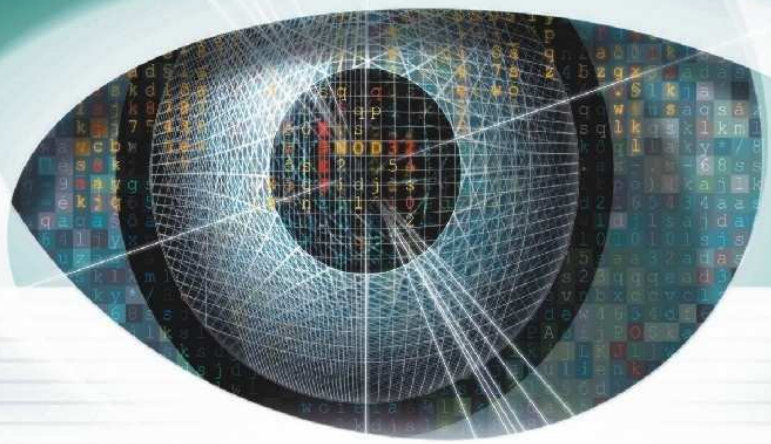
system
antywirusowy



NOD 32
antivirus system

Podręcznik użytkownika

polska wersja językowa

ESET

Kontakt

Producent:

Eset Software
1172 Orange Ave
Coronado
California, 92118
USA
Tel: (619) 437–7037
www.nod32.com

Dystrybutor w Polsce:

DAGMA Sp. z o.o.
ul. Pszczyńska 15
40–478 Katowice, Polska
Tel: +48 32 259–11–00
Fax: +48 32 259–11–90
www.nod32.pl
www.dagma.pl

E–mail:

sprawy handlowe	sales@nod32.pl
sprawy techniczne	support@nod32.pl

W przypadku wystąpienia problemów technicznych podczas pracy z NOD32, skontaktuj się z producentem lub dystrybutorem systemu w Polsce. Informacje o zidentyfikowanych problemach i proponowanych rozwiązaniach znajdziesz w sekcji Pomoc na stronie www.nod32.pl

Spis treści

Informacje ogólne

Wprowadzenie

Witamy w szybko powiększającej się rodzinie użytkowników programu antywirusowego NOD32 firmy ESET. W ciągu ostatnich kilku lat udało nam się opracować produkt charakteryzujący się bardzo wysoką stabilnością, niezawodnością oraz skutecznością w wykrywaniu i eliminowaniu wirusów, czego dowodem jest szereg międzynarodowych wyróżnień i certyfikatów. W chwili obecnej oddajemy do Państwa dyspozycji nową, udoskonaloną wersję programu NOD32 v. 2.7. Wszelkie zmiany oraz udoskonalenia programu NOD32 zostały wprowadzone w znacznej mierze dzięki cennym sugestiom oraz pomysłom użytkowników programu. Za wszelkie uwagi dotyczące programu NOD32 serdecznie dziękujemy. Jesteśmy przekonani, że program NOD32 v. 2.7 spełni Państwa oczekiwania oraz wymagania dotyczące skutecznej i niezawodnej ochrony antywirusowej.

Instrukcja została przygotowana w formacie PDF i do jej odczytania konieczna jest bezpłatna przeglądarka „Acrobat Reader", której wersja instalacyjna znajduje się na płycie CD razem z programem NOD32 lub może być pobrana ze strony producenta przeglądarki (www.adobe.com). Pomoc dotyczącą programu NOD32 i jego poszczególnych modułów można również uzyskać wciskając klawisz F1 lub przycisk POMOC w głównym oknie programu.

Zachęcamy użytkowników do przesyłania do nas swoich pytań, pomysłów i komentarzy dotyczących systemu. Z całą pewnością zostaną one dokładnie przeanalizowane i wykorzystane przy opracowywaniu kolejnych wersji oprogramowania.

Aktualne informacje (o systemie, wirusach, wyróżnieniach, nowościach) można uzyskać odwiedzając strony poświęcone NOD32: w języku angielskim www.nod32.com oraz w języku polskim www.nod32.pl.

Dziękujemy za zaufanie i wybór systemu antywirusowego NOD32!
Przekazujemy pozdrowienia,
Producent firma ESET, LLC oraz dystrybutor w Polsce DAGMA sp. z o.o.

Analiza heurystyczna

Czy posiadając dobry system ochrony antywirusowej możesz czuć się bezpieczny? I tak i nie! Tak, bo dobre programy są sprawdzone i posiadają dużą, często aktualizowaną bazę szczepionek wirusowych. Nie – bo nawet najbardziej obszerna konwencjonalna baza nie zawiera remedium na coś co jeszcze nie istnieje, nie zostało zbadane i opisane. Ponad 80% wartości szkód wywołują wirusy całkiem nowe, o których jeszcze nikt nie słyszał! Nie należy jednak bezradnie rozkładać rąk, bowiem problem rozpoznawania i usuwania nowych wirusów udało się rozwiązać poprzez zastosowanie **zaawansowanych narzędzi heurystycznych**.

Wszystkie moduły skanujące programu NOD32 (**AMON, IMON, EMON, DMON**) zostały wyposażone w nową, **zaawansowaną heurystykę,** obok znanej już z poprzedniej wersji standardowej analizy heurystycznej. Zadaniem zaawansowanej analizy heurystycznej jest monitorowanie oraz dokładne sprawdzanie czy wraz z przesyłaną pocztą elektroniczną do komputera nie próbuje przedostać się jakiś nowy robak lub trojan.

Czym jest heurystyka? Heurystyka jest techniką wykrywania nieznanych i niezidentyfikowanych wirusów. Analiza heurystyczna polega na dokładnym monitorowaniu zawartości pliku oraz sprawdzaniu, czy plik nie wykazuje zachowań charakterystycznych dla wirusa. Na podstawie dokonanej analizy następuje rozpoznanie czy plik może być zainfekowany, czy też jest w pełni bezpieczny dla użytkownika, gdyż nie zawiera złośliwych kodów.

Mówiąc krótko, **zaawansowana heurystyka jest tym co najbardziej odróżnia programy dobre od systemów bardzo dobrych i naprawdę skutecznych.**

Czy słyszałeś o słynnych wirusach Opaserv, Blaster czy Bugbear, które w ciągu ostatnich kilku miesięcy spowodowały mnóstwo szkód materialnych i zamieszania na całym świecie? Myślę, że tak! Być może nawet Tobie przydarzyło się w związku z nimi coś przykrego? **Najprawdopodobniej nie wiesz jednak, że wszystkich tych problemów można było uniknąć, gdyż istniało narzędzie, które potrafiło te wirusy wykrywać i neutralizować zanim jeszcze zostały stworzone.**

Takim narzędziem jest właśnie system NOD32 posiadający **moduły zaawansowanego heurystycznego wykrywania wirusów**, który na podstawie ich zachowań rozpoznaje nowe pojawiające się dopiero zagrożenia wirusowe i jest w stanie je eliminować! **W opinii wielu fachowców z branży skuteczność wykrywania wirusów przez zaawansowany moduł heurystyczny NOD32 nie ma sobie równych.**

NOD32 jest bardzo szybki, skuteczny, łatwo się instaluje, automatycznie aktualizuje za pośrednictwem Internetu, chroni zarówno pliki jak i pocztę elektroniczną, ma niewielkie wymagania systemowe, konkurencyjną cenę, bezpłatną pomoc techniczną i polską wersję językową – czyli to co powinien mieć najlepszy program antywirusowy.

Opis systemu

Nowa generacja systemu antywirusowego NOD32 jest produktem najwyższej jakości, co jest wynikiem wieloletniego doświadczenia oraz zastosowania najnowocześniejszych technologii. Intencją twórców było wyposażenie użytkownika we wszystkie środki niezbędne do skutecznego wykrywania i usuwania wirusów. Bardzo sobie cenimy zaufanie do naszego produktu, które motywuje nas do dalszej, jeszcze bardziej wytężonej pracy. Dotychczasowe imponujące sukcesy programu NOD32 dają gwarancję, że jest on skutecznym i niezawodnym narzędziem, które dba o pełne bezpieczeństwo Twoich danych.

NOD32 składa się z czterech modułów skanujących:

NOD32 – samodzielny, 32–bitowy skaner „na żądanie"

AMON – rezydentny skaner antywirusowy

IMON – monitor internetowy, skanujący pocztę elektroniczną na stacjach roboczych

DMON – rezydentny skaner dokumentów Microsoft Office

EMON – skaner poczty Microsoft Outlook, skanujący pocztę elektroniczną odbieraną i wysyłaną przy pomocy programu Microsoft Outlook.

Dodatkowo jest dostępny:
NOD32DOS – 32–bitowy program uruchamiany w środowisku DOS lub w trybie awaryjnym systemu Windows.

Aby ułatwić korzystanie z pomocy, wszystkie moduły są ze sobą kompatybilne, a panele kontrolne są zbudowane w podobny sposób. Ponadto opisy

poszczególnych (nawet identycznych) modułów zostały zamieszczone niezależnie od siebie.

Wymagania sprzętowe i systemowe

Minimalne wymagania dla systemu Windows:

Wspierane są poniższe systemy operacyjne:

- Windows 98/ ME
- Windows NT / 2000
- Windows XP – 32 - bitowy i 64 bitowy
- Windows 2003
- Windows Vista 32 -bitowy i 64 - bitowy

Procesor Pentium/Celeron/AMD 300 MHz
30MB wolnego miejsca na dysku
128MB RAM
Karta graficzna VGA, zalecana SVGA, rozdzielczość 800x600, High Color

Małe wymagania sprzętowe udało się uzyskać dzięki zaprogramowaniu kluczowych modułów systemu przy pomocy języka ASSEMBLER.

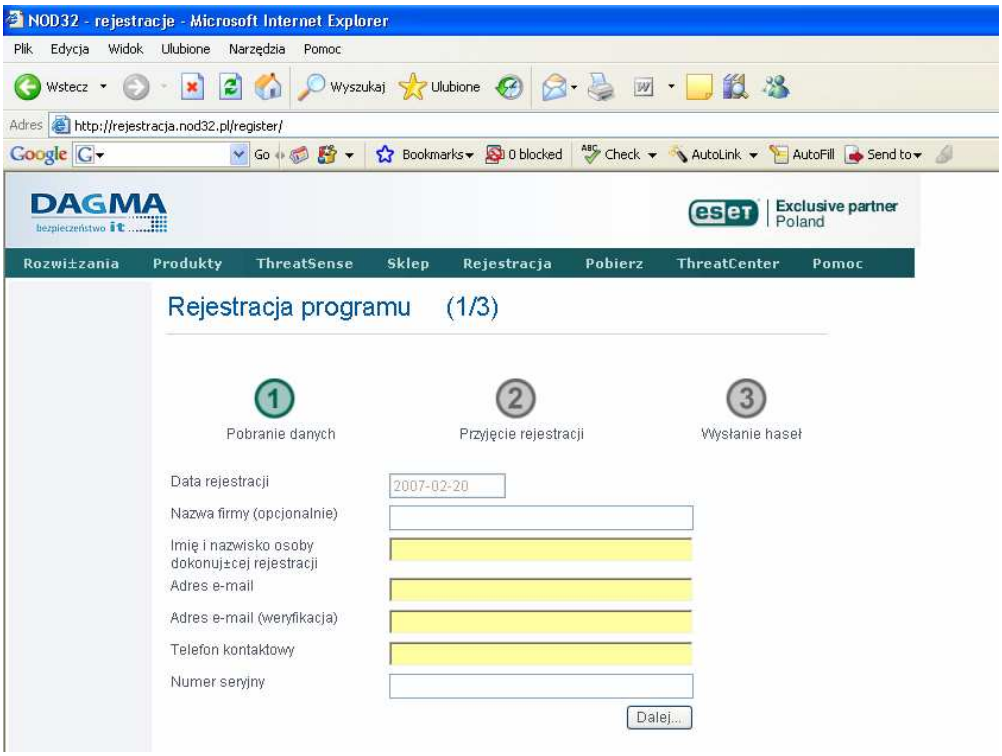
Rejestracja użytkownika

W przypadku programu NOD32 konieczna jest rejestracja użytkownika, ponieważ umożliwia aktualizację bazy wirusów i komponentów programu w trybie on–line.

Rejestracji można dokonać na stronie http://rejestracja.nod32.pl/ . Należy wypełnić wymagane pola:
Nazwa firmy (opcjonalnie)
Imię i nazwisko osoby dokonującej rejestracji
Adres e–mail
Telefon kontaktowy
Numer seryjny programu podany na Certyfikacie
i nacisnąć przycisk ***Dalej***. Za pośrednictwem poczty elektronicznej zostaną przesłane **nazwa użytkownika** i **hasło**, które po wprowadzeniu w odpowiednie pola Systemu NOD32, umożliwią aktualizowanie programu NOD32 w okresie obowiązywania licencji. Więcej informacji można znaleźć w rozdziale „System NOD32".

Należy upewnić się, że wprowadzone dane są poprawne. W przypadku gdy zostanie podany błędny adres e–mail, nazwa użytkownika i hasło nie zostaną dostarczone.

UWAGA: Numer seryjny programu NOD32 można zarejestrować tylko jeden raz!!!



UWAGA : Użytkownicy korporacyjni oraz indywidualni, którzy otrzymali **nazwę użytkownika** i **hasło** w momencie zakupu (podane na Certyfikacie), nie muszą rejestrować programu.

Test skanera

Po zakończeniu konfiguracji zalecamy przetestowanie ustawień. W tym celu należy wejść na stronę internetową http://wirusy.pl/testuj_poczte . Można z niej wysłać „zawirusowaną" wiadomość, która pozwoli przetestować konfigurację ochrony antywirusowej naszej skrzynki pocztowej. Przesyłany plik nie jest zainfekowany, tzn. nie zawiera prawdziwego wirusa, a jedynie charakterystyczny ciąg znaków (sygnaturę), która jest rozpoznawana przez większość programów antywirusowych jako „wirus testowy" o nazwie **EICAR**. Jego działanie polega jedynie na jednorazowym wyświetleniu wiadomości informacyjnej. Jeżeli skaner

programu NOD32 (IMON lub EMON) poinformuje nas o znalezionym „wirusie testowym", będzie to oznaczać, że konfiguracja przebiegła pomyślnie i nasza poczta jest sprawdzana na obecność wirusów.

UWAGA: Dla pewności sugerujemy niezależne wysłanie „wirusa testowego" EICAR na każde z zainstalowanych na stacji kont poczty elektronicznej.

Instalacja Systemu Antywirusowego NOD32

Przed rozpoczęciem instalacji należy sprawdzić czy na dysku znajduje się wystarczająco dużo miejsca. Instalacja programu NOD wymaga około 30 MB wolnego miejsca na dysku.

UWAGA: Jednoczesne użytkowanie dwóch rezydentnych skanerów antywirusowych w systemie Windows może doprowadzić do niestabilności systemu. Jeszcze przed instalacją programu NOD32, należy sprawdzić czy na komputerze nie ma innych programów antywirusowych. Jeżeli w systemie jest już zainstalowany jakiś program antywirusowy to należy go odinstalować lub wyłączyć jego rezydentny skaner.

Pobranie oprogramowania

Pliki instalacyjne programu NOD32 można znaleźć:

na płycie CD. Po umieszczeniu płyty w napędzie automatycznie wyświetli się menu prezentujące możliwe do wybrania opcje instalacyjne (wersja standardowa lub wersja administracyjna). Następnie należy wybrać odpowiednią wersję językową programu.

Na płycie znajdują się zarówno wersje programu przeznaczone dla systemu Windows 98/ME jak i Windows NT/2000/XP/2003/Vista. Program instalacyjny sprawdzi system operacyjny i automatycznie wybierze odpowiednią wersję programu.

Jeżeli nie nastąpi samoczynne uruchomienie programu instalacyjnego, należy ręcznie uruchomić program instalacyjny przechodząc na Start, następnie Uruchom i wpisać literę odpowiadającą napędowi CD–ROM, np. D:.

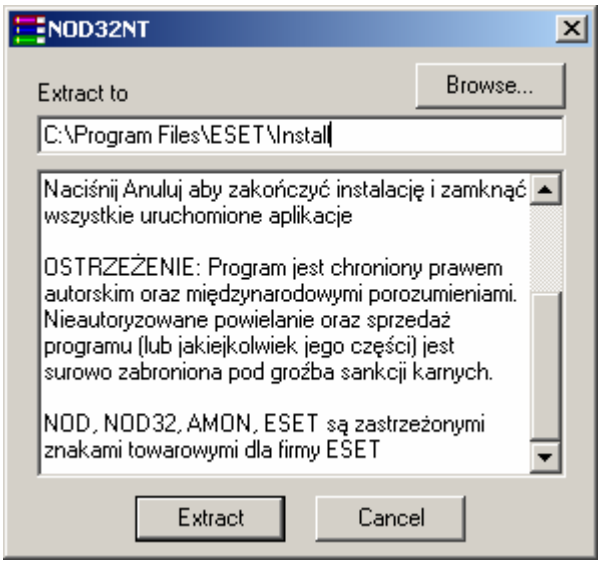
Następnie należy przejść do katalogu:

\Polska\Pelna\Win95st – pełna wersja polska dla systemów Windows 98/ME

\Polska\Pelna\Winntst – pełna wersja polska dla systemów Windows NT/2000/XP/2003/Vista

i uruchomić plik SETUP.EXE.

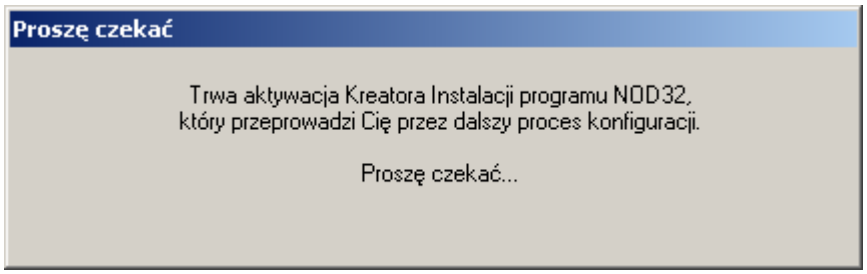
na stronie www.nod32.com/download i www.nod32.pl/download. Należy upewnić się, że pobierana wersja jest odpowiednia dla danego systemu operacyjnego, np. Windows 98/Me lub Windows NT/2000/XP/2003/Vista. Po pobraniu odpowiedniego pliku należy go uruchomić i nacisnąć ***Extract***, aby kontynuować instalację.



Wcześniejsze wersje programu NOD32

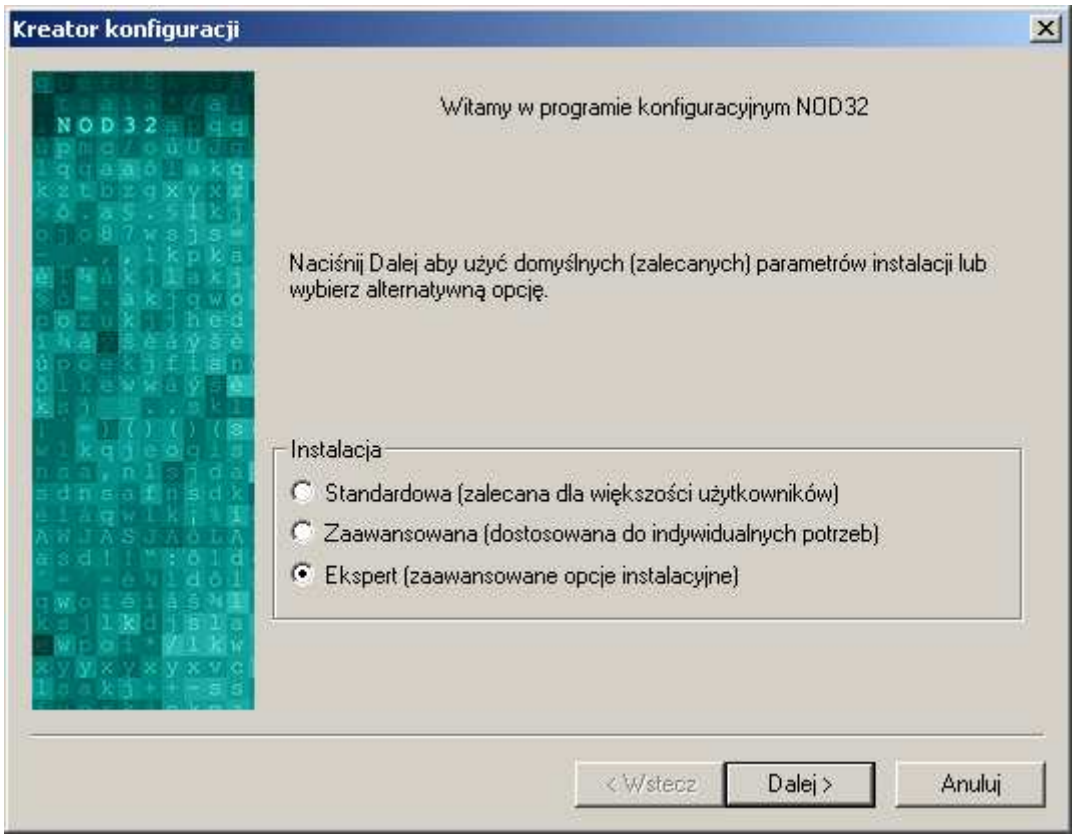
W pierwszym kroku, program instalacyjny NOD32 poszukuje poprzednich wersji programu NOD32, które mogą już być zainstalowane w systemie. Jeżeli program jest już zainstalowany w systemie należy przejść do rozdziału Reinstalacja systemu antywirusowego NOD32 w dalszej części dokumentacji.

Po uruchomieniu pliku SETUP.EXE pojawia się okno informujące o rozpoczęciu procesu instalacji programu NOD32



Typy instalacji

Instalacja programu NOD32 rozpoczyna się wyborem typu instalacji:
standardowa – zalecana dla większości użytkowników
zaawansowana – przeznaczona dla administratorów
ekspert – pozwalająca na ręczne ustawienie wszystkich opcji instalacyjnych.



Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

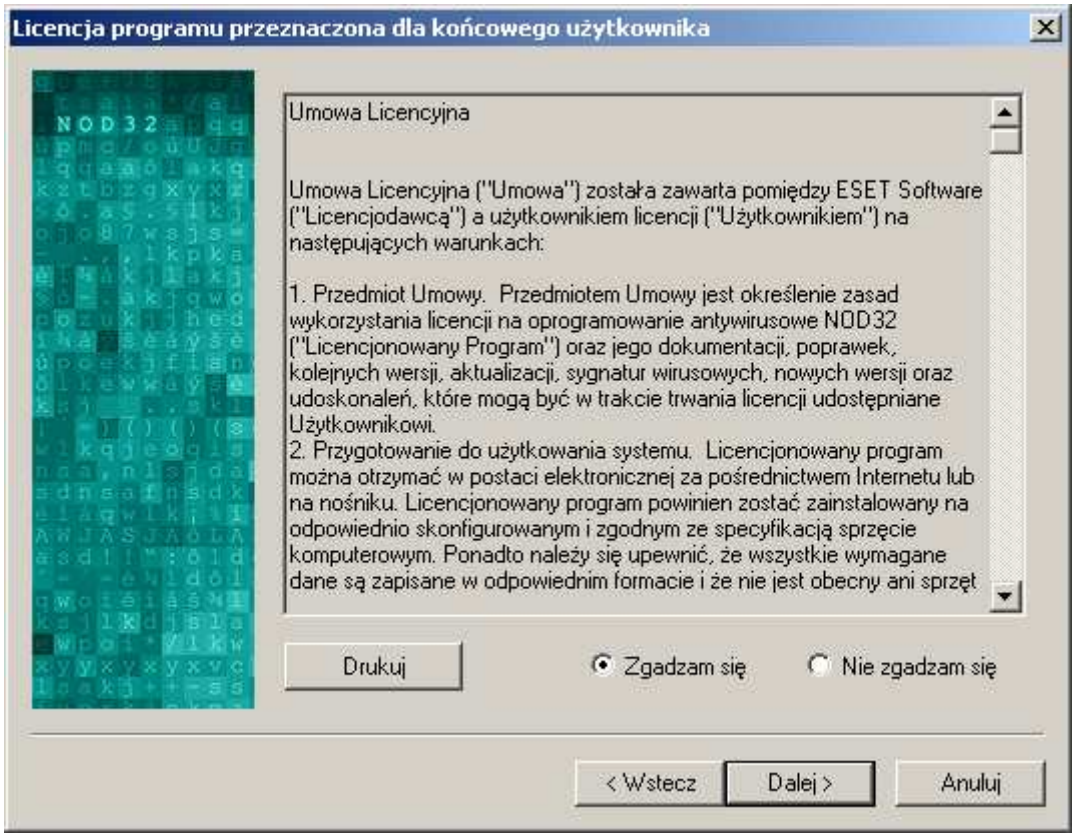
W zależności od wybranego typu instalacji dostępne są różne opcje konfiguracji systemu.

Opcje	Standardowa	Zaawansowana	Ekspert
Wybór folderu docelowego		X	X
Włączenie/wyłączenie trybu cichego		X	X
Zabezpieczenie ustawień hasłem		X	X
Interfejs graficzny użytkownika			X
Włączenie/wyłączenie okna powitalnego NOD32			X
Powiadomienia wysyłane pocztą i przy pomocy Windows Messenger			X
Wybór serwera aktualizacji oraz wpisanie nazwy użytkownika i hasła	X	X	X
Wybór połączenia z Internetem i ustawienia serwera Proxy	X	X	X
Konfiguracja automatycznej aktualizacji		X	X
Automatyczne włączenie modułu AMON w trakcie uruchomienia komputera	X	X	X
Umieszczenie ikony skanera „na żądanie” na pulpicie		X	X
Dołączenie skanera „na żądanie” do menu kontekstowego		X	X
Włączenie/wyłączenia modułu IMON, konfiguracja skuteczności i kompatybilności IMON–a		X	X
Włączenie/wyłączenie modułu EMON – skaner poczty Microsoft Outlook	X	X	X

Większość opcji jest dostępna w konsoli systemu i może zostać skonfigurowana po zakończeniu procesu instalacji programu NOD32.

Umowa licencyjna

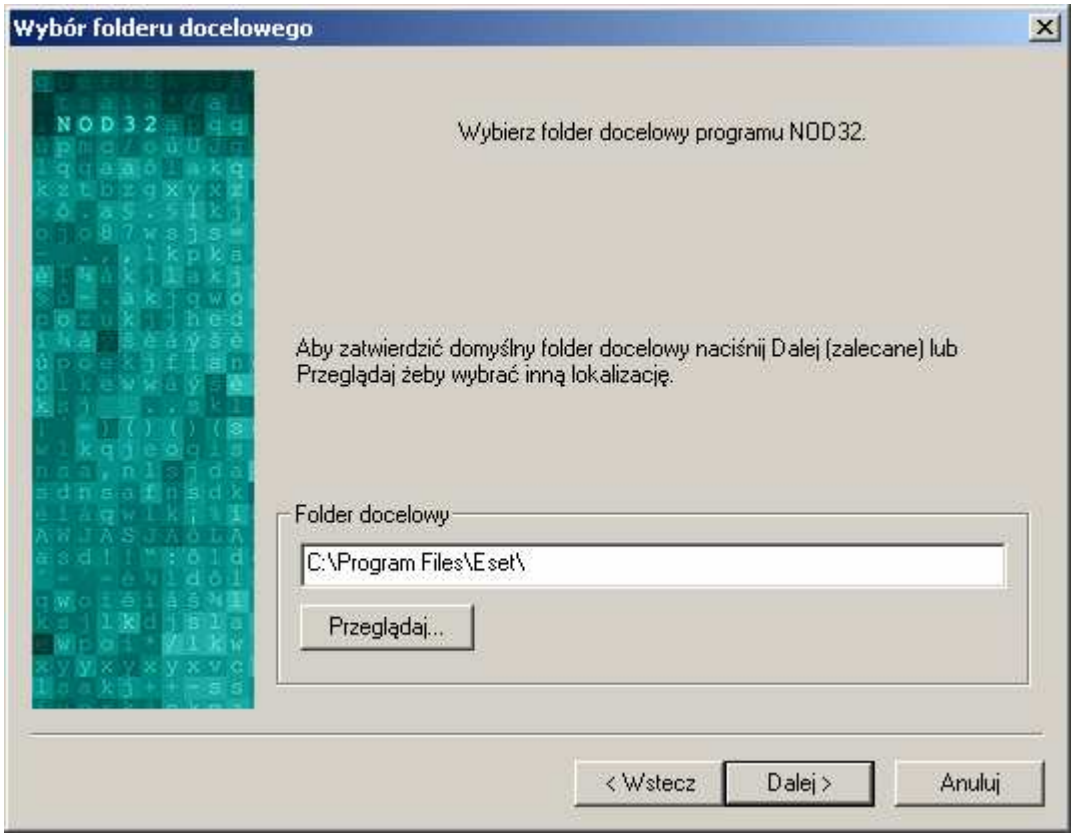
Po wybraniu typu instalacji kolejne okno wyświetla treść umowy licencyjnej, z którą należy się zapoznać, a następnie zaakceptować, aby kontynuować instalację.



Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Docelowy folder programu NOD32

Należy wybrać folder docelowy gdzie zostanie zainstalowany program NOD32. Zalecane jest pozostawienie domyślnej ścieżki instalacyjnej.

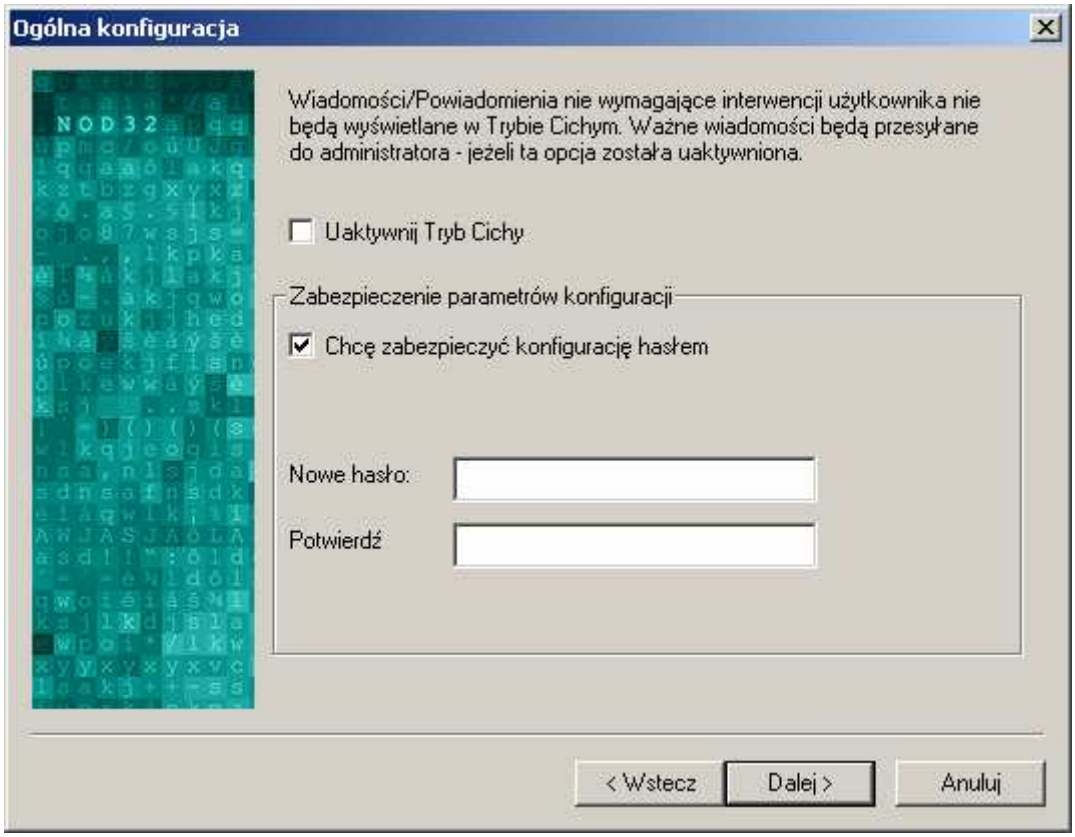


Opcja dostępna w wersjach zaawansowanej i ekspert

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Konfiguracja trybu wyświetlania komunikatów

Istnieje możliwość aktywowania trybu cichego. W tym trybie wyświetlane będą jedynie informacje o wirusach wykrytych przez monitor antywirusowy AMON. Cichy tryb wpływa również na redukcję ruchu w sieci generowanego przez użytkowników. Nie będą wyświetlane informacje o zaktualizowanej bazie, zaktualizowanych komponentach programu, itp.



Opcje dostępne w wersjach zaawansowanej i ekspert

Zabezpieczenie hasłem parametrów konfiguracji

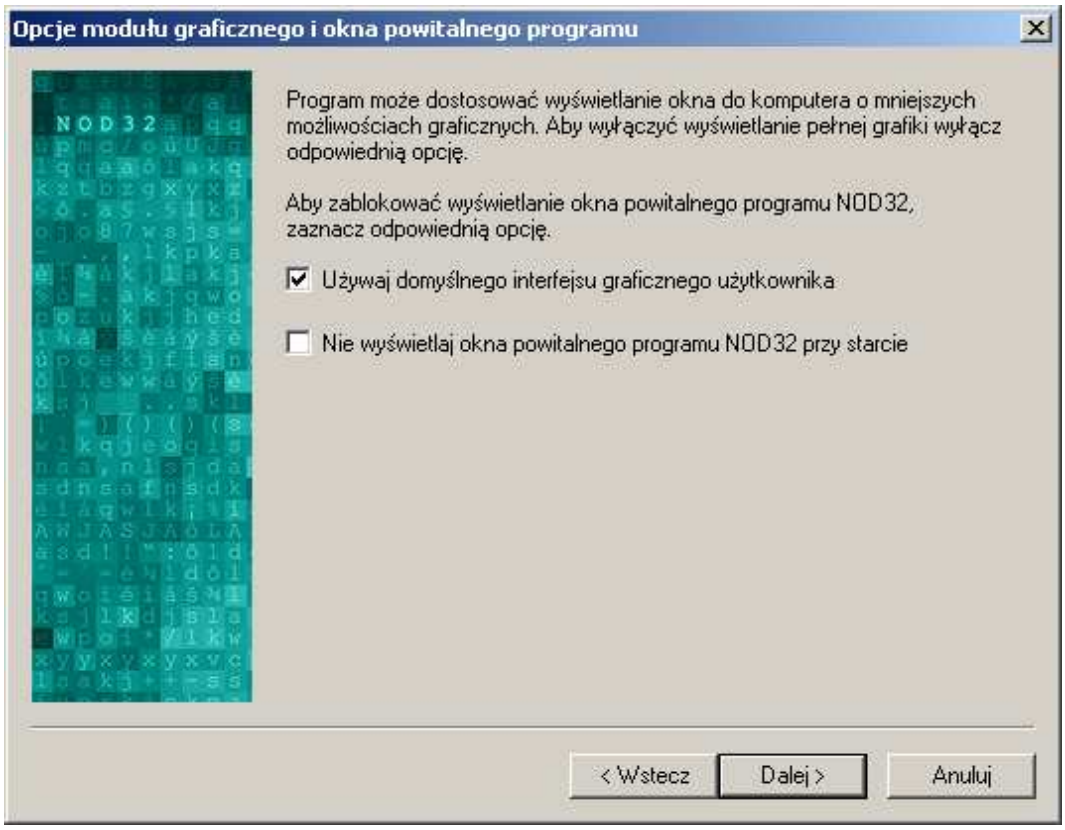
Aby uniknąć nieautoryzowanych modyfikacji, ogólne parametry konfiguracji systemu NOD32 mogą być zabezpieczone hasłem. W tym celu należy ustawić hasło zabezpieczające.

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Opcje modułu graficznego i okna powitalnego programu

Program NOD32 może być wyświetlany w dwóch trybach: graficznym NOD32 i standardowym Windows. Domyślnie jest używany tryb graficzny, jeżeli jest obsługiwany przez komputer.

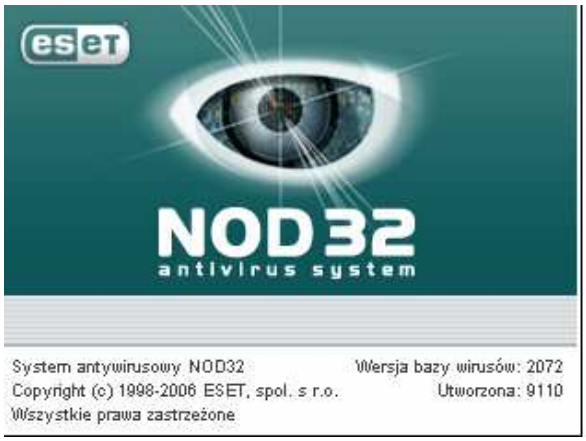
Aby używać domyślnego interfejsu graficznego programu NOD32 należy zaznaczyć opcję *„Używaj domyślnego interfejsu graficznego użytkownika*". W przeciwnym przypadku zostanie ustawiony domyślny interfejs systemu Windows.



Opcje dostępne w wersji ekspert

Okno powitalne systemu NOD32

Podczas startu systemu wyświetlane jest okno powitalne systemu NOD32.



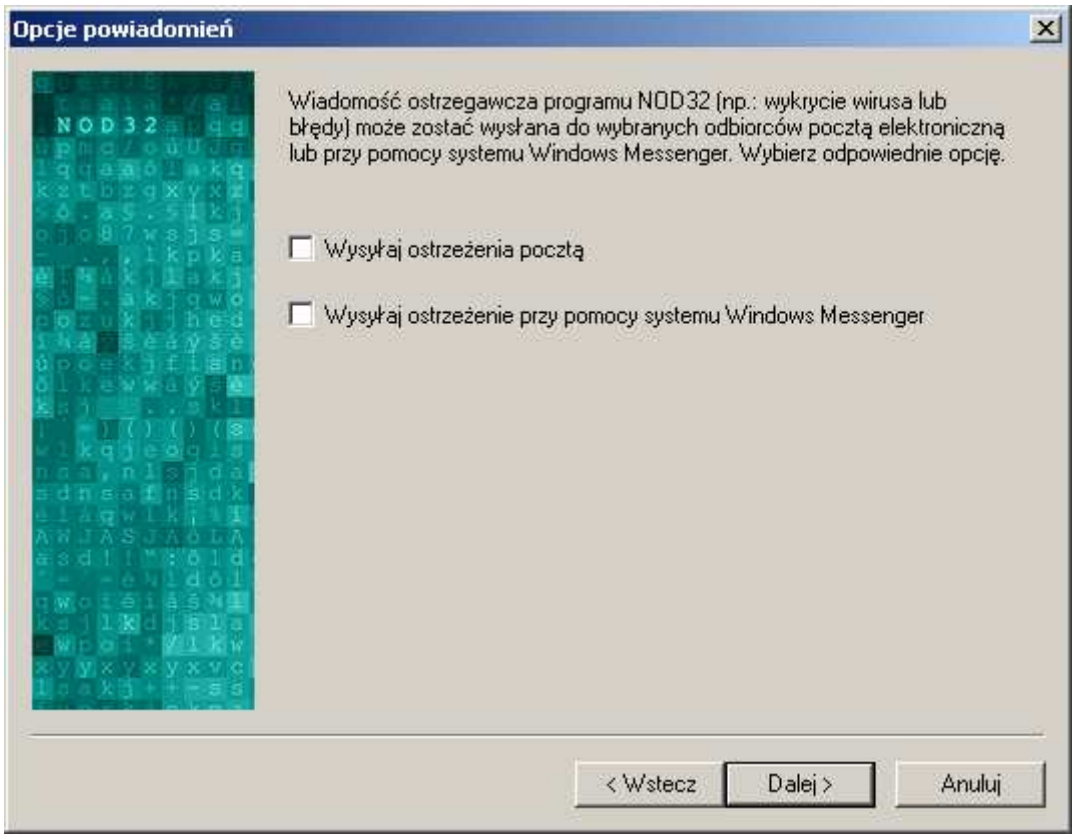
Aby wyłączyć okno powitalne należy zaznaczyć opcję *„Nie wyświetlaj okna powitalnego programu NOD32 przy starcie”*.

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Wybór powiadomień

Opcje powiadomień są używane do konfigurowania komunikacji między systemem NOD32 a zdalnym użytkownikiem lub administratorem systemu. Wyszczególnione są dwa sposoby wysyłania powiadomień:
SMTP (poczta e–mail)
System Windows ® Messenger

Aby wysyłać powiadomienia przez serwer SMTP należy zaznaczyć opcję *„Wysyłaj ostrzeżenia pocztą*”.
Aby wysyłać powiadomienia przy pomocy Windows Messenger należy zaznaczyć opcję *„Wysyłaj ostrzeżenie przy pomocy systemu Windows Messenger*”.



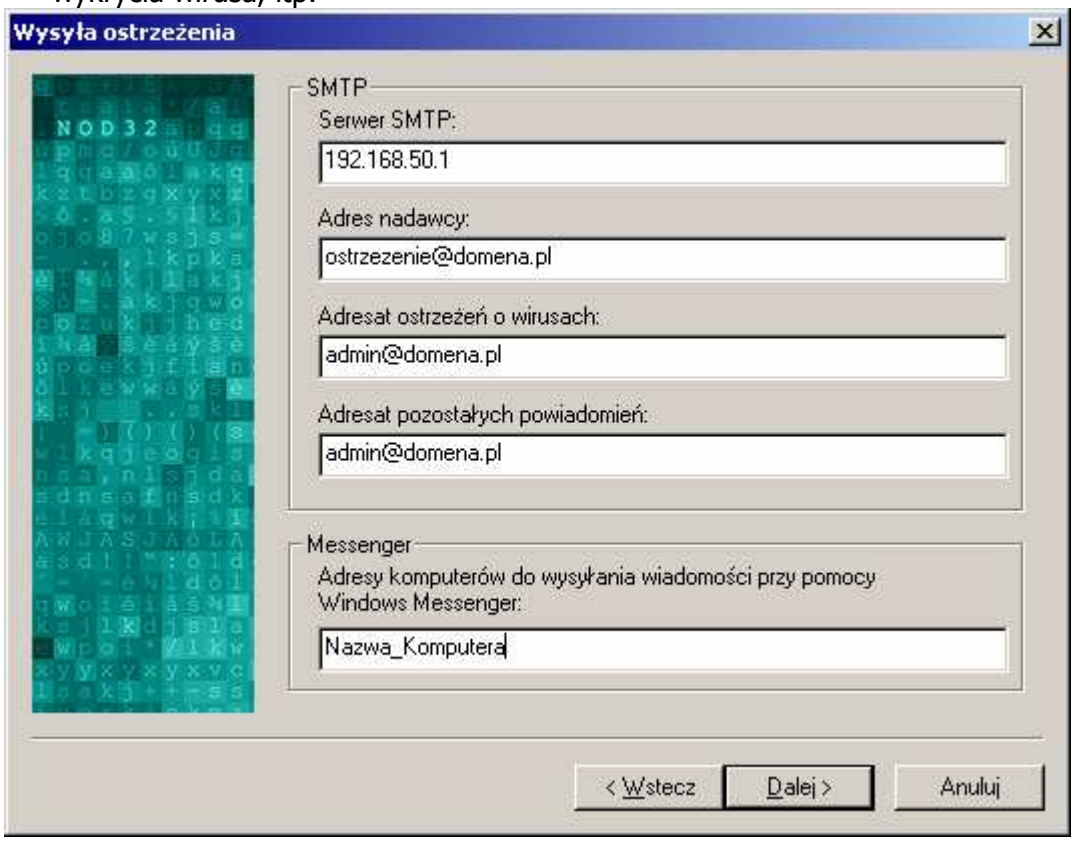
Opcje dostępne w wersji ekspert

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Ustawienia powiadomień

W wyświetlonym oknie należy wpisać odpowiednie informacje tak, aby powiadomienia o wirusach i zdarzeniach były wysyłane na zdefiniowany adres. Wyszczególnione są dwa rodzaje powiadomień, które mogą być wysyłane:
Ostrzeżenia o infekcjach (wirusach)

Powiadomienia o pozostałych zdarzeniach, np. aktualizacja bazy wirusów, wykrycia wirusa, itp.



Opcja dostępna w wersji ekspert

Aby wysłać wiadomość przy pomocy określonego serwera SMTP należy:
Wprowadzić nazwę serwera SMTP
Wprowadzić adres nadawcy wiadomości, np. nod32@domena.pl
Wprowadzić adres odbiorcy (odbiorców) wiadomości z ostrzeżeniem o wirusie, np. admin@domena.pl
Wprowadzić adres odbiorcy (odbiorców) wiadomości z pozostałymi ostrzeżeniami (problem z wykonaniem automatycznej aktualizacji), np. admin@domena.pl

UWAGA: Istnieje możliwość określenia więcej niż jednego adresu odbiorcy. W tym celu należy wprowadzić kolejno adresy oddzielając je znakiem średnika (;).

Aby wysłać wiadomość przy pomocy usługi Windows® Messenger należy wprowadzić adres IP lub nazwę komputera, który będzie otrzymywać wiadomości.

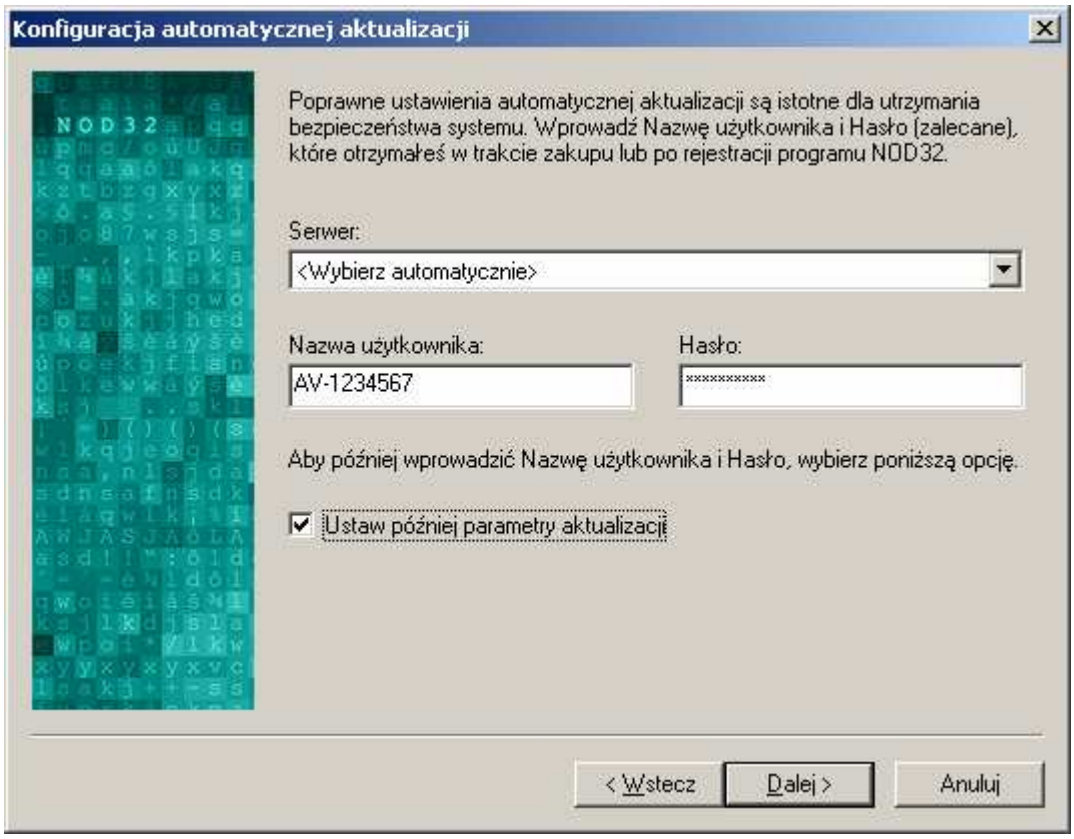
UWAGA: Istnieje możliwość określenia więcej niż jednego komputera. W tym celu należy wprowadzić kolejno nazwy komputerów oddzielając je znakami średnika (;), przecinka (,) lub spacji ( ).
Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Serwer aktualizacyjny, nazwa użytkownika i hasło

Aktualizacja systemu NOD32 może odbywać się w trybie on–line przez Internet, z lokalnej sieci komputerowej, dyskietki lub CD–ROM–u w przypadku wolnostojących stanowisk.

Aktualizacja w trybie on–line odbywa się za pośrednictwem Internetu z jednego z serwerów aktualizacyjnych (niezbędne jest aktywne połączenie z Internetem!), których adresy znajdują się w polu *Serwer*. Domyślnie ustawiona jest opcja Wybierz automatycznie. Oznacza to, że podczas aktualizacji program w pierwszej kolejności próbuje łączyć się z serwerem www.nod32.pl. Jeżeli jest on niedostępny próbuje łączyć się z pozostałymi serwerami znajdującymi się na liście, np. www.nod32.com, itd.

Do aktualizacji niezbędne jest podanie nazwy użytkownika oraz hasła, które znajdują się na Certyfikacie lub zostały dostarczone pocztą elektroniczną po zarejestrowaniu programu.
Należy zwrócić szczególną uwagę na wprowadzane dane, ponieważ użycie małych i dużych liter ma znaczenie. Wpisanie niepoprawnej nazwy użytkownika lub hasła spowoduje brak aktualizacji. Wybór opcji *„Ustaw później parametry aktualizacji"* nie jest zalecany, ponieważ bardzo istotne jest dokonanie aktualizacji natychmiast po zainstalowaniu systemu antywirusowego NOD32.

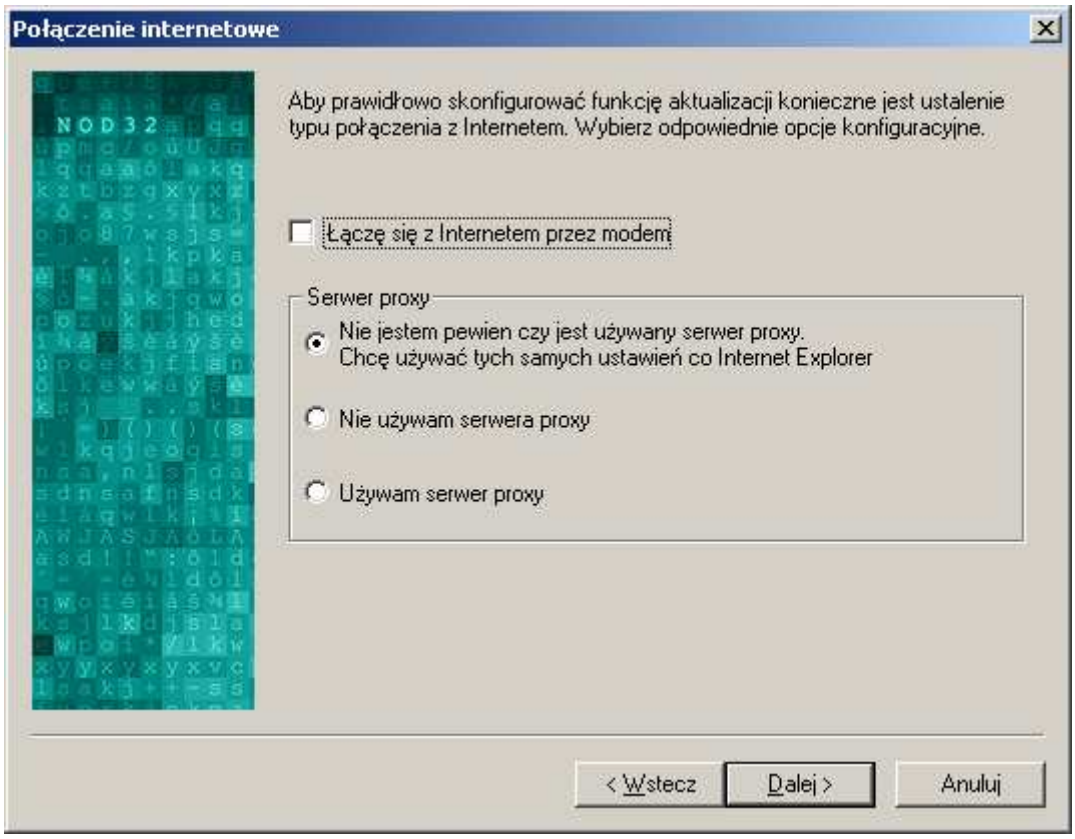


Opcja dostępna we wszystkich wersjach instalacji

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Połączenie z Internetem

Połączenie komputera z Internetem może odbywać się przez modem, sieć lokalną LAN lub za pośrednictwem serwera proxy. Informacje dotyczące serwera proxy są dostarczane przez Dostawcę Usług Internetowych (ISP) lub administratora sieci.



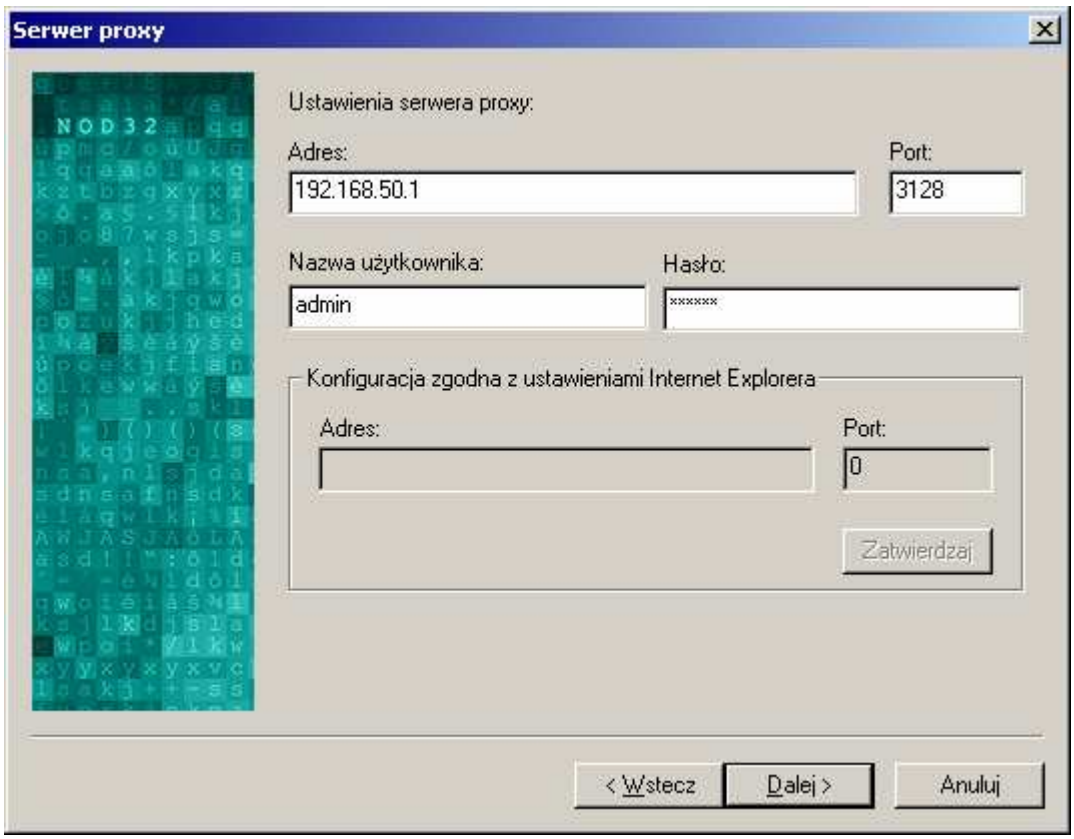
Opcje dostępne we wszystkich wersjach instalacji

Moduł aktualizacji Systemu NOD32 może pobrać ustawienia serwera proxy bezpośrednio z programu Internet Explorer. Czasami jednak jest konieczna ręczna konfiguracja serwera proxy, w tym celu należy zaznaczyć opcję *„Używam serwera proxy".*

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Ustawienia serwera proxy

W wyświetlonym oknie należy wprowadzić nazwę lub adres IP i port serwera proxy oraz wprowadzić nazwę użytkownika i hasło dostępu do serwera proxy.



Opcja dostępna przy konfiguracji połączenia internetowego przez serwer proxy

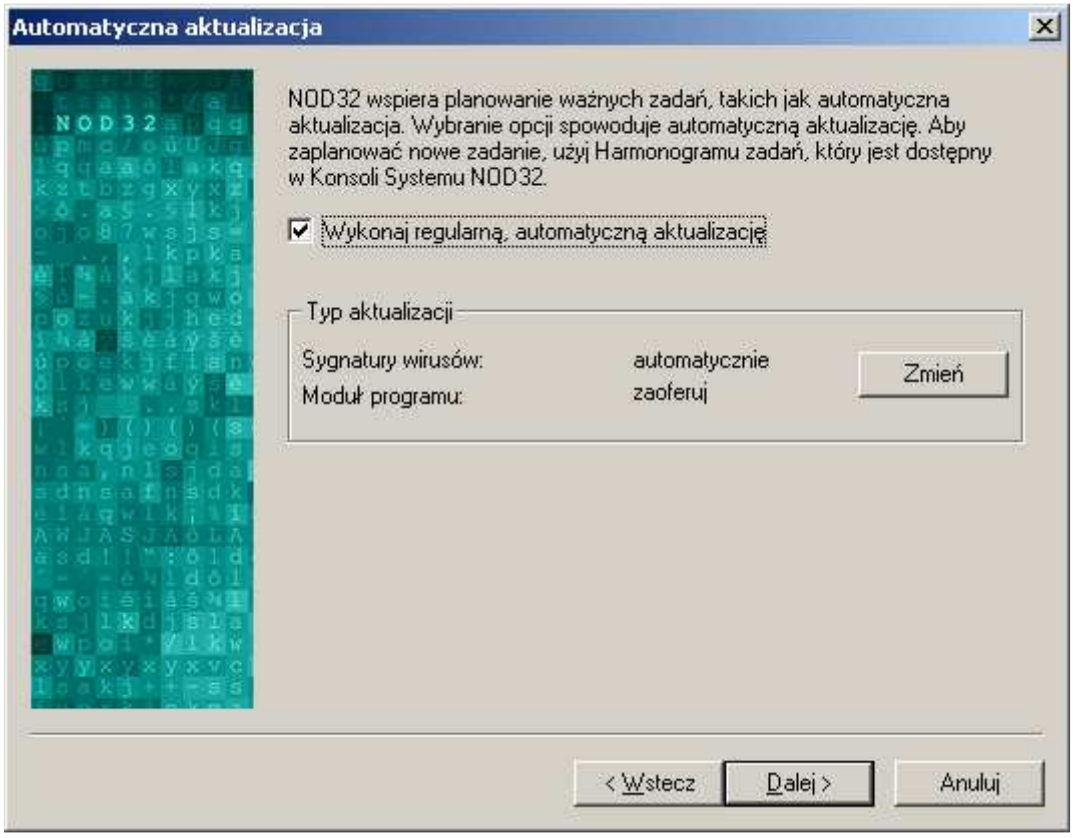
UWAGA: Nazwa użytkownika i hasło dostępu do serwera proxy nie są dostarczane przez Producenta/Dystrybutora Systemu Antywirusowego NOD32. W tym celu proszę skontaktować się z Dostawcę Usług Internetowych (ISP) lub administratorem sieci.

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Automatyczna aktualizacja

System Antywirusowy NOD32 zapewnia automatyczną aktualizację przez Internet wszystkich komponentów, tj. bazy wirusów, komponentów programu.

Aby program automatycznie wykonywał aktualizację należy zaznaczyć opcję „*Wykonaj regularną, automatyczną aktualizację*".

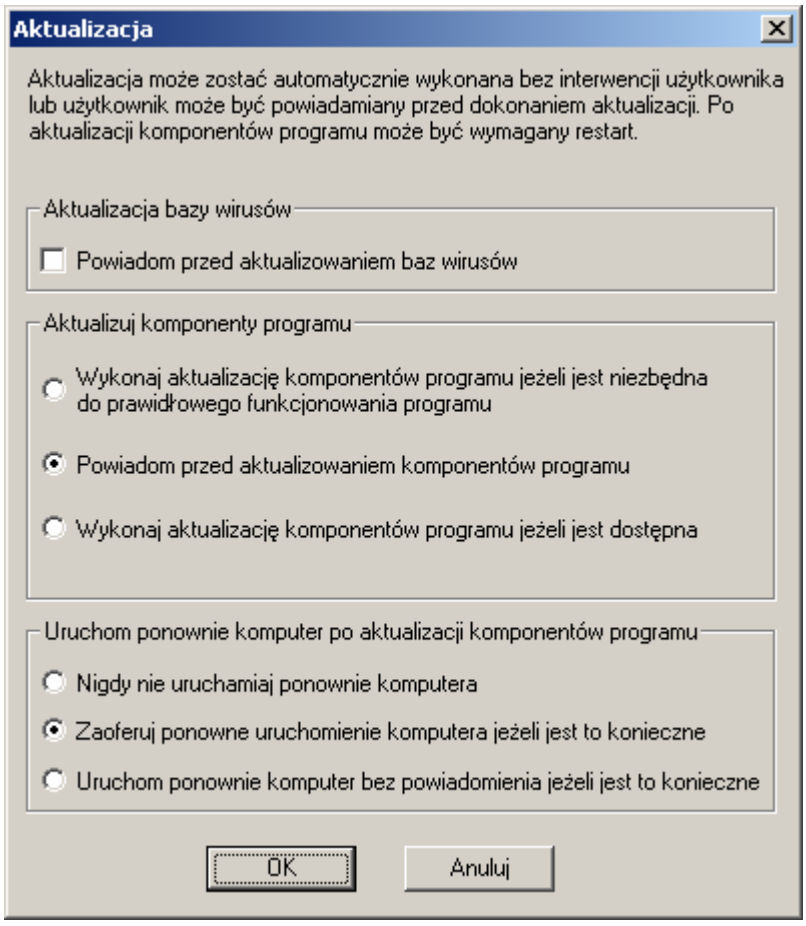


Opcje dostępne w wersjach zaawansowanej i ekspert

Aby zmienić domyślne ustawienia automatycznej aktualizacji należy nacisnąć ***Zmień***.
Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Ustawienia aktualizacji baz wirusów

System Antywirusowy NOD32 wspiera kilka scenariuszy aktualizacji. Dostępne opcje konfiguracji:



Opcje dostępne przy zmianie ustawień automatycznej aktualizacji

„Powiadom przed aktualizowaniem baz wirusów” – jeżeli opcja zostanie zaznaczona, system aktualizacji będzie powiadamiać użytkownika przed każdą aktualizacją baz wirusów. W przypadku gdy opcja nie jest zaznaczona, aktualizacja baz wirusów będzie przebiegać automatycznie.

Obok aktualizacji baz wirusów można również aktualizować komponenty programu:

„Wykonaj aktualizację komponentów programu jeżeli jest niezbędna do prawidłowego funkcjonowania programu” – aktualizacja wykona się automatycznie, tylko w przypadku, gdy jest to konieczne dla zachowania pełnej funkcjonalności programu.

„Powiadom przed aktualizowaniem komponentów programu” – za każdym razem zostanie wyświetlone zapytanie z informacją o dostępnej nowej aktualizacji komponentów.

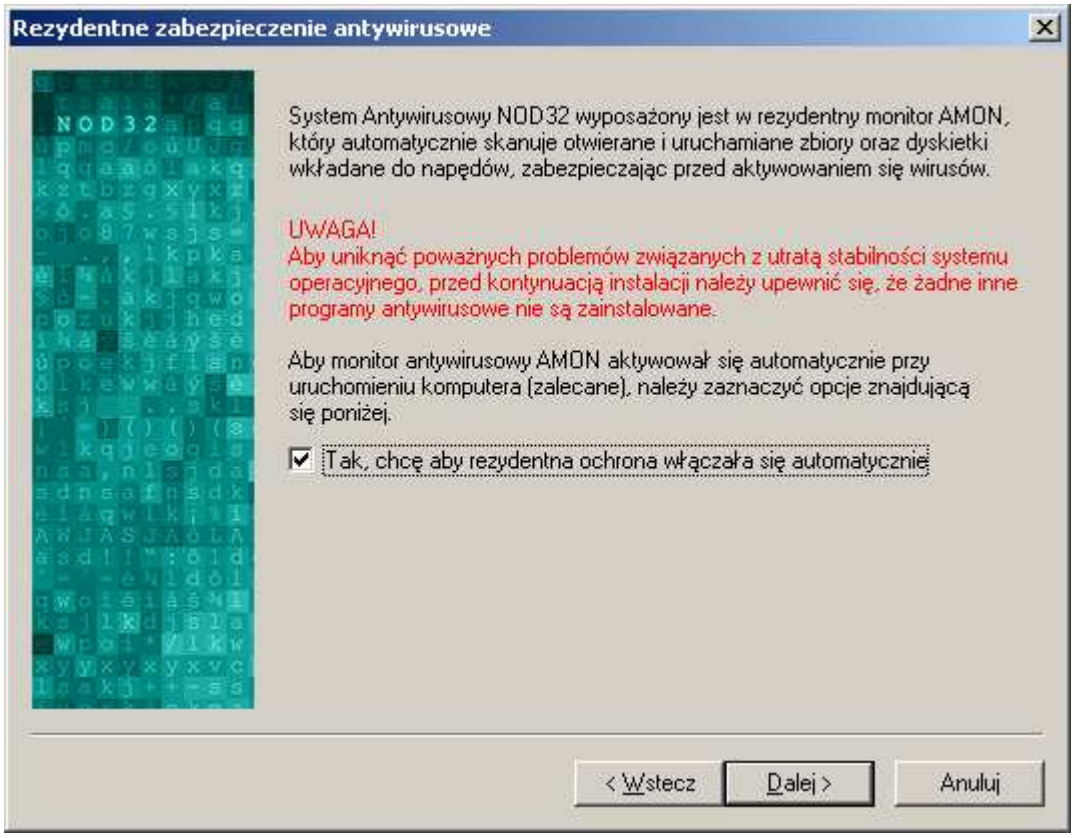
„Wykonaj aktualizację komponentów programu jeżeli jest dostępna” – zapewnia w pełni automatyczną aktualizację komponentów programu.

Aktualizacja baz wirusów odbywa się 'w locie' (nie wymaga ponownego uruchomienia systemu), natomiast w przypadku aktualizacji niektórych komponentów programu może być wymagane ponowne uruchomienie systemu operacyjnego. Istnieje możliwość zdefiniowania opcji automatycznego ponownego uruchomienia systemu w sekcji „*Uruchom ponownie komputer po aktualizacji komponentów programu”*.

Aby zachować zmiany należy nacisnąć ***Ok***. Aby anulować zmiany należy nacisnąć ***Anuluj***.

Rezydentne zabezpieczenie antywirusowe AMON

Rezydentny skaner antywirusowy AMON monitoruje w czasie rzeczywistym wszystkie potencjalnie zagrożone czynności wykonywane zarówno przez system jak i przez użytkownika.
Monitor antywirusowy AMON automatycznie skanuje wszystkie otwierane i uruchamiane pliki znajdujące się zarówno na dyskach lokalnych, sieciowych, jak i napędach dyskietek i CD–ROM, zabezpieczając przed aktywowaniem się wirusów.



Opcja dostępna we wszystkich wersjach instalacji

Zalecane jest automatyczne aktywowanie modułu AMON przy każdym uruchomieniu systemu, dlatego też należy zaznaczyć opcję „*Tak, chcę aby rezydentna ochrona włączała się automatycznie*".

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Dodatkowe możliwości uruchomienia skanera na żądanie NOD32

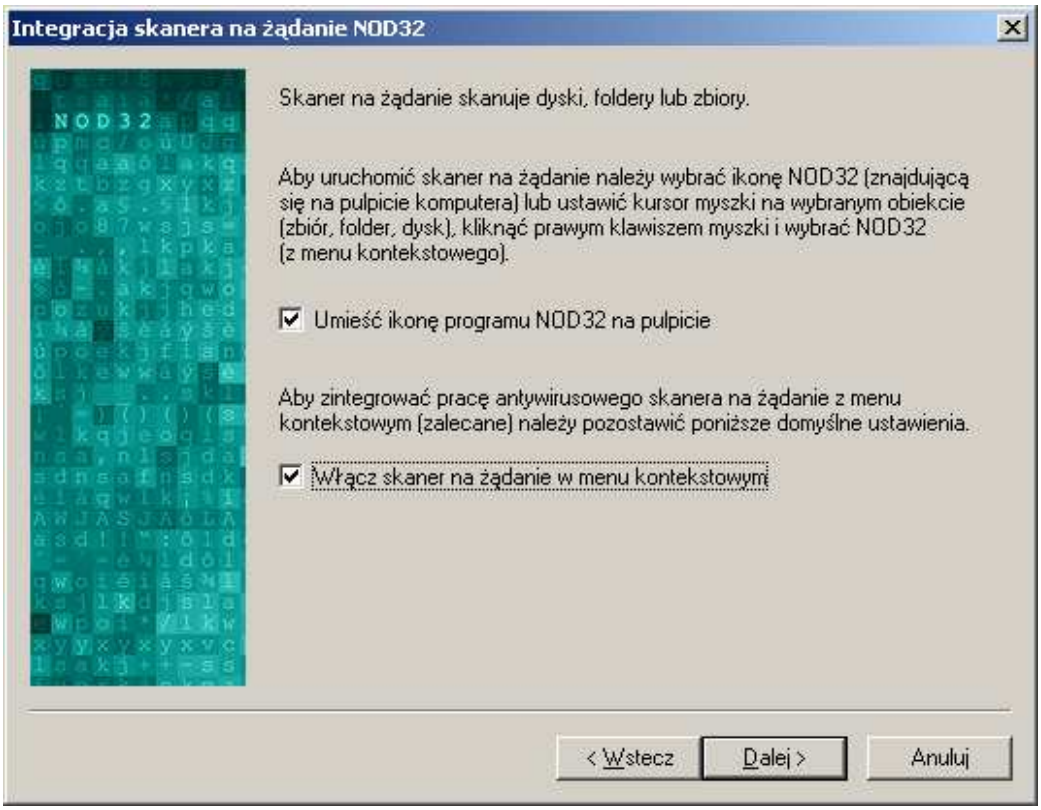
Skaner na żądanie NOD32 można włączyć uruchamiając program znajdujący się w:

- C:\Program Files\Eset\nod32.exe
- Start>Programy>Eset>NOD32

Jednocześnie można tak skonfigurować program NOD32, aby do menu kontekstowego został dołączony skaner na żądanie NOD32, a jego skrót  umieszczony na pulpicie.

Aby umieścić skrót do programu NOD32 na pulpicie zaznacz opcję „*Umieść ikonę programu NOD32 na pulpicie*".

Aby dołączyć skaner na żądanie NOD32 do menu kontekstowego należy zaznaczyć opcję „*Włącz skaner na żądanie w menu kontekstowym*".



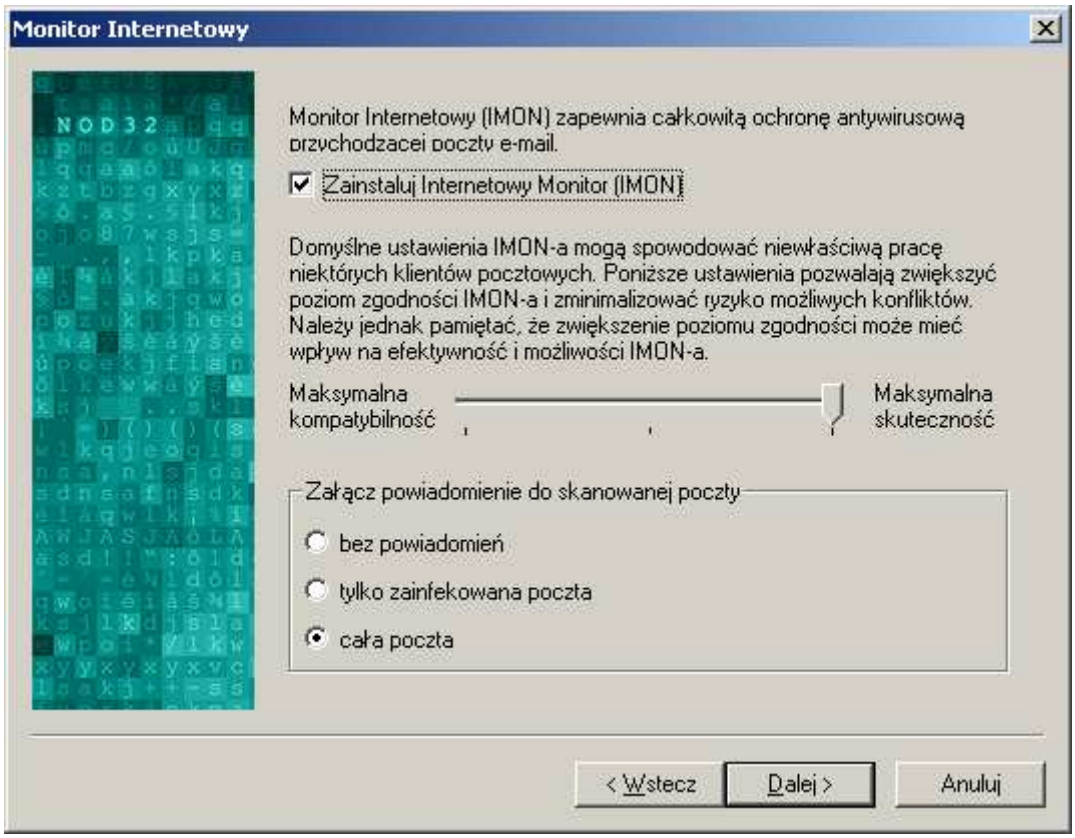
Opcje dostępne w wersjach zaawansowanej i ekspert

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Monitor Internetowy

Kolejnym etapem instalacji jest aktywowanie/deaktywowanie Monitora Internetowego IMON. Zapewnia on całkowitą ochronę antywirusową poczty elektronicznej pobieranej z serwera przy pomocy protokołu POP3, bez względu na klienta pocztowego.

Aby włączyć skanowanie poczty przychodzącej przez Monitor Internetowy IMON należy zaznaczyć opcję „*Zainstaluj Internetowy Monitor (IMON)*".



Opcje dostępne w wersjach zaawansowanej i ekspert

Domyślnie IMON ustawiony jest na maksymalną skuteczność skanera. Ustawienia skanera IMON pozwalają zwiększyć poziom zgodności modułu IMON i zminimalizować ryzyko możliwych konfliktów. Należy jednak pamiętać, że zwiększenie poziomu zgodności może mieć wpływ na efektywność i możliwości modułu IMON.

Powiadomienia w skanowanej poczcie

Do każdej przeskanowanej wiadomości może zostać dołączone powiadomienie o wyniku skanowania.

Aby żadne powiadomienie nie było dołączane do wiadomości należy zaznaczyć opcję *„bez powiadomień”*.

Aby do zainfekowanej wiadomości było dołączane powiadomienie należy zaznaczyć opcję *„tylko zainfekowana poczta”*. Wtedy do każdej zainfekowanej poczty zostanie dołączone powiadomienie w postaci:

```
__________ NOD32 1.517 (20030924) Powiadomienie__________
Ostrzeżenie: System Antywirusowy NOD32 wykrył następującą
infekcję w tej wiadomości:
 eicar.com – Eicar plik testowy
http://www.nod32.pl
```

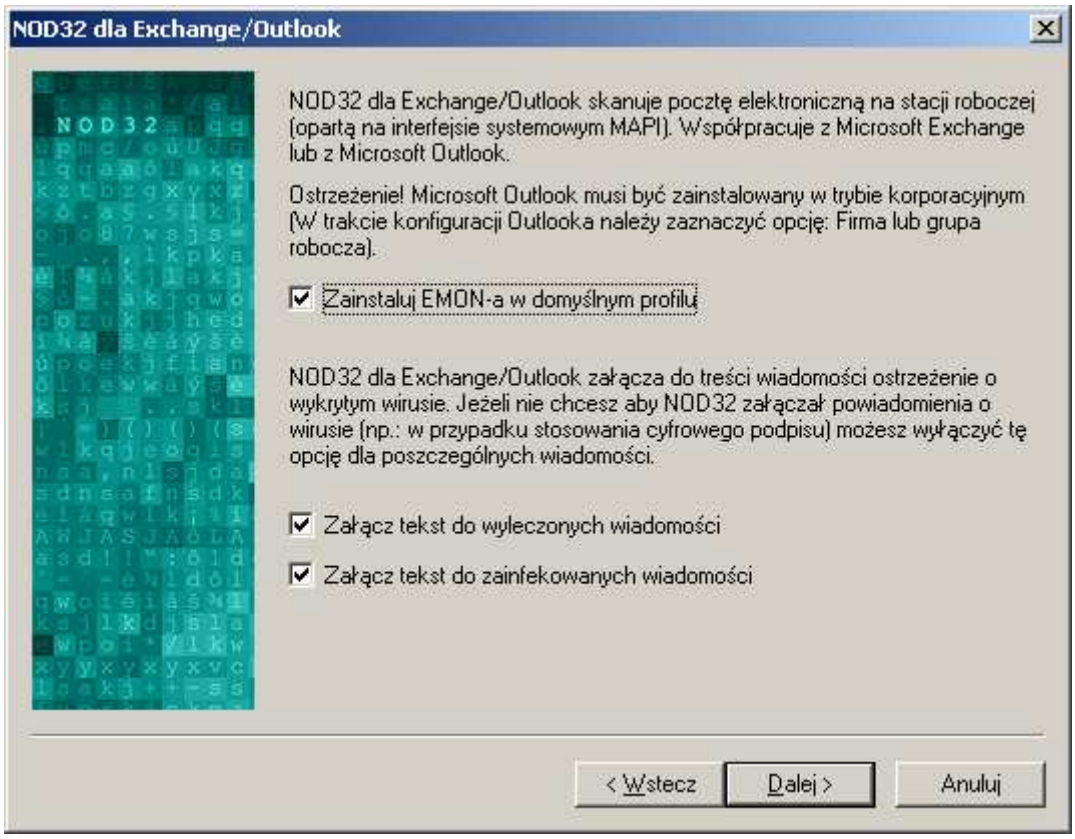
Aby do każdej wiadomości było dołączane powiadomienie należy zaznaczyć opcję *„cała poczta”*. Wtedy do każdej wiadomości zostanie dołączone powiadomienie w postaci:

```
__________ NOD32 Informacje 1.517 (20030924) __________
Wiadomość została sprawdzona przez System Antywirusowy NOD32
http://www.nod32.com lub http://www.nod32.pl
```

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Ochrona poczty Microsoft Outlook

Skaner EMON dla klientów Microsoft Outlook skanuje całą pocztę przychodzącą i wychodzącą odbieraną przy pomocy programu Microsoft Outlook.



Opcje dostępne w wersjach zaawansowanej i ekspert

Powiadomienia w skanowanej poczcie

Skaner poczty Microsoft Outlook może dołączać do treści wiadomości ostrzeżenie o wykrytym wirusie oraz o wyniku skanowania.

Aby do każdej zainfekowanej wiadomości było dołączane powiadomienie należy zaznaczyć opcję *„Załącz tekst do zainfekowanych wiadomości"*. Wtedy do każdej zainfekowanej wiadomości zostanie dołączone powiadomienie postaci:

```
__________ NOD32 1.517 (20030924) Powiadomienie__________
Ostrzeżenie: System Antywirusowy NOD32 wykrył następującą
infekcję w tej wiadomości:
 eicar.com – Eicar plik testowy
http://www.nod32.pl
```

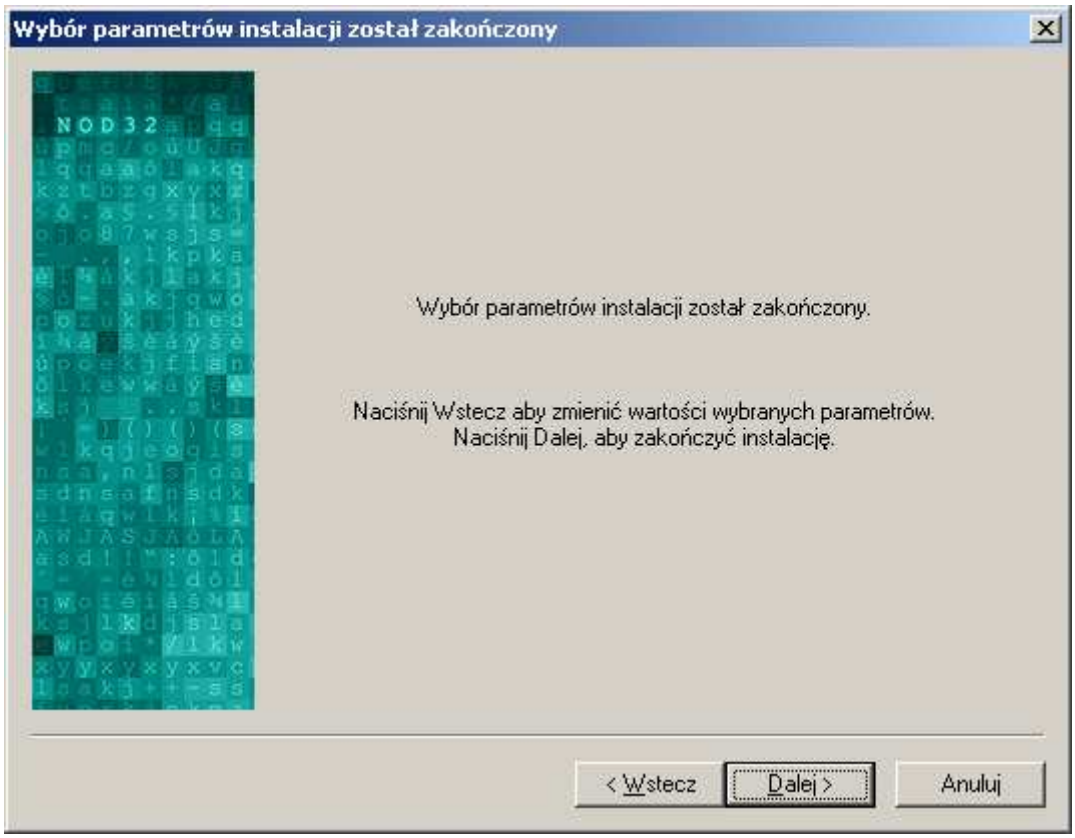
Aby do każdej wyleczonej wiadomości było dołączane powiadomienie należy zaznaczyć opcję *„Załącz tekst do wyleczonych wiadomości*". Wtedy do każdej wyleczonej wiadomości zostanie dołączone powiadomienie postaci:

```
__________ NOD32 1.517 (20030924) Powiadomienie__________
Ostrzeżenie: System Antywirusowy NOD32 wykrył następującą
infekcję w tej wiadomości:
 eicar.com – Eicar plik testowy – usuniety
http://www.nod32.pl
```

Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby kontynuować instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

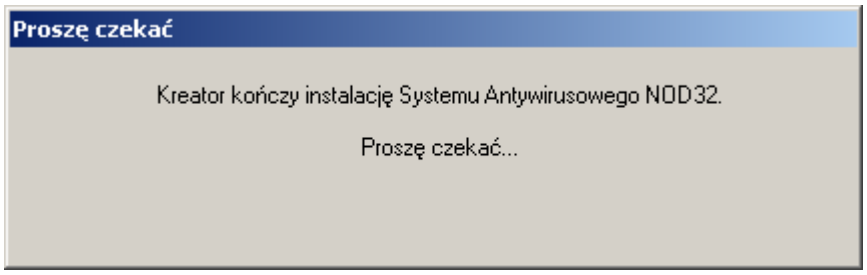
Zakończenie instalacji

Po ustawieniu wszystkich parametrów kreator instalacji zakończy swoje działanie.

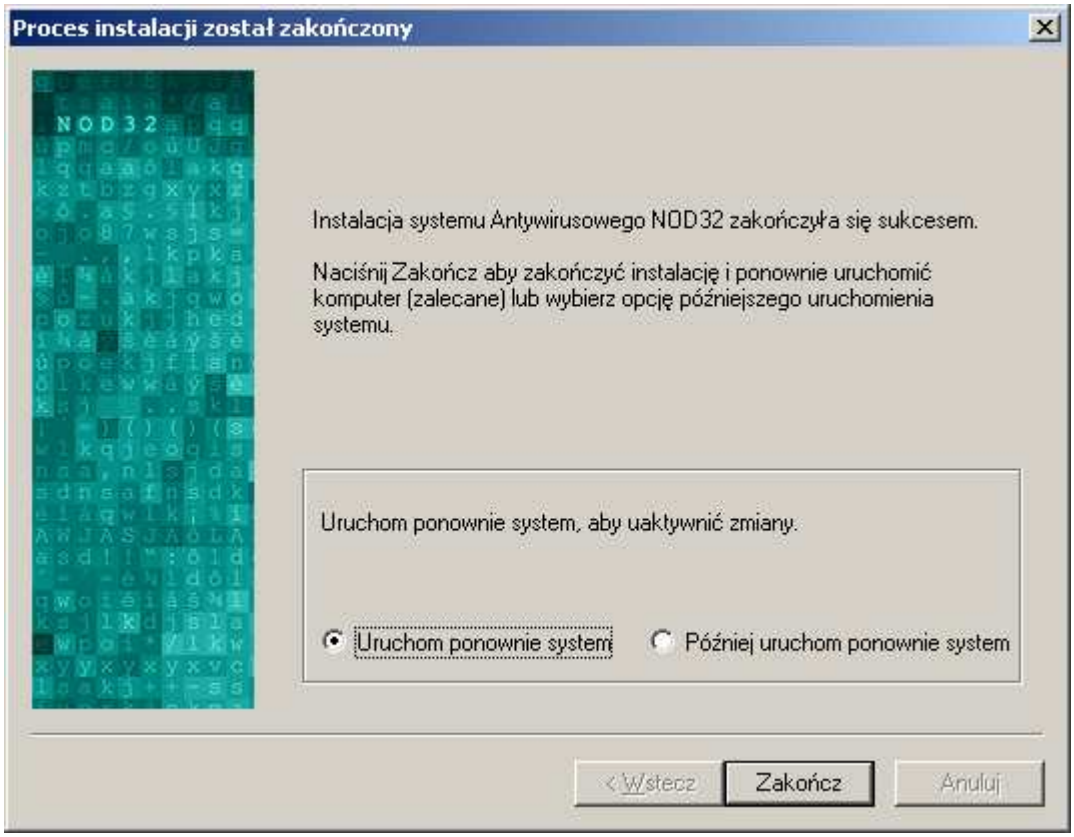


Aby zmienić wartości wcześniej wybranych parametrów należy nacisnąć ***Wstecz***. Aby zakończyć instalację należy nacisnąć ***Dalej***. Aby anulować instalację należy nacisnąć ***Anuluj***.

Następnie pojawi się okno informujące o zakończeniu instalacji systemu antywirusowego NOD32.



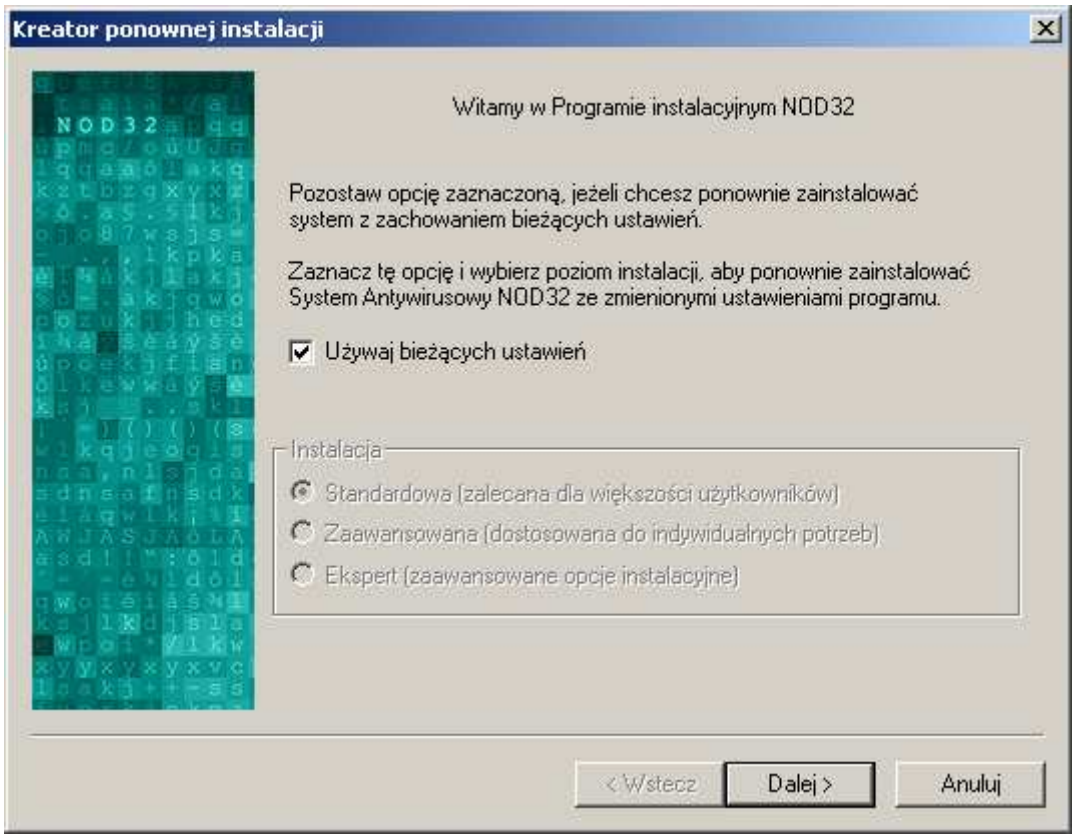
Jeżeli instalacja programu NOD32 została zakończona sukcesem należy ponownie uruchomić system.



Aby zakończyć instalację i ponownie uruchomić komputer należy zaznaczyć opcję „*Uruchom ponownie system*" i nacisnąć ***Zakończ***. Aby zakończyć instalację i później uruchomić system należy zaznaczyć opcję „*Później uruchom ponownie system*" i nacisnąć ***Zakończ***.

Reinstalacja Systemu Antywirusowego NOD32

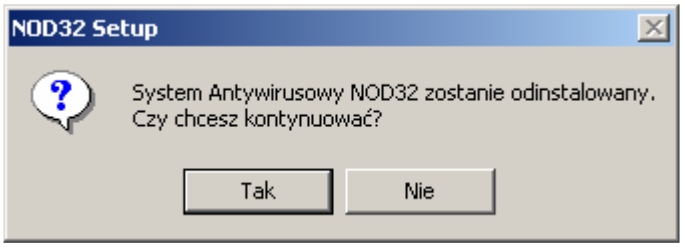
W przypadku wykrycia starszych wersji instalacja programu polega na zastąpieniu starej wersji nową z zachowaniem dotychczasowej konfiguracji.



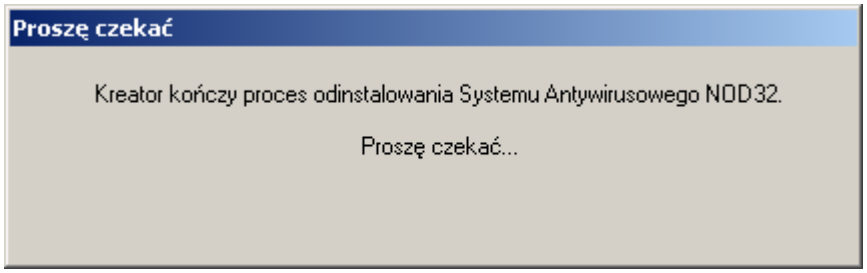
Deinstalacja Systemu Antywirusowego NOD32

Aby odinstalować System Antywirusowy NOD32 należy uruchomić deinstalację z:
Start > Programy > Eset > Deinstalacja
Start > Ustawienia > Panel Sterowania > Dodaj/ Usuń programy > System Antywirusowy NOD32

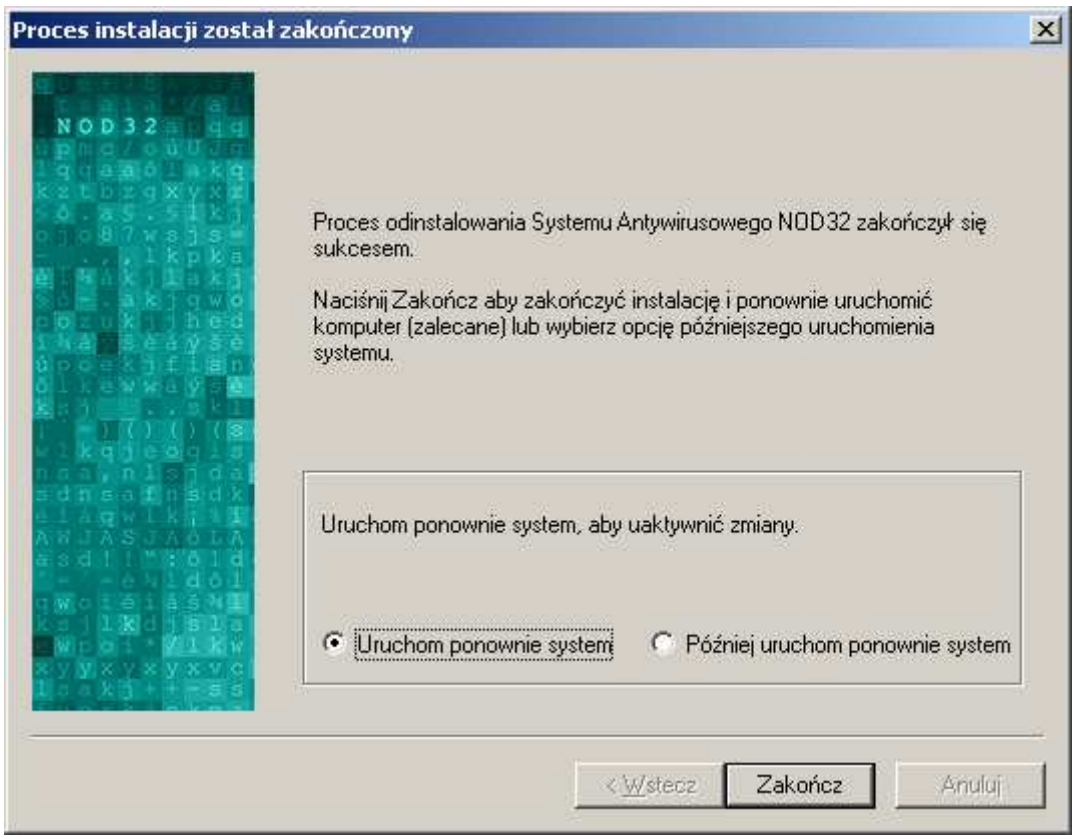
Pojawi się okno informujące o deinstalacji Systemu Antywirusowego NOD32. Jeżeli program ma zostać odinstalowany z systemu należy zaznaczyć ***Tak***, w przeciwnym przypadku należy zaznaczyć ***Nie***.



Po zatwierdzeniu deinstalacji programu NOD32 pojawi się okno informujące o procesie odinstalowania Systemu Antywirusowego NOD32.



Po zakończonym procesie deinstalacji należy uruchomić ponownie system.



Aby zakończyć deinstalację i ponownie uruchomić komputer należy zaznaczyć opcję „*Uruchom ponownie system*" i nacisnąć ***Zakończ***. Aby zakończyć deinstalację i później uruchomić system należy zaznaczyć opcję „*Później uruchom ponownie system*" i nacisnąć ***Zakończ***.

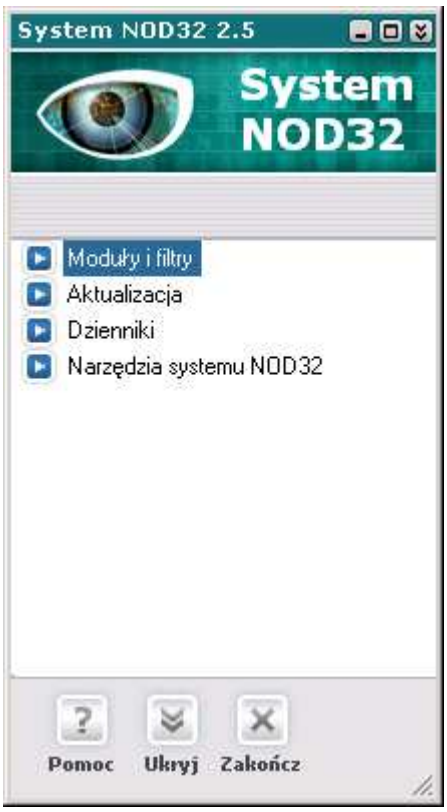
System NOD32

Po zainstalowaniu programu należy sprawdzić czy na pasku zadań – w prawym dolnym rogu ekranu (obok zegara systemowego) – pojawiła się ikona programu NOD32.

Kliknięcie myszą na ikonie otwiera konsolę **Systemu NOD32** pozwalającą na konfigurację opcji programu i wszystkich modułów programu NOD32

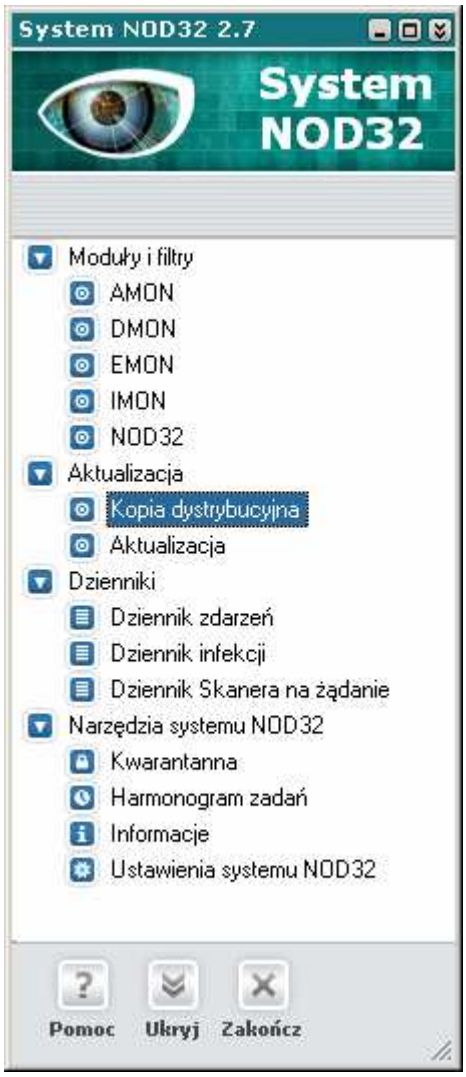
UWAGA: Pierwszą czynnością, którą należy wykonać po zainstalowaniu programu jest pobranie z Internetu najnowszej bazy wirusów i komponentów programu.
Jest to niezbędne, aby zapewnić ochronę przed nowymi wirusami. Informacje dotyczące aktualizacji systemu NOD32 można znaleźć w rozdziale „Aktualizacja”.

Kolejnym krokiem po aktualizacji jest przeskanowanie zasobów komputera programem antywirusowym NOD32 (więcej informacji o tym jak skanować zasoby komputera znajduje się w rozdziale „Skaner na żądanie NOD32").



Menu **Systemu NOD32** podzielone jest na cztery grupy:
Moduły i filtry
Aktualizacja
Dzienniki
Narzędzia systemu NOD32

Aby przechodzić między grupami w oknie konsoli należy użyć myszki lub klawiszy strzałek (góra/dół), każdą z grup można rozwinąć klikając na ikonę z lewej strony nazwy grupy lub przy pomocy klawisza: „strzałka w prawo".



W grupach umieszczone są komponenty programu. Po lewej stronie każdego z nich znajduje się ikona. Kolor niebieski oznacza normalne funkcjonowanie, kolor czerwony lub szary informuje nas, że dany moduł jest wyłączony lub nie został załadowany do pamięci komputera.

Poniżej znajdują się skrócone informacje dotyczące poszczególnych grup. Pełny opis znajduje się w dalszej części podręcznika.

Moduły i filtry

Rezydentne moduły i filtry usuwają istniejące wirusy i chronią przed nowymi infekcjami komputera.

AMON – monitor rezydentny, sprawdza na bieżąco wszystkie pliki

IMON – monitor internetowy – sprawdza przychodzącą pocztę (protokół POP3) i otwierane strony HTTP

EMON – Skaner poczty Microsoft Outlook

DMON – skaner dokumentów Microsoft Office

NOD32 – skaner na żądanie (sprawdza wybrane dyski/foldery)

Aktualizacja

- **Aktualizacja** – zapewnia konfigurację i automatyczną aktualizację baz wirusów i komponentów Systemu Antywirusowego NOD32.
- **Kopia dystrybucyjna** – moduł ten dostępny jest tylko w wersji administracyjnej dostarczanej w pakiecie dla sieci korporacyjnych. Moduł ten jest odpowiedzialny za generowanie i aktualizację kopii plików aktualizacyjnych dystrybuowanych w sieci lokalnej.

Dzienniki

Zawiera dokładne informacje dotyczące pracy modułów Systemu NOD32 (aktualizacja, AMON, IMON, EMON, DMON skaner na żądanie itp.). Wszystkie ważne wydarzenia i błędy są zapisywane w osobnych dziennikach zdarzeń. Dostępne są trzy odrębne dzienniki:

- **Dziennik zdarzeń**
- **Dziennik infekcji**
- **Dziennik Skanera na żądanie**

Narzędzia systemu NOD32

W tej grupie można znaleźć narzędzia i moduły służące do zarządzania folderem kwarantanny, Harmonogram zadań, informacje o systemie antywirusowym i systemie operacyjnym, narzędzia do konfigurowania wyglądu programu NOD32, zabezpieczenia hasłem, powiadomienia i zarządzanie dziennikami.

Kwarantanna – zarządzanie folderem kwarantanny

Harmonogram zadań – zarządzanie i planowanie zadań wykonywanych automatycznie

Informacje – zawiera informacje o wersji zainstalowanego programu i bazy wirusów oraz informacje o systemie operacyjnym

Ustawienia systemu NOD32 – ustawienia hasła, wyglądu zewnętrznego, powiadomień, zarządzanie dziennikami i inne opcje.

