System antywirusowy NOD32
polska wersja językowa

przewodnik użytkownika

www.NOD32.pl

2001

Informacje kontaktowe

producent:
ESET, LLC
Suite 300
4025 Camino del Rio South
San Diego, CA 92108
www.nod32.com

dystrybutor w Polsce:
DAGMA sp. z o.o.
ul. Pszczyńska 15
40-478 Katowice, Poland
Tel: +48-32-202 11 22
Fax: +48-32-202 55 55
www.nod32.pl
www.dagma.pl

E-mail:
sprawy handlowe – nod_sales@nod32.pl
sprawy techniczne – nod_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 Techniczna na stronie www.nod32.pl

Spis treści

Wprowadzenie

Witamy w szybko rosnącej rodzinie użytkowników programu antywirusowego NOD32. W okresie ostatnich kilku lat udało nam się opracować produkt, który charakteryzuje się bardzo wysoką stabilnością i niezawodnością oraz skutecznością w wykrywaniu i eliminowaniu zagrożeń wirusowych. Zostało to potwierdzone szeregiem międzynarodowych wyróżnień i certyfikatów. W tej chwili do Państwa dyspozycji przedstawiamy polską wersję systemu.

Dla Państwa wygody przygotowaliśmy przewodnik użytkownika programu antywirusowego NOD32. Zawiera on najbardziej istotne informacje niezbędne do zainstalowania i uruchomienia programu oraz postępowania w sytuacjach awaryjnych. Więcej można się dowiedzieć z pełnej instrukcji systemu dostępnej na dysku i na stronie www.NOD32.pl w formacie pdf . Do odczytania instrukcji konieczna jest bezpłatna przeglądarka „Acrobat Reader", której wersja instalacyjna znajduje się na płycie lub może być pobrana ze strony producenta (www.adobe.com). Pomoc dotyczącą programu NOD32 i jego poszczególnych modułów można 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.

4

Analiza heurystyczna

Czy posiadając dobry system ochrony antywirusowej możesz się czuć 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. A najwięcej (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 jednak rozwiązać poprzez zastosowanie **zaawansowanych narzędzi heurystycznych**.

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

Czy słyszałeś o słynnych wirusach Romeo i Julia, LoveLetter, MTX, Kurnikova, 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 **moduł 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!**

Oczywiście, rewelacyjna heurystyka to nie wszystko co NOD32 ma do zaoferowania! Jest bardzo szybki, skuteczny, łatwo się instaluje, automatycznie aktualizuje za pośrednictwem Internetu, chroni zarówno zbiory jak i pocztę elektroniczną, ma małe wymagania systemowe, rozsądną cenę, bezpłatną pomoc techniczną i polską wersję językową – czyli to co powinien mieć każdy dobry program!

Jednak nie każdy dobry program antywirusowy ma to co NOD32 – REWELACYJNĄ HEURYSTYKĘ!

Opis systemu, wymagania sprzętowe, nośniki

Nowa generacja systemu antywirusowego NOD32 jest produktem najwyższej jakości, co jest wynikiem naszego wieloletniego doświadczenia oraz zastosowania najnowocześniejszych technologii. Intencją twórców było wyposażenie użytkownika we wszystkie środki do niezawodnego wykrywania i usuwania wirusów komputerowych, jakie mogą mu być potrzebne. Bardzo sobie cenimy zaufanie do naszego produktu, które motywuje nas do dalszej jeszcze bardziej wytężonej pracy. Dotychczasowe imponujące sukcesy NOD-a są gwarancją, że będzie on narzędziem, które efektywnie dba o bezpieczeństwo Twoich danych.

System antywirusowy NOD32 składa się z trzech programów:

- NOD32 – samodzielnego, 32-bitowego skanera „na żądanie" dla Windows®95, Windows®98, WindowsNT® i Windows®2000,

- AMON-a – rezydentnego skanera antywirusowego dla wymienionych wyżej platform,

- NOD32DOS – program uruchamiany w środowisku DOS.

Szczegółowe informacje jak obsługiwać wymienione moduły programu znajdziesz w instrukcji zamieszczonej na płycie CD oraz plikach pomocy dostępnych w dowolnym momencie pod klawiszem F1. Mając na uwadze łatwość obsługi, programy NOD32 i AMON mają prawie (lub całkowicie) identyczne panele kontrolne. W celu ułatwienia posługiwania się podręcznikiem, opisy poszczególnych (nawet identycznych) paneli zostały wykonane niezależnie dla każdego z modułów systemu.

Wymagania systemowe. NOD32 ma niewielkie wymagania systemowe. W przypadku stanowisk pracujących pod systemem operacyjnym DOS wystarczy procesor 386DX, 10MB wolnej przestrzeni na dysku, 12MB RAM i karta graficzna VGA. Do pracy pod systemem Windows wymagany jest procesor 386DX (zalecany Pentium), 30MB przestrzeni na dysku, 32MB RAM i karta graficzna typu VGA (zalecana SVGA 800x600, 65536 kolorów). Tak małe wymagania sprzętowe udało się uzyskać dzięki zaprogramowaniu kluczowych modułów systemu przy pomocy języka niskiego poziomu ASSEMBLER.

System NOD32 może zostać bezpośrednio pobrany z serwera internetowego, lub dostarczony na nośniku CD-ROM. W przypadku instalacji programu z nośnika istotne jest natychmiastowe zarejestrowanie systemu i ściągnięcie z serwera internetowego najbardziej aktualnej bazy danych wirusów. Patrz rozdział „Aktualizacja systemu".

Instalacja systemu antywirusowego NOD32

Przed rozpoczęciem instalacji należy sprawdzić, czy na dysku znajduje się wystarczająco dużo miejsca. Instalacja 32-bitowego programu NOD wymaga około 30 MB wolnej przestrzeni.

Instalacja rozpoczyna się od uruchomienia programu SETUP.EXE znajdującego się w folderze \win95PL\disk1 płyty instalacyjnej dla systemów Windows 9x lub \winntPL\disk1 dla systemów Windows NT/2000.

W pierwszym kroku, program instalacyjny NOD poszukuje poprzednich wersji programu, które mogą już być zainstalowane na dysku. W przypadku wykrycia starszych wersji, dalsza instalacja polega na zastąpieniu starej wersji nową z zachowaniem dotychczasowej konfiguracji.

Jeżeli NOD32 nie był do tej pory instalowany na dysku, po zaakceptowaniu umowy licencyjnej instalator pozwala na wybór **foldera docelowego**, do którego program zostanie zainstalowany. W dalszej części instalator zapyta, czy przy każdym uruchomieniu Windows powinien automatycznie uruchamiać się skaner rezydentny AMON (należy wybrać tą opcję), czy chcemy aby program się automatycznie aktualizował (należy wybrać tą opcję) oraz czy chcemy zainstalować skaner antywirusowy dla poczty elektronicznej. Jeżeli używasz programu Microsoft Outlook zaznacz opcję **Skaner poczty NOD32 dla MAPI**, jeżeli programu Outlook Experss, Eudora lub Netscape Messenger zaznacz opcję **Skaner poczty NOD32 dla POP3** (jeżeli masz wątpliwości, którą opcję wybrać, możesz nie instalować skanera poczty teraz i zainstalować go później, w dowolnym momencie). W końcowej części instalacji pojawi się okno pozwalające na dołączenie skanera NOD32 do menu kontekstowego oraz umieszczenie ikony NOD32 na pulpicie. Po zakończeniu instalacji zalecane jest ponowne uruchomienie systemu Windows.

Po poprawnym zakończeniu instalacji i ponownym uruchomieniu komputera NOD32 poprosi o skonfigurowanie **Konsoli administratora NOD32** (patrz rozdział „Aktualizacja systemu”) i **Skanera NOD32 dla POP3** (jeśli
wybraliśmy go w procesie instalacji; patrz rozdział „Konfigurowanie skanera NOD32 dla POP3”). Opis sposobu konfiguracji Skanera poczty NOD32 dla MAPI dostępny jest w pliku readme.txt oraz instrukcji użytkownika dostępnej na płycie CD.

