

KASPERSKY LAB

Kaspersky Internet Security 7.0

Podręcznik użytkownika

KASPERSKY INTERNET SECURITY 7.0

Podręcznik użytkownika

© Kaspersky Lab

<http://www.kaspersky.pl>

Lipiec 2007

Zastrzegam się prawo wprowadzania zmian technicznych. Treść niniejszego podręcznika nie stanowi podstawy do jakichkolwiek roszczeń wobec firmy Kaspersky Lab. Opisane w podręczniku oprogramowanie Kaspersky Internet Security dostarczane jest na podstawie umowy licencyjnej. Nieautoryzowane rozpowszechnianie całości lub fragmentów niniejszego podręcznika w jakiegokolwiek postaci jest zabronione.

Wymienione w podręczniku nazwy firm oraz znaki towarowe zostały użyte w celach informacyjnych i są zastrzeżone przez ich właścicieli.

© Copyright Kaspersky Lab.

Wszelkie prawa zastrzeżone.

Kaspersky Lab Polska Sp. z o.o.

42-200 Częstochowa, ul. Krótka 27A

tel./fax: (34) 368 18 14, 368 18 15

www.kaspersky.pl info@kaspersky.pl

<http://www.viruslist.pl> - najświeższe informacje o zagrożeniach internetowych

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	11
ROZDZIAŁ 2. KASPERSKY INTERNET SECURITY 7.0.....	15
2.1. Nowości w Kaspersky Internet Security 7.....	15
2.2. Metody ochrony oferowane przez Kaspersky Internet Security.....	18
2.2.1. Składniki ochrony w czasie rzeczywistym.....	18
2.2.2. Zadania skanowania antywirusowego	21
2.2.3. Aktualizacja	21
2.2.4. Usługi.....	22
2.3. Wymagania sprzętowe i programowe.....	23
2.4. Pakiety dystrybucyjne.....	23
2.5. Usługi świadczone zarejestrowanym użytkownikom	24
ROZDZIAŁ 3. INSTALACJA KASPERSKY INTERNET SECURITY 7.0.....	25
3.1. Instalacja przy użyciu kreatora instalacji.....	25
3.2. Kreator konfiguracji.....	29
3.2.1. Wykorzystanie obiektów zachowanych z wersji 5.0.....	30
3.2.2. Aktywacja programu.....	30
3.2.2.1. Wybór metody aktywacji programu	30
3.2.2.2. Wprowadzanie kodu aktywacyjnego.....	31
3.2.2.3. Rejestracja użytkownika.....	31
3.2.2.4. Uzyskiwanie klucza licencyjnego	31
3.2.2.5. Wybór klucza licencyjnego.....	32
3.2.2.6. Finalizowanie aktywacji programu	32
3.2.3. Wybór trybu ochrony.....	32
3.2.4. Konfiguracja ustawień aktualizacji	33
3.2.5. Konfiguracja terminarza skanowania	34

3.2.6. Ograniczanie dostępu do programu.....	35
3.2.7. Kontrola integralności aplikacji.....	35
3.2.8. Konfiguracja ustawień zapory sieciowej	36
3.2.8.1. Określanie stanu ochrony dla stref.....	36
3.2.8.2. Tworzenie listy aplikacji sieciowych	37
3.2.9. Finalizowanie działania kreatora konfiguracji.....	38
3.3. Instalacja programu z poziomu wiersza poleceń	38
<u>ROZDZIAŁ 4. INTERFEJS PROGRAMU</u>	39
4.1. Ikona zasobnika systemowego.....	39
4.2. Menu kontekstowe.....	40
4.3. Główne okno programu	41
4.4. Okno ustawień programu.....	45
<u>ROZDZIAŁ 5. ROZPOCZĘCIE PRACY</u>	47
5.1. Stan ochrony komputera.....	47
5.2. Weryfikacja stanu poszczególnych składników ochrony	49
5.3. W jaki sposób należy wykonać skanowanie komputera	50
5.4. W jaki sposób należy wykonać skanowanie obszarów krytycznych.....	50
5.5. W jaki sposób należy wykonać skanowanie plików, folderów lub dysków	51
5.6. W jaki sposób należy przeprowadzić uczenie modułu Anti-Spam	52
5.7. Jak uaktualnić program.....	53
5.8. Jak postępować, gdy ochrona nie działa	53
<u>ROZDZIAŁ 6. ZARZĄDZANIE OCHRONĄ</u>	54
6.1. Włączanie i wyłączanie ochrony komputera.....	54
6.1.1. Wstrzymywanie ochrony	54
6.1.2. Wyłączanie ochrony.....	55
6.1.3. Wstrzymywanie / zatrzymywanie składników ochrony, zadań skanowania i aktualizacji	56
6.1.4. Wznawianie ochrony komputera.....	57
6.2. Typy wykrywanego szkodliwego oprogramowania	57
6.3. Tworzenie strefy zaufanej.....	58
6.3.1. Reguły wykluczeń	60

<i>Spis treści</i>	7
6.3.2. Zaufane aplikacje.....	64
6.4. Pomoc techniczna	67
6.5. Zamykanie aplikacji	68
<u>ROZDZIAŁ 7. ZARZĄDZANIE LICENCJAMI</u>	<u>70</u>
<u>ROZDZIAŁ 8. MODYFIKACJA, NAPRAWIENIE LUB USUNIĘCIE PROGRAMU 72</u>	<u>72</u>
8.1. Modyfikacja, naprawienie lub usunięcie programu przy użyciu kreatora instalacji.....	72
8.2. Dezinstalacja programu przy użyciu wiersza poleceń	74
<u>DODATEK A. INFORMACJE DODATKOWE</u>	<u>75</u>
A.1. Lista plików skanowanych według rozszerzenia	75
A.2. Poprawne maski wykluczeń	78
A.3. Poprawne maski wykluczeń zgodne z klasyfikacją Encyklopedii Wirusów	79
<u>DODATEK B. KASPERSKY LAB</u>	<u>80</u>
B.1. Inne produkty Kaspersky Lab.....	81
B.2. Kontakt z firmą Kaspersky Lab.....	90

ROZDZIAŁ 1. ZAGROŻENIA DLA BEZPIECZEŃSTWA KOMPUTERA

Szybki rozwój technologii informatycznych oraz ich udział w każdym aspekcie ludzkiego życia przyczyniają się do wzrostu liczby 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, zakłócanie ich funkcjonowania, a w konsekwencji naruszanie zasobów informacyjnych organizacji. Tego typu działania mogą spowodować duże straty finansowe.

Zagrożone są nie tylko duże firmy. Celem ataków mogą być również użytkownicy indywidualni. Przy pomocy odpowiednich narzędzi atakujący uzyskują dostęp do osobistych danych (kont bankowych oraz numerów kart kredytowych i haseł) lub powodują wadliwe działanie systemu. W konsekwencji zaatakowany komputer może zostać użyty jako część sieci zainfekowanych komputerów (zombie) używanych przez hakerów do atakowania serwerów, wysyłania spamu, zbierania poufnych informacji i rozsyłania nowych wirusów i trojanów.

W dzisiejszych czasach każdy użytkownik komputera zdaje sobie sprawę, że informacje są bardzo cenne i powinny być chronione. Informacje muszą być dostępne dla różnych grup użytkowników w tym samym czasie (dla pracowników, klientów i partnerów biznesowych). Jest to podstawowy wymóg tworzenia wszechstronnych systemów bezpieczeństwa. System taki musi uwzględniać wszystkie możliwe źródła zagrożeń (włącznie z czynnikiem ludzkim) i korzystać ze środków ochrony na poziomie fizycznym, administracyjnym i programowym.

1.1. Źródła zagrożeń

Źródło zagrożeń może stanowić jeden człowiek, grupa ludzi lub nawet niektóre zjawiska niezwiązane z działalnością człowieka. Źródła zagrożeń można podzielić na trzy grupy:

- **Czynnik ludzki.** Do tej grupy zagrożeń można zaliczyć 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 przestępcze.
 - *Wewnętrzne*, włączając działania użytkowników domowych i korporacyjnych. Działania wykonywane przez tę 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 niezależne 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

Dzięki nowoczesnej technologii komputerowej oraz powstawaniu narzędzi komunikacyjnych hakerzy dysponują większą liczbą sposobów rozsyłania zagrożeń. Poniżej znajduje się ich szczegółowy opis:

Internet

Internet jest siecią unikatową, ponieważ nie stanowi niczyjej własności 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 zdalne komputery i firmowe serwery. Efektem tych ataków może być uniemożliwienie korzystania z zasobu, użycie go jako elementu sieci komputerów zombie lub w celu uzyskania pełnego dostępu do tego zasobu oraz przechowywanych na nim informacji.

Od czasu, kiedy możliwe stało się korzystanie z kart kredytowych i płatności elektronicznych w sklepach internetowych, aukcjach oraz bankach internetowych, oszustwa internetowe związane z tego typu dziedziną stały się jednym z najbardziej powszechnych przestępstw.

Sieć lokalna

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. Z tego powodu, jeżeli chociaż jeden z komputerów jest zainfekowany, pozostałe są również narażone na ryzyko infekcji. W celu uniknięcia tego typu sytuacji chroniony powinien być zarówno styk sieci z Internetem jak i poszczególne komputery.

Poczta elektroniczna

Od czasu, gdy praktycznie każdy komputer posiada zainstalowany program pocztowy, a szkodliwe programy potrafią uzyskać dostęp do zawartości elektronicznej książki adresowej, poczta elektroniczna traktowana jest jako źródło rozprzestrzeniania się szkodliwych programów. Użytkownik zainfekowanego komputera może nieświadomie wysłać zainfekowane wiadomości do innych użytkowników, którzy mogą je dalej rozprzestrzeniać. Często zainfekowany plik nie jest wykrywany podczas wysyłania na zewnątrz dużej firmy. W przypadku wystąpienia tego typu zdarzenia zainfekowana zostanie większa grupa użytkowników. Mogą to być setki lub tysiące osób, które z kolei wyślą zainfekowane pliki do dziesiątków tysięcy użytkowników.

Poza zagrożeniami związanymi ze szkodliwym oprogramowaniem występuje problem z niechcianą pocztą elektroniczną – spamem. Mimo że spam nie stanowi bezpośredniego zagrożenia dla komputera użytkownika, powoduje on zwiększanie obciążenia na serwerach pocztowych, zmniejszanie przepustowości, zaśmiecanie skrzynek pocztowych i marnowanie czasu pracy, powodując straty finansowe.

Ponadto, hakerzy zaczęli korzystać z programów rozsyłających masowo wiadomości pocztowe oraz socjotechniki w celu przekonywania użytkowników do otwierania wiadomości e-mail lub klikania odsyłaczy do specjalnie przygotowanych witryn internetowych. Filtracja spamu przeprowadzana jest w celu blokowania niechcianych wiadomości oraz przeciwdziałania nowym typom oszustw internetowych, takich jak phishing oraz blokowania rozprzestrzeniania się szkodliwych programów.

Nośniki wymienne

Nośniki wymienne, takie jak dyski, dyskietki, karty flash, używane są do przenoszenia i przechowywania 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. Ten rozdział zawiera informacje dotyczące zagrożeń blokowanych przez Kaspersky Internet Security.

Robaki

Ta kategoria szkodliwych programów rozprzestrzenia się, wykorzystując luki w systemach operacyjnych komputerów. Programy te nazywane są robakami ze względu na ich zdolność infekowania jednego komputera z poziomu innego przy użyciu sieci, poczty elektronicznej i innych kanałów. Dzięki temu robaki mogą rozprzestrzeniać się bardzo szybko.

Robaki penetrują komputer, określają adresy IP innych maszyn, a następnie przesyłają na nie swoje kopie. Mogą również wykorzystywać dane zawarte w książkach adresowych klientów pocztowych. Niektóre z tych szkodliwych programów tworzą pliki robocze na dyskach systemowych, mogą jednak zostać uruchomione bez jakichkolwiek 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, którym jest 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 ani danych. Trojany nie mogą same włamać się do komputera. Są one rozsyłane przez hakerów, którzy „ukrywają” je pod postacią programów użytkowych. Mogą powodować większe szkody niż tradycyjne ataki wirusów.

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 programy spyware najczęściej skanują określone foldery oraz rejestr systemu w celu utworzenia listy oprogramowania zainstalowanego na komputerze;
- gromadzenie informacji o jakości połączenia sieciowego, przepustowości, prędkości połączenia modemowego itp.

Oprogramowanie riskware

Riskware to potencjalnie niebezpieczne oprogramowanie niezawierające szkodliwych funkcji, lecz mogące zostać użyte przez hakerów jako składnik pomocniczy dla szkodliwego kodu, ponieważ zawiera ono luki i błędy. Tego typu programy mogą stanowić zagrożenie dla danych. Obejmują one 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. Przeglądarka wyświetla inne strony internetowe niż żądane przez użytkownika.

Żarty

Programy, które nie powodują żadnych bezpośrednich uszkodzeń komputera, lecz wyświetlają w pewnych okolicznościach komunikaty mówiące o wystąpieniu uszkodzenia lub możliwości wystąpienia awarii. 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 działań 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 obejmują narzędzia hakerskie (Hack Tools), moduły do tworzenia wirusów, skanery luk w systemie, programy łamiące hasła oraz inne typy programów penetrujących system.

Ataki hakerów

Ataki hakerów mogą być inicjowane przez hakerów lub przez szkodliwe programy. Ich celem jest wykradanie informacji ze zdalnego komputera, powodowanie nieprawidłowego funkcjonowania systemu lub uzyskiwanie pełnej kontroli nad zasobami systemowymi.

Niektóre rodzaje oszustw internetowych

Phishing jest oszustwem internetowym wykorzystującym masowe wysyłanie wiadomości pocztowych w celu wykradania poufnych informacji od użytkownika, głównie w celach finansowych. Wiadomości phishingowe tworzone są w taki sposób, aby jak najbardziej przypominały korespondencję wysłaną przez banki i przedsiębiorstwa. Wiadomości te zawierają odsyłacze do fałszywych witryn internetowych utworzonych przez hakerów w celu przekonania użytkowników, że mają do czynienia z oryginalną stroną WWW danej organizacji. Na takiej witrynie użytkownik proszony jest o podanie, na przykład, swojego numeru karty kredytowej i innych poufnych informacji.

Dialery przekierowujące na płatne witryny internetowe – rodzaj oszustwa internetowego polegający na nieautoryzowanym wykorzystaniu modemu do łączenia się z płatnymi usługami internetowymi (zazwyczaj witrynami zawierającymi treści pornograficzne). Dialery zainstalowane przez hakerów inicjują połączenia modemowe z płatnymi numerami. Połączenia z tymi numerami telefonicznymi są zwykle bardzo drogie, co powoduje, że użytkownik płaci bardzo duże rachunki za telefon.

Treści reklamowe

Do tego typu zagrożeń zaliczane są okna wyskakujące i banery zawierające treści reklamowe, które wyświetlane są podczas przeglądania stron internetowych. Zazwyczaj informacje zawarte w tych oknach są bezużyteczne dla użytkownika. Okna wyskakujące i banery reklamowe uniemożliwiają użytkownikom wykonywanie zadań i obciążają przepustowość łącza.

Spam

Spam jest anonimową wiadomością pocztową. Spam zawiera treści reklamowe, polityczne, prowokujące oraz prośby o udzielenie wsparcia. Innym rodzajem spamu są wiadomości zawierające prośby o dokonanie inwestycji lub zaangażowanie się w system piramidalny, wiadomości mające na celu wykradanie haseł i numerów kart kredytowych oraz wiadomości zawierające prośbę do odbiorców, aby przesłali je do swoich znajomych (popularne łańcuszki).

Spam znacząco zwiększa obciążenie serwerów pocztowych i ryzyko utracenia ważnych danych.

Kaspersky Internet Security wykorzystuje dwie metody wykrywania i blokowania tego typu zagrożeń:

- *Konwencjonalna* – metoda oparta na wyszukiwaniu szkodliwych obiektów przy wykorzystaniu sygnatur zagrożeń zawartych w regularnie uaktualnianej bazie danych. Metoda ta wymaga przynajmniej jednego przypadku infekcji w celu dodania sygnatury zagrożenia do baz danych i dystrybucji tego uaktualnienia do użytkowników.
- *Proaktywna* – w przeciwieństwie do poprzedniego rodzaju ochrony, metoda ta polega na analizowaniu nie kodu, lecz podejrzanego zachowania w systemie. Ma ona na celu wykrywanie nowych zagrożeń, które nie zostały jeszcze zdefiniowane w bazie danych.

Poprzez zastosowanie tych dwóch metod Kaspersky Internet Security zapewnia wszechstronną ochronę komputera przed znanymi i nowymi zagrożeniami.

Uwaga:

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 INTERNET SECURITY 7.0

Kaspersky Internet Security 7.0 oferuje nowe podejście do ochrony informacji.

To, co wyróżnia Kaspersky Internet Security 7.0 na tle innego oprogramowania, włączając inne produkty Kaspersky Lab, to wszechstronne podejście do ochrony danych.

2.1. Nowości w Kaspersky Internet Security 7.

Kaspersky Internet Security 7.0 (dalej zwany “Kaspersky Internet Security” lub “program”) oferuje nowe podejście do ochrony danych. Główną zaletą programu jest integracja i zwiększenie wydajności funkcji wszystkich produktów w jednym programie. Program zapewnia zarówno ochronę antywirusową, jak również zabezpieczenie przed spamem i atakami hakerów. Nowe moduły chronią użytkowników przed nieznanymi zagrożeniami, oszustwami internetowymi oraz pozwalają na monitorowanie dostępu użytkownika do Internetu.

Nie trzeba już instalować kilku produktów w celu zapewnienia całkowitego bezpieczeństwa. Instalacja programu Kaspersky Internet Security 7.0 w zupełności wystarczy.

Wszechstronna ochrona zapewnia nadzorowanie wszystkich kanałów, przez które dane mogą napływać do komputera lub być transmitowane na zewnątrz. Elastyczne ustawienia wszystkich składników programu umożliwiają maksymalne dostosowanie go do potrzeb użytkownika. Dostępna jest również opcja jednoczesnej konfiguracji wszystkich ustawień ochrony.

Poniżej przedstawiono nowe funkcje zastosowane w programie Kaspersky Internet Security 7.0.

Nowe funkcje ochrony

- Kaspersky Internet Security chroni zarówno przed znanymi szkodliwymi programami, jak również przed programami, które nie zostały jeszcze wykryte. Główną zaletą programu jest moduł ochrony proaktywnej. Służy on do analizowania zachowania aplikacji zainstalowanych na komputerze, monitorowania zmian w rejestrze systemowym, śledzenia makr oraz przeciwdziałania ukrytym zagrożeniom. W celu wykrywania różnych rodzajów szkodliwych programów składnik ten korzysta z analizy heurystycznej. Przechowuje on również historię szkodliwej aktywności, dzięki czemu możliwe jest cofnięcie wykonanego działania i przywrócenie systemu do stanu sprzed aktywności szkodliwego oprogramowania.
- Program chroni przed rootkitami i dialerami, blokując niebezpieczne reklamy, okna wyskakujące i szkodliwe skrypty pobrane ze stron internetowych, oraz umożliwia wykrywanie phishingu. Aplikacja chroni także przed nieautoryzo-

waną transmisją poufnych danych (hasła dostępu do połączeń internetowych, poczty elektronicznej lub serwerów itp).

