

KASPERSKY LAB

Kaspersky[®] Anti-Virus for Windows
Servers 6.0

PODREČZNIK UŻYTKOWNIKA

KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Podręcznik użytkownika

© Kaspersky Lab
<http://www.kaspersky.pl>

Kwiecień 2007

Spis treści

ROZDZIAŁ 1.	ZAGROŻENIA DLA BEZPIECZEŃSTWA KOMPUTERA	8
1.1.	Źródła zagrożeń.....	8
1.2.	Sposoby rozprzestrzeniania się zagrożeń.....	9
1.3.	Rodzaje zagrożeń	10
ROZDZIAŁ 2.	KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0 ...	14
2.1.	Nowości w Kaspersky Anti-Virus for Windows Servers 6.0.....	14
2.2.	Metody ochrony oferowane przez Kaspersky Anti-Virus for Windows Servers	15
2.2.1.	Ochrona plików	16
2.2.2.	Zadania skanowania antywirusowego.....	16
2.2.3.	Usługi	17
2.3.	Wymagania sprzętowe i programowe	18
2.4.	Pakiet dystrybucyjny.....	19
2.5.	Usługi świadczone zarejestrowanym użytkownikom	20
ROZDZIAŁ 3.	INSTALACJA KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0	21
3.1.	Instalacja przy użyciu kreatora instalacji.....	21
3.2.	Kreator konfiguracji.....	25
3.2.1.	Wykorzystanie obiektów zachowanych z wersji 5.0.....	26
3.2.2.	Aktywacja programu	26
3.2.2.1.	Wybór metody aktywacji programu.....	26
3.2.2.2.	Wybór klucza licencyjnego	27
3.2.2.3.	Finalizowanie aktywacji programu	27
3.2.3.	Konfiguracja ustawień aktualizacji	27
3.2.4.	Konfiguracja terminarza skanowania.....	28
3.2.5.	Ograniczanie dostępu do programu	29
3.2.6.	Finalizowanie działania kreatora konfiguracji	29
3.3.	Instalacja programu z poziomu wiersza poleceń	30
3.4.	Aktualizacja z wersji 5.0 do 6.0	30
ROZDZIAŁ 4.	INTERFEJS PROGRAMU	31

4.1. Ikona zasobnika systemowego.....	31
4.2. Menu kontekstowe	32
4.3. Główne okno programu.....	33
4.4. Okno ustawień programu.....	36
ROZDZIAŁ 5. ROZPOCZĘCIE PRACY	38
5.1. Jaki stan ochrony posiada komputer?	38
5.1.1. Wskaźniki ochrony.....	39
5.1.2. Stan składników programu Kaspersky Anti-Virus for Windows Servers	42
5.1.3. Statystyki działania programu	43
5.2. W jaki sposób wykonać skanowanie serwera.....	44
5.3. W jaki sposób wykonać skanowanie obszarów krytycznych.....	44
5.4. W jaki sposób wykonać skanowanie plików, folderów lub dysków	45
5.5. W jaki sposób dokonać aktualizacji programu	46
5.6. Co należy zrobić, jeżeli ochrona jest wyłączona	47
ROZDZIAŁ 6. ZARZĄDZANIE OCHRONĄ.....	49
6.1. Wstrzymywanie i wznowianie ochrony komputera	49
6.1.1. Wstrzymywanie ochrony	50
6.1.2. Zatrzymywanie ochrony serwera	51
6.1.3. Wstrzymywanie / wyłączanie składników ochrony oraz zadań skanowania i aktualizacji	52
6.1.4. Przywracanie ochrony komputera	53
6.1.5. Wyłączanie programu.....	53
6.2. Wybieranie szkodliwych programów do monitorowania	53
6.3. Tworzenie strefy zaufanej	54
6.3.1. Reguły wykluczeń.....	56
6.3.2. Zaufane aplikacje.....	59
6.4. Uruchamianie zadań skanowania przy użyciu profilu innego użytkownika.....	62
6.5. Konfiguracja terminarza zadania	64
6.6. Opcje wydajności.....	66
6.7. Konfiguracja serwera wieloprocessorowego.....	67
ROZDZIAŁ 7. OCHRONA ANTYWIRUSOWA SYSTEMU PLIKÓW SERWERA	68
7.1. Wybór poziomu ochrony	69
7.2. Ustawienia ochrony systemu plików.....	70
7.2.1. Definiowanie typów skanowanych plików.....	71

7.2.2. Definiowanie obszaru ochrony.....	74
7.2.3. Konfiguracja ustawień zaawansowanych.....	75
7.2.4. Przywracanie domyślnych ustawień modułu Ochrona plików.....	78
7.2.5. Wybór akcji dla obiektów.....	79
7.2.6. Tworzenie szablonu powiadomienia.....	81
7.3. Odraczanie leczenia.....	81
ROZDZIAŁ 8. SKANOWANIE KOMPUTERA NA OBECNOŚĆ WIRUSÓW ...	82
8.1. Zarządzanie zadaniami skanowania.....	83
8.2. Tworzenie listy skanowanych obiektów.....	83
8.3. Tworzenie zadań skanowania.....	85
8.4. Konfiguracja zadań skanowania.....	86
8.4.1. Wybór poziomu ochrony.....	87
8.4.2. Definiowanie typów skanowanych obiektów.....	88
8.4.3. Przywracanie domyślnych ustawień skanowania.....	91
8.4.4. Wybór akcji dla obiektów.....	92
8.4.5. Dodatkowe ustawienia skanowania.....	94
8.4.6. Definiowanie globalnych ustawień skanowania dla wszystkich zadań.....	95
ROZDZIAŁ 9. TESTOWANIE DZIAŁANIA KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	96
9.1. Wirus testowy EICAR i jego modyfikacje.....	96
9.2. Testowanie modułu Ochrona plików.....	98
9.3. Testowanie zadań skanowania antywirusowego.....	99
ROZDZIAŁ 10. AKTUALIZACJA PROGRAMU	101
10.1. Uruchamianie aktualizacji.....	103
10.2. Cofanie aktualizacji.....	103
10.3. Tworzenie zadań aktualizacji.....	104
10.4. Konfiguracja ustawień aktualizacji.....	105
10.4.1. Wybór źródła uaktualnień.....	105
10.4.2. Wybór metody aktualizacji.....	108
10.4.3. Konfiguracja ustawień sieciowych.....	110
10.4.4. Współdzielenie uaktualnień.....	112
10.4.5. Działania podejmowane po zakończeniu aktualizacji.....	114
ROZDZIAŁ 11. OPCJE ZAAWANSOWANE	115
11.1. Kwarantanna dla potencjalnie zainfekowanych obiektów.....	116

11.1.1. Akcje podejmowane na obiektach poddanych kwarantannie.....	117
11.1.2. Konfiguracja kwarantanny.....	119
11.2. Kopie zapasowe niebezpiecznych obiektów.....	119
11.2.1. Akcje podejmowane na kopiach zapasowych obiektów.....	120
11.2.2. Konfiguracja kopii zapasowych.....	122
11.3. Raporty.....	122
11.3.1. Konfiguracja ustawień raportów.....	125
11.3.2. Zakładka <i>Wykryto</i>	126
11.3.3. Zakładka <i>Zdarzenia</i>	126
11.3.4. Zakładka <i>Statystyki</i>	128
11.3.5. Zakładka <i>Ustawienia</i>	128
11.3.6. Zakładka <i>Zablokowani użytkownicy</i>	129
11.4. Informacje ogólne o programie.....	130
11.5. Zarządzanie licencjami.....	131
11.6. Pomoc techniczna.....	133
11.7. Konfiguracja interfejsu Kaspersky Anti-Virus for Windows Servers.....	134
11.8. Wykorzystywanie zaawansowanych ustawień.....	136
11.8.1. Powiadomienia o zdarzeniach generowanych przez Kaspersky Anti-Virus for Windows Servers.....	137
11.8.1.1. Typy zdarzeń i metody dostarczania powiadomień.....	138
11.8.1.2. Konfiguracja wysyłania powiadomień za pośrednictwem poczty elektronicznej.....	139
11.8.1.3. Konfiguracja dziennika zdarzeń.....	141
11.8.2. Autoochrona programu i ograniczenia dostępu.....	142
11.8.3. Rozwiązywanie problemów z innymi aplikacjami.....	143
11.9. Importowanie i eksportowanie ustawień Kaspersky Anti-Virus for Windows Servers.....	144
11.10. Przywracanie ustawień domyślnych.....	144
ROZDZIAŁ 12. ZARZĄDZANIE PROGRAMEM PRZY UŻYCIU KASPERSKY ADMINISTRATION KIT.....	146
12.1. Zarządzanie aplikacją.....	148
12.1.1. Uruchamianie/Zatrzymywanie działania aplikacji.....	149
12.1.2. Konfiguracja ustawień aplikacji.....	150
12.1.3. Konfiguracja ustawień zaawansowanych.....	152
12.2. Zarządzanie zadaniami.....	153
12.2.1. Uruchamianie i zatrzymywanie zadań.....	154

12.2.2. Tworzenie zadań	155
12.2.2.1. Tworzenie zadań lokalnych	155
12.2.2.2. Tworzenie zadania grupowego	157
12.2.2.3. Tworzenie zadań globalnych	158
12.2.3. Konfiguracja ustawień zadania	158
12.3. Zarządzanie profilami	159
12.3.1. Tworzenie profili	160
12.3.2. Przeglądanie i modyfikacja ustawień profilu	162
ROZDZIAŁ 13. PRACA Z PROGRAMEM PRZY UŻYCIU WIERSZA	
POLECEŃ 164	
13.1. Aktywowanie aplikacji	165
13.2. Zarządzanie modulem Ochrona plików i zadaniami	166
13.3. Skanowanie antywirusowe	168
13.4. Aktualizacja programu	172
13.5. Cofanie aktualizacji	173
13.6. Eksportowanie ustawień	174
13.7. Importowanie ustawień	175
13.8. Uruchamianie programu	175
13.9. Zatrzymywanie działania programu	176
13.10. Przeglądanie pomocy	176
13.11. Kody zwracane przez interfejs wiersza poleceń	176
ROZDZIAŁ 14. MODYFIKOWANIE, NAPRAWIANIE I USUWANIE	
PROGRAMU 178	
14.1. Modyfikowanie, naprawianie i usuwanie programu przy użyciu kreatora instalacji	178
14.2. Dezinstalacja programu z poziomu wiersza poleceń	181
ROZDZIAŁ 15. NAJCZĘŚCIEJ ZADAWANE PYTANIA	182
DODATEK 1. INFORMACJE DODATKOWE	184
1.1. Lista plików skanowanych według rozszerzenia	184
1.2. Możliwe maski wykluczeń	186
1.3. Maski zgodne z klasyfikacją Encyklopedii Wirusów	187
DODATEK 2. KASPERSKY LAB	188
2.1. Inne produkty firmy Kaspersky Lab	189
2.2. Kontakt z firmą Kaspersky Lab	195

ROZDZIAŁ 1. ZAGROŻENIA DLA BEZPIECZEŃSTWA KOMPUTERA

Z uwagi na szybki rozwój technologii informatycznej oraz jej udział w każdym aspekcie ludzkiego życia, wzrosła liczba działań skierowanych na złamanie zabezpieczeń.

Cybernetyczni kryminaliści wykazują duże zainteresowanie działalnością struktur państwowych oraz środowisk korporacyjnych. Podejmują oni działania mające na celu kradzież oraz ujawnianie poufnych informacji, niszczenie reputacji przedsiębiorstw i instytucji, naruszanie ich funkcjonowania oraz w konsekwencji naruszanie zasobów informacyjnych organizacji. Tego typu działania mogą spowodować duże straty finansowe.

Przy pomocy odpowiednich narzędzi, atakujący uzyskują dostęp do osobistych danych (kont bankowych oraz numerów kart kredytowych i haseł) lub powodują wadliwe działanie systemu.

W dzisiejszych czasach, każdy użytkownik komputera zdaje sobie sprawę, że informacje są cenną wartością i powinny być chronione. Informacje muszą być dostępne dla różnych grup użytkowników w tym samym czasie (dla pracowników, klientów i partnerów biznesowych). Dlatego jest to podstawowy powód potrzeby tworzenia wszechstronnych systemów bezpieczeństwa. Tego typu system musi brać pod uwagę wszystkie możliwe źródła zagrożeń, zarówno czynnik ludzki, zagrożenia utworzone przez człowieka albo naturalne klęski i korzystać z kompletnych środków ochronnych na poziomie fizycznym, administracyjnym i programowym.

1.1. Źródła zagrożeń

Źródło zagrożeń może stanowić osoba, grupa ludzi lub nawet niektóre zjawiska nie związane z działalnością człowieka. Źródła zagrożeń pogrupować można w trzy grupy:

Czynnik ludzki. Do tej grupy zagrożeń zaliczyć można działania uzyskiwania autoryzowanego lub nieautoryzowanego dostępu do danych przez człowieka. Zagrożenia z tej grupy można podzielić na:

- *Zewnętrzne*, włączając cybernetycznych przestępców, hakerów, oszustów Internetowych, partnerów łamiących reguły i struktury kryminalne.
- *Wewnętrzne*, włączając działania użytkowników domowych i korporacyjnych. Działania wykonane przez tą grupę mogą być celowe lub przypadkowe.

Czynnik technologiczny. Grupa ta jest związana z problemami technicznymi - przestarzałymi narzędziami, niskiej jakości oprogramowaniem i sprzętem do przetwarzania informacji. Prowadzi to do częstych awarii sprzętu i utraty danych.

Czynnik naturalny. Grupa ta zawiera dowolną liczbę zdarzeń spowodowanych przez naturę lub przez inne zdarzenia niezależnie od ludzkiej aktywności.

Podczas tworzenia systemu bezpieczeństwa danych należy wziąć pod uwagę wszystkie trzy źródła zagrożeń. Niniejszy podręcznik zawiera jedynie informacje dotyczące jednego z czynników - zagrożenia zewnętrzne związane z działalnością człowieka.

1.2. Sposoby rozprzestrzeniania się zagrożeń

Ze względu na nowoczesną technologię komputerową oraz tworzenie narzędzi komunikacyjnych, hakerzy posiadają więcej sposobów rozsyłania zagrożeń. Poniżej znajduje się ich szczegółowy opis:

Internet

Internet jest siecią unikatową, ponieważ nie jest niczyją własnością i nie jest ograniczony barierami geograficznymi. Pozwoliło to na zwiększanie liczby zasobów sieciowych i wymianę informacji. W dzisiejszych czasach, każdy może uzyskać dostęp do danych w Internecie lub utworzyć własną stronę Internetową.

Dlatego też, te cechy witryn Internetowych umożliwiają hakerom popełnianie przestępstw w Internecie, utrudniając ich wykrycie i ukaranie.

Hakerzy umieszczają wirusy i inne szkodliwe programy na stronach Internetowych maskując je jako darmowe oprogramowanie. Ponadto, skrypty uruchamiane automatycznie po otwarciu witryny Internetowej mogą spowodować uruchomienie niebezpiecznych działań na komputerze użytkownika, włączając modyfikację rejestru systemowego, kradzież danych osobistych i instalację szkodliwego oprogramowania.

Przy użyciu technologii sieciowych, hakerzy mogą atakować zdalnie komputery i firmowe serwery. Tego typu ataki mogą przyczynić się do

nieprawidłowego funkcjonowania systemu operacyjnego lub uzyskania przez hakerów pełnego dostępu do atakowanego komputera oraz informacji na nim przechowywanych. Mogą oni również użyć go jako komputer wchodzący w skład części sieci zainfekowanych komputerów zombie.

Intranet

Intranet stanowi wewnętrzną sieć użytkownika, utworzoną w celu przenoszenia informacji wewnątrz firmy lub sieci domowej. Intranet jest obszarem do przechowywania, wymiany i uzyskiwania dostępu do informacji przez wszystkie komputery w sieci. Oznacza to, że jeżeli w sieci zainfekowany jest jeden komputer, pozostałe komputery również w dużym stopniu narażone są na infekcję. W celu uniknięcia tego typu sytuacji, chronione powinny być zarówno styk sieci z internetem jak i poszczególne komputery.

Poczta elektroniczna

Od czasu, gdy praktycznie każdy komputer posiada zainstalowany program pocztowy oraz gdy szkodliwe programy potrafią uzyskać dostęp do zawartości adresowej książki elektronicznej, tego typu uwarunkowanie zaliczyć można do rozprzestrzeniania się szkodliwych programów. Użytkownik zainfekowanego komputera nieświadomie może wysłać zainfekowane wiadomości pocztowe do znajomych lub współpracowników, którzy z kolei prześlą więcej zainfekowanych wiadomości pocztowych. Typowe jest, że zainfekowany plik nie jest wykrywany podczas wysyłania na zewnątrz dużej firmy. W przypadku wystąpienia tego typu zdarzenia, zainfekowana zostanie większa grupa użytkowników. Mogą ich być setki lub tysiące, którzy z kolei wyślą zainfekowane pliki do dziesiątków tysięcy użytkowników.

Nośniki wymienne

Nośniki wymienne, takie jak dyski, dyskietki, karty flash używane są do przechowywania i przesyłania informacji.

Po uruchomieniu zainfekowanego pliku zapisanego na dysku wymiennym możliwe jest uszkodzenie danych zapisanych na komputerze i rozprzestrzenienie się wirusa na inne komputery sieciowe.

1.3. Rodzaje zagrożeń

W dzisiejszych czasach występuje wiele rodzajów zagrożeń mogących zainfekować komputer. Sekcja ta zawiera informacje dotyczące zagrożeń, przed którymi chroni program Kaspersky Anti-Virus for Windows Servers.

Robaki

Ta kategoria szkodliwych programów rozprzestrzenia się na skutek wykorzystania luk w systemach operacyjnych komputerów. Klasa ta została nazwana zgodnie ze sposobem rozprzestrzeniania się robaków między komputerami, przy użyciu sieci komputerowych i wiadomości pocztowych. Pozwala to na szybkie rozprzestrzenianie się robaków.

Robaki penetrują komputer, określają adresy IP innych maszyn, a następnie przesyłają na nie swoje kopie. Robaki mogą również wykorzystywać dane zawarte w książkach adresowych klientów pocztowych. Niektóre z tych szkodliwych programów tworzą pliki robocze na dyskach systemowych, ale mogą być uruchamiane bez żadnych zasobów systemowych za wyjątkiem pamięci RAM.

Wirusy

Wirusy infekują programy komputerowe poprzez dodawanie kodu modyfikującego sposób działania zainfekowanej aplikacji. Ta prosta definicja przedstawia podstawowe działanie wirusa - *infekcja*.

Trojany

Trojany są programami, które wykonują na komputerach nieautoryzowane działania takie jak usuwanie informacji z dysków twardych, modyfikowanie systemu, kradzież poufnych danych itp. Programy tego typu nie są wirusami, ponieważ nie infekują innych komputerów lub danych. Trojany nie mogą same włamać się do komputera. Są one rozsyłane przez hakerów, którzy "ukrywają" je pod postacią programów użytkowych. Mogą one powodować większe uszkodzenia w porównaniu z regularnymi atakami wirusowymi.

W ostatnich latach najszybciej rozprzestrzeniającym się (przy użyciu wirusów i Trojanów) rodzajem szkodliwego oprogramowania uszkadzającego dane komputera stały się robaki internetowe. Niektóre szkodliwe programy łączą w sobie funkcje dwóch lub nawet trzech powyższych klas.

Adware

Adware to program, który (bez wiedzy użytkownika) jest osadzony w innej aplikacji w celu wyświetlania reklam. Z reguły oprogramowanie adware dodawane jest do aplikacji darmowych (tzw. freeware). Moduł reklamowy zlokalizowany jest w interfejsie programu. Programy adware często wykorzystywane są do gromadzenia danych dotyczących użytkownika komputera oraz do wysyłania tych informacji przez Internet, zmieniania ustawień przeglądarki internetowej (strony startowej i stron wyszukiwania, poziomów zabezpieczeń itp.) oraz obciążania połączenia bez możliwości jego kontrolowania przez użytkownika. Tego typu działania mogą prowadzić do naruszenia reguł bezpieczeństwa oraz bezpośrednich strat finansowych.

Spyware

Oprogramowanie służące do rejestrowania informacji o użytkowniku lub organizacji bez ich wiedzy. Użytkownik może nawet nie być świadomy obecności tego typu oprogramowania na komputerze. Programy typu spyware wykorzystywane są w następujących celach:

- śledzenie działań użytkownika wykonywanych na komputerze
- gromadzenie informacji o zawartości dysku twardego; w tym przypadku, zazwyczaj tego typu programy skanują pewne foldery oraz rejestr systemu w celu utworzenia listy oprogramowania zainstalowanego na komputerze
- gromadzenie informacji o jakości połączenia sieciowego, przepustowości, prędkości połączenia modemowego itp..

Riskware

Riskware to potencjalnie niebezpieczne oprogramowanie niezawierające szkodliwych funkcji, lecz mogące zostać użyte przez hakerów jako składnik pomocniczy dla szkodliwego kodu. W niektórych warunkach tego typu programy mogą stanowić ryzyko dla danych przechowywanych na komputerze. Tego typu programy zawierają narzędzia do zdalnej administracji, narzędzia do przełączania układów klawiatury, klientów IRC, serwery FTP oraz wszystkie narzędzia do celowego zatrzymywania lub ukrywania procesów.

Innym rodzajem szkodliwych programów (podobnych do adware, spyware i riskware) są aplikacje, które podłączają się do przeglądarki internetowej i przekierowują ruch.

Żarty

Programy, które nie powodują żadnych bezpośrednich uszkodzeń komputera, lecz wyświetlają komunikaty mówiące o wystąpieniu uszkodzenia lub możliwości wystąpienia uszkodzenia po spełnieniu odpowiednich kryteriów. Tego typu programy generują częste ostrzeżenia dla użytkownika o niebezpieczeństwie, które nie istnieje, na przykład: wyświetlane są komunikaty o formatowaniu dysku twardego, (co nie jest prawdą), "wykryciu" wirusów w pliku, który nie jest zainfekowany.

Rootkity

Są to narzędzia używane w celu maskowania szkodliwej aktywności. Ukrywają one szkodliwe programy przed programami antywirusowymi. Rootkity mogą zmodyfikować system operacyjny oraz zmienić jego główne funkcje w celu ukrycia swojej obecności oraz akcji wykonywanych przez intruza na zainfekowanym komputerze.

Inne niebezpieczne programy

Są to programy przeznaczone do tworzenia innych szkodliwych programów, przeprowadzania ataków DoS na zdalne serwery, przejmowania kontroli nad innymi komputerami itp. Tego typu programy zawierają narzędzia hakerskie (Hack Tools), moduły do tworzenia wirusów, skanery luk w systemie, programy łamiące hasła oraz inne typy programów penetrujących system.

Ostrzeżenie!

W dalszej części dokumentu termin "wirus" będzie odnosił się do szkodliwych i niebezpiecznych programów. Jeżeli będzie to wymagane, podany zostanie także typ szkodliwego oprogramowania.

ROZDZIAŁ 2. KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Kaspersky Anti-Virus for Windows Servers 6.0 jest programem nowej generacji do ochrony danych.

2.1. Nowości w Kaspersky Anti-Virus for Windows Servers 6.0

Nowe funkcje dostępne w Kaspersky Anti-Virus for Windows Servers.

Nowe funkcje ochrony

Ulepszono technologię ochrony antywirusowej dla plików: możliwe jest teraz zmniejszenie obciążenia systemu oraz zwiększenie prędkości skanowania plików. Zapewniają to technologie iChecker i iSwift. Podczas pracy w tym trybie, program nie skanuje plików, które nie uległy zmianie od czasu ostatniego skanowania.

Proces skanowania odbywa się w tle umożliwiając administratorowi pracę na komputerze. Jeżeli jedna z operacji wymaga zasobów systemowych, skanowanie antywirusowe zostanie wstrzymane do czasu zakończenia tej operacji. Następnie skanowanie zostanie wznowione.

Dla obszarów krytycznych komputera, których infekcja może spowodować poważne konsekwencje utworzone zostało oddzielne zadanie. Zadanie to można skonfigurować, aby było ono automatycznie uruchamiane podczas ładowania systemu operacyjnego.

Funkcja powiadamiania użytkownika (patrz rozdział 11.8.1 na stronie 137) została rozbudowana o dodatkowe zdarzenia występujące podczas pracy programu. Możliwe jest wybranie metody powiadamiania dla każdego z tych zdarzeń: wiadomość e-mail, powiadomienia dźwiękowe, komunikaty wyskakujące.

Dodano nowe funkcje autoochrony aplikacji: ochrona przed nieautoryzowanym zdalnym zarządzaniem, ochrona plików aplikacji przed nieautoryzowanym dostępem lub modyfikacją oraz ochrona hasłem ustawień programu.

Nowy interfejs programu

Nowy interfejs Kaspersky Anti-Virus for Windows Servers ułatwia korzystanie z programu i upraszcza wykonywanie operacji. Możliwe jest również zmienianie wyglądu programu przy zastosowaniu własnych schematów graficznych i kolorystycznych.

Program regularnie wyświetla wskazówki i podpowiedzi podczas funkcjonowania: Kaspersky Anti-Virus for Windows Servers wyświetla komunikaty informacyjne dotyczące poziomu ochrony, wskazówki i porady dotyczące funkcjonowania programu oraz zawiera podzielony na sekcje system pomocy.

Nowa funkcja pobierania uaktualnień

Ta wersja programu zawiera nową, ulepszoną procedurę aktualizacji: Kaspersky Anti-Virus automatycznie monitoruje sygnatury zagrożeń oraz moduły programu niezbędne do jego funkcjonowania. Po wykryciu przez program najnowszych uaktualnień, są one pobierane i instalowane na komputerze.

Program pobiera tylko nowe uaktualnienia ignorując pliki, które już zostały pobrane. Dzięki temu rozmiar pobieranych uaktualnień może być mniejszy nawet o 90%.

Uaktualnienia pobierane są z najbliższego źródła.

Program posiada funkcję cofania aktualizacji, dzięki której można przywrócić ostatnią działającą wersję sygnatur, jeżeli, na przykład, zostaną one uszkodzone lub wystąpi błąd podczas ich kopiowania.

Dodano funkcję pozwalającą na dystrybuowanie uaktualnień do foldera lokalnego w celu udostępnienia ich innym komputerom sieciowym. Umożliwia to zmniejszenie przesyłanego ruchu sieciowego.

2.2. Metody ochrony oferowane przez Kaspersky Anti-Virus for Windows Servers

Kaspersky Anti-Virus for Windows Servers zawiera:

Moduł Ochrona plików, który monitoruje system plików komputera.

Zadania skanowania antywirusowego (patrz rozdział 2.2.2 na stronie 16) sprawdzające komputer lub indywidualne pliki, foldery, dyski lub obszary w poszukiwaniu wirusów.

Narzędzia (patrz rozdział 2.2.3 na stronie 17) zapewniające pomoc dla programu oraz rozszerzające jego funkcjonalność.

2.2.1. Ochrona plików

System plików serwera jest chroniony w czasie rzeczywistym przez moduł **Ochrona plików**.

System plików może zawierać wirusy i inne niebezpieczne programy. Szkodliwe programy mogą znajdować się w systemie od dłuższego czasu, po przeniesieniu ich do systemu na dyskietce lub z Internetu, bez wcześniejszego ich otwierania. Aktywacja wirusa może nastąpić po otwarciu zainfekowanego pliku.

Ochrona plików jest składnikiem służącym do monitorowania systemu plików komputera. Skanuje on wszystkie pliki, które mogą zostać otwarte, uruchomione lub zapisane na serwerze oraz wszystkie podłączone dyski twarde. Kaspersky Anti-virus przechwytuje każdy otwierany plik i skanuje go w poszukiwaniu znanych wirusów. Jeżeli plik nie jest zainfekowany można dalej z niego korzystać natomiast, jeżeli jest on zainfekowany następuje próba jego wyleczenia. Jeżeli nie można wyleczyć pliku, zostaje on usunięty, a jego kopia zapisywana jest w folderze kopii zapasowej lub przenoszona do foldera kwarantanny.

2.2.2. Zadania skanowania antywirusowego

Poza nieustannym monitorowaniem potencjalnych źródeł występowania szkodliwych programów, ważne jest również okresowe wykonywanie skanowania komputera w poszukiwaniu wirusów. Jest to niezbędne w celu wykluczenia możliwości rozprzestrzenienia się szkodliwych programów, które nie zostały wykryte przez moduł Ochrona plików np.: z powodu niskiego poziomu zabezpieczeń.

Kaspersky Anti-Virus for Windows Servers oferuje trzy rodzaje zadań skanowania antywirusowego:

Obszary krytyczne

Skanowanie wszystkich obszarów krytycznych komputera w poszukiwaniu wirusów. Dotyczy to: pamięci systemowej, programów ładowanych do pamięci podczas startu systemu, sektorów startowych dysków twardych i katalogów systemowych *Windows* i *system32*. Zadanie to ma na celu szybkie wykrycie aktywnych wirusów w systemie bez konieczności przeprowadzania pełnego skanowania komputera.

Skanuj Mój komputer

Skanowanie komputera w poszukiwaniu wirusów obejmujące wszystkie dyski twarde, pamięć i pliki.

Obiekty startowe

Skanowanie w poszukiwaniu wirusów wszystkich programów automatycznie ładowanych do pamięci podczas startu systemu operacyjnego oraz pamięci RAM i sektorów startowych dysków twardego komputera.

Dostępna jest również opcja tworzenia innych zadań skanowania antywirusowego oraz definiowania dla nich terminarza skanowania.

2.2.3. Usługi

Kaspersky Anti-Virus for Windows Servers zawiera wiele przydatnych narzędzi. Stworzone one zostały w celu świadczenia pomocy w czasie rzeczywistym oraz rozszerzenia możliwości programu.

Aktualizacja

Aby skutecznie chronić się przed atakami hakerów i usuwać wirusy oraz inne niebezpieczne programy, Kaspersky Anti-Virus for Windows Servers wymaga aktualnych baz danych. *Usługa* ta stworzona została w celu pobierania uaktualnień. Jest ona odpowiedzialna za pobieranie uaktualnień antywirusowych baz danych i modułów programu Kaspersky Anti-virus for Windows Servers.

Funkcja aktualizacji pozwala na zapisanie pobranych uaktualnień i udostępnienie ich innym komputerom działającym w obrębie tej samej sieci lokalnej. Pozwala to na zmniejszenie obciążenia łącza internetowego.

Pliki danych

Moduł Ochrona plików, zadanie skanowania antywirusowego lub aktualizacja programu tworzy raport ze swojego funkcjonowania. Raporty zawierają informacje dotyczące zakończonych operacji i ich wyników. Dzięki raportom, użytkownik będzie zawsze na bieżąco ze wszystkimi operacjami wykonywanymi przez składniki programu Kaspersky Anti-Virus for Windows Servers. Jeżeli pojawią się problemy, można będzie wysłać raporty do firmy Kaspersky Lab w celu dokonania ich analizy i uzyskania pomocy w rozwiązaniu problemu.

Kaspersky Anti-Virus for Windows Servers przenosi wszystkie podejrzane pliki do specjalnego obszaru zwanego Kwarantanną. Przechowywane są one tam w postaci zaszyfrowanej w celu uniknięcia infekcji komputera.

Można przeprowadzać skanowanie tych obiektów w poszukiwaniu wirusów, przywracać je do ich wcześniejszych lokalizacji, usuwać lub samodzielnie dodawać do kwarantanny. Wszystkie pliki, które nie są zainfekowane zostaną automatycznie przywrócone do ich oryginalnych lokalizacji.

Kopia zapasowa zawiera kopie plików wyleczonych i usuniętych przez program. Kopie te tworzone są w przypadku wystąpienia potrzeby przywrócenia plików lub uzyskania informacji o ich infekcji. Kopie zapasowe plików są również zapisywane w zaszyfrowanej postaci w celu uniknięcia przyszłych infekcji.

Możliwe jest ręczne przywrócenie pliku z foldera kopii zapasowej do oryginalnej lokalizacji i usunięcie jego kopii.

Pomoc techniczna

Dla zarejestrowanych użytkowników programu Kaspersky Anti-virus dostępna jest usługa pomocy technicznej. Aby dowiedzieć się w jaki sposób można uzyskać pomoc należy przejść na zakładkę *Pomoc*.

Program zawiera listę najczęściej zadawanych pytań, która może pomóc w samodzielnym rozwiązaniu problemu. Użytkownik może także wysłać raport o wystąpieniu błędu lub pytanie związane z funkcjonowaniem programu. W tym celu można skorzystać z formularza dostępnego na stronie internetowej.

Pomoc techniczna świadczona przez Kaspersky Lab jest dostępna jest także za pośrednictwem poczty elektronicznej i telefonu.

2.3. Wymagania sprzętowe i programowe

Do poprawnej pracy programu Kaspersky Anti-Virus, komputer musi spełniać następujące wymagania:

Wymagania ogólne:

50 MB wolnego miejsca na dysku twardym

napęd CD-ROM (w celu instalacji Kaspersky Anti-Virus for Windows Servers 6.0 z płyty CD)

Microsoft Internet Explorer 5.5 lub nowszy (w celu aktualizacji antywirusowych baz danych i modułów programu przez Internet)

Microsoft Windows Installer 2.0

System operacyjny:

Microsoft Windows 2000 Server/Advanced Server Service Pack 4 lub nowszy, ze wszystkimi dostępnymi aktualizacjami.

Microsoft Windows NT Server 4.0 Service Pack 6a.

Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, wszystkie pakiety Service Pack oraz dostępne aktualizacje.

Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

2.4. Pakiet dystrybucyjny

Oprogramowanie można nabyć u jednego z naszych dystrybutorów (pakiet dystrybucyjny) lub za pośrednictwem sklepów internetowych (na przykład www.kaspersky.pl/store.html).

W skład pakietu dystrybucyjnego wchodzi:

- Zapieczętowana koperta zawierająca nośnik instalacyjny
- Wydrukowany kod aktywacyjny lub klucz licencyjny zapisany na nośniku instalacyjnym.
- Podręcznik użytkownika
- Umowa licencyjna

Przed otwarciem koperty zawierającej nośnik instalacyjny należy uważnie przeczytać treść Umowy licencyjnej.

W przypadku zakupu programu Kaspersky Anti-Virus for Windows Servers przez Internet, należy pobrać jego kopię ze strony internetowej firmy Kaspersky Lab (**Download** → **Produkty**). Podręcznik użytkownika można pobrać ze strony **Download** → **Dokumentacja**.

Po zaksięgowaniu wpłaty, na adres poczty elektronicznej użytkownika (podany podczas zamawiania produktu) przesłany zostanie klucz licencyjny lub kod aktywacyjny.

Umowa licencyjna stanowi prawne porozumienie między użytkownikiem a firmą Kaspersky Lab definiujące warunki, na jakich można użytkować zakupionego oprogramowania.

Należy uważnie przeczytać postanowienia umowy licencyjnej.

W przypadku braku zgody z postanowieniami Umowy licencyjnej możliwe jest zwrócenie pakietu dystrybutorowi, u którego dokonano zakupu i otrzymanie zwrotu kwoty zapłaconej za program. W tym przypadku koperta zawierająca nośnik instalacyjny musi pozostać zapieczętowana.

Otwarcie zapieczętowanej koperty zawierającej nośnik instalacyjny jest równoznaczne z zaakceptowaniem wszystkich postanowień Umowy licencyjnej.

2.5. Usługi świadczone zarejestrowanym użytkownikom

Firma Kaspersky Lab świadczy wszystkim zarejestrowanym użytkownikom swoich produktów szeroki wachlarz usług.

Po wykupieniu subskrypcji i zarejestrowaniu programu, podczas trwania okresu licencjonowania użytkownikom świadczone są następujące usługi:

Darmowe uaktualnienia programu

Pomoc techniczna dotycząca instalacji, konfiguracji i użytkowania produktu; usługa ta jest świadczona za pośrednictwem telefonu i poczty elektronicznej

informacje na temat nowych produktów firmy Kaspersky Lab oraz nowych wirusów pojawiających się na świecie (usługa dostępna tylko dla użytkowników zarejestrowanych przez Internet)

Firma Kaspersky Lab nie świadczy pomocy technicznej dotyczącej działania systemów operacyjnych oraz innych technologii.

ROZDZIAŁ 3. INSTALACJA KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Istnieje możliwość pełnej lub częściowej instalacji programu Kaspersky Anti-Virus for Windows Servers na komputerze.

Jeżeli wybrana została instalacja częściowa, należy wybrać składniki, które mają zostać zainstalowane. Pozostałe składniki programu mogą zostać zainstalowane później. Wymagany będzie posiadanie nośnika instalacyjnego. Zalecane jest skopiowanie zawartości nośnika instalacyjnego na dysk twardy.

Aplikacja może zostać zainstalowana na jeden ze sposobów:

- Przy użyciu kreatora instalacji (patrz rozdział 3.1 na stronie 21)
- Z poziomu wiersza poleceń (patrz rozdział 3.3 na stronie 30)
- Przy użyciu Kaspersky Administration Kit (szczegółowe informacje znajdują się w Podręczniku administratora Kaspersky Administration Kit)

3.1. Instalacja przy użyciu kreatora instalacji

Przed rozpoczęciem instalacji programu Kaspersky Anti-Virus zaleca się zamknąć wszystkie inne aplikacje uruchomione na komputerze.

Aby zainstalować program Kaspersky Anti-Virus for Windows Servers na komputerze należy uruchomić plik (.msi) znajdujący się na płycie instalacyjnej.

Notatka:

Instalacja aplikacji za pomocą pakietu dystrybucyjnego pobranego z Internetu jest identyczna jak instalacja za pomocą pakietu dystrybucyjnego znajdującego się na płycie CD.

Uruchomiony zostanie kreator instalacji programu. Każde okno posiada następujące przyciski umożliwiające zarządzanie procesem instalacji. Poniżej znajduje się krótki opis ich funkcji:

Dalej – zaakceptowanie działań i kontynuowanie instalacji.

Wstecz – powrót do poprzedniego etapu instalacji.

Anuluj – przerwanie instalacji programu.

Zakończ – zakończenie instalacji programu.

Szczegółowy opis każdego kroku instalacji jest zamieszczony poniżej.

Krok 1. Sprawdzenie wersji systemu operacyjnego w celu instalacji na komputerze Kaspersky Anti-Virus for Windows Servers

Zanim program zostanie zainstalowany, instalator sprawdza system operacyjny oraz pakiety uaktualnień w celu porównania zgodności z wymogami oprogramowania Kaspersky Anti-Virus for Windows Servers. Komputer jest również sprawdzany na obecność wymaganych programów oraz weryfikowane są uprawnienia użytkownika odnośnie instalacji oprogramowania.

Jeżeli program ustali, że pewien wymagany pakiet uaktualnień nie został zainstalowany na komputerze, wyświetlony zostanie stosowny komunikat. Przed instalacją programu Kaspersky Anti-Virus for Windows Servers należy zainstalować wymagane pakiety Service Pack przy użyciu narzędzia **Windows Update**.

Krok 2. Uruchomienie kreatora instalacji

Jeżeli system spełnia wszystkie wymagania, po uruchomieniu instalatora na ekranie zostanie wyświetlone okno informujące o rozpoczęciu instalacji programu Kaspersky Anti-Virus for Windows Servers.

Aby kontynuować instalację, należy kliknąć przycisk **Dalej**. Aby przerwać instalację należy kliknąć przycisk **Anuluj**.

Krok 3. Przeczytanie Umowy licencyjnej

Kolejne okno dialogowe zawiera treść Umowy licencyjnej, która jest prawnym porozumieniem pomiędzy użytkownikiem, a firmą Kaspersky Lab. Należy uważnie przeczytać jej treść i w przypadku zaakceptowania wszystkich jej postanowień wybrać **Akceptuję postanowienia umowy licencyjnej** i następnie kliknąć przycisk **Dalej**. Procedura instalacji będzie kontynuowana.

Krok 4. Wybór foldera instalacyjnego

W kolejnej fazie procesu instalacji Kaspersky Anti-Virus for Windows Servers wybrany zostanie folder instalacyjny produktu. Domyślną ścieżką dostępu do tego foldera jest:

<Dysk>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers – dla 32-bitowych systemów

<Dysk>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers – dla 64-bitowych systemów

Aby zmienić domyślną ścieżkę dostępu, należy ją wprowadzić ręcznie lub kliknąć przycisk **Przełączaj** oraz użyć standardowego okna wyboru w celu zlokalizowania i wybrania folderu.

W przypadku ręcznego wprowadzania pełnej nazwy foldera instalacyjnego, nie można przekroczyć 200 znaków lub używać znaków specjalnych.

Aby kontynuować instalację, należy kliknąć przycisk **Dalej**.

Krok 5. Wybór typu instalacji

Na tym etapie, należy wybrać typ instalacji programu. Dostępne są trzy opcje:

Pełna. Jeżeli wybrana zostanie ta opcja, zainstalowane zostaną wszystkie składniki Kaspersky Anti-Virus for Windows Servers.

Niestandardowa. Po wybraniu tej opcji należy wybrać składniki programu, które zostaną zainstalowane. Szczegółowe informacje na ten temat znajdują się w sekcji Krok 6.

W celu wybrania typu instalacji, należy kliknąć odpowiedni przycisk.

Krok 6. Wybór instalowanych składników

Krok ten dostępny jest jedynie po wybraniu opcji **Niestandardowa**.

Jeżeli wybrana została Niestandardowa instalacja, użytkownik może wbrać, które składniki Kaspersky Anti-Virus for Windows Servers zostaną zainstalowane na komputerze. Domyślnie instalowane są moduł Ochrona plików, zadania skanowania antywirusowego oraz wtyczka dla agenta administracyjnego w celu zdalnego zarządzania przy użyciu Kaspersky Administration Kit.

W celu wybrania składników, które mają zostać zainstalowane, należy kliknąć prawym przyciskiem myszy na ikonie składnika i z menu kontekstowego wybrać opcję **Zostanie zainstalowany na lokalnym dysku twardym**. W dolnej części

okna wyświetlone są szczegółowe informacje dotyczące wybranych składników, ich funkcji ochronnych oraz wymaganego miejsca do instalacji.

Jeżeli składnik ma nie zostać zainstalowany, z menu kontekstowego należy wybrać polecenie **Składnik nie zostanie zainstalowany na lokalnym dysku twardej**.

Po wybraniu żądanych składników, należy kliknąć przycisk **Dalej**. Aby powrócić do listy domyślnych składników, należy kliknąć przycisk **Resetuj**.

Krok 7. Wyszukiwanie innych programów antywirusowych

W kolejnym kroku program instalacyjny sprawdzi, czy w systemie zostały zainstalowane inne aplikacje antywirusowe, łącznie z innymi produktami Kaspersky Lab, które mogą przeszkadzać w prawidłowej instalacji Kaspersky Anti-Virus for Windows Servers.

Program instalacyjny wyświetli na ekranie listę wykrytych programów. Przed kontynuowaniem instalacji program zapyta czy mają być one odinstalowane.

Użytkownik może skorzystać z ręcznego lub automatycznego trybu usuwania wykrytych aplikacji antywirusowych (tylko produkty Kaspersky Lab będą mogły zostać automatycznie usunięte).

Aby kontynuować instalację, należy kliknąć przycisk **Dalej**.

Krok 8. Kończenie instalacji programu

W tym kroku program zaproponuje zakończenie instalacji programu. Można użyć ustawień ochrony, antywirusowych baz danych oraz baz antyspamowych, jeżeli zostały one zachowane z poprzedniej wersji programu Kaspersky Anti-Virus for Windows Servers (na przykład: zainstalowana była wersja beta i instalowana jest wersja komercyjna).

Poniżej znajduje się opis użycia opcji opisanych powyżej.

Jeżeli na komputerze zainstalowana była wcześniej poprzednia wersja programu Kaspersky Anti-Virus for Windows Servers i zachowane zostały bazy danych podczas jej dezinstalacji, można ich użyć w bieżącej wersji. W tym celu należy zaznaczyć **Sygnatury zagrożeń**. Bazy danych zawarte w programie instalacyjnym nie będą kopiowane do komputera.

W celu użycia ustawień ochrony skonfigurowanych w poprzedniej wersji programu, należy zaznaczyć opcję **Ustawienia ochrony**.

Nie jest zalecane usuwanie zaznaczenia z opcji **Włącz autoochronę przed instalacją** podczas instalacji programu Kaspersky Anti-Virus 6.0. Jeżeli moduły ochrony będą włączone, możliwe będzie poprawne cofnięcie zmian instalacyjnych w przypadku wystąpienia błędu w czasie instalacji. Podczas ponownej instalacji programu, zalecane jest usunięcie zaznaczenia z tej opcji.

Jeżeli aplikacja jest instalowana zdalnie poprzez Zdalny Pulpit Windows, zaleca się usunięcie zaznaczenia z opcji **Włącz autoochronę przed instalacją**. W przeciwnym przypadku procedura instalacji może nie zakończyć się lub zakończyć się poprawnie.

Aby automatycznie dodać do listy wykluczenia zalecane przez firmę Microsoft należy zaznaczyć opcję **Wyklucz ze skanowania obszary zalecane przez Microsoft**.

Aby po instalacji dodać ścieżkę dostępu do pliku avp.com do zmiennej środowiskowej %PATH% należy zaznaczyć opcję **Dodaj ścieżkę dostępu do pliku avp.com do zmiennej %PATH%**.

Aby kontynuować instalację, należy kliknąć przycisk **Dalej**.

Krok 9. Finalizowanie instalacji

Na ekranie wyświetlone zostanie okno **Instalacja została zakończona** informujące użytkownika, że instalacja programu Kaspersky Anti-Virus została pomyślnie zakończona.

W celu uruchomienia kreatora konfiguracji należy kliknąć **Dalej**.

Jeżeli instalacja zakończyła się pomyślnie, konieczne będzie ponowne uruchomienie komputera. Na ekranie wyświetlony zostanie odpowiedni komunikat.

3.2. Kreator konfiguracji

Po zakończeniu instalacji programu Kaspersky Anti-Virus for Windows Servers 6.0 uruchomiony zostanie kreator wstępnej konfiguracji. Stworzony on został w celu pomocy we wstępnej konfiguracji podstawowych ustawień programu zgodnych z funkcjami i przeznaczeniem komputera.

Interfejs kreatora podobny jest do standardowego kreatora systemu Windows i składa się z kilku etapów pomiędzy którymi można się przemieszczać przy użyciu przycisków **Wstecz** i **Dalej** lub zakończyć korzystanie z niego klikając przycisk **Zakończ**. Kliknięcie przycisku **Anuluj** zatrzyma kreatora w dowolnym momencie.

Jeżeli działanie kreatora konfiguracji zostanie zakończone poprzez zamknięcie okna, aplikacja nie zostanie uruchomiona. Przy każdej próbie uruchomienia aplikacji uruchamiany będzie kreator konfiguracji do momentu, aż procedura wstępnej konfiguracji ustawień zostanie pomyślnie zakończona.

3.2.1. Wykorzystanie obiektów zachowanych z wersji 5.0

To okno kreatora zostanie wyświetlone na ekranie, jeżeli na komputerze zainstalowany był wcześniej program Kaspersky Anti-Virus 5.0. Użytkownik zostanie poproszony o wybranie danych używanych w wersji 5.0, które mają zostać zaimportowane do wersji 6.0. Mogą one zawierać pliki poddane kwarantannie, znajdujące się w folderze kopii zapasowych lub ustawienia ochrony.

Aby użyć tych danych w wersji 6.0, należy zaznaczyć odpowiednie pola.

3.2.2. Aktywacja programu

Przed aktywacją programu należy upewnić się, że na komputerze ustawiona jest poprawna data i godzina.

Aktywacja programu wymaga zainstalowania pliku klucza licencyjnego dla Kaspersky Anti-Virus, który zweryfikuje datę wygaśnięcia licencji.

Klucz licencyjny zawiera informacje systemowe niezbędne do funkcjonowania wszystkich funkcji programu oraz inne informacje:

Informacje o pomocy technicznej (kto jej udziela i gdzie ją uzyskać)

Nazwę programu, numer i datę wygaśnięcia licencji

3.2.2.1. Wybór metody aktywacji programu

Aktywacja programu wymaga zainstalowania pliku klucza licencyjnego otrzymanego po zakupie produktu. Jeżeli użytkownik nie posiada klucza licencyjnego, należy go zakupić. W tym celu należy kliknąć komercyjny, w celu otworzenia strony aktywacji produktów firmy Kaspersky Lab. Należy postępować zgodnie z instrukcjami opisanymi na stronie internetowej.

Aby przetestować program przed jego zakupem można zainstalować wersję testową. W tym celu należy pobrać i zainstalować 30 dniowy testowy klucz licencyjny. W tym celu należy kliknąć testowy i postępować zgodnie z poleceniami wyświetlanymi na stronie.

W celu aktywacji aplikacji należy wybrać jedną z opcji:

- Przy użyciu klucza licencyjnego.** Należy wybrać tę metodę aktywacji w przypadku posiadania klucza licencyjnego dla programu Kaspersky Anti-Virus 6.0.

- ☛ **Aktywuj później.** Po wybraniu tej opcji, etap aktywacji zostanie pominięty. Na komputerze zainstalowany zostanie program Kaspersky Anti-Virus 6.0 for Windows Servers możliwy będzie dostęp do jego wszystkich funkcji za wyjątkiem aktualizacji (aktualizację można będzie wykonać tylko raz po zainstalowaniu programu).

3.2.2.2. Wybór klucza licencyjnego

Jeżeli użytkownik posiada plik klucza licencyjnego dla programu Kaspersky Anti-Virus for Windows Servers 6.0, kreator zaproponuje jego instalację. W celu instalacji pliku klucza licencyjnego należy użyć przycisku **Przełączaj** i wskazać lokalizację do pliku klucza licencyjnego o rozszerzeniu .key w oknie wyboru klucza licencyjnego.

Po pomyślnym zainstalowaniu klucza licencyjnego, w dolnej części okna wyświetlone zostaną informacje dotyczące licencjonowania: imię i nazwisko osoby, która zarejestrowała oprogramowanie, numer licencji, typ licencji (pełna, beta, demo itp.), oraz data wygaśnięcia okresu licencjonowania.

3.2.2.3. Finalizowanie aktywacji programu

Kreator wstępnej konfiguracji wyświetli informacje o pomyślnej aktywacji programu. Wyświetlone zostaną również informacje dotyczące zainstalowanego klucza licencyjnego: imię i nazwisko osoby, która zarejestrowała oprogramowanie, numer licencji, typ licencji (pełna, beta, demo itp.), oraz data wygaśnięcia okresu licencjonowania.

3.2.3. Konfiguracja ustawień aktualizacji

Bezpieczeństwo komputera zależy bezpośrednio od regularnej aktualizacji antywirusowych baz danych i modułów programu. W oknie tym, kreator wstępnej konfiguracji zaproponuje wybór trybu aktualizacji oraz możliwe będzie skonfigurowanie terminarza.

- ☛ **Automatycznie.** Kaspersky Anti-Virus automatycznie szuka nowych aktualizacji z uwzględnieniem zdefiniowanej częstotliwości. Procedura ta wykonywana jest częściej w trakcie trwania epidemii wirusa, oraz rzadziej po ich zakończeniu. Po wykryciu przez program najnowszych uaktualnień, są one pobierane i instalowane na komputerze. Jest to domyślne ustawienie.
- ☛ **Co 2 godziny.** Aktualizacja uruchamiana będzie automatycznie zgodnie z terminarzem. Możliwe jest skonfigurowanie terminarza przez kliknięcie przycisku **Zmień**. ☛ **Ręcznie.** Po wybraniu tej opcji, aktualizacja uruchamiana będzie ręcznie przez użytkownika.

Należy zauważyć, że sygnatury zagrożeń i moduły programu dołączone do oprogramowania mogą być przestarzałe w momencie instalacji programu. Dlatego też, zalecane jest pobieranie najnowszych aktualizacji. Aby to wykonać należy kliknąć przycisk **Uaktualnij teraz**. Kaspersky Anti-Virus for Windows Servers pobierze niezbędne uaktualnienia z serwerów aktualizacji i zainstaluje je na komputerze.

W celu dokonania konfiguracji procesu aktualizacji (konfiguracji ustawień sieciowych, wyboru źródła pobierania uaktualnień lub najbliższej położonego serwera aktualizacji), należy kliknąć odsyłacz **Ustawienia**.

3.2.4. Konfiguracja terminarza skanowania

Jednym z kluczowych elementów ochrony komputera jest wykonywanie skanowania wybranych obszarów komputera w poszukiwaniu szkodliwego oprogramowania.

Po zainstalowaniu programu Kaspersky Anti-Virus for Windows Servers, tworzone są trzy domyślne zadania skanowania antywirusowego. W oknie tym należy wybrać ustawienia skanowania:

Obiekty startowe

Domyślnie Kaspersky Anti-Virus skanuje obiekty startowe podczas uruchamiania. W celu zmodyfikowania ustawień terminarza skanowania obiektów startowych należy kliknąć przycisk **Zmień**.

Obszary krytyczne

W celu automatycznego skanowania krytycznych obszarów komputera (pamięć systemowa, obiekty startowe, foldery systemowe Windows Server) na obecność wirusów, należy zaznaczyć odpowiednią opcję. Możliwe jest skonfigurowanie terminarza przez kliknięcie przycisku **Zmień**.

Domyślnie automatyczne skanowanie jest wyłączone.

Mój komputer

W celu automatycznego uruchamiania zadania skanowania antywirusowego komputera, należy zaznaczyć odpowiednie pole. Możliwe jest skonfigurowanie terminarza przez kliknięcie przycisku **Zmień**.

Domyślnie automatyczne skanowanie komputera zgodnie z terminarzem jest wyłączone. Jednakże, zalecane jest przeprowadzenie pełnego skanowania serwera po instalacji programu.

3.2.5. Ograniczanie dostępu do programu

Z uwagi na możliwość użytkowania komputera przez wielu użytkowników oraz możliwość wyłączenia ochrony przez szkodliwe programy, dostępna jest opcja ochrony dostępu do programu za pomocą hasła. Za pomocą hasła można chronić program przed nieautoryzowanymi próbami wyłączenia ochrony lub zmiany ustawień.

W celu włączenia ochrony hasłem, należy zaznaczyć opcję **Włącz ochronę hasłem** i wypełnić pola **Nowe hasło** oraz **Potwierdzenie hasła**.

Należy wybrać obszar ochrony hasłem:

- Wszystkie działania (za wyjątkiem powiadomień o niebezpiecznych zdarzeniach)**. Żądanie podania hasła podczas próby wykonania dowolnego działania przez użytkownika za wyjątkiem odpowiedzi na powiadomienia pojawiające się po wykryciu niebezpiecznych obiektów.
- Wybrane operacje:**
 - Zapisanie ustawień programu** – żądanie podania hasła przy próbie zapisania zmian w ustawieniach aplikacji.
 - Zakończenie działania programu** – żądanie podania hasła podczas próby zamknięcia programu przez użytkownika.
 - Zatrzymanie/wstrzymanie usług ochrony lub zadań skanowania antywirusowego** – żądanie podania hasła przy próbie zatrzymania lub całkowitego wyłączenia dowolnego składnika ochrony lub zadania skanowania antywirusowego.

3.2.6. Finalizowanie działania kreatora konfiguracji

W ostatnim oknie kreatora wyświetlona zostanie informacja o pomyślnym zakończeniu instalacji i konfiguracji programu. Aby natychmiast uruchomić aplikację, należy zaznaczyć pole **Uruchom produkt**.

Jeżeli w czasie instalacji pojawił się problem (np.: niekompatybilność z innym oprogramowaniem antywirusowym), użytkownik zostanie poproszony o ponowne uruchomienie komputera.

3.3. Instalacja programu z poziomu wiersza poleceń

W celu zainstalowania programu Kaspersky Anti-Virus 6.0 for Windows Servers należy wprowadzić w wierszu poleceń następującą instrukcję:

```
msiexec /i <nazwa_pakietu>
```

Uruchomiony zostanie kreator instalacji (patrz rozdział 3.1 na stronie 21). Po zakończeniu instalacji należy ponownie uruchomić komputer.

Podczas instalacji z poziomu wiersza poleceń można także skorzystać z następujących modyfikatorów.

W celu zainstalowania aplikacji w tle, bez ponownego uruchamiania komputera (komputer powinien zostać zrestartowany ręcznie po zakończeniu instalacji), należy wpisać:

```
msiexec /i <nazwa_pakietu> /qn
```

W celu zainstalowania aplikacji w tle, z ponownym uruchomieniem komputera, należy wpisać:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

W celu zainstalowania aplikacji w tle i chronić instalację hasłem przy użyciu Kaspersky Administration Kit, należy wpisać:

```
msiexec /i <nazwa_pakietu> KLUNINSTPASSWD=***** /qn
```

3.4. Aktualizacja z wersji 5.0 do 6.0

Jeżeli na serwerze jest zainstalowany program Kaspersky Anti-Virus 5.0 for Windows Servers, można uaktualnić go do Kaspersky Anti-Virus 6.0.

Po uruchomieniu programu instalacyjnego aplikacji Kaspersky Anti-Virus 6.0 użytkownik otrzyma informację o konieczności usunięcia produktu w wersji 5.0. Po zakończeniu dezinstalacji programu, należy ponownie uruchomić komputer. Po uruchomieniu komputera, rozpoczęta zostanie instalacja wersji 6.0.

Ostrzeżenie!

Podczas instalacji programu Kaspersky Anti-Virus 6.0 for Windows Servers z foldera sieciowego zabezpieczonego hasłem na wersję 5.0, wersja 5.0 zostanie odinstalowana a komputer uruchomi się ponownie bez automatycznego rozpoczęcia instalacji wersji 6.0. Spowoduje to przerwanie procesu instalacji. W celu poprawnego zainstalowania programu, należy uruchomić program instalacyjny z lokalnego foldera.

ROZDZIAŁ 4. INTERFEJS PROGRAMU

Kaspersky Anti-Virus for Windows Servers zawiera prosty w użyciu interfejs. Niniejszy rozdział zawiera podstawowe informacje dotyczące następujących elementów interfejsu:

Ikona zasobnika systemowego (patrz rozdział 4.1 na stronie 31)

Menu kontekstowe (patrz rozdział 4.2 na stronie 32)



Okno główne (patrz rozdział 4.3 na stronie 33)

Okno ustawień programu (patrz rozdział 4.4 na stronie 36)




4.1. Ikona zasobnika systemowego

Po zainstalowaniu programu Kaspersky Anti-Virus for Windows Servers, w zasobniku systemu Windows pojawi się ikona programu.

Ikona obrazuje funkcje wykonywane przez program Kaspersky Anti-Virus for Windows Servers. Obrazuje ona stan ochrony i wyświetla funkcje wykonywane przez program.

Jeżeli ochrona jest włączona, ikona jest kolorowa  (stan aktywny). Jeżeli ochrona jest wyłączona, ikona jest szara  (stan nieaktywny), oznacza to, że ochrona jest całkowicie wyłączona lub wstrzymane jest działanie pewnych składników.

Ikona programu Kaspersky Anti-Virus for Windows Servers zmienia się w zależności od wykonywanej operacji:

	Skanywanie pliku otwieranego, zapisywanego lub uruchamianego przez użytkownika lub przez pewien program.
	Uaktualnianie baz danych i modułów programu Kaspersky Anti-Virus.
	wystąpił błąd w niektórych składnikach programu Kaspersky Anti-Virus.

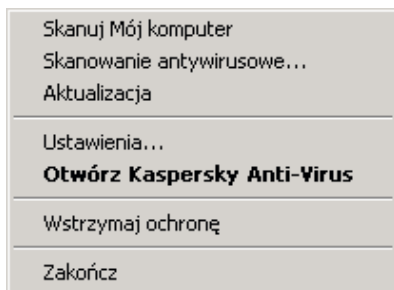
Ikona pozwala również na dostęp do podstawowych elementów interfejsu programu: menu kontekstowego (patrz rozdział 4.2 na stronie 32) oraz okna głównego programu (patrz rozdział 4.3 na stronie 33).

W celu otwarcia menu kontekstowego, należy kliknąć prawym przyciskiem myszy na ikonie programu.

W celu otwarcia okna głównego programu Kaspersky Anti-Virus for Windows Servers w sekcji Ochrona (jest to domyślna sekcja wyświetlana po otwarciu programu), należy dwukrotnie kliknąć lewym przyciskiem myszy na ikonie programu. Jednorazowe kliknięcie spowoduje otwarcie okna głównego w sekcji, która była aktywna przed ostatnim zamknięciem okna programu.

4.2. Menu kontekstowe

Z poziomu menu kontekstowego można uruchamiać podstawowe zadania ochrony (patrz rys. 1).



Rysunek 1. Menu kontekstowe

Menu kontekstowe programu Kaspersky Anti-Virus for Windows Servers zawiera następujące polecenia:

Skanuj Mój komputer – uruchomienie pełnego skanowania komputera w poszukiwaniu niebezpiecznych obiektów. Przeskanowane zostaną pliki na wszystkich dyskach twardej, włączając nośniki wymienne.

Skanowanie antywirusowe... – wybór obiektów i rozpoczęcie ich skanowania w poszukiwaniu wirusów. Domyślna lista zawiera różne foldery plików, takie jak folder Moje Dokumenty, folder startowy, pocztowe bazy danych, wszystkie dyski twarde znajdujące się na komputerze itp. Możliwe jest dodanie do tej listy żądanych plików i rozpoczęcie skanowania antywirusowego.

Aktualizacja – pobieranie i instalowanie uaktualnień modułów programu i sygnatur zagrożeń.

Aktywuj... – aktywacja programu. Ten element dostępny jest jedynie w przypadku, gdy program nie został aktywowany.

Ustawienia... – przeglądanie i konfigurowanie ustawień dla programu Kaspersky Anti-Virus for Windows Servers.

Otwórz Kaspersky Anti-Virus – otwarcie okna głównego programu (patrz rozdział 4.3 na stronie 33).

Wstrzymaj / Wznów ochronę – tymczasowe włączenie lub wyłączenie modułu **Ochrona plików**. Ten element nie wpływa na zadania pobierania uaktualnień i skanowania komputera.

Zakończ – zakończenie działania programu Kaspersky Anti-Virus for Windows Servers.

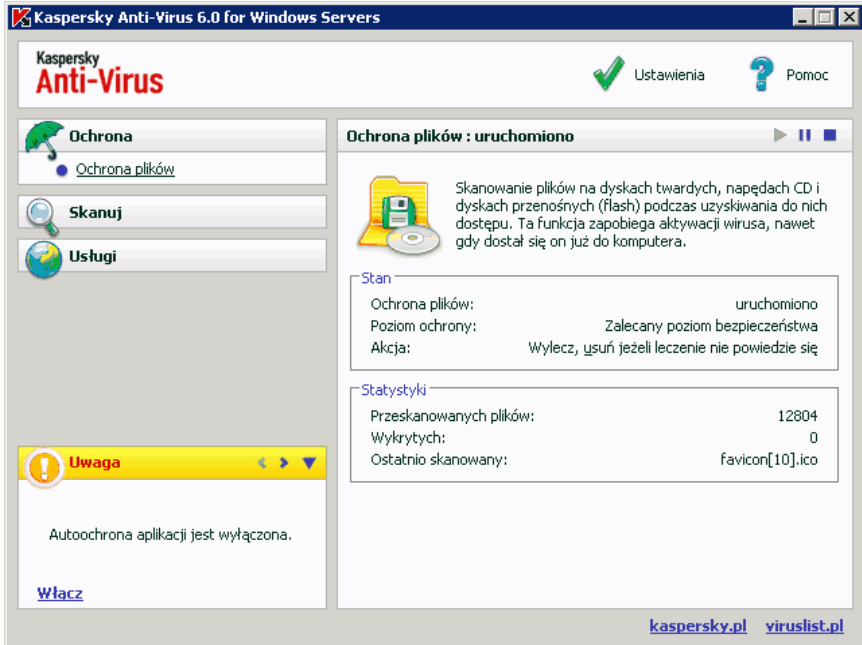
Jeżeli uruchomione jest zadanie skanowania antywirusowego, w menu kontekstowym wyświetlana będzie nazwa zadania oraz procentowy postęp. Po wybraniu zadania, można przejść do okna zawierającego raporty w celu wyświetlenia bieżących wyników wydajności.

4.3. Główne okno programu

Główne okno programu Kaspersky Anti-Virus for Windows Servers (patrz rys. 2) jest podzielone na dwie części:

w lewej sekcji okna znajduje się panel nawigacyjny, umożliwiający szybki i prosty dostęp do dowolnego składnika, wykonywanie skanowania antywirusowego lub użycie narzędzi dołączonych do programu;


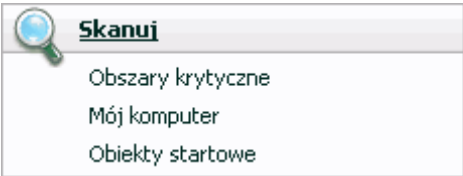
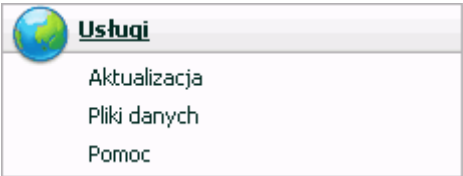
w prawej sekcji okna znajduje się panel informacyjny, zawierający informacje dotyczące wybranego w lewej sekcji składnika ochrony oraz wyświetlający ustawienia dla każdego z nich, a także udostępniający narzędzia do wykonywania skanowania, pracy z obiektami poddanymi kwarantannie i kopiami zapasowymi obiektów, zarządzanie kluczami licencyjnymi itp.



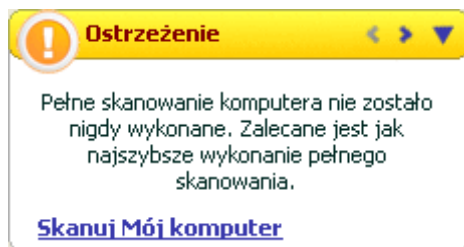
Rysunek 2. Główne okno Kaspersky Anti-Virus for Windows Servers

Po wybraniu elementu lub składnika w lewej sekcji okna, informacje o tym elemencie wyświetlone zostaną w prawej sekcji okna.

W dalszej części tego rozdziału opisane zostaną elementy okna głównego w celu przedstawienia bardziej szczegółowych informacji na ich temat.

Sekcja głównego okna	Przeznaczenie
<p>Okno to z reguły informuje o stanie ochrony komputera. Do tego celu przeznaczona jest sekcja Ochrona.</p> 	<p>W tej sekcji wyświetlane są ogólne informacje na temat działań wykonywanych przez Kaspersky Anti-Virus for Windows Servers oraz statystyki.</p>
<p>Do skanowania komputera w poszukiwaniu szkodliwych plików i programów, należy skorzystać z sekcji Skanuj znajdującej się w oknie głównym programu.</p> 	<p>Sekcja ta zawiera listę obiektów, które można użyć do skanowania antywirusowego.</p> <p>Możliwe jest również utworzenie zadania skanowania antywirusowego, które będzie widoczne w panelu nawigacyjnym. Funkcja ta upraszcza uruchamianie skanowania antywirusowego.</p> <p>W sekcji zawarte są domyślne zadania utworzone przez ekspertów z firmy Kaspersky Lab, które wykonywane są najczęściej. W ich skład wchodzi skanowanie obszarów krytycznych komputera, skanowanie obiektów startowych oraz pełne skanowanie komputera.</p>
<p>Sekcja Usługi zawiera dodatkowe funkcje programu Kaspersky Anti-Virus for Windows Servers.</p> 	<p>Z poziomu tej sekcji można uaktualnić aplikację, przeglądać raporty z działania programu i jego składników, przeglądać kwarantannę i kopię zapasową, przeglądać informacje na temat pomocy technicznej oraz zarządzać licencjami.</p>

W sekcji **Komentarze i podpowiedzi** wyświetlane są informacje i wskazówki podczas korzystania z programu.



W tej sekcji można przeczytać informacje na temat możliwości podniesienia poziomu ochrony serwera. Wyświetlane są także informacje na temat bieżącego działania aplikacji oraz jej ustawień.

Każdy element panelu nawigacyjnego skojarzony jest ze specjalnym menu kontekstowym. Menu dla modułu Ochrona plików umożliwia szybki dostęp do jego konfiguracji oraz raportów. Dodatkowe menu dla zadań skanowania oraz aktualizacji pozwala na tworzenie własnych zadań poprzez kopiowanie istniejących zadań.

Możliwe jest zmienianie wyglądu interfejsu programu poprzez tworzenie własnych schematów graficznych i kolorystycznych.

4.4. Okno ustawień programu

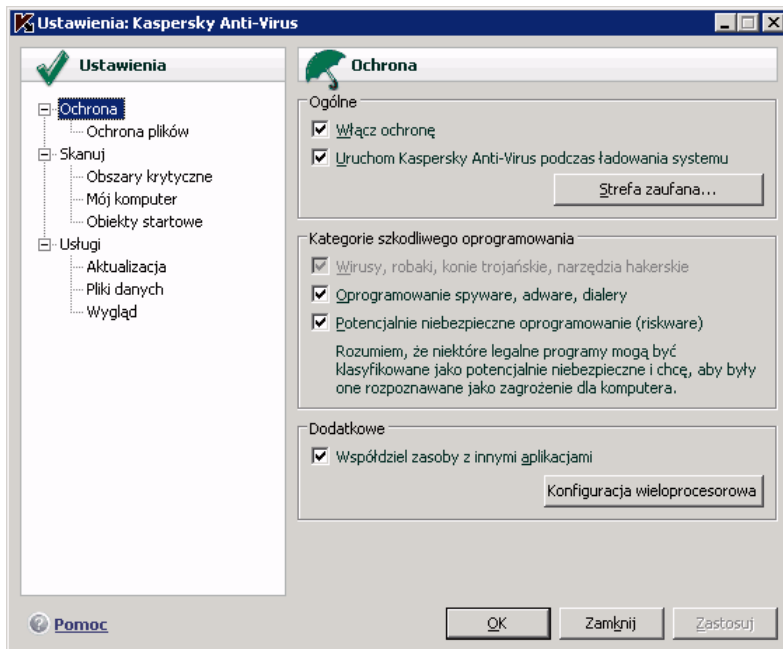
Z poziomu okna głównego programu można otworzyć okno ustawień Kaspersky Anti-Virus for Windows Servers (patrz rozdział 4.3 na stronie 33). W tym celu, należy kliknąć odsyłacz Ustawienia znajdujący się w górnej części okna.

Okno ustawień (patrz rys. 3) posiada identyczną strukturę jak okno główne programu:

w lewej sekcji okna można uzyskać szybki i prosty dostęp do ustawień każdego składnika programu, zadań skanowania oraz usług;

w prawej sekcji okna zawarta jest lista ustawień dla składnika wybranego w lewej sekcji okna.

Po wybraniu dowolnej sekcji, składnika lub zadania, w lewej sekcji okna ustawień, w prawej sekcji wyświetlone zostaną podstawowe ustawienia dla wybranego elementu. W celu konfiguracji zaawansowanych ustawień, należy otworzyć okna ustawień kolejnych poziomów. Szczegółowy opis ustawień programu dla poszczególnych sekcji znaleźć można w podręczniku użytkownika.



Rysunek 3. Okno ustawień Kaspersky Anti-Virus for Windows Servers

ROZDZIAŁ 5. ROZPOCZĘCIE PRACY

Jednym z głównych założeń firmy Kaspersky Lab w tworzeniu programu Kaspersky Anti-Virus for Windows Servers było zapewnienie optymalnej konfiguracji dla wszystkich opcji programu.

W celu uproszczenia rozpoczęcia korzystania z programu, wszystkie etapy wstępnej konfiguracji programu połączone zostały w jednym kreatorze konfiguracji programu (patrz rozdział 3.2 na stronie 25) uruchamianym podczas instalacji programu. Postępując zgodnie z instrukcjami kreatora, można aktywować program, skonfigurować ustawienia pobierania aktualizacji i uruchamiania skanowania, zdefiniować hasła dostępu do programu.

Po zainstalowaniu i uruchomieniu programu, zalecane jest przeprowadzenie następujących czynności:

Sprawdzenie bieżącego stanu ochrony (patrz rozdział 5.1 na stronie 38) w celu upewnienia się, że Kaspersky Anti-Virus for Windows Servers pracuje zgodnie z odpowiednim poziomem ochrony.

Uaktualnienie programu (patrz rozdział 5.5 na stronie 46) (jeżeli nie zostanie to wykonane automatycznie po zainstalowaniu programu).

Przeskanowanie komputera (patrz rozdział 5.2 na stronie 44) w poszukiwaniu wirusów.

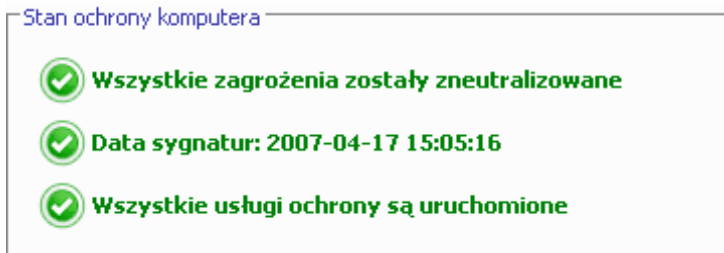
5.1. Jaki stan ochrony posiada komputer?

Informacje dotyczące stanu ochrony znajdują się w oknie głównym programu w sekcji **Ochrona**. W tej sekcji wyświetlany jest *bieżący stan ochrony komputera* oraz *ogólne statystyki*.

W sekcji **Stan ochrony komputera** wyświetlany jest bieżący stan ochrony komputera przy użyciu specjalnych wskaźników (patrz rozdział 5.1.1 na stronie 39). Sekcja **Statystyki** (patrz rozdział 5.1.2 na stronie 42) umożliwia analizę operacji wykonywanych podczas bieżącej sesji programu.




5.1.1. Wskaźniki ochrony

Sekcja **Stan ochrony komputera** zawiera trzy wskaźniki obrazujące poziom ochrony komputera w danym momencie oraz wyświetlające problemy dotyczące ustawień programu i jego działania.




Rysunek 4. Wskaźniki obrazujące stan ochrony komputera


Stopień ważności wyświetlanych zdarzeń odpowiada jednej z następujących wartości wskaźnika:

-  – *stan ochrony komputera nie budzi zastrzeżeń*; informuje on o prawidłowym poziomie ochrony i braku problemów z ustawieniami i funkcjonowaniem poszczególnych składników programu.
-  – w funkcjonowaniu Kaspersky Anti-Virus for Windows Servers *wystąpiło przynajmniej jedno odstępstwo od zalecanego poziomu ochrony*, mogące spowodować naruszenie bezpieczeństwa danych. Należy zapoznać się z zaleceniami ekspertów z firmy Kaspersky Lab. Zalecane działania dostępne są w postaci odsyłaczy.
-  – *stan ochrony komputera jest krytyczny*. Należy zapoznać się z zaleceniami ekspertów z firmy Kaspersky Lab. Zalecane działania dostępne są w postaci odsyłaczy.



Poniżej przedstawione zostały wskaźniki ochrony oraz sytuacje o których każdy z nich informuje.


Pierwszy wskaźnik obrazuje postępowanie ze szkodliwymi plikami i programami na komputerze. Wskaźnik przyjmuje jedną następujących wartości:

	<p><i>Nie wykryto zagrożeń</i></p> <p>Kaspersky Anti-Virus for Windows Servers nie wykrył na komputerze żadnego szkodliwego pliku lub programu.</p>
---	---



	<p><i>Wszystkie zagrożenia zostały zneutralizowane</i></p> <p>Kaspersky Anti-Virus for Windows Servers wyleczył wszystkie pliki i programy zainfekowane wirusami i usunął te, których nie udało się wyleczyć.</p>
	<p><i>Wykryto zagrożenia</i></p> <p>Istnieje ryzyko infekcji komputera. Kaspersky Anti-Virus for Windows Servers wykrył szkodliwe programy (wirusy, trojany, robaki itp.), które muszą zostać zneutralizowane. W tym celu, należy użyć odsyłacza Neutralizuj wszystkie. W celu wyświetlenia szczegółowych informacji dotyczących szkodliwych obiektów, należy kliknąć przycisk Szczegóły.</p>


Drugi wskaźnik obrazuje szczegółowość ochrony komputera. Wskaźnik przyjmuje jedną następujących wartości:

	<p><i>Data sygnatur (data, czas)</i></p> <p>Sygnatury zagrożeń oraz moduły aplikacji używane przez program Kaspersky Anti-Virus for Windows Servers są aktualne.</p>
	<p><i>Sygnatury zagrożeń są nieaktualne</i></p> <p>Moduły programu i sygnatury zagrożeń programu Kaspersky Anti-Virus for Windows Servers nie były uaktualniane od kilku dni. Istnieje ryzyko zainfekowania komputera nowymi szkodliwymi programami, które pojawiły się od momentu ostatniej aktualizacji programu. Zalecane jest uaktualnienie Kaspersky Anti-Virus for Windows Servers. W tym celu, należy użyć odsyłacza Uaktualnij teraz.</p>
	<p><i>Sygnatury są częściowo uszkodzone</i></p> <p>Sygnatury zagrożeń są częściowo uszkodzone. W takim przypadku zaleca się ponownie uruchomienie aktualizacji programu. W przypadku ponownego wystąpienia tego samego błędu, należy skontaktować się z działem pomocy technicznej firmy Kaspersky Lab.</p>
	<p><i>Uruchom ponownie komputer</i></p> <p>Aby program działał poprawnie należy ponownie uruchomić system operacyjny. Należy zachować zmiany i zamknąć wszystkie używane pliki oraz użyć odsyłacza Uruchom komputer</p>

	<u>ponownie.</u>
	<p><i>Uaktualnienia programu są wyłączone</i></p> <p>Usługi aktualizacji modułów programu i sygnatur zagrożeń są wyłączone. W celu utrzymania ochrony w czasie rzeczywistym zalecane jest włączenie pobierania aktualizacji.</p>
	<p><i>Sygnatury zagrożeń są bardzo stare</i></p> <p>Kaspersky Anti-Virus for Windows Servers nie był aktualizowany od dłuższego czasu. Istnieje duże ryzyko zainfekowania komputera. Należy uaktualnić program najszybciej jak jest to możliwe. W tym celu, należy użyć odsyłacza <u>Uaktualnij teraz</u>.</p>
	<p><i>Sygnatury są uszkodzone</i></p> <p>Sygnatury zagrożeń są całkowicie uszkodzone. W takim przypadku zaleca się ponownie uruchomienie aktualizacji programu. W przypadku ponownego wystąpienia tego samego błędu, należy skontaktować się z działem pomocy technicznej firmy Kaspersky Lab.</p>

Trzeci wskaźnik obrazuje bieżącą funkcjonalność programu. Wskaźnik przyjmuje jedną następujących wartości:

	<p><i>Wszystkie składniki ochrony są uruchomione</i></p> <p>Kaspersky Anti-Virus for Windows Servers chroni wszystkie możliwe kanały komputera przed penetracją szkodliwych programów.</p>
	<p><i>Ochrona nie jest zainstalowana</i></p> <p>Podczas instalacji Kaspersky Anti-Virus for Windows Servers nie zainstalowano żadnych składników ochrony. Oznacza to, że można jedynie wykonywać skanowanie antywirusowe. W celu zapewnienia maksymalnej ochrony należy zainstalować składniki ochrony.</p>
	<p><i>Wszystkie usługi ochrony zostały wstrzymane</i></p> <p>Działanie składnika ochrony zostało wstrzymane. W celu wznowienia działania składnika należy wybrać opcję Wznów ochronę z menu kontekstowego programu, które zostanie wyświetlone po kliknięciu prawym przyciskiem myszy na ikonie programu znajdującej się w zasobniku systemowym.</p>

	<p><i>Wszystkie usługi ochrony są wyłączone</i></p> <p>Ochrona jest całkowicie wyłączona. Składnik ochrony nie jest uruchomiony. W celu wznowienia działania składnika należy wybrać opcję Wznów ochronę z menu kontekstowego programu, które zostanie wyświetlone po kliknięciu prawym przyciskiem myszy na ikonie programu znajdującej się w zasobniku systemowym.</p>
	<p><i>Niektóre usługi ochrony nie działają prawidłowo</i></p> <p>Podczas działania jednego lub więcej składników programu Kaspersky Anti-Virus wystąpił błąd wewnętrzny. W takim przypadku należy włączyć składnik lub ponownie uruchomić komputer, ponieważ może to być spowodowane tym, że sterowniki składnika nie zostały zarejestrowane po aktualizacji.</p>

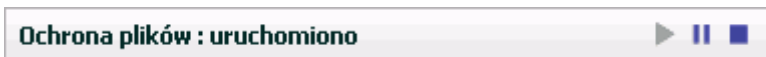
5.1.2. Stan składników programu Kaspersky Anti-Virus for Windows Servers

W celu sprawdzenia, w jaki sposób Kaspersky Anti-Virus for Windows Servers chroni system plików lub w celu przeglądania zadań skanowania lub postępu pobierania uaktualnień, należy otworzyć odpowiednią sekcję okna głównego.

Przykładowo, w celu przeglądania bieżącego stanu ochrony antywirusowej dla plików, należy w lewej sekcji okna głównego programu wybrać element **Ochrona plików**. Szczegółowe informacje dotyczące funkcjonowania składnika wyświetlone zostaną w prawej sekcji okna głównego programu.

W przypadku składników ochrony, prawy panel podzielony jest na pasek stanu, sekcję **Stanu** oraz sekcję **Statystyki**.

Dla składnika **Ochrona plików**, pasek stanu wygląda następująco:



Ochrona plików : uruchomiono – ochrona plików jest aktywna i działa zgodnie z wybranym poziomem (patrz rozdział 7.1 na stronie 69).

Ochrona plików: wstrzymano – działanie modułu Ochrona plików jest wstrzymane na pewien okres czasu. Składnik automatycznie wznowi funkcjonowanie po wygaśnięciu przydzielonego okresu czasu lub po ponownym uruchomieniu programu. Możliwe jest również ręczne

wznowienie ochrony dla plików. W tym celu, należy kliknąć przycisk ► znajdujący się na pasku stanu.

Ochrona plików : zatrzymano – działanie składnika zostało zatrzymane przez użytkownika. Możliwe jest również ręczne wznowienie ochrony dla plików. W tym celu, należy kliknąć przycisk ► znajdujący się na pasku stanu.

Ochrona plików : nieuruchomiono – moduł ochrony plików nie jest dostępny. Na przykład, nie zainstalowano klucza licencyjnego dla programu.

Ochrona plików : wyłączono (błąd) – podczas uruchamiania składnika wystąpił błąd. Po wystąpieniu błędu, należy skontaktować się z pomocą techniczną firmy Kaspersky Lab.

Ustawienia wykorzystywane przez składnik wyświetlane są w sekcji **Stan**:

Ochrona plików – bieżący stan składnika (uruchomiono, zatrzymano, wstrzymano, itd.).

Poziom ochrony – zestaw parametrów zdefiniowanych dla działania składnika. Domyślnie wybrany jest **zalecany poziom ochrony**, co oznacza, że skanowane są wyłącznie obiekty systemu plików, które mogą zostać zainfekowane. Na przykład, pliki wykonywalne (.exe).

Akcja jaka ma zostać podjęta po wykryciu niebezpiecznego obiektu.

Zadania skanowania i aktualizacji nie zawierają sekcji **Stan**. Poziom ochrony, akcje podejmowane po wykryciu niebezpiecznego programu oraz tryb uruchamiania zadania aktualizacji wyświetlane są w sekcji **Ustawienia**.

Sekcja **Statystyki** zawiera informacje dotyczące funkcjonowania składników ochrony, aktualizacji lub zadań skanowania antywirusowego.

5.1.3. Statystyki działania programu

Statystyki programu znaleźć można w sekcji **Statystyki** znajdującej się w sekcji **Ochrona** w oknie głównym programu. Zawierają one informacje dotyczące ochrony komputera, zarejestrowanych od momentu instalacji programu Kaspersky Anti-Virus for Windows Servers.

Statystyki	
Przeskanowanych plików:	14110
Wykrytych:	0
Ostatnio skanowany:	bmp.lnk

Rysunek 5. Statystyki programu

W celu wyświetlenia raportu zawierającego szczegółowe informacje należy kliknąć w tym polu lewym przyciskiem myszy. Na zakładkach wyświetlane są:

Informacje o znalezionych obiektach i stanie, który został do nich przydzielony (patrz rozdział 11.3.2 na stronie 126)

Dziennik zdarzeń (patrz rozdział 11.3.3 na stronie 126)

Ogólne statystyki komputera (patrz rozdział 11.3.4 na stronie 128)

Ustawienia programu (patrz rozdział 11.3.5 na stronie 128)

5.2. W jaki sposób wykonać skanowanie serwera

Po zainstalowaniu programu wyświetlony zostanie komunikat informujący, że pełne skanowanie komputera nie zostało dotychczas wykonane i zalecane jest jego natychmiastowe przeprowadzenie.

Kaspersky Anti-Virus zawiera zestaw domyślnych zadań skanowania antywirusowego komputera. Są one dostępne sekcji **Skanuj** okna głównego programu.

Po wybraniu zadania **Mój komputer**, w prawej części okna głównego programu możliwe będzie przeglądanie statystyk dotyczących informacji odnośnie skanowania oraz ustawień dla tego zadania: wybranego poziomu ochrony oraz akcji, które będą podejmowane po wykryciu niebezpiecznych obiektów.

W celu przeskanowania komputera w poszukiwaniu szkodliwych programów należy,

Kliknąć przycisk **Skanuj** znajdujący się w prawej części okna.

Program rozpocznie skanowanie serwera wyświetlając szczegóły dotyczące skanowania w specjalnym oknie. Możliwe jest ukrycie okna informacyjnego skanowania. W tym celu, należy je zamknąć; nie spowoduje to zatrzymania skanowania.

5.3. W jaki sposób wykonać skanowanie obszarów krytycznych

Bardzo ważne jest zabezpieczenie tych obszarów w celu prawidłowego funkcjonowania komputera. Stworzone zostało specjalne zadanie skanowania

dla tego typu obszarów. Znajduje się ono w oknie głównym programu w sekcji **Skanuj**.

Po wybraniu zadania **Obszary krytyczne**, w prawej części okna głównego programu możliwe będzie przeglądanie statystyk dotyczących informacji odnośnie skanowania tych obszarów oraz ustawień dla tego zadania: wybranego poziomu ochrony oraz akcji, które będą podejmowane po wykryciu zagrożenia. Możliwe jest również wybranie, które z obszarów krytycznych mają zostać przeskanowane i natychmiastowe uruchomienie skanowania wybranych obszarów.

W celu przeskanowania obszarów krytycznych w poszukiwaniu szkodliwych programów należy,

Kliknąć przycisk **Skanuj** znajdujący się w prawej części okna.

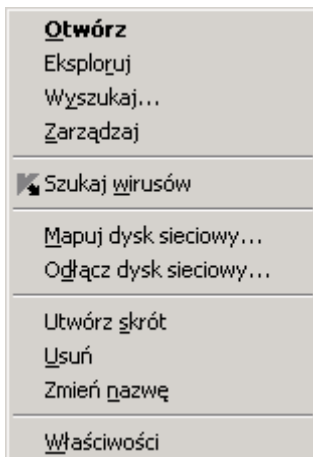
Program rozpocznie skanowanie wybranych obszarów krytycznych, wyświetlając szczegóły dotyczące skanowania w specjalnym oknie. Możliwe jest ukrycie okna informacyjnego skanowania. W tym celu, należy je zamknąć; nie spowoduje to zatrzymania skanowania.

5.4. W jaki sposób wykonać skanowanie plików, folderów lub dysków

Czasami istnieje potrzeba przeskanowania indywidualnych obiektów na obecność wirusów: na przykład, jednego z dysków twardych. Obiekty przeznaczone do skanowania mogą zostać wybrane przy użyciu standardowych narzędzi systemu **Microsoft Windows Server** (na przykład **Eksploratora Windows**, sekcji **Mój komputer**, pulpitu itd.).

Aby wykonać skanowanie obiektu,

Kliknąć prawym przyciskiem żądany obiekt i z menu kontekstowego, które zostanie wyświetlone na ekranie wybrać polecenie **Szukaj wirusów** (patrz rys. 6).



Rysunek 6. Skanowanie wybranego obiektu przy użyciu standardowych narzędzi systemu Microsoft Windows Server

Program rozpocznie skanowanie wybranych obiektów, wyświetlając szczegóły dotyczące skanowania w specjalnym oknie. Możliwe jest ukrycie okna informacyjnego skanowania. W tym celu, należy jej zamknąć; nie spowoduje to zatrzymania skanowania.

5.5. W jaki sposób dokonać aktualizacji programu

Firma Kaspersky Lab aktualizuje sygnatury zagrożeń i moduły programu Kaspersky Anti-Virus for Windows Servers przy użyciu serwerów aktualizacji.

Serwery uaktualnień firmy Kaspersky Lab są miejscami w Internecie, w których firma Kaspersky Lab przechowuje aktualizacje programu.

Uwaga!

W celu uaktualnienia programu Kaspersky Anti-Virus for Windows Servers wymagane jest posiadanie dostępu do Internetu.

Domyślnie, Kaspersky Anti-Virus for Windows Servers automatycznie wyszukuje aktualizacje na serwerach firmy Kaspersky Lab. Jeżeli na serwerze dostępne są nowe uaktualnienia, Kaspersky Anti-Virus pobierze je i zainstaluje w tle.

W celu ręcznej aktualizacji programu Kaspersky Anti-Virus for Windows Servers należy,

wybrać sekcję **Aktualizacja** znajdującą się w sekcji **Usługi** okna głównego programu i kliknąć przycisk **Uaktualnij teraz** wyświetlany w prawym w prawej części okna.

Kaspersky Anti-Virus for Windows Servers rozpocznie pobieranie uaktualnień, wyświetlając w specjalnym oknie szczegóły dotyczące aktualizacji.

5.6. Co należy zrobić, jeżeli ochrona jest wyłączona

W przypadku wystąpienia problemów w funkcjonowaniu modułu Ochrona plików, należy sprawdzić jego stan. Jeżeli jego stan to *nie uruchomiono* lub *błąd w działaniu*, należy spróbować ponownie uruchomić aplikację.

Jeżeli ponowne uruchomienie programu nie rozwiąże problemu, zalecane jest naprawienie potencjalnych błędów przy użyciu funkcji przywracania aplikacji (**Start** → **Programy** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Modyfikuj, Napraw lub Usuń**).

Jeżeli procedura przywracania nie rozwiąże problemu, zalecane jest skontaktowanie się z działem pomocy technicznej firmy Kaspersky Lab. Należy zapisać raport z funkcjonowania składnika i wysłać go do firmy Kaspersky Lab w celu analizy.

W celu zapisania raportu do pliku należy:

1. Wybrać składnik **Ochrona plików** w sekcji **Ochrona** znajdujący się w oknie głównym programu i kliknąć lewym przyciskiem myszy w sekcji **Statystyki**.
2. Kliknąć przycisk **Zapisz jako** i w oknie które zostanie otwarte określić nazwę dla pliku raportu.

Aby zapisać raport z uruchamiania lub stanu wszystkich składników Kaspersky Anti-Virus (Ochrona plików, zadania skanowania antywirusowego, usługi):

1. Wybrać sekcję **Ochrona** w oknie głównym programu i kliknąć lewym przyciskiem myszy w polu **Statystyki**.

lub

Kliknąć przycisk Wszystkie raporty znajdujący się w oknie raportów każdego składnika. Na zakładce **Raporty** wyświetlona zostanie lista raportów dla wszystkich składników programu.

2. Kliknąć przycisk **Zapisz jako** i w oknie które zostanie otwarte określić nazwę dla pliku raportu.

ROZDZIAŁ 6. ZARZĄDZANIE OCHRONĄ

Kaspersky Anti-Virus for Windows Servers pozwala na wielozadaniowe zarządzanie ochroną serwera:

Włączanie, wyłączenie i wstrzymywanie działania programu (patrz rozdział 6.1 na stronie 49).

Definiowanie typów niebezpiecznych programów (patrz rozdział 6.2 na stronie 53), przed którymi chronił będzie program Kaspersky Anti-Virus for Windows Servers.

Tworzenie list wykluczeń z ochrony (patrz rozdział 6.3 na stronie 54).

Tworzenie własnych zadań skanowania i aktualizacji (patrz rozdział 6.4 na stronie 62).

Konfigurowanie terminarza skanowania antywirusowego (patrz rozdział 6.5 na stronie 64).

Konfigurowanie ustawień wydajności (patrz rozdział 6.6 na stronie 66).

6.1. Wstrzymywanie i wznowianie ochrony komputera

Domyślnie Kaspersky Anti-Virus chroni komputer użytkownika natychmiast po jego uruchomieniu. Świadczył będzie o tym napis Kaspersky Anti-Virus 6.0, znajdujący się w prawym górnym rogu ekranu. Moduł Ochrona plików (patrz rozdział 2.2.1 na stronie 16) jest domyślnie uruchomiony.

Możliwe jest wyłączenie ochrony oferowanej przez program Kaspersky Anti-Virus for Windows Servers.

Ostrzeżenie!

Firma Kaspersky Lab **nie zaleca wyłączenia ochrony**, ponieważ może to spowodować zainfekowanie komputera i utratę danych.

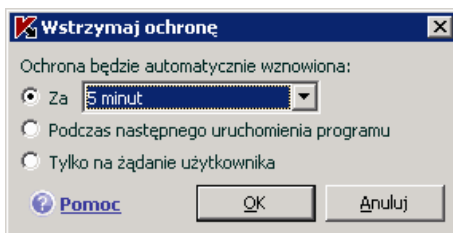
Należy pamiętać o tym, że w takim przypadku ochrona jest omawiana w kontekście modułu Ochrona plików. Wyłączenie lub wstrzymanie tego składnika nie ma wpływu na działanie zadań skanowania i aktualizacji programu.

6.1.1. Wstrzymywanie ochrony

Wstrzymanie ochrony oznacza tymczasowe wyłączenie działania modułu Ochrona plików.

W celu wstrzymania funkcjonowania programu Kaspersky Anti-Virus for Windows Servers należy:


1. Z menu kontekstowego programu wybrać opcję **Wstrzymaj ochronę** (patrz rozdział 4.2 na stronie 32).
2. W oknie, które zostanie otwarte należy wybrać jedną z następujących opcji (patrz rys. 7):
 - **Za <przedział czasu>** - ochrona zostanie włączona po upływie określonego okresu czasu. Przy użyciu listy rozwijalnej należy wybrać przedział czasu.
 - **Podczas następnego uruchomienia programu** - ochrona zostanie wznowiona po uruchomieniu programu z menu Start lub po ponownym uruchomieniu komputera (jeżeli wybrane jest automatyczne uruchamianie programu wraz ze startem systemu (patrz rozdział 6.1.5 na stronie 53).
 - **Tylko na żądanie użytkownika** - ochrona będzie nieaktywna, dopóki użytkownik jej nie wznowi. W celu wznowienia ochrony należy wybrać opcję **Wznów ochronę** z menu kontekstowego programu.



Rysunek 7. Okno wstrzymywania ochrony

Wskazówka:


Możliwe jest również wyłączenie ochrony komputera przy użyciu jednej z następujących metod:

- Kliknięcie przycisku  w sekcji Ochrona.
- Wybranie opcji **Zakończ** z menu kontekstowego. W tym przypadku program zostanie wyładowany z pamięci komputera.

Po wstrzymaniu ochrony, wstrzymane zostanie również działanie modułu Ochrona plików. Zobrazowane jest to przez:

Nieaktywna (szara) ikona modułu **Ochrona plików** wyświetlana w sekcji **Ochrona** okna głównego programu.

Nieaktywną (czarno białą) ikonę programu w zasobniku systemowym.

Trzeci wskaźnik ochrony komputera, pokazuje, że  **Wszystkie usługi ochrony zostały wstrzymane** (patrz rozdział 5.1.1 na stronie 39).

6.1.2. Zatrzymywanie ochrony serwera

Zatrzymanie ochrony oznacza całkowite wyłączenie modułu Ochrona plików. Zadania skanowania i aktualizacji będą kontynuować działanie.

Jeżeli ochrona jest zatrzymana, może ona zostać włączona jedynie przez administratora: moduł Ochrona plików nie zostanie automatycznie włączone po ponownym uruchomieniu systemu lub programu. Należy zapamiętać, że jeżeli wystąpi konflikt programu Kaspersky Anti-Virus for Windows Servers z innymi programami zainstalowanymi na serwerze, można wstrzymać wstrzymać działanie modułu Ochrona plików lub utworzyć listę wykluczeń (patrz rozdział 6.3 na stronie 54).


W celu całkowitego wyłączenia ochrony należy:

1. Otworzyć główne okno Kaspersky Anti-Virus for Windows Servers.
2. Wybrać sekcję **Ochrona** i kliknąć odsyłacz Ustawienia.
3. W oknie ustawień programu, należy usunąć zaznaczenie z opcji **Włącz ochronę**.

Po wyłączeniu ochrony zatrzymane zostanie działanie modułu Ochrona plików. Zobrazowane jest to przez:

Nieaktywna (szara) ikona modułu **Ochrona plików** wyświetlana w sekcji **Ochrona** okna głównego programu.


Nieaktywną (czarno białą) ikonę programu w zasobniku systemowym.


Trzeci wskaźnik ochrony komputera, pokazuje, że  **Wszystkie usługi ochrony zostały wstrzymane** (patrz rozdział 5.1.1 na stronie 39).

6.1.3. Wstrzymywanie / wyłączenie składników ochrony oraz zadań skanowania i aktualizacji

Dostępnych jest wiele metod wyłączenia modułu Ochrony plików, skanowania antywirusowego lub aktualizacji. Przed wykonaniem tej czynności, należy zweryfikować konieczność wyłączenia ochrony. Możliwe jest rozwiązanie problemu w inny sposób, na przykład: zmieniając poziom bezpieczeństwa. W przypadku pracy z bazą danych niezawierającą wirusów, należy dodać jej pliki do wykluczeń (patrz rozdział 6.3 na stronie 54).


W celu wstrzymania działania modułu Ochrona plików oraz zadań skanowania i aktualizacji należy:


Wybrać składnik lub zadanie w lewej części okna głównego programu i kliknąć przycisk  znajdujący się na pasku.

Stan składnika/zadania zmieniony zostanie na **wstrzymano**. Składnik lub zadanie pozostanie wstrzymane do momentu jego wznowienia po kliknięciu przycisku .

Po wstrzymaniu składnika lub zadania, statystyki dla bieżącej sesji programu Kaspersky Anti-Virus zostaną zapisane. Statystyki będą rejestrowane dalej natychmiast po zmianie stanu składnika lub zadania.

W celu zatrzymania działania składnika ochrony lub zadania:

Kliknąć przycisk  znajdujący się na pasku stanu. Można także zatrzymać działanie składnika przy użyciu okna ustawień. W tym celu należy usunąć zaznaczenie z opcji **Włącz <nazwa składnika>** znajdującej się w sekcji **Ogólne**.

Stan składnika/zadania zmieniony zostanie na **wyłączone**. Składnik lub zadanie pozostanie wyłączone do momentu jego włączenia po kliknięciu przycisku . W przypadku zadań skanowania i aktualizacji, należy wykonać jedną z następujących czynności: kontynuowanie działania przerwanej zadania lub ponowne jego uruchomienie.

Po zatrzymaniu działania składnika lub zadania, statystyki dla bieżącej sesji zostaną usunięte po ponownym uruchomieniu składnika lub zadania.

6.1.4. Przywracanie ochrony komputera

W przypadku wstrzymania lub wyłączenia ochrony komputera, można ją wznowić przy użyciu następujących metod:


Z poziomu menu kontekstowego.

W tym celu, należy wybrać polecenie **Wznów ochronę**.

Z poziomu okna głównego programu.

Aby to zrobić należy kliknąć przycisk  znajdujący się na pasku stanu wyświetlanym w sekcji **Ochrona** głównego okna programu.

Stan ochrony zostanie natychmiast zmieniony na *uruchomiono*. Ikona programu znajdująca się w zasobniku systemowym stanie się aktywna. Trzeci wskaźnik

ochrony (patrz rozdział 5.1.1 na stronie 39) będzie wyświetlał stan 
Wszystkie składniki ochronne są włączone.

6.1.5. Wyłączanie programu

W celu wyłączenia programu Kaspersky Anti-Virus for Windows Servers, należy wybrać opcję **Zakończ** znajdującą się w menu kontekstowym programu (patrz rozdział 4.2 na stronie 32). Program zostanie wyłączony, pozostawiając komputer bez ochrony.

Po zamknięciu programu, można włączyć go ponownie uruchamiając Kaspersky Anti-Virus for Windows Servers z menu Start (**Start** → **Programy** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Kaspersky Anti-Virus 6.0 for Windows Servers**).

Można równie automatycznie wznowić ochronę po ponownym uruchomieniu komputera. W celu włączenia tej funkcji, należy zaznaczyć opcję **Uruchom Kaspersky Anti-Virus podczas startu systemu** znajdującą się w oknie ustawień programu w sekcji **Ochrona**.

6.2. Wybieranie szkodliwych programów do monitorowania

Kaspersky Anti-Virus for Windows Servers chroni przed różnymi typami szkodliwych programów. Niezależnie od ustawień, program zawsze skanuje i neutralizuje wirusy, trojany i programy typu backdoor. Tego programy mogą wyrządzić największe uszkodzenia na komputerze. W celu zwiększenia

bezpieczeństwa komputera, można rozszerzyć listę zagrożeń, które będą wykrywane przez program poprzez włączenie monitorowania różnych typów niebezpiecznych programów.

W celu wybrania rodzaju szkodliwych programów, przed którymi chronić będzie Kaspersky Anti-Virus for Windows Servers, należy wybrać sekcję **Ochrona** w oknie ustawień programu (patrz rozdział 4.4 na stronie 36).

Sekcja **Kategorie szkodliwego oprogramowania** zawiera następujące typy zagrożeń:

- Wirusy, robaki, konie trojańskie, narzędzia hakerskie.** Grupa ta zawiera najbardziej powszechne kategorie szkodliwych programów. Jest to minimalny dopuszczalny poziom ochrony. Zgodnie z zaleceniami ekspertów z firmy Kaspersky Lab, nie można usunąć tych obiektów z listy elementów monitorowanych przez program Kaspersky Anti-Virus.
- Spyware, adware, dialery.** Grupa ta zawiera potencjalnie niebezpieczne oprogramowanie, które może stanowić źródło zagrożenia dla danych użytkownika.
- Potencjalnie niebezpieczne oprogramowanie (riskware).** Grupa ta zawiera programy, które jako takie nie są szkodliwe lub niebezpieczne. Jednak, w pewnych okolicznościach, mogą one zostać użyte w celu wyrządzenia szkody w komputerze. Jednakże, w pewnych okolicznościach mogą one zostać użyte w celu wyrządzenia szkody w komputerze.

Grupy opisane powyżej obejmują pełny obszar sygnatur zagrożeń, które wykrywane są przez program podczas skanowania obiektów.

Po wybraniu wszystkich grup, Kaspersky Anti-Virus for Windows Servers zapewnia najpełniejszą możliwą ochronę antywirusową komputera. W przypadku, gdy druga i trzecia grupa jest wyłączona, program chronić będzie jedynie przed najbardziej powszechnymi szkodliwymi programami. Nie są wliczane w to potencjalnie niebezpieczne programy oraz takie, które po zainstalowaniu na komputerze mogą uszkodzić pliki lub spowodować kradzież pieniędzy.

Ekspersi z firmy Kaspersky Lab nie zalecają wyłączenia monitorowania dla drugiej grupy. W sytuacji, w której Kaspersky Anti-Virus sklasyfikuje program jako wirusa, a w rzeczywistości tak nie jest, zalecane jest zdefiniowanie dla niego wykluczenia (patrz rozdział 6.3 na stronie 54).

6.3. Tworzenie strefy zaufanej

Zaufana strefa jest listą obiektów utworzoną przez administratora, które nie są monitorowane przez program Kaspersky Anti-Virus for Windows Servers. Innymi słowy, jest to grupa programów wykluczonych z ochrony.

Administrator tworzy zaufaną strefę w oparciu o właściwości używanych przez niego plików i programów zainstalowanych na komputerze. Może okazać się niezbędne utworzenie tego typu listy wykluczeń, jeżeli na przykład, Kaspersky Anti-Virus for Windows Servers blokuje dostęp do obiektu lub programu, który w opinii użytkownika jest całkowicie bezpieczny.

Możliwe jest wykluczanie z obszaru skanowania określonych formatów plików, użycie masek plików, wykluczanie określonych obszarów (na przykład, folderu lub programu), wykluczanie procesów programu lub obiektów według przypisanego do nich werdyktu zgodnego z nazewnictwem Encyklopedii Wirusów.

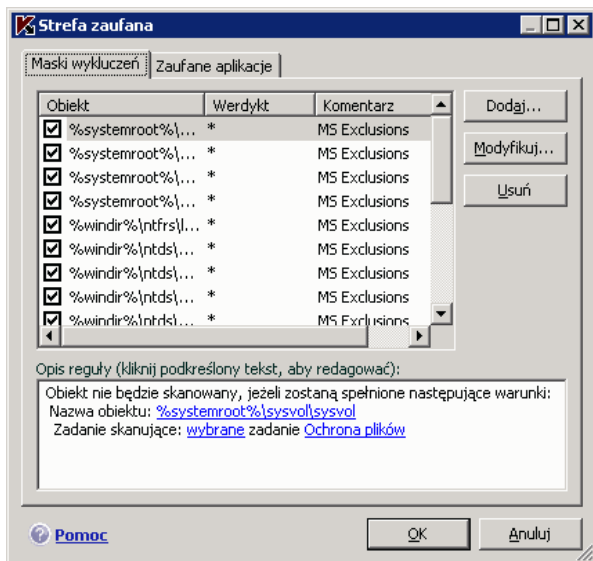
Uwaga!

Wykluczone obiekty nie są skanowane nawet jeżeli folder lub dysk, gdzie się one znajdują znajduje się na liście skanowanych obiektów. Jeżeli ten obiekt zostanie bezpośrednio wybrany do skanowania, wykluczenie nie zostanie użyte.

W celu utworzenia listy wykluczeń należy,

1. Otworzyć okno ustawień programu Kaspersky Anti-Virus for Windows Servers i wybrać sekcję **Ochrona**.
2. Kliknąć przycisk **Strefa zaufana**, znajdujący się w sekcji **Ogólne**.

Dokonać konfiguracji reguł dla obiektów i utworzyć listę zaufanych aplikacji w oknie, które zostanie otwarte (patrz rys. 8).



Rysunek 8. Tworzenie strefy zaufanej

6.3.1. Reguły wykluczeń

Reguły wykluczeń są zestawem warunków używanych przez Kaspersky Anti-Virus for Windows Servers w celu wyłączenia obiektów z obszaru skanowania.

Użytkownik może wykluczyć ze skanowania określone formaty plików, użyć masek plików lub wykluczyć żądany obszar (na przykład, folder lub aplikację), procesy programu lub obiekty na podstawie werdyktu zgodnego z nazewnictwem stosowanym w Encyklopedii Wirusów.

Werdykt to *stan*, jaki Kaspersky Anti-Virus przypisuje obiektowi podczas skanowania. *Werdykt* jest przypisywany jest na podstawie klasyfikacji Encyklopedii Wirusów tworzonej przez Kaspersky Lab i obejmującej szkodliwe oprogramowanie oraz potencjalnie niebezpieczne aplikacje.

Potencjalnie niebezpieczne aplikacje nie posiadają szkodliwych funkcji, lecz mogą zostać wykorzystane jako dodatkowy składnik złośliwego kodu, ponieważ zawierają wiele luk i błędów. Kategorie ta zawiera, przykładowo: programy do zdalnej administracji, klientów IRC, usługi FTP, narzędzia do celowego zatrzymywania lub ukrywania procesów, keyloggery, autodialery itp. Programy takie nie są klasyfikowane jako wirusy. Można je podzielić na kilka kategorii: Adware, Jokes, Riskware itp. (więcej informacji o potencjalnie niebezpiecznych programach wykrywanych przez Kaspersky Anti-Virus zawiera Encyklopedia Wirusów: <http://www.viruslist.pl>). Po wykonaniu skanowania, tego typu programy

mogą zostać zablokowane. Z uwagi na to, że wiele z nich jest bardzo popularnych, dostępna jest opcja ich wykluczenia z obszaru skanowania. W tym celu należy dodać do strefy zaufanej nazwę lub maskę obiektu zgodnie z nazewnictwem stosowanym w Encyklopedii Wirusów.

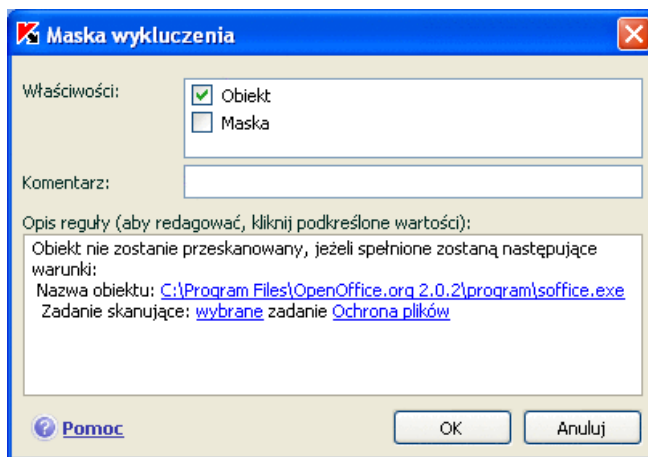
Na przykład: użytkownik w codziennej pracy używa programu Remote Administrator. Jest to narzędzie pozwalające na zdalny dostęp do innego komputera. Kaspersky Anti-Virus for Windows Servers wykrywa ten rodzaj aktywności aplikacji jako potencjalnie niebezpieczny i może go zablokować. W celu zapobiegnięcia zablokowania aplikacji przez program, należy utworzyć regułę wykluczającą i jako werdykt należy podać not-a-virus:RemoteAdmin.Win32.RAdmin.22.

Po dodaniu wykluczenia utworzona zostanie reguła, która będzie wykorzystywana przez moduł Ochrona plików oraz zadania skanowania antywirusowego. Reguły wykluczeń można tworzyć przy użyciu specjalnego okna, które dostępne jest w oknie ustawień programu, z poziomu okna powiadomienia o wykryciu obiektu i z poziomu okna raportów.

*W celu dodania wykluczenia na zakładce **Maska wykluczeń** należy:*

1. Kliknąć przycisk **Dodaj** na zakładce **Maska wykluczeń**.
2. W oknie, które zostanie otwarte (patrz rys. 9), należy wybrać typ wykluczenia w sekcji **Właściwości**:

- Obiekt** – wykluczenie ze skanowania określonego obiektu, foldera lub plików pasujących do podanych masek.
- Werdykt** – wykluczenie ze skanowania obiektów w oparciu o stan przydzielony do nich w encyklopedii wirusów.



Rysunek 9. Tworzenie reguły wykluczenia

W przypadku jednoczesnego zaznaczenia obu pól, utworzona zostanie reguła dla obiektu w oparciu o stan przydzielony do niego na podstawie nazewnictwa stosowanego w Encyklopedii Wirusów. Stosowane będą następujące reguły:

- Po określeniu pliku jako **Obiektu** oraz statusu w sekcji **Werdykt**, określony plik zostanie wykluczony wykluczeniem tylko wtedy, gdy podczas skanowania zostanie sklasyfikowany jako zdefiniowany rodzaj zagrożenia.
 - Jeżeli jako **Obiekt** wybrany zostanie obszar lub folder oraz stan (lub maska typu werdyktu) jako **Werdykt**, obiekt posiadający ten stan zostanie wykluczony ze skanowania jedynie w obrębie tego obszaru lub foldera.
3. Następnie należy przypisać wartości do wybranych typów wykluczeń. W tym celu należy kliknąć lewym przyciskiem myszy odsyłacz znajdujący się obok typu wykluczenia w sekcji **Opis reguły**:
- Dla typu **Obiekt**, należy wprowadzić nazwę obiektu w oknie, które zostanie otwarte (może nim być plik, określony katalog lub maska pliku) (patrz rozdział 1.2 na stronie 186). W celu rekursywnego wykluczenia ze skanowania obiektu (pliku, maski pliku, foldera), należy zaznaczyć opcję **Włączając podfoldery**.
 - Wprowadzić pełną nazwę zagrożenia, które ma zostać wykluczone z obszaru skanowania (zgodnie z nazewnictwem stosowanym w Encyklopedii wirusów) lub użyć maski jako werdyktu (patrz rozdział 1.3 na stronie 187).
- Dla niektórych werdyktów, w polu **Ustawienia zaawansowane**, można przypisać dodatkowe warunki reguły.
4. Zdefiniować, które składniki programu Kaspersky Anti-Virus for Windows Servers mają używać tej reguły. Jeżeli wybrano opcję dowolne, reguła zostanie zastosowana dla **wszystkich składników**. Aby ograniczyć liczbę modułów stosujących regułę, należy kliknąć odsyłacz dowolny - zostanie on zmieniony na wybrany. W oknie, które pojawi się na ekranie, należy zaznaczyć opcje dla modułów programu, które będą stosować regułę.

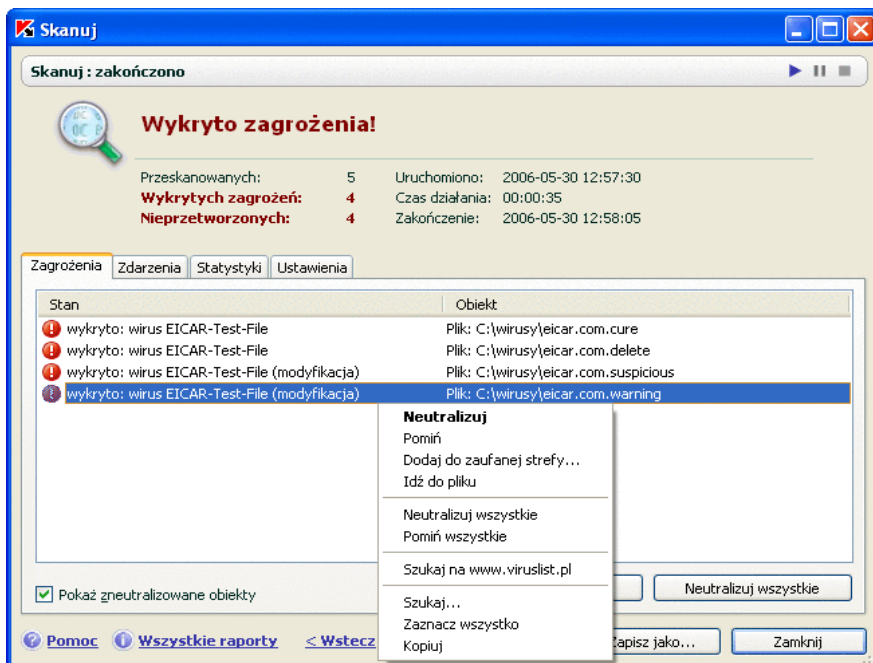
W celu utworzenia reguły wykluczenia z poziomu okna powiadomień o wykryciu niebezpiecznego obiektu należy:

1. Użyć odsyłacza Dodaj do zaufanej strefy w oknie powiadomienia.
2. W oknie które zostanie otwarte, należy upewnić się że wszystkie reguły wykluczenia są zgodne z wybranymi ustawieniami. Program automatycznie uzupełni nazwę obiektu i typ zagrożenia w oparciu o

informacje zawarte w powiadomieniu. W celu utworzenia reguły, należy kliknąć przycisk **OK**.

W celu utworzenia reguły wykluczenia z poziomu okna raportów należy:

1. Wybrać w oknie raportu obiekt, który ma zostać dodany do wykluczeń.
2. Otworzyć menu kontekstowe i wybrać opcję **Dodaj do zaufanej strefy**.



Rysunek 10. Tworzenie reguł wykluczeń z poziomu okna raportów

6.3.2. Zaufane aplikacje

Kaspersky Anti-Virus for Windows Servers umożliwia utworzenie listy zaufanych aplikacji, których aktywność plikowa (nawet podejrzana) nie będzie monitorowana.

Na przykład: użytkownik przekonany jest o bezpieczeństwie obiektów używanych przez **Notatnik** systemu Windows Server i nie ma potrzeby ich skanowania. W celu wykluczenia obiektów używanych przez ten proces z obszaru skanowania, należy dodać program **Notepad** do listy zaufanych aplikacji. Jednakże, plik wykonywalny i proces zaufanej aplikacji nadal będzie skanowany. W celu

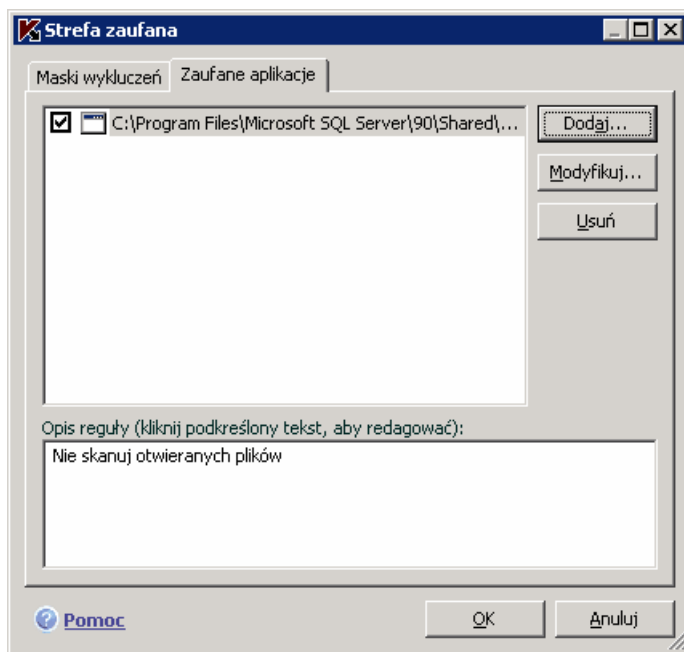
całkowitego wykluczenia aplikacji ze skanowania należy użyć reguł wykluczeń (patrz rozdział 6.3.1 na stronie 56).

Ponadto, niektóre działania klasyfikowane jako niebezpieczne są działaniami standardowymi dla wielu programów. Na przykład: programy przełączające układ klawiatury regularnie przechwytyją tekst wprowadzany na klawiaturze. W celu przerwania monitorowania aktywności tego typu programów, zalecane jest dodanie ich do listy zaufanych aplikacji.

Przy użyciu wykluczeń dla zaufanych aplikacji można również rozwiązać potencjalne problemy związane ze zgodnością pomiędzy programem Kaspersky Anti-Virus for Windows Servers i innymi aplikacjami (na przykład: ruch sieciowy z innego komputera, który został już przeskanowany przez aplikację antywirusową) i może zwiększyć wydajność pracy komputera, co jest szczególnie ważne podczas używania aplikacji serwerowych.

Domyślnie, Kaspersky Anti-Virus for Windows Servers skanuje obiekty otwierane, uruchamiane lub zapisywane przez proces dowolnego programu.

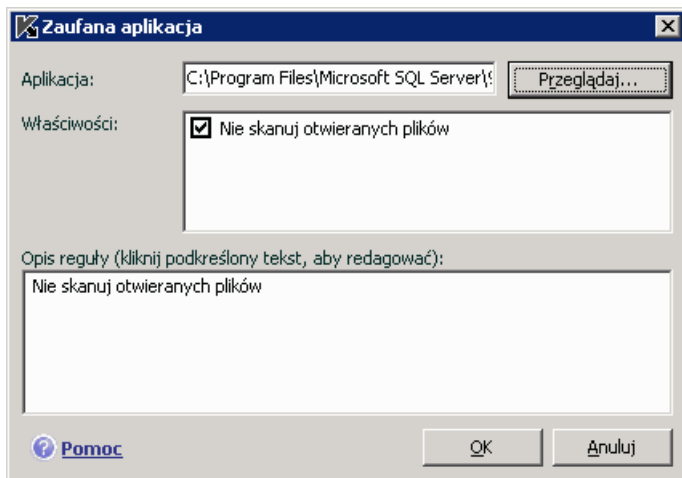
Możliwe jest utworzenie listy zaufanych aplikacji na specjalnej zakładce **Zaufane aplikacje** (patrz Rysunek 11). Domyślnie lista zawiera aplikacje, które zgodnie z zaleceniami ekspertów z firmy Kaspersky Lab nie powinny być monitorowane. Jeżeli znajdujące się na liście aplikacje mają być skanowane, należy odznaczyć znajdujące się przy nich pola. Można dodawać i modyfikować elementy listy przy użyciu przycisków **Dodaj**, **Modyfikuj** i **Usuń**.



Rysunek 11. Lista zaufanych aplikacji

W celu dodania programu do listy zaufanych aplikacji należy:

1. Kliknąć przycisk **Dodaj** znajdujący się w prawej części okna.
2. W oknie **Zaufane aplikacje** (patrz rys. 12), należy wybrać aplikację przy pomocy przycisku **Przełączaj**. Otwarte zostanie menu kontekstowe, w którym należy kliknąć przycisk **Przełączaj** w celu wybrania ścieżki dostępu do pliku wykonywalnego lub przycisk **Aplikacje** w celu wyświetlenia listy uruchomionych aplikacji i wybrania żądanych aplikacji.



Rysunek 12. Dodawanie aplikacji do listy zaufanych aplikacji

Po wybraniu aplikacji, Kaspersky Anti-Virus for Windows Servers zapamięta wewnętrzne atrybuty pliku wykonywalnego i używał ich będzie do identyfikowania programu jako zaufanego, podczas skanowania.

Ścieżka dostępu do pliku uzupełniania jest automatycznie po wybraniu jego nazwy.

3. Określić działania wykonywane przez ten proces, które nie będą monitorowane przez Kaspersky Anti-Virus:

- Nie skanuj otwieranych plików** – wykluczenie z obszaru skanowania wszystkich plików które otwierane są przez proces zaufanej aplikacji.

6.4. Uruchamianie zadań skanowania przy użyciu profilu innego użytkownika

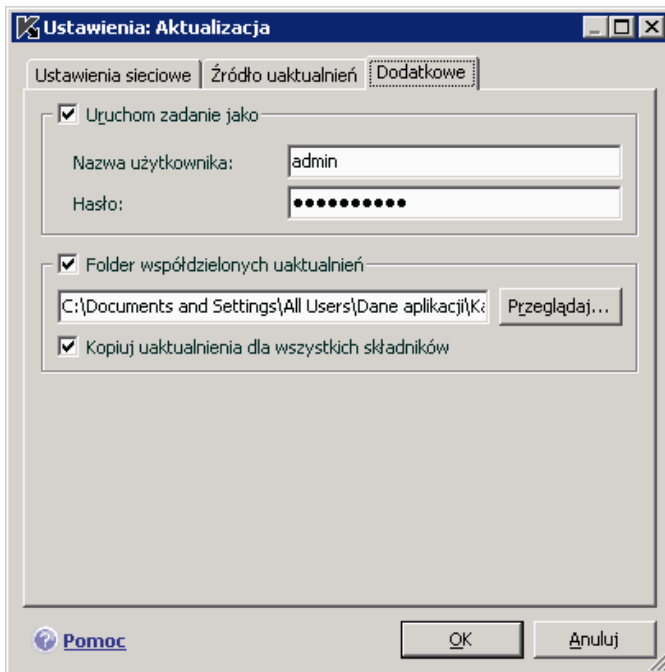
Kaspersky Anti-Virus for Windows Servers 6.0 posiada funkcję uruchamiania zadań za pośrednictwem konta innego użytkownika. Funkcja ta jest domyślnie wyłączona i zadania uruchamiane są z poziomu konta na które zalogował się użytkownik.

Na przykład, może okazać się niezbędne uzyskanie dostępu do określonego obiektu podczas skanowania. Przy użyciu tej funkcji, można skonfigurować uruchamianie zadań przez za pomocą profili użytkowników posiadających odpowiednie uprawnienia.

Aktualizacje programu mogą być wykonywane ze źródła, do którego użytkownik nie posiada dostępu (na przykład: folder sieciowy) lub z serwera proxy dostępnego dla autoryzowanych użytkowników. Można użyć tej funkcji w celu uruchamiania procesu aktualizacji z poziomu konta innego użytkownika posiadającego odpowiednie uprawnienia.

W celu skonfigurowania zadania skanowania do uruchamiania za pośrednictwem wskazanego konta należy:

1. Wybrać nazwę zadania w sekcji Skanuj (skanowanie antywirusowe) lub w sekcji **Usługi** (zadania aktualizacji i współdzielenia uaktualnień) znajdującej się w oknie głównym programu i użyć odsyłacza Ustawienia w celu otwarcia okna ustawień zadania.
2. Kliknąć przycisk **Ustawienia** znajdujący się w oknie ustawień zadania i przejść na zakładkę **Zaawansowane** w oknie, które zostanie otwarte (patrz rys. 13).
3. W celu włączenia tej funkcji, należy zaznaczyć opcję **Uruchom zadanie jako**. Następnie należy podać informacje wymagane do zalogowania (nazwę użytkownika i hasło).



Rysunek 13. Konfiguracja uruchamiania zadania aktualizacji za pośrednictwem konta innego użytkownika

6.5. Konfiguracja terminarza zadania

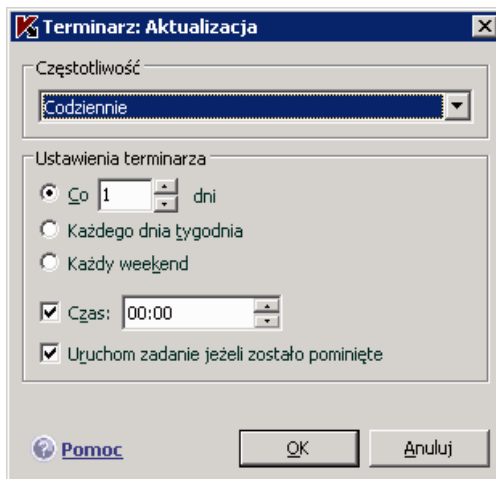
Możliwe jest ręczne lub automatyczne (przy użyciu terminarza) uruchomienie skanowania antywirusowego, aktualizacji oraz zadań współdzielenia aktualizacji.

Preinstalowane zadania skanowania antywirusowego oraz aktualizacji uruchamiane są automatycznie zgodnie z terminarzem. Wyjątkiem jest skanowanie obiektów startowych, które uruchamiane jest podczas każdego uruchamiania komputera. Zadania aktualizacji domyślnie uruchamiane są co dwie godziny.

Aby zmodyfikować ustawienia terminarza, w głównym oknie programu w sekcji **Skanuj** (skanowanie na obecność wirusów) lub sekcji **Usługi** (zadania aktualizacji i współdzielenia uaktualnień) należy wybrać nazwę zadania oraz otworzyć okno ustawień przez kliknięcie przycisku Ustawienia.

W celu uruchamiania zadań zgodnie z terminarzem, należy wybrać automatyczne uruchamianie zadań w sekcji **Tryb uruchamiania**. W oknie

Terminarz (patrz Rysunek 14), które zostanie otwarte po kliknięciu przycisku **Zmień** można modyfikować ustawienia uruchamiania zadania skanowania.



Rysunek 14. Konfiguracja terminarza zadań

Najważniejszym elementem jest zdefiniowanie częstotliwości uruchamiania zadania. Można wybrać jedną z następujących opcji:

- O określonym czasie.** Zadanie uruchamiane będzie raz dziennie o określonym czasie.
- Podczas uruchamiania programu.** Zadanie będzie uruchamiane wraz z każdym uruchomieniem programu Kaspersky Anti-Virus.
- Uruchom po każdej aktualizacji.** Zadanie będzie uruchamiane po wykonaniu każdej aktualizacji sygnatur zagrożeń (ta opcja dotyczy wyłącznie zadań skanowania antywirusowego).
- Co N minut.** Przedział czasu pomiędzy kolejnymi skanowaniami jest określony w minutach. Nie może on przekroczyć 59 minut. W ustawieniach terminarza należy określić liczbę minut pomiędzy uruchamianiem zadań skanowania.
- Co N godzin.** Zadanie uruchamiane będzie z odstępstwem określonej liczby godzin. W ustawieniach terminarza należy określić liczbę godzin: Co N godzin i wybrać wartość dla N. Na przykład, Co 1 godzinę w celu uruchamiania zadania co godzinę.
- Codziennie** – okres pomiędzy skanowaniami jest wyrażony liczbą dni. W ustawieniach terminarza należy określić częstotliwość uruchamiania zadania:

Wybrać **Co N dni** i określić wartość dla n. Należy wprowadzić Co 2 dni, aby skanowanie było uruchamiane co 2 dni.

Należy wybrać **Każdy dzień tygodnia**, aby skanowanie wykonywane było codziennie od poniedziałku do piątku.

Należy wybrać **Każdy weekend**, aby skanowanie wykonywane było tylko w **soboty i niedziele**.

Poza częstotliwością, należy określić porę dnia (dzień lub noc) uruchamiania zadania w polu **Czas**.

- ☛ **Co tydzień** – zadanie skanowania będzie uruchamiane w określone dni tygodnia. Po wybraniu tej opcji należy wybrać dni, w które uruchamiane będzie zadanie. Dodatkowo, polu Czas należy wprowadzić czas uruchamiania zadania skanowania.
- ☛ **Co N miesięcy** – zadanie skanowania uruchamiane będzie raz w miesiącu, w określonym dniu i czasie.

Jeżeli zadanie skanowania zostanie pominięte (na przykład: komputer był wyłączony), można skonfigurować automatyczne uruchamianie pominiętego zadania, gdy tylko będzie to możliwe. W tym celu należy w oknie terminarza zaznaczyć pole **Uruchom zadanie jeżeli zostało pominięte**.

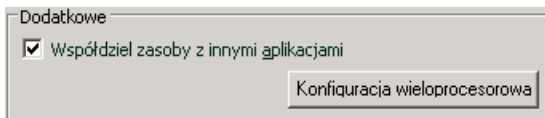
6.6. Opcje wydajności

Skanowanie antywirusowe powoduje obciążenie głównego procesora i podsystemów dyskowych, spowalniając pracę innych programów. Domyślnie, w przypadku zaistnienia takiej sytuacji, program wstrzyma zadania skanowania antywirusowego i zwolni zasoby systemowe dla aplikacji użytkownika.

Jednak, istnieje wiele programów, które mogą zostać uruchomione po zwolnieniu zasobów procesora i pracować w tle. Aby skanowanie antywirusowe nie było zależne od działania takich programów, należy usunąć zaznaczenie z pola **Współdziel zasoby z innymi**.

Należy pamiętać o tym, że ustawienie to może być konfigurowane indywidualnie dla każdego zadania skanowania antywirusowego. W przypadku wybrania tej opcji, konfiguracja dla specyficznego zadania będzie posiadała wyższy priorytet.

Po kliknięciu przycisku **Konfiguracja wieloprocessorowa...** zostanie otwarte okno, w którym można skonfigurować ustawienia działania programu Kaspersky Anti-Virus na serwerze wieloprocessorowym (patrz rozdział 6.7 na stronie 67).



Rysunek 15. Konfiguracja wydajności serwera

W celu konfiguracji ustawień wydajności:

W głównym oknie programu przejść do sekcji **Ochrona** i kliknąć Ustawienia. Skonfigurować ustawienia wydajności w sekcji **Dodatkowe**.

6.7. Konfiguracja serwera wieloprotocessorowego

W tym oknie można skonfigurować ustawienia wydajności serwera w przypadku używania konfiguracji wieloprotocessorowej.

Liczba instancji silnika antywirusowego – liczba kopii silnika antywirusowego, która ma być uruchomiona podczas działania programu Kaspersky Anti-Virus na serwerze. Liczba ta określa ilość równoległe uruchomionych procesów antywirusowych.

Kilka uruchomionych kopii silnika antywirusowego oznacza szybsze działanie i wykonywanie funkcji antywirusowych. To ustawienie wpływa na ogólną wydajność serwera.

Dodatkowo jednoczesne uruchomienie kilku procesów antywirusowych na serwerze zapewnia ciągłą ochronę w przypadku wystąpienia błędów jednego z silników.


W celu automatycznego rozdzielenia procesów antywirusowych między procesorami należy zaznaczyć pole **Do zarządzania procesami równoległymi użyj specjalnego sterownika**.

Jeżeli pole to nie jest zaznaczone, można ręcznie regulować obciążenie serwera, na przykład zarezerwować część procesorów dla przetwarzania antywirusowego, a część dla bezpośrednich zadań serwera. W tym celu należy w polu **Wykorzystane procesory** usunąć zaznaczenie z procesorów przeznaczonych dla bieżących zadań serwera.

W przypadku uruchomienia programu na serwerze wieloprotocessorowym, eksperci z firmy Kaspersky Lab zalecają pozostawienia przynajmniej jednego procesora dla bieżących zadań serwera.

ROZDZIAŁ 7. OCHRONA ANTYWIRUSOWA SYSTEMU PLIKÓW SERWERA

Kaspersky Anti-Virus zawiera moduł *Ochrona plików*, który chroni system plików serwera przed infekcją. Uruchamiany jest on wraz ze startem systemu operacyjnego i rezyduje w pamięci RAM komputera. Skanuje on wszystkie pliki otwierane, zapisywane lub uruchamiane.

Wskaźnikiem funkcjonowania tego składnika jest ikona programu Kaspersky Anti-Virus for Windows Servers znajdująca się w zasobniku systemowym, przedstawiająca skanowanie plików w następujący sposób .

Moduł ochrony plików domyślnie *skanuje tylko nowe lub zmodyfikowane pliki*. Innymi słowy, skanuje on pliki, które zostały dodane lub zmienione od czasu poprzedniego skanowania. Pliki skanowane są za pomocą następujących algorytmów:

1. Moduł przechwytuje próby dostępu do plików wykonywane przez użytkowników lub programy.
2. Moduł ochrony plików skanuje bazy danych iChecker™ oraz iSwift™ w celu uzyskania informacji o przechwyconych plikach. Na podstawie tych informacji podejmowana jest decyzja o potrzebie skanowania obiektu.

Proces skanowania obejmuje następujące etapy:

1. Wykonywana jest analiza pliku w poszukiwaniu wirusów. Szkodliwe obiekty wykrywane są w oparciu o porównywanie z sygnaturami zagrożeń używanymi przez program. Sygnatury zawierają opis wszystkich znanych szkodliwych programów, zagrożeń i ataków sieciowych oraz metody ich neutralizowania.
2. Po zakończeniu analizy możliwe są następujące akcje:
 - a. Jeżeli w pliku wykryty zostanie szkodliwy kod, moduł **Ochrona plików** zablokuje dostęp do pliku, umieści jego kopię w folderze *Kopii zapasowej* i podejmie próbę jego wyleczenia. Jeżeli plik zostanie pomyślnie wyleczony, stanie się on dostępny dla użytkownika. Jeżeli leczenie nie będzie możliwe, plik zostanie usunięty.

- b. Jeżeli w pliku wykryty zostanie kod, który może być szkodliwy lecz nie ma na to 100% pewności, plik zostanie umieszczony w *Kwarantannie*.
- c. Jeżeli w pliku nie zostanie wykryty szkodliwy kod, zostanie on natychmiast przywrócony.

7.1. Wybór poziomu ochrony

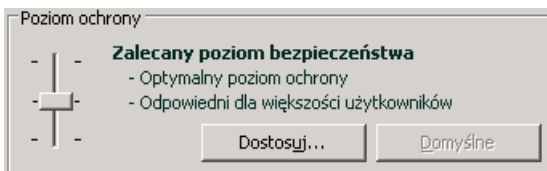
Moduł Ochrona plików chroni pliki używane przez użytkownika na jednym z następujących poziomów bezpieczeństwa (patrz rys. 16):

Wysoki – poziom zapewniający najbardziej szczegółowe monitorowanie otwieranych, zapisywanych i uruchamianych plików.

Zalecany – poziom ochrony zalecany przez ekspertów z firmy Kaspersky Lab. Obejmuje on skanowanie następujących kategorii obiektów:

- programy i pliki według zawartości
- tylko nowe obiekty i obiekty zmodyfikowane od czasu ostatniego skanowania
- osadzone obiekty OLE

Niski – poziom zapewniający minimalne obciążenie systemu kosztem wykluczenia pewnych obiektów z obszaru skanowania.



Rysunek 16. Poziom bezpieczeństwa modułu **Ochrona plików**

Domyślnie, poziom bezpieczeństwa dla plików ustawiony jest na **Zalecany**.

Można zwiększyć lub zmniejszyć poziom bezpieczeństwa plików przez wybranie żądanego poziomu lub zmianę ustawień bieżącego.

W celu zmiany poziomu ochrony należy:

Wybrać poziom przy użyciu suwaka. Dostosowując poziom ochrony, użytkownik definiuje współczynnik prędkości skanowania plików (im mniej typów plików jest skanowanych tym większa jest prędkość skanowania).

Jeżeli żaden z dostępnych poziomów ochrony nie spełnia wymagań użytkownika, należy zmodyfikować ustawienia ochrony. W tym celu, jako punkt początkowy, należy wybrać poziom ochrony zbliżony do wymagań użytkownika i dokonać modyfikacji jego ustawień. W tym przypadku, poziom ochrony zostanie ustawiony na **Ustawienia niestandardowe**. Poniżej znajduje się przykład definiowania poziomu ochrony.

Przykład:

Użytkownik wykonuje na komputerze pracę wymagającą korzystania z dużej liczby typów plików, często o dość dużym rozmiarze. Aby podczas skanowania nie doszło do pominięcia jakichkolwiek plików ze względu na ich rozmiar lub rozszerzenie, nawet jeżeli może to wpłynąć na wydajność komputera.

Wskazówka:

W oparciu o dane źródłowe, istnieje duże ryzyko zainfekowania szkodliwym programem. Rozmiar i typ przetwarzanych plików jest dość zróżnicowany i pominięcie ich podczas skanowania może stanowić ryzyko dla danych. Użytkownik chce skanować używane pliki według zawartości, a nie rozszerzenia.

Zalecane jest rozpoczęcie pracy z **Zalecanym poziomem bezpieczeństwa** i dokonanie następujących zmian: usunięcie ograniczenia skanowania plików o określonym rozmiarze i zoptymalizowanie operacji wykonywanych przez moduł **Ochrona plików** poprzez skanowanie tylko nowych i zmodyfikowanych plików. W tym przypadku, zmniejszone zostanie zużycie zasobów podczas skanowania i możliwa będzie wygodna praca z innymi aplikacjami.

W celu modyfikacji ustawień poziomu bezpieczeństwa należy:

Kliknąć odsyłacz **Ustawienia** w oknie ustawień modułu **Ochrona plików**. Dokonać modyfikacji ustawień modułu ochrony plików w oknie, które zostanie otwarte i kliknąć przycisk **OK**.

Po zmodyfikowaniu parametrów poziom bezpieczeństwa antywirusowego zostanie zmieniony na **Ustawienia niestandardowe**. Jest to czwarty poziom bezpieczeństwa wykorzystujący ustawienia zdefiniowane przez użytkownika.

7.2. Ustawienia ochrony systemu plików

Ustawienia określają w jaki sposób moduł Ochrona plików będzie chronił komputer. Ustawienia można podzielić na następujące grupy:

Ustawienia związane z definiowaniem typów plików (patrz rozdział 7.2.1 na stronie 71), które będą skanowane w poszukiwaniu wirusów.

Ustawienia związane z definiowaniem obszaru ochrony (patrz rozdział 7.2.2 na stronie 74).

Ustawienia związane z akcjami podejmowanymi przez program po wykryciu niebezpiecznych obiektów (patrz rozdział 7.2.5 na stronie 79).

Dodatkowe ustawienia modułu Ochrona plików (patrz rozdział 7.2.3 na stronie 75).

W następnych sekcjach tego podręcznika przedstawione zostaną szczegółowe informacje dotyczące tych grup.

7.2.1. Definiowanie typów skanowanych plików

Podczas wyboru typów skanowanych plików, określone są formaty plików, rozmiar oraz napędy które będą skanowane w poszukiwaniu wirusów podczas otwierania, wykonywania lub zapisywania.

W celu uproszczenia konfiguracji, wszystkie pliki podzielone zostały na dwie grupy: *proste* i *złożone*. Proste pliki nie zawierają żadnych obiektów (na przykład: pliki .txt). Obiekty złożone mogą zawierać wiele obiektów, natomiast każdy z nich może zawierać również wiele zagnieżdżonych poziomów. Dostępnych jest wiele przykładów: archiwa, pliki zawierające makra, arkusze kalkulacyjne, wiadomości elektroniczne zawierające załączniki itp.

Typy skanowanych plików zdefiniowane są w sekcji **Typy plików** (patrz Rysunek 17). Należy wybrać jedną z trzech opcji:

- ☛ **Skanuj wszystkie pliki.** Po wybraniu tej opcji skanowane będą wszystkie otwierane, uruchamiane lub zapisywane obiekty systemu plików.
- ☛ **Programy i dokumenty (według zawartości).** Po wybraniu tej grupy plików, moduł ochrony plików skanował będzie jedynie potencjalnie infekowalne pliki - pliki, które mogą zostać zainfekowane przez wirusy.

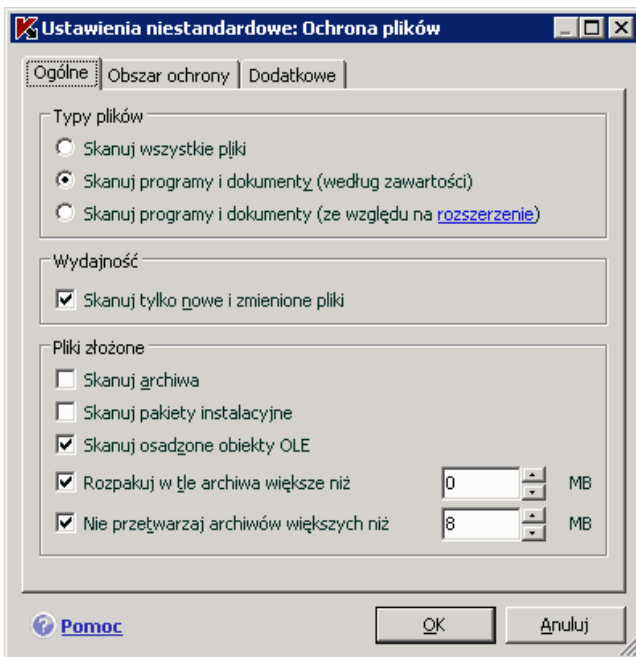
Informacja:

Istnieją formaty plików, do których wirusy nie mogą dodać swojego kodu i aktywować go. Przykładem takich plików są pliki .txt.

Istnieją również formaty plików, które mogą zawierać kod wykonywalny. Przykładowymi formatami plików są .exe, .dll lub .doc. Ryzyko umieszczenia w nich szkodliwego kodu jest bardzo wysokie.

Przed rozpoczęciem skanowania antywirusowego pliku, analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu pliku (txt, doc, exe itd.). Jeżeli analiza wykaże że format pliku nie jest infekowalny, plik ten nie zostanie przeskanowany stanie się natychmiast dostępny dla użytkownika. Jeżeli format pliku jest infekowalny, plik zostanie przeskanowany na obecność wirusów.

- **Skanuj programy i dokumenty (według rozszerzenia).** Po wybraniu tej opcji, moduł Ochrona plików skanował będzie jedynie potencjalnie zainfekowane pliki, natomiast format pliku określany będzie według rozszerzenia. Przy użyciu odsyłacza rozszerzenia, można wyświetlić listę rozszerzeń skanowanych plików (patrz rozdział 1.1 na stronie 184).



Rysunek 17. Wybór typów skanowanych plików

Informacja:

Należy mieć na uwadze, że wirus może zostać przesłany do komputera w pliku o rozszerzeniu .txt, który w rzeczywistości jest plikiem wykonywalnym o zmienionej nazwie i rozszerzeniu. Po wybraniu opcji **Programy i dokumenty (według rozszerzenia)** tego typu plik zostanie pominięty podczas skanowania. Jeżeli wybrana została opcja **Programy i dokumenty (według zawartości)** ignorująca rozszerzenia, program analizował będzie nagłówki plików i wykryje, że plik jest wykonywalny (.exe). Plik może zostać całkowicie przeskanowany w poszukiwaniu wirusów.

W sekcji **Wydajność** można zdefiniować skanowanie tylko nowych plików oraz zmodyfikowanych od czasu ostatniego skanowania. Ten tryb wyraźnie redukuje czas skanowania i powoduje zwiększenie wydajności programu. Aby wybrać ten tryb należy zaznaczyć opcję **Skanuj tylko nowe i zmienione pliki**. Tryb będzie stosowany zarówno dla prostych jak i złożonych plików.

W sekcji **Pliki złożone** należy wybrać typy skanowanych plików złożonych:

- Skanuj wszystkie/tylko nowe archiwa** – skanowanie archiwów .zip, .cab, .rar oraz .arj, włączając archiwa zabezpieczone hasłem.
- Skanuj wszystkie/tylko nowe pakiety instalacyjne** – skanowanie archiwów samorozpakowujących.
- Skanuj wszystkie/tylko nowe osadzone obiekty OLE** – skanowanie obiektów osadzonych w plikach (na przykład: arkusz kalkulacyjny programu Excel lub makro osadzone w pliku programu MS Word, załączniki wiadomości pocztowych itp.).

Można wybrać skanowanie wszystkich plików lub tylko nowych plików dla każdego typu złożonego pliku. W tym celu, należy użyć odsyłacza znajdującego się obok nazwy obiektu. Jeżeli w sekcji **Wydajność** zdefiniowano skanowanie tylko nowych i zmodyfikowanych plików, nie będzie możliwe wybranie typu skanowanych plików złożonych.

W celu określenia plików złożonych, które będą skanowane w poszukiwaniu wirusów należy użyć następujących ustawień:

- Rozpakuj w tle archiwa większe niż ... MB**. Jeżeli rozmiar obiektu złożonego przekroczy to ograniczenie, program przeskanuje go jako pojedynczy obiekt (poprzez analizę jego nagłówka) i udostępni użytkownikowi. Obiekty zawarte w tym pliku zostaną przeskanowane później. Jeżeli nie wybrano tej opcji, dostęp do plików większych niż wskazany rozmiar będzie blokowany do czasu ich przeskanowania.
- Nie przetwarzaj archiwów większych niż... MB**. Po wybraniu tej opcji program nie będzie skanował plików o rozmiarze większym od zdefiniowanego.

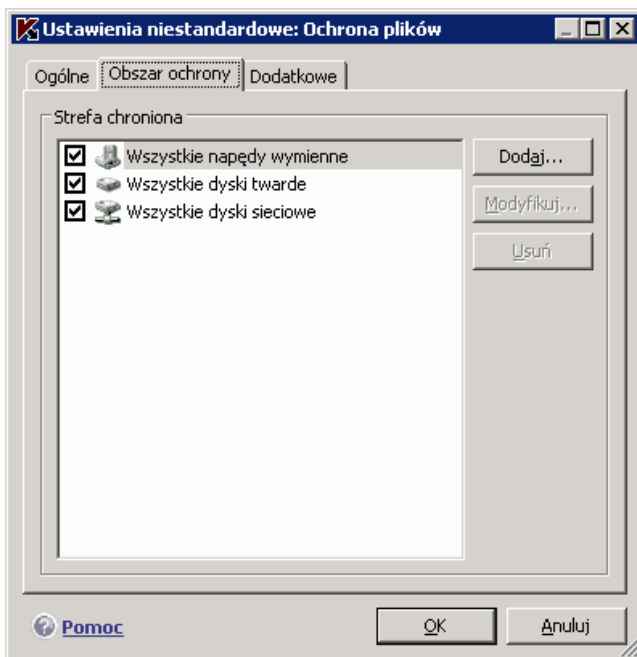
7.2.2. Definiowanie obszaru ochrony

Moduł Ochrona plików domyślnie skanuje wszystkie używane pliki, niezależnie od ich lokalizacji (dysk twardy, CD-ROM lub pamięć flash).

Można ograniczyć obszar skanowania. W tym celu należy:

1. W oknie głównym programu wybrać moduł **Ochrona plików** i przejść do okna ustawień klikając odsyłacz Ustawienia.
2. Kliknąć przycisk Ustawienia, a następnie w oknie, które zostanie otwarte przełączyć się do zakładki **Obszar ochrony** (patrz rys. 18).

Na zakładce wyświetlona jest lista obiektów, które będą skanowane przez moduł Ochrona plików. Domyślnie ochrona jest włączona dla wszystkich obiektów zapisanych na dyskach twardych, nośnikach wymiennych oraz dyskach sieciowych podłączonych do komputera. Można modyfikować zawartość listy przy użyciu przycisków **Dodaj**, **Modyfikuj** i **Usuń**.



Rysunek 18. Tworzenie strefy zaufanej

Aby zredukować liczbę chronionych obiektów, można skorzystać z jednej z następujących metod:

Określić foldery, dyski twarde i pliki, które wymagają ochrony.

Utworzyć listę obiektów, które nie muszą być chronione.

Połączyć dwie powyższe metody - zdefiniować chroniony obszar z wykluczeniem pewnych obiektów.

W przypadku dodawania obiektów do skanowania możliwe jest używanie masek. Należy pamiętać, że można wprowadzać tylko maski z bezwzględnymi ścieżkami dostępu do obiektów:

C:\dir* lub **C:\dir*** lub **C:\dir** - wszystkie pliki w folderze C:\dir\

C:\dir*.exe – wszystkie pliki posiadające rozszerzenie .exe znajdujące się w folderze C:\dir\

C:\dir*.ex? – wszystkie pliki posiadające rozszerzenie .ex? znajdujące się w folderze C:\dir\, gdzie ? może być dowolnym znakiem

C:\dir\test – tylko plik C:\dir\test

W celu rekursywnego skanowania wszystkich podrzędnych obiektów należy zaznaczyć opcję **Włączając podfoldery**.

Ostrzeżenie!

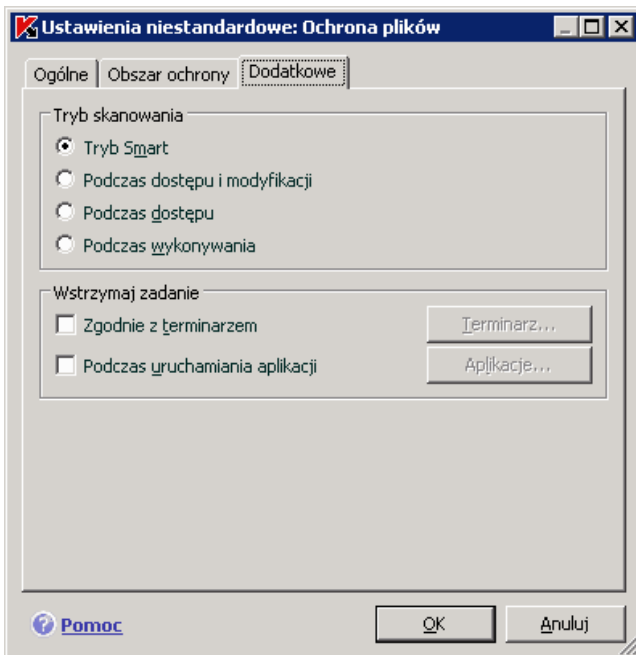
Należy pamiętać, że moduł Ochrona plików skanował będzie jedynie pliki znajdujące się w utworzonym obszarze ochrony. Pliki niewchodzące w skład obszaru ochrony nie będą skanowane. Zwiększa to ryzyko zainfekowania komputera.

7.2.3. Konfiguracja ustawień zaawansowanych

W sekcji ustawień dodatkowych modułu Ochrona plików można skonfigurować tryb skanowania oraz opcje tymczasowego wstrzymywania składnika ochrony.

W celu skonfigurowania dodatkowych ustawień ochrony plików należy:

1. Wybrać sekcję **Ochrona plików** w oknie głównym programu i przejść do okna ustawień składnika poprzez kliknięcie odsyłacza [Ustawienia](#).
2. Kliknąć przycisk **Dostosuj** i przejść do zakładki **Dodatkowe** w oknie, które zostanie wyświetlone (patrz Rysunek 19).



Rysunek 19. Konfiguracja zaawansowanych ustawień modułu Ochrona plików

Tryb skanowania określa sposób przetwarzania plików przez moduł Ochrony plików. Dostępne są następujące opcje:

Tryb Smart. Tryb ten ma na celu przyspieszenie przetwarzania i przekazywania obiektów użytkownikowi. W tym trybie działania, program podejmuje decyzję o jego skanowaniu w oparciu o analizę akcji wykonywanych na pliku.

Na przykład, podczas korzystania z pliku programu Microsoft Office, Kaspersky Anti-Virus skanuje ten plik tylko podczas jego otwarcia i zamknięcia. Wszystkie operacje odbywające się pomiędzy tymi czynnościami są pomijane podczas skanowania.

Tryb Smart jest domyślnie włączony.

Podczas dostępu i modyfikacji – moduł Ochrona plików skanuje pliki podczas ich otwierania lub modyfikacji.

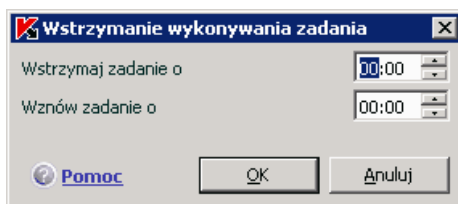
Podczas dostępu – pliki skanowane są wyłącznie podczas ich otwierania.

Podczas modyfikacji – pliki skanowane są wyłącznie podczas próby zapisania ich zmodyfikowanej zawartości.

Podczas wykonywania – pliki skanowane są wyłącznie podczas próby ich uruchomienia.

Podczas wykonywania zadań, które wymagają dużej ilości zasobów systemowych, możliwe jest wstrzymanie działania modułu Ochrona plików. W celu zmniejszenia obciążenia i zagwarantowania, że użytkownik uzyska szybszy dostęp do plików, zaleca się skonfigurowanie składnika w celu jego wyłączenia na pewien okres czasu lub gdy uruchomione są pewne programy.

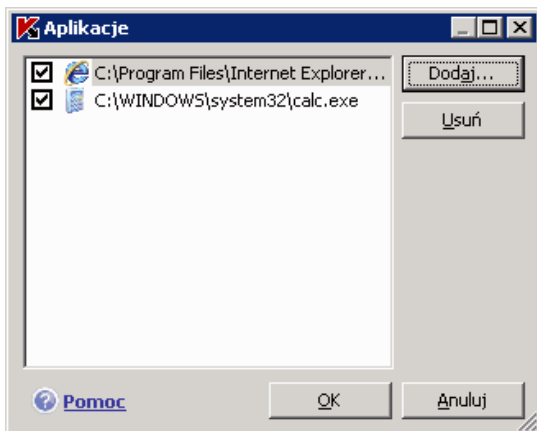
W celu wstrzymania działania składnika na określony czas należy zaznaczyć opcję **Zgodnie z terminarzem** i w oknie (patrz rys. 19), które zostanie otwarte kliknąć **Terminarz**, w celu zdefiniowania przedziału czasu dla wyłączenia i wstrzymania składnika. Aby to zrobić należy w odpowiednich polach wprowadzić wartość w formacie HH:MM.



Rysunek 20. Konfiguracja terminarza wstrzymania działania składnika

W celu wyłączenia działania składnika podczas pracy z programami wymagającymi większej ilości zasobów systemowych, należy zaznaczyć opcję **Podczas uruchamiania aplikacji** i zmodyfikować listę aplikacji znajdującą się w oknie (patrz Rysunek 21), które zostanie wyświetlone po kliknięciu przycisku **Aplikacje**.

W celu dodania aplikacji do listy należy kliknąć przycisk **Dodaj**. Zostanie otwarte menu kontekstowe, a przy użyciu przycisku **Przeglądaj** można otworzyć standardowe okno wyboru plików w celu wskazania pliku wykonywalnego aplikacji. Można również wyświetlić listę obecnie uruchomionych aplikacji i przy użyciu polecenia **Aplikacje** i wskazać żądaną aplikację.



Rysunek 21. Tworzenie listy aplikacji

Aby usunąć aplikację z listy należy wybrać ją z listy i kliknąć przycisk **Usuń**.

Można tymczasowo wstrzymać skanowanie antywirusowe wykonywane przez moduł ochrony plików w czasie korzystania z określonej aplikacji. Aby to zrobić należy usunąć zaznaczenie z pola znajdującego się przy nazwie aplikacji. Nie ma konieczności usuwania go z listy.

7.2.4. Przywracanie domyślnych ustawień modułu Ochrona plików

Podczas konfigurowania modułu Ochrona plików, można zawsze powrócić do ustawień zalecanych. Według ekspertów z firmy Kaspersky Lab są one optymalne i połączone w **Zalecany poziom bezpieczeństwa**.

W celu przywrócenia domyślnych ustawień modułu Ochrona plików należy:

1. W oknie głównym programu wybrać moduł **Ochrona plików** i przejść do okna ustawień klikając odsyłacz Ustawienia.
2. W sekcji **Poziom ochrony** wybrać opcję **Domyślny**.

Jeżeli podczas konfigurowania ustawień ochrony plików zmodyfikowano listę obiektów objętych ochroną, program zapyta, czy zapisać tę listę do przyszłego użytku (może to być przydatne po przywróceniu ustawień domyślnych). W celu zapisania listy obiektów należy zaznaczyć **Zakres ochrony** w oknie **Przywróć ustawienia**, które zostanie wyświetlone na ekranie.

7.2.5. Wybór akcji dla obiektów

Jeżeli moduł ochrony plików wykryje infekcję lub prawdopodobieństwo infekcji podczas skanowania antywirusowego pliku, dalsze postępowanie programu zależy od stanu obiektu i wybranych działań.

Moduł Ochrona plików może nadać obiektowi etykietę jednego z następujących stanów:

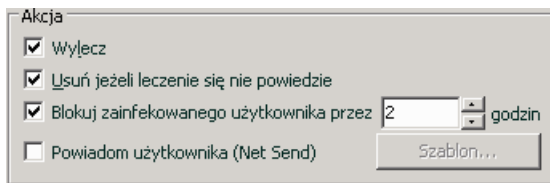
Szkodliwy program (na przykład: wirus, trojan).

Potencjalnie zainfekowany, jeżeli podczas skanowania nie można jednoznacznie stwierdzić czy obiekt jest zainfekowany. Oznacza to, że program wykrył w pliku sekwencję kodu nieznanego wirusa lub zmodyfikowany kod znanego wirusa.

Domyślnie, wszystkie zainfekowane pliki są przedmiotem leczenia i jeżeli są potencjalnie zainfekowane umieszczane są w kwarantannie.

W celu modyfikacji akcji podejmowanej na obiekcie należy:

W oknie głównym programu wybrać moduł **Ochrona plików** i przejść do okna ustawień klikając odsyłacz Ustawienia. Wszystkie potencjalne akcje wyświetlane są w odpowiednich sekcjach (patrz rys. 22).



Rysunek 22. Akcje, które mogą zostać podjęte przez moduł Ochrona plików na niebezpiecznych obiektach

Wybrana akcja	Operacje wykonywane przez program
<input checked="" type="checkbox"/> Wylecz <input type="checkbox"/> Usuń jeżeli leczenie się nie powiedzie	Dostęp do obiektu zostanie zablokowany i program podejmie próbę jego wyleczenia. Kopia obiektu zostanie zapisana w folderze kopii zapasowej. Po pomyślnym wyleczeniu obiektu, zostanie on przywrócony do użytku. Jeżeli obiekt nie będzie mógł zostać wyleczony, zostanie on przeniesiony do kwarantanny. Informacje o tym

Wybrana akcja	Operacje wykonywane przez program
	zdarzeniu zostaną zapisane w raporcie. Próbę wyleczenia obiektu będzie można wykonać później.
<input checked="" type="checkbox"/> Wylecz <input checked="" type="checkbox"/> Usuń jeżeli leczenie się nie powiedzie	Dostęp do obiektu zostanie zablokowany i program podejmie próbę jego wyleczenia. Kopia obiektu zostanie zapisana w folderze kopii zapasowej. Po pomyślnym wyleczeniu obiektu, zostanie on przywrócony do użytku. Jeżeli nie można wyleczyć obiektu, zostanie on usunięty.
<input type="checkbox"/> Wylecz <input checked="" type="checkbox"/> Usuń	Moduł Ochrona plików zablokuje dostęp do obiektu i usunie go.
<input checked="" type="checkbox"/> Zablokuj zainfekowanego użytkownika przez ... godzin	<p>Zablokowany zostanie dostęp do serwera lub komputera, z którego wystąpiła próba skopiowania zainfekowanego lub potencjalnie zainfekowanego obiektu.</p> <p>To działanie może być dodatkowo stosowane dla akcji związanych z przetwarzaniem pliku (leczenie lub usuwanie).</p> <p>Należy pamiętać o tym, że w przypadku gdy użytkownik ma już otwartą sesję i zaloguje się do systemu ponownie, Kaspersky Anti-Virus będzie traktował to jako inne połączenie i nie będzie go blokował.</p>
<input checked="" type="checkbox"/> Powiadom użytkownika (Net Send)	<p>Powiadamia użytkownika komputera, z którego próbowano skopiować zainfekowane lub potencjalnie zainfekowane pliki na serwer. Powiadomienie wysyłane jest przy użyciu Net Send.</p> <p>W celu skonfigurowania szablonu powiadomienia należy kliknąć przycisk</p>

Wybrana akcja	Operacje wykonywane przez program
	Szablon.

Przed podjęciem próby leczenia lub usunięcia obiektu, Kaspersky Anti-Virus tworzy jego kopię zapasową i umieszcza w odpowiednim folderze na wypadek potrzeby jego przywrócenia lub pojawienia się możliwości jego wyleczenia.

7.2.6. Tworzenie szablonu powiadomienia

W tym oknie możliwe jest utworzenie treści szablonu powiadomienia dla użytkowników, z komputerów których próbowano skopiować na serwer zainfekowane/potencjalnie zainfekowane pliki.

W celu wyświetlenia większej liczby informacji treść powiadomienia może zawierać makra: ścieżkę dostępu do niebezpiecznego obiektu oraz nazwę zagrożenia. W celu dodania makr do tekstu powiadomienia należy kliknąć **Makra**.

W celu przywrócenia domyślnej treści szablonu powiadomienia należy kliknąć przycisk **Domyślny**.

7.3. Odraczenie leczenia

Kaspersky Anti-Virus for Windows Servers blokuje dostęp do zainfekowanych plików, jeżeli są one w danym momencie leczone oraz jeżeli nie mogły zostać wyleczone lub usunięte.

W celu odzyskania dostępu do zablokowanych obiektów, należy najpierw je wyleczyć. W tym celu należy:

1. W oknie głównym programu wybrać sekcję **Ochrona plików** i kliknąć lewym przyciskiem myszy w sekcji **Statystyki**.
2. Na zakładce Wykrytych wybrać jeden z obiektów i kliknąć przycisk **Akcje**, następnie polecenie **Neutralizuj wszystkie**.

Po pomyślnym wyleczeniu obiektu, zostanie on udostępniony użytkownikowi. Jeżeli nie można go wyleczyć, można go usunąć lub pominąć. W drugim przypadku, przywrócony zostanie dostęp do pliku. Jednakże, zwiększy to znacznie ryzyko infekcji komputera. Nie jest zalecane pomijanie szkodliwych obiektów.

ROZDZIAŁ 8. SKANOWANIE KOMPUTERA NA OBECNOŚĆ WIRUSÓW

Kaspersky Anti-Virus for Windows Servers umożliwia skanowanie indywidualnych elementów w poszukiwaniu wirusów (plików, folderów, dysków, urządzeń plug-and-play) lub całego komputera. Poprzez wykonywanie skanowania antywirusowego można zatrzymać rozprzestrzenienie się niebezpiecznego kodu, który nie został wykryty przez moduł Ochrona plików.

Kaspersky Anti-Virus for Windows Servers oferuje trzy rodzaje zadań skanowania:

Obszary krytyczne

Skanowanie wszystkich obszarów krytycznych komputera w poszukiwaniu wirusów. Dotyczy to: pamięci systemowej, programów ładowanych do pamięci podczas startu systemu, sektorów startowych dysków twardych i katalogów systemowych *Windows* i *system32*. Zadanie to ma na celu szybkie wykrycie aktywnych wirusów w systemie bez konieczności przeprowadzania pełnego skanowania komputera.

Mój komputer

Skanowanie komputera w poszukiwaniu wirusów obejmujące wszystkie dyski twarde, pamięć i pliki.

Obiekty startowe

Skanowanie w poszukiwaniu wirusów wszystkich programów uruchamianych wraz ze startem systemu operacyjnego.

Domyślnymi ustawieniami dla tych zadań są ustawienia zalecane przez ekspertów z firmy Kaspersky Lab. Możliwe jest modyfikowanie tych ustawień (patrz rozdział 8.4 na stronie 86) lub utworzenie terminarza (patrz rozdział 6.5 na stronie 64) uruchamiania zadań.

Istnieje również możliwość tworzenia własnych zadań (patrz rozdział 8.3 na stronie 85) przez użytkownika oraz terminarza dla nich. Na przykład, użytkownik może utworzyć zadanie skanowania pocztowych baz danych raz w tygodniu lub zadanie skanowania antywirusowego dla folderu **Moje dokumenty**.

Ponadto, możliwe jest przeskanowanie dowolnego obiektu w poszukiwaniu wirusów bez konieczności tworzenia specjalnego zadania skanowania. Wybór obiektu do przeskanowania można dokonać z poziomu interfejsu programu

Kaspersky Anti-Virus for Windows Servers lub przy użyciu standardowych narzędzi systemu Windows Server (na przykład **Eksploratora Windows**, sekcji **Mój komputer** itd.).

Możliwe jest wyświetlenie pełnej listy zadań skanowania antywirusowego komputera w sekcji **Skanuj**, znajdującej się na lewym panelu głównego okna aplikacji.

8.1. Zarządzanie zadaniami skanowania


Zadanie skanowanie antywirusowego uruchamiane może być ręcznie lub automatycznie przy użyciu terminarza (patrz rozdział 6.5 na stronie 64).

W celu ręcznego uruchomienia zadania skanowania antywirusowego należy:


Wybrać nazwę zadania w sekcji **Skanuj** znajdującej się w oknie głównym programu i kliknąć przycisk  znajdujący się na pasku stanu.

Aktualnie wykonywane zadania (włącznie z zadaniami utworzonymi przez Kaspersky Administration Kit) można wyświetlić otwierając menu kontekstowe ikony programu znajdującej się w zasobniku systemowym.

W celu wstrzymania zadania należy:

Kliknąć przycisk  znajdujący się na pasku stanu. Stan zadania zmieniony zostanie na *wstrzymano*. Zadanie zostanie wstrzymane do momentu jego ponownego ręcznego lub automatycznego wznowienia (według terminarza).

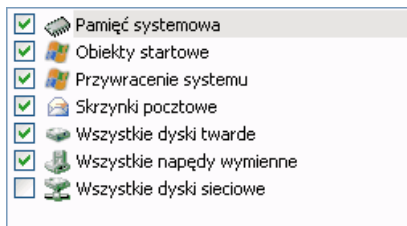
W celu zatrzymania zadania należy:

Kliknąć przycisk  znajdujący się na pasku stanu. Stan zadania zmieniony zostanie na *zatrzymano*. Zadanie zostanie przerwane do momentu jego ponownego ręcznego lub automatycznego uruchomienia (według terminarza). Podczas kolejnego uruchomienia zadania program wyświetli zapytanie o kontynuację zadania od momentu jego przerwania.

8.2. Tworzenie listy skanowanych obiektów

W celu wyświetlenia listy obiektów które zostaną przeskanowane za pomocą określonych zadań, należy wybrać nazwę zadania (na przykład: **Mój komputer**)

znajdującą się w sekcji **Skanuj** w oknie głównym programu. Lista obiektów wyświetlona zostanie w prawej części okna poniżej paska stanu (patrz rys. 23).



Rysunek 23. Tworzenie listy skanowanych obiektów

Lista skanowanych obiektów jest już utworzona dla domyślnych zadań tworzonych podczas instalacji programu. Podczas tworzenia zadań przez użytkownika lub wyboru obiektów dla zadania skanowania antywirusowego, możliwe jest utworzenie listy obiektów.

Możliwe jest modyfikowanie zawartości listy poprzez dodawanie i usuwanie z niej obiektów przy pomocy przycisków znajdujących się po prawej stronie listy. W celu dodania nowego obiektu do listy, należy kliknąć przycisk **Dodaj** i w oknie które zostanie otwarte wybrać obiekt, który ma być skanowany.

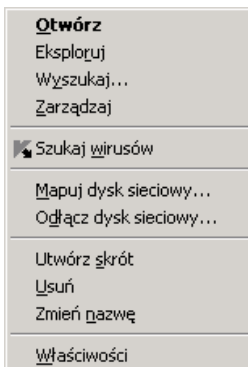
W celu ułatwienia zarządzania zawartością listy można korzystać z kategorii obiektów takich jak, pocztowe bazy danych, pamięć RAM, obiekty startowe, kopia zapasowa systemu operacyjnego oraz pliki poddane kwarantannie przez Kaspersky Anti-Virus.

Ponadto, podczas dodawania do obszaru skanowania foldera zawierającego obiekty osadzone można modyfikować poziom zagnieżdżenia. W tym celu należy użyć odpowiednich poleceń z menu kontekstowego.

Aby usunąć obiekt, należy wybrać go na liście (nazwa obiektu zostanie podświetlona) i kliknąć przycisk **Usuń**. Można tymczasowo wyłączyć skanowanie indywidualnych obiektów dowolnego zadania bez usuwania ich z listy. W tym celu, należy usunąć zaznaczenie z obiektu którego skanowanie ma nie być wykonywane.

W celu uruchomienia zadania skanowania należy kliknąć przycisk **Skanuj** lub wybrać polecenie **Uruchom** z poziomu menu kontekstowego, które zostanie otwarte po kliknięciu przycisku **Akcje**.

Ponadto, możliwe jest wybranie obiektu który zostanie przeskanowany przy użyciu standardowych narzędzi systemu Windows Server (na przykład Eksploratora Windows, sekcji Mój komputer itd.) (patrz rys. 24). W tym celu, należy umieścić kursor na nazwie żadanego obiektu i z poziomu menu kontekstowego systemu Windows Server wybrać polecenie **Szukaj wirusów**.



Rysunek 24. Uruchamianie skanowania obiektu przy użyciu menu kontekstowego Windows

8.3. Tworzenie zadań skanowania

W celu dokonania skanowania antywirusowego obiektów na komputerze, należy użyć wbudowanych zadań skanowania dołączonych do programu i utworzyć własne zadania. Nowe zadania tworzone są w oparciu o istniejące zadania skanowania.

W celu utworzenia nowego zadania skanowania antywirusowego należy:

1. W sekcji **Skanuj** wybrać zadanie którego ustawienia pokrywają się z wymaganiami użytkownika.
2. Otworzyć menu kontekstowe (przez kliknięcie prawym przyciskiem myszy na nazwie zadania) lub kliknąć przycisk **Akcje** (znajdujący się z prawej strony listy skanowanych obiektów) i wybrać opcję **Zapisz jako....**
3. W oknie które zostanie otwarte podać nazwę dla nowego zadania i kliknąć przycisk **OK**. Następnie zadanie o wybranej nazwie pojawi się na liście zadań w sekcji **Skanuj**.

Uwaga!

Liczba zadań, które może utworzyć użytkownik jest ograniczona. Maksymalną liczbą zadań jest cztery.

Utworzone zadanie dziedziczy wszystkie właściwości zadania w oparciu o które zostało ono utworzone. W kolejnym kroku konieczne jest przeprowadzenie dalszej konfiguracji zadania poprzez utworzenie listy skanowanych obiektów (patrz rozdział 8.2 na stronie 83), skonfigurowanie ustawień (patrz rozdział 8.4 na stronie 86) działania zadania, jeżeli okaże się to konieczne skonfigurowanie

terminarza w celu automatycznego uruchamiania zadania (patrz rozdział 6.5 na stronie 64).

W celu zmiany nazwy zadania należy:

Wybrać zadanie w sekcji **Skanuj** znajdującej się w oknie głównym programu. Następnie kliknąć prawym przyciskiem myszy na nazwie zadania w celu otwarcia menu kontekstowego lub kliknąć przycisk **Akcje** (z prawej strony listy skanowanych obiektów) i wybrać opcję **Zmień nazwę**.

W oknie które zostanie otwarte należy podać nową nazwę dla zadania i kliknąć przycisk **OK**. Nazwa zadania zostanie również zmieniona w sekcji **Skanuj**.

W celu usunięcia zadania należy:

Wybrać zadanie w sekcji **Skanuj** znajdującej się w oknie głównym programu. Kliknąć prawym przyciskiem myszy na nazwie zadania w celu otwarcia menu kontekstowego lub kliknąć przycisk **Akcje** znajdujący się z prawej strony listy skanowanych obiektów i wybrać opcję **Usuń**.

W oknie potwierdzenia należy potwierdzić usunięcie zadania. Następnie zadanie zostanie usunięte z listy zadań znajdującej się w sekcji **Skanuj**.

Uwaga!

Możliwe jest jedynie zmienianie nazwy i usuwanie zadań utworzonych przez użytkownika.

8.4. Konfiguracja zadań skanowania

Rodzaj metod używanych do skanowania obiektów określany jest przez zestaw właściwości przydzielonych do każdego zadania.

W celu konfiguracji ustawień zadania należy:

Wybrać nazwę zadania w sekcji **Skanuj** znajdującej się w oknie głównym programu i użyć odsyłacza Ustawienia w celu otwarcia okna ustawień zadania.

Możliwe jest użycie okna ustawień dla każdego zadania w celu:

Wyboru poziomu bezpieczeństwa, który zostanie użyty przez zadanie (patrz rozdział 8.4.1 na stronie 87)

Modyfikacji zaawansowanych ustawień:

- zdefiniowanie typów plików skanowanych na obecność wirusów (patrz rozdział 8.4.2 na stronie 88)

- skonfigurowanie uruchamiania zadania przy użyciu określonego profilu użytkownika (patrz rozdział 6.4 na stronie 62)
- skonfigurowanie zaawansowanych ustawień skanowania (patrz rozdział 8.4.5 na stronie 94)

przywroćenia domyślnych ustawień skanowania (patrz rozdział 8.4.3 na stronie 91).

wybrać akcje podejmowane przez program po wykryciu zainfekowanego lub podejrzanego obiektu (patrz rozdział 8.4.4 na stronie 92)

utworzenie terminarza (patrz rozdział 6.5 na stronie 64) automatycznego uruchamiania zadań.

Ponadto, możliwe jest konfigurowanie ustawień globalnych (patrz rozdział 8.4.6 na stronie 95) dla uruchamiania wszystkich zadań.

Niniejsza sekcja zawiera szczegółowy opis ustawień dla powyższych zadań.

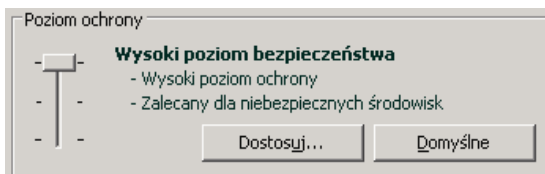
8.4.1. Wybór poziomu ochrony

Do każdego zadania skanowania antywirusowego można przypisać poziom ochrony (patrz rys. 25):

Wysoki – najbardziej szczegółowe skanowanie całego komputera lub indywidualnych dysków, folderów lub plików. Zalecane jest używanie tego poziomu w przypadku podejrzenia infekcji komputera.

Zalecany – poziom zalecany przez ekspertów z firmy Kaspersky Lab. Skanowane obejmuje te same obiekty jak w przypadku poziomu **Wysoki** za wyjątkiem baz danych wiadomości pocztowych.

Niski – poziom zapewniający minimalne obciążenie systemu kosztem wykluczenia pewnych obiektów z obszaru skanowania.



Rysunek 25. Wybór poziomu ustawień dla skanowania

Domyślnym poziomem dla skanowania plików jest poziom **Zalecany**.

Można zmniejszyć lub zwiększyć poziom bezpieczeństwa skanowania poprzez wybranie odpowiedniego poziomu przy użyciu suwaka lub zmianę ustawień dla obecnie wybranego poziomu.

W celu modyfikacji poziomu bezpieczeństwa należy:

Wybrać poziom przy użyciu suwaka. Dostosowując poziom ochrony, użytkownik definiuje współczynnik prędkości skanowania plików (im mniej typów plików jest skanowanych tym większa jest prędkość skanowania).

Jeżeli żaden z dostępnych poziomów ochrony nie spełnia wymagań użytkownika, należy zmodyfikować ustawienia skanowania. W tym celu, jako punkt początkowy, należy wybrać poziom ochrony zbliżony do wymagań użytkownika i dokonać modyfikacji jego ustawień. W tym przypadku, poziom ochrony zostanie ustawiony na **Ustawienia niestandardowe**.

W celu modyfikacji ustawień poziomu bezpieczeństwa należy:

kliknąć odsyłacz **Ustawienia** w oknie ustawień zadania. Dokonać modyfikacji ustawień w oknie, które zostanie otwarte i kliknąć przycisk **OK**.

Wynikiem będzie utworzenie czwartego poziomu bezpieczeństwa - **Ustawienia niestandardowe**, który wykorzystuje ustawienia zdefiniowane przez użytkownika.

8.4.2. Definiowanie typów skanowanych obiektów

Podczas wyboru typów skanowanych obiektów, określone są formaty plików, rozmiar oraz napędy które będą skanowane w poszukiwaniu wirusów podczas uruchamiania tego zadania.

Typy skanowanych plików zdefiniowane są w sekcji **Typy plików** (patrz rys. 26). Wybrać jedną z trzech opcji:

- Skanuj wszystkie pliki.** Po wybraniu tej opcji skanowane będą wszystkie obiekty systemu plików.
- Skanuj programy i dokumenty (według zawartości).** Po wybraniu tej grupy plików, moduł ochrony plików skanował będzie jedynie potencjalnie zainfekowane pliki - pliki mogące zawierać wirusy.

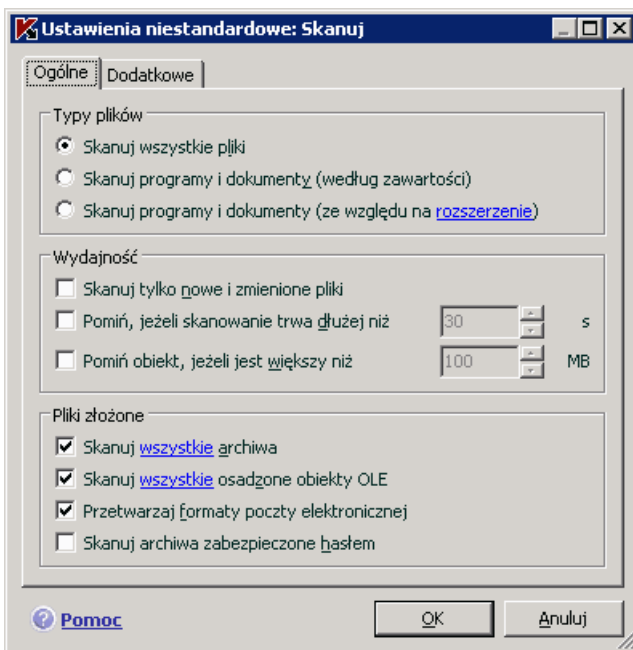
Informacja:

Istnieją formaty plików, do których wirusy nie mogą się dodać samodzielnie, ponieważ kod takich plików nie zawiera żadnych luk. Przykładem takich plików są pliki .txt.

Istnieją również formaty plików, które zawierają lub mogą zawierać kod wykonywalny. Przykładowymi formatami plików są .exe, .dll lub .doc. Ryzyko występowania szkodliwego kodu w takich plikach jest stosunkowo wysokie.

Przed rozpoczęciem skanowania antywirusowego pliku, analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu pliku (txt, doc, exe itd.).

- ☛ **Skanuj programy i dokumenty (według rozszerzenia).** W tym przypadku, program skanował będzie jedynie potencjalnie zainfekowane pliki, natomiast format pliku określany będzie według rozszerzenia. Przy użyciu odsyłacza, można wyświetlić listę rozszerzeń plików (patrz rozdział 1.1 na stronie 184).



Rysunek 26. Konfiguracja ustawień skanowania

Wskazówka:

Należy mieć na uwadze, że wirus może zostać przesłany do komputera w pliku o rozszerzeniu .txt, który w rzeczywistości jest plikiem wykonywalnym o zmienionej nazwie i rozszerzeniu. Po wybraniu opcji **Programy i dokumenty (według rozszerzenia)** tego typu plik zostanie pominięty podczas skanowania. Jeżeli wybrana została opcja **Programy i dokumenty (według zawartości)**, moduł ochrony plików analizował będzie nagłówki plików w celu uzyskania informacji o rozszerzeniu i całkowicie przeskanuje go w poszukiwaniu wirusów.

W sekcji **Wydajność** można zdefiniować skanowanie tylko plików nowych i zmodyfikowanych od czasu ostatniego skanowania lub tylko nowych plików. Ten tryb wyraźnie redukuje czas skanowania i powoduje zwiększenie wydajności programu. Aby to zrobić należy zaznaczyć **Skanuj tylko nowe i zmienione pliki**. Ten tryb działania odnosi się do plików prostych i złożonych.

W sekcji **Wydajność** możliwe jest także określenie ograniczenia czasu i rozmiaru pliku dla skanowania.

Pomiń, jeżeli skanowanie trwa dłużej niż... sek. Należy zaznaczyć tę opcję i wprowadzić maksymalny czas skanowania dla obiektu. Następnie, jeżeli czas ten zostanie przekroczony, obiekt zostanie usunięty z kolejki do skanowania.

Pomiń obiekt, jeżeli jest większy niż...MB. Należy zaznaczyć tę opcję i wprowadzić maksymalny rozmiar dla obiektu. Następnie, jeżeli rozmiar ten zostanie przekroczony, obiekt zostanie usunięty z kolejki w celu skanowania.

W sekcji **Pliki złożone**, należy wybrać pliki złożone do skanowania:

Skanuj wszystkie/tylko nowe archiwa – skanowanie archiwów .rar, .arj, .zip, .cab, .lha, .jar i .ice.

Uwaga!

Kaspersky Anti-Virus nie usuwa automatycznie formatów plików, których nie obsługuje (na przykład .ha, .uue, .tar), nawet po wybraniu opcji automatycznego leczenia lub usuwania obiektów w przypadku braku możliwości ich wyleczenia.

W celu usunięcia takich skompresowanych plików należy kliknąć odsyłacz **Usuń archiwa** znajdujący się w powiadomieniu o wykryciu niebezpiecznego obiektu. Komunikat ten zostanie wyświetlony na ekranie, jeżeli zaznaczona jest opcja **Pytaj o akcję podczas skanowania/Pytaj o akcję po zakończeniu skanowania** (patrz rozdział 8.4.4 na stronie 92). Możliwe jest także ręczne usunięcie zainfekowanych archiwów.

Skanuj wszystkie/tylko nowe osadzone obiekty OLE – skanowanie obiektów osadzonych w plikach (na przykład: arkusz kalkulacyjny programu

Excel lub makro osadzone w pliku programu MS Word, załączniki wiadomości pocztowych itp.).

Można wybrać skanowanie wszystkich plików lub tylko nowych plików dla każdego typu złożonego pliku. W tym celu, należy użyć odsyłacza znajdującego się obok nazwy obiektu. Jego wartość ulegnie zmianie po kliknięciu na nim lewym przyciskiem myszy. Jeżeli w sekcji **Wydajność** zdefiniowano skanowanie tylko nowych i zmodyfikowanych plików, nie będzie możliwe wybranie typu skanowanych plików złożonych.

Przetwarzaj formaty poczty elektronicznej – skanowanie wiadomości e-mail i pocztowych baz danych. Jeżeli ta opcja nie jest zaznaczona, pliki wiadomości pocztowych będą skanowane jako pliki binarne (bez analizy formatu pliku), i jeżeli plik nie jest zainfekowany oraz wybrana została opcja Skanuj wszystkie pliki, w raporcie umieszczony zostanie stan OK. Jeżeli wybrano skanowanie według typu lub rozszerzenia, obiekt zostanie pominięty ze względu na format.

Należy zapamiętać poniższe punkty skanowania zabezpieczonych hasłem pocztowych baz danych:

- Kaspersky Anti-Virus for Windows Servers wykrywa szkodliwy kod w bazach danych programu Microsoft Outlook 2000 lecz nie przeprowadza ich leczenia;
- Kaspersky Anti-Virus for Windows Servers nie obsługuje skanowania zabezpieczonych hasłem pocztowych baz danych programu Microsoft Office Outlook 2003.

Skanuj archiwa zabezpieczone hasłem – skanowanie archiwów zabezpieczonych hasłem. Po wybraniu tej opcji wyświetlane będzie okno z prośbą o podanie hasła przed wykonaniem skanowania archiwum. Jeżeli opcja ta nie jest zaznaczona, archiwa zabezpieczone hasłem będą pomijane.

8.4.3. Przywracanie domyślnych ustawień skanowania

Podczas konfigurowania ustawień zadań skanowania, można zawsze powrócić do ustawień zalecanych. Według ekspertów z firmy Kaspersky Lab są one optymalne i połączone w **Zalecany poziom bezpieczeństwa**.

W celu przywrócenia domyślnych ustawień skanowania należy:

1. Wybrać nazwę zadania w sekcji **Skanuj** znajdującej się w oknie głównym programu i użyć odsyłacza Ustawienia w celu otwarcia okna ustawień zadania.

2. W sekcji **Poziom ochrony** wybrać opcję **Domyślny**.

8.4.4. Wybór akcji dla obiektów

Jeżeli podczas skanowania wykryty zostanie zainfekowany lub podejrzany plik, dalsze postępowanie programu zależy od stanu obiektu i wybranych akcji.

Po zakończeniu skanowania do obiektu może zostać przypisany jeden z następujących stanów:

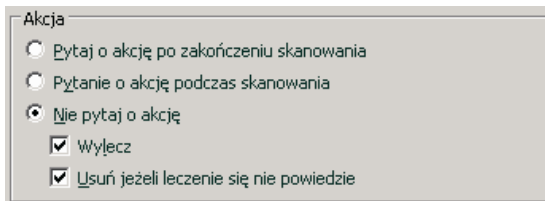
Szkodliwy program (na przykład: wirus, trojan).

Potencjalnie zainfekowany, jeżeli podczas skanowania nie można jednoznacznie stwierdzić czy obiekt jest zainfekowany. Oznacza to, że program wykrył w pliku sekwencję kodu nieznanego wirusa lub zmodyfikowany kod znanego wirusa.

Domyślnie, wszystkie zainfekowane pliki są przedmiotem leczenia i jeżeli są potencjalnie zainfekowane umieszczane są w kwarantannie.

W celu modyfikacji akcji podejmowanej na obiekcie należy:

W oknie głównym programu wybrać nazwę zadania w sekcji **Skanuj** i przejść do okna ustawień klikając odsyłacz **Ustawienia**. Wszystkie możliwe działania zostaną wyświetlone w odpowiednich sekcjach (patrz rys. 27).



Rysunek 27. Wybór akcji podejmowanych na niebezpiecznych obiektach

Wybrana akcja	W przypadku wykrycia szkodliwego lub potencjalnie zainfekowanego obiektu
<input checked="" type="radio"/> Pytaj o akcję po zakończeniu skanowania	Program nie przetwarza obiektów do momentu zakończenia skanowania. Po zakończeniu skanowania wyświetlone zostanie okno zawierające listę wykrytych obiektów oraz pytanie o ich przetworzenie.

<input checked="" type="radio"/> Pytaj o akcję podczas skanowania	Program wyświetli ostrzeżenie zawierające informacje dotyczące wykrytego szkodliwego kodu lub potencjalnie zainfekowanego pliku i możliwe do podjęcia akcje.
<input checked="" type="radio"/> Nie pytaj o akcję	Program zapisuje informacje dotyczące wykrytych obiektów w raportach bez ich przetwarzania lub powiadamiania użytkownika. Używanie tej funkcji nie jest zalecane, ponieważ zainfekowane lub potencjalnie zainfekowane obiekty pozostają w komputerze i uniknięcie infekcji jest praktycznie niemożliwe.
<input checked="" type="radio"/> Nie pytaj o akcję <input checked="" type="checkbox"/> Wylecz	Program podejmie próbę wyleczenia wykrytego obiektu bez pytania użytkownika o potwierdzenie. Jeżeli wyleczenie pliku będzie możliwe, zostanie on przeniesiony do foldera kopii zapasowej w celu późniejszego wyleczenia. Jeżeli program nie będzie mógł wyleczyć obiektu, dostęp do niego zostanie zablokowany.
<input checked="" type="radio"/> Nie pytaj o akcję <input checked="" type="checkbox"/> Wylecz <input checked="" type="checkbox"/> Usuń jeżeli leczenie się nie powiedzie	Program podejmie próbę wyleczenia wykrytego obiektu bez pytania użytkownika o potwierdzenie. Jeżeli nie można wyleczyć obiektu, zostanie on usunięty. Jego kopia zostanie zapisana w folderze kopii zapasowej.
<input checked="" type="radio"/> Nie pytaj o akcję <input type="checkbox"/> Wylecz <input checked="" type="checkbox"/> Usuń	Obiekt zostanie automatycznie usunięty.

Przed podjęciem próby leczenia lub usunięcia obiektu, Kaspersky Anti-Virus tworzy jego kopię zapasową i umieszcza w folderze kopii zapasowej na wypadek potrzeby jego przywrócenia lub pojawienia się możliwości jego wyleczenia (patrz rozdział 12.2 na stronie 153).

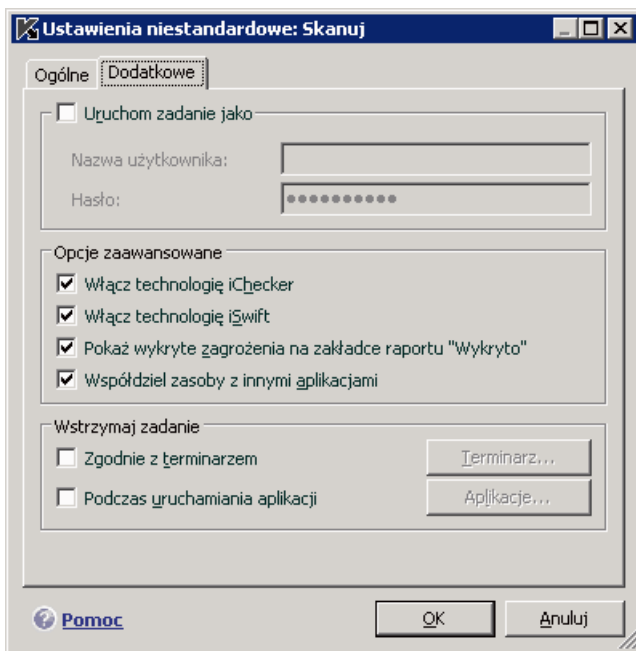
W przypadku przypisania do obiektu stanu potencjalnie zainfekowany, jest on przenoszony do Kwarantanny bez próby jego wyleczenia.

8.4.5. Dodatkowe ustawienia skanowania

Poza konfiguracją podstawowych ustawień skanowania, można również użyć ustawień zaawansowanych (patrz rysunek. 28):

- Włącz technologię iChecker** – użycie technologii, która może zwiększyć prędkość skanowania dzięki wykluczeniu określonych obiektów ze skanowania. Obiekt jest wykluczony ze skanowania przy użyciu specjalnego algorytmu. Algorytm ten wykorzystuje datę publikacji bazy sygnatur zagrożeń, datę ostatniego skanowania obiektu oraz datę ostatniej modyfikacji ustawień.

Na przykład: użytkownik posiada plik archiwum, który został przeskanowany przez program i do którego przydzielony został stan niezainfekowany. Następnie program pominie to archiwum, jeśli nie zostało ono zmodyfikowane lub jeżeli nie zmieniono ustawień skanowania. Jeżeli struktura archiwum zostanie zmieniona z powodu dodania nowego obiektu, zmienione zostaną ustawienia skanowania lub uaktualnione zostaną sygnatury zagrożeń, program przeskanuje archiwum ponownie.



Rysunek 28. Zaawansowane ustawienia skanowania

Ograniczeniem technologii iChecker™ jest możliwość jej wykorzystania wyłącznie dla obiektów, których struktura jest rozpoznawana przez program Kaspersky Anti-Virus for Windows Servers (na przykład, .exe, .dll, .lnk, .lff, .inf, .sys, .com, .chm, .zip, .rar).

- Włącz technologię iSwift.** Technologia ta jest implementacją technologii iChecker dla komputerów wykorzystujących system plików NTFS. Ograniczeniem technologii iSwift jest jej powiązanie z konkretną lokalizacją pliku w systemie plików oraz możliwość jej zastosowania wyłącznie dla systemu plików NTFS.
- Pokaż wykryte zagrożenia na zakładce raportu "Wykryto"** – wyświetlanie listy wykrytych zagrożeń podczas skanowania na zakładce raportu **Wykryto** (patrz rozdział 11.3.2 na stronie 126). Wyłączenie tej funkcji może być odpowiednie dla specjalnych zadań skanowania lub przykładowo zbiorów tekstowych w celu zwiększenia prędkości skanowania.
- Współdziel zasoby z innymi aplikacjami** – wstrzymanie zadania skanowania w przypadku, gdy procesor wymaga więcej mocy obliczeniowej dla innych aplikacji.

8.4.6. Definiowanie globalnych ustawień skanowania dla wszystkich zadań

Każde zadanie skanowania uruchamiane jest zgodnie ze swoimi ustawieniami. Domyślnie, zadania utworzone po instalacji programu na komputerze używają ustawień zalecanych przez ekspertów z firmy Kaspersky Lab.

Możliwe jest konfigurowanie globalnych ustawień skanowania dla wszystkich zadań. Jako punkt wyjściowy użytkownik użyje zestawu ustawień używanych do skanowania indywidualnych obiektów.


W celu przydzielenia globalnych ustawień skanowania dla wszystkich zadań należy:

1. Wybrać sekcję **Skanuj** i kliknąć odsyłacz Ustawienia.
2. W oknie które zostanie otwarte należy dokonać konfiguracji ustawień skanowania: wybrać poziom bezpieczeństwa (patrz rozdział 8.4.1 na stronie 87), skonfigurować ustawienia zaawansowane i wybrać działania podejmowane na obiektach (patrz rozdział 8.4.4 na stronie 92).
3. W celu zastosowania nowych ustawień dla wszystkich zadań, należy kliknąć przycisk **Zastosuj** znajdujący się w sekcji **Inne zadania skanowania**. W oknie dialogowym, które zostanie wyświetlone należy zatwierdzić globalne ustawienia.

ROZDZIAŁ 9. TESTOWANIE DZIAŁANIA KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Po zainstalowaniu i skonfigurowaniu programu Kaspersky Anti-Virus można przeprowadzić kilka testów pozwalających na upewnienie się, że ochrona działa prawidłowo.

9.1. Wirus testowy EICAR i jego modyfikacje

Wirus testowy został stworzony przez instytut  (The European Institute for Computer Antivirus Research) w celach testowania funkcjonalności oprogramowania antywirusowego.

EICAR NIE JEST WIRUSEM i nie zawiera kodu, który mógłby uszkodzić komputer. Jednak, większość programów antywirusowych identyfikuje go jako wirusa.

Do testowania funkcjonalności programu antywirusowego nigdy nie należy używać prawdziwych wirusów!

Wirusa testowego można pobrać z witryny instytutu EICAR: http://www.eicar.org/anti_virus_test_file.htm.

Plik pobrany ze strony internetowej EICAR zawiera kod standardowego wirusa testowego. Kaspersky Anti-Virus wykryje go, sklasyfikuje jako **wirusa** i podejmie akcję zdefiniowaną dla tego typu zagrożenia.

W celu przetestowania zachowania programu Kaspersky Anti-Virus podczas wykrywania różnych typów obiektów należy zmodyfikować zawartość pliku zawierającego standardowego wirusa testowego poprzez dodanie jednego z poniższych tekstów (przedrostków) na początku zawartości pliku.

Przedrostek	Status wirusa testowego	Akcja podjęta przez aplikację po przetworzeniu obiektu
Brak prefiksu, standardowy wirus testowy	Plik zawiera wirusa testowego. Brak możliwości wyleczenia obiektu.	Aplikacja zidentyfikuje obiekt jako szkodliwy i z powodu braku możliwości wyleczenia - usunie go.
CORR-	Uszkodzony.	Aplikacja ma dostęp do obiektu, ale nie może go przeskanować, ponieważ obiekt jest uszkodzony (na przykład, naruszona struktura pliku, nieprawidłowy format pliku).
SUSP- WARN-	Plik zawiera wirusa testowego (modyfikację). Brak możliwości wyleczenia obiektu.	Obiekt ten jest modyfikacją znanego lub nieznanego wirusa. W momencie wykrycia bazy danych sygnatur zagrożeń nie zawierają opisu procedury leczenia tego obiektu. Aplikacja umieści obiekt w kwarantannie w celu jego późniejszego przetworzenia przy użyciu zaktualizowanych sygnatur zagrożeń.
ERRO-	Błąd przetwarzania.	Podczas przetwarzania obiektu wystąpił błąd: aplikacja nie ma dostępu do skanowanego obiektu, nastąpiło naruszenie jego integralności (na przykład brak zakończenia w archiwum wielowoluminowym) lub nie można nawiązać połączenia z obiektem (w przypadku skanowania obiektu na dysku sieciowym).
CURE-	Plik zawiera wirusa testowego. Może zostać wyleczony. Obiekt może zostać poddany leczeniu; tekst w kodzie wirusa zostanie	Obiekt zawiera wirusa, który może zostać wyleczony. Aplikacja przeskanuje obiekt w poszukiwaniu wirusów, po czym zostanie on całkowicie wyleczony.

Przedrostek	Status wirusa testowego	Akcja podjęta przez aplikację po przetworzeniu obiektu
	zamieniony na CURE.	
DELE-	Plik zawiera wirusa testowego. Brak możliwości wyleczenia obiektu.	Obiekt zawiera wirusa, który nie może zostać wyleczony lub jest to trojan. Aplikacja usuwa te obiekty.

W pierwszej kolumnie tabeli znajdują się prefiksy, które należy dodać na początku kodu standardowego wirusa testowego. Druga kolumna opisuje stan i reakcję programu Kaspersky Anti-Virus na wykrycie modyfikacji wirusa testowego. Trzecia kolumna zawiera informacje na temat obiektów z tym samym stanem, które zostały przetworzone przez aplikację.

Wartości w ustawieniach skanowania antywirusowego określają akcje podejmowane na każdym z obiektów.

9.2. Testowanie modułu Ochrona plików

W celu przetestowania funkcjonalności Ochrony plików należy:

1. Utworzyć na dysku folder i skopiować do niego pobranego wirusa testowego oraz jego modyfikację (patrz rozdział 9.1 na stronie 96).
2. Zezwolić na raportowanie o wszystkich wydarzeniach w celu przechowywania w pliku raportu informacji na temat uszkodzonych obiektów i obiektów, które nie zostały przeskanowane z powodu wystąpienia błędów. W tym celu należy zaznaczyć opcję **Zapisuj zdarzenia informacyjne** znajdującą się w oknie konfiguracji raportu (patrz rozdział 11.3.1 na stronie 125).
3. U uruchomić wirusa testowego lub jego modyfikację.

Moduł Ochrona plików przechwyci próbę dostępu do pliku, przeskanuje go i poinformuje użytkownika, że został wykryty niebezpieczny obiekt.

W przypadku wybrania różnych opcji przetwarzania wykrytych obiektów, można testować reakcję Ochrony plików na wykrywanie różnych typów obiektów.

Szczegóły działania Ochrony plików znajdują się w raporcie składnika.

9.3. Testowanie zadań skanowania antywirusowego

W celu przetestowania zadań skanowania antywirusowego należy:

1. Utworzyć na dysku folder i skopiować do niego pobranego wirusa testowego (patrz rozdział 9.1 na stronie 96) oraz jego modyfikacje.
2. Utworzyć nowe zadanie skanowania antywirusowego (patrz rozdział 8.3 na stronie 85) i jako obiekt do skanowania wskazać folder zawierający testowe wirusy (patrz rozdział 9.1 na stronie 96).
3. Zezwolić na raportowanie o wszystkich wydarzeniach w celu przechowywania w pliku raportu informacji na temat uszkodzonych obiektów i obiektów, które nie zostały przeskanowane z powodu wystąpienia błędów. W tym celu należy zaznaczyć opcję **Zapisuj zdarzenia informacyjne** znajdującą się w oknie konfiguracji raportu.
4. Uruchomić zadanie skanowania antywirusowego (patrz rozdział 8.1 na stronie 83).