Po zakończeniu konfiguracji na pulpicie pojawi się ikona skanera „na żądanie” NOD32 (dyskietka z niebieskim krzyżem) a na pasku zadań ikona rezydentnego skanera AMON (dyskietka z czerwonym krzyżem) oraz Konsoli administratora NOD32 (dyskietka z symbolem CC). Jeżeli został zainstalowany skaner poczty POP3, pojawi się również jego ikona (biała koperta z czerwonym krzyżem).

Odinstalowanie programu następuje po wybraniu opcji Odinstaluj (Uninstall) z grupy programów ESET z menu Start.

Ostrzeżenie: Jednoczesne użytkowanie dwóch rezydentnych skanerów antywirusowych na platformie Windows może doprowadzić do niestabilności systemu. W związku z tym, jeżeli instalujemy NOD32 w systemie, w którym zainstalowany jest również inny program antywirusowy, należy wcześniej odinstalować lub wyłączyć dotychczasowy skaner.

Rejestracja użytkownika

W przypadku programu NOD32 zarejestrowanie się użytkownika jest konieczne, gdyż uruchamia ono możliwość aktualizowania bazy danych wirusów i zbiorów systemowych w trybie on-line.

Aktualizacja systemu

Sprawna aktualizacja systemu antywirusowego jest sprawą pierwszoplanową! Pierwszą aktualizację należy wykonać niezwłocznie po zainstalowaniu programu. Jest to szczególnie istotne w przypadku programów instalowanych z płyty CD-ROM, gdyż znajdujące się na nich wersje nigdy nie są najbardziej aktualne.

Aktualizacja systemu NOD32 może odbywać się w trybie on-line poprzez Internet lub z lokalnej sieci komputerowej oraz w przypadku wolno stojących stanowisk z dyskietki (sposób aktualizacji z dyskietki lub sieci opisany jest w instrukcji zamieszczonej na płycie CD).

Aktualizacja w trybie on-line odbywa się za pośrednictwem Internetu z jednego z serwerów aktualizacyjnych (niezbędne jest aktywne połączenie z Internetem!), których adresy znajdziesz na karcie licencyjnej dostarczonej wraz z systemem. Do aktualizacji niezbędne jest wykorzystanie nazwy użytkownika oraz hasła, które zostaną dostarczone po zarejestrowaniu oprogramowania (patrz rozdział „Rejestracja użytkownika").

Konfiguracja opcji aktualizacji jest możliwa w zakładce **Aktualizacja** w Konsoli administratora (okno, które pojawia się na ekranie automatycznie po ponownym uruchomieniu systemu zaraz po zakończeniu instalacji; można je także wywołać klikając na ikonę Konsoli Administratora na pasku zadań). Przed dokonaniem aktualizacji należy dokonać konfiguracji programu podając nazwę serwera, z którego aktualizacja zostanie pobrana, wprowadzić nazwę użytkownika i hasło oraz w **Setup połączenia** ustawić sposób łączenia się komputera z Internetem (sieć/połączenie stałe/modem). Po zakończeniu konfiguracji należy kliknąć na **Aktualizuj teraz** i program zostanie zaktualizowany.

Aby dopisać serwer aktualizacyjny do listy dostępnych serwerów należy wybierać przycisk **Serwery...**, w polu **Nowy** wpisać adres, np. http://www.nod32.pl, i kliknąć przycisk **Dodaj serwer** i **Zamknij**. Następnie w polu **Serwer:** wybrać opcję www.nod32.pl.
Więcej informacji na temat konfiguracji aktualizacji znajdziesz w pliku pomocy po naciśnięciu klawisza F1 lub w instrukcji na CD.

Skanowania zasobów komputera

Po zainstalowaniu i zaktualizowaniu systemu, należy wykonać skanowanie zasobów komputera, by upewnić się, że żaden z plików nie zawiera wirusa. Do tego celu służy skaner **NOD32** „na żądanie", którego ikona znajduje się na pulpicie (dyskietka z niebieskim krzyżem).