Przyciski

Trzy przyciski umieszczone w dolnej części głównego okna konsoli Systemu NOD32 służą do uzyskania pomocy, ukrywania okna konsoli na pasku zadań oraz do zamknięcia Systemu NOD32 (nie zalecane).

Pomoc – wywołuje system pomocy Systemu NOD32.

Ukryj – standardowy sposób zamykania konsoli – okno programu zostaje zamknięte (schowane), powiadomienia będą wysyłane (jeśli ta funkcja została skonfigurowana).

Zakończ – tej opcji proszę nie używać (z wyjątkiem sytuacji awaryjnych), gdyż ogranicza funkcjonalność systemu antywirusowego – wymusza zamknięcie aplikacji, ikona programu znika z paska zadań, nie będą pojawiały się żadne komunikaty o wirusach, zostanie wyłączone wysyłanie wiadomości/powiadomień, itp.

Moduły i filtry

AMON – rezydentny monitor antywirusowy

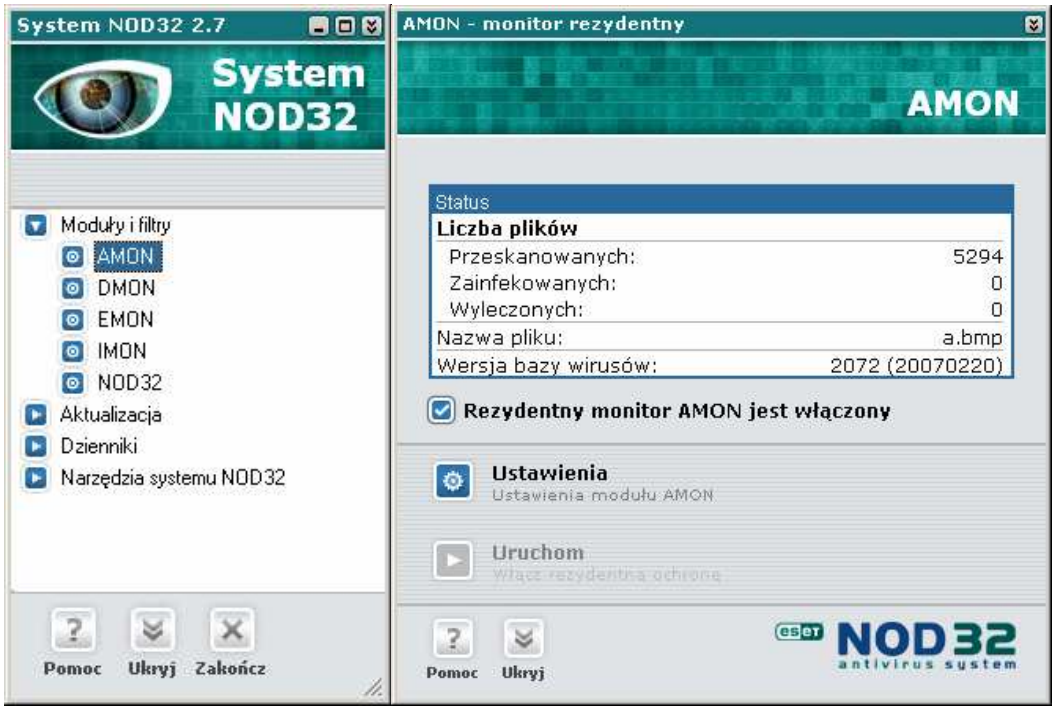
AMON (Antywirusowy MONitor) – rezydujący w pamięci komputera moduł – jest najważniejszym elementem ochrony antywirusowej. AMON monitoruje czynności wykonywane podczas pracy na plikach, tj: otwieranie, tworzenie, wykonywanie i zmiana nazwy plików. Automatycznie wykrywa i usuwa lub neutralizuje rezydujące w plikach wirusy. Zalecane jest automatyczne włączanie modułu AMON w trakcie uruchamiania komputera. Opcja ta może być wybrana w trakcie procesu instalacji lub później, w oknie konfiguracyjnym monitora AMON (zakładka Zabezpieczenia).

AMON określany jest często jako monitor antywirusowy lub skaner plików w czasie rzeczywistym (real–time, on–access scanner). Działa automatycznie – na bieżąco sprawdzając te pliki, które są używane. Należy odróżnić go od skanera na żądanie (on–demand scanner), którego używa się do sprawdzenia wybranego dysku lub folderu.

AMON musi być kompatybilny z systemem operacyjnym zainstalowanym na komputerze i wymaga posiadania ważnych uprawnień systemowych (pracuje na poziomie sterowników systemu). Kompatybilność z innymi usługami zainstalowanymi na komputerze jest sprawdzana podczas instalacji systemu antywirusowego NOD32. Jeśli testy zakończyły się sukcesem AMON jest uruchamiany automatycznie po każdym włączeniu komputera.

UWAGA: Używanie dwóch lub więcej monitorów antywirusowych może spowodować poważne problemy w pracy systemu operacyjnego a nawet brak możliwości uruchomienia (zwłaszcza w przypadku systemów Windows

NT/2000/XP/2003/Vista). Istnieje możliwość zainstalowania dwóch (lub więcej) systemów antywirusowych na komputerze, ale tylko jeden rezydentny monitor antywirusowy może być uruchomiony w danym momencie.



Należy pamiętać, że aby AMON spełniał swoją funkcję, musi być **uruchomiony** (załadowany do pamięci) i **włączony** (aktywny). AMON może znajdować się w trzech stanach (każdy z nich oznaczony jest w Konsoli Systemu innym kolorem ikony umieszczonej obok modułu AMON):

- Uruchomiony i włączony (moduł działa, jest załadowany do pamięci i wykonuje skanowanie w tle), ikona modułu AMON jest niebieska. AMON
- Uruchomiony i wyłączony (załadowany do pamięci, ale nie wykonuje skanowania w tle), ikona modułu AMON jest czerwona. AMON
- Zatrzymany i wyłączony (nie załadowany do pamięci), ikona modułu AMON jest szara. AMON

Stany 2 i 3 – (wyłączony AMON) nie są zalecane, ponieważ oznacza to, że nie jest aktywna żadna rezydentna ochrona antywirusowa plików na komputerze.

Aby uruchomić monitor AMON należy wykonać następujące czynności:

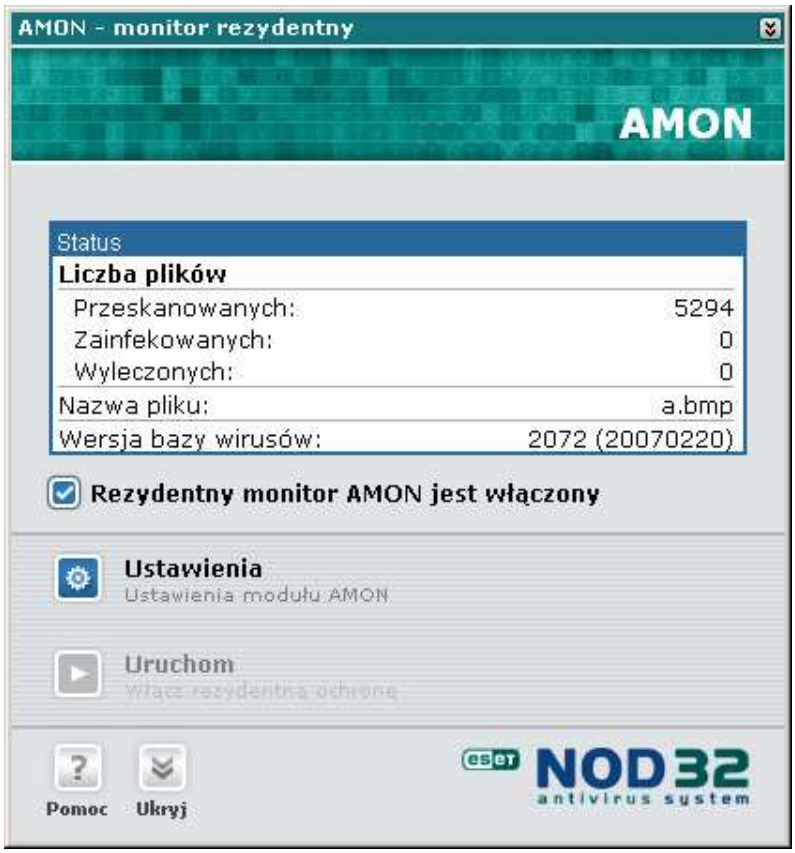
Jeśli jest w stanie 3 (szara ikona), należy kliknąć na jego ikonę w Konsoli Systemu co spowoduje otwarcie okna modułu AMON. Następnie nacisnąć przycisk ***Uruchom*** umieszczony w dolnej części okna modułu AMON. Spowoduje to przejście do stanu 2. Aby przełączyć go w stan 1, należy wykonać podane poniżej operacje.

Jeśli AMON jest w stanie 2 (czerwona ikona) – AMON jest załadowany do pamięci ale skanowanie jest wyłączone (stan nie zalecany). Aby to zmienić należy w oknie modułu AMON zaznaczyć opcję *„Rezydentny monitor (AMON) jest włączony"*. Czynność ta spowoduje przełączenie modułu AMON do aktywnego (zalecanego) stanu (ikona niebieska).

Aby sprawdzić pracę modułu AMON, należy zwrócić uwagę na górną część okna zawierającą informację o liczbie przeskanowanych plików (*„Liczba plików przeskanowanych:*"). Proszę ją zapamiętać, a następnie uruchomić i wyłączyć jakąś aplikacje lub otworzyć i zamknąć jakiś dokument. Jeśli AMON jest uruchomiony właściwie, nowa wartość parametru (przeskanowane pliki) zwiększy się.

Opis okna modułu AMON

Aby otworzyć okno modułu AMON należy kliknąć na jego ikonę w głównym oknie Systemu NOD32.



W głównym oknie modułu AMON widoczne są statystyki zawierające informacje o łącznej liczbie przeskanowanych, zainfekowanych i wyleczonych plików. Dostępna jest również nazwa ostatnio lub obecnie skanowanego pliku oraz informacje o zainstalowanej wersji bazy wirusów z datą wydania, która jest przedstawiona w następującym formacie: YYYYMMDD, czyli czterocyfrowy rok, dwucyfrowy miesiąc i dwucyfrowy dzień miesiąca.

Opcja „*Rezydentny monitor (AMON) jest włączony*" pozwala na włączenie lub zatrzymanie głównej funkcji modułu AMON: rezydentnego skanowania. Opcja ta jest dostępna (ikona jest koloru niebieskiego, a nie szarego) tylko w przypadku, gdy AMON jest załadowany do pamięci operacyjnej. Jeśli AMON nie jest załadowany należy to zrobić klikając przycisk ***Uruchom*** w dolnej części okna. Wyładowanie monitora AMON z pamięci możliwe jest przez naciśnięcie przycisku ***Zatrzymaj*** (pojawia się zamiast przycisku ***Uruchom***, w tym samym miejscu).

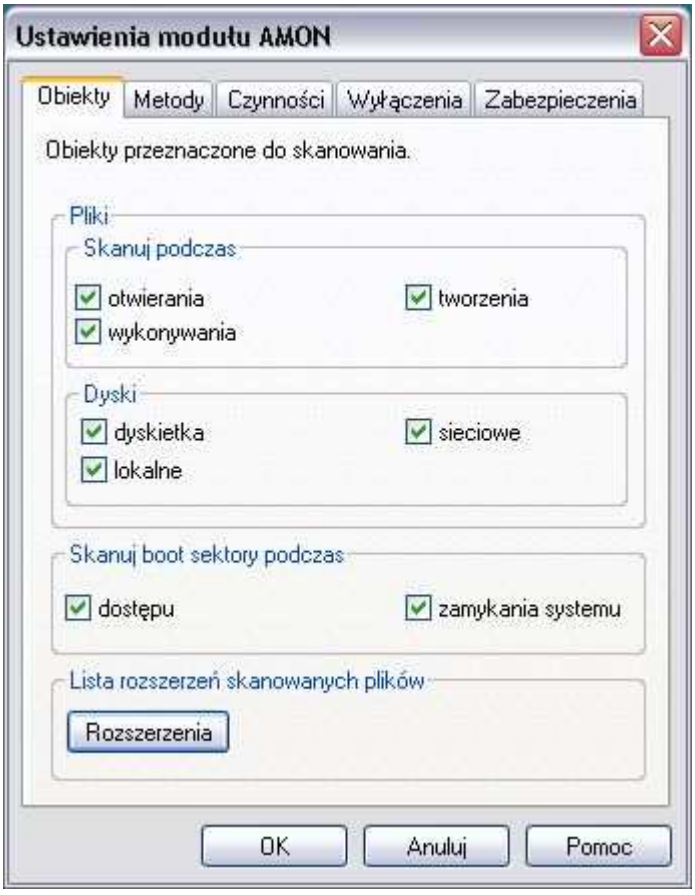
Kliknięcie na przycisk ***Ustawienia*** w głównym oknie modułu AMON otwiera okno pozwalające na konfigurację parametrów modułu AMON.

Ustawienia modułu AMON

Rezydentny skaner antywirusowy AMON monitoruje w czasie rzeczywistym wszystkie potencjalnie zagrożone czynności wykonywane zarówno przez system jak i przez użytkownika. Nie jest zalecane modyfikowanie domyślnych ustawień bez pełnej świadomości tego, co zostaje zmienione, ponieważ może to spowodować osłabienie ochrony antywirusowej i doprowadzić do infekcji systemu!

Dostępnych jest pięć zakładek konfiguracyjnych: Obiekty, Metody, Czynności, Wyłączenia i Zabezpieczenia.

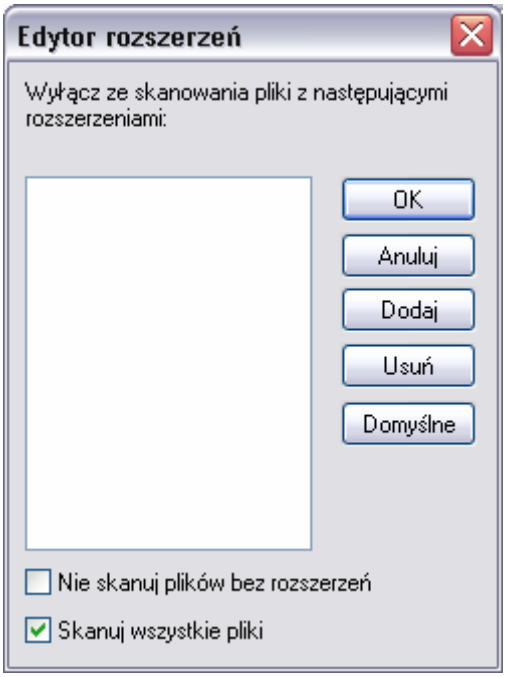
Obiekty



W domyślnej konfiguracji AMON skanuje pliki podczas otwierania, wykonywania (uruchamiania) i tworzenia.

Obiekty skanowane przez monitor antywirusowy to: d*yskietki* oraz d*yski Lokalne* i s*ieciowe*.
AMON skanuje także boot sektory dyskietek podczas dostępu do dyskietki i przy zamykaniu systemu. Ta ostatnia opcja jest szczególnie ważna, ponieważ jeśli w napędzie (podczas zamykania systemu) pozostała dyskietka z zainfekowanym sektorem rozruchowym (wirus boot sektorowy), wyłączenie tej opcji może doprowadzić do infekcji komputera w trakcie następnego uruchomienia.

Aby uruchomić Edytor rozszerzeń, pozwalający na edycję listy rozszerzeń plików przeznaczonych do skanowania (przez moduł AMON) należy kliknąć na przycisk ***Rozszerzenia***.



Edytor rozszerzeń jest specjalną funkcją, przeznaczoną dla zaawansowanych użytkowników. Lista rozszerzeń plików przeznaczonych do skanowania przez Monitor Antywirusowy (AMON) jest definiowana domyślnie (optymalizacja bezpieczeństwa i efektywności). Jeżeli w wyniku nowego zagrożenia istnieje konieczność uzupełnienia listy lub modyfikacji istniejących rozszerzeń, niezbędne zmiany są uwzględniane automatycznie w bieżącej aktualizacji programu.

UWAGA: Usunięcie jakiegokolwiek rozszerzenia z listy rozszerzeń może doprowadzić do infekcji systemu!

Lista rozszerzeń

Lista rozszerzeń plików przeznaczonych do skanowania jest przedstawiona w głównej części okna. Nawigacja listy odbywa się przy użyciu paska przewijania umieszczonego po prawej stronie okna. Aby podświetlić rozszerzenie należy kliknąć na nim kursorem myszki.

Przyciski:

OK – modyfikacja listy rozszerzeń zostaje zatwierdzona.

Anuluj – przycisk anuluje zmiany i zamyka okno.

Dodaj – aby dodać rozszerzenie należy nacisnąć przycisk ***Dodaj***, wypełnić pole dialogowe i zatwierdzić dwa razy przyciskami ***OK***.

Usuń – aby usunąć dowolne rozszerzenie (operacja może spowodować osłabienie ochrony antywirusowej) należy podświetlić wybrane rozszerzenie oraz nacisnąć przyciski ***Usuń*** i ***OK***

Domyślne – aby przywrócić domyślne ustawienia rozszerzeń (zalecane) należy nacisnąć przycisk ***Domyślne***, a następnie ***OK***.

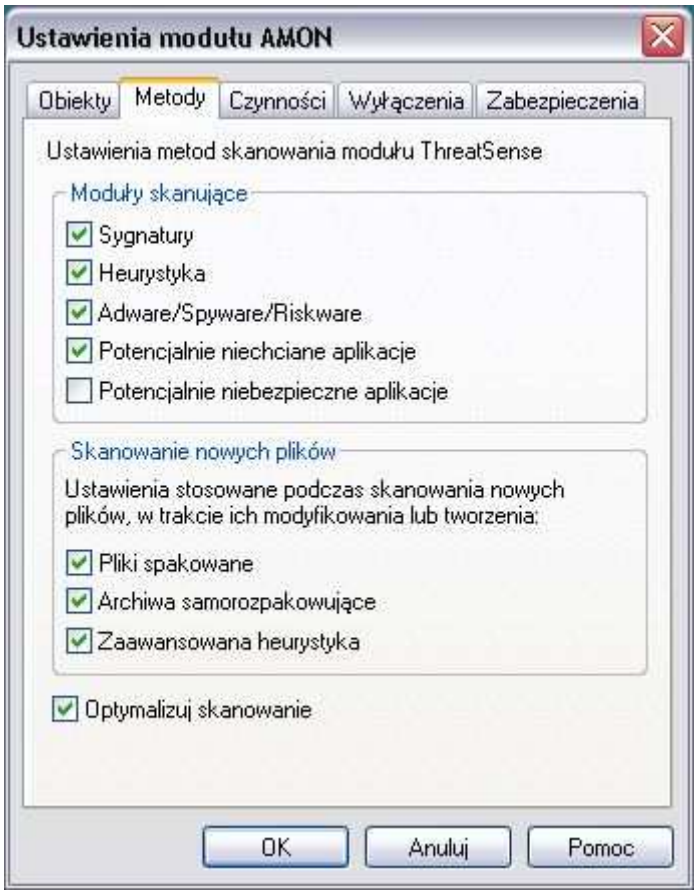
Edytor rozszerzeń pozwala również na szybkie wybranie opcji skanowania wszystkich plików lub plików bez rozszerzeń.

Dodatkowe opcje:

„Skanuj pliki bez rozszerzeń” – opcja ta powoduje skanowanie plików bez rozszerzeń.

„Skanuj wszystkie pliki" – gdy ta opcja będzie zaznaczona to domyślnie wszystkie pliki będą skanowane, natomiast edytor rozszerzeń zmienia swoje właściwości: w oknie rozszerzeń może być tworzona lista rozszerzeń plików wyłączonych ze skanowania. Dodatkowo pojawia się nowa opcja pozwalająca wyłączyć ze skanowania pliki bez rozszerzeń. (Opcja wybrana domyślnie)

Metody



Wszystkie moduły Systemu Antywirusowego NOD32 używają pięciu podstawowych metod skanowania:

„Sygnatury" – skanowanie sygnaturowe polega na analizie i identyfikacji poszczególnych wirusów na podstawie ich „sygnatur" – specyficznych elementów kodu zgromadzonych w bazie danych wirusów.

„Heurystyka" – są to złożone algorytmy, które pozwalają na wykrywanie nowych, nieznanych jeszcze wirusów.

„Adware/Spyware/Riskware" - wykrywanie zagrożeń typu Adware: (małe programy, których działanie polega na pobieraniu reklam z Internetu i wyświetlanie ich), Spyware (programy, które zbierają poufne informacje o użytkowniku i wysyłają je przy pomocy Internetu), Riskware (programy, które mogą być wykorzystywane przez hakerów)

„Potencjalnie niechciane aplikacje" - programy, które nie zawsze stanowią zagrożenie bezpieczeństwa; Aplikacje te zwykle wymagają zgody użytkownika przed instalacją i mogą mieć wpływ na zachowanie systemu.

„Potencjalnie niebezpieczne aplikacje" - zazwyczaj komercyjne programy wykorzystywane przez hakerów (np. narzędzia zdalnego dostępu i administracji)

UWAGA: Zalecane jest zaznaczenie wszystkich metod. Najwyższy poziom ochrony jest zapewniony przez jednoczesne użycie obu wymienionych metod.

Dodatkowo od wersji 2.5 programu NOD32 zostały wprowadzone odrębne ustawienia skanowania w przypadku nowych, zainfekowanych plików:

„Pliki spakowane" - wybranie tej opcji powoduje skanowanie wewnątrz plików spakowanych programami: UPX, AsPack, FSG, Petite, Neolite, ExeStealth, yoda's Crypter, PECompact, Pklite, Lzexe, Diet, Exepack, CPAV i innymi programami pakującymi typu 'runtime packers' (zalecane).

„Archiwa samorozpakowujące" - skanuje wewnątrz plików spakowanych, samorozpakowujących (SFX).

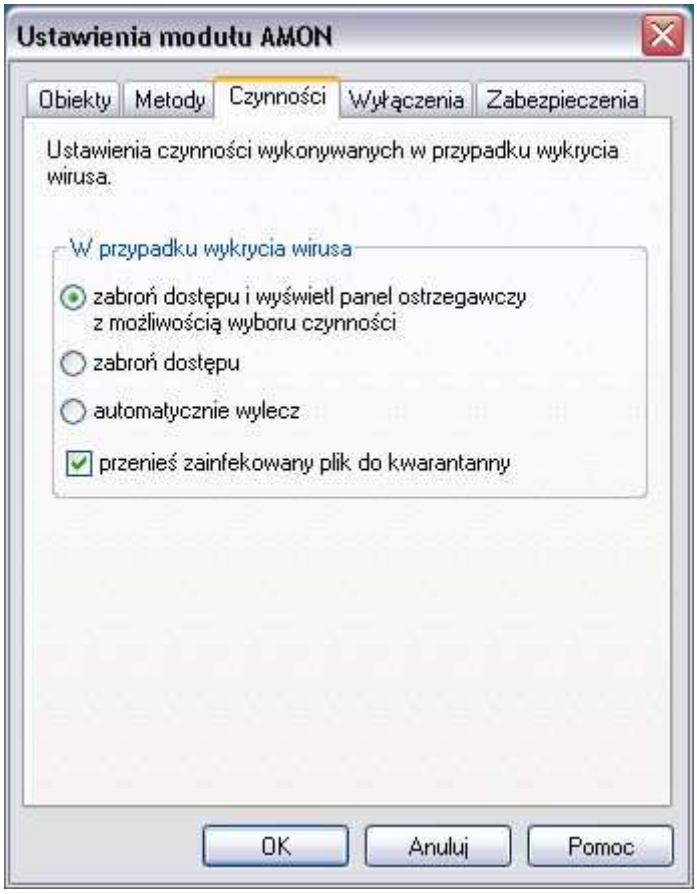
„Zaawansowana heurystyka" - rozszerza możliwości analizy heurystycznej programu NOD32 i zwiększa wykrywanie nowych zagrożeń włączając w to robaki, trojany i inne wirusy (zalecane).

„Przenieś do kwarantanny" - włączenie tej opcji umożliwia izolowanie wszystkich zainfekowanych i podejrzanych plików. Każdy tworzony plik, który jest zainfekowany automatycznie jest przenoszony do kwarantanny (zalecane jest włączenie tej opcji).

UWAGA: Zalecane jest zaznaczenie wszystkich metod. Najwyższy poziom ochrony jest zapewniony przez jednoczesne użycie obu wymienionych metod.

„Optymalizuj skanowanie" - dzięki tej opcji skaner skanuje szybciej, ponieważ nie skanuje powtórnie już przeskanowanych plików. Pliki będą skanowane ponownie jeśli zostały zmienione lub program antywirusowy został zaktualizowany.

Czynności



W przypadku wykrycia wirusa przez Monitor Antywirusowy (AMON), może być zrealizowany jeden z trzech scenariuszy:

*zabroń dostępu i wyświetl panel ostrzegawczy z możliwością w*yboru *czynności*

zabroń dostępu

automatycznie wylecz

Dodatkowo dostępna jest opcja *„przenieś zainfekowany plik do kwarantanny"*

Domyślny scenariusz to: (1.) *„zabroń dostępu do zainfekowanego pliku i wyświetl panel ostrzegawczy z możliwością wyboru czynności*". Wyboru oferowanych czynności możemy dokonać w zakładce Zabezpieczenia.

Opcjonalnie, dostęp do zainfekowanego pliku może być zablokowany bez podejmowania / oferowania czynności (scenariusz 2).

W przypadku żądania automatycznego leczenia zainfekowanych plików, należy wybrać opcję *„automatycznie wylecz"* (scenariusz 3). AMON w pierwszej kolejności spróbuje automatycznie wyleczyć zainfekowany plik. W przypadku, gdy pliku nie można wyleczyć (robak/trojan), AMON zablokuje dostęp do pliku.

Aby przenieść plik do kwarantanny przed podjęciem akcji leczenia, należy zaznaczyć opcję *„przenieś zainfekowany plik do kwarantanny* . Plik zostanie zapisany w katalogu kwarantanny. Domyślna lokalizacja kwarantanny to: C:\Program Files\Eset\infected.

Wyłączenia

Zakładka Wyłączenia pozwala na tworzenie/edycję listy plików, folderów i boot sektorów dyskietek wyłączonych ze skanowania. Zalecane jest pozostawienie domyślnych ustawień.

Aby wyłączyć obiekty ze skanowania przez moduł AMON należy nacisnąć przycisk ***Dodaj***.

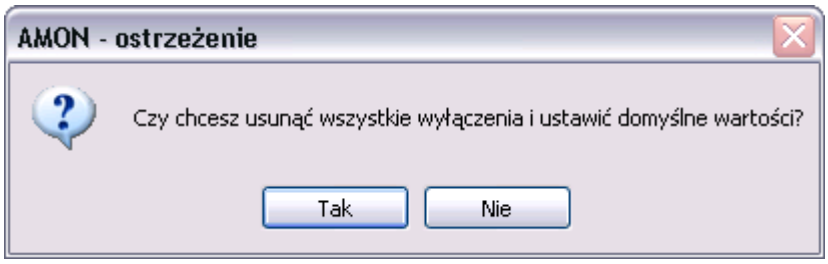
Opcja *„Wyłącz obiekt ze skanowania*: *na stałe | tymczasowo"*. Obiekt może być tymczasowo wykluczony ze skanowania (tylko do momentu ponownego uruchomienia komputera) lub na stałe – będzie obowiązywać przez cały czas (chyba, że wpis zostanie usunięty ręcznie).

„Wyłączony obiekt" – należy wybrać typ obiektu:

„folder" – po wybraniu można zdefiniować czy wyłączone ze skanowania mają być także podfoldery (opcja *Wyłącz podfoldery*). Pełną ścieżkę folderu należy wpisać w pole *Nazwa folderu* lub wskazać ją wciskając przycisk ***Folder***

„plik" – należy podać pełną ścieżkę pliku w polu *Nazwa pliku* lub wskazać ją wciskając przycisk ***Plik***

W zakładce Wyłączenia znajduje się również przycisk ***Domyślne***, który przywraca domyślną (pustą) listę wykluczeń. Wyzerowanie listy należy zatwierdzić przyciskiem ***Tak***.



Przycisk ***Zmień*** służy do edycji wyłączeń znajdujących się na liście.
Przycisk ***Usuń*** usuwa wybrany wpis z listy wyłączeń.

Zabezpieczenia

W przypadku wykrycia wirusa na ekranie monitora może pojawić się okno ostrzegawcze zawierające możliwe do wykonania akcje (zależy to od ustawień w zakładce Czynności). Wyboru wyświetlanych czynności możemy dokonać w zakładce Zabezpieczenia:

„Wylecz" – usuwa wirusy z zainfekowanych plików (leczy plik)

„Usuń plik" – usuwa zainfekowany plik

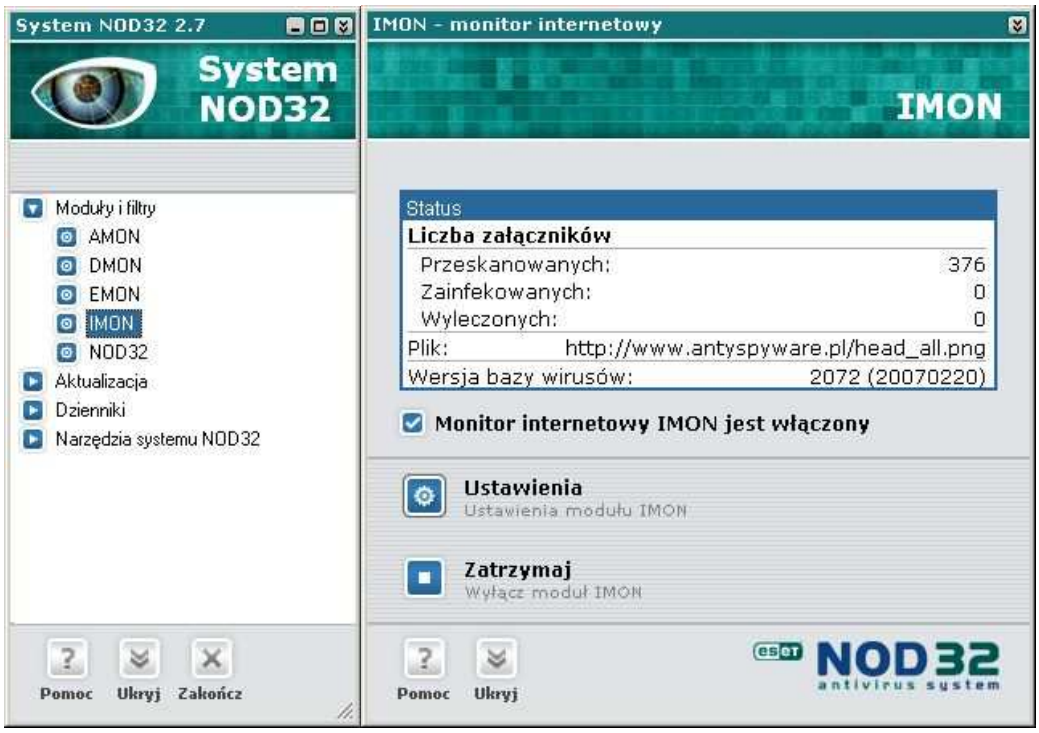
„Zmień nazwę" – zmienia nazwę zainfekowanego pliku (plik pozostanie nadal zainfekowany, ale nie będzie się samoczynnie uruchamiać)

„Zastąp" – zastępuje zainfekowany boot sektor czystą kopią

AMON jest najistotniejszym modułem ochrony antywirusowej i powinien być włączany automatycznie przy każdym uruchomieniu komputera. Służy do tego opcja *„Automatyczna aktywacja modułu AMON"* – jeśli jest zaznaczona, to po uruchomieniu komputera AMON uruchomi się automatycznie.
„Aktualizuj bazę wirusów zaraz po pobieraniu plików aktualizacyjnych" – gdy ta opcja jest włączona to po pobraniu plików aktualizacyjnych z Internetu od razu są one przetwarzane i baza wirusów zostaje uaktualniona. Zalecane jest pozostawienie jej włączonej.
Po ustawieniu opcji na zakładkach w oknie konfiguracyjnym modułu AMON należy potwierdzić zmiany przyciskiem ***OK***.

IMON – Monitor Internetowy

Podczas gdy AMON monitoruje przetwarzane pliki, moduł IMON na bieżąco sprawdza przychodzącą pocztę (protokół POP3) i przeglądane strony internetowe (protokół HTTP).
IMON jest programem bardzo łatwym w obsłudze i – aby skanować pocztę i strony internetowe – nie wymaga żadnej konfiguracji (pracuje na poziomie Winsock–a). Także przy dodawaniu nowego konta pocztowego użytkownik nie musi pamiętać o tym, żeby włączyć sprawdzanie tego konta.



IMON sprawdza pocztę przychodzącą z Internetu i wszystkie przeglądane strony internetowe. Przy otwieraniu pobranych już wiadomości pliki do nich załączone są sprawdzane przez modułu AMON (sprawdza on załącznik zapisywany tymczasowo na dysku). Dlatego zawsze należy upewnić się, że moduł IMON jest włączony i zaktualizować program do najnowszej wersji. Jeżeli np. IMON był wyłączony, to do lokalnej skrzynki odbiorczej komputera mogła przedostać się wiadomość z wirusem. Włączenie modułu IMON po odebraniu tej wiadomości (niezależnie czy była odczytana, czy nie) nie spowoduje jej ponownego sprawdzenia. Aczkolwiek, jeśli AMON jest aktywny, to wirus zostanie wykryty przy próbie zapisania zainfekowanego załącznika. Można też przeskanować pliki poczty przy użyciu skanera na żądanie NOD32.

Należy pamiętać, że IMON (podobnie jak AMON) aby spełniał swoją funkcję, musi być **uruchomiony** (załadowany do pamięci) i **włączony** (aktywny). Włączanie i wyłączanie modułu IMON jest bardzo podobne jak w przypadku modułu AMON. Dlatego poniższy opis jest bardzo zbliżony do opisu AMON. Należy jednak pamiętać, że moduł internetowy bardziej integruje się z systemem operacyjnym i

dlatego jego faktyczne załadowania lub wyładowania z pamięci następują dopiero po ponownym uruchomieniu komputera.

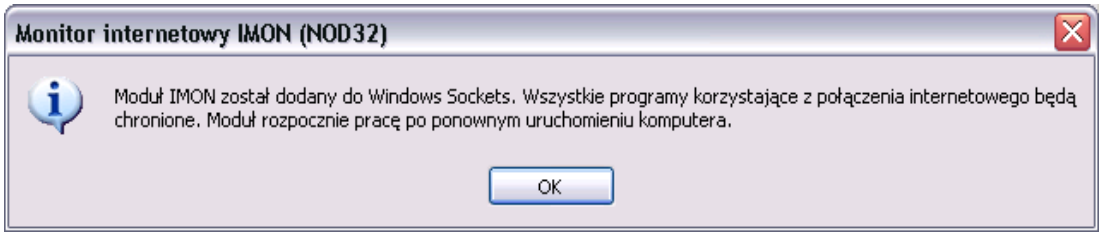
IMON może znajdować się w trzech stanach (każdy z nich oznaczony jest w konsoli Systemu innym kolorem ikonki umieszczonej obok modułu IMON):

- Uruchomiony i włączony (moduł działa, jest załadowany do pamięci i wykonuje skanowanie w tle), ikonka IMON–a jest niebieska .
- Uruchomiony i wyłączony (załadowany do pamięci, ale nie wykonuje skanowania w tle), ikonka IMON–a jest czerwona .
- Zatrzymany i wyłączony (nie załadowany do pamięci), ikona IMON–a jest szara .

Stany 2 i 3 – (wyłączony IMON) nie są wskazane, ponieważ nie jest aktywna ochrona POP3 i HTTP na tym komputerze.

Aby uruchomić monitor IMON należy wykonać następujące czynności:

Jeśli jest w stanie 3 (szara ikona), należy kliknąć na jego ikonę w Systemie NOD32, co spowoduje otwarcie okna modułu IMON. Następnie nacisnąć przycisk ***Uruchom*** umieszczony w dolnej części okna modułu IMON. Pojawi się okno informujące o konieczności ponownego uruchomienia komputera aby wszystkie zmiany zostały zapisane i uaktywnione.



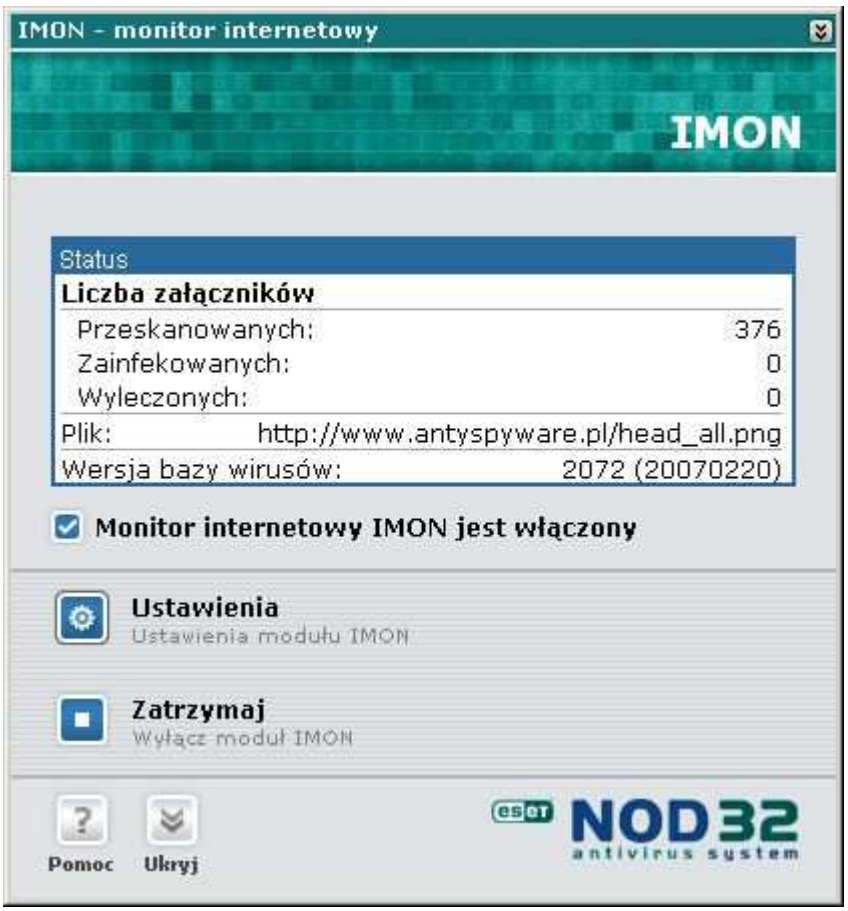
Następnie należy koniecznie uruchomić komputer ponownie, aby IMON faktycznie się załadował. Po ponownym uruchomieniu IMON przejdzie do stanu 2, ale dopiero wykonanie czynności podanych poniżej spowoduje przełączenie go w stan 1 – działanie modułu.

Jeśli IMON jest w stanie 2 (czerwona ikona) – IMON jest załadowany do pamięci ale sprawdzanie poczty jest wyłączone (nie wskazany stan). Aby to zmienić należy w oknie IMON–a zaznaczyć opcję "*Monitor Internetowy IMON jest*

włączony". Czynność ta spowoduje przełączenie modułu IMON do aktywnego (zalecanego) stanu z normalną ikoną. Aby sprawdzić pracę modułu IMON, należy zwrócić uwagę na górną część okna zawierającą informacje o liczbie sprawdzonych załączników ("*Liczba załączników przeskanowanych:*"). Należy ją zapamiętać a następnie uruchomić program pocztowy i odebrać nowe wiadomości lub otworzyć przeglądarkę i otworzyć dowolną stronę Internetową. Następnie należy powrócić do okna modułu IMON i sprawdzić ponownie parametr „*Liczba załączników przeskanowanych:*". Jeśli IMON jest uruchomiony właściwie, nowa wartość parametru zwiększy się.

Opis okna modułu IMON

Aby otworzyć okno modułu IMON należy kliknąć na ikonę programu w głównym oknie Systemu NOD32.

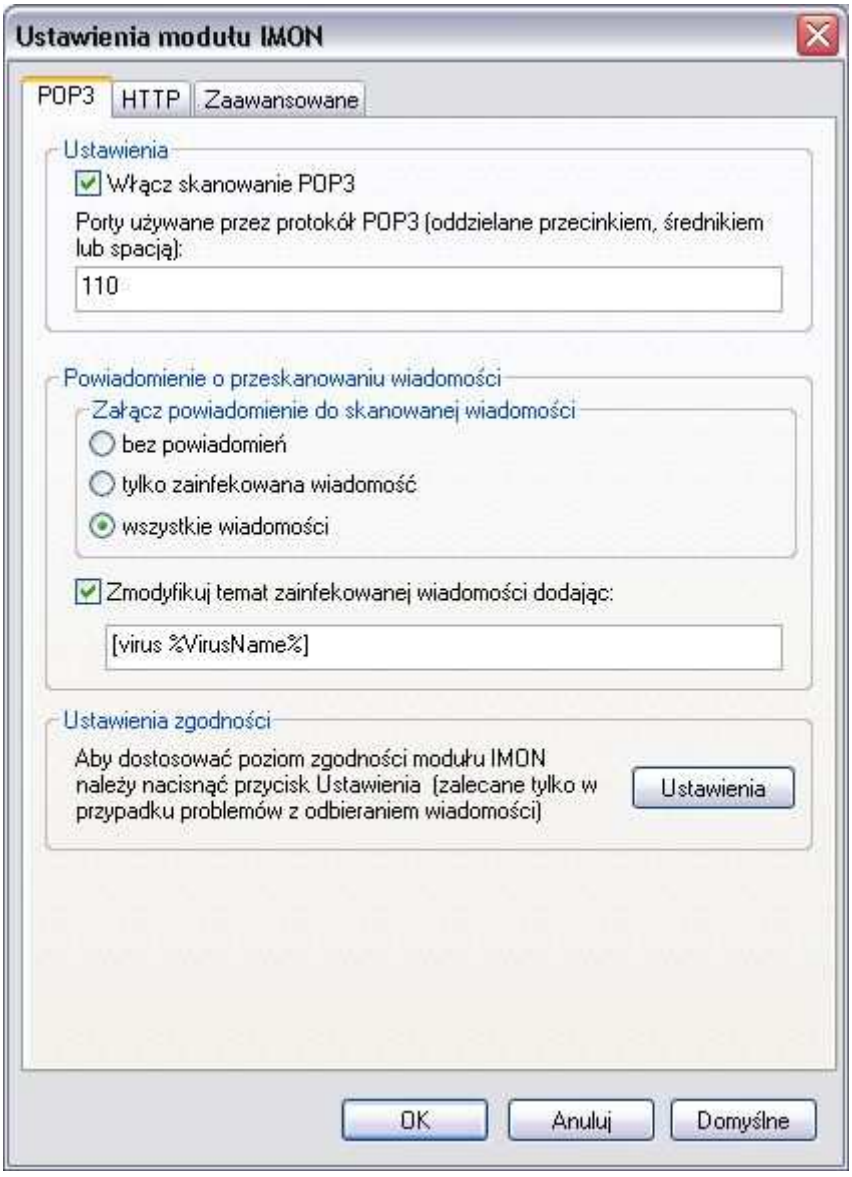


W górnej części okna znajdują się statystyki zawierające informacje o łącznej liczbie Przeskanowanych, Zainfekowanych i Wyleczonych załączników. Pokazana jest tam również wersja bazy wirusów używana w procesie skanowania i data jej wydania, przedstawiona w formacie: YYYYMMDD (czterocyfrowy rok, dwucyfrowy miesiąc i dwucyfrowy dzień miesiąca). Należy pamiętać o zapewnieniu ciągłej i częstej aktualizacji.

Zawartość okna modułu IMON (dostępne przyciski) zależy od stanu IMON–a w trakcie uruchomienia. Opcja *„Monitor Internetowy IMON jest włączony"* pozwala na włączenie lub zatrzymanie głównej funkcji IMON–a: monitorowania przychodzącej poczty i przeglądanych stron. Opcja ta jest dostępna (ikona nie jest koloru szarego) tylko w przypadku, gdy IMON jest załadowany do pamięci operacyjnej. Do załadowania monitora internetowego IMON do pamięci służy przycisk ***Uruchom***, do wyładowania – przycisk ***Zatrzymaj***, ale w obydwu przypadkach, aby zmiany się uaktywniły, konieczne jest jeszcze ponowne uruchomienie komputera (samo naciśnięcie przycisku ***Uruchom/Zakończ*** definiuje tylko, czy przy ponownym uruchomieniu komputera załadować do pamięci moduł IMON czy też nie).

Aby przejść do parametrów konfiguracji modułu IMON należy wybrać przycisk ***Ustawienia*** w głównym oknie modułu IMON.

Ustawienia modułu IMON – skaner POP3

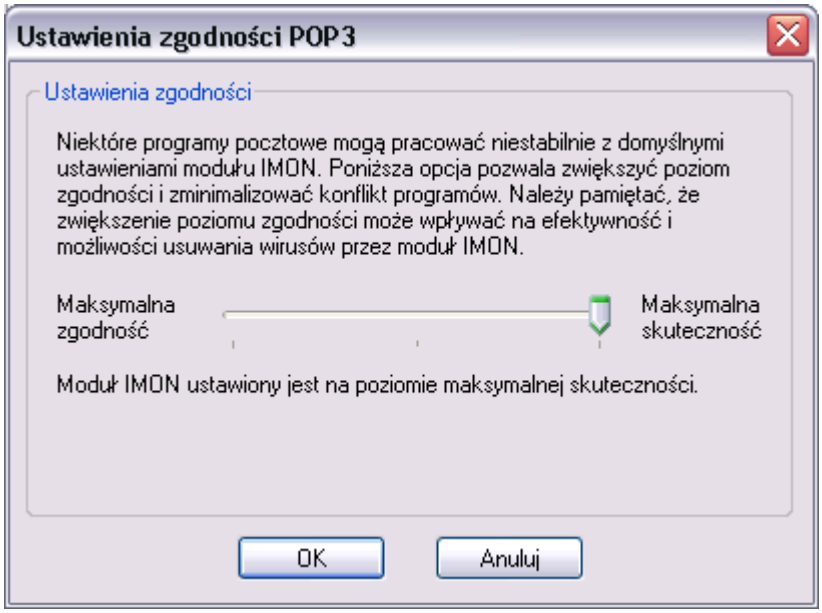


„Porty używane przez protokół POP3" – należy wprowadzić numer portu używanego do odbierania poczty przy pomocy protokołu POP3. Domyślnie jest to port 110.

IMON może dodawać powiadomienia do każdej sprawdzonej wiadomości pocztowej (*„cała poczta"*) lub tylko do zainfekowanych wiadomości (*„tylko zainfekowane wiadomości"*). Opcję dodawania powiadomień można również

całkowicie wyłączyć (*„bez powiadomień”*). Dodatkowo program może dodać informacje o wykrytym wirusie do tematu wiadomości. W tym celu należy zaznaczyć odpowiednią opcje.

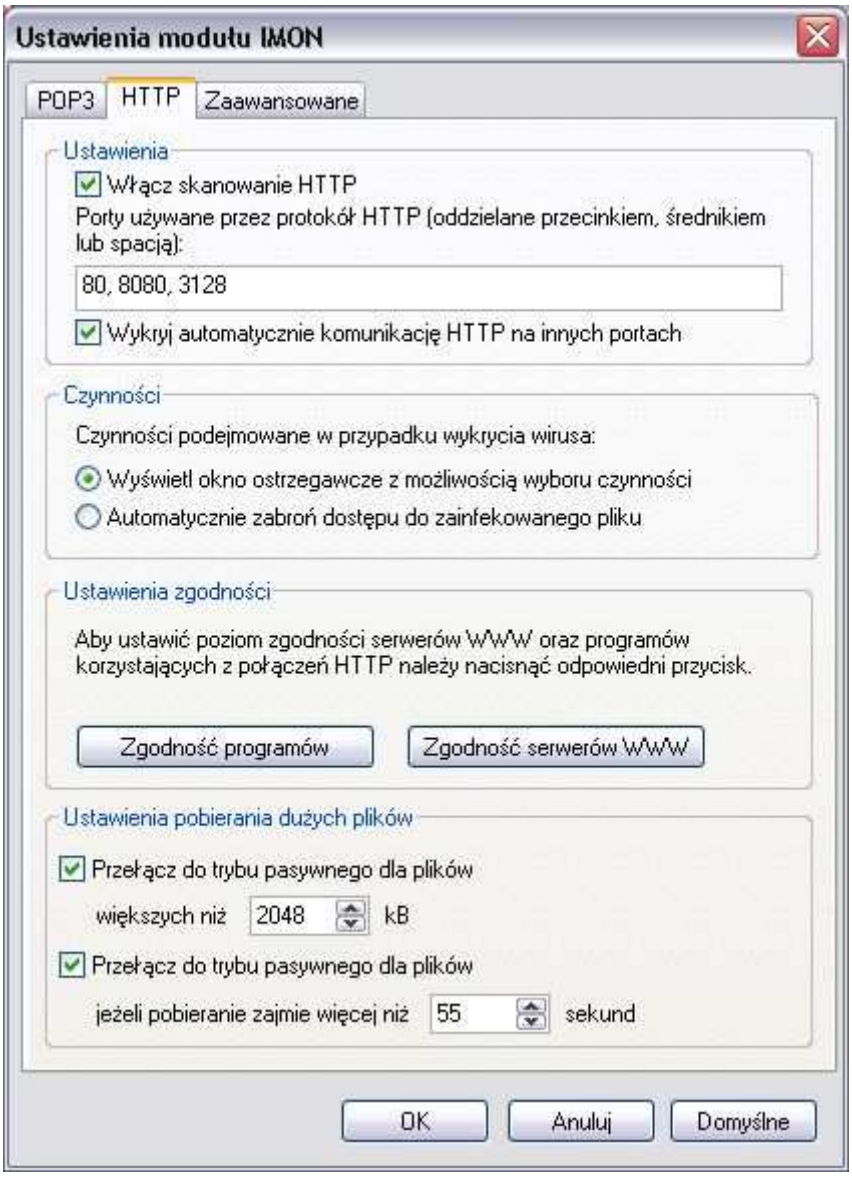
W sekcji *Ustawienia zgodności* znajduje się przycisk ***Ustawienia,*** który umożliwia zmianę poziomu integracji skanera POP3 z systemem operacyjnym. Zmiana tych opcji pomaga w rozwiązywaniu problemów systemu związanych z działaniem modułu IMON.



Znajduje się tam suwak stopnia integracji skanera POP3 z systemem. Standardowo powinien być przesunięty na pozycję *„Maksymalna skuteczność”* (prawa strona). Natomiast jeżeli pojawiają się problemy z połączeniem w czasie gdy działa IMON (gdy IMON jest wyłączony to nie występują), wtedy należy przetestować czy sytuacja ulegnie poprawie jeśli przesunie się suwak zgodności na pozycję *„Maksymalna zgodność”* (w lewo). Jeśli problem ustąpił warto przetestować zachowanie systemu w ustawieniu środkowym – pośrednim. Należy pamiętać, że w przypadku ustawienia *„Maksymalna zgodność”* nie są dodawane powiadomienia do wiadomości pocztowych i wirusy nie są usuwane ponieważ skaner POP3 nie ma możliwości ingerencji w odbierane wiadomości. W tym

przypadku zostanie jedynie wyświetlona informacja o wykrytej infekcji, dlatego bardzo ważne jest by AMON był zawsze uruchomiony i aktywny.

Ustawienia modułu IMON – skaner HTTP

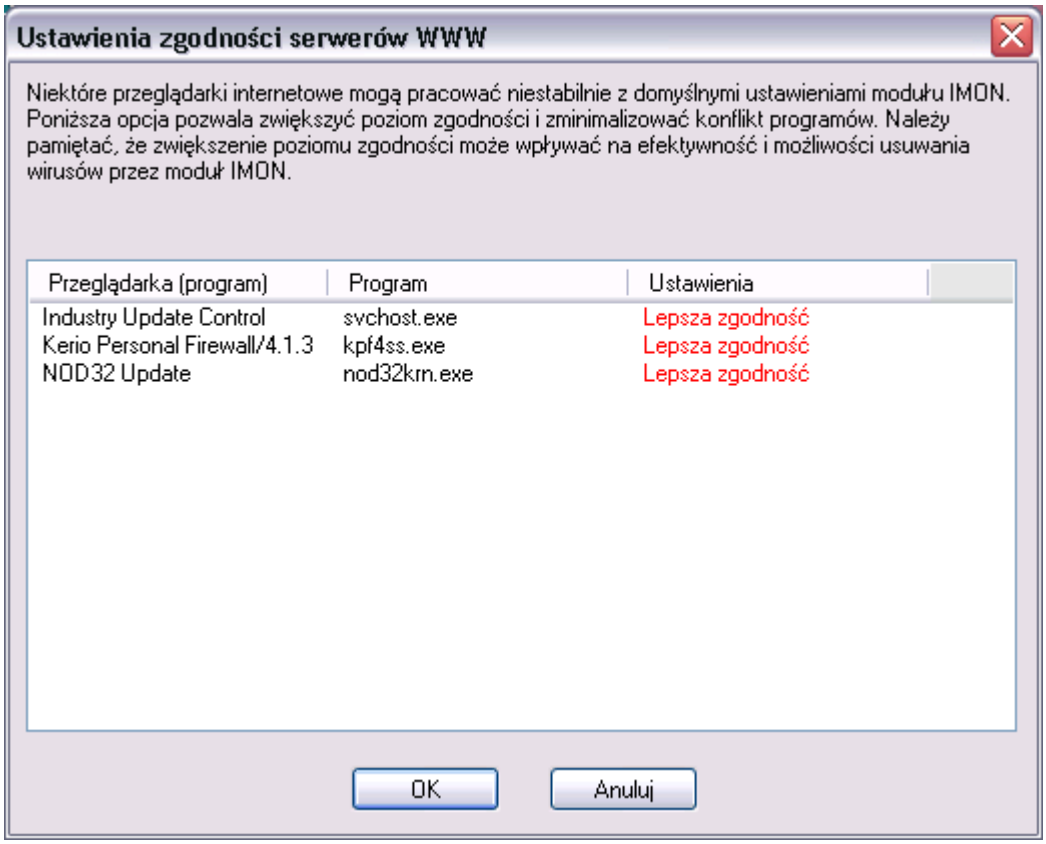


„Porty używane przez protokół HTTP” – należy wprowadzić numery portów używane do przeglądania stron internetowych przez przeglądarkę internetową (porty oddzielamy przecinkiem, średnikiem lub spacją). Domyślnie są to porty 80,

8080, 3128. Jeśli dostęp do Internetu odbywa się przy pomocy serwera Proxy, należy uwzględnić to również w ustawieniach podając odpowiednie porty.
Istnieje możliwość monitorowania wszelkich zmian w systemie przez skaner HTTP i w przypadku wykrycia komunikacji HTTP na innych portach skaner automatycznie zmodyfikuje listę, dodając nowe porty.

W przypadku wykrycia infekcji na przeglądanych stronach skaner HTTP może automatycznie zabronić dostępu do zainfekowanego pliku lub wyświetlić standardowy panel ostrzegawczy z możliwością wyboru czynności. Proszę wybrać odpowiednią opcję. Zalecaną opcją jest *„Automatycznie zabroń dostępu do zainfekowanego pliku”*.

W sekcji *Ustawienia zgodności* znajduje się dwa przyciski ***Zgodność programów*** i ***Zgodność serwerów WWW,*** które umożliwiają zmianę poziomu integracji skanera HTTP z przeglądarką internetową i wszystkimi programy działającymi na bazie przeglądarki internetowej. Zmiana tych opcji pomaga w rozwiązywaniu problemów systemu związanych z działaniem modułu IMON. Dostępne opcje to lepsza skuteczność i lepsza zgodność.



Skaner HTTP może pracować w trybie „pasywnym" lub „aktywnym". W trybie pasywnym części pobranego pliku są od razu wysyłane do oczekującej aplikacji, podczas gdy skaner HTTP gromadzi wszystkie fragmenty pobranego pliku w katalogu tymczasowym. W momencie pobrania ostatniego kawałka pliku IMON może przeskanować cały plik. Jeśli zostanie wykryta infekcja, IMON blokuje dostęp do pliku, przerywa połączenie z serwerem i wyświetla okno ostrzegawcze. Wadą tego rozwiązania jest fakt, że jeden z pobranych fragmentów może zawierać najważniejszy kod wirusa. Co więcej, jeśli aplikacja wielokrotnie próbuje pobrać zainfekowany plik, może użyć już zgromadzonych danych i pobrać jedynie zakończenie pliku. W tym przypadku IMON nie znajdzie nic podejrzanego w końcowej partii pliku.

W trybie aktywnym, IMON w pierwszej kolejności pobiera i skanuje cały plik a następnie przesyła go do oczekującej aplikacji. Procedura ta jest pewniejsza, ponieważ w tym przypadku aplikacja nie otrzyma żadnej części z pobieranego pliku. Wadą tego rozwiązania jest fakt, że aplikacja otrzymuje dane tylko raz. W przypadku gdy pobieranie trwa dłużej niż 5 sekund, w prawym dolnym rogu

pojawia się okienko z paskiem postępu. Tryb aktywny nie jest zalecany w przypadku gdy dane muszą być pobierane ciągle (np.: multimedia, pliki typu audio/video).

„Przełącz do pasywnego typu dla plików większych niż ... KB" - wybranie tej opcji spowoduje, że dla wszystkich plików większych niż zdefiniowany rozmiar, skaner HTTP będzie automatycznie przełączać się w tryb pasywny.

„Przełącz do pasywnego typu dla plików jeśli pobieranie zajmie więcej niż ... sekund" - wybranie tej opcji spowoduje, że dla wszystkich plików pobieranych dłużej niż zdefiniowany czas, skaner HTTP będzie automatycznie przełączać się w tryb pasywny

Zaawansowane ustawienia modułu IMON

Zakładka ***Zaawansowane*** umożliwia ustawienie dodatkowej konfiguracji modułu IMON.

Dostępne opcje to:

„Zapisuj do dziennika infekcji próby włamania” - Jeśli opcja jest włączona, każda próba infekcji komputera będzie odnotowywana w dzienniku infekcji systemu NOD32. Należy pamiętać o tym, że wirusy próbują czasem włamać się na komputer wykorzystując luki w systemach operacyjnych. Omawiana tutaj cecha systemu NOD32 jest odpowiedzialna za monitorowanie tego typu infekcji. Wyłączenie tej opcji nie spowoduje wyłączenia monitorowania prób włamań.

„Automatycznie wykryj i zastosuj zmiany ustawień w sieci" - IMON monitoruje wszelkie zmiany w konfiguracji sieci i próbuje je naprawiać aby skaner poczty i HTTP mógł poprawnie pracować. Jeśli jakiś inny program używa tych samych technik co IMON, należy wyłączyć tą opcje. Aby ręcznie wykryć zmiany w konfiguracji i naprawić je należy kliknąć na przycisk ***Wykryj***.

W sekcji *Wyłączenie programów ze skanowania modułu IMON* można dodać określony program lub plik dll do listy programów wyłączonych ze skanowania. Należy używać tej cechy w przypadku napotkania problemów z komunikacją sieciową (np. problem z połączeniem się z serwerem bazodanowym).

W przypadku pobierania dużych plików z Internetu, IMON może wyświetlać pasek postępu pobierania pliku w postaci małego okienka w prawym dolnym rogu. Pasek przewijania pozwala na określenie czy okno postępu ma być przeźroczyste (100%) czy nieprzeźroczyste (0%).

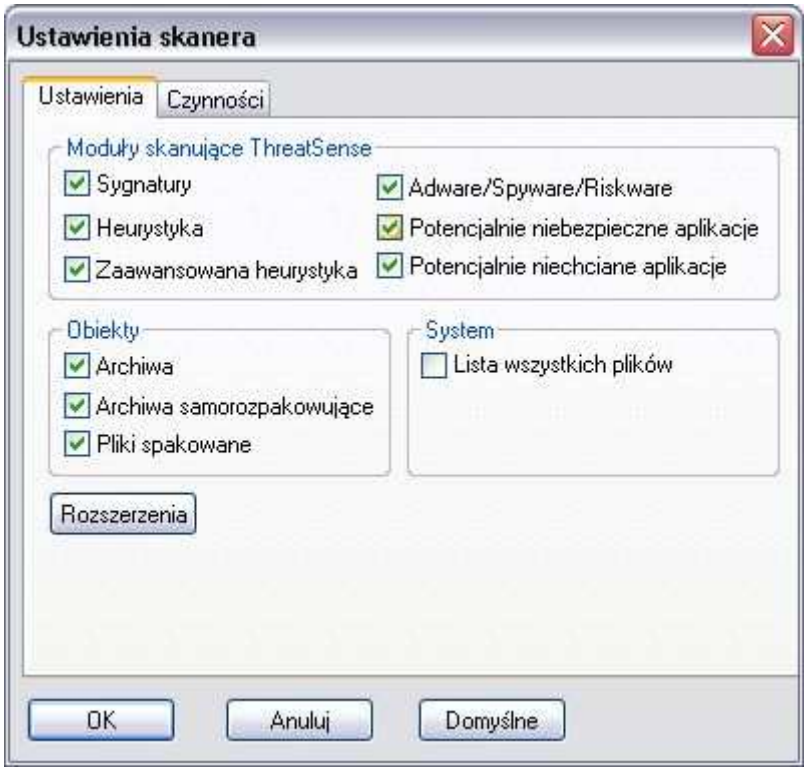
Sekcja *Ustawienia skanowania* zawiera ustawienia skanera: metody skanowania, czynności podejmowane w przypadku wykrycia infekcji i rozszerzenia przeznaczone do skanowania.

Ostatnia sekcja *Blokowanie dostępu do stron zawierających tylko zainfekowane pliki* - po zaznaczeniu tej opcji NOD32 będzie automatycznie blokować dostęp do stron zawierających jedynie zainfekowane pliki. Lista stron jest na bieżąco aktualizowana przez producenta.

Ustawienia skanowania modułu IMON

W tej sekcji znajduje się przycisk ***Konfiguracja*** pozwalający na zmianę opcji skanera. Opcja pozwala dostosować ustawienia skanera sprawdzającego pliki pobierane z Internetu.

Okno *Ustawienia skanera* pozwala określić:



Metody skanujące ThreatSense (wszystkie metody powinny być włączone):

„Sygnatury" **–** sprawdzanie na podstawie bazy wirusów.

„Heurystyka" **–** umożliwia wykrycie nieznanych wirusów na podstawie analizy pliku.

„Zaawansowana heurystyka" – rozszerza możliwości analizy heurystycznej programu NOD32 i zwiększa wykrywanie nowych zagrożeń włączając w to robaki, trojany i inne wirusy (zalecane).

„Adware/Spyware/Riskware" – wykrywanie zagrożeń typu Adware: (małe programy, których działanie polega na pobieraniu reklam z Internetu i wyświetlanie ich), Spyware (programy, które zbierają poufne informacje o użytkowniku i wysyłają je przy pomocy Internetu), Riskware (programy, które mogą być wykorzystywane przez hakerów)

„Potencjalnie niechciane aplikacje" - programy, które nie zawsze stanowią zagrożenie bezpieczeństwa; Aplikacje te zwykle wymagają zgody użytkownika przed instalacją i mogą mieć wpływ na zachowanie systemu.

„Potencjalnie niebezpieczne aplikacje" – zazwyczaj komercyjne programy wykorzystywane przez hakerów (np. narzędzia zdalnego dostępu i administracji)

Grupa **Obiekty** pozwala na wybór dodatkowych typów plików, które będą skanowane: *pliki spakowane* (runtime packers, UPX, itp.) *archiwa samorozpakowujące* (exe) oraz *archiwa* (ZIP, itp.). Zalecane jest włączenie sprawdzania wszystkich obiektów.

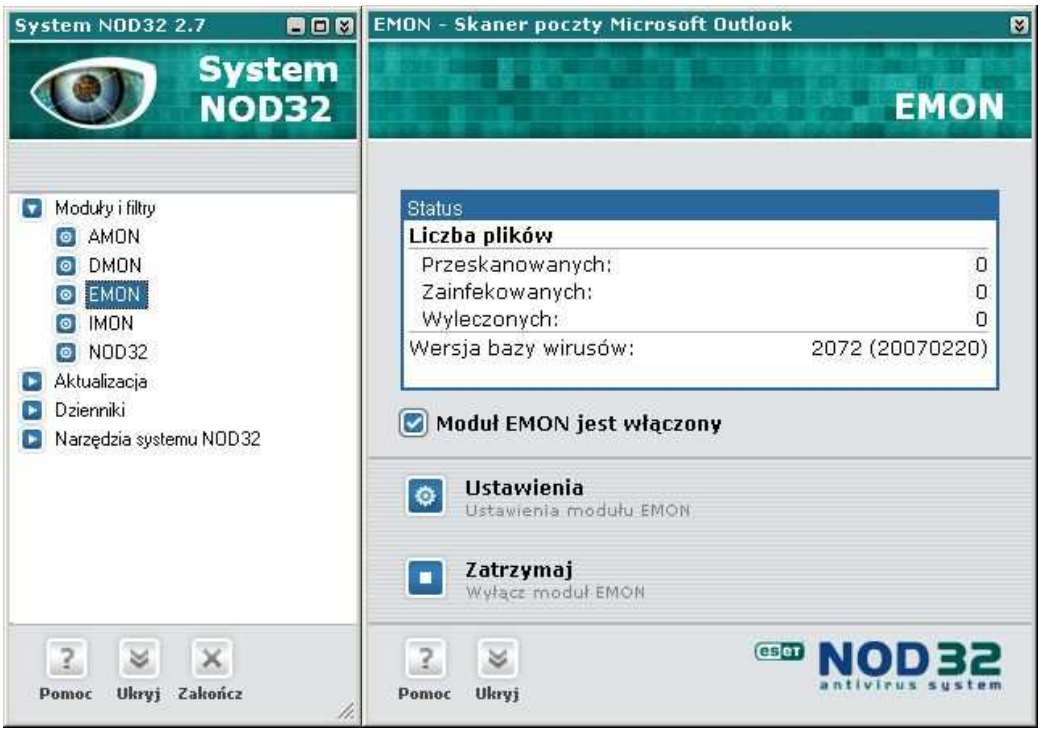
Przycisk ***Rozszerzenia*** pozwala zdefiniować rozszerzenia plików, które mają być skanowane. Zalecane jest pozostawienie ustawienia domyślnego – sprawdzanie wszystkich załączników (opcja *„skanuj wszystkie pliki"* włączona, brak rozszerzeń wyłączonych ze skanowania). Dokładniejsze informacje o definiowaniu rozszerzeń można znaleźć w opisie: konfiguracja AMON–a, edytor rozszerzeń.

Zaznaczenie opcji *„Lista wszystkich plików"* spowoduje, że jeśli w wiadomości zostanie znaleziony chociaż jeden wirus, to w Dzienniku infekcji we wpisie dotyczącym tego skanowania znajdą się informacje nie tylko o zainfekowanych, ale o wszystkich plikach dołączonych do tej wiadomości.

Zakładka **Czynności** pozwala zdefiniować akcję podejmowaną po znalezieniu wirusa. Jeśli zdefiniowaną czynnością jest wylecz plik, to w przypadku gdy wyleczenie infekcji nie jest możliwe (np. nieusuwalny wirus, robak lub trojan) wykonywana jest dodatkowa czynność zdefiniowana w grupie *Nieusuwalny wirus*.
Wybranie: *zaoferuj czynność* spowoduje, że użytkownik zostanie zapytany jak postąpić z załącznikiem za każdym razem, gdy program znajdzie wirusa w wiadomości pocztowej.
Jeśli program ma automatycznie zająć się wirusem należy zdefiniować odpowiednie akcje. Zalecane jest wybranie opcji: *wylecz plik*, a w przypadku nieusuwalnego wirusa – *usuń plik*.
Opcja *rozłącz* przerywa połączenie z serwerem i nie będzie możliwe odebranie bieżących ani dalszych wiadomości (ustawienie nie jest zalecane, może uniemożliwić odbiór poczty zgłaszając błąd połączenia).
Wybór opcji *„Kwarantanna"* sprawi, że przed każdorazowym podjęciem akcji, kopia zainfekowanego pliku zostanie umieszczona w specjalnym folderze kwarantanny przeznaczonym dla zawirusowanych plików. Kwarantanna przydatna jest, żeby sporządzić kopię zapasową pliku (np. w przypadku gdyby później możliwe było częściowe odzyskanie informacji ze pliku). Należy jednak pamiętać o okresowym usuwaniu plików z kwarantanny, aby nie przepełnić dysku na którym są one umieszczane. Więcej informacji znajduje się w części opisującej Kwarantannę.
Zatwierdzenie zmian następuje po naciśnięciu przycisku ***OK***.

EMON – poczty Microsoft Outlook

Moduł EMON skanuje wysyłaną i odbieraną pocztę na stacjach roboczych. Współpracuje z MS Exchange i MS Outlook.
Jego działanie jest bardzo podobne do działania modułu IMON.



EMON może znajdować się w trzech stanach (każdy z nich oznaczony jest w konsoli Systemu innym kolorem ikonki umieszczonej obok modułu EMON):

Uruchomiony i włączony (moduł działa, jest załadowany do pamięci i wykonuje skanowanie w tle), ikonka modułu EMON jest niebieska .

Uruchomiony i wyłączony (załadowany do pamięci, ale nie wykonuje skanowania w tle), ikonka modułu EMON jest czerwona .

Zatrzymany i wyłączony (nie załadowany do pamięci), ikona modułu EMON jest szara .

UWAGA: Stany 2 i 3 – (wyłączony EMON) nie są wskazane, ponieważ nie jest aktywna ochrona poczty.

Aby uruchomić monitor EMON należy zaznaczyć opcję *„Moduł EMON jest włączony”*.

Opis okna modułu EMON

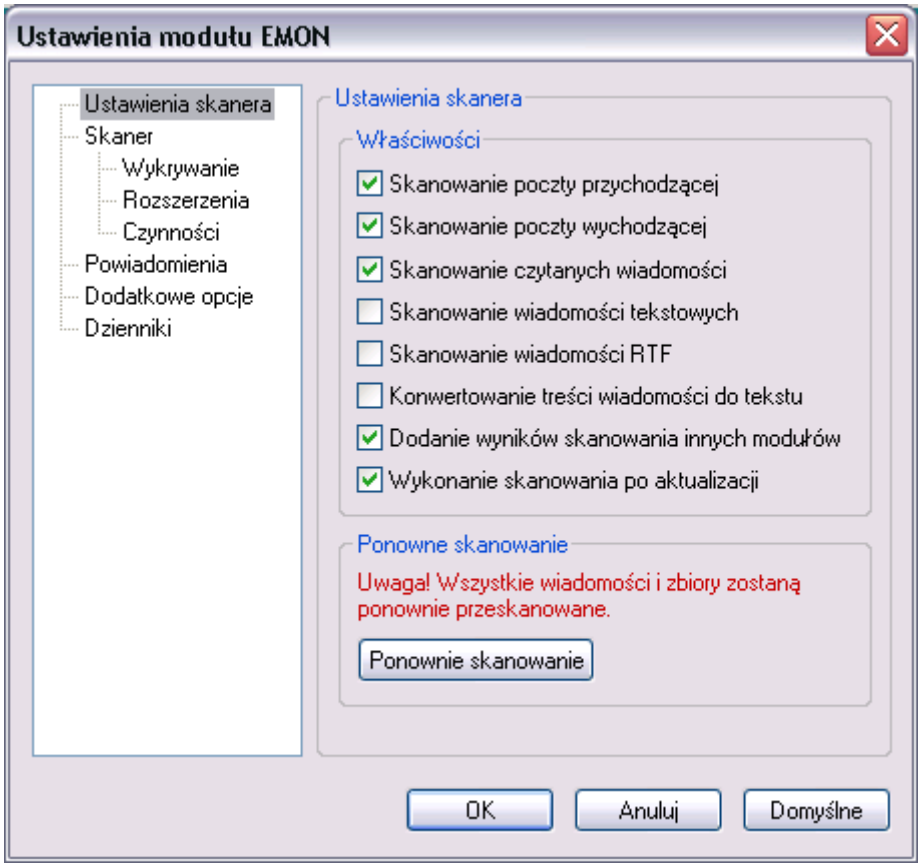
Aby otworzyć okno modułu EMON należy kliknąć na ikonę programu w głównym oknie Systemu NOD32.

W górnej części okna znajdują się statystyki zawierające informacje o łącznej liczbie Przeskanowanych, Zainfekowanych i Wyleczonych załączników. Pokazana jest tam również wersja bazy wirusów używana w procesie skanowania i data jej wydania, przedstawiona w formacie: YYYYMMDD (czterocyfrowy rok, dwucyfrowy miesiąc i dwucyfrowy dzień miesiąca). Należy pamiętać o zapewnieniu ciągłej i częstej aktualizacji.

Opcja *„Moduł EMON jest włączony”* pozwala na włączenie lub zatrzymanie głównej funkcji modułu EMON: monitorowania poczty przychodzącej i wychodzącej.

Aby przejść do parametrów konfiguracji modułu EMON należy wybrać przycisk ***Ustawienia*** w głównym oknie modułu EMON.

Ustawienia modułu EMON – ustawienia skanera



Dostępne są następujące opcje skanera poczty:

„Skanowanie poczty przychodzącej” - włączenie tej opcji spowoduje skanowanie wszystkich odbieranych wiadomości.

„Skanowanie poczty wychodzącej” - włączenie tej opcji spowoduje skanowanie wszystkich wysyłanych wiadomości.

„Skanowanie czytanych wiadomości” - włączenie tej opcji spowoduje skanowanie wiadomości przed jej otwarciem.

„Skanowanie wiadomości tekstowych” - włączenie tej opcji spowoduje skanowanie treści wiadomości tekstowych.

„Skanowanie wiadomości RTF” - włączenie tej opcji spowoduje skanowanie treści wiadomości w formacie RTF (Rich Text Format).

„Konwertowanie treści wiadomości do tekstu" - włączenie tej opcji spowoduje przekonwertowanie wszystkich wiadomości do formatu tekstowego. Proces konwertowania rozpocznie się po zakończeniu skanowania.

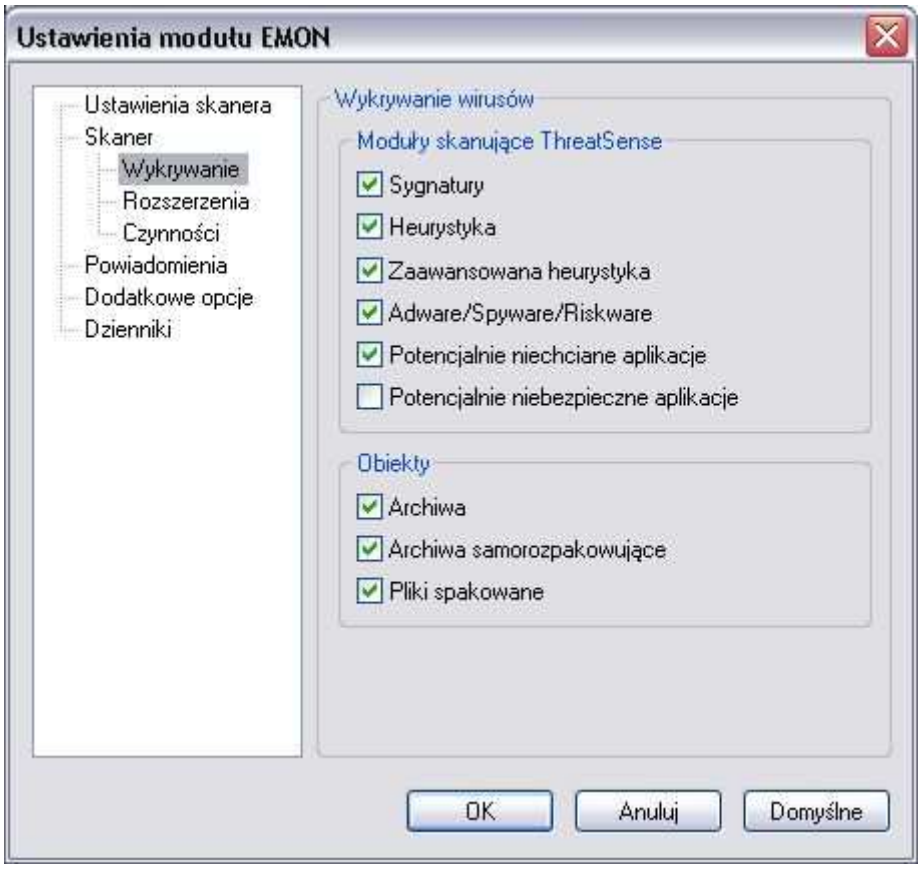
„Dodanie wyników skanowania innych modułów" - jeśli ta opcja jest włączona to wiadomości sprawdzone wcześniej przez inne moduły programu NOD32 (np. IMON) i oznaczone jako zainfekowane nie będą ponownie skanowane. EMON oznaczy tą pocztę jako zainfekowaną nawet jeśli wirus został już wcześniej usunięty.

„Wykonanie skanowania po aktualizacji" - włączenie tej opcji spowoduje ponowne skanowanie wszystkich wiadomości po każdej aktualizacji baz wirusów. Po przeskanowaniu wszystkich wiadomości.

„Ponowne skanowanie" - wybranie tej opcji spowoduje wyzerowanie rezultatów skanowania i wszystkie wiadomości będą skanowane ponownie. (Dzieje się tak również automatycznie po każdej aktualizacji baz wirusów).

W każdym momencie można przywrócić domyślne ustawienia wybierając przycisk Domyślne .

Ustawienia modułu EMON – wykrywanie



Metody skanujące ThreatSense:

„Sygnatury" - skanowanie sygnaturowe polega na analizie i identyfikacji poszczególnych wirusów na podstawie ich "sygnatur" - specyficznych elementów kodu zgromadzonych w bazie danych aktualizowanej przez producenta.

„Heurystyka" - są to złożone algorytmy, które pozwalają na wykrywanie nowych, nieznanych jeszcze wirusów.

„Zaawansowana heurystyka"-rozszerza możliwości analizy heurystycznej programu NOD32 i zwiększa wykrywanie nowych zagrożeń włączając w to robaki, trojany i inne wirusy (zalecane).

„Adware/Spyware/Riskware" -wykrywanie zagrożeń typu Adware: (małe programy, których działanie polega na pobieraniu reklam z Internetu i

wyświetlanie ich), Spyware (programy, które zbierają poufne informacje o użytkowniku i wysyłają je przy pomocy Internetu), Riskware (programy, które mogą być wykorzystywane przez hakerów)

„Potencjalnie niechciane aplikacje" - programy, które nie zawsze stanowią zagrożenie bezpieczeństwa; Aplikacje te zwykle wymagają zgody użytkownika przed instalacją i mogą mieć wpływ na zachowanie systemu.

„Potencjalnie niebezpieczne aplikacje" - zazwyczaj komercyjne programy wykorzystywane przez hakerów (np. narzędzia zdalnego dostępu i administracji)

UWAGA! Najwyższy poziom ochrony jest zapewniony przez jednoczesne użycie wszystkich wymienionych metod.

W grupie opcji Obiekty należy wybrać typy plików przeznaczone do skanowania (archiwa, archiwa samorozpakowujące, pliki spakowane, itp.).

Ustawienia modułu EMON – rozszerzenia

Zakładka **Rozszerzenia** pozwala zdefiniować rozszerzenia plików, które mają być skanowane. Zalecane jest pozostawienie ustawienia domyślnego – sprawdzanie wszystkich załączników (opcja *skanuj wszystkie pliki* włączona, brak rozszerzeń wyłączonych ze skanowania). Dokładniejsze informacje o definiowaniu rozszerzeń można znaleźć w opisie: konfiguracja modułu AMON, edytor rozszerzeń.

Przyciski umożliwiają edycję listy rozszerzeń:

Dodaj - Aby dodać nowe rozszerzenie należy wybrać przycisk Dodaj, wprowadzić nowe rozszerzenie i zatwierdzić przyciskiem OK.

Usuń - Aby usunąć rozszerzenie z listy (tylko w uzasadnionych przypadkach) należy podświetlić wybrane rozszerzenie, wybrać przycisk Usuń i zatwierdzić przyciskiem OK.

Domyślne - Aby przywrócić domyślne ustawienia listy rozszerzeń należy wybrać przycisk Domyślne i zatwierdzić przyciskiem OK.

Ustawienia modułu EMON – czynności

Zakładka **Czynności** pozwala zdefiniować akcję podejmowaną po znalezieniu wirusa. Jeśli zdefiniowaną czynnością jest wylecz plik, to w przypadku gdy wyczyszczenie infekcji nie jest możliwe (np. nieusuwalny wirus, robak lub trojan) wykonywana jest dodatkowa czynność zdefiniowana w grupie *Nieusuwalny wirus*.

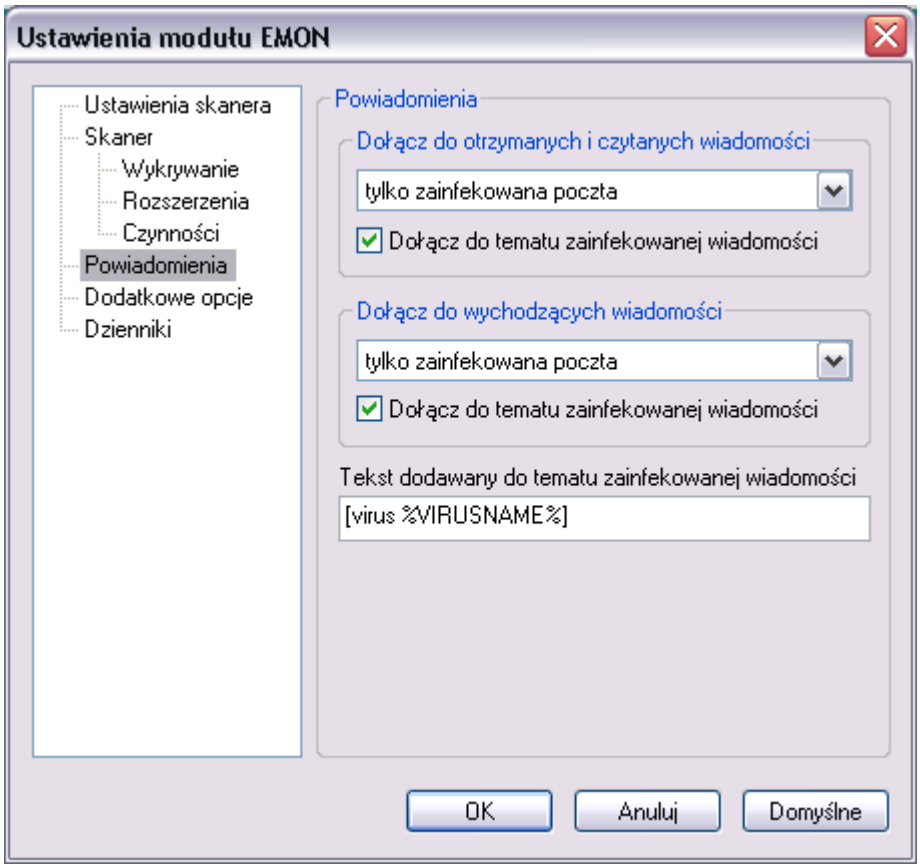
Wybranie opcji *„zaoferuj czynność"* spowoduje, że użytkownik zostanie zapytany jak postąpić z załącznikiem za każdym razem, gdy program znajdzie wirusa w wiadomości pocztowej.

Jeśli program ma automatycznie zająć się wirusem należy zdefiniować odpowiednie akcje dla wszystkich typów plików dostępnych na liście rozwijanej. Zalecane jest wybranie opcji: *wylecz plik*, a w przypadku nieusuwalnego wirusa – *usuń plik*.

Wybór opcji *„Kwarantanna"* sprawi, że przed każdorazowym podjęciem akcji, kopia pliku zostanie umieszczona w specjalnym folderze kwarantanny przeznaczonym dla zawirusowanych plików. Kwarantanna przydatna jest, żeby sporządzić kopię zapasową pliku (np. gdyby później możliwe było częściowe odzyskanie informacji ze pliku). Należy jednak pamiętać o okresowym usuwaniu plików z kwarantanny, aby nie przepełnić dysku na którym są one umieszczane. Więcej informacji znajduje się w części opisującej Kwarantannę.

Zatwierdzenie zmian następuje po naciśnięciu przycisku ***OK***.

Ustawienia modułu EMON – powiadomienia



Po sprawdzeniu wiadomości przez monitor EMON, do tematu i treści wiadomości może zostać dodana informacja o wyniku skanowania.

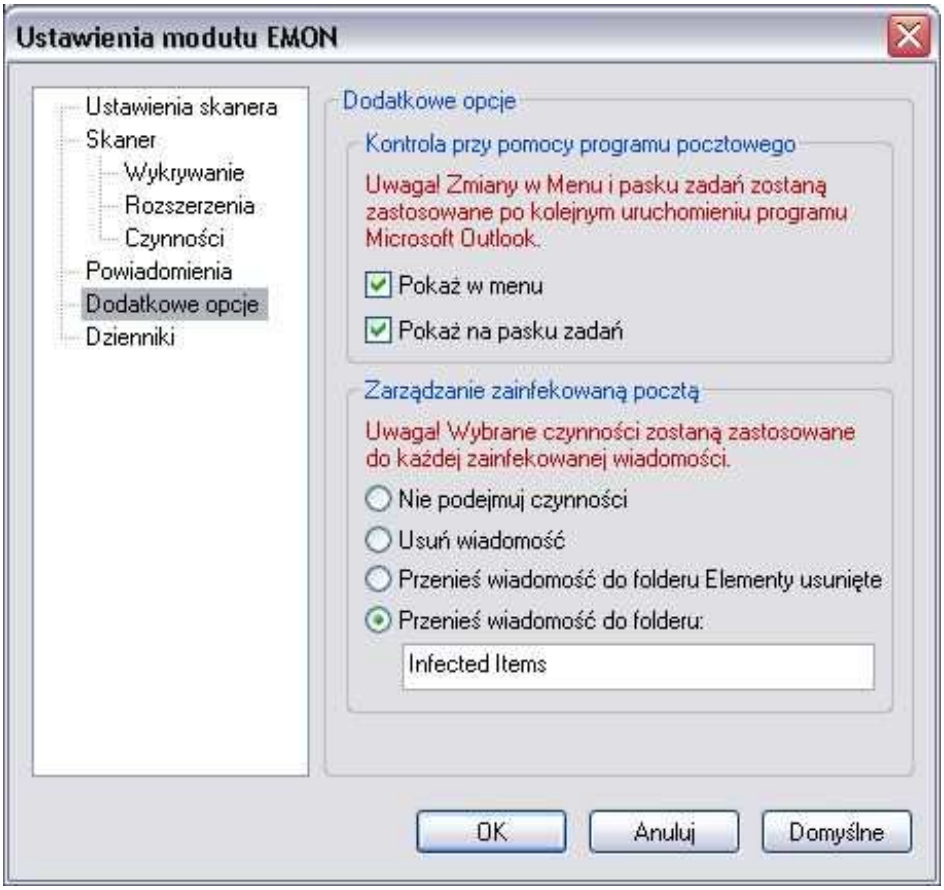
W sekcji *„Dołącz do otrzymanych i czytanych wiadomości"* można określić, do których wiadomości będzie dodawane powiadomienie. Dostępne opcje to *bez powiadomień, tylko zainfekowana poczta, cała poczta.*

Jeśli EMON ma również modyfikować temat zainfekowanej wiadomości, dodając wiadomość ostrzegawczą należy zaznaczyć opcję *„Dołącz do tematu zainfekowanej wiadomości"*

Podobnie działają ustawienia wiadomości wychodzących .

Użytkownik może również zdefiniować tekst informacji dodawanej do tematu wiadomości w polu: „*Tekst dodawany do tematu zainfekowanej wiadomości*". Ciąg znaków %VIRUSNAME% zostanie zastąpiony nazwą wykrytego wirusa.

Ustawienia modułu EMON – dodatkowe opcje



Aby ułatwić pracę użytkownikowi można dodać ikonę skanera na żądanie NOD32 do menu lub umieścić ją na pasku zadań. W tym celu należy zaznaczyć opcje: *„Pokaż w menu"* i *„Pokaż na pasku zadań"* .

W sekcji *Zarządzanie zainfekowaną pocztą* można zdefiniować czynności, które zostaną zastosowane do wszystkich zainfekowanych wiadomości. Jest to dodatkowa czynność, która w przeciwieństwie do zakładki **Czynności** , gdzie definiujemy czynność w przypadku wykrycia infekcji w załączniku, umożliwia ustawienie czynności dla całych wiadomości:

„Nie podejmuj czynności „- jeśli jest włączona to żadna akcja nie będzie podjęta.

„Usuń wiadomość" - wszystkie zainfekowane wiadomości będą usuwane.

„ Przenieś wiadomość do folderu Elementy usunięte" - w tym przypadku wszystkie zainfekowane wiadomości zostaną przesunięte do folderu Elementy usunięte.

„Przenieś wiadomość do folderu" - wszystkie zainfekowane wiadomości będą kopiowane do specjalnego folderu utworzonego w programie Microsoft Outlook.

Ustawienia modułu EMON – dzienniki

Zakładka **Dzienniki** określa ustawienia dotyczące zbierania informacji o infekcjach i błędach programu i zapisywania ich w centralnych dziennikach

programu NOD32 dostępnych z poziomu konsoli Systemu NOD32. Możliwe są następujące opcje:

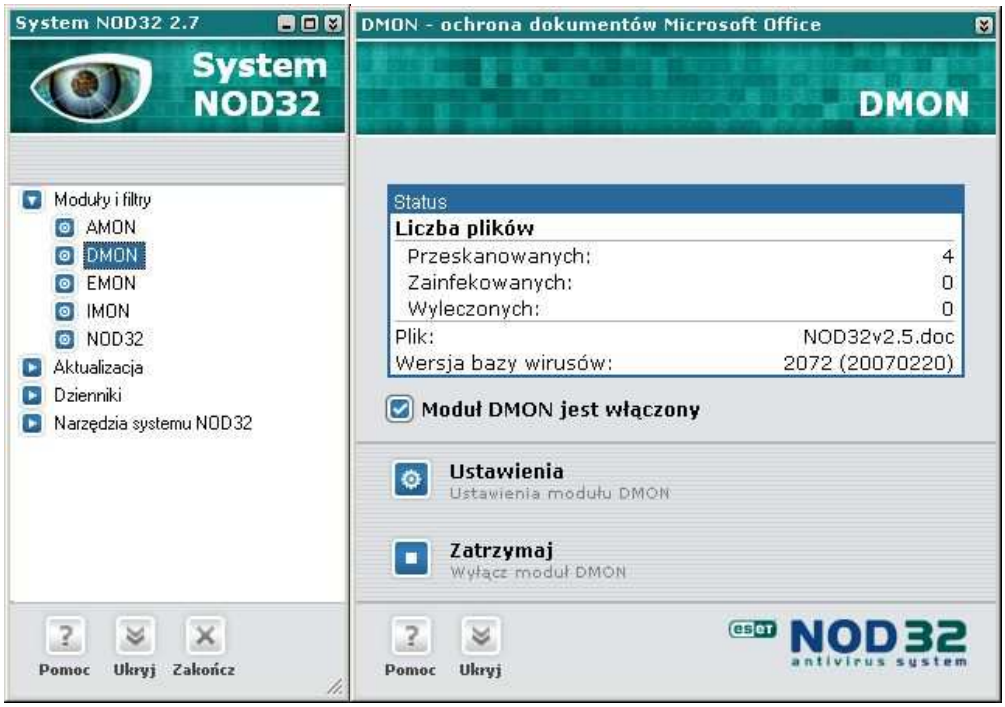
„Zapisuj wszystkie pliki do dziennika zdarzeń" - w tym przypadku wszystkie skanowane pliki zostaną zapisane w dzienniku zdarzeń.

„Synchronizowanie dzienników zdarzeń" - jeśli opcja jest włączona to wszystkie informacje będą na bieżąco zapisywane na dysku, bez przechowywania w pamięci.

„Zakres" - określa poziom szczegółowości danych zapisywanych w dzienniku zdarzeń. Najwyższy poziom, będzie zapisywać dokładnie wszystkie informacje o błędach i operacjach monitora EMON

DMON – skaner dokumentów Microsoft Office

Aby otworzyć okno modułu DMON należy kliknąć na ikonę programu w głównym oknie Systemu NOD32.



DMON jest nowym monitorem Systemu Antywirusowego NOD32, który zapewnia skanowanie dokumentów Microsoft Office i plików pobieranych automatycznie z Internetu przy pomocy Internet Explorer-a (np. elementy Microsoft ActiveX). DMON zapewnia dodatkową ochronę dla systemu.

UWAGA! DMON współpracuje wyłącznie z aplikacjami, które wspierają interfejs MS Antivirus API, np.: Microsoft Office 2000 (wersja 9.0 lub wyższa) lub Microsoft Internet Explorer (wersja 5.0 lub wyższa).

DMON może znajdować się w trzech stanach (każdy z nich oznaczony jest w konsoli Systemu innym kolorem ikonki umieszczonej obok modułu DMON):

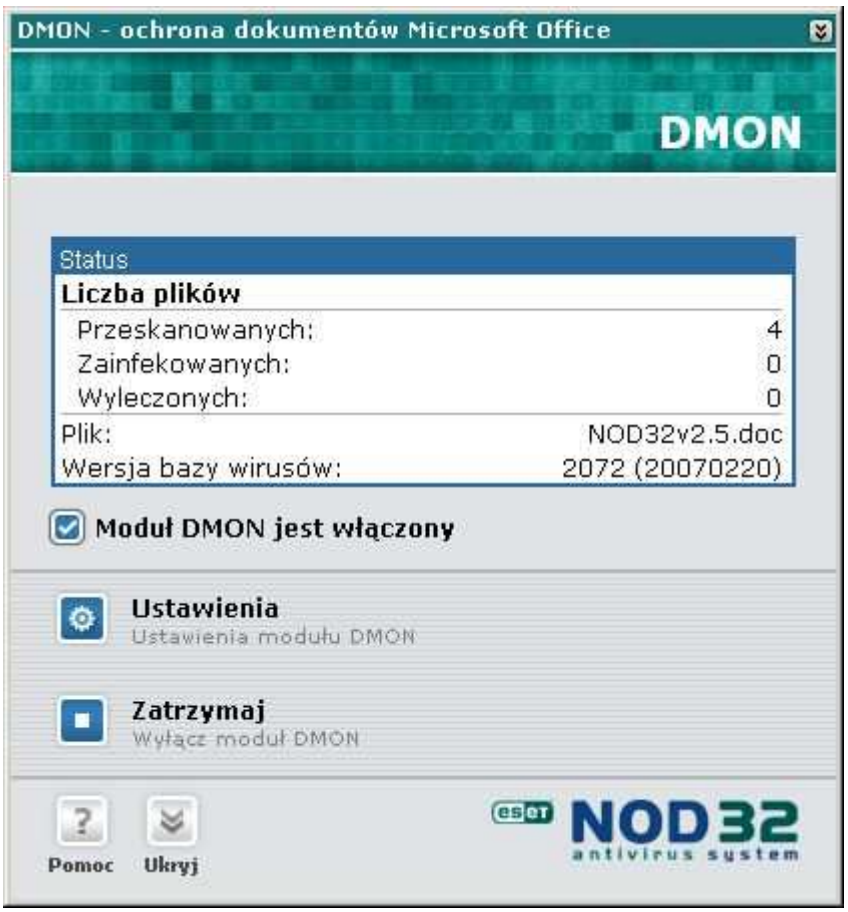
- Uruchomiony i włączony (moduł działa, jest załadowany do pamięci i wykonuje skanowanie w tle), ikonka DMON–a jest niebieska  .
- Uruchomiony i wyłączony (załadowany do pamięci, ale nie wykonuje skanowania w tle), ikonka DMON–a jest czerwona  .
- Zatrzymany i wyłączony (nie załadowany do pamięci), ikona DMON–a jest szara  .

UWAGA: Stany 2 i 3 – (wyłączony DMON) nie są wskazane, ponieważ nie jest aktywna ochrona poczty.

Aby uruchomić monitor DMON należy zaznaczyć opcję *„Moduł DMON jest włączony”*.

Opis okna modułu DMON

Aby otworzyć okno modułu DMON należy kliknąć na ikonę programu w głównym oknie Systemu NOD32.



W górnej części okna znajdują się statystyki zawierające informacje o łącznej liczbie Przeskanowanych, Zainfekowanych i Wyleczonych załączników. Pokazana jest tam również wersja bazy wirusów używana w procesie skanowania i data jej wydania, przedstawiona w formacie: YYYYMMDD (czterocyfrowy rok, dwucyfrowy miesiąc i dwucyfrowy dzień miesiąca). Należy pamiętać o zapewnieniu ciągłej i częstej aktualizacji.

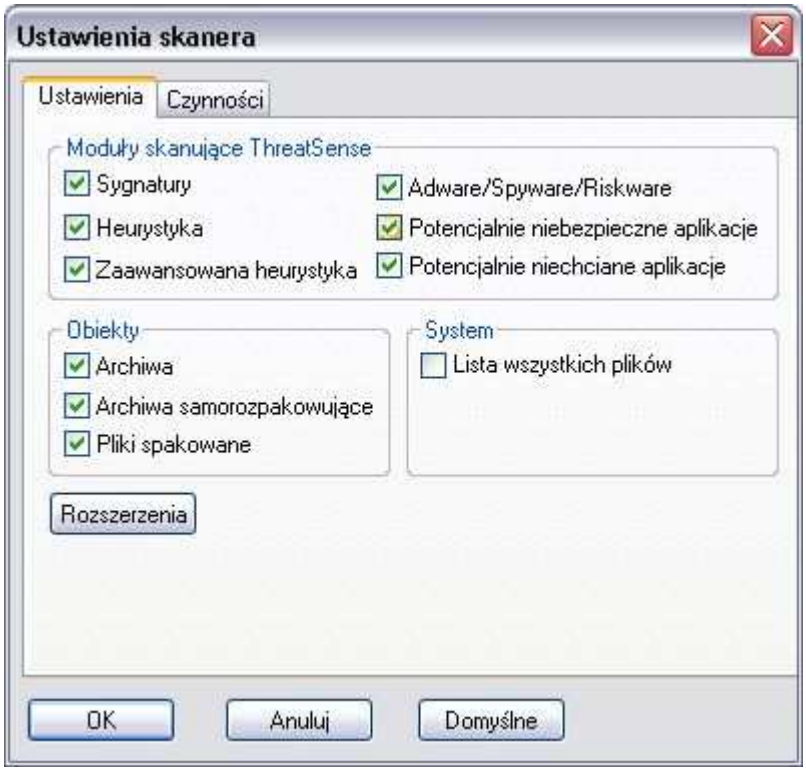
Opcja *„Moduł DMON jest włączony"* pozwala na włączenie lub zatrzymanie głównej funkcji modułu DMON: monitorowania dokumentów Microsoft Office.

Aby przejść do parametrów konfiguracji modułu DMON należy wybrać przycisk ***Ustawienia*** w głównym oknie modułu DMON.

Ustawienia skanowania modułu DMON

W tej sekcji znajduje się przycisk ***Konfiguracja*** pozwalający na zmianę opcji skanera. Opcja pozwala dostosować ustawienia skanera sprawdzającego pliki pobierane z Internetu.

Okno *Ustawienia skanera* pozwala określić:



Metody skanujące ThreatSense (wszystkie metody powinny być włączone):

„Sygnatury" **–** sprawdzanie na podstawie bazy wirusów.

„Heurystyka" **–** umożliwia wykrycie nieznanych wirusów na podstawie analizy pliku.

„Zaawansowana heurystyka" – rozszerza możliwości analizy heurystycznej programu NOD32 i zwiększa wykrywanie nowych zagrożeń włączając w to robaki, trojany i inne wirusy (zalecane).

„Adware/Spyware/Riskware" – wykrywanie zagrożeń typu Adware: (małe programy, których działanie polega na pobieraniu reklam z Internetu i wyświetlanie ich), Spyware (programy, które zbierają poufne informacje o

użytkowniku i wysyłają je przy pomocy Internetu), Riskware (programy, które mogą być wykorzystywane przez hakerów)

„Potencjalnie niechciane aplikacje" - programy, które nie zawsze stanowią zagrożenie bezpieczeństwa; Aplikacje te zwykle wymagają zgody użytkownika przed instalacją i mogą mieć wpływ na zachowanie systemu

„Potencjalnie niebezpieczne aplikacje" – zazwyczaj komercyjne programy wykorzystywane przez hakerów (np. narzędzia zdalnego dostępu i administracji)

Grupa **Obiekty** pozwala na wybór dodatkowych typów plików, które będą skanowane: *pliki spakowane* (runtime packers, UPX, itp.) *archiwa samorozpakowujące* (exe) oraz *archiwa* (ZIP, itp.). Zalecane jest włączenie sprawdzania wszystkich obiektów.

Przycisk ***Rozszerzenia*** pozwala zdefiniować rozszerzenia plików, które mają być skanowane. Zalecane jest pozostawienie ustawienia domyślnego – sprawdzanie wszystkich załączników (opcja *„skanuj wszystkie pliki"* włączona, brak rozszerzeń wyłączonych ze skanowania). Dokładniejsze informacje o definiowaniu rozszerzeń można znaleźć w opisie: konfiguracja AMON–a, edytor rozszerzeń.

Zaznaczenie opcji *„Lista wszystkich plików"* spowoduje, że jeśli w wiadomości zostanie znaleziony chociaż jeden wirus, to w Dzienniku infekcji we wpisie dotyczącym tego skanowania znajdą się informacje nie tylko o zainfekowanych, ale o wszystkich plikach dołączonych do tej wiadomości.

Zakładka **Czynności** pozwala zdefiniować akcję podejmowaną po znalezieniu wirusa. Jeśli zdefiniowaną czynnością jest wylecz plik, to w przypadku gdy wyleczenie infekcji nie jest możliwe (np. nieusuwalny wirus, robak lub trojan) wykonywana jest dodatkowa czynność zdefiniowana w grupie *Nieusuwalny wirus*. Wybranie: *zaoferuj czynność* spowoduje, że użytkownik zostanie zapytany jak postąpić z załącznikiem za każdym razem, gdy program znajdzie wirusa w wiadomości pocztowej.

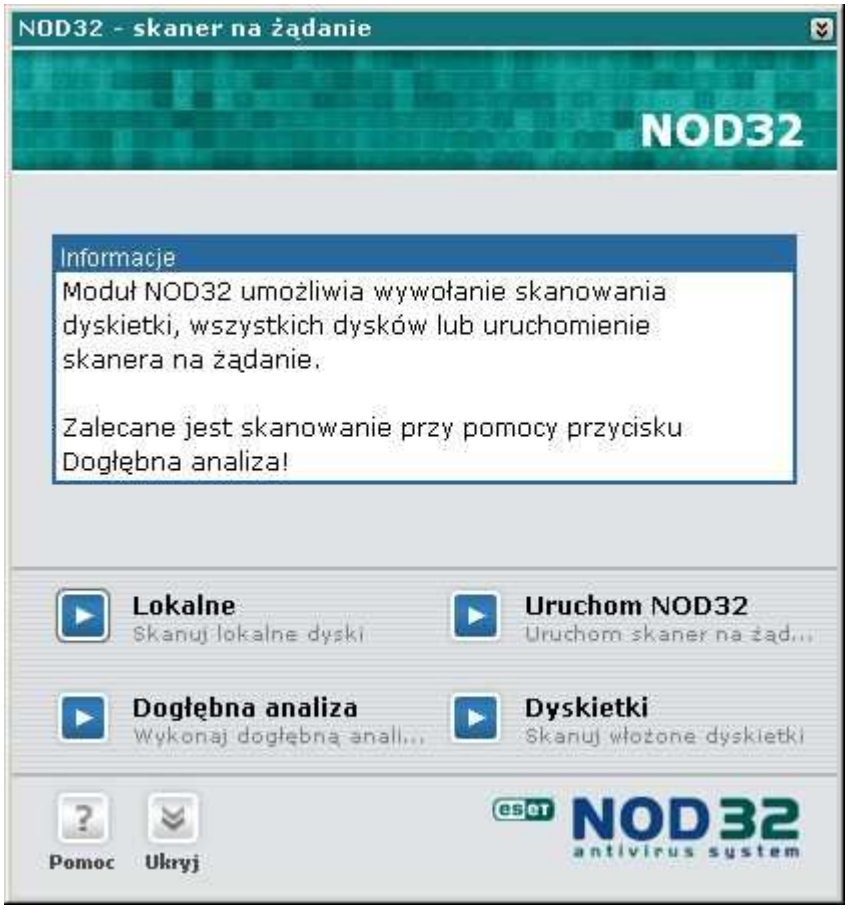
Jeśli program ma automatycznie zająć się wirusem należy zdefiniować odpowiednie akcje. Zalecane jest wybranie opcji: *wylecz plik*, a w przypadku nieusuwalnego wirusa – *usuń plik*.

Wybór opcji *„Kwarantanna"* sprawi, że przed każdorazowym podjęciem akcji, kopia zainfekowanego pliku zostanie umieszczona w specjalnym folderze kwarantanny przeznaczonym dla zawirusowanych plików. Kwarantanna przydatna jest, żeby sporządzić kopię zapasową pliku (np. w przypadku gdyby później możliwe było częściowe odzyskanie informacji ze pliku). Należy jednak pamiętać o okresowym usuwaniu plików z kwarantanny, aby nie przepełnić dysku na

którym są one umieszczane. Więcej informacji znajduje się w części opisującej Kwarantannę.

Zatwierdzenie zmian następuje po naciśnięciu przycisku ***OK***.

NOD32 – skaner na żądanie



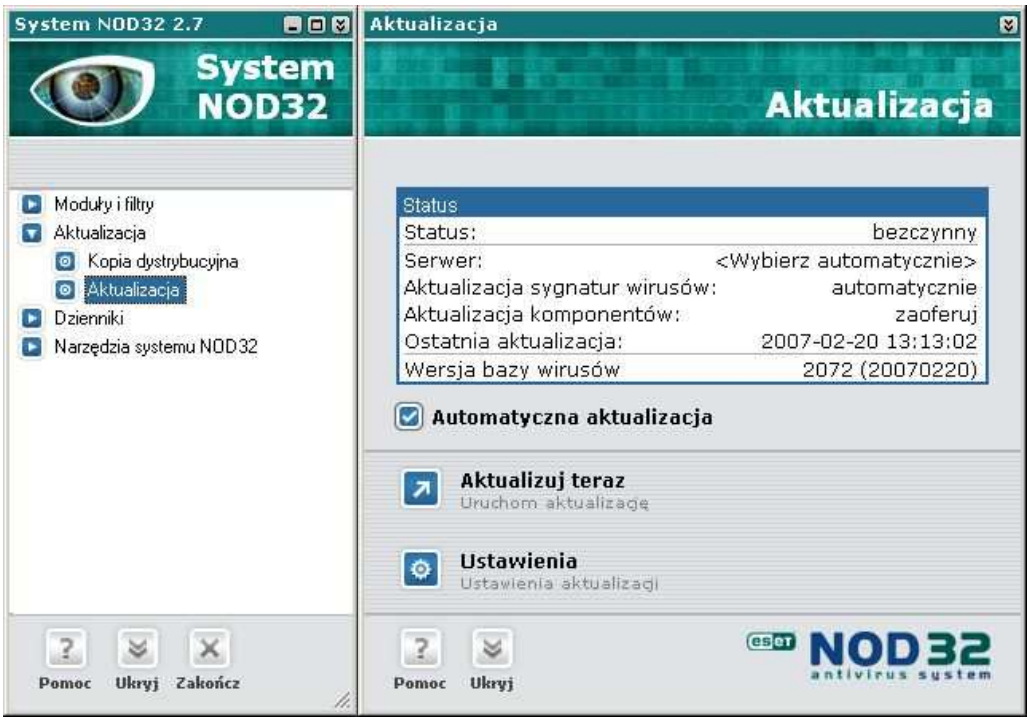
Moduł NOD32 umożliwia uruchomienie skanera na żądanie. Przycisk ***Lokalne*** uruchomi skanowanie wszystkich lokalnych dysków twardych, ***Dyskietki*** pozwala na automatyczne przeskanowanie dyskietek umieszczonych w napędach dyskietek, ***Dogłębna analiza*** dokona dokładnego skanowania całego dysku natomiast naciśnięcie przycisku ***Uruchom NOD32*** uruchomi skaner na żądanie. Więcej informacji na temat skanera na żądanie można uzyskać w rozdziale „Skaner na żądanie NOD32".

UWAGA! Zalecane jest skanowanie dysku przy użyciu przycisku ***Dogłębna analiza***.

Aktualizacja

Częsta aktualizacja jest niezbędna dla zagwarantowania prawidłowego działania programu antywirusowego. System Antywirusowy NOD32 zapewnia automatyczną aktualizację (przez Internet) wszystkich komponentów (tj. baza wirusów, moduł analizy heurystycznej).

Aby otworzyć okno Aktualizacji w głównym oknie **Systemu NOD32** należy rozwinąć grupę komponentów *Aktualizacja* i wybrać moduł *Aktualizacja*.



W górnej części okna znajdują się informacje dotyczące nazwy serwera aktualizacyjnego (domyślnie *<Wybierz automatycznie>*), daty ostatniej aktualizacji, itp. Przedstawiona jest tam również wersja bazy wirusów używana w

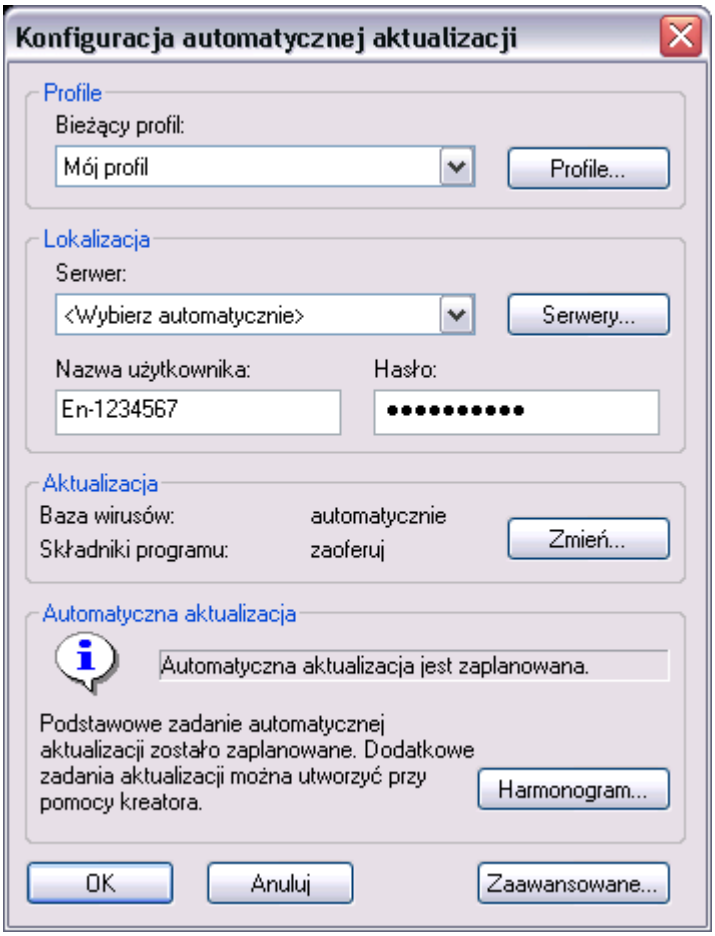
procesie skanowania i data jej wydania, w formacie: YYYYMMDD (czterocyfrowy rok, dwucyfrowy miesiąc i dwucyfrowy dzień miesiąca).

Opcja *„Automatyczna aktualizacja"*, jest zaznaczona gdy w Harmonogramie Zadań ustawione jest zadanie aktualizacji programu NOD32 (więcej informacji na temat automatycznej aktualizacji można znaleźć w części dokumentacji dotyczącej Harmonogramu Zadań). W tym przypadku ikona przy module aktualizacji jest koloru niebieskiego  . Jeżeli w Harmonogramie Zadań nie jest zdefiniowane żadne zadanie związane z automatyczną aktualizacją, wtedy opcja *„Automatyczna aktualizacja"* jest wyłączona a ikona aktualizacji jest koloru czerwonego  .

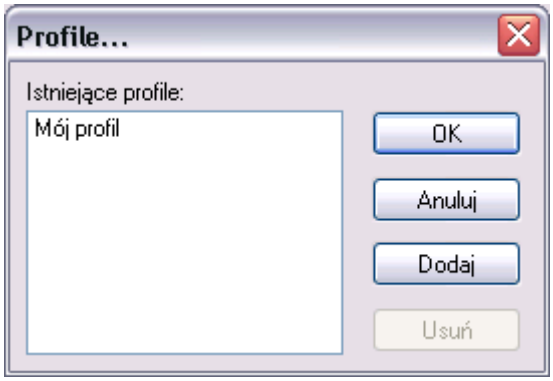
Aby uruchomić aktualizację na żądanie, należy nacisnąć przycisk ***Aktualizuj teraz***. Program pobierze niezbędne dane i zaktualizuje się.

Konfiguracja aktualizacji

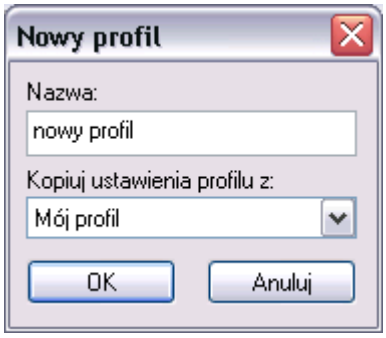
Aby zmienić konfigurację aktualizacji należy nacisnąć przycisk ***Ustawienia***



Profile służą do przechowywania ustawień parametrów aktualizacji. W zależności od zaistniałych okoliczności (tj. częsta zmiana serwera aktualizacji, zmiana ustawień połączenia sieci LAN/ modem), można używać różnych profili aktualizacji.



Aby zdefiniować nowy profil aktualizacji należy kliknąć na przycisk ***Profile***, wybrać przycisk ***Dodaj*** i wprowadzić nazwę dla nowego profilu. Można też wybrać istniejący profil i przekopiować jego ustawienia do tworzonego profilu. Wszystkie zmiany należy zatwierdzić przyciskiem ***OK***. Po zdefiniowaniu i skonfigurowaniu nowego profilu można uruchomić nowe zadanie aktualizacji w Harmonogramie zadań (używające nowego profilu).

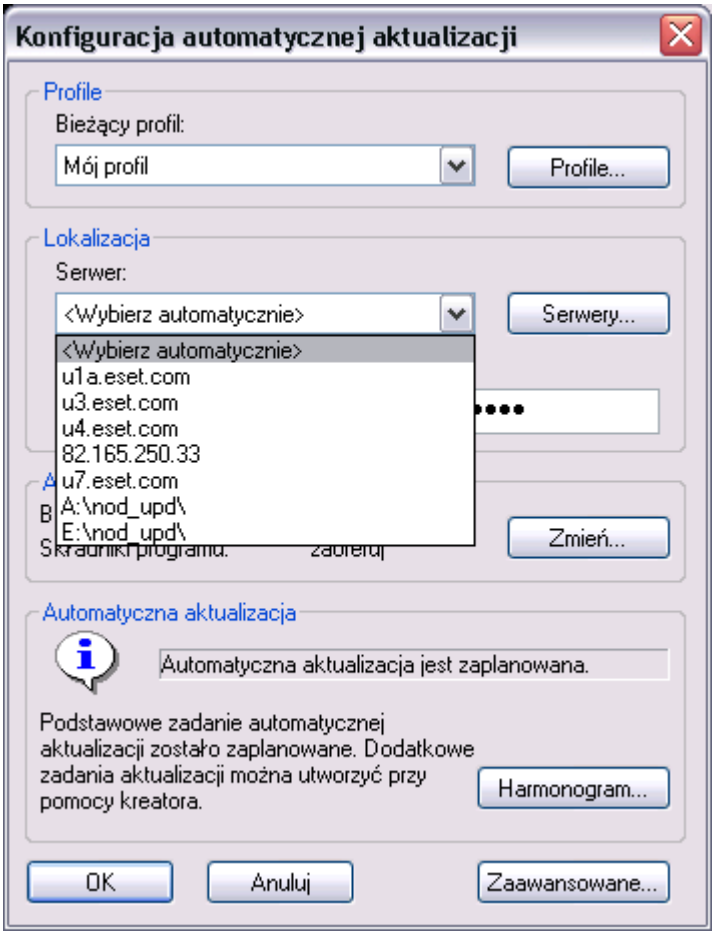


Aby zmienić profil aktualizacji należy kliknąć na przycisk ***Profile***, wybrać z listy jeden z dostępnych profili i zatwierdzić wybór przyciskiem ***OK***.

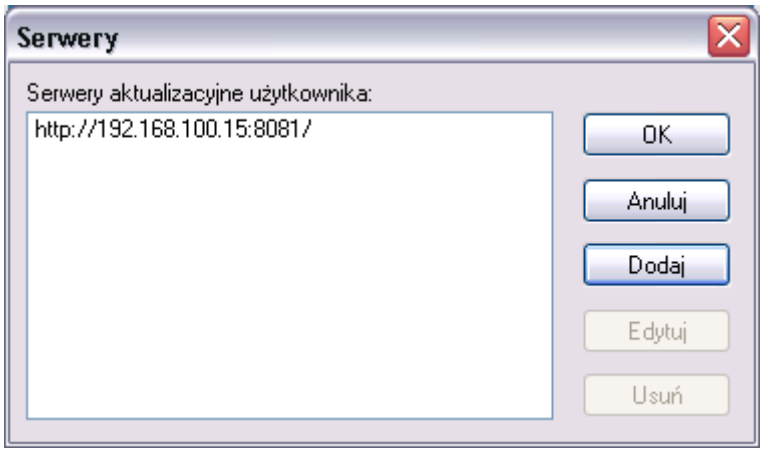
System Antywirusowy NOD32 aktualizuje się ze specjalnie wyznaczonych serwerów aktualizacji.

Serwerów aktualizacji mogą być serwery internetowe, zdefiniowane automatycznie na liście serwerów, folder udostępniony w sieci lokalnej, serwer HTTP w sieci lokalnej, dysk CD itp. Należy upewnić się, że każdy komputer ma dostęp do jakiegoś serwera aktualizacji (zawierającego najnowsze bazy wirusów).

Nowością jest możliwość wybrania opcji *„<Wybierz automatycznie>”,* która zapewnia poszukiwanie aktywnego, najszybszego serwera, przed rozpoczęciem procesu aktualizacji (uwzględnia tylko serwery internetowe).



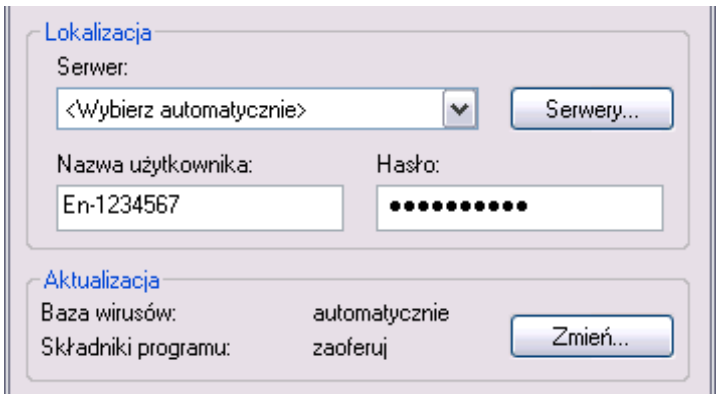
Aby zdefiniować nowy lub edytować ostatnio dodany serwer aktualizacji należy kliknąć na przycisk ***Serwery...,*** wybrać przycisk ***Dodaj***, a następnie wprowadzić nazwę nowego serwera lub ścieżkę dostępu do plików aktualizacyjnych. Wszelkie zmiany należy zatwierdzić przyciskiem ***OK***.



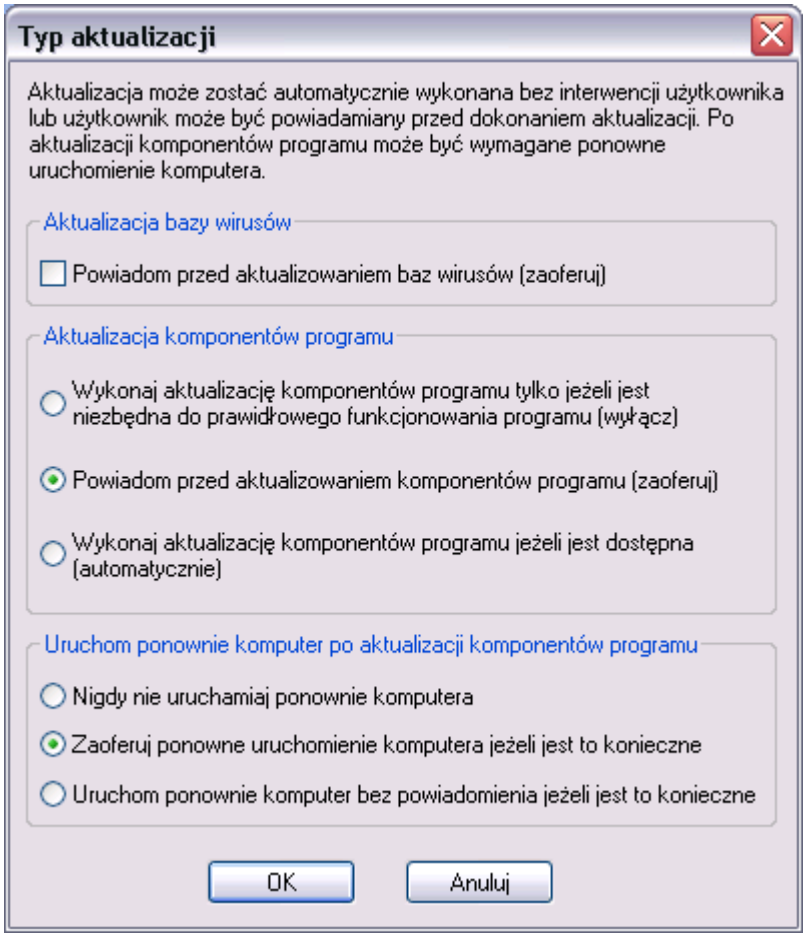
Nowy serwer pojawi się na liście serwerów aktualizacji. Aby ustawić go jako domyślny należy kliknąć na listę serwerów i wybrać z listy.

Serwery aktualizacyjne Producenta wymagają autoryzacji przy pomocy nazwy użytkownika i hasła. Aktualizacja z serwera zawierającego kopie dystrybucyjną (w sieci lokalnej) wymaga zdefiniowania użytkownika i nadania mu odpowiednich praw dostępu do folderu zawierającego aktualizację.

Niezwykle ważne jest poprawne ustawienie zadania automatycznej aktualizacji – zapewnia to maksymalny poziom ochrony antywirusowej. Aby dokonać aktualizacji z Internetu konieczne jest posiadanie prawidłowej ważnej nazwy użytkownika i hasła. Można je otrzymać w trakcie zakupu programu – na certyfikacie programu NOD32 będzie wpisana nazwa użytkownika i hasło. Jeśli na certyfikacie nie ma użytkownika i hasła należy najpierw zarejestrować program w Internecie używając numeru seryjnego. Wynikiem poprawnej rejestracji Programu NOD32 jest nazwa użytkownika i hasło przesłane na nasze konto pocztowe (poczta elektroniczna).



Aby uniknąć błędów w takcie wprowadzania użytkownika i hasła należy użyć metody dostępnej w systemie operacyjnym Windows: *„Kopiuj”* i *„Wklej”*.
System Antywirusowy NOD32 wspiera kilka scenariuszy aktualizacji. Aby zmienić typ aktualizacji należy kliknąć na przycisk ***Zmień*** w sekcji *Typ aktualizacji* i wybrać odpowiednie ustawienia. Dostępne są następujące opcje konfiguracji:



„Powiadom przed aktualizowaniem baz wirusów (zaoferuj)” – jeżeli opcja zostanie wybrana system aktualizacji będzie powiadamiać użytkownika przed każdą aktualizacją baz wirusów. W przypadku gdy opcja nie zostanie wybrana aktualizacja będzie przebiegać w pełni automatycznie.

Obok aktualizacji baz wirusów można również aktualizować komponenty programu. Dostępne są następujące możliwości:

„Wykonaj aktualizację komponentów programu tylko jeżeli jest niezbędna do prawidłowego funkcjonowania programu (wyłącz)" – aktualizacja wykona się automatycznie, jeżeli jest to konieczne do zachowania pełnej funkcjonalności programu.

„Powiadom przed aktualizowaniem komponentów programu (zaoferuj)" – zawsze zostanie wyświetlone zapytanie czy aktualizować komponenty programu.

„Wykonaj aktualizację komponentów programu jeżeli jest dostępna (automatycznie)" – zapewnia w pełni automatyczną aktualizację komponentów programu.

Aktualizacja baz wirusów odbywa się 'w locie' (nie wymaga ponownego uruchomienia systemu), natomiast w przypadku aktualizacji niektórych komponentów programu może być wymagane ponowne uruchomienie systemu operacyjnego. W sekcji **Uruchom ponownie komputer po aktualizacji komponentów programu** istnieje możliwość zdefiniowania opcji ponownego uruchomienia systemu. Należy wybrać jedną z dostępnych opcji:

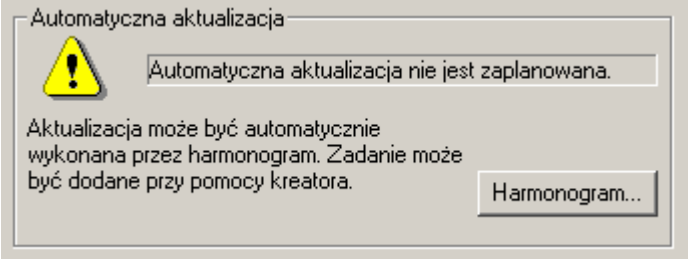
„Nigdy nie uruchamiaj ponownie komputera"

„Zaoferuj ponowne uruchomienie komputera jeśli jest to konieczne"

„Uruchom ponownie komputer bez powiadomienia jeśli jest to konieczne"

UWAGA: System NOD32 zapewnia inkrementacyjną (przyrostową) aktualizację baz wirusów i kompleksową aktualizację wykonywalnych komponentów programu NOD32.

Aby sprawdzić czy zostało uruchomione zadanie aktualizacji należy zapoznać się z informacją zawartą w grupie *Automatyczna aktualizacja*. Jeśli nie została zaplanowana automatyczna aktualizacja (tj. nie jest uruchomione żadne zadanie w Harmonogramie zadań) pojawia się odpowiednie ostrzeżenie.



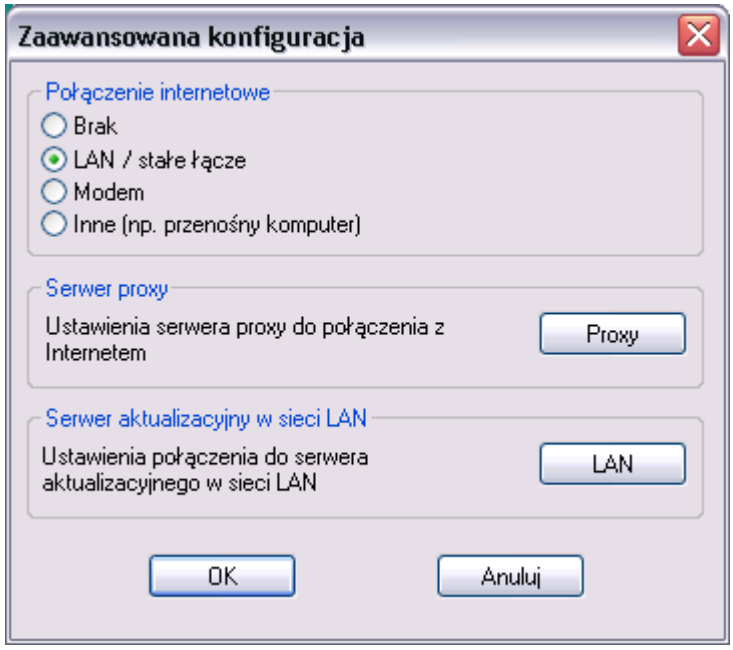
Jeżeli wyświetlony jest tekst: *„Automatyczna aktualizacja nie jest zaplanowana"* należy niezwłocznie utworzyć zadanie aktualizacji klikając na przycisk ***Harmonogram*** lub włączyć istniejące w *Harmonogramie* zadanie aktualizacji (Więcej informacji można znaleźć w rozdziale Harmonogram zadań).

Zaawansowane opcje konfigurowania aktualizacji (przycisk ***Zaawansowane...***) pozwalają na skonfigurowanie:

Typu połączenia internetowego

Serwera proxy

Serwera aktualizacyjnego w sieci LAN



Połączenie internetowe

Należy wybrać typ połączenia odpowiedni dla sieci/ komputera tak aby proces aktualizacji przebiegał bez problemów. Dostępne są następujące opcje:

Brak – w przypadku gdy nie jest znana konfiguracja sieci

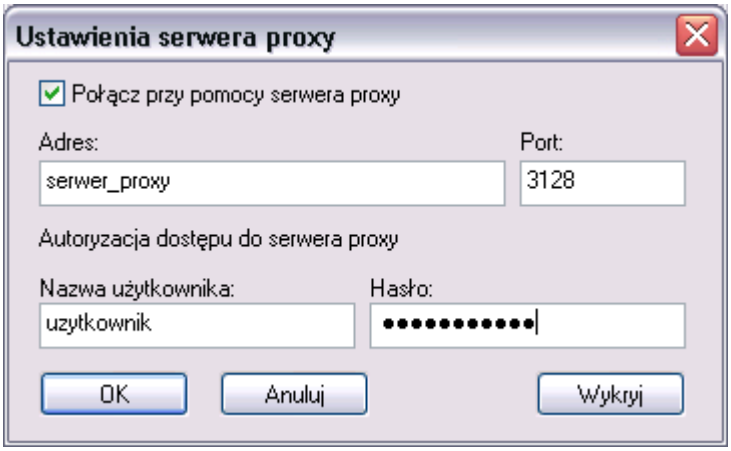
LAN/ stałe łącze – komputer jest podłączony do sieci lokalnej

Modem – połączenie z Internetem odbywa się poprzez modem

Inne – połączenie z Internetem przy pomocy GPRS itp

Serwer proxy

Połączenie komputera z Internetem może odbywać się bezpośrednio lub za pośrednictwem serwera proxy. Ustawienia serwera proxy są dokonywane przez Dostawcę Usług Internetowych (ISP) lub przez administratora sieci.
W przypadku używania serwera proxy wymagane jest skonfigurowanie: nazwy serwera proxy, numeru portu, nazwy użytkownika i hasła aby przeglądarka internetowa (np. Internet Explorer) mogła uzyskać dostęp do Internetu.

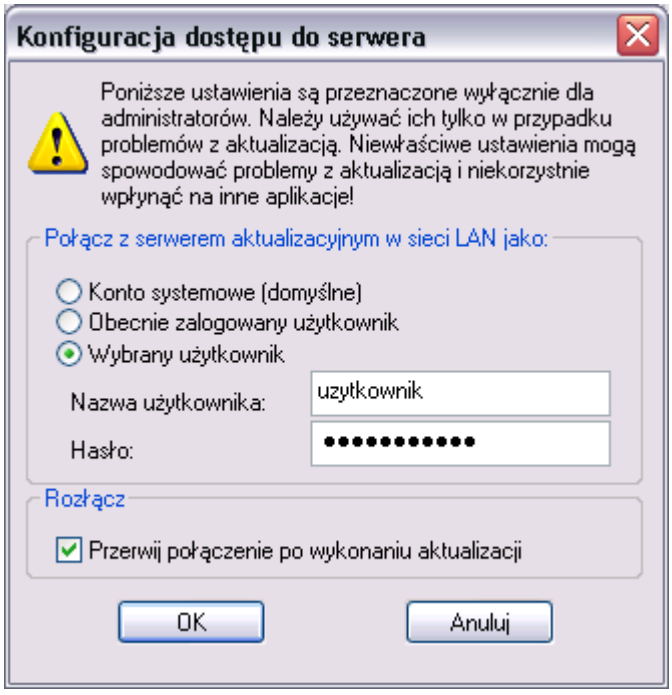


Moduł aktualizacji Systemu NOD32 może pobrać ustawienia serwera proxy bezpośrednio z przeglądarki Internet Explorer. Czasami jednak jest konieczna ręczna konfiguracja serwera proxy, w tym celu należy wybrać opcję „*LAN/ stałe łącze*", kliknąć na przycisk ***Proxy*** w grupie *Serwer proxy, z*aznaczyć opcję „Połącz przy pomocy *serwera proxy"* i wprowadzić adres IP, port serwera proxy (jeśli jest używany) oraz nazwę użytkownika i hasło dostępu do serwera proxy.

UWAGA: Nazwa użytkownika i hasło nie są dostarczane przez Producenta/ Dystrybutora Systemu Antywirusowego NOD32. Zmiany w konfiguracji zatwierdzamy przyciskiem ***OK***.

Serwer aktualizacyjny w sieci LAN

Należy zawsze pamiętać o fakcie, że NOD32 domyślnie pracuje jako użytkownik systemowy, dlatego też nie posiada uprawnień sieciowych zalogowanego użytkownika. W przypadku, gdy aktualizacja dokonywana jest z sieci lokalnej należy wybrać opcję *„Wybrany użytkownik"* i podać nazwę i hasło użytkownika posiadającego dostęp do serwera aktualizacji (Novell NetWare, Windows NT 4.0/ 2000, itp.). W tym przypadku należy również zaznaczyć opcję *„Przerwij połączenie po wykonaniu aktualizacji"*, która spowoduje zamknięcie połączenia i wylogowanie zdefiniowanego użytkownika po wykonaniu aktualizacji.
Jeżeli użytkownik pracujący na konfigurowanym komputerze na stałe posiada uprawnienia do serwera aktualizacji można wybrać opcję *„Obecnie zalogowany użytkownik"*.



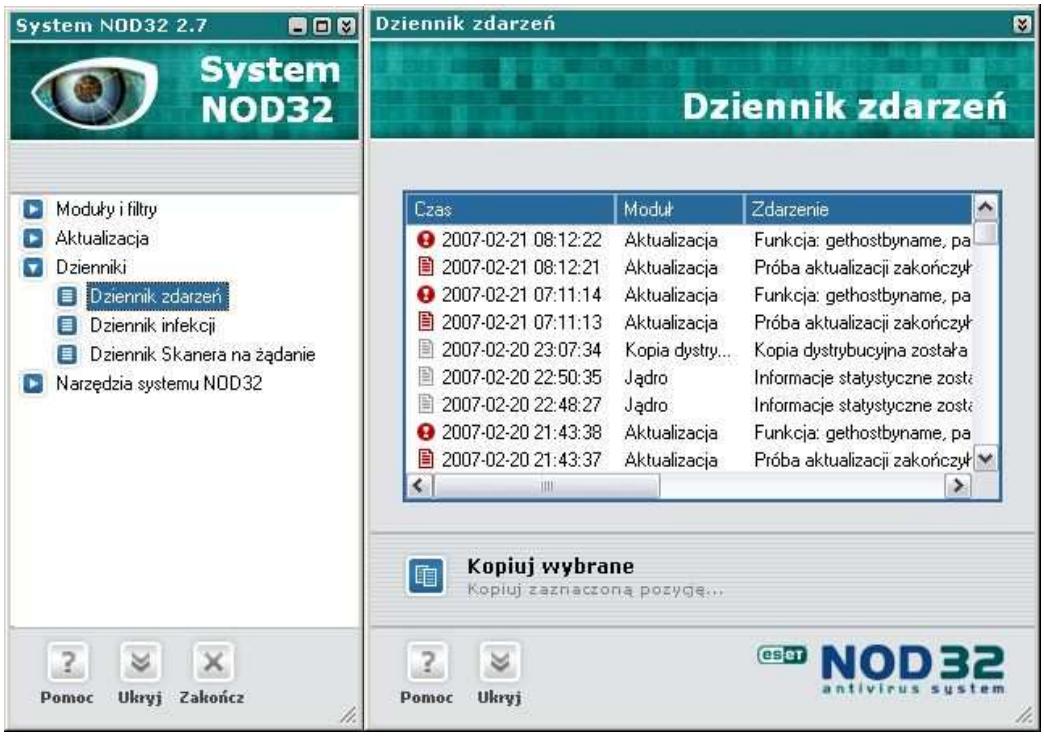
UWAGA: Po zakończeniu procesu konfiguracji wyświetla się okno Aktualizacji. Należy upewnić się, że komputer jest podłączony do Internetu i kliknąć na ikonę

Aktualizuj teraz. System Antywirusowy NOD32 zostanie zaktualizowany lub zostanie wyświetlona informacja: *"Wersja programu NOD32 jest aktualna. Aktualizacja nie jest wymagana"* – oznacza to, że posiadana wersja programu NOD32 jest aktualna.

Dzienniki

Dziennik zdarzeń

Dziennik zdarzeń zawiera informacje o wynikach wszystkich wykonanych procesów i o błędach programu NOD32.
Aby otworzyć okno dziennika zdarzeń w głównym oknie **Systemu NOD32** należy rozwinąć grupę *Dzienniki* i wybrać *Dziennik zdarzeń*.



W głównym oknie znajdują się informacje o zdarzeniach:

Czas – data i czas wystąpienia zdarzenia

Moduł– nazwa modułu, który wygenerował zdarzenie

Zdarzenie – krótki opis zdarzenia, np. *„Baza sygnatur wirusów zaktualizowała się do wersji 1.1150"*

Użytkownik – nazwa zalogowanego użytkownika w momencie wystąpienia zdarzenia

Każde zdarzenie może być skopiowane w celu przesłania go do producenta lub do wsparcia technicznego (support@nod32.pl), w tym celu należy zaznaczyć wybraną pozycję lub kilka pozycji z listy zdarzeń i kliknąć prawym klawiszem myszki na zaznaczonej pozycji. Następnie należy wybrać opcję *„Kopiuj zaznaczone"* z pojawiającego się menu kontekstowego. Można również nacisnąć przycisk ***Kopiuj wybrane***. Informacje przechowywane w schowku mogą być wklejone (kombinacja klawiszy Ctrl–V) do wiadomości i przesłane do wsparcia technicznego.

Menu kontekstowe otrzymywane po kliknięciu prawym klawiszem na wybranych zadaniach zawiera następujące opcje:

Kopiuj wszystkie – kopiuje wszystkie zdarzenia z listy

Kopiuj zaznaczone – kopiuje wybrane zdarzenia z listy

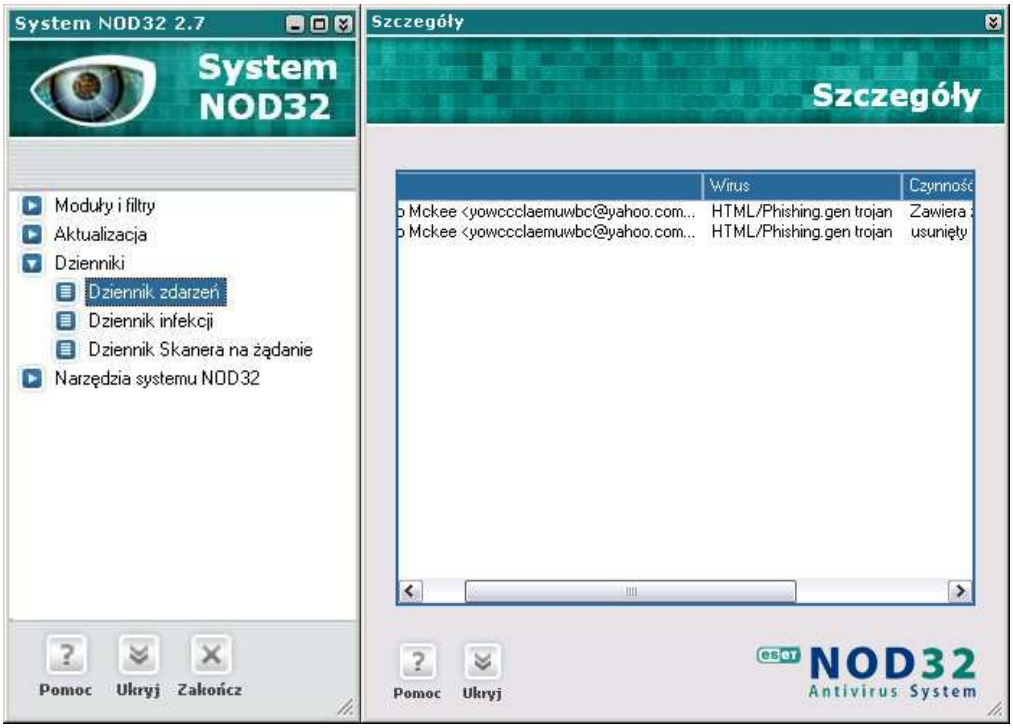
Usuń wybrane – usuwa wybrane zdarzenia z listy

Usuń dziennik – usuwa wszystkie pozycje z Dziennika zdarzeń

Dziennik infekcji

Dziennik infekcji zawiera informacje o wszystkich infekcjach wykrytych przez moduły AMON, IMON, EMON i DMON.

Aby otworzyć okno dziennika infekcji w głównym oknie **Systemu NOD32** należy rozwinąć grupę *Dzienniki* i wybrać *Dziennik infekcji*.



W głównym oknie znajdują się informacje o infekcjach:

Czas – data i czas wystąpienia zdarzenia

Moduł – nazwa modułu, który wygenerował zdarzenie

Obiekt – informacja o typie zainfekowanego obiektu (np. plik, wiadomość pocztowa)

Nazwa – dokładna nazwa zainfekowanego obiektu wraz ze ścieżką dostępu

Wirus – nazwa wirusa

Czynność – opis czynności wykonanej na zainfekowanym pliku (np. wyleczony)

Użytkownik – nazwa zalogowanego użytkownika w momencie wystąpienia infekcji

Informacje – dodatkowe informacje dotyczące infekcji

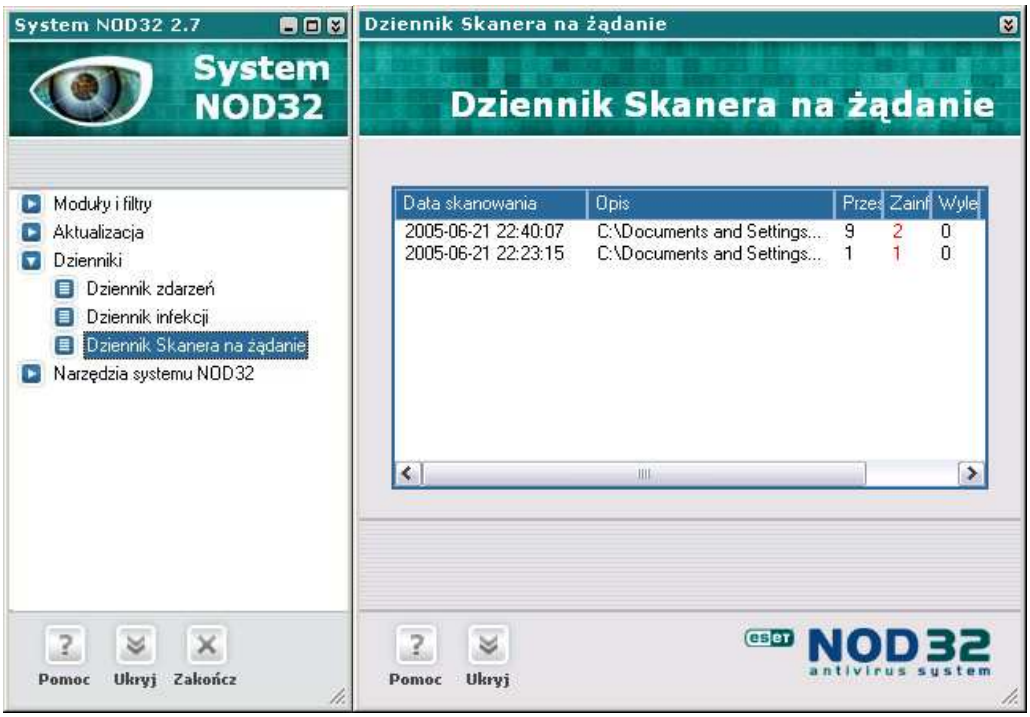
Każde zdarzenie może być skopiowane w celu przesłania go do producenta lub do wsparcia technicznego (support@nod32.pl). W tym celu należy zaznaczyć wybraną pozycję lub kilka pozycji z listy dziennika i kliknąć prawym klawiszem myszki na zaznaczonej pozycji. Następnie należy wybrać opcję *„Kopiuj*

zaznaczone" z pojawiającego się menu kontekstowego. Można również nacisnąć przycisk ***Kopiuj do schowka***. Informacje przechowywane w schowku mogą być wklejone (kombinacja klawiszy Ctrl–V) do wiadomości i przesłane do wsparcia technicznego.

Menu kontekstowe, otrzymywane po kliknięciu prawym klawiszem na wybranych infekcjach, zawiera następujące opcje:
Szczegóły – wyświetla dokładne informacje dotyczące wykrytej infekcji
Kopiuj wszystkie – kopiuje wszystkie zdarzenia z listy
Kopiuj zaznaczone – kopiuje wybrane zdarzenia z listy
Usuń wybrane – usuwa wybrane zdarzenia z listy
Usuń dzienniki – usuwa wszystkie pozycje z dziennika

Dziennik Skanera na żądanie

Dziennik Skanera na żądanie zawiera dokładne raporty skanera na żądanie.
Aby otworzyć okno dziennika skanera w głównym oknie **Systemu NOD32** należy rozwinąć grupę *Dzienniki* i wybrać *Dziennik Skanera na żądanie.*



W głównym oknie znajdują się wszystkie raporty skanowania. Dostępne są następujące informacje:

Data skanowania – data i czas uruchomienia skanera na żądanie

Opis – zawiera dokładne informacje na temat przeskanowanych zasobów, np. c:;d:\test

Przeskanowane – liczba sprawdzonych plików

Zainfekowane – liczba wykrytych infekcji

Wyleczone – liczba wyleczonych plików

Status – status Skanera na żądanie

Status

Dostępne są następujące stany:

zakończone – skanowanie zostało zakończone

przerwane przez użytkownika – proces skanowania został przerwany przez użytkownika

czekaj – skaner na żądanie jest uruchomiony, ale nie został uruchomiony proces skanowania

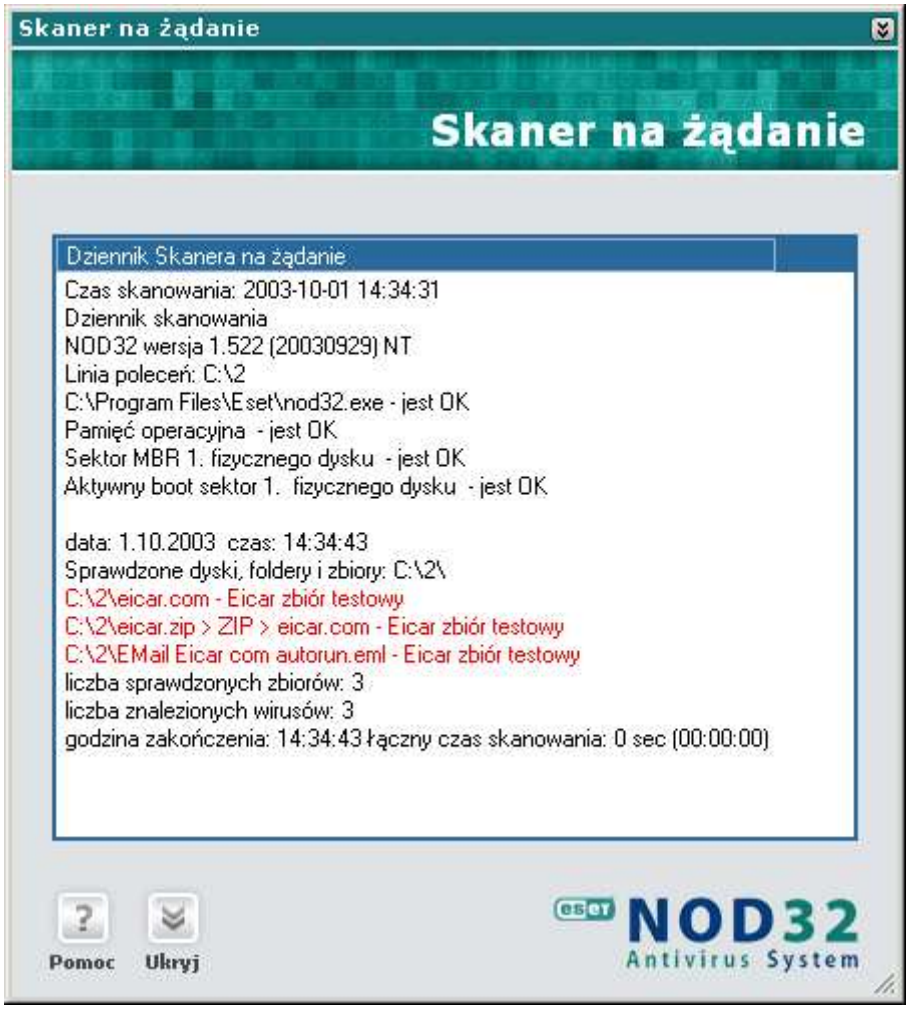
skanowanie – jest uruchomiony proces skanowania zasobów komputera

leczenie – jest uruchomiony proces leczenia zasobów komputera

Menu kontekstowe otrzymywane po kliknięciu prawym klawiszem na wybranych raportach zawiera następujące opcje:

Szczegóły – wyświetla dokładny raport skanowania

Usuń wybrane – usuwa wybrany raport skanowania



Narzędzia Systemu NOD32

Kwarantanna

W wielu przypadkach „zainfekowane" pliki (zwłaszcza robaki i trojany) faktycznie zawierają tylko kod robaka. Leczenie takiego wirusa byłoby jednoznaczne z usunięciem pliku. Nie jest to jednak reguła. Zdarza się bowiem, że zainfekowany plik zawiera ważne dla nas dane. W tym przypadku NOD32 leczy zainfekowane pliki.

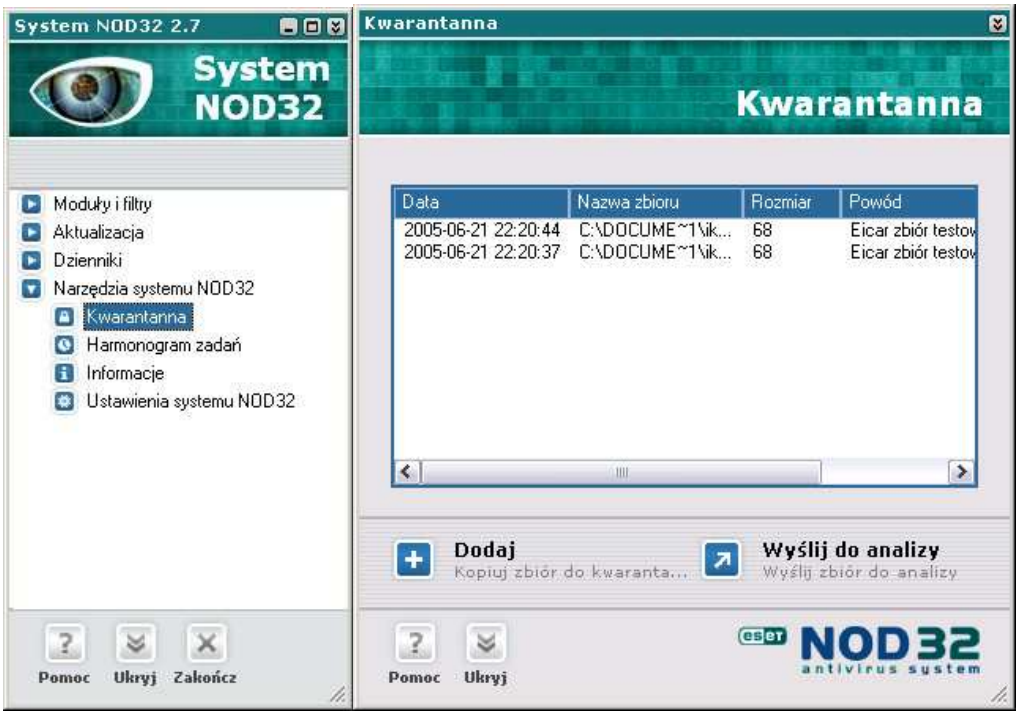
Jeżeli program NOD32 nie potrafi wyleczyć ważnego dla nas pliku można wysłać go do Laboratorium firmy Eset w celu przebadania lub do wsparcia technicznego programu NOD32. W tym celu można kliknąc prawym klawiszem na wybrany wirus w katalogu kwarantanny i wybrać opcje *„Wyślij do analizy"* z dostępnego menu kontekstowego.

Folder *Kwarantanny* jest miejscem, gdzie należy umieścić zainfekowany/ podejrzany plik aby uniknąć dalszego rozprzestrzeniania się wirusa. Umieszczone w *Kwarantannie* pliki są odpowiednio zakodowane aby nie mogły się samoistnie uaktywnić.

Dodatkowo została wprowadzona opcja automatycznego wysyłania nowych wirusów z kwarantanny (wykrytych przy pomocy analizy heurystycznej) do laboratorium firmy ESET.

Lokalizacja Kwarantanny jest ustawiona domyślnie, ale można ją zmienić wpisując odpowiednią ścieżkę dostępu w zakładce Zaawansowane.

Aby otworzyć okno kwarantanny w głównym oknie **Systemu NOD32** należy rozwinąć grupę *„Narzędzia systemu NOD32"* i wybrać moduł *Kwarantanna.*



W głównym oknie Kwarantanny przechowywane są informacje o zainfekowanych plikach:

Data – data i czas uruchomienia skanera na żądanie lub według harmonogramu

Nazwa pliku – dokładna nazwa zainfekowanego obiektu wraz z oryginalną ścieżką dostępu

Rozmiar – rozmiar zainfekowanego pliku

Powód – powód umieszczenia pliku w folderze kwarantanny (np. nazwa wirusa, którym plik jest zainfekowany)

Ilość – podaje ile wirusów tego samego typu znajduje się w kwarantannie

Menu kontekstowe otrzymywane po kliknięciu prawym klawiszem na wybranych pozycjach kwarantanny zawiera następujące opcje:

Dodaj – dodaje wybrany plik do katalogu kwarantanny

Wyślij do analizy – wysyła podejrzany plik do laboratorium firmy ESET

Odtwarzaj – przywraca zainfekowany plik do pierwotnej lokalizacji

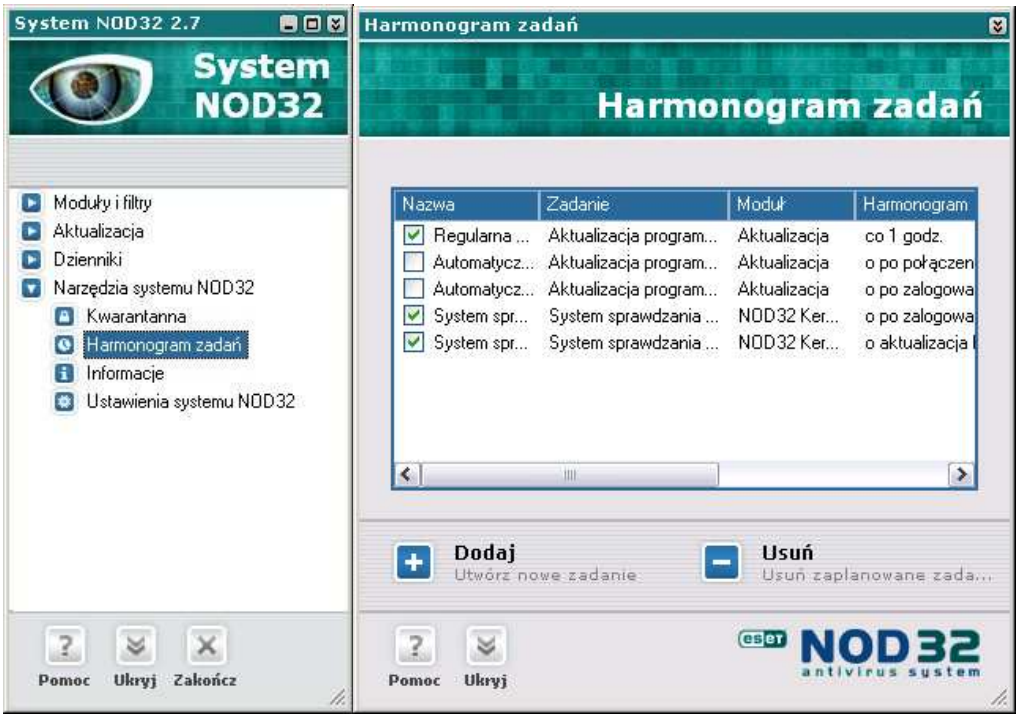
Odtwarzaj do... – zapisuje zainfekowany plik w wybranym folderze na dysku

Usuń – usuwa zainfekowany plik z folderu kwarantanny

Harmonogram zadań

NOD32 posiada wbudowany Harmonogram zadań, który umożliwia nam zarządzanie zadaniami i tworzenie nowych zadań.

Aby otworzyć okno harmonogramu w głównym oknie **Systemu NOD32** należy rozwinąć grupę *Narzędzia systemu NOD32* i wybrać moduł *Harmonogram zadań*.



W trakcie instalacji tworzone są domyślne zadania aktualizacji przez modem i przez sieć lokalną (LAN). Odpowiednio aktywowane jest jedno z nich – w zależności od wyboru sposobu łączenia się z Internetem w trakcie instalacji.

W głównym oknie harmonogramu przechowywane są informacje o wszystkich utworzonych zadaniach:

Nazwa – nazwa zdefiniowanego zadania – powinna być adekwatna do wykonywanego zadania

Zadanie – podaje typ zadnia. Dostępne są następujące typy: aktualizacja NOD32, skaner na żądanie, wykonanie zewnętrznej aplikacji

Moduł – podaje nazwę modułu wykonującego zdefiniowane zadanie

Harmonogram – zawiera informacje o czasie wykonania zdefiniowanego zadania

Specjalne ustawienia – zawiera informacje o używanym profilu, o specjalnych przełącznikach, itp.

Ostatnio aktywowane – data ostatniej aktywacji zadania

Menu kontekstowe, otrzymywane po kliknięciu prawym klawiszem na wybranych pozycjach harmonogramu, zawiera następujące opcje:

Nowe zadanie – wywołuje kreatora nowych zadań

Uruchom teraz – wybranie tej opcji spowoduje natychmiastowe uruchomienie wybranego zadania

Szczegóły – wyświetla dokładny raport dotyczący zadania znajdującego się na liście

Zmień – pozwala na edycję ustawień (np. czasu wykonywania) zadań znajdujących się na liście Harmonogramu

Usuń – usuwa wybrane zadanie

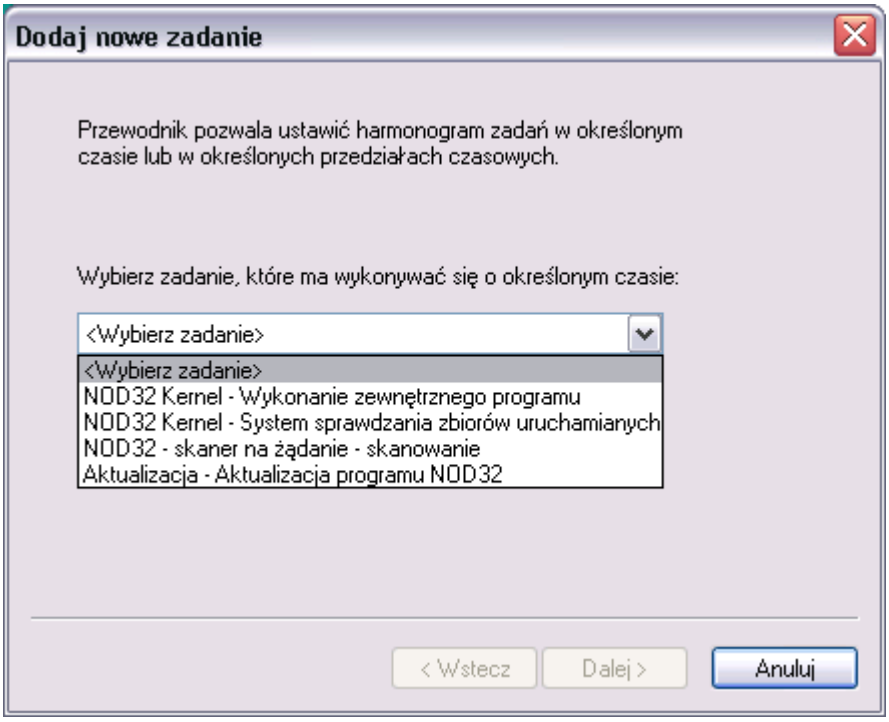
Dodawanie nowych zadań

Aby dodać nowe zadanie do listy zadań *Harmonogramu* należy wybrać opcję **Dadaj zadanie** z menu kontekstowego (prawy klawisz myszki) lub nacisnąć przycisk ***Dodaj*** umieszczony w dolnej części okna. Dostępne są trzy podstawowe zadania:

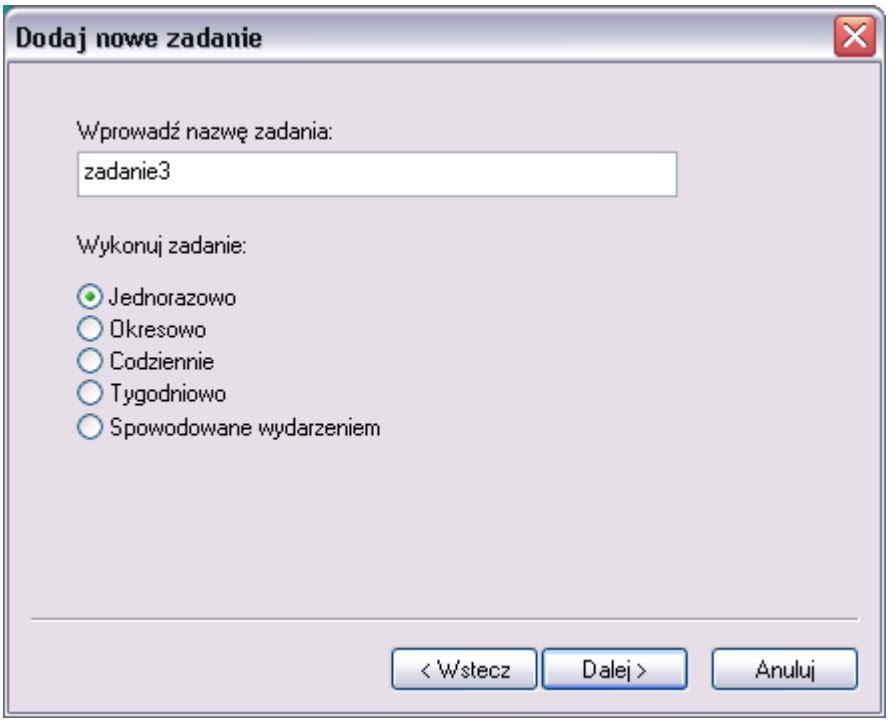
NOD32 Kernel – wykonanie zewnętrznego programu

NOD32 – skaner na żądanie

NOD32 – aktualizacja NOD32



Po wybraniu odpowiedniego zadania z listy dostępnych zadań należy wprowadzić nazwę nowego zadania i wybrać jedną z opcji dotyczących okresu wykonania.



Zadanie może być wykonane:

Jednorazowo – zostanie wykonane tylko raz określonego dnia i o określonej godzinie

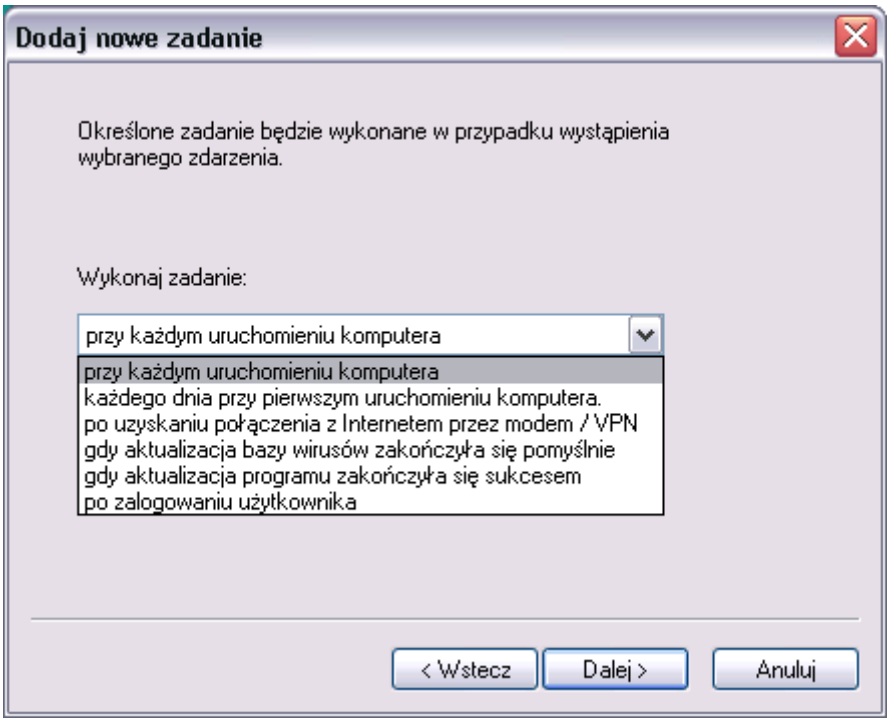
UWAGA: Nie należy wybierać minionej daty i czasu. Aby przywołać kalendarz on–line należy kliknąć na przycisk rozwijania w okienku dialogowym daty.

Okresowo – będzie wykonywane w określonych przedziałach czasowych

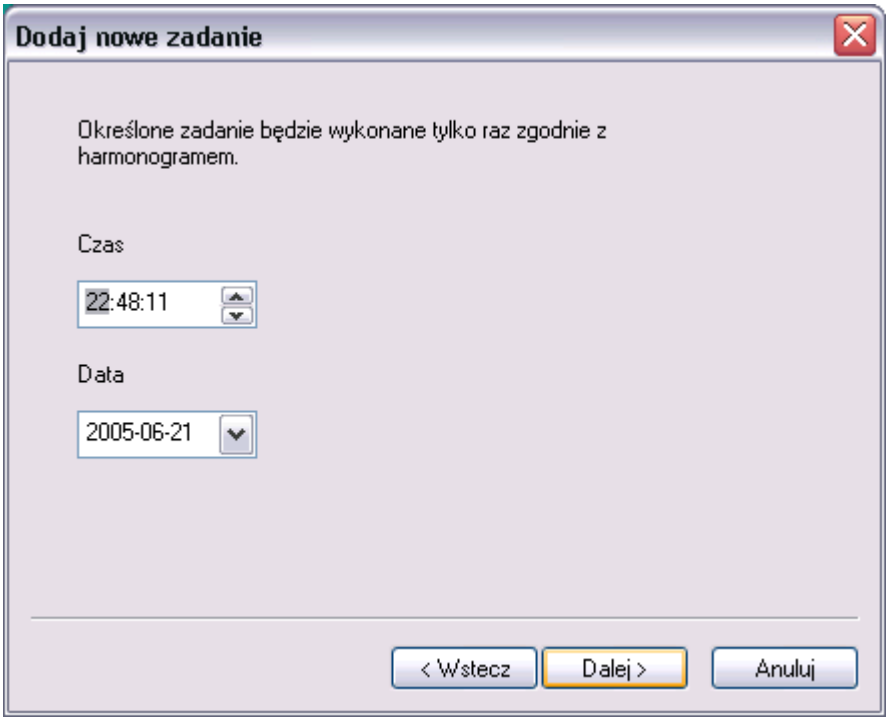
Codziennie – będzie uruchamiane każdego dnia o ustalonej godzinie

Tygodniowo – będzie wykonywane w ustalonych dniach o ustalonej godzinie

Spowodowane wydarzeniem – zostanie wykonane po zajściu ustalonego zdarzenia, np. zostanie uruchomiony skaner na żądanie *„gdy aktualizacja bazy wirusów zakończyła się pomyślnie"*. W tym przypadku można zdefiniować czas co ile ma być wykonywane zadanie, np. nie częściej niż co 24 godziny.



W kolejnym kroku należy określić czas wykonania (odpowiednio do wybranej wcześniej opcji).

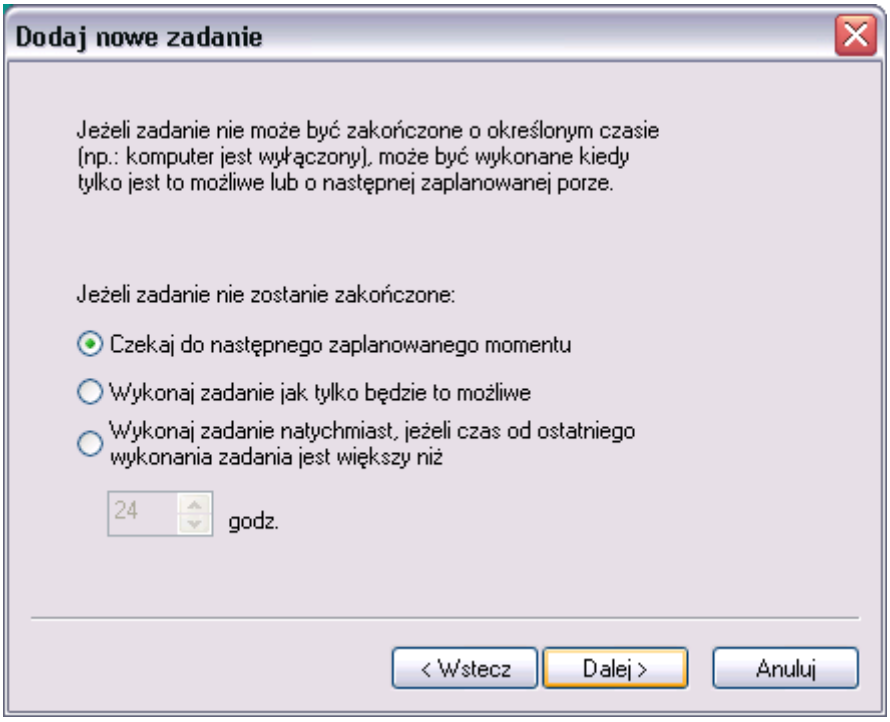


Istnieje możliwość zdefiniowania opcji na wypadek gdyby zadanie nie mogło być wykonane w terminie (komputer był wyłączony lub dostęp do Internetu był zablokowany). Dostępne są trzy opcje:

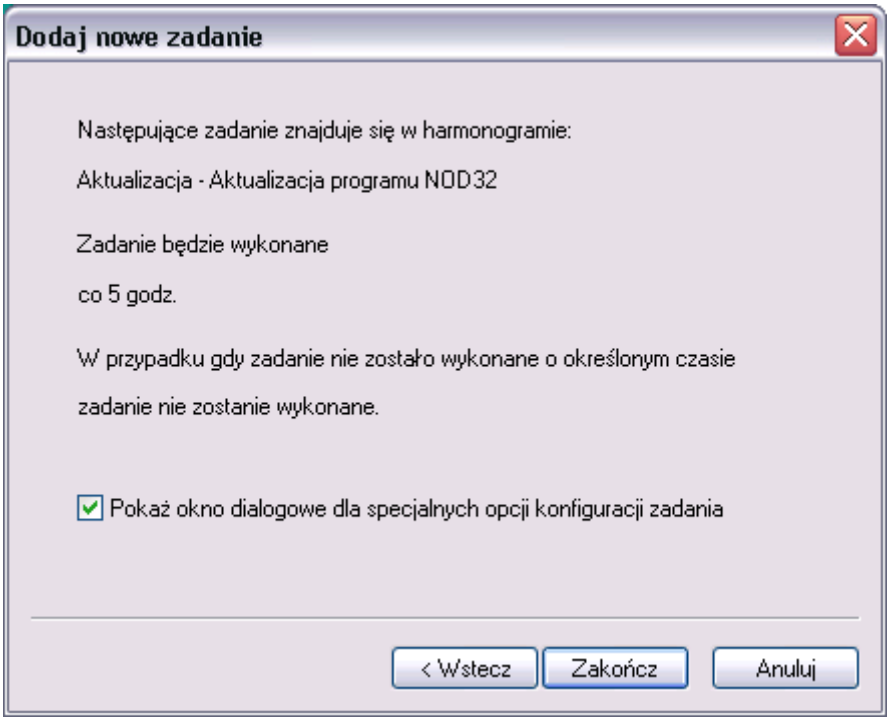
„Czekaj do następnego zaplanowanego momentu"

„Wykonaj zadanie jak tylko będzie to możliwe"

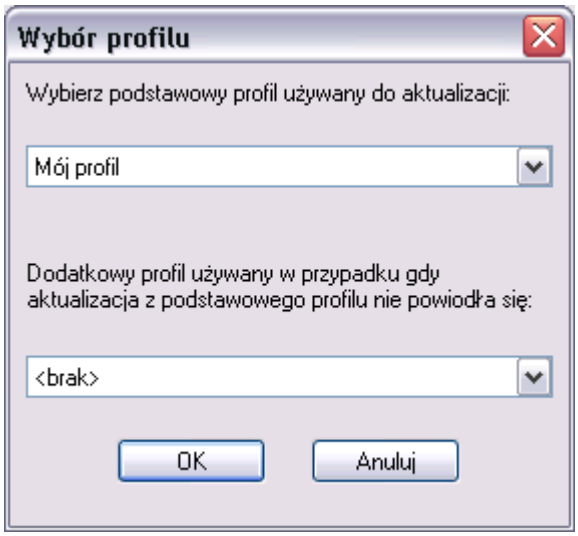
„Wykonaj zadanie natychmiast, jeżeli czas od ostatniego wykonania zadania jest większy niż" – w przypadku wybrania tej opcji należy podać liczbę godzin.



Po ustaleniu wszystkich opcji pojawia się okno podsumowujące tworzone zadanie. Aby zmienić dowolną opcję należy kliknąć na przycisk ***Wstecz,*** aby zatwierdzić należy kliknąć ***Zakończ***.



Wybrane zadania posiadają możliwość określania dodatkowych opcji, np. profili. Aby dokonać dodatkowych ustawień należy zamknąć okno z podsumowaniem i przejść do dalszej konfiguracji.



System NOD32 posiada dwa standardowo wbudowane profile:
Domyślny profil skanowania
Domyślny profil aktualizacji

Najważniejsze ustawienia Domyślnego profilu skanowania to: skanowanie wszystkich dysków oraz domyślne parametry skanowania, metody diagnozowania, czynności w przypadku wykrycia infekcji, itp.)
Podstawowymi cechami Domyślnego profilu aktualizacji jest definicja serwera aktualizacji. Domyślne profile mogą być zmieniane odpowiednio w modułach aktualizacja i Skaner na żądanie, gdzie można również tworzyć własne profile. Więcej informacji na temat profili znajduje się w rozdziałach dotyczących aktualizacji i skanera na żądanie.

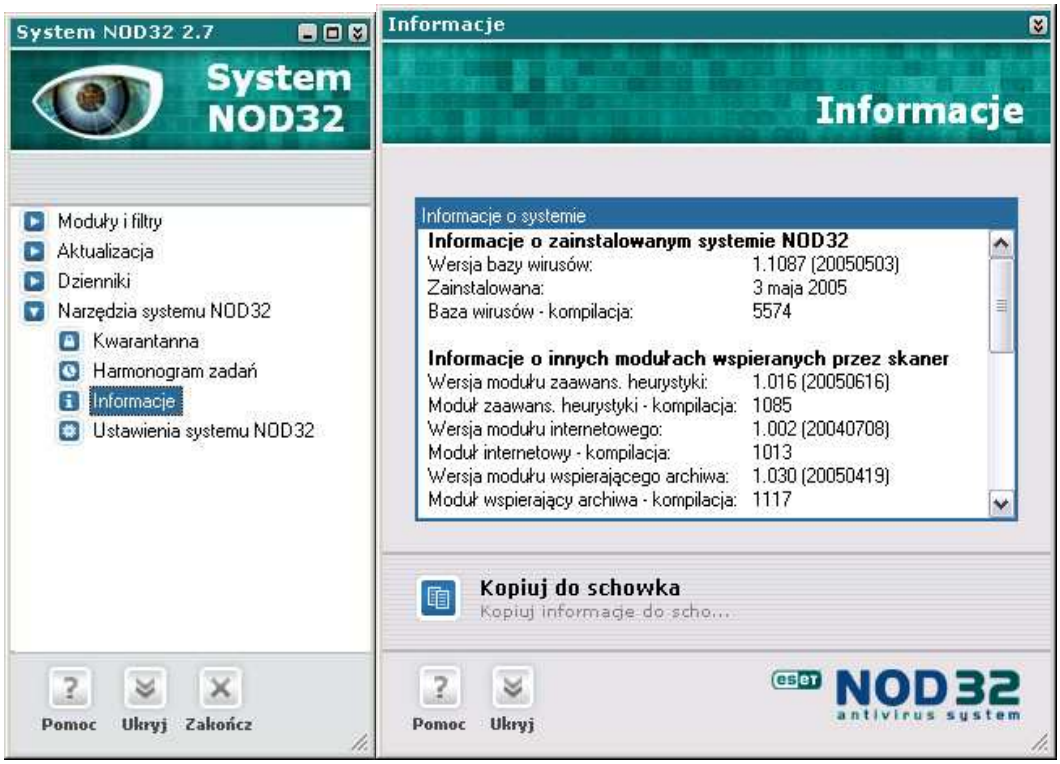
Nowe zadanie pojawia się na liście zaplanowanych zadań. Aby zmodyfikować, usunąć, wykonać wybrane zadanie lub zobaczyć szczegóły dotyczące tego

zadania należy zaznaczyć wybrane zadanie (na liście zadań), kliknąć prawym klawiszem myszki a następnie wybrać odpowiednią opcję z menu kontekstowego.

Informacje

Zakładka *Informacje* zawiera powiązane informacje dotyczące: zainstalowanego systemu NOD32, zainstalowanych komponentów systemu (modułów NOD32) i systemu operacyjnego.

Aby otworzyć okno zawierające informacje, w głównym oknie **Systemu NOD32** należy rozwinąć grupę *Narzędzia systemu NOD32* i wybrać moduł *Informacje*.



Wszystkie informacje zawarte w tej zakładce są ważne w przypadku wystąpienia jakiegokolwiek problemu i potrzeby skorzystania z pomocy technicznej. Przed skontaktowaniem się z pomocą techniczną należy upewnić się czy na komputerze jest zainstalowana najnowsza wersja Systemu NOD32. Większość problemów technicznych wynika z używania nieaktualnych wersji Systemu NOD32.

Aby sprawdzić wersję najnowszej bazy wirusów i wersję Systemu Antywirusowego należy w przeglądarce internetowej wpisać www.nod32.com lub www.nod32.pl

Numer aktualnie dostępnej wersji bazy wirusów systemu NOD32 jest umieszczony na stronie Producenta: www.nod32.com lub stronie Dystrybutora: www.nod32.pl. Należy porównać go z wersją bazy wirusów zainstalowanej na komputerze (**Wersja bazy wirusów**). Jeśli wersje bazy wirusów różnią się należy niezwłocznie uruchomić proces aktualizacji systemu NOD32 i po dokonanej aktualizacji przeskanować zasoby komputera skanerem na żądanie

Wysyłając zgłoszenie problemu do pomocy technicznej należy zawsze umieszczać informacje zawarte w zakładce *Informacje*. Aby umieścić zawartość okna Informacje należy użyć przycisku ***Kopiuj do schowka*** umieszczonego w dolnej części okna.
W tym celu należy:

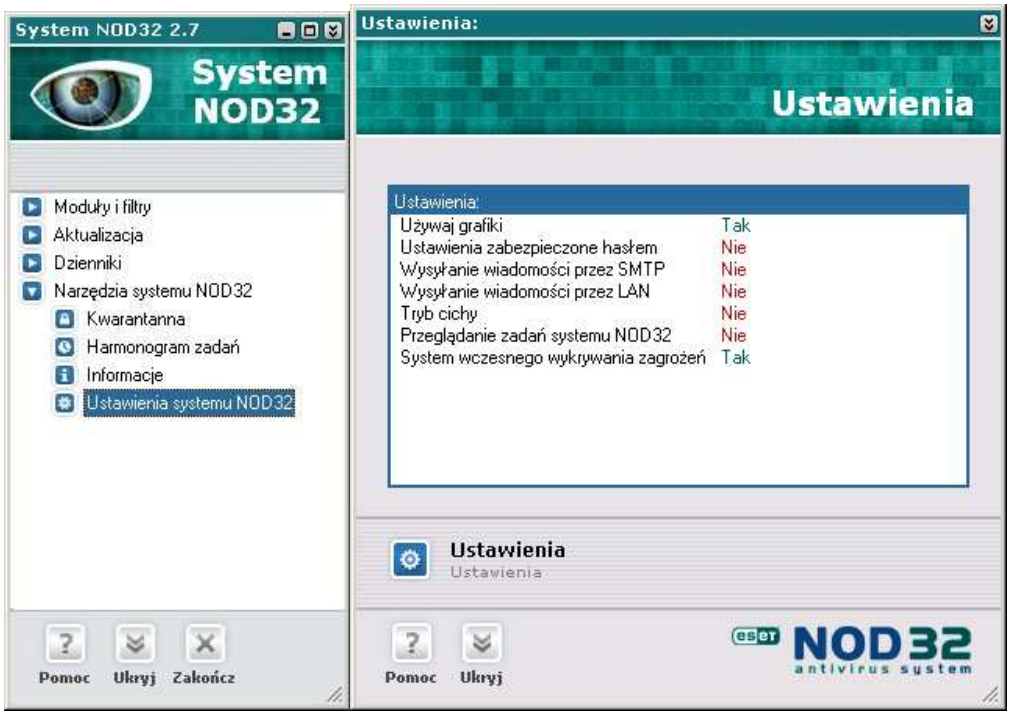
Kliknąć na ikonę ***Kopiuj do schowka*** umieszczoną w dolnej części okna Informacje.

Otworzyć klienta pocztowego i utworzyć nową wiadomość

Umieścić kursor myszki w treści wiadomości i nacisnąć kombinację klawiszy Ctrl+V, aby przekopiować zawartość schowka.

Ustawienia systemu NOD32

Umożliwia konfigurację dodatkowych opcji systemu NOD32: zabezpieczenie hasłem parametrów konfiguracji i możliwości odinstalowania programu NOD32, definiowanie powiadomień, administracja dziennikami, lokalizacja katalogu kwarantanny, itp.
Aby otworzyć okno konfiguracji systemu NOD32, w głównym oknie **Systemu NOD32** należy rozwinąć grupę *Narzędzia systemu NOD32* i wybrać moduł *Ustawienia systemu NOD32*.



Główne okno konfiguracji NOD32 wyświetla podsumowanie dotyczące wybranych opcji:

„Używaj grafiki": NOD32 wspiera wyświetlanie w postaci graficznej lub przy pomocy standardowego systemu graficznego Windows®.

„Ustawienia zabezpieczone hasłem": aby uniknąć nieautoryzowanych zmian, ważne ustawienia Systemu Antywirusowego NOD32 mogą zostać zabezpieczone hasłem.

„Wysyłanie wiadomości przez SMTP": komunikacja systemu NOD32 z użytkownikiem lub administratorem przy pomocy poczty elektronicznej.

„Wysyłanie wiadomości przez LAN": komunikacja systemu NOD32 z użytkownikiem lub administratorem (wysyłanie powiadomień na wybrany komputer w sieci lokalnej) przy pomocy usługi Windows® Messenger

„Tryb Cichy": definiuje typ komunikacji systemu NOD32 z użytkownikiem.

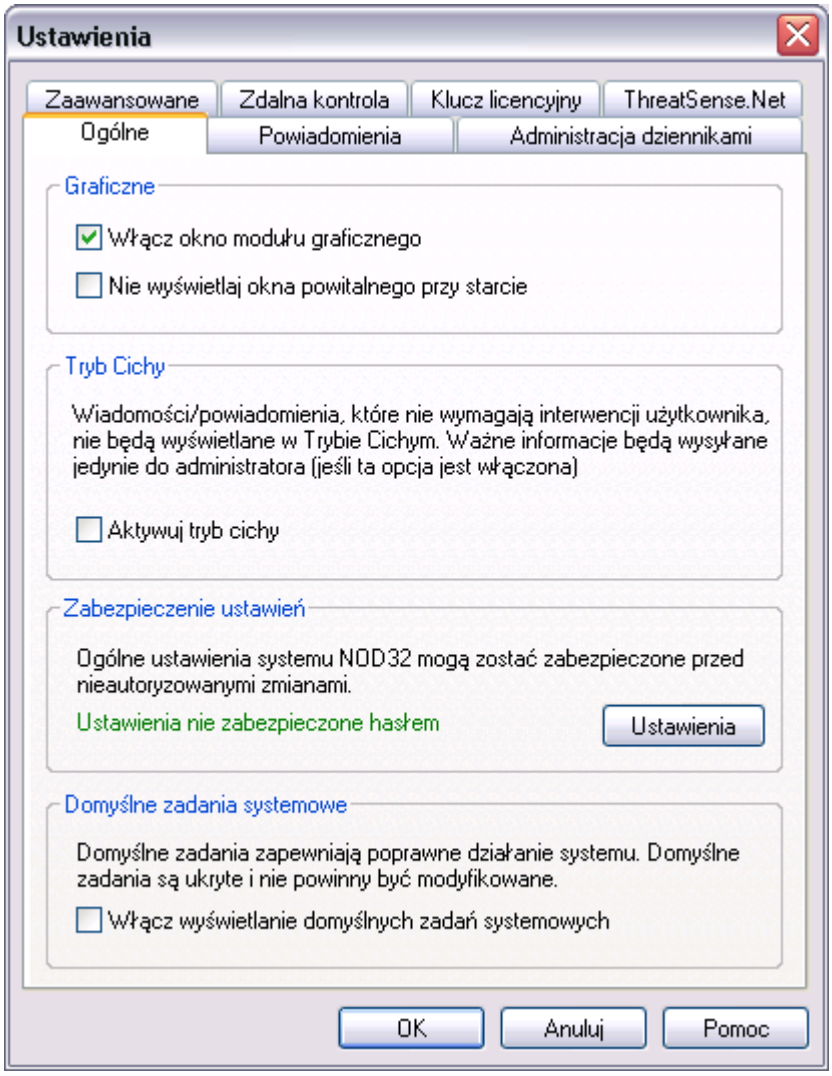
„Przeglądanie zadań systemu NOD32": kontroluje wyświetlanie informacji o domyślnych zadaniach systemu NOD32.

„System wczesnego wykrywania zagrożeń" – ustawienia dotyczące automatycznego wysyłania próbek wirusów do laboratorium

Aby przejść do trybu konfiguracji należy wybrać przycisk ***Ustawienia*** umieszczony w dolnej części okna.

Ogólne

Pierwsza zakładka **Ogólne** pozwala na zmianę opcji dotyczących grafiki, hasła, typu komunikacji systemu NOD32 z użytkownikiem i wyświetlania zadań systemowych. Poniżej zostały opisane poszczególne opcje.



Program NOD32 może być wyświetlany w dwóch trybach. Domyślnie jest używany tryb graficzny (jeżeli tylko komputer wspiera taki tryb). W przeciwnym przypadku używany jest standardowy tryb systemu Windows.

Aby wyłączyć okno powitalne należy zaznaczyć opcję: *„Nie wyświetlaj okna powitalnego przy starcie”*.

Aby uniknąć wyświetlania nieistotnych (dla przeciętnego użytkownika) informacji można aktywować *Tryb Cichy*. W tym trybie wyświetlane będą jedynie informacje o wirusach wykrytych przez monitor antywirusowy AMON i monitory poczty IMON/ EMON. *Tryb Cichy* wpływa również na redukcję ruchu w sieci (generowanego przez użytkowników).

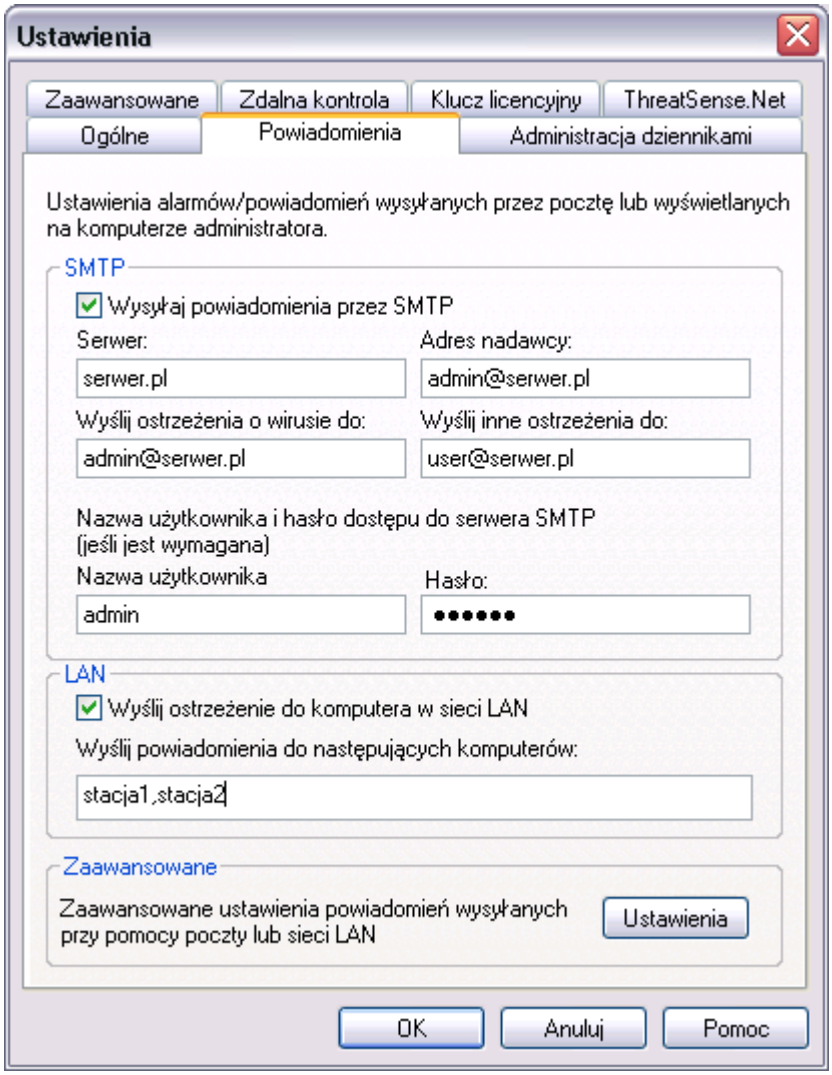
Aby zabezpieczyć parametry konfiguracyjne systemu NOD32 przed nieautoryzowaną modyfikacją, możliwością wyłączenia monitorów AMON/ EMON/ IMON i odinstalowania systemu NOD32 należy ustawić hasło zabezpieczające. W tym celu należy wybrać przycisk ***Konfiguracja...*** i wprowadzić hasło. Hasło należy przechowywać w bezpiecznym miejscu.

Aby usunąć hasło zabezpieczające należy wybrać przycisk ***Bez hasła***.

Domyślne zadania systemowe zapewniają poprawne działanie systemu. Przykładem systemowego zadania jest administracja dziennikami uruchamiana z Harmonogramu zadań.

Powiadomienia

Zakładka **Powiadomienia** jest używana do konfigurowania komunikacji między systemem NOD32 a zdalnym użytkownikiem lub administratorem systemu.



Wyszczególnione są dwa rodzaje powiadomień, które mogą być wysyłane zdalnie:
Ostrzeżenia o infekcjach (wirusach)
Powiadomienia o pozostałych zdarzeniach

Możemy użyć dwóch alternatywnych sposobów wysyłania powiadomień:
SMTP (poczta e–mail)
LAN (usługa posłaniec)

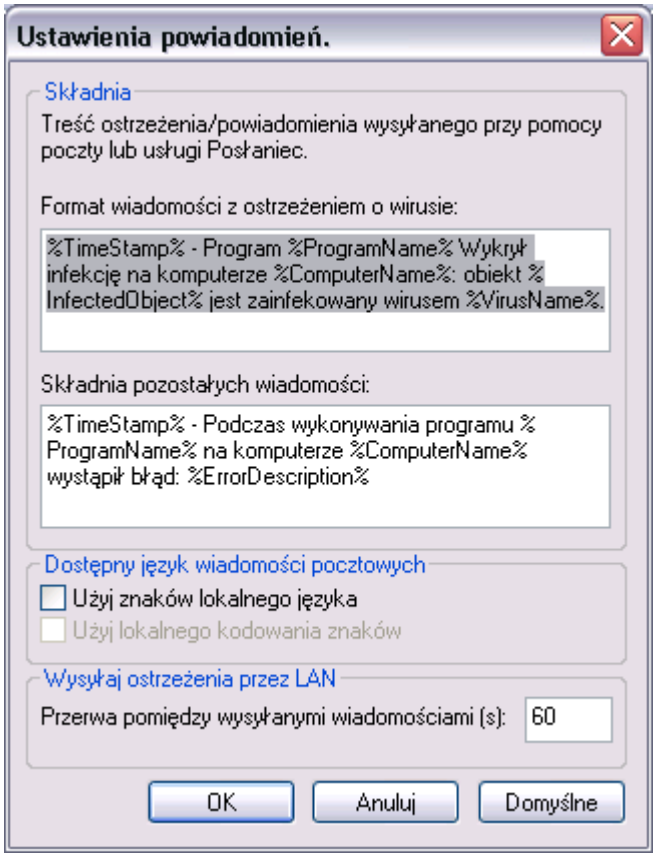
Aby zdefiniować wysyłanie powiadomień przy pomocy poczty elektronicznej należy zaznaczyć opcję *„Wysyłaj powiadomienia przez SMTP",* a następnie wprowadzić nazwę serwera pocztowego. W kolejnym kroku należy podać adres nadawcy wiadomości (np. admin@serwer.pl), adres odbiorcy (odbiorców) wiadomości z ostrzeżeniem o wirusie i adres odbiorcy (odbiorców) wiadomości z pozostałymi ostrzeżeniami (np. problem z wykonaniem automatycznej aktualizacji).

UWAGA: Istnieje możliwość określenia więcej niż jednego adresu odbiorcy. W tym celu należy wprowadzić kolejno adresy oddzielając je znakiem średnika (;).

W przypadku, gdy serwer pocztowy wymaga uwierzytelnienia należy wprowadzić również nazwę użytkownika i hasło w odpowiednie pola.

Aby wysłać wiadomość przy pomocy usługi Posłaniec w sieci LAN należy zaznaczyć opcję *„Wyślij ostrzeżenie do komputera w sieci LAN"* i wprowadzić nazwy komputerów, które będą otrzymywać wiadomości.

Dodatkowo istnieje możliwość zdefiniowania treści wysyłanych wiadomości. W tym celu należy kliknąć na przycisk ***Ustawienia,*** umieszczony w grupie *Zaawansowane*.



Alerty wirusowe i powiadomienia generowane przez system NOD32 posiadają domyślny format, który został zoptymalizowany dla większości sytuacji (zawiera specjalne słowa kluczowe). Jednak w pewnych okolicznościach zachodzi konieczność zmiany treści powiadomienia. Wszystkie słowa kluczowe są poprzedzone znakiem procentu (%) i w trakcie generowania wiadomości są zastępowane np. oryginalną nazwą wirusa, nazwą zainfekowanego pliku, itp. Dostępne są następujące słowa kluczowe:

%TimeStamp% – data i czas zdarzenia

%ProgramName% – nazwa modułu, który wygenerował powiadomienie/ alert

%ComputerName% – nazwa NetBIOS–owa komputera, na którym wystąpiło zdarzenie

%InfectedObject% – nazwa zainfekowanego pliku, wiadomości itp.

%VirusName% – identyfikacja infekcji

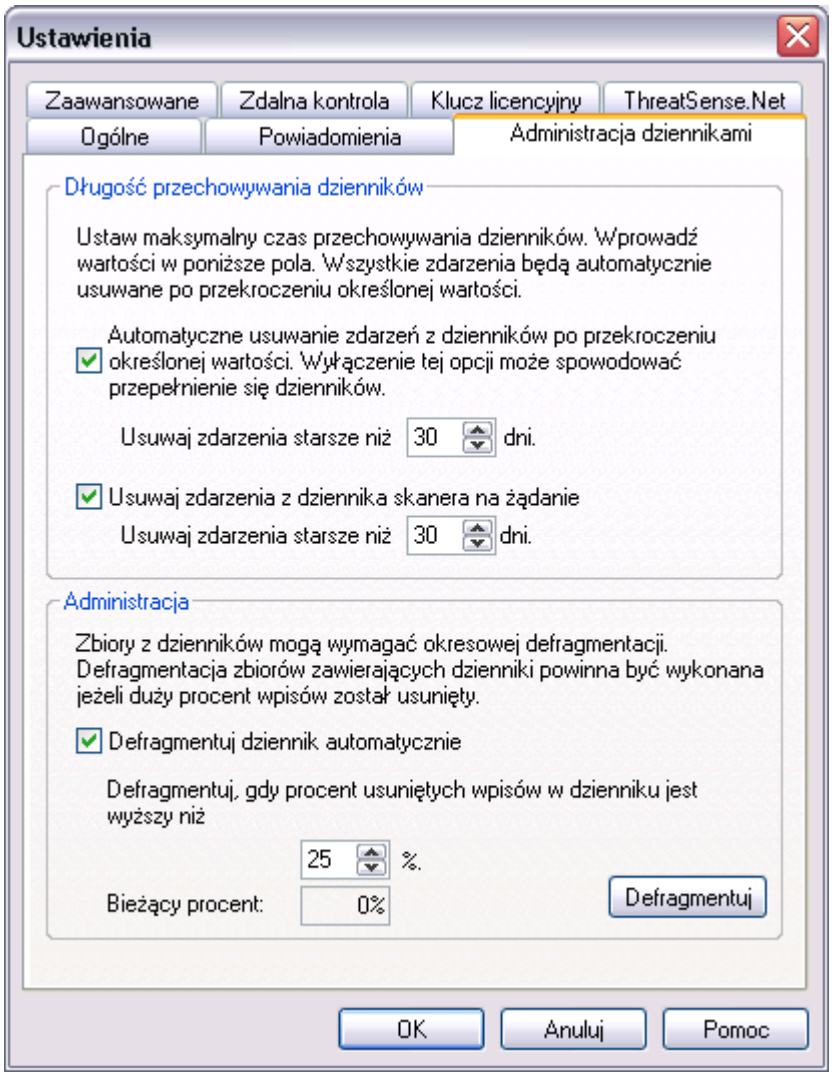
%ErrorDescription% – opis zdarzenia nie związanego z infekcją

Aby zresetować zmodyfikowany format wiadomości i powrócić do domyślnych fabrycznych ustawień należy kliknąć na przycisk ***Domyślne***.

Aby zmienić domyślną częstotliwość wysyłania wiadomości przez LAN należy wpisać nową wartość (w sekundach) w polu *„Przerwa pomiędzy wysyłanymi wiadomościami (s):”*.

Administracja dziennikami

Bardzo istotną cechą programu NOD32 jest możliwość generowania plików z zapisami dzienników. Jednak niewłaściwy sposób administrowania *Dziennikami* może spowodować przepełnienie dysku. Aby uniknąć tej sytuacji należy w zakładce Administracja dziennikami zdefiniować długość przechowywania zdarzeń w dziennikach. Zalecane jest przechowywanie wpisów nie dłużej niż przez 30 dni.



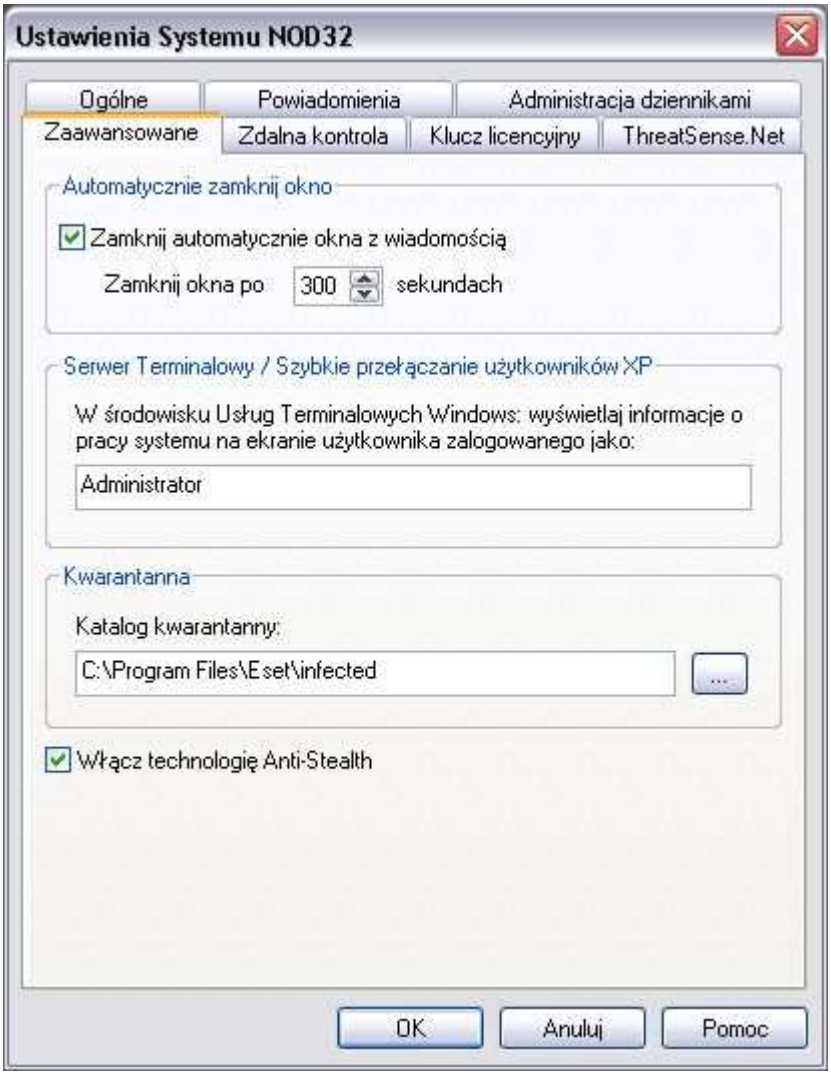
Sekcja *Długość przechowywania dzienników* zawiera dwie opcje wyboru. Pierwsza dotyczy usuwania wpisów z dziennika dotyczących wszystkich zdarzeń tj. aktualizacji baz wirusów, aktualizacji programu, infekcji wykrytych przez monitory i filtry antywirusowe. Druga opcja dotyczy jedynie wpisów dokonywanych przez Skaner na żądanie. W jednym i drugim przypadku możemy ustawić dowolny czas (liczony w dniach).

Sekcja *Administracja* zawiera ustawienia dotyczące automatycznego defragmentowania dzienników. Defragmentowanie dzienników w przypadku usunięcia więcej niż 25% wpisów powoduje zmniejszenie zajętości dysku i szybszy dostęp do pozostałych informacji. Zalecane jest pozostawienie domyślnych ustawień.

Aby uruchomić defragmentację ręcznie należy wybrać przycisk ***Defragmentuj***.

Zaawansowane

Zakładka Zaawansowane pozwala na skonfigurowanie dodatkowych opcji Systemu NOD32.



„Zamknij automatycznie okna z wiadomością" – automatycznie zamyka okna z wiadomościami wysyłanymi przez program antywirusowy (po upływie określonego czasu). Należy zaznaczyć odpowiednią opcję i określić przedział czasowy.

"*Serwer Terminalowy / Szybkie przełączanie użytkowników XP"* – wiadomość ostrzegawcza jest wysyłana do użytkownika, którego działania spowodowały błąd

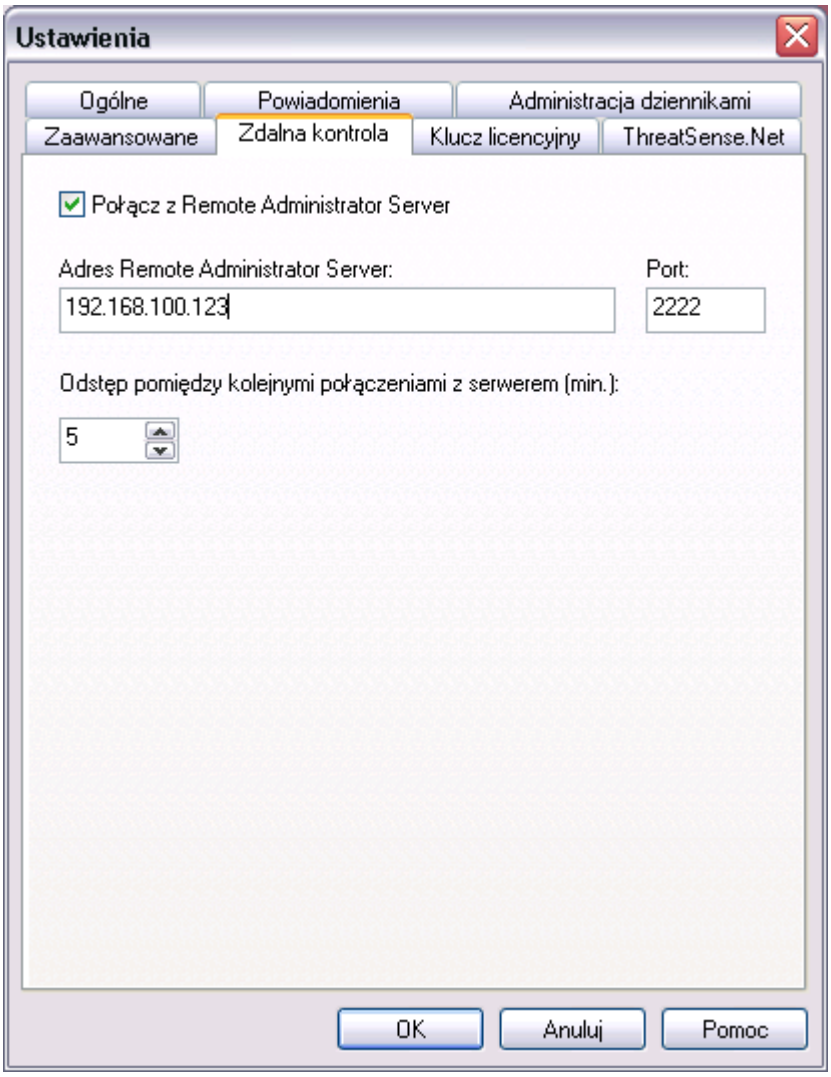
lub infekcję. W przypadku, gdy użytkownik nie może być określony (akcja powodująca wysłanie wiadomości została wywołana przez system), wiadomość zostanie wysłana do zdefiniowanego użytkownika np. do Administratora.

"*Katalog kwarantanny*" – wszystkie zainfekowane lub potencjalnie zainfekowane pliki są zapisywane w tym katalogu w postaci zakodowanej (aby uniknąć dalszej infekcji). Opcja zapisywania zainfekowanych plików w katalogu kwarantanny przez różne moduły programu NOD32 musi być określona podczas procesu konfiguracji każdego odrębnego modułu.

"*Włącz technologie Anti-stealth*" – technologia Anti-Stealth służy do eliminowania aktywnych , zagnieżdżonych w systemie rootkitów

Zdalna kontrola

Zakładka Zdalna kontrola pozwala na określenie parametrów połączenia ze serwerem *Remote Administration Server (RA)*.



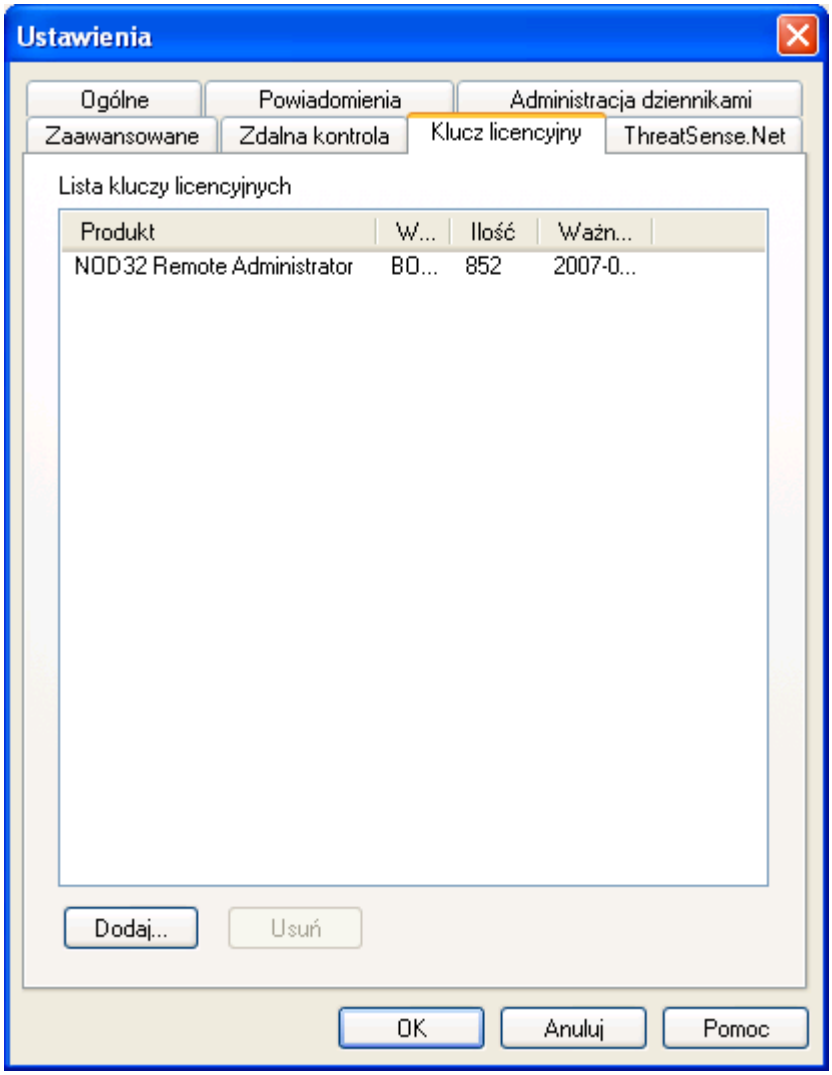
Jeśli w sieci lokalnej znajduje się serwer zdalnej kontroli RA należy włączyć opcję *„Połącz z Remote Administrator Server"* i wprowadzić nazwę serwera lub jego adres IP. Istnieje również możliwość zdefiniowania czasu po jakim nastąpi komunikacja między stacją a serwerem.

Klucz licencyjny

Zakładka Klucz licencyjny umożliwia zarządzanie kluczami dla innych produktów takich jak Remote Administrator, NOD32 for Kerio Mail Server, NOD32 for Kerio

Winroute Firewall, etc. Zakładka zawiera listę używanych kluczy oraz informacje o nazwie produktu, nazwie właściciela, liczbie licencji i dacie ważności.

Aby dodać lub usunąć klucz należy wybrać odpowiedni przycisk.



ThreatSense.Net

Zadaniem systemu wczesnego wykrywania zagrożeń ThreatSense.Net jest udoskonalenie oferowanej ochrony antywirusowej. Dzięki włączeniu i używaniu tego systemu przez użytkowników programu NOD32, firma Eset (producent

programu NOD32) jest w stanie dowiedzieć się o nowych zagrożeniach jak tylko się pojawiają. TreatSence.Net silnie współpracuje z heurystyką dostarczając im wszystkie nowe zagrożenia, dzięki czemu możemy w rekordowym tempie przygotować odpowiednią szczepionkę.
Istnieją dwie możliwości:

1. Wyłączenie systemu wczesnego wykrywania zagrożeń. Użytkownik nie traci na funkcjonalności programu NOD32, który zapewnia najlepszą ochronę przed wszelkimi zagrożeniami.
2. Włączenie systemu wczesnego wykrywania zagrożeń. W tym przypadku będą zbierane statystyki i próbki nowych wirusów, które następnie program sam automatycznie prześle do laboratorium firmy Eset w celu przeprowadzenia dokładnej analizy. System wczesnego ostrzegania (ThreatSense.Net) zbiera informacje o komputerze dotyczące nowych zagrożeń, zawierające próbkę nowego wirusa lub kopię zainfekowanego pliku, ścieżkę dostępu do zainfekowanego pliku, jego nazwę, informację o czasie i dacie utworzenia, nazwę procesu, który utworzył zainfekowany plik, dane dotyczące systemu operacyjnego. Niektóre z tych informacji mogą zawierać dane poufne o użytkowniku i komputerze, np. nazwa użytkownika w ścieżce dostępu. Przykład pliku z informacją przesyłaną do laboratorium jest dostępny tutaj.

Ponieważ istnieje możliwość, że czasem mogą zostać ujawnione informacje o użytkowniku lub jego komputerze, laboratorium firmy Eset zapewnia, że nie zależy im na gromadzeniu tych informacji do żadnych innych celów tylko do przygotowania odpowiedzi na nowe zagrożenia w możliwie najkrótszym czasie. Wszystkie otrzymane dane są traktowane bardzo poważnie i nie są udostępniane osobom trzecim.

Domyślnie NOD32 jest skonfigurowany w taki sposób aby pytał przed każdym wysłaniem podejrzanego pliku do laboratorium firmy Eset. Dodatkowo pliki zawierające rozszerzenia .doc lub .xls są zawsze wyłączone z wysyłana do laboratorium, ponieważ mogą zawierać poufne informacje o firmie. Użytkownik

może zdefiniować własną listę rozszerzeń wyłączonych z wysyłania do laboratorium. Pliki z tymi rozszerzeniami nie będą raportowane.

Mamy nadzieję, że technologia wczesnego wykrywania zagrożeń (ThreatSense.Net) umożliwi lepszą ochronę i uczyni Internet jeszcze bezpieczniejszym miejscem.

Ustawienia systemu wczesnego wykrywania zagrożeń (TreatSense.Net) – podejrzane pliki

W pierwszej zakładce **Podejrzane pliki** można zdefiniować kiedy i które podejrzane pliki będą wysyłane do laboratorium w celu przeprowadzenia dalszej analizy. Dostępne są następujące opcje:

„Nie wysyłaj" - próbki nigdy nie będą wysyłane do dalszej analizy. Jedynie, gdy ustawione jest wyświetlanie powiadomień z możliwością wyboru czynności w przypadku wykrycia wirusa, możemy wysłać próbkę do laboratorium klikając na przycisk wyślij do analizy .

„Pytaj przed wysłaniem" - podejrzane pliki będą kolekcjonowane i program NOD32 będzie pytać przed ich wysłaniem do laboratorium.

„Wyślij bez pytania" - każdy podejrzany plik będzie wysyłany automatycznie bez informowania o tym użytkownika.

UWAGA: Po wyłączeniu systemu wczesnego wykrywania zagrożeń (ThreatSense.Net), pliki zatwierdzone wcześniej do wysłania mogą być nadal wysłane w późniejszym terminie (zależy to od ustawień dotyczących czasu wysyłania podejrzanych plików).

Przykład wysyłanych informacji do laboratorium firmy ESET:

```
# utc_time=2005-04-14 07:21:28
# country="Polska"
# language="POLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1463[1].exe
```

Dodatkowo Zgłoszenie może być wysłane:

„Natychmiast" - w tym przypadku, podejrzane pliki będą wysyłane natychmiast lub jeśli będzie to możliwe (opcja zalecana jeśli dysponujemy stałym połączeniem z Internetem)

„Podczas aktualizacji" - NOD32 będzie kolekcjonować wszystkie podejrzane pliki, które zostaną wysłane podczas kolejnej aktualizacji programu (opcja zalecana w przypadku połączenia modemowego)

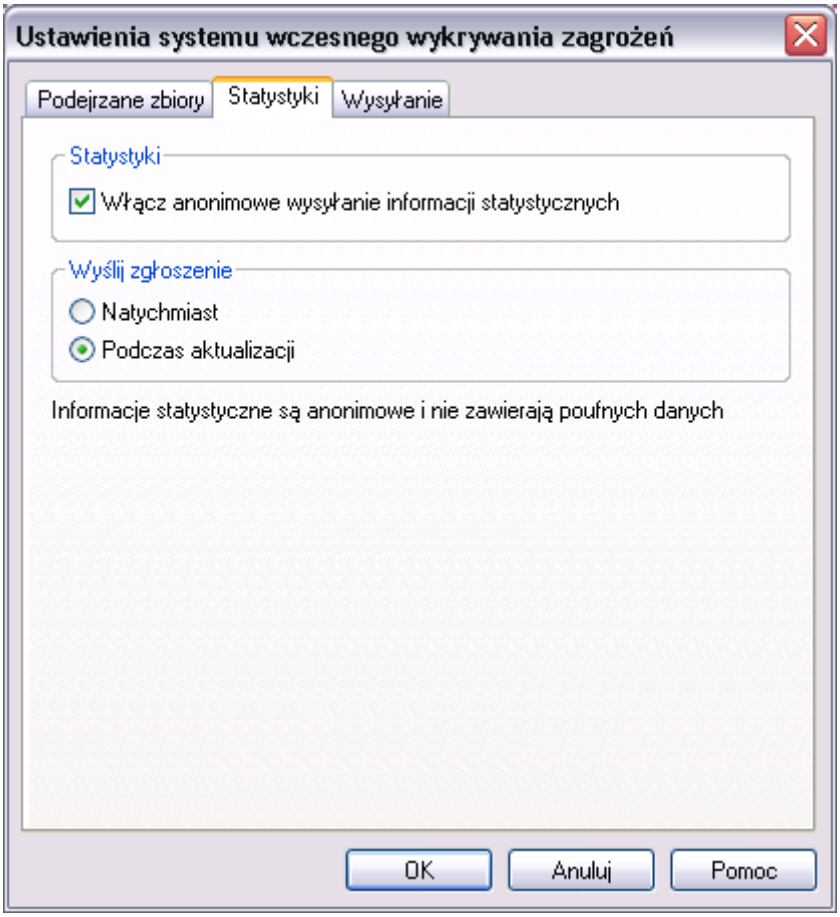
Monitor wyłączeń umożliwia wyłączenie pewnych plików i folderów. Pliki i foldery znajdujące się na liście nie będą wysyłane do laboratorium, nawet jeśli zawierają podejrzany kod. Funkcja ta umożliwia ochronę poufnych informacji takich jak dokumenty lub bazy danych. Najbardziej popularne typy plików, które mogą zawierać poufne informacje już znajdują się na liście.

Aby dodać plik/ folder należy wybrać przycisk ***Dodaj*** , który umożliwia wprowadzenie nazwy lub ścieżki dostępu do pliku lub folderu. Można używać znaków specjalnych aby dodać grupę plików. Znak pytajnika (?) reprezentuje jeden dowolny znak podczas gdy gwiazdka (*) reprezentuje dowolny ciąg znaków. Np. wpis *.TXT oznacza wyłączenie ze skanowania wszystkich plików tekstowych (z dowolna nazwą).

Przycisk ***Zmień*** - Umożliwia edycję wybranej pozycji z listy wyjątków
Przycisk ***Usuń*** - usuwa wybraną pozycję z listy wyjątków

Adres zwrotny - jest przesyłany wraz z próbką wirusa do firmy ESET. Podanie adresu zwrotnego jest opcjonalne. Firma Eset odpowiada na wiadomości, w przypadku gdy potrzebne są dodatkowe informacje dotyczące wykrytego zagrożenia.

Ustawienia systemu wczesnego wykrywania zagrożeń (TreatSense.Net) – statystyki



System wczesnego wykrywania zagrożeń (ThreatSense.Net) zbiera anonimowe informacje o komputerze dotyczące nowych zagrożeń, które zawierają: nazwę zainfekowanego pliku, informację o dacie i czasie wykrycia wirusa, wersji programu NOD32 i informacje o systemie operacyjnym i ustawień lokalnych. Statystyki są dostarczane do laboratorium firmy Eset raz lub dwa razy dziennie.

Zaleca się włączenie opcji włącz anonimowe wysyłanie informacji statystycznych. Przykład danych statystycznych wysyłanych do laboratorium firmy ESET”

```
# version=1
# utc_time=2005-04-02 19:46:50
# local_time=2005-04-02 21:46:50 (+0100, Central Europe Standard Time)
# utc_time_from=2005-04-02 18:59:11
# utc_time_to=2005-04-02 19:46:50
```

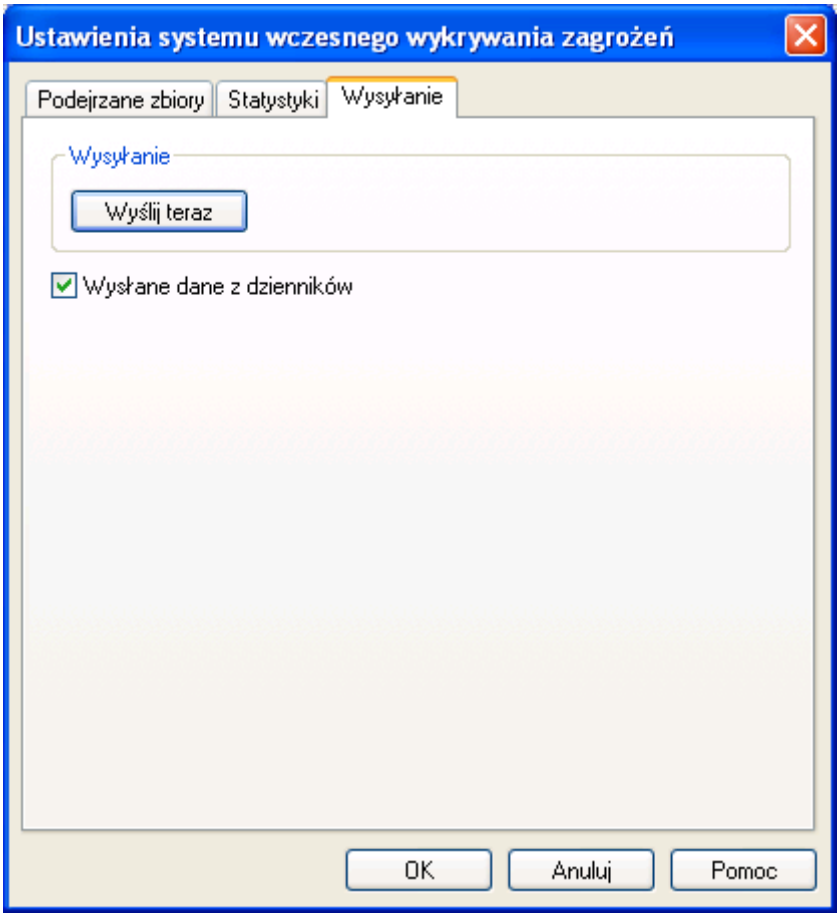
```
# country="Polska"
# language="POLSKI"
# osver=5.1.2600 NT Service Pack 2
# engine=5417
# components=2.50.2
2005-04-02 18: moduleid=4e4f4d41 virus="~OK" count=426
2005-04-02 18: moduleid=484f4d49 virus="~OK" count=1
2005-04-02 19: moduleid=4e4f4d41
virus="@INFECT=inf@TYPE=Trojan@NAME=Win32/TrojanDownloader.Small.NB
X@CLN=BAA" count=2
2005-04-02 19: moduleid=4e4f4d41 virus="~OK" count=2202
2005-04-02 19: moduleid=484f4d49 virus="~OK" count=482
```

Użytkownik może podjąć decyzję, kiedy będą wysyłane pakiety statystyczne do laboratorium firmy ESET. Istnieją dwie możliwości:

„Natychmiast” - po wybraniu tej opcji dane statystyczne będą wysyłane od razu, zaraz o ich utworzeniu (opcja zalecana w przypadku posiadania stałego łącza internetowego)

„Podczas aktualizacji” - w tym przypadku wszystkie dane statystyczne będą kolekcjonowane i wysyłane podczas kolejnej aktualizacji (zalecane w przypadku połączenia modemowego).

Ustawienia systemu wczesnego wykrywania zagrożeń (TreatSense.Net) – wysyłanie



Zakładka **Wysyłanie** umożliwia wymuszenie wysłania podejrzanego pliku do laboratorium oraz włączenie zapisywania wszystkich wysłanych danych w dziennikach zdarzeń.

„Wyślij teraz" - wymusza wysłanie podejrzanych plików i pakietów statystycznych, które zostały zgromadzone przez system.

„Zapisuj w dzienniku informacje o wysłanych danych" - opcja umożliwia zapisywanie w dzienniku zdarzeń wszystkich informacji o wysyłanych plikach i innych danych.

Skaner „na żądanie” NOD32

Skaner na żądanie (czasami również nazywany Skaner NOD32) jest używany do skanowania zasobów komputera na życzenie użytkownika lub według harmonogramu. Zalecane jest, aby pierwsze skanowanie wykonać po instalacji programu, po dokonaniu aktualizacji bazy wirusów i komponentów programu.
Jeżeli wykonanie aktualizacji nie jest możliwe, zalecane jest przeprowadzenie skanowania przy pomocy posiadanej wersji.

Do wykrywania wirusów NOD32 wykorzystuje moduł analizy heurystycznej, który zapewnia skuteczność programu nawet w przypadku występowania przerw w aktualizacji bazy wirusów. Oznacza to, że nasz komputer jest stosunkowo bezpieczny nawet jeżeli z różnych powodów przez kilka dni nie było możliwe aktualizowanie systemu.

UWAGA: Nie oznacza to, że można w ogóle zaniechać aktualizacji! Moduł heurystyczny daje bardzo wysokie prawdopodobieństwo wykrywania wirusów (również dotychczas nieznanych!), ale nie daje 100% pewności. Aktualne bazy

sygnatur wirusowych są niezbędne do zapewnienia maksymalnej skuteczności ochrony.

Bieżące aktualizowanie systemu jest również niezbędne ze względu na rozwiązywanie problemów technicznych. Bezpłatna pomoc producenta i dystrybutora jest zapewniona tylko dla najbardziej aktualnej wersji systemu.

Dla zapewnienia bezpieczeństwa, skanowanie zasobów powinno odbywać się regularnie. Zalecane jest wykonywać je nie rzadziej niż raz w tygodniu, a dodatkowo po każdej aktualizacji systemu lub bazy sygnatur wirusowych.

UWAGA: WAŻNA INFORMACJA dotycząca skanowania na żądanie i usuwania wirusów na żądanie!

Przed rozpoczęciem skanowania i usuwania wirusów na żądanie zalecane jest zakończenie wszystkich uruchomionych aplikacji.

Po zakończeniu usuwania wirusów, system może zaproponować ponowne uruchomienie komputera. Należy wykonać to niezwłocznie by uniknąć dalszego rozprzestrzeniania się wirusów. Do tego czasu nie należy uruchamiać innych aplikacji.

Aby upewnić się co do skuteczności usunięcia wirusów, po ponownym uruchomieniu komputera , należy powtórzyć skanowanie.

Skaner może być uruchomiony z Konsoli Systemu NOD32 lub automatycznie przy pomocy Harmonogramu zadań.

Aby uruchomić Skaner ręcznie, należy kliknąć na ikonę NOD32 umieszczoną na pulpicie. Drugą możliwością uruchomienia Skanera na żądanie NOD32 jest stworzenie nowego zadania w Harmonogramie zadań, w tym celu należy otworzyć **System NOD32** klikając na zielono – białą ikonę umieszczoną w prawym dolnym rogu pulpitu (na pasku zadań). Dodatkowo istnieje możliwość uruchomienia Skanera na żądanie z menu kontekstowego. W tym celu należy kliknąć prawym klawiszem myszki na wybranym folderze/ pliku i wybrać opcję System Antywirusowy NOD32.

UWAGA: Opcja „Włącz skaner na żądanie w menu kontekstowym" musi zostać włączona w trakcie instalacji Systemu Antywirusowego NOD32.

Po uruchomieniu *Skanera na żądanie* rozpoczyna się automatyczny proces skanowania pamięci operacyjnej w poszukiwaniu wirusów. Kolejnym etapem jest automatyczne przeprowadzenie testu poprawności Skanera.

Główne okno Skanera na żądanie zawiera pięć zakładek:

1. Skanowane obiekty
2. Dziennik skanowania
3. Czynności
4. Konfiguracja
5. Profile

Dolna sekcja *Skanera na żądanie* pozostaje bez zmian niezależnie od wyboru zakładki. Opis przycisków znajduje się poniżej.

Przyciski kontrolne

Skanuj

Zapewnia skanowanie wszystkich wybranych obiektów. W momencie wybrania przycisku ***Skanuj*** zakładka Skanowane obiekty automatycznie zostaje zastąpiona zakładką Dziennik skanowania, a przycisk ***Skanuj*** przyciskiem ***Stop***. Naciśnięcie przycisku ***Stop*** powoduje przerwanie procesu skanowania. W zakładce Dziennik skanowania wyświetlane są wyniki skanowania. W przypadku wykrycia wirusa informacje w Dzienniku skanowania są zaznaczone na czerwono. Zainfekowane pliki można wyleczyć przy pomocy przycisku ***Wylecz*** lub poprzez kliknięcie prawym klawiszem myszy na informację w Dzienniku skanowania dotyczącą skanowanego obiektu (zaznaczona na czerwono) i wybranie opcji ***Usuń*** z pojawiającego się menu kontekstowego.

Wylecz

Wybranie przycisku ***Wylecz*** powoduje skanowanie wszystkich wybranych obiektów i w przypadku wykrycia infekcji zostaje podjęta odpowiednia czynność usuwania infekcji, która jest wcześniej definiowana w zakładce Czynności. W chwili uruchomienia procesu skanowania/leczenia przycisk ***Wylecz*** zostaje zastąpiony przyciskiem ***Stop***, który może być użyty do przerwania procesu skanowania.

Zakończ

Wybranie przycisku ***Zakończ*** powoduje wyjście z programu. Jeżeli używany profil zmienił się podczas działania programu zostanie wyświetlone zapytanie o zapisanie modyfikacji profilu.

Wersja

W lewym dolnym rogu okna wyświetlana jest informacja o wersji bazy wirusów, np. 2.129(20020621)NT. Oznacza to, że program korzysta z bazy o numerze

2.129 z dnia 2002–06–21 (format daty jest następujący: YYYYMMDD) przeznaczonej dla systemu operacyjnego opartego na technologii NT.

Pomoc

Wybranie przycisku ***Pomoc*** udostępnia system pomocy on–line. Ten sam efekt jest również uzyskiwany za każdym razem gdy zostanie naciśnięty klawisz F1.

Zakładka Skanowane obiekty

Zakładka umożliwia określenie obiektów przeznaczonych do skanowania. W górnej części zakładki znajduje się okno *Dyski*, natomiast w dolnej okno *Foldery i pliki*.

Dyski

Aby wybrać lub anulować wybór napędu, należy użyć klawisza spacji lub dwa razy kliknąć lewym przyciskiem myszki na wybranym napędzie.
Okno *Dyski* jest podzielone na trzy kolumny:

Dyski – wyświetla ikonę i nazwę dysku

Typ – określa typ dysku

Połączony z – wyświetla nazwę dysku sieciowego

Po prawej stronie okna *Dyski* znajdują się dwie możliwe do wyboru opcje:

Lokalne – zaznacza / odznacza wszystkie dyski lokalne

Sieciowe – zaznacza / odznacza wszystkie dyski sieciowe

Poniżej znajdują się dwa przyciski:

Zaznacz wszystkie – powoduje wybór wszystkich napędów

Odznacz wszystkie – anuluje wybór wszystkich napędów

Foldery i pliki

W oknie wyświetlana jest lista wybranych indywidualnie folderów i plików, które mają być sprawdzane pod względem obecności wirusów. Zawartość listy może być zmieniana przy pomocy dwóch przycisków:

Dodaj – otwiera nowe okno dialogowe z dostępnymi przyciskami: ***OK, Anuluj, Folder..., Plik....*** Aby dodać nowy folder/plik należy wprowadzić odpowiednią nazwę (wraz ze ścieżką dostępu) lub kliknąć na przyciski: ***Folder...*** aby przeglądać dysk w poszukiwaniu wybranego folderu / ***Plik...*** aby przeglądać dostępne foldery w poszukiwaniu wybranego pliku.

Usuń – usuwa zaznaczone foldery/pliki z listy. Aby usunąć obiekt z listy należy go podświetlić i kliknąć na przycisk ***Usuń***.

Poniżej również znajdują się dwa przyciski:

Zaznacz wszystkie – powoduje zaznaczenie wszystkich wybranych obiektów

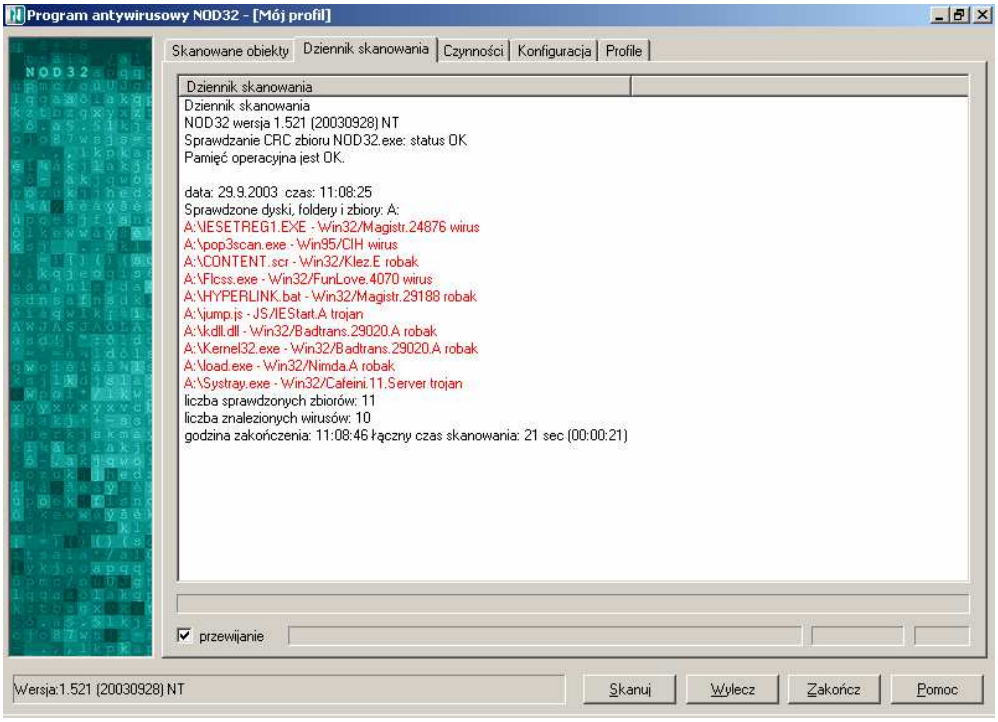
Odznacz wszystkie – anuluje zaznaczenie wszystkich wybranych obiektów

Zakładka Dziennik skanowania

W Dzienniku skanowania znajdują się informacje dotyczące każdego przeprowadzonego skanowania.

Wybór opcji *przewijanie* powoduje automatyczne przewijanie się Dziennika skanowania w trakcie skanowania (zawsze widoczne będą ostatnie wyniki skanowania). Jeżeli opcja nie zostanie zaznaczona widoczne będą pierwsze wyniki skanowania. Aby zobaczyć więcej konieczne będzie ręczne przewijanie listy skanowanych plików.

Zakres i format wyświetlanych informacji jest konfigurowany w grupie Dziennik skanowania, zakładki ***Konfiguracja***.



Dziennik skanowania zawiera informacje o bieżącej wersji bazy wirusów oraz szczegółowe informacje dotyczące skanowania:

- Data i czas skanowania
- Lista zainfekowanych plików (zaznaczone na czerwono)
- Nazwy plików, które nie zostały przeskanowane, ponieważ były używane przez system lub są uszkodzone (zaznaczone na niebiesko)
- Informacja o zakończeniu skanowania, np. skanowanie przerwane przez użytkownika
- Liczba sprawdzonych plików
- Liczba znalezionych wirusów
- Godzina zakończenia
- Łączny czas skanowania

Sekcja ***Uwagi***: zawiera wyjaśnienia dotyczące błędów, które wystąpiły w trakcie skanowania.

Dodatkowo ***Dziennik skanowania*** jest zintegrowany z Dziennikiem zdarzeń, który jest dostępny w ***Konsoli Systemu NOD32***.

Wskazówka: Aby usunąć wpisy w Dzienniku skanowania należy kliknąć prawym klawiszem na dowolny wpis i wybrać ***Wykasuj dziennik***. Aby wyleczyć zainfekowany plik, należy kliknąć prawym klawiszem myszy na informacji dotyczącej zainfekowanego obiektu w Dzienniku skanowania i wybrać opcję ***Usuń***.

Zakładka Czynności

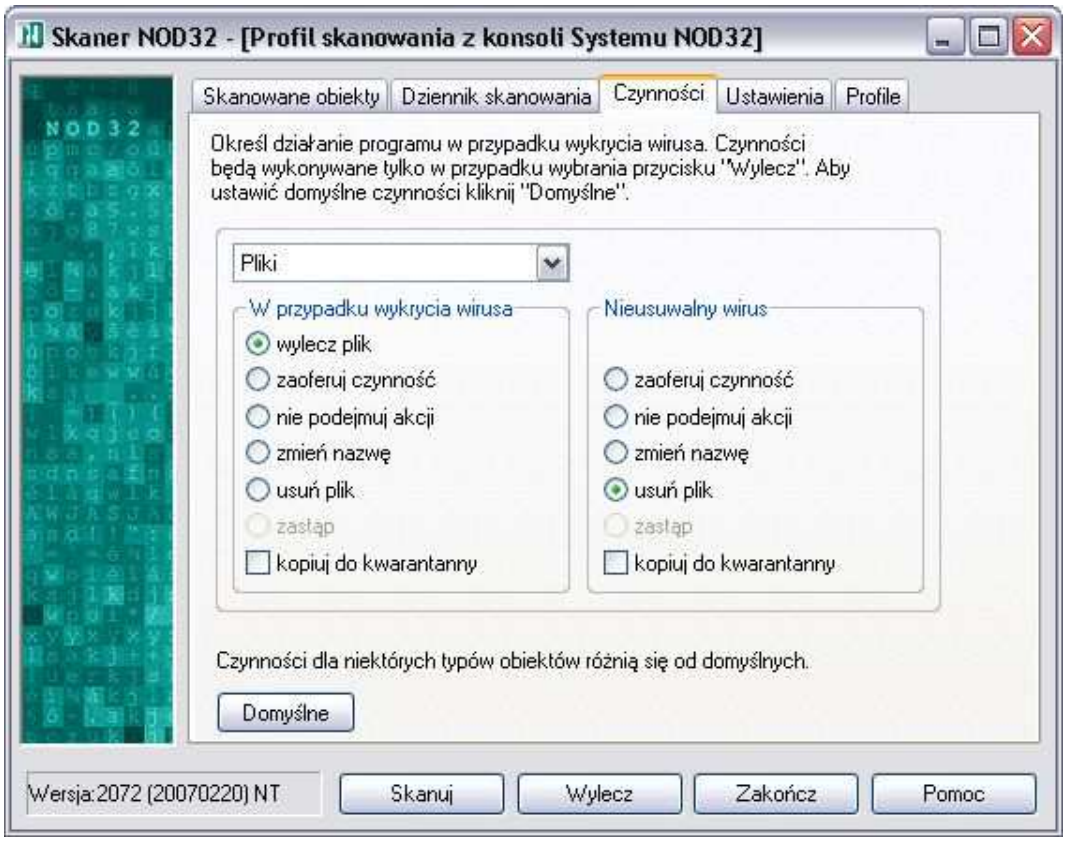
Czynności, zdefiniowane w tej zakładce są podejmowane w przypadku wykrycia wirusa, po naciśnięciu przycisku ***Wylecz***. Zależą one od rodzaju zainfekowanego obiektu (plik, boot sektor, pamięć operacyjna, itp.).

W pierwszym kroku należy dokonać wyboru czynności, które mają być przeprowadzone w przypadku wykrycia wirusa w danym obiekcie. W tym celu należy kliknąć na strzałkę rozwijanej listy i wybrać obiekt z pojawiającego się menu. (Obiekt „Pliki" jest ustawiony domyślnie).
Obiekty dostępne na liście:

- *Pliki* – ustawienie czynności w przypadku wykrycia wirusa w plikach
- *Boot sektory* – ustawienie czynności w przypadku wykrycia wirusa w boot sektorach dysków logicznych
- *Archiwa* – ustawienie czynności w przypadku wykrycia wirusa w skompresowanych archiwach, np. ZIP, ARJ i inne
- *Pliki spakowane* – ustawienie czynności w przypadku wykrycia wirusa w plikach wykonywalnych spakowanych wewnętrznie utworzonych przez programy pakujące, np. PKLite, LZExe, Diet i inne
- *Poczta* – ustawienie czynności w przypadku wykrycia wirusa w plikach poczty (typu .eml)
- *Foldery poczty* – ustawienie czynności w przypadku wykrycia wirusa w plikach folderów poczty Outlook Express (typu .dbx)
- *Pamięć operacyjna* – ustawienie czynności w przypadku wykrycia wirusa w pamięci operacyjnej komputera

Lista czynności możliwych do wybrania (w zależności od obiektu) zawiera następujące opcje:

- *wylecz plik/boot sektor* – powoduje automatyczne usuniecie wirusa z zainfekowanego pliku
- *zaproponuj rozwiązanie* – wyświetla panel zawierający propozycje sugerowanych w danej sytuacji czynności
- *nie podejmuj akcji* – pozostawia plik bez dokonywania jakichkolwiek zmian
- *zmień nazwę* – zmienia nazwę zainfekowanego pliku
- *usuń plik* – usuwa cały zainfekowany plik
- *zastąp (tylko dla boot sektorów)* – zastępuje boot sektor standardowym kodem
- *Kwarantanna* – przenosi zainfekowany plik w postaci zaszyfrowanej do specjalnego folderu



Kwarantanna jest niezależna od pozostałych opcji. Jest to folder, w którym są przechowywane zainfekowane (podejrzane) pliki w zaszyfrowanej formie.

Jeżeli co najmniej jedna z czynności, które powinny być podjęte w przypadku wykrycia wirusa, różni się od domyślnych ustawień, pod oknem wyboru opcji pojawia się odpowiedni komunikat. Aby powrócić do domyślnych ustawień dla wszystkich obiektów należy użyć przycisku ***Domyślne***.

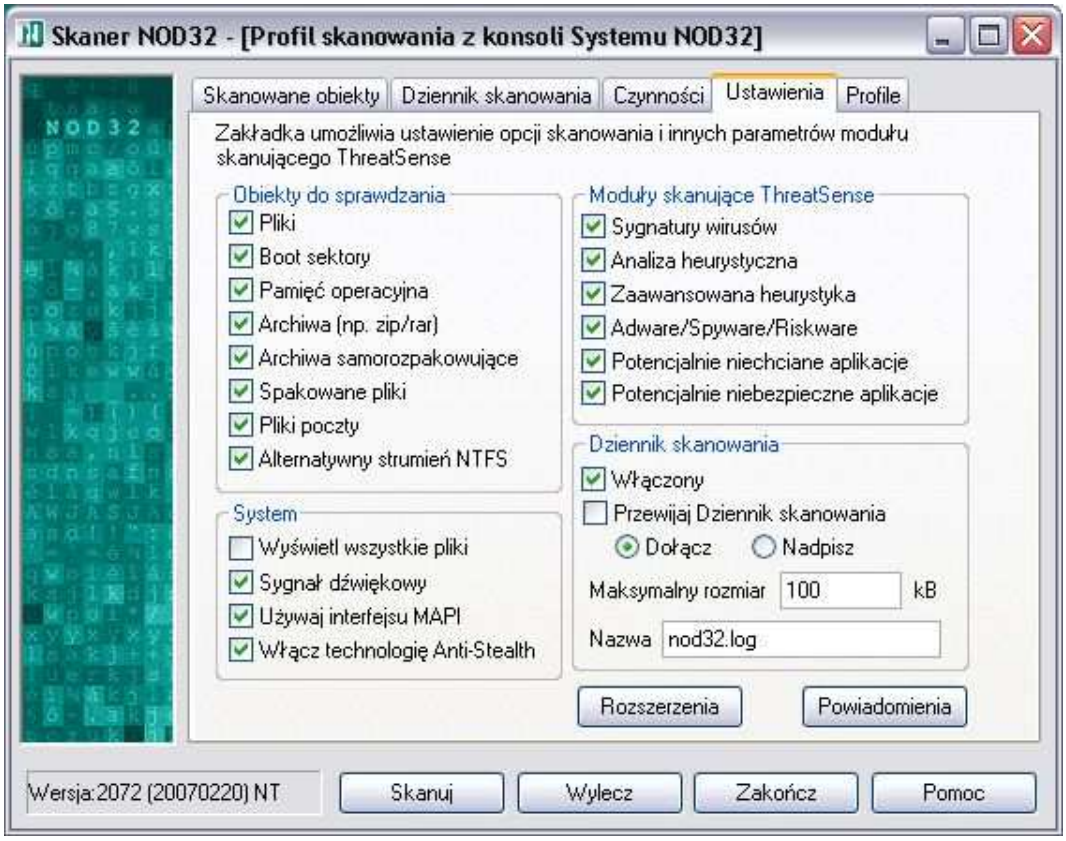
Przykład

Jeśli została wybrana opcja „usuń plik" jednocześnie z opcją „Kwarantanna" to wybrany plik przed usunięciem zostaje zaszyfrowany i przeniesiony do katalogu kwarantanny.

W przypadku pojawienia się pliku (robaki, trojany), którego nie można wyleczyć, istnieje możliwość zdefiniowania dodatkowej opcji. Jeśli została wybrana opcja *„wylecz plik/boot sektor",* a wirus jest nieusuwalny, to druga proponowana przez system czynność jest wyświetlona w sąsiednim oknie.

Zakładka Konfiguracja

Zakładka Konfiguracja zawiera opcje dotyczące ustawień: obiektów do sprawdzania, metod diagnozowania, systemu, czułości analizy heurystycznej, dziennika skanowania.



Obiekty do sprawdzania

Opcje zawarte w tej grupie są rozszerzeniem zakładki Skanowane obiekty. W tej zakładce użytkownik ma możliwość wyboru dodatkowych opcji skanowania, np. jeśli został wybrany lokalny dysk C: jako obiekt przeznaczony do skanowania i wybrany jest domyślny profil skanowania, skaner nie będzie skanować archiwów, spakowanych plików i plików poczty (Outlook Express).
Dostępne opcje w polu „Obiekty do skanowania”:

- *„Pliki"* – włącza skanowanie plików
- *„Boot sektory"* – włącza skanowanie boot sektorów dysków logicznych
- *„Pamięć operacyjna"* – włącza skanowanie pamięci operacyjnej komputera
- *„Spakowane pliki"* – włącza skanowanie plików wykonywalnych spakowanych wewnętrznie utworzonych przez programy pakujące, np. PKLite, LZExe, Diet i inne
- *„Archiwa"* – włącza skanowanie skompresowanych archiwów, np. ZIP, ARJ i inne
- *„Archiwa samorozpakowujące"* - skanuje wewnątrz plików spakowanych, samorozpakowujących (SFX).
- *Pliki poczty* – włącza skanowanie plików programów pocztowych (Outlook Express)

Metody diagnozowania

Metody skanowania są kluczem do sukcesu każdego programu antywirusowego. NOD32 obok standardowej metody sygnaturowej posiada również rewelacyjną **Analizę heurystyczną**. Zalecane jest jednoczesne używanie obu metod, ponieważ wyłączenie choć jednej powoduje obniżenie możliwości Systemu Antywirusowego. ***Sygnatury wirusów*** reprezentują bazę wirusów, która jest aktualizowana okresowo przy pomocy automatycznego modułu aktualizacji konfigurowanego w Systemu NOD32. Zalecane jest aktualizowanie baz wirusów nawet co godzinę. Do przeprowadzenia aktualizacji potrzebna jest nazwa użytkownika i hasło umożliwiające poprawną autoryzację na Serwerze Aktualizacji. ***Analiza heurystyczna*** pozwala na wykrywanie najnowszych infekcji, które nie są jeszcze uwzględnione w bazie sygnatur wirusów.
Dostępne mnetody skanujące ThreatSense (wszystkie metody powinny być włączone):

„Sygnatury wirusów" **–** sprawdzanie na podstawie bazy wirusów.

„Analiza heurystystyczna" **–** umożliwia wykrycie nieznanych wirusów na podstawie analizy pliku.

„Zaawansowana heurystyka" – rozszerza możliwości analizy heurystycznej programu NOD32 i zwiększa wykrywanie nowych zagrożeń włączając w to robaki, trojany i inne wirusy (zalecane).

„Adware/Spyware/Riskware" – wykrywanie zagrożeń typu Adware: (małe programy, których działanie polega na pobieraniu reklam z Internetu i wyświetlanie ich), Spyware (programy, które zbierają poufne informacje o użytkowniku i wysyłają je przy pomocy Internetu), Riskware (programy, które mogą być wykorzystywane przez hakerów)

„Potencjalnie niechciane aplikacje" - programy, które nie zawsze stanowią zagrożenie bezpieczeństwa; Aplikacje te zwykle wymagają zgody użytkownika przed instalacją i mogą mieć wpływ na zachowanie systemu.

„Potencjalnie niebezpieczne aplikacje" – zazwyczaj komercyjne programy wykorzystywane przez hakerów (np. narzędzia zdalnego dostępu i administracji)

System

Grupa System umożliwia konfigurację następujących opcji:

- *Wyświetl wszystkie pliki* – Wybór tej opcji spowoduje wyświetlenie w Dzienniku zdarzeń listy wszystkich skanowanych plików (nawet jeżeli nie były one zainfekowane). Zaznaczenie tej opcji spowoduje znaczne zwiększenie rozmiaru pliku Dziennika zdarzeń.
- *Sygnał dźwiękowy* – W przypadku wykrycia infekcji (wirusa) zostanie wygenerowany sygnał dźwiękowy
- *Używaj interfejsu MAPI* – Wspiera dostęp do plików poczty klienta MS Outlook® przy użyciu interfejsu MAPI

Dziennik skanowania

W tej sekcji można dokonać ustawień dotyczących Dziennika skanowania:

Włączony – powoduje zapisywanie treści dziennika zdarzeń na dysku

Przewijaj dziennik zdarzeń – powoduje automatyczne przewijanie treści dziennika

Dołącz – nowy wpis do dziennika zostanie dołączony do poprzednich (jeżeli istnieją)

Nadpisz – nowy wpis do dziennika zawsze zastępuje dotychczasowe

Maksymalny rozmiar – określa maksymalny rozmiar dziennika w kB

Nazwa – można określić nową nazwę pliku dziennika zdarzeń, jeżeli nazwa domyślna "nod32.log" musi zostać zmieniona

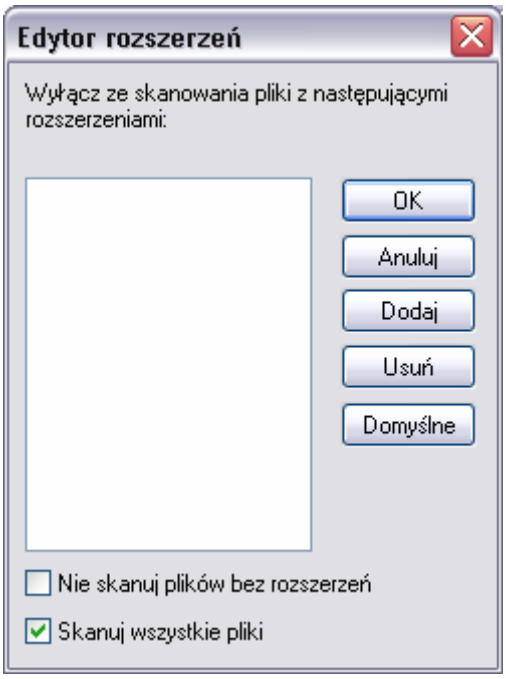
Przyciski

Rozszerzenia – Przycisk umożliwia edycję rozszerzeń plików, które mają być skanowane.

Powiadomienia – Przycisk umożliwia szybkie włączenie systemu powiadomień.

Edytor rozszerzeń

Edytor rozszerzeń jest specjalną funkcją, przeznaczoną dla zaawansowanych użytkowników. Zestaw rozszerzeń plików przeznaczonych do skanowania jest stale aktualizowany razem z aktualizacją baz wirusów i komponentów programu. Usunięcie jakiegokolwiek rozszerzenia może spowodować infekcję systemu!



Lista rozszerzeń plików przeznaczonych do skanowania jest przedstawiona w głównej części okna. Nawigacja listy odbywa się przy użyciu paska przewijania umieszczonego po prawej stronie okna. Aby podświetlić rozszerzenie należy ustawić na nim kursor myszki i kliknąć.

Przyciski

OK – Każda modyfikacja listy rozszerzeń musi być zaakceptowana przy użyciu przycisku ***OK***.

Anuluj – Przycisk Anuluj zamyka okno i przywraca zakładkę Konfiguracja

Dodaj – Aby dodać rozszerzenie należy nacisnąć na przycisk ***Dodaj***, wypełnić pole dialogowe i zatwierdzić przyciskiem ***OK***.

Usuń – Aby usunąć dowolne rozszerzenie (operacja może spowodować zagrożenie bezpieczeństwa) należy podświetlić wybrane rozszerzenie, nacisnąć przyciski ***Usuń*** i ***OK***.

Domyślne – Aby przywrócić domyślne ustawienia rozszerzeń (zalecane) należy nacisnąć przycisk ***Domyślne*** a następnie ***OK***.

Dodatkowe opcje:

Skanuj pliki bez rozszerzeń – Opcja ta powoduje skanowanie plików bez rozszerzeń.

Skanuj wszystkie pliki – gdy ta opcja będzie zaznaczona Edytor rozszerzeń zmienia swoje właściwości: w oknie rozszerzeń może być tworzona lista rozszerzeń plików wyłączonych ze skanowania. Dodatkowo pojawia się nowe okno wyboru pozwalające wyłączyć ze skanowania pliki bez rozszerzeń (opcja ustawiona domyślnie).

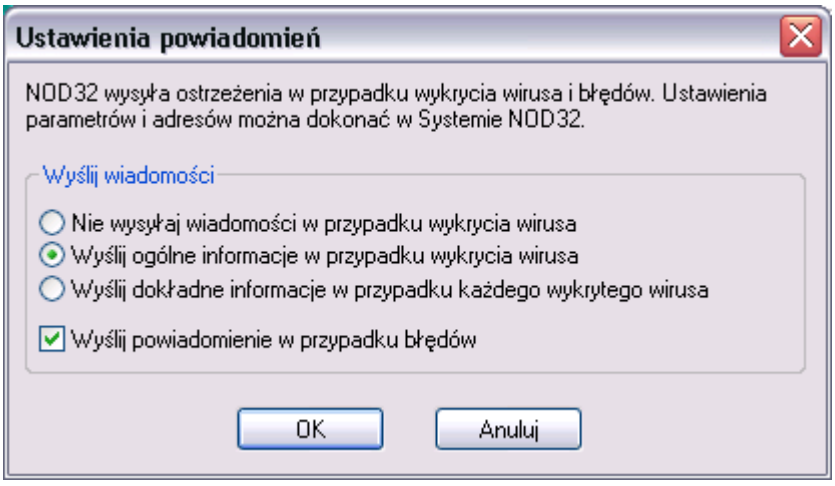
Lista rozszerzeń plików przeznaczonych do skanowania przez skaner antywirusowy NOD32 jest definiowana domyślnie (aby zoptymalizować efektywność i bezpieczeństwo). Jeżeli w wyniku nowego zagrożenia istnieje konieczność rozszerzenia lub modyfikacji listy, niezbędne zmiany są uwzględnione w bieżącej aktualizacji. Dlatego nie jest zalecane wybieranie opcji „*Skanuj wszystkie pliki*", ponieważ może to niepotrzebnie spowalniać proces skanowania.

UWAGA: Usuwanie domyślnych rozszerzeń nie jest zalecane i może spowodować zniszczenie lub utratę danych.

Edytor rozszerzeń pozwala również na szybkie wybranie opcji skanowania wszystkich plików lub plików bez rozszerzeń.

Powiadomienia

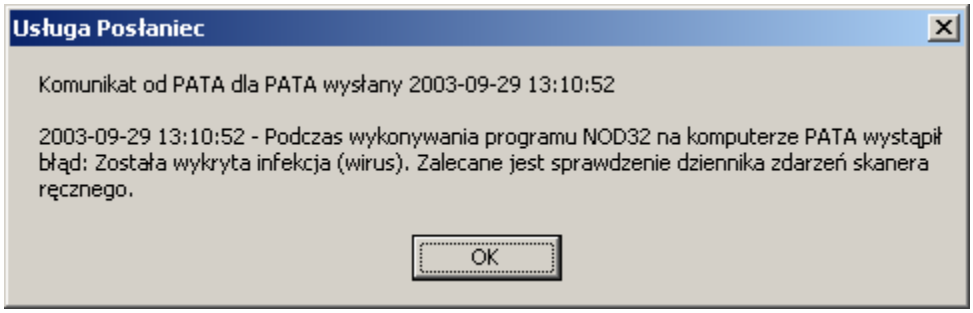
W przypadku wykrycia infekcji lub innych ważnych zdarzeń (takich jak pojawiające się błędy, zakończenie procesu aktualizacji) może być wysłana wiadomość/powiadomienie z określonego komputera na zdefiniowany wcześniej adres e–mail (lub grupę adresów). Opcja *„Powiadomienia"* pozwala na szybkie włączenie powiadomień.



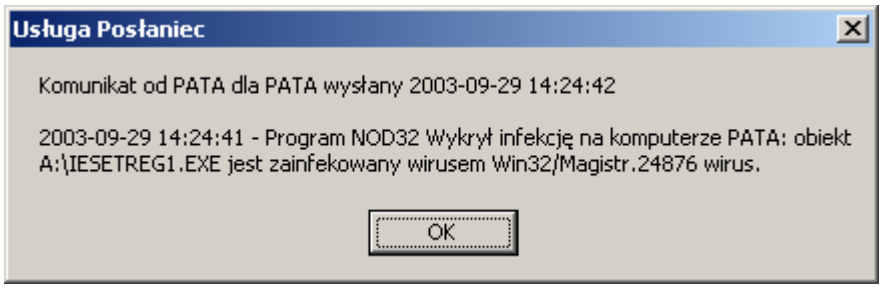
Ustawienie wiadomości/powiadomień:

„Nie wysyłaj wiadomości w przypadku wykrycia infekcji (wirusa)" – żadna wiadomość nie zostanie wysłana w przypadku wykrycia wirusa

„Wyślij ogólne informacje w przypadku wykrycia infekcji (wirusa)" – zostanie wyświetlona lub przesłana wiadomość treści:



Wyślij dokładne informacje w przypadku każdej wykrytej infekcji (wirusa) – zostanie wyświetlona lub przesłana wiadomość treści:



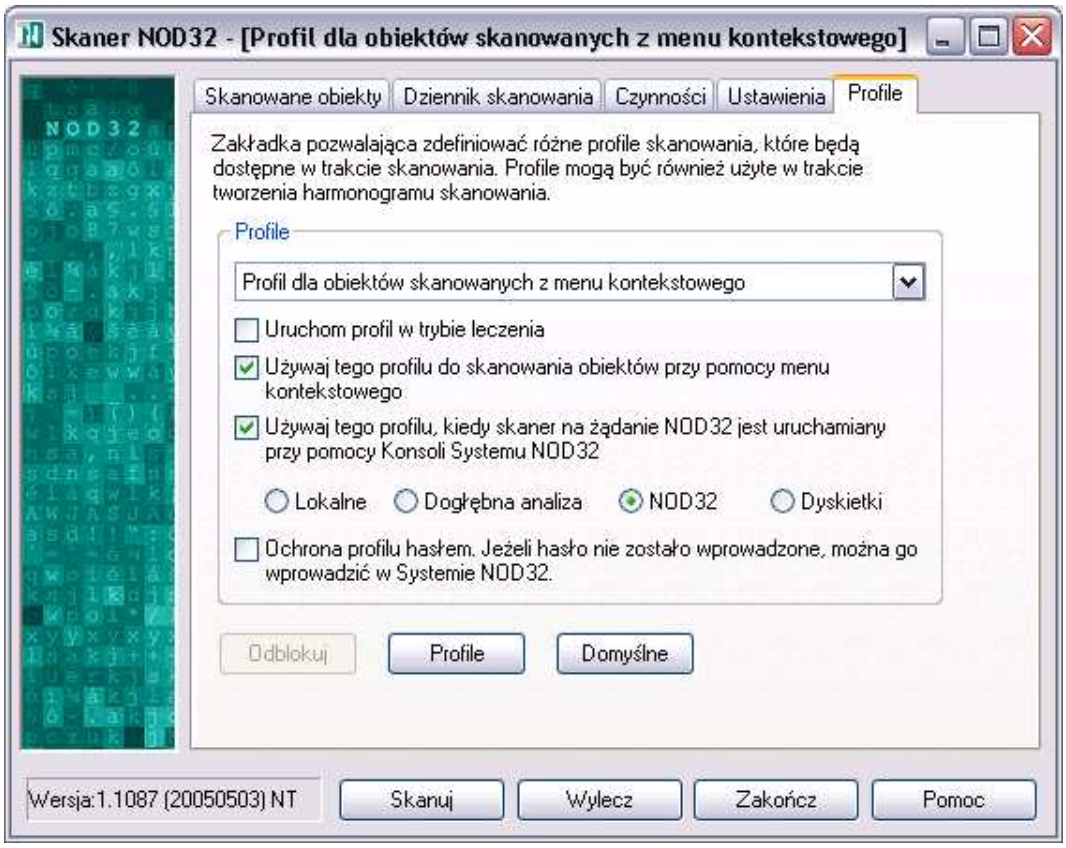
Wyślij powiadomienie w przypadku błędów – zostanie wyświetlona lub przesłana wiadomość informująca o błędach podczas uruchamiania skanera na żądanie, itp

Wybór ostatniej opcji nie jest uzależniony od pozostałych.

Zakładka Profile

Zakładka Profile służy do tworzenia lub wyboru specjalnych ustawień parametrów skanowania. Wszystkie ustawienia opcji Skanera na żądanie mogą być zapisane w wybranym profilu (zakładka Profile). Aby zapisać zmiany, należy kliknąć na przycisk ***Zapisz***. W oknie Zapisz profil istnieje możliwość wybrania istniejącego profilu (do edycji) lub stworzenia nowego. Aby utworzyć nowy profil, należy wybrać przycisk ***Nowy*** i wprowadzić nową nazwę.

Aby zabezpieczyć hasłem każdy profil (wraz z jego ustawieniami) należy wybrać opcję „Ochrona profilu hasłem" dla tego profilu i wprowadzić hasło ustawione w **Systemu NOD32**. Wszystkie profile, dla których wybraliśmy opcje ochrony, będą zabezpieczone tym samym hasłem.



W celu przywrócenia domyślnych ustawień wybranego profilu należy użyć przycisku ***Domyślne***.

Skaner na żądanie może używać szczególnych ustawień parametrów skanowania, zapisywanych w odrębnych profilach. Profile skanowania są tworzone w programie NOD32. W tym celu należy:

Wybrać zakładkę Profile
Kliknąć na przycisk ***Profile***
Wybrać przycisk ***Nowy***
Wprowadzić nazwę dla nowego profilu
Zatwierdzić przyciskiem ***Zapisz***

Aby zapisać ustawienia na dysku należy kliknąć na przycisk ***OK***.

Postępowanie w przypadku wykrycia infekcji

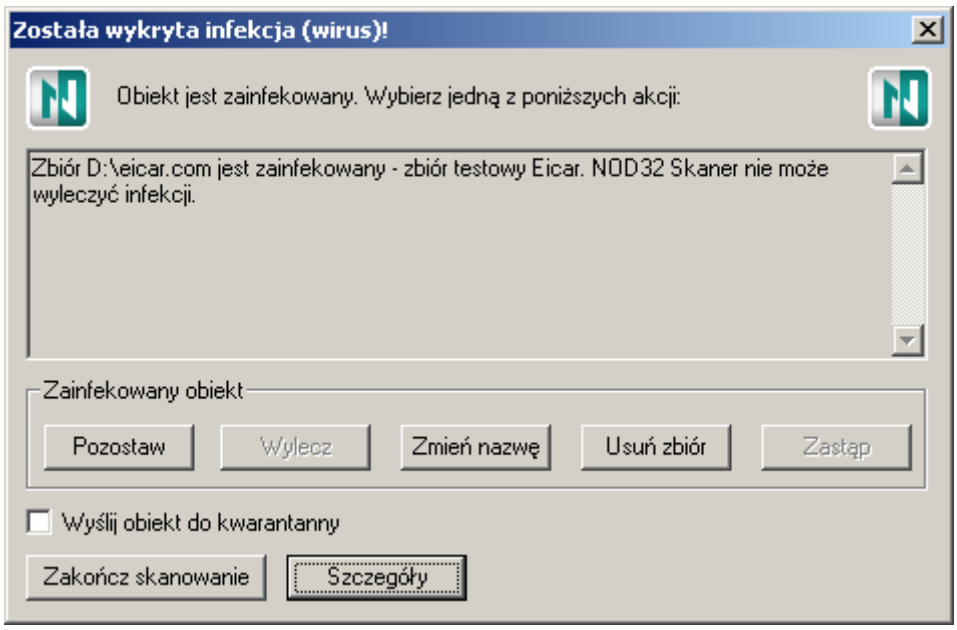
System Antywirusowy NOD32 jest wyposażony w zaawansowany skaner analizy heurystycznej z minimalną liczbą fałszywych alarmów. Analiza heurystyczna pozwala na wykrywanie dużej części nieznanych jeszcze (nie analizowanych) wirusów. Jeżeli taka sytuacja ma miejsce, system klasyfikuje ten plik jako *'prawdopodobnie nieznany jeszcze wirus'*. W tej sytuacji zalecane jest wysłanie takiego pliku do laboratorium firmy ESET w celu przebadania go, ponieważ możliwe jest, że wirus już zainfekował nasze dane.
Prosimy o wysłanie '*zainfekowanego*' pliku na adres: sample@eset.com lub support@nod32.pl.

Po dokonanej analizie zawirusowanego pliku, zostanie zwrócony oczyszczony plik (w przypadku gdy wirus był usuwalny) z informacją na temat wykrytego wirusa.

Jeżeli w trakcie skanowania na żądanie zostały wykryte infekcje należy uruchomić skaner ponownie, ale zamiast przycisku ***Skanuj*** należy wybrać ***Wylecz***. W trybie „leczenia" (jeśli została wykryta infekcja) wykonywane są zdefiniowane wcześniej czynności. W większości przypadków NOD32 jest w stanie wyleczyć zainfekowany obiekt. Jednakże duża liczba powstałych ostatnio robaków komputerowych musi być usunięta, ponieważ wewnątrz pliku znajduje się tylko kod robaka.

W przypadku ewentualnych wątpliwości dotyczących wybranych (zainfekowanych) plików prosimy o wysłanie kopii pliku na wyżej wymienione adresy.

Po wykryciu wirusa panel informacji o wykryciu infekcji zostanie wyświetlony, jeżeli skaner pracuje w trybie usuwania wirusów (przycisk ***Wylecz***), a nie skanowania.



Górna część panelu wyświetla przewijające się okno z informacją o pliku, w którym wykryto wirusa. Wyświetlone są również dodatkowe dane, takie jak nazwa i charakterystyka wirusa, oraz czy może on być usunięty przy pomocy tego programu.

Sekcja *Zainfekowany plik* zawiera cztery przyciski:
Pozostaw – pozostawia plik bez dokonywania zmian
Wylecz – powoduje usunięcie wirusa ze pliku
Zmień nazwę – zmienia nazwę pliku zawierającego wirusa by zapobiec jego przypadkowemu uruchomieniu
Usuń plik – usuwa zainfekowany plik

W przypadku przeniknięcia wirusa do boot sektora, nazwa sekcji zmienia się na: *Zainfekowany boot sektor* i wyświetlają się trzy przyciski:
Pozostaw bez zmian – pozostawia boot sektor bez dokonywania żadnych zmian
Usuń wirusa – uruchamia proces usuwania wirusa
Zastąp – zastępuje zainfekowane rekordy boot sektora standardowym kodem.

Dolna część panelu zawiera dwa przyciski:

Zakończ skanowanie – powoduje on natychmiastowe przerwanie procesu skanowania

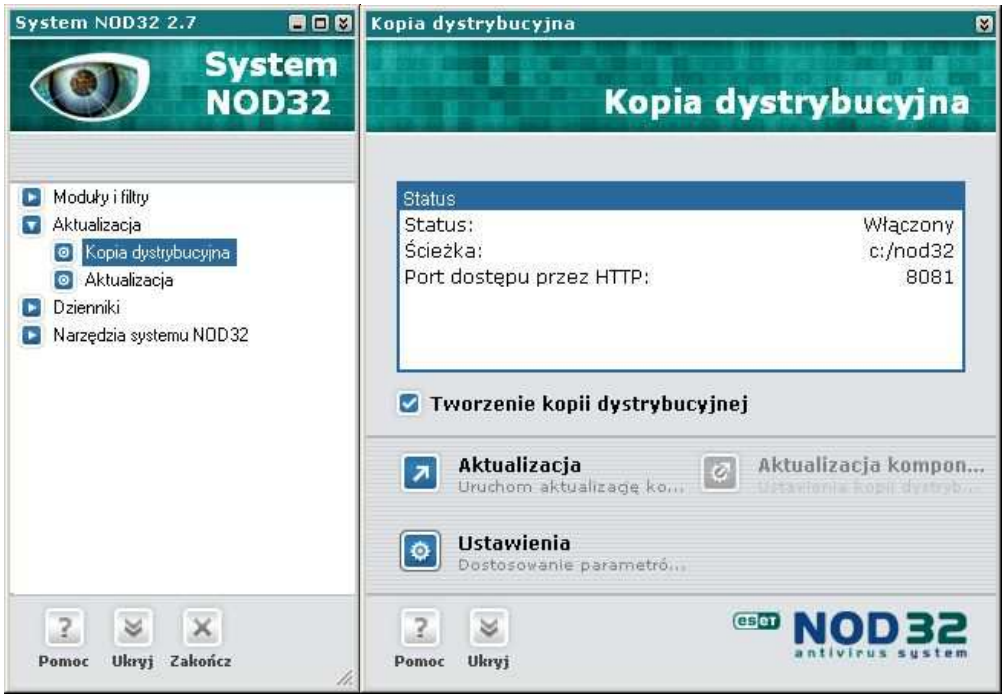
Szczegóły – powoduje wyświetlenie dokładnych informacji dotyczących wykrytego wirusa: nazwa pliku i nazwa wirusa.

Kopia dystrybucyjna

Opcja *„Kopia dystrybucyjna"* jest stosowana do generowania i aktualizowania repozytorium plików aktualizacyjnych dla systemu antywirusowego NOD32 w lokalnej sieci korporacyjnej. Jeżeli kopia dystrybucyjna jest dostępna stacje robocze mogą aktualizować się z zasobów lokalnej sieci (nie łączą się z Internetem).

Aby otworzyć okno modułu kopii dystrybucyjnej w głównym oknie **Systemu NOD32** należy rozwinąć grupę komponentów *Aktualizacja* i wybrać *Kopia dystrybucyjna*.

UWAGA: Moduł jest dostępny tylko w wersji administracyjnej systemu NOD32.



W górnej części okna znajdują się informacje dotyczące: statusu modułu (włączony/wyłączony nie skonfigurowany), ścieżki dostępu do folderu zawierającego repozytorium, portu dostępu przez HTTP, itp.

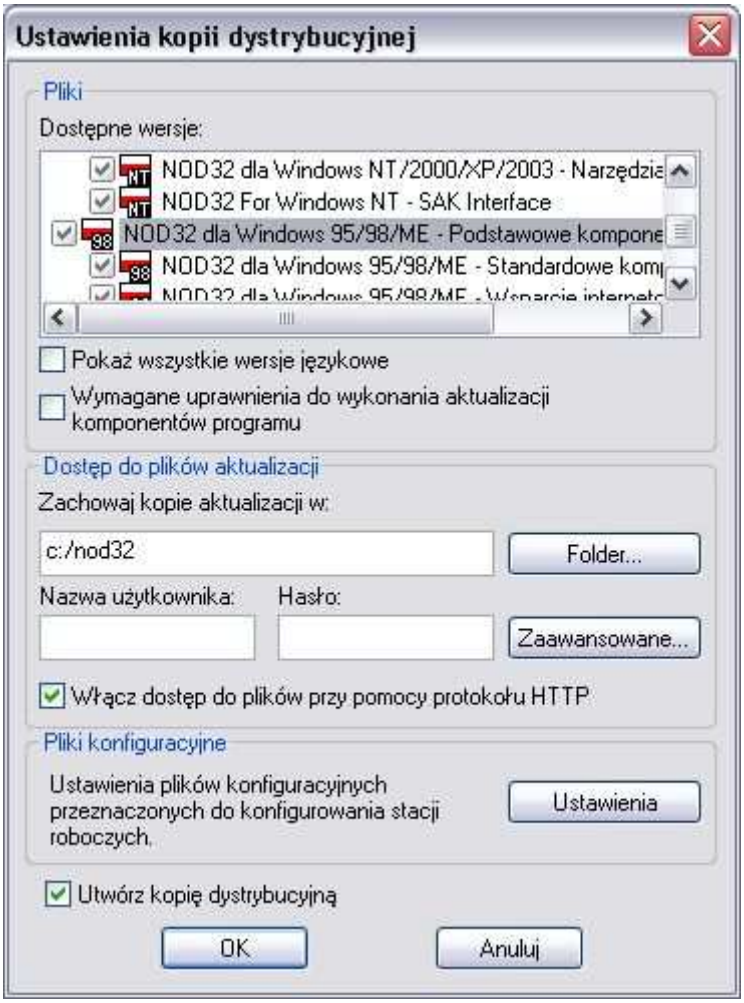
Opcja *„Tworzenie kopii aktualizacyjnych”* jest zaznaczona gdy moduł jest skonfigurowany i włączony. W tym przypadku ikona jest koloru niebieskiego . Jeżeli nie zostało skonfigurowane generowanie kopii dystrybucyjnej, opcja jest wyłączona, a ikona jest koloru czerwonego .

Aby ręcznie zaktualizować kopię plików aktualizacyjnych należy kliknąć na przycisk ***Aktualizacja***. Domyślnie akcja wykonywana jest automatycznie (po automatycznym zaktualizowaniu Systemu NOD32 na komputerze odpowiedzialnym za tworzenie kopii dystrybucyjnej).

W celu dokonania zmian w konfiguracji kopii dystrybucyjnej i tworzenia nowych lub modyfikowania istniejących plików konfiguracyjnych należy wybrać przycisk ***Ustawienia***.

Konfiguracja kopii dystrybucyjnej

Aby utworzyć kopię dystrybucyjną należy wybrać *„Utwórz kopię aktualizacji”* i wybrać odpowiednie opcje konfiguracji.



W górnej części okna wyświetlona jest lista wszystkich dostępnych wersji plików aktualizacyjnych dostarczonych przez producenta. Dwukrotne kliknięcie na wersję

wyświetla listę dostępnych komponentów. Należy wybrać komponenty, które mają być aktualizowane w lokalnej kopii plików aktualizacyjnych. Aby wyświetlić listę wszystkich dostępnych wersji językowych należy wybrać opcję *„Pokaż wszystkie wersje językowe"*.

W kolejnym kroku należy podać ścieżkę dostępu do folderu gdzie zostanie utworzona kopia dystrybucyjna (*„Zachowaj kopie aktualizacji w:"*). Folder musi zostać wcześniej utworzony i udostępniony (wszystkie stacje w sieci korporacyjnej muszą mieć do niego zdalny dostęp). Aby pozostałe stacje w sieci korporacyjnej aktualizowały się z tego folderu należy dodać w każdym module aktualizacji (na każdej stacji roboczej) nowy serwer aktualizacyjny – ścieżka zdalnego dostępu do tego folderu, np. *nazwa_komputera**mirror*.

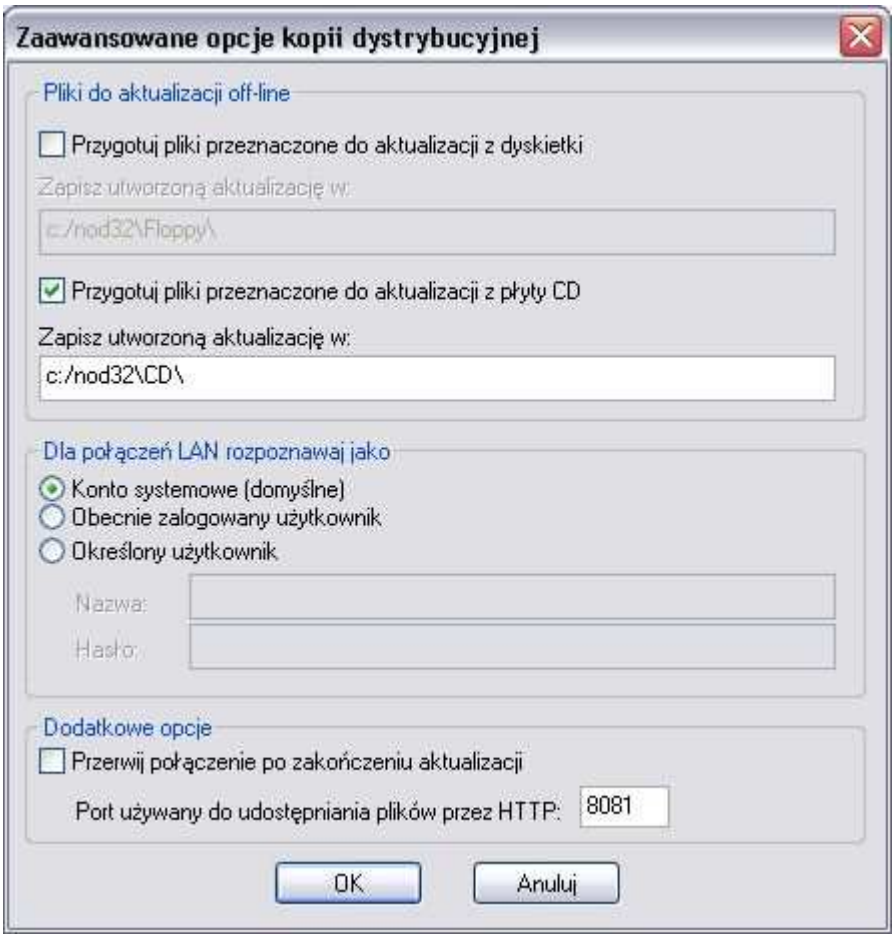
Istnieją dwie możliwości wprowadzenia ścieżki dostępu do folderu kopii dystrybucyjnej. Można to zrobić ręcznie lub należy nacisnąć przycisk ***Folder*** służący do przeglądania zasobów dysku w celu zlokalizowania docelowego folderu aktualizacyjnego.

Folder z aktualizacją może być umieszczony:

- na sieciowym dysku (np. z systemem operacyjnym Windows NT/2000/XP lub Novell NetWare). Należy wtedy wprowadzić nazwę użytkownika i hasło z prawami zapisu do tego folderu.
- na dysku lokalnym – nazwa użytkownika i hasło nie są wymagane.

Kolejna opcja: *„Włącz dostęp do plików przy pomocy protokołu HTTP"* umożliwia pracę NOD32 jako prostego serwera HTTP, pliki aktualizacyjne są dostępne przez HTTP. Cecha jest użyteczna w przypadku, gdy konieczne jest pobieranie aktualizacji przez HTTP.

Przycisk ***Zaawansowane*** umożliwia między innymi tworzenie plików aktualizacyjnych przeznaczonych do aktualizacji z dyskietki lub CD i ustawianie hasła dostępu do sieci LAN.



Aby utworzyć płytę aktualizacyjną, np. CD, przeznaczoną do aktualizowania stacji roboczych nie podłączonych do sieci, należy wybrać opcję: *„Przygotuj pliki przeznaczone do aktualizacji z płyty CD”,* a następnie wybrać folder, w którym zostanie utworzona aktualizacja. Domyślnie aktualizacja umieszczana jest w folderze *CD* umieszczonym w zasobach kopii dystrybucyjnej, np. *nazwa_komputera**mirror**CD*\. Tak utworzony podfolder *NOD_UPD* folderu *CD* należy zapisać do głównego folderu na płycie. Aby zaktualizować wybraną stację roboczą z CD, należy otworzyć zakładkę *Aktualizacja* programu NOD32, kliknąć na przycisk *Konfiguracja* i zmienić serwer aktualizacji. Należy wybrać napęd CD z listy serwerów (np. *X*:*nod_upd*, gdzie *X:* jest literą napędu CD–ROM). Wszystkie zmiany należy zaakceptować przyciskiem ***OK*** i uruchomić proces aktualizacji (przycisk ***Aktualizuj teraz***).

Należy zawsze pamiętać, iż NOD32 domyślnie pracuje jako użytkownik systemowy, dlatego też nie posiada uprawnień sieciowych zalogowanego użytkownika. W przypadku gdy kopia dystrybucyjna jest tworzona na serwerze w sieci lokalnej należy wybrać opcję *„Wybrany użytkownik"* oraz wprowadzić nazwę użytkownika i hasło posiadającego dostęp do serwera zawierającego folder kopii dystrybucyjnej (Novell NetWare, Windows NT 4.0/ 2000, itp.). Następnie należy zaznaczyć opcję *„Przerwij połączenie po wykonaniu aktualizacji"*, która spowoduje zamknięcie połączenia i wylogowanie zdefiniowanego użytkownika po wykonaniu aktualizacji.

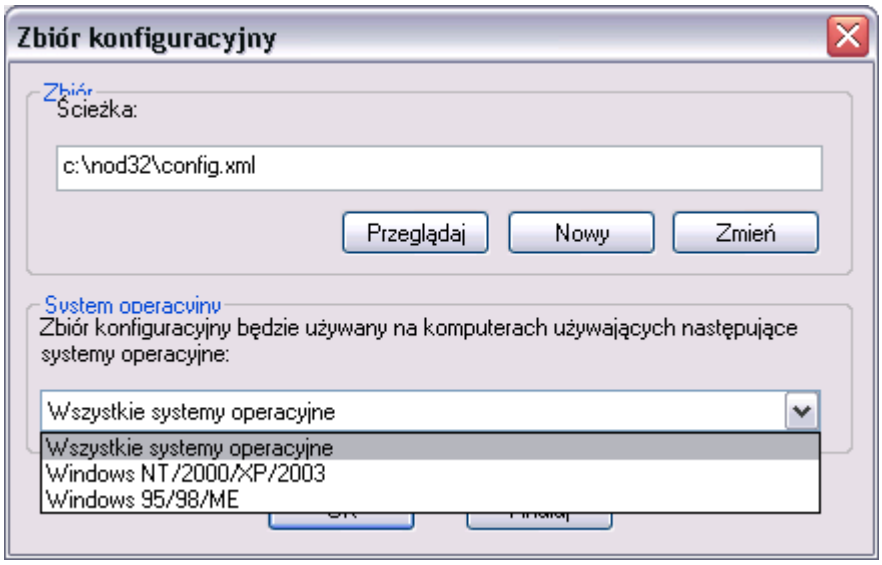
Jeżeli użytkownik pracujący na komputerze, który ma generować kopie dystrybucyjną i zapisywać ja na serwerze na stałe posiada uprawnienia do serwera aktualizacji, można wybrać opcję *„Obecnie zalogowany użytkownik"*. W tym przypadku należy pamiętać, że kopia dystrybucyjna będzie tworzona po zalogowaniu się użytkownika.

Opcja *„Port używany do dostarczania plików"* umożliwia wybranie portu, który będzie używany do aktualizacji przez HTTP.

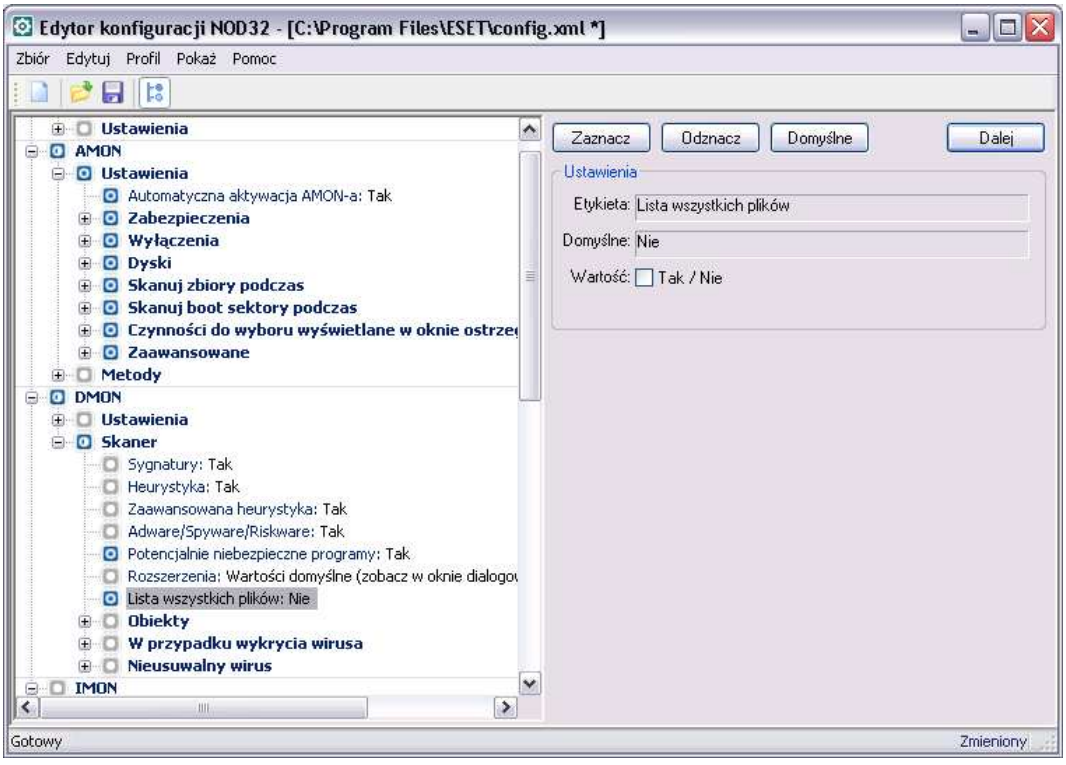
Pliki konfiguracyjne

Plik konfiguracyjny jest używany do modyfikowania konfiguracji **Systemu Antywirusowego NOD32** na stacjach roboczych w sieci LAN. Pliki wspierają różne systemy operacyjne.

Aby tworzyć lub edytować istniejące pliki konfiguracyjne należy wybrać przycisk ***Ustawienia***, a następnie przycisk ***Dodaj***. Aby edytować istniejący plik konfiguracyjny należy wybrać przycisk ***Przeglądaj***, wskazać miejsce położenia pliku i kliknąć kolejno ***Otwórz*** i ***Edytuj***. Aby stworzyć nowy plik konfiguracyjny należy wybrać przycisk ***Nowy*** i podać nazwę nowego pliku. W obu przypadkach zostanie uruchomiony Edytor konfiguracji NOD32, który umożliwia dokonanie zmian ustawień i zapisanie ich do pliku.



UWAGA: Do pliku zostaną zapisane tylko pozycje, które zostały zmienione (ikona jest koloru niebieskiego). Więcej informacji na temat Edytora konfiguracji można znaleźć w podrozdziale „Edytor konfiguracji NOD32".



Plik konfiguracyjny jest przeznaczony dla różnych systemów operacyjnych. Dostępne są następujące opcje:

Wszystkie systemy operacyjne
Windows NT/2000/XP
Windows 95/98/ME

UWAGA: Plik konfiguracyjny nie może być umieszczony w tym samym folderze co kopia dystrybucyjna.

Po utworzeniu pliku konfiguracyjnego w folderze kopii dystrybucyjnej jest tworzony plik tymczasowy o nazwie nodxxxx.xml (xxxx jest losowo generowaną liczbą), który zawiera tylko zmienione wartości i jest wczytywany przez stacje robocze w momencie aktualizacji.
Pliki konfiguracyjne utworzone w ten sposób mogą być użyte w procesie zdalnej instalacji lub do zmiany konfiguracji stacji roboczych aktualizujących się z lokalnej kopii dystrybucyjnej.
Aby zdalnie zainstalować oprogramowanie na stacjach roboczych można użyć skryptów logowania (Serwery Windows NT/2000/2003 lub Novell NetWare) lub Konsola Zdalnego Zarządzania Systemu NOD32.

Parametry linii poleceń

Parametry linii poleceń użyte z programem instalacyjnym umożliwiają zainstalowanie programu NOD32 z predefiniowanymi opcjami określonymi w pliku konfiguracyjnym, ponowne uruchomienie komputera, itp.
/SILENTMODE – aktywuje cichy tryb instalacji (instalacja będzie odbywać się 'w tle', bez interwencji użytkownika)
/UNINSTALL – odinstaluje obecnie zainstalowaną wersję
/FORCEOLD – wymusza ponowną instalację, nawet gdy nowsza wersja jest już zainstalowana.

/CFG= – definiuje nazwę pliku konfiguracyjnego, który będzie użyty w procesie instalacji (domyślnie nod32.xml)
/REBOOT – wymusza ponowne uruchomienie stacji po zakończonym procesie instalacji (należy stosować w cichym trybie instalacji)
/PWD= – pozwala na wprowadzenie hasła wymaganego do ponownej instalacji/ odinstalowania programu (należy stosować w cichym trybie instalacji)
/INSTMFC – umożliwia zainstalowanie biblioteki MFC – jeżeli jest wymagana (należy stosować w cichym trybie instalacji)

Przykład
następujący przykład przedstawia jak uruchomić instalację Systemu Antywirusowego NOD32 w tle, konfiguracja jest pobierana z serwera. Po wykonanej instalacji stacja automatycznie uruchomi się ponownie.
setup.exe /cfg="\\server\nod32\config.xml" /silentmode /reboot

Edytor konfiguracji NOD32

Edytor Konfiguracji pozwala na edycję i tworzenie plików konfiguracyjnych Systemu Antywirusowego NOD32. W lewej części głównego okna jest umieszczone drzewo konfiguracyjne, natomiast w prawej części można dokonywać zmian ustawień poszczególnych (wybranych) pozycji. Dla wygody pozycje w drzewie konfiguracyjnym zostały posortowane hierarchicznie zgodnie z modułami Systemu NOD32 lub nazwami profili. Każda pozycja w drzewie konfiguracji może być w dwóch stanach – zaznaczona lub nie zaznaczona.

UWAGA: Tylko zaznaczone pozycje zostaną zapisane!

W momencie otwarcia pliku konfiguracyjnego tylko pozycje występujące w pliku .xml będą zaznaczone. Aby zaznaczyć lub odznaczyć pozycję należy kliknąć na

niej dwa razy lub wybrać przycisk ***Zaznacz***/ ***Odznacz***. Aby przechodzić między pozycjami w drzewie konfiguracyjnym należy kliknąć na przycisk ***Dalej*** lub nacisnąć klawisz ***Enter***. Domyślne opcje dla poszczególnych pozycji mogą być odzyskane poprzez wybranie przycisku ***Domyślne***.

Opcjonalnie wszystkie podstawowe operacje mogą być wykonane z podręcznego menu Edytora.

Przyciski ***Zaznacz***, ***Odznacz*** i ***Domyślne*** są stosowane tylko w przypadku wybranych pozycji drzewa konfiguracyjnego. Jeżeli są jakieś dodatkowe podpunkty, wybrana funkcja zostanie zastosowana również dla nich.

Specjalne typy pozycji mają przypisaną nazwę profilu.

Zaznaczanie/odznaczanie pozycji w drzewie konfiguracyjnym dotyczy również profili. Jeżeli jakaś pozycja zawiera profil i zostanie odznaczona, to po zapisaniu zmian pozycja wraz z swoim profilem zostanie usunięta.

Profile i opcje dodawania ich są wspierane tylko w wybranych modułach. Lista modułów jest dostępna w menu Profil/Nowy Profil.

Pozycja *Profil* zawiera specjalną opcję przechowującą nazwę profilu (ikona z gwiazdką). Ikona z gwiazdką oznacza, że pozycja nie może być zaznaczona/odznaczona – jest zaznaczana/odznaczana automatycznie, gdy co najmniej jedna pod–pozycja pozycji profil jest zmieniona.

Aby dodać nowy profil do wybranego modułu należy zaznaczyć co najmniej jedną opcję aby profil mógł być zachowany i wprowadzić nową nazwę.

UWAGA: W momencie tworzenia nowego pliku, wszystkie wartości są ustawione domyślnie. Aby później powrócić do oryginalnych ustawień należy wybrać przycisk **Domyślne**.

Aby wyświetlić tylko zmienione pozycje w drzewie konfiguracji należy kliknąć na ikonę  .

Menu Edytora Konfiguracji

Plik

Nowy

Tworzy nowy plik konfiguracyjny z domyślnymi wartościami. Wszystkie pozycje są odznaczone. Aby zapisać pozycję należy ją wcześniej zaznaczyć.

Otwórz...

Otwiera istniejący plik konfiguracyjny. Jeżeli opcja *Pokaż wszystkie pozycje* jest włączona, wszystkie pozycje będą wyświetlone.

Zapisz

Zapisuje konfigurację i zmiany w bieżącym pliku. W przypadku tworzenia nowego pliku należy podać nazwę, pod którą będzie zapisany nowy plik konfiguracyjny.

Zapisz jako...

Zapisuje konfigurację pod nową nazwą.

Zapisz wybrane jako...

Zapisuje wybrane pozycje w nowym pliku konfiguracyjnym.

Eksportuj...

Zapisuje konfigurację pod nową nazwą. Nazwa i status bieżącego pliku nie zostanie zmieniona.

Zamknij

Zamyka bieżący plik konfiguracyjny.

Wyjdź

Zamyka Edytor Konfiguracji.

Edytuj

Zaznacz

Zaznacza wybrane pozycje w drzewie konfiguracyjnym.

Odznacz

Odznacza wybrane pozycje w drzewie konfiguracyjnym.

Zaznacz wszystkie

Zaznacza wszystkie pozycje w drzewie konfiguracyjnym.

Odznacz wszystkie

Odznacza wszystkie pozycje w drzewie konfiguracyjnym.

Ustaw domyślne wartości

Ustawia domyślne wartości dla wybranej pozycji w drzewie konfiguracyjnym.

Dalej

Przechodzi do kolejnej pozycji w drzewie konfiguracyjnym.

Profil

Nowy profil

Otwiera okno w którym można dodać nowy profil do wybranego modułu.

Usuń wybrany profil

Opcja jest dostępna, jeżeli pozycja profilu (który ma zostać usunięty) jest zaznaczona. Profil zostanie usunięty z drzewa a zmiany dokonane w bieżącym pliku zostaną zapisane po wyborze przycisku ***Zapisz***.

Pokaż

Pasek narzędzi

Wyświetla/ ukrywa pasek narzędzi.

Pasek stanu

Wyświetla/ ukrywa pasek stanu.

Wszystkie pozycje

Opcja jest aktywna, gdy jest otwarty plik konfiguracyjny. Włączenie opcji spowoduje wyświetlenie się wszystkich pozycji pliku (zaznaczonych i niezaznaczonych). Jeżeli opcja nie jest wybrana, tylko zaznaczone pozycje

będą pokazane. Można również włączyć/ wyłączyć opcję klikając na ikonę  .

Pomoc

Edytor konfiguracji NOD32 pomoc

Pomoc edytora konfiguracji.

Index

Wyświetla index pomocy.

Znajdź

Wyświetla zakładkę Szukaj.

ESET w Internecie

Otwiera stronę internetową Producenta Systemu Antywirusowego NOD32.

Edytorze Konfiguracji NOD32

Wyświetla numer wersji Edytora Konfiguracji NOD32 .

NOD32 dla DOS

Rozdział zawiera podstawowe informacje dotyczące używania i konfiguracji programu NOD32 dla DOS–a. Użytkownicy systemu Windows będą z niego korzystać przede wszystkim w przypadku awarii systemu. Program ten jest jedynie skanerem „na żądanie" i nie posiada rezydentnego skanera. W chwili pisania podręcznika NOD32 dla DOS–a dostępny jest tylko w angielskiej wersji językowej. Polska wersja jest w przygotowaniu. Należy pamiętać, że wersja dla DOS–a nie umożliwia inkrementacyjnej aktualizacji bazy danych i za każdym razem należy pobierać z serwera aktualizacyjnego pełną wersję programu.

NOD32 dla DOS–a można uruchamiać bezpośrednio z płyty CD–ROM lub dyskietki, przy pomocy polecenia ***nod32dos.exe***. Po uruchomieniu, zostaje załadowany gotowy do pracy skaner programu NOD32.

W zakładce Targets (Obiekty skanowania) można wybrać dyski, które mają być skanowane. Możliwe jest wybieranie dysków indywidualnie lub grupowo – wszystkie dyski lokalne (***Local***), sieciowe (***Network***), dyskietki lub CD–ROM–y.

Istnieje także możliwość zaznaczenia do skanowania jedynie wybranych katalogów. W celu przeskanowania wybranych katalogów należy w bloku ***Directories*** wybrać ***Add*** (dodaj) a następnie w oknie *Add directory* wpisać pełną ścieżkę dostępu do katalogu, który ma być skanowany (np. C:\Windows\System32). Aby usunąć wybrany katalog należy podświetlić go i przycisnąć ***Remove***.

Po zakończeniu konfiguracji można przystąpić do skanowania wybierając ***Scan*** (jeżeli chcemy tylko wykonać skanowanie) lub ***Clean*** (gdy chcemy, by system wykonał skanowanie i usunął znalezione wirusy).

Przed pierwszym skanowaniem należy sprawdzić i ewentualnie zmodyfikować opcje skanowania. W tym celu w zakładce Setup należy wybrać odpowiednie przełączniki w blokach: ***Diagnostics Targets*** (Obiekty skanowania), ***Diagnostics methods*** (Metody skanowania), ***Heuristic sensitivity*** (Czułość analizy heurystycznej), ***On virus detection*** (Po wykryciu wirusa), ***Log*** (Dziennik zdarzeń), ***On virus detection*** (Po wykryciu wirusa, którego nie udało się usunąć) oraz ***System*** (System).

Konfiguracja

Diagnostics Targets (Obiekty, które mają być skanowane): – w tym bloku można wybrać obiekty do skanowania

Files (Pliki)

Boot sectors (Boot sektory)

Memory (Pamięć)

Diagnostics methods (Metody skanowania) – należy wybrać metody skanowania

Signatures (Sygnatury)
Heuristics (Analiza heurystyczna)
Runtime packers (Programy pakujące pliki)
Archives (Archiwa)

Heuristic sensitivity (Czułość analizy heurystycznej) – blok ten jest odpowiedzialny za ustawienie czułości analizy heurystycznej

Safe (Podstawowa)
Standard (Standardowa)
Deep (Wysoka)

On virus detection (Po wykryciu wirusa) – w tym bloku deklarujemy jaka akcja ma być podjęta w przypadku wykrycia wirusa.

Clean (Usuń wirusa)
Offer an action (Zaproponuj rozwiązanie)
Leave unchanged (Pozostaw bez zmian)
Rename (Zmień nazwę)
Delete (Usuń plik)
Replace (Przenieś do katalogu kwarantanny)

Log (Dziennik zdarzeń) – opcje dotyczące Dziennika zdarzeń

Enabled (Włącz dziennik)
Wrap log (Przewijaj dziennik zdarzeń)
Append (Dopisuj)
Overwrite (Nadpisuj)

Należy wybrać wielkość (***Max. Length [Kb]***) i nazwę (***Name***) Dziennika zdarzeń.

On virus detection (Po wykryciu wirusa) – w przypadku gdy wirus nie może zostać automatycznie usunięty, można wybrać akcję dodatkową

Offer an action (Zaproponuj rozwiązanie)
Leave unchanged (Pozostaw bez zmian)

Rename (Zmień nazwę)

Delete (Usuń plik)

Replace (Przenieś do katalogu kwarantanny)

System

List all files (Wyświetlaj wszystkie skanowane pliki)

Sound signal (Sygnał dźwiękowy)

Ponadto, istnieje możliwość wyboru typów plików do skanowania (***Extensions***). Możliwe jest wybranie skanowania wszystkich plików, bądź tylko plików o wybranych rozszerzeniach. Lista skanowanych rozszerzeń może być modyfikowana: dodawanie nowych rozszerzeń (***Add***), usuwanie (***Delete***) i przywracanie domyślnej listy rozszerzeń (***Default***).

Przycisk (***Save***) powoduje zapisanie wybranych ustawień do pliku nod32.cfg. Ustawienia domyślne można w każdej chwili przywrócić przyciskiem (***Defaults***). Ustawienia wcześniej zapisane na dysku można wczytać przyciskiem (***Load***).

W zakładce ***Log*** (Dziennik skanowania) zapisywane są wszystkie wyniki skanowania.

Uruchamianie programów NOD32 i NOD32DOS z linii komend

NOD32 i NOD32DOS można uruchamiać z linii komend posługując się w tym celu komendą ***NOD32.EXE*** i odpowiednimi przełącznikami.

Format komend ma następującą postać:

NOD32.EXE [przełącznik1, przełącznik2, ...] [ścieżka1, ścieżka2, ...]

Możliwe do zastosowania parametry oraz ich format zostały opisane w rozdziale *Parametry używane przez NOD32*. Ścieżki określają odpowiednie nazwy dysków, folderów lub plików.

UWAGA: Wszystkie znaki specjalne (np. spacja) jak również całe ścieżki muszą być umieszczane w cudzysłowie, np. „*C:\Program Files*".

Parametry używane przez NOD32

Większość parametrów jest włączana lub wyłączna przy pomocy znaku plus (+) lub minus (–). Na przykład aby włączyć test poprawności programu NOD32 należy użyć przełącznika "/selfcheck+" , natomiast aby wyłączyć: "/selfcheck–".

Ogólne

/help – wyświetla listę przełączników programu

/selfcheck+ (–) – włączenie (wyłączenie) testu poprawności programu NOD32

/expire+ (–) – włączenie (wyłączenie) powiadomienia o ważności programu

/subdir+ (–) – włączenie (wyłączenie) skanowania podfolderów

/multi+ (–) – włączenie (wyłączenie) plikowego skanowania dyskietek

/sound+ (–) – włączenie (wyłączenie) ostrzeżenia dźwiękowego

/list+ – tworzenie listy wszystkich testowanych obiektów w Dzienniku zdarzeń

/list– – tworzenie listy tylko zainfekowanych obiektów w Dzienniku zdarzeń

/break+ (–) – włączenie (wyłączenie) przerwy w skanowaniu

/scroll+ (–) – włączenie (wyłączenie) przewijania Dziennika zdarzeń

/quit+ (–) – program automatyczne zamyka się (nie zamyka się) po wykonaniu skanowania

Wykrywanie

/pattern+ (–) – włączenie (wyłączenie) skanowania przy użyciu sygnatur/ baz wirusów

/heur+ (–) – włączenie (wyłączenie) analizy heurystycznej

/scanfile+ (–) – włączenie (wyłączenie) skanowania plików

/scanboot+ (–) – włączenie (wyłączenie) skanowania boot sektorów

/scanmbr+ (–) – włączenie (wyłączenie) skanowania MBR

/arch+ (–) – włączenie (wyłączenie) skanowania archiwów (ZIP, ARJ i RAR)

/pack+ (–) – włączenie (wyłączenie) skanowania programów pakujących pliki

/local – skanowanie wszystkich lokalnych dysków

/networkScan – skanowanie wszystkich dysków sieciowych

/ext=<LIST> – dodawanie nowego rozszerzenia do listy skanowanych rozszerzeń (Zbiorowe wprowadzanie rozszerzeń np. /ext=EXT1,EXT2)

/all – skanowanie wszystkich plików bez względu na rozszerzenie

Analiza Heurystyczna

/heursafe – ustawienie czułości analizy heurystycznej na podstawowy poziom (minimalizuje generowanie fałszywych alarmów)

/heurstd – ustawienie czułości analizy heurystycznej na standardowy poziom

/heurdeep – ustawienie czułości analizy heurystycznej na wysoki poziom

Dziennik zdarzeń

/log+ (–) – włączenie (wyłączenie) generowania Dziennika zdarzeń
/wrap+ (–) – włączenie (wyłączenie) zawijania informacji w Dzienniku zdarzeń
/logappend – włączenie dopisywania informacji do Dziennika zdarzeń
/logrewrite – włączenie nadpisywania Dziennika zdarzeń
/logsize=N – ustawienie maksymalnej wielkości Dziennika zdarzeń (rozmiar N KB))
/log=<FILENAME> – ustawienie nazwy Dziennika zdarzeń (np. /log=NOD.LOG)

Czynności

/clean – leczenie zainfekowanych obiektów (jeśli jest możliwe)
/prompt – proponowanie rozwiązania przy każdym zainfekowanym obiekcie
/rename – zmiana nazwy zainfekowanych plików
/delete – usuwanie zainfekowanych plików
/replace – zastępowanie kodu zainfekowanego boot sektora nie zainfekowanym, standardowym kodem.

UWAGA: Jeśli zostały użyte przełączniki: /prompt, /rename, /delete/ lub /replace jednocześnie z przełącznikiem /clean, odpowiednia czynność zostanie wykonana tylko w przypadku gdy zainfekowany plik nie może być wyleczony (jest zainfekowany robakiem lub trojanem).