Po uruchomieniu skanowania, w przypadku wykrycia podejrzanego lub zainfekowanego obiektu, na ekranie zostanie wyświetlona informacja o obiekcie z prośbą o wybranie następczej czynności:



Rysunek 29. Wykryto niebezpieczny obiekt w ruchu internetowym

W przypadku wybrania różnych opcji przetwarzania wykrytych obiektów, można testować reakcję Kaspersky Anti-Virus na wykrywanie różnych typów obiektów.

W raporcie składnika możliwe jest przeglądanie szczegółów działania zadania skanowania antywirusowego.

ROZDZIAŁ 10. AKTUALIZACJA PROGRAMU

Wykonywanie aktualizacji oprogramowania antywirusowego jest jedną z najważniejszych czynności w ochronie danych. Z uwagi na częste pojawianie się nowych wirusów, trojanów i szkodliwego oprogramowania, ważne jest wykonywanie regularnych aktualizacji aplikacji w celu stałej ochrony informacji użytkownika.

Uaktualnianie aplikacji dotyczy pobierania i instalacji na komputerze następujących elementów:

Sygnatury zagrożeń

Aplikacja wykorzystuje sygnatury zagrożeń do ochrony informacji przechowywanych na komputerze. Moduły programu zapewniające ochronę komputera używają ich do wyszukiwania i leczenia szkodliwych obiektów na komputerze użytkownika. Do sygnatur dodawane są co godzinę nowe wpisy zawierające definicje nowych zagrożeń oraz metody ich neutralizacji. Dlatego też, zalecane jest regularne wykonywanie aktualizacji.

Poprzednie wersje aplikacji firmy Kaspersky Lab obsługiwały zarówno bazy standardowe jak i rozszerzone. Każda z tych baz zapewniała ochronę komputera przed różnymi typami niebezpiecznych obiektów. W programie Kaspersky Anti-Virus for Windows Servers nie ma konieczności wyboru zestawu sygnatur zagrożeń. W chwili obecnej program używa sygnatur zagrożeń zapewniających ochronę przed wieloma szkodliwymi i potencjalnie niebezpiecznymi obiektami oraz przed atakami hakerów.

Moduły aplikacji

Poza aktualizacją sygnatur zagrożeń, możliwe jest również uaktualnianie modułów programu Kaspersky Anti-Virus. Nowe uaktualnienia dla aplikacji pojawiają się regularnie.

Głównym źródłem aktualizacji dla programu Kaspersky Anti-Virus for Windows Servers są serwery aktualizacji firmy Kaspersky Lab. Poniżej znajduje się kilka adresów:

<http://downloads1.kaspersky-labs.com/updates/>

<http://downloads2.kaspersky-labs.com/updates/>

<ftp://downloads1.kaspersky-labs.com/updates/>

Aby możliwe było pobieranie uaktualnień z serwerów aktualizacji, komputer musi być podłączony do Internetu.

Jeżeli użytkownik nie ma dostępu do serwerów uaktualnień firmy Kaspersky Lab (brak dostępu do Internetu), może on skontaktować się z naszym biurem celem uzyskania informacji na temat otrzymywania uaktualnień antywirusowych baz danych na płytach CD-ROM.

Uaktualnienia mogą być pobierane przy użyciu jednej z następujących metod:

Automatycznie. Kaspersky Anti-Virus automatycznie szuka nowych aktualizacji z uwzględnieniem zdefiniowanej częstotliwości. Procedura ta wykonywana jest częściej w trakcie trwania epidemii wirusa, oraz rzadziej po ich zakończeniu. Po wykryciu przez program najnowszych uaktualnień, są one pobierane i instalowane na komputerze. Jest to ustawienie domyślne.

Zgodnie z terminarzem. Aktualizacja uruchamiana będzie automatycznie zgodnie z terminarzem.

Ręcznie. Po wybraniu tej opcji, aktualizacja uruchamiana będzie ręcznie przez użytkownika.

Podczas procesu aktualizacji, aplikacja porównuje używane sygnatury zagrożeń i moduły programu z wersjami dostępnymi na serwerze aktualizacji. Jeżeli na serwerze znajduje się najnowsza wersja sygnatur i modułów, odpowiednia informacja na ten temat zostanie wyświetlona w głównym oknie programu. Jeżeli wersja sygnatur zagrożeń i modułów programu znajdujących się na komputerze różni się od wersji znajdującej się na serwerach aktualizacji, aplikacja pobierze jedynie brakujące części uaktualnień. Moduł aktualizacji nie pobiera sygnatur zagrożeń i modułów programu, które już znajdują się na komputerze użytkownika, co znacznie zwiększa prędkość pobierania uaktualnień oraz zmniejsza ruch sieciowy.

Przed wykonaniem aktualizacji sygnatur zagrożeń, Kaspersky Anti-Virus for Windows Servers tworzy ich kopie zapasowe, które mogą zostać użyte w celu cofnięcia aktualizacji (patrz rozdział 10.2 na stronie 103). Jeżeli, na przykład, podczas procesu pobierania sygnatury zagrożeń zostaną uszkodzone, w łatwy sposób będzie można przeprowadzić cofnięcie do poprzedniej wersji i spróbować pobrać sygnatury w późniejszym terminie.

W trakcie wykonywania aktualizacji, możliwe jest współdzielenie pobranych uaktualnień do foldera lokalnego (patrz rozdział 10.4.4 na stronie 112). Funkcja ta pozwala na aktualizację baz danych i modułów używanych na komputerach sieciowych przez aplikacje w wersjach 6.0 w celu zmniejszenia obciążenia łącza internetowego.

10.1. Uruchamianie aktualizacji

Proces aktualizacji może zostać uruchomiony w każdej chwili. Uaktualnienia pobierane będą ze źródła aktualizacji wybranego przez użytkownika (patrz rozdział 10.4.1 na stronie 105).

Proces aktualizacji można uruchomić z poziomu:

menu kontekstowego (patrz rozdział 4.2 na stronie 32).

okna głównego programu (patrz rozdział 4.3 na stronie 33)

W celu uruchomienia aktualizacji z poziomu menu kontekstowego należy:

1. Kliknąć prawym przyciskiem myszy na ikonie programu znajdującej się w zasobniku systemowym w celu otwarcia menu kontekstowego.
2. Wybrać polecenie **Aktualizacja**.

W celu uruchomienia aktualizacji z poziomu okna głównego programu należy:

1. Wybrać sekcję **Aktualizacja** w sekcji **Usługi**.
2. Kliknąć przycisk **Aktualizuj teraz!** znajdujący się w prawym panelu okna głównego lub użyć przycisku ► na pasku.

Postęp procesu aktualizacji wyświetlony zostanie w specjalnym oknie. W celu ukrycia okna postępu należy kliknąć **Zamknij**. Aktualizacja będzie kontynuowana w tle.

Należy pamiętać o tym, że po zaznaczeniu odpowiedniej opcji pobierane uaktualnienia będą automatycznie dystrybuowane do lokalnego źródła aktualizacji (patrz sekcja 10.4.4 na stronie 112).

10.2. Cofanie aktualizacji

Każdorazowo podczas uruchamiania procesu aktualizacji, Kaspersky Anti-Virus for Windows Servers tworzy kopię zapasową bieżących sygnatur zagrożeń, a następnie rozpoczyna pobieranie uaktualnień. W ten sposób można przywrócić poprzednią wersję sygnatur jeżeli aktualizacja się nie powiedzie.

Opcja umożliwiająca cofnięcie aktualizacji może okazać się przydatna w przypadku gdy, przykładowo aktualizacja sygnatur zagrożeń się nie powiedzie z powodu błędu połączenia. Możliwe jest cofnięcie do poprzedniej wersji sygnatur i późniejsze wykonanie aktualizacji.

W celu cofnięcia sygnatur zagrożeń do poprzedniej wersji należy:

1. wybrać opcję **Aktualizacja** znajdującą się w sekcji Usługi w oknie głównym programu i kliknąć przycisk **Uaktualnij teraz** znajdujący się w prawej części okna.
2. Kliknąć przycisk **Cofnij** znajdujący się w prawym panelu okna głównego.

10.3. Tworzenie zadań aktualizacji

Kaspersky Anti-Virus posiada wbudowane zadanie aktualizacji służące do uaktualniania sygnatur zagrożeń oraz modułów programu. Użytkownik może tworzyć własne zadania aktualizacji z różnymi ustawieniami i terminarzami uruchamiania.

Przykład: Użytkownik zainstalował program Kaspersky Anti-Virus na laptopie, który jest użytkowany w domu i w biurze. W domu program jest uaktualniany z serwerów Kaspersky Lab, natomiast w biurze wykorzystywany jest do tego lokalny folder zdefiniowany przez administratora firmowej sieci. Aby wyeliminować konieczność częstego modyfikowania ustawień wbudowanego zadania aktualizacji, można utworzyć własne.

W celu utworzenia zaawansowanego zadania aktualizacji należy:

1. Wybrać sekcję **Usługi** w oknie głównym programu, otworzyć menu kontekstowe modułu **Aktualizacja** (należy kliknąć odsyłacz prawym przyciskiem myszy) i wybrać polecenie **Zapisz jako**.
2. Wprowadzić nazwę zadania w oknie, które zostanie wyświetlone na ekranie i kliknąć **OK**. W sekcji **Usługi** okna głównego programu, wyświetlone zostanie nowe zadanie o podanej nazwie.

Uwaga!

Liczba zadań aktualizacji, które może utworzyć użytkownik w programie Kaspersky Anti-Virus jest ograniczona. Można utworzyć maksymalnie dwa zadania.

Nowe zadanie odziedziczy wszystkie ustawienia od zadania, na podstawie którego zostało utworzone, za wyjątkiem ustawień terminarza. Domyślnie, automatyczne skanowanie dla nowego zadania jest wyłączone. Następnie należy skonfigurować ustawienia zadania poprzez określenie źródła uaktualnień (patrz rozdział 10.4.1 na stronie 105), zdefiniowanie ustawień sieciowych (patrz rozdział 10.4.3 na stronie 110), i jeżeli jest to konieczne włączenie uruchamiania zadania z odpowiednimi uprawnieniami (patrz rozdział 6.4 na stronie 62) oraz skonfigurować terminarz (patrz rozdział 6.5 na stronie 64).

W celu zmiany nazwy zadania należy:

Wybrać zadanie w sekcji **Usługi** znajdującej się w oknie głównym programu, otworzyć jego menu kontekstowe i wybrać polecenie **Zmień nazwę**.

W oknie które zostanie otwarte należy podać nową nazwę dla zadania i kliknąć przycisk **OK**. Nazwa zadania zostanie zmieniona w sekcji **Usługi**.

W celu usunięcia zadania należy:

Wybrać zadanie w sekcji **Usługi** znajdującej się w oknie głównym programu, otworzyć jego menu kontekstowe i wybrać polecenie **Usuń**.

Na ekranie wyświetlone zostanie okno z prośbą o potwierdzenie usunięcia zadania. Zadanie zostanie usunięte z listy zadań sekcji **Usługi**.

Uwaga!

Zmiana nazwy lub usuwanie możliwe jest tylko dla zadań utworzonych przez użytkownika.

10.4. Konfiguracja ustawień aktualizacji

Ustawienia aktualizacji określają następujące parametry:

- Źródło, z którego pobierane i instalowane są uaktualnienia (patrz rozdział 10.4.1 na stronie 105)
- Tryb uruchamiania procedury aktualizacji (patrz rozdział 10.4.2 na stronie 108)
- Rodzaj uaktualnianych obiektów
- Działania podejmowane po zakończeniu aktualizacji (patrz rozdział 10.4.4 na stronie 112)

Niniejsza sekcja zawiera szczegółowy opis zagadnień przedstawionych powyżej.

10.4.1. Wybór źródła uaktualnień

Źródło aktualizacji jest miejscem, z którego pobierane są uaktualnienia sygnatur zagrożeń i modułów programu Kaspersky Anti-Virus.

Można użyć jednego z poniższych źródeł aktualizacji:

Serwer administracyjny – scentralizowane miejsce przechowywania znajdujące się na serwerze administracyjnym Kaspersky Administration Kit (więcej informacji na ten temat zawiera podręcznik dla administratora narzędzia Kaspersky Administration Kit).

Serwery aktualizacji firmy Kaspersky Lab – specjalne serwery zawierające uaktualnienia sygnatur zagrożeń oraz modułów aplikacji Kaspersky Lab.

Serwer HTTP, serwer FTP lub folder sieciowy – lokalny serwer przechowujący najnowsze uaktualnienia.

Jeżeli użytkownik nie ma dostępu do serwerów uaktualnień firmy Kaspersky Lab (brak dostępu do Internetu), może on skontaktować się z naszym biurem celem uzyskania informacji na temat otrzymywania uaktualnień antywirusowych baz danych na płytach CD-ROM.

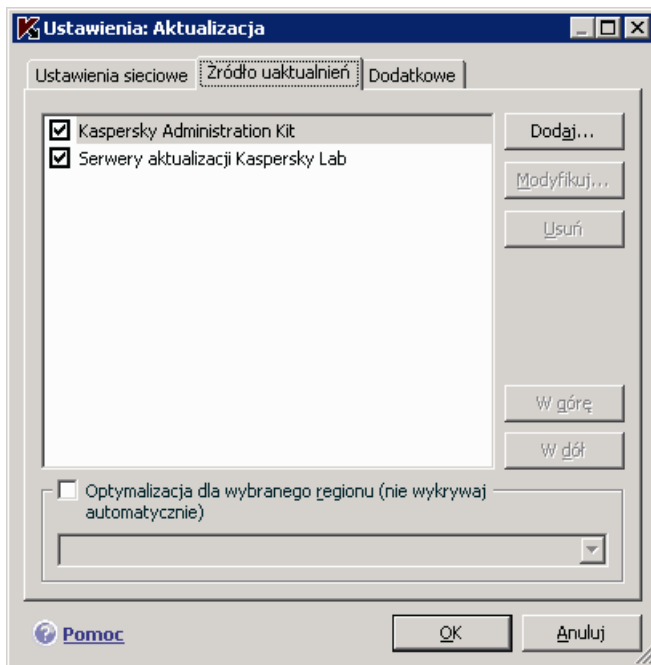
Uwaga!

Podczas zamawiania uaktualnień, należy określić czy uaktualnienie dla modułów programu mają również zostać przesłane.

Można skopiować uaktualnienia z nośnika i zapisać je na witrynie FTP lub HTTP lub w folderze lokalnym lub sieciowym.

Na zakładce **Źródła uaktualnień** należy wybrać źródło pobierania aktualizacji (patrz rys. 30).

Domyślnie, uaktualnienia pobierane są z serwerów aktualizacji firmy Kaspersky Lab. Lista serwerów reprezentowana przez ten element nie może być modyfikowana. Podczas procesu aktualizacji, Kaspersky Anti-Virus for Windows Servers odwołuje się do tej listy, wybierając adres pierwszego serwera i próbuje pobrać z niego pliki. Jeżeli nie można pobrać uaktualnień z pierwszego serwera na liście, aplikacja podejmuje próbę połączenia i pobrania uaktualnień z kolejnego serwera. Proces ten trwa aż do chwili pomyślnego pobrania uaktualnień. Adres serwera, z którego uaktualnienia zostały pomyślnie pobrane jest automatycznie umieszczany na początku listy. Podczas kolejnej próby pobrania uaktualnień, aplikacja spróbuje połączyć się z nim w pierwszej kolejności.



Rysunek 30. Wybór źródła uaktualnień

W celu pobrania uaktualnień z witryny FTP lub HTTP należy:

1. Kliknąć przycisk **Dodaj**.
2. W polu **Źródło** znajdującym się oknie **Wybierz źródło aktualizacji** wybrać docelową witrynę FTP lub HTTP lub określić adres IP, nazwę domenową lub adres URL.

Uwaga!

W przypadku wybrania źródła aktualizacji znajdującego się poza siecią lokalną (LAN) wymagane jest połączenie z Internetem.

W celu uaktualnienia z lokalnego foldera należy:

1. Kliknąć przycisk **Dodaj**.
2. W oknie **Wybierz źródło aktualizacji** należy wybrać folder lub określić pełną ścieżkę dostępu do tego foldera w polu **Źródło**.

Kaspersky Anti-Virus for Windows Servers doda nowe źródło aktualizacji na początek listy i automatycznie je włączy, przez zaznaczenie pola znajdującego się przy nazwie źródła.

Jeżeli jako aktywne ustawiono kilka źródeł aktualizacji, aplikacja będzie podejmowała próby nawiązywania połączenia z każdym z nich, począwszy od szczytu listy; uaktualnienia zostaną pobrane z pierwszego dostępnego źródła. W celu zmodyfikowania kolejności źródeł aktualizacji na liście należy użyć przycisków **W górę** oraz **W dół**.

W celu modyfikacji listy, należy użyć przycisków **Dodaj**, **Modyfikuj** i **Usuń**. Nie można modyfikować lub usuwać źródeł serwery firmy Kaspersky Lab lub serwer Kaspersky Administration Kit.

Jeżeli aktualizacja wykonywana jest z serwerów aktualizacji Kaspersky Lab, można określić optymalną lokalizację dla serwerów z których pobierane będą uaktualnienia. Firma Kaspersky Lab posiada serwery w kilku krajach. Po wybraniu serwera, który znajduje się możliwie najbliżej lokalizacji użytkownika, aktualizacje będą pobierane znacznie szybciej.

Aby użyć najbliższego serwera, należy zaznaczyć opcję **Optymalizacja dla wybranego regionu (nie wykrywaj automatycznie)** i wybrać z listy rozwijalnej kraj najmniej oddalony od lokalizacji użytkownika. Jeżeli to pole zostanie zaznaczone, podczas aktualizacji program będzie korzystał z serwerów znajdujących się w wybranym regionie. Domyślnie pole to nie jest zaznaczone a informacje na temat bieżącej lokalizacji pobierane są z rejestru systemu operacyjnego.

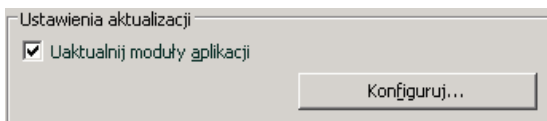
10.4.2. Wybór metody aktualizacji

Podczas konfiguracji ustawień aktualizacji, ważne jest zdefiniowanie rodzaju pobieranych uaktualnień oraz metody aktualizacji.

Uaktualniane obiekty to składniki (patrz rys. 31), dla których pobrane zostaną aktualizacje:

- sygnatury zagrożeń
- moduły programu

Sygnatury zagrożeń są zawsze aktualizowane, natomiast moduły aplikacji aktualizowane są tylko wtedy, jeżeli funkcja taka została włączona.



Rysunek 31. Wybór uaktualnianych obiektów

W celu pobrania i zainstalowania modułów programu należy:

Zaznaczyć opcję **Uaktualnij moduły programu** w oknie **Aktualizacja**.

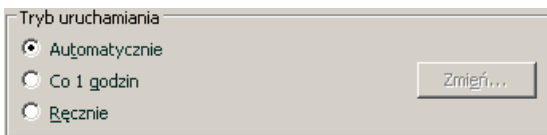
Jeżeli w źródle aktualizacji znajdują się najnowsze uaktualnienia modułów programu, na ekranie wyświetlone zostanie okno zawierające opis wszystkich zmian wprowadzonych w modułach programu. Bazując na opisie, użytkownik może zdecydować czy uaktualnienia mają zostać zainstalowane.

Metody definiują (patrz rys. 32) sposób pobierania uaktualnień. Można wybrać jedną z następujących metod:

Automatycznie. Kaspersky Anti-Virus automatycznie szuka nowych aktualizacji z uwzględnieniem zdefiniowanej częstotliwości (patrz rozdział 10.4.1 na stronie 105). Po wykryciu przez program najnowszych uaktualnień, są one pobierane i instalowane na komputerze.

Jeżeli *źródłem aktualizacji* jest zasób sieciowy, Kaspersky Anti-Virus for Windows Workstations próbuje uruchomić aktualizację po upływie czasu określonego w poprzednim pakiecie uaktualnień.

Jeżeli jako źródło aktualizacji wybrany został folder lokalny, aplikacja próbuje pobierać uaktualnienia z częstotliwością określoną w ostatnio pobranym pakiecie uaktualnień. Ta opcja pozwala firmie Kaspersky Lab regulować częstotliwość aktualizacji programu w przypadku epidemii wirusowej lub innych potencjalnie niebezpiecznych sytuacji. Aplikacja pobierała będzie na bieżąco najnowsze uaktualnienia sygnatur zagrożeń, ataków sieciowych i modułów programu, chroniąc przed penetracją komputera przez szkodliwe oprogramowanie.



Rysunek 32. Wybór trybu pobierania aktualizacji

Zgodnie z terminarzem. Aktualizacja uruchamiana będzie automatycznie zgodnie z terminarzem. Domyślnie aktualizacje pobierane są codziennie. W celu zmodyfikowania domyślnego terminarza należy kliknąć przycisk **Zmień...** i dokonać niezbędnych modyfikacji w oknie które zostanie otwarte (patrz rozdział 6.5 na stronie 64). Tryb ten jest używany domyślnie.

Ręcznie. W przypadku wybrania tej opcji, użytkownik ręcznie uruchamia proces pobierania aktualizacji. Kaspersky Anti-Virus for Windows Servers wyświetla powiadomienia o konieczności przeprowadzenia aktualizacji w następujący sposób:

przy użyciu komunikatu wyskakującego informującego o konieczności wykonania aktualizacji programu wyświetlanego nad ikoną programu w zasobniku systemowym (jeżeli powiadomienia są włączone; patrz rozdział 11.8.1 na stronie 137);

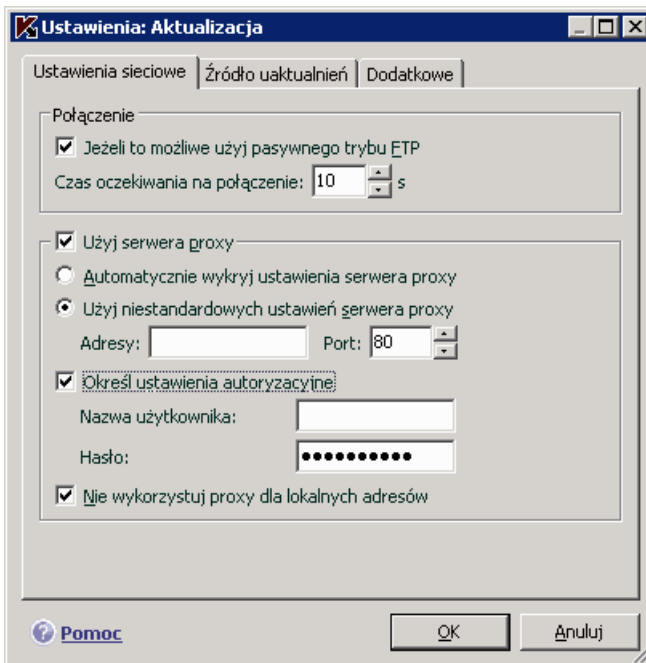
poprzez wskaźnik wyświetlany w oknie głównym programu informujący o konieczności dokonania aktualizacji programu (patrz rozdział 5.1.1 na stronie 39).

poprzez polecenie informujące o potrzebie wykonania aktualizacji wyświetlane w sekcji informacyjnej znajdującej się w oknie głównym programu (patrz rozdział 4.3 na stronie 33)

10.4.3. Konfiguracja ustawień sieciowych

Jeżeli uaktualnienia pobierane mają być z serwerów aktualizacji firmy Kaspersky Lab lub z witryn FTP lub HTTP, należy najpierw sprawdzić ustawienia sieciowe.

Wszystkie ustawienia znajdują się na zakładce **Ustawienia sieciowe** (patrz rys. 33).



Rysunek 33. Konfiguracja ustawień sieciowych dla aktualizacji

Jeżeli uaktualnienia pobierane są z serwera FTP w trybie pasywnym należy zaznaczyć opcję **Jeżeli to możliwe użyj pasywnego trybu FTP** (na przykład: w środowisku z zaporą ogniową). W przypadku pracy w aktywnym trybie FTP, należy usunąć zaznaczenie z tego pola.

W polu **Czas oczekiwania na połączenie (sek.)** należy zdefiniować maksymalny czas nawiązywania połączenia z serwerem aktualizacji. Jeżeli połączenie nie zostanie nawiązane, po upływie tego czasu program spróbuje nawiązać połączenie z następnym serwerem aktualizacji. Próby te będą ponawiane aż do nawiązania połączenia lub do momentu wykorzystania wszystkich źródeł aktualizacji dostępnych na liście.

Jeżeli serwer proxy jest wykorzystywany do nawiązywania połączenia z Internetem, należy zaznaczyć pole **Użyj serwera proxy** oraz, jeżeli jest to wymagane, określić następujące ustawienia:

Określić ustawienia serwera proxy, które będą używane podczas aktualizacji:

- Automatycznie wykryj ustawienia serwera proxy.** W przypadku wybrania tej opcji ustawienia serwera proxy zostaną automatycznie wykryte przy użyciu protokołu WPAD (Web Proxy Auto-Discovery Protocol). Jeżeli adres nie zostanie wykryty przy użyciu protokołu, Kaspersky Anti-Virus użyje ustawień serwera proxy określonych w ustawieniach Microsoft Internet Explorer.
- Użyj niestandardowych ustawień serwera proxy.** Użycie serwera proxy, który inny niż jest to zdefiniowane w ustawieniach połączenia przeglądarki. W polu Adres należy podać adres IP lub nazwę serwera proxy oraz w polu Port określić numer portu używanego przez serwer proxy do pobierania aktualizacji.

Określić, czy na serwerze proxy wymagana jest autoryzacja. *Autoryzacja* jest procesem weryfikującym dane rejestracyjne użytkownika w celu kontroli dostępu.

Jeżeli w celu nawiązania połączenia z serwerem proxy wymagana jest autoryzacja, należy zaznaczyć pole **Określ ustawienia autoryzacyjne** i określić nazwę użytkownika i hasło w polach znajdujących się poniżej. W przypadku wystąpienia takiego zdarzenia, w pierwszej kolejności nastąpi autoryzacja NTLM a następnie BASIC.

Jeżeli pole to nie jest zaznaczone lub jeżeli jest puste, autoryzacja NTLM odbędzie się przy użyciu konta użytkownika, z poziomu którego uruchomiono aktualizację (patrz rozdział 6.4 na stronie 62).

Jeżeli serwer proxy wymaga **uwierzytelniania** oraz nie wprowadzono nazwy użytkownika i hasła lub wprowadzone dane nie zostały zaakceptowane przez serwer proxy, podczas uruchomienia pobierania uaktualnień wyświetlone zostanie okno z prośbą o podanie nazwy użytkownika i hasła. Jeżeli uwierzytelnienie się powiedzie, nazwa użytkownika i hasło zostaną użyte podczas kolejnej aktualizacji programu. W przeciwnym wypadku ustawienia uwierzytelniania będzie trzeba wprowadzić ponownie.

W celu uniemożliwienia użycia serwera proxy w przypadku, gdy źródłem aktualizacji jest folder lokalny, należy zaznaczyć opcję **Nie wykorzystuj proxy dla lokalnych adresów.**

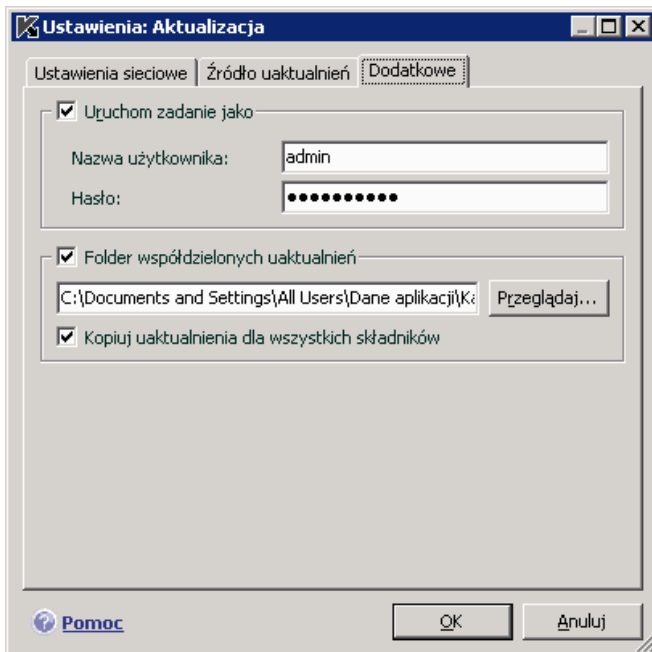
10.4.4. Współdzielenie uaktualnień

Dystrybucja aktualizacji pozwala na zoptymalizowanie obciążenia firmowej sieci. Proces kopiowania aktualizacji obejmuje dwa etapy:

Jeden z komputerów w sieci pobiera uaktualnienia sygnatur zagrożeń i modułów programu z serwerów Kaspersky Lab lub z innego źródła aktualizacji. Po pobraniu uaktualnienia zapisywane są w folderze z publicznym dostępem.

Pozostałe komputery działające w sieci pobierają uaktualnienia z publicznego foldera.

W celu włączenia opcji współdzielenia uaktualnień należy zaznaczyć pole **Folder współdzielenia aktualizacji** na zakładce **Dodatkowe** oraz w polu znajdującym się poniżej określić folder współdzielony, w którym umieszczane będą pobrane uaktualnienia (patrz rys. 34). Ścieżkę dostępu można wprowadzić ręcznie lub wskazać ją w oknie, które zostanie otwarte po kliknięciu przycisku **Przeglądaj**. Jeżeli pole to jest zaznaczone, uaktualnienia zostaną automatycznie skopiowane do tego foldera po ich pobraniu.



Rysunek 34. Ustawienia narzędzia kopiowania uaktualnień

Możliwe jest także określenie metody współdzielenia uaktualnień:

- *całkowita*, która pozwala na pobieranie sygnatur zagrożeń i aktualizacji składników dla wszystkich produktów Kaspersky Lab z linii 6.0. W celu wybrania pełnej aktualizacji należy zaznaczyć pole **Pobierz uaktualnienia dla wszystkich składników**.
- *niestandardowe*, które pozwala na pobieranie sygnatur zagrożeń i aktualizacji tylko dla zainstalowanych składników programu Kaspersky Anti-Virus 6.0. W tym wypadku należy usunąć zaznaczenie z pola **Kopiuje uaktualnienia dla wszystkich składników**.

Jeżeli inne komputery sieciowe mają pobierać aktualizacje z foldera, który zawiera aktualizacje pobrane z Internetu, należy podjąć następujące czynności:

1. Udzielić dostępu do tego foldera współdzielonego dla użytkowników zdalnych.
2. Wskazać ten folder współdzielony jako źródło uaktualnień na komputerach sieci lokalnej.

10.4.5. Działania podejmowane po zakończeniu aktualizacji

Każda aktualizacja sygnatur zagrożeń zawiera nowe elementy zapewniające ochronę komputera przed najnowszymi zagrożeniami.

Firma Kaspersky Lab zaleca *wykonywanie skanowania obiektów poddanych kwarantannie* oraz *obiektów startowych* po każdej aktualizacji bazy danych.

Dlaczego te obiekty powinny być skanowane?

Folder kwarantanny zawiera obiekty, które zostały oznaczone przez program jako podejrzane lub prawdopodobnie zainfekowane (patrz rozdział 11.1 na stronie 116). Przy użyciu najnowszej wersji sygnatur zagrożeń, program Kaspersky Anti-Virus for Windows Servers może dokonać identyfikacji zagrożenia oraz zneutralizować je.

Domyślnie, aplikacja skanuje obiekty poddane kwarantannie po każdej aktualizacji sygnatur zagrożeń. Zalecane jest również okresowe przeglądanie obiektów poddanych kwarantannie, ponieważ ich stan może ulec zmianie po wykonaniu wielu skanowań. Możliwe może być przywrócenie niektórych tego typu obiektów do poprzedniej lokalizacji oraz kontynuowanie pracy z nimi.

W celu wyłączenia skanowania obiektów poddanych kwarantannie należy usunąć zaznaczenie z pola **Przeskanuj kwarantannę** znajdującego się w sekcji **Działanie wykonywane po aktualizacji**.

Obiekty startowe są krytyczne dla bezpieczeństwa komputera. Jeżeli jeden z nich będzie zainfekowany, może uniemożliwić załadowanie systemu operacyjnego. Kaspersky Anti-Virus for Windows Servers posiada wbudowane zadanie skanowania obiektów startowych (patrz Rozdział 8. na stronie 82). Zalecane jest utworzenie terminarza uruchamiania tego zadania w celu jego automatycznego uruchamiania po każdej aktualizacji sygnatur zagrożeń (patrz rozdział 6.5 na stronie 64).

ROZDZIAŁ 11. OPCJE ZAAWANSOWANE

Kaspersky Anti-Virus for Windows Servers posiada również inne funkcje rozszerzające jego funkcjonalność.

Program zapisuje niektóre obiekty w specjalnych obszarach, gwarantując tym samym maksymalną ochronę danych.

Kopia zapasowa zawiera kopie obiektów zmienionych lub usuniętych przez program Kaspersky Anti-Virus for Windows Servers (patrz rozdział 11.2 na stronie 119). Jeżeli dowolny obiekt zawiera ważne dla użytkownika informacje oraz gdy nie można w pełni go naprawić podczas przetwarzania antywirusowego, można przywrócić obiekt z foldera kopii zapasowej.

Kwarantanna zawiera potencjalnie zainfekowane obiekty, które nie mogły zostać przetworzone przy użyciu bieżących sygnatur zagrożeń (patrz rozdział 11.1 na stronie 116).

Zalecane jest regularne badanie listy przechowywanych obiektów. Niektóre z nich mogą być przeterminowane, natomiast niektóre mogą zostać przywrócone.

Zaawansowane opcje zawierają wiele użytecznych funkcji. Na przykład:

Pomoc techniczna zapewnia wszechstronną pomoc dla programu Kaspersky Anti-Virus for Windows Servers (patrz rozdział 11.5 na stronie 131). Firma Kaspersky Lab oferuje wiele kanałów pomocy: pomoc on-line, forum użytkowników, itp.

Funkcja powiadamiania służy do powiadamiania użytkownika o kluczowych operacjach i stanach programu Kaspersky Anti-Virus for Windows Servers (patrz rozdział 11.8.1 na stronie 137). Mogą nimi być zdarzenia o naturze informacyjnej lub błędy krytyczne, które należy natychmiast wyeliminować.

Funkcja autoochrony chroni pliki programu przed modyfikacją lub ich uszkodzeniem przez hakerów, blokuje zdalne zarządzanie funkcjami programu oraz narzuca ograniczenia w wykonywaniu określonych działań w programie Kaspersky Anti-Virus for Windows Servers przez innych użytkowników korzystających z komputera (patrz rozdział 11.8.1.3 na stronie 141). Na przykład: zmiana poziomu ochrony może wpłynąć na bezpieczeństwo danych zapisanych na komputerze.

Menedżer kluczy licencyjnych umożliwia uzyskanie szczegółowych informacji dotyczących licencji, aktywację kopii programu i zarządzanie kluczami licencyjnymi.

Program oferuje również wbudowaną pomoc (patrz rozdział 11.4 na stronie 130) oraz szczegółowe raporty (patrz rozdział 11.3 na stronie 122) z funkcjonowania wszystkich składników ochrony oraz zadań skanowania antywirusowego.

Istnieje również możliwość zmiany wyglądu programu Kaspersky Anti-Virus for Windows Servers oraz dostosowywanie interfejsu programu (patrz rozdział 11.7 na stronie 134).

Niniejsza sekcja zawiera szczegółowe informacje dotyczące tych funkcji.

11.1. Kwarantanna dla potencjalnie zainfekowanych obiektów

Kwarantanna jest specjalnym obszarem, w którym umieszczane są potencjalnie zainfekowane obiekty.

Potencjalnie zainfekowane obiekty są obiektami podejrzanymi o infekcję wirusem lub modyfikacją wirusa.

Dlaczego potencjalnie zainfekowany? Nie zawsze jednoznacznie można określić czy obiekt jest zainfekowany. Spowodowane to może być wieloma przyczynami:

Kod skanowanego obiektu przypomina znane zagrożenie, lecz jest ono częściowo zmodyfikowane.

Sygnatury zagrożeń zawierają zagrożenia, które zostały już zbadane przez firmę Kaspersky Lab. Jeżeli szkodliwy program jest zmodyfikowany, a zmiany nie zostały jeszcze umieszczone w sygnaturach, Kaspersky Anti-Virus for Windows Servers sklasyfikuje obiekt zainfekowany zmodyfikowanym szkodliwym programem jako potencjalnie zainfekowany oraz wskazywał będzie zagrożenie podobne do tej infekcji.

Kod wykrytego obiektu przypomina strukturę szkodliwego programu. Jednakże, sygnatury zagrożeń nie zawierają podobnej struktury.

Istnieje duże prawdopodobieństwo, że jest to nowy typ zagrożenia, tak więc Kaspersky Anti-Virus for Windows Servers sklasyfikuje obiekt jako potencjalnie zainfekowany.

Heurystyczny analizator kodu wykrywa potencjalne wirusy, identyfikując aż do 92% nowych wirusów. Ten mechanizm jest dość efektywny i bardzo rzadko generuje błąd w identyfikacji.

Potencjalnie zainfekowany obiekt może zostać wykryty i umieszczony w folderze kwarantanny przez moduł Ochrony plików lub podczas skanowania antywirusowego.

Możliwe jest umieszczenie obiektu w kwarantannie klikając przycisk **Podдай kwarantannie** znajdujący się w oknie powiadomień wyświetlanym po wykryciu potencjalnie zainfekowanego obiektu.

Obiekty są przenoszone do kwarantanny, a nie kopiowane. Obiekt jest usuwany z dysku lub wiadomości pocztowej i zapisywany w folderze kwarantanny. Pliki w folderze kwarantanny zapisywane są w specjalnym formacie i nie stanowią zagrożenia.

11.1.1. Akcje podejmowane na obiektach poddanych kwarantannie

Całkowita liczba obiektów zapisanych w kwarantannie wyświetlana jest po kliknięciu odsyłacza **Pliki danych** znajdującego się w sekcji **Usługi** okna głównego aplikacji. W prawej części okna znajduje się specjalna sekcja **Kwarantanna** wyświetlająca:

liczbę potencjalnie zainfekowanych obiektów wykrytych podczas funkcjonowania programu Kaspersky Anti-Virus for Windows Servers;

bieżący rozmiar foldera kwarantanny.

Możliwe jest usunięcie wszystkich obiektów znajdujących się w folderze kwarantanny przy użyciu przycisku **Wyczyść**. Należy pamiętać o tym, że kopie zapasowe obiektów oraz raporty również zostaną usunięte.

W celu uzyskania dostępu do obiektów zapisanych w Kwarantannie należy:

klikać lewym przyciskiem myszy w obrębie sekcji **Kwarantanna**.

Na zakładce **Kwarantanna** można wykonywać następujące działania (patrz rys. 35):

Przenieść do kwarantanny plik podejrzany o infekcję, który nie jest wykrywany przez program. W tym celu, należy kliknąć przycisk **Dodaj** i w oknie wyboru plików wskazać żądany plik. Plik zostanie dodany do listy i zawierał będzie stan *dodany przez użytkownika*.

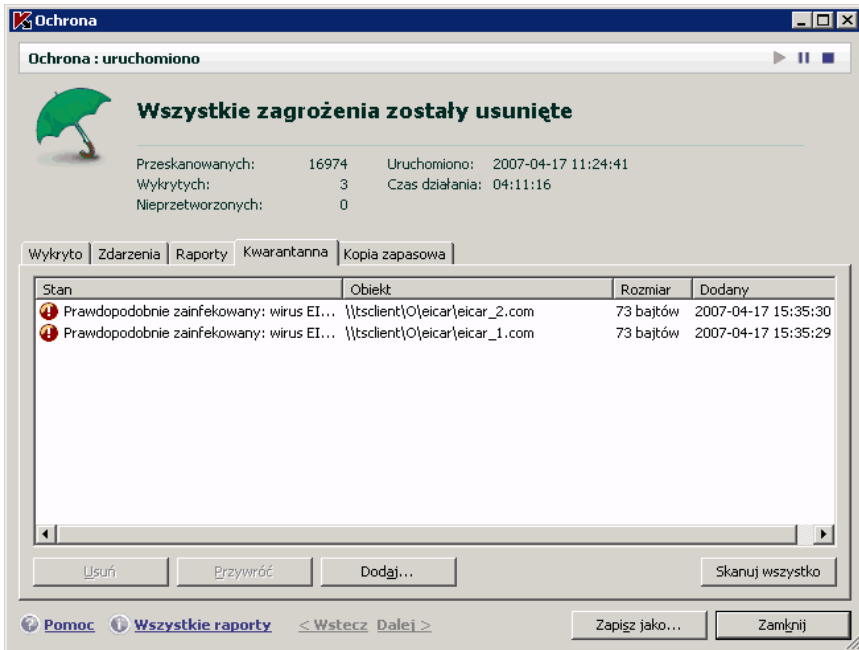
Skanować i leczyć wszystkie potencjalnie zainfekowane obiekty znajdujące się w kwarantannie przy użyciu bieżących sygnatur zagrożeń. W tym celu należy kliknąć przycisk **Skanuj wszystko**.

Po zakończeniu skanowania i leczenia dowolnego obiektu znajdującego się w kwarantannie, jego stan może ulec zmianie na zainfekowany, potencjalnie zainfekowany, fałszywy alarm, OK itp.

Stan zainfekowany oznacza, że obiekt został zidentyfikowany jako zainfekowany lecz nie mógł zostać wyleczony. Zalecane jest usuwanie tego typu obiektów.

Wszystkie obiekty oznaczone jako *falszywy alarm* mogą zostać przywrócone, ponieważ ich poprzedni stan *potencjalnie zainfekowany* nie został potwierdzony przez program po ponownym przeskanowaniu.

Przywracać pliki do foldera wybranego przez użytkownika lub do ich oryginalnego foldera, przed tym jak zostały one przeniesione do kwarantanny (domyślnie). W celu przywrócenia obiektu, należy wybrać go z listy i kliknąć przycisk **Przywróć**. Podczas przywracania obiektów z archiwów, pocztowych baz danych oraz plików poczty elektronicznej umieszczonych w kwarantannie, należy również wskazać folder do którego zostaną one przywrócone.



Rysunek 35. Lista obiektów poddanych kwarantannie

Wskazówka:

Zalecane jest przywracanie jedynie obiektów posiadających stan *falszywy alarm*, *OK* i *wyleczony*, ponieważ przywracanie innych obiektów może spowodować infekcję komputera.

Usuwać dowolne obiekty lub grupy wybranych obiektów umieszczonych w kwarantannie. Obiekty, których nie można wyleczyć można jedynie usunąć. W celu usunięcia obiektów, należy zaznaczyć je na liście i kliknąć przycisk **Usuń**.

11.1.2. Konfiguracja kwarantanny

Możliwe jest konfigurowanie ustawień kwarantanny:

Definiowanie automatycznego skanowania obiektów zapisanych w kwarantannie po każdej aktualizacji sygnatur zagrożeń (patrz rozdział 10.4.4 na stronie 112).

Uwaga!

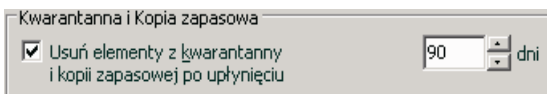
Nie będzie możliwe natychmiastowe wykonanie skanowania obiektów umieszczonych w kwarantannie po aktualizacji sygnatur zagrożeń jeżeli użytkownik pracuje z folderem kwarantanny.

Definiowanie maksymalnego czasu przechowywania obiektów w kwarantannie.

Domyślnym czasem przechowywania obiektów w kwarantannie jest 30 dni. Po upływie tego czasu obiekty są usuwane. Można zmienić czas przechowywania obiektów w kwarantannie lub wyłączyć to ograniczenie.

W tym celu należy:

1. Otworzyć okno ustawień programu Kaspersky Anti-Virus for Windows Servers przez kliknięcie odsyłacza Ustawienia znajdującego się w oknie głównym programu.
2. W drzewie ustawień kliknąć odsyłacz **Pliki danych**.
3. W sekcji **Kwarantanna i Kopia zapasowa** (patrz rys. 36), należy podać czas po upływie którego obiekty w folderze kwarantanny i kopii zapasowej będą automatycznie usuwane. Aby wyłączyć automatyczne usuwanie plików należy usunąć zaznaczenie z opcji.



Rysunek 36. Konfiguracja okresu przechowywania obiektów w kwarantannie

11.2. Kopie zapasowe niebezpiecznych obiektów

W niektórych przypadkach po wyleczeniu obiektów utracona zostaje ich integralność. Jeżeli wyleczony plik zawiera ważne informacje i po zakończeniu leczenia jest on częściowo lub w pełni uszkodzony, można podjąć próbę przywrócenia oryginalnego obiektu z kopii zapasowej.

Kopia zapasowa jest kopią oryginalnego niebezpiecznego obiektu tworzoną podczas leczenia lub usuwania obiektu. Zapisywana jest ona w folderze kopii zapasowej.

Folder kopii zapasowej jest specjalnym obszarem zawierającym kopie zapasowe niebezpiecznych obiektów. Pliki kopii zapasowej zapisywane są w specjalnym formacie i nie stanowią zagrożenia.

11.2.1. Akcje podejmowane na kopiach zapasowych obiektów

Całkowita liczba kopii zapasowych obiektów wyświetlana jest po kliknięciu odsyłacza **Pliki danych** znajdującego się w sekcji **Usługi** głównego okna. W prawej części okna znajduje się specjalne pole Kopia zapasowa wyświetlające:

liczbę kopii zapasowych obiektów utworzonych przez program Kaspersky Anti-Virus for Windows Servers

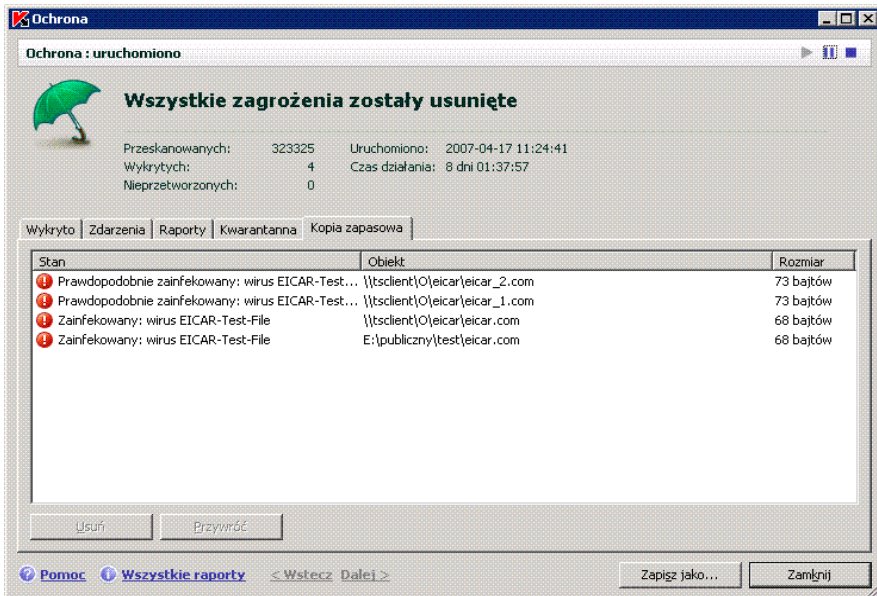
bieżący rozmiar foldera kopii zapasowej.

Możliwe jest usunięcie wszystkich kopii zapasowych obiektów przy użyciu przycisku **Wyczyść**. Należy pamiętać o tym, że obiekty poddane kwarantannie oraz raporty również zostaną usunięte.

W celu uzyskania dostępu do kopii niebezpiecznych obiektów należy:

kliknąć lewym przyciskiem myszy w obrębie pola **Kopia zapasowa**.

Lista kopii zapasowych wyświetlana jest na zakładce **Kopia zapasowa** (patrz rys. 37). Dla każdej z kopii wyświetlane są następujące informacje: pełna nazwa obiektu wraz ze ścieżką dostępu do oryginalnej lokalizacji, stan obiektu przydzielony podczas skanowania oraz jego rozmiar.



Rysunek 37. Kopie zapasowe usuniętych lub wyleczonych obiektów

Można przywracać wybrane kopie przy użyciu przycisku **Przywróć**. Obiekt przywracany z kopii zapasowej posiada tę samą nazwę jak przed jego leczeniem.

Jeżeli w oryginalnej lokalizacji znajduje się obiekt o tej samej nazwie (jest to możliwe gdy utworzona została kopia przywracanego obiektu przed jego leczeniem), wyświetlone zostanie ostrzeżenie. Można zmienić lokalizację przywracanego obiektu lub jego nazwę.

Zalecane jest wykonanie skanowania obiektów zaraz po ich przywróceniu. Istnieje możliwość wyleczenia obiektu przy użyciu aktualnych sygnatur zagrożeń bez utraty jego integralności.

Nie zaleca się przywracania kopii zapasowych obiektów jeżeli nie jest to absolutnie konieczne. Może to doprowadzić do zainfekowania komputera.

Zalecane jest regularne badanie foldera kopii zapasowej i jego opróżnianie przy użyciu przycisku **Usuń**. Można również skonfigurować program do automatycznego usuwania najstarszych kopii (patrz rozdział 11.2.2 na stronie 122).

11.2.2. Konfiguracja kopii zapasowych

Możliwe jest zdefiniowanie maksymalnego czasu przechowywania obiektów w folderze kopii zapasowej.

Domyślnym czasem przechowywania obiektów w kopii zapasowej jest 90 dni. Po upływie tego czasu kopie są usuwane. Można zmienić czas przechowywania kopii lub wyłączyć to ograniczenie. W tym celu należy:

1. Otworzyć okno ustawień programu Kaspersky Anti-Virus for Windows Servers przez kliknięcie odsyłacza Ustawienia znajdującego się w oknie głównym programu.
2. W drzewie ustawień kliknąć odsyłacz **Pliki danych**.
3. W sekcji **Kwarantanna i Kopia zapasowa** (patrz rys. 36) należy podać czas po upłynięciu którego, obiekty w kwarantannie i kopii zapasowej będą automatycznie usuwane. Aby wyłączyć automatyczne usuwanie plików należy usunąć zaznaczenie z opcji.