- Ulepszono technologię ochrony antywirusowej dla plików: zmniejszono obciążenie systemu przy jednoczesnym zwiększeniu prędkości skanowania plików. Osiągnięto to dzięki technologiom iChecker oraz iSwift. Podczas pracy w tym trybie program nie musi przetwarzać plików, które nie uległy zmianie od czasu ostatniego skanowania.
- Proces skanowania odbywa się w tle – użytkownik może w tym czasie korzystać z komputera bez żadnych przeszkód. Skanowanie przebiega teraz szybko i bez wykorzystania znacznej ilości zasobów systemowych. Jeżeli operacje wykonywane przez użytkownika wymagają większej ilości zasobów systemowych, skanowanie antywirusowe zostanie wstrzymane do czasu zakończenia wykonywania tych działań. Gdy zasoby zostaną zwolnione, skanowanie zostanie automatycznie wznowione.
- Dla obszarów krytycznych komputera, których infekcja może spowodować poważne konsekwencje, utworzone zostało oddzielne zadanie. Można skonfigurować to zadanie do każdorazowego uruchamiania podczas startu systemu operacyjnego.
- Ulepszono ochronę poczty elektronicznej przed szkodliwymi programami i spamem. Program skanuje wiadomości pocztowe wysyłane za pośrednictwem następujących protokołów:
 - IMAP, SMTP, POP3, niezależnie od klienta pocztowego
 - NNTP (tylko skanowanie w poszukiwaniu wirusów), niezależnie od klienta pocztowego
 - MAPI, HTTP (przy wykorzystaniu wtyczek dla programu MS Outlook oraz The Bat!).
- Dostępne są specjalne wtyczki dla najbardziej popularnych klientów pocztowych, takich jak Microsoft Outlook, Microsoft Outlook Express (Poczta systemu Windows) i The Bat!, umożliwiające konfigurację ochrony poczty przed wirusami oraz spamem bezpośrednio w kliencie pocztowym.
- Anti-Spam uczy się podczas pracy użytkownika z pocztą elektroniczną. Moduł uwzględnia szczegóły związane ze stylem pracy użytkownika i zapewnia maksymalną wygodę konfiguracji ochrony przed spamem. Proces uczenia się odbywa się z wykorzystaniem samouczącego się algorytmu iBayes. Dodatkowo, użytkownik może tworzyć czarne i białe listy adresów oraz kluczowych fraz.
- Anti-Spam korzysta z bazy danych phishingu. Umożliwia ona filtrowanie wiadomości pocztowych stworzonych w celu uzyskiwania informacji poufnych lub finansowych.
- Program filtruje ruch przychodzący i wychodzący, śledząc i blokując zagrożenia związane z typowymi atakami sieciowymi. Dodatkowo aplikacja umożliwia korzystanie z Internetu w trybie ukrycia.
- Użytkownik może sam zdecydować o tym, która sieć jest w 100% zaufana, a którą należy monitorować ze szczególną ostrożnością.

- Funkcja powiadamiania użytkownika została rozbudowana o dodatkowe zdarzenia występujące podczas pracy programu. Dla każdego z tych zdarzeń można wybrać następujące metody powiadamiania: wiadomość e-mail, powiadomienia dźwiękowe, komunikaty wyskakujące.
- Dodano możliwość skanowania danych przesyłanych za pośrednictwem bezpiecznych połączeń SSL.
- Dodano nowe funkcje autoochrony programu: ochrona przed zdalnym zarządzaniem oraz zabezpieczenie ustawień programu za pomocą hasła. Funkcje te chronią przed wyłączeniem lub zmodyfikowaniem ustawień ochrony przez szkodliwe programy, hakerów i nieautoryzowanych użytkowników.
- Dodano nową funkcję tworzenia dysku ratunkowego. Przy użyciu dysku ratunkowego można ponownie uruchomić system operacyjny po atakach wirusów i przeskanować komputer w poszukiwaniu szkodliwych plików.
- Nowy moduł, Kontrola rodzicielska, pozwala użytkownikom na monitorowanie dostępu do Internetu. Funkcja blokuje lub zezwala na dostęp do określonych zasobów internetowych. Ponadto, komponent pozwala na ograniczenie czasu, w którym użytkownik ma dostęp do Internetu.
- Dodano moduł News Agent, który służy do śledzenia nowości Kaspersky Lab w czasie rzeczywistym.
- Nowy interfejs programu
- Nowy interfejs Kaspersky Internet Security ułatwia korzystanie z programu i upraszcza wykonywanie operacji. Możliwe jest również zmienianie wyglądu programu przy zastosowaniu własnych schematów graficznych i kolorystycznych (skór).
- Podczas funkcjonowania program regularnie wyświetla wskazówki i podpowiedzi: Kaspersky Internet Security wyświetla komunikaty informacyjne dotyczące poziomu ochrony, wskazówki i porady dotyczące funkcjonowania programu oraz zawiera podzielony na sekcje system pomocy. Wbudowany kreator ochrony pozwala na wykonanie kompletnego zrzutu stanu ochrony komputera i umożliwia natychmiastowe zgłoszenie problemu do działu pomocy technicznej.

Nowe funkcje aktualizacji

- Program zawiera nową, ulepszoną procedurę aktualizacji: Kaspersky Internet Security automatycznie monitoruje sygnatury zagrożeń oraz moduły programu niezbędne do jego funkcjonowania. Uaktualnienia pobierane są automatycznie, gdy możliwe jest nawiązanie połączenia z serwerami firmy Kaspersky Lab.
- Program pobiera tylko nowe uaktualnienia. Dzięki temu rozmiar pobieranych uaktualnień jest ponad dziesięciokrotnie mniejszy.
- Podczas pobierania uaktualnień określone jest optymalne źródło, które ustawiane jest jako źródło domyślne.
- Można zrezygnować z wykorzystania serwera proxy, jeżeli uaktualnienia pobierane są z lokalnego foldera. Redukuje to ruch sieciowy na serwerze proxy.

- Program posiada funkcję cofania aktualizacji, dzięki której można przywrócić ostatnią działającą wersję baz danych, jeżeli, na przykład, zostaną one uszkodzone lub wystąpi błąd podczas ich kopiowania.
- Dodano nową funkcję, która pozwala na kopiowanie aktualizacji do foldera lokalnego. Inne komputery znajdujące się w sieci pobierają z niego aktualizacje, zmniejszając tym samym ruch w sieci Internet.

2.2. Metody ochrony oferowane przez Kaspersky Internet Security

Program Kaspersky Internet Security został stworzony z myślą o ochronie przed różnego rodzaju zagrożeniami. Innymi słowy, oddzielne składniki programu zajmują się poszczególnymi zagrożeniami, monitorują je oraz wykonują niezbędne działania w celu ochrony przed szkodliwymi skutkami. Dzięki takiemu podejściu program jest elastyczny i wygodny w konfiguracji i może zostać szybko dostosowany do specyficznych wymagań użytkownika.

Kaspersky Internet Security zawiera:

- Składniki ochrony w czasie rzeczywistym (rozdział 2.2.1 na stronie 18) zapewniające wszechstronną ochronę wszystkich kanałów transmisji i wymiany danych na komputerze.
- Zadania skanowania antywirusowego (rozdział 2.2.2 na stronie 21) sprawdzające komputer lub poszczególne pliki, foldery, dyski lub obszary w poszukiwaniu wirusów.
- Moduł aktualizacji (rozdział 2.2.3 na stronie 21) zapewniający regularne uaktualnianie modułów aplikacji oraz sygnatur zagrożeń, spamu oraz ataków hakerów.

2.2.1. Składniki ochrony w czasie rzeczywistym

Poniższe składniki chronią komputer w czasie rzeczywistym:

Ochrona plików

System plików może zawierać wirusy i inne niebezpieczne programy. Szkodliwe programy mogą znajdować się w systemie od dłuższego czasu, po przeniesieniu ich na dyskietce lub z Internetu, bez wcześniejszego ich otwierania. Aktywacja wirusa może nastąpić po otwarciu takiego pliku lub podczas kopiowania go na inny dysk twardy.

Ochrona plików jest składnikiem służącym do monitorowania systemu plików komputera. Skanuje on wszystkie pliki, które mogą zostać otwarte, uruchomione lub zapisane na komputerze, oraz wszystkie podłączone dyski twarde. Kaspersky Internet Security przechwytuje każdy otwierany plik i skanuje go w poszukiwaniu znanych wirusów. Jeżeli plik nie jest zainfekowany, można

dalej z niego korzystać, jeżeli natomiast jest 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 kwwarantanny.

Ochrona poczty

Wiadomości e-mail wykorzystywane są na szeroką skalę przez hakerów do rozsyłania szkodliwych programów. Są one jedną z najbardziej popularnych metod rozprzestrzeniania się robaków internetowych. Dlatego monitorowanie poczty elektronicznej jest bardzo ważne.

Ochrona poczty jest składnikiem służącym do skanowania wszystkich odbieranych i wysyłanych wiadomości pocztowych. Wiadomości pocztowe analizowane są pod kątem występowania szkodliwych programów. Jeżeli wiadomość nie zawiera niebezpiecznych obiektów, program zezwala na dostęp do niej.

Ochrona WWW

Podczas otwierania stron internetowych istnieje ryzyko infekcji wirusami załączonymi do skryptów uruchamianych na stronach internetowych oraz ryzyko związane z pobieraniem niebezpiecznych obiektów na dysk komputera.

Ochrona WWW jest składnikiem służącym do przeciwdziałania tego typu sytuacjom. Przechwytuje on i blokuje niebezpieczne skrypty na stronach internetowych. Monitorowany jest cały ruch HTTP.

Ochrona proaktywna

Każdego dnia pojawia się coraz więcej nowych szkodliwych programów. Są one bardziej skomplikowane i złożone, a wykorzystywane przez nie metody rozprzestrzeniania stają się coraz trudniejsze do wykrycia.

W celu wykrycia nowego szkodliwego programu, zanim zdąży on wyrządzić jakiegokolwiek szkody, firma Kaspersky Lab opracowała specjalny składnik – *Ochrona proaktywna*. Został on stworzony w celu monitorowania i analizowania zachowania wszystkich programów zainstalowanych na komputerze. Kaspersky Internet Security podejmuje decyzje w oparciu o analizę działań wykonywanych przez aplikację. Ochrona proaktywna chroni komputer zarówno przed znanymi wirusami, jak również przed nowymi zagrożeniami, które nie zostały jeszcze odkryte i sklasyfikowane.

Kontrola prywatności

Ostatnio coraz popularniejsze stają się różne oszustwa internetowe (phishing, automatyczne dialery, aplikacje kradnące poufne informacje). Takie działania mogą prowadzić do poważnych strat finansowych.

Kontrola prywatności śledzi i blokuje tego typu działania na komputerze. Na przykład: składnik blokuje banery reklamowe i okna wyskakujące przeszkadzające podczas pracy w Internecie, blokuje programy próbujące się automatycznie załadować i analizuje strony internetowe w poszukiwaniu phishingu.

Zapora sieciowa

Hakerzy są w stanie wykorzystać każdą potencjalną lukę w celu dostania się do komputera. Może to być otwarte połączenie sieciowe, transmisja danych pomiędzy komputerami itp.

Zapora sieciowa służy do ochrony komputera podczas pracy z Internetem i innymi sieciami komputerowymi. Moduł monitoruje przychodzące oraz wychodzące połączenia i skanuje porty a także pakiety danych.

Dodatkowo, Zapora sieciowa blokuje niechciane reklamy (banery oraz okna wyskakujące), co pozwala na ograniczenie ilości pobieranych danych i zwiększa wygodę pracy z Internetem.

Anti-Spam

Chociaż spam nie stanowi bezpośredniego zagrożenia dla komputera użytkownika, powoduje zwiększenie obciążenia na serwerach pocztowych, zmniejszenie przepustowości, zaśmiecanie skrzynek pocztowych i marnowanie czasu pracy, powodując straty finansowe.

Anti-Spam jest wtyczką dla klienta pocztowego zainstalowanego na komputerze służącą do skanowania wszystkich odbieranych i wysyłanych wiadomości pocztowych w poszukiwaniu spamu. Wszystkie wiadomości zawierające spam są oznaczane specjalnym nagłówkiem. Anti-Spam można również skonfigurować do przetwarzania spamu według preferencji użytkownika (automatyczne usuwanie, przenoszenie do specjalnego foldera itp.).

Kontrola rodzicielska

Jedną z cech Internetu jest brak cenzury. Wiele stron WWW zawiera nielegalne lub niepożądane informacje a także treści przeznaczone wyłącznie dla dorosłych. Każdego dnia pojawiają się nowe witryny zawierające informacje związane z rasizmem, pornografią, bronią i narkotykami. Często strony te zawierają wiele szkodliwych programów, które uruchamiają się podczas ich przeglądania.

Możliwość ograniczania dostępu do takich stron WWW stanowi obecnie niezbędną funkcję oprogramowania służącego do ochrony.

Kontrola rodzicielska pozwala na monitorowanie dostępu do określonych stron WWW. Mogą to być dowolne strony zdefiniowane przez użytkownika w interfejsie Kaspersky Internet Security. Program kontroluje nie tylko zawartość otwieranych stron WWW, lecz także czas spędzony online. Dostęp do Internetu może być dozwolony w określonym czasie dnia. Możliwe jest także włączenie blokowania dostępu do Internetu po spędzeniu online określonego czasu w ciągu 24 godzin.

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 składniki ochrony z powodu zbyt niskiego poziomu zabezpieczeń lub z innych przyczyn.

Kaspersky Internet Security oferuje cztery rodzaje zadań skanowania antywirusowego:

Skanowanie obszarów krytycznych

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

Skanowanie komputera

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

Skanowanie obiektów startowych

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

Wykrywanie rootkitów

Skanowanie komputera pod kątem obecności rootkitów, które ukrywają szkodliwe programy w systemie operacyjnym. Narzędzia te są instalowane w systemie, ukrywają swoją obecność oraz obecność procesów, folderów oraz kluczy rejestru dowolnych szkodliwych programów zdefiniowanych w konfiguracji rootkita.

Dostępna jest również opcja tworzenia innych zadań skanowania antywirusowego oraz definiowania dla nich terminarza skanowania. Na przykład można utworzyć zadanie skanowania pocztowych baz danych raz w tygodniu lub zadanie skanowania foldera **Moje dokumenty**.

2.2.3. Aktualizacja

Aby skutecznie chronić przed atakami hakerów i usuwać wirusy oraz inne niebezpieczne programy, Kaspersky Internet Security wymaga aktualnych baz danych. Aktualność bazy danych zapewnia moduł Aktualizacja. Moduł ten aktualizuje bazy danych sygnatur zagrożeń oraz pliki wykonywalne wykorzystywane przez Kaspersky Internet Security.

Funkcja dystrybucji uaktualnień pozwala na zapisanie uaktualnień baz danych i modułów aplikacji pobranych z serwerów firmy Kaspersky Lab oraz udostępnienie ich innym komputerom działającym w obrębie tej samej sieci lokalnej w celu zmniejszenia obciążenia firmowego łącza internetowego.

2.2.4. Usługi

Kaspersky Internet Security zawiera wiele przydatnych usług. Stworzone one zostały do świadczenia pomocy w czasie rzeczywistym oraz rozszerzenia możliwości programu.

Raporty i pliki danych

Każdy składnik ochrony, 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 Internet Security. Jeżeli pojawią się problemy, możliwe będzie wysłanie raportów do firmy Kaspersky Lab w celu dokonania ich analizy i uzyskania pomocy w rozwiązaniu problemu.

Kaspersky Internet Security przenosi wszystkie podejrzone 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 nowe obiekty. 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 celu umożliwienia przywrócenia plików lub informacji o ich infekcji. Kopie zapasowe plików również są przechowywane w zaszyfrowanej postaci w celu uniknięcia przyszłych infekcji. Możliwe jest przywrócenie pliku z foldera kopii zapasowej do oryginalnej lokalizacji oraz usunięcie kopii.

Aktywacja

Wraz z zakupem Kaspersky Internet Security użytkownik staje się stroną umowy licencyjnej (drugą stroną umowy jest firma Kaspersky Lab). Umowa definiuje wszystkie zasady korzystania z aplikacji oraz dostępu do pomocy technicznej. Okres ważności licencji oraz inne informacje niezbędne do zapewnienia pełnej funkcjonalności programu zapisane są w kluczu licencyjnym.

Przy użyciu funkcji *Aktywacja* można zapoznać się ze szczegółowymi informacjami na temat wykorzystywanego klucza lub nabyć nowy klucz.

Pomoc

Dla zarejestrowanych użytkowników programu Kaspersky Internet Security dostępna jest usługa pomocy technicznej. W celu uzyskania informacji na temat dostępu do pomocy technicznej należy użyć funkcji *Pomoc*.

Klikając odpowiednie odsyłacze można przejść do forum użytkowników programów Kaspersky Lab, wystać raport o błędzie do działu pomocy technicznej lub przekazać własną opinię o używanym programie poprzez wypełnienie specjalnego formularza.

Użytkownik ma także dostęp do pomocy technicznej online – służy do tego specjalny Panel Klienta. Pomoc techniczna dostępna jest również za pośrednictwem poczty elektronicznej oraz telefonu.

2.3. Wymagania sprzętowe i programowe

Aby program KasperskyInternet Security 7.0 działał poprawnie, komputer musi spełniać następujące wymagania:

Wymagania ogólne:

- 50 MB wolnego miejsca na dysku twardym
- napęd CD-ROM (w celu instalacji Kaspersky Internet Security 7.0 z płyty CD)
- Microsoft Internet Explorer 5.5 lub nowszy (w celu aktualizacji bazy danych sygnatur oraz modułów program z Internetu)
- Instalator Microsoft Windows 2.0

Microsoft Windows 2000 Professional (Service Pack 2 lub nowszy), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 2 lub nowszy), Microsoft Windows XP Professional x64 Edition:

- procesor Intel Pentium 300 MHz lub nowszy (lub kompatybilny)
- 128 MB of RAM

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Intel Pentium 800 MHz 32-bit (x86)/ 64-bit (x64) lub szybszy (lub kompatybilny)
- 512 MB pamięci RAM

2.4. Pakiety dystrybucyjne

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
- Podręcznik użytkownika
- Kod aktywacyjny programu nadrukowany na certyfikacie autentyczności
- Umowa licencyjna

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

Jeżeli Kaspersky Internet Security został zakupiony w sklepie internetowym, należy pobrać produkt z witryny internetowej Kaspersky Lab **Download** → **Produkty**). Podręcznik użytkownika można pobrać z sekcji **Download** → **Dokumentacja**.

Kod aktywacyjny przesyłany jest pocztą elektroniczną po uregulowaniu płatności.

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

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 INTERNET SECURITY 7.0

Aplikacja może zostać zainstalowana przy użyciu kreatora instalacji (patrz rozdział 3.1 na stronie 25) lub wiersza poleceń (patrz rozdział 3.3 na stronie 38).

W trakcie pracy z kreatorem instalacji można wybrać opcję instalacji ekspresowej. Ten typ instalacji nie wymaga podejmowania żadnych działań ze strony użytkownika: aplikacja zostanie zainstalowana przy użyciu ustawień domyślnych zalecanych przez ekspertów z firmy Kaspersky Lab. W ostatnim etapie instalacji aplikacja będzie musiała zostać aktywowana.

Instalacja niestandardowa umożliwia wybór składników do zainstalowania i foldera docelowego, aktywację aplikacji oraz wykonanie wstępnej konfiguracji przy użyciu specjalnego kreatora.

3.1. Instalacja przy użyciu kreatora instalacji

Przed rozpoczęciem instalacji Kaspersky Internet Security należy zakończyć działanie wszystkich innych uruchomionych aplikacji.

Aby zainstalować Kaspersky Internet Security na komputerze, należy otworzyć plik Instalatora Microsoft Windows znajdujący się na instalacyjnej płycie CD.

Informacja:

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. Weryfikacja wymagań systemowych w celu instalacji na komputerze Kaspersky Internet Security

Przed rozpoczęciem instalacji instalator sprawdzi system operacyjny oraz pakiety uaktualnień w celu porównania zgodności z wymaganiami oprogramowania Kaspersky Internet Security. Komputer jest również sprawdzany pod kątem obecności 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 Internet Security należy zainstalować wymagane pakiety Service Pack oraz oprogramowanie 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 Internet Security.

Aby kontynuować instalację, należy kliknąć przycisk **Dalej**. W celu przerwania instalacji 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. W celu przerwania instalacji należy kliknąć przycisk **Anuluj**.

Krok 4. Wybór typu instalacji

Na tym etapie działania kreatora należy wybrać typ instalacji:

Instalacja ekspresowa. Po wybraniu tej opcji Kaspersky Internet Security zostanie zainstalowany z użyciem ustawień domyślnych zalecanych przez ekspertów firmy Kaspersky Lab. Po zakończeniu instalacji uruchomiony zostanie kreator aktywacji (patrz rozdział 3.2.2 na stronie 30).