Uruchom skaner a następnie zaznacz dyski lub foldery, które chcesz skanować klikając na nie dwukrotnie (dyski lub foldery wybrane do skanowania są odznaczone czerwonym √). Po wybraniu zasobów, które mają być sprawdzane kliknij na przycisk **Skanuj**. System rozpocznie od sprawdzenia pamięci operacyjnej komputera a następnie będzie skanować zaznaczone zasoby. Wyniki skanowania zostaną umieszczone w **Dzienniku zdarzeń**. W przypadku znalezienia wirusa zainfekowane pliki zostaną oznaczone kolorem czerwonym. Informacje, jak usunąć wirusy z

zainfekowanych plików znajdziesz w zbiorach pomocy po wciśnięciu klawisza F1.

Generowanie dyskietki ratunkowej

Uwaga! Należy pamiętać o utworzeniu dyskietki ratunkowej, która jest niezbędna w przypadku awarii systemu.

Posiadanie dyskietki ratunkowej pomaga uruchomić i „wyleczyć" zainfekowany komputer. Należy jej używać, gdy istnieje podejrzenie, że program antywirusowy uległ uszkodzeniu i nie działa poprawnie lub że wirus uszkodził system operacyjny (Windows) i nie działa on prawidłowo.

Zestaw ratunkowy składa się z **dyskietki startowej** zawierającej system operacyjny, która pozwala na uruchomienie komputera oraz **dyskietki ratunkowej**, na której umieszczony jest program antywirusowy. Do przygotowania zestawu ratunkowego niezbędne są dwie czyste, sformatowane dyskietki.

Sposób przygotowania **dyskietki startowej** znajdziesz w dokumentacji swojego systemu operacyjnego (Windows). Opisz tą dyskietkę jako „**dyskietka startowa"**. Na drugą dyskietkę, oznaczoną jako **„dyskietka ratunkowa"** należy skopiować pliki **nod32dos.exe**, **nod32.000** z katalogu DOS32, który znajduje się na płycie z programem NOD32.

Uwaga!!

1) **Do tworzenia zestawu ratunkowego należy używać komputera, który został wcześniej sprawdzony przez skaner antywirusowy NOD32.**
2) **Należy pamiętać o aktualizacji programu NOD32 dla DOS na „dyskietce ratunkowej". Aktualizację wersji DOS wykonujemy poprzez ściągnięcie pełnego programu NOD32 dla DOS z serwera aktualizacyjnego i zastąpienie plików na dyskietce aktualnymi wersjami.**

Uruchamianie systemu z dyskietki ratunkowej

W przypadku jeżeli wystąpi awaria systemu, której przyczyną może być infekcja wirusowa, należy ponownie uruchomić komputer posługując się
dyskietką startową z utworzonego wcześniej zestawu awaryjnego. (Należy zwrócić uwagę na to by w BIOS-ie była wybrana opcja uruchamiania systemu z dyskietki.)

Po uruchomieniu komputera – dyskietkę startową zastępujemy w napędzie **dyskietką ratunkową** i wpisujemy polecenie **a:\nod32dos.exe.** Uruchomi ono skaner NOD32 dla DOS-a. Należy wybrać dyski, które mają być skanowane i uruchomić skaner (więcej informacji na ten temat w rozdziale „NOD32 dla DOS-a"). Po zakończeniu usuwamy dyskietkę ze stacji dysków i ponownie uruchamiamy system.

Jeżeli zamierzamy zainstalować NOD32 na komputerze, który mógł być wcześniej zainfekowany, wskazane jest przed rozpoczęciem instalacji uruchomienie go z **dyskietki startowej** i sprawdzenie dysków skanerem **nod32dos.exe**.

Elementy systemu NOD32

System NOD32 składa się z czterech programów: Skanera NOD32 „na żądanie", rezydentnego skanera AMON, Konsoli administratora oraz Skanera poczty POP3 i MAPI. W dalszej części rozdziału przedstawione zostały zastosowania oraz funkcje każdego z nich.