11.3. Raporty

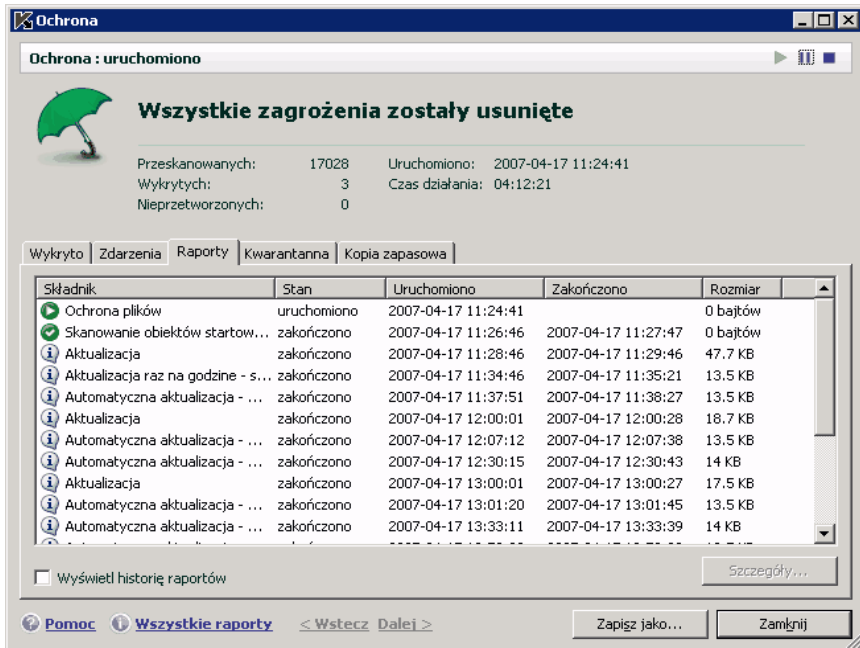
Akcje wykonywane przez składniki programu Kaspersky Anti-Virus for Windows Servers oraz zadania skanowania antywirusowego i aktualizacji zapisywane są w raportach.

Całkowita liczba raportów utworzonych przez program i ich rozmiar wyświetlany jest po kliknięciu odsyłacza **Pliki danych** znajdującego się w sekcji **Usługi** w oknie głównym programu. Informacje te wyświetlane są w polu *Raporty*.

W celu wyświetlenia raportów należy:

Kliknąć lewym przyciskiem myszy w sekcji *Raporty*. Spowoduje to otwarcie okna *Ochrona*, w którym wyświetlany jest stan ochrony komputera. Otwarte zostanie okno na zakładce **Raporty** (patrz rys. 38).

Na zakładce Raporty wyświetlana jest lista raportów utworzonych przez moduł Ochrona plików oraz zadania skanowania antywirusowego i aktualizacji uruchomione podczas bieżącej sesji Kaspersky Anti-Virus for Windows Servers. Przy nazwie każdego składnika lub zadania wyświetlany jest jego stan (na przykład, *zatrzymano* lub *zakończono*). W celu wyświetlenia pełnej historii tworzenia raportu dla bieżącej sesji programu, należy zaznaczyć opcję **Wyświetl historię raportów**.



Rysunek 38. Raporty z funkcjonowania programu

W celu wyświetlenia wszystkich zapisanych zdarzeń dla modułu Ochrona plików lub zadania należy:

wybrać nazwę składnika lub zadania na zakładce **Raporty** i kliknąć przycisk **Szczegóły**.

Wyświetlone zostanie okno zawierające szczegółowe informacje dotyczące działania żądanego składnika lub zadania. Statystyki wyświetlane są w górnej części okna, natomiast informacje szczegółowe znajdują się na zakładkach.

Na zakładce **Zagrożenia** wyświetlana jest lista niebezpiecznych obiektów wykrytych przez moduł Ochrona plików lub zadanie skanowania antywirusowego.

Na zakładce **Zdarzenia** wyświetlane są zdarzenia generowane przez składnik lub zadanie.

Na zakładce **Statystyki** wyświetlane są szczegółowe statystyki dla wszystkich skanowanych obiektów.

Na zakładce **Ustawienia** wyświetlane są ustawienia używane przez moduł Ochrona plików, zadanie skanowania antywirusowego lub aktualizacje sygnatur zagrożeń.

Na zakładce **Zablokowani użytkownicy** wyświetlana jest lista użytkowników, którzy próbowali skopiować na serwer podejrzany lub zainfekowany plik.

Możliwe jest wyeksportowanie do pliku tekstowego wszystkich raportów. Funkcja ta jest użyteczna w przypadku wystąpienia błędu, którego użytkownik sam nie może rozwiązać i konieczne jest skontaktowanie się z działem pomocy technicznej firmy Kaspersky Lab. Po wystąpieniu tego typu sytuacji, należy wysłać raport w postaci pliku tekstowego do działu pomocy technicznej celem rozwiązania problemu przez ekspertów z firmy Kaspersky Lab.

W celu wyeksportowania raportu do pliku tekstowego należy:

kliknąć przycisk **Zapisz jako** oraz określić lokalizację w której zapisany ma zostać plik raportu.

Po zakończeniu operacji, należy kliknąć przycisk **Zamknij**.

Wszystkie zakładki za wyjątkiem zakładek **Ustawienia** i **Statystyki** posiadają przycisk **Akcje**, który można użyć do definiowania odpowiedzi dla obiektów z listy. Po kliknięciu tego przycisku otwarte zostanie menu kontekstowe zawierające następujące elementy (zawartość menu jest różna w zależności od składnika - wszystkie możliwe opcje znajdują się poniżej):

Wylecz – próba wyleczenia niebezpiecznego obiektu. Jeżeli obiekt nie zostanie pomyślnie wyleczony, można pozostawić go na liście w celu ponownego przeskanowania po aktualizacji sygnatur zagrożeń lub go usunąć. Akcję można zastosować dla jednego lub kilku wybranych obiektów z listy.

Pomiń – usunięcie wpisu raportu informującego o wykryciu obiektu.

Dodaj do zaufanej strefy – wykluczenie obiektu z ochrony. Otwarte zostanie okno zawierające regułę wykluczeń dla obiektu.

Idź do pliku – otwarcie foldera, w którym znajduje się obiekt.

Wylecz wszystkie – neutralizacja wszystkich obiektów znajdujących się na liście. Kaspersky Anti-Virus for Windows Servers podejmie próbę przetworzenia obiektów przy użyciu sygnatur zagrożeń.

Pomiń wszystkie – usunięcie raportów na temat wykrytych obiektów. Użycie tej funkcji, spowoduje pozostawienie na komputerze wszystkich wykrytych niebezpiecznych obiektów.

Przeszukaj www.viruslist.pl – wyświetlenie opisu obiektu znajdującego się w encyklopedii wirusów na stronie firmy Kaspersky Lab.

Przeszukaj www.google.pl – wyszukanie informacji o obiekcie przy użyciu wyszukiwarki.

Znajdź – wyszukanie obiektów na liście według nazwy lub stanu.

Ponadto, możliwe jest sortowanie w porządku malejącym lub rosnącym wyświetlanych w oknie informacji dla każdej z kolumn. W tym celu należy kliknąć nagłówki kolumny.

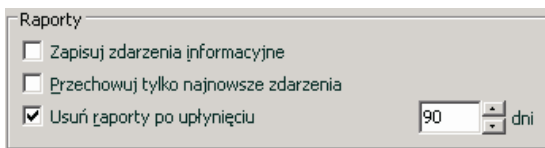
Niebezpieczne obiekty wykryte przez Kaspersky Anti-Virus mogą być przetwarzane przy użyciu przycisku **Neutralizuj** (w celu przetworzenia jednego obiektu lub zaznaczonej grupy obiektów) lub **Neutralizuj wszystkie** (w celu przetworzenia wszystkich obiektów znajdujących się na liście). Podczas przetwarzania każdego z obiektów wyświetlone zostanie okno, w którym będzie można wybrać akcję jaka będzie miała zostać podjęta na wykrytym obiekcie.

Po zaznaczeniu opcji **Zastosuj do wszystkich** znajdującej się w oknie powiadomienia, wybrana akcja będzie stosowana dla wszystkich obiektów o tym samym statusie, wybranych z listy przed rozpoczęciem przetwarzania.

11.3.1. Konfiguracja ustawień raportów

W celu konfiguracji ustawień tworzenia i zapisywania raportów należy:

1. Otworzyć okno ustawień programu Kaspersky Anti-Virus for Windows Servers przez kliknięcie odsyłacza Ustawienia znajdującego się w oknie głównym programu.
2. W drzewie ustawień kliknąć odsyłacz **Pliki danych**.
3. W sekcji **Raporty** dokonać następującej konfiguracji (patrz rys. 39):
 - Włączyć lub wyłączyć zapisywanie zdarzeń informacyjnych. Powiadomienia informacyjne nie są istotne dla ochrony komputera. W celu zapisywania zdarzeń należy zaznaczyć opcję **Zapisuj zdarzenia informacyjne**;
 - Wybrać zapisywanie tylko tych zdarzeń, które wystąpiły od czasu ostatniego uruchomienia zadania. Ustawienie to zapewnia mniejsze użycie miejsca na dysku. Jeżeli zaznaczona została opcja **Przechowuj tylko najnowsze zdarzenia**, informacje zawarte w raporcie będą uaktualniane po każdym ponownym uruchomieniu zadania. Zastępowane są wyłącznie informacje nie posiadające priorytetu krytycznego.
 - Określić czas przechowywania raportów. Domyślnie raporty przechowywane są przez 90 dni, następnie są one usuwane. Można zmienić czas przechowywania raportów lub usunąć ograniczenie.

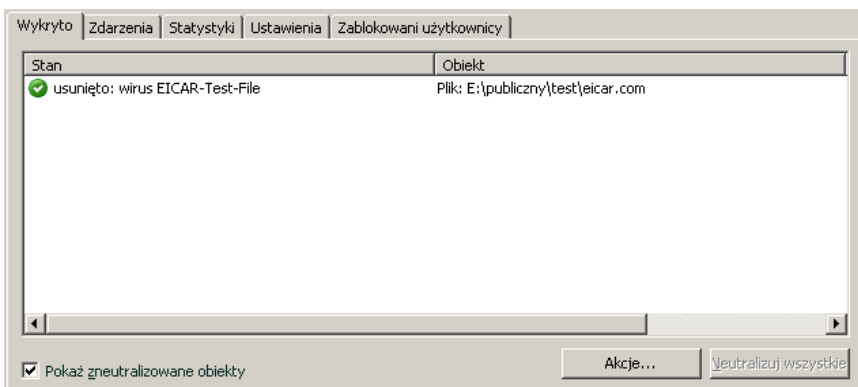


Rysunek 39. Konfiguracja ustawień raportów

11.3.2. Zakładka *Wykryto*

Na tej zakładce (patrz rys. 40) wyświetlana jest lista niebezpiecznych obiektów wykrytych przez Kaspersky Anti-Virus for Windows Servers. Dla każdego obiektu wyświetlana jest jego pełna nazwa wraz z przydzielonym przez program podczas skanowania lub przetwarzania stanem.

Jeżeli lista ma zawierać zarówno niebezpieczne jak i pomyślnie zneutralizowane obiekty, należy zaznaczyć opcję **Pokaż zneutralizowane obiekty**.



Rysunek 40. Lista wykrytych niebezpiecznych obiektów

Niebezpieczne obiekty wykryte przez Kaspersky Anti-Virus mogą być przetwarzane przy użyciu przycisku **Przetwórz** (w celu przetworzenia jednego obiektu lub zaznaczonej grupy obiektów) lub **Przetwórz wszystko** (w celu przetworzenia wszystkich obiektów znajdujących się na liście). Podczas przetwarzania każdego z obiektów wyświetlone zostanie okno, w którym będzie można wybrać akcję jaka będzie miała zostać podjęta na wykrytym obiekcie.

Po zaznaczeniu opcji **Zastosuj do wszystkich** znajdującej się w oknie powiadomienia, wybrana akcja będzie stosowana dla wszystkich obiektów o tym samym statusie, wybranych z listy przed rozpoczęciem przetwarzania.

11.3.3. Zakładka *Zdarzenia*

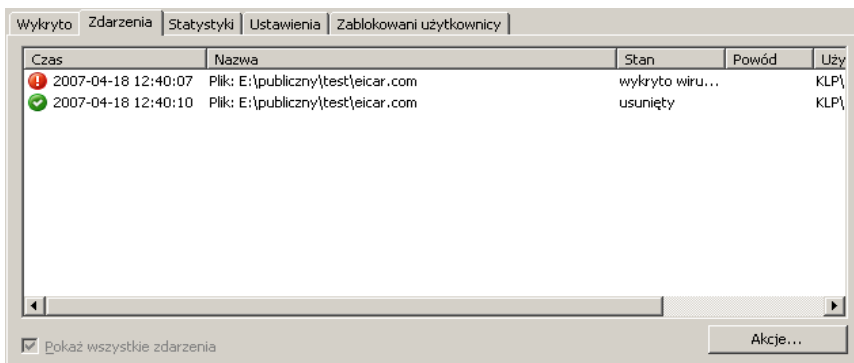
Na tej zakładce (patrz rys. 41) wyświetlana jest lista wszystkich ważnych zdarzeń dotyczących funkcjonowania modułu Ochrona plików, zadań skanowania antywirusowego oraz uaktualnień sygnatur zagrożeń.

Dostępne zdarzenia:

Krytyczne zdarzenia są to zdarzenia krytyczne będące źródłem problemów w funkcjonowaniu programu lub luk występujących na komputerze. Na przykład: *wykryto wirusa, błąd w działaniu*.

Ważne zdarzenia są to zdarzenia które muszą zostać zbadane, ponieważ odnoszą się do ważnych sytuacji w funkcjonowaniu programu. Na przykład: *zatrzymano*.

Komunikaty informacyjne są to wiadomości informacyjne, które zwykle nie zawierają ważnych informacji. Na przykład: *OK, nieprzetworzony*. Zdarzenia te zapisywane są, jeżeli zaznaczona została opcja **Pokaż wszystkie zdarzenia**.



Rysunek 41. Zdarzenia wygenerowane przez składnik

Format wyświetlanych zdarzeń może się różnić w zależności od składnika lub zadania. Dla zadań aktualizacji dostępne są następujące informacje:

Nazwa zdarzenia

Nazwa obiektu związanego ze zdarzeniem

Data i czas wystąpienia zdarzenia

Rozmiar załadowanego pliku

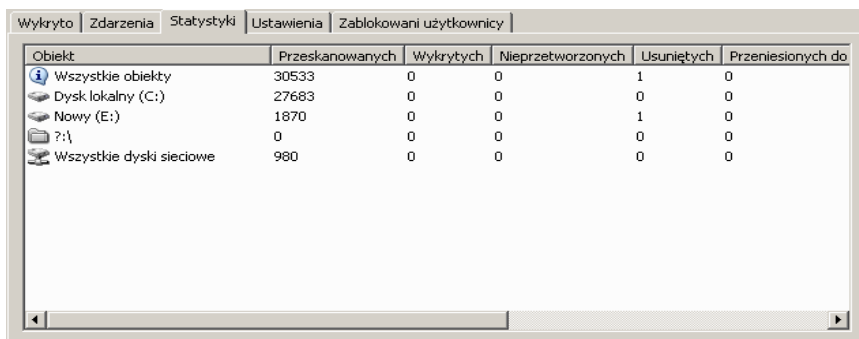
Dla zadań skanowania antywirusowego zdarzenia zawierają nazwę skanowanego obiektu oraz stan przydzielony do obiektu podczas skanowania/przetwarzania.

11.3.4. Zakładka *Statystyki*

Na tej zakładce (patrz rys. 42) wyświetlane są zawiera szczegółowe statystyki dotyczące funkcjonowania modułu ochrona plików oraz zadań skanowania antywirusowego. Znajdują się tu informacje dotyczące:

Liczby obiektów, które zostały przeskanowane w poszukiwaniu zagrożeń podczas trwania bieżącej sesji modułu Ochrona plików lub po zakończeniu wykonywania zadania skanowania. Wyświetlana jest liczba przeskanowanych archiwów, skompresowanych plików oraz zabezpieczonych hasłem i uszkodzonych obiektów.

Liczby wykrytych niebezpiecznych obiektów, obiektów nie wyleczonych, obiektów usuniętych i umieszczonych w folderze kwarantanny.



Obiekt	Przeskanowanych	Wykrytych	Nieprzetworzonych	Usuniętych	Przeniesionych do
Wszystkie obiekty	30533	0	0	1	0
Dysk lokalny (C:)	27683	0	0	0	0
Nowy (E:)	1870	0	0	1	0
?:\	0	0	0	0	0
Wszystkie dyski sieciowe	980	0	0	0	0

Rysunek 42. Statystyki składnika

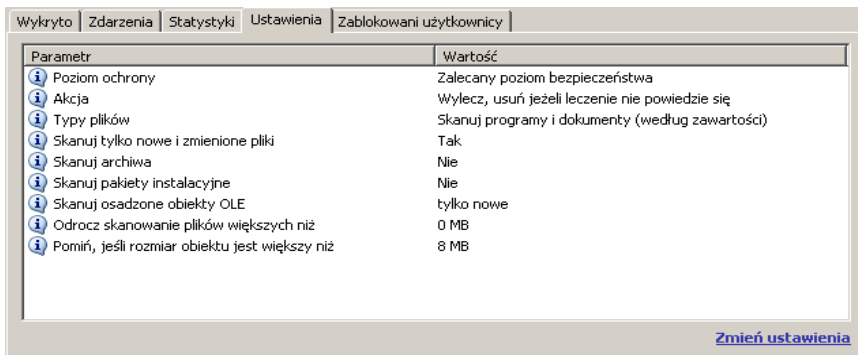
11.3.5. Zakładka *Ustawienia*

Na zakładce **Ustawienia** (patrz rys. 43) wyświetlane są informacje dotyczące ustawień modułu Ochrona plików oraz zadań skanowania antywirusowego i aktualizacji programu. Na tej zakładce można znaleźć informacje dotyczące poziomu bezpieczeństwa dla modułu Ochrona plików lub zadań skanowania antywirusowego, rodzaju akcji podejmowanych po wykryciu niebezpiecznych obiektów lub ustawień używanych podczas pobierania uaktualnień. W celu konfiguracji składnika należy użyć odsyłacza Modyfikuj ustawienia.

W tym oknie można skonfigurować zaawansowane ustawienia skanowania:

Ustalanie priorytetu zadań skanowania wykorzystywanego gdy procesor jest obciążony. Opcja **Współdziel zasoby z innymi aplikacjami** jest domyślnie zaznaczona. Po zaznaczeniu tej opcji, program śledzi obciążenie procesora oraz dysków twardych pod kątem aktywności innych aplikacji. Jeżeli obciążenie

procesora zostanie wyraźnie zwiększone uniemożliwiając poprawne funkcjonowanie aplikacjom użytkownika, program zredukuje aktywność skanowania. Spowoduje to zwiększenie czasu skanowania oraz zwolnienie zasobów dla aplikacji użytkownika.



Rysunek 43. Ustawienia składnika

Definiowanie trybu pracy komputera po zakończeniu procesu skanowania. Można wybrać wyłączenie komputera, ponowne uruchomienie lub przejście w stan wstrzymania lub hibernacji. W celu wybrania tej opcji, należy kliknąć odsyłacz lewym przyciskiem myszy, aż do uzyskania żądanej opcji.

11.3.6. Zakładka **Zablokowani użytkownicy**

Każdy komputer, który podejmuje próbę skopiowania zainfekowanego lub podejrzanego pliku na serwer zostanie zablokowany. Zablokowanie komputera może być także stosowane dla akcji związanych z przetwarzaniem pliku (leczenie lub usuwanie).

Na tej zakładce wyświetlane lista zablokowanych komputerów zawierająca informacje o dacie i czasie ich zablokowania oraz czasie, który pozostał do ich odblokowania.

Wykryto Zdarzenia Statystyki Ustawienia Zablokowani użytkownicy				
Czas	Użytkownik	Komputer	Pozostało	
2007-04-18 12:40:10	SERWER\Gość	192.168.0.60	01:48:52	

Rysunek 44. Lista zablokowanych użytkowników

11.4. Informacje ogólne o programie

Ogólne informacje o programie dostępne są z poziomu sekcji **Usługi** znajdującej się w oknie głównym programu (patrz rys. 45).

Rysunek 45. Informacje o programie, licencji oraz systemie operacyjnym

Wszystkie informacje podzielone są na trzy sekcje:

Wersja programu, data ostatniej aktualizacji oraz liczba znanych zagrożeń wyświetlana jest w polu **Informacje o produkcie**.

Podstawowe informacje dotyczące systemu operacyjnego znajdują się w polu **Informacje o systemie**.

Podstawowe informacje dotyczące licencji dla programu Kaspersky Anti-Virus znajdują się w polu **Informacje o licencji**.

Wszystkie wyżej wymienione informacje niezbędne są podczas kontaktu z działem pomocy technicznej firmy Kaspersky Lab (patrz rozdział 11.5 na stronie 131).

11.5. Zarządzanie licencjami

Do prawidłowego funkcjonowania programu Kaspersky Anti-Virus for Windows Servers niezbędny jest *klucz licencyjny*. Po zakupie programu użytkownik otrzymuje klucz umożliwiający korzystanie z programu od dnia jego pierwszej instalacji.

Jeżeli komercyjny klucz licencyjny nie zostanie zainstalowany lub użytkownik nie aktywuje wersji trzydziestodniowej, Kaspersky Anti-Virus pobierze uaktualnienia tylko raz. Program nie będzie pobierał żadnych nowych uaktualnień.

Jeżeli aktywowano wersję trzydziestodniową, po upływie tego okresu Kaspersky Anti-Virus przestanie się uruchamiać.

Po wygaśnięciu komercyjnego klucza licencyjnego program będzie kontynuował działanie, ale nie będzie pobierał nowych uaktualnień sygnatur zagrożeń. Możliwe będzie wykonywanie skanowania oraz używanie składników ochrony przy wykorzystaniu sygnatur zagrożeń pobranych przed wygaśnięciem okresu licencjonowania. Firma Kaspersky Lab nie może zagwarantować ochrony komputera przed wirusami, które pojawią się po wygaśnięciu klucza licencyjnego.

W celu uniknięcia infekcji komputera nowymi wirusami zalecane jest przedłużenie okresu licencjonowania programu Kaspersky Anti-Virus for Windows Servers. Na dwa tygodnie przed wygaśnięciem okresu licencjonowania program wyświetlał będzie odpowiednie powiadomienie po każdym uruchomieniu.

Aby odnowić licencję należy zakupić nowy klucz licencyjny. W tym celu należy:

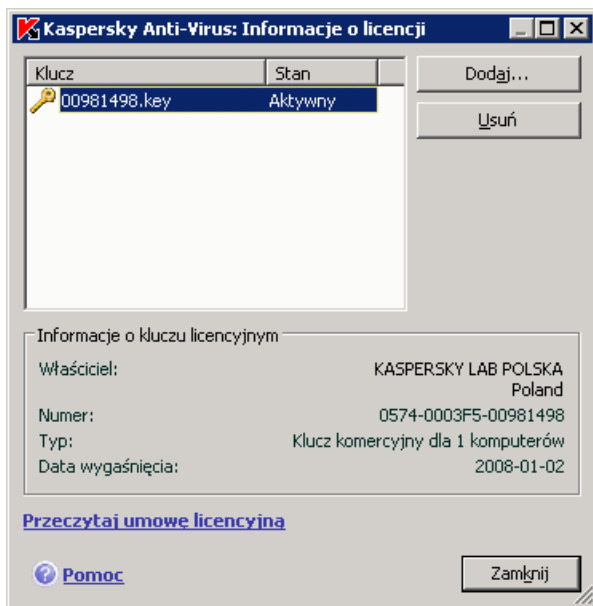
Skontaktować się z dystrybutorem, u którego produkt został zakupiony.

lub:

Zakupić klucz licencyjny bezpośrednio w firmie Kaspersky Lab. W tym celu należy kliknąć odsyłacz Odnów licencję znajdujący się w oknie zarządzania licencjami (patrz rys. 46). Następnie należy wypełnić formularz zamówienia znajdujący się w sklepie internetowym firmy Kaspersky Lab. Po dokonaniu wpłaty, na adres podany w formularzu zamówienia wysłany zostanie klucz licencyjny lub kod aktywacyjny.

Firma Kaspersky Lab oferuje specjalne rabaty dla osób przedłużających licencję.

Informacje o używanym kluczu licencyjnym wyświetlane są w polu **Informacje o licencji** znajdującym się w sekcji **Usługi** okna głównego programu. W celu otwarcia okna menedżera licencji należy kliknąć lewym przyciskiem myszy na tym polu. W oknie, które zostanie wyświetlone (patrz rys. 46), na ekranie można przejrzeć informacje o bieżącym kluczu, dodać lub usunąć klucz.



Rysunek 46. Informacje o licencji

Po zaznaczeniu klucza na liście znajdującej się w oknie **Informacje o licencji**, wyświetlone zostaną informacje o numerze, typie i dacie wygaśnięcia licencji. W celu dodania nowego klucza licencyjnego należy kliknąć **Dodaj** i aktywować aplikację przy użyciu kreatora aktywacji. W celu usunięcia klucza z listy należy użyć przycisku **Usuń**.

W celu przejrzania postanowień umowy licencyjnej należy kliknąć [Przeczytaj umowę licencyjną](#). Aby dokonać zakupu licencji w sklepie internetowym firmy Kaspersky Lab, należy kliknąć [Kup licencję](#).

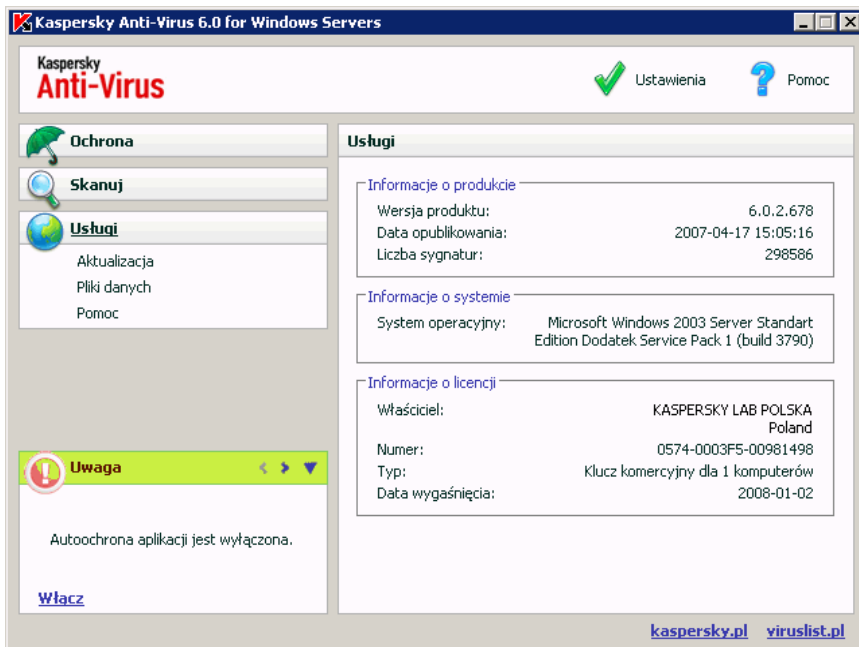
11.6. Pomoc techniczna

Kaspersky Anti-Virus for Windows Servers udostępnia wiele możliwości zgłaszania pytań i problemów związanych z funkcjonowaniem programu. Są one dostępne w sekcji **Pomoc** (patrz rys. 47) sekcji **Usługi** głównego okna.

W zależności od rodzaju problemu, dostępnych jest kilka usług pomocy technicznej:

Forum użytkowników. To źródło jest dedykowaną sekcją witryny firmy Kaspersky Lab zawierającą pytania, komentarze i sugestie użytkowników programu. Użytkownik może przeglądać zawartość forum i publikować własne komentarze. Może on również odnaleźć odpowiedź na pytanie.

W celu uzyskania dostępu forum należy użyć odsyłacza **Forum użytkowników**.



Rysunek 47. Informacje o produkcie

Baza wiedzy. To źródło jest również dedykowaną sekcją witryny firmy Kaspersky Lab i zawiera zalecenia techniczne dotyczące używania oprogramowania firmy Kaspersky Lab oraz odpowiedzi na najczęściej zadawane pytania. Przy użyciu tego źródła należy spróbować znaleźć odpowiedź na pytanie lub rozwiązanie problemu.

W celu uzyskania pomocy technicznej z poziomu witryny Internetowej należy użyć odsyłacza [Baza wiedzy](#).

Komentarze dotyczące funkcjonowania programu. Ta usługa utworzona została w celu wysyłania komentarzy i sugestii dotyczących funkcjonowania programu lub zgłaszania problemów mających miejsce w trakcie funkcjonowania programu. Użytkownik musi wypełnić specjalny formularz znajdujący się na stronie Internetowej firmy w celu szczegółowego opisanie zaistniałej sytuacji. W celu rozwiązania problemu eksperci z firmy Kaspersky Lab muszą uzyskać pewne informacje na temat systemu. Użytkownik może sam opisać cechy systemu lub automatycznie wygenerować informacje przy użyciu odpowiedniego narzędzia.

W celu przejścia do formularza należy użyć odsyłacza [Zgłoś błąd lub sugestię](#).

Pomoc techniczna. Jeżeli niezbędna jest pomoc dla programu Kaspersky Anti-Virus należy kliknąć odsyłacz znajdujący się w polu **Lokalna pomoc techniczna**. Otwarta zostanie strona internetowa, na której znajdują się informacje dotyczące sposobu kontaktu z ekspertami firmy Kaspersky Lab.

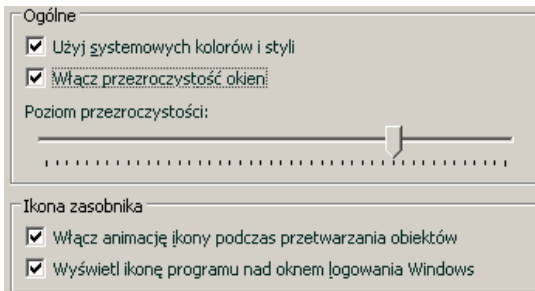
11.7. Konfiguracja interfejsu

Kaspersky Anti-Virus for Windows Servers

Kaspersky Anti-Virus for Windows Servers oferuje opcję modyfikacji wyglądu interfejsu programu przy użyciu skór. Użytkownik może również konfigurować użycie aktywnych elementów interfejsu programu takich jak ikona zasobnika systemowego oraz komunikaty wyskakujące.

W celu konfiguracji interfejsu programu należy:

1. Otworzyć okno ustawień klikając odsyłacz [Ustawienia](#) znajdujący się w oknie głównym programu.
2. W drzewie ustawień programu kliknąć odsyłacz **Wygląd** znajdujący się w sekcji **Usługi** (patrz rys. 48).



Rysunek 48. Konfiguracja ustawień interfejsu programu

W prawej części okna ustawień możliwe jest zdefiniowanie:

Wyświetlania ikony programu Kaspersky Anti-Virus for Windows Servers podczas uruchamiania systemu operacyjnego.

Domyślnie ikona wyświetlana jest w prawym górnym rogu ekranu podczas ładowania programu. Informuje ona o ochronie komputera przed wszystkimi typami zagrożeń. Jeżeli użytkownik nie chce korzystać z tej opcji należy usunąć zaznaczenie z pola **Wyświetl ikonę programu nad oknem logowania Windows**.

Animacji ikony znajdującej się w zasobniku systemowym.

W zależności od wykonywanych operacji wygląd ikony zasobnika systemowego ulega zmianie. Animacja ikony zasobnika systemowego jest domyślnie włączona. W celu wyłączenia animacji ikony zasobnika systemowego należy usunąć zaznaczenie z pola **Włącz animację ikony podczas przetwarzania obiektów**. Po wyłączeniu tej opcji ikona obrazowała będzie jedynie stan ochrony komputera: jeżeli ochrona jest włączona ikona jest czerwona, natomiast gdy ochrona jest wyłączona ikona jest szara.

Stopnia przezroczystości komunikatów wyskakujących.

Wszystkie operacje programu Kaspersky Anti-Virus for Windows Servers wymagające natychmiastowej reakcji użytkownika wyświetlane są przy pomocy komunikatów wyskakujących wyświetlanych nad ikoną zasobnika systemowego. Okna komunikatów wyskakujących są półprzezroczyste i nie kolidują z wykonywanymi przez użytkownika operacjami. Po umieszczeniu kursora na komunikacie okno stanie się w pełni widoczne. Możliwe jest modyfikowanie poziomu przezroczystości tego typu komunikatów wyskakujących. W tym celu należy zmienić położenie suwaka **Poziom przezroczystości** na żądaną pozycję. W celu usunięcia przezroczystości, należy usunąć zaznaczenie z pola **Włącz przezroczystość okien**.

Użycia skór dla interfejsu programu utworzonych przez użytkownika.

Istnieje możliwość zmieniania wszystkich kolorów, czcionek, ikon oraz tekstów używanych w interfejsie programu Kaspersky Anti-Virus for Windows Servers. Użytkownik może tworzyć własne schematy graficzne lub własną lokalizację w innym języku. W celu użycia skóry w polu **Folder zawierający skóry** należy określić folder, w którym zapisane są skóry. W celu wybrania foldera należy użyć przycisku **Przełączaj**.

Domyślnie skóra programu używa systemowych kolorów i stylów. Można je usunąć poprzez usunięcie zaznaczenia z pola **Użyj systemowych kolorów i stylów**. Po usunięciu zaznaczenia z tej opcji użyte zostaną ustawienia zdefiniowane w wybranej skórze.

Ustawienia interfejsu programu Kaspersky Anti-Virus for Windows Servers zdefiniowane przez użytkownika nie zostaną zapisane w przypadku przywrócenia domyślnych ustawień lub dezinstalacji programu.

11.8. Wykorzystywanie zaawansowanych ustawień

Kaspersky Anti-Virus for Windows Servers oferuje następujące zaawansowane funkcje:

Powiadomienia o określonych zdarzeniach, które miały miejsce podczas funkcjonowania programu.

Autoochrona programu Kaspersky Anti-Virus for Windows Servers przed wyłączaniem, usuwaniem lub modyfikowaniem modułów programu oraz ochrona programu za pomocą hasła.

Rozwiązywanie problemów współpracy Kaspersky Anti-Virus z innymi programami.

W celu konfiguracji tych ustawień należy:

1. Otworzyć okno ustawień programu klikając odsyłacz [Ustawienia](#) znajdujący się w jego oknie głównym.
2. W drzewie ustawień wybrać sekcję **Usługi**.

W prawej części okna możliwe jest definiowanie użycia dodatkowych funkcji programu.

11.8.1. Powiadomienia o zdarzeniach generowanych przez Kaspersky Anti-Virus for Windows Servers

Podczas działania programu Kaspersky Anti-Virus for Windows Servers wystąpić mogą różnego rodzaju zdarzenia. Mogą one mieć charakter informacyjny lub zawierać ważne informacje. Na przykład: zdarzenie może poinformować użytkownika o pomyślnym uaktualnieniu programu lub zarejestrować błąd w module, który musi być natychmiast wyeliminowany.

W celu otrzymywania aktualnych informacji o działaniu programu Kaspersky Anti-Virus for Windows Servers można użyć funkcji powiadamiania.

Powiadomienia mogą być dostarczane na kilka sposobów:

Komunikaty wyskakujące wyświetlane nad ikoną programu znajdującą się w zasobniku systemowym

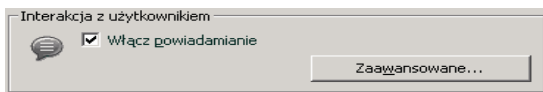
Komunikaty dźwiękowe

Wiadomości e-mail

Informacja w raporcie

W celu użycia tej funkcji należy:

1. Zaznaczyć opcję **Włącz powiadomianie** znajdującą się w sekcji **Interakcja z użytkownikiem** (patrz rys. 49).



Rysunek 49. Włączenie powiadamiania

2. Zdefiniować typ zdarzeń, o których program Kaspersky Anti-Virus for Windows Servers ma powiadamiać oraz metodę ich dostarczania (patrz rozdział 11.8.1.1 na stronie 138).
3. Skonfigurować ustawienia powiadamiania za pośrednictwem poczty elektronicznej, jeżeli wybrana została ta metoda (patrz rozdział 11.8.1.2 na stronie 139).

11.8.1.1. Typy zdarzeń i metody dostarczania powiadomień

Podczas funkcjonowania programu Kaspersky Anti-Virus for Windows Servers mogą wystąpić następujące rodzaje zdarzeń:

Krytyczne zdarzenia dotyczą ważnych zdarzeń. Zalecane jest używanie powiadomień, ponieważ zdarzenia te są źródłem problemów w funkcjonowaniu programu lub luk występujących w ochronie komputera. Na przykład: *sygnatury zagrożeń są uszkodzone* lub *licencja wygasła*.

Błędy w funkcjonowaniu – zdarzenia związane z błędami uniemożliwiającymi działanie programu. Na przykład, *brak licencji* lub *sygnatur zagrożeń*.

Ważne zdarzenia są zdarzeniami, które muszą zostać zbadane, ponieważ odnoszą się do ważnych sytuacji w funkcjonowaniu programu. Na przykład: *ochrona jest wyłączona* lub *pełne skanowanie komputera nie zostało przeprowadzone od długiego czasu*.

Powiadomienia informacyjne związane są z mało istotnymi zdarzeniami, które nie wymagają od użytkownika podejmowania żadnych działań. Na przykład: *wyleczono wszystkie zainfekowane obiekty*.

W celu określenia zdarzeń o których powiadamiał będzie program oraz metod dostarczania powiadomień należy:

1. Kliknąć odsyłacz **Ustawienia** znajdujący się w oknie głównym programu.
2. W oknie ustawień programu należy w sekcji **Usługi** zaznaczyć opcję **Włącz powiadomienia** i dokonać modyfikacji ustawień klikając przycisk **Ustawienia**.

W oknie **Ustawienia powiadomień**, które zostanie otwarte, możliwe jest konfigurowanie następujących metod powiadamiania dla zdarzeń wymienionych powyżej (patrz rys. 50):

Komunikaty wyskakujące pojawiające się nad ikoną programu w zasobniku systemowym; komunikaty te zawierają informacje o zdarzeniach.

Aby użyć tego typu powiadamiania, należy zaznaczyć opcję **Dymek**, przy odpowiednich zdarzeniach.

Włącz powiadomienia dźwiękowe

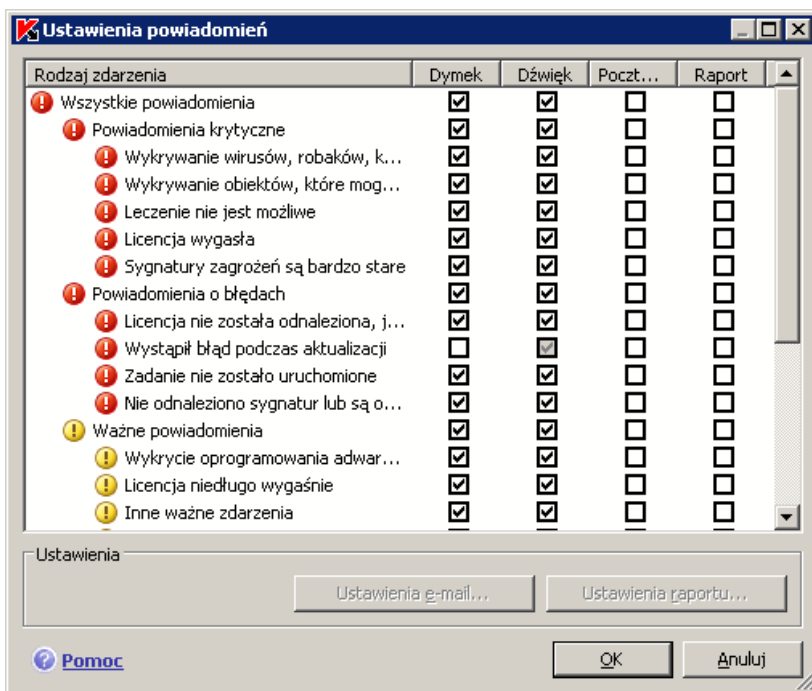
Aby występowaniu zdarzenia towarzyszył dźwięk, należy zaznaczyć opcję **Dźwięk** przy odpowiednich zdarzeniach.

Powiadomienia e-mail

W celu użycia tego typu powiadomienia należy zaznaczyć pole znajdujące się w sekcji **E-mail** obok żądanego zdarzenia oraz dokonać konfiguracji wysyłania powiadomień (patrz rozdział 11.8.1.2 na stronie 139).

Zapisz zdarzenie w raporcie

Aby informacje o zdarzeniach były rejestrowane w raporcie, należy zaznaczyć żądane opcje w kolumnie **Raport** i skonfigurować ustawienia raportowania w oknie, które pojawi się po kliknięciu przycisku **Ustawienia raportu** (patrz rozdział 11.8.1.3 na stronie 141).

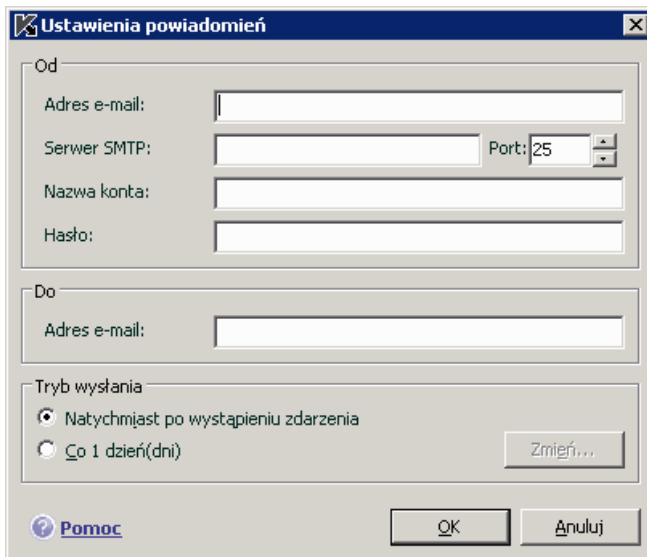


Rysunek 50. Typy zdarzeń i metody dostarczania powiadomień

11.8.1.2. Konfiguracja wysyłania powiadomień za pośrednictwem poczty elektronicznej

Po wybraniu zdarzeń (patrz rozdział 11.8.1.1 na stronie 138), o których użytkownik chce otrzymywać powiadomienia za pośrednictwem poczty elektronicznej należy dokonać konfiguracji dostarczania powiadomień. W tym celu należy:

1. Otworzyć okno ustawień programu klikając odsyłacz Ustawienia znajdujący się w jego oknie głównym.
2. W drzewie ustawień kliknąć odsyłacz **Usługi**.
3. W sekcji **Interakcja z użytkownikiem** kliknąć przycisk **Zaawansowane** znajdujący się w prawej części okna.
4. Na zakładce **Ustawienia powiadamiania**, zaznaczyć opcję w kolumnie **Email** dla wszystkich zdarzeń, po wystąpieniu których powinny być wysyłane powiadomienia pocztą elektroniczną.
5. W oknie, które zostanie otwarte po kliknięciu przycisku **Ustawienia powiadomień**, zdefiniować następujące ustawienia wysyłania powiadomień przy użyciu poczty elektronicznej:
 - Podać adres e-mail nadawcy w sekcji **Od: Adres e-mail**.
 - Określić adres e-mail na który wysyłane będą powiadomienia w sekcji **Do: Adres e-mail**.
 - Określić metodę dostarczania powiadomień e-mail w sekcji **Tryb wysyłania**. W celu natychmiastowego wystania powiadomienia po wystąpieniu zdarzenia należy zaznaczyć opcję **Natychmiast po wystąpieniu zdarzenia**. Dla powiadomień, które mają być wysyłane o określonym czasie należy zdefiniować terminarz po kliknięciu przycisku **Zmień**. Domyślnie powiadomienia są wysyłane raz dziennie.



Rysunek 51. Konfiguracja ustawień wysyłania powiadomień za pośrednictwem poczty elektronicznej

11.8.1.3. Konfiguracja dziennika zdarzeń

W celu konfiguracji ustawień raportowania zdarzeń należy:

1. Otworzyć okno ustawień aplikacji poprzez kliknięcie odsyłacza Ustawienia w oknie głównym.
2. W drzewie ustawień kliknąć odsyłacz **Usługi**.
3. W sekcji **Interakcja z użytkownikiem** kliknąć przycisk **Zaawansowane** znajdujący się w prawej części okna.

W oknie **Ustawienia powiadomień** wybrać opcję raportowania informacji o wystąpieniu zdarzenia i kliknąć przycisk **Ustawienia raportu**.

Kaspersky Anti-Virus wyposażony jest w możliwość zapisywania informacji o zdarzeniach występujących podczas jego pracy w dzienniku zdarzeń systemu Windows (**Aplikacja**) lub w specjalnym raporcie Kaspersky Anti-Virus (**Dziennik zdarzeń Kaspersky Lab**).

Raporty można przeglądać przy pomocy narzędzia Microsoft Windows **Podgląd zdarzeń**. Aby je uruchomić należy kliknąć **Start** → **Ustawienia** → **Panel sterowania** → **Narzędzia administracyjne** → **Podgląd zdarzeń**.

11.8.2. Autoochrona programu i ograniczenia dostępu

Kaspersky Anti-Virus for Windows Servers zapewnia ochronę komputera przed szkodliwymi programami, przez co może on być również celem ataków szkodliwych programów usiłujących go zablokować lub nawet usunąć z komputera.

Ponadto, komputer może być używany przez wielu użytkowników posiadających różny stopień umiejętności. Pozostawienie dostępu do programu oraz jego ustawień może znacznie obniżyć bezpieczeństwo komputera.

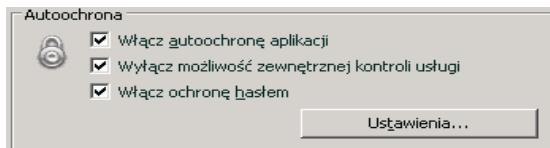
W celu zagwarantowania stabilności systemu bezpieczeństwa komputera do programu dodane zostały funkcje autoochrony, ochrony przed zdalnym dostępem oraz mechanizmy ochrony hasłem.

W celu włączenia autoochrony należy:

1. Otworzyć okno ustawień programu klikając odsyłacz Ustawienia znajdujący się w oknie głównym programu.
2. W drzewie ustawień wybrać sekcję **Usługi**.
3. Przy użyciu sekcji **Autoochrona** dokonać następujących ustawień (patrz rys. 52):

- Włącz autoochronę.** Po wybraniu tej opcji, program chronił będzie swoje pliki, procesy w pamięci oraz wpisy rejestru systemowego przed usunięciem lub modyfikacją.
- Wyłącz możliwość zewnętrznej kontroli programu.** Po wybraniu tej opcji, blokowane będą wszelkie próby zewnętrznej kontroli programu przez programy do zdalnej administracji.

Po wystąpieniu jednej z wymienionych wyżej akcji wyświetlony zostanie komunikat nad ikoną programu znajdującą się w zasobniku systemowym (jeżeli usługa powiadomień nie została wyłączona przez użytkownika).



Rysunek 52. Konfiguracja autoochrony programu

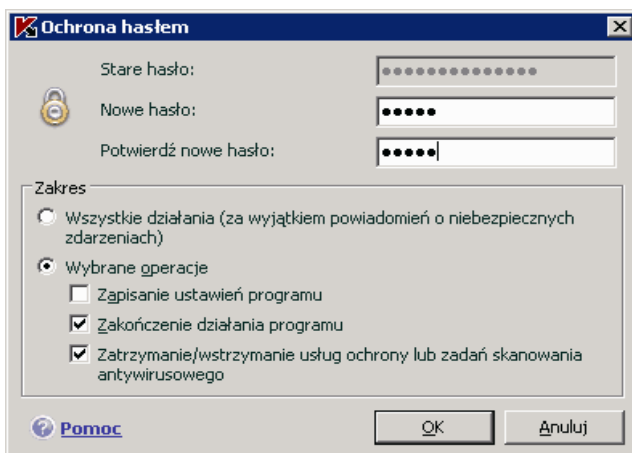
W celu włączenia ochrony programu za pomocą hasła należy zaznaczyć opcję **Włącz ochronę hasłem.** Kliknąć przycisk **Ustawienia** w celu otwarcia okna **Ochrona hasłem** oraz wprowadzić hasło i wskazać obszar objęty ograniczeniem

dostępu (patrz rys. 53). Możliwe jest blokowanie dowolnych operacji wykonywanych przez program za wyjątkiem powiadamiania o wykryciu niebezpiecznego obiektu. Można również chronić przed wykonaniem jednej z następujących akcji:

- Modyfikacja ustawień programu
- Zakończenie działania Kaspersky Anti-Virus for Windows Servers
- Wyłączenie lub wstrzymywanie ochrony komputera

Możliwość wykonania każdej z wyżej wymienionych akcji prowadzi do obniżenia poziomu ochrony komputera, dlatego też należy ustalić, którzy użytkownicy serwera mogą wykonywać tego typu akcje.

Za każdym razem, gdy dowolny użytkownik serwera spróbuje wykonania wybranych akcji, program wyświetlać będzie żądanie podania hasła.



Rysunek 53. Ustawienia ochrony programu za pomocą hasła

11.8.3. Rozwiązywanie problemów z innymi aplikacjami

W pewnych okolicznościach Kaspersky Anti-Virus może wchodzić w konflikty z innymi programami zainstalowanymi na komputerze. Ma to związek z mechanizmami autoochrony wbudowanymi w te programy, które włączają się gdy Kaspersky Anti-Virus skanuje je w poszukiwaniu szkodliwego kodu. Do aplikacji tych należą: wtyczka Authenica dla programu Acrobat Reader, która weryfikuje dostęp do plików .pdf, Oxygen Phone Manager II oraz niektóre gry komputerowe zabezpieczone przy użyciu technologii DRM.

W celu wyeliminowania takich problemów należy zaznaczyć opcję **Tryb zgodności z programami wykorzystującymi metody autoochrony** znajdującą się w sekcji **Usługi** okna konfiguracji programu. Aby to ustawienie zaczęło działać, należy ponownie uruchomić komputer.

11.9. Importowanie i eksportowanie ustawień Kaspersky Anti-Virus for Windows Servers

Kaspersky Anti-Virus for Windows Servers posiada funkcję importowania oraz eksportowania ustawień.

Ustawienia są zapisywane w specjalnym pliku konfiguracyjnym.

W celu wyeksportowania bieżących ustawień programu należy:

1. Otworzyć główne okno Kaspersky Anti-Virus for Windows Servers.
2. Przejść do sekcji **Usługi** i kliknąć Ustawienia.
3. Kliknąć przycisk **Zapisz** znajdujący się w sekcji **Zarządzanie ustawieniami**.
4. Wprowadzić nazwę dla pliku konfiguracyjnego i wskazać folder, w którym zostanie on zapisany.

W celu zaimportowania ustawień z pliku konfiguracyjnego należy:

1. Otworzyć główne okno Kaspersky Anti-Virus for Windows Servers.
2. Przejść do sekcji **Usługi** i kliknąć Ustawienia.
3. Kliknąć przycisk **Otwórz** i wskazać lokalizację pliku konfiguracyjnego zawierającego ustawienia programu Kaspersky Anti-Virus for Windows Servers, które mają zostać zaimportowane.

11.10. Przywracanie ustawień domyślnych

W każdej chwili można przywrócić zalecane ustawienia programu. Ustawienia te są optymalne i są one zalecane przez ekspertów z firmy Kaspersky Lab. Może to zostać wykonane przy użyciu Kreatora konfiguracji.

W celu zresetowania ustawień ochrony należy:

1. Wybrać sekcję **Usługi** i kliknąć odsyłacz Ustawienia w celu wyświetlenia okna ustawień programu.
2. Kliknąć przycisk **Resetuj** znajdujący się w sekcji **Zarządzanie ustawieniami**.

W oknie, które zostanie otwarte należy określić ustawienia, dla których powinny zostać przywrócone domyślne wartości.

Domyślnie program zapisuje wszystkie niestandardowe ustawienia na liście (nie są one zaznaczone). Jeżeli nie ma potrzeby zachowania określonych ustawień, należy je zaznaczyć.

Po zakończeniu konfiguracji ustawień, należy kliknąć przycisk **Dalej**. Uruchomiony zostanie Kreator wstępnej konfiguracji. Należy postępować zgodnie z jego poleceniami.

Po zakończeniu pracy z kreatorem konfiguracji programu, dla modułu Ochrona plików ustawiony zostanie **Zalecany** poziom bezpieczeństwa, za wyjątkiem ustawień które zostały zachowane. Ponadto, ustawienia skonfigurowane w kreatorze konfiguracji programu również zostaną zastosowane.

ROZDZIAŁ 12. ZARZĄDZANIE PROGRAMEM PRZY UŻYCIU KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit jest systemem umożliwiającym scentralizowane wykonywanie kluczowych zadań administracyjnych podczas zarządzania systemem ochrony sieci korporacyjnej opartym na produktach firmy Kaspersky Lab.

Kaspersky Anti-Virus 6.0 for Windows Servers jest jednym z produktów firmy Kaspersky Lab, którym można zarządzać za pomocą własnego interfejsu, wiersza poleceń (metody te opisane są w tym podręczniku) lub za pomocą Kaspersky Administration Kit (w przypadku gdy komputer jest częścią scentralizowanego systemu zdalnego zarządzania).

Przy użyciu Kaspersky Administration Kit można zarządzać aplikacją na dwa sposoby.

Lokalnie: w przypadku tej opcji, należy na komputerze zainstalować program Kaspersky Anti-Virus 6.0 for Windows Servers, agenta sieciowego (administracyjnego) oraz Konsolę administracyjną, które są elementem pakietu Kaspersky Administration Kit. W tym przypadku możliwe będzie lokalne zarządzanie działaniem aplikacji przy użyciu Konsoli administracyjnej.

Jeżeli użytkownik planuje w przyszłości zdalnie zarządzać aplikacją poprzez Kaspersky Administration Kit, podczas instalacji agenta administracyjnego, należy upewnić się, że adres serwera administracyjnego (nazwa i port) jest poprawny.

W przypadku lokalnego zarządzania aplikacją przy użyciu konsoli administracyjnej, użytkownik może pracować jedynie z elementami dostępnymi w węźle **Komputer lokalny** (patrz Rysunek 54).

W tym trybie, można zarządzać zadaniami i ustawieniami programu Kaspersky Anti-Virus zainstalowanym na danym komputerze.

Zdalnie – w przypadku tej opcji należy:

- zainstalować serwer administracyjny w sieci; zainstalować konsolę administracyjną w miejscu pracy administratora (szczegółowe informacje na ten temat znajdują się w

podręczniku administratora dla Kaspersky Administration Kit 6.0);

- Na serwerach sieciowych zainstalować Kaspersky Anti-Virus 6.0 for Windows Servers oraz agenta administracyjnego (zawartego w pakiecie Kaspersky Administration Kit). Szczegółowe informacje na temat zdalnej instalacji programu Kaspersky Anti-Virus na komputerach sieciowych znajdują się w podręczniku administratora dla Kaspersky Administration Kit 6.0.

Konsola administracyjna (patrz Rysunek 54) umożliwia zarządzanie aplikacją przy użyciu Kaspersky Administration Kit. Posiada ona **standardowy interfejs MMC** (Microsoft Management Console) i umożliwia administratorowi na wykonywanie następujących czynności:

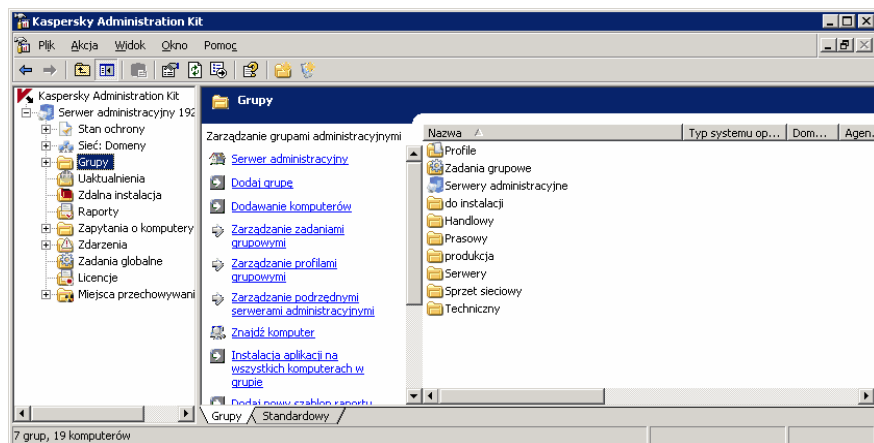
Zdalna instalacja Kaspersky Anti-Virus 6.0 for Windows Servers oraz agenta administracyjnego na komputerach sieciowych

Zdalna konfiguracja Kaspersky Anti-Virus na komputerach sieciowych

Aktualizacja sygnatur zagrożeń oraz modułów Kaspersky Anti-Virus

Zarządzanie licencjami dla aplikacji zainstalowanych na komputerach sieciowych

Przeglądanie informacji na temat działania programu na komputerach klienckich



Rysunek 54. Konsola administracyjna Kaspersky Administration Kit

Podczas zarządzania programem za pomocą Kaspersky Administration Kit, administrator określa ustawienia dla profili, zadań i aplikacji.

Ustawienia aplikacji obejmują ogólne ustawienia ochrony, ustawienia Kopii zapasowej i Kwarantanny, ustawienia tworzenia raportów itp.

Zadanie jest określonym działaniem wykonywanym przez aplikację. Zadania dla Kaspersky Anti-Virus for Windows Servers można podzielić na typy w zależności od funkcji przez nie wykonywanych (zadania skanowania antywirusowego, zadania aktualizacji programu, zadania cofania aktualizacji oraz zadania instalacji kluczy licencyjnych). Każde zadanie posiada zestaw ustawień Kaspersky Anti-Virus, które są wykorzystywane podczas wykonywania zadania (*ustawienia zadania*).

Kluczowym elementem scentralizowanego zarządzania jest grupowanie komputerów zdalnych i zarządzanie ich ustawieniami poprzez tworzenie i konfigurację profili grupowych.

Profil definiuje zestaw ustawień programu dla komputerów klienckich należących do grupy. Profile zawierają ustawienia programu oraz ustawienia dla wszystkich typów zadań, za wyjątkiem ustawień specyficznych dla pewnych typów zadań.

12.1. Zarządzanie aplikacją

Kaspersky Administration Kit umożliwia uruchamianie i wstrzymywanie działania programu Kaspersky Anti-Virus na poszczególnych komputerach klienckich, jak również konfiguracją ogólnych ustawień aplikacji, takich jak włączanie/wyłączanie ochrony komputera, ustawienia Kopii zapasowej i Kwarantanny oraz ustawienia tworzenia raportów.

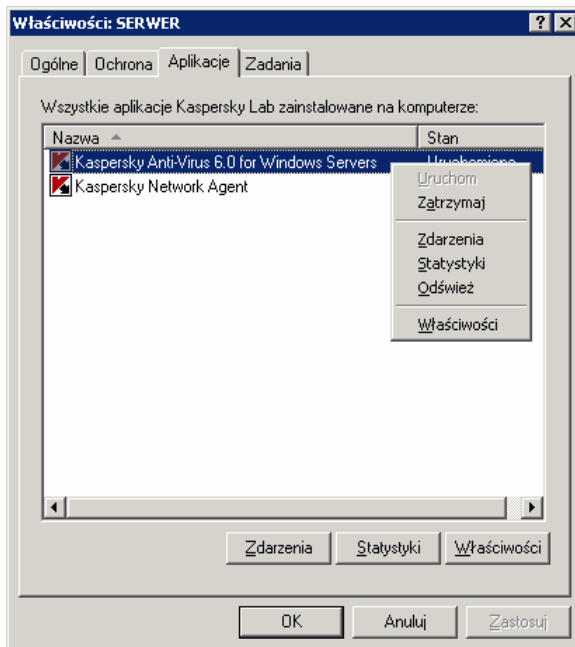
W celu konfiguracji ustawień aplikacji:

1. Wybrać folder grupy, do której należy komputer kliencki (patrz Rysunek 54).
2. W panelu widoku szczegółowego wybrać komputer, którego ustawienia mają zostać zmodyfikowane. Z menu kontekstowego lub menu **Akcja** wybrać działanie **Właściwości**.
3. Na zakładce **Aplikacje** znajdującej się w oknie właściwości komputera klienckiego (patrz Rysunek 55) wyświetlana jest lista aplikacji firmy Kaspersky Lab zainstalowanych na komputerze klienckim.

Pod listą aplikacji znajdują się przyciski umożliwiające:

- Przeglądanie listy zdarzeń, które wystąpiły podczas działania aplikacji na komputerze klienckim i zostały zarejestrowane na serwerze administracyjnym
- Przeglądanie bieżących statystyk działania aplikacji

- Konfigurację ustawień programu (patrz rozdział 12.1.2 na stronie 150)



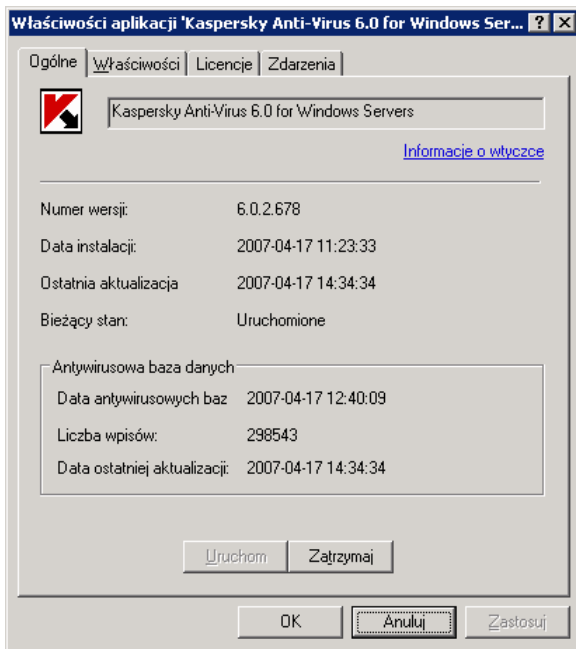
Rysunek 55. Lista aplikacji firmy Kaspersky Lab

12.1.1. Uruchamianie/Zatrzymywanie działania aplikacji

Można uruchomić lub zatrzymać działanie Kaspersky Anti-Virus na zdalnych komputerach przy użyciu poleceń menu kontekstowego dla okna właściwości komputera (patrz Rysunek 55).

Te same działania można wykonać przy użyciu przycisków Uruchom/Zatrzymaj dostępnych na zakładce **Ogólne** okna **Ustawienia** (patrz Rysunek 56).

W górnej części okna wyświetlana jest nazwa zainstalowanej aplikacji, informacja o wersji, data instalacji, jej stan (czy aplikacja jest uruchomiona czy też zatrzymana na lokalnym komputerze) oraz informacja o stanie bazy danych sygnatur zagrożeń.



Rysunek 56. Konfiguracja ustawień Kaspersky Anti-Virus.
Zakładka **Ogólne**

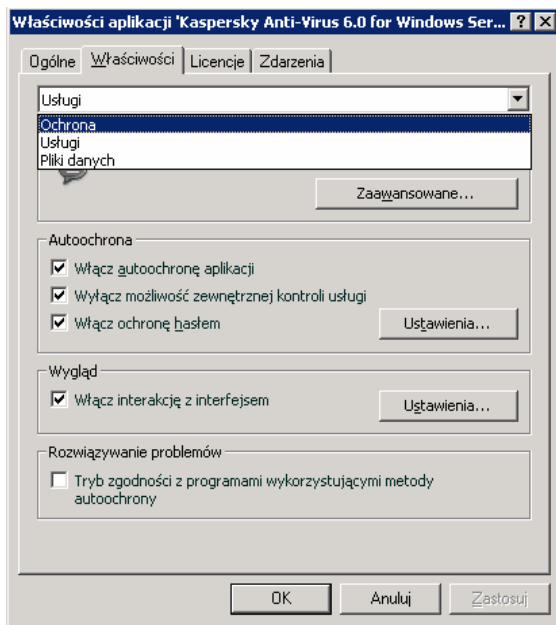
12.1.2. Konfiguracja ustawień aplikacji

W celu przejrzania lub modyfikacji ustawień aplikacji należy:

1. Otworzyć okno właściwości komputera klienckiego i przełączyć się do zakładki **Aplikacje** (patrz Rysunek 54).
2. Wybrać **Kaspersky Anti-Virus 6.0 for Windows Servers**. Kliknąć przycisk **Właściwości**, aby otworzyć okno ustawień aplikacji.

Wszystkie zakładki, za wyjątkiem zakładki **Ustawienia** są standardowymi zakładkami Kaspersky Administration Kit. Szczegółowe informacje na temat tych zakładek znajdują się w podręczniku administratora tego produktu.

Jeżeli dla aplikacji utworzono profil (patrz rozdział **Błąd! Nie można odnaleźć źródła odwołania.** na stronie **Błąd! Nie zdefiniowano zakładki.**), w którym zablokowano możliwość modyfikacji ustawień, nie będzie można ich modyfikować z poziomu okna ustawień aplikacji.



Rysunek 57. Konfiguracja ustawień Kaspersky Anti-Virus.
Zakładka **Właściwości**

Na zakładce **Właściwości** można konfigurować ogólne oraz systemowe ustawienia Kaspersky Anti-Virus, ustawienia Kopii zapasowej i Kwarantanny oraz ustawienia tworzenia raportów. Aby to zrobić należy wybrać żądany element z listy rozwijalnej dostępne w górnej części zakładki, a następnie zdefiniować parametry tych ustawień:

Ochrona

W tym oknie można:

- Włączyć/Wyłączyć ochronę komputera (patrz rozdział 6.1 na stronie 49)
- Skonfigurować automatyczne uruchamianie aplikacji podczas ładowania systemu operacyjnego (patrz rozdział 6.1.5 na stronie 53)
- Utworzyć strefę zaufaną oraz listę wykluczeń (patrz rozdział 6.3 na stronie 54)
- Wybrać typy szkodliwych programów, które będą wykrywane przez aplikację (patrz rozdział 6.2 na stronie 53)
- Konfigurować ustawienia wydajności aplikacji dla konfiguracji

wieloprocessorowych (patrz rozdział 6.7 na stronie 67)
Usługi
<p>Konfiguracja ustawień systemowych obejmuje:</p> <ul style="list-style-type: none"> • Konfigurację powiadomień o wystąpieniu zdarzeń (patrz rozdział 11.8.1 na stronie 137) • Zarządzanie działaniem funkcji autoochrony aplikacji oraz ochrony ustawień aplikacji (patrz rozdział 11.8.2 na stronie 142) • Konfigurację wyglądu aplikacji (patrz rozdział 12.3.1 na stronie 160) • Konfigurację ustawień zgodności Kaspersky Anti-Virus z innymi aplikacjami (patrz rozdział 11.8.3 na stronie 143)
Pliki danych
<p>W tym oknie można skonfigurować ustawienia generowania raportów oraz statystyk (patrz rozdział 11.3.1 na stronie 125) oraz określić czas przechowywania obiektów w Kopii zapasowej (patrz rozdział 11.2.2 na stronie 122) i Kwarantannie (patrz rozdział 11.1.2 na stronie 119).</p>

12.1.3. Konfiguracja ustawień zaawansowanych

Podczas konfiguracji Kaspersky-Anti-Virus przy użyciu Kaspersky Administration Kit, można włączyć/wyłączyć możliwość interakcji z użytkownikiem lub zdefiniować informacje na temat pomocy technicznej. W tym celu należy:

1. Otworzyć okno właściwości komputera klienckiego i przełączyć się do zakładki **Aplikacje** (patrz Rysunek 55).
2. Wybrać **Kaspersky Anti-Virus 6.0 for Windows Servers** i kliknąć przycisk **Właściwości**. Otwarte zostanie okno ustawień aplikacji (patrz Rysunek 56). Z listy rozwijalnej znajdującej się w górnej części zakładki wybrać element **Usługi**.
3. W oknie, które zostanie otwarte (patrz Rysunek 57), kliknąć przycisk **Ustawienia** znajdujący się w sekcji **Wygląd**.

Na zakładce **Usługi** w sekcji **Wygląd** można także włączyć/wyłączyć interakcyjność interfejsu Kaspersky Anti-Virus na zdalnym komputerze: wyświetlanie ikony Kaspersky Anti-Virus w zasobniku systemowym, wyświetlanie

powiadomień o wystąpieniu zdarzeń (na przykład, po wykryciu niebezpiecznego obiektu).

Jeżeli interakcja z interfejsem jest wyłączona (opcja **Włącz interakcję z interfejsem** nie jest zaznaczona), użytkownik będzie obserwował komunikaty programu, jednak nie będzie mógł na nie reagować, ani zmieniać ustawień aplikacji

Na zakładce **Niestandardowe informacje o pomocy technicznej**, okna które zostanie otwarte po kliknięciu przycisku **Ustawienia** można zmodyfikować informacje na temat pomocy technicznej dla użytkowników. Informacje te są wyświetlane w sekcji **Pomoc** okna głównego Kaspersky Anti-Virus (patrz rys. 47).

Aby zmienić informacje wyświetlane w górnym polu należy wpisać żądany tekst. W dolnym polu można utworzyć listę odsyłaczy wyświetlanych w polu **Pomoc WWW** dostępnych w sekcji **Pomoc** zakładki **Usługi**.

W celu redagowania listy zasobów należy skorzystać z przycisków **Dodaj**, **Modyfikuj** oraz **Usuń**. Kaspersky Anti-Virus doda nowy odsyłacz na początek listy. Aby zmienić porządek wyświetlania odsyłaczy należy użyć przycisków **W górę** i **W dół**.

Jeżeli okno nie zawiera żadnych danych, wyświetlane będą domyślne informacje o pomocy technicznej. Domyślnych informacji nie można modyfikować.

12.2. Zarządzanie zadaniami

Ten rozdział zawiera informacje na temat zarządzania zadaniami dla Kaspersky Anti-Virus 6.0 for Windows Servers. Szczegółowe informacje na temat zarządzania zadaniami przy użyciu Kaspersky Administration Kit 6.0 znajdują się w podręczniku administratora dla tego produktu.

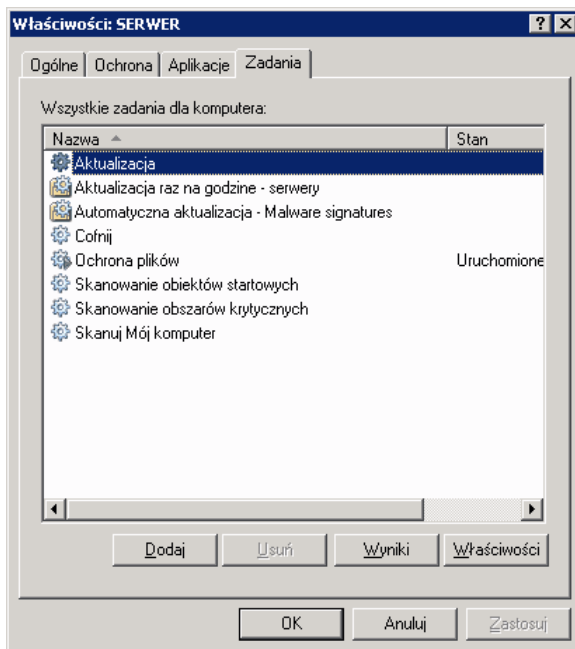
Podczas instalacji aplikacji na każdym komputerze tworzony jest zestaw zadań systemowych. Lista ta (patrz Rysunek 58) obejmuje zadania ochrony w czasie rzeczywistym (Ochrona plików), zadania skanowania antywirusowego (Mój komputer, obiekty startowe, obszary krytyczne) oraz zadania aktualizacji (aktualizacja sygnatur zagrożeń i modułów aplikacji, cofanie uaktualnień, współdzielenie uaktualnień).

Można uruchamiać zadania systemowe, konfigurować ich ustawienia oraz terminarz, ale nie można ich usuwać.

Użytkownik może tworzyć własne zadania, takiej jak skanowanie antywirusowe, pobieranie i cofanie aktualizacji oraz instalacja klucza licencyjnego.

W celu przejrzania listy zadań utworzonych dla komputera klienckiego należy:

1. Wybrać folder grupy, do której należy komputer kliencki (patrz Rysunek 54).
2. W panelu widoku szczegółowego wybrać komputer, dla którego ma zostać utworzone zadanie lokalne i z menu **Akcja** lub menu kontekstowego wybrać polecenie **Zadania**. Otwarte zostanie okno właściwości komputera klienckiego.
3. Na zakładce **Zadania** (patrz Rysunek 58) wyświetlona zostanie lista wszystkich zadań utworzonych dla komputera klienckiego.



Rysunek 58. Lista zadań dla aplikacji

12.2.1. Uruchamianie i zatrzymywanie zadań

Zadania mogą być uruchamiane na komputerze klienckim, tylko jeżeli odpowiadająca im aplikacja jest uruchomiona (patrz rozdział 12.1.1 na stronie 149). Jeżeli działanie aplikacji zostanie zatrzymane, wykonywanie wszystkich

zadań zostanie również zatrzymane.

Zadania mogą być uruchamiane i wstrzymywane zgodnie z terminarzem lub ręcznie przy użyciu poleceń menu kontekstowego oraz okna przeglądania zadań. Można również wstrzymywać i wznowiać działanie zadań.

W celu ręcznego uruchomienia/zatrzymania/wznowienia działania zadania:

W panelu widoku szczegółowego wybrać żądane zadanie i z menu kontekstowego lub menu **Akcja** wybrać polecenie **Uruchom/Zatrzymaj/Wstrzymaj/Wznów**.

Te same operacje można wykonywać przy użyciu przycisków znajdujących się na zakładce **Ogólne** okna ustawień zadania (patrz Rysunek 59).

12.2.2. Tworzenie zadań

Podczas pracy z aplikacją przy użyciu Kaspersky Administration Kit można tworzyć:

- Zadania lokalne, konfigurowane dla poszczególnych komputerów
- Zadania grupowe, konfigurowane dla komputerów należących do jednej grupy administracyjnej
- Zadania globalne, konfigurowane dla dowolnego zestawu komputerów należących do wielu różnych grup administracyjnych

Można modyfikować ustawienia zadania, monitorować jego działanie, kopiować i przenosić zadania z jednej grupy do innej oraz usuwać. Działania te można wykonywać przy użyciu standardowych poleceń **Kopiuj/Wklej**, **Wytnij/Wklej** lub **Usuń**. Polecenia te dostępne są w menu kontekstowym lub menu **Akcja**.

12.2.2.1. Tworzenie zadań lokalnych

W celu utworzenia zadani lokalnego należy wykonać następujące czynności:

1. Otworzyć okno właściwości komputera klienckiego na zakładce **Zadania** (patrz Rysunek 58).
1. Kliknąć przycisk **Dodaj** aby dodać zadanie. Spowoduje to uruchomienie Kreatora tworzenia nowego zadania. Interfejs kreatora podobny jest do standardowego kreatora systemu Windows i składa się z kilku etapów, pomiędzy którymi można się przemieszczać przy użyciu przycisków **Wstecz** i **Dalej** lub zakończyć korzystanie z niego klikając przycisk **Zakończ**. Można przerwać działanie kreatora w dowolnym momencie poprzez kliknięcie przycisku **Anuluj**.

Krok 1. Wprowadzenia ogólnych informacji o zadaniu

W pierwszym oknie kreatora należy podać nazwę zadania (pole **Nazwa**).

Krok 2. Wybór aplikacji i typu zadania

Na tym etapie należy wybrać aplikację, dla której tworzone jest zadanie (Kaspersky Anti-Virus 6.0 for Windows Servers). Wymagane jest również wybranie typu zadania:

- *Skanowanie antywirusowe* – skanowanie na obecność wirusów obszarów wskazanych przez użytkownika
- *Aktualizacja* – pobieranie uaktualnień sygnatur zagrożeń oraz modułów programu
- *Cofanie aktualizacji* – cofnięcie ostatnio przeprowadzonej aktualizacji programu
- *Instalacja klucza licencyjnego* – dodanie nowego klucza licencyjnego dla aplikacji

Krok 3. Konfiguracja ustawień wybranego typu zadania

W zależności od wybranego typu zadania, dostępne będą różne rodzaje okien:

SKANOWANIE ANTYWIRUSOWE

Konfiguracja zadania skanowania antywirusowego wymaga utworzenia listy obiektów przeznaczonych do skanowania (patrz rozdział 8.2 na stronie 83) oraz określenia jakie akcje ma wykonać Kaspersky Anti-Virus po wykryciu niebezpiecznego obiektu (patrz rozdział 8.4.4 na stronie 92).

AKTUALIZACJA

W przypadku zadań pobierania uaktualnień sygnatur zagrożeń oraz modułów aplikacji, należy określić źródło, z którego będą pobierane uaktualnienia (patrz rozdział 10.4.1 na stronie 105). Domyślnym źródłem uaktualnień jest serwer Kaspersky Administration Kit.

COFANIE AKTUALIZACJI

W przypadku tego zadania nie jest konieczne definiowanie żadnych ustawień.

INSTALACJA KLUCZA LICENCYJNEGO

Dla zadania instalacji klucza należy przy użyciu przycisku **Przeglądaj** określić ścieżkę dostępu pliku klucza licencyjnego. Aby dodać zapasowy klucz licencyjny należy zaznaczyć opcję **Dodaj jako klucz zapasowy**. Klucz zapasowy

zostanie automatycznie aktywowany po wygaśnięciu obecnie wykorzystywanego.

Informacje na temat dodawanego klucza licencyjnego (numer licencji, typ, data wygaśnięcia) wyświetlane są w dolnej części okna.

Krok 4. Konfigurowanie uruchamiania zadania przy użyciu wskazanego konta użytkownika

Na tym etapie należy wskazać konto użytkownika posiadającego uprawnienia dostępu do skanowanych obiektów lub do źródła uaktualnień (patrz rozdział 6.4 na stronie 62).

Krok 5. Konfiguracja terminarza

Po zakończeniu konfiguracji ustawień zadania, kreator wyświetli okno umożliwiające zdefiniowanie trybu automatycznego uruchamiania zadania.

Aby to zrobić należy w górnej części okna wybrać częstotliwość uruchamiania zadania, a w dolnej części okna skonfigurować ustawienia terminarza.

Krok 6. Kończenie tworzenia zadania

W ostatnim oknie kreatora wyświetlana jest informacja o pomyślnym zakończeniu tworzenia zadania.

12.2.2.2. Tworzenie zadania grupowego

W celu utworzenia zadania grupowego należy wykonać następujące czynności:

1. Wybrać z drzewa konsoli grupę, dla której ma zostać utworzone zadanie.
2. Otworzyć folder **Zadania grupowe**, wywołać menu kontekstowe i kliknąć polecenie **Nowy→Zadanie grupowe** lub kliknąć to samo polecenie z menu **Akcja**. Uruchomiony zostanie kreator tworzenia nowego zadania. Działanie tego kreatora jest podobne jak w przypadku tworzenia zadań lokalnych (patrz rozdział 12.2.2.1 na stronie 155). Należy postępować zgodnie z jego poleceniami.

Po zakończeniu działania kreatora do foldera **Zadania grupowe** dodane zostanie nowe zadanie. Zadanie to będzie wyświetlane i wykonywane we wszystkich grupach podrzędnych.

12.2.2.3. Tworzenie zadań globalnych

W celu utworzenia zadania globalnego należy wykonać następujące czynności:

1. Z drzewa konsoli wybrać węzeł **Zadania globalne**, otworzyć menu kontekstowe i kliknąć polecenie **Nowy** → **Zadanie**. Polecenie to można również wybrać z menu **Akcja**.
2. Uruchomiony zostanie kreator tworzenia nowego zadania. Działanie tego kreatora jest podobne jak w przypadku tworzenia zadań lokalnych (patrz rozdział 12.2.2.1 na stronie 155).
3. Utworzyć listę komputerów sieciowych, na których zadanie będzie uruchamiane. Można wybierać komputery z wielu różnych folderów lub wybrać cały folder (szczegółowe informacje na ten temat znajdują się w podręczniku administratora dla Kaspersky Administration Kit 6.0).

Zadania globalne wykonywane są tylko na wskazanych komputerach. Jeżeli do grupy administracyjnej, dla której utworzone zostało zadanie globalne, dodane zostaną nowe komputery klienckie, zadanie globalne nie będzie na nich uruchamiane. Konieczne będzie utworzenie nowego zadania lub dokonanie odpowiednich zmian w ustawieniach bieżącego zadania.

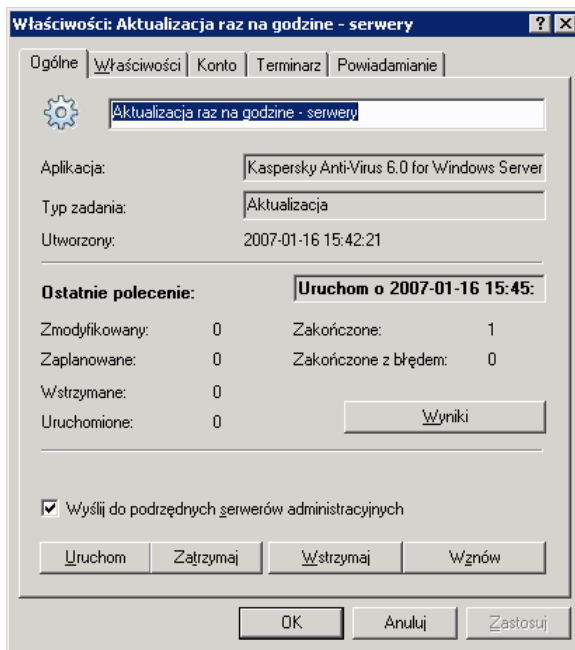
Po zakończeniu działania kreatora do foldera **Zadania globalne** dodane zostanie nowe zadanie.

12.2.3. Konfiguracja ustawień zadania

W celu przejrzania i konfiguracji zadania dla komputera klienckiego należy:

1. Otworzyć okno właściwości komputera klienckiego na zakładce **Zadania** (patrz Rysunek 58).
2. Wybrać zadanie z listy i kliknąć przycisk **Właściwości**. Otwarte zostanie okno ustawień zadania (patrz Rysunek 60).

Wszystkie zakładki za wyjątkiem zakładki **Ustawienia** są standardowymi zakładkami Kaspersky Administration Kit 6.0. Szczegółowe informacje na ich temat znajdują się w podręczniku administratora dla Kaspersky Administration Kit 6.0. Na zakładce **Ustawienia** dostępne są ustawienia Kaspersky Anti-Virus. Zawartość zakładek zależna jest od wybranego typu zadania.



Rysunek 59. Przeglądanie i konfiguracja ustawień zadania

Konfiguracja ustawień zadań przy użyciu interfejsu Kaspersky Administration Kit jest podobna do konfiguracji zadań przy użyciu lokalnego interfejsu Kaspersky Anti-Virus, za wyjątkiem ustawień specyficznych dla zadań. Szczegółowe informacje na temat konfiguracji zadań znajdują się w Rozdział 7. – Rozdział 10. .

Jeżeli dla aplikacji utworzono profil (patrz rozdział 12.3 na stronie 159) blokujący możliwość modyfikacji pewnych ustawień, nie będzie można ich modyfikować z poziomu zadań.

12.3. Zarządzanie profilami

Tworzenie profili umożliwia zastosowanie identycznych ustawień aplikacji i zadań, dla komputerów klienckich należących do pojedynczej grupy administracyjnej.

Ten rozdział zawiera informacje na temat tworzenia i konfiguracji profili dla Kaspersky Anti-Virus 6.0 for Windows Servers. Szczegółowe informacje na


temat zarządzania profilami dostępne są w podręczniku administratora Kaspersky Administration Kit 6.0.

12.3.1. Tworzenie profili

W celu utworzenia profilu dla Kaspersky Anti-Virus należy:

1. Z foldera **Grupy** (patrz Rysunek 54), wybrać grupę komputerów, dla której ma zostać utworzony nowy profil.
2. Otworzyć folder Profile, otworzyć menu kontekstowe i użyć polecenia **Nowy**→**Profil**. Uruchomiony zostanie kreator tworzenia nowego profilu.

Interfejs kreatora podobny jest do standardowego kreatora systemu Windows i składa się z kilku etapów, pomiędzy którymi można się przemieszczać przy użyciu przycisków **Wstecz** i **Dalej** lub zakończyć korzystanie z niego klikając przycisk **Zakończ**. Kliknięcie przycisku **Anuluj** zatrzyma kreatora w dowolnym momencie.

Podczas każdego etapu konfiguracji profilu, można blokować ustawienia przy użyciu przycisku . Jeżeli przycisk zablokowania jest wciśnięty, ustawienie funkcji programu do której się on odnosi będzie stosowane na komputerach klienckich.

Krok 1. Wprowadzenia ogólnych informacji o profilu

W pierwszym oknie kreatora należy podać nazwę profilu (pole **Nazwa**). W kolejnym oknie z listy **Aplikacja** należy wybrać **Kaspersky Anti-Virus 6.0 for Windows Servers**.

Krok 2. Wybór stanu profilu

W tym oknie można określić status tworzonego profilu. Aby to zrobić należy wybrać żądaną opcję: profil aktywny, profil nieaktywny lub profil użytkownika mobilnego (zostanie użyty po odłączeniu komputera od sieci lokalnej).

Dla jednej aplikacji może zostać utworzonych wiele różnych profili, ale tylko jeden z nich może być aktywny.

Krok 3. Wybór i konfiguracja składników ochrony

Na tym etapie można włączyć/wyłączyć ochronę komputera oraz moduł Ochrona plików. Domyślnie ochrona jest włączona oraz uruchamiany jest moduł Ochrona plików.

Aby dokonać konfiguracji ustawień ochrony lub skonfigurować moduł Ochrona plików, należy wybrać odpowiedni element z listy i kliknąć przycisk **Ustawienia**.

Krok 4. Konfiguracja zadań skanowania

Na tym etapie należy skonfigurować ustawienia, które będą wykorzystywane przez zadania skanowania antywirusowego.

W sekcji **Poziom ochrony** należy wybrać jeden z predefiniowanych poziomów (patrz rozdział 7.1 na stronie 69). Aby dokonać konfiguracji wybranego poziomu należy kliknąć przycisk **Ustawienia**. Aby przywrócić ustawienia domyślnego poziomu ochrony, należy kliknąć przycisk **Domyślne**.

W sekcji **Akcja** należy wybrać działanie jakie zostanie podjęte przez Kaspersky Anti-Virus po wykryciu niebezpiecznego obiektu.

Krok 5. Konfiguracja ustawień aktualizacji

W tym oknie można skonfigurować ustawienia współdzielenia uaktualnień dla Kaspersky Anti-Virus.

W sekcji **Ustawienia aktualizacji**, należy określić czy moduły aplikacji powinny być także aktualizowane (patrz rozdział 10.4.2 na stronie 108). W oknie, które zostanie otwarte należy kliknąć przycisk Ustawienia i skonfigurować ustawienia sieciowe (patrz rozdział 10.4.3 na stronie 110) oraz wybrać źródło uaktualnień (patrz rozdział 10.4.1 na stronie 105).

W sekcji **Działania podejmowane po zakończeniu aktualizacji** można włączyć/skanowanie Kwarantanny po pobraniu nowych uaktualnień (patrz rozdział 10.4.4 na stronie 112).

Krok 6. Wymuszanie stosowania profilu

Na tym etapie można wybrać metodę dystrybucji profilu na komputery klienckie należące do grupy (szczegółowe informacje na ten temat znajdują się w podręczniku administratora dla Kaspersky Administration Kit 6.0).


Krok 7. Określanie metody pierwszego wymuszenia stosowania profilu

Na tym etapie należy w oknie **Wymuszanie stosowania profilu** wybrać metodę pierwszego zastosowania profilu na komputerach klienckich należących do grupy (szczegółowe informacje na ten temat znajdują się w podręczniku administratora dla Kaspersky Administration Kit 6.0).

Krok 8. Kończenie tworzenia profilu

W ostatnim oknie kreatora zostanie wyświetlona informacja o pomyślnym utworzeniu profilu.

Po zakończeniu działania kreatora utworzony profil dla Kaspersky Anti-Virus zostanie dodany do foldera **Profile** odpowiedniej grupy.

Można modyfikować ustawienia utworzonego profilu oraz skonfigurować blokady modyfikacji ustawień przy użyciu przycisku . Użytkownik komputera klienckiego nie będzie mógł modyfikować ustawień, które zostały zablokowane w ten sposób. Profil zostanie zastosowany na komputerach klienckich przy pierwszej synchronizacji klienta z serwerem.

Można kopiować lub przenosić profile z jednej grupy do innej oraz usuwać. Działania te można wykonywać przy użyciu standardowych poleceń **Kopiuj/Wklej**, **Wytnij/Wklej** lub **Usuń**. Polecenia te dostępne są w menu kontekstowym lub menu Akcja.

12.3.2. Przeglądanie i modyfikacja ustawień profilu

W trakcie modyfikacji profilu można zmieniać ustawienia oraz blokować możliwość zmiany ustawień w grupach zagnieżdżonych i zadaniach dla aplikacji.

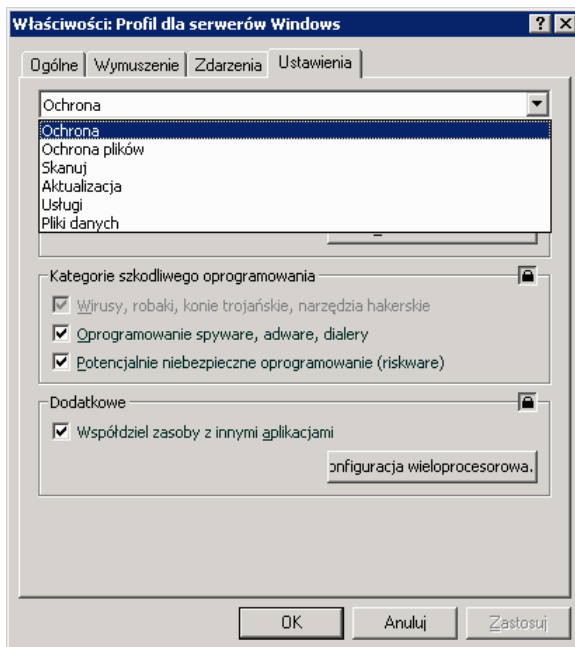
W celu przejrzania lub zmodyfikowania ustawień profilu należy:

3. Z foldera **Grupy** drzewa konsoli należy wybrać grupę komputerów, której ustawienia mają zostać zmodyfikowane.
4. Wybrać folder **Profile** należący do grupy. W panelu widoku szczegółowego wyświetlona zostanie lista wszystkich profili utworzonych dla grupy.
5. Wybrać z listy żądany profil dla **Kaspersky Anti-Virus 6.0 for Windows Servers** (nazwa aplikacji wyświetlana jest w kolumnie **Aplikacja**).
6. Wywołać menu kontekstowe dla wybranego profilu i kliknąć polecenie **Właściwości**. Na ekranie zostanie wyświetlone okno ustawień profilu dla Kaspersky Anti-Virus 6.0 (patrz Rysunek 60).

Wszystkie zakładki za wyjątkiem zakładki **Ustawienia** są standardowymi zakładkami Kaspersky Administration Kit 6.0. Szczegółowe informacje na ich temat znajdują się w podręczniku administratora dla Kaspersky Administration Kit 6.0.

Na zakładce **Ustawienia** wyświetlane są ustawienia Kaspersky Anti-Virus 6.0. Ustawienia profilu obejmują ustawienia programu (patrz rozdział 12.1.2 na stronie 150) oraz ustawienia zadań (patrz rozdział 12.2 na stronie 153)

Aby to zrobić należy wybrać żądany element z listy rozwijalnej dostępnej w górnej części zakładki, a następnie zdefiniować parametry tych ustawień.



Rysunek 60. Przeglądanie i konfigurowanie ustawień profilu

ROZDZIAŁ 13. PRACA Z PROGRAMEM PRZY UŻYCIU WIERZSA POLECEŃ

Można korzystać z funkcji programu Kaspersky Anti-Virus for Windows Servers przy użyciu wiersza poleceń. Możliwe jest wykonywanie następujących operacji:

- Uruchamianie, zatrzymywanie, wstrzymywanie i wznowianie działania modułu Ochrona plików
- Uruchamianie, wyłączenie, wstrzymywanie i wznowianie skanowania antywirusowego
- Uzyskiwanie informacji o bieżącym stanie modułu Ochrona plików, zadań oraz ich statystyk
- Skanowanie wybranych obiektów
- Uaktualnianie sygnatur zagrożeń i modułów programu
- Wyświetlanie pomocy dla składni wiersza poleceń
- Wyświetlanie pomocy dla składni poleceń

Składnia wiersza poleceń:

```
avp.com <polecenie> [ustawienia]
```

Dostęp do programu należy uzyskać z wiersza poleceń z foldera instalacyjnego programu lub przez określenie pełnej ścieżki dostępu do pliku `avp.com`.

Jako <polecenia> można użyć:

ADDKEY	Aktywacja aplikacji przy użyciu klucza licencyjnego (polecenie może być wykonane tylko w przypadku wprowadzenia hasła w interfejsie programu)
START	Uruchomienie modułu Ochrona plików lub zadania
PAUSE	Wstrzymanie działania modułu ochrona plików lub zadania (polecenie może być wykonane tylko w przypadku wprowadzenia hasła w interfejsie programu)

RESUME	Wznowienie działania modułu Ochrona plików lub zadania
STOP	Zatrzymanie działania modułu Ochrona plików lub zadania (polecenie może być wykonane tylko w przypadku wprowadzenia hasła w interfejsie programu)
STATUS	Wyświetlenie stanu modułu Ochrona plików lub zadania
STATISTICS	Wyświetlenie statystyk dla modułu Ochrona plików lub zadania
HELP	Wyświetlenie pomocy dla składni poleceń oraz lista poleceń
SCAN	Uruchomienie skanowania antywirusowego obiektów
UPDATE	Rozpoczęcie pobierania uaktualnień
ROLLBACK	Cofnięcie ostatnio przeprowadzonej aktualizacji programu (polecenie może być wykonane tylko w przypadku wprowadzenia hasła w interfejsie programu)
EXIT	Zamknięcie programu (polecenie można wywołać jedynie z hasłem przydzielonym w interfejsie programu)
IMPORT	Importowanie ustawień programu Kaspersky Anti-Virus for Windows Servers (polecenie może być wykonane tylko w przypadku wprowadzenia hasła w interfejsie programu)
EXPORT	Eksportowanie ustawień Kaspersky Anti-Virus for Windows Servers

Każdemu poleceniu odpowiadają jego własne ustawienia specyficzne dla konkretnego składnika programu Kaspersky Anti-Virus for Windows Servers.

13.1. Aktywowanie aplikacji

Aktywację programu można przeprowadzić przy użyciu pliku klucza licencyjnego (polecenie ADDKEY).

Składnia polecenia:

```
ADDKEY <nazwa_pliku > /password=<hasło>
```

Opis parametrów:

<nazwa_pliku>	Nazwa pliku klucza licencyjnego (plik z rozszerzeniem <i>.key</i>).
<hasło>	Hasło dostępu do programu Kaspersky Anti-Virus przypisane w interfejsie aplikacji.

Należy pamiętać o tym, że nie można uruchomić tego polecenia bez wprowadzenia hasła .

Przykład:

```
avp.com ADDKEY 00000000.key /password=<hasło_użytkownika >
```

13.2. Zarządzanie modułem Ochrona plików i zadaniami

Możliwe jest zarządzanie modułem Ochrona plików i zadaniami programu Kaspersky Anti-Virus z poziomu wiersza poleceń przy użyciu następujących poleceń:

START

PAUSE (polecenie może być wykonane tylko w przypadku wprowadzenia hasła w interfejsie programu)




RESUME

STOP (polecenie może być wykonane tylko w przypadku wprowadzenia hasła w interfejsie programu)

STATUS

STATISTICS

Zadanie lub składnik, do którego odnosi się polecenie musi zostać określone jako jego parametr.

Należy pamiętać o tym, że polecenia **START/PAUSE/STOP** odpowiadają przyciskom ,  oraz  dostępnym w interfejsie programu (patrz rozdział 5.1.2 na stronie 42).

Składnia polecenia:

```
avp.com <polecenie> <profil>
avp.com STOP
        PAUSE <profil> /password=<hasło>
```

Dla można <profil> można użyć jednej z następujących wartości:

RTP	<p>Wszystkie składniki ochrony</p> <p>Polecenie <code>avp.com START RTP</code> uruchamia moduł Ochrona plików, w przypadku gdy jego działanie II zostało wstrzymane przy użyciu interfejsu użytkownika lub polecenia PAUSE z wiersza poleceń.</p> <p>Jeżeli składnik został wyłączony przy użyciu przycisku ■ z poziomu interfejsu użytkownika lub poleceniem STOP z wiersza poleceń, w celu jego uruchomienia należy wykonać polecenie <code>avp.com START FM</code>.</p>
FM	Ochrona plików
UPDATER	Aktualizacja
RetranslationCfg	Dystrybucja uaktualnień do lokalnego źródła
Rollback	Cofnięcie ostatniej aktualizacji programu
SCAN_OBJECTS	Wykonanie zadania skanowania antywirusowego
SCAN_MY_COMPUTER	Wykonanie skanowania komputera
SCAN_CRITICAL_AREAS	Wykonanie zadania skanowania obszarów krytycznych
SCAN_STARTUP	Wykonanie zadania skanowania obiektów startowych
SCAN_QUARANTINE	Wykonanie zadania skanowania kwarantanny
<nazwa zadania >	Wykonanie zadania zdefiniowanego przez

użytkownika

Składniki i zadania uruchomione z wiersza poleceń są uruchamiane z ustawieniami skonfigurowanymi w interfejsie programu.

Przykłady:

W celu włączenia modułu Ochrona plików należy wprowadzić następujące polecenie:

```
avp.com START FM
```

W celu przerwania zadania skanowania całego komputera należy wprowadzić następujące polecenie:

```
avp.com STOP SCAN_MY_COMPUTER  
/password=<your_password>
```

13.3. Skanowanie antywirusowe

Uruchomienie skanowania antywirusowego określonych obszarów i przetwarzanie szkodliwych obiektów z poziomu wiersza poleceń przedstawia się następująco:

```
avp.com SCAN [<skanowany obiekt >] [<akcja>] [<typy  
plików >] [<wykluczenia>] [<plik konfiguracyjny >]  
[<ustawienia raportowania >] [<ustawienia  
zaawansowane >]
```

W celu wykonania skanowania obiektów można również użyć zadań utworzonych w programie Kaspersky Anti-Virus for Windows Servers uruchamiając wybrane zadanie z poziomu wiersza poleceń (patrz rozdział 13.1 na stronie 165). Zadanie uruchomione zostanie z ustawieniami skonfigurowanymi w interfejsie programu.

Opis parametrów:

<skanowany obiekt > - ten parametr określa listę obiektów, które zostaną przeskanowane na obecność szkodliwego kodu.

Może on zawierać kilka wartości oddzielonych znakiem spacji.

<pliki>	<p>Lista ścieżek dostępu do plików i/lub folderów, które zostaną przeskanowane. Można podać bezwzględne lub względne ścieżki dostępu. Elementy listy oddzielone są znakiem spacji.</p> <p>Informacje:</p> <p>Jeżeli nazwa obiektu zawiera spację należy umieścić ją w cudzysłowie.</p> <p>Po wybraniu określonego foldera przeskanowane zostaną wszystkie pliki znajdujące się w nim.</p>
/MEMORY	Obiekty pamięci systemowej
/STARTUP	Obiekty startowe
/MAIL	Pocztowe bazy danych
/REMDRIVES	Wszystkie napędy wymienne
/FIXDRIVES	Wszystkie dyski wewnętrzne
/NETDRIVES	Wszystkie dyski sieciowe
/QUARANTINE	Obiekty poddane kwarantannie
/ALL	Pełne skanowanie
/@:<filelist.lst>	<p>Ścieżka dostępu do pliku zawierającego listę obiektów i folderów przeznaczonych do skanowania. Plik powinien posiadać format tekstowy i każdy skanowany obiekt musi znajdować się w nowej linii.</p> <p>Można podać bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli ścieżka zawiera spację należy umieścić ją w cudzysłowie.</p>
<p><akcja> - ten parametr zawiera zestaw akcji podejmowanych po wykryciu podczas skanowania szkodliwych obiektów. Jeżeli parametr nie został zdefiniowany domyślną akcją jest /i8.</p>	
/i0	na obiekcie nie są podejmowane żadne akcje; informacja na ten temat zostanie zapisana w raporcie.

/i1	Leczenie zainfekowanych obiektów lub ich pomijanie w przypadku braku możliwości wyleczenia
/i2	Leczenie zainfekowanych obiektów lub ich usuwanie w przypadku braku możliwości wyleczenia. Wykluczenia: nie należy usuwać zainfekowanych obiektów wchodzących w skład plików złożonych; Usuwane są obiekty złożone posiadające wykonywalne nagłówki (archiwa sfx) (jest to ustawienie domyślne).
/i3	Leczenie zainfekowanych obiektów lub ich usuwanie w przypadku braku możliwości wyleczenia. Usuwanie wszystkich obiektów złożonych jeżeli nie można usunąć zainfekowanych załączników.
/i4	Leczenie zainfekowanych obiektów lub ich usuwanie w przypadku braku możliwości wyleczenia. Usuwanie wszystkich obiektów złożonych jeżeli nie można usunąć zainfekowanych załączników.
/i8	Pytaj o akcję po wykryciu zainfekowanego obiektu.
/i9	Pytaj o akcję po zakończeniu skanowania.
<typy plików> - ten parametr definiuje typy plików, które będą skanowane. Jeżeli parametr nie został zdefiniowany, wartością domyślną jest /fi.	
/fe	Skanowanie tylko potencjalnie infekowalnych plików (według rozszerzenia)
/fi	Skanowanie tylko potencjalnie infekowalnych plików według zawartości (wartość domyślna)
/fa	Skanowanie wszystkich plików
<wykluczenia> - ten parametr definiuje obiekty wykluczone z obszaru skanowania. Może on zawierać wiele wartości oddzielonych spacją.	
-e:a	Wyłączenie skanowania archiwów

-e:b	Wyłączenie skanowania pocztowych baz danych
-e: m	Wyłączenie skanowania pocztowych formatów tekstowych
-e:<maska plików>	Wykluczenie ze skanowania obiektów o podanej masce
-e:<liczba sekund>	Pominięcie skanowania obiektów, jeżeli trwa ono dłużej niż <liczba sekund> .
-es:<rozmiar>	Pominięcie skanowania plików większych (w MB) niż <rozmiar> .
<p><plik konfiguracyjny> - definiuje ścieżkę dostępu do pliku ustawień zawierającego ustawienia programu używane podczas skanowania.</p> <p>Plik konfiguracyjny jest zapisywany w formacie binarnym (.dat), jeżeli nie zostanie określony inny format i może zostać wykorzystany później do importowania ustawień na innych komputerach.</p> <p>Można podać bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli parametr nie został zdefiniowany, użyte zostaną wartości zdefiniowane w interfejsie programu Kaspersky Anti-Virus for Windows Servers.</p>	
/C:<plik_ustawień >	Użycie wartości ustawień zawartych w pliku <plik_ustawień>
<p><ustawienia raportowania> - ten parametr określa format raportu dla wyników skanowania.</p> <p>Można podać bezwzględną lub względną ścieżkę do pliku. Jeżeli parametr nie został zdefiniowany, wyniki skanowania oraz wszystkie zdarzenia wyświetlane będą na ekranie.</p>	
/R:<plik_raportu >	Zapisywanie tylko ważnych zdarzeń do pliku
/RA:<plik_raportu>	Zapisywanie wszystkich zdarzeń do pliku
<p><ustawienia zaawansowane> – ustawienia, które określają użycie technologii skanowania antywirusowego.</p>	
/iChecker=<on:off>	Włączenie/ wyłączenie wykorzystywania technologii iChecker.

/iSwift=<on:off>	Włączenie/ wyłączenie wykorzystywania technologii iSwift.
-------------------------------	---

Przykłady:

*Uruchomienie skanowania pamięci RAM, programów uruchamianych przy starcie systemu operacyjnego, pocztowych baz danych, folderów **Moje Dokumenty i Program Files** oraz pliku **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Zatrzymanie skanowania żądanych obiektów i uruchomienie pełnego skanowania komputera, następnie kontynuowanie skanowania żądanych obiektów:

```
avp.com PAUSE SCAN_OBJECTS
/password=<hasło_użytkownika>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Skanowanie pamięci RAM oraz obiektów zapisanych w pliku **object2scan.txt**. Użycie pliku konfiguracyjnego **scan_setting.txt**. Wygenerowanie raportu zawierającego wszystkie zdarzenia po zakończeniu skanowania:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

13.4. Aktualizacja programu

Składnia polecenia aktualizacji modułów programu Kaspersky Anti-Virus for Windows Servers oraz sygnatur zagrożeń z poziomu wiersza poleceń jest następująca:

```
avp.com UPDATE [<ścieżka_dostępu/URL>]
[/R[A]:<plik_raportu>] [/C:<plik_ustawień>] [/APP]
```

Opis parametrów:

[<ścieżka_dostępu/U RL>]	Serwer HTTP, FTP lub folder sieciowy zawierający aktualizacje. Jeżeli ścieżka nie zostanie zdefiniowana, źródło aktualizacji pobrane zostanie z ustawień modułu aktualizacji.
-----------------------------	---

<pre>/R[A]:<plik_raport ></pre>	<p>/R:<plik_raportu> – zapisywanie tylko ważnych zdarzeń do raportu.</p> <p>/R[A]:<plik_raport> – zapisz w raporcie wszystkie zdarzenia.</p> <p>Można podać bezwzględną lub względną ścieżkę do pliku. Jeżeli parametr nie został zdefiniowany, wyniki skanowania oraz wszystkie zdarzenia wyświetlane będą na ekranie.</p>
<pre>/C:<plik_ustawień></pre>	<p>Ścieżka dostępu do pliku konfiguracyjnego zawierającego ustawienia aktualizacji.</p> <p>Plik konfiguracyjny jest plikiem tekstowym, zawierającym grupę ustawień wiersza poleceń dla aktualizacji programu.</p> <p>Można podać bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli parametr nie został zdefiniowany użyte zostaną wartości zdefiniowane w interfejsie programu Kaspersky Anti-Virus for Windows Servers.</p>
<pre>/APP</pre>	<p>Aktualizacja modułów programu</p>

Przykłady:

Aktualizacja sygnatur zagrożeń po zapisaniu wszystkich zdarzeń w raporcie:

```
avp.com UPDATE /RA:avbases_upd.txt
```

Aktualizacja modułów programu Kaspersky Anti-Virus for Windows Servers przy użyciu ustawień zawartych w pliku updateapp.ini:

```
avp.com UPDATE /APP /C:updateapp.ini
```

13.5. Cofanie aktualizacji

Składnia polecenia:

```
ROLLBACK [/R[A]:<plik_raportu >] [/password=<hasło>]
```

/R[A]:<plik_raportu>	<p>/R:<plik_raportu> – zapisywanie tylko ważnych zdarzeń do raportu.</p> <p>/R[A]:<plik_raportu> – zapisywanie w raporcie wszystkich zdarzeń.</p> <p>Można podać bezwzględną lub względną ścieżkę do pliku. Jeżeli parametr nie został zdefiniowany, wyniki skanowania oraz wszystkie zdarzenia wyświetlane będą na ekranie.</p>
<hasło>	Hasło dostępu do programu Kaspersky Anti-Virus przypisane w interfejsie aplikacji.

Należy pamiętać o tym, że nie można uruchomić tego polecenia bez wprowadzenia hasła.

Przykłady:

```
avp.com ROLLBACK /RA:rollback.txt
[/password=<hasło>]
```

13.6. Eksportowanie ustawień

Składnia polecenia:

```
avp.com EXPORT <profil> <nazwa_pliku>
```

Opis parametrów:

<profil>	<p>Eksportowanie ustawień modułu Ochrona plików lub zadania.</p> <p>Jako <profil> można użyć dowolnej wartości opisanej w rozdziale 13.2 na stronie 166.</p>
-----------------------	---

<nazwa_pliku>	<p>Ścieżka dostępu pliku, do którego wyeksportowane zostaną ustawienia Kaspersky Anti-Virus for Windows Servers. Można podać bezwzględną lub względną ścieżkę do pliku.</p> <p>Plik konfiguracyjny jest zapisywany w formacie binarnym (.dat), jeżeli nie zostanie określony inny format i może zostać wykorzystany później do importowania ustawień na innych komputerach. Plik konfiguracyjny może zostać zapisany jako plik tekstowy. W tym celu, w nazwie pliku należy użyć rozszerzenia .txt. Należy pamiętać o tym, że ustawienia ochrony nie mogą być importowane z pliku tekstowego.</p>
----------------------------	--

Przykłady:

```
avp.com EXPORT c:\settings.dat
```

13.7. Importowanie ustawień

Składnia polecenia:

```
avp.com IMPORT <plik_ustawień> [/password=<hasło>]
```

<plik_ustawień>	<p>Ścieżka dostępu do pliku, z którego mają zostać zaimportowane ustawienia Kaspersky Anti-Virus for Windows Servers. Można podać bezwzględną lub względną ścieżkę do pliku.</p> <p>Ustawienia mogą zostać zaimportowane wyłącznie z plików binarnych.</p>
------------------------------	--

Przykłady:

```
avp.com IMPORT c:\settings.dat  
/password=<hasło_użytkownika >
```

13.8. Uruchamianie programu

Składnia polecenia:

```
avp.com
```

13.9. Zatrzymywanie działania programu

Składnia polecenia:

```
avp.com EXIT /password=<hasło>
```

<hasło>	Hasło do programu Kaspersky Anti-Virus wprowadzone w interfejsie programu.
---------	--

Należy pamiętać o tym, że nie można uruchomić tego polecenia bez wprowadzenia hasła.

13.10. Przeglądanie pomocy

Polecenie to służy do przeglądania pomocy na temat składni wiersza poleceń:

```
avp.com [ /? | HELP ]
```

W celu wyświetlenia pomocy dotyczącej składni określonego polecenia należy użyć następujących poleceń:

```
avp.com <polecenie> /?
avp.com HELP <polecenie>
```

13.11. Kody zwracane przez interfejs wiersza poleceń

Niniejsza sekcja zawiera listę kodów zwracanych w wierszu poleceń. Kody ogólne mogą być zwracane w wierszu poleceń przez dowolne polecenie. Kody zwracane przez program obejmują kody ogólne oraz kody specyficzne dla konkretnego typu zadania.

Kody ogólne	
0	Operacja zakończona pomyślnie
1	Błędna wartość parametru
2	Nieznany błąd

3	Błąd podczas wykonywania zadania
4	Zadanie zostało anulowane
Kody zwracane przez zadania skanowania antywirusowego	
101	Wszystkie niebezpieczne obiekty zostały przetworzone
102	Wykryto niebezpieczne obiekty

ROZDZIAŁ 14. MODYFIKOWANIE, NAPRAWIANIE I USUWANIE PROGRAMU

Aplikacja może zostać zdezinstalowana w następujący sposób:

- przy użyciu kreatora instalacji programu (patrz rozdział 14.2 na stronie 181).
- z poziomu wiersza poleceń (patrz rozdział 14.2 na stronie 181).
- przy użyciu Kaspersky Administration Kit (szczegółowe informacje znajdują się w podręczniku administratora Kaspersky Administration Kit)

14.1. Modyfikowanie, naprawianie i usuwanie programu przy użyciu kreatora instalacji

W przypadku wykrycia błędów podczas funkcjonowania programu w skutek nieprawidłowej jego konfiguracji lub uszkodzenia pliku, należy dokonać naprawy programu.

W celu naprawy lub modyfikacji brakujących składników programu Kaspersky Anti-Virus for Windows Servers lub usunięcia programu należy:

1. Zakończyć działanie programu. W tym celu należy kliknąć prawym przyciskiem myszy na ikonie programu znajdującej się w zasobniku systemowym i z menu kontekstowego wybrać polecenie **Zakończ**.
2. Włożyć płytę instalacyjną programu do napędu CD-ROM, jeżeli użyta została ona do instalacji programu. Jeżeli program Kaspersky Anti-Virus for Windows Servers zainstalowany został z innego źródła (folder publiczny, folder na dysku twardym itp.), należy upewnić się, że pliki instalacyjne znajdują się w tym folderze i można uzyskać do nich dostęp.
3. Kliknąć **Start** → **Programy** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Modyfikuj, Napraw lub Usuń**.

Następnie uruchomiony zostanie kreator instalacji programu. Poniżej przedstawione zostały etapy naprawy, modyfikowania lub usuwania programu.

Step 1. Uruchomienie kreatora instalacji

Po wykonaniu wszystkich opisanych wyżej kroków niezbędnych do naprawy lub modyfikacji programu otwarte zostanie okno instalacyjne Kaspersky Anti-Virus for Windows Servers. W celu kontynuacji należy kliknąć przycisk **Dalej**.

Step 2. Wybór operacji



Na tym etapie należy wybrać operację, która ma zostać uruchomiona. Możliwe jest modyfikowanie składników programu, naprawianie zainstalowanych składników, usuwanie składników lub całego programu. W celu uruchomienia żądanej operacji należy kliknąć odpowiedni przycisk. W zależności od wybranej opcji program wykona odpowiednią operację.

Modyfikacja programu podobna jest do instalacji programu przy użyciu niestandardowych ustawień, gdzie użytkownik może definiować składniki, które mają zostać zainstalowane, a które mają zostać usunięte.

Naprawa programu zależy od zainstalowanych składników. Naprawione zostaną wszystkie pliki zainstalowanych składników i dla każdego z nich ustawiony zostanie zalecany poziom bezpieczeństwa.

Uwaga!

Jeżeli Kaspersky Anti-Virus 6.0 zostanie zdeinstalowany zdalnie, serwer nie zostanie ponownie uruchomiony. W celu pełnego usunięcia składników aplikacji i zapewnienia poprawnego działania systemu operacyjnego zalecane jest ponowne uruchomienie systemu operacyjnego.

Podczas usuwania programu można określić, które dane utworzone i używane przez program mają zostać zapisane na komputerze. Aby usunąć wszystkie dane Kaspersky Anti-Virus for Windows Servers należy wybrać opcję  **Kompletna dezinstalacja**. Aby zachować dane programu należy wybrać opcję  **Zapisz obiekty aplikacji** oraz wybrać obiekty, które zostaną zapisane:

Dane aktywacyjne – informacje na temat aktywacji programu.

Sygnatury zagrożeń – kompletny zestaw sygnatur zagrożeń niebezpiecznych programów, wirusów i innych zagrożeń zawartych w ostatniej aktualizacji.

Kopie zapasowe – kopie zapasowe usuniętych lub wyleczonych obiektów. Zalecane jest ich zapisanie na wypadek potrzeby ich późniejszego przywrócenia.

Pliki kwarantanny – pliki potencjalnie zainfekowane przez wirusy lub ich modyfikacje. Pliki te zawierają kod podobny do kodu znanego wirusa, lecz nie

można jednoznacznie stwierdzić czy są one szkodliwe. Zalecane jest zapisanie tych plików, ponieważ mogą one zostać wyleczone po aktualizacji sygnatur zagrożeń lub mogą nie stanowić zagrożenia.

Ustawienia aplikacji – ustawienia programu Kaspersky Anti-Virus.

Dane iSwift – baza danych zawierająca informacje dotyczące obiektów skanowanych w systemie plików NTFS. Informacje te mogą zwiększyć prędkość skanowania. W przypadku korzystania z tej bazy danych Kaspersky Anti-Virus for Windows Servers skanuje tylko te pliki, które uległy modyfikacji od czasu ostatniego skanowania.

Uwaga!

Jeżeli pomiędzy dezinstalacją jednej wersji programu Kaspersky Anti-Virus for Windows Servers, a instalacją innej upłynął długi okres czasu, nie jest zalecane używanie bazy danych iSwift zapisanej wcześniej. W tym czasie niebezpieczny program może dokonać penetracji komputera, ponieważ nie zostanie on wykryty przez bazę danych, co może spowodować infekcję.

W celu uruchomienia wybranej operacji należy kliknąć przycisk **Dalej**. Program rozpocznie kopiowanie niezbędnych plików do komputera lub usuwanie wybranych składników i danych.

Step 3. Lista programów mogących wpływać na poprawną modyfikację, naprawienie lub usunięcie programu

Jeżeli program wykryje, że jego pliki są wykorzystywane przez inne aplikacje zostaną one wyświetlone na ekranie. Z reguły lista zawiera aplikacje, wykorzystujące wtyczki Kaspersky Anti-Virus for Windows Servers. Użytkownik zostanie poproszony o zakończenie działania tych programów.

Aby kontynuować działanie, należy kliknąć **Pomiń**. Aby kontynuować działanie po zamknięciu tych aplikacji należy kliknąć **Ponów**.

Step 4. Kończenie modyfikacji, naprawy lub usunięcia programu

Po zakończeniu procesu modyfikacji, instalacji lub usuwania programu, na ekranie zostanie wyświetlony odpowiedni komunikat.

Proces usuwania programu wymaga ponownego uruchomienia komputera, w celu zastosowania zmian wprowadzonych w systemie. Program zapyta użytkownika, czy chce on ponownie uruchomić komputer. Należy kliknąć **Tak**, aby natychmiast ponownie uruchomić komputer. Aby uruchomić ponownie komputer w późniejszym terminie, należy kliknąć **Nie**.

14.2. Dezinstalacja programu z poziomu wiersza poleceń

W celu dezinstalacji programu Kaspersky Anti-Virus for Windows Servers z poziomu wiersza poleceń należy wpisać polecenie:

```
msiexec /x <nazwa_pakietu >
```

Uruchomiony zostanie kreator instalacji. Może on zostać wykorzystany do dezinstalacji aplikacji.

Można również użyć poniższych poleceń.

W celu dezinstalacji aplikacji w tle bez ponownego uruchamiania komputera (użytkownik będzie musiał ręcznie uruchomić ponownie komputer po zakończeniu dezinstalacji) należy wpisać:

```
msiexec /x <nazwa_pakietu > /qn
```

W celu dezinstalacji aplikacji w tle z ponownym uruchomieniem komputera, należy wpisać:

```
msiexec /x <nazwa_pakietu> ALLOWREBOOT=1 /qn
```

Jeżeli podczas instalacji programu zostało wprowadzone hasło chroniące przed dezinstalacją programu poprzez Kaspersky Administration Kit, podczas dezinstalacji programu należy wprowadzić to hasło. W przeciwnym przypadku nie będzie można usunąć programu.

W celu dezinstalacji aplikacji w tle i wprowadzenia hasła poprzez Kaspersky Administration Kit, należy wpisać:

```
msiexec /x <nazwa_pakietu> KLUNINSTPASSWD=***** /qn
```

ROZDZIAŁ 15. NAJCZĘŚCIEJ ZADAWANE PYTANIA

Ten rozdział zawiera odpowiedzi na najczęściej zadawane pytania dotyczące instalacji, konfiguracji i użytkowania programu Kaspersky Anti-Virus for Windows Servers; poniżej znajdują się szczegółowe odpowiedzi na te pytania.

Pytanie: *Czy można wykorzystywać program Kaspersky Anti-Virus 6.0 for Windows Servers z aplikacjami antywirusowymi innych producentów?*

Nie. Przed rozpoczęciem instalacji programu Kaspersky Anti-Virus for Windows Servers zaleca się usunięcie wszelkich innych aplikacji antywirusowych zainstalowanych na komputerze w celu uniknięcia konfliktów.

Pytanie: *Kaspersky Anti-Virus for Windows Servers nie skanuje plików, które zostały już wcześniej przeskanowane. Dlaczego?*

To prawda. Kaspersky Anti-Virus for Windows Servers nie powtarza skanowania plików, które nie uległy zmianie od czasu ostatniego skanowania.

Jest to możliwe dzięki zastosowaniu nowych technologii iChecker oraz iStream. Technologie te wykorzystują bazy danych sum kontrolnych oraz alternatywne strumienie danych w systemie plików NTFS.

Pytanie: *Do czego potrzebny jest klucz licencyjny? Czy Kaspersky Anti-Virus for Windows Servers będzie działał bez niego?*

Kaspersky Anti-Virus for Windows Servers nie uruchomi się bez klucza licencyjnego, możliwe jednak będzie uzyskanie dostępu do modułu aktualizacji oraz do sekcji związanej z pomocą techniczną.

Jeżeli użytkownik chce przetestować program Kaspersky Anti-Virus for Windows Servers przed jego zakupem, firma Kaspersky Lab może dostarczyć 30-dniowy klucz testowy. Po upływie tego okresu czasu klucz utraci ważność.

Pytanie: *Po zainstalowaniu programu Kaspersky Anti-Virus for Windows Servers system operacyjny zaczął się "dziwnie zachowywać" (pojawiają się "niebieskie ekrany", system często się restartuje itp.) Co należy zrobić?*

Konflikty programu Kaspersky Anti-Virus for Windows Servers z innymi aplikacjami zainstalowanymi na komputerze występują bardzo rzadko, jednak nie można ich całkowicie wykluczyć.

W celu przywrócenia poprawnej funkcjonalności systemu należy:

1. Wcisnąć i przytrzymać klawisz **F8** podczas włączania komputera aż do pojawienia się na ekranie menu startowego.
2. Wybrać **Tryb awaryjny** i uruchomić system operacyjny.
3. Otworzyć Kaspersky Anti-Virus for Windows Servers.
4. W oknie głównym programu kliknąć odsyłacz **Ustawienia** i wybrać sekcję **Ochrona**.
5. Usunąć zaznaczenie z opcji **Uruchom Kaspersky Anti-Virus for Windows Servers 6.0** podczas ładowania systemu i kliknąć **OK**.
6. Uruchomić system operacyjny w normalnym trybie.

Skontaktować się z działem pomocy technicznej. Informacje o możliwościach kontaktu z działem pomocy technicznej można znaleźć na stronie internetowej firmy Kaspersky Lab (**Usługi→Pomoc techniczna**). Należy opisać problem oraz warunki, w których się pojawia.

Do wiadomości należy dołączyć plik zawierający kompletne informacje o systemie operacyjnym Microsoft Windows. W celu utworzenia takiego pliku należy:

1. Kliknąć prawym przyciskiem myszy element **Mój komputer** i z menu kontekstowego wybrać **Właściwości**.
2. W oknie **Właściwości** systemu przejść do zakładki **Zaawansowane** i kliknąć przycisk **Ustawienia** w sekcji **Uruchamianie i odzyskiwanie**.
3. W oknie **Uruchamianie i odzyskiwanie** wybrać z listy rozwijalnej znajdującej się w sekcji **Zapisywanie informacji o debugowaniu** element **Pełny zrzut pamięci**.


Domyślnie zrzut pamięci zapisywany jest w folderze systemowym z nazwą *memory.dmp*. W celu zapisania go w innym folderze należy zmienić zawartość sekcji Plik zrzutu.

4. Wykonać czynności, które spowodowały wystąpienie problemu związanego z działaniem programu Kaspersky Anti-Virus for Windows Servers.
5. Upewnić się, że pełny zrzut pamięci został pomyślnie zapisany.

DODATEK 1. INFORMACJE DODATKOWE

Ten dodatek zawiera dodatkowe materiały dotyczące formatów plików i masek rozszerzeń używanych w ustawieniach programu Kaspersky Anti-Virus for Windows Servers.

1.1. Lista plików skanowanych według rozszerzenia

Po wybraniu opcji  **Skanuj programy i dokumenty (według rozszerzenia)** moduł Ochrony plików będzie skanował na obecność wirusów pliki posiadające następujące rozszerzenia.

com – plik wykonywalny nie większy niż 64 KB

exe – plik wykonywalny lub archiwum samorozpakowujące

sys – sterownik systemowy

prg – program tekstowy dla dBase, Clipper lub Microsoft Visual FoxPro lub program dla WAVmaker

bin – plik binarny

bat – plik wsadowy

cmd – plik wiersza poleceń dla systemu Microsoft Windows NT (podobny do pliku .bat dla systemu DOS), OS/2

dpl – skompresowana biblioteka Borland Delphi

dll – biblioteka ładowana dynamicznie

scr – wygaszacz ekranu dla Microsoft Windows

cpl – moduł panelu sterowania dla Microsoft Windows

ocx – obiekt Microsoft OLE (Object Linking and Embedding)

tsp – program uruchamiany trybie split-time

drv – sterownik urządzenia

vxd – wirtualny sterownik urządzenia Microsoft Windows

pif – plik informacyjny o aplikacji

lnk – plik skrótu Microsoft Windows

reg – klucz rejestru systemowego Microsoft Windows

ini – plik inicjacyjny

cla – klasa Java
vbs – skrypt Visual Basic
vbe – rozszerzenie BIOS-u kart graficznych
js, jse – tekst źródłowy JavaScript
htm – dokument hipertekstowy
htt – nagłówek hipertekstowy Microsoft Windows
hta – plik hipertekstowy wykorzystywany do aktualizacji rejestru systemowego
asp – skrypt Active Server Pages
chm – skompilowany plik HTML
pht – plik HTML z wbudowanymi skryptami PHP
php – skrypt wykorzystywany do tworzenia plików HTML
wsh – plik hosta skryptów systemu Windows
wsf – skrypt Microsoft Windows
the – tapeta pulpitu Microsoft Windows 95
hlp – plik pomocy w formacie Win Help
eml – plik wiadomości pocztowej Microsoft Outlook Express
nws – plik wiadomości grup dyskusyjnych Microsoft Outlook Express
msg – plik wiadomości pocztowej Microsoft Mail
plg – Poczta elektroniczna
mbx – baza danych zapisanych wiadomości Microsoft Office Outlook
doc – dokument Microsoft Office Word
dot – szablon dokumentu Microsoft Office Word
fpm – program bazodanowy, plik startowy dla Microsoft Visual FoxPro
rtf – dokument Rich Text Format
shs – wycinek Shell Scrap Object Handler
dwg – baza danych AutoCAD blueprint
msi – pakiet instalatora Microsoft Windows
otm – projekt VBA dla Microsoft Office Outlook
pdf – dokument Adobe Acrobat
swf – plik Shockwave Flash
jpg, jpeg, png – skompresowany format graficzny
emf – rozszerzony format graficzny nowej generacji stosowany w Microsoft Windows, zawierający instrukcje dla systemu operacyjnego jak wyświetlać grafikę wektorową i rastrową. Pliki EMF nie są obsługiwane przez 16-bitowe wersje Microsoft Windows
ico – plik ikony

ov? – Pliki wykonywalne Microsoft DOS

*xl** – dokumenty i pliki Microsoft Office Excel, takie jak: *xla* - rozszerzenie Microsoft Office Excel, *xlc* - diagram, *xlt* - szablon dokumentu itd.

*pp** – dokumenty i pliki Microsoft Office PowerPoint, takie jak: *pps* - slajd Microsoft Office PowerPoint, *ppt* - prezentacja itd.

*md** – dokumenty i pliki Microsoft Office Access, takie jak: *mda* - grupa robocza Microsoft Office Access, *mdb* - baza danych itd.

Należy pamiętać, że bieżące rozszerzenie pliku może nie odpowiadać wewnętrznemu formatowi pliku.

1.2. Możliwe maski wykluczeń

Poniżej znajduje się kilka przykładów dozwolonych masek, które mogą zostać użyte podczas tworzenia listy wykluczeń dla plików:

1. Maski nie posiadające ścieżek dostępu do plików:
 - ***.exe** – wszystkie pliki posiadające rozszerzenie **.exe**
 - ***.ex?** – wszystkie pliki posiadające rozszerzenie **.ex?**, gdzie **?** może być dowolnym znakiem
 - **test** – wszystkie pliki posiadające nazwę **test**
2. Maski posiadające bezwzględne ścieżki dostępu do plików:
 - **C:\dir\.*** lub **C:\dir*** lub **C:\dir** – wszystkie pliki znajdujące się w folderze **C:\dir**
 - **C:\dir*.exe** – wszystkie pliki posiadające rozszerzenie **.exe** znajdujące się w folderze **C:\dir**
 - **C:\dir*.ex?** – wszystkie pliki posiadające rozszerzenie **.ex?** znajdujące się w folderze **C:\dir**, gdzie **?** może być dowolnym znakiem
 - **C:\dir\test** – tylko plik **C:\dir\test**
 - W celu wyłączenia rekursywnego skanowania plików w podfolderach tego foldera, należy usunąć zaznaczenie z pola **Włączając podfoldery**.
3. Maski posiadające względne ścieżki dostępu do plików:
 - **dir\.*** lub **dir*** lub **dir** – wszystkie pliki we wszystkich folderach **dir**

- **dir\test** – wszystkie pliki posiadające nazwę *test* znajdujące się w folderach *dir*
- **dir*.exe** – wszystkie pliki posiadające rozszerzenie *.exe* znajdujące się we wszystkich folderach *dir*
- **dir*.ex?** – wszystkie pliki posiadające rozszerzenie *.ex?* znajdujące się we wszystkich folderach *C:\dir*, gdzie ? może być dowolnym znakiem

W celu wyłączenia rekursywnego skanowania plików w podfolderach tego foldera, należy usunąć zaznaczenie z pola **Włączając podfoldery**.

Wskazówka:

Maski wykluczeń **.** oraz *** mogą zostać użyte tylko w przypadku zdefiniowania werdyktu wykluczającego zagrożenie zgodnego z nazewnictwem stosowanym w Encyklopedii Wirusów. Zdefiniowane zagrożenie nie będzie wykrywane w żadnym obiekcie. Używanie tych masek bez wybierania werdyktu powoduje wyłączenie monitorowania.

Nie jest również zalecane wybieranie jako wykluczenia napędu wirtualnego utworzonego na podstawie foldera systemu plików przy użyciu polecenia *subst*. Nie jest konieczne wykonywanie tej czynności ponieważ podczas skanowania aplikacja traktuje taki napęd wirtualny jak folder i skanuje go.

1.3. Maski zgodne z klasyfikacją Encyklopedii Wirusów

Podczas dodawania zagrożeń o określonym statusie zgodnym z nazewnictwem stosowanym w Encyklopedii Wirusów, można określić:

- pełna nazwa zagrożenia zgodna z nazewnictwem stosowanym w Encyklopedii wirusów dostępnej na stronie www.viruslist.pl (na przykład, **not-a-virus:RiskWare.RemoteAdmin.RA.311** lub **Flooder.Win32.Fuxx**);
- nazwa zagrożenia w oparciu o maskę. Na przykład:
 - **not-a-virus*** – wykluczenie z obszaru skanowania potencjalnie niebezpiecznych programów oraz programów-żartów (jokes).
 - ***Riskware.*** – wykluczenie z obszaru skanowania oprogramowania typu riskware.
 - ***RemoteAdmin.*** – wykluczenie z obszaru skanowania wszystkich narzędzi zdalnej administracji.

DODATEK 2. KASPERSKY LAB

Założona w roku 1997 firma Kaspersky Lab przez wielu ekspertów uważana jest za lidera w dziedzinie zabezpieczeń informacji. Tworzy szeroką gamę programów zabezpieczających i dostarcza wszechstronne i wydajne rozwiązania chroniące komputery i sieci komputerowe przed wszelkimi typami szkodliwych programów, niechcianymi wiadomościami e-mail oraz atakami hakerów.

Kaspersky Lab jest firmą międzynarodową. Główna siedziba firmy znajduje się w Rosji, natomiast filie w Wielkiej Brytanii, Francji, Niemczech, Japonii, USA (Kanadzie), krajach Beneluksu, Chinach, Polsce i Rumunii. We Francji działa także specjalny dział firmy - Europejskie Centrum Badań Antywirusowych. Sieć partnerów Kaspersky Lab składa się z ponad 500 firm na całym świecie.

Obecnie Kaspersky Lab zatrudnia ponad 450 specjalistów. Każdy z nich jest biegły w technologiach antywirusowych, 10 z nich posiada tytuł M.B.A., 16 doktoraty, a dwóch ekspertów posiada członkostwo organizacji Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab oferuje najlepsze systemy zabezpieczeń oparte na doświadczeniu i wiedzy zdobytej na przestrzeni ponad 14 lat walki z wirusami komputerowymi. Dokładna analiza działania wirusów komputerowych pozwala na dostarczenie kompletnej ochrony zarówno przed bieżącymi, jak i przyszłymi zagrożeniami. Odporność na przyszłe ataki jest podstawową polityką bezpieczeństwa zaimplementowaną we wszystkich produktach Kaspersky Lab. Rozwiązania firmy są zawsze przynajmniej o jeden krok przed produktami oferowanymi przez konkurencję.

Lata ciężkiej pracy uczyniły z Kaspersky Lab jednego czołowych producentów oprogramowania zabezpieczającego. Flagowy produkt firmy, Kaspersky Anti-Virus, zapewnia kompletną ochronę wszystkich węzłów sieci, łącznie ze stacjami roboczymi, serwerami plików, bramami pocztowymi, zaporami ogniowymi i komputerami kieszonkowymi. Wygodne i łatwe w użytkowaniu narzędzia zarządzające zapewniają zaawansowaną automatyzację ochrony antywirusowej wewnątrz sieci firmowej. Technologia antywirusowa opracowana przez firmę Kaspersky Lab wykorzystywana jest przez firmy takie jak: Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Izrael), Sybari (USA), G Data (Niemcy), Deerfield (USA), Alt-N (USA), Microworld (Indie), BorderWare (Kanada) itd.

Klienci Kaspersky Lab korzystają z szerokiego zakresu dodatkowych usług, które zapewniają nie tylko stabilne działanie użytkowanych produktów, ale także spełniają specyficzne wymagania firm. Firma Kaspersky Lab uaktualnia sygnatury zagrożeń raz na godzinę. Firma zapewnia swoim klientom pomoc techniczną dostępną przez e-mail i telefon.

2.1. Inne produkty firmy Kaspersky Lab

Kaspersky Lab News Agent

News Agent przeznaczony jest do okresowego dostarczania informacji o nowościach oraz powiadamiania o bieżącym stanie aktywności wirusowej. Program okresowo odczytuje listę dostępnych kanałów z nowościami oraz ich zawartość z serwera firmy Kaspersky Lab.

Produkt posiada następujące możliwości:

Animacja bieżącego stanu aktywności wirusowej na ikonie w zasobniku systemowym.

Zapisywanie i rezygnacja z kanałów nowości.

Pobieranie nowości z każdego wybranego kanału o określonej częstotliwości oraz powiadamianie o świeżych nowościach.

Przeglądanie nowości wybranego kanału.

Przeglądanie listy kanałów i ich stanu.

Otwieranie stron ze szczegółami nowości w przeglądarce.

News Agent jest niezależną aplikacją przeznaczoną dla systemu Windows, która może być używana niezależnie lub może być dołączona do innych zestawów oprogramowania firmy Kaspersky Lab.

Kaspersky® OnLine Scanner

Program ten jest darmową usługą przeznaczoną dla użytkowników odwiedzających witrynę firmy Kaspersky Lab. Usługa ta umożliwia wydajne skanowanie antywirusowe komputera w trybie online oraz wyleczenie zainfekowanych plików. Kaspersky OnLine Scanner uruchamiany jest w przeglądarce internetowej. Dlatego też, użytkownicy mogą szybko przetestować swoje komputery w przypadku podejrzenia infekcji. Przy użyciu tej usługi, możliwe jest:

Wykluczanie z obszaru skanowania archiwów oraz pocztowych baz danych.

Wybór standardowych/rozszerzonych antywirusowych baz danych do skanowania.

Zapisywanie raportów o wynikach skanowania w plikach txt lub html.

Kaspersky® OnLine Scanner Pro

Program ten jest darmową usługą przeznaczoną dla użytkowników odwiedzających witrynę firmy Kaspersky Lab. Usługa ta umożliwia wydajne skanowanie antywirusowe komputera w trybie online oraz wyleczenie

zainfekowanych plików. Kaspersky OnLine Scanner Pro uruchamiany jest w przeglądarce internetowej. Przy użyciu tej usługi, możliwe jest:

Wykluczanie z obszaru skanowania archiwów oraz pocztowych baz danych.

Wybór standardowych/rozszerzonych antywirusowych baz danych do skanowania.

Zapisywanie raportów o wynikach skanowania w plikach txt lub html.

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 stworzony został w celu ochrony komputerów osobistych przed szkodliwym oprogramowaniem jako optymalna kombinacja metod ochrony antywirusowej i nowych technologii ochrony proaktywnej.

Program zapewnia kompleksową ochronę antywirusową włączając:

- Skanowanie antywirusowe ruchu pocztowego przesyłanego przy użyciu protokołów transmisji danych (POP3, IMAP i NNTP dla odbieranych wiadomości e-mail oraz SMTP dla wysyłanych wiadomości e-mail) niezależnie od używanego klienta pocztowego oraz leczenie pocztowych baz danych.
- Skanowanie antywirusowe w czasie rzeczywistym ruchu Internetowego przesyłanego przez protokół HTTP.
- Skanowanie antywirusowe indywidualnych plików, folderów lub dysków twardych. Ponadto, użytkownik ma do dyspozycji predefiniowane zadania skanowania antywirusowego dla obszarów krytycznych i obiektów startowych systemu operacyjnego.

Ochrona proaktywna oferuje następujące funkcje:

Kontrolę integralności aplikacji. Program pozwala użytkownikom na tworzenie listy kontrolowanych aplikacji. Pozwala to zapobiec naruszeniu integralności aplikacji w przypadku działalności szkodliwego oprogramowania.

Monitorowanie procesów w pamięci RAM. Kaspersky Anti-Virus 6.0 powiadamia użytkowników o wykryciu niebezpiecznych, podejrzanych lub ukrytych procesów oraz w przypadku wystąpienia nieautoryzowanych zmian standardowych procesów.

Monitorowanie zmian w rejestrze systemowym odpowiadające kontroli wewnętrznego rejestru systemowego.

Blokowanie niebezpiecznych makr VBA w dokumentach pakietu Microsoft Office.

Przywracanie systemu po jego uszkodzeniu przez szkodliwy program typu spyware realizowane poprzez rejestrowanie wszystkich zmian w rejestrze systemowym komputera i systemie plików w celu ich cofnięcia.

Kaspersky® Internet Security 6.0

Kaspersky Internet Security 6.0 to zintegrowane rozwiązanie służące do ochrony komputerów przed wszelkimi zagrożeniami: wirusami, hackerami, spamem oraz oprogramowaniem spyware. Łatwy w obsłudze interfejs programu umożliwia konfigurację i zarządzanie wszystkimi jego składnikami.

Antywirusowe składniki ochrony pełnią następujące funkcje:

Skanowanie antywirusowe ruchu pocztowego przesyłanego przy użyciu protokołów transmisji danych (POP3, IMAP i NNTP dla odbieranych wiadomości e-mail oraz SMTP dla wysyłanych wiadomości e-mail) niezależnie od używanego klienta pocztowego oraz leczenie pocztowych baz danych. Program zawiera wtyczki dla najpopularniejszych programów pocztowych (Microsoft Office Outlook, Microsoft Outlook Express i The Bat!) oraz posiada możliwość leczenia ich pocztowych baz danych.

Skanowanie antywirusowe w czasie rzeczywistym ruchu Internetowego przesyłanego przez protokół HTTP.

Skanowanie antywirusowe indywidualnych plików, folderów lub dysków twardych. Ponadto, użytkownik ma do dyspozycji predefiniowane zadania skanowania antywirusowego dla obszarów krytycznych i obiektów startowych systemu operacyjnego.

Ochrona proaktywna: program nieustannie monitoruje aktywność aplikacji i procesów uruchomionych w pamięci komputera zapobiegając szkodliwym zmianom w systemie plików oraz rejestrze systemowym oraz pozwala także na cofnięcie wszystkich zmian wykonanych w systemie przez szkodliwe programy.

Ochrona przed oszustwami internetowymi jest zapewniana dzięki możliwości rozpoznawania phishingu. Mechanizm ten zapobiega wyciekowi poufnych informacji (przede wszystkim haseł, numerów kont bankowych oraz kart kredytowych) i blokuje uruchamianie niebezpiecznych skryptów występujących na stronach WWW, okien wyskakujących oraz banerów reklamowych. Funkcja **blokowania nieautoryzowanych połączeń** telefonicznych zapewnia, że modem użytkownika nie będzie wykorzystywany przez szkodliwe programy.

Kaspersky Internet Security 6.0 **rejestruje próby skanowania portów komputera**, co bardzo często poprzedza wystąpienie ataku sieciowego, i skutecznie chroni przed wszystkimi znanymi rodzajami ataków hackerów. Program wykorzystuje reguły w celu kontrolowania ruchu sieciowego i śledzi wszystkie pakiety danych przepływające przez komputer. **Tryb ukrycia** (wykorzystujący technologię SmartStealth) **uniemożliwia wykrycie chronionego komputera w sieci**. Po włączeniu tego trybu program zezwoli wyłącznie na aktywność sieciową zainicjowaną przez użytkownika.

Aplikacja wykorzystuje złożone mechanizmy filtrowania antyspamowego dla przychodzących wiadomości e-mail:

- weryfikacja czarnych i białych list (włącznie z adresami stron zawierających phishing)
- analiza fraz występujących w treści wiadomości.

- analiza treści wiadomości przy użyciu samouczącego się algorytmu.
- rozpoznawanie spamu w grafice.

Kaspersky® Security for PDA

Kaspersky Security for PDA zapewnia skuteczną ochronę antywirusową danych przechowywanych na urządzeniach PDA oraz smartfonach. Program zawiera optymalne połączenie następujących narzędzi antywirusowych:

- **skaner antywirusowy** pozwalający na skanowanie danych przechowywanych na urządzeniu PDA lub smartfonie oraz kartach pamięci na żądanie użytkownika;
- **monitor antywirusowy** służący do wykrywania wirusów w plikach kopiowanych z innych komputerów przenośnych lub przesyłanych z wykorzystaniem technologii HotSync.

Kaspersky Security for PDA chroni komputer kieszonkowy (PDA) przed nieautoryzowanym dostępem poprzez szyfrowanie zarówno dostępu do urządzenia jak i danych przechowywanych na kartach pamięci.

Kaspersky Anti-Virus Mobile

Kaspersky Anti-Virus Mobile oferuje ochronę antywirusową dla urządzeń przenośnych działających pod kontrolą systemu operacyjnego Symbian OS oraz Microsoft Windows Mobile. Program obejmuje następujące funkcje:

- **Skanowanie na żądanie** pamięci urządzenia, kart pamięci oraz wybranych folderów lub plików. Wykryte zainfekowane obiekty mogą zostać przeniesione do foldera kwarantanny lub usunięte.
- **Skanowanie w czasie rzeczywistym** – automatyczne skanowanie wszystkich przychodzących lub zmodyfikowanych obiektów podczas uzyskiwania dostępu do nich
- **Terminarz skanowania danych** przechowywanych w pamięci urządzenia
- **Ochrona przed spamem docierającym w wiadomościach sms oraz mms**

Kaspersky Anti-Virus® Business Optimal

Pakiet ten zapewnia konfigurowalne rozwiązanie antywirusowe dla małych i średnich sieci firmowych.

Kaspersky Anti-Virus Business Optimal zapewnia kompletną ochronę¹ antywirusową dla:

¹ W zależności od wybranego pakietu dystrybucyjnego.

- *stacji roboczych pracujących* pod kontrolą systemów Windows 98/ME, Windows NT/2000/XP i Linux.
- *serwerów plików pracujących* pod kontrolą systemów Windows NT 4.0 Server, Windows 2000/2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD, OpenBSD, Linux, serwerów Samba
- *systemów poczty elektronicznej* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail i Qmail
- *bram internetowych*: CheckPoint Firewall-1 i Microsoft ISA Server 2000 Standard Edition oraz Microsoft ISA Server 2004 Standard Edition

Pakiet Kaspersky Anti-Virus Business Optimal zawiera Kaspersky Administration Kit, unikatowe narzędzie służące do automatycznego rozsyłania aktualizacji oraz do zdalnej administracji ochroną antywirusową.

Użytkownik może dowolnie wybierać pomiędzy wymienionymi wersjami aplikacji antywirusowych, w zależności od posiadanych aplikacji oraz systemu operacyjnego.

Kaspersky® Corporate Suite

Ten pakiet umożliwia dostarczenie skalowalnej ochrony antywirusowej sieciom korporacyjnym dowolnej wielkości i złożoności. Składniki pakietu zostały zaprojektowane w celu ochrony każdego węzła sieci korporacyjnej, także w środowisku mieszanym. Wszystkie składniki pakietu mogą być zarządzane z poziomu jednej konsoli i posiadać ujednoczony interfejs użytkownika. Kaspersky Corporate Suite zapewnia system ochrony, który jest w pełni zgodny ze specyficznymi potrzebami konfiguracji sieciowej użytkownika.

Kaspersky Corporate Suite oferuje kompletną ochronę antywirusową dla:

- *stacji roboczych pracujących pod kontrolą systemów Windows 98/ME, Windows NT/2000/XP i Linux;*
- *serwerów plików i aplikacji pracujących pod kontrolą systemów Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, Linux; Samba file storage*
- *systemów poczty elektronicznej* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, sendmail, postfix, exim
- *bram internetowych*: CheckPoint Firewall -1; Microsoft ISA Server 2000 Enterprise Edition, Microsoft ISA Server 2004 Enterprise Edition
- *komputerów kieszonkowych (PDA)* z systemami operacyjnymi Symbian OS, Microsoft Windows CE oraz Palm OS, a także smartfonów z systemami operacyjnymi Microsoft Windows Mobile 2003 for Smartphone i Microsoft Smartphone 2002.

Pakiet Kaspersky Corporate Suite zawiera Kaspersky Administration Kit, unikatowe narzędzie służące do automatycznego rozsyłania aktualizacji oraz do zdalnej administracji ochroną antywirusową.

Użytkownik może dowolnie wybierać pomiędzy wymienionymi wersjami aplikacji antywirusowych, w zależności od posiadanych aplikacji oraz systemu operacyjnego.

Kaspersky® Anti-Spam

Kaspersky Anti-Spam jest oprogramowaniem wykorzystującym najnowsze technologie w celu ochrony małych i średnich sieci przed atakiem niepożądanych wiadomości e-mail (spam). Produkt łączy w sobie rewolucyjną technologię analizy lingwistycznej oraz wszystkie współczesne metody filtrowania wiadomości e-mail (włączając czarne listy DNS i właściwości listów). Jest to unikatowa kombinacja usług umożliwiająca identyfikację i usunięcie do 95% niepożądanego ruchu pocztowego.

Zainstalowany na wejściu do sieci, gdzie monitoruje przychodzący ruch pocztowy pod kątem obecności spamu, Kaspersky Anti-Spam staje się barierą dla niechcianych wiadomości e-mail. Produkt jest kompatybilny z dowolnym systemem pocztowym i może być zainstalowany na istniejącym serwerze pocztowym, jak i na wyznaczonym do tego celu komputerze.

Wysoka wydajność Kaspersky Anti-Spam została osiągnięta przez codzienne uaktualnianie antyspamowych baz danych próbkami dostarczanymi przez specjalistów z laboratorium lingwistycznego. Uaktualnienia baz danych wykonywane są co 20 minut.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange przeznaczony jest do przetwarzania antywirusowego przychodzących i wychodzących wiadomości pocztowych oraz wiadomości przechowywanych na serwerze, włączając wiadomości w publicznych folderach oraz filtrowanie korespondencji przy użyciu "inteligentnych" technik rozpoznawania spamu w połączeniu z technologiami firmy Microsoft. Aplikacja skanuje wszystkie przychodzące wiadomości do serwera Exchange Server przez protokół SMTP, sprawdzając je w poszukiwaniu obecności wirusów za pomocą technologii antywirusowej oraz obecności spamu. Filtrowanie bazuje na atrybutach formalnych (adres pocztowy, adres IP, rozmiar wiadomości, nagłówek) i analizowana jest zawartość wiadomości i jej załączniki, włączając unikatowe sygnatury graficzne do identyfikacji graficznego spamu. Aplikacja skanuje zarówno zawartość wiadomości, jak również jej załączniki.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway jest wszechstronnym rozwiązaniem zapewniającym kompletną ochronę systemu pocztowego. Aplikacja zainstalowana pomiędzy

siecią korporacyjną a Internetem skanuje wszystkie składniki wiadomości pocztowych w poszukiwaniu obecności wirusów i innego szkodliwego oprogramowania (Spyware, Adware itp.). Umożliwia ona również scentralizowane filtrowanie antyspamowe wiadomości. Program zawiera również dodatkowe funkcje filtrowania ruchu pocztowego w oparciu o nazwę, załączniki MIME oraz narzędzia zmniejszające obciążenie systemu pocztowego i zapobiegające przed atakami hakerów.

Kaspersky Anti-Virus® for Proxy Servers

Kaspersky Anti-Virus for Proxy Servers jest zintegrowanym rozwiązaniem antywirusowym służącym do ochrony ruchu sieciowego przesyłanego za pośrednictwem protokołu HTTP. Aplikacja skanuje ruch WWW w czasie rzeczywistym, chroni przed szkodliwymi programami atakującymi podczas surfowania w Internecie i skanuje pliki pobierane z Internetu.

Kaspersky Anti-Virus® for MIMESweeper for SMTP

Kaspersky Anti-Virus for MIMESweeper for SMTP oferuje szybkie skanowanie ruchu SMTP na serwerach wykorzystujących Clearswift MIMESweeper.

Program ma postać wtyczki do rozwiązania Clearswift MIMESweeper for SMTP i skanuje w czasie rzeczywistym ruch pocztowy w poszukiwaniu wirusów e-mail.

2.2. Kontakt z firmą Kaspersky Lab

W przypadku pojawienia się pytań, komentarzy lub sugestii można je przesłać do jednego z naszych dystrybutorów lub bezpośrednio do Kaspersky Lab. We wszystkich sprawach związanych z naszym produktem można się kontaktować za pośrednictwem poczty elektronicznej i telefonicznie. Wszystkie uwagi i sugestie zostaną przeczytane i rozważone.

Pomoc techniczna	Informacje na temat pomocy technicznej znajdują się na stronie http://www.kaspersky.pl/services.html?s=support Pomoc techniczna: www.kaspersky.com/helpdesk.html
Informacje ogólne	WWW: http://www.kaspersky.pl http://www.viruslist.pl Email: info@kaspersky.pl

