

**PODRĘCZNIK
UŻYTKOWNIKA**

**KASPERSKY
INTERNET
SECURITY 2010**

Drogi Użytkowniku,

dziękujemy za wybór naszego produktu. Mamy nadzieję, że ten podręcznik będzie pomocny podczas pracy i odpowie na większość pytań.

Uwaga! Prawa autorskie do tego dokumentu są własnością firmy Kaspersky Lab i są chronione przez obowiązujące prawo. Nieupoważnione kopiowanie i rozpowszechnianie dokumentu lub jego poszczególnych części wiąże się z odpowiedzialnością prawną, administracyjną lub karną obowiązującą na terytorium Polski.

Kopiowanie, rozpowszechnianie - również w formie przekładu dowolnych materiałów - możliwe jest tylko po uzyskaniu pisemnej zgody firmy Kaspersky Lab.

Podręcznik wraz z zawartością graficzną może być wykorzystany tylko do celów informacyjnych, niekomercyjnych i indywidualnych użytkownika.

Dokument może zostać zmieniony bez uprzedniego poinformowania. Najnowsza wersja podręcznika jest zawsze dostępna na stronie www.kaspersky.pl.

Firma Kaspersky Lab nie ponosi odpowiedzialności za treść, jakość, aktualność i wiarygodność wykorzystywanych w dokumencie materiałów, prawa do których zastrzeżone są przez inne podmioty oraz za możliwe szkody związane z wykorzystaniem tych materiałów.

Dokument zawiera nazwy stanowiące zastrzeżone znaki towarowe, prawa do których posiadają ich właściciele.

Data opublikowania: 10/13/09

© 1997-2009 Kaspersky Lab ZAO. Wszelkie prawa zastrzeżone.

<http://www.kaspersky.pl>
<http://pomoc.kaspersky.pl>

SPIS TREŚCI

WSTĘP	6
Zawartość	6
Pomoc dla ZAREJESTROWANYCH użytkowników	7
Wymagania sprzętowe i programowe	7
KASPERSKY INTERNET SECURITY 2010	9
Uzyskiwanie informacji na temat aplikacji	9
Wyszukiwanie informacji przez użytkownika	9
Kontakt z działem sprzedaży	11
Kontakt z działem pomocy technicznej	11
Forum Internetowe firmy Kaspersky Lab	13
NOWOŚCI W KASPERSKY INTERNET SECURITY 2010	14
KONCEPCJA OCHRONY KOMPUTERA UŻYTKOWNIKA	16
Zadania skanowania antywirusowego	17
Aktualizacja	17
Ochrona danych i aktywności online	18
Filtrowanie programów i dostępu do danych	18
Kreatory i narzędzia	19
Usługi	20
INSTALACJA APLIKACJI	22
Krok 1. Wyszukiwanie nowszej wersji aplikacji	23
Krok 2. Weryfikacja wymagań systemowych	23
Krok 3. Wybór typu instalacji	23
Krok 4. Zapoznanie się z umową licencyjną	24
Krok 5. Zasady korzystania z Kaspersky Security Network	24
Krok 6. Wybór folderu instalacyjnego	25
Krok 7. Wybór instalowanych składników	26
Krok 8. Wyłączenie Zapory Sieciowej Microsoft Windows	26
Krok 9. Wykorzystanie parametrów aplikacji zachowanych z poprzedniej instalacji	27
Krok 10. Wyszukiwanie innych programów antywirusowych	28
Krok 11. Kończenie instalacji programu	28

Krok 12. Finalizowanie instalacji	29
ROZPOCZĘCIE PRACY	30
Kreator konfiguracji aplikacji	31
Krok 1. Aktywacja programu	31
Aktywacja wersji komercyjnej	32
Aktywacja wersji testowej	33
Zakończenie aktywacji	33
Krok 2. Wybór trybu ochrony	33
Krok 3. Konfiguracja aktualizacji programu	34
Krok 4. Ograniczenie dostępu do aplikacji	35
Krok 5. Wybór wykrywanych zagrożeń	36
Krok 6. Wyłączanie DNS	36
Krok 7. Analiza systemu	36
Krok 8. Zakończenie pracy kreatora	37
Wybór typu sieci	37
Aktualizacja aplikacji	38
Skanowanie komputera w poszukiwaniu wirusów	38
Skanowanie komputera w poszukiwaniu luk	39
Zarządzanie licencją	40
Subskrypcja automatycznego przedłużenia licencji	41
Uczestnictwo w Kaspersky Security Network	43
Zarządzanie ochroną	44
Stan ochrony	46
Wstrzymywanie ochrony	47
KOMPONENTY OCHRONY	49
Ochrona systemu plików	49
Ochrona poczty	51
Ochrona ruchu sieciowego	53
Ochrona ruchu komunikatorów internetowych	56
Kontrola aplikacji	57
Bezpieczne środowisko dla uruchamiania programów	60
Zapora sieciowa	61
Ochrona proaktywna	61
Ochrona przed atakami sieciowymi	62

Anti-Spam	63
Blokowanie banerów	66
Kontrola rodzicielska	67
SKANOWANIE KOMPUTERA.....	70
AKTUALIZACJA	72
FUNKCJE DODATKOWE.....	74
RAPORTY	75
POWIADOMIENIA	76
ROZWIĄZYWANIE PROBLEMÓW	79
KASPERSKY SECURITY NETWORK	80
KASPERSKY LAB	87
UMOWA LICENCYJNA	89

WSTĘP

ZAWARTOŚĆ

Kaspersky Internet Security można nabyć poprzez naszych partnerów (wersja pudełkowa) lub w jednym ze sklepów internetowych (np. <http://www.kaspersky.pl/store.html>).

Wersja pudełkowa produktu zawiera:

- Zaklejoną kopertę z nośnikiem instalacyjnym zawierającym pliki programu oraz dokumentację w formacie PDF.
- Dokumentację w formie drukowanej.
- Certyfikat Autentyczności zawierający kod aktywacyjny.

Umowa Licencyjna to posiadające moc prawną porozumienie zawarte między Tobą a Kaspersky Lab, w której wymienione są warunki, zgodnie z którymi możesz korzystać z zakupionego oprogramowania.

Dokładne zapoznanie się z Umową Licencyjną jest obowiązkiem każdego użytkownika. Należy tego dokonać przed otwarciem zabezpieczonej koperty zawierającej nośnik instalacyjny oraz Certyfikat Autentyczności.

Jeżeli nie zgadzasz się z postanowieniami Umowy Licencyjnej, możesz dokonać zwrotu zakupionego oprogramowania w zamian za zwrot poniesionych. Aby dokonanie zwrotu było możliwe, koperta z nośnikiem instalacyjnym i Certyfikatem Autentyczności musi pozostać nienaruszona.

Otwarcie koperty zawierającej nośnik instalacyjny i Certyfikat Autentyczności jest jednoznaczne z akceptacją Umowy Licencyjnej.

Podczas zakupu Kaspersky Internet Security w sklepie internetowym użytkownik pobiera oprogramowanie ze strony internetowej Kaspersky Lab wraz z niniejszym podręcznikiem. Kod aktywacyjny jest wysyłany pocztą elektroniczną po uiszczeniu opłaty.

POMOC DLA ZAREJESTROWANYCH UŻYTKOWNIKÓW

Firma Kaspersky Lab zapewnia legalnym użytkownikom szeroki zakres usług pozwalających zwiększyć efektywność wykorzystywanego oprogramowania.

Nabywając licencję stajesz się zarejestrowanym użytkownikiem i w ciągu czasu trwania licencji możesz korzystać z następujących usług:

- Cogodzinna aktualizacja baz programu i uaktualnianie produktu do nowych wersji;
- Konsultacja telefoniczna i za pośrednictwem poczty elektronicznej w przypadku wyniknięcia problemów związanych z instalacją, ustawieniami i użytkowaniem oprogramowania;
- Powiadomianie o nowym oprogramowaniu lub nowych wersjach produktów Kaspersky Lab.

Kaspersky Lab nie oferuje konsultacji odnośnie problemów z działaniem i użytkowaniem systemów operacyjnych, innego oprogramowania a także działania różnych technologii.

WYMAGANIA SPRZĘTOWE I PROGRAMOWE

Aby aplikacja działała poprawnie, komputer powinien spełniać następujące wymagania:

▶ *Wymagania ogólne:*

- 375 MB wolnego miejsca na dysku twardym.
- Napęd CD-ROM (w celu instalacji aplikacji z płyty CD).

- Microsoft Internet Explorer 6.0 lub nowszy (do aktualizacji bazy danych sygnatur oraz modułów programu).
- Microsoft Windows Installer 2.0.
- ▶ *Wymagania dla systemów: Microsoft Windows XP Home Edition (Service Pack 2), Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition:*
 - Procesor Intel Pentium 300 MHz lub szybszy (lub kompatybilny).
 - 256 MB dostępnej pamięci RAM.
- ▶ *Wymagania dla systemów: Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:*
 - Procesor Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) lub szybszy (lub kompatybilny).
 - 512 MB dostępnej pamięci RAM.
- ▶ *Wymagania dla systemów: Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:*
 - Procesor Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) lub szybszy (lub kompatybilny).
 - 1 GB dostępnej pamięci RAM (32-bit); 2 GB dostępnej pamięci RAM (64-bit).

KASPERSKY INTERNET SECURITY 2010

Kaspersky Internet Security 2010 to innowacyjne podejście do bezpieczeństwa danych.

Główną cechą wyróżniającą Kaspersky Internet Security 2010 wśród dostępnych produktów, w tym także innego oprogramowania Kaspersky Lab, jest kompleksowe podejście do ochrony danych na komputerze użytkownika.

UZYSKIWANIE INFORMACJI NA TEMAT APLIKACJI

Kaspersky Lab oferuje wiele źródeł informacji dotyczących zakupu, instalacji oraz użytkowania aplikacji.

Użytkownik może wybrać dogodnie dla siebie źródło informacji w zależności od tego, jak pilny jest dany problem.

WYSZUKIWANIE INFORMACJI PRZEZ UŻYTKOWNIKA

Możliwe jest skorzystanie z następujących źródeł informacji:

- Strona internetowa Kaspersky Lab;
- Zakładka pomocy interaktywnej;
- Zakładka pomocy technicznej na stronie internetowej Kaspersky Lab (Baza wiedzy);
- System informacji elektronicznej;
- Dokumentacja.

Zakładka na stronie internetowej Kaspersky Lab

<http://www.kaspersky.pl/products.html?s=home&show=prods>

Na tej zakładce znajdują się podstawowe informacje o oprogramowaniu, jego możliwościach i właściwościach.

Zakładka pomocy technicznej (Baza wiedzy) na stronie internetowej

<http://support.kaspersky.pl/kis2010>

Na zakładce tej znajdują się artykuły publikowane przez specjalistów pomocy technicznej.

Artykuły zawierają przydatne, aktualne informacje, porady i odpowiedzi na najczęściej zadawane pytania. Są one pogrupowane wg następujących tematów: „Praca z plikami kluczami”, „Ustawienia aktualizacji baz”, „Likwidacja awarii podczas pracy”. Artykuły są pomocne przy rozwiązywaniu problemów dotyczących nie tylko danego oprogramowania, ale także innych produktów Kaspersky Lab.

Pomoc interaktywna

W zakładce pomocy znajduje się sukcesywnie aktualizowana baza najczęściej zadawanych pytań i udzielanych odpowiedzi. Korzystanie z serwisu wymaga połączenia z Internetem.

Aby przejść na stronę serwisu, w oknie głównym programu kliknij odnośnik **Pomoc**, a następnie w otworzonym oknie kliknij przycisk **Pomoc interaktywna**.

System informacji elektronicznej

W skład oprogramowania wchodzi plik zawierający informacje, w jaki sposób zarządzać ochroną komputera: monitorować stan ochrony, sprawdzać poszczególne obszary komputera w poszukiwaniu wirusów itp. Znajdują się tam także informacje odnoszące się do każdego okna programu: spis i charakterystyka prezentowanych w nim parametrów oraz lista rozwiązywanych problemów.

W celu przejścia do pliku informacji kliknij przycisk **Informacja** w danym oknie lub naciśnij klawisz <F1>.

Dokumentacja

Oprogramowanie Kaspersky Internet Security zawiera **Podręcznik Użytkownika** (w formacie .pdf). Dokument ten zawiera charakterystykę funkcji i możliwości programu oraz podstawowe schematy pracy.

KONTAKT Z DZIAŁEM SPRZEDAŻY

W przypadku pojawienia się pytań dotyczących wyboru lub zakupu aplikacji, czy też przedłużenia okresu licencyjnego należy skontaktować się z działem sprzedaży pod numerem telefonu **0 801 000 215** lub **(34) 368 18 14**.

Usługa jest świadczona w języku polskim.

Pytania do działu sprzedaży można także wysłać za pośrednictwem poczty elektronicznej: spredaz@kaspersky.pl.

KONTAKT Z DZIAŁEM POMOCY TECHNICZNEJ

Każdy użytkownik produktów Kaspersky Lab może korzystać z bezpłatnej pomocy technicznej dostępnej za pośrednictwem telefonu lub poprzez Internet.

Inżynierowie pomocy technicznej udzielą odpowiedzi na pytania związane z instalacją i użytkowaniem aplikacji w przypadku zainfekowania komputera oraz pomogą wyeliminować konsekwencje aktywności szkodliwego oprogramowania.

Pomoc techniczna za pośrednictwem telefonu

W przypadku wystąpienia problemu informacje można uzyskać pod numerem telefonu **0 801 000 215** lub **(34) 368 18 14**.

Pomoc techniczna dla użytkowników aplikacji firmy Kaspersky Lab jest świadczona od poniedziałku do piątku (w godzinach 8:00 – 19:00) oraz w soboty (w godzinach 9:00 – 13:00).

Aby uzyskać pomoc techniczną, musisz podać numer kodu aktywacyjnego lub numer klucza licencyjnego.

Kontakt z działem pomocy technicznej przy użyciu wiadomości e-mail (tylko dla zarejestrowanych użytkowników)

Pytania do działu pomocy technicznej mogą być także kierowane za pośrednictwem formularza znajdującego się na stronie internetowej <http://support.kaspersky.ru/helpdesk.html?LANG=pl>.

Pytania mogą być wysyłane w języku polskim, rosyjskim, angielskim, niemieckim, francuskim i hiszpańskim.

W celu wysłania wiadomości z pytaniem musisz podać **numer klienta** oraz **hasło** uzyskane podczas rejestracji na stronie działu pomocy technicznej.

Ważne!

W celu rejestracji wypełnij i wyślij formularz znajdujący się na stronie <https://support.kaspersky.com/pl/PersonalCabinet/Registration/Form/>. Podczas rejestracji podaj kod aktywacyjny aplikacji lub numer pliku klucza.

Odpowiedź specjalistów z działu pomocy technicznej zostanie przesłana na adres e-mail, z którego wysłałeś wiadomość oraz na adres podany w **Panelu klienta** – <https://support.kaspersky.com/pl/PersonalCabinet>.

Formularz pozwala na szczegółowe opisanie problemu. W poszczególnych polach formularza podaj następujące informacje:

- **Typ zapytania.** Pytania zadawane przez użytkowników najczęściej są specjalnie pogrupowane, np. „Problemy z instalacją/usuwaniem programu” lub „Problemy związane ze skanowaniem/usuwaniem wirusów”. Jeżeli nie możesz zdecydować się na konkretny temat, wybierz sekcję „Pytania ogólne”.
- **Nazwa aplikacji.** Tutaj podaj nazwę używanej aplikacji Kaspersky Lab.
- **Treść zapytania.** W tym polu bardzo szczegółowo opisz zaistniały problem.
- **Numer klienta i hasło.** W tym polu podaj numer klienta oraz hasło otrzymane podczas rejestracji w dziale pomocy technicznej.
- **Adres e-mail.** Odpowiedź na zadane pytanie zostanie wysłana na podany adres.

FORUM INTERNETOWE FIRMY KASPERSKY LAB

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, można przedyskutować je ze specjalistami z firmy Kaspersky Lab lub innymi użytkownikami oprogramowania na forum internetowym znajdującym się pod adresem: <http://forum.kaspersky.com> (forum dostępne jest wyłącznie w języku angielskim i rosyjskim).

Na forum można także znaleźć wcześniej opublikowane informacje, dodać swój komentarz, utworzyć nowe zapytanie lub skorzystać z wyszukiwarki.

NOWOŚCI W KASPERSKY INTERNET SECURITY 2010

Kaspersky Internet Security 2010 jest uniwersalnym rozwiązaniem służącym do ochrony danych. Aplikacja umożliwia nie tylko ochronę antywirusową, ale także ochronę przed spamem i atakami sieciowymi. Poszczególne składniki aplikacji pozwalają chronić komputer przed nieprzewidywanymi zagrożeniami, kradzieżą internetową a także kontrolować uzyskiwanie dostępu do Internetu przez różnych użytkowników komputera.

Aplikacja zapewnia kompletną ochronę wszystkich kanałów przepływu i przekazu danych. Przejrzysta konfiguracja umożliwia optymalne dostosowanie aplikacji do indywidualnych potrzeb każdego użytkownika.

Nowe funkcje w programie Kaspersky Internet Security 2010.

Nowe funkcje ochrony:

- Kaspersky Internet Security zawiera moduł **Filtrowanie aplikacji**, który razem z **Ochroną proaktywną** i **Monitorem sieci** stanowi nowe, uniwersalne podejście do ochrony systemu przed wszelkimi znanymi i całkowicie nowymi zagrożeniami. Komponent rejestruje działania programów w systemie i optymalizuje ich funkcjonowanie wykorzystując listy zaufanych aplikacji (z uwzględnieniem stopnia ich wiarygodności). Ponadto moduł kontroluje dostęp do poufnych danych użytkownika, parametrów i obiektów systemu operacyjnego a także uniemożliwia wykonanie przez programy niebezpiecznych działań w systemie.
- Nowy komponent Ochrona komunikatorów zapewnia ochronę podczas pracy z większością programów umożliwiających szybką wymianę informacji w Internecie. Moduł skanuje informacje w poszukiwaniu szkodliwego oprogramowania.
- Mechanizm uruchamiania aplikacji w chronionym środowisku wirtualnym – Bezpieczne uruchamianie (sandbox). Uruchamianie przeglądarek internetowych w takim środowisku umożliwia bezpieczne przeglądanie zasobów internetowych, chroni przed wniknięciem do komputera szkodliwych programów, zapewnia ochronę danych przed niekontrolowaną modyfikacją lub usunięciem, a także pozwala na

usuwanie wszelkich śladów Twojej aktywności w Internecie (pliki tymczasowe, pliki cookie, lista odwiedzanych stron internetowych itp.).

- Kaspersky Internet Security zawiera moduł filtrowania odnośników, działający w ramach Ochrony WWW. System filtruje wszystkie odnośniki znajdujące się na stronie internetowej w poszukiwaniu podejrzanej i phishingowej zawartości. Moduł ma postać wtyczki dla przeglądarek Microsoft Internet Explorer i Mozilla Firefox.
- Kontrola dostępu do stron internetowych o charakterze phishingowym jest realizowana poprzez filtrowanie odsyłaczy znajdujących się w wiadomościach e-mail i na stronach internetowych, a także podczas próby połączenia ze stroną internetową. Podczas filtrowania wykorzystywana jest baza adresów internetowych zawierających treści phishingowe. Filtrowanie jest przeprowadzane w ramach modułów Ochrona WWW, Ochrona komunikatorów oraz Anti-Spam.
- Do listy zadań filtrowania dodane zostało nowe narzędzie – filtrowanie luk, które ułatwia wyszukiwanie oraz usuwanie zagrożeń bezpieczeństwa i błędów w programach zainstalowanych na komputerze a także w systemie operacyjnym.

Nowe funkcje interfejsu programu:

- Centrum ochrony stanowi nowoczesne do podejście zarządzania bezpieczeństwem. Ochrona komputera jest realizowana w trzech kierunkach: pliki i poufne dane użytkownika, obiekty systemu operacyjnego i programy zainstalowane na komputerze a także praca w Sieci. Za każdy aspekt ochrony odpowiada konkretny zbiór komponentów Kaspersky Internet Security. Korzystając z centrum ochrony możesz ocenić, który komponent chroni określony zbiór zasobów i szybko dokonać odpowiednich zmian w ustawieniach.
- Nowa sekcja – Kontrola aplikacji – umożliwi uzyskiwanie szybkiego dostępu do parametrów ochrony odpowiedzialnych za wykrywanie niebezpiecznych działań w systemie, a także pozwala kontrolować dostęp do Twoich poufnych danych. Sekcja ta umożliwi również uruchamianie programów w bezpiecznym środowisku.
- Kreatory i narzędzia pomocne w rozwiązywaniu specyficznych zadań związanych z bezpieczeństwem komputera są zgromadzone osobnym dziale **Ochrona+**.

KONCEPCJA OCHRONY KOMPUTERA UŻYTKOWNIKA

Kaspersky Internet Security zapewnia ochronę komputera przed znanymi i nowymi zagrożeniami, atakami i oszustwami sieciowymi, spamem i innymi niechcianymi informacjami. Za ochronę przed poszczególnymi rodzajami zagrożeń odpowiadają indywidualne moduły aplikacji. Taka konstrukcja systemu ochrony pozwala na łatwe dostosowanie programu do Twoich indywidualnych potrzeb.

Kaspersky Internet Security zawiera następujące funkcje i możliwości:

- Moduły zapewniające ochronę:
 - plików i poufnych danych;
 - systemu;
 - pracy w sieci oraz Internecie.
- Zadania skanowania antywirusowego: umożliwiają skanowanie pojedynczych plików, folderów, dysków lub zdefiniowanych obszarów w poszukiwaniu szkodliwego kodu. Możliwe jest także szybkie uruchomienie pełnego skanowania całego komputera.
- Aktualizacja: gwarantuje aktualny stan wewnętrznych modułów aplikacji a także baz używanych do skanowania w poszukiwaniu szkodliwych programów i wykrywania ataków hakerów czy też spamu.
- Kreatory i narzędzia: ułatwiają wykonywanie zadań związanych z działaniem programu Kaspersky Internet Security.
- Funkcje pomocy: zapewniają dodatkowe informacje na temat obsługi programu oraz rozszerzają jego funkcjonalność.

ZADANIA SKANOWANIA ANTYWIRUSOWEGO

Poza ochroną w czasie rzeczywistym wszystkich źródeł przenikania złośliwych programów jednym z najważniejszych zadań ochrony jest regularne skanowanie komputera pod kątem obecności wirusów. Jest to czynność konieczna w celu uniknięcia rozprzestrzenienia się złośliwych programów, które nie zostały wykryte przez komponenty ochrony, np. z powodu niskiego stopnia ochrony.

W celu przeprowadzania skanowania antywirusowego Kaspersky Internet Security wykonuje następujące czynności:

- **Skanowanie obiektów.** Skanowanie obiektów wybranych przez użytkownika. Możliwe jest skanowanie dowolnego obiektu systemu plików komputera.
- **Pełne skanowanie.** Szczegółowe skanowanie całego systemu. Domyślnie skanowane są: pamięć systemowa, pliki autostartu, pliki przywracania systemu, poczta, dyski twarde, wymienne i sieciowe.
- **Szybkie skanowanie.** Skanowanie obiektów uruchamianych podczas startu systemu w poszukiwaniu wirusów.

AKTUALIZACJA

Uaktualnianie programu Kaspersky Internet Security jest konieczne, aby aplikacja zawsze reagowała na najnowsze ataki sieciowe, unieszkodliwiała wirusy lub inne niebezpieczne programy. Za pobieranie uaktualnień antywirusowych baz danych oraz modułów programu odpowiada składnik **Aktualizacja**.

Funkcja kopiowania aktualizacji pozwala zachować w katalogu lokalnym aktualizację baz i modułów programowych dostarczanych z serwerów Kaspersky Lab, a następnie umożliwić dostęp do nich innym komputerom sieci w celu optymalizacji ruchu sieciowego.

OCHRONA DANYCH I AKTYWNOŚCI ONLINE

Kaspersky Internet Security chroni dane na komputerze użytkownika przed złośliwymi programami i niekontrolowanym dostępem a także umożliwia bezpieczne nawiązywanie połączeń z siecią lokalną i Internetem.

Chronione obiekty podzielono na trzy grupy:

- Pliki, poufne dane, parametry dostępu do różnych zasobów (loginy użytkownika i hasła), informacje o kartach bankowych itd. Obiekty tego typu są chronione przez Ochronę plików, Kontrolę aplikacji oraz Ochronę proaktywną.
- Programy zainstalowane na komputerze i obiekty systemu operacyjnego. Obiekty tego typu są chronione przez Ochronę poczty, Ochronę WWW, Ochronę komunikatorów, Filtrowanie aplikacji, Ochronę proaktywną, Blokowanie ataków sieciowych, oraz Anti-Spam.
- Praca w sieci: przeglądanie stron internetowych, korzystanie z systemów płatniczych, ochrona poczty przed spamem oraz wirusami itd. Obiekty te są chronione przez Ochronę poczty, Ochronę WWW, Ochronę komunikatorów, Zaporę sieciową, Blokowanie ataków sieciowych, Anti-Spam, Monitor sieci, Anti-Phishing, Blokowanie banerów oraz Kontrolę rodzicielską.

FILTROWANIE PROGRAMÓW I DOSTĘPU DO DANYCH

Kaspersky Internet Security zapobiega wykonywaniu przez programy niebezpiecznych dla systemu działań, umożliwia kontrolę dostępu do poufnych danych użytkownika i uruchamianie programów w bezpiecznym środowisku z pomocą następujących narzędzi:

- **Kontrola aplikacji.** Komponent ten rejestruje i kontroluje wszystkie działania wykonywane przez aplikacje w systemie, klasyfikując je pod kątem grupy, do której należą. Dla każdej grupy programów dostępny jest szereg reguł. Reguły te definiują uprawnienia programów do rozmaitych zasobów.

- **Ochrona tożsamości elektronicznej.** Kontrola aplikacji zarządza uprawnieniami programów do wykonywania działań związanych z Twoimi poufnymi danymi. Zaliczają się do nich pliki, foldery i klucze rejestru zawierające parametry pracy oraz inne ważne zasoby najczęściej wykorzystywanych programów. Program chroni także folder Moje Dokumenty, pliki cookie oraz dane dotyczące Twojej aktywności podczas pracy z komputerem.
- **Bezpieczne uruchamianie (Sandbox).** Kaspersky Internet Security zapewnia maksymalne bezpieczeństwo obiektów systemu operacyjnego i osobistych danych użytkowników dzięki możliwości uruchamiania programów w chronionym środowisku wirtualnym.

KREATORY I NARZĘDZIA

Zapewnienie ochrony komputera jest niełatwym zadaniem, które wymaga wiedzy o systemie operacyjnym oraz sposobach wykorzystania jego słabych punktów. Informacje na temat bezpieczeństwa systemu są obszerne i różnorodne, co utrudnia ich analizę i przetwarzanie.

W celu ułatwienia wykonywania określonych zadań ochrony komputera Kaspersky Internet Security został wyposażony w zestaw kreatorów i narzędzi:

- Kreator konfiguracji przeglądarki przeprowadzający analizę ustawień przeglądarki Microsoft Internet Explorer oraz ich ocenę, przede wszystkim pod kątem bezpieczeństwa.
- Kreator przywracania systemu służący do eliminowania śladów obecności szkodliwych obiektów w systemie.
- Kreator czyszczenia śladów aktywności wyszukujący i eliminujący ślady Twojej aktywności w systemie oraz ustawieniach systemu operacyjnego, które pozwalają cyberprzestępcom na gromadzenie informacji o Twoich działaniach.
- Kreator tworzenia dysku ratunkowego wykorzystywany do przywracania funkcjonalności systemu po ataku szkodliwego kodu, który uszkodził pliki systemu operacyjnego i uniemożliwia jego uruchomienie.
- Kreator wyszukiwania luk pozwalający na identyfikowanie luk w systemie operacyjnym i programach zainstalowanych na komputerze.

- System analizy pakietów sieciowych przechwytyjący pakiety i wyświetlający informacje o nich.
- Monitor sieci wyświetlający informacje o aktywności sieciowej na komputerze.
- Klawiatura wirtualna zapobiegająca przechwytywaniu danych wprowadzanych z klawiatury.

USŁUGI

Kaspersky Internet Security jest wyposażony w zestaw usług. Mają one na celu zapewnienie ochrony komputera, zwiększenie możliwości oraz ułatwienie pracy z programem.

Pliki danych i raporty

Podczas pracy aplikacji tworzony jest raport dotyczący każdego z komponentów ochrony, zadań filtrowania czy aktualizacji aplikacji. Zawiera on informacje o wykonywanych operacjach i rezultatach pracy, dzięki czemu w każdej chwili możesz zapoznać się ze szczegółami dotyczącymi działania dowolnego składnika programu Kaspersky Internet Security. W przypadku wyniknięcia problemów raporty można wysyłać do Kaspersky Lab, gdzie specjaliści dokładnie przeanalizują sytuację i pomogą w jej rozwiązaniu.

Kaspersky Internet Security przenosi do kwarantanny wszystkie obiekty podejrzane z punktu bezpieczeństwa. Przechowywane są one w zaszyfrowanej postaci, aby uniknąć zarażenia komputera. Program pozwala na skanowanie tych obiektów w poszukiwaniu wirusów, przywracanie ich do stanu wyjściowego, usuwanie – możesz nawet samodzielnie dodać dowolny obiekt do kwarantanny. Wszystkie obiekty, które w wyniku skanowania okażą się niezainfekowane są automatycznie przywracane do stanu wyjściowego.

Kopie obiektów, które zostały wyleczone lub usunięte przez program Kaspersky Internet Security w procesie leczenia, przechowywane są w obszarze kopii zapasowej. Kopie te umożliwiają przywrócenie obiektów w razie potrzeby. Kopie zapasowe obiektów są przechowywane w postaci zaszyfrowanej w celu uniknięcia zarażenia komputera.

Program pozwala na usuwanie oraz przywracanie do stanu pierwotnego obiektów z obszaru kopii zapasowej.

Zarządzanie licencjami

Przed instalacją programu Kaspersky Internet Security musisz zaakceptować postanowienia Umowy Licencyjnej określającej prawa, na podstawie których możesz użytkować aplikację oraz uzyskiwać dostęp do aktualnych baz danych i pomocy technicznej. Wszystkie terminy i inne informacje wymagane do pełnej funkcjonalności programu zawarte są w pliku klucza stanowiącego integralną część aplikacji.

Przy użyciu sekcji **Zarządzanie licencjami** możesz uzyskać szczegółowe informacje dotyczące zakupionej licencji oraz nabyć nową lub odnowić bieżącą licencję.

Pomoc

Wszyscy zarejestrowani użytkownicy aplikacji mogą korzystać z usług pomocy technicznej. Aby dowiedzieć się, gdzie możesz uzyskać pomoc techniczną, użyj funkcji **Pomoc techniczna**.

Poprzez kliknięcie odpowiedniego odsyłacza możesz udać się na forum użytkowników produktów Kaspersky Lab, wysłać raport na temat błędu do działu pomocy technicznej lub zgłosić sugestię poprzez wypełnienie specjalnego formularza.

Za pomocą Internetu możesz także skorzystać z pomocy technicznej i Panelu klienta.

INSTALACJA APLIKACJI

Kaspersky Internet Security instalowany jest na komputerze w trybie interaktywnym przy użyciu kreatora instalacji.

Przed rozpoczęciem instalacji programu należy zakończyć działanie wszystkich innych uruchomionych aplikacji

W celu zainstalowania aplikacji uruchom plik dystrybucyjny (plik z rozszerzeniem *.exe).

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

Kreator instalacji przeprowadzi skanowanie aplikacji w poszukiwaniu pakietu instalacyjnego (plik z rozszerzeniem *.msi). Jeżeli taki plik zostanie odnaleziony, kreator przeprowadzi skanowanie w poszukiwaniu nowej wersji aplikacji na serwerach internetowych Kaspersky Lab. Jeżeli plik pakietu instalacyjnego nie zostanie odnaleziony, kreator zaproponuje jego pobranie. Po pobraniu pliku uruchomiona zostanie instalacja aplikacji. Jeżeli proces pobierania pliku zostanie anulowany, instalacja aplikacji zostanie wznowiona w trybie standardowym.

Uruchomiony zostanie kreator instalacji programu. Każde okno posiada 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. WYSZUKIWANIE NOWSZEJ WERSJI APLIKACJI

W tym kroku kreator instalacji sprawdzi, czy na serwerach aktualizacji Kaspersky Lab znajduje się nowsza wersja instalowanej aplikacji.

Jeśli okaże się, że na serwerach aktualizacji Kaspersky Lab nie ma nowszej wersji aplikacji, kreator rozpocznie instalację.

W przypadku odnalezienia nowszej wersji aplikacji, kreator zaproponuje jej pobranie. Jeżeli zadanie zostanie anulowane, kreator rozpocznie instalację obecnej wersji. Jeżeli instalowana będzie nowsza wersja, pliki instalacyjne zostaną pobrane na komputer.

KROK 2. WERYFIKACJA WYMAGAŃ SYSTEMOWYCH

Przed rozpoczęciem instalacji kreator sprawdzi system operacyjny oraz pakiety uaktualnień w celu porównania ich zgodności z wymaganiami oprogramowania. Weryfikowana jest również obecność wymaganych programów oraz uprawnienia użytkownika związane z instalacją oprogramowania.

Jeżeli program ustali, że któryś z wymaganych pakietów uaktualnień nie został zainstalowany, wyświetlony zostanie stosowny komunikat. Przed instalacją aplikacji zalecane jest zainstalowanie pakietów Service Pack oraz wymaganych uaktualnień przy użyciu narzędzia Windows Update.

KROK 3. WYBÓR TYPU INSTALACJI

Jeżeli okaże się, że Twój system spełnia wymagania sprzętowe i programowe, na serwerach aktualizacji Kaspersky Lab nie ma nowszej wersji programu lub zrezygnowałeś z instalacji nowszej wersji, na komputerze zostanie uruchomiony kreator instalacji bieżącej wersji Kaspersky Internet Security.

W tym momencie możesz wybrać typ instalacji:

- *Instalacja ekspresowa.* Po wybraniu tej opcji aplikacja zostanie zainstalowana z użyciem ustawień domyślnych zalecanych przez ekspertów firmy Kaspersky Lab. Po zakończeniu instalacji uruchomiony zostanie kreator konfiguracji ustawień aplikacji.
- *Instalacja niestandardowa.* Po wybraniu tej opcji będziesz mógł wybrać składni aplikacji i folder instalacyjny. Możesz także dokonać aktywacji i konfiguracji aplikacji przy użyciu specjalnego kreatora.

W pierwszym przypadku kreator instalacji zaproponuje Ci zapoznanie się z warunkami licencji, a także zasadami użytkowania Kaspersky Security Network. Następnie program zostanie zainstalowany na komputerze, bez Twojego udziału.

W drugim przypadku będziesz musiał brać czynny udział w całym procesie instalacji.

W celu kontynuacji instalacji kliknij przycisk **Dalej**, natomiast w celu rezygnacji – **Anuluj**.

KROK 4. ZAPOZNANIE SIĘ Z UMOWĄ LICENCYJNĄ

Kolejne okno dialogowe zawiera treść Umowy Licencyjnej, która stanowi prawne porozumienie między Tobą a firmą Kaspersky Lab. Musisz uważnie przeczytać jej treść i w przypadku zaakceptowania wszystkich postanowień wybrać opcję **Akceptuję postanowienia umowy licencyjnej**, a następnie kliknąć przycisk **Dalej**. Procedura instalacji będzie kontynuowana.

W celu przerwania instalacji kliknij przycisk **Anuluj**.

KROK 5. ZASADY KORZYSTANIA Z KASPERSKY SECURITY NETWORK

Na tym etapie program instalacyjny zaproponuje Ci uczestnictwo w programie Kaspersky Security Network, które obejmuje wysyłanie do firmy Kaspersky Lab

informacji o nowych zagrożeniach, jakie pojawiają się na Twoim komputerze, unikatowego identyfikatora przydzielonego do Twojego komputera i pewnych informacji o systemie.

Ważne!

Kaspersky Lab gwarantuje, że w obrębie Kaspersky Security Network nie są gromadzone i rozpowszechniane dane osobowe użytkowników.

Jeżeli chcesz uczestniczyć w systemie Kaspersky Security Network, zaznacz pole **Zgadzam się na uczestnictwo w Kaspersky Security Network**.

Następnie kliknij przycisk **Dalej**. Instalacja będzie kontynuowana.

KROK 6. WYBÓR FOLDERU INSTALACYJNEGO

Krok ten jest dostępny jedynie po wybraniu niestandardowego typu instalacji (patrz **Krok 3. Wybór typu instalacji**).

W tej fazie procesu instalacji możesz wskazać folder, w którym program zostanie zainstalowany. Domyślnie program instalowany jest w folderze:

- **<Dysk> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2010** – dla systemów 32-bitowych.
- **<Dysk> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2010** – dla systemów 64-bitowych.

Aby zmienić domyślną ścieżkę dostępu do folderu instalacyjnego, wprowadź ją ręcznie lub kliknij przycisk **Przełączaj**; w celu zlokalizowania i wybrania folderu użyj standardowego okna wyboru systemu Windows.

Ważne!

W przypadku ręcznego wprowadzania pełnej nazwy folderu instalacyjnego nie możesz wpisać więcej niż 200 znaków, ani używać znaków specjalnych.

Aby kontynuować instalację, kliknij przycisk **Dalej**.

KROK 7. WYBÓR INSTALOWANYCH SKŁADNIKÓW

Ważne!

Krok ten jest dostępny jedynie po wybraniu niestandardowego typu instalacji (patrz **Krok 3. Wybór typu instalacji**).

W tym kroku możesz wybrać składniki aplikacji, które zostaną zainstalowane. Domyślnie instalowane są wszystkie moduły aplikacji: ochrona, skanowanie oraz aktualizacja.

Aby zdecydować, które składniki mają zostać zainstalowane, przeczytaj ich krótkie opisy. W tym celu należy wybrać z listy dany moduł - polu znajdującym się poniżej sekcji wyboru pojawią się szczegółowe informacje na temat składnika wraz z ilością miejsca wymaganego do jego instalacji.

Aby pominąć instalację składnika, wybierz z menu kontekstowego opcję **Cały składnik będzie niedostępny**. Pominięcie instalacji składnika może pozbawić komputer ochrony przed dużą liczbą niebezpiecznych programów.

W celu wybrania składników, które mają zostać zainstalowane otwórz menu kontekstowe poprzez kliknięcie ikony znajdującej się obok nazwy składnika i wybierz opcję **Zostanie zainstalowany na lokalnym dysku twardym**.

Po wybraniu składników kliknij przycisk **Dalej**. Aby powrócić do listy domyślnie instalowanych składników, kliknij przycisk **Przywróć**.

KROK 8. WYŁĄCZENIE ZAPORY SIECIOWEJ MICROSOFT WINDOWS

Ważne!

Krok ten dostępny jest jedynie dla komputerów, na których Zapora Sieciowa Microsoft Windows jest włączona.

Na tym etapie instalacji aplikacja zaproponuje wyłączenie Zapory Sieciowej Microsoft Windows, ponieważ pełne bezpieczeństwo pracy w Sieci zapewni użytkownikowi Monitor sieciowy wchodzący w skład Kaspersky Internet Security.

W celu wykorzystania modułu programu Kaspersky Internet Security jako podstawowego środka ochrony pracy w Sieci kliknij przycisk **Dalej**. Zapora Sieciowa Microsoft Windows zostanie automatycznie wyłączona.

Aby korzystać z ochrony komputera przy pomocy Zapory Sieciowej Microsoft Windows, wybierz opcję **Wykorzystaj Zaporę Sieciową Microsoft Windows**. W tym przypadku zapora programu Kaspersky Internet Security zostanie zainstalowana, jednak pozostanie nieaktywna w celu uniknięcia konfliktów w pracy programów.

KROK 9. WYKORZYSTANIE PARAMETRÓW APLIKACJI ZACHOWANYCH Z POPRZEDNIEJ INSTALACJI

Na tym etapie możesz zdecydować, czy chcesz wykorzystać parametry ochrony i bazy aplikacji, w tym bazy modułu Anti-Spam, jeżeli zostały one zachowane na komputerze podczas usuwania poprzedniej wersji Kaspersky Internet Security.

Jeżeli na Twoim komputerze zainstalowana była wcześniejsza wersja Kaspersky Internet Security i przy jej usuwaniu zachowane zostały bazy programu, możesz wykorzystać je w bieżącej wersji. W tym celu zaznacz pole **Bazy aplikacji**. Bazy wchodzące w skład instalowanej aplikacji nie będą kopiowane na komputer.

Aby wykorzystać parametry ochrony ustawione i zapisane na komputerze w poprzedniej wersji, zaznacz pole **Parametry pracy aplikacji**.

Wskazane jest również wykorzystanie baz modułu Anti-Spam, jeżeli zostały one zachowane podczas usuwania poprzedniej wersji programu. W celu uwzględnienia tych baz zaznacz pole **Antyspamowe bazy danych**.

KROK 10. WYSZUKIWANIE INNYCH PROGRAMÓW ANTYWIRUSOWYCH

W tym kroku program instalacyjny sprawdzi, czy w systemie zostały zainstalowane inne aplikacje antywirusowe, łącznie z produktami Kaspersky Lab, które mogą przeszkadzać w prawidłowym działaniu aplikacji.

Program instalacyjny wyświetli na ekranie listę wykrytych programów. Przed kontynuowaniem instalacji zostanie wyświetlone zapytanie, czy mogą one zostać odinstalowane.

Możliwe jest skorzystanie z ręcznego lub automatycznego trybu usuwania wykrytych aplikacji antywirusowych.

Jeżeli na liście programów antywirusowych będzie znajdowała się aplikacja Kaspersky Lab w wersji 8.0, zalecane jest zachowanie pliku klucza przed jej usunięciem, ponieważ może on zostać użyty do zainstalowania nowej wersji. Zalecane jest także zachowanie zawartości folderów Kopii zapasowej i Kwarantanny. Obiekty te zostaną automatycznie przeniesione do odpowiednich folderów w nowej wersji aplikacji.

W przypadku automatycznego usunięcia wersji 8.0 informacje na temat jej aktywacji zostaną zapisane przez program oraz zostaną wykorzystane podczas instalacji wersji 2010.

Aby kontynuować instalację, kliknij przycisk **Dalej**.

KROK 11. KOŃCZENIE INSTALACJI PROGRAMU

Na tym etapie kreator zaproponuje zakończenie instalacji programu.

Podczas kolejnej i niestandardowej instalacji (patrz **Krok 3. Wybór typu instalacji**) nie jest zalecane usuwanie zaznaczenia z opcji **Włącz autoochronę przed instalacją**. Jeżeli moduły ochrony będą włączone, możliwe będzie cofnięcie zmian w przypadku wystąpienia błędu podczas instalacji. Podczas nowej instalacji programu zalecane jest usunięcie zaznaczenia z tej opcji.

Ważne!

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

Aby kontynuować instalację, kliknij przycisk **Dalej**.

Pakiet aplikacji zawiera moduły służące do przechwytywania ruchu sieciowego, dlatego podczas procesu instalacji bieżące połączenia sieciowe zostaną przerwane. Większość połączeń zostanie automatycznie wznowiona w krótkim czasie.

KROK 12. FINALIZOWANIE INSTALACJI

W oknie **Finalizowanie instalacji** wyświetlane są informacje na temat zakończenia procesu instalacji aplikacji.

Kolejnym krokiem jest skonfigurowanie aplikacji w celu zapewnienia maksymalnej ochrony danych na komputerze. Służy do tego kreator konfiguracji (patrz rozdział **Kreator konfiguracji aplikacji**).

Aby przejść do konfiguracji aplikacji, kliknij przycisk **Dalej**.

ROZPOCZĘCIE PRACY

Jednym z głównych założeń specjalistów z Kaspersky Lab było przygotowanie optymalnych ustawień predefiniowanych dla wszystkich parametrów programu Kaspersky Internet Security. Dzięki temu każdy użytkownik, niezależnie od stopnia zaawansowania może skutecznie chronić swój komputer bez spędzania dodatkowego czasu na konfigurowaniu aplikacji.

Dla Twojej wygody wszystkie etapy wstępnej konfiguracji zostały zebrane w jednym kreatorze konfiguracji aplikacji (patrz rozdział **Kreator konfiguracji aplikacji**), który uruchamia się natychmiast po zakończeniu instalacji programu. Postępując zgodnie z zaleceniami kreatora możesz aktywować program, skonfigurować ustawienia aktualizacji, ograniczyć dostęp do ustawień programu przy pomocy hasła i wykonać inne działania konfiguracyjne.

Istnieje prawdopodobieństwo, że Twój komputer został zainfekowany przed instalacją Kaspersky Internet Security. W celu wykrycia szkodliwych programów należy wykonać skanowanie komputera.

W wyniku działania szkodliwego programu oraz awarii systemu operacyjnego komputer może zostać uszkodzony. Aby odnaleźć luki w zabezpieczeniach zainstalowanych programów oraz nieprawidłowości w ustawieniach systemu, uruchom kreator analizy bezpieczeństwa (patrz rozdział **Kreator analizy bezpieczeństwa**).

Podczas instalacji może się okazać, że bazy danych aplikacji znajdujące się w pakiecie instalacyjnym są przeterminowane. W celu ich uaktualnienia uruchom aktualizację aplikacji (jeżeli nie została ona uruchomiona automatycznie po zakończeniu instalacji przez kreator konfiguracji).

Moduł antyspamowy wbudowany w aplikację wykorzystuje samouczący się algorytm do wykrywania niechcianych wiadomości e-mail. Aby skonfigurować ten moduł do pracy z korespondencją elektroniczną, uruchom kreator uczenia modułu Anti-Spam.

Po wykonaniu wszystkich opisanych powyżej działań aplikacja będzie gotowa do pracy. W celu dokonania oceny poziomu ochrony komputera uruchom kreator zarządzania ochroną (patrz rozdział **Zarządzanie ochroną**).

KREATOR KONFIGURACJI APLIKACJI

Kreator konfiguracji aplikacji jest uruchamiany po zakończeniu procesu instalacji. Pomaga on w przeprowadzeniu wstępnej konfiguracji parametrów programu Kaspersky Internet Security.

Kreator konfiguracji aplikacji posiada przystępny interfejs w formie następujących po sobie okien (kroków), przechodzenie między którymi umożliwiają przyciski **Wstecz** i **Dalej**. Zakończenie pracy kreatora umożliwia przycisk **Anuluj**.

KROK 1. AKTYWACJA PROGRAMU

Procedura aktywacji aplikacji polega na rejestracji licencji, w wyniku której na komputer pobierany jest plik klucza. Licencja określa Twoje prawa odnośnie użytkownika programu oraz okres jego działania.

Plik klucza zawiera informacje niezbędne do zapewnienia optymalnej pracy programu Kaspersky Internet Security, a także pewne dane dodatkowe:

- informację o pomocy (kto jej udziela i jak można z niej skorzystać);
- nazwę i numer pliku klucza a także termin upłynięcia ważności licencji.

Aktywacja aplikacji wymaga połączenia z Internetem.

Do otrzymania pliku klucza konieczne jest podanie kodu aktywacyjnego, który otrzymałeś podczas zakupu programu. Dostępne są następujące warianty aktywacji Kaspersky Internet Security:

- **Aktywacja wersji komercyjnej.** Wybierz ten wariant, jeżeli posiadasz komercyjną wersję programu. Po podaniu kodu aktywacyjnego kreator pobierze i zainstaluje odpowiedni plik klucza, który umożliwi Ci korzystanie ze wszystkich funkcji programu w ciągu czasu trwania licencji.
- **Aktywacja wersji testowej.** Wybierz ten wariant, jeżeli chcesz aktywować wersję testową, zanim zdecydujesz się na zakup licencji komercyjnej. Kreator pobierze testowy plik klucza, który umożliwi Ci na korzystanie z funkcji programu przez ograniczony czas.

- **Pomiń aktywację.** Wybierz ten wariant, aby dokonać aktywacji w późniejszym terminie. Aplikacja zostanie zainstalowana na komputerze wraz ze wszystkimi funkcjami oprócz aktualizacji (będziesz mógł dokonać tylko jednej aktualizacji – tuż po zakończeniu instalacji).

Jeżeli Kaspersky Internet Security był wcześniej zainstalowany, a następnie usunięty z zachowaniem informacji o aktywacji, krok ten zostanie pominięty.

AKTYWACJA WERSJI KOMERCYJNEJ

Po wybraniu tego wariantu aktywacja aplikacji jest przeprowadzana za pośrednictwem serwera Kaspersky Lab (wymagane jest połączenie z Internetem).

Aktywacja jest przeprowadzana na podstawie wprowadzenia kodu aktywacyjnego, który otrzymałeś podczas zakupu oprogramowania Kaspersky Internet Security.

Kod aktywacyjny składa się z czterech sekcji rozdzielonych myślnikami, z których każda zawiera po pięć znaków, np. 11111-11111-11111-11111.

Po podaniu kodu aktywacyjnego, kreator przesyła go do serwera aktywacji Kaspersky Lab, gdzie jest on weryfikowany. Po pomyślnym zakończeniu weryfikacji kodu kreator pobiera z serwera plik klucza i instaluje go automatycznie. Po zakończeniu procesu aktywacji na ekranie pojawi się okno z dokładną informacją na temat zakupionej licencji.

W przypadku aktywacji subskrypcji, oprócz wyżej wymienionej informacji, pojawia się także informacja o statusie subskrypcji (patrz sekcja **Zgoda na automatyczne przedłużenie licencji**).

Jeżeli weryfikacja kodu aktywacyjnego nie przebiegnie pomyślnie, na ekranie pojawi się odpowiednie powiadomienie. W takim przypadku zwróć się do firmy, w której zakupiłeś program Kaspersky Internet Security.

Jeżeli okres aktywacji przy pomocy danego kodu został przekroczony, na ekranie pojawi się odpowiednie powiadomienie. Proces aktywacji zostanie przerwany i kreator zaproponuje Ci skontaktowanie się z działem pomocy technicznej Kaspersky Lab.

Jeżeli podczas połączenia z serwerem aktywacji wystąpią błędy i nie otrzymasz pliku klucza, skontaktuj się z działem pomocy technicznej Kaspersky Lab.

AKTYWACJA WERSJI TESTOWEJ

Z tego wariantu aktywacji możesz skorzystać przed podjęciem decyzji o zakupie wersji komercyjnej programu Kaspersky Internet Security. W procesie aktywacji otrzymasz bezpłatny plik klucza z licencją ograniczoną czasowo. Po upływie czasu trwania licencji testowej nie możesz ponownie aktywować wersji testowej.

Jeżeli podczas połączenia z serwerem aktywacji wystąpią błędy i nie otrzymasz pliku klucza, skontaktuj się z działem pomocy technicznej Kaspersky Lab.

ZAKOŃCZENIE AKTYWACJI

Kreator aktywacji poinformuje Cię o pomyślnym zakończeniu aktywacji programu Kaspersky Internet Security. Oprócz tego na ekranie pojawi się informacja o licencji: typ (komercyjna, testowa itd.), data upływu okresu ważności licencji a także liczba komputerów objętych licencją.

W przypadku aktywacji subskrypcji w miejscu daty upływu terminu działania klucza znajduje się informacja o statusie przedłużenia licencji (patrz rozdział **Zgoda na automatyczne przedłużenie licencji**)

KROK 2. WYBÓR TRYBU OCHRONY

Kaspersky Internet Security umożliwia wybór trybu ochrony.

Do wyboru są dwa tryby ochrony:

- *Automatyczny.* Po wystąpieniu zdarzenia związanego z bezpieczeństwem program automatycznie wykona działanie zalecane przez ekspertów Kaspersky Lab. Jeżeli pojawi się zagrożenie, aplikacja podejmie próbę leczenia, a jeżeli okaże się to niemożliwe, niebezpieczny obiekt zostanie usunięty. Obiekty podejrzane są automatycznie przenoszone do kwarantanny. O występujących zdarzeniach i działaniach programu informują komunikaty.
- *Interaktywny.* W tym trybie aplikacja reaguje na występowanie zdarzeń wskazanych przez Ciebie w ustawieniach poszczególnych składników ochrony. W przypadku pojawienia się sytuacji wymagających Twojej

ingerencji, aplikacja wyświetla komunikaty oferując możliwość wyboru działania.

Komunikaty o zidentyfikowaniu aktywnego zarażenia wyświetlane są niezależnie od wyboru trybu ochrony

KROK 3. KONFIGURACJA AKTUALIZACJI PROGRAMU

Ważne!

Krok ten zostanie pominięty, jeżeli wybrałeś tryb instalacji ekspresowej. Parametry programu konfigurowane na tym etapie są ustawiane domyślnie.

Jakość ochrony komputera zależy bezpośrednio od regularnych aktualizacji baz i modułów aplikacji. W tym oknie kreatora konfiguracji możesz wybrać tryb aktualizacji programu Kaspersky Internet Security i ustawić parametry terminarza:

- **Aktualizacja automatyczna.** Kaspersky Internet Security będzie automatycznie sprawdzał obecność uaktualnień w źródle aktualizacji, we wskazanych odstępach czasu. Częstotliwość poszukiwania uaktualnień może zostać zwiększona w czasie epidemii wirusów. Aplikacja identyfikuje nowe aktualizacje a następnie ściąga je na komputer. Jest to domyślny tryb aktualizacji.
- **Zaplanowana aktualizacja** (w zależności od parametrów terminarza częstotliwość pobierania uaktualnień może ulegać zmianie). Aktualizacja będzie instalowana automatycznie zgodnie z podanymi przez Ciebie odstępami czasu. Parametry terminarza można ustawić w oknie, które otworzy się po kliknięciu przycisku **Ustawienia**.
- **Ręczna aktualizacja.** W tym przypadku samodzielnie dokonujesz aktualizacji aplikacji.

Ważne!

Bazy i moduły wchodzące w skład aplikacji mogą się okazać przeterminowane w momencie instalacji. Ekspersi z Kaspersky Lab zalecają natychmiastowe pobranie najnowszych uaktualnień poprzez kliknięcie przycisku **Aktualizuj teraz**. Program otrzyma niezbędny zbiór aktualizacji z serwerów Kaspersky Lab i zainstaluje je na Twoim komputerze.

Jeżeli bazy wchodzące w skład pakietu instalacyjnego uległy znacznemu przedawnieniu, uaktualnienia mogą posiadać znaczne rozmiary (do kilkudziesięciu MB), w wyniku czego pobieranie może obciążyć połączenie internetowe.

W celu przejścia do konfiguracji parametrów aktualizacji (patrz rozdział **Aktualizacja**) kliknij przycisk **Ustawienia**.

KROK 4. OGRANICZENIE DOSTĘPU DO APLIKACJI

Ważne!

Krok ten zostanie pominięty, jeżeli wybrałeś tryb instalacji ekspresowej. Parametry programu konfigurowane na tym etapie są ustawiane domyślnie.

Ze względu na to, że z komputera może korzystać wielu użytkowników o różnym stopniu zaawansowania, jak również biorąc pod uwagę fakt, że ochrona może zostać wyłączona przez złośliwe programy, zaleca się ograniczenie dostępu do programu Kaspersky Internet Security przy pomocy hasła. Hasło pozwala chronić aplikację przed próbami niekontrolowanego wyłączenia ochrony lub zmianą jej parametrów.

W celu włączenia ochrony zaznacz pole **Włącz ochronę hasłem** i wypełnij pola **Nowe hasło** oraz **Potwierdzenie hasła**.

Poniżej przedstawione zostało spektrum działania ograniczenia dostępu:

- **Konfiguracja ustawień aplikacji** – żądanie hasła przy próbie zapisu zmian parametrów programu Kaspersky Internet Security.
- **Zakończenie działania aplikacji** – żądanie hasła przy próbie zakończenia pracy programu.

KROK 5. WYBÓR WYKRYWANYCH ZAGROŻEŃ

Ważne!

Krok ten zostanie pominięty, jeżeli wybrałeś tryb instalacji ekspresowej. Parametry programu konfigurowane na tym etapie są ustawiane domyślnie.

Na tym etapie możesz wybrać kategorie zagrożeń wykrywanych przez program Kaspersky Internet Security. Programy stwarzające zagrożenia dla komputera są zawsze wykrywane przez Kaspersky Internet Security. Należą do nich wirusy, robaki i trojany.

KROK 6. WYŁĄCZANIE DNS

Krok ten zostanie pominięty, jeżeli wybrałeś tryb instalacji ekspresowej. Parametry programu konfigurowane na tym etapie są ustawiane domyślnie.

Funkcja buforowania nazw domen znacznie skraca czas łączenia się komputera z serwisami internetowymi. Jest to jednak niebezpieczna luka, którą cyberprzestępcy mogą wykorzystać w celu otrzymania dostępu do Twoich danych.

W celu podniesienia stopnia bezpieczeństwa komputera zaznacz pole **Wyłącz pamięć podręczną DNS**.

Po wyłączeniu pamięci podręcznej DNS mogą pojawić się problemy w pracy programów, wykorzystujących wiele połączeń jednocześnie (np. aplikacje obsługujące sieci wymiany plików P2P).

Na tym etapie możesz także włączyć umieszczanie w raportach wpisów dotyczących zdarzeń informacyjnych. W tym celu zaznacz pole **Zapisuj zdarzenia informacyjne**.

KROK 7. ANALIZA SYSTEMU

Na tym etapie zbierane są informacje o programach zainstalowanych wchodzących w skład systemu Microsoft Windows. Programy te zapisywane są na liście aplikacji, które bez ograniczeń mogą wykonywać operacje w systemie.

KROK 8. ZAKOŃCZENIE PRACY KREATORA

Ostatnie okno kreatora informuje o zakończeniu instalacji aplikacji. Aby rozpocząć pracę z Kaspersky Internet Security, upewnij się, że pole

Uruchom Kaspersky Internet Security jest zaznaczone i kliknij przycisk **Zakończ**.

WYBÓR TYPU SIECI

Po zakończeniu instalacji aplikacji Zapora sieciowa dokona analizy aktywnych połączeń sieciowych. Do każdego połączenia zostanie przypisany stan określający dozwolone aktywności sieciowe.

Jeśli wybrałeś interaktywny tryb ochrony, Kaspersky Internet Security będzie informował Cię o wykryciu każdego połączenia sieciowego. W celu wybrania statusu połączenia możesz użyć okna powiadomienia. Dostępne są następujące możliwości:

- **Sieć publiczna.** Sieci o tym statusie nie mogą nawiązywać łączności z zewnątrz z Twoim komputerem. Uzyskiwanie dostępu do publicznych folderów i drukarek także nie jest dozwolone. Status ten jest zalecany dla sieci Internet.
- **Sieć lokalna.** Dla sieci o tym statusie uzyskiwanie łączności z publicznymi folderami i drukarkami jest dozwolone. Status ten zaleca się przypisywać chronionym sieciom lokalnym (na przykład, sieciom korporacyjnym).
- **Sieć zaufana.** Dla sieci o tym statusie dozwolona jest wszelka aktywność. Status ten może być przypisywany wyłącznie do całkowicie bezpiecznych połączeń.

Każdy ze statusów obejmuje zestaw reguł zarządzających aktywnością sieciową. W późniejszym terminie możesz zmienić status przypisany do sieci w momencie jej pierwszego wykrycia.

AKTUALIZACJA APLIKACJI

Do przeprowadzenia aktualizacji niezbędne jest połączenie z Internetem.

Kaspersky Internet Security zawiera bazy danych, w których znajdują się sygnatury zagrożeń, próbki fraz charakterystycznych dla spamu oraz opisy ataków sieciowych. Jednak, w momencie instalacji może się okazać, że bazy danych dostarczone wraz z pakietem instalacyjnym są przestarzałe.

Podczas pracy z kreatorem istnieje opcja wyboru trybu uruchomienia aktualizacji (Krok 3. Konfiguracja aktualizacji programu). Domyślnie Kaspersky Internet Security automatycznie sprawdza, czy istnieją nowe aktualizacje do pobrania na stronie internetowej Kaspersky Lab. Dostępne uaktualnienia są automatycznie pobierane i instalowane na komputerze.

Jeżeli okaże się, że bazy wchodzące w skład pakietu instalacyjnego są całkowicie przestarzałe, pobieranie kompletu nowych baz może znacznie obciążyć łącze internetowe.

W celu zagwarantowania aktualnego stanu ochrony komputera pobierz wszystkie najświeższe uaktualnienia dla programu Kaspersky Internet Security natychmiast po zakończeniu instalacji.

► *W celu ręcznego wywołania aktualizacji programu Kaspersky Internet Security wykonaj następujące czynności:*

1. Otwórz okno główne aplikacji.
2. W lewej części okna kliknij sekcję **Aktualizacja**.
3. Kliknij przycisk **Uruchom aktualizację**.

SKANOWANIE KOMPUTERA W POSZUKIWANIU WIRUSÓW

Twórcy szkodliwego oprogramowania przykładają ogromną wagę do ukrywania swoich działań w systemie. Z tego względu w wielu przypadkach możesz w ogóle nie zauważyć obecności takich aplikacji w swoim systemie.

Po zakończeniu instalacji program automatycznie uruchamia **szybkie skanowanie**. Zadanie to wyszukuje i neutralizuje szkodliwe programy znajdujące się w obiektach ładowanych wraz ze startem systemu operacyjnego.

Ekspersi z Kaspersky Lab zalecają także wykonanie **pełnego skanowania**.

- ▶ *Aby uruchomić zadanie skanowania antywirusowego wykonaj następujące czynności:*
 1. Otwórz okno główne aplikacji.
 2. W lewej części okna wybierz sekcję **Skanuj Komputer**.
 3. Kliknij przycisk **Uruchom pełne skanowanie**. Aby zatrzymać wykonywanie zadania, kliknij przycisk **Zatrzymaj pełne skanowanie**.

SKANOWANIE KOMPUTERA W POSZUKIWANIU LUK

W wyniku niekontrolowanej aktywności na komputerze, wywołanej lukami w systemie lub działaniem szkodliwych programów, parametrom systemu operacyjnego w wielu przypadkach przypisywane są błędne wartości. Ponadto programy zainstalowane na komputerze mogą posiadać luki, z wykorzystaniem których cyberprzestępcy wykonują szkodliwe działania.

W celu odnalezienia i usunięcia opisanych problemów bezpieczeństwa specjaliści z Kaspersky Lab zalecają uruchomić *szukanie luk* natychmiast po zainstalowaniu programu. W trakcie wykonywania zadania program szuka luk w zainstalowanych programach, a także uszkodzeń i nieprawidłowości w parametrach systemu operacyjnego oraz przeglądarki internetowej.

- ▶ *W celu uruchomienia zadania wyszukiwania luk wykonać następujące czynności:*
 1. Otwórz okno główne programu.
 2. W lewej części okna wybierz sekcję **Skanuj Komputer**.
 3. Kliknij przycisk **Uruchom wykrywanie luk**.

4. W oknie, które pojawi się na ekranie, jeszcze raz kliknij przycisk **Uruchom wykrywanie luk**.

ZARZĄDZANIE LICENCJĄ

Możliwość korzystania z funkcji programu Kaspersky Internet Security zapewnia plik klucza, który jest instalowany na komputerze w procesie aktywacji. Plik klucza zawiera informację o licencji: typ, okres ważności oraz liczba komputerów objętych licencją.

Bez pliku klucza (jeżeli nie dokonałeś aktywacji wersji komercyjnej lub testowej) program będzie pracował w trybie jednokrotnej aktualizacji. Nie będzie możliwości ponownych aktualizacji.

Jeżeli dokonałeś aktywacji wersji testowej, po zakończeniu okresu ważności uruchomienie programu Kaspersky Internet Security będzie niemożliwe.

Po zakończeniu okresu ważności licencji komercyjnej program zachowa swoje funkcje z wyjątkiem możliwości aktualizacji baz. Będziesz w dalszym ciągu mógł sprawdzać komputer przy użyciu skanowania i korzystać ze składników ochrony, jednak wyłącznie z użyciem baz uaktualnianych do momentu wygaśnięcia licencji.

W celu uniknięcia zarażenia komputera przez nowe wirusy zalecamy przedłużenie licencji na oprogramowanie Kaspersky Internet Security. Program automatycznie będzie Cię powiadamiał o zbliżającym się terminie wygaśnięcia licencji. Komunikat taki zacznie pojawiać się na ekranie komputera dwa tygodnie przed wygaśnięciem licencji i będzie wyświetlany podczas każdego uruchomienia programu Kaspersky Internet Security.

W oknie **Zarządzanie licencjami** wyświetlane są następujące informacje o licencji: typ (komercyjna, komercyjna z subskrypcją, komercyjna z subskrypcją na ochronę, testowa), liczba komputerów objętych licencją, data upływu terminu licencji i liczba dni do tego czasu. Informacja o upływie terminu licencji nie pojawia się, jeśli korzystasz z licencji komercyjnej z subskrypcją lub licencji komercyjnej z subskrypcją na ochronę (patrz rozdział **Subskrypcja automatycznego przedłużenia licencji**).

W celu zapoznania się z warunkami licencji kliknij odsyłacz **Przeczytaj umowę licencyjną** znajdujący się w dolnej części okna **Zarządzanie licencjami**. W celu usunięcia pliku klucza kliknij przycisk z czerwonym symbolem X znajdujący się z prawej strony numeru licencji. W celu aktywacji nowej licencji kliknij przycisk **Aktywuj nową licencję**.

Przy pomocy przycisków **Kup licencję (Odnów licencję)** możesz kupić lub przedłużyć licencję w sklepie internetowym Kaspersky Lab.

SUBSKRYPCJA AUTOMATYCZNEGO PRZEDŁUŻENIA LICENCJI

Subskrypcja pozwala automatycznie przedłużyć okres trwania licencji. Do uruchomienia tej funkcji niezbędny jest kod aktywacyjny, który otrzymałeś przy zakupie programu Kaspersky Internet Security.

Jeśli w momencie aktywacji subskrypcji posiadałeś już aktywną licencję z ograniczonym okresie licencjonowania, zostanie ona automatycznie zastąpiona przez licencję subskrypcyjną. W celu rezygnacji z subskrypcji należy skontaktować się ze sprzedawcą, u którego zakupiony został Kaspersky Internet Security.

W celu określenia stanu subskrypcji wykorzystywane są następujące informacje:

- *W realizacji.* Aktywacja subskrypcji znajduje się w trakcie realizacji (zamówienia jest przetwarzane przez serwer). Dostępne są wszystkie funkcje Kaspersky Internet Security. Jeżeli po upływie określonego czasu realizacja subskrypcji nie będzie dokonana, otrzymasz powiadomienie o tym, że aktualizacja subskrypcji nie została wykonana. Dodatkowo funkcja aktualizacji zostanie wyłączona (w przypadku licencji z subskrypcją) oraz wyłączona zostaną wszystkie moduły ochronne (w przypadku licencji z subskrypcją ochrony).
- *Aktywowana.* Subskrypcja została aktywowana bezterminowo lub na pewien okres czasu (została określona data zakończenia subskrypcji).
- *Przedłużona.* Subskrypcja została przedłużona bezterminowo lub na pewien okres czasu.
- *Błąd.* Podczas aktualizacji subskrypcji wystąpił błąd.
- *Wygasła. Okres karencji.* Uplłynął termin ważności subskrypcji lub termin aktualizacji jej stanu. Po wygaśnięciu okresu automatycznej aktualizacji subskrypcji, musisz ręcznie uaktualnić jej stan. Po wygaśnięciu terminu ważności subskrypcji możesz odnowić subskrypcję kontaktując się ze sprzedawcą, u którego zakupiony został Kaspersky Internet Security. W celu wykorzystania innego kodu aktywacji musisz najpierw usunąć bieżącą licencję subskrypcji.

- *Wygasa. Upłynął okres karencji.* Upłynął termin ważności subskrypcji lub okres karencji umożliwiający przedłużenie licencji. W celu przedłużenia subskrypcji lub zakupienia nowej skontaktuj się z dostawcą subskrypcji.
- *Rezygnacja z subskrypcji.* Nastąpiła rezygnacja korzystania z subskrypcji automatycznego przedłużenia licencji.
- *Wymagana jest aktualizacja subskrypcji.* Z pewnych powodów stan subskrypcji nie był aktualizowany przez pewien okres czasu. W celu uaktualnienia subskrypcji należy kliknąć przycisk **Uaktualnij stan subskrypcji**.
- *Zatrzymana.* Subskrypcja automatycznego przedłużenia licencji została wstrzymana.
- *Wznowiona.* Subskrypcja została wznowiona.

Jeżeli upłynął termin ważności subskrypcji oraz okres karencji, w ciągu którego dostępna była możliwość jej przedłużenia (stan subskrypcji – *Wygasa*), Kaspersky Internet Security powiadomi o tym i uniemożliwi próby automatycznego przedłużenia licencji. W przypadku licencji z subskrypcją wszystkie funkcje aplikacji będą dostępne, za wyjątkiem możliwości aktualizacji baz danych programu. W przypadku licencji z subskrypcją ochrony, wyłączone zostaną komponenty odpowiedzialne za ochronę komputera, wykonywanie zadań skanowania oraz możliwość aktualizacji.

Jeżeli z jakichkolwiek przyczyn licencja nie została przedłużona (stan subskrypcji - *Wymagana aktualizacja*) w odpowiednim czasie (np. komputer był wyłączony przez cały okres kiedy możliwe było przedłużenie licencji), możesz ręcznie uaktualnić jej stan. Do czasu przedłużenia subskrypcji Kaspersky Internet Security uniemożliwia aktualizację baz danych aplikacji (w przypadku licencji z subskrypcją), wstrzymaniu ulega także ochrona komputera i uruchamianie zadań skanowania (w przypadku licencji z subskrypcją ochrony).

W przypadku korzystania z subskrypcji nie możesz użyć innego kodu aktywacyjnego w celu przedłużenia licencji. Będzie to możliwe dopiero po upływie terminu ważności subskrypcji (stan subskrypcji – *Wygasa*). W celu przedłużenia okresu ważności licencji możesz skorzystać z okresu karencji, podczas którego dostępne będą wszystkie funkcje aplikacji.

Jeżeli w trakcie korzystania z subskrypcji znajdzie konieczność ponownej instalacji aplikacji na komputerze, wymagana będzie ręczna aktywacja programu przy pomocy kodu aktywacyjnego otrzymanego przy zakupie programu.

Zbiór możliwych do wykonania działań na subskrypcji może różnić się w zależności od jej dostawcy. Okres karencji, w trakcie którego możliwe jest przedłużenie licencji może także nie być dostępny (tryb domyślny).

UCZESTNICTWO W KASPERSKY SECURITY NETWORK

Codziennie na świecie pojawia się ogromna liczba nowych zagrożeń. W celu usprawnienia gromadzenia statystyk dotyczących nowych typów zagrożeń i ich źródeł, jak również rozwoju metod ich eliminacji Kaspersky Lab udostępnia usługę Kaspersky Security Network.

Uczestnictwo w Kaspersky Security Network obejmuje wysłanie do firmy Kaspersky Lab następujących informacji:

- Unikatowego identyfikatora przydzielonego Twojemu komputerowi przez aplikację. Identyfikator ten charakteryzuje ustawienia sprzętowe komputera i nie zawiera żadnych informacji osobowych.
- Informacje o zagrożeniach wykrytych przez moduły aplikacji. Struktura i treść informacji zależy od typu wykrytych zagrożeń.
- Informacje o systemie: wersja systemu operacyjnego, zainstalowane pakiety uaktualnień, usługi i sterowniki, wersje przeglądarki i klienta pocztowego, rozszerzenia przeglądarki, wersja zainstalowanej aplikacji firmy Kaspersky Lab.

Kaspersky Security Network gromadzi również zaawansowane statystyki zawierające:

- Informacje o plikach wykonywalnych i podpisanych aplikacjach pobranych na Twój komputer.
- Informacje o aplikacjach uruchomionych na Twoim komputerze.

Informacje statystyczne są wysyłane po zakończeniu aktualizacji aplikacji.

Ważne!

Kaspersky Lab gwarantuje, że w obrębie Kaspersky Security Network nie są gromadzone i rozpowszechniane dane osobowe użytkowników.

- ▶ W celu skonfigurowania ustawień wysyłania statystyk wykonaj następujące czynności:
 1. Otwórz okno ustawień aplikacji.
 2. W lewej części okna wybierz sekcję **Opinia**.
 3. W celu potwierdzenia udziału w Kaspersky Security Network należy zaznaczyć pole **Zgadzam się na uczestnictwo w Kaspersky Security Network**. W celu potwierdzenia zgody na wysyłanie rozszerzonych statystyk należy zaznaczyć pole **Wyrażam zgodę na wysyłanie rozszerzonych statystyk w strukturach Kaspersky Security Network**.

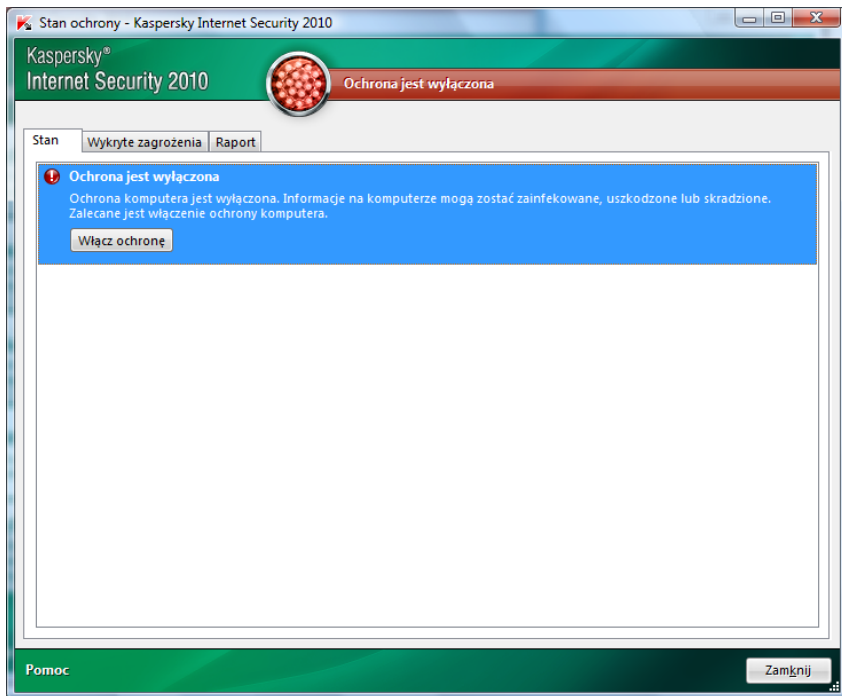
ZARZĄDZANIE OCHRONĄ

Zmiana koloru ikony stanu komputera oraz panelu, w którym ta ikona się znajduje wskazuje na problemy związane z ochroną komputera. Po pojawieniu się problemów takich problemów zaleca się ich natychmiastowe usunięcie.



Rysunek 1. Bieżący stan ochrony komputera

Listę problemów, które wystąpiły, ich opisy oraz proponowane rozwiązania można przeglądać w oknie **Stan ochrony** (patrz rysunek poniżej), która pojawi się po kliknięciu odnośnika **Napraw teraz** (patrz rysunek powyżej).



Rysunek 2. Rozwiązywanie problemów związanych z ochroną

Możliwe jest przeglądanie listy bieżących problemów. Problemy są uporządkowane zgodnie z priorytetem: od krytycznych (ikona koloru czerwonego), przez mniej ważne (ikona koloru żółtego), po komunikaty informacyjne (ikona koloru zielonego). Do każdego problemu dołączany jest szczegółowy opis. Dostępne są następujące akcje:

- *Usuń natychmiast.* Wyeliminowanie zagrożenia (jest to akcja zalecana).
- *Wylecz później.* Jeżeli z jakiegoś powodu natychmiastowe wyeliminowanie jest niemożliwe, można odroczyć to działanie i powrócić do niego później. W tym celu użyj opcji **Ukryj wiadomość**.

Opcja ta jest niedostępna w przypadku poważnych problemów. Do takich problemów zalicza się, na przykład, szkodliwe obiekty, które nie

zostały wyleczone, nieudaną próbę uruchomienia jednego lub kilku składników ochrony lub uszkodzenie plików programu.

W celu wyświetlenia ukrytych wiadomości na liście ogólnej zaznacz pole

Wyświetl ukryte wiadomości

STAN OCHRONY

Informacje o pracy komponentów Kaspersky Internet Security oraz zadań skanowania komputera w poszukiwaniu wirusów są dostępne w sekcji zawierającej całościową informację o stanie ochrony komputera. W tym miejscu możesz zapoznać się z liczbą niebezpiecznych obiektów odnalezionych podczas pracy aplikacji, a także dowiedzieć się, które z nich zostały wyleczone, usunięte lub umieszczone w kwarantannie.

O tym, że aplikacja znalazła niebezpieczne obiekty informuje zmiana koloru ikony statusu ochrony i panelu, na którym jest ona wyświetlana. W przypadku odnalezienia szkodliwych obiektów, kolor ikony i panelu zmienia się na czerwony. W takim przypadku powinieneś niezwłocznie usunąć wszystkie powstałe zagrożenia.

- ▶ *W celu zapoznania się ze stanem ochrony komputera wykonaj następujące czynności:*
 1. Otwórz okno główne aplikacji.
 2. Kliknij odnośnik **Raport**.
- ▶ *W celu usunięcia problemów powstałych w wyniku ochrony komputera wykonaj następujące czynności:*
 1. Otwórz okno główne aplikacji.
 2. Kliknij odnośnik **Raport**.
 3. W otwartym oknie, na zakładce **Status** wykonaj niezbędne czynności. Aby wcześniej ukryte informacje ponownie były widoczne w ogólnym spisie zaznacz pole **Pokaż ukryte informacje**.

- ▶ *W celu rozpoczęcia pracy ze zidentyfikowanym obiektem wykonaj następujące czynności:*
 1. Otwórz okno główne aplikacji.
 2. Kliknij przycisk **Raport**.
 3. W otwartym oknie, na zakładce **Wykryte zagrożenia** wybierz z listy żądany obiekt i kliknij go prawym przyciskiem myszy, aby otworzyć jego menu kontekstowe.
 4. Wybierz żądane działanie z otwartego menu.

- ▶ *W celu zapoznania się z raportem z pracy komponentów ochrony wykonaj następujące czynności:*
 1. Otwórz okno główne aplikacji.
 2. Kliknij odnośnik **Raport**.
 3. W otwartym oknie przejdź do zakładki **Raport**.

WSTRZYMYWANIE OCHRONY

Wstrzymanie ochrony oznacza wyłączenie na określony czas wszystkich składników ochrony. Informuje o tym:

- Nieaktywna (szara) ikona aplikacji w zasobniku systemowym;
- Czerwony kolor ikony i panelu statusu w oknie głównym programu Kaspersky Internet Security.

Jeżeli w chwili wstrzymania ochrony aktywne były połączenia sieciowe, na ekranie pojawi się informacja o przerwaniu tych połączeń.

► W celu wstrzymania ochrony komputera wykonaj następujące czynności:

1. Z menu kontekstowego aplikacji wybierz polecenie **Wstrzymaj ochronę**.
2. W oknie, które zostanie otwarte, wybierz kiedy ochrona ma zostać wyłączona:
 - **Wstrzymaj na <przedział czasu>** - ochrona zostanie wznowiona po upływie zdefiniowanego czasu. W celu określenia przedziału czasu skorzystaj z listy rozwijalnej.
 - **Wstrzymaj do restartu** – ochrona zostanie wznowiona po ponownym uruchomieniu systemu (o ile został włączony tryb umożliwiający uruchomienie aplikacji podczas uruchomienia komputera).
 - **Wstrzymaj** – ochrona nie będzie wznowiana automatycznie. Aby włączyć ochronę, wybierz polecenie **Wznów ochronę** z menu kontekstowego aplikacji.

KOMPONENTY OCHRONY

OCHRONA SYSTEMU PLIKÓW

Ochrona plików pozwala uniknąć zainfekowania systemu plików. Komponent uruchamia się przy starcie systemu operacyjnego, stale znajduje się w pamięci operacyjnej komputera i skanuje wszystkie otwierane, modyfikowane i zapisywane pliki.

Domyślnie Ochrona plików sprawdza tylko nowe i zmienione pliki. Podczas skanowania plików wykorzystywany jest zbiór parametrów nazywany poziomem ochrony. W przypadku wykrycia zagrożeń Ochrona plików wykonuje określone działanie.

Stopień ochrony plików i pamięci jest określany za pomocą parametrów, które:

- tworzą bezpieczne środowisko;
- określają wykorzystywaną metodę skanowania;
- określają metodę skanowania plików złożonych (a także plików o dużych rozmiarach);
- definiują tryb skanowania;
- pozwalają wstrzymać pracę komponentu zgodnie z ustawieniami lub w czasie pracy określonych aplikacji.

Specjaliści z Kaspersky Lab nie zalecają samodzielnego ustawiania parametrów pracy Ochrony plików. W większości przypadków wystarczająca jest zmiana poziomu ochrony. W każdej chwili możesz przywrócić domyślne parametry pracy Ochrony plików.

- ▶ *W celu zmiany parametrów pracy Ochrony plików wykonaj następujące czynności:*
 1. Otwórz okno główne programu i kliknij odnośnik **Ustawienia** znajdujący się w górnej części okna.
 2. W oknie, które pojawi się na ekranie, w sekcji **Ochrona** wybierz komponent **Ochrona plików**.

3. Kliknij przycisk **Ustawienia** dla wybranego komponentu.
4. Przeprowadź konfigurację parametrów komponentu.

ALGORYTM PRACY KOMPONENTU

Ochrona plików jest uruchamiana podczas startu systemu operacyjnego, rezyduje w pamięci operacyjnej komputera i skanuje wszystkie otwierane, modyfikowane oraz zapisywane obiekty.

Domyślnie Ochrona plików skanuje tylko nowe lub zmienione pliki, czyli te, które zostały dodane lub zmodyfikowane od momentu ostatniego skanowania. Proces skanowania pliku odbywa się zgodnie z następującym algorytmem:

1. Komponent przechwytuje polecenie żądanie użytkownika lub innej aplikacji względem pliku.
2. Ochrona plików szuka informacji o przechwyconym pliku w bazach iChecker i iSwift i na podstawie otrzymanych informacji podejmuje decyzje o konieczności skanowania pliku.

Podczas skanowania wykonywane są następujące:

1. Plik jest analizowany w poszukiwaniu szkodliwego kodu. Identyfikacja niebezpiecznych programów jest przeprowadzana w oparciu o bazy Kaspersky Internet Security, które zawierają opisy wszystkich znanych na chwilę bieżącą szkodliwych programów i zagrożeń sieciowych. W bazach programu zapisane są także metody likwidacji zagrożeń.
2. Na podstawie rezultatów analizy możliwe są następujące warianty działania Kaspersky Internet Security:
 - a. Jeżeli w pliku został zidentyfikowany szkodliwy kod, Ochrona plików blokuje go, tworzy kopię zapasową i próbuje przeprowadzić leczenie. Po pomyślnym wyleczeniu plik może być wykorzystywany w dalszej pracy. Jeżeli leczenie nie powiedzie się, plik jest usuwany.
 - b. Jeżeli w pliku został znaleziony kod podobny do szkodliwego (nie można w stu procentach potwierdzić jego szkodliwości), obiekt trafia do kwarantanny.
 - c. Jeśli w pliku nie znaleziono szkodliwego kodu, plik od razu może być wykorzystywany w dalszej pracy.

W przypadku wykrycia zainfekowanego lub podejrzanego obiektu aplikacja wyświetli odpowiedni komunikat. Na ekranie pojawi się powiadomienie z zapytaniem odnośnie dalszych czynności. Program zaproponuje:

- Umieszczenie zagrożenia w kwarantannie w celu późniejszego przeskanowania z użyciem uaktualnionych baz;
- Usunięcie obiektu;
- Odroczenie działania (jeżeli nie masz pewności, czy obiekt jest niebezpieczny).

OCHRONA POCZTY

Ochrona poczty skanuje przychodzące i wychodzące wiadomości e-mail w poszukiwaniu niebezpiecznych obiektów. Moduł jest uruchamiany podczas startu systemu operacyjnego, znajduje się stale w pamięci operacyjnej komputera i skanuje wszystkie wiadomości przesyłane za pośrednictwem protokołów POP3, SMTP, IMAP, MAPI oraz NNTP.

Podczas skanowania poczty wykorzystywany jest zbiór parametrów nazywany poziomem ochrony. W przypadku wykrycia zagrożeń Ochrona poczty wykonuje określone działanie. Reguły, według których przeprowadzane jest sprawdzanie poczty są określone za pomocą parametrów, które odpowiadają za:


- ochronę wiadomości;
- użycie metod analizy heurystycznej;
- skanowanie plików złożonych;
- filtrowanie załączonych plików.

Specjaliści z Kaspersky Lab nie zalecają samodzielnego ustawiania parametrów pracy Ochrony poczty. W większości przypadków wystarczająca jest zmiana poziomu ochrony. W każdej chwili możesz przywrócić domyślne parametry pracy Ochrony poczty.

- W celu zmiany parametrów pracy Ochrony poczty wykonaj następujące czynności:
1. Otwórz okno główne aplikacji i kliknij odnośnik **Ustawienia** w górnej części okna.
 2. W oknie, które pojawi się na ekranie, w sekcji **Ochrona** wybierz komponent **Ochrona poczty**.
 3. Kliknij przycisk **Ustawienia** dla wybranego komponentu.
 4. Wprowadź żądane zmiany w parametrach komponentu.

ALGORYTM PRACY KOMPONENTU

W skład aplikacji Kaspersky Internet Security wchodzi komponent umożliwiający skanowanie poczty w poszukiwaniu niebezpiecznych obiektów – *Ochrona poczty*. Jest on uruchamiany podczas startu systemu operacyjnego, znajduje się stale w pamięci operacyjnej komputera i skanuje wszystkie wiadomości pocztowe przesyłane za pośrednictwem protokołów POP3, SMTP, IMAP, MAPI oraz NNTP. Skanowane są także chronione połączenia (SSL) w protokołach POP3 i IMAP.

Podczas pracy komponentu ikona programu Kaspersky Internet Security, znajdująca się w zasobniku systemowym, przybiera następującą postać .

Domyślnie ochrona poczty działa według następującego algorytmu:

1. Każda przychodząca lub wychodząca wiadomość jest przechwytywana przez komponent.
2. Następuje analiza poszczególnych elementów wiadomości: tytuł, treść, załączniki.
3. Treść i załączniki wiadomości (w tym także załączone obiekty OLE) są sprawdzane w poszukiwaniu niebezpiecznych obiektów). Szkodliwe obiekty rozpoznawane są na podstawie baz programu Kaspersky Internet Security, a także przy użyciu algorytmu heurystycznego. Bazy zawierają opisy wszystkich znanych na chwilę bieżącą szkodliwych programów i zagrożeń sieciowych a także metody ich likwidacji. Algorytm heurystyczny pozwala wykrywać nowe zagrożenia, które nie zostały jeszcze dodane do baz.

4. Na podstawie rezultatów analizy możliwe są następujące warianty działania Kaspersky Internet Security:
- Jeśli treść lub załącznik wiadomości zawiera szkodliwy kod, Ochrona poczty blokuje ją, tworzy kopię zapasową i próbuje unieszkodliwić obiekt. W wyniku pomyślnego leczenia wiadomość staje się dostępna dla użytkownika. Jeśli nie udało się przeprowadzić skutecznego leczenia, zarażony obiekt zostaje usunięty z wiadomości. W wyniku analizy antywirusowej w temacie wiadomości pojawia specjalny tekst informujący o tym, że wiadomość została sprawdzona przez Kaspersky Internet Security.
 - Jeśli treść lub załącznik wiadomości zawiera kod podobny do szkodliwego (nie można w stu procentach potwierdzić jego szkodliwości), podejrzany obiekt trafia do kwarantanny.
 - Jeśli w wiadomości nie wykryto szkodliwego kodu, staje się ona od razu dostępną dla użytkownika.

Dla programu Microsoft Office Outlook dostępna jest specjalna wtyczka pozwalająca na precyzyjniejsze skonfigurowanie ochrony poczty.

Jeżeli korzystasz z programu pocztowego The Bat!, Kaspersky Internet Security może być wykorzystywany jednocześnie z innymi programami antywirusowymi dla programu TheBat!. Ustawienia analizy ruchu pocztowego są konfigurowane bezpośrednio w programie The Bat! i nadpisują ustawienia ochrony poczty zdefiniowane w ustawieniach Kaspersky Internet Security.

Podczas pracy z pozostałymi aplikacjami pocztowymi (w tym Microsoft Outlook Express, Poczta systemu Windows, Mozilla Thunderbird, Eudora, Incredimail) Ochrona poczty skanuje wiadomości przesyłane za pośrednictwem protokołów SMTP, POP3, IMAP oraz NNTP.

Ważne!

Podczas pracy z klientem pocztowym Thunderbird nie są sprawdzane wiadomości przesyłane za pośrednictwem protokołu IMAP w przypadku, jeśli wykorzystywane są filtry przenoszące wiadomości z folderu **Odebrane**.

OCHRONA RUCHU SIECIOWEGO

Podczas pracy w Internecie informacje znajdujące się na komputerze są narażone na zainfekowanie niebezpiecznymi programami. Zagrożenia takie mogą przeniknąć do Twojego komputera podczas pobierania darmowych

aplikacji lub przeglądania niepewnych stron WWW (które wcześniej zostały narażone na ataki hakerów). Ponadto robaki sieciowe mogą przeniknąć do Twojego komputera jeszcze przed otwarciem jakiegokolwiek strony WWW lub pobraniem pliku – bezpośrednio podczas nawiązywania połączenia z Internetem.

W celu zapewnienia bezpieczeństwa pracy w Internecie program Kaspersky Internet Security został wyposażony w komponent *Ochrona WWW*. Chroni on informacje przesyłane do komputera użytkownika przy użyciu protokołu HTTP, a także uniemożliwia instalację na komputerze niebezpiecznych skryptów.

Ochrona WWW analizuje ruch HTTP przesyłany tylko przez porty zdefiniowane na liście portów kontrolowanych. Lista portów najczęściej wykorzystywanych dla przepływu i ruchu HTTP wchodzi w skład Kaspersky Internet Security. Jeśli użytkownik korzysta z portów nieuwzględnionych w spisie w celu zapewnienia ochrony płynącego przez nie ruchu należy dodać je do listy.

Jeśli użytkownik znajduje się niebezpiecznym środowisku podczas pracy w Internecie zaleca się wykorzystanie Ochrony WWW. Jeśli komputer użytkownika znajduje się w Sieci chronionej zaporą sieciową lub filtrami ruchu HTTP moduł Ochrona WWW zapewni mu dodatkową ochronę.

Skanowanie ruchu jest wykonywane z użyciem określonych parametrów zwanych poziomem bezpieczeństwa. Przy wykryciu zagrożenia Ochrona WWW wykonuje określone działanie.

Parametry te można podzielić na następujące grupy:

- parametry definiujące zakres ochrony;
- parametry określające wydajność ochrony ruchu (wykorzystanie analizy heurystycznej, optymalizacja skanowania).

Specjaliści Kaspersky Lab nie zalecają samodzielnego ustawiania parametrów pracy modułu Ochrony WWW. W większości przypadków wystarczy wybrać inny poziom bezpieczeństwa.

► *Aby zmienić parametry pracy Ochrony WWW wykonaj następujące czynności:*

1. Otwórz okno główne aplikacji programu i w górnej części okna kliknij odsyłacz **Ustawienia**.
2. W otwartym oknie z sekcji **Ochrona** wybierz komponent **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** dla tego komponentu.

4. Wprowadź wymagane zmiany w ustawieniach.

ALGORYTMY PRACY KOMPONENTU

Moduł *Ochrona WWW* chroni informacje przesyłane przy użyciu protokołu HTTP i zapobiega instalacji na komputerze niebezpiecznych skryptów.

Przeanalizujemy dokładnie schemat pracy modułu. Ochrona ruchu HTTP zachodzi według następującego algorytmu:

1. Każda strona WWW lub plik, do którego użytkownik lub aplikacja próbuje uzyskać dostęp z wykorzystaniem protokołu HTTP, jest przechwytywany i analizowany przez moduł ochrony WWW w poszukiwaniu wirusów. Identyfikacja niebezpiecznych obiektów jest wykonywana w oparciu o bazy danych sygnatur zagrożeń oraz z użyciem algorytmu heurystycznego. Bazy danych zawierają sygnatury wszystkich obecnie znanych szkodliwych programów i sposoby ich usuwania. Analiza heurystyczna pozwala znajdować nowe wirusy. Które nie zostały jeszcze sklasyfikowane w bazach danych.
2. Po zakończeniu analizy możliwe są następujące scenariusze akcji:
 - Jeżeli strona WWW lub obiekt, do którego próbujesz otworzyć zawierają szkodliwy kod, dostęp do nich zostanie zablokowany. Dodatkowo na ekranie wyświetlone zostanie powiadomienie o tym, że dany obiekt lub strona są zainfekowane.
 - Jeśli plik lub strona internetowa nie zawierają szkodliwego kodu, będziesz mógł uzyskać do nich dostęp.

Skanowanie skryptów wykonywane jest według następującego algorytmu:

1. Każdy znajdujący się na stronie internetowej skrypt jest przechwytywany przez moduł ochrony WWW i analizowany w poszukiwaniu szkodliwego kodu.
2. Jeżeli skrypt zawiera szkodliwego kodu, Ochrona WWW blokuje go, i informuje o tym użytkownika przy użyciu pomocą specjalnej wiadomości wyświetlanej na ekranie.
3. Jeżeli skrypt nie zawiera szkodliwego kodu, zostanie on uruchomiony.

Skrypty są przechwytywane tylko na stronach internetowych, otwieranych za pomocą Microsoft Internet Explorer.

OCHRONA RUCHU KOMUNIKATORÓW INTERNETOWYCH

Duża popularność w ostatnim czasie programów szybkiej wymiany informacji – komunikatorów internetowych, obok wygody pracy w Internecie stworzyła potencjalne zagrożenie bezpieczeństwa komputera. Za pośrednictwem komunikatorów internetowych mogą zostać przekazane wiadomości, zawierające odsyłacze do podejrzanych stron, a także stron stworzonych przez cyberprzestępców w celu przeprowadzania ataków phishingowych. Złośliwe programy wykorzystują komunikatory internetowe do rozsyłania spamu lub odsyłaczy do programów (lub samych programów), które kradną loginy i hasła użytkowników.

Do zapewnienia bezpieczeństwa pracy z komunikatorami internetowymi przeznaczony jest komponent Ochrona komunikatorów. Chroni on informacje przesyłane na komputer użytkownika protokołami komunikatorów internetowych.

Produkt zapewnia bezpieczną pracę z wieloma komunikatorami, na przykład ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent i IRC.

Aplikacje Yahoo! Messenger i Google Talk wykorzystują protokół SSL. W celu kontrolowania ruchu tych aplikacji przez Ochronę komunikatorów, program musi użyć skanowania połączeń szyfrowanych. W tym celu należy zaznaczyć opcję

Skanuj połączenia szyfrowane znajdującą się sekcji **Sieć**.

Skanowanie ruchu jest wykonywane z wykorzystaniem określonego zbioru parametrów. W przypadku wykrycia zagrożeń w wiadomości Ochrona komunikatorów zamienia tę wiadomość na ostrzeżenie dla użytkownika.

Poziom ochrony ruchu komunikatorów internetowych na komputerze użytkownika jest określany przez zbiór parametrów. Parametry te można podzielić na następujące grupy:

- Parametry tworzące chroniony obszar;
 - Parametry określające metody skanowania;
- ▶ *W celu zmiany parametrów pracy Ochrony komunikatorów wykonaj następujące czynności:*
1. Otwórz okno główne programu i kliknij odsyłacz **Ustawienia** znajdujący się w górnej części okna.

2. W otwartym oknie w sekcji **Ochrona** wybierz komponent **Ochrona komunikatorów**.
3. Wprowadź żądane zmiany w ustawieniach komponentu.

ALGORYTM PRACY KOMPONENTU

W skład Kaspersky Internet Security wchodzi komponent Ochrona komunikatorów zapewniający skanowanie wiadomości przesyłanych za pomocą komunikatorów internetowych w poszukiwaniu niebezpiecznych obiektów. Jest on uruchamiany podczas ładowania systemu operacyjnego, rezyduje w pamięci operacyjnej komputera i skanuje wszystkie odbierane i wysyłane wiadomości.

Domyślna ochrona ruchu komunikatorów internetowych wykonywana jest według następującego algorytmu:

1. Komponent przechwytuje każdą odbieraną lub wysyłaną wiadomość.
2. Ochrona komunikatorów skanuje wiadomość w poszukiwaniu niebezpiecznych obiektów lub odsyłaczy. Odsyłacza porównywane są z bazą danych podejrzanych adresów internetowych, lub adresów odsyłających do stron phishingowych. W przypadku wykrycia zagrożenia tekst wiadomości jest zamieniany na ostrzeżenie dla użytkownika.
3. Jeżeli w wiadomości nie znaleziono zagrożeń, będziesz mógł przeczytać jej treść.

Pliki przekazywane za pośrednictwem komunikatorów internetowych są skanowane przez moduł Ochrona plików (patrz sekcja Ochrona systemu plików na stronie 49) w momencie próby ich zapisania.

KONTROLA APLIKACJI

Wszystkie programy można rozdzielić na trzy grupy biorąc pod uwagę kryterium bezpieczeństwa systemu:

- *Bezpieczne*. Do tej grupy należą programy opracowane przez znanych producentów i zaopatrzone w podpis cyfrowy. Programy te mogą wykonywać dowolne działania w systemie.

- *Niebezpieczne.* Do tej grupy należą znane na chwilę obecną zagrożenia. Konieczna jest blokada takich aplikacji.
- *Nieznane.* Do tej grupy należą programy, nie posiadające podpisu cyfrowego. Najczęściej nie są one niebezpieczne dla systemu, ale decyzję o bezpiecznym korzystaniu z tych programów można podjąć dopiero po przeprowadzeniu analizy ich zachowania. Dobrym rozwiązaniem jest ograniczenie dostępu tych programów do zasobów systemu.

Komponent Kontrola aplikacji rejestruje działania różnych aplikacji w systemie i zarządza ich działaniem biorąc pod uwagę przynależność do konkretnej grupy. Każdej grupie programów przyporządkowany jest zbiór reguł. Reguły te regulują dostęp aplikacji do różnych zasobów:

- plików i folderów;
- kluczy rejestru;
- adresów sieciowych;
- środowiska uruchomieniowego.

Przy próbie skorzystania programu z zasobu, komponent sprawdza czy program posiada niezbędne prawa dostępu i wykonuje akcję zdefiniowaną przez reguły.

- ▶ *W celu zmiany parametrów pracy Kontroli aplikacji wykonaj następujące czynności:*
 1. Otwórz główne okno programu i kliknij odsyłacz **Ustawienia** znajdujący się w górnej części okna.
 2. W otwartym oknie w sekcji **Ochrona** wybierz komponent **Kontrola aplikacji**.
 3. Wprowadź żądane zmiany w ustawieniach.
- ▶ *Możesz także:*
 1. Otworzyć główne okno programu i wybrać sekcję **Bezpieczna strefa**.
 2. W prawej części okna kliknij odsyłacz **Aktywność aplikacji**.
 3. W otwartym oknie **Kontrola aktywności aplikacji** możesz dokonać żądanych zmian.

ALGORYTM PRACY KOMPONENTU

Przy pierwszym uruchomieniu aplikacji Kontrola aplikacji skanuje ją zgodnie z następującym algorytmem:

1. Przeprowadza skanowanie aplikacji w poszukiwaniu wirusów.
2. Sprawdza, czy aplikacja jest podpisana cyfrowo. Jeśli tak, zostaje przeniesiona do grupy **Zaufane**. Jeśli aplikacja nie ma podpisu cyfrowego (lub jeśli podpis cyfrowy jest uszkodzony lub znajduje się na „czarnej liście”), komponent przechodzi do następnego kroku.
3. Szuka uruchamianej aplikacji w wewnętrznej bazie znanych programów wchodzącej w skład Kaspersky Internet Security. Jeżeli w bazie istnieje informacja o uruchamianej aplikacji, zostaje ona przeniesiona do odpowiedniej grupy. Jeżeli informacji o danym programie nie ma w bazie, komponent przechodzi do następnej czynności.
4. Wysyła informację o pliku wykonywalnym aplikacji do bazy znanych programów, znajdującej się na serwerze Kaspersky Lab. Jeżeli w bazie istnieje zapis odnośnie danej aplikacji, zostaje ona przyporządkowana do odpowiedniej grupy. Jeżeli nie udało się nawiązać połączenia z bazą (np. komputer nie jest podłączony do Internetu), komponent przechodzi do następnej czynności.
5. Generuje współczynnik zagrożenia ze strony programu za pomocą analizy heurystycznej. Programy posiadające niską wartość klasyfikatora zostają przyporządkowane do grupy Niskie ograniczenia. Jeżeli wartość klasyfikatora programu jest wysoka, Kaspersky Internet Security powiadomi o tym użytkownika i zaleci wybór grupy, do której aplikacja zostanie przyporządkowana.

Po wykonaniu skanowania na ekranie pojawi się powiadomienie o rozwiązaniu zastosowanym odnośnie programu. Powiadomianie jest domyślnie wyłączone.

Przy powtórnym uruchomieniu programu Kontrola aplikacji sprawdza jej integralność. Jeżeli aplikacja nie została zmodyfikowana, komponent zastosuje dla niej istniejącą regułę. Jeżeli program został zmodyfikowany, Kontrola aplikacji przeanalizuje go zgodnie z powyższym algorytmem.

BEZPIECZNE ŚRODOWISKO DLA URUCHAMIANIA PROGRAMÓW

Dla komputerów pracujących na Microsoft Windows XP x64 bezpieczne środowisko wykonawcze programów nie jest dostępne.

W celu zapewnienia maksymalnego bezpieczeństwa obiektów systemu operacyjnego i danych osobowych użytkownika specjaliści Kaspersky Lab zalecają uruchamianie podejrzanych programów w chronionym bezpiecznym środowisku wirtualnym – Bezpiecznym środowisku.

W Bezpiecznym środowisku zaleca się uruchamianie programów, w przypadku których pochodzenie nie jest znane. Pozwoli to na uniknięcie zmian obiektów systemu operacyjnego, które mogą doprowadzić do jego niestabilnej pracy lub uszkodzenia.

W przypadku komputerów pracujących na Microsoft Windows Vista x64 i Microsoft Windows 7 x64 funkcje niektórych programów uruchamianych w Bezpiecznym środowisku są ograniczone. Jeżeli włączone zostało powiadomienie **W trybie bezpiecznym funkcjonalność aplikacji jest ograniczona**, podczas uruchamiania takich programów na ekranie pojawi się odpowiednie ostrzeżenie.

Uruchomienie przeglądarek internetowych w Bezpiecznym środowisku umożliwia bezpieczne przeglądanie zasobów internetowych, w tym także ochronę przed wniknięciem do komputera złośliwych programów i ochronę danych użytkownika przed niekontrolowanymi zmianami i usunięciem, a także możliwość usunięcia wszystkich obiektów nagromadzonych podczas pracy w Internecie: pliki tymczasowe, ciasteczka, historia itp. Microsoft Internet Explorer znajduje się na liście programów, które są domyślnie uruchamiane w Bezpiecznym środowisku.

Aplikacja jest uruchamiana w Bezpiecznym środowisku zgodnie z wybranym trybem pracy. Dla szybkiego uruchomienia aplikacji w Bezpiecznym środowisku przewidziana jest możliwość tworzenia skrótów.

Aby w czasie pracy w normalnym środowisku dostępne były pliki zapisane lub zmienione w Bezpiecznym środowisku, konieczne jest wykorzystanie specjalnie stworzonego w tym celu folderu współdzielonego Bezpiecznego środowiska. Pliki, które zostaną zapisane w tym folderze podczas oczyszczania Bezpiecznego środowiska nie zostaną usunięte.

Instalację aplikacji, z którymi następnie użytkownik planuje pracować w Bezpiecznym środowisku zaleca się przeprowadzać w normalnym środowisku Microsoft Windows.

ZAPORA SIECIOWA

Zapora sieciowa to komponent umożliwiający bezpieczną pracę w sieci lokalnej i Internecie. Filtruje on aktywność sieciową według dwóch rodzajów reguł: *reguła dla aplikacji i reguła dla pakietów*.

Zapora sieciowa analizuje parametry sieci, z którą komputer jest połączony. Jeżeli aplikacja pracuje w trybie interaktywnym, podczas pierwszego połączenia z daną siecią Zapora sieciowa wyświetli żądanie o wybór stanu sieci. W trybie automatycznym Zapora sieciowa określa stan na podstawie typu sieci, zakresu adresów IP i innych danych. W zależności od stanu sieci zapora wykorzystuje różne reguły filtrowania aktywności sieciowej.

- ▶ *W celu zmiany ustawień Zapory sieciowej wykonaj następujące czynności:*
 1. Otwórz okno główne programu i kliknij odsyłacz **Ustawienia** w górnej części okna.
 2. W otwartym oknie w sekcji **Ochrona** wybierz komponent **Zapora sieciowa**.
 3. Kliknij przycisk **Ustawienia**.
 4. Parametry pracy Zapory sieciowej możesz zmienić na zakładkach **Reguły filtrowania** oraz **Sieci**.

OCHRONA PROAKTYWNA

Kaspersky Internet Security chroni komputer użytkownika nie tylko przed znanymi zagrożeniami, ale również przed nieznanymi, które nie zostały jeszcze sklasyfikowane bazach danych Kaspersky Internet Security. Do tego celu służy specjalnie opracowany komponent – *Ochrona proaktywna*.

Technologie prewencyjne, na których oparta jest Ochrona proaktywna, pozwalają zaoszczędzić czas i zablokować zagrożenie zanim wyrządzi szkody w

systemie. W odróżnieniu od technologii reaktywnych, dokonujących analizy na podstawie sygnatur z baz danych Kaspersky Internet Security, technologie prewencyjne identyfikują nowe zagrożenie na komputerze użytkownika na podstawie szeregu działań wykonywanych przez analizowany program. Jeżeli w wyniku analizy aktywności okaże się, że czynności aplikacji budzą podejrzenia, Kaspersky Internet Security blokuje aktywność tej aplikacji.

Analiza aktywności jest prowadzona względem wszystkich programów, w tym także względem tych, które zostały przyporządkowane przez Kontrolę aplikacji do grupy **Zaufane** (patrz strona 57). Dla programów tego typu użytkownik może wyłączyć komunikaty ochrony proaktywnej.

W odróżnieniu od komponentu Kontrola aplikacji, Ochrona proaktywna reaguje na określony ciąg czynności aplikacji.

- ▶ *W celu zmiany parametrów pracy Ochrony proaktywnej wykonaj następujące czynności:*
 1. Otwórz okno główne aplikacji i kliknij odsyłacz **Ustawienia** w górnej części okna.
 2. W otwartym oknie w sekcji **Ochrona** wybierz komponent **Ochrona proaktywna**.
 3. Wprowadzić żądane zmiany w ustawieniach.

OCHRONA PRZED ATAKAMI SIECIOWYMI

Ochrona przed atakami sieciowymi uruchamiana jest podczas startu systemu operacyjnego i analizuje przychodzący ruch sieciowy w poszukiwaniu prób ataków sieciowych. Jeżeli Kaspersky Internet Security zidentyfikuje próbę ataku na komputer użytkownika blokuje aktywność sieciową komputera atakującego. Domyślnie atakujący komputer blokowany jest przez godzinę. Na ekranie pojawia się komunikat (patrz sekcja Powiadomienia na stronie 76) o próbie ataku sieciowego wraz ze podaniem informacji o komputerze atakującym.

Charakterystyka znanych na chwilę obecną ataków sieciowych i metody walki z nimi znajduje się w bazach danych Kaspersky Internet Security. Lista ataków, wykrywanych przez Ochronę przed atakami sieciowymi, jest uzupełniana podczas aktualizacji (patrz sekcja Aktualizacja na stronie 72) baz danych.

ANTI-SPAM

Kaspersky Internet Security zawiera komponent *Anti-Spam* umożliwiający wykrywanie niechcianych wiadomości pocztowych (spamu) i ich przetwarzanie zgodnie z regułami klienta pocztowego. Działania te pozwalają na znaczne zaoszczędzenie czasu podczas pracy z pocztą elektroniczną.

Anti-Spam korzysta z samouczącego się algorytmu (patrz sekcja Algorytm pracy komponentu na stronie 64), pozwalającemu komponentowi wraz z upływem czasu bardziej efektywnie odróżniać spam od czystych wiadomości. Aby Anti-Spam efektywnie rozpoznawał spam i zwykłą pocztę należy go nauczyć.

Zalecane jest przeprowadzenie procesu uczenia algorytmu komponentu Anti-Spam.

Anti-Spam jako moduł rozszerzenia (wtyczka) przeznaczony jest dla następujących klientów pocztowych:

- Microsoft Office Outlook;
- Microsoft Outlook Express (Windows Mail);
- The Bat!;
- Thunderbird.

Poprzez tworzenie list dozwolonych i zabronionych nadawców użytkownik może wskazać komponentowi, z których adresów dostarczane są czyste wiadomości, a z których spam. Ponadto Anti-Spam może analizować wiadomości w poszukiwaniu fraz znajdujących się na listach zwrotów dozwolonych i zabronionych lub wyrażen niecenzuralnych.

Anti-Spam pozwala na przeglądanie poczty na serwerze i usuwanie niepotrzebnych wiadomości bez konieczności ich pobierania na komputer.

- *W celu zmiany parametrów pracy modułu Anti-Spam wykonaj następujące czynności:*
1. Otwórz główne okno aplikacji i kliknij odnośnik **Ustawienia** w górnej części okna.
 2. W otworzonym oknie w sekcji **Ochrona** wybrać komponent **Anti-Spam**.
 3. Kliknij przycisk **Ustawienia** dla wybranego komponentu.

4. Wprowadź żądane zmiany w ustawieniach komponentu.

ALGORYTM PRACY KOMPONENTU

Skanowanie wiadomości przez komponent Anti-Spam dzieli się na dwa etapy:

1. Użycie stałych kryteriów filtrowania. Kryteria te pozwolą szybko określić czy wiadomość jest spamem. Anti-Spam nadaje wiadomości status *spam* lub *czysta wiadomość* i kończy skanowanie, a wiadomość zostaje przekazana do klienta pocztowego (patrz poniżej kroki 1 – 5).
2. Analiza wiadomości, które spełniły szczegółowe kryteria w poprzednich krokach. Wiadomości takie nie mogą być jednoznacznie potraktowane jako spam. Dlatego też Anti-Spam musi określić *prawdopodobieństwo* oznaczenia ich jako spam.

Algorytm pracy Anti-Spamu:

1. Sprawdzanie czy adres nadawcy nie znajduje się na liście dozwolonych zabronionych nadawców.
 - Jeżeli adres nadawcy znajduje się na liście dozwolonych nadawców, wiadomość otrzymuje status *czysta wiadomość*.
 - Jeżeli adres nadawcy znajduje się na liście zabronionych nadawców, wiadomość otrzymuje status *spam*.
2. Jeżeli wiadomość została wysłana przy pomocy Microsoft Exchange Server, a skanowanie takich wiadomości jest wyłączone to wiadomość zyskuje status *czysta wiadomość*.
3. Wiadomość jest analizowana w poszukiwaniu zwrotów należących do listy dozwolonych fraz. Jeżeli zostanie znaleziona, przynajmniej jedna fraza należąca do tej listy, to wiadomość otrzymuje status *czysta wiadomość*. Domyślnie krok ten jest pomijany.
4. Wiadomość jest analizowana w poszukiwaniu zabronionych fraz. Zidentyfikowanie w wiadomości słów z listy zabronionych fraz zwiększa prawdopodobieństwo zaklasyfikowania wiadomości jako spam. Jeżeli szacowane prawdopodobieństwo przewyższy określoną wartość wiadomość otrzymuje status *spam* lub *potencjalny spam*. Wiadomość jest analizowana także w poszukiwaniu wierszy należących do listy fraz niecenzuralnych. Domyślnie krok ten jest pomijany.

5. Jeżeli treść wiadomości zawiera adres znajdujący się w bazie danych adresów phishingowych lub podejrzanych adresów internetowych wiadomość otrzymuje status *spam*.
6. Analiza wiadomości pocztowych jest prowadzona także przy pomocy reguł heurystycznych. Jeżeli w wyniku tej analizy okaże się, że wiadomość zawiera cechy charakterystyczne dla spamu, zwiększa się prawdopodobieństwo zaklasyfikowania wiadomości jako spam.
7. Prowadzona jest analiza wiadomości przy pomocy technologii GSG. Anti-Spam analizuje przy tym obrazy wchodzące w skład wiadomości pocztowej. Jeżeli znalezione zostaną w nich cechy charakterystyczne dla spamu zwiększy się prawdopodobieństwo uznania wiadomości za spam.
8. Prowadzona jest analiza załączników wiadomości w formacie .rtf. Anti-Spam szuka w załączonych dokumentach cech charakterystycznych dla spamu. Po zakończeniu analizy Anti-Spam szacuje o ile zwiększyło się prawdopodobieństwo tego, że wiadomość jest spamem. Domyślnie technologia ta jest wyłączona.
9. Dokonywane jest także skanowanie poszukiwaniu obecności innych cech charakterystycznych dla spamu. Odnalezienie każdej z tych cech zwiększa prawdopodobieństwo zaklasyfikowania wiadomości jako spam.
10. Jeżeli przeprowadzony został proces uczenia Anti-Spamu, wiadomość jest sprawdzana przy pomocy technologii iBayes. Samouczący się algorytm iBayes oblicza prawdopodobieństwo uznania wiadomości jako spam na podstawie częstotliwości w jej tekście zwrotów charakterystycznych dla spamu.

W wyniku analizy wiadomości program określa prawdopodobieństwo uznania jej jako spam. Twórcy spamu sukcesywnie udoskonalają techniki jego maskowania. Dlatego też najczęściej obliczone prawdopodobieństwo nie osiąga określonej wartości. W celu efektywnego filtrowania wiadomości Anti-Spam wykorzystuje dwa parametry:

- *Klasyfikator spamu* – wartość prawdopodobieństwa, której przekroczenie klasyfikuje wiadomość jako spam. Jeżeli prawdopodobieństwo jest mniejsze od danej wartości, to Anti-Spam nadaje wiadomości status *potencjalny spam*;
- *Klasyfikator podejrzania obecności spamu* – wartość prawdopodobieństwa, którego przekroczenie klasyfikuje wiadomość jako potencjalny spam. Jeżeli prawdopodobieństwo jest mniejsze od tej wartości, to Anti-Spam uznaje wiadomość jako czystą.

W zależności od wyznaczonych wartości czynników spamu i potencjalnego spamu wiadomości otrzymują status spam lub potencjalny spam. Oprócz tego domyślnie wiadomościom przyporządkowana jest etykieta **[!! SPAM]** lub **[!! Probable Spam]** w polu **Temat** odpowiednio do nadanego statusu. Następnie wiadomości są przetwarzane zgodnie z regułami określonymi przez użytkownika w ustawieniach klienta pocztowego.

BLOKOWANIE BANERÓW

Blokowanie banerów blokuje reklamy wyświetlane w postaci banerów, wbudowanych do interfejsu programów zainstalowanym na Twoim komputerze oraz wyświetlanych na stronach internetowych.

Banery reklamowe nie tylko nie zawierają pożytecznych informacji, ale dekoncentrują użytkownika i spowalniają ruch sieciowy. Ten komponent blokuje najbardziej popularne banery. Maski ich adresów znajdują się w bazach danych Kaspersky Internet Security. Możesz wyłączyć blokowanie banerów lub stworzyć własne listy dozwolonych lub zabronionych banerów.

Lista masek najbardziej popularnych banerów reklamowych została stworzona przez specjalistów z Kaspersky Lab i dodana do baz danych Kaspersky Internet Security. Jeżeli blokowanie banerów nie zostało wyłączone, banery spełniające maski z tej listy będą blokowane. W celu zablokowania banerów, których maski nie znajdują się w bazach danych, wykorzystywany jest analizator heurystyczny.

Oprócz tego użytkownik może stworzyć „białą” i „czarną” listę banerów, na podstawie której zostanie dozwolone lub zabronione wyświetlanie banerów.

Domyślnie po zainstalowaniu Kaspersky Internet Security komponent Blokowanie banerów jest wyłączony.

- ▶ *W celu zmiany parametrów pracy komponenty Blokowanie banerów wykonaj następujące czynności:*
 1. Otwórz okno główne programu i kliknij odsyłacz **Ustawienia** znajdujący się w górnej części okna.
 2. W otwartym oknie w sekcji **Ochrona** wybierz komponent **Blokowanie banerów**.
 3. Wprowadź żądane zmiany.

KONTROLA RODZICIELSKA

Kontrola rodzicielska – jest to komponent aplikacji kontrolujący dostęp użytkowników do zasobów internetowych. Głównym zadaniem kontroli rodzicielskiej jest ograniczenie dostępu do następujących zasobów:

- Stron internetowych przeznaczonych dla dorosłych prezentujących pornografię, przemoc, narkotyki, przemoc itd.;
- Stron internetowych, stanowiących potencjalną przyczynę strat czasu (czaty, gry on-line), lub pieniędzy (sklepy internetowe, aukcje).

Często strony tego typu zawierają dużą ilość złośliwych programów. Pobieranie danych z tych zasobów (strony z grammi online) prowadzi do zwiększenia ilości ruchu sieciowego.

Ograniczenie dostępu użytkownika do zasobów internetowych jest realizowane poprzez przyznanie mu jednego z trzech profili do pracy w Internecie. Dla każdego profilu można ustawić ograniczenia przeglądania i czasu przeglądania zasobów internetowych.

Domyślnie wszystkim użytkownikom przyznawany jest profil **Dziecko**, posiadający maksymalny poziom ograniczeń. Profil można połączyć z nazwami użytkowników systemu Microsoft Windows. W tym przypadku użytkownik otrzymuje dostęp do zasobów internetowych zgodnie z parametrami swojego profilu.

Dostęp do profilu **Rodzic** lub **Nastolatek** należy chronić hasłem. Przełączenie na profil chroniony hasłem jest możliwy dopiero po wprowadzeniu hasła.

Każdy profil reguluje dostęp do stron internetowych w oparciu o jeden z poziomów ograniczeń. Poziom ograniczenia to zestaw parametrów weryfikujących dostęp do danego zasobu.

Zaleca się ochronę Kaspersky Internet Security hasłem w celu uniknięcia niekontrolowanego wyłączenia komponentu.

Po instalacji Kaspersky Internet Security Kontrola rodzicielska jest wyłączona.

- ▶ *W celu zmiany parametrów pracy Kontroli rodzicielskiej wykonaj następujące czynności:*

1. Otwórz okno główne programu i kliknij odsyłacz **Ustawienia** znajdujący się w górnej części okna.

2. W otwartym oknie sekcji **Ochrona** wybierz komponent **Kontrola rodzicielska**.
3. Kliknij przycisk **Ustawienia** dla wybranego komponentu.
4. Wprowadź żądane zmiany.

ALGORYTM PRACY KOMPONENTU

Przeanalizujmy ogólny algorytm działania komponentu **Kontrola rodzicielska**:

1. Po autoryzacji użytkownika w trakcie uruchamiania systemu ładowany jest profil odpowiadający mu profil.
2. Podczas próby otwarcia strony internetowej przez użytkownika Kontrola rodzicielska wykonuje następujące czynności:
 - sprawdza ograniczenia czasu spędzanego online;
 - jeżeli aktywny jest tryb uzyskiwania dostępu tylko do wybranych stron, sprawdza czy wprowadzony adres znajduje się na liście z dozwolonych adresów internetowych;
 - jeżeli aktywny jest tryb z ograniczeniami komponent wykonuje następujące czynności:
 - sprawdza czy wprowadzony adres znajduje się na liście z dozwolonych lub zablokowanych adresów internetowych;
 - analizuje zawartość strony w celu sprawdzenia, czy strona nie należy do jednej z zabronionych kategorii.

Jeżeli chociaż jeden z tych warunków nie zostanie spełniony, dostęp do strony internetowej będzie zablokowany. W przeciwnym przypadku strona internetowa zostanie otwarta.

Jeżeli w sieci użytkownika wykorzystywany jest serwer proxy wykorzystujący niestandardowy numer portu, to należy dodać ten port do listy portów monitorowanych. W innym przypadku kontrola rodzicielska może pracować niepoprawnie i pomijać zabronione strony Internetowe.

Jeśli po zakończeniu skanowania otwierana strona internetowa jest określona jako zabroniona to dostęp do niej jest blokowany. W przeciwnym razie strona internetowa jest otwierana w oknie przeglądarki.

SKANOWANIE KOMPUTERA

Skanowanie komputera w poszukiwaniu wirusów i luk jest jedną z ważniejszych czynności zapewniających bezpieczeństwo komputera. W wyniku skanowania komputera może zostać wykryty szkodliwy kod, który z jakiś powodów nie został wykryty przez ochronę w czasie rzeczywistym (znajdował się na dysku przed zainstalowaniem Kaspersky Internet Security). Skanowanie luk pozwala wykryć luki w oprogramowaniu, które mogą zostać wykorzystane przez cyberprzestępców w celu rozpowszechniania złośliwych obiektów i umożliwienia dostępu do Twoich osobistych danych.

Specjaliści Kaspersky Lab opracowali następujące zadania skanowania komputera:

- **Skanowanie obiektów.** Skanowanie obiektów, wybranych przez użytkownika. Możliwe jest skanowanie dowolnego obiektu systemu plików komputera. W ramach określonego zadania możliwe jest także ustawienie parametrów skanowania dysków wymiennych.
- **Pełne skanowanie.** Szczegółowe skanowanie całego systemu. Domyślnie skanowane są następujące obiekty: pamięć systemowa, pliki uruchamiane podczas ładowania systemu, pliki przywracania systemu, poczta, dyski twarde, wymienne i sieciowe.
- **Szybkie skanowanie.** Skanowanie obiektów uruchamianych podczas startu systemu.

Pełne i szybkie skanowanie należą do specyficznych zadań. Podczas ich wykonywania nie zaleca się dokonywania zmian na liście obiektów analizowanych przez te zadania.

Każde skanowanie dokonuje analizy określonego obszaru i może być uruchomione zgodnie z terminarzem. Zestaw parametrów skanowania na obecność wirusów określany jest jako poziom bezpieczeństwa. Domyślnie przewidziane są trzy poziomy.

Po uruchomieniu skanowania na obecność wirusów postęp jego wykonania przedstawiony jest w sekcji **Skanowanie** okna głównego Kaspersky Internet Security przy nazwie uruchomionego zadania. Po wykryciu zagrożenia program wykonuje odpowiednią akcję.

Podczas wyszukiwania zagrożeń informacja o jego wynikach jest zapisywana w raporcie Kaspersky Internet Security.

AKTUALIZACJA

Regularne wykonywanie aktualizacji zapewnia wysoki poziom ochrony komputera. Każdego dnia pojawiają się nowe wirusy, trojany i inne złośliwe programy. Informacje o zagrożeniach oraz sposobach ich neutralizacji znajdują się w bazach Kaspersky Internet Security, dlatego też bardzo ważnym elementem ochrony jest ich aktualizacja.

Komponent aktualizacji pobiera i instaluje na komputerze następujące obiekty:

- Bazy danych Kaspersky Internet Security.

Ochrona informacji wykorzystuje bazy danych zawierające sygnatury zagrożeń i ataków sieciowych a także metody ich wykrywania i neutralizacji. Co godzinę do baz danych dodawane są informacje o nowych zagrożeniach. Dlatego też zalecane jest regularne wykonywanie aktualizacji.

Razem z bazami Kaspersky Internet Security aktualizowane są również sterowniki sieciowe, umożliwiające przechwytywanie ruchu sieciowego przez komponenty ochrony.

- Moduły aplikacji.

Oprócz baz danych pobierane są także moduły Kaspersky Internet Security. Aktualizacje tego typu usuwają wykryte błędy w działaniu Kaspersky Internet Security, dodają nowe funkcje lub ulepszają już istniejące.

Serwery uaktualnień Kaspersky Lab są głównym źródłem aktualizacji dla programu Kaspersky Internet Security.

Do pobierania aktualizacji z serwerów Kaspersky Lab wymagane jest podłączenie komputera do Internetu. Domyślnie parametry połączenia z Internetem określone są automatycznie. Jeśli parametry serwera proxy nie zostaną wykryte automatycznie można je zdefiniować ręcznie.

Podczas aktualizacji moduły aplikacji oraz bazy danych znajdujące się na komputerze użytkownika porównywane ze znajdującymi się w źródle aktualizacji. Jeżeli na komputerze zainstalowana jest najnowsza wersja baz danych i modułów na ekranie zostanie wyświetlona informacja, że system ochrony komputera jest aktualny. W przeciwnym przypadku na komputerze zainstalowane zostaną brakujące uaktualnienia. Pobieranie tylko brakujących

danych pozwala na znaczne zmniejszenie ilości ruchu sieciowego i zwiększenie szybkości dostarczenia uaktualnień na komputery użytkowników.

Jeżeli bazy danych nie były aktualizowane przez dłuższy okres czasu, pakiet uaktualnień może posiadać duży rozmiar i obciążyć ruch sieciowy (do kilku MB).

Przed rozpoczęciem aktualizacji bazy danych Kaspersky Internet Security tworzy jej kopię zapasową na wypadek, jeżeli będziesz chciał wrócić do jej poprzedniej wersji.

Konieczne jest przywrócenie baz danych w przypadku, jeśli zostały one uaktualnione i podczas pracy zostały uszkodzone. Można wówczas wykorzystać ich poprzednią wersję, a następnie spróbować ponownie je uaktualnić.

Aktualizacje Kaspersky Internet Security możesz skopiować do lokalnego foldera. Opcja ta pozwala aktualizować bazy i moduły aplikacji na komputerach w sieci lokalnej, bez konieczności ich pobierania z serwerów internetowych Kaspersky Lab.

Możesz także włączyć tryb aktualizacji automatycznej. Funkcja ta jest domyślnie włączona.

W sekcji **Aktualizacja** głównego okna programu znajdują się informacje o bieżącym stanie baz danych Kaspersky Internet Security:

- data i czas opublikowania;
- ilość i rodzaje wpisów w bazach;
- status baz (aktualne, nieaktualne lub uszkodzone).

Możesz przeglądać raporty aktualizacji zawierające wszystkie informacje o zdarzeniach mających miejsce podczas procesu aktualizacji (odsylacz **Raport** w górnej części okna). Dodatkowym źródłem informacji o zagrożeniach jest raport o aktywności wirusów dostępny stronie www.kaspersky.pl, który zostanie wyświetlony po kliknięciu odsylacza **Informacje o aktywności wirusów**.

FUNKCJE DODATKOWE

Zapewnienie bezpieczeństwa komputerom nie jest łatwym zadaniem. Wymaga wiedzy o działaniu systemu operacyjnego i sposobach wykorzystania jego słabych punktów. Ponadto duża ilość i różnorodność informacji o bezpieczeństwie systemu utrudnia analizę i przetwarzanie zagrożeń.

W celu ułatwienia rozwiązywania specyficznych problemów w zakresie bezpieczeństwa komputera Kaspersky Internet Security zawiera wiele kreatorów i narzędzi:

- Klawiatura wirtualna uniemożliwia przechwytywanie danych wprowadzanych za pośrednictwem klawiatury.
- Kontrola rodzicielska, monitoruje dostęp użytkowników komputera do Internetu.
- Kreator tworzenia dysku ratunkowego przywracający działanie systemu po ataku wirusa, w przypadku uszkodzenia plików systemowych i braku możliwości jego normalnego uruchomienia.
- Kreator ustawień przeglądarki, wykonujący analizę ustawień przeglądarki Microsoft Internet Explorer w poszukiwaniu problemów związanych z bezpieczeństwem.
- Analizator pakietów sieciowych przechwytyjący pakiety sieciowe i wyświetlający szczegółowe informacje na ich temat.
- Kreator przywracania systemu eliminujący pozostałości szkodliwych obiektów w systemie.
- Kreator czyszczenia śladów aktywności wyszukujący i usuwający ślady aktywności użytkownika w systemie.

RAPORTY

Wynik działania każdego z komponentów aplikacji, skanowania w poszukiwaniu wirusów oraz aktualizacji jest zapisywane w raporcie.

Pracując z raportami możesz wykonywać następujące czynności:

- wybrać komponent lub zadanie, dla którego chcesz wyświetlić raport zdarzeń;
- zarządzać grupowaniem prezentacją danych na ekranie;
- utworzyć terminarz, zgodnie z którym będzie przypominał o przygotowanym raporcie;
- wybierać rodzaje zdarzeń, które będą zapisywane w raporcie;
- wybrać sposób prezentacji informacji statystycznych (tabela lub wykresy);
- zapisywać raport do pliku;
- filtrować zawartość raportu;
- wyszukiwać zdarzeń, które miały miejsce w systemie i zostały przetworzone przez aplikację.

POWIADOMIENIA

Jeżeli podczas działania aplikacji wystąpi zdarzenie, na ekranie wyświetlony zostanie specjalny komunikat. W zależności od wagi zdarzenia występują następujące rodzaje powiadomień:

- **Alarm.** Wystąpienie zdarzenia krytycznego. Na przykład wykrycie w systemie szkodliwego kodu lub niebezpiecznej aktywności. W takim przypadku musisz natychmiast zdecydować o działaniu, które zostanie wykonane przez program. Okno powiadomień tego typu wyświetlane jest w kolorze czerwonym.
- **Ostrzeżenie.** Wystąpiło potencjalne niebezpieczne zdarzenie. Na przykład, w systemie wykryto potencjalnie zainfekowane pliki lub podejrzaną aktywność. Musisz postępować zgodnie z zaobserwowanym poziomem zagrożenia. Okno takich powiadomień wyświetlane jest w kolorze żółtym.
- **Informacja.** To powiadomienie odnosi się do zdarzeń informacyjnych, które nie są krytyczne. Okno takich powiadomień wyświetlane jest w kolorze zielonym.

Okno powiadomienia składa się z czterech części:

1. *Nagłówek okna.* W nagłówku okna pojawia się krótki opis zdarzenia, na przykład: podejrzana aktywność, nowa sieć, alarm, wirus.
2. *Opis zdarzenia.* W tej części znajduje się dokładna informacja o przyczynie pojawienia się komunikatu: nazwa aplikacji, nazwa wykrytego zagrożenia, parametry zidentyfikowanego połączenia sieciowego i inne.
3. *Obszar wyboru czynności.* W tym miejscu użytkownik może wybrać jedną z możliwych czynności podejmowanych względem określonego zdarzenia. Zaproponowane warianty czynności zależą od typu zdarzenia, na przykład: **Leczyć**, **Usunąć**, **Pominąć** – w przypadku wykrycia wirusa, **Zezwolić**, **Zablokować** – w przypadku odpowiedzi programu na wykonywanie potencjalnie niebezpiecznych działań. Działanie zalecane przez specjalistów Kaspersky Lab wyróżnione jest pogrubioną czcionką.

W przypadku wyboru czynności **Zezwolić**, **Blokować** otworzone zostaje okno, w którym użytkownik może wybrać tryb zastosowanego

działania. Dla akcji **Zezwolić** możesz wybrać jeden z następujących trybów:

- **Zawsze zezwalaj**. Wybranie tego wariantu akcji spowoduje wprowadzenie zmian w regułach dostępu programu do zasobów systemowych.
- **Zezwól teraz**. Wariant ten należy wybrać, w celu zastosowania określonego działania względem wszystkich analogicznych zdarzeń, wykrytych w trakcie sesji działania aplikacji. Sesja działania aplikacji to czas od momentu jej uruchomienia do momentu jej zamknięcia lub ponownego uruchomienia.
- **Dodaj do zaufanych**. Wybranie tego wariantu akcji spowoduje dodanie aplikacji do grupy **Zaufane**.

Dla akcji **Blokuj** możesz wybrać jeden z następujących trybów:

- **Zawsze blokuj**. Wariant ten należy wybrać, w celu zablokowania wykrytej aktywności programu poprzez wprowadzenie zmian w regułach dostępu aplikacji do zasobów systemu.
 - **Blokuj teraz**. Wariant ten należy wybrać w celu zastosowania określonego działania względem wszystkich analogicznych zdarzeń, wykrytych w trakcie sesji działania aplikacji. Sesja działania aplikacji to czas od momentu jej uruchomienia do momentu wyłączenia lub ponownego uruchomienia.
 - **Zakończ**. Wariant ten należy wybrać, w celu zakończenia działania aplikacji.
4. *Obszar wyboru czynności dodatkowej.* W tym miejscu możesz wybrać czynności dodatkowe:
- **Dodać do wyjątków**. Jeżeli masz pewność, że wykryty obiekt jest bezpieczny, możesz dodać go do strefy zaufanej. Dzięki temu podczas kolejnego wykrycia obiektu, program nie będzie wyświetlał dodatkowych ostrzeżeń.

- **Zastosować dla wszystkich obiektów.** Zaznacz to pole, aby określone działanie było stosowane do wszystkich obiektów posiadających podobny status w analogicznych sytuacjach.

ROZWIĄZYWANIE PROBLEMÓW

Jeżeli podczas korzystania z Kaspersky Internet Security wystąpią problemy, spróbuj znaleźć jego rozwiązanie w systemie pomocy lub Bazie wiedzy Kaspersky Lab. Baza wiedzy stanowi element strony internetowej Serwisu pomocy technicznej dostępnego pod adresem <http://pomoc.kaspersky.pl>. Zawiera ona odpowiedzi na najczęściej zadawane pytanie związane z produktami Kaspersky Lab.

▶ *Aby przejść do „Bazy wiedzy” wykonaj następujące czynności:*

1. Otwórz główne okno programu.
2. W dolnej części okna kliknij odsyłacz **Pomoc techniczna**.
3. W oknie, które zostanie otwarte kliknij odsyłacz **Baza wiedzy**.

Kolejną możliwością uzyskania informacji o działaniu aplikacji jest forum internetowe użytkowników Kaspersky Lab. Jest to również sekcja na stronie internetowej Serwisu pomocy technicznej. Zawiera pytania, odpowiedzi oraz rady użytkowników programu. Może zapoznać się tematami forum, dodać komentarz, lub próbować znaleźć odpowiedź na swoje pytanie.

▶ *Aby przejść na forum użytkowników, wykonaj następujące czynności:*

1. Otwórz główne okno programu.
2. W dolnej części okna kliknij odsyłacz **Pomoc techniczna**.
3. W oknie, które zostanie otwarte kliknij odsyłacz **Forum użytkowników**.

Jeżeli nie znalazłeś rozwiązania problemu w systemie pomocy, Bazie wiedzy lub na forum użytkowników, skontaktuj się z działem pomocy technicznej Kaspersky Lab.

KASPERSKY SECURITY NETWORK

A. WSTĘP

NALEŻY UWAŻNIE PRZECZYTAĆ NINIEJSZE INFORMACJE. ZAWIERA ON WAŻNE INFORMACJE, Z KTÓRYMI NALEŻY SIĘ ZAPOZNAĆ PRZED ROZPOCZĘCIEM UŻYTKOWANIA USŁUG LUB OPROGRAMOWANIA FIRMY KASPERSKY LAB. KONTYNUUJĄC UŻYTKOWANIE OPROGRAMOWANIA LUB USŁUG KASPERSKY LAB UŻYTKOWNIK AKCEPTUJE NINIEJSZE OŚWIADCZENIE O GROMADZENIU DANYCH. Firma Kaspersky Lab zastrzega sobie prawo do modyfikowania niniejszego Oświadczenia o Gromadzeniu Danych w dowolnym czasie poprzez opublikowanie zmian w niniejszym oknie. Aby przekonać się, czy treść oświadczenia uległa zmianie od ostatniego czytania, należy sprawdzić datę jego opublikowania. Dalsze użytkowanie usług lub oprogramowania Kaspersky Lab będzie równoznaczne z zaakceptowaniem wszystkich zmian.

Firma Kaspersky Lab i jej partnerzy (dalej, "Kaspersky Lab") stworzyła niniejsze Oświadczenie o Gromadzeniu danych w celu poinformowania i ujawnienia swoich praktyk gromadzenia oraz rozpowszechniania danych na użytek oprogramowania Kaspersky Anti-Virus oraz Kaspersky Internet Security.

Oświadczenie Kaspersky Lab

Firma Kaspersky Lab jest zaangażowana w dostarczanie najlepszych usług wszystkim swoim klientom i rozumie ich potencjalne obawy, jakie mogą powstać w związku z Gromadzeniem Danych. Kaspersky Lab zdaje sobie sprawę z tego, że użytkownicy mogą mieć pytania odnośnie metod wykorzystywanych do gromadzenia i wysyłania danych przez usługę Kaspersky Security Network. Z tego powodu firma Kaspersky Lab przygotowała niniejsze oświadczenie, które informuje o zasadach Gromadzenia Danych, na których opiera się działanie usługi Kaspersky Security Network.

Niniejsze Oświadczenie o Gromadzeniu Danych zawiera ogólne i techniczne informacje o krokach podjętych przez Kaspersky Lab w celu poszanowania obaw użytkownika odnośnie Gromadzenia Danych. Oświadczenie zostało zorganizowane ze względu na najważniejsze procesy i zagadnienia, dzięki czemu użytkownik może szybko przejrzeć interesujące go informacje. Podsumowując, u podstaw wszystkich działań podejmowanych przez Kaspersky Lab leży spełnienie wszelkich potrzeb i oczekiwań użytkowników. Gromadzenie Danych nie jest tutaj wyjątkiem.

Dane i informacje są gromadzone przez Kaspersky Lab i jeżeli po przeczytaniu

niniejszego Oświadczenia o Gromadzeniu Danych pojawiają się jakiegokolwiek wątpliwości lub pytania, należy nawiązać kontakt z działem pomocy technicznej firmy Kaspersky Lab.

Czym jest Kaspersky Security Network?

Usługa Kaspersky Security Network umożliwia użytkownikom produktów Kaspersky Lab z całego świata wspomaganie identyfikacji zagrożeń oraz zminimalizowanie czasu potrzebnego na zapewnienie ochrony przed nowymi (występującymi "na wolności") zagrożeniami atakującymi ich komputery. W celu zidentyfikowania nowych zagrożeń i ich źródeł a także w celu usprawnienia ochrony użytkownika i funkcjonalności produktu usługa Kaspersky Security Network gromadzi wybrane dane związane z ochroną oraz aplikacjami i wysyła te dane do Kaspersky Lab, gdzie są one poddawane analizie. Dane takie nie zawierają żadnych informacji pozwalających na zidentyfikowanie użytkownika i są wykorzystywane przez Kaspersky Lab wyłącznie w celu udoskonalania produktów służących do ochrony oraz dalszego ulepszania rozwiązań pozwalających na zwalczanie zagrożeń i wirusów. W przypadku omyłkowej transmisji jakichkolwiek osobowych danych użytkownika firma Kaspersky Lab zachowa je i będzie chronić zgodnie z zapisami niniejszego Oświadczenia o Gromadzeniu Danych.

Przystępując do usługi Kaspersky Security Network użytkownicy produktów Kaspersky Lab z całego świata przyczyniają się do zwiększenia bezpieczeństwa w Internecie.

Kwestie prawne

Z uwagi na to, że usługa Kaspersky Security Network może być używana w obrębie różnych jurysdykcji (łącznie z jurysdykcją Stanów Zjednoczonych), może ona podlegać różnemu prawodawstwu. Firma Kaspersky Lab ujawni bez zgody użytkownika informacje pozwalające na zidentyfikowanie go, jeżeli będzie to wymagane przez obowiązujące przepisy prawa lub w ujawni je w dobrej wierze mając przekonanie o tym, że ujawnienie to będzie niezbędne do prowadzenia dochodzeń lub ochrony przed szkodliwymi działaniami gości, partnerów lub innych osób związanych z Kaspersky Lab a także mienia Kaspersky Lab. Mając na względzie powyższe informacje, prawo związane z danymi i informacjami gromadzonymi przez usługę Kaspersky Security Network może się różnić w zależności od kraju. Na przykład, pewne informacje osobowe gromadzone na obszarze Unii Europejskiej i jej państw członkowskich podlegają dyrektywom Unii Europejskiej dotyczących danych osobowych, prywatności i komunikacji elektronicznej, włączając (lecz nie ograniczając do): dyrektywę 2002/58/EC Parlamentu Europejskiego oraz Rady z dnia 12 lipca 2002 dotyczącą przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej; dyrektywę 95/46/EC Parlamentu Europejskiego oraz Rady z dnia 24 października 1995 dotyczącą ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego obiegu tychże danych; decyzję Komisji Europejskiej 497/2001/EC dotyczącą klauzul umownych

odnoszących się do przekazywania danych osobowych do państw trzecich.

Usługa Kaspersky Security Network poinformuje w odpowiedni sposób użytkownika, podczas wstępnego gromadzenia wspomnianych wyżej danych, o jakimkolwiek współdzieleniu tych danych w celach biznesowych i pozwoli użytkownikowi na wyrażenie zgody (dla państw członkowskich Unii Europejskiej wymagających wyrażenia zgody) lub na zabronienie (dla wszystkich pozostałych państw) komercyjnego wykorzystywania tych danych i/lub przesyłania ich do jakichkolwiek stron trzecich.

Organ prawny lub sądowy może zażądać od Kaspersky Lab ujawnienia pewnych informacji pozwalających na zidentyfikowanie użytkownika. W przypadku wystąpienia takiego żądania Kaspersky Lab udostępni te informacje po uprzednim otrzymaniu odpowiedniej dokumentacji. Kaspersky Lab może także udostępnić takie informacje organom prawnym w celu ochrony swojego mienia lub zdrowia i bezpieczeństwa osób, w zakresie dozwolonym przez prawo.

Deklaracje dotyczące ochrony danych osobowych przeznaczone dla władz państw członkowskich Unii Europejskiej muszą być przygotowywane z uwzględnieniem prawa obowiązującego dla tych państw członkowskich. Informacje o takich deklaracjach będą dostępne w usłudze Kaspersky Security Network.

B. GROMADZONE INFORMACJE

Dane gromadzone przez Kaspersky Lab

Użytkownik może udostępnić dane na mocy niniejszego oświadczenia a usługa Kaspersky Security Network będzie gromadziła i wysyłała do Kaspersky Lab podstawowe i rozszerzone dane dotyczące potencjalnych zagrożeń skierowanych na komputer użytkownika. Gromadzone dane obejmują:

Dane podstawowe

- informacje o sprzęcie i oprogramowaniu wykorzystywanym w komputerze, które nie pozwalają na zidentyfikowanie użytkownika, łącznie z: wersją zainstalowanego systemu operacyjnego, wersjami uaktualnień systemu operacyjnego, obiektami jądra, sterownikami, usługami, rozszerzeniami Internet Explorera, rozszerzeniami drukarek, rozszerzeniami Eksploratora Windows, pobranymi plikami programów, elementami startowymi, apletami panelu sterowania, zapisami rejestru, adresami IP, rodzajami przeglądarek, klientami poczty elektronicznej oraz numerem wersji produktu Kaspersky Lab;
- unikatowy identyfikator generowany przez produkt Kaspersky Lab w celu zidentyfikowania danego komputera, bez możliwości zidentyfikowania użytkownika - identyfikator nie zawiera żadnych danych osobowych;
- informacje o stanie ochrony antywirusowej komputera oraz dane o

wszelkich plikach lub działaniach, które mogą mieć związek ze szkodliwym oprogramowaniem (na przykład: nazwa wirusa, data/czas wyleczenia, nazwy/ścieżki i rozmiar zainfekowanych plików, adres IP oraz port ataku sieciowego, nazwy aplikacji podejrzewanych o zawieranie szkodliwego oprogramowania). Należy zwrócić uwagę na to, że wymienione powyżej informacje nie pozwalają na zidentyfikowanie użytkownika.

Dane rozszerzone

- informacje o pobranych cyfrowo podpisanych aplikacjach (adres URL, rozmiar plików, nazwa podpisującego);
- informacje o plikach wykonywalnych aplikacji (rozmiar, atrybuty, data utworzenia, informacje o nagłówkach PE, region, nazwa, lokalizacja oraz użyty program pakujący).

Pliki i/lub ich elementy

Usługa Kaspersky Security Network może gromadzić i przysyłać całe pliki i/lub ich elementy do Kaspersky Lab, w celu poddania ich dodatkowej analizie. Przesyłanie plików i/lub ich elementów ma miejsce tylko, gdy użytkownik zaakceptował dokument Oświadczenie o Gromadzeniu Danych.

Zabezpieczanie transmisji oraz przechowywanie danych

Kaspersky Lab zobowiązuje się chronić wszystkie gromadzone informacje. Gromadzone informacje są przechowywane na serwerach z ograniczonym i kontrolowanym dostępem.

Kaspersky Lab korzysta z infrastruktury przechowywania danych chronionej przy użyciu zapór sieciowych i systemów haseł charakteryzujących się najwyższą jakością. Kaspersky Lab stosuje szereg technologii bezpieczeństwa i specjalne procedury w celu ochrony gromadzonych informacji przed takimi zagrożeniami jak nieautoryzowany dostęp, wykorzystanie lub ujawnienie. Polityki bezpieczeństwa wykorzystywane w Kaspersky Lab są okresowo analizowane i w razie potrzeby uaktualniane. Dostęp do gromadzonych danych posiada jedynie autoryzowany personel. Kaspersky Lab dokłada wszelkich starań, aby informacje użytkownika były traktowane z najwyższym poziomem bezpieczeństwa i zgodnie z niniejszym Oświadczeniem o Gromadzeniu Danych. Niestety, żaden mechanizm przesyłania danych nie może zostać uznany za całkowicie bezpieczny. W rezultacie, mimo że Kaspersky Lab stosuje wszelkie dostępne metody ochrony danych użytkownika, nie jest możliwe zagwarantowanie bezpieczeństwa danych przesyłanych do Kaspersky Lab lub z produktów lub usług Kaspersky Lab, włączając (lecz nie ograniczając do) usługę Kaspersky Security Network, i użytkownik korzysta z tych usług na własne ryzyko.

Gromadzone dane mogą być przesyłane do serwerów Kaspersky Lab i firma

Kaspersky Lab podjęła wszelkie wymagane kroki w celu zapewnienia, że gromadzone informacje, w razie przesyłania, będą należycie chronione. Kaspersky Lab traktuje gromadzone dane jako informacje poufne i dane te podlegają procedurom bezpieczeństwa i korporacyjnym politykom Kaspersky Lab dotyczącym ochrony i korzystania z informacji poufnych. Po dotarciu zgromadzonych danych do firmy Kaspersky Lab są one przechowane na serwerze wyposażonym w funkcje ochrony fizycznej i elektronicznej, łącznie z wykorzystaniem procedur logowania i zapór sieciowych zaprojektowanych w celu blokowania nieautoryzowanego dostępu do danych spoza siedziby Kaspersky Lab. Przetwarzanie i przechowywanie danych gromadzonych przez usługę Kaspersky Security Network i objętych niniejszym Oświadczeniem o Gromadzeniu Danych podlega jurysdykcji Stanów Zjednoczonych i może podlegać innym jurysdykcjom obowiązującym w krajach, w których firma Kaspersky Lab prowadzi swoją działalność. Wszyscy pracownicy Kaspersky Lab są świadomi i zobowiązani do przestrzegania polityk bezpieczeństwa stosowanych w firmie. Dane użytkownika są dostępne wyłącznie dla tych pracowników, którzy potrzebują ich do wykonywania swoich obowiązków. Żadne z przechowywanych danych nie będą łączone z jakimkolwiek informacjami pozwalającymi na zidentyfikowanie użytkownika. Kaspersky Lab nie łączy informacji przechowywanych przez usługę Kaspersky Security Network z żadnymi danymi, listami kontaktowymi lub informacjami o subskrypcji, które są gromadzone przez Kaspersky Lab w celach promocyjnych lub innych.

C. WYKORZYSTYWANIE GROMADZONYCH DANYCH

W jaki sposób wykorzystywane są osobiste informacje użytkownika

Kaspersky Lab gromadzi dane w celu analizowania i identyfikowania źródeł potencjalnych zagrożeń oraz udoskonalania możliwości swoich produktów w wykrywaniu niebezpiecznych zachowań, stron WWW służących do oszukiwania użytkowników, oprogramowania crimeware i innych rodzajów zagrożeń internetowych. Wszystkie działania związane z gromadzeniem danych mają na celu zapewnienie w przyszłości możliwie najwyższego poziomu ochrony użytkownikom produktów Kaspersky Lab.

Ujawnianie informacji stronom trzecim

Kaspersky Lab może ujawnić gromadzone informacje po otrzymaniu wezwania do ujawnienia od organu związanego z egzekwowaniem prawa, w odpowiedzi na wezwanie sądowe, w związku z jakimkolwiek innym postępowaniem sądowym lub w dobrej wierze, jeżeli firma Kaspersky Lab uzna, że ujawnienie informacji jest konieczne do osiągnięcia zgodności z przepisami prawa, ustawami, wezwaniem sądowym, jakimkolwiek innym postępowaniem sądowym lub żądaniem prawomocnego organu. Kaspersky Lab może także ujawnić informacje pozwalające na zidentyfikowanie użytkownika w przypadku przekonania o tym, że ujawnienie tych informacji jest niezbędne do zidentyfikowania, nawiązania kontaktu lub podjęcia działań prawnych przeciwko stronie, która może naruszać niniejsze Oświadczenie o Gromadzeniu Danych,

warunki umów zawartych przez użytkownika z Kaspersky Lab lub w celu ochrony użytkowników. W celu działania na rzecz zwiększania świadomości, wykrywania i zapobiegania zagrożeniom internetowym Kaspersky Lab może dzielić się pewnymi informacjami z organizacjami badawczymi i z innymi producentami oprogramowania bezpieczeństwa.

Kaspersky Lab może także wykorzystywać dane statystyczne wynikające ze zgromadzonych informacji w celu śledzenia i publikowania raportów dotyczących trendów w rozwoju zagrożeń bezpieczeństwa.

Wybór pozostawiony użytkownikowi

Udział w usłudze Kaspersky Security Network jest opcjonalny. Użytkownik może w dowolnym momencie aktywować i dezaktywować usługę Kaspersky Security Network przy użyciu odpowiednich ustawień w interfejsie użytkowanego produktu Kaspersky Lab. Należy jednak mieć świadomość tego, że po wyłączeniu usługi Kaspersky Security Network firma Kaspersky Lab może nie być w stanie dostarczać użytkownikowi pewnych usług zależnych od gromadzenia tych danych. Po zakończeniu się okresu licencyjnego użytkowanego produktu Kaspersky Lab pewne funkcje oprogramowania Kaspersky Lab mogą w dalszym ciągu działać, lecz żadne informacje nie będą automatycznie wysyłane do Kaspersky Lab.

Kaspersky Lab zastrzega sobie prawo do nieregularnego wysyłania ostrzeżeń informujących użytkowników o wprowadzaniu zmian, które mogą wpłynąć na możliwość korzystania z pewnych usług Kaspersky Lab. Firma Kaspersky Lab zastrzega sobie także prawo do kontaktowania się z użytkownikiem, jeżeli zostanie do tego zobowiązana z powodu toczącego się postępowania prawnego lub po wykryciu jakiegokolwiek naruszenia stosownych licencji, gwarancji i umów.

Kaspersky Lab zastrzega sobie te prawa, ponieważ w ograniczonych przypadkach może zająć potrzeba poinformowania użytkownika o sprawach, które mogą być dla niego ważne. Prawa te nie zezwalają Kaspersky Lab na wysyłanie do użytkownika jakichkolwiek informacji marketingowych o nowych lub istniejących usługach.

D. GROMADZENIE DANYCH – ŻĄDANIA I ZAŻALENIA

Kaspersky Lab traktuje wszelkie żądania i zażalenia użytkowników związane z Gromadzeniem Danych z najwyższym poszanowaniem i uwagą. Jeżeli użytkownik uważa, że doświadczył jakiegokolwiek niezgodności z niniejszym Oświadczeniem o Gromadzeniu Danych w odniesieniu do jego danych lub informacji lub ma inne żądania lub zażalenia związane z tą kwestią, może on skontaktować się z działem pomocy technicznej firmy Kaspersky Lab.

W wiadomości należy szczegółowo opisać rodzaj żądania. Kaspersky Lab

ustosunkuje się do żądania lub zażalenia najszybciej jak to będzie możliwe.

Udostępnianie informacji jest dobrowolne. Funkcja gromadzenia danych może zostać w dowolnym momencie wyłączona przez użytkownika przy użyciu sekcji "Opinia" znajdującej się w oknie "Ustawienia" produktu Kaspersky Lab.

© 1997-2009 Kaspersky Lab ZAO. Wszelkie prawa zastrzeżone.

KASPERSKY LAB

Firma Kaspersky Lab została założona w 1997 roku. Obecnie jest czołowym producentem oprogramowania: antywirusowego, antyspamowego oraz chroniącego przed atakami sieciowymi. Tworzy szeroką gamę programów zabezpieczających 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 firma międzynarodową. Główna siedziba znajduje się w Rosji. Firma posiada swoje oddziały w Wielkiej Brytanii, Francji, Niemczech, Japonii, Krajach Beneluksu, Chinach, Polsce, Rumunii oraz Stanach Zjednoczonych. We Francji działa także specjalny dział firmy – Europejskie Centrum Badań Antywirusowych. Partnerami firmy Kaspersky Lab jest ponad 500 przedsiębiorstw na całym świecie.

Obecnie Kaspersky Lab zatrudnia ponad 1000 specjalistów, 10 z nich posiada tytuł M.B.A., 16 – doktoraty. Najlepsi eksperci firmy Kaspersky Lab są członkami organizacji Computer Anti-virus Researcher's Organization (CARO).

Naszą firmę wyróżnia jedyna w swoim rodzaju wiedza zebrana przez specjalistów podczas ponad czternastoletniej, ciągłej walki przeciwko wirusom komputerowym. Dokładna analiza działania wirusów komputerowych pozwala na dostarczenie kompletnej ochrony zarówno przed bieżącymi, jak i przyszłymi zagrożeniami. Zaletą ta jest podstawą produktów i usług firmy Kaspersky Lab. Przez cały czas produkty firmy Kaspersky pozostają o krok przed produktami innych producentów oprogramowania antywirusowego.

Lata ciężkiej pracy sprawiły, że nasza firma znajduje się w ścisłej czołówce producentów oprogramowania antywirusowego. Kaspersky Lab jako pierwszy opublikował wiele nowoczesnych standardów oprogramowania antywirusowego. Flagowy produkt firmy, Kaspersky Anti-Virus zapewnia kompletną ochronę wszystkich węzłów w sieci, łącznie ze stacjami roboczymi, serwerami plików, systemami pocztowymi, zaporami ogniowymi, bramami internetowymi i komputerami kieszonkowymi. Wygodne i łatwe w użytkowaniu narzędzia zarządzające zapewniają zaawansowaną automatyzację ochrony antywirusowej wewnątrz sieci firmowej. Wiele firm używa silnika programu Kaspersky Anti-Virus w swoich produktach. Do producentów tych należą: Nokia ICG (USA), Aladdin (Izrael), Sybari (USA), G Data (Niemcy), Deerfield (USA), Alt-N (USA), Microworld (Indie), BorderWare (Kanada).

Klienci Kaspersky Lab korzystają z szerokiego zakresu dodatkowych usług, które zapewniają nie tylko stabilne działanie użytkowanych produktów, ale także spełniają specyficzne wymagania firm. Nasza firma projektuje, wdraża i obsługuje korporacyjne rozwiązania antywirusowe. Firma Kaspersky Lab

uaktualnia sygnatury zagrożeń raz na godzinę. Firma zapewnia swoim klientom pomoc techniczną w wielu językach.

W przypadku pojawienia się pytań, można je przesłać do jednego z naszych dystrybutorów lub bezpośrednio do Kaspersky Lab. Pomoc techniczna jest świadczona za pośrednictwem telefonu i poczty elektronicznej. Użytkownik uzyska szczegółowe odpowiedzi na wszystkie pytania.

WWW: <http://www.kaspersky.pl>

Encyklopedia wirusów: <http://www.viruslist.pl>

Laboratorium antywirusowe: nowywirus@kaspersky.pl
(wyłącznie do wysyłania nowych wirusów w archiwach)
<http://support.kaspersky.ru/helpdesk.html?LANG=pl>
(formularz pomocy technicznej)

Forum internetowe Kaspersky Lab <http://forum.kaspersky.com>

UMOWA LICENCYJNA

UMOWA LICENCYJNA UŻYTKOWNIKA KOŃCOWEGO FIRMY KASPERSKY LAB

WAŻNA INFORMACJA PRAWNA DLA WSZYSTKICH UŻYTKOWNIKÓW: PRZED ROZPOCZĘCIEM KORZYSTANIA Z OPROGRAMOWANIA NALEŻY UWAŻNIE PRZECZYTAĆ NINIEJSZĄ UMOWĘ LICENCYJNĄ.

KLIKAJĄC PRZYCISK WYRAŻAM ZGODĘ NA UMOWIE LICENCYJNEJ LUB WPISUJĄC ODPOWIEDNI(E) SYMBOL(E), UŻYTKOWNIK WYRAŻA ZGODĘ NA PRZESTRZEGANIE JEJ WARUNKÓW I ZASAD. **CZYNNOŚĆ TA JEST JEDNOZNACZNA ZE ZŁOŻENIEM PODPISU A UŻYTKOWNIK WYRAŻA ZGODĘ NA PRZESTRZEGANIE NINIEJSZEJ UMOWY, KTÓREJ STAJE SIĘ STRONĄ ORAZ WYRAŻA ZGODĘ NA EGZEKWOWANIE JEJ POSTANOWIEŃ W SPOSÓB OBOWIĄZUJĄCY W PRZYPADKU WSZELKICH WYNEGOCJOWANYCH, PISEMNYCH UMÓW PODPISANYCH PRZEZ UŻYTKOWNIKA.** JEŻELI UŻYTKOWNIK NIE WYRAŻA ZGODY NA WSZYSTKIE LUB NIEKTÓRE ZASADY I WARUNKI NINIEJSZEJ UMOWY, POWINIEN PRZERWAĆ INSTALACJĘ OPROGRAMOWANIA I ZREZYGNOWAĆ Z INSTALACJI.

PO KLIKNIECIU PRZYCISKU WYRAŻENIA ZGODY W OKNIE UMOWY LICENCYJNEJ LUB PO WPISANIU ODPOWIEDNIEGO SYMBOLU/ODPOWIEDNICH SYMBOLI, UŻYTKOWNIK NABYWA PRAWO DO KORZYSTANIA Z OPROGRAMOWANIA NA ZASADACH I WARUNKACH ZAWARTYCH W NINIEJSZEJ UMOWIE.

1. Definicje

- 1.1. **Oprogramowanie** oznacza oprogramowanie, w tym Aktualizacje i powiązane materiały.
- 1.2. **Posiadacz praw** (posiadacz wszystkich praw, wyłącznych bądź innych praw do Oprogramowania) oznacza firmę Kaspersky Lab ZAO, spółkę zarejestrowaną zgodnie z przepisami prawa obowiązującego na terenie Federacji Rosyjskiej.
- 1.3. **Komputer(y)** oznacza(-ją) sprzęt komputerowy, w tym komputery osobiste, laptopy, stacje robocze, palmtopy, telefony „smart phone”, produkty kieszonek lub inne urządzenia elektroniczne, do których przeznaczone jest Oprogramowanie, na których zostanie ono zainstalowane i/lub będzie użytkowane.
- 1.4. **Użytkownik końcowy** oznacza osobę(-y) fizyczną(-e) instalującą(-e) lub korzystającą(-e) w imieniu własnym z legalnej kopii Oprogramowania; lub, jeżeli Oprogramowanie jest pobierane lub instalowane w imieniu organizacji, np. pracodawcy, „Użytkownik” oznacza organizację, na potrzeby której Oprogramowanie zostaje pobrane lub zainstalowane i niniejszym przyjmuje się, iż taka organizacja upoważniła osobę przyjmującą warunki tej umowy do uczynienia tego w jej imieniu. Dla celów niniejszej umowy, termin „organizacja”, obejmuje, bez ograniczeń, każdą spółkę, spółkę z ograniczoną odpowiedzialnością, korporację, stowarzyszenie, spółkę kapitałową, zarząd powierniczy, spółkę joint venture, organizację pracowniczą, organizację nie posiadającą osobowości prawnej lub organizację rządowe.

- 1.5. **Partner(-rzy)** oznacza(-ją) organizacje lub osoby fizyczne, zajmujące się dystrybucją Oprogramowania w oparciu o licencję i umowę zawartą z Posiadaczem praw.
- 1.6. **Aktualizacja(-e)** oznacza(-ją) wszelkie ulepszenia, rewizje, poprawki do usterek programowych, usprawnienia, naprawy, modyfikacje, kopie, dodatki lub zestawy konserwacyjne, itp.
- 1.7. **Instrukcja użytkownika** oznacza instrukcję użytkownika, przewodnik administratora, dokumentacja i związane z nimi materiały objaśniające lub inne.

2. **Przyznanie licencji**

- 2.1. Posiadacz praw niniejszym przyznaje Użytkownikowi niewyłączną licencję na przechowywanie, pobieranie, instalację, uruchamianie i wyświetlanie („użytkowanie”) Oprogramowania na określonej liczbie komputerów w celu ochrony komputera Użytkownika, na którym zainstalowane zostało Oprogramowanie przed zagrożeniami opisanymi w Instrukcji użytkownika, zgodnie z wszelkimi wymogami technicznymi opisanymi w Instrukcji użytkownika i stosownie do zasad i warunków niniejszej Umowy („Licencja”), a Użytkownik przyjmuje warunki niniejszej Licencji:

Wersja próbna. Jeżeli użytkownik otrzymał, pobrał oraz/lub zainstalował wersję próbną Oprogramowania i otrzymał niniejszym licencję ewaluacyjną na Oprogramowanie, jeżeli nie zostało to inaczej określone, może wykorzystywać je wyłącznie w celach ewaluacyjnych i wyłącznie jednorazowo, w określonym przedziale czasowym począwszy od dnia pierwszej instalacji. Wykorzystywanie Oprogramowania do innych celów lub w okresie wykraczającym poza okres ewaluacji jest surowo wzbronione.

Oprogramowanie wielośrodowiskowe; Oprogramowanie wielojęzyczne; Podwójne nośniki oprogramowania; Kopie zbiorowe; Pakiety. W przypadku Użytkowników korzystających z innych wersji Oprogramowania lub innych wersji językowych Oprogramowania, posiadających Oprogramowanie na kilku nośnikach, w postaci kopii zbiorowej bądź w pakiecie wraz z innym oprogramowaniem, całkowita ilość komputerów, na których zainstalowane zostały wszystkie wersje Oprogramowania odpowiadać będzie ilości licencji otrzymanych od Posiadacza praw *zakładając*, że warunki licencjonowania nie stanowią inaczej, każda zakupiona licencja uprawnia Użytkownika do zainstalowania i korzystania z Oprogramowania na takiej ilości komputerów, jaka określona została w paragrafach 2.2 oraz 2.3.

- 2.2. Jeżeli Oprogramowanie zostało zakupione na nośniku fizycznym, Użytkownik może z niego korzystać w celu ochrony komputera(-ów) w liczbie określonej na opakowaniu.
- 2.3. Jeżeli Oprogramowanie zostało zakupione w Internecie, Użytkownik może z niego korzystać w celu ochrony komputerów w liczbie określonej przy zakupie Licencji na Oprogramowanie.
- 2.4. Użytkownik ma prawo do wykonania kopii oprogramowania wyłącznie w celu stworzenia kopii zapasowej, która zastąpi legalnie posiadaną kopię na wypadek jej utraty, zniszczenia lub uszkodzenia uniemożliwiającego jej użytkowanie. Kopii zapasowej nie wolno użytkować do innych celów i musi ona zostać zniszczona po utracie przez Użytkownika prawa do użytkowania Oprogramowania lub po wygaśnięciu bądź wycofaniu licencji Użytkownika z jakiegokolwiek powodu, stosownie do prawa obowiązującego w kraju zamieszkania Użytkownika lub w kraju, w którym Użytkownik korzysta z Oprogramowania.
- 2.5. Użytkownik może przekazać niewyłączną licencję na korzystanie z Oprogramowania innym osobom fizycznym lub prawnym w zakresie udzielonym

Użytkownikowi przez Posiadacza praw pod warunkiem, że osoba otrzymująca wyrazi zgodę na przestrzeganie wszystkich zasad i warunków niniejszej Umowy oraz w pełni zastąpi dotychczasowego Użytkownika jako posiadacz licencji udzielonej przez Posiadacza praw. W przypadku pełnego przeniesienia praw nadanych przez Posiadacza praw na korzystanie z Oprogramowania, Użytkownik ma obowiązek zniszczenia wszelkich posiadanych kopii Oprogramowania, w tym kopii zapasowych. Osoba otrzymująca przekazaną licencję musi wyrazić zgodę na przestrzeganie wszystkich zasad i warunków niniejszej Umowy. Jeżeli osoba otrzymująca nie wyrazi zgody na przestrzeganie wszystkich zasad i warunków niniejszej Umowy, nie może zainstalować bądź/ani użytkować Oprogramowania. Użytkownik oświadcza również, jako osoba otrzymująca przekazywaną licencję, że nie posiada żadnych dodatkowych lub większych praw niż oryginalny Użytkownik końcowy, który dokonał zakupu Oprogramowania od Posiadacza praw.

- 2.6. Z chwilą aktywacji Oprogramowania lub po instalacji pliku klucza licencyjnego (z wyjątkiem jego wersji próbnej), Użytkownik zyskuje prawo do otrzymywania następujących usług w okresie oznaczonym na opakowaniu Oprogramowania (jeżeli Oprogramowanie zostało zakupione na nośniku fizycznym) lub zdefiniowanym podczas jego zakupu (jeżeli Oprogramowanie zostało zakupione w Internecie):
- Aktualizacje Oprogramowania poprzez Internet po opublikowaniu ich na stronie internetowej przez Posiadacza praw lub w formie innych usług online. Wszelkie otrzymane przez Użytkownika Aktualizacje stają się częścią Oprogramowania i mają wobec nich zastosowanie zasady i warunki niniejszej Umowy;
 - Pomoc techniczna za pośrednictwem Internetu oraz telefonicznie w postaci infolinii Pomocy technicznej.

3. Aktywacja i okres obowiązywania

- 3.1. Od Użytkownika, który zmodyfikuje swój komputer lub wprowadzi zmiany do zainstalowanego na nim oprogramowania innych dostawców, Posiadacz praw może wymagać przeprowadzenia ponownej aktywacji Oprogramowania lub instalacji pliku klucza licencyjnego. Posiadacz praw zastrzega sobie prawo do wykorzystania wszelkich środków oraz procedur weryfikacyjnych celem zweryfikowania wiarygodności Licencji oraz/lub kopii Oprogramowania zainstalowanego oraz/lub wykorzystywanego na komputerze Użytkownika.
- 3.2. Jeżeli Oprogramowanie zostało zakupione na nośniku fizycznym, może ono być wykorzystywane, po przyjęciu warunków niniejszej Umowy, w okresie oznaczonym na opakowaniu, począwszy od akceptacji niniejszej Umowy.
- 3.3. Jeżeli Oprogramowanie zostało zakupione w Internecie, może ono być wykorzystywane, po przyjęciu warunków niniejszej Umowy, w okresie zdefiniowanym przy zakupie.
- 3.4. Użytkownik ma prawo do nieodpłatnego korzystania z wersji próbnej oprogramowania w sposób określony w paragrafie 2.1 w pojedynczym okresie ewaluacji (30 dni) począwszy od momentu aktywacji Oprogramowania na zasadach określonych niniejszą Umową *zakładając*, że wersja próbna nie upoważnia Użytkownika do korzystania z Aktualizacji oraz Pomocy technicznej za pośrednictwem Internetu oraz telefonicznej w postaci infolinii Pomocy technicznej.
- 3.5. Posiadana przez Użytkownika Licencja na korzystanie z Oprogramowania wydana zostaje na okres zdefiniowany w paragrafie 3.2 lub 3.3 (odpowiednio), a ilość czasu pozostałą do zakończenia okresu użytkowania można sprawdzić za pomocą środków opisanych w Instrukcji Użytkownika.

- 3.6. Jeśli Użytkownik nabył Oprogramowanie z zamiarem użytkowania na więcej niż jednym komputerze, wtedy licencja Użytkownika na korzystanie z Oprogramowania jest ograniczona do czasu począwszy od daty aktywacji Oprogramowania lub instalacji pliku klucza licencyjnego na pierwszym komputerze.
- 3.7. Nie naruszając wszelkich innych środków prawnych ani prawa equity, które mogą przysługiwać Posiadaczowi praw, w przypadku złamania przez Użytkownika któregokolwiek z postanowień i warunków niniejszej Umowy, Posiadacz praw w każdej chwili i bez powiadomienia Użytkownika może wycofać niniejszą Licencję na użytkowanie Oprogramowania, nie refundując ceny zakupu w całości ani w części.
- 3.8. Użytkownik wyraża zgodę na to, iż korzystając z Oprogramowania oraz wszelkich raportów lub informacji od niego pochodzących, będzie przestrzegać wszystkich mających zastosowanie przepisów prawa międzynarodowego, krajowego, stanowego, przepisów oraz praw lokalnych, w tym, bez ograniczeń, prawa prywatności, praw autorskich, praw kontroli eksportu oraz prawa dotyczącego pornografii.
- 3.9. Z wyjątkiem okoliczności, w których postanowienia niniejszej Umowy stanowią inaczej, Użytkownik nie ma prawa do przeniesienia nadanych mu z mocy niniejszej Umowy praw bądź wynikających z niej zobowiązań.

4. Pomoc techniczna

Pomoc techniczna opisana w paragrafie 2.6 niniejszej Umowy zapewniana będzie Użytkownikowi po zainstalowaniu najnowszej Aktualizacji Oprogramowania (z wyjątkiem wersji jego próbnej).

Pomoc techniczna: <http://support.kaspersky.com>

5. Gromadzenie informacji

- 5.1. Wyrażając zgodę na zasady i warunki niniejszej Umowy, Użytkownik zgadza się na dostarczenie Posiadaczowi praw informacji o plikach wykonywalnych i ich sumach kontrolnych w celu udoskonalenia zapewnianego Użytkownikowi poziomu ochrony.
- 5.2. Aby lepiej uświadomić sobie nowe zagrożenia i ich źródła oraz udoskonalić oferowany Użytkownikowi poziom zabezpieczenia, Posiadacz praw, za zgodą Użytkownika wyrażoną w Oświadczeniu o Gromadzeniu Danych Sieci Kaspersky Security Network, wyraźnie upoważnia go otrzymaniu tych informacji. Użytkownik ma prawo dezaktywować usługę Kaspersky Security Network podczas instalacji. Również po zainstalowaniu, Użytkownik może w każdej chwili aktywować i dezaktywować usługę Kaspersky Security Network na stronie opcji Oprogramowania.

Użytkownik dodatkowo uznaje i wyraża zgodę na to, iż wszelkie informacje zgromadzone przez Posiadacza praw mogą zostać wykorzystane do śledzenia oraz publikacji raportów o trendach w zakresie zagrożeń wg wyłącznego uznania Posiadacza praw.

- 5.3. Oprogramowanie nie przetwarza żadnych danych pozwalających na identyfikację jednostki, nie łączy też przetwarzania danych z żadnymi informacjami osobowymi.
- 5.4. Jeżeli Użytkownik nie życzy sobie, aby informacje zebrane przez Oprogramowanie zostały przesłane Posiadaczowi praw, powinien on zrezygnować z aktywacji lub dezaktywować usługę Kaspersky Security Network.

6. Ograniczenia

- 6.1. Użytkownik nie będzie emulować, klonować, wynajmować, używać, wypożyczać na zasadach leasingu, odsprzedawać, modyfikować, dekompilować, poddawać inżynierii wstecznej lub demontażowi ani tworzyć prac pochodnych w oparciu o Oprogramowanie lub jakąkolwiek jego część z wyjątkiem, kiedy jest to dozwolone w postaci niezbywalnego prawa nadanego Użytkownikowi poprzez odpowiednie prawa, Użytkownik nie sprowadzi też żadnej części Oprogramowania do postaci czytelnej dla człowieka, nie przeniesie licencjonowanego Oprogramowania lub jego podzbioru, oraz nie zezwoli na to stronie trzeciej, z wyjątkiem wypadków, kiedy niniejsze restrykcje są wyraźnie zakazane przez obowiązujące prawo. Ani kod binarny Oprogramowania ani jego kod źródłowy nie mogą być wykorzystywane bądź poddawane inżynierii wstecznej w celu stworzenia algorytmu programu, który jest zastrzeżony. Wszelkie prawa, które nie zostały wyraźnie nadane na mocy niniejszej Umowy są zastrzeżone przez Posiadacza praw oraz/lub odpowiednio, jego dostawców. Wszelkie przejawy nieautoryzowanego użycia Oprogramowania spowodują natychmiastowe i automatyczne rozwiązanie niniejszej Umowy oraz odebranie nadanej w ramach umowy Licencji, mogą również spowodować rozpoczęcie postępowania przeciwko Użytkownikowi z powództwa cywilnego oraz/lub karnego.
- 6.2. Użytkownik nie dokona cesji swoich praw do korzystania z Oprogramowania na stronę trzecią, poza wyjątkami określonymi w paragrafie 2.5 niniejszej Umowy.
- 6.3. Użytkownik nie udostępni stronom trzecim kodu aktywacyjnego ani/bądź pliku klucza licencyjnego, nie zezwoli również stronom trzecim na korzystanie z kodu aktywacyjnego ani/bądź pliku klucza licencyjnego stanowiących poufne dane będące własnością Posiadacza praw oraz dołoży uzasadnionych starań w celu ochrony kodu aktywacyjnego oraz/lub pliku klucza licencyjnego pod warunkiem iż, jak określone to zostało w paragrafie 2.5 niniejszej Umowy, Użytkownik może przekazać kod aktywacyjny oraz/lub plik klucza licencyjnego stronom trzecim.
- 6.4. Użytkownik nie będzie wynajmował, używał ani wypożyczał Oprogramowania na zasadach leasingu żadnej stronie trzeciej.
- 6.5. Użytkownik nie będzie wykorzystywał Oprogramowania do tworzenia danych lub oprogramowania wykorzystywanego do wykrywania, blokowania lub usuwania zagrożeń opisanych w Instrukcji użytkownika.
- 6.6. Posiadacz praw ma prawo do zablokowania pliku klucza licencyjnego lub rozwiązania Umowy Licencyjnej na korzystanie z Oprogramowania zawartej z Użytkownikiem bez jakiegokolwiek refundacji w wypadku złamania przez Użytkownika któregokolwiek z postanowień i warunków niniejszej Umowy.
- 6.7. Użytkownikom korzystającym z próbnej wersji Oprogramowania nie przysługuje prawo do otrzymywania Pomocy technicznej opisanej w paragrafie 4 niniejszej Umowy, a Użytkownik nie ma prawa do przekazania licencji bądź scedowania praw do korzystania z Oprogramowania na jakąkolwiek stronę trzecią.

7. Ograniczona gwarancja i wyłączenie odpowiedzialności

- 7.1. Posiadacz praw gwarantuje, że Oprogramowanie w istotnym zakresie będzie zgodne ze specyfikacją oraz opisem zawartym w Instrukcji użytkownika *pod warunkiem, że ta ograniczona gwarancja nie będzie miała zastosowania w następujących przypadkach:* (w) niedobory w funkcjonalności komputera Użytkownika i związane z tym naruszenia, za które Posiadacz praw wyraźnie zrzeka się wszelkiej odpowiedzialności gwarancyjnej; (x) wadliwe działanie, uszkodzenia lub awarie powstałe na skutek nadużyć; wypadków; zaniedbań; niewłaściwej instalacji, użytkowania lub konserwacji; kradzieży; wandalizmu; siły

- wyższej; aktów terroryzmu; awarii lub przeciążenia sieci zasilania; ofiar; przeróbki, niedozwolonych modyfikacji lub napraw przeprowadzonych przez jednostki inne, niż Posiadacz praw; lub jakiegokolwiek inne działania stron trzecich lub Użytkownika oraz z przyczyn będących poza zasięgiem wpływu Posiadacza praw; (y) wszelkie wady, o których Użytkownik nie powiadomił Posiadacza praw w możliwie szybkim terminie od ich stwierdzenia; oraz (z) niekompatybilność spowodowana sprzętem komputerowym oraz/lub elementami oprogramowania zainstalowanego na komputerze Użytkownika.
- 7.2. Użytkownik oświadcza, akceptuje oraz zgadza się, iż żadne oprogramowanie nie jest wolne od błędów oraz, że zalecane jest wykonywanie kopii zapasowych zawartości dysku komputera, z częstotliwością oraz o niezawodności odpowiadającej Użytkownikowi.
- 7.3. Posiadacz praw nie udziela jakiegokolwiek gwarancji na to, że Oprogramowanie będzie funkcjonowało poprawnie w przypadku pogwałcenia zasad opisanych w Instrukcji użytkownika lub w niniejszej Umowie.
- 7.4. Posiadacz praw nie gwarantuje, że Oprogramowanie będzie funkcjonowało poprawnie, jeżeli Użytkownik nie będzie regularnie pobierał Aktualizacji opisanych w paragrafie 2.6 niniejszej Umowy.
- 7.5. Posiadacz praw nie gwarantuje ochrony przed zagrożeniami opisanymi w Instrukcji użytkownika po upływie okresu zdefiniowanego w paragrafach 3.2 lub 3.3 niniejszej Umowy lub po wygaśnięciu Licencji na korzystanie z Oprogramowania z jakiegokolwiek powodu.
- 7.6. OPROGRAMOWANIE UDOSTĘPNIONE JEST UŻYTKOWNIKOWI W STANIE „TAKIM, JAKIM JEST” A POSIADACZ PRAW NIE SKŁADA JAKIKOLWIEK OŚWIADCZEŃ ANI NIE UDZIELA ZAPEWNIENI CO DO JEGO WYKORZYSTYWANIA LUB DZIAŁANIA. WYJĄWSZY WSZELKIE GWARANCJE, WARUNKI, OŚWIADCZENIA LUB POSTANOWIENIA, KTÓRYCH NIE MOŻNA WYKLUCZYĆ LUB OGRANICZYĆ W ŚWIETLE OBOWIĄZUJĄCEGO PRAWA, POSIADACZ PRAW I JEGO PARTNERZY NIE SKŁADAJĄ ŻADNYCH ZAPEWNIENI, WARUNKÓW, OŚWIADCZEŃ ANI POSTANOWIENI (WYRAŻONYCH LUB DOMNIEMANYCH Z MOCY USTAWY, PRAWA ZWYCZAJOWEGO, ZWYCZAJU, WYKORZYSTANIA LUB INNYCH) W JAKIKOLWIEK KWESTIACH, W TYM, BEZ OGRANICZEŃ, W KWESTIACH NIENARUSZANIA PRAW STRON TRZECICH, POKUPNOŚCI, SATYSFAKCJONUJĄCEJ JAKOŚCI, INTEGRACJI LUB PRZYDATNOŚCI DO DANEGO CELU. UŻYTKOWNIK PONOSI CAŁKOWITĄ ODPOWIEDZIALNOŚĆ ZA WADY ORAZ CAŁKOWITE RYZYKO W KWESTII DZIAŁANIA ORAZ ODPOWIEDZIALNOŚCI ZA WYBÓR ODPOWIEDNIEGO OPROGRAMOWANIA DO OSIĄGNIĘCIA ŻĄDANYCH REZULTATÓW, ORAZ ZA INSTALACJĘ, KORZYSTANIE I WYNIKI UZYSKANE W REZULTACIE STOSOWANIA OPROGRAMOWANIA. BEZ OGRANICZEŃ DLA POWYŻSZYCH POSTANOWIENI, POSIADACZ PRAW NIE SKŁADA ŻADNYCH OŚWIADCZEŃ ANI ZAPEWNIENI, ŻE OPROGRAMOWANIE BĘDZIE WOLNE OD BŁĘDÓW, PRZERW W FUNKCJONOWANIU LUB INNYCH AWARII LUB TEŻ, ŻE OPROGRAMOWANIE SPEŁNI WSZELKIE LUB WSZYSTKIE WYMAGANIA UŻYTKOWNIKA BEZ WZGLĘDU NA TO, CZY ZOSTAŁY ONE UJAWNIONE POSIADACZOWI PRAW.

8. Wyłączenie i ograniczenie odpowiedzialności

W NAJSZERSZYM PRAWNIE DOPUSZCZALNYM ZAKRESIE, W ŻADNYM WYPADKU POSIADACZ PRAW ANI JEGO PARTNERZY NIE BĘDĄ ODPOWIEDZIALNI ZA JAKIEKOLWIEK SPECJALNE, PRZYPADKOWE, DOMNIEMANE, POŚREDNIE LUB WYNIKOWE SZKODY (W TYM, M. IN., ZADOŚCUCZYNIENIE ZA UTRATĘ ZYSKÓW

LUB INFORMACJI POUFNYCH LUB INNYCH, PRZERWY W PROWADZENIU DZIAŁALNOŚCI, UTRATĘ PRYWATNOŚCI, KORUPCJĘ, ZNISZCZENIE ORAZ UTRATĘ DANYCH LUB PROGRAMÓW, ZA NIEMOŻNOŚĆ WYWIĄZANIA SIĘ Z JAKIKOLWIEK OBOWIĄZKÓW, W TYM WSZELKICH OBOWIĄZKÓW USTAWOWYCH, OBOWIĄZKU DOBREJ WIARY LUB NALEŻYTEJ STARANNOŚCI, ZA ZANIEDBANIE, STRATY EKONOMICZNE ORAZ WSZELKIE INNE STRATY PIENIĘŻNE) POWSTAŁE NA SKUTEK LUB W JAKIKOLWIEK SPOSÓB ZWIĄZANE Z WYKORZYSTANIEM LUB NIEMOŻNOŚCIĄ WYKORZYSTANIA OPROGRAMOWANIA, ZAPEWNIENIEM LUB NIEMOŻNOŚCIĄ ZAPEWNIENIA WSPARCIA LUB INNYCH USŁUG, INFORMACJI, OPROGRAMOWANIA ORAZ ZWIĄZANEJ Z OPROGRAMOWANIEM TREŚCI LUB W INNY SPOSÓB POWSTAŁYCH W WYNIKU KORZYSTANIA Z OPROGRAMOWANIA BĄDŹ W RAMACH LUB W ZWIĄZKU Z JAKIKOLWIEK POSTANOWIENIEM NINIEJSZEJ UMOWY LUB ZŁAMANIEM WARUNKÓW UMOWNYCH BĄDŹ DELIKTOWYCH (W TYM Z ZANIEDBANIE, WPROWADZENIEM W BĄDŹ, ODPOWIEDZIALNOŚCIĄ LUB OBOWIĄZKIEM BEZPOŚREDNIM) LUB INNYM ZŁAMANIEM OBOWIĄZKU USTAWOWEGO, LUB JAKIKOLWIEK NARUSZENIEM WARUNKÓW GWARANCJI PRZEZ POSIADACZA PRAW LUB KTÓREGOKOLWIEK Z JEGO PARTNERÓW NAWET, JEŻELI POSIADACZ PRAW LUB JEGO PARTNERZY ZOSTALI POINFORMOWANI O MOŻLIWOŚCI ZAISTNIENIA TAKICH SZKÓD.

UŻYTKOWNIK WYRAŻA ZGODĘ NA TO, IŻ W WYPADKU GDY POSIADACZ PRAW ORAZ/LUB JEGO PARTNERZY ZOSTANĄ UZNANI ZA ODPOWIEDZIALNYCH, ODPOWIEDZIALNOŚĆ POSIADACZA PRAW ORAZ/LUB JEGO PARTNERÓW OGRANICZAĆ SIĘ BĘDZIE DO KOSZTÓW OPROGRAMOWANIA. W ŻADNYM WYPADKU ODPOWIEDZIALNOŚĆ POSIADACZA PRAW ORAZ/LUB JEGO PARTNERÓW NIE PRZEKROCZY OPŁAT ZA OPROGRAMOWANIE WNIESIONYCH NA RZECZ POSIADACZA PRAW LUB JEGO PARTNERÓW (W ZALEŻNOŚCI OD OKOLICZNOŚCI).

NIC CO STANOWI TREŚĆ NINIEJSZEJ UMOWY NIE WYKLUCZA ANI NIE OGRANICZA ŻADNYCH ROSZCZEŃ DOTYCZĄCYCH ŚMIERCI ORAZ ODNIESIONYCH OBRAŹEN CIELESNYCH. PONADTO, W PRZYPADKU GDY ZRZECZENIE SIĘ ODPOWIEDZIALNOŚCI, WYŁĄCZENIE LUB OGRANICZENIE W TREŚCI NINIEJSZEJ UMOWY NIE MOŻE ZOSTAĆ WYŁĄCZONE LUB OGRANICZONE W ŚWIETLE OBOWIĄZUJĄCEGO PRAWA, WTEDY TAKIE ZRZECZENIE SIĘ ODPOWIEDZIALNOŚCI, WYŁĄCZENIE LUB OGRANICZENIE NIE BĘDZIE MIAŁO ZASTOSOWANIA W PRZYPADKU UŻYTKOWNIKA, KTÓREGO W DAŁSZYM CIĄGU OBOWIĄZYWAĆ BĘDĄ POZOSTAŁE ZRZECZENIA SIĘ ODPOWIEDZIALNOŚCI, WYŁĄCZENIA ORAZ OGRANICZENIA.

9. GNU oraz licencje stron trzecich

Oprogramowanie może zawierać programy komputerowe licencjonowane (lub sublicencjonowane) użytkownikowi w ramach Powszechnej Licencji Publicznej GNU lub innych, podobnych licencji na bezpłatne oprogramowanie które, poza innymi uprawnieniami, pozwalają użytkownikowi na kopiowanie, modyfikowanie oraz redystrybucję niektórych programów lub ich części oraz udostępniają kod źródłowy („Wolne Oprogramowanie”). Jeżeli licencje te wymagają, aby dla każdego oprogramowania przekazywanego innym w formie wykonywalnego formatu binarnego udostępniony został tym użytkownikom również kod źródłowy, powinien on zostać udostępniony użytkownikowi po otrzymaniu prośby przesłanej na adres: source@kaspersky.com lub kod źródłowy został dołączony do Oprogramowania. Jeżeli jakiegokolwiek licencje Wolnego Oprogramowania wymagają, aby Posiadacz praw udostępnił prawo do korzystania, kopiowania oraz modyfikowania programu w ramach Wolnego Oprogramowania

wykraczające poza prawa przyznane z mocy niniejszej Umowy, wtedy prawa te stają się nadrzędne do zawartych w niniejszej Umowie praw i restrykcji.

10. Prawo własności intelektualnej

- 10.1 Użytkownik zgadza się, że Oprogramowanie oraz jego autorstwo, systemy, pomysły, metody działania, dokumentacja oraz inne zawarte w Oprogramowaniu informacje stanowią własność intelektualną oraz/lub cenne tajemnice handlowe Posiadacza praw lub jego partnerów oraz, że Posiadacz praw oraz, odpowiednio, jego partnerzy, chronieni są przepisami prawa cywilnego i karnego oraz przepisami o prawie autorskim, tajemnicy handlowej, znaku towarowym oraz prawem patentowym Federacji Rosyjskiej, Unii Europejskiej oraz Stanów Zjednoczonych i innych krajów, jak również traktatami międzynarodowymi. Niniejsza Umowa nie nadaje Użytkownikowi żadnych praw własności intelektualnej, w tym do znaków towarowych lub usługowych Posiadacza praw oraz/lub jego partnerów („Znaki towarowe”). Użytkownik może korzystać ze znaków towarowych tylko w zakresie identyfikacji wydruków stworzonych przez Oprogramowanie, stosownie do zaakceptowanych praktyk dotyczących znaków towarowych, w tym identyfikacji nazwy posiadacza znaku towarowego. Takie wykorzystanie znaku towarowego nie daje Użytkownikowi jakichkolwiek praw własności w stosunku do Znak towarowego. Posiadacz praw oraz/lub jego partnerzy posiadają oraz zachowują wszelkie prawa, tytuł własności oraz prawo do udziału w zyskach z Oprogramowania, w tym, bez ograniczeń, wszelkich korekt błędów, usprawnień, Aktualizacji lub innych modyfikacji Oprogramowania dokonanych przez Posiadacza praw lub jakąkolwiek stronę trzecią oraz wszelkich praw autorskich, patentów, praw do tajemnic handlowych, znaków towarowych oraz innych zawartych w nich własności intelektualnych. Posiadanie, instalacja ani korzystanie z Oprogramowania przez Użytkownika nie powoduje przeniesienia na niego jakiegokolwiek tytułu własności intelektualnej Oprogramowania, a Użytkownik nie nabywa żadnych praw do Oprogramowania z wyjątkiem wyraźnie określonych niniejszą Umową. Wszystkie kopie Oprogramowania wykonane w ramach niniejszej Umowy muszą zawierać te same zastrzeżenia prawne pojawiające się na oraz w Oprogramowaniu. Z wyjątkiem jak określono to w treści niniejszej Umowy, nie powoduje ona przyznania Użytkownikowi żadnych praw do własności intelektualnej Oprogramowania, a Użytkownik potwierdza, że Licencja, w sposób określony niniejszą Umową, nadaje Użytkownikowi jedynie prawo do ograniczonego korzystania z Oprogramowania na zasadach i warunkach określonych niniejszą Umową. Posiadacz praw zastrzega sobie wszelkie prawa, które nie zostały w sposób wyraźny przyznane Użytkownikowi w ramach niniejszej Umowy.
- 10.2 Użytkownik poświadcza, iż kod źródłowy, kod aktywacyjny oraz/lub plik klucza licencyjnego do Oprogramowania są własnością Posiadacza praw oraz stanowią tajemnice handlowe Posiadacza praw. Użytkownik wyraża zgodę na niedokonywanie modyfikacji, adaptacji, tłumaczenia, inżynierii wstecznej, dekompilacji, dezasemblacji lub jakichkolwiek innych prób zmierzających do odkrycia kodu źródłowego Oprogramowania.
- 10.3 Użytkownik wyraża zgodę na niedokonywanie jakichkolwiek modyfikacji lub zmian w Oprogramowaniu. Użytkownik nie ma prawa usuwać lub zmieniać zawiadomień o ochronie praw autorskich ani innych zastrzeżeń prawnych na kopiach Oprogramowania.

11. Prawo właściwe; Arbitraż

Niniejsza Umowa podlega przepisom prawa Federacji Rosyjskiej i będzie interpretowana zgodnie z jego zasadami bez odniesienia do konfliktu przepisów i zasad prawa. Niniejsza Umowa nie podlega przepisom Konwencji Narodów Zjednoczonych w kwestii Umów dotyczących międzynarodowej sprzedaży towarów, których zastosowanie jest wyraźnie wykluczone. Wszelkie spory powstałe w związku z interpretacją lub wykonaniem postanowień niniejszej Umowy lub ich złamania, wyjąwszy zawarcie bezpośredniej ugody, rozstrzygać będzie Trybunał Międzynarodowego Arbitrażu Handlowego przy Izbie Handlu i Przemysłu Federacji Rosyjskiej w Moskwie w Federacji Rosyjskiej. Jakiegokolwiek odszkodowanie przyznane przez sędziego arbitrażowego będzie ostateczne i wiążące dla obu stron, a wyrok w sprawie odszkodowania może być egzekwowany przez jakikolwiek sąd właściwy. Żadne z postanowień Rozdziału 11 nie zabrania Stronie ubiegania się o godziwe zadośćuczynienie w sądzie właściwym ani jego uzyskania, zarówno przed, w trakcie, jak i po zakończeniu postępowania arbitrażowego.

12. Okres wszczynania powództwa.

Żaden rodzaj powództwa, bez względu na formę, będący wynikiem lub związany z transakcjami przeprowadzonymi w ramach niniejszej Umowy, nie może zostać wszczęty przez którąkolwiek ze stron niniejszej Umowy po upływie jednego (1) roku od zaistnienia podstawy powództwa lub odkrycia jej istnienia, z wyjątkiem powództwa o naruszenie praw własności intelektualnej, które może być wszczęte w maksymalnym, mającym zastosowanie okresie dozwolonym przez prawo.

13. Całość umowy; Zasada rozdzielności; Zaniechanie zrzeczenia się praw.

Niniejsza Umowa stanowi całość porozumienia pomiędzy Użytkownikiem a Posiadaczem praw i unieważnia wszelkie uprzednie pisemne lub ustne porozumienia, propozycje, zawiadomienia lub ogłoszenia dotyczące Oprogramowania lub treści niniejszej Umowy. Użytkownik potwierdza, iż zapoznał się z treścią niniejszej Umowy, zrozumiał ją oraz wyraża zgodę na przestrzeganie jej postanowień. Jeżeli któregokolwiek z postanowień niniejszej Umowy zostanie uznane przez sąd właściwy za nieważne lub z jakiegokolwiek powodu niewykonywalne w całości bądź w części, postanowienie takie zostanie wąsko zinterpretowane tak, aby stało się zgodne z prawem oraz egzekwowalne, a całość Umowy nie zostanie wobec powyższego uznana za nieważną, a pozostała jej część zachowa moc obowiązującą ze wszystkimi konsekwencjami prawnymi i podlegać będzie wykonaniu w maksymalnym, dozwolonym prawnie i na zasadach słuszności zakresie, zachowując jednocześnie, w najszerszym prawnie dopuszczalnym zakresie, swoje początkowe intencje. Odstąpienie od jakiegokolwiek postanowienia lub warunku niniejszej Umowy nie będzie ważne o ile nie zostanie sporządzone na piśmie i podpisane przez Użytkownika oraz upoważnionego do tego przedstawiciela Posiadacza praw pod warunkiem, iż zrzeczenie się dochodzenia praw z tytułu naruszenia któregokolwiek z postanowień niniejszej Umowy nie będzie stanowiło zrzeczenia się dochodzenia praw z tytułu jakichkolwiek wcześniejszych, współczesnych ani późniejszych naruszeń. Zaniechanie przez Posiadacza praw nalegania na wykonanie lub ścisłego egzekwowania wykonania któregokolwiek z postanowień niniejszej Umowy bądź jakiegokolwiek prawa, nie będzie interpretowane jako odstąpienie od tego postanowienia lub prawa.

14. Informacje kontaktowe.

W przypadku pytań dotyczących niniejszej Umowy lub chęci skontaktowania się z Posiadaczem praw z jakiegokolwiek powodu, prosimy o kontakt z Biurem Obsługi Klienta:

Kaspersky Lab ZAO, 10 build.1 1st Volokolamsky Proezd
Moskwa, 123060
Federacja Rosyjska
Tel.: +7-495-797-8700
Stel: +7-495-645-7939
Email: info@kaspersky.com
Strona internetowa: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. Wszystkie prawa zastrzeżone. Niniejsze oprogramowanie oraz towarzysząca mu dokumentacja są objęte oraz chronione prawem autorskim i międzynarodowymi umowami o ochronie praw autorskich, a także prawem oraz traktatami dotyczącymi własności intelektualnej.