Skaner NOD32 „na żądanie"

Skaner „na żądanie" służy do sprawdzania czy zasoby komputera (pamięć operacyjna, zbiory na dyskach) nie zawierają wirusów. Pierwsze skanowanie przy pomocy skanera powinno zostać wykonane zaraz po zainstalowaniu systemu. Jeżeli jest to możliwe, przed skanowaniem należy zarejestrować program i wykonać jego aktualizację. Jeżeli nie, zalecane jest przeprowadzenie skanowania przy pomocy posiadanej wersji. Do poszukiwania wirusów, NOD32 wykorzystuje moduł analizy heurystycznej, który zapewnia skuteczność programu nawet w przypadku jeżeli baza danych wirusów nie była przez pewien czas aktualizowana. **Oznacza to,** że nasz komputer jest stosunkowo bezpieczny nawet jeżeli z różnych powodów przez kilka dni nie było możliwe aktualizowanie systemu. **Nie oznacza to**, że można w ogóle zaniechać aktualizacji! Moduł heurystyczny daje bardzo wysokie prawdopodobieństwo wykrywania wirusów (również takich, które do tej pory nie były znane!) ale nie daje 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. Proponujemy wykonywać je nie rzadziej niż raz w tygodniu a dodatkowo po każdej aktualizacji systemu lub bazy sygnatur wirusowych.

UWAGA! WAŻNA INFORMACJA (dotycząca skanowania i usuwania wirusów na żądanie)!

1) Przed rozpoczęciem skanowania i usuwania wirusów na żądanie, zalecane jest zakończenie wszystkich uruchomionych aplikacji.
2) 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.
3) By upewnić się co do skuteczności usunięcia wirusów, należy powtórzyć skanowanie po ponownym uruchomieniu komputera.

Skaner rezydentny AMON

AMON jest rezydentnym modułem, który powinien przez cały czas pozostawać aktywny w pamięci operacyjnej systemu. Śledzi on wszystko co dzieje się ze zbiorami (tworzonymi, otwieranymi, uruchamianymi, zapisywanymi, archiwizowanymi, itp.) i analizuje, czy nie zawierają wirusów. W przypadku zagrożenia, automatycznie usuwa wirusa lub izoluje zawierający go zbiór. Jeżeli nie ma istotnych powodów by dezaktywować AMON-a nigdy nie należy tego robić!

O tym, że moduł został uruchomiony świadczy ikona dyskietki z czerwonym krzyżem na pasku narzędzi. Klikając na nią możemy stwierdzić, czy moduł AMON-a jest aktywny. Jeżeli tak, w lewym górnym rogu okna AMON-a pulsuje logo NOD-a.

W trakcie instalacji system proponuje automatyczne aktywowanie AMON-a przy każdym uruchomieniu systemu – bez ważnych powodów nie należy zmieniać tej opcji! Podobnie jak w przypadku skanera na żądanie, wiele opcji dotyczących funkcjonowania AMON-a podlega konfiguracji. Szczegółowe informacje na ten temat znajdziesz w plikach pomocy (wciśnij klawisz F1).

Konsola administratora

Moduł Konsoli administratora NOD32 (NOD32CC) realizuje między innymi automatyczną aktualizację systemu antywirusowego NOD32. Szczegółowe informacje na temat korzystania z Konsoli administratora w trybie „stacja robocza" znajdziesz w pliku pomocy (klawisz F1). Informacje na temat instalowania Konsoli administratora w trybie „LAN" znajdują się w instrukcji użytkownika na płycie CD.

Skanowanie poczty, praca w Internecie

Ponieważ obecnie dominująca (ponad 95%) liczba infekcji wirusowych dociera do użytkowników komputerów poprzez Internet, bardzo istotne jest zabezpieczenie się przed tymi zagrożeniami. Poniżej przedstawiamy podstawowe informacje na temat instalacji i konfiguracji NOD32 do współpracy z programami pocztowymi korzystającymi z protokołu POP3 (np. Outlook Express, Netscape Messenger, Eudora, itp.). NOD32 współpracuje również z programami korzystającymi z interfejsu MAPI (np. Microsoft Outlook). Szczegółowe informacje na temat współpracy i konfiguracji do pracy z MAPI znajdziesz w pliku readme.txt oraz instrukcji użytkownika na płycie CD.

Jak działa ten skaner?
Skaner NOD 32 dla POP3 sprawdza wszystkie wiadomości w chwili ich przesyłania z serwera poczty (POP3 serwer) do programu pocztowego (POP3 klient). W chwili przechodzenia danych przez skaner są one sprawdzane na obecność wirusów. W przypadku znalezienia wirusa zostaje wyświetlony komunikat ostrzegawczy.

Jest to tylko alarm ostrzegający przed otwieraniem zainfekowanego załącznika. Decyzja, co zrobić z zainfekowanym załącznikiem należy do użytkownika. Skaner sam nie usuwa wirusa! Do tego celu należy użyć skanera „na żądanie".

Aby usunąć wirusy z zainfekowanych załączników wiadomości należy uruchomić skaner **NOD32** i zaznaczyć „Foldery osobiste" w polu **Foldery** zakładki **Obiekty** i wybrać **Usuń wirusy**. Dodatkowo, w przypadku infekcji zalecamy przeskanowanie całych zasobów komputera, które mogły ulec zarażeniu.

Pomimo, że zainfekowana wiadomość dociera do skrzynki pocztowej, zasoby komputera są bezpieczne! W momencie, gdy nastąpi próba otwarcia zainfekowanego załącznika przez użytkownika lub jego samoistnego aktywowania się (tego typu wirusy już występują), pełną ochronę zasobów komputera przejmuje AMON – rezydujący w pamięci monitor, który nie pozwoli rozprzestrzenić się wirusowi.

Instalacja skanera NOD32 dla POP3

W czasie pierwszej instalacji NOD-a na stacji roboczej pojawia się okno dialogowe, dające możliwość instalacji rezydentnego modułu ochrony poczty NOD32 dla POP3. Moduł ten można także zainstalować w późniejszym okresie (patrz instrukcja na dysku CD), jeżeli nie zrobiliśmy tego przy pierwszej instalacji lub zablokować, jeżeli chcemy przestać z niego korzystać.

Konfigurowanie skanera NOD32 dla POP3.

W celu zapewnienia poprawnej i skutecznej pracy skanera musi on zostać odpowiednio skonfigurowany. Po pierwszej instalacji NOD32 i po ponownym uruchomieniu systemu Windows na ekranie pojawia się okno konfiguracyjne skanera **Setup NOD32 dla POP3** (jeśli wybraliśmy go w trakcie instalacji). Przed rozpoczęciem konfiguracji należy pamiętać o zamknięciu programu pocztowego. Dostępne są dwa sposoby konfiguracji: automatyczna i ręczna. Automatyczna konfiguracja polega na samoczynnym pobraniu danych kont z Microsoft Outlook lub Outlook Express i sprowadza się do wybrania opcji **Auto Konf** w oknie **Setup NOD32 dla POP3**. Po wykonaniu tej czynności zaimportowane zostaną dane wszystkich kont z naszego domyślnego klienta pocztowego, który również zostanie skonfigurowany do współpracy ze skanerem pocztowym.

Skaner poczty można skonfigurować także w późniejszym terminie uruchamiając skaner **NOD32 dla POP3** (klikając na ikonę białej koperty z czerwonym krzyżem na pasku zadań), następnie wcisnąć przycisk **Setup** i w polu **Konta** wybrać **Auto Konf**.

Po zakończeniu konfiguracji odbierana poczta w pierwszej kolejności będzie skanowana przez skaner NOD32 dla POP3, a dopiero potem umieszczana w skrzynce odbiorczej.

Ręczna konfiguracja pozwala na ustawienie opcji skanera dla POP3 i konfigurację domyślnego klienta pocztowego. Opcja ta jest przydatna w przypadku gdy np.: dodajemy nowe konto i została szczegółowo opisana w
pełnej instrukcji użytkownika. Sposób wykonania ręcznej konfiguracji opisany jest w instrukcji na płycie CD.

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 wyświetlaniu wiadomości informacyjnej. Jeżeli skaner NOD32 dla POP3 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.

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 chwili obecnej 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 poskanowania 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**)** i **System (**System**)**.

Diagnostics Targets (Obiekty skanowania) – 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 zbiory)
- 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 zbiory)
- 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 plików 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.

Postępowanie w sytuacjach awaryjnych

Stosowanie programu NOD32 minimalizuje ryzyko związane z zakłóceniem pracy systemu przez działanie wirusów komputerowych. Infekcja może jednak mieć miejsce w przypadku, gdy nie została zaktualizowana baza sygnatur wirusowych, został źle zainstalowany skaner poczty elektronicznej lub operator wyłączył moduł rezydentnego skanera pamięci AMON.