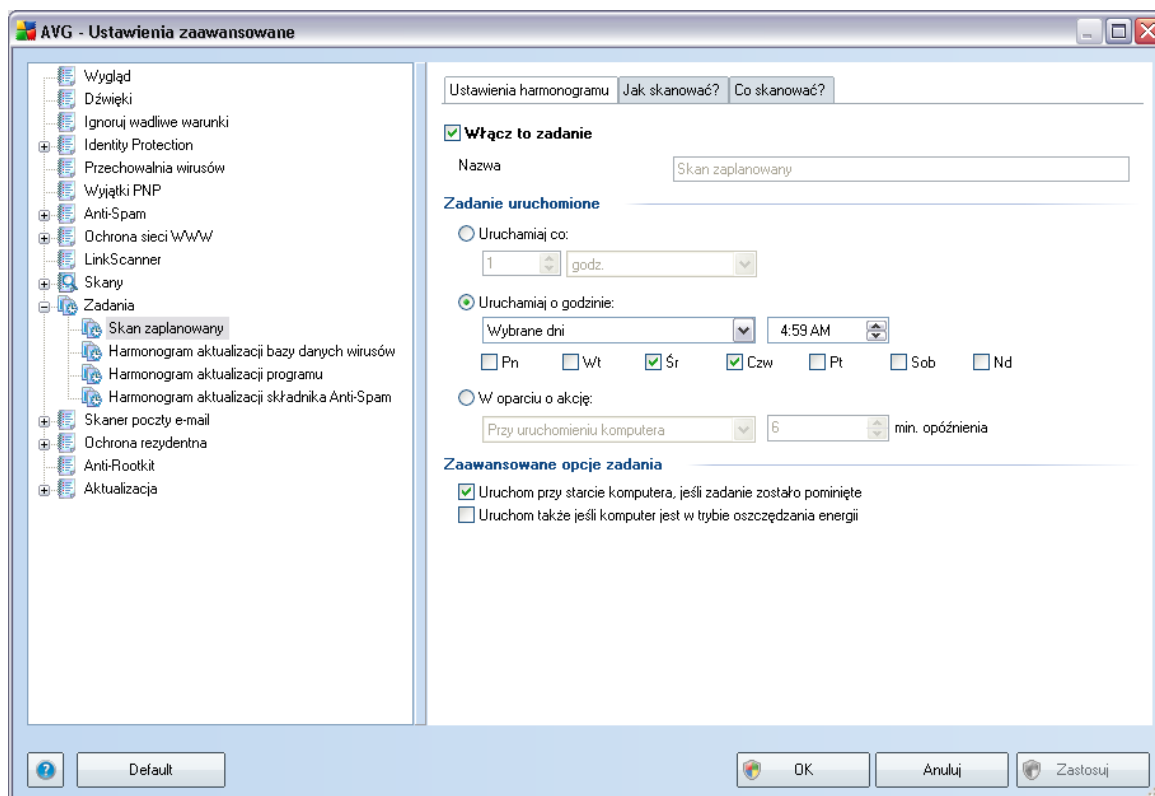
9.9. Zaplanowane zadania

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

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

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

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

W tym samym oknie mozna szczególowo okreslic nastepujace parametry skanowania:

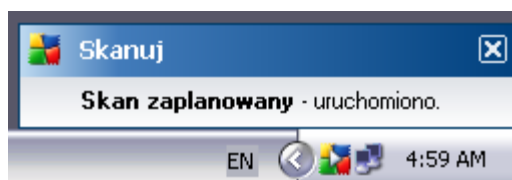
Zadanie uruchomione

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

Zaawansowane opcje harmonogramu

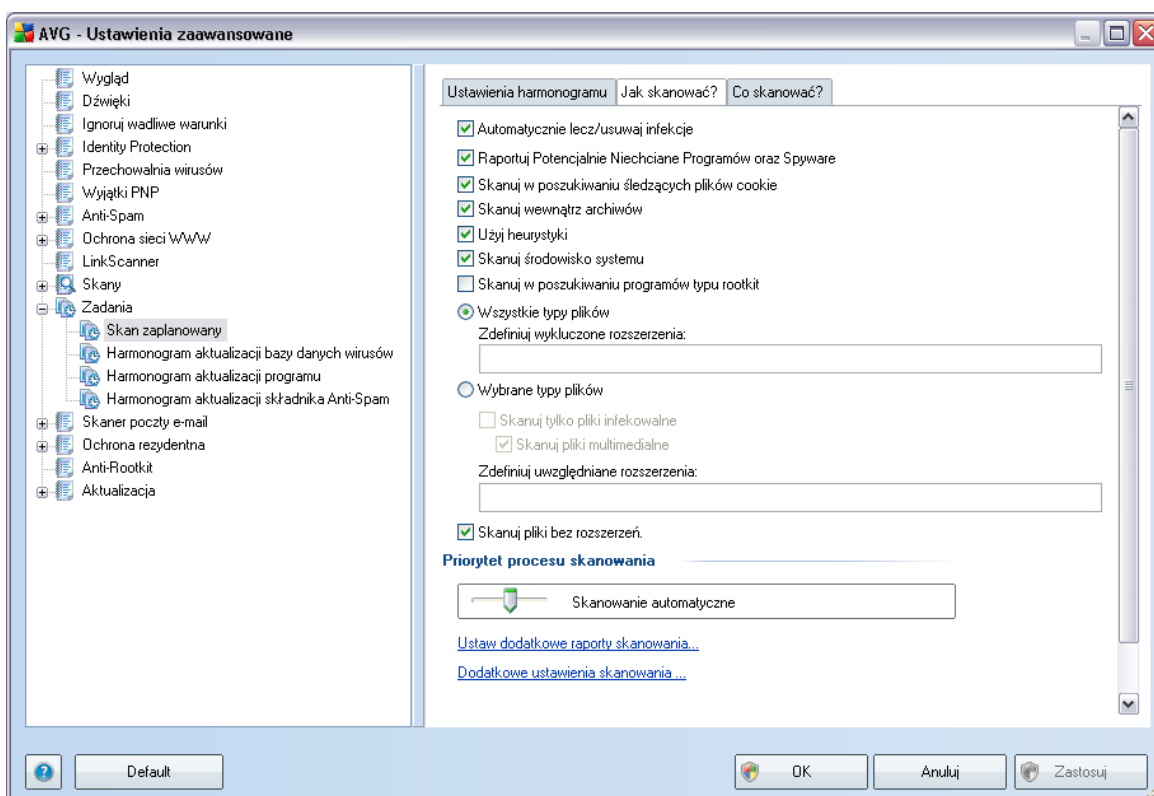
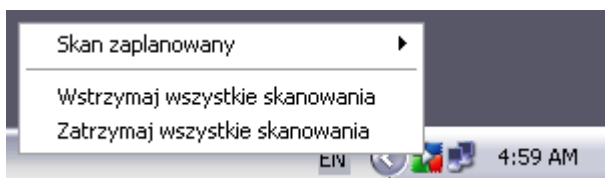
Ta sekcja umozliwia zdefiniowanie warunków uruchamiania skanowania w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

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



Nastepnie pojawi sie tam nowa ikona AVG (kolorowa, z biala strzalka — jak powyzej),

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. 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 próbe automatycznego wyleczenia go. Jesli zainfekowanego pliku nie mozna wyleczyc, lub jesli opcja ta zostanie wyliczona, system powiadomi o wykryciu wirusa i zapyta o sposob reakcji na infekcje. Zalecana czynnoscia jest przeniesienie zainfekowanego pliku do [Przechowalni wirusów](#).

- **Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujace** — (domyslnie wlaczona) parametr ten kontroluje funkcje skladnika [Anti-Virus](#), które pozwalaja [wykrywac potencjalnie niechciane programy](#) (pliki wykonywalne mogace dzialac jak oprogramowanie szpiegujace lub reklamowe), a nastepnie blokowac je lub usuwac.
- **Skanuj w poszukiwaniu sledzacych plików cookie** — (domyslnie wlaczona) ten parametr skladnika [Anti-Spyware](#) okresla, czy wykrywane maja byc pliki cookie (uzywane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach — np. preferencji wygladu witryny i zawartosc koszyków w sklepach internetowych).
- **Skanuj wewnatrz archiwów** — (domyslnie wlaczona) parametr ten okresla, czy skanowanie ma obejmowac wszystkie pliki, nawet te znajdujace sie wewnatrz niektórych typów archiwów, np. ZIP, RAR itd.
- **Uzyj heurystyki** — (domyslnie wlaczona) analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w srodowisku wirtualnej maszyny) jest jedna z metod wykrywania wirusów w czasie rzeczywistym.
- **Skanuj srodowisko systemu** — (domyslnie wlaczona) skanowanie obejmie takze obszary systemowe komputera.
- **Skanuj w poszukiwaniu programów typu rootkit** — zaznaczenie tej pozycji pozwala dolaczyc wykrywanie programów typu rootkit do operacji skanowania calego komputera. Test Anti-Rootkit mozna takze uruchomic niezaleznie, dzieki interfejsowi skladnika **Anti-Rootkit**

Nastepnie nalezy zdecydowac, czy skanowane maja byc

- **Wszystkie typy plików** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen plików, który nie powinny byc skanowane; LUB
- **Wybrane typy plików** — skanowane beda tylko pliki infekowalne (pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe i niewykonywalne), z uwzglednieniem multimediów (plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowanie skróci sie jeszcze bardziej, poniewaz takie pliki czesto sa duze, a nie sa podatne na

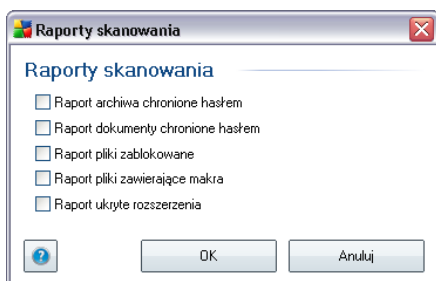
infekcje). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

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

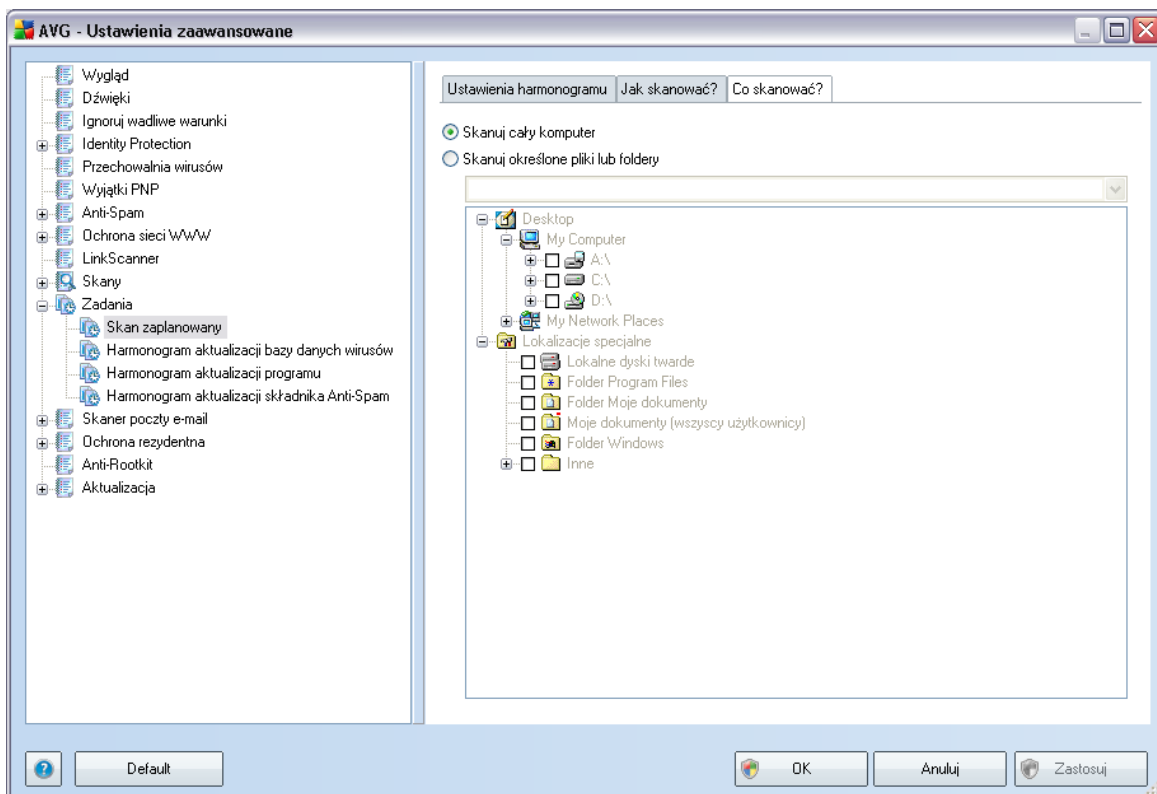
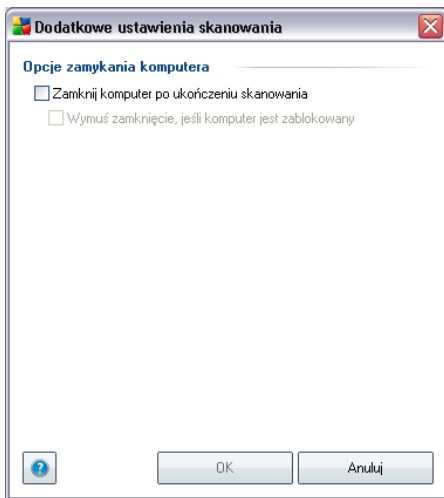
Priorytet procesu skanowania

W sekcji **Priorytet procesu skanowania** mozna szczególowo okreslic zadana predkosc skanowania, w zalezności 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 włączony, 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:



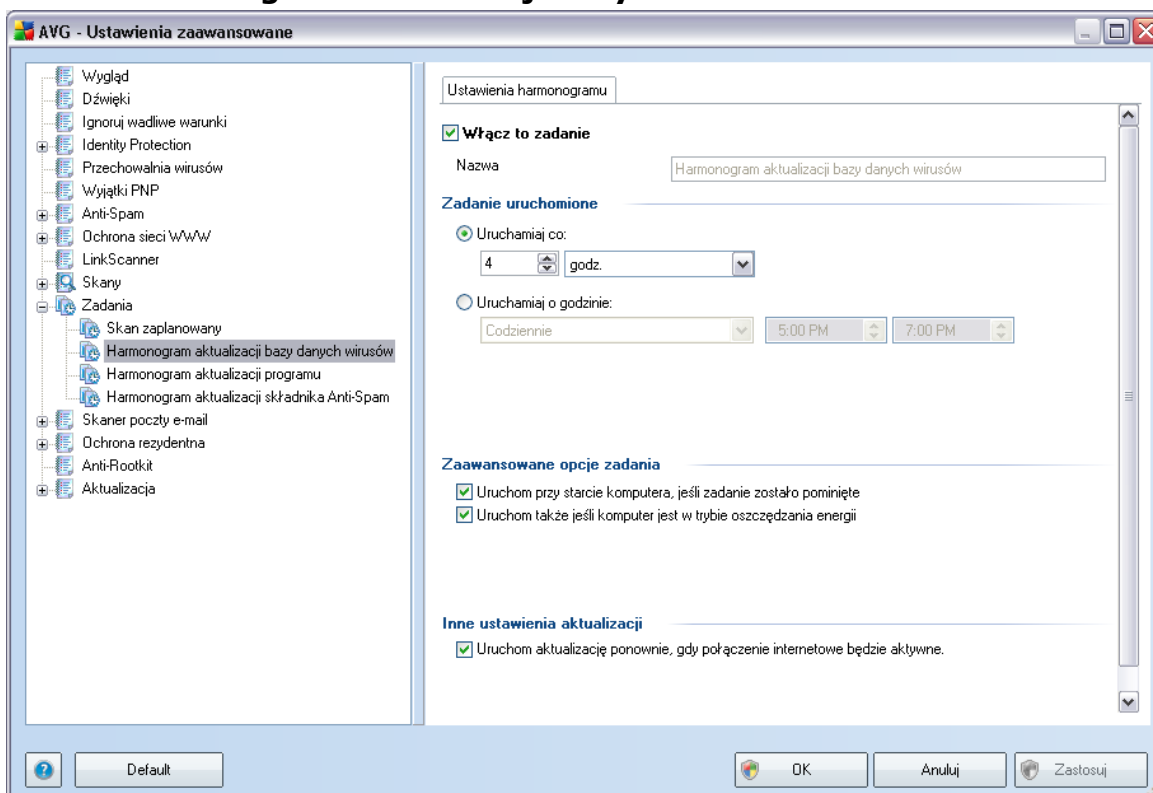
Dodatkowe ustawienia skanowania — link ten pozwala otworzyc nowe okno dialogowe **Opcje zamykania komputera**, w którym mozna okreslic, czy komputer ma byc zamykany automatycznie po zakonczeniu procesu skanowania. Wybranie pierwszej opcji (**Zamknij komputer po ukonczeniu skanowania**) powoduje aktywowanie 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.

9.9.2. 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** (wyłączone dla harmonogramów domyślnych) 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 zidentyfikować.

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 akcje, np. uruchomienie komputera**).

Zaawansowane opcje harmonogramu

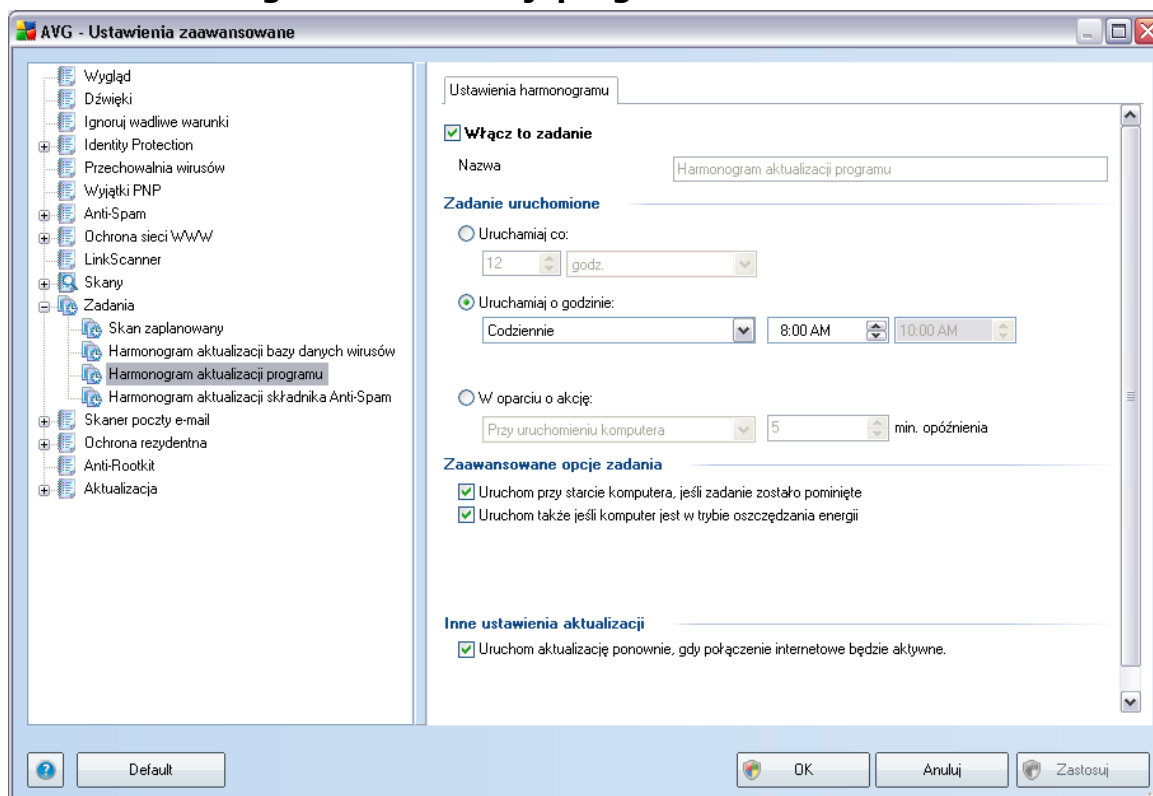
Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji bazy wirusów w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

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](#)*).

9.9.3. 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

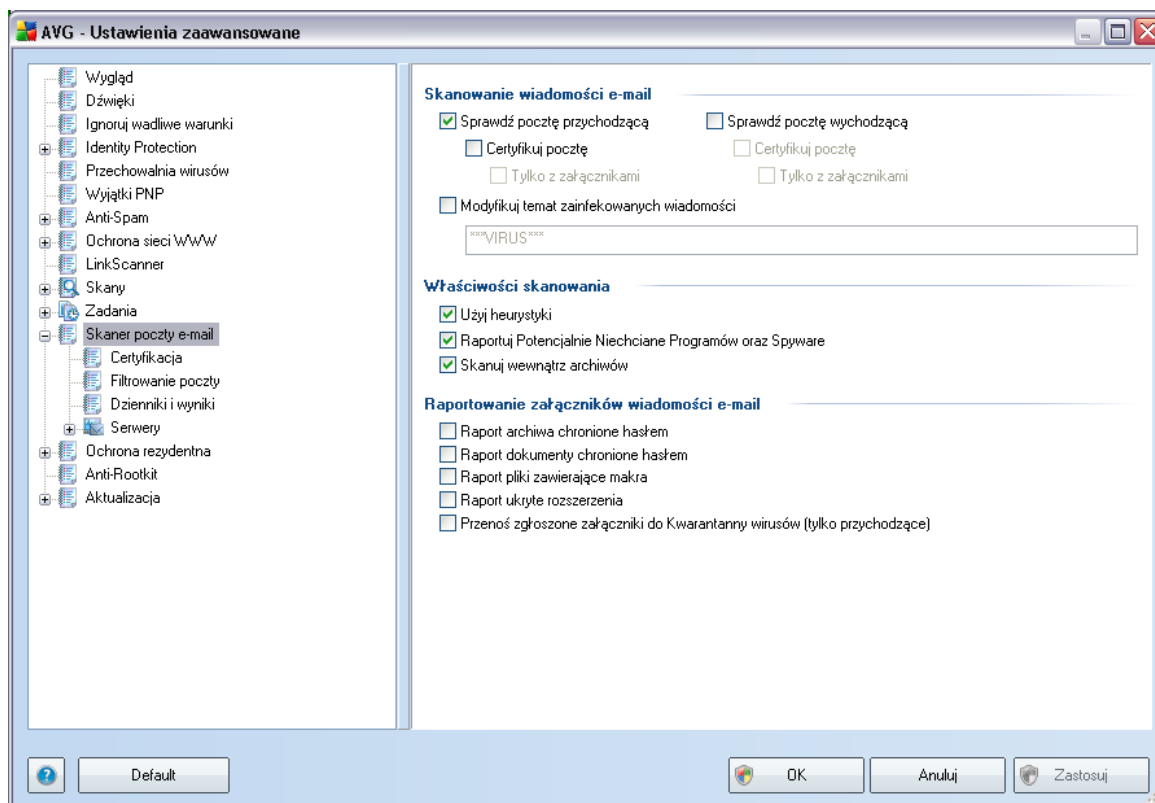
Ta sekcja umożliwi zdefiniowanie warunków uruchamiania aktualizacji programu w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

Inne ustawienia aktualizacji

Na koniec należy zaznaczyć pole wyboru **Uruchom aktualizacje 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](#)).

9.10. Skaner poczty e-mail

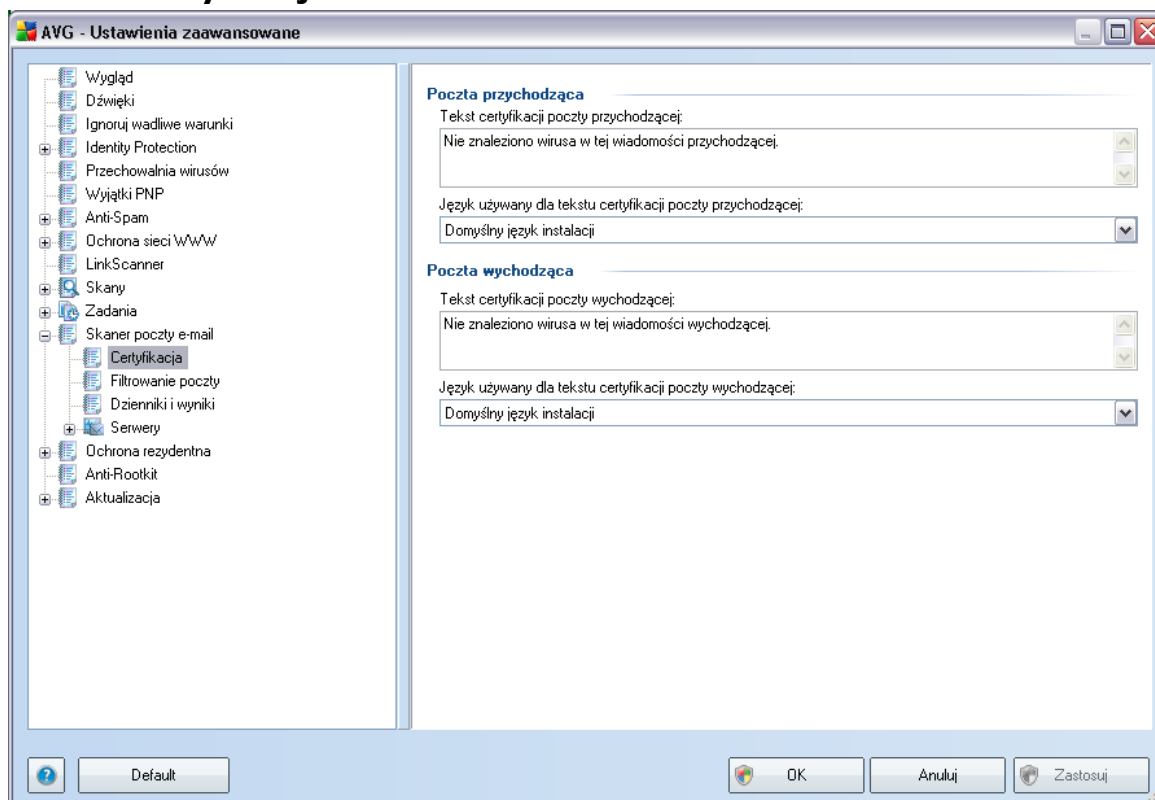


Okno **Skaner poczty e-mail** podzielone jest na trzy sekcje:

- **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 (domyślnie 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**).

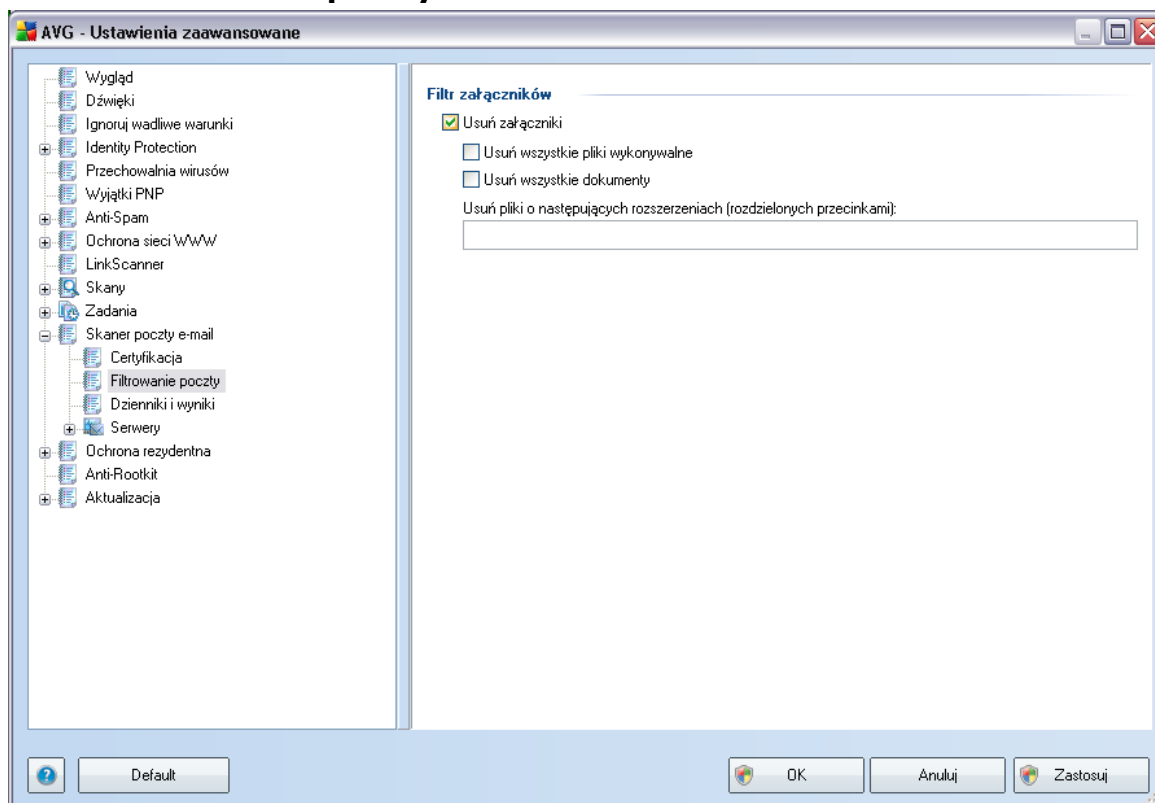
- **Raportowanie załączników e-mail** — należy określić, czy system ma powiadamiać pocztą e-mail o archiwach zabezpieczonych hasłem, dokumentach zabezpieczonych hasłem, plikach zawierających makra i/lub plikach o ukrytych rozszerzeniach, które zostaną wykryte jako załączniki do skanowanych wiadomości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

9.10.1. Certyfikacja



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

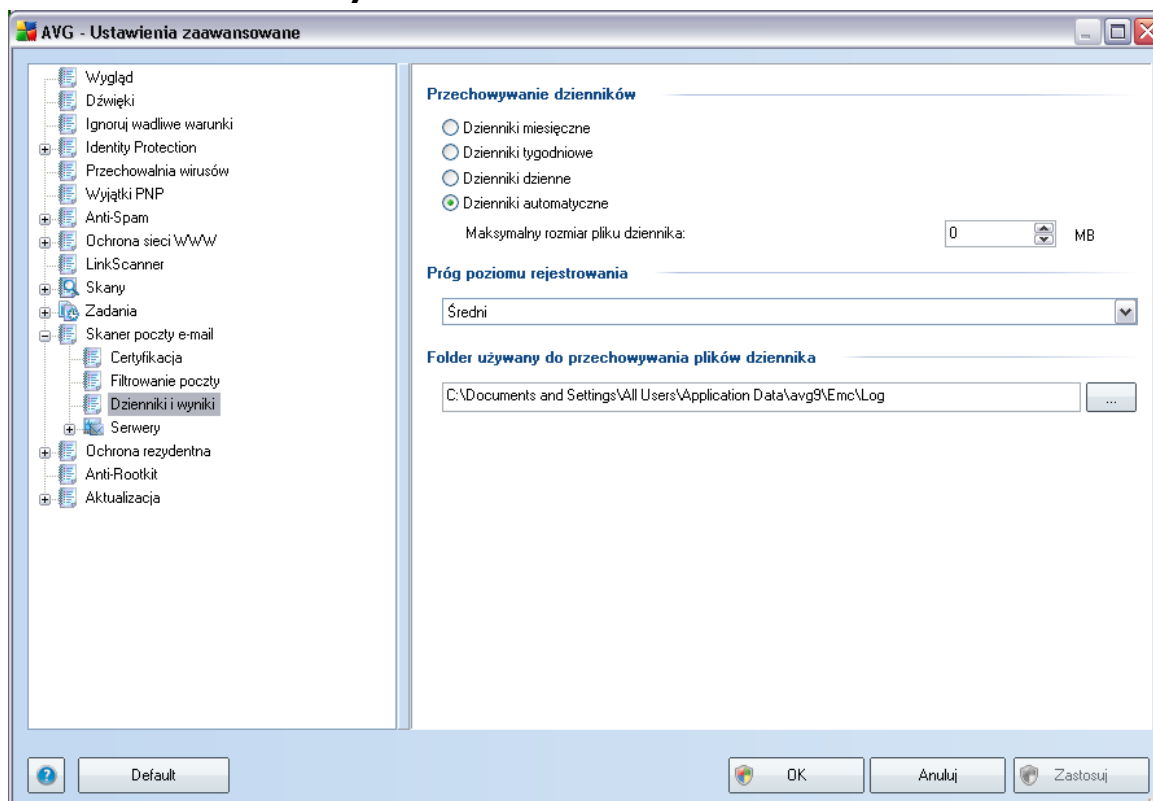
9.10.2. Filtrowanie poczty



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

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

9.10.3. Dzienniki i Wyniki

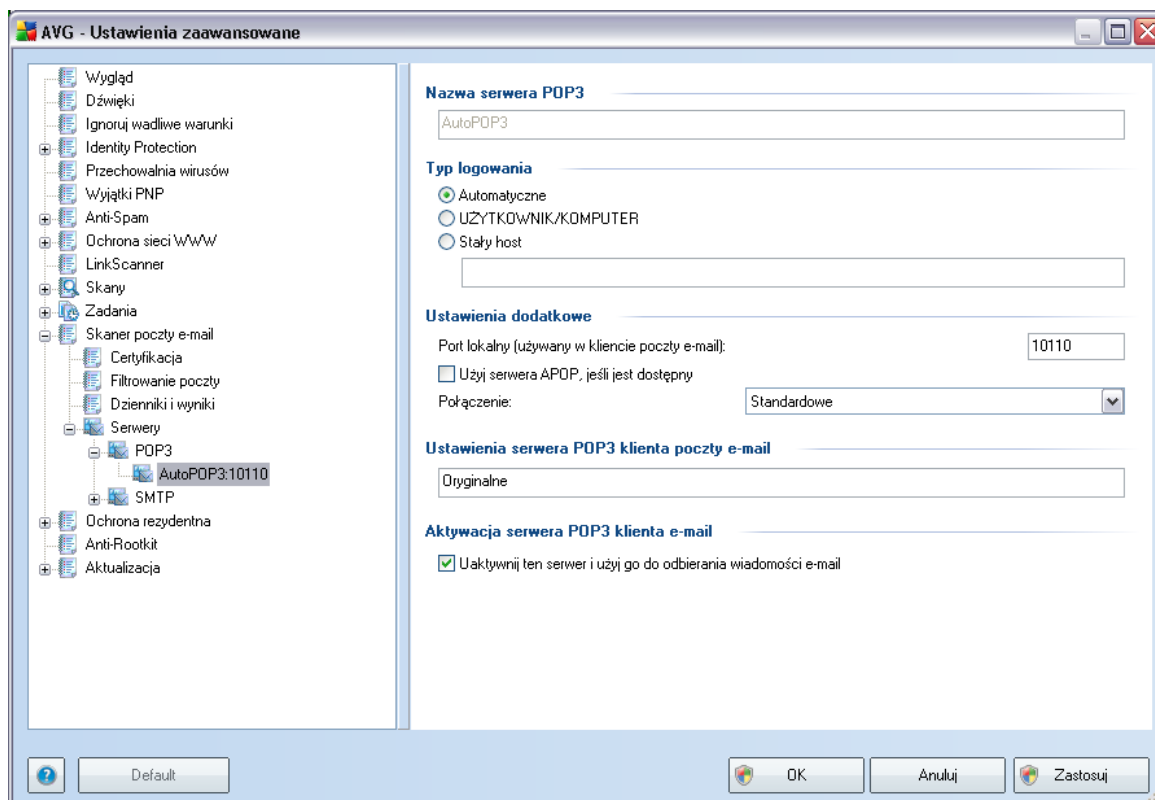


W oknie **Dzienniki i wyniki** można określić parametry przechowywania wyników skanowania poczty e-mail. Okno to podzielone jest na dwa obszary:

- **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.

9.10.4. Serwery

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

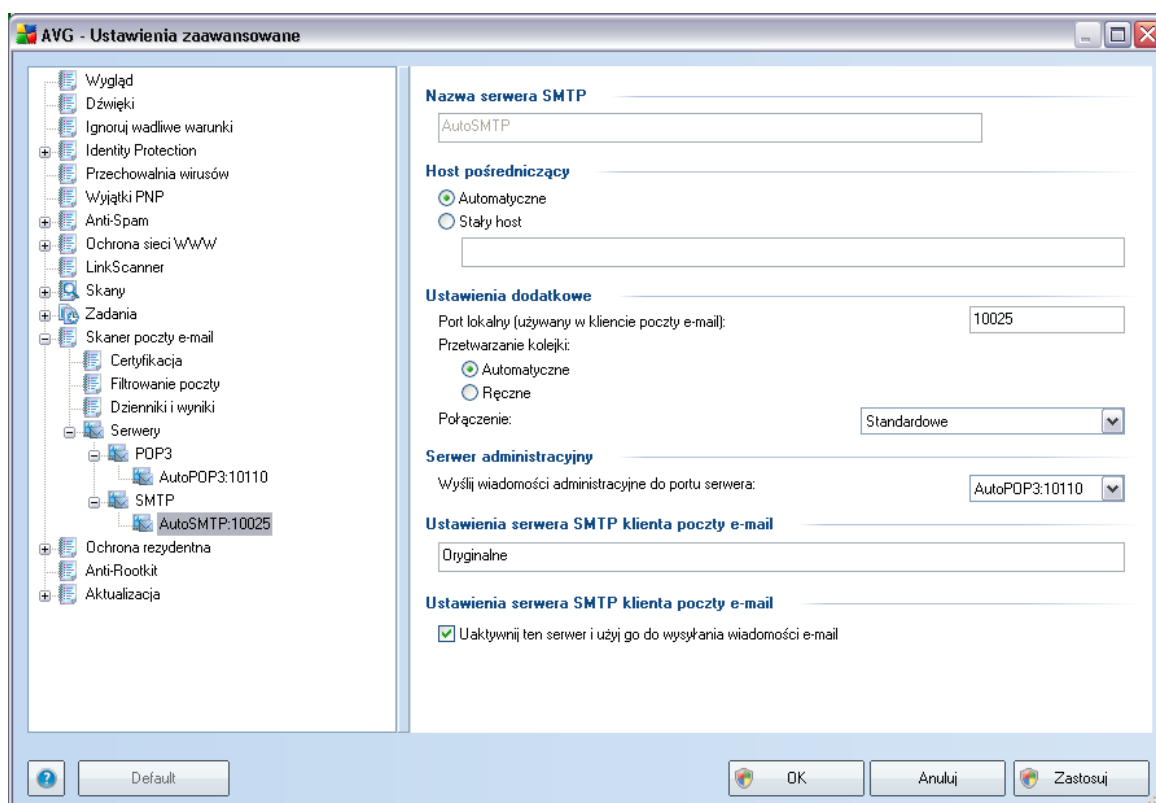


W tym oknie dialogowym (dostępnym z menu **Serwery / POP3**) można zdefiniować (na potrzeby **Skamera poczty e-mail**) nowy serwer poczty przychodzącej, korzystający z protokołu POP3:

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

- **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.
- **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:
 - **Port lokalny** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w kliencie poczty jako port docelowy serwera POP3.
 - **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 wysłaniu go w formie zaszyfrowanej, która korzysta ze zmiennego klucza nadesłanego przez serwer. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
 - **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:

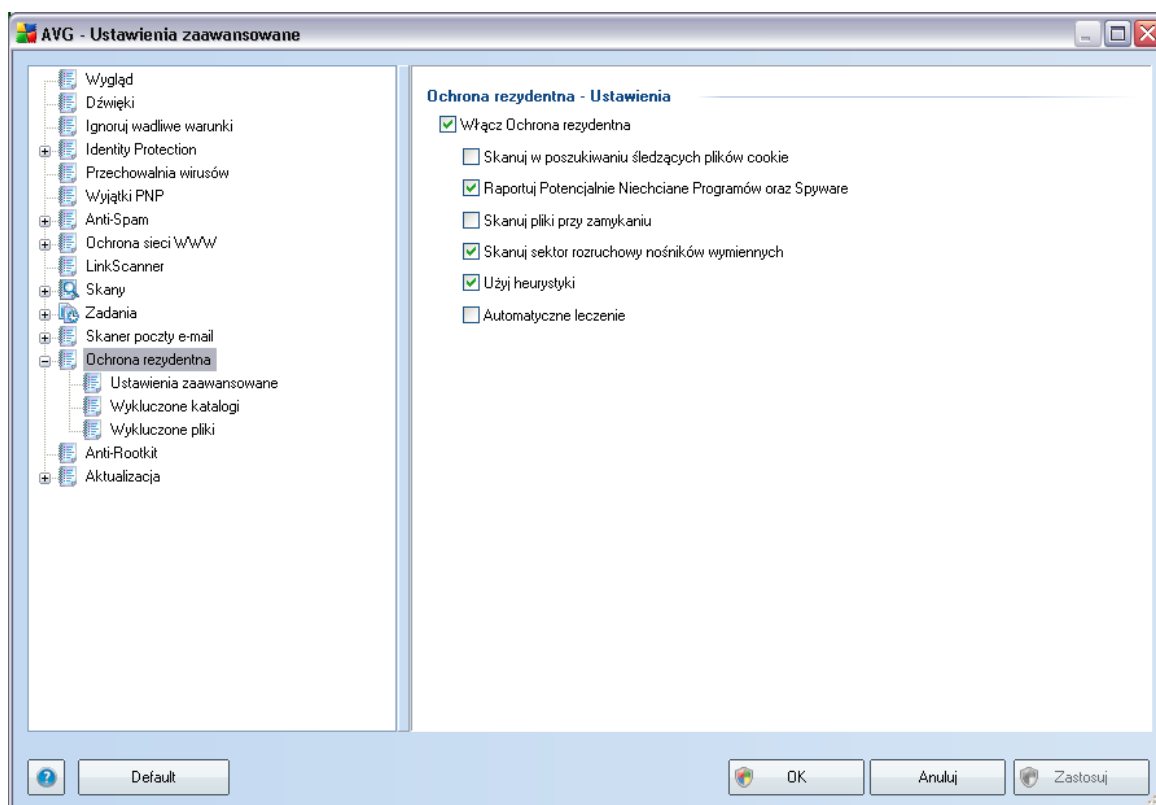
- **Nazwa serwera SMTP** — należy podać nazwę serwera lub zachować domyślną (AutoSMTP).
- **Host pośredniczący** — definiuje metodę określania serwera pocztowego dla wiadomości wychodzących:
 - **Automatyczne** — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail
 - **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:
 - **Port lokalny** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port komunikacji SMTP.
 - **Przetwarzanie kolejki** — określa zachowanie **skanera poczty e-mail** podczas przetwarzania wymagań dotyczących wysyłania wiadomości e-mail:
 - Automatycznie — poczta wychodząca jest natychmiast dostarczana (wysyłana) do docelowego serwera pocztowego.
 - Reczne — wiadomości są umieszczane w kolejce wiadomości wychodzących i wysyłane w późniejszym terminie.
 - **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.

9.11. Ochrona rezydentna

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



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

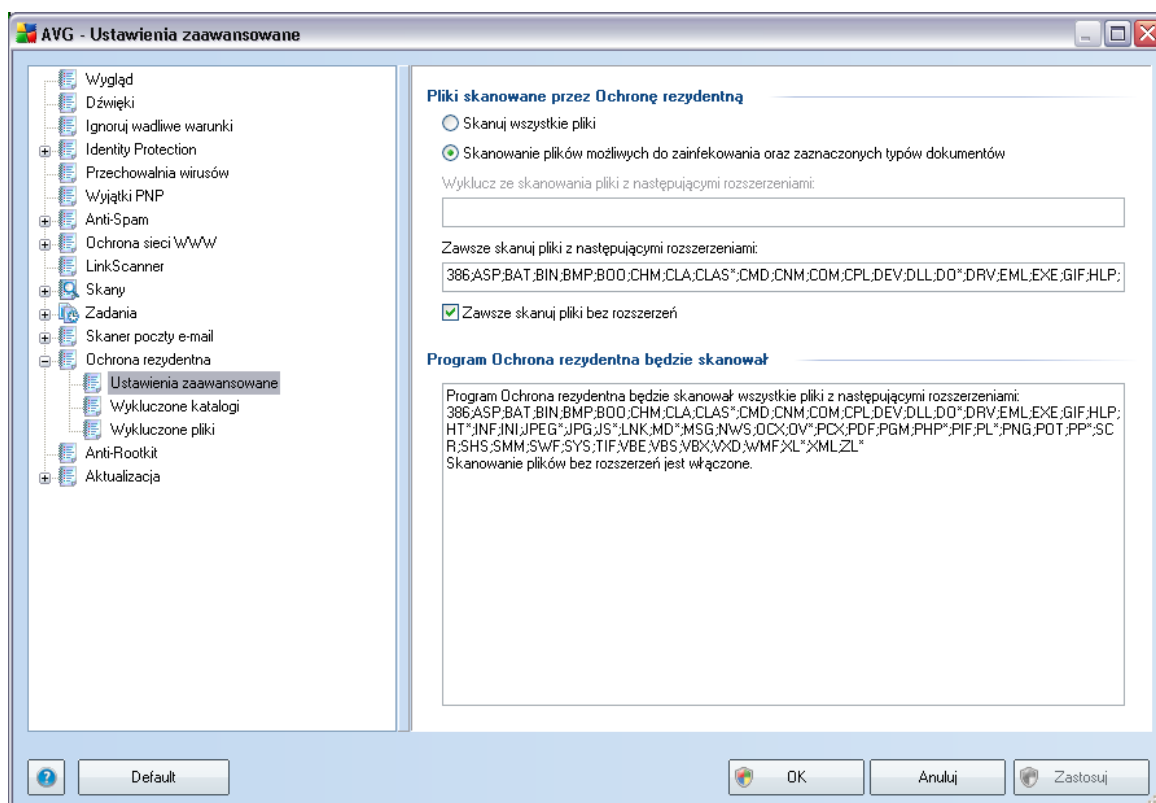
- ***Skanuj w poszukiwaniu śledzących plików cookie*** — parametr ten określa, czy w czasie skanowania mają być wykrywane pliki cookie. (*Pliki cookie w protokole HTTP są używane do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencje dotyczące wyglądu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

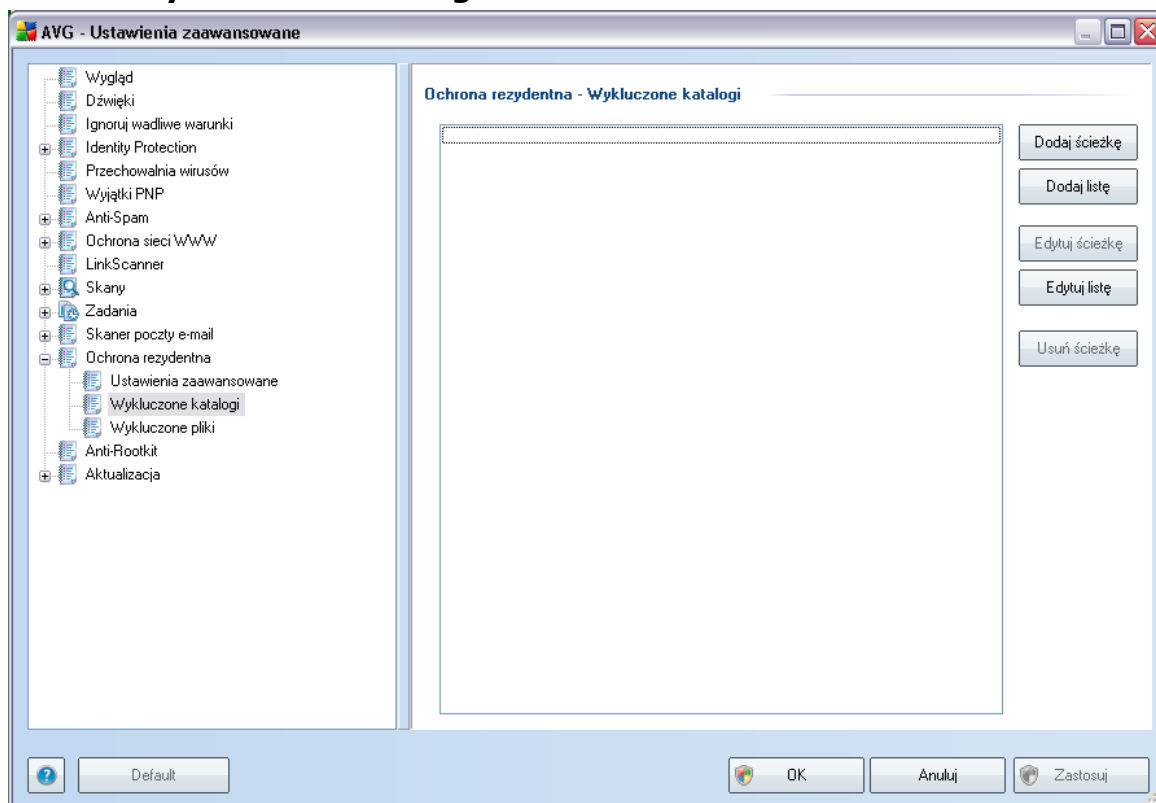
9.11.1. Ustawienia zaawansowane

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



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

9.11.2. Wykluczenia katalogów



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

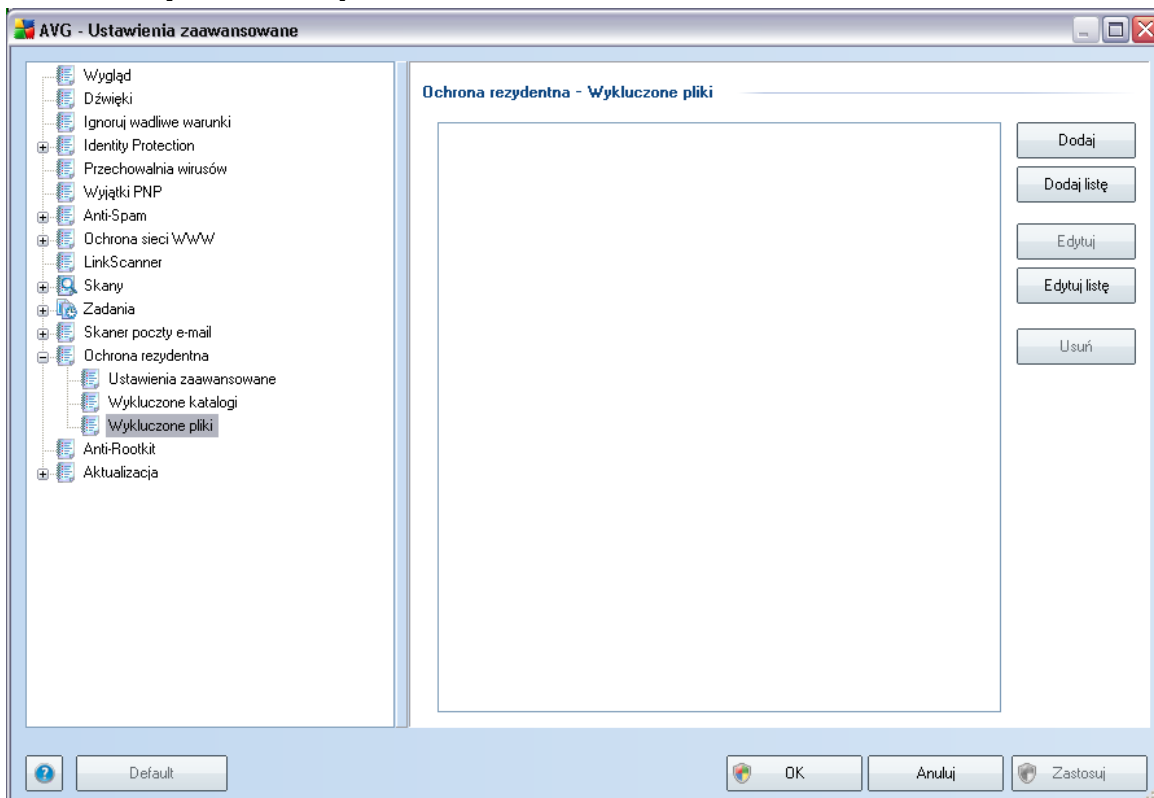
Jesli nie jest to konieczne, zdecydowanie zalecamy nie wykluczać żadnych katalogów ze skanowania!

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 sciezke** — umożliwia usuniecie z listy wybranego folderu.

9.11.3. 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**.

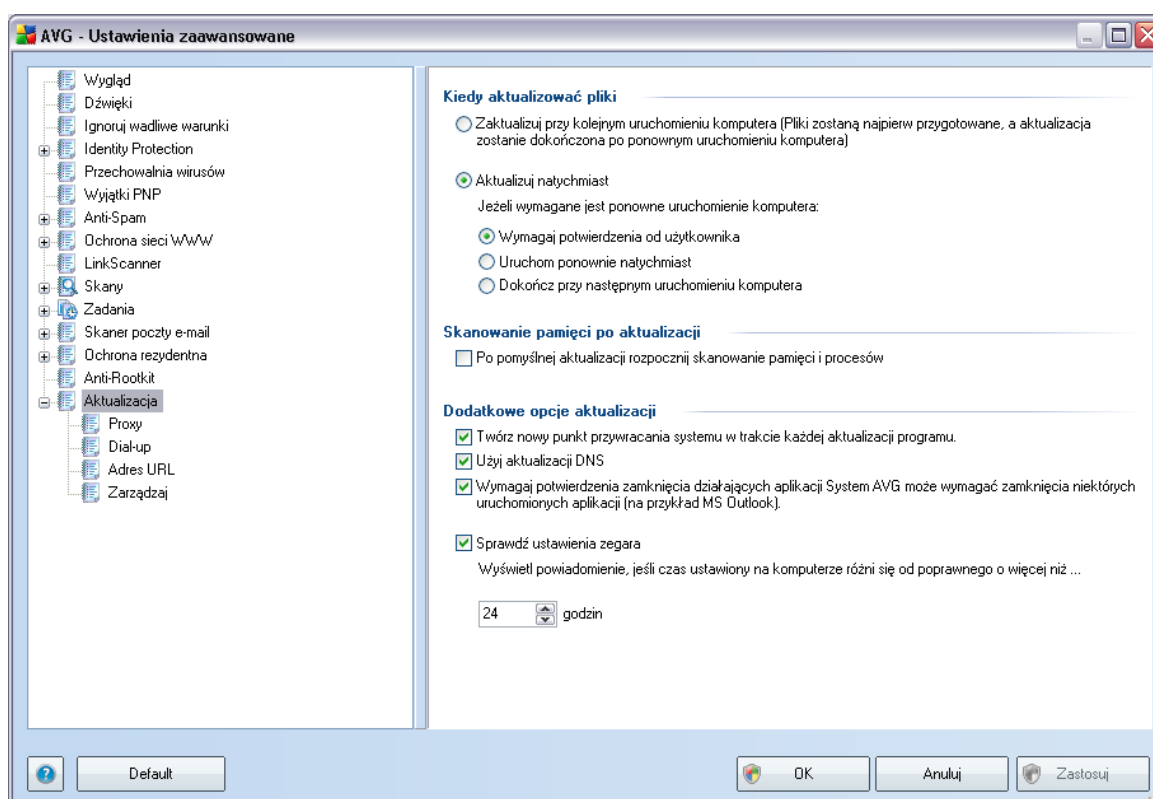
Jesli nie jest to konieczne, zdecydowanie zalecamy nie wylaczac zadnych katalogow ze skanowania!

W bieżącym oknie dostępne są następujące przyciski kontrolne:

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

- **Dodaj listę** — umożliwia podanie listy katalogów, które zostaną wykluczone ze skanowania przez **Ochronę Rezydentną**.
- **Edytuj** — umożliwia edycję określonej ścieżki dostępu do wybranego folderu.
- **Edytuj listę** — umożliwia edycję listy folderów.
- **Usuń** — umożliwia usunięcie z listy ścieżki dostępu do wybranego folderu.

9.12. Aktualizacja



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

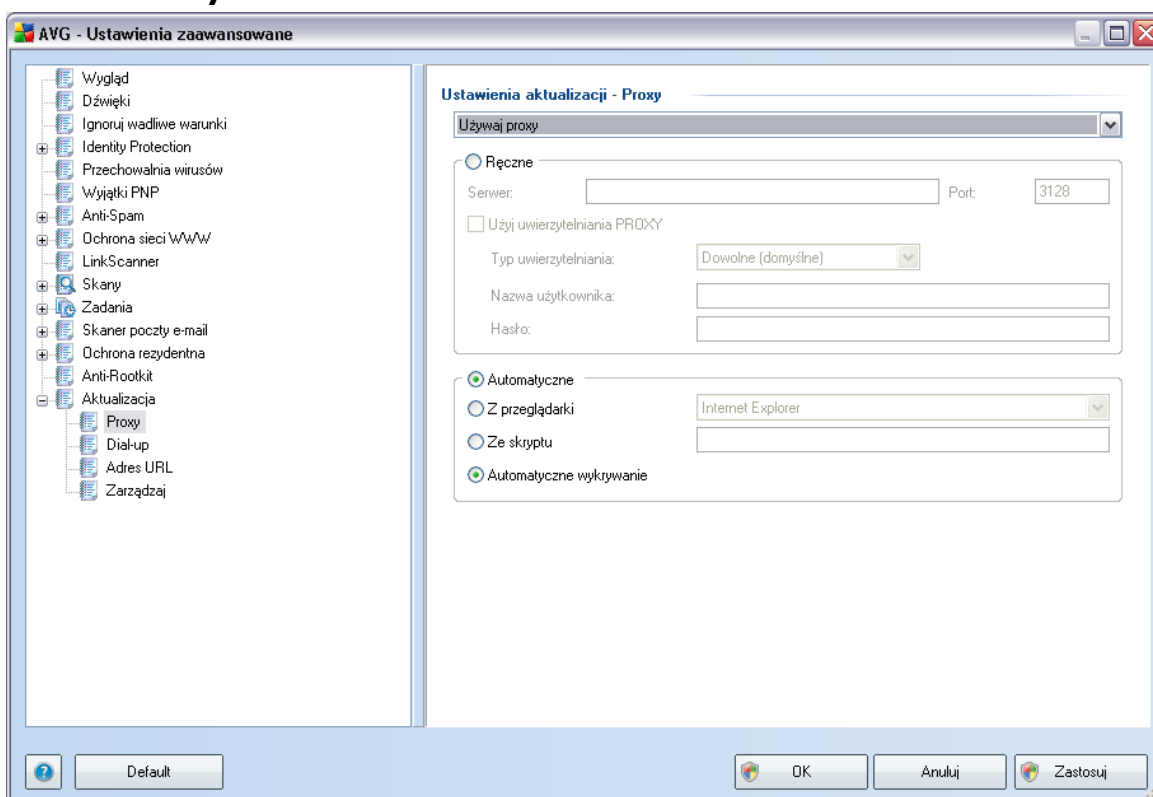
Pole to należy zaznaczyć, jeśli po każdej pomyslniej aktualizacji system ma uruchamiać skanowanie pamięci. Pobrana aktualizacja mogła zawierać nowe definicje wirusów, które mogą zostać zastosowane podczas takiego skanowania.

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 niedoswiadczonym użytkownikom! 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.

9.12.1. 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 zezwolić na korzystanie z obu opcji jednocześnie. Dlatego też w oknie **Ustawienia aktualizacji – Proxy** należy najpierw wybrać jedną z dostępnych opcji:

- **Używaj proxy**

- **Nie używaj proxy**
- **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 Ręcznie aktywuje odpowiednią sekcję**) należy podać następujące informacje:

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

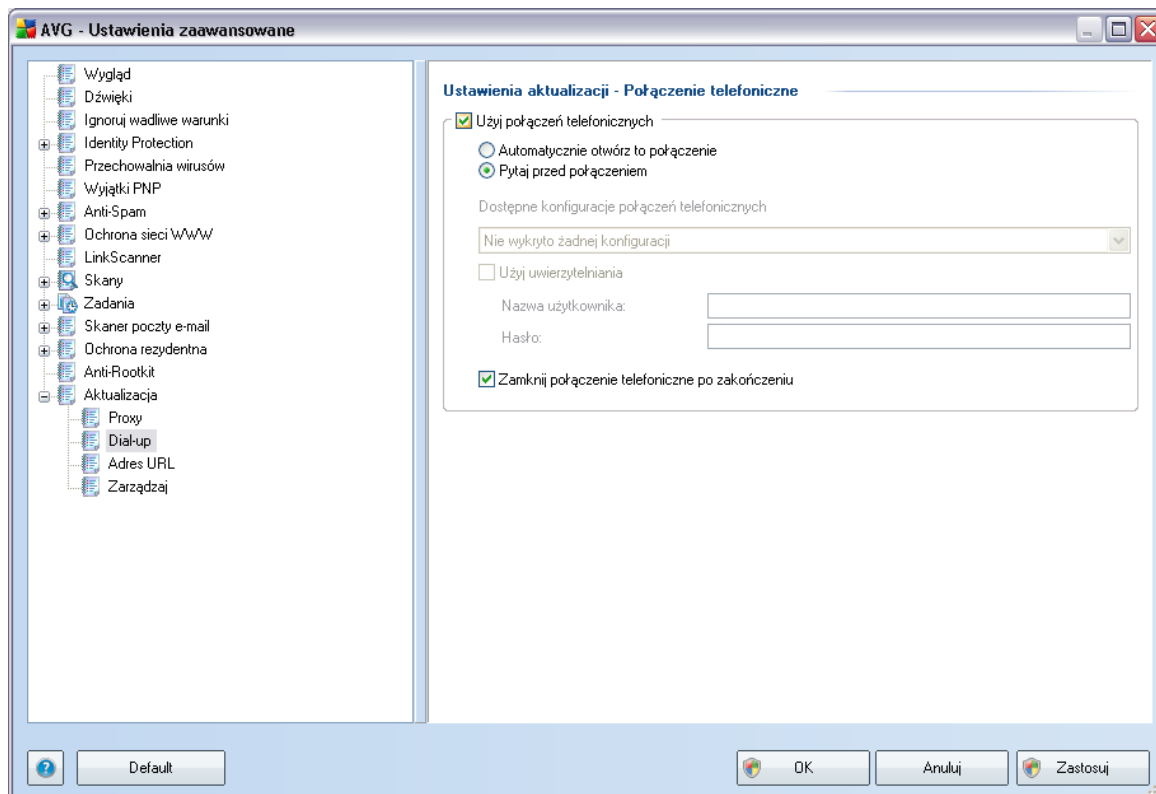
Zdarza się, że na serwerze proxy dla każdego użytkownika skonfigurowane są odrębne reguły. Jeśli serwer proxy jest skonfigurowany w ten sposób, należy zaznaczyć opcję **Użyj uwierzytelniania PROXY**, aby serwer weryfikował nazwę użytkownika i hasło przed nawiązaniem połączenia.

Konfiguracja automatyczna

W przypadku wybrania konfiguracji automatycznej (zaznaczenie **opcji Automatycznie aktywuje 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.

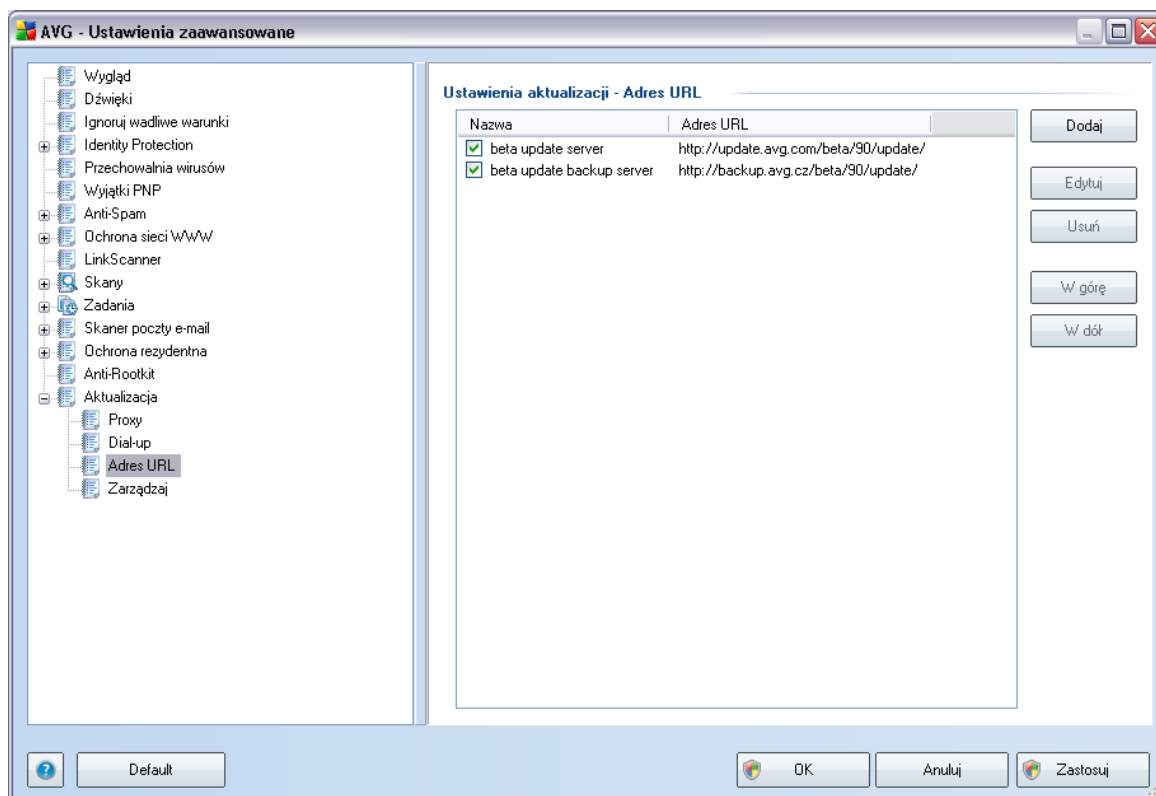
9.12.2. Połączenie telefoniczne



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**).

9.12.3. URL

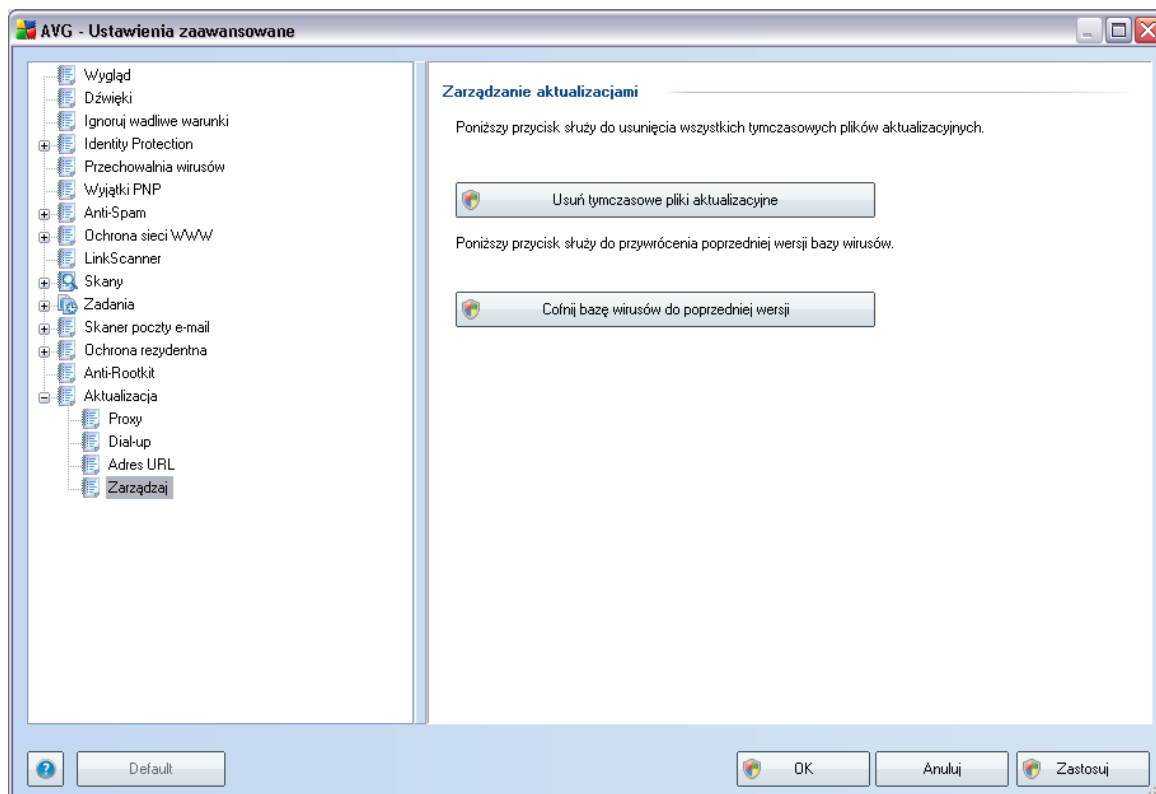


W oknie **URL** znajduje się lista adresów internetowych, z których można pobierać pliki aktualizacyjne. Listę i jej elementy można modyfikować za pomocą następujących przycisków kontrolnych:

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

9.12.4. Zarządzaj

Okno dialogowe **Zarządzaj** zawiera dwa przyciski:

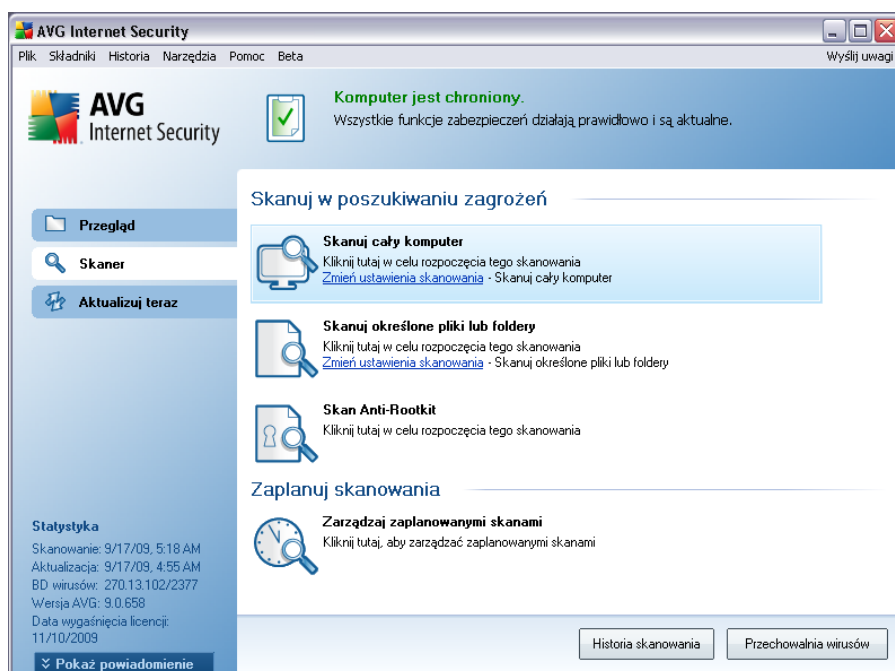


- **Usun tymczasowe pliki aktualizacyjne** — pozwala usunąć z dysku twardego wszystkie zbędne pliki aktualizacyjne (sa one domyślnie przechowywane przez 30 dni)
- **Cofnij bazę wirusów do poprzedniej wersji** — pozwala usunąć z dysku twardego ostatnią wersję bazy wirusów i przywrócić ją do poprzedniego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

10. Skanowanie AVG

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

10.1. 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:
 - [Skan całego komputera](#)
 - [Skan określonych plików lub folderów](#)
- [Planowanie testów](#) — w tym obszarze można definiować nowe testy i tworzyć nowe harmonogramy w zależności od potrzeb.

Przyciski kontrolne

Interfejs skanera zawiera następujące przyciski kontrolne:

- **Historia skanowania** — wyświetla okno dialogowe [Przegląd wyników skanowania](#), które zawiera pełną historię testów.
- **Przechowalnia wirusów** — otwiera nowe okno z zawartością [Przechowalni wirusów](#), w której izolowane są wykryte infekcje.

10.2. Wstępnie zdefiniowane testy

Jedną z głównych funkcji aplikacji **AVG 9 Anti-Virus** 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.

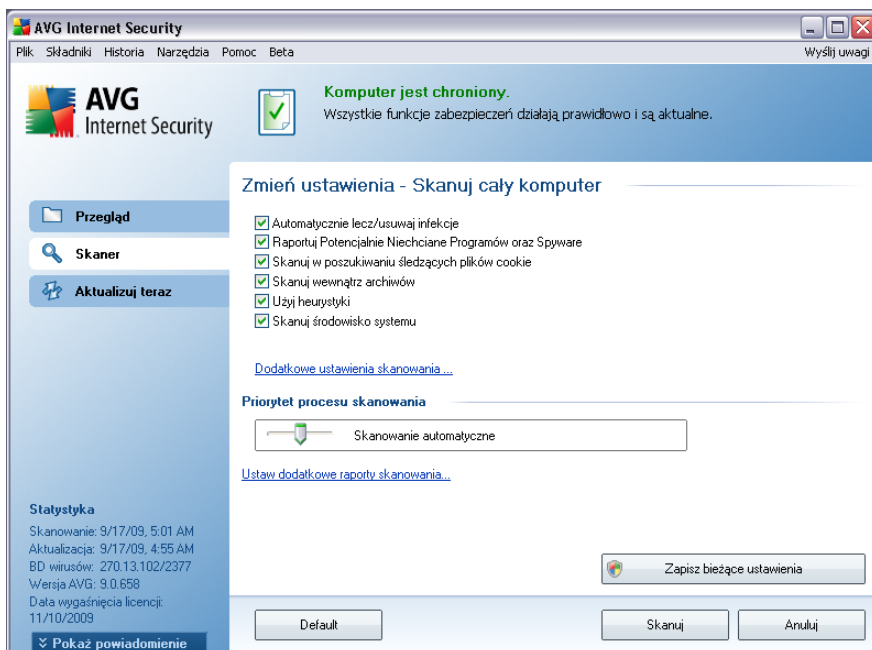
System **AVG 9 Anti-Virus** oferuje dwa typy skanowania zdefiniowane wstępnie przez AVG:

10.2.1. Skan całego komputera

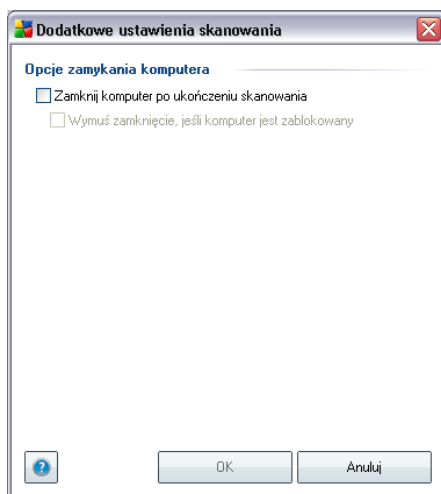
Skanuj cały komputer — skanuje cały komputer w poszukiwaniu możliwych infekcji i/lub potencjalnie niechcianych programów. Test ten obejmuje wszystkie dyski twarde komputera. Wykryte infekcje są leczone lub przenoszone do [Przechowalni wirusów](#). Skanowanie całego komputera powinno być regularnie przeprowadzane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

Uruchamianie skanowania

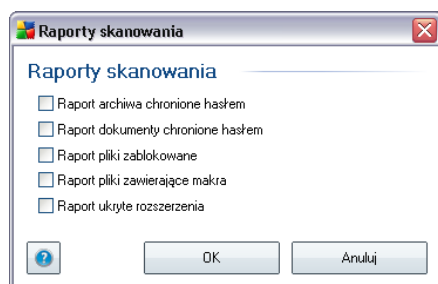
Skanowanie całego komputera można uruchomić bezpośrednio z poziomu [interfejsu skanera](#), klikając ikonę odpowiedniego testu. Dla tego skanowania nie można określać dalszych ustawień; jest ono uruchamiane natychmiast w oknie dialogowym **Skanowanie w toku** (patrz ilustracja). W razie potrzeby skanowanie można tymczasowo przerwać (**Wstrzymaj**) lub anulować (**Zatrzymaj**).



- **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:



- **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 wtedy, gdy jest zablokowany (**Wymus zamknięcie, jeśli komputer jest zablokowany**).
- **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, którymi 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 multimedialnych (*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.

10.2.2. Skan określonych plików lub folderów

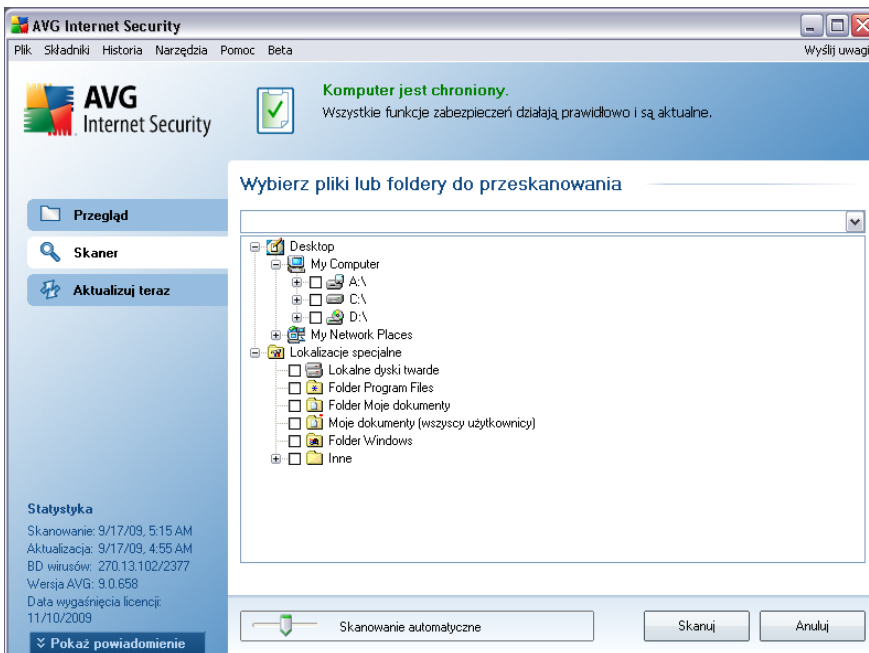
Skan określonych plików lub folderów – skanowane są tylko wskazane obszary komputera (wybrane foldery, a także dyski twarde, pamięci flash, CD itd.). Postępowanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu całego komputera: każdy znaleziony wirus jest leczony lub przenoszony do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

Uruchamianie skanowania

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

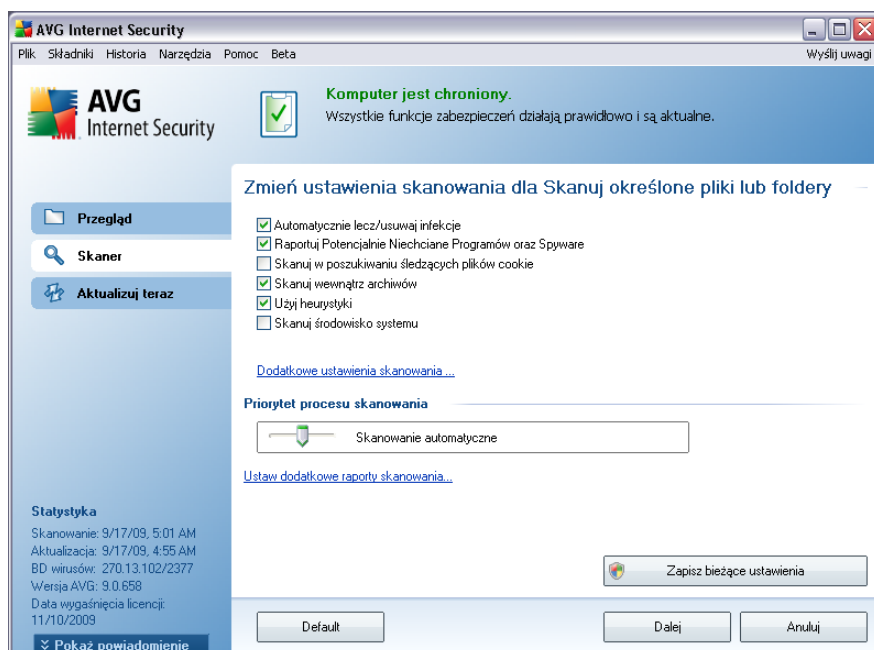
Można także przeskanować wybrany folder, wykluczając jednocześnie ze skanowania wszystkie jego podfoldery: należy wprowadzić znak minus „-” przed jego nazwą w wygenerowanej ścieżce (*patrz ilustracja*). Aby wykluczyć cały folder ze skanowania, należy użyć parametru „!”.

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

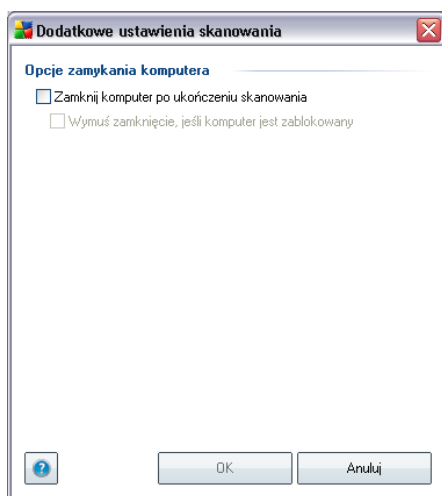


Edycja konfiguracji skanowania

Zdefiniowane wstępne ustawienia domyślne testu **Skan określonych plików lub folderów** można edytować. Kliknięcie linku **Zmien ustawienia skanowania określonych plików lub folderów** powoduje otwarcie okna dialogowego **zmiany ustawień dla skanowania określonych plików lub folderów**. **Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!**



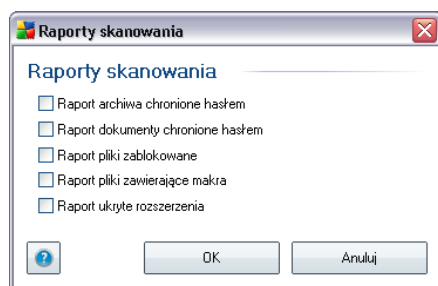
- **Parametry skanowania** — na liście parametrów skanowania można włączać/wyłączać określone parametry w zależności od potrzeb (*szczegółowy opis tych ustawień zawiera rozdział [Zaawansowane ustawienia AVG / Skany / Skanowanie określonych plików lub folderów](#)*).
- **Dodatkowe ustawienia skanowania** — link do okna dialogowego "Dodatkowe ustawienia skanowania", w którym można określić następujące parametry:



- **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 (**Wymuś zamknięcie, jeśli komputer jest zablokowany**).
- **Zdefiniuj typy plików do skanowania** — następnie należy zdecydować, czy skanowane mają być:
 - **Wszystkie typy plików** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń 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 multimediiów (*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 niezmięnianie 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 (*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*).

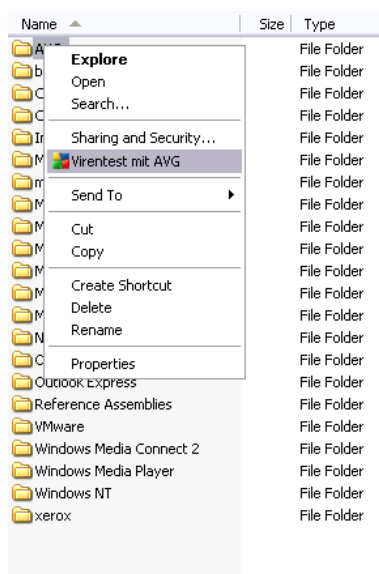
- Ustaw dodatkowe raporty skanowania** — łącze pozwala otworzyć nowe okno dialogowe **Raporty skanowania**, w którym można określić, co ma być zgłaszane:



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](#)).

10.3. Skan z poziomu eksploratora systemu Windows

Oprócz wstępnie zdefiniowanych testów obejmujących cały komputer lub wybrane obszary, system **AVG 9 Anti-Virus** 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.

10.4. Skan z poziomu wiersza poleceń

AVG 9 Anti-Virus 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 wymaganym parametrem jest **/SCAN**, który pozwala określić, jakie obszary komputera mają być skanowane. Bardziej szczegółowe informacje na temat opcji zawiera [przeгляд parametrów wiersza polecen](#).

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.

10.4.1. Parametry skanowania z wiersza poleceń

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 plików
- **/@** 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** Usuwanie automatycznie
- **/TRASH** [Przenies zainfekowane pliki do Przechowalni wirusów](#)
- **/QT** Szybki test
- **/MACROW** Raportuj pliki zawierajace makra
- **/PWDW** Raportuj pliki chronione haslem
- **/IGNLOCKED** Ignoruj pliki zablokowane
- **/REPORT** Raportuj do pliku /nazwa pliku/
- **/REPAPPEND** Dopisz do pliku raportu
- **/REPOK** Raportuj niezainfekowane pliki jako OK
- **/NOBREAK** Nie zezwalaj na przerwanie klawiszami CTRL-BREAK
- **/BOOT** Wlacz sprawdzanie MBR/sektora rozruchowego
- **/PROC** Skanuj aktywne procesy

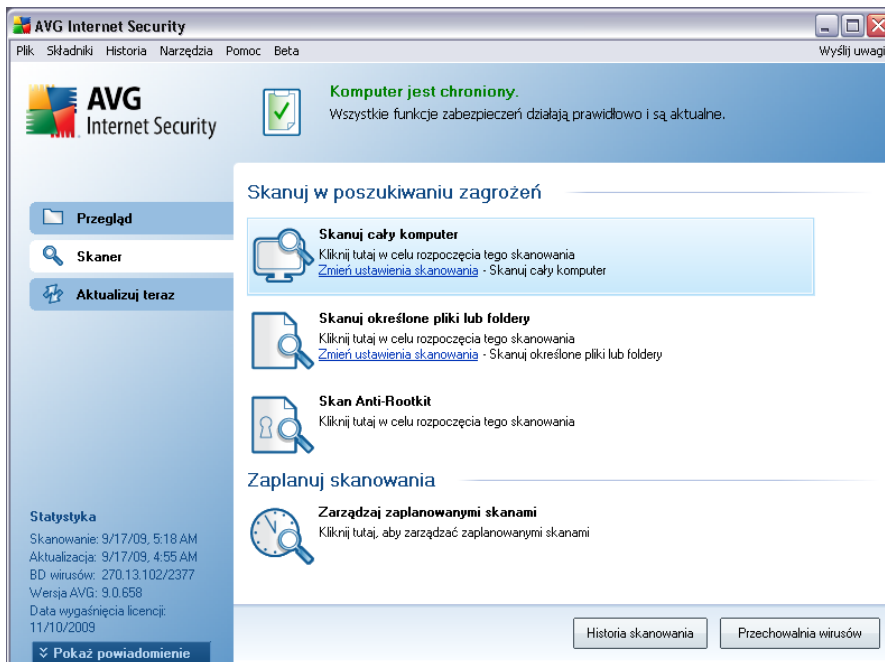
- **/PUP** Raportuj [potencjalnie niechciane programy](#)
- **/REG** Skanuj Rejestr
- **/COO** Skanuj pliki cookie
- **/?** Wyświetl pomoc na ten temat
- **/HELP** Wyświetl pomoc na ten temat
- **/PRIORITY** Ustaw priorytet skanowania /Niski, Auto, Wysoki/
(zobacz [Ustawienia zaawansowane / Skany](#))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

10.5. Planowanie skanowania

System **AVG 9 Anti-Virus** 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.

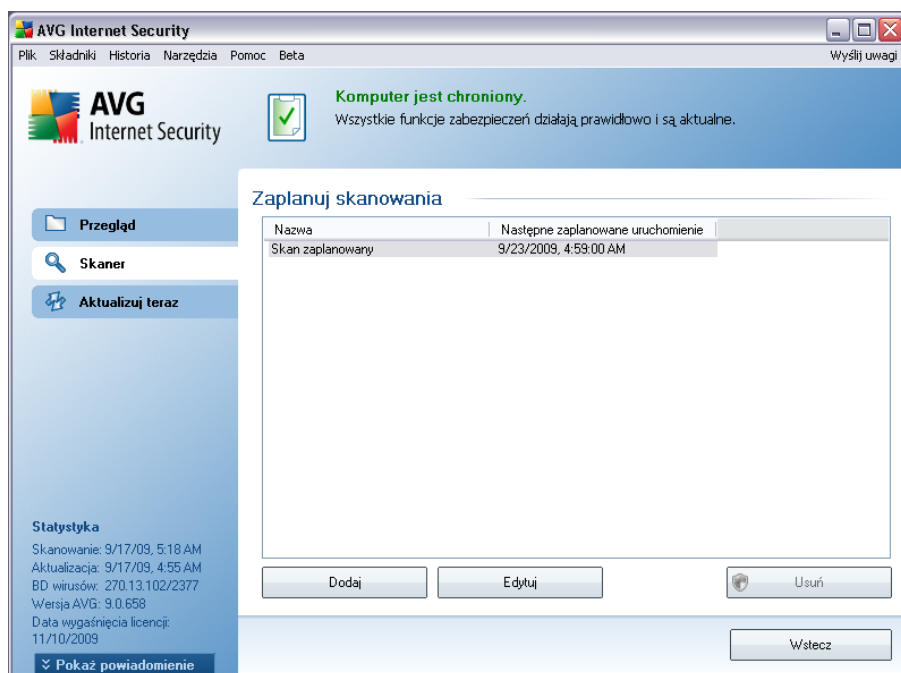
Skan całego komputera należy uruchamiać regularnie co najmniej raz na tydzień. Jeśli jest to możliwe, należy skanować komputer codziennie — zgodnie z domyślną konfiguracją harmonogramu skanowania. Jeśli komputer działa 24 godziny na dobę, można zaplanować skanowanie poza czasem pracy. Jeśli komputer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

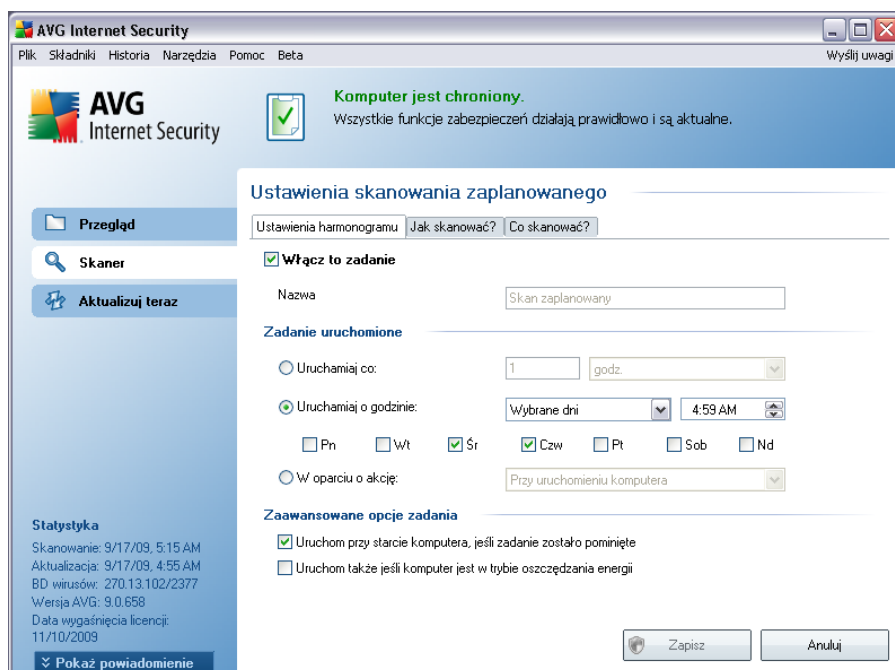


Zawartość okna można edytować, używając następujących przycisków:

- **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 skanowań. 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](#)

10.5.1. Ustawienia harmonogramu

Aby zaplanować nowy test i uruchamiać go regularnie, należy przejść do okna dialogowego **Ustawienia zaplanowanego testu** (klikając przycisk **Dodaj harmonogram skanowania** w oknie dialogowym **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 określać w nazwie skanowania, czy skanowany jest cały komputer, czy tylko jego wybrane obszary — własne testy użytkownika są zawsze specyficznym [skanowaniem określonych plików lub folderów](#).

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

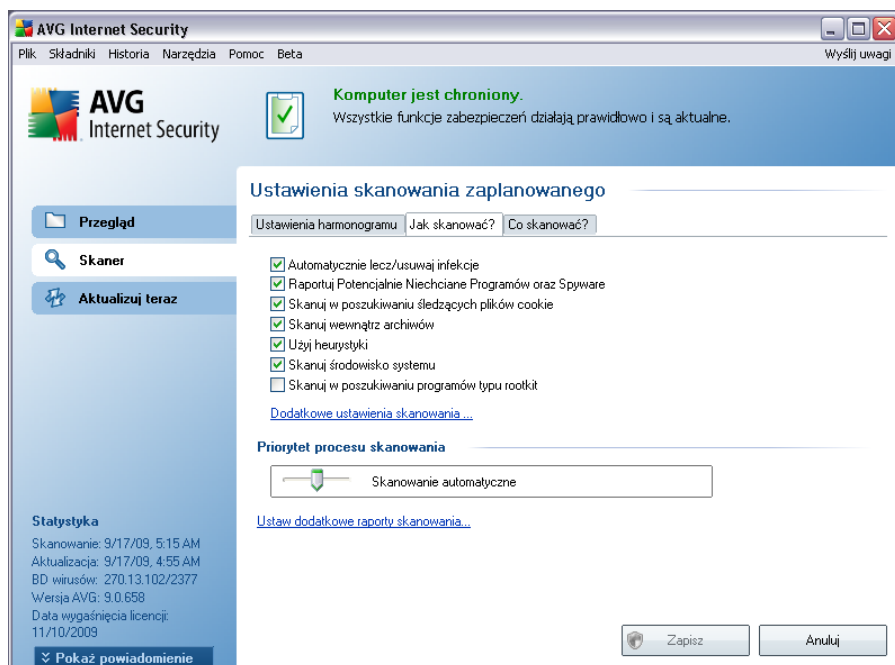
- **Zadanie uruchomione** — należy określić interwał przeprowadzanych testów. Skanowanie może być powtarzane w określonych odstępach czasu (**Uruchamiaj co**) lub o zadanej godzinie (**Uruchamiaj o określonej godzinie**), a także na skutek wystąpienia zdefiniowanego zdarzenia (**W oparciu o akcje, np.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

10.5.2. Jak skanować?



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

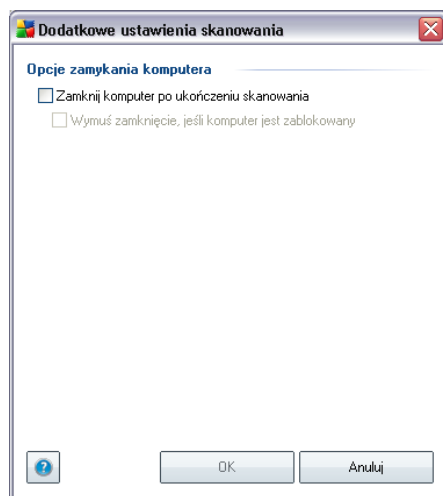
- **Automatycznie lecz/usuwać infekcje** — (domyślnie włączona) jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowanego pliku nie można wyleczyć, lub jeśli opcja ta zostanie wyłączona, system powiadomi o wykryciu wirusa i zapyta o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

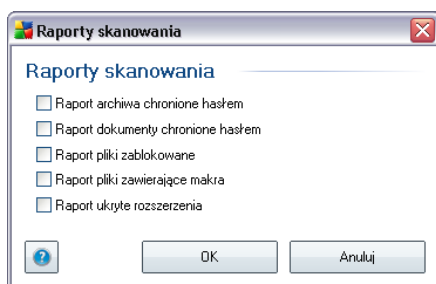
Następnie można zmienić konfigurację skanowania zgodnie z poniższym opisem:

- **Dodatkowe ustawienia skanowania** — link ten otwiera nowe okno dialogowe **Dodatkowe ustawienia skanowania**, w którym można określić następujące parametry:



- **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, jeśli jest zablokowany (**Wymuś zamknięcie, jeśli komputer jest zablokowany**).

- **Zdefiniuj typy plików do skanowania** — należy zdecydować, które z poniższych elementów mają być skanowane:
 - **Wszystkie typy plików** z opcja zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, które 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 skanowanie 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 niezmięnie 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: Domyślnie konfiguracja jest ustawiona pod kątem optymalnej wydajności.

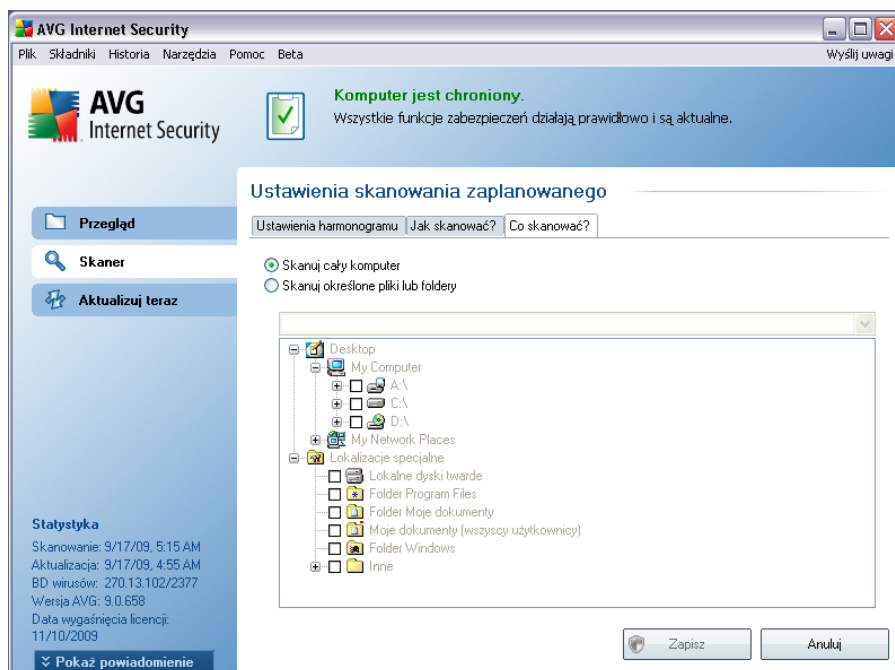
Konfiguracje skanowania należy zmieniać tylko w uzasadnionych sytuacjach. Stanowczo zaleca się stosowanie wstępnie zdefiniowanych ustawień. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Więcej opcji dostępne jest w oknie **Ustawienia zaawansowane**, (**Menu główne/Plik/Ustawienia 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 **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**.

10.5.3. Co skanować?



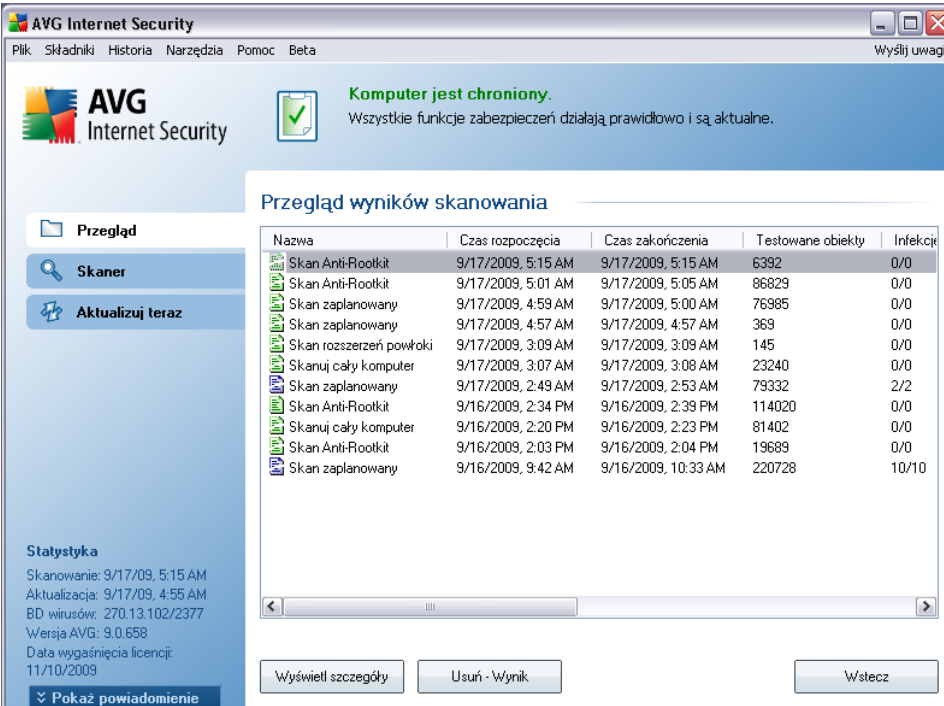
Na karcie **Co skanowac?** można określić, czy planowane jest [skanowanie całego komputera](#), czy [skanowanie określonych plików lub folderów](#). W przypadku skanowania określonych plików lub folderów, w dolnej części okna dialogowego aktywowane jest drzewo katalogów, w którym można wybrać obszar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

10.6. Przegląd wyników skanowania



The screenshot shows the AVG Internet Security interface. At the top, it says "Komputer jest chroniony." (Computer is protected). Below this, there is a section titled "Przegląd wyników skanowania" (Scan results overview) containing a table with the following data:


Nazwa	Czas rozpoczęcia	Czas zakończenia	Testowane obiekty	Infekcji
Skan Anti-Rootkit	9/17/2009, 5:15 AM	9/17/2009, 5:15 AM	6392	0/0
Skan Anti-Rootkit	9/17/2009, 5:01 AM	9/17/2009, 5:05 AM	86829	0/0
Skan zaplanowany	9/17/2009, 4:59 AM	9/17/2009, 5:00 AM	76985	0/0
Skan zaplanowany	9/17/2009, 4:57 AM	9/17/2009, 4:57 AM	369	0/0
Skan rozszerzeń powłoki	9/17/2009, 3:09 AM	9/17/2009, 3:09 AM	145	0/0
Skanuj cały komputer	9/17/2009, 3:07 AM	9/17/2009, 3:08 AM	23240	0/0
Skan zaplanowany	9/17/2009, 2:49 AM	9/17/2009, 2:53 AM	79332	2/2
Skan Anti-Rootkit	9/16/2009, 2:34 PM	9/16/2009, 2:39 PM	114020	0/0
Skanuj cały komputer	9/16/2009, 2:20 PM	9/16/2009, 2:23 PM	81402	0/0
Skan Anti-Rootkit	9/16/2009, 2:03 PM	9/16/2009, 2:04 PM	19689	0/0
Skan zaplanowany	9/16/2009, 9:42 AM	9/16/2009, 10:33 AM	220728	10/10

At the bottom of the window, there are buttons for "Wyświetl szczegóły" (Show details), "Usuń - Wynik" (Remove - Result), and "Wstecz" (Back). On the left side, there is a sidebar with "Przegląd" (Overview), "Skaner" (Scanner), and "Aktualizuj teraz" (Update now) buttons, along with a "Statystyka" (Statistics) section showing scan and update dates, virus database version, and license expiration date.

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 infekcje, ale zainfekowany obiekt został automatycznie usunięty;

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

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

Uwaga: Szczegółowe informacje na temat każdego testu zawiera okno [Wyniki skanowania](#) dostępne po kliknięciu przycisku **Wświetl 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**.

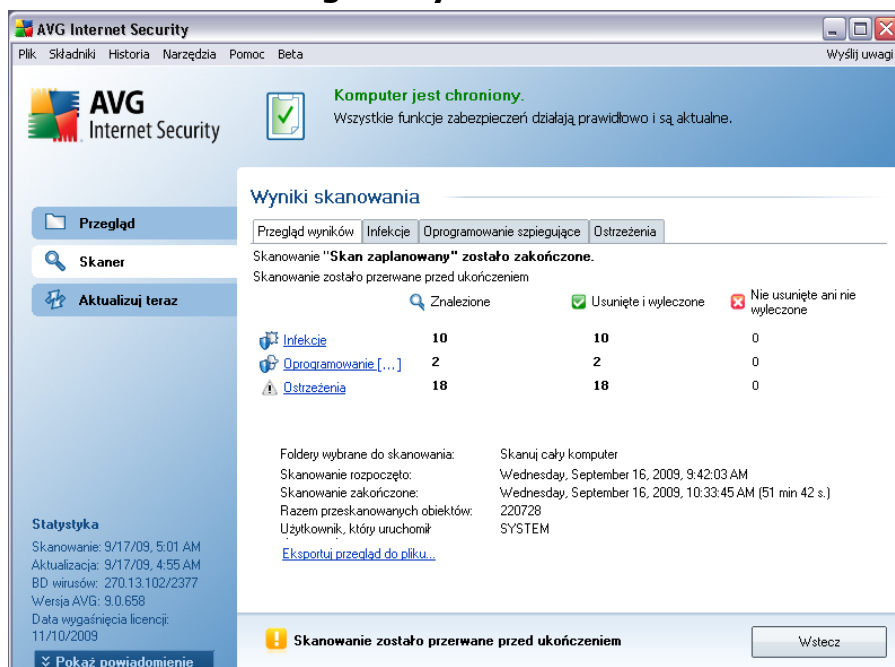
10.7. Szczegóły wyników skanowania

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.
- **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.

10.7.1. Karta "Przegląd wyników"



AVG Internet Security

Plik Składniki Historia Narzędzia Pomoc Beta Wyslij uwagi

AVG Internet Security Komputer jest chroniony. Wszystkie funkcje zabezpieczeń działają prawidłowo i są aktualne.

Wyniki skanowania

Przegląd wyników | Infekcje | Oprogramowanie szpiegujące | Ostrzeżenia

Skanowanie "Skan zaplanowany" zostało zakończone.
Skanowanie zostało przerwane przed ukończeniem.

	Znalezione	Usunięte i wyleczone	Nie usunięte ani nie wyleczone
Infekcje	10	10	0
Oprogramowanie [...]	2	2	0
Ostrzeżenia	18	18	0

Foldery wybrane do skanowania: Skanuj cały komputer
 Skanowanie rozpoczęto: Wednesday, September 16, 2009, 9:42:03 AM
 Skanowanie zakończone: Wednesday, September 16, 2009, 10:33:45 AM (51 min 42 s.)
 Razem przeskanowanych obiektów: 220728
 Użytkownik, który uruchomił: SYSTEM

[Eksportuj przegląd do pliku...](#)

Statystyka
 Skanowanie: 9/17/09, 5:01 AM
 Aktualizacja: 9/17/09, 4:55 AM
 BD wirusów: 270.13.102/2377
 Wersja AVG: 9.0.658
 Data wygaśnięcia licencji: 11/10/2009

! Skanowanie zostało przerwane przed ukończeniem Wstecz

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

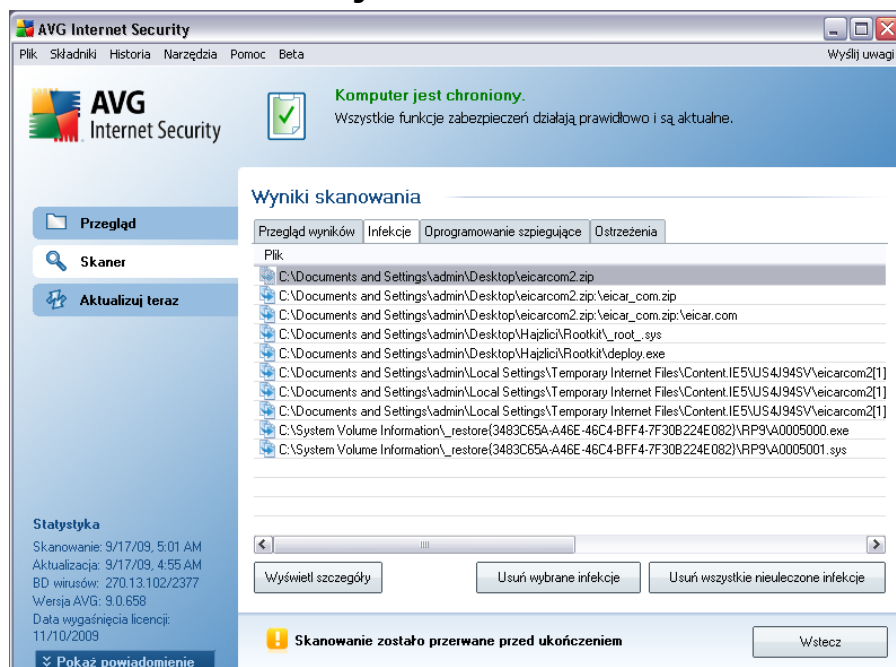
- wykrytych [infekcjach wirusowych/programach szpiegujących](#)
- usuniętych [infekcjach wirusowych/programach szpiegujących](#)
- liczbie [infekcji wirusowych/programów szpiegujących](#), których nie udało się usunąć ani wyleczyć.

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](#).

10.7.2. Karta "Infekcje"



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

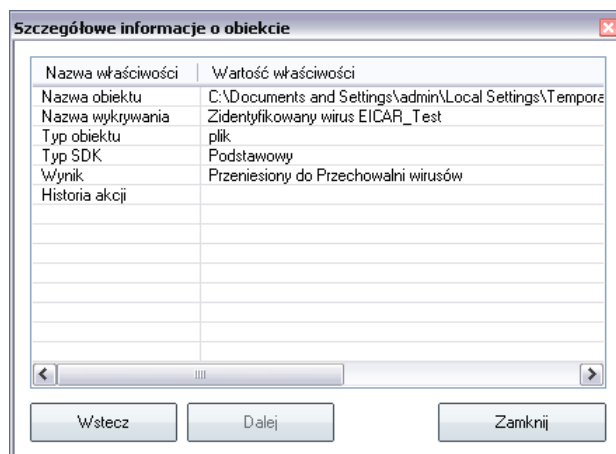
- **Plik** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego obiektu.
- **Infekcje** — nazwa wykrytego [wirusa](#) (*szczegółowe informacje na temat wirusów zawiera [Encyklopedia Wirusów](#) dostępna online*).
- **Wynik** — określa bieżący stan zainfekowanego obiektu, który wykryto podczas skanowania:
 - **Zainfekowany** — zainfekowany obiekt został wykryty i pozostawiony w oryginalnej lokalizacji (*np. jeśli [wylaczono opcje automatycznego leczenia](#) w szczegółowych ustawieniach skanowania*).
 - **Wyleczony** — zainfekowany obiekt został automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
 - **Przeniesiony do Przechowalni** — zainfekowany obiekt został przeniesiony do [Przechowalni wirusów](#).

- **Usunięty** — zainfekowany obiekt został usunięty.
- **Dodany do listy wyjątków PNP** — znaleziony obiekt został uznany za wyjątek i dodany do listy wyjątków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie [Wyjątki PNP](#)*).
- **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanować.
- **Obiekt potencjalnie niebezpieczny** — obiekt został uznany za potencjalnie niebezpieczny, ale nie zainfekowany (*może na przykład zawierać makra*); informacje te należy traktować wyłącznie jako ostrzeżenie.
- **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 przeniesc wybrane obiekty do [Przechowalni wirusów](#).
- **Usun wszystkie niewyleczone pliki** — pozwala usunac wszystkie znalezione obiekty, których nie mozna wyleczyc ani przeniesc do [Przechowalni wirusów](#).
- **Zamknij wyniki** — powoduje zamknięcie szczegółowych wyników i powrót do okna [Przegląd wyników skanowania](#).

10.7.3. Karta "Oprogramowanie szpiegujace"

Karta **Oprogramowanie szpiegujace** jest wyswietlana w oknie dialogowym **Wyniki skanowania** tylko, jesli podczas skanowania wykryto [oprogramowanie szpiegujace](#). Karta jest podzielona na trzy obszary, które zawieraja następujace informacje:

- **Plik** — pelna sciezka do oryginalnej lokalizacji zainfekowanego obiektu.
- **Infekcje** — nazwa wykrytego [oprogramowania szpiegujacego](#) (szczegółowe informacje na temat wirusów zawiera [Encyklopedia Wirusów](#) dostepna online).
- **Wynik** — okresla biezacy stan obiektu, który wykryto podczas skanowania:
 - **Zainfekowany** — zainfekowany obiekt zostal wykryty i pozostawiony w oryginalnej lokalizacji (np. jesli [wylaczono opcje automatycznego leczenia](#) w szczegółowych ustawieniach skanowania).
 - **Wyleczony** — zainfekowany obiekt zostal automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
 - **Przeniesiony do Przechowalni** — zainfekowany obiekt zostal przeniesiony do [Przechowalni wirusów](#).
 - **Usuniety** — zainfekowany obiekt zostal usuniety.
 - **Dodany do listy wyjątków PNP** — znaleziony obiekt zostal uznany za wyjątek i dodany do listy wyjątków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie [Wyjątki PNP](#)*).
 - **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanowac.
 - **Obiekt potencjalnie niebezpieczny** — obiekt zostal uznany za

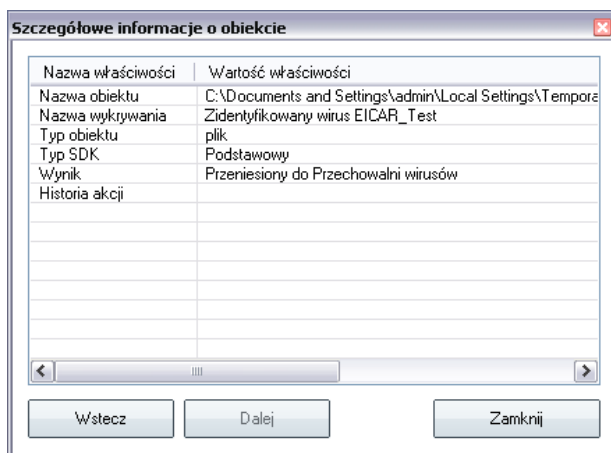
potencjalnie niebezpieczny, ale nie zainfekowany (może np. zawierać makra); informacja ta jest wyłącznie ostrzeżeniem.

- 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**:

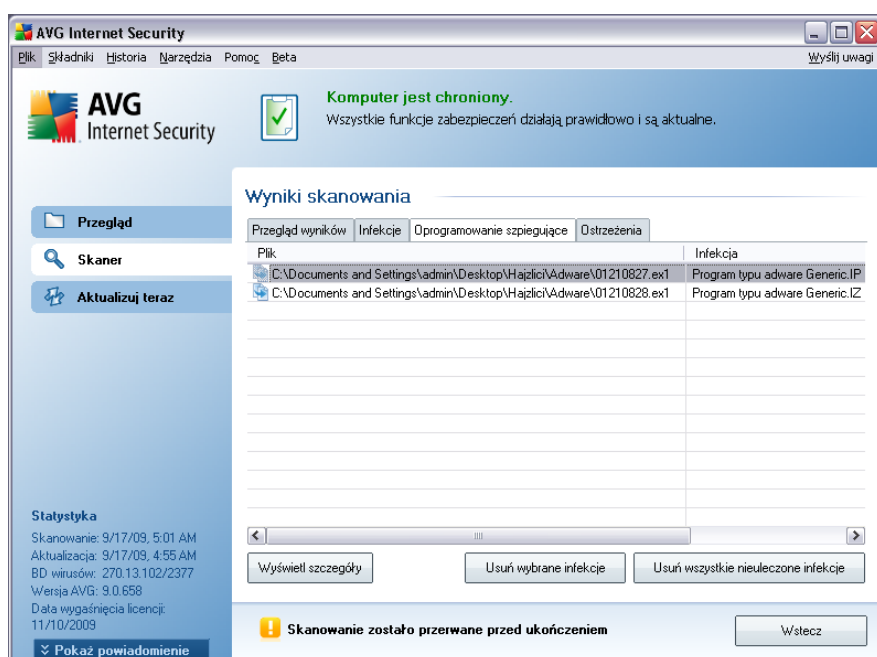


Można w nim znaleźć informacje o lokalizacji wykrytego pliku (**Nazwa właściwości**). Przyciski **Wstecz** i **Dalej** służą do nawigacji między pozycjami listy. Przycisk **Zamknij** zamyka okno.

- **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](#).

10.7.4. Karta "Ostrzeżenia"

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



Oto krótki opis najbardziej popularnych obiektów tego typu:

- **Pliki ukryte** Pliki ukryte są domyślnie niewidoczne dla użytkownika w systemie Windows. Niektóre wirusy mogą próbować uniknąć wykrycia przez wykorzystanie tej właściwości. Jeśli system AVG zgłasza obecność ukrytego pliku, który może być szkodliwy, można przenieść go do **Przechowalni wirusów AVG**.
- **Pliki cookie** Pliki cookie to pliki tekstowe wykorzystywane przez strony internetowe do przechowywania informacji właściwych dla danego użytkownika. Są one później używane do ładowania witryn internetowych dostosowanych do wymagań użytkownika, itp.

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

10.7.5. Karta "Informacje"

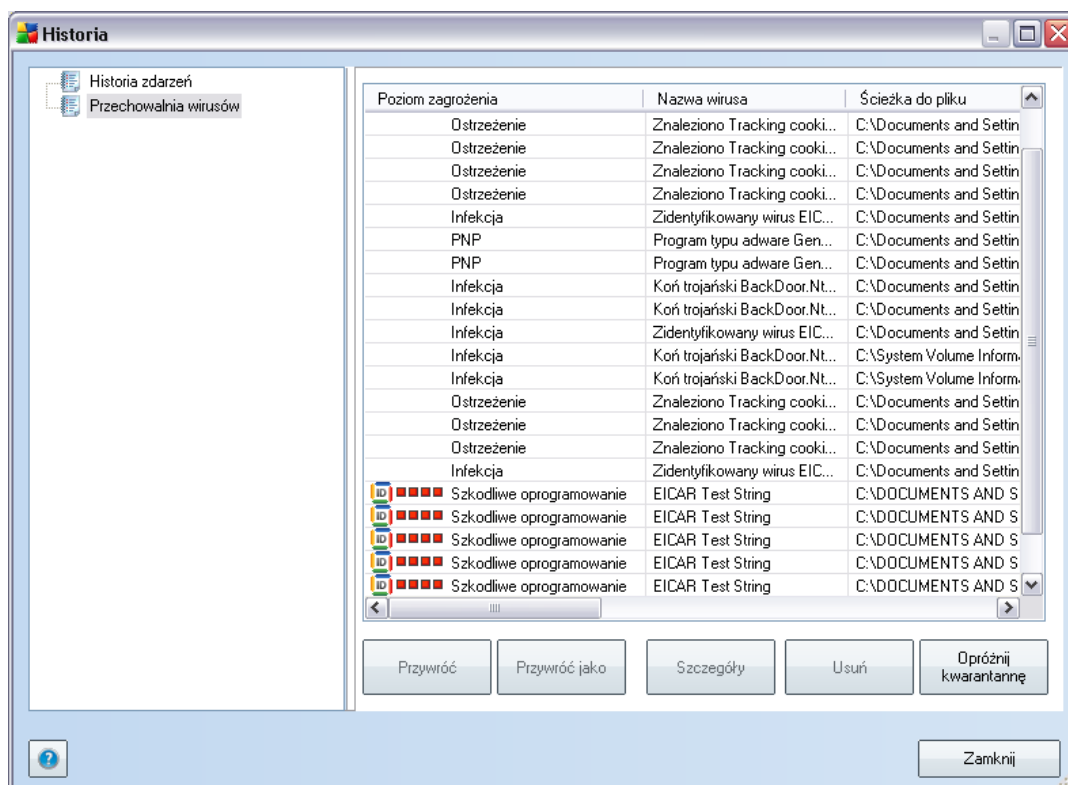
Karta **Informacje** zawiera dane dotyczące znalezionych obiektów, których nie można zakwalifikować jako infekcje, oprogramowanie szpiegujące itp. Obiektów tych nie można w stu procentach uznać za niebezpieczne, ale często wymagają one uwagi użytkownika. Skaner AVG jest w stanie wykryć pliki, które mogą 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.
- **Niewłaściwa ścieżka do pliku** — jeżeli jakiś ważny plik systemowy jest uruchamiany z innej ścieżki niż domyślna (np. plik "winlogon.exe" jest uruchamiany z folderu innego niż Windows), system AVG zgłasza tę niezgodność. W niektórych przypadkach wirusy używają nazw standardowych procesów systemowych, aby ich obecność w systemie była trudniejsza do wychwycenia przez użytkownika.
- **Plik zablokowany** — raportowany plik jest zablokowany, dlatego nie może zostać przeskanowany przez system AVG. Oznacza to zazwyczaj, że dany plik

jest stale używany przez system (np. plik wymiany).

10.8. Przechowalnia wirusów



Przechowalnia wirusów to bezpieczne środowisko przeznaczone do zarządzania podejrzanymi/zainfekowanymi obiektami, które zostały wykryte podczas testów 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. Zalecany rozwiązaniem jest przeniesienie obiektu do **Przechowalni wirusów**, skąd można będzie podjąć dalsze działania związane z analizą, wyleczeniem lub usunięciem pliku.

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

- **Zagrożenie** — zawiera graficzną reprezentację poziomu znalezionej zagrożenia w czterostopniowej skali — od "nieistotne" (■□□□) do "bardzo niebezpieczne" (■□□■)

- **Typ infekcji** — klasyfikuje obiekty według poziomu infekcji (*wszystkie obiekty na liście są prawdopodobnie lub na pewno zainfekowane*).
- **Nazwa wirusa** — nazwa wykrytej infekcji pochodząca z [Encyklopedii wirusów](#) (online).
- **Ścieżka do pliku** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego pliku.
- **Pierwotna nazwa obiektu** — wszystkie wykryte obiekty na liście zostały oznaczone standardowymi nazwami określanymi przez AVG w trakcie skanowania. W przypadku gdy obiekt miał określoną nazwę, która jest znana (np. nazwa załącznika wiadomości e-mail, która nie odpowiada faktycznej zawartości załącznika), jest ona podawana w tej kolumnie.
- **Data zachowania** — data i godzina wykrycia podejrzanego pliku i przeniesienia go do **Przechowalni**.

Przyciski kontrolne

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

- **Przywróć** — przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- **Przywróć jako** — jeśli zainfekowany obiekt ma zostać przeniesiony poza **Przechowalnię**, do określonego folderu, ten przycisk pozwala zapisać obiekt z nazwą inną niż pierwotna. Jeśli nazwa pierwotna nie jest znana, użyta zostanie nazwa standardowa.
- **Usuń** — usuwa bezpowrotnie zainfekowany plik z **Przechowalni wirusów**.
- **Opróżnij przechowalnię** — usuwa bezpowrotnie całą zawartość **Przechowalni wirusów**.

11. Aktualizacje AVG

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

11.1. Poziomy aktualizacji

Program AVG oferuje dwa poziomy aktualizacji:

- **Aktualizacja definicji** zawiera uzupełnienia niezbędne do zapewnienia niezawodnej ochrony antywirusowej. Na ogół nie zawiera modyfikacji programu i aktualizuje tylko 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.

11.2. 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.

11.3. Proces aktualizacji

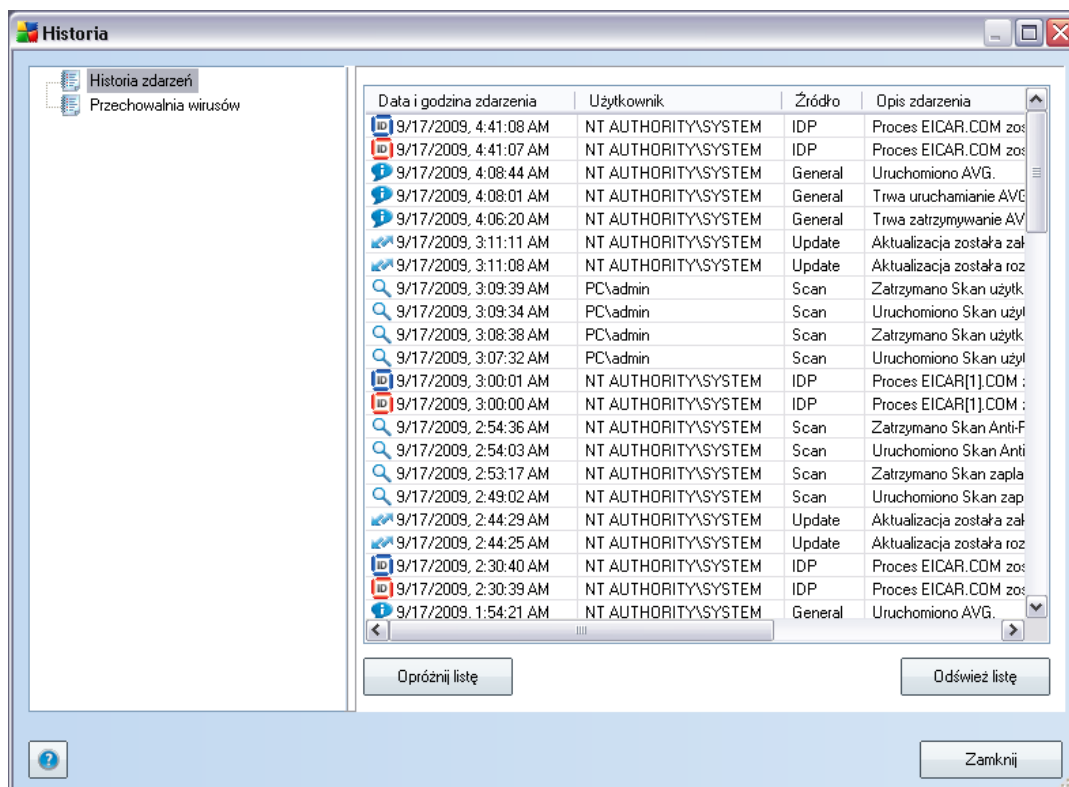
Aktualizacje można uruchamiać na zadanie, gdy są potrzebne, klikając link [Aktualizuj teraz](#). Link ten jest zawsze dostępny w głównym oknie [interfejsu użytkownika AVG](#). Mimo to, zaleca się regularne aktualizowanie systemu, zgodnie z harmonogramem,

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!

12. 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 Anti-Virus**. **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.
- **Odswież listę** — powoduje odświeżenie zawartości listy zdarzeń.

13. FAQ i pomoc techniczna

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

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