Instalacja niestandardowa. Po wybraniu tej opcji możliwe będzie wybranie składników aplikacji, foldera instalacyjnego, aktywowanie aplikacji oraz konfiguracja aplikacji przy użyciu specjalnego kreatora (patrz rozdział 3.2 na stronie 29).

W pierwszym przypadku instalacja zostanie wykonana bez udziału użytkownika, tzn. poszczególne kroki opisane w tym rozdziale zostaną pominięte. Natomiast w drugim przypadku konieczne będzie wprowadzenie lub potwierdzenie pewnych danych.

Krok 5. Wybór foldera instalacyjnego

W kolejnej fazie procesu instalacji Kaspersky Internet Security należy wskazać folder, w którym program zostanie zainstalowany. Domyślnie program instalowany jest w folderze: <Dysk>\Program Files\Kaspersky Lab\Kaspersky Internet Security 7.0\.

Aby zmienić domyślną ścieżkę dostępu do foldera instalacyjnego, 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 wpisać więcej niż 200 znaków ani używać znaków specjalnych.

Aby kontynuować instalację, należy kliknąć przycisk Dalej.

Krok 6. Wybór instalowanych składników

Krok ten dostępny jest jedynie po wybraniu opcji Niestandardowa.

Jeżeli wybrany zostanie niestandardowy typ instalacji, możliwe będzie wybranie składników Kaspersky Internet Security, które zostaną zainstalowane. Domyślnie wybrane są wszystkie zadania ochrony w czasie rzeczywistym oraz skanowania antywirusowego.

W celu wybrania składników, które mają zostać zainstalowane, należy kliknąć prawym przyciskiem myszy ikonę 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.

W celu pominięcia instalacji składnika z menu kontekstowego należy wybrać opcję **Cały składnik będzie niedostępny**. Pominięcie instalacji składnika może pozbawić komputer użytkownika ochrony przed dużą liczbą niebezpiecznych programów.


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

Krok 7. Wyłączenie zapory systemu Microsoft Windows

Krok ten dostępny jest jedynie w przypadku instalacji składnika Zapora sieciowa programu Kaspersky Internet Security na komputerze, na którym włączona jest zapora systemu Microsoft Windows.

Kreator instalacji Kaspersky Internet Security wyświetlił zapytanie o wyłączenie zapory systemu Microsoft Windows, ponieważ moduł Zapora sieciowej zawarty w programie Kaspersky Internet Security posiada pełną funkcjonalność zapory sieciowej.

Jeżeli **Zapora sieciowa** ma zostać użyta jako podstawowy element ochrony sieci, należy kliknąć **Dalej**. Zapora systemu Windows zostanie automatycznie wyłączona.

Jeżeli użytkownik chce nadal używać zapory systemu Microsoft Windows należy wybrać opcję  **Zachowaj włączoną zaporę systemu Microsoft Windows**. W tym przypadku zaporę sieciową Kaspersky Internet Security zostanie zainstalowana, ale w celu uniknięcia konfliktów zostanie wyłączona.

Krok 8. Wyszukiwanie innych programów antywirusowych

W kolejnym kroku program instalacyjny sprawdzi, czy w systemie zostały zainstalowane inne aplikacje antywirusowe, włączając produkty Kaspersky Lab, które mogą przeszkadzać w prawidłowym działaniu Kaspersky Internet Security.

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.

Jeżeli na liście programów antywirusowych będą się znajdować Kaspersky Anti-Virus® Personal lub Kaspersky Anti-Virus® Personal Pro, zalecane jest zachowanie klucza licencyjnego przed ich usunięciem, ponieważ będą one mogły zostać użyte przez Kaspersky Internet Security 7.0. Zalecane jest również zachowanie zawartości folderów **Kopii zapasowej** i **Kwarantanny**. Obiekty te zostaną automatycznie przeniesione do folderów Kwarantanny i Kopii zapasowej Kaspersky Internet Security.

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

Krok 9. Kończenie instalacji programu

W tym kroku program zaproponuje zakończenie instalacji programu. Możliwe będzie zaimportowanie ustawień ochronny, baz danych sygnatur, antyspamowej bazy danych, które zostały zachowane podczas deinstalacji poprzedniej wersji Kaspersky Internet Security.

Poniżej znajduje się opis użycia opcji opisanych powyżej.

Jeżeli na komputerze była zainstalowana poprzednia wersja (kompilacja) Kaspersky Internet Security i bazy danych aplikacji zostały zachowane, możliwe będzie ich zaimportowanie przez obecnie instalowaną wersję. W tym celu należy zaznaczyć opcję **Bazy danych aplikacji**. Bazy danych dostarczone w pakiecie dystrybucyjnym aplikacji nie zostaną skopiowane na komputer.

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

Zalecane jest również użycie antyspamowej bazy danych zachowanej z poprzedniej wersji aplikacji. W ten sposób nie będzie potrzeby ponownego uczenia modułu Anti-Spam. W celu użycia poprzednio utworzonej bazy danych należy zaznaczyć opcję **Antyspamowe bazy danych**.

Nie jest zalecane usuwanie zaznaczenia z opcji **Włącz autoochronę przed instalacją podczas instalacji** Kaspersky Internet Security. 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 zaznaczenie z opcji **Włącz autoochronę przed instalacją**. W przeciwnym wypadku procedura instalacji może nie zakończyć się lub zakończyć się poprawnie.

Aby kontynuować instalację, należy kliknąć przycisk Dalej.

Krok 10. Finalizowanie instalacji

W oknie **Finalizowanie instalacji** wyświetlane są informacje na temat zakończenia procesu instalacji Kaspersky Internet Security.

Po pomyślnym zakończeniu instalacji wyświetlony zostanie komunikat informujący o konieczności ponownego uruchomienia komputera. Po ponownym załadowaniu systemu operacyjnego komputera uruchomiony zostanie Kreator konfiguracji Kaspersky Internet Security.

Jeżeli nie będzie wymagany ponowny rozruch komputera, należy kliknąć przycisk **Dalej** w celu uruchomienia Kreatora konfiguracji.

3.2. Kreator konfiguracji

Kreator konfiguracji Kaspersky Internet Security 7.0 uruchamiany jest po zakończeniu instalacji programu. Został on stworzony w celu ułatwienia 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** umożliwia przerwanie działania kreatora w dowolnym momencie.

Można pominąć etap konfiguracji ustawień podczas instalacji programu zamykając okno kreatora. W przyszłości możliwe będzie jego ponowne uruchomienie z poziomu interfejsu programu. Kreator zostanie uruchomiony przy próbie przywrócenia domyślnych ustawień Kaspersky Internet Security.

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 przez wersję 5.0 aplikacji, które mają zostać zaimportowane do wersji 7.0. Mogą to być pliki poddane kwarantannie, znajdujące się w folderze kopii zapasowych lub ustawienia ochrony.

W celu użycia tych danych w wersji 7.0 należy zaznaczyć odpowiednie pola.

3.2.2. Aktywacja programu

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

Program jest aktywowany poprzez instalację klucza licencyjnego, który zostanie użyty przez Kaspersky Internet Security w celu sprawdzenia licencji oraz określenia daty jej wygaśnięcia.

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


- informacje o pomocy technicznej (kto jej udziela i gdzie ją uzyskać);
- nazwę programu, numer i datę wygaśnięcia licencji.




Uwaga!

Aby aktywować program, należy posiadać połączenie z Internetem. Jeżeli podczas instalacji programu użytkownik nie jest połączony z Internetem, można dokonać aktywacji (patrz Rozdział 8. na stronie 72) w późniejszym terminie przy użyciu interfejsu programu.

3.2.2.1. Wybór metody aktywacji programu

W zależności od tego, czy użytkownik posiada klucz licencyjny dla programu Kaspersky Internet Security, czy też niezbędne jest uzyskanie go z jednego z serwerów firmy Kaspersky Lab, istnieje kilka opcji aktywacji programu:

-  **Aktywuj przy użyciu kodu aktywacyjnego.** Należy wybrać ten sposób aktywacji w przypadku zakupu pełnej wersji programu, w której znajdował się kod aktywacyjny. Kod ten jest używany w celu otrzymania klucza licencyjnego, który pozwala użytkownikowi na dostęp do wszystkich funkcji programu, aż do chwili wygaśnięcia licencji.

-  **Aktywuj wersję testową (30-dniową).** Należy wybrać tę opcję aktywacji w przypadku chęci zainstalowania wersji testowej programu przed podjęciem decyzji odnośnie zakupu wersji komercyjnej. Użytkownik uzyska darmowy klucz licencyjny aktywny przez określony czas testowy.
-  **Zastosuj bieżący klucz licencyjny.** Należy wybrać tę metodę aktywacji w przypadku posiadania klucza licencyjnego dla programu Kaspersky Internet Security 7.0.
-  **Aktywuj później.** Po wybraniu tej opcji etap aktywacji zostanie pominięty. Na komputerze zainstalowany zostanie program Kaspersky Internet Security, możliwy będzie dostęp do jego wszystkich funkcji za wyjątkiem aktualizacji (aktualizację można będzie wykonać tylko raz po zainstalowaniu programu).

3.2.2.2. Wprowadzanie kodu aktywacyjnego

W celu aktywacji programu należy podać kod aktywacyjny dostarczony wraz z aplikacją. Jeżeli program został zakupiony przez Internet, kod aktywacyjny zostanie przesłany w wiadomości e-mail. W przypadku zakupu wersji pudełkowej, kod aktywacyjny będzie wydrukowany na certyfikacie autentyczności.

Kod aktywacyjny ma postać sekwencji czterech ciągów (każdy składa się z pięciu znaków) oddzielonych myślnikami (bez spacji). Na przykład: 11111-11111-11111-11111.

W dolnej części okna należy wprowadzić numer oraz hasło klienta, jeżeli użytkownik przeszedł procedurę rejestracji i otrzymał te dane. Jeżeli rejestracja nie została jeszcze przeprowadzona, należy pozostawić te pola puste – kreator zażąda informacji kontaktowych i przeprowadzi rejestrację w kolejnym kroku. Na końcu procedury rejestracji użytkownik otrzyma numer oraz hasło klienta. Dane te są niezbędne do korzystania z pomocy technicznej. Podczas przeprowadzania rejestracji przy użyciu kreatora aktywacji numer klienta można zaobserwować w sekcji Pomoc (rozdział 6.4 na stronie 67) okna głównego aplikacji.

3.2.2.3. Rejestracja użytkownika

Ten etap aktywacji wymaga od użytkownika wprowadzenia informacji kontaktowych: adres e-mail, miasto i kraj zamieszkania. Te informacje są wymagane przez dział pomocy technicznej firmy Kaspersky Lab do identyfikacji użytkownika.

Po wprowadzeniu tych informacji kreator aktywacji wyśle je do serwera aktywacji i użytkownikowi zostanie przydzielony identyfikator oraz hasło dostępu do Panelu klienta i witryny pomocy technicznej. Informacje na temat identyfikatora (ID) klienta wyświetlane są w sekcji Pomoc (rozdział 6.4 na stronie 67) okna głównego aplikacji.

3.2.2.4. Uzyskiwanie klucza licencyjnego

Kreator konfiguracji programu nawiązuje połączenie z serwerem firmy Kaspersky Lab i przesyła dane rejestracyjne użytkownika (kod aktywacyjny i informacje osobowe), które są weryfikowane na serwerze.

Jeżeli weryfikacja kodu aktywacyjnego zakończy się pomyślnie, kreator konfiguracji pobierze plik klucza licencyjnego. W przypadku instalacji wersji demonstracyjnej programu (z 30 dniowym okresem ważności klucza licencyjnego) kreator konfiguracji pobierze klucz trial bez konieczności podawania kodu aktywacyjnego.

Pobrany plik zostanie automatycznie zainstalowany i wyświetlone zostanie okno informujące o zakończeniu procesu aktywacji programu zawierające informacje dotyczące licencji.

Jeżeli weryfikacja kodu aktywacyjnego zakończy się błędem, na ekranie wyświetlony zostanie odpowiedni komunikat. W przypadku wystąpienia tego typu sytuacji należy skontaktować się z dystrybutorem, u którego zakupiony został program, w celu uzyskania dodatkowych informacji.

3.2.2.5. Wybór klucza licencyjnego

Jeżeli użytkownik posiada plik klucza licencyjnego dla programu Kaspersky Internet Security 7.0, kreator zaproponuje jego instalację. W celu instalacji pliku klucza licencyjnego należy użyć przycisk Przeglądaj i wskazać lokalizację pliku klucza licencyjnego. Plik ten posiada rozszerzenie .key. Należy to zrobić przy pomocy standardowego okna wyboru plików.

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, trial itp.) oraz data zakończenia okresu licencjonowania.

3.2.2.6. Finalizowanie aktywacji programu

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

3.2.3. Wybór trybu ochrony

W tym oknie Kreator konfiguracji zapyta użytkownika o wybór trybu ochrony, w jakim program będzie działać:

Podstawowa. Jest to ustawienie domyślne, przeznaczone dla mniej doświadczonych użytkowników komputerów i oprogramowania antywirusowego. W tym trybie składniki aplikacji będą działać z wykorzystaniem zalecanego poziomu ochrony, a użytkownik będzie powiadamiany wyłącznie o niebezpiecznej aktywności (takiej jak wykrycie wirusa, podejrzana aktywność).

Interaktywna. Ten tryb zapewnia bardziej zoptymalizowaną ochronę danych komputera niż tryb podstawowy. W tym trybie możliwe jest śledzenie prób modyfikacji ustawień systemowych, podejrzanej aktywności w systemie i nieautoryzowanej aktywności sieciowej.

Wszelka aktywność wymieniona wyżej może być symptomem szkodliwych programów lub standardową aktywnością niektórych programów używanych na komputerze. Dla każdego przypadku niezbędne będzie podjęcie decyzji o zezwoleniu na tego typu aktywność lub zabronieniu jej.

W przypadku wybrania tego trybu, należy określić, kiedy powinien on zostać użyty:



- Włącz tryb uczenia Zapory sieciowej** – pytanie użytkownika o podjęcie decyzji przy próbie nawiązania połączenia z zasobem sieciowym przez programy zainstalowane na komputerze. Można zezwolić na połączenie, zablokować je lub skonfigurować odpowiednią regułą zapory sieciowej dla tego programu. W przypadku wyłączenia trybu uczenia, zapora sieciowa pracuje z minimalnymi ustawieniami ochrony, udzielając dostępu do zasobów sieciowych wszystkim aplikacjom.
- Włącz monitorowanie rejestru** – pytanie użytkownika o podjęcie decyzji przy próbie wykrycia modyfikacji rejestru systemowego.


Jeżeli aplikacja jest zainstalowana na komputerze działającym pod kontrolą Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista lub Microsoft Windows Vista x64, tryb interaktywny opisany poniżej nie jest dostępny.

- Włącz analizę integralności aplikacji** – pytanie użytkownika o podjęcie działania podczas ładowania modułów do monitorowanych aplikacji.
- Włącz zaawansowaną ochronę proaktywną** – włączenie analizy wszelkiej podejrzanej aktywności w systemie, włączając otwieranie przeglądarki internetowej z parametrami, ładowanie programu do pamięci procesu, przechwytywanie okien (te ustawienia są domyślnie wyłączone).

3.2.4. Konfiguracja ustawień aktualizacji

Poziom ochrony komputera bezpośrednio zależy od regularności aktualizacji baz danych sygnatur zagrożeń oraz modułów aplikacji. W oknie tym kreator wstępnej konfiguracji zaproponuje wybór trybu aktualizacji oraz możliwe będzie skonfigurowanie terminarza.

-  **Automatycznie.** Kaspersky Internet Security automatycznie szuka nowych uaktualnień zgodnie ze zdefiniowaną częstotliwością. Procedura ta wykonywana jest częściej w trakcie trwania epidemii wirusa, rzadziej natomiast po ich zakończeniu. Po wykryciu przez program najnowszych uaktualnień są one pobierane i instalowane na komputerze. Jest to ustawienie domyślne.
-  **Co n dni.** 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 pamiętać, że sygnatury zagrożeń i moduły programu dołączone do oprogramowania mogą być przestarzałe w momencie jego instalacji. Dlatego też, zalecane jest pobranie najnowszych uaktualnień. Aby to wykonać, należy kliknąć przycisk **Uaktualnij teraz**. Kaspersky Internet Security pobierze wymagane uaktualnienia z serwerów firmy Kaspersky Lab 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.

3.2.5. Konfiguracja terminarza skanowania

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

Podczas instalacji Kaspersky Internet Security tworzone są trzy domyślne zadania skanowania antywirusowego. W oknie tym należy wybrać ustawienia zadań skanowania:

Skanowanie obiektów startowych

Kaspersky Internet Security skanuje obiekty startowe podczas uruchamiania systemu operacyjnego. W celu zmodyfikowania ustawień terminarza skanowania obiektów startowych należy kliknąć przycisk **Zmień**.

Skanowanie obszarów krytycznych

W celu automatycznego skanowania obszarów krytycznych komputera (pamięci systemowej, obiektów startowych, sektorów startowych, folderów systemowych Microsoft Windows) w poszukiwaniu wirusów należy zaznaczyć odpowiednie pole. Możliwe jest skonfigurowanie terminarza przez kliknięcie przycisku **Zmień**.

Domyślnie automatyczne uruchamianie tego zadania skanowania jest wyłączone.

Pełne skanowanie komputera

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 komputera po instalacji programu.

3.2.6. Ograniczanie dostępu do programu

Z uwagi na możliwość użytkowania serwera przez wielu użytkowników oraz możliwość wyłączenia ochrony przez szkodliwe programy dostępna jest opcja ochrony dostępu do programu Kaspersky Internet Security lub modyfikacji ustawień przy użyciu 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:

- Modyfikacja 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 wstrzymania lub całkowitego wyłączenia ochrony w czasie rzeczywistym lub zadań skanowania antywirusowego.

3.2.7. Kontrola integralności aplikacji

Na tym etapie kreator konfiguracji Kaspersky Internet Security dokona analizy aplikacji zainstalowanych na komputerze (plików bibliotek, podpisów cyfrowych producentów), obliczy sumy kontrolne dla plików aplikacji oraz utworzy listę zaufanych aplikacji. Na przykład, lista ta domyślnie zawiera wszystkie aplikacje cyfrowo podpisane przez firmę Microsoft.

W przyszłości Kaspersky Internet Security będzie wykorzystywał informacje zebrane podczas analizy aplikacji w celu zapobiegnięcia umieszczenia niebezpiecznego kodu w modułach aplikacji użytkownika.

Analiza aplikacji zainstalowanych na komputerze może zająć chwilę czasu.

3.2.8. Konfiguracja ustawień zapory sieciowej

Zapora sieciowa jest składnikiem Kaspersky Internet Security nadzorującym pracę komputera w sieci lokalnej i Internecie. Na tym etapie kreator konfiguracji zaproponuje utworzenie listy reguł dla zapory sieciowej, służących do analizowania aktywności sieciowej komputera.

3.2.8.1. Określanie stanu ochrony dla stref

Na tym etapie kreator konfiguracji analizuje środowisko sieciowe komputera. W oparciu o tą analizę obszar sieci dzielony jest na strefy:

Internet – Globalna Sieć. W tej strefie program Kaspersky Internet Security pracuje jako osobista zapora sieciowa. Wszelka aktywność sieciowa regulowana jest przez domyślne reguły filtrowania pakietów i reguły dla aplikacji w celu zapewnienia maksymalnej ochrony. Podczas pracy w tej strefie nie można zmieniać ustawień ochrony, poza włączeniem **Trybu ukrycia** w celu zwiększenia bezpieczeństwa.

Strefy bezpieczeństwa – pewne strefy, w większości odpowiadające podsieciom, do których dołączony jest komputer (mogą nimi być podsieci lokalne w domu lub w pracy). Takie strefy są traktowane jako obszary umiarkowanego ryzyka. Użytkownik może zmieniać ich stan (w oparciu o poziom zaufania) oraz konfigurować reguły filtrowania pakietów i reguły dla aplikacji.

Wszystkie znalezione strefy zostaną wyświetlone na liście. Każda z nich wyświetlana jest wraz z opisem, adresem i maską podsieci oraz oceną, czy aktywność sieciowa ma być dozwolona czy blokowana przez moduł zapory sieciowej.

- **Internet.** Jest to domyślny stan przypisany do Internetu. Podczas korzystania z niego komputer jest celem wszelkich potencjalnych rodzajów zagrożeń. Użycie tego stanu jest również zalecane dla sieci, które nie są chronione przez jakiegokolwiek programy antywirusowe, zapory sieciowe, filtry itp. Po wybraniu tego stanu program zapewnia maksymalną ochronę oferując:
 - blokowanie aktywności sieciowej NetBIOS w obrębie podsieci
 - reguły blokujące dla aplikacji i filtrowania pakietów zezwalające na aktywność sieciową NetBIOS w obrębie tej podsieci

Nawet po utworzeniu ogólnie dostępnego katalogu informacje w nim zawarte nie będą dostępne dla użytkowników podsieci o tym stanie. Ponadto, po wybraniu tego stanu nie będzie można uzyskać dostępu do plików i drukarek na komputerach w innych sieciach.

- **Sieć lokalna.** Program przydziela ten stan do większości stref ochrony znalezionych podczas analizy środowiska sieciowego komputera, za wyjątkiem Internetu. Zalecane jest zastosowanie tego stanu do stref o średnim współczynniku ryzyka (na przykład, korporacyjnych sieci lokalnych). Po wybraniu tego stanu program:

- zezwala na dowolną aktywność sieciową NetBIOS w obrębie podsieci
- oferuje reguły blokujące dla aplikacji i filtrowania pakietów zezwalające na aktywność sieciową NetBIOS w obrębie tej podsieci

Należy wybrać ten stan w celu udzielenia dostępu do pewnych folderów lub drukarek na komputerze i blokowania innej aktywności zewnętrznej.

- **Zaufana.** Ten status jest przyznawany sieci, która jest całkowicie bezpieczna w opinii użytkownika, a komputer nie jest celem ataków i prób uzyskania dostępu do danych podczas korzystania z niej. Wszelka aktywność sieciowa jest dozwolona podczas korzystania z tego typu sieci. Nawet jeżeli wybrana zostanie maksymalna ochrona i utworzone zostaną reguły blokujące, nie będą one funkcjonowały dla zdalnych komputerów znajdujących się w zaufanej sieci.

Możliwe jest użycie trybu ukrycia w celu zwiększenia bezpieczeństwa podczas korzystania z Internetu. Funkcja ta umożliwia jedynie aktywność sieciową zainicjowaną przez użytkownika, co oznacza, że komputer staje się niewidzialny dla otoczenia. Tryb ten nie wpływa na wydajność pracy komputera podczas korzystania z Internetu.

Nie jest zalecane używanie trybu ukrycia w przypadku, gdy komputer pełni rolę serwera (na przykład serwera pocztowego lub serwera internetowego). W przeciwnym razie, komputery łączące się z serwerem nie zostaną połączone.

W celu zmiany stanu strefy lub włączenia/wyłączenia trybu ukrycia należy wybrać go z listy i użyć odpowiednich odsyłaczy w polu **Opis reguły** znajdującym się poniżej listy. Podobne czynności, wraz z modyfikowaniem adresów oraz masek podsieci, można wykonywać w oknie **Właściwości strefy**, które zostanie otwarte po kliknięciu przycisku **Modyfikuj**.

Podczas przeglądania listy można dodać do niej nową strefę. W tym celu należy kliknąć przycisk **Odśwież**. Zapora sieciowa wyszuka potencjalne strefy do rejestracji i jeżeli jakąś wykryje, zaproponuje dla niej wybór stanu. Ponadto, można ręcznie dodać nowe strefy do listy (na przykład po podłączeniu komputera do nowej sieci). W tym celu należy użyć przycisku **Dodaj** i wprowadzić niezbędne informacje w oknie **Właściwości strefy**.

W celu usunięcia definicji sieci z listy należy kliknąć przycisk **Usuń**.

3.2.8.2. Tworzenie listy aplikacji sieciowych

Kreator wstępnej konfiguracji programu analizuje zainstalowane na komputerze oprogramowanie i tworzy listę aplikacji korzystających z połączeń sieciowych.

Zapora sieciowa utworzy regułę kontrolowania aktywności sieciowej dla każdej tego typu aplikacji. Reguły stosowane są zgodnie z szablonami dla typowych aplikacji korzystających z połączeń sieciowych, utworzonymi przez firmę Kaspersky Lab i dołączonymi do oprogramowania.

W celu przejrzania listy aplikacji sieciowych oraz reguł stosowanych dla nich przez Zaporę sieciową należy kliknąć przycisk **Aplikacje**.

W celu zwiększenia bezpieczeństwa można wyłączyć pamięć podręczną DNS podczas używania zasobów internetowych. Funkcja ta drastycznie redukuje czas łączenia komputera z żądanymi zasobami internetowymi; jednakże, stanowi ona niebezpieczną lukę, umożliwiającą hakerom kradzież danych z uwagi na brak ich śledzenia przez zaporę sieciową. Dlatego też, w celu zwiększenia poziomu bezpieczeństwa komputera zalecane jest wyłączenie tej funkcji.

3.2.9. Finalizowanie działania kreatora konfiguracji

W ostatnim oknie kreatora zaproponowane zostanie ponowne uruchomienie komputera w celu dokończenia instalacji programu. Jest to niezbędne w celu poprawnego zarejestrowania w systemie sterowników Kaspersky Internet Security.

Można odłożyć ponowne uruchomienie komputera na później. Należy jednak pamiętać, że pewne składniki programu mogą nie działać.

3.3. Instalacja programu z poziomu wiersza poleceń

Aby zainstalować Kaspersky Internet Security przy użyciu wiersza poleceń, należy wykonać następujące polecenie:

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

Uruchomiony zostanie kreator instalacji (rozdział 3.1 na stronie 25). 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 <nazwa_pakietu> ALLOWREBOOT=1 /qn
```

ROZDZIAŁ 4. INTERFEJS PROGRAMU

Kaspersky Internet Security posiada prosty w użyciu interfejs. W tym rozdziale opisane zostaną jego podstawowe elementy (ikona zasobnika systemowego, menu kontekstowe, główne okno, okno ustawień programu).



Poza głównym interfejsem programu dostępne są wtyczki do następujących aplikacji Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail), The Bat!, Microsoft Internet Explorer, Microsoft Windows Explorer.

Wtyczki rozszerzają funkcjonalność tych programów, oferując dostęp do zarządzania i konfigurowania programu Kaspersky Internet Security z poziomu interfejsów tych programów.






4.1. Ikona zasobnika systemowego

Po zainstalowaniu programu Kaspersky Internet Security w zasobniku systemu Windows pojawi się ikona programu.

Ikona obrazuje funkcje wykonywane przez program Kaspersky Internet Security. Obrazuje ona stan ochrony i funkcji wykonywanych przez program.

Jeżeli ikona jest aktywna  (kolorowa), oznacza to, że komputer jest chroniony. Jeżeli ikona jest nieaktywna  (szara), oznacza to, że ochrona jest częściowo lub całkowicie wyłączona (rozdział 2.2.1 na stronie 18).

Ikona programu Kaspersky Internet Security zmienia się w zależności od wykonywanej operacji:

-  Skanowanie wiadomości pocztowych.
-  Skanowanie skryptów.
-  Skanowanie pliku otwieranego, zapisywanego lub uruchamianego przez użytkownika lub przez pewien program.
-  Aktualizacja baz danych i modułów Kaspersky Internet Security.
-  Błąd podczas działania Kaspersky Internet Security.

Ikona pozwala również na dostęp do podstawowych elementów interfejsu programu: menu kontekstowego (rozdział 4.2 na stronie 40) oraz okna głównego programu (rozdział 4.3 na stronie 41).

W celu otwarcia menu kontekstowego należy kliknąć prawym przyciskiem myszy ikonę programu.

W celu otwarcia okna głównego programu Kaspersky Internet Security w sekcji **Ochrona** (jest to domyślna sekcja wyświetlana po otwarciu programu) należy dwukrotnie kliknąć lewym przyciskiem myszy ikonę programu. Jednorazowe kliknięcie spowoduje otwarcie okna głównego w sekcji, która była aktywna przed ostatnim zamknięciem okna programu

Jeżeli dostępne są nowości publikowane przez firmę Kaspersky Lab, w zasobniku systemowym pojawi się odpowiednia ikona. Po dwukrotnym kliknięciu ikony wyświetlone zostanie okno, w którym dostępne będą najnowsze informacje.

4.2. Menu kontekstowe

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

Menu kontekstowe Kaspersky Internet Security zawiera następujące polecenia:

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

Skanowanie antywirusowe – wybranie obiektów i rozpoczęcie skanowania. Domyślna lista zawiera obiekty, 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 – uruchomienie aktualizacji baz danych i modułów Kaspersky Internet Security.

Monitor sieci – przeglądanie listy nawiązanych połączeń sieciowych, otwartych portów i ruchu.

Zablokuj ruch sieciowy – tymczasowe zablokowanie wszystkich możliwości nawiązania połączeń sieciowych. W przypadku wybrania tej opcji z menu, poziom ochrony zapory sieciowej zostanie zmieniony na **Blokuj wszystko**. W celu zezwolenia komputerowi na aktywność siecią należy wybrać odpowiedni poziom ochrony zapory sieciowej lub ponownie wybrać to polecenie.

Aktywuj – aktywacja programu. Należy aktywować posiadaną wersję programu Kaspersky Internet Security w celu uzyskania statusu zarejestrowanego użytkownika, który zapewnia użytkownikowi pełną funkcjonalność aplikacji i dostęp do pomocy technicznej. To polecenie dostępne jest jedynie w przypadku, gdy program nie został aktywowany.

Ustawienia – przeglądanie i konfiguracja ustawień Kaspersky Internet Security.

Otwórz Kaspersky Internet Security – otwarcie głównego okna programu (rozdział 4.3 na stronie 41).

Wstrzymaj ochronę / Wznów ochronę – tymczasowe wyłączenie lub włączenie działania składników ochrony w czasie rzeczywistym (rozdział 2.2.1 na stronie 18). To polecenie nie wpływa na działanie zadań pobierania uaktualnień i skanowania komputera.

Informacje o programie – wyświetlenie okna z informacjami na temat Kaspersky Internet Security.

Zakończ – zakończenie działania Kaspersky Internet Security (po wybraniu tego polecenia aplikacja zostanie wyładowana z pamięci RAM komputera).



Rysunek 1. Menu kontekstowe

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

4.3. Główne okno programu

Główne okno programu Kaspersky Internet Security (Rysunek 2) jest podzielona na trzy logiczne części:

- w górnej części okna wyświetlany jest bieżący stan ochrony komputera. Dostępne są trzy stany ochrony (rozdział 5.1 na stronie 47), a każdy z nich reprezentowany jest przez inny kolor. Kolor zielony oznacza, że komputer jest w pełni chroniony, natomiast kolory czerwony i żółty wskazują na istnienie różnych problemów w konfiguracji i działaniu Kaspersky Internet Security.

W celu uzyskania informacji na temat szybkiego rozwiązania problemu należy użyć Kreatora ochrony, który zostanie uruchomiony po kliknięciu odsyłacza powiadomienia.









Rysunek 2. Główne okno Kaspersky Internet Security

- *panel nawigacyjny* (lewa część okna) umożliwia szybki i łatwy dostęp do dowolnego składnika, zadań skanowania antywirusowego, aktualizacji i usług dodatkowych;
- 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.

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
 Ochrona <ul style="list-style-type: none"> <input checked="" type="radio"/> Ochrona plików <ul style="list-style-type: none"> Ochrona poczty Ochrona WWW Ochrona proaktywna Zapora sieciowa Ochrona prywatności Anti-Spam Kontrola rodzicielska 	<p>Podstawowym przeznaczeniem sekcji Ochrona jest dostęp do głównych składników ochrony w czasie rzeczywistym.</p> <p>W celu przejrzania stanu składnika ochrony lub jego modułów, skonfigurowania jego ustawień lub otwarcia raportu należy wybrać składnik z listy znajdującej się na zakładce Ochrona.</p> <p>Ta sekcja zawiera również odsyłacze do najczęściej wykorzystywanych zadań: skanowania antywirusowego i aktualizacji. Można przejrzeć informacje na temat stanu tych zadań, skonfigurować je lub uruchomić.</p>
 Skanuj <ul style="list-style-type: none"> Obszary krytyczne Mój komputer Obiekty startowe Wykrywanie rootkitów 	<p>Sekcja Skanuj umożliwi dostęp do zadań skanowania obiektów na obecność wirusów. Znajdują się na niej zadania utworzone przez ekspertów z firmy Kaspersky Lab (skanowanie obszarów krytycznych, obiektów startowych, pełne skanowanie komputera, skanowanie w poszukiwaniu rootkitów) oraz zadania utworzone przez użytkownika.</p> <p>Po wybraniu zadania w prawym panelu wyświetlone zostaną informacje na jego temat oraz możliwe będzie skonfigurowanie jego ustawień, utworzenie listy obiektów przeznaczonych do skanowania lub uruchomienie zadania.</p> <p>W celu przeskanowania pojedynczego obiektu (pliku, foldera lub dysku) należy z prawego panelu dla sekcji Skanuj dodać żądany obiekt do listy skanowanych obiektów i uruchomić zadanie.</p> <p>Możliwe będzie również utworzenie dysku ratunkowego.</p>

 Aktualizacja	<p>W sekcji Aktualizacja dostępne są informacje na temat aktualizacji aplikacji: data opublikowania baz danych i liczba sygnatur wirusów.</p> <p>Odpowiednie odsyłacze mogą zostać użyte w celu rozpoczęcia aktualizacji, przejrzania szczegółowego raportu, skonfigurowania zadania aktualizacji, cofnięcia aktualizacji do jej poprzedniej wersji.</p>
 Raporty i pliki danych	<p>Sekcja Raporty i pliki danych może zostać użyta w celu przejrzania szczegółowego raportu na temat dowolnego składnika aplikacji, zadania aktualizacji lub skanowania oraz w celu pracy z obiektami umieszczonymi w folderze kwarantanny lub kopii zapasowej.</p>
 Aktywacja	<p>Sekcja Aktywacja używana jest w celu zarządzania kluczami licencyjnymi wymaganymi do dostępu do pełnej funkcjonalności aplikacji (rozdział 7 na stronie 70).</p> <p>Jeżeli klucz nie jest zainstalowany, zalecane jest natychmiastowe jego nabycie i aktywowanie aplikacji (rozdział 3.2.2 na stronie 30).</p> <p>Jeżeli klucz jest zainstalowany, w sekcji tej znajdują się informacje na temat typu użytego klucza oraz data utraty jego ważności. Po zakończeniu okresu ważności bieżącego klucza można go przedłużyć na stronie internetowej firmy Kaspersky Lab.</p>
 Pomoc	<p>W sekcji Pomoc wyświetlane są informacje na temat pomocy technicznej świadczonej zarejestrowanym użytkownikom programu Kaspersky Internet Security.</p>

Każdy element panelu nawigacyjnego posiada własne menu kontekstowe. Menu zawiera polecenia, które pomagają w szybkiej konfiguracji, zarządzaniu oraz przeglądaniu raportów składników ochrony. Dostępne jest również dodatkowe menu dla

zadań skanowania antywirusowego, które można użyć do tworzenia własnych zadań opartych na wybranych zadaniach.

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

W dolnej części okna dostępne są dwa przyciski Pomoc (umożliwia dostęp do systemu pomocy Kaspersky Internet Security) i Ustawienia (otwiera okno ustawień aplikacji).

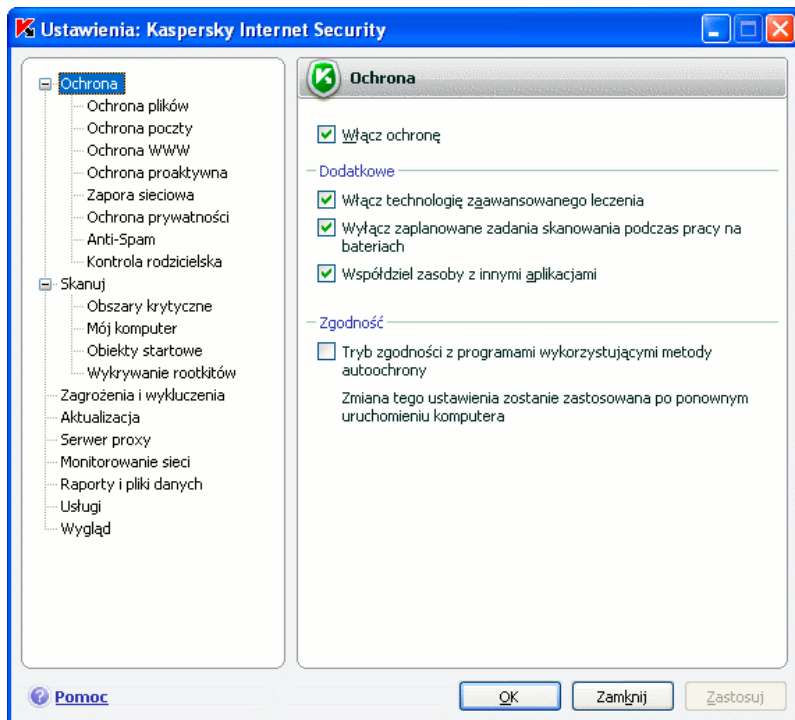
4.4. Okno ustawień programu

Okno ustawień Kaspersky Internet Security może zostać otwarte z poziomu głównego okna (rozdział 4.3 na stronie 41) lub menu kontekstowego (rozdział 4.2 na stronie 40). W tym celu należy kliknąć przycisk **Ustawienia** w dolnej części okna głównego lub wybrać odpowiednią opcję z menu kontekstowego aplikacji.

Układ okna ustawień (Rysunek 3) przypomina układ głównego okna:

- w lewej sekcji okna można uzyskać szybki i prosty dostęp do ustawień każdego składnika programu, aktualizacji, zadań skanowania antywirusowego oraz ogólnych ustawień aplikacji;
- 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 jest zawarty w dalszej części tego podręcznika.



Rysunek 3. Okno ustawień Kaspersky Internet Security

ROZDZIAŁ 5. ROZPOCZĘCIE PRACY

Jednym z głównych założeń firmy Kaspersky Lab w tworzeniu programu Kaspersky Internet Security było zapewnienie optymalnej konfiguracji dla wszystkich opcji programu. Mniej zaawansowani użytkownicy mogą bez trudu chronić swój komputer zaraz po instalacji programu, bez wykonywania czasochłonnej konfiguracji ustawień.

Jednakże, szczegóły konfiguracji komputera lub zadań, do których jest on wykorzystywany, mogą być bardzo różne. Dlatego też, zalecane jest wykonanie wstępnej konfiguracji programu w celu jego dostosowania do potrzeb użytkownika.

W celu uproszczenia rozpoczęcia korzystania z programu wszystkie etapy wstępnej konfiguracji (rozdział 3.2 na stronie 29) programu połączone zostały w jednym kreatorze konfiguracji programu uruchamianym podczas instalacji programu. Postępując zgodnie z instrukcjami kreatora, można aktywować program, skonfigurować ustawienia pobierania uaktualnień i uruchamiania skanowania, zdefiniować hasła dostępu do programu i skonfigurować moduł zapory sieciowej w celu dostosowania jego działania do właściwości sieci, z której korzysta użytkownik.

Po zainstalowaniu i uruchomieniu programu zalecane jest wykonanie następujących czynności:

- Sprawdzenie bieżącego stanu ochrony (rozdział 5.1 na stronie 47) w celu upewnienia się, czy Kaspersky Internet Security działa z wykorzystaniem odpowiedniego poziomu ochrony.
- Przeprowadzenie uczenia modułu Anti-Spam (rozdział 5.6 na stronie 52) przy użyciu wiadomości użytkownika.
- Uaktualnienie programu (rozdział 5.7 na stronie 53), jeżeli nie zostało to wykonane przez kreator konfiguracji po zakończeniu instalacji programu.
- Przeskanowanie komputera w poszukiwaniu wirusów (rozdział 5.3 na stronie 50).

5.1. Stan ochrony komputera

Stan ochrony wyświetlany jest w górnej części okna głównego. Reprezentowany jest przy pomocy trzech kolorów analogicznie do świateł w ruchu drogowym. W zależności od sytuacji, schemat kolorów górnej sekcji okna może się zmieniać. Po wykryciu zagrożenia wyświetlone zostaną odpowiednie informacje. Informacje te mają postać odsyłaczy, których kliknięcie spowoduje uruchomienie Kreatora ochrony.

Do zobrazowania stanu ochrony wykorzystywane są następujące kolory:

- Główne okno aplikacji jest zielone. Ten wskaźnik ochrony oznacza, że komputer jest w pełni chroniony.

Oznacza to, że bazy danych są regularnie aktualizowane, wszystkie składniki ochrony są aktywne, aplikacja działa z wykorzystaniem ustawień zalecanych

przez ekspertów z firmy Kaspersky Lab oraz nie wykryto szkodliwego oprogramowania.

- Główne okno aplikacji jest żółte. Poziom ochrony komputera jest niższy od zalecanego. Ten stan ochrony oznacza, że wykryto problemy w konfiguracji lub działaniu aplikacji.
- Mogą to być, na przykład, drobne odstępstwa od ustawień zalecanych, bazy danych nie były aktualizowane od kilku dni, nie przeprowadzono uczenia modelu antyspamowego.
- Główne okno aplikacji jest czerwone. Ten stan oznacza, iż istnieje duże ryzyko zainfekowania komputera lub utraty danych. Na przykład, jedna lub więcej usług ochrony nie zostało uruchomionych, produkt nie był aktualizowany od bardzo długiego czasu, wykryto zagrożenia, które muszą zostać szybko zneutralizowane, produkt nie został aktywowany.

W przypadku wystąpienia problemów z systemem ochrony, zalecane jest ich szybkie rozwiązanie. W tym celu można użyć Kreatora ochrony, który może zostać uruchomiony po kliknięciu odsyłacza powiadomienia. Kreator ochrony umożliwia przejrzanie wszystkich wykrytych zagrożeń oraz podjęcie odpowiednich działań w celu ich neutralizacji. Priorytet zagrożenia oznaczany jest przy pomocy odpowiedniego koloru wskaźnika:



– ten wskaźnik oznacza, że wykryto zagrożenia, które nie są krytyczne dla ochrony komputera, ale mogą obniżyć ogólny poziom ochrony. Należy zapoznać się z zaleceniami ekspertów z firmy Kaspersky Lab.



– ten wskaźnik oznacza, że wykryto zagrożenia krytyczne dla ochrony komputera. Należy zastosować się do podanych przez program zaleceń. Mają one na celu poprawienie ochrony komputera. Zalecane działania dostępne są w postaci odsyłaczy.

W celu przejrzania listy zagrożeń należy kliknąć przycisk Dalej. Dla każdego zagrożenia wyświetlany jest szczegółowy opis wraz z listą dostępnych akcji:

- **Natychmiastowa neutralizacja zagrożenia.** Przy użyciu odpowiednich odsyłaczy można wyeliminować zagrożenie. Szczegółowe informacje na temat danego zagrożenia można znaleźć w pliku raportu. Zalecana akcja spowoduje natychmiastową neutralizację zagrożenia.
- **Odłożenie neutralizacji zagrożenia.** Jeżeli z pewnych powodów nie będzie można natychmiast zneutralizować zagrożenia, można odłożyć tę akcję i wrócić do niego później. W tym celu należy kliknąć odsyłacz Pomiń.

Ta akcja nie jest dostępna dla zagrożeń krytycznych. Zagrożenia tego typu obejmują, na przykład, brak możliwości leczenia szkodliwych obiektów, błędy w działaniu składników programu lub uszkodzenie baz danych programu.

Jeżeli w trakcie pracy z kreatorem nie zostały zneutralizowane wszystkie zagrożenia, w górnej części okna będzie wyświetlane powiadomienie o konieczności ich neutralizacji. Po ponownym otwarciu Kreatora ochrony, pominięte (odroczone) zagrożenia nie będą znajdować się na liście aktywnych zagrożeń. W dowolnym momencie moż-

na do nich wrócić i zneutralizować odroczone zagrożenia poprzez kliknięcie odsyłacza [Przejrzyj pominięte](#) zagrożenia wyświetlanym w ostatnim oknie kreatora.

5.2. Weryfikacja stanu poszczególnych składników ochrony

W celu wyświetlenia stanu dowolnego składnika ochrony w czasie rzeczywistym należy otworzyć główne okno aplikacji i wybrać żądany składnik w sekcji **Ochrona**. Ogólne informacje na temat wybranego składnika zostaną wyświetlone w prawej części okna.

Najważniejszy jest stan składnika:

- *<nazwa składnika>*: *uruchomiono* – ochrona zapewniana przez składnik jest na zalecanym poziomie.
- *<nazwa składnika>*: *wstrzymano* – działanie składnika zostało wstrzymane na pewien okres czasu. Działanie składnika zostanie automatycznie wznowione po upływie zdefiniowanego przedziału czasu lub ponownym uruchomieniu aplikacji. Działanie składnika może zostać wznowione ręcznie. W tym celu należy kliknąć odsyłacz [Wznów działanie](#).
- *<nazwa składnika>*: *zatrzymano* – działanie składnika zostało zatrzymane przez użytkownika. Ochrona może zostać wznowiona poprzez kliknięcie odsyłacza [Włącz](#).
- *<nazwa składnika>*: *nie uruchomiono* – ochrona wykonywana przez składnik nie jest dostępna z pewnego powodu.
- *<nazwa składnika>*: *wyłączono (błąd)* – działanie składnika zakończyło się błędem.

Jeżeli podczas działania składnika wystąpił błąd, należy spróbować uruchomić go ponownie. Jeżeli błąd będzie się powtarzał, należy przejrzeć raport składnika, który może zawierać przyczynę jego występowania. Jeżeli użytkownik nie może sam rozwiązać problemu, należy zapisać raport z funkcjonowania składnika przy użyciu polecenia **Akcja** → **Zapisz jako** oraz skontaktować się z działem pomocy technicznej firmy Kaspersky Lab.

Poza stanem składnika mogą być również wyświetlane informacje na temat wykorzystywanych ustawień (takich jak, poziom ochrony, czynności wykonywane na niebezpiecznych obiektach). Jeżeli składnik składa się z więcej niż jednego modułu, wyświetlany jest także stan każdego z nich: włączony lub wyłączony. W celu zmodyfikowania bieżących ustawień składnika należy kliknąć [Ustawienia](#).

Dodatkowo dla każdego ze składników wyświetlane są statystyki działania. W celu wyświetlenia szczegółowego raportu należy kliknąć [Otwórz raport](#).

Jeżeli z pewnych przyczyn działanie składnika jest wstrzymane lub zatrzymane, wyniki jego działania przed wyłączeniem można przeglądać po kliknięciu odsyłacza [Otwórz ostatni raport](#).

5.3. W jaki sposób należy wykonać skanowanie komputera

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

Kaspersky Internet Security zawiera zadanie skanowania komputera w poszukiwaniu wirusów. Znajduje się ono w sekcji **Skanuj** głównego okna programu.

Po wybraniu zadania **Skanuj Mój komputer** wyświetlone zostaną ustawienia zadania: bieżący poziom ochrony oraz działania, które będą podejmowane po wykryciu niebezpiecznych obiektów. Dostępny jest także raport z ostatniego skanowania.

W celu przeskanowania komputera w poszukiwaniu szkodliwych programów należy:

1. Wybrać zadanie **Mój komputer** znajdujące się w sekcji **Skanuj** głównego okna programu.
2. Kliknąć odsyłacz [Uruchom skanowanie](#).

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

5.4. W jaki sposób należy wykonać skanowanie obszarów krytycznych

Komputer zawiera pewne obszary, które są krytyczne dla jego ochrony. Są one jednym z głównych celów ataków szkodliwych programów dążących do uszkodzenia systemu operacyjnego, procesora, pamięci itp.

Bardzo ważne jest zabezpieczenie tych obszarów w celu zapewnienia prawidłowego funkcjonowania komputera. W tym celu stworzone zostało specjalne zadanie skanowania tego typu obszarów. Znajduje się ono w sekcji **Skanuj** okna głównego programu.

Po wybraniu zadania **Obszary krytyczne** wyświetlone zostaną jego ustawienia: bieżący poziom ochrony oraz działania, które będą podejmowane po wykryciu szkodliwych obiektów. 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:

1. Wybrać zadanie **Obszary krytyczne** w sekcji **Skanuj** okna głównego aplikacji.
2. Kliknąć odsyłacz [Uruchom skanowanie](#).

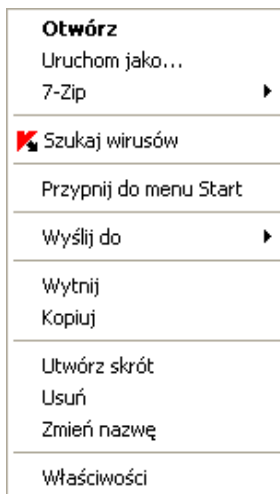
Program rozpocznie skanowanie wybranych obszarów krytycznych, wyświetlając szczegóły dotyczące skanowania w specjalnym oknie. Możliwe jest ukrycie okna skanowania. W tym celu należy je zamknąć. Nie spowoduje to zatrzymania skanowania.

5.5. W jaki sposób należy wykonać skanowanie plików, folderów lub dysków

W pewnych okolicznościach może zająć potrzeba wykonania skanowania wybranych obiektów zamiast całego komputera. Obiekty takie mogą obejmować, na przykład, dysk twardy, na którym przechowywane są pliki programów i gier, pocztowe bazy danych przyniesione z biura, archiwum dołączone do otrzymanej wiadomości pocztowej itd. Obiekty przeznaczone do skanowania mogą zostać wybrane przy użyciu standardowych narzędzi systemu Windows (na przykład **Eksploratora Windows**, sekcji **Mój komputer** itd.).

W celu przeskanowania obiektu należy:

Kliknąć prawym przyciskiem żądany obiekt i z menu kontekstowego, które zostanie wyświetlone na ekranie, wybrać polecenie **Szukaj wirusów** (Rysunek 4).



Rysunek 4. Skanowanie obiektu wybranego przy użyciu standardowych narzędzi systemu Microsoft Windows

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

5.6. W jaki sposób należy przeprowadzić uczenie modułu Anti-Spam

Jednym z etapów rozpoczęcia pracy z programem jest przeprowadzenie uczenia modułu Anti-Spam na poczcie elektronicznej użytkownika. Spam jest niechcianą wiadomością pocztową. Bardzo trudno jest stwierdzić, która z wiadomości otrzymanych od innych użytkowników stanowi spam. Istnieje wiele kategorii wiadomości pocztowych, które z dużą dokładnością mogą zostać sklasyfikowane jako spam (na przykład, masowo rozsyłane wiadomości, reklamy). Wiadomości tego typu mogą również znajdować się w skrzynkach odbiorczych niektórych użytkowników.

Z tego powodu użytkownik powinien określić, które z wiadomości mają być klasyfikowane jako spam. Po zakończeniu instalacji Kaspersky Internet Security zaproponuje użytkownikowi rozpoczęcie uczenia modułu Anti-Spam. Operację tę można wykonać przy pomocy specjalnych przycisków, które zostały dołączone do klienta pocztowego (Outlook, Outlook Express (poczta systemu Windows), The Bat!) lub za pomocą specjalnego kreatora uczenia.

Uwaga!

Ta wersja Kaspersky Internet Security nie posiada wtyczek antyspamowych dla 64-bitowych wersji programów Microsoft Office Outlook, Microsoft Outlook Express oraz The Bat!

W celu przeprowadzenia uczenia modułu Anti-Spam przy pomocy specjalnych przycisków należy:

1. Otworzyć domyślny program pocztowy (np.: Microsoft Office Outlook). W pasku narzędzi widoczne będą dwa przyciski: **Spam** i **Czysta wiadomość**.
2. Wybrać jedną lub więcej akceptowanych wiadomości pocztowych i kliknąć przycisk **Czysta wiadomość**. Od tego momentu korespondencja pochodząca z adresów występujących w zaznaczonych wiadomościach nie będzie nigdy klasyfikowana jako spam.
3. Wybrać jedną lub więcej wiadomości pocztowych zawierających spam i kliknąć przycisk **Spam**. Od tego momentu korespondencja posiadająca cechy występujące w zaznaczonych wiadomościach będzie zawsze traktowana jako spam.

W celu przeprowadzenia uczenia modułu Anti-Spam przy pomocy kreatora uczenia należy:

Wybrać moduł **Anti-Spam** w sekcji **Ochrona** znajdującej się w oknie głównym aplikacji i kliknąć odsyłacz [Uruchoom kreator uczenia](#).

Po otrzymaniu nowej wiadomości elektronicznej i zapisaniu jej w skrzynce odbiorczej moduł Anti-Spam przeskanuje ją w poszukiwaniu spamu i w przypadku jego wykrycia dołączy do jej tematu specjalny znacznik [**Spam**]. W wykorzystywanym programie pocztowym użytkownik może stworzyć regułę usuwającą lub przenoszącą takie wiadomości do specjalnego foldera.

5.7. Jak uaktualnić program

Firma Kaspersky Lab regularnie tworzy uaktualnienia sygnatur zagrożeń oraz modułów programu Kaspersky Internet Security i umieszcza je na specjalnych serwerach.

Serwery uaktualnień firmy Kaspersky Lab są miejscami w Internecie, gdzie firma Kaspersky Lab przechowuje uaktualnienia aplikacji.

Uwaga!

W celu aktualizacji programu Kaspersky Internet Security konieczny jest dostęp do Internetu.

Kaspersky Internet Security automatycznie wyszukuje uaktualnienia na serwerach firmy Kaspersky Lab. Po pojawieniu się uaktualnień pobiera je i instaluje w tle.

W celu ręcznej aktualizacji programu Kaspersky Internet Security należy:

1. Wybrać sekcję Aktualizacja okna głównego programu.
2. Kliknąć Uaktualnij sygnatury.

Kaspersky Internet Security rozpocznie pobieranie uaktualnień, wyświetlając informacje szczegółowe w specjalnym oknie.

5.8. Jak postępować, gdy ochrona nie działa

W przypadku wystąpienia problemów w funkcjonowaniu jednego ze składników ochrony, należy sprawdzić jego stan. Jeżeli stan składnika wyświetlany jest w postaci nie jest uruchomiony lub uruchomiony (błąd podsystemu), należy spróbować uruchomić ponownie program.

Jeżeli ponowne uruchomienie programu nie rozwiąże problemu, zalecane jest rozwiązanie ich przy pomocy funkcji naprawienia aplikacji (**Start**→**Programy**→**Kaspersky Internet Security 7.0**→**Modyfikuj, napraw lub usuń**).

Jeżeli funkcja naprawienia nie rozwiąże problemu, zalecane jest skontaktowanie się z działem pomocy technicznej firmy Kaspersky Lab. Wymagane będzie również zapisanie raportu z działania składnika i wysłanie go do działu pomocy technicznej firmy Kaspersky Lab.

W celu zapisania raportu z działania składnika należy:

1. Wybrać składnik z sekcji **Ochrona** okna głównego aplikacji i kliknąć odsyłacz Otwórz raport (jeżeli składnik jest obecnie uruchomiony) lub Otwórz ostatni raport (jeżeli składnik jest wyłączony).
2. W oknie raportu kliknąć **Akcja** → **Zapisz jako** i w oknie, które zostanie otwarte, określić nazwę dla pliku raportu.

ROZDZIAŁ 6. ZARZĄDZANIE OCHRONĄ

Rozdział ten zawiera informacje na temat konfiguracji ogólnych ustawień aplikacji wykorzystywanych przez wszystkie składniki ochrony w czasie rzeczywistym oraz zadania, jak również informacje na temat tworzenia obszaru ochrony, list zagrożeń wykrywanych przez program oraz listy zaufanych aplikacji wykluczonych z ochrony.

6.1. Włączanie i wyłączanie ochrony komputera

Kaspersky Internet Security uruchamia się domyślnie podczas włączenia komputera i zapewnia ochronę przez cały czas pracy. Świadczy o tym napis *Kaspersky Internet Security 7.0* wyświetlany w prawym górnym rogu ekranu logowania systemu Windows. Wszystkie składniki ochrony w czasie rzeczywistym są uruchomione (rozdział 2.2.1 na stronie 18).

Możliwe jest całkowite lub częściowe wyłączenie ochrony oferowanej przez program Kaspersky Internet Security.

Uwaga!

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

Należy pamiętać o tym, że w takim przypadku ochrona jest omawiana w kontekście składników ochrony. Wyłączenie lub wstrzymanie wybranych składników ochrony nie ma wpływu na działanie zadań skanowania i aktualizacji programu.

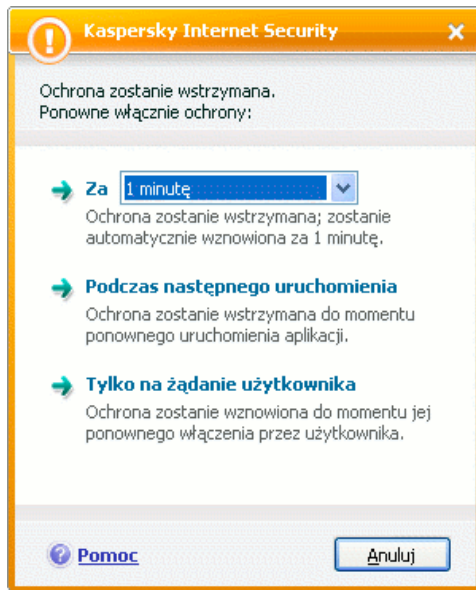
6.1.1. Wstrzymywanie ochrony

Wstrzymanie ochrony oznacza tymczasowe wyłączenie wszystkich składników monitorujących pliki zapisane na komputerze, odbieraną i wysyłaną pocztę elektroniczną, wykonywane skrypty, zachowanie aplikacji, zaporę sieciową, moduł antyspamowy oraz Kontrolę rodzicielską.

W celu wstrzymania ochrony komputera w czasie rzeczywistym:

1. Z menu kontekstowego programu (rozdział 4.2 na stronie 40) należy wybrać opcję **Wstrzymaj ochronę**.
2. W oknie **Wstrzymaj ochronę** (Rysunek 5), które zostanie otwarte, należy zdefiniować warunek automatycznego wznowienia ochrony:
 - **Za <przedział czasu>** – ochrona zostanie wznowiona po upływie określonego przedziału czasu. Przedział czasu należy wybrać przy użyciu listy rozwijalnej.

- 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 (rozdział 6.5 na stronie 68)).
- 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 5. Okno wstrzymywania ochrony

Jeżeli ochrona zostanie wstrzymana, wszystkie składniki będą nieaktywne. Zobrazowane jest to przez:

- Nieaktywne (szare) nazwy wyłączonych składników ochrony w sekcji Ochrona okna głównego programu.
- Nieaktywną (czarno białą) ikonę programu w zasobniku systemowym.

6.1.2. Wyłączanie ochrony

Wyłączenie ochrony oznacza całkowite wyłączenie działania składników ochrony w czasie rzeczywistym. W tym trybie funkcjonują wyłącznie zadania skanowania antywirusowego i aktualizacji.

Jeżeli ochrona jest wyłączona, może ona zostać włączona jedynie przez użytkownika. Składniki ochrony nie zostaną automatycznie włączone po ponownym uruchomieniu systemu lub programu. Jeżeli wystąpi konflikt programu Kaspersky Internet Security z innymi aplikacjami zainstalowanymi na komputerze, nie jest wymagane

całkowite zatrzymywanie ochrony. Można wyłączyć pojedyncze składniki ochrony lub utworzyć listę wykluczeń (rozdział 6.3 na stronie 58).

W celu wyłączenia ochrony należy:

1. Otworzyć okno ustawień aplikacji i kliknąć sekcję **Ochrona**.
2. Usunąć zaznaczenie z opcji **Włącz ochronę**.

W wyniku wyłączenia ochrony zatrzymane zostanie działanie wszystkich składników programu. Zobrazowane jest to przez:

- Niekatywnie (szare) nazwy wyłączonych składników ochrony w sekcji **Ochrona** okna głównego programu.
- Niekatywną (czarno-białą) ikonę programu w zasobniku systemowym.

6.1.3. Wstrzymywanie / zatrzymywanie składników ochrony, zadań skanowania i aktualizacji

Dostępnych jest wiele metod wyłączania składników ochrony. Przed wykonaniem tej czynności należy rozważyć konieczność jej wykonania. Często występujący problem może zostać rozwiązany w inny sposób, na przykład poprzez zmianę poziom ochrony. Jeżeli program wykrywa zagrożenie w obiekcie, który z całą pewnością jest bezpieczny, można dodać go do listy wykluczeń (rozdział 6.3 na stronie 58).

W celu wstrzymania działania składnika ochrony należy:

Otworzyć okno główne aplikacji, wybrać składnik z sekcji **Ochrona** i kliknąć odsyłacz Wstrzymaj.

Stan składnika zmieni się na wstrzymano. Działanie składnika lub zadania będzie wstrzymane do momentu ponownego uruchomienia programu lub kliknięcia Wznów działanie.

Po wstrzymaniu działania składnika statystyki dla bieżącej sesji programu Kaspersky Internet Security zostaną zapisane i będą gromadzone dalej po wznowieniu działania składnika.

W celu zatrzymania działania składnika ochrony należy:

Otworzyć okno główne aplikacji, wybrać składnik z sekcji **Ochrona** i kliknąć odsyłacz Zatrzymaj.

Stan składnika zostanie zmieniony na wyłączony oraz nazwa składnika wyświetlana w sekcji **Ochrona** będzie nieaktywna (szara). Ochrona realizowana przez ten składnik zostanie wyłączona do momentu wznowienia działania składnika przy użyciu odsyłacza Włącz.

Działanie dowolnego składnika może zostać wyłączone przy użyciu okna ustawień aplikacji. W tym celu należy otworzyć okno ustawień, wybrać składnik w sekcji **Ochrona** i usunąć zaznaczenie z opcji **Włącz <nazwa składnika>**.

Po wyłączeniu działania składnika wszystkie statystyki z poprzedniej sesji jego działania zostaną usunięte. Po wznowieniu jego działania będą one rejestrowane od nowa.

Pewne składniki ochrony zostaną również wyłączone po wyłączeniu ochrony komputera w czasie rzeczywistym (rozdział 6.1.2 na stronie 55).

6.1.4. Wznawianie ochrony komputera

Po wstrzymaniu lub wyłączeniu ochrony komputera można ją wznowić przy użyciu następujących metod:

- *Z poziomu menu kontekstowego.*

W tym celu należy wybrać opcję **Wznów ochronę**.

- *Z poziomu okna głównego programu.*

W lewej części okna głównego programu wybrać sekcję **Ochrona** i kliknąć odsyłacz Wznów ochronę.

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

6.2. Typy wykrywanego szkodliwego oprogramowania

Kaspersky Internet Security chroni przed różnymi rodzajami szkodliwych programów. Niezależnie od ustawień program wykrywa i neutralizuje wirusy, trojany, backdoory oraz narzędzia hakerskie. Tego typu programy mogą wyrządzić największe szkody w komputerze. W celu zwiększenia bezpieczeństwa komputera można rozszerzyć listę zagrożeń, które będą wykrywane przez program, poprzez włączenie monitorowania różnych typów potencjalnie niebezpiecznych aplikacji.

W celu wybrania rodzaju szkodliwych programów, przed którymi będzie chronił Kaspersky Internet Security, należy w oknie ustawień aplikacji wybrać sekcję **Zagrożenia i wykluczenia** (Rysunek 6).

Pole **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 i jego wyłączenie spowodowałoby zwiększenie ryzyka zainfekowania komputera. Zgodnie z zaleceniami ekspertów z firmy Ka-

spersky Lab, nie można usunąć tych obiektów z listy elementów monitorowanych przez program Kaspersky Internet Security.

- 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.

Opisane wyżej grupy obejmują pełny obszar sygnatur zagrożeń wykrywanych przez program podczas skanowania obiektów.

Po wybraniu wszystkich grup Kaspersky Internet Security zapewnia najpełniejszą ochronę antywirusową komputera. W przypadku, gdy druga i trzecia grupa jest wyłączona, program będzie chronił jedynie przed najbardziej powszechnymi szkodliwymi programami. Ochrona nie będzie obejmowała potencjalnie niebezpiecznych programów oraz takich, które po zainstalowaniu na komputerze mogą uszkodzić pliki, umożliwić kradzież pieniędzy lub inne niepożądane działania.

Ekspersi z firmy Kaspersky Lab nie zalecają wyłączania monitorowania dla drugiej grupy. Jeżeli Kaspersky Internet Security sklasyfikuje pewien program jako potencjalnie niebezpieczny wirus, a w rzeczywistości tak nie jest, zalecane jest zdefiniowanie dla niego wykluczenia (rozdział 6.3 na stronie 58).

W celu wybrania typu monitorowanych szkodliwych programów należy:

otworzyć okno ustawień aplikacji i wybrać **Zagrożenia i wykluczenia**. Konfiguracji należy dokonać w sekcji **Kategorie szkodliwego oprogramowania** (Rysunek 6).

- Kategorie szkodliwego oprogramowania
- Wirusy, robaki, konie trojańskie, narzędzia hakerskie
 - Oprogramowanie spyware, adware, dialery
 - Potencjalnie niebezpieczne oprogramowanie (riskware)

Rozumiem, że niektóre legalne programy mogą być klasyfikowane jako potencjalnie niebezpieczne i chcę, aby były one rozpoznawane jako zagrożenie dla komputera.

Rysunek 6. Wybór typu wykrywanych zagrożeń

6.3. Tworzenie strefy zaufanej

Strefa zaufana jest utworzoną przez użytkownika listą obiektów, które nie są monitorowane przez Kaspersky Internet Security. Innymi słowy, jest to grupa programów wykluczonych z ochrony.

Użytkownik tworzy strefę zaufaną w oparciu o właściwości używanych przez niego plików i programów zainstalowanych na komputerze. Utworzenie tego typu listy wykluczeń może okazać się niezbędne, jeżeli na przykład Kaspersky Internet Security blokuje dostęp do obiektu lub programu, który w opinii użytkownika jest całkowicie bezpieczny.

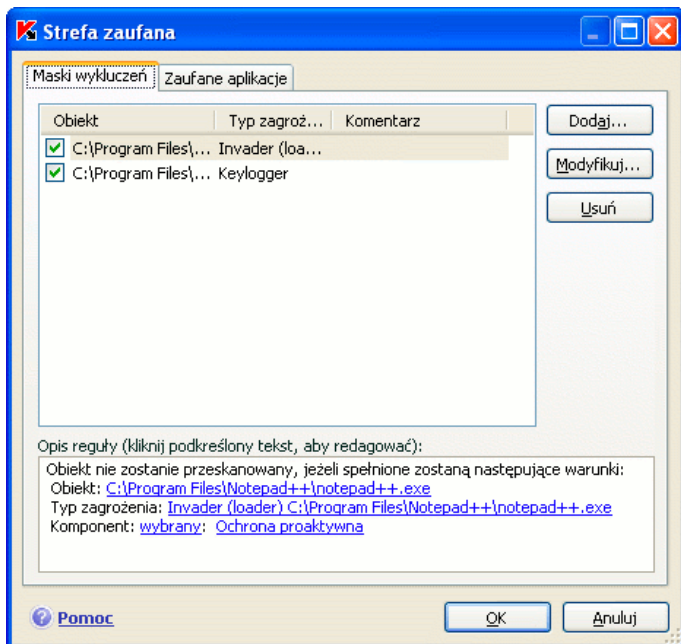
Możliwe jest wykluczanie z obszaru skanowania określonych formatów plików, użycie masek plików, wykluczanie określonych obszarów (na przykład folderu lub programu), wykluczanie procesów programu lub obiektów według stanu przydzielonego im podczas skanowania.

Uwaga!

Wykluczone obiekty nie są skanowane, nawet jeżeli folder lub dysk, na którym się znajdują, widnieje na liście skanowanych obiektów. Jeżeli taki obiekt zostanie bezpośrednio wybrany do skanowania, wykluczenie nie zostanie uwzględnione.

W celu utworzenia listy wykluczeń należy:

1. Otworzyć okno ustawień aplikacji i wybrać sekcję Zagrożenia i wykluczenia (Rysunek 6).
2. Kliknąć przycisk Strefa zaufana znajdujący się w sekcji Wykluczenia.
3. Dokonać konfiguracji reguł dla obiektów i utworzyć listę zaufanych aplikacji w oknie, które zostanie otwarte (Rysunek 7).



Rysunek 7. Tworzenie strefy zaufanej

6.3.1. Reguły wykluczeń

Reguły wykluczeń to zestawy warunków używanych przez Kaspersky Internet Security w celu wykluczenia 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 klasyfikacji dostępnej w Encyklopedii Wirusów.

Typ zagrożenia jest stanem przydzielanym przez Kaspersky Internet Security do obiektu po podczas skanowania. Werdykt przydzielany jest w oparciu o klasyfikację szkodliwych lub potencjalnie niebezpiecznych programów znajdującą się w Encyklopedii Wirusów firmy Kaspersky Lab.

Potencjalnie niebezpieczne aplikacje nie posiadają szkodliwych funkcji, mogą jednak zostać wykorzystane jako dodatkowy składnik złośliwego kodu, ponieważ zawierają wiele luk i błędów. Kategoria ta zawiera, przykładowo: programy do zdalnej administracji, klienci IRC, usługi FTP, narzędzia do celowego zatrzymywania lub ukrywania procesów, keyloggersy, autodialery itp. Programy takie nie są klasyfikowane jako wirusy. Mogą one być podzielone na wiele typów, np.: adware, jokes (żarty) riskware itp. Szczegółowe informacje dotyczące niebezpiecznych programów wykrywanych przez Kaspersky Internet Security można znaleźć w Encyklopedii Wirusów (na stro-

nie 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 wykluczenia ich z obszaru skanowania. W tym celu jako wykluczenie należy określić werdykt przydzielony do żądanej aplikacji.

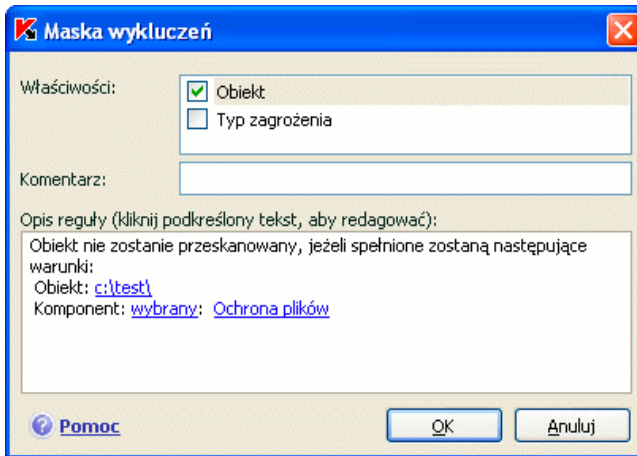
Na przykład: użytkownik w codziennej pracy używa programu do zdalnej administracji. Jest to narzędzie pozwalające na zdalny dostęp do innego komputera. Kaspersky Internet Security wykrywa aktywność takich aplikacji jako podejrzaną i może zablokować program. W celu uniemożliwienia zablokowania aplikacji przez program należy utworzyć regułę wykluczającą jej blokowanie.

Podczas dodawania wykluczenia tworzone są reguły dla poszczególnych składników programu (Ochrona plików, Ochrona poczty, Ochrona proaktywna, Kontrola prywatności) i zadań 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 **Maski wykluczeń** należy:

1. Kliknąć przycisk **Dodaj** w oknie **Maski wykluczeń** (Rysunek 7).
2. W oknie, które zostanie otwarte (Rysunek 8), wybrać typ zagrożenia w sekcji **Właściwości**:

- Obiekt** – wykluczenie ze skanowania określonego obiektu, foldera lub plików pasujących do podanych masek.
- Typ zagrożenia** – wykluczenie ze skanowania obiektów w oparciu o stan przydzielony do nich na podstawie nazewnictwa Encyklopedii Wirusów.



Rysunek 8. Tworzenie reguły wykluczenia

W przypadku jednoczesnego zaznaczenia obu pól, utworzona zostanie reguła dla obiektu o określonym typie werdyktu. W tej sytuacji zastosowane zostaną następujące reguły:

- Jeżeli zdefiniowane zostaną: plik jako **Obiekt** oraz odpowiedni stan jako **Typ zagrożenia**, plik zostanie wykluczony tylko wtedy, gdy podczas skanowania zostanie sklasyfikowany jako wskazane zagrożenie.
 - Jeżeli zdefiniowane zostaną: obszar lub folder jako **Obiekt** oraz odpowiedni stan (lub maska werdyktu) jako **Typ zagrożenia**, obiekt posiadający dany stan zostanie wykluczony z obszaru skanowania jedynie w obrębie zdefiniowanego 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 pola **Obiekt** należy wprowadzić jego nazwę w oknie, które zostanie otwarte (może to być plik, folder lub maska pliku). W celu rekursywnego wykluczenia ze skanowania obiektu (pliku, maki pliku, foldera) należy zaznaczyć opcję **Włączając podfoldery**. Na przykład, jeżeli jako wykluczenie zdefiniowano **C:\Program Files\winword.exe** i zaznaczona została opcja włączająca podfoldery, plik **winword.exe** będzie wykluczony ze skanowania, jeżeli zostanie znaleziony w dowolnym podfolderze znajdującym się w **C:\Program Files**.
- Wprowadzić pełną nazwę zagrożenia (zgodnie z nazewnictwem stosowanym w Encyklopedii Wirusów), które ma zostać wykluczone z obszaru skanowania lub użyć maski jako typu zagrożenia.

Dla niektórych typów zagrożeń można przypisać zaawansowane warunki stosowania wykluczeń w polu **Ustawienia zaawansowane**. W większości przypadków pole to jest wypełniane automatycznie podczas dodawania reguły z poziomu powiadomienia modułu Ochrona proaktywna.

Możliwe jest dodanie zaawansowanych ustawień dla (między innymi) następujących typów werdyktów:

- **Invader** (osadzany w procesach programów). Dla takiego werdyktu, jako dodatkowy warunek wykluczenia, można określić nazwę, maskę lub pełną ścieżkę do obiektu dołączanego programu (na przykład, pliku .dll).
- **Launching Internet Browser**. Dla tego werdyktu jako dodatkowe ustawienia wykluczenia, można zdefiniować ustawienia otwierania przeglądarki. Na przykład, w ustawieniach analizy aktywności aplikacji modułu Ochrona proaktywna można zablokować możliwość otwierania przeglądarki z pewnymi ustawieniami (parametrami). Można utworzyć regułę wykluczenia dla przeglądarki internetowej, zezwalającą na otwieranie odsyłaczy do domeny **www.kaspersky.pl** wyświetlanych w oknach programu Microsoft Office Outlook. W tym celu należy wybrać Microsoft Office Outlook jako **Obiekt** i **Launching Internet Browser** jako **Typ zagrożenia** oraz w polu **Ustawienia zaawansowane** podać maskę domeny, dla której zezwolono na działanie.

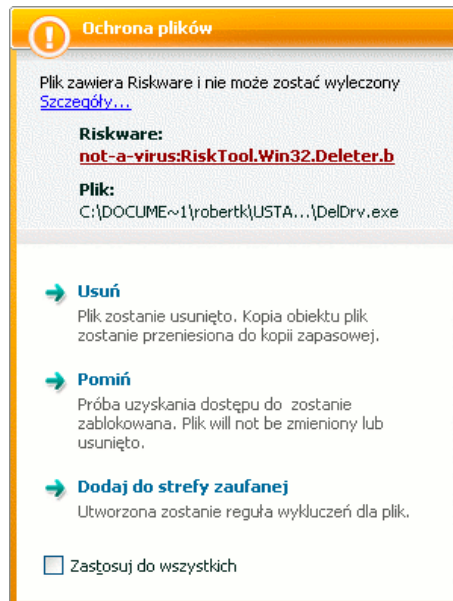
4. Zdefiniować składniki programu Kaspersky Internet Security, które będą używać tej reguły. Jeżeli wybrano opcję dowolne, reguła będzie stosowana przez wszystkie składniki. Aby ograniczyć liczbę modułów stosujących regułę, należy kliknąć odsyłacz dowolne – zostanie on zmieniony na wybrane. W oknie, które zostanie wyświetlone 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:

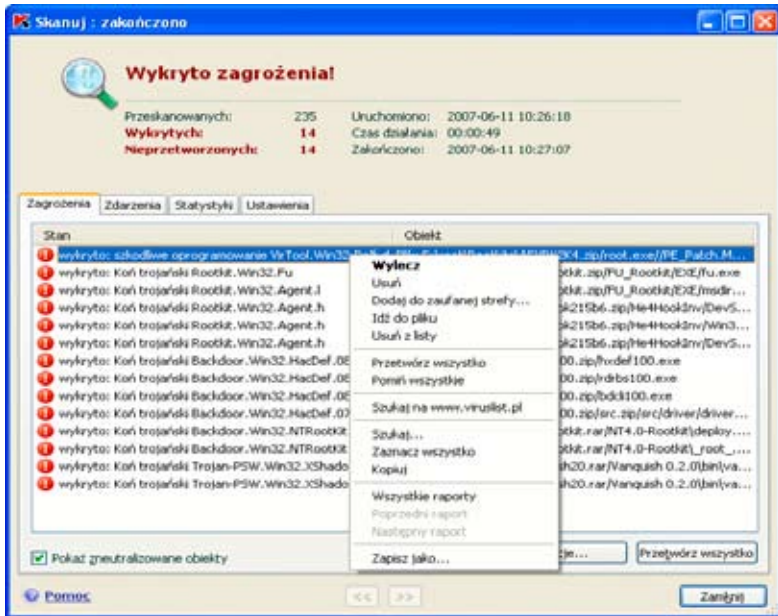
1. Użyć odsyłacz Dodaj do zaufanej strefy w oknie powiadomienia (Rysunek 9).
2. W oknie, które zostanie otwarte, należy upewnić się, czy wszystkie reguły wykluczenia są zgodne z wybranymi ustawieniami. Program automatycznie uzupełni nazwę obiektu i typ zagrożenia w oparciu o informacje zawarte w powiadomieniu. W celu utworzenia reguły należy kliknąć przycisk **OK**.

W celu utworzenia reguły wykluczenia z poziomu okna raportu należy:

1. Wybrać w oknie raportu obiekt, który ma zostać dodany do wykluczeń.
2. Otworzyć menu kontekstowe i wybrać polecenie **Dodaj do zaufanej strefy** (Rysunek 10).
3. Otwarte zostanie okno ustawień dla wykluczeń. Należy upewnić się, czy wszystkie reguły wykluczenia są zgodne z żądanymi ustawieniami. Program automatycznie uzupełni nazwę obiektu i typ zagrożenia w oparciu o informacje zawarte w raporcie. W celu utworzenia reguły należy kliknąć przycisk **OK**.



Rysunek 9. Powiadomienie o wykryciu niebezpiecznego obiektu



Rysunek 10. Tworzenie reguł wyłączeń z poziomu okna raportów

6.3.2. Zaufane aplikacje

Kaspersky Internet Security umożliwia utworzenie listy zaufanych aplikacji, których aktywność plikowa, sieciowa (niezależnie do jej charakteru) oraz dostęp do rejestru nie będą monitorowane.

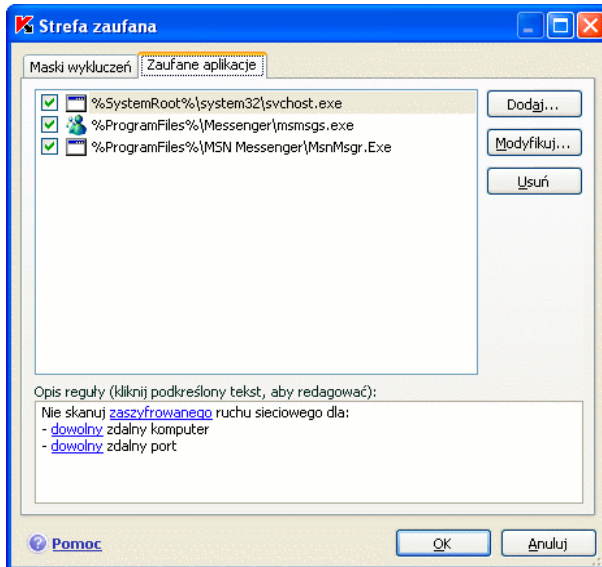
Przykład: użytkownik przekonany jest o bezpieczeństwie obiektów używanych przez notatnik systemu Windows i uważa, że nie ma potrzeby ich skanowania. W celu wyłączenia ze skanowania obiektów używanych przez ten proces należy do listy zaufanych aplikacji dodać Notatnik. Jednakże, plik wykonywalny i proces zaufanej aplikacji nadal będzie skanowany. W celu całkowitego wyłączenia aplikacji z obszaru skanowania należy użyć reguł wyłączeń (rozdział 6.3.1 na stronie 60).

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 wyłączeń dla zaufanych aplikacji można również rozwiązać potencjalne problemy związane ze zgodnością pomiędzy programem Kaspersky Internet Security i innymi aplikacjami oraz zwiększyć wydajność pracy komputera, co jest szczególnie ważne podczas używania aplikacji serwerowych.

Domyślnie Kaspersky Internet Security skanuje otwierane, uruchomione lub zapisywane obiekty przez dowolny proces oraz monitoruje aktywność wszystkich programów i przesyłanego przez nie ruchu sieciowego.

Możliwe jest utworzenie listy zaufanych aplikacji na specjalnej zakładce **Zaufane aplikacje** (Rysunek 11). Domyślna lista tworzona jest podczas instalacji i zawiera informacje o aplikacjach, których aktywność nie jest skanowana (zgodnie z zaleceniami ekspertów z firmy Kaspersky Lab). Jeżeli użytkownik nie ufa aplikacjom znajdującym się na liście, można usunąć zaznaczenia z odpowiednich pól. Można dodawać i modyfikować zawartość listy przy użyciu przycisków **Dodaj**, **Modyfikuj** i **Usuń**.



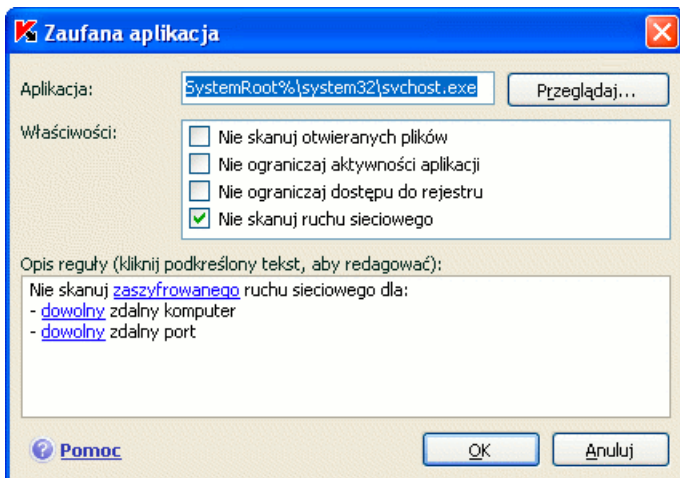
Rysunek 11. Lista zaufanych aplikacji

W celu dodania programu do listy zaufanych aplikacji należy:

1. Kliknąć przycisk **Dodaj** znajdujący się z prawej strony zakładki **Zaufane aplikacje**.
2. W oknie **Zaufana aplikacja** (Rysunek 12), które zostanie otwarte i wybrać aplikację przy użyciu przycisku **Przełączaj**. Otwarte zostanie menu kontekstowe, w którym należy kliknąć przycisk **Przełączaj** w celu wybrania ścieżki do pliku wykonywalnego lub przycisk **Aplikacje** w celu wyświetlenia listy uruchomionych aplikacji i wybrania żądanych aplikacji.

Po wybraniu aplikacji Kaspersky Internet Security zapamięta wewnętrzne atrybuty pliku wykonywalnego i będzie ich używał do identyfikowania programu jako zaufanego podczas skanowania.

Ścieżka do pliku uzupełniania jest automatycznie po wybraniu jego nazwy.



Rysunek 12. Dodawanie aplikacji do listy zaufanych aplikacji

3. Określić działania wykonywane przez ten proces, które nie będą monitorowane:

- Nie skanuj otwieranych plików** – wykluczenie z obszaru skanowania wszystkich plików, które są otwierane przez proces zaufanej aplikacji.
- Nie ograniczaj aktywności aplikacji** – wykluczenie z obszaru ochrony proaktywnej wszelkiej aktywności, która jest udziałem zaufanej aplikacji.
- Nie ograniczaj dostępu do rejestru** – wykluczenie z obszaru skanowania prób uzyskania dostępu do rejestru systemowego przez zaufane aplikacje.
- Nie skanuj ruchu sieciowego** – wykluczenie z obszaru skanowania ruchu sieciowego inicjowanego przez zaufaną aplikację. Ze skanowania można wykluczyć cały ruch sieciowy lub tylko zaszyfowany (SSL). W celu zdefiniowania wykluczenia należy kliknąć odsyłacz całego. Zostanie on zmieniony na zaszyfowanego. Dodatkowo dla wykluczenia można przypisać zdalny port/komputer. W celu utworzenia wykluczenia należy kliknąć odsyłacz dowolny, co spowoduje jego zmianę na wybrany. W oknie, które zostanie otwarte, należy podać żądane wartości dla portu lub komputera.

Należy pamiętać o tym, że jeżeli opcja zostanie zaznaczona Nie skanuj ruchu sieciowego, ruch dla aplikacji nie będzie skanowany jedynie pod kątem obecności wirusów i spamu. Opcja ta nie ma wpływu na skanowanie ruchu sieciowego przez moduł zapory sieciowej. Aktywność sieciowa aplikacji będzie analizowana z wykorzystaniem ustawień modułu zapory sieciowej.

6.4. Pomoc techniczna

Informacje na temat pomocy technicznej świadczonej przez firmę Kaspersky Lab zarejestrowanym użytkownikom dostępne są w sekcji Pomoc okna głównego aplikacji.

W górnej części sekcji wyświetlane są ogólne informacje na temat aplikacji: wersja, data opublikowania sygnatur zagrożeń oraz informacje na temat systemu operacyjnego komputera.

Jeżeli podczas działania Kaspersky Internet Security pojawią się problemy, należy spróbować znaleźć ich rozwiązanie w systemie pomocy, bazie wiedzy lub witrynie pomocy technicznej. Baza wiedzy jest oddzielną sekcją witryny pomocy technicznej, która zawiera zalecenia ekspertów dla użytkowników produktów Kaspersky Lab oraz odpowiedzi na najczęściej zadawane pytania. Przy użyciu tych źródeł należy spróbować znaleźć odpowiedź na pytanie lub rozwiązanie problemu. W celu przejścia Bazy wiedzy należy kliknąć odsyłacz [Pomoc przez WWW](#).

Forum użytkowników produktów firmy Kaspersky Lab jest kolejnym źródłem informacji. Jest ono dostępne jako osobna sekcja witryny internetowej działu pomocy technicznej i zawiera pytania, informacje i odpowiedzi. Można tu przeglądać tematy ogólne, zostawić informacje lub znaleźć odpowiedź na pytanie. W celu odwiedzenia forum należy kliknąć [Forum użytkowników](#).

W przypadku nie znalezienia rozwiązania problemu w Pomocy programy, Bazie wiedzy lub Forum użytkowników, należy skontaktować się z działem pomocy technicznej firmy Kaspersky Lab.

Aby móc uzyskać pomoc techniczną, należy być zarejestrowanym użytkownikiem komercyjnej wersji Kaspersky Internet Security. Pomoc techniczna nie jest świadczona użytkownikom wersji testowych.

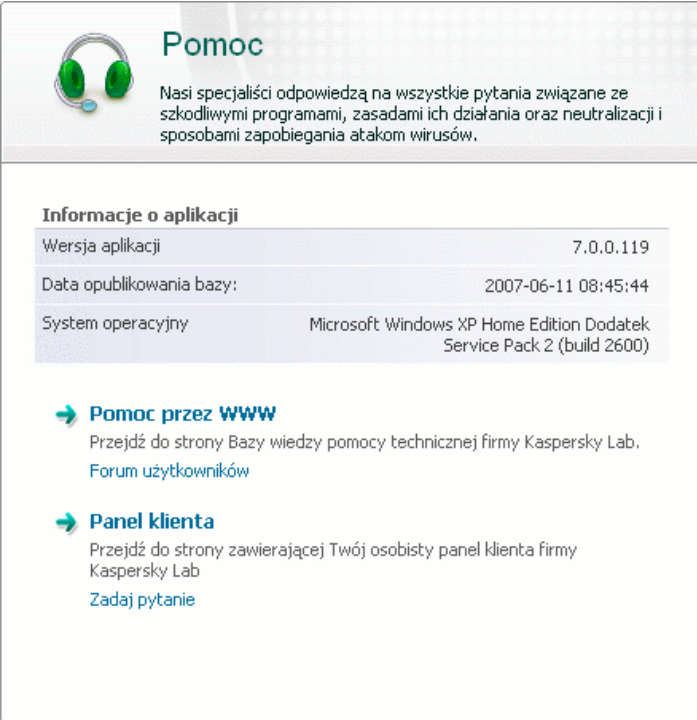
Rejestracja użytkownika dokonywana jest przy użyciu Kreatora aktywacji (rozdział 3.2.2 na stronie 30), jeżeli aplikacja jest aktywowana przy użyciu kodu aktywacyjnego. Identyfikator klienta (ID) jest przyznawany na końcu procesu aktywacji i jest wyświetlany w sekcji **Pomoc** okna głównego programu. Numer klienta jest osobistym numerem identyfikacyjnym, który jest wymagany w celu uzyskania pomocy technicznej za pośrednictwem telefonu lub Internetu.

Jeżeli aktywacja odbywa się przy użyciu pliku klucza, należy się zarejestrować bezpośrednio na stronie internetowej działu pomocy technicznej.

Nowa usługa nazwana [Panel klienta](#) zapewnia użytkownikowi dostęp do jego własnej sekcji strony internetowej firmy Kaspersky Lab. Panel klienta umożliwia:

- wysyłania zapytań do działu pomocy technicznej bez konieczności logowania się;
- wymianę wiadomości z działem pomocy technicznej bez użycia poczty elektronicznej;
- monitorowanie stanu zapytań w czasie rzeczywistym;
- przeglądanie pełnej historii zapytań do działu pomocy technicznej;
- uzyskiwanie kopii zapasowej pliku klucza.

W celu uzyskania pomocy technicznej należy wypełnić formularz internetowy, który zostanie wyświetlony po kliknięciu odsyłacza [Zadaj pytanie](#). Należy przejść do Panelu klienta na stronie internetowej działu pomocy technicznej, która zostanie otwarta, oraz wypełnić formularz.



Pomoc

Nasi specjaliści odpowiedzą na wszystkie pytania związane ze szkodliwymi programami, zasadami ich działania oraz neutralizacji i sposobami zapobiegania atakom wirusów.

Informacje o aplikacji

Wersja aplikacji	7.0.0.119
Data opublikowania bazy:	2007-06-11 08:45:44
System operacyjny	Microsoft Windows XP Home Edition Dodatek Service Pack 2 (build 2600)

→ **Pomoc przez WWW**
Przejdź do strony Bazy wiedzy pomocy technicznej firmy Kaspersky Lab.
[Forum użytkowników](#)

→ **Panel klienta**
Przejdź do strony zawierającej Twój osobisty panel klienta firmy Kaspersky Lab
[Zadaj pytanie](#)

Rysunek 13. Informacje o pomocy technicznej

W nagłych przypadkach można użyć numerów telefonów znajdujących się w systemie pomocy (rozdział B2. na stronie 90). Telefoniczna pomoc techniczna dostępna jest w języku polskim.

6.5. Zamykanie aplikacji

Jeżeli działanie aplikacji Kaspersky Internet Security musi zostać zakończone, należy wybrać polecenie **Zakończ** z menu kontekstowego aplikacji (rozdział 4.2, na stronie 40). Spowoduje to wyładowanie aplikacji z pamięci komputera, co jest równoznaczne z całkowitym wyłączeniem ochrony komputera.

Jeżeli w momencie zamykania aplikacji będą nawiązane połączenia sieciowe, wyświetlony zostanie komunikat potwierdzający ich zerwanie. Jest to wymagane do poprawnego zakończenia działania aplikacji. Zerwanie połączeń nastąpi automatycznie

po 10 sekundach lub kliknięciu przycisku **Tak**. Większość połączeń zostanie ponownie nawiązanych po pewnym okresie czasu.

Należy pamiętać, że jeżeli trwa pobieranie plików i nie jest używany menedżer pobierania, zostanie ono przerwane. W celu uzyskania pliku konieczne będzie ponowne rozpoczęcie pobierania.

Można również nie zrywać nawiązanych połączeń sieciowych poprzez kliknięcie przycisku **Nie** w oknie powiadomienia. Spowoduje to kontynuowanie działania aplikacji.

Jeżeli działanie aplikacji zostanie zakończone, ochrona może zostać wznowiona poprzez ponowne uruchomienie aplikacji Kaspersky Internet Security przez wybranie **Start** → **Programy** → **Kaspersky Internet Security 7.0** → **Kaspersky Internet Security 7.0**.

Ochrona zostanie również automatycznie wznowiona po ponownym załadowaniu systemu operacyjnego. Aby włączyć ten tryb, należy kliknąć sekcję Usługi okna ustawień aplikacji i zaznaczyć opcję **Uruchom podczas ładowania systemu** w grupie **Automatyczne uruchamianie**.

ROZDZIAŁ 7. ZARZĄDZANIE LICENCJAMI

Do poprawnego działania Kaspersky Internet Security wymagany jest *plik klucza licencyjnego*. 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 Internet Security pobierze uaktualnienia tylko raz. Program nie będzie pobierał żadnych nowych uaktualnień.

Jeżeli aktywowano wersję trzydziestodniową, po upływie tego okresu Kaspersky Internet Security przestanie się uruchamiać.

Po wygaśnięciu komercyjnego klucza licencyjnego program będzie kontynuował działanie, ale nie będzie pobierał nowych uaktualnień sygnatur zagrożeń. Komputer będzie chroniony przez zadania działające w czasie rzeczywistym oraz możliwe będzie wykonywanie skanowania komputera, wykorzystywana będzie baza danych sygnatur zagrożeń opublikowana maksymalnie w dniu wygaśnięcia licencji. Firma Kaspersky Lab nie może zagwarantować ochrony komputera przed wirusami, które pojawiają się po zakończeniu okresu licencjonowania.

W celu uniknięcia infekcji komputera nowymi wirusami zalecane jest przedłużenie okresu licencjonowania programu Kaspersky Internet Security. Dwa tygodnie przed zakończeniem okresu licencjonowania program rozpocznie wyświetlanie odpowiedniego powiadomienia po każdym jego uruchomieniu.

Informacje na temat bieżącego klucza licencyjnego wyświetlane są w sekcji **Aktywacja** (Rysunek 14) okna głównego aplikacji. W sekcji Zainstalowane klucze dostępny numer identyfikacyjny klucza, typ (komercyjny, trial, testowy), liczba komputerów, na których można zainstalować ten klucz, data wygaśnięcia i liczba dni pozostałych do jego wygaśnięcia. W celu przejrzania dodatkowych informacji należy kliknąć [Przeglądaj informacje o kluczach](#).

W celu zapoznania się z postanowieniami umowy licencyjnej należy kliknąć odsyłacz [Przeczytaj umowę licencyjną](#). W celu usunięcia klucza z listy należy kliknąć przycisk [Usuń klucz](#).

W celu zakupienia lub odnowienia klucza należy:

1. Zakupić nowy klucz przez kliknięcie [Kup nowy klucz](#) (jeżeli aplikacja nie była aktywowana) lub [Przedłuż ważność klucza](#). Na stronie, która zostanie otwarta, wyświetlona zostanie informacja na temat możliwości zakupu klucza licencyjnego w sklepie internetowym firmy Kaspersky Lab lub u jednego z jej partnerów.

W przypadku zakupienia produktu przez Internet plik klucza lub kod aktywacyjny zostanie przesłany na adres e-mail określony przez użytkownika w formularzu podczas zamawiania produktu.

2. Zainstalować klucz licencyjny, klikając [Zainstaluj klucz](#) w sekcji **Aktywacja** okna głównego Kaspersky Internet Security lub menu kontekstowym aplikacji. Spowoduje to uruchomienie kreatora aktywacji (rozdział 3.2.2 na stronie 30).

Aktywacja

W procesie aktywacji pobierany jest klucz, dzięki któremu możliwe jest korzystanie z wszystkich funkcji programu, uaktualnień oraz pomocy technicznej.

Zainstalowane klucze

07C2-00048D-015C8CAA Komercyjny dla 5 komputerów

Data wygaśnięcia klucza: 2008-05-20

Liczba dni do wygaśnięcia licencji: 344

→ **Przedłuż okres ważności klucza**
Odnowienie klucza w firmie Kaspersky Lab.
[Zainstaluj klucz](#) | [Przeczytaj umowę licencyjną](#)

→ **Przeglądaj informacje o kluczach**
Kliknij, aby wyświetlić szczegółowe informacje o kluczach.
[Usuń klucz](#)

Rysunek 14. Zarządzanie licencjami

Firma Kaspersky Lab przewiduje specjalne rabaty dla użytkowników przedłużających licencję. Szczegółowe informacje na ten temat znajdują się w **sklepie internetowym** firmy Kaspersky Lab.

ROZDZIAŁ 8. MODYFIKACJA, NAPRAWIENIE LUB USUNIĘCIE PROGRAMU

Aplikacja może zostać zdezinstalowana w następujący sposób:

- Przy użyciu kreatora instalacji programu (rozdział 8.1 na stronie 72)
- Przy użyciu wiersza poleceń (rozdział 8.2 na stronie 74)

8.1. Modyfikacja, naprawienie lub usunięcie programu przy użyciu kreatora instalacji

W przypadku wykrycia błędów podczas funkcjonowania programu w skutek nieprawidłowej jego konfiguracji lub uszkodzenia pliku, należy dokonać naprawy programu.

Modyfikowanie programu Kaspersky Internet Security pozwala na zainstalowanie brakujących jego składników lub usunięcie zbędnych.

W celu naprawy lub modyfikacji brakujących składników programu Kaspersky Internet Security lub usunięcia programu należy:

1. Zakończyć działanie programu. W tym celu należy kliknąć prawym przyciskiem myszy ikonę programu znajdującą 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 Kaspersky Internet Security został zainstalowany z innego źródła (sieciowego foldera współdzielonego, foldera lub dysku twardego itd.), należy upewnić się, czy pakiet instalacyjny jest dostępny.
3. Wybrać **Start** → **Programy** → **Kaspersky Internet Security 7.0** → **Modyfikuj, napraw lub usuń**.



Następnie uruchomiony zostanie kreator instalacji programu. Poniżej przedstawione zostały etapy naprawy, modyfikowania lub usuwania programu.

Krok 1. 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.

Podczas usuwania programu można określić, które dane utworzone i używane przez program mają zostać zapisane na komputerze. W celu usunięcia wszystkich danych Kaspersky Internet Security należy wybrać  **Całkowita dezinstalacja**. W celu zapisania danych należy wybrać  **Zapisz obiekty aplikacji** oraz wybrać z listy obiekty, które zostaną zachowane:

- *Dane aktywacyjne* – klucz licencyjny aplikacji.
- *Bazy danych aplikacji* – kompletny zestaw sygnatur zagrożeń niebezpiecznych programów, wirusów i innych zagrożeń zawartych w ostatniej aktualizacji.
- *Antyspamowe bazy danych* – baza danych używana do wykrywania wiadomości pocztowych zawierających spam. Te bazy danych zawierają szczegółowe informacje na temat czystych wiadomości oraz spamu.
- *Kopie zapasowe* – kopie zapasowe usuniętych lub wyleczonych obiektów. Zalecane jest ich zapisanie na wypadek potrzeby ich późniejszego przywrócenia.
- *Kwarantanna* – 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 ich zachowanie, ponieważ plik może nie być zainfekowany lub zostać wyleczony po aktualizacji baz danych.
- *Ustawienia ochrony* – konfiguracja wszystkich składników programu.
- *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 Internet Security skanuje tylko te pliki, które uległy modyfikacji od czasu ostatniego skanowania.

Uwaga!

Jeżeli pomiędzy dezinstalacją jednej wersji programu Kaspersky Internet Security 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.

Krok 2. 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 zaproponuje użytkownikowi ponowne uruchomienie komputera. Należy kliknąć **Tak**, aby natychmiast ponownie uruchomić komputer. Aby uruchomić ponownie komputer w późniejszym terminie, należy kliknąć **Nie**.

8.2. Dezinstalacja programu przy użyciu wiersza poleceń

W celu dezinstalacji Kaspersky Internet Security przy użyciu wiersza poleceń należy wykonać następujące polecenie:

```
msiexec /x <nazwa_pakietu>
```

Uruchomiony zostanie kreator instalacji. Może on zostać wykorzystany do dezinstalacji aplikacji (Rozdział 8. na stronie 72).

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 wykonać następujące polecenie:

```
msiexec /x <nazwa_pakietu> /qn
```


W celu dezinstalacji aplikacji w tle z ponownym uruchomieniem komputera należy wykonać następujące polecenie:

```
msiexec /x <nazwa_pakietu> ALLOWREBOOT=1 /qn
```

DODATEK A. INFORMACJE DODATKOWE

Ten dodatek zawiera dodatkowe materiały dotyczące formatów plików i masek rozszerzeń używanych w ustawieniach programu Kaspersky Internet Security.

A.1. Lista plików skanowanych według rozszerzenia

Po zaznaczeniu opcji  **Skanuj programy i dokumenty (według rozszerzenia)** moduł Ochrona plików będzie skanował pliki posiadające następujące rozszerzenia. Dodatkowo, w przypadku włączenia opcji filtrowania załączników, pliki te zostaną przeskanowane przez moduł Ochrona poczty.

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 konfiguracyjny hosta skryptów 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 – email

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.
--

A.2. Poprawne maski wykluczeń

Poniżej znajduje się kilka przykładów dozwolonych masek, które mogą zostać użyte podczas tworzenia listy wykluczeń dla plików:

- 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
- Maski posiadające bezwzględne ścieżki dostępu do plików:
 - 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 wyłączenia rekursywnego skanowania plików w podfolderach tego foldera należy usunąć zaznaczenie z pola **Włączając podfoldery**.
- Maski posiadające względne ścieżki dostępu do plików:
 - dir*.*** lub **dir*** lub **dir** – wszystkie pliki znajdujące się we wszystkich folderach dir\
 - dir\test** – wszystkie pliki posiadające nazwę test znajdujące się w folderach
 - 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 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 przypisania werdyktu wykluczanego zagrożenia zgodnie z nazewnictwem stosowanym w Encyklopedii Wirusów. Zdefiniowane zagrożenie nie będzie wykrywane w żadnym obiekcie. Użycie tych masek bez wybrania werdyktu praktycznie spowoduje 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.

A.3. Poprawne maski wykluczeń zgodne z klasyfikacją Encyklopedii Wirusów

Podczas dodawania zagrożeń o określonym statusie zgodnym z nazewnictwem stosowanym w Encyklopedii Wirusów można określić:

- pełną nazwę zagrożenia zgodną 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**);
- nazwę zagrożenia według maski. 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 B. KASPERSKY LAB

Założona w roku 1997 firma Kaspersky Lab uważana jest przez wielu ekspertów 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 z 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.

B.1. Inne produkty 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. Umożliwia on wydajne skanowanie antywirusowe komputera w trybie online. Kaspersky On-Line Scanner uruchamiany jest w przeglądarce internetowej przy użyciu technologii Microsoft ActiveX®. Dlatego też, użytkownicy mogą szybko przetestować swoje komputery w przypadku podejrzenia infekcji. Przy pomocy 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. Umożliwia on wydajne skanowanie antywirusowe i leczenie komputera w trybie online. Kaspersky On-Line Scanner uruchamiany jest w przeglądarce internetowej przy użyciu technologii Microsoft ActiveX®. Dlatego też, użytkownicy mogą szybko przetestować swoje komputery w przypadku podejrzenia infekcji. Przy pomocy 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 7.0

Kaspersky Anti-Virus 6.0 stworzony został w celu ochrony komputerów osobistych przed szkodliwym oprogramowaniem jako optymalne połączenie 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 twardej. 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 7.0 powiadamia użytkowników o wykryciu niebezpiecznych, podejrzanych lub ukrytych procesów oraz w przypadku wystąpienia nieautoryzowanych zmian standardowych procesów.
- **Monitorowanie zmian w rejestrze systemowym** przy użyciu specjalnego systemu kontroli rejestru.
- **Monitorowanie ukrytych procesów** pozwala na zapewnienie ochrony przed szkodliwym kodem ukrytym w systemie operacyjnym przy użyciu technologii rootkit.
- **Analizator heurystyczny.** Podczas skanowania programu, analizator emuluje jego wykonywanie i rejestruje każdą podejrzaną aktywność, taką jak otwieranie i zapisywanie pliku, przechwytywanie wektorów przerwań itp. Na bazie tej procedury podejmowana jest decyzja o zgłoszeniu prawdopodobnej infekcji. Emulacja przeprowadzana jest w odizolowanym, wirtualnym środowisku, dzięki czemu nie stanowi żadnego zagrożenia dla bezpieczeństwa komputera.
- **Przywracanie systemu po ataku szkodliwego programu.** Operacja ta jest możliwa dzięki rejestrowaniu przez program wszystkich zmian zachodzących w rejestrze systemowym oraz systemie plików.

Kaspersky Anti-Virus Mobile

Kaspersky Anti-Virus Mobile zapewnia ochronę antywirusową urządzeń przenośnych działających pod kontrolą systemów Symbian OS oraz Microsoft Windows Mobile. Program oferuje szczegółowe skanowanie antywirusowe obejmujące:

- **Skanowanie na żądanie** wbudowanej pamięci urządzenia, kart pamięci, wybranych folderów lub poszczególnych plików. Zainfekowane pliki są przenieszone do kwarantanny lub usuwane.
- **Skanowanie w czasie rzeczywistym** – wszystkie przychodzące i wychodzące pliki są automatycznie skanowane. Program kontroluje również próby uzyskiwania dostępu do obiektów.
- **Ochrona przed spamem w wiadomościach tekstowych.**

Kaspersky Anti-Virus for File Servers

Pakiet zapewnia ochronę serwerów plików działających pod kontrolą systemów operacyjnych Microsoft Windows, Novell NetWare, Linux oraz Samba przed wszelkimi rodzajami szkodliwego oprogramowania. Pakiet obejmuje następujące aplikacje Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Produkt oferuje następujące funkcje:

- Ochrona systemu plików serwera w czasie rzeczywistym: Wszystkie pliki przechowywane na serwerze są skanowane podczas otwierania i zapisywania;
- Zapobieganie epidemiom wirusów;
- Skanowanie na żądanie całego systemu plików serwera lub poszczególnych plików i folderów;
- Wykorzystywanie metod optymalizujących skanowanie obiektów w systemie plików serwera;
- Przywracanie systemu po ataku wirusa;
- Skalowalność pakietu uwzględniająca dostępne zasoby systemowe;
- Monitorowanie obciążenia systemu;
- Tworzenie listy zaufanych procesów, których aktywność nie jest kontrolowana przez program;
- Zdalne zarządzanie pakietem obejmujące możliwość scentralizowanej instalacji, konfiguracji i administracji;
- Zapisywanie kopii zapasowych leczonych i usuwanych obiektów w celu zapewnienia możliwości ich późniejszego przywrócenia;

- Przenoszenie do kwarantanny podejrzanych obiektów;
- Wysyłanie powiadomień o zdarzeniach występujących podczas pracy programu; powiadomienia są wysyłane do administratora;
- Zapisywanie szczegółowych raportów;
- Automatyczna aktualizacja baz danych programu.

Kaspersky Open Space Security

Kaspersky Open Space Security jest pakietem produktów zaprojektowanym w celu zapewnienia ochrony sieci o dowolnych rozmiarach i infrastrukturze – od podstawowych aż po rozległe i złożone. Pakiet oferuje scentralizowaną ochronę i obsługę zdalnych biur oraz użytkowników urządzeń mobilnych.

Pakiet obejmuje cztery produkty:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Szczegóły dotyczące poszczególnych produktów znajdują się poniżej.

Kaspersky Work Space Security zapewnia scentralizowaną ochronę stacji roboczych, zarówno tych znajdujących się w obrębie sieci korporacyjnej, jak i użytkowanych poza firmą, przed wszystkimi rodzajami zagrożeń internetowych, łącznie z wirusami, oprogramowaniem spyware, atakami hakerów oraz spamem.

Produkt oferuje następujące funkcje:

- Zintegrowana ochrona przed wirusami, oprogramowaniem spyware, atakami hakerów oraz spamem;
- Ochrona proaktywna przed najnowszymi oraz nieznanymi szkodliwymi programami;
- Zapora sieciowa z wbudowanym systemem wykrywania włamań (IDS) oraz systemem zapobiegania włamaniom (IPS);
- Likwidowanie wszystkich zmian dokonywanych w systemie przez szkodliwe programy;
- Ochrona przed phishingiem oraz spamem;
- Inteligentne zarządzanie zasobami systemowymi podczas skanowania w poszukiwaniu szkodliwych programów;
- Zdalne zarządzanie pakietem obejmujące możliwość scentralizowanej instalacji, konfiguracji i administracji;
- Obsługa Cisco® NAC (Network Admission Control);
- Skanowanie poczty elektronicznej oraz ruchu internetowego w czasie rzeczywistym;

- Blokowanie okien wyskakujących oraz banerów;
- Bezpieczne korzystanie z wszystkich typów sieci, łącznie z WiFi;
- Narzędzia pozwalające na utworzenie dysku ratunkowego umożliwiającego przywrócenie systemu po ataku wirusa;
- Zaawansowany system raportowania;
- Automatyczna aktualizacja baz danych programu;
- Pełna obsługa platform 64-bitowych;
- Optymalizacja dla laptopów (integracja z technologią Intel® Centrino® Duo);
- Zdalne leczenie komputerów przy użyciu technologii Intel® Active Management, Intel® vPro™.

Kaspersky Business Space Security chroni stacje robocze i serwery plików przed wszelkimi rodzajami wirusów, trojanów i robaków, zapobiega epidemiom i dba o bezpieczeństwo firmowych danych bez żadnego ograniczania dostępu do nich. Produkt powstał z uwzględnieniem wymagań serwerów działających pod dużym obciążeniem.

Produkt oferuje następujące funkcje:

- Zdalne zarządzanie pakietem obejmujące możliwość scentralizowanej instalacji, konfiguracji i administracji;
- Obsługa Cisco® NAC (Network Admission Control);
- Ochrona stacji roboczych i serwerów plików przed wszelkimi zagrożeniami internetowymi;
- Technologia iSwift zapobiegająca powtórnemu skanowaniu tych samych plików w sieci;
- Rozkład obciążenia między procesorami serwera;
- Przenoszenie do kwarantanny podejrzanych obiektów wykrywanych na stacjach roboczych;
- Likwidowanie wszystkich zmian dokonywanych w systemie przez szkodliwe programy;
- Skalowalność pakietu uwzględniająca dostępne zasoby systemowe;
- Ochrona proaktywna przed nowymi szkodliwymi programami, których sygnatury nie zostały jeszcze dodane do baz danych;
- Skanowanie ruchu pocztowego i internetowego w czasie rzeczywistym;
- Zapora sieciowa z systemem wykrywania włamań i mechanizmem informującym o atakach sieciowych;
- Ochrona podczas pracy z sieciami Wi-Fi;
- Autoochrona programu przed szkodliwymi programami;
- Automatyczna aktualizacja baz danych.

Kaspersky Enterprise Space Security zawiera komponenty służące do ochrony stacji roboczych oraz serwerów przed wszelkimi zagrożeniami internetowymi. Produkt usuwa wirusy z wiadomości e-mail i chroni wszystkie firmowe dane.

Produkt oferuje następujące funkcje:

- Ochrona stacji roboczych, serwerów plików oraz serwerów poczty przed wirusami, trojanami i robakami;
- Ochrona systemów pocztowych Sendmail, Qmail, Postfix oraz Exim;
- Skanowanie wszystkich wiadomości e-mail przechowywanych na serwerze Microsoft Exchange Server (łącznie z folderami współdzielonymi);
- Przetwarzanie wiadomości e-mail, baz danych i innych obiektów serwerów Lotus Domino;
- Ochrona przed phishingiem i spamem;
- Zapobieganie masowym wysyłkom wiadomości e-mail oraz epidemiom wirusów;
- Skalowalność pakietu uwzględniająca dostępne zasoby systemowe;
- Zdalne zarządzanie pakietem obejmujące możliwość scentralizowanej instalacji, konfiguracji i administracji;
- Obsługa Cisco® NAC (Network Admission Control);
- Ochrona proaktywna stacji roboczych przed nowymi szkodliwymi programami, których sygnatury nie zostały jeszcze dodane do baz danych;
- Zapora sieciowa z systemem wykrywania włamań i mechanizmem informującym o atakach sieciowych;
- Ochrona podczas pracy z sieciami Wi-Fi;
- Skanowanie ruchu internetowego w czasie rzeczywistym;
- Likwidowanie wszystkich zmian dokonywanych w systemie przez szkodliwe programy;
- Dynamiczne wykorzystywanie zasobów podczas skanowania antywirusowego;
- Przenoszenie podejrzanych obiektów do kwarantanny;
- Rozbudowany system rejestrowania raportów dotyczących funkcjonowania ochrony;
- Automatyczna aktualizacja baz danych.

Kaspersky Total Space Security chroni wszystkie przychodzące i wychodzące dane, łącznie z pocztą elektroniczną, ruchem internetowym i komunikacją siecią. Produkt zawiera komponenty zapewniające ochronę stacji roboczych i urządzeń przenośnych. Użytkownicy mogą korzystać z bezpiecznego i szybkiego dostępu do firmowych danych, zasobów Internetu oraz poczty elektronicznej.

Produkt oferuje następujące funkcje:

- Zintegrowana ochrona przed wirusami, oprogramowaniem spyware,

atakami hakerów oraz spamem na wszystkich poziomach sieci korporacyjnej – od stacji roboczych po bramy internetowe;

- Proaktywna ochrona przed najnowszymi i nieznanymi zagrożeniami;
- Ochrona serwerów poczty oraz serwerów plików;
- Skanowanie ruchu internetowego (HTTP/FTP) w czasie rzeczywistym;
- Skalowalność pakietu uwzględniająca dostępne zasoby systemowe;
- Blokowanie dostępu z zainfekowanych stacji roboczych;
- Zapobieganie epidemiom wirusów;
- Scentralizowany system raportowania;
- Zdalne zarządzanie pakietem obejmujące możliwość scentralizowanej instalacji, konfiguracji i administracji;
- Obsługa Cisco® NAC (Network Admission Control);
- Obsługa sprzętowych serwerów proxy;
- Filtracja ruchu internetowego z uwzględnieniem list zaufanych serwerów, typów obiektów oraz grup użytkowników;
- Technologia iSwift eliminująca konieczność powtórnego skanowania obiektów, które nie uległy żadnym zmianom;
- Inteligentne zarządzanie zasobami systemowymi podczas skanowania;
- Zapora sieciowa z systemem wykrywania włamań i mechanizmem informującym o atakach sieciowych;
- Bezpieczne korzystanie z wszystkich typów sieci, łącznie z WiFi;
- Ochrona przed phishingiem oraz spamem;
- Zdalne leczenie komputerów przy użyciu technologii Intel® Active Management, Intel® vPro™;
- Likwidowanie zmian dokonywanych w systemie przez szkodliwe programy;
- Autoochrona przed szkodliwymi programami;
- Pełna obsługa 64-bitowych systemów operacyjnych;
- Automatyczna aktualizacja baz danych.

Kaspersky Security for Mail Servers

Kaspersky Security for Mail Server zapewnia ochronę serwerów poczty oraz pracy grupowej przed szkodliwymi programami i spamem. Produkt zawiera aplikacje chroniące wszystkie popularne serwery poczty, łącznie z Microsoft Exchange, Lotus Notes / Domino, Sendmail, Qmail, Postfix oraz Exim. Rozwiązanie może być również stosowane na komputerach wydzielonych do pełnienia funkcji bramy pocztowej. Pakiet obejmuje następujące produkty:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.

- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Funkcje pakietu:

- Efektywna ochrona przed szkodliwymi i potencjalnie niebezpiecznymi programami;
- Filtrowanie spamu;
- Skanowanie przychodzących i wychodzących wiadomości e-mail oraz ich załączników;
- Skanowanie antywirusowe wszystkich wiadomości przechowywanych na serwerze Microsoft Exchange, łącznie z obiektami znajdującymi się w folderach publicznych;
- Skanowanie wiadomości, baz danych oraz innych obiektów przechowywanych na serwerach Lotus Notes / Domino;
- Filtrowanie wiadomości na podstawie typu załącznika;
- Przenoszenie podejrzanych obiektów do kwarantanny;
- Przenoszenie podejrzanych obiektów do kwarantanny;
- Zapobieganie epidemiom wirusów;
- Monitorowanie stanu systemu ochrony wraz z funkcją wyświetlania powiadomień;
- System generowania raportów dotyczących stanu ochrony;
- Skalowalność pakietu uwzględniająca dostępne zasoby systemowe;
- Automatyczna aktualizacja baz danych.

Kaspersky Security for Internet Gateways

Kaspersky Security for Internet Gateways zapewnia bezpieczny dostęp do Internetu wszystkim pracownikom firmy. Rozwiązanie automatycznie usuwa szkodliwe i potencjalnie niebezpieczne programy z przychodzącego ruchu HTTP/FTP. Pakiet obejmuje następujące produkty:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Funkcje pakietu:

- Efektywna ochrona przed szkodliwymi i potencjalnie niebezpiecznymi programami;
- Skanowanie w czasie rzeczywistym ruchu internetowego (przesyłanego za pośrednictwem protokołów HTTP/FTP);
- Filtrowanie ruchu internetowego z wykorzystaniem listy zaufanych serwerów oraz z uwzględnieniem typów obiektów i grup użytkowników;
- Przenoszenie podejrzanych obiektów do kwarantanny;
- Łatwy w użytkowaniu system zarządzania;

- System generowania raportów dotyczących stanu ochrony;
- Obsługa sprzętowych serwerów proxy;
- Skalowalność pakietu uwzględniająca dostępne zasoby systemowe;
- Automatyczna aktualizacja baz danych.

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 listy RBL 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 dostarczonymi przez specjalistów z laboratorium lingwistycznego. Antyspamowe bazy danych są uaktualniane co 20 minut.

Kaspersky Anti-Virus for MIMESweeper

Kaspersky Anti-Virus for MIMESweeper zapewnia wydajne skanowanie ruchu na serwerach wykorzystujących oprogramowanie Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Kaspersky Anti-Virus for MIMESweeper oferuje dodatkową warstwę ochrony serwera poczty działającego w sieci korporacyjnej. Aplikacja współpracuje z rozwiązaniem Clearswift MIMESweeper i skanuje w czasie rzeczywistym wszystkie odbierane oraz wysyłane wiadomości e-mail. Jeżeli jest to możliwe, zainfekowane wiadomości e-mail są natychmiast leczone.

B.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 Baza wiedzy: support.kaspersky.com/pl
Informacje ogólne	WWW: http://www.kaspersky.pl http://www.viruslist.pl Email: info@kaspersky.pl

Podręcznik zawiera jedynie najważniejsze informacje dotyczące pracy z systemem Kaspersky Anti-Virus. Menu i inne informacje mogą się różnić od opisanych w tym podręczniku. Spowodowane jest to ciągłym rozwojem programu. Więcej informacji można znaleźć w systemie pomocy oraz w elektronicznej wersji podręcznika.

