

Kaspersky Anti-Virus 2012

**KASPERSKY** **lab**

Podręcznik użytkownika

WERSJA APLIKACJI: 12.0

Drogi Użytkowniku,

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

Ostrzeżenie! Dokumentacja ta jest własnością firmy Kaspersky Lab ZAO (zwanej dalej Kaspersky Lab): wszystkie prawa do tego dokumentu są chronione przez prawodawstwo Federacji Rosyjskiej i umowy międzynarodowe. Nielegalne kopiowanie i dystrybucja tego dokumentu, lub jego części, będzie skutkować odpowiedzialnością cywilną, administracyjną lub karną, zgodnie z obowiązującym prawem.

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 ten może zostać zmodyfikowany bez uprzedniego informowania. Najnowsza wersja podręcznika jest zawsze dostępna na stronie <http://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.

W dokumencie tym użyte zostały zastrzeżone znaki towarowe, do których prawa posiadają ich właściciele.

Data korekty dokumentu: 19.04.2011

© 1997-2011 Kaspersky Lab ZAO. Wszelkie prawa zastrzeżone.

<http://www.kaspersky.pl>  
<http://support.kaspersky.com/pl>

# SPIS TREŚCI

W tym podręczniku .....	8
Oznaczenia stosowane w dokumencie.....	10
Źródła informacji dla niezależnych badań.....	11
Forum internetowe firmy Kaspersky Lab .....	12
Kontakt z działem sprzedaży .....	12
Kontakt z zespołem tworzącym dokumentację poprzez e-mail.....	12
Nowości.....	13
Pakiet dystrybucyjny.....	13
Usługi świadczone zarejestrowanym użytkownikom .....	14
Wymagania sprzętowe i programowe.....	14
Standardowa procedura instalacji.....	16
Krok 1. Wyszukiwanie nowszej wersji aplikacji .....	17
Krok 2. Weryfikowanie wymagań systemowych.....	17
Krok 3. Wybieranie typu instalacji .....	18
Krok 4. Przeglądanie treści umowy licencyjnej .....	18
Krok 5. Kaspersky Security Network - Oświadczenie o Gromadzeniu Danych .....	18
Krok 6. Wyszukiwanie niekompatybilnych aplikacji.....	18
Krok 7. Wybieranie folderu docelowego.....	19
Krok 8. Przygotowywanie do instalacji .....	19
Krok 9. Instalowanie.....	20
Krok 10. Finalizowanie instalacji .....	20
Krok 11. Aktywowanie aplikacji.....	20
Krok 12. Rejestrowanie użytkownika .....	20
Krok 13. Finalizowanie procesu aktywacji.....	21
Aktualizowanie poprzedniej wersji Kaspersky Anti-Virus .....	21
Krok 1. Wyszukiwanie nowszej wersji aplikacji .....	22
Krok 2. Weryfikowanie wymagań systemowych.....	22
Krok 3. Wybieranie typu instalacji .....	22
Krok 4. Przeglądanie treści umowy licencyjnej .....	22
Krok 5. Kaspersky Security Network - Oświadczenie o Gromadzeniu Danych .....	23
Krok 6. Wyszukiwanie niekompatybilnych aplikacji.....	23
Krok 7. Wybieranie folderu docelowego.....	23
Krok 8. Przygotowywanie do instalacji .....	24
Krok 9. Instalowanie.....	24
Krok 10. Kończenie działania kreatora.....	24
Niestandardowe scenariusze instalacji.....	25
Rozpoczęcie pracy .....	25
Dezinstalowanie aplikacji.....	25
Krok 1. Zapisywanie danych do ponownego użycia.....	26
Krok 2. Potwierdzenie dezinstalacji aplikacji .....	26
Krok 3. Dezinstalowanie aplikacji. Kończenie dezinstalacji.....	26
Informacje o Umowie licencyjnej .....	27
Informacje o dostarczaniu danych .....	27
Informacje o licencji .....	27
Informacje o kodzie aktywacyjnym .....	28
Ikona obszaru powiadomień paska zadań.....	29

Menu kontekstowe.....	30
Okno główne programu Kaspersky Anti-Virus .....	31
Okna powiadomień i wiadomości wyskakujące .....	32
Okno ustawień aplikacji .....	34
Gadżet Kaspersky Lab .....	35
News Agent .....	36
Włączanie i wyłączanie automatycznego uruchamiania .....	37
Ręczne uruchamianie i zatrzymywanie działania aplikacji.....	37
Diagnostyka i eliminacja problemów w ochronie komputera.....	39
Włączanie i wyłączanie ochrony .....	40
Wstrzymywanie i wznawianie ochrony .....	41
Jak aktywować aplikację.....	43
Jak kupić lub odnowić licencję.....	44
Co zrobić, gdy pojawiają się powiadomienia aplikacji.....	45
Jak aktualizować bazy danych i moduły aplikacji .....	45
Jak przeprowadzić skanowanie obszarów krytycznych komputera w poszukiwaniu wirusów .....	46
Jak skanować plik, folder, dysk lub inny obiekt w poszukiwaniu wirusów.....	46
Jak przeprowadzić pełne skanowanie komputera w poszukiwaniu wirusów .....	48
W jaki sposób wykonać skanowanie komputera w poszukiwaniu luk .....	48
Jak chronić dane osobiste przed kradzieżą .....	49
Ochrona przed phishingiem .....	49
Ochrona przed przechwytywaniem danych wprowadzanych z klawiatury .....	50
Co zrobić, gdy podejrzewasz, że obiekt jest zainfekowany wirusem .....	51
Co zrobić, gdy podejrzewasz, że komputer został zainfekowany .....	52
Jak przywrócić plik, który został usunięty lub wyleczony przez aplikację .....	53
Tworzenie i korzystanie z dysku ratunkowego.....	53
Tworzenie dysku ratunkowego.....	54
Uruchamianie komputera z dysku ratunkowego .....	56
Jak wyświetlić raport z działania aplikacji .....	56
Przywracanie ustawień domyślnych programu.....	57
Przenoszenie ustawień Kaspersky Anti-Virus do produktu zainstalowanego na innym komputerze .....	57
Jak przejść z Kaspersky Anti-Virus do Kaspersky Internet Security .....	58
Przejście do wersji komercyjnej .....	59
Tymczasowe przełączenie do wersji testowej.....	60
Jak używać gadżetu Kaspersky Lab.....	61
Jak sprawdzić reputację aplikacji.....	62
Ogólne ustawienia ochrony .....	64
Ograniczanie dostępu do programu Kaspersky Anti-Virus.....	65
Wybieranie trybu ochrony .....	65
Skanowanie .....	66
Skanowanie antywirusowe.....	66
Wykrywanie luk.....	74
Zarządzanie zadaniami skanowania. Menedżer zadań .....	74
Aktualizacja .....	74
Wybieranie źródła uaktualnień.....	75
Tworzenie terminarza uruchamiania aktualizacji.....	77
Cofanie ostatniej aktualizacji.....	78
Uruchamianie aktualizacji z poziomu konta innego użytkownika .....	78
Korzystanie z serwera proxy .....	79

Ochrona plików.....	79
Włączanie i wyłączanie modułu Ochrona plików.....	80
Automatyczne wstrzymywanie modułu Ochrona plików.....	80
Tworzenie obszaru ochrony modułu Ochrona plików.....	81
Zmienianie i przywracanie poziomu ochrony plików.....	82
Wybieranie trybu skanowania plików.....	82
Używanie analizy heurystycznej.....	83
Wybieranie technologii skanowania plików.....	83
Zmienianie akcji podejmowanej na zainfekowanych plikach.....	83
Skanowanie plików złożonych przez moduł Ochrona plików.....	84
Optymalizacja skanowania plików.....	85
Ochrona poczty.....	85
Włączanie i wyłączanie modułu Ochrona poczty.....	86
Tworzenie obszaru ochrony modułu Ochrona poczty.....	87
Zmienianie i przywracanie poziomu ochrony.....	87
Używanie analizy heurystycznej.....	88
Zmienianie akcji podejmowanej na zainfekowanych wiadomościach e-mail.....	88
Filtrowanie załączników w wiadomościach e-mail.....	88
Skanowanie plików złożonych przez moduł Ochrona poczty.....	89
Skanowanie poczty elektronicznej w programie Microsoft Office Outlook.....	89
Skanowanie poczty elektronicznej w programie The Bat!.....	89
Ochrona WWW.....	90
Włączanie i wyłączanie modułu Ochrona WWW.....	92
Zmienianie i przywracanie poziomu ochrony ruchu sieciowego.....	92
Zmienianie akcji podejmowanej na niebezpiecznych obiektach w ruchu sieciowym.....	92
Sprawdzanie odnośników na stronach internetowych.....	93
Używanie analizy heurystycznej.....	95
Blokowanie niebezpiecznych skryptów.....	95
Optymalizacja skanowania.....	96
Tworzenie listy zaufanych adresów.....	96
Ochrona komunikatorów.....	97
Włączanie i wyłączanie modułu Ochrona komunikatorów.....	97
Tworzenie obszaru ochrony modułu Ochrona komunikatorów.....	97
Sprawdzanie odnośników w wiadomościach przesyłanych poprzez komunikatory internetowe.....	98
Używanie analizy heurystycznej.....	98
Ochrona proaktywna.....	98
Włączanie i wyłączanie modułu Ochrona proaktywna.....	99
Tworzenie grupy zaufanych aplikacji.....	99
Korzystanie z listy niebezpiecznej aktywności.....	99
Zmienianie akcji wykonywanej na niebezpiecznej aktywności aplikacji.....	100
Kontrola systemu.....	100
Włączanie i wyłączanie modułu Kontrola systemu.....	101
Używanie schematów niebezpiecznej aktywności (BBS).....	101
Cofanie działań szkodliwego programu.....	102
Ochrona sieci.....	102
Skanowanie połączeń szyfrowanych.....	103
Konfigurowanie serwera proxy.....	105
Tworzenie listy monitorowanych portów.....	105
Strefa zaufana.....	106

Tworzenie listy zaufanych aplikacji .....	107
Tworzenie reguł wykluczeń .....	107
Wydajność i kompatybilność z innymi aplikacjami .....	108
Wybieranie kategorii wykrywanych zagrożeń .....	108
Oszczędzanie baterii .....	109
Technologia zaawansowanego leczenia .....	109
Zarządzanie zasobami komputera podczas skanowania antywirusowego .....	109
Uruchamianie zadań w tle .....	110
Tryb pełnoekranowy. Profil gracza .....	111
Autoochrona programu Kaspersky Anti-Virus .....	111
Włączanie i wyłączanie autoochrony .....	112
Ochrona przed kontrolą zewnętrzną .....	112
Kwarantanna i Kopia zapasowa .....	112
Przechowywanie obiektów Kwarantanny i Kopii zapasowej .....	113
Pracowanie z plikami poddanymi kwarantannie .....	113
Pracowanie z obiektami w Kopii zapasowej .....	115
Skanowanie plików w Kwarantannie po aktualizacji .....	115
Dodatkowe narzędzia zwiększające bezpieczeństwo komputera .....	116
Czyszczenie śladów aktywności .....	116
Konfigurowanie ustawień przeglądarki dla bezpiecznej pracy .....	118
Cofanie zmian dokonanych przez kreatory .....	119
Raporty .....	120
Tworzenie raportu dla wybranego modułu ochrony .....	121
Filtrowanie danych .....	121
Wyszukiwanie zdarzeń .....	122
Zapisywanie raportu do pliku .....	122
Przechowywanie raportów .....	123
Czyszczenie raportów aplikacji .....	123
Zapisywanie w raporcie zdarzeń informacyjnych .....	123
Konfigurowanie powiadamiania o dostępności raportu .....	124
Wygląd aplikacji. Zarządzanie aktywnymi elementami interfejsu .....	124
Przenikanie okien powiadomień .....	124
Animacja ikony aplikacji w obszarze powiadomień .....	124
Tekst na ekranie logowania Microsoft Windows .....	125
Powiadomienia .....	125
Włączanie i wyłączanie powiadomień .....	125
Konfigurowanie metody powiadamiania .....	126
Wyłączanie otrzymywania nowości .....	127
Kaspersky Security Network .....	127
Włączanie i wyłączanie uczestnictwa w Kaspersky Security Network .....	127
Sprawdzanie połączenia z Kaspersky Security Network .....	128
Informacje o pliku testowym EICAR .....	129
Testowanie działania aplikacji przy pomocy pliku testowego EICAR .....	129
Informacje o typach pliku testowego EICAR .....	131
Jak uzyskać pomoc techniczną .....	132
Korzystanie z pliku śledzenia i skryptu AVZ .....	132
Tworzenie raportu o stanie systemu .....	133
Tworzenie pliku śledzenia .....	133
Wysyłanie plików danych .....	133

Wykonywanie skryptu AVZ .....	134
Pomoc techniczna za pośrednictwem telefonu.....	135
Uzyskiwanie pomocy technicznej poprzez Moje konto .....	135
Pracowanie z aplikacją z poziomu wiersza poleceń .....	137
Aktywowanie aplikacji .....	139
Uruchamianie aplikacji .....	139
Zatrzymywanie działania aplikacji .....	139
Zarządzanie składnikami i zadaniami programu .....	139
Skanowanie antywirusowe.....	141
Aktualizowanie aplikacji .....	143
Cofanie ostatniej aktualizacji.....	144
Eksportowanie ustawień ochrony.....	144
Importowanie ustawień ochrony.....	145
Tworzenie pliku śledzenia .....	145
Przeglądanie pomocy .....	146
Kody zwrotne wiersza poleceń.....	146
Lista powiadomień programu Kaspersky Anti-Virus .....	147
Powiadomienia w dowolnym trybie ochrony.....	147
Powiadomienia w interaktywnym trybie ochrony.....	152

# INFORMACJE O PODRĘCZNIKU

Pozdrowienia od specjalistów z Kaspersky Lab!

Podręcznik ten zawiera informacje o instalacji, konfiguracji i korzystaniu z Kaspersky Anti-Virus. Mamy nadzieję, że informacje zawarte w podręczniku ułatwią Ci pracę z aplikacją.

Celem podręcznika jest:

- pomoc w instalacji, aktywacji i korzystaniu z Kaspersky Anti-Virus;
- zapewnienie szybkiego wyszukiwania informacji dotyczących problemów z aplikacją;
- przedstawienie alternatywnych źródeł informacji o programie i sposobów otrzymania pomocy technicznej.

Do właściwego wykorzystania aplikacji użytkownik powinien posiadać podstawową znajomość obsługi komputera: znać interfejs używanego systemu operacyjnego, znać podstawowe techniki typowe dla tego systemu, wiedzieć jak pracować z pocztą i Internetem.

## W TEJ SEKCJI:

---

W tym podręczniku.....	<a href="#">8</a>
Oznaczenia stosowane w dokumencie .....	<a href="#">10</a>

## W TYM PODRĘCZNIKU

Podręcznik składa się z następujących sekcji.

### Źródła informacji o aplikacji

Sekcja zawiera opis źródeł informacji o aplikacji i listę stron internetowych, na których możesz porozmawiać o programie.

### Kaspersky Anti-Virus

Sekcja opisuje cechy aplikacji i przedstawia krótkie informacje o jej funkcjach i składnikach. Dowiesz się, jakie elementy wchodzi w skład pakietu dystrybucyjnego, oraz jakie usługi są dostępne dla zarejestrowanych użytkowników aplikacji. Sekcja zawiera informacje o wymaganiach sprzętowych i programowych, które komputer musi spełniać, aby instalacja aplikacji była możliwa.

### Instalowanie i dezinstalowanie aplikacji

Sekcja zawiera informacje o sposobach instalacji aplikacji na komputerze oraz o metodach jej dezinstalacji.

### Licencjonowanie aplikacji

Ta sekcja zawiera informacje dotyczące ogólnych zasad związanych z aktywacją aplikacji. Należy zapoznać się z informacjami zawartymi w tej sekcji, aby dowiedzieć się więcej o przeznaczeniu umowy licencyjnej, typach licencji, sposobach aktywacji aplikacji i odnawianiu licencji.

## **Interfejs aplikacji**

Sekcja zawiera informacje o podstawowych elementach interfejsu graficznego aplikacji: ikonie aplikacji, menu kontekstowym ikony aplikacji, oknie głównym, oknie ustawień i oknach powiadomień.

## **Uruchamianie i zatrzymywanie działania aplikacji**

Ta sekcja zawiera informacje o uruchamianiu i zamykaniu aplikacji.

## **Zarządzanie ochroną komputera**

Znaleźć tu można informacje o wykrywaniu zagrożeń dla bezpieczeństwa komputera i o sposobie konfigurowania poziomu ochrony. Zapoznaj się z tą sekcją, aby dowiedzieć się więcej o włączaniu, wyłączeniu i wstrzymywaniu ochrony w trakcie pracy z aplikacją.

## **Rozwiązywanie podstawowych problemów**

Ta sekcja zawiera informacje o rozwiązywaniu najpowszechniejszych problemów związanych z ochroną komputera przy pomocy aplikacji.

## **Zaawansowane ustawienia aplikacji**

Sekcja ta zawiera szczegółowe informacje dotyczące konfigurowania każdego składnika aplikacji.

## **Testowanie działania aplikacji**

Dostępne są tu informacje dotyczące sposobu sprawdzania, czy aplikacja wykrywa wirusy i ich modyfikacje i wykonuje na nich odpowiednie akcje.

## **Kontakt z działem pomocy technicznej**

Sekcja zawiera informacje dotyczące sposobów kontaktu z pomocą techniczną firmy Kaspersky Lab.

## **Dodatek**

Sekcja ta zawiera dodatkowe informacje uzupełniające niniejszy dokument.

## **Słownik**

Jest to miejsce zawierające listę terminów z ich definicjami, które użyte zostały w niniejszym dokumencie.

## **Kaspersky Lab ZAO**

Sekcja zawiera informacje o firmie Kaspersky Lab.

## **Informacje o kodzie firm trzecich**

Z tej sekcji można się dowiedzieć o kodzie firm trzecich wykorzystanym w aplikacji.

## **Indeks**

Sekcja ta umożliwia szybkie odnalezienie potrzebnych informacji w dokumencie.

## OZNACZENIA STOSOWANE W DOKUMENCIE

W tekście znajdują się elementy znaczeniowe, na które należy zwrócić szczególną uwagę - ostrzeżenia, porady, przykłady.

Oznaczenia stosowane w dokumencie służą do wyróżnienia elementów znaczeniowych. Oznaczenia stosowane w dokumencie i przykłady ich użycia przedstawione zostały w poniższej tabeli.

Tabela 1. Oznaczenia stosowane w dokumencie

PRZYKŁADOWY TEKST	OPIS OZNACZEŃ STOSOWANYCH W DOKUMENCIE
Pamiętaj, że...	Ostrzeżenia są wyróżnione kolorem czerwonym i znajdują się w ramkach. Ostrzeżenia zawierają informacje o prawdopodobnie niechcianych akcjach, które mogą prowadzić do utraty danych lub błędów w działaniu komputera.
Zalecamy...	Uwagi znajdują się w ramkach. Uwagi mogą zawierać przydatne porady, zalecenia, szczególne wartości lub pewne ważne cechy działania aplikacji.
<b>Przykład:</b> ...	Przykłady znajdują się na żółtym tle pod nagłówkiem "Przykład".
Aktualizacja to... Występuje zdarzenie Bazy danych są nieaktualne.	Następujące elementy znaczeniowe wyróżnione są w tekście kursywą: <ul style="list-style-type: none"> <li>• nowe pojęcia;</li> <li>• nazwy stanów aplikacji i zdarzeń.</li> </ul>
Wciśnij <b>ENTER</b> . Wciśnij <b>ALT+F4</b> .	Nazwy klawiszy oznaczone są pogrubioną czcionką i wielkimi literami. Nazwy klawiszy połączone znakiem + (plus) oznaczają kombinację klawiszy. Klawisze te należy wciskać jednocześnie.
Kliknij przycisk <b>Włącz</b> .	Nazwy elementów interfejsu aplikacji, takie jak pola do wprowadzania danych, elementy menu i przyciski wyróżnione są pogrubioną czcionką.
➡ W celu skonfigurowania terminarza zadania:	Frazy wprowadzające do instrukcji oznaczone są kursywą i towarzyszy im znak strzałki.
Wprowadź help w wierszu poleceń. Pojawi się następująca wiadomość: Określ datę w formacie dd:mm:rr.	Następujące typy tekstu są wyróżnione specjalną czcionką: <ul style="list-style-type: none"> <li>• tekst wiersza poleceń;</li> <li>• treść wiadomości wyświetlanej na ekranie przez aplikację;</li> <li>• dane, które powinien wprowadzić użytkownik.</li> </ul>
<adres IP Twojego komputera>	Zmienne znajdują się w nawiasach ostrych. Zamiast zmiennej należy wpisywać odpowiadającą jej wartość, pomijając nawiasy.

# ŹRÓDŁA INFORMACJI O APLIKACJI

Sekcja zawiera opis źródeł informacji o aplikacji i listę stron internetowych, na których możesz porozmawiać o programie.

Możesz wybrać dogodne źródło informacji w zależności od tego, jak pilne i ważne jest dane pytanie.

## W TEJ SEKCJI:

Źródła informacji dla niezależnych badań .....	<a href="#">11</a>
Forum internetowe firmy Kaspersky Lab .....	<a href="#">12</a>
Kontakt z działem sprzedaży.....	<a href="#">12</a>
Kontakt z zespołem tworzącym dokumentację poprzez e-mail .....	<a href="#">12</a>

## ŹRÓDŁA INFORMACJI DLA NIEZALEŻNYCH BADAŃ

Do wyszukania informacji dotyczących aplikacji możesz wykorzystać następujące źródła:

- stronę aplikacji na witrynie Kaspersky Lab;
- stronę aplikacji na witrynie internetowej działu pomocy technicznej (Baza Wiedzy);
- pomoc elektroniczną;
- dokumentację.

Jeśli nie potrafisz rozwiązać problemu samodzielnie, zalecamy skontaktowanie się z pomocą techniczną firmy Kaspersky Lab (sekcja "Pomoc techniczna za pośrednictwem telefonu" na stronie [135](#)).

Aby skorzystać ze źródeł informacji dostępnych na witrynie Kaspersky Lab, konieczne jest nawiązanie połączenia z Internetem.

### Strona aplikacji na witrynie Kaspersky Lab

Witryna Kaspersky Lab zawiera osobną stronę dla każdej aplikacji.

Na takiej stronie internetowej ([http://www.kaspersky.pl/kaspersky\\_anti\\_virus](http://www.kaspersky.pl/kaspersky_anti_virus)) znajdziesz ogólne informacje o aplikacji, jej funkcjach i właściwościach.

Strona <http://www.kaspersky.pl> zawiera odnośnik do sklepu internetowego. Możesz w nim kupić lub odnowić licencję dla aplikacji.

### Strona aplikacji na witrynie internetowej działu pomocy technicznej (Baza Wiedzy)

Baza wiedzy jest oddzielną sekcją strony pomocy technicznej, która zawiera zalecenia dotyczące korzystania z aplikacji Kaspersky Lab. Baza wiedzy zawiera odnośniki do artykułów pogrupowane według tematów.

Na stronie internetowej aplikacji w Bazie wiedzy (<http://support.kaspersky.com/pl/kav2012>) możesz przeczytać artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły mogą zawierać odpowiedzi na pytania spoza zakresu programu Kaspersky Anti-Virus, związane z innymi aplikacjami Kaspersky Lab. Mogą zawierać również nowości z działu pomocy technicznej.

### **Pomoc elektroniczna**

Pomoc elektroniczna aplikacji zawiera pliki pomocy.

Pomoc kontekstowa udostępnia informacje o każdym oknie aplikacji, wymienia i opisuje związane z nim ustawienia i listę zadań.

Pełna pomoc zawiera szczegółowe informacje o zarządzaniu ochroną komputera przy pomocy aplikacji.

### **Dokumentacja**

Podręcznik użytkownika zawiera informacje dotyczące instalacji, aktywacji i konfiguracji aplikacji, a także danych operacyjnych aplikacji. Dokument opisuje również interfejs aplikacji i przedstawia sposoby rozwiązywania podstawowych problemów pojawiających się podczas pracy z aplikacją.

## **FORUM INTERNETOWE FIRMY KASPERSKY LAB**

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, można przedyskutować je ze specjalistami firmy Kaspersky Lab lub innymi użytkownikami jej oprogramowania na forum internetowym znajdującym się pod adresem <http://forum.kaspersky.com>.

Na tym forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

## **KONTAKT Z DZIAŁEM SPRZEDAŻY**

Jeśli masz pytania dotyczące wyboru, zakupu lub odnowienia licencji dla aplikacji, skontaktuj się ze specjalistami z działu sprzedaży w jeden z następujących sposobów:

- Dzwoniąc do naszego biura (<http://www.kaspersky.pl/about.html?s=contact>).
- Przesyłając wiadomość ze swoim pytaniem na adres [sprzedaz@kaspersky.pl](mailto:sprzedaz@kaspersky.pl).

Dział sprzedaży czynny jest od poniedziałku do piątku w godzinach 8 - 16.

## **KONTAKT Z ZESPOŁEM TWORZĄCYM DOKUMENTACJĘ POPURZEZ E-MAIL**

Aby skontaktować się z zespołem tworzącym dokumentację, wyślij wiadomość na adres [dokumentacja@kaspersky.pl](mailto:dokumentacja@kaspersky.pl). Jako temat wiadomości podaj "Opinia o dokumentacji: Kaspersky Anti-Virus".

# KASPERSKY ANTI-VIRUS

Sekcja opisuje cechy aplikacji i przedstawia krótkie informacje o jej funkcjach i składnikach. Dowiesz się, jakie elementy wchodzi w skład pakietu dystrybucyjnego, oraz jakie usługi są dostępne dla zarejestrowanych użytkowników aplikacji. Sekcja zawiera informacje o wymaganiach sprzętowych i programowych, które komputer musi spełniać, aby instalacja aplikacji była możliwa.

## W TEJ SEKCJI:

---

Nowości.....	<a href="#">13</a>
Pakiet dystrybucyjny .....	<a href="#">13</a>
Usługi świadczone zarejestrowanym użytkownikom .....	<a href="#">14</a>
Wymagania sprzętowe i programowe .....	<a href="#">14</a>

## Nowości

Nowości w Kaspersky Anti-Virus:

- Udoskonalony interfejs programu Kaspersky Anti-Virus umożliwia szybszy dostęp do funkcji aplikacji.
- Udoskonalono wykonywanie operacji na Kwarantannie i Kopii zapasowej (strona [112](#)): teraz znajdują się one na dwóch oddzielnych zakładkach i każda z nich posiada swój unikatowy obszar.
- Dodano Menedżera zadań do łatwego zarządzania zadaniami w Kaspersky Anti-Virus (sekcja "Zarządzanie zadaniami skanowania. Menedżer zadań" na stronie [74](#)).
- Uczestnictwo w Kaspersky Security Network (strona [127](#)) umożliwia nam zidentyfikowanie reputacji aplikacji i stron internetowych w oparciu o dane otrzymywane od użytkowników z całego świata.
- Podczas włączonej Ochrony WWW można oddzielnie włączyć analizę heurystyczną do sprawdzania stron internetowych w poszukiwaniu elementów phishingu (sekcja "Używanie analizy heurystycznej" na stronie [95](#)). Podczas sprawdzania stron pod kątem phishingu, analiza heurystyczna zostanie zastosowana bez względu na to, czy została włączona dla Ochrony WWW.
- Zmieniono wygląd gadżetu Kaspersky Lab (strona [35](#)).

## PAKIET DYSTRYBUCYJNY

Możesz kupić aplikację na jeden z następujących sposobów:

- **Wersja pudełkowa.** Dostępna w sklepach naszych dystrybutorów.
- **W sklepie internetowym.** Dostępna w sklepie internetowym Kaspersky Lab (<http://www.kaspersky.pl>, sekcja Sklep).

Jeśli zakupiłeś wersję pudełkową aplikacji, pakiet dystrybucyjny zawiera następujące elementy:

- zaklejoną kopertę z płytą instalacyjną, która zawiera pliki aplikacji i dokumentację;
- skróconą wersję Podręcznika użytkownika z kodem aktywacyjnym;
- umowę licencyjną określającą warunki, na których możesz używać zakupionej aplikacji.

Zawartość pakietu dystrybucyjnego może różnić się w zależności od regionu, w którym aplikacja jest rozpowszechniana.

Jeśli kupisz Kaspersky Anti-Virus w sklepie internetowym, skopiuj aplikację ze strony internetowej sklepu. Informacje wymagane do aktywacji aplikacji zostaną przesłane na Twój adres e-mail po dokonaniu płatności.

Aby uzyskać więcej informacji dotyczących zakupu i pakietu dystrybucyjnego, skontaktuj się z działem sprzedaży.

## USŁUGI ŚWIADCZONE ZAREJESTROWANYM UŻYTKOWNIKOM

Po zakupie licencji użytkownika dla aplikacji stajesz się zarejestrowanym użytkownikiem aplikacji Kaspersky Lab i możesz korzystać z następujących usług podczas całego okresu ważności licencji:

- aktualizacji baz danych i otrzymywania nowych wersji aplikacji;
- konsultacji za pośrednictwem telefonu i poczty elektronicznej w sprawach związanych z instalacją, konfiguracją i korzystaniem z aplikacji;
- otrzymywania powiadomień o opublikowaniu nowych aplikacji Kaspersky Lab i nowych wirusach. Aby korzystać z tej usługi, należy na stronie pomocy technicznej wyrazić zgodę na otrzymywanie wiadomości o nowościach od Kaspersky Lab.

Kaspersky Lab nie oferuje konsultacji odnośnie problemów związanych z działaniem systemów operacyjnych, oprogramowania firm trzecich, a także działania różnych technologii.

## WYMAGANIA SPRZĘTOWE I PROGRAMOWE

Aby aplikacja Kaspersky Anti-Virus działała poprawnie, komputer powinien spełniać określone wymagania:

Wymagania ogólne:

- 480 MB wolnego miejsca na dysku twardym (włączając w to 380 MB na dysku systemowym).
- CD / DVD-ROM (aby zainstalować program Kaspersky Anti-Virus z załączonego nośnika CD).
- Dostęp do Internetu (aby aktywować aplikację oraz aktualizować bazy danych i moduły aplikacji).
- Microsoft Windows Explorer 6.0 lub nowszy.
- Microsoft Windows Installer 2.0.

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

- Procesor Intel Pentium 800 MHz 32-bitowy (x86) / 64-bitowy (x64) lub szybszy (lub kompatybilny odpowiednik);

- 512 MB wolnej 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, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- Procesor Intel Pentium 1 GHz 32-bitowy (x86) / 64-bitowy (x64) lub szybszy (lub kompatybilny odpowiednik).
- 1 GB wolnej pamięci RAM (dla 32-bitowych systemów operacyjnych); 2 GB wolnej pamięci RAM (dla 64-bitowych systemów operacyjnych).

Wymagania dla netbooków:

- Procesor Intel Atom 1.6 GHz lub kompatybilny odpowiednik.
- Karta graficzna Intel GMA950 z pamięcią RAM większą bądź równą 64 MB (lub kompatybilny odpowiednik).
- Ekran nie mniejszy niż 10.1".

# INSTALOWANIE I DEZINSTALOWANIE APLIKACJI

Sekcja zawiera informacje o sposobach instalacji aplikacji na komputerze oraz o metodach jej dezinstalacji.

## W TEJ SEKCJI:

Standardowa procedura instalacji .....	<a href="#">16</a>
Aktualizowanie poprzedniej wersji Kaspersky Anti-Virus.....	<a href="#">21</a>
Niestandardowe scenariusze instalacji .....	<a href="#">25</a>
Rozpoczęcie pracy .....	<a href="#">25</a>
Dezinstalowanie aplikacji .....	<a href="#">25</a>

## STANDARDOWA PROCEDURA INSTALACJI

Instalacja Kaspersky Anti-Virus jest przeprowadzana w trybie interaktywnym przy użyciu Kreatora instalacji.

Kreator składa się z szeregu okien (kroków) przełączanych przy pomocy przycisków **Wstecz** i **Dalej**. W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**. W celu zatrzymania kreatora w dowolnym momencie użyj przycisku **Anuluj**.

Jeśli aplikacja chroni więcej niż jeden komputer (maksymalna liczba komputerów jest zależna od posiadanej licencji), należy zainstalować ją w ten sam sposób na wszystkich komputerach. Pamiętaj, że w tym przypadku, zgodnie z umową licencyjną, ważność licencji liczona jest od daty pierwszej aktywacji programu. Kiedy aktywujesz aplikację na drugim komputerze i na następnych, okres ważności licencji zmniejsza się o czas, który upłynął od pierwszej aktywacji. Ważność licencji dla wszystkich zainstalowanych kopii programu skończy się więc w tym samym momencie.

➤ *W celu zainstalowania programu Kaspersky Anti-Virus*

uruchom plik instalacyjny (z rozszerzeniem EXE) znajdujący się na płycie CD zawierającej program.

Proces instalacji programu Kaspersky Anti-Virus z pliku instalacyjnego pobranego z sieci odbywa się w ten sam sposób, co z pliku znajdującego się na CD.

**W TEJ SEKCJI:**

Krok 1. Wyszukiwanie nowszej wersji aplikacji .....	<a href="#">17</a>
Krok 2. Weryfikowanie wymagań systemowych .....	<a href="#">17</a>
Krok 3. Wybieranie typu instalacji .....	<a href="#">18</a>
Krok 4. Przeglądanie treści umowy licencyjnej .....	<a href="#">18</a>
Krok 5. Kaspersky Security Network - Oświadczenie o Gromadzeniu Danych .....	<a href="#">18</a>
Krok 6. Wyszukiwanie niekompatybilnych aplikacji .....	<a href="#">18</a>
Krok 7. Wybieranie folderu docelowego .....	<a href="#">19</a>
Krok 8. Przygotowywanie do instalacji .....	<a href="#">19</a>
Krok 9. Instalowanie .....	<a href="#">20</a>
Krok 10. Finalizowanie instalacji .....	<a href="#">20</a>
Krok 11. Aktywowanie aplikacji .....	<a href="#">20</a>
Krok 12. Rejestrowanie użytkownika .....	<a href="#">20</a>
Krok 13. Finalizowanie procesu aktywacji .....	<a href="#">21</a>

**KROK 1. WYSZUKIWANIE NOWSZEJ WERSJI APLIKACJI**

Przed rozpoczęciem instalacji Kreator instalacji sprawdzi, czy na serwerach aktualizacji Kaspersky Lab znajduje się nowsza wersja Kaspersky Anti-Virus.

Jeżeli program nie odnajdzie nowszej wersji na serwerach aktualizacji Kaspersky Lab, zostanie uruchomiony Kreator instalacji bieżącej wersji.

Jeżeli na serwerach aktualizacji znajduje się nowsza wersja Kaspersky Anti-Virus, zostanie wyświetlone pytanie o jej pobranie i zainstalowanie na komputerze. Zaleca się zainstalowanie nowej wersji aplikacji, ponieważ nowsze wydania zawierają udoskonalenia zapewniające bardziej niezawodną ochronę komputera. Jeżeli anulujesz pobieranie nowej wersji, zostanie uruchomiony Kreator instalacji bieżącej wersji. Jeżeli zdecydujesz się na zainstalowanie nowszej wersji, zostaną pobrane pliki dystrybucyjne produktu, a Kreator instalacji nowej wersji zostanie uruchomiony automatycznie. W celu uzyskania szczegółowych informacji dotyczących procedury instalacji zapoznaj się z odpowiednią dokumentacją.

**KROK 2. WERYFIKOWANIE WYMAGAŃ SYSTEMOWYCH**

Przed zainstalowaniem na Twoim komputerze programu Kaspersky Anti-Virus instalator analizuje system operacyjny i dodatki Service Pack w celu sprawdzenia, czy odpowiadają wymaganiom programowym instalacji (sekcja "Wymagania sprzętowe i programowe" na stronie [14](#)). Dodatkowo instalator sprawdza obecność wymaganego oprogramowania i uprawnienia niezbędne do zainstalowania aplikacji. Jeżeli program ustali, że jakiegokolwiek z wymagań nie jest spełnione, wyświetlony zostanie stosowny komunikat.

Jeśli komputer spełnia wszystkie wymagania, Kreator wyszuka aplikacje, których uruchomienie wraz z Kaspersky Anti-Virus mogłoby wywołać konflikt. Po odnalezieniu takich programów Kaspersky Internet Security zasugeruje, aby usunąć je ręcznie.

W przypadku odnalezienia wcześniejszej wersji Kaspersky Anti-Virus lub Kaspersky Internet Security, wszystkie dane, które mogą zostać wykorzystane przez program Kaspersky Anti-Virus 2012 (dane aktywacyjne, ustawienia programu itd.), zostaną zapisane i użyte podczas instalacji, a wcześniejsza wersja aplikacji zostanie odinstalowana.

## KROK 3. WYBIERANIE TYPU INSTALACJI

Na tym etapie możesz wybrać najbardziej odpowiedni dla Ciebie typ instalacji programu Kaspersky Anti-Virus:

- *Instalacja standardowa.* Po wybraniu tej opcji (zaznaczenie z pola **Zmień ustawienia instalacji** jest usunięte) aplikacja zostanie zainstalowana w całości z ustawieniami zalecanymi przez ekspertów z Kaspersky Lab.
- *Instalacja niestandardowa.* W tym przypadku (zaznaczone jest pole **Zmień ustawienia instalacji**) aplikacja zażąda wskazania foldera, w którym ma zostać zainstalowana (sekcja "Krok 7. Wybieranie folderu docelowego" na stronie [19](#)), i w razie konieczności wyłączenia ochrony procesu instalacji (sekcja "Krok 8. Przygotowywanie do instalacji" na stronie [19](#)).

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

## KROK 4. PRZEGLĄDANIE TREŚCI UMOWY LICENCYJNEJ

Na tym etapie powinieneś przeczytać umowę licencyjną zawieraną między Tobą a firmą Kaspersky Lab.

Przeczytaj uważnie umowę i, w przypadku akceptacji wszystkich jej warunków, kliknij przycisk **Zgadzam się**. Procedura instalacji będzie kontynuowana.

Jeśli nie akceptujesz warunków umowy licencyjnej, anuluj instalację aplikacji, klikając przycisk **Anuluj**.

## KROK 5. KASPERSKY SECURITY NETWORK - OŚWIADCZENIE O GROMADZENIU DANYCH

W tym kroku Kreatora zaproponowane zostanie uczestnictwo w Kaspersky Security Network. Z uczestnictwem wiąże się przesyłanie do firmy Kaspersky Lab informacji o nowych zagrożeniach wykrytych na Twoim komputerze, uruchamianych aplikacjach, pobranych podpisanych aplikacjach i Twoim systemie. Kaspersky Lab gwarantuje, że nie będą wysyłane żadne dane osobiste użytkownika.

Przeczytaj treść Oświadczenia o Gromadzeniu Danych. Aby przeczytać pełną wersję Oświadczenia, kliknij przycisk **Pełna treść Oświadczenia o Gromadzeniu Danych**. Jeżeli zgadzasz się z jego wszystkimi warunkami, w oknie kreatora zaznacz pole **Akceptuję warunki uczestnictwa w Kaspersky Security Network**.

Kliknij przycisk **Dalej**, jeśli wybrałeś instalację niestandardową (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)). Jeżeli wybrałeś instalację standardową, kliknij przycisk **Zainstaluj**. Procedura instalacji będzie kontynuowana.

## KROK 6. WYSZUKIWANIE NIEKOMPATYBILNYCH APLIKACJI

Na tym etapie aplikacja sprawdza, czy na komputerze znajdują się jakieś programy niekompatybilne z Kaspersky Anti-Virus.

Jeśli nie wykryto takich programów, Kreator automatycznie przechodzi do następnego kroku.

Jeśli wykryto jakieś niekompatybilne aplikacje, zostaną one wyświetlone na ekranie i zasugerowane zostanie ich usunięcie. Aplikacje, których Kaspersky Anti-Virus nie może usunąć automatycznie, powinny zostać usunięte ręcznie. Po usunięciu niekompatybilnych aplikacji będziesz musiał ponownie uruchomić komputer w celu kontynuowania instalacji programu Kaspersky Anti-Virus.

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

## KROK 7. WYBIERANIE FOLDERU DOCELOWEGO

Ten krok Kreatora instalacji staje się dostępny po wybraniu instalacji niestandardowej (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)). W instalacji standardowej krok ten jest pomijany, a aplikacja zostaje zainstalowana w folderze domyślnym.

Na tym etapie musisz wybrać folder docelowy, w którym zostanie zainstalowany Kaspersky Anti-Virus. Domyślnie wybrana zostaje następująca ścieżka dostępu:

- <disk>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2012 – dla systemów 32-bitowych;
- <disk> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2012 – dla systemów 64-bitowych.

Aby zainstalować Kaspersky Anti-Virus w innym folderze, wprowadź w odpowiednim polu ścieżkę dostępu lub kliknij przycisk **Przełóżaj** i wskaż folder w oknie, które pojawi się na ekranie.

Pamiętaj o następujących ograniczeniach:

- Aplikacja nie może zostać zainstalowana na dysku sieciowym lub wymiennym, bądź na dyskach wirtualnych (utworzonych przy pomocy polecenia SUBST).
- Zalecamy unikanie instalacji aplikacji do folderu, który zawiera już pliki i inne foldery, ponieważ modyfikowanie jego zawartości będzie wkrótce zablokowane.
- Ścieżka dostępu nie może mieć więcej niż 160 znaków ani zawierać znaków specjalnych /, ?, :, \*, ", >, < lub |.

Aby sprawdzić, czy na dysku jest wystarczająco dużo miejsca potrzebnego do zainstalowania aplikacji, kliknij przycisk **Użycie dysku**. W otwartym oknie wyświetlona zostanie informacja o dostępnym miejscu na dysku. Aby zamknąć okno, kliknij przycisk **OK**.

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

## KROK 8. PRZYGOTOWYWANIE DO INSTALACJI

Ten krok Kreatora instalacji staje się dostępny po wybraniu instalacji niestandardowej (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)). W instalacji standardowej krok ten jest pomijany.

Proces instalacji powinien być chroniony, ponieważ Twój komputer może być zainfekowany szkodliwymi programami mogącymi mieć wpływ na instalację programu Kaspersky Anti-Virus.

Domyślnie włączona jest ochrona procesu instalacji – w oknie Kreatora zaznaczone jest pole **Chroń proces instalacji**.

Zaleca się usunięcie zaznaczenia z tego pola, gdy aplikacja nie może zostać zainstalowana (na przykład podczas instalacji zdalnej przy użyciu Zdalnego pulpitu Windows). Przyczyną takiej sytuacji może być włączona ochrona.

W tym przypadku powinieneś przerwać instalację, uruchomić ją ponownie, zaznaczyć pole **Zmień ustawienia instalacji** w kroku Kreatora Wybierz typ instalacji (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)), a po przejściu do kroku Przygotowywanie do instalacji usunąć zaznaczenie z pola **Chroń proces instalacji**.

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

Podczas instalowania aplikacji na komputerze działającym pod kontrolą systemu Microsoft Windows XP przerwane zostaną aktywne połączenia sieciowe. Większość z przerwanych połączeń zostanie przywrócona.

## KROK 9. INSTALOWANIE

Instalacja programu może zająć trochę czasu. Poczekaj, aż zostanie ona zakończona.

Po zakończeniu instalacji Kreator automatycznie przejdzie do następnego kroku.

Jeśli podczas instalacji wystąpi błąd będący wynikiem działania szkodliwego programu, Kreator instalacji zaoferuje pobranie specjalnego narzędzia *Kaspersky Virus Removal Tool*, które służy do neutralizowania infekcji.

Po wyrażeniu zgody na zainstalowanie tego narzędzia Kreator pobierze je z serwera Kaspersky Lab i automatycznie zainstaluje. W przypadku, gdy Kreator nie będzie mógł pobrać narzędzia, wyświetlony zostanie odnośnik do jego ręcznego pobrania.

Po zakończeniu pracy z narzędziem należy je usunąć i ponownie rozpocząć proces instalacyjny.

## KROK 10. FINALIZOWANIE INSTALACJI

W ostatnim oknie Kreatora zostanie wyświetlona informacja o pomyślnym zakończeniu instalacji aplikacji. Aby uruchomić Kaspersky Anti-Virus, zaznacz pole **Uruchom Kaspersky Anti-Virus** i kliknij przycisk **Zakończ**.

W pewnych przypadkach wymagane będzie ponowne uruchomienie systemu operacyjnego. Jeżeli pole **Uruchom Kaspersky Anti-Virus 2012** jest zaznaczone, aplikacja zostanie automatycznie uruchomiona po ponownym uruchomieniu systemu operacyjnego.

Jeżeli przed zamknięciem Kreatora zaznaczenie z pola zostało usunięte, należy uruchomić aplikację ręcznie (sekcja "Ręczne uruchamianie i zatrzymywanie działania aplikacji" na stronie [37](#)).

## KROK 11. AKTYWOWANIE APLIKACJI

*Aktywacja* to procedura aktywacji licencji, która umożliwia wykorzystanie pełnej wersji aplikacji i wszystkich jej funkcji do momentu wygaśnięcia licencji.

Aby dokonać aktywacji aplikacji, konieczny jest dostęp do Internetu.

Dostępne są następujące opcje aktywacji programu Kaspersky Anti-Virus:

- **Aktywuj wersję komercyjną.** Wybierz tę opcję i wprowadź kod aktywacyjny, jeśli kupiłeś wersję komercyjną.

Jeśli wprowadzisz kod aktywacyjny dla Kaspersky Internet Security, przełączenie do tej aplikacji nastąpi po zakończeniu aktywacji.

- **Aktywuj wersję testową.** Wybierz tę opcję, jeśli chcesz zainstalować wersję testową przed zakupem licencji komercyjnej. Będziesz mógł korzystać z pełnej wersji programu przez czas przeznaczony dla wersji testowej. Po wygaśnięciu licencji testowej nie można aktywować jej ponownie.

## KROK 12. REJESTROWANIE UŻYTKOWNIKA

Krok ten jest dostępny tylko podczas aktywowania komercyjnej wersji aplikacji. Podczas aktywowania wersji testowej jest on pomijany.

Jeżeli chcesz kontaktować się z działem pomocy technicznej Kaspersky Lab, musisz się zarejestrować.

Jeżeli wyrażasz zgodę na rejestrację, w odpowiednich polach wpisz dane rejestracyjne, a następnie kliknij przycisk **Dalej**.

## KROK 13. FINALIZOWANIE PROCESU AKTYWACJI

Kreator aktywacji poinformuje Cię, że program Kaspersky Anti-Virus został pomyślnie aktywowany. Dodatkowo wyświetlane są informacje na temat licencji: typ licencji (komercyjna lub testowa), data wygaśnięcia oraz liczba komputerów, dla których przeznaczona jest licencja.

Jeśli aktywowałeś subskrypcję, informacja o jej stanie będzie wyświetlana w miejscu daty wygaśnięcia licencji.

W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

## AKTUALIZOWANIE POPRZEDNIEJ WERSJI KASPERSKY ANTI-VIRUS

Jeżeli na komputerze zainstalowany jest program Kaspersky Anti-Virus 2010 lub 2011, możesz wykonać jego aktualizację do Kaspersky Anti-Virus 2012. Jeśli posiadasz aktywną licencję dla Kaspersky Anti-Virus 2010 lub 2011, nie musisz aktywować aplikacji: Kreator instalacji automatycznie otrzyma informacje o Twojej licencji z Kaspersky Anti-Virus 2010 lub 2011 i użyje jej podczas procesu instalacji.

Instalacja Kaspersky Anti-Virus jest przeprowadzana w trybie interaktywnym przy użyciu Kreatora instalacji.

Kreator składa się z szeregu okien (kroków) przełączanych przy pomocy przycisków **Wstecz** i **Dalej**. W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**. W celu zatrzymania kreatora w dowolnym momencie użyj przycisku **Anuluj**.

Jeśli aplikacja chroni więcej niż jeden komputer (maksymalna liczba komputerów jest zależna od posiadanej licencji), należy zainstalować ją w ten sam sposób na wszystkich komputerach. Pamiętaj, że w tym przypadku, zgodnie z umową licencyjną, ważność licencji liczona jest od daty pierwszej aktywacji programu. Kiedy aktywujesz aplikację na drugim komputerze i na następnych, okres ważności licencji zmniejsza się o czas, który upłynął od pierwszej aktywacji. Ważność licencji dla wszystkich zainstalowanych kopii programu skończy się więc w tym samym momencie.

### ➤ *W celu zainstalowania programu Kaspersky Anti-Virus*

uruchom plik instalacyjny (z rozszerzeniem EXE) znajdujący się na płycie CD zawierającej program.

Proces instalacji programu Kaspersky Anti-Virus z pliku instalacyjnego pobranego z sieci odbywa się w ten sam sposób, co z pliku znajdującego się na CD.

### W TEJ SEKCJI:

Krok 1. Wyszukiwanie nowszej wersji aplikacji .....	<a href="#">22</a>
Krok 2. Weryfikowanie wymagań systemowych .....	<a href="#">22</a>
Krok 3. Wybieranie typu instalacji .....	<a href="#">22</a>
Krok 4. Przeglądanie treści umowy licencyjnej.....	<a href="#">22</a>
Krok 5. Kaspersky Security Network - Oświadczenie o Gromadzeniu Danych .....	<a href="#">23</a>
Krok 6. Wyszukiwanie niekompatybilnych aplikacji .....	<a href="#">23</a>
Krok 7. Wybieranie folderu docelowego .....	<a href="#">23</a>
Krok 8. Przygotowywanie do instalacji .....	<a href="#">24</a>
Krok 9. Instalowanie .....	<a href="#">24</a>
Krok 10. Kończenie działania kreatora .....	<a href="#">24</a>

## KROK 1. WYSZUKIWANIE NOWSZEJ WERSJI APLIKACJI

Przed rozpoczęciem instalacji Kreator instalacji sprawdzi, czy na serwerach aktualizacji Kaspersky Lab znajduje się nowsza wersja Kaspersky Anti-Virus.

Jeżeli program nie odnajdzie nowszej wersji na serwerach aktualizacji Kaspersky Lab, zostanie uruchomiony Kreator instalacji bieżącej wersji.

Jeżeli na serwerach aktualizacji znajduje się nowsza wersja Kaspersky Anti-Virus, zostanie wyświetlone pytanie o jej pobranie i zainstalowanie na komputerze. Zaleca się zainstalowanie nowej wersji aplikacji, ponieważ nowsze wydania zawierają udoskonalenia zapewniające bardziej niezawodną ochronę komputera. Jeżeli anulujesz pobranie nowej wersji, zostanie uruchomiony Kreator instalacji bieżącej wersji. Jeżeli zdecydujesz się na zainstalowanie nowszej wersji, zostaną pobrane pliki dystrybucyjne produktu, a Kreator instalacji nowej wersji zostanie uruchomiony automatycznie. W celu uzyskania szczegółowych informacji dotyczących procedury instalacji zapoznaj się z odpowiednią dokumentacją.

## KROK 2. WERYFIKOWANIE WYMAGAŃ SYSTEMOWYCH

Przed zainstalowaniem na Twoim komputerze programu Kaspersky Anti-Virus instalator analizuje system operacyjny i dodatki Service Pack w celu sprawdzenia, czy odpowiadają wymaganiom programowym instalacji (sekcja "Wymagania sprzętowe i programowe" na stronie [14](#)). Dodatkowo instalator sprawdza obecność wymaganego oprogramowania i uprawnienia niezbędne do zainstalowania aplikacji. Jeżeli program ustali, że jakiegokolwiek z wymagań nie jest spełnione, wyświetlony zostanie stosowny komunikat.

Jeśli komputer spełnia wszystkie wymagania, Kreator wyszuka aplikacje, których uruchomienie wraz z Kaspersky Anti-Virus mogłoby wywołać konflikt. Po odnalezieniu takich programów Kaspersky Internet Security zasugeruje, aby usunąć je ręcznie.

W przypadku odnalezienia wcześniejszej wersji Kaspersky Anti-Virus lub Kaspersky Internet Security, wszystkie dane, które mogą zostać wykorzystane przez program Kaspersky Anti-Virus 2012 (dane aktywacyjne, ustawienia programu itd.), zostaną zapisane i użyte podczas instalacji, a wcześniejsza wersja aplikacji zostanie odinstalowana.

## KROK 3. WYBIERANIE TYPU INSTALACJI

Na tym etapie możesz wybrać najbardziej odpowiedni dla Ciebie typ instalacji programu Kaspersky Anti-Virus:

- *Instalacja standardowa.* Po wybraniu tej opcji (zaznaczenie z pola **Zmień ustawienia instalacji** jest usunięte) aplikacja zostanie zainstalowana w całości z ustawieniami zalecanymi przez ekspertów z Kaspersky Lab.
- *Instalacja niestandardowa.* W tym przypadku (zaznaczone jest pole **Zmień ustawienia instalacji**) aplikacja zażąda wskazania foldera, w którym ma zostać zainstalowana (sekcja "Krok 7. Wybieranie folderu docelowego" na stronie [19](#)), i w razie konieczności wyłączenia ochrony procesu instalacji (sekcja "Krok 8. Przygotowywanie do instalacji" na stronie [19](#)).

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

## KROK 4. PRZEGLĄDANIE TREŚCI UMOWY LICENCYJNEJ

Na tym etapie powinieneś przeczytać umowę licencyjną zawieraną między Tobą a firmą Kaspersky Lab.

Przeczytaj uważnie umowę i, w przypadku akceptacji wszystkich jej warunków, kliknij przycisk **Zgadzam się**. Procedura instalacji będzie kontynuowana.

Jeśli nie akceptujesz warunków umowy licencyjnej, anuluj instalację aplikacji, klikając przycisk **Anuluj**.

## KROK 5. KASPERSKY SECURITY NETWORK - OŚWIADCZENIE O GROMADZENIU DANYCH

W tym kroku Kreatora zaproponowane zostanie uczestnictwo w Kaspersky Security Network. Z uczestnictwem wiąże się przesyłanie do firmy Kaspersky Lab informacji o nowych zagrożeniach wykrytych na Twoim komputerze, uruchamianych aplikacjach, pobranych podpisanych aplikacjach i Twoim systemie. Kaspersky Lab gwarantuje, że nie będą wysyłane żadne dane osobiste użytkownika.

Przeczytaj treść Oświadczenia o Gromadzeniu Danych. Aby przeczytać pełną wersję Oświadczenia, kliknij przycisk **Pełna treść Oświadczenia o Gromadzeniu Danych**. Jeżeli zgadzasz się z jego wszystkimi warunkami, w oknie kreatora zaznacz pole **Akceptuję warunki uczestnictwa w Kaspersky Security Network**.

Kliknij przycisk **Dalej**, jeśli wybrałeś instalację niestandardową (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)). Jeżeli wybrałeś instalację standardową, kliknij przycisk **Zainstaluj**. Procedura instalacji będzie kontynuowana.

## KROK 6. WYSZUKIWANIE NIEKOMPATYBILNYCH APLIKACJI

Na tym etapie aplikacja sprawdza, czy na komputerze znajdują się jakieś programy niekompatybilne z Kaspersky Anti-Virus.

Jeśli nie wykryto takich programów, Kreator automatycznie przechodzi do następnego kroku.

Jeśli wykryto jakieś niekompatybilne aplikacje, zostaną one wyświetlone na ekranie i zasugerowane zostanie ich usunięcie. Aplikacje, których Kaspersky Anti-Virus nie może usunąć automatycznie, powinny zostać usunięte ręcznie. Po usunięciu niekompatybilnych aplikacji będziesz musiał ponownie uruchomić komputer w celu kontynuowania instalacji programu Kaspersky Anti-Virus.

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

## KROK 7. WYBIERANIE FOLDERU DOCELOWEGO

Ten krok Kreatora instalacji staje się dostępny po wybraniu instalacji niestandardowej (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)). W instalacji standardowej krok ten jest pomijany, a aplikacja zostaje zainstalowana w folderze domyślnym.

Na tym etapie musisz wybrać folder docelowy, w którym zostanie zainstalowany Kaspersky Anti-Virus. Domyślnie wybrana zostaje następująca ścieżka dostępu:

- <dysk>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2012 – dla systemów 32-bitowych;
- <dysk> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2012 – dla systemów 64-bitowych.

Aby zainstalować Kaspersky Anti-Virus w innym folderze, wprowadź w odpowiednim polu ścieżkę dostępu lub kliknij przycisk **Przełączaj** i wskaż folder w oknie, które pojawi się na ekranie.

Pamiętaj o następujących ograniczeniach:

- Aplikacja nie może zostać zainstalowana na dysku sieciowym lub wymiennym, bądź na dyskach wirtualnych (utworzonych przy pomocy polecenia SUBST).
- Zalecamy unikanie instalacji aplikacji do folderu, który zawiera już pliki i inne foldery, ponieważ modyfikowanie jego zawartości będzie wkrótce zablokowane.
- Ścieżka dostępu nie może mieć więcej niż 160 znaków ani zawierać znaków specjalnych /, ?, :, \*, ", >, < lub |.

Aby sprawdzić, czy na dysku jest wystarczająco dużo miejsca potrzebnego do zainstalowania aplikacji, kliknij przycisk **Użycie dysku**. W otwartym oknie wyświetlona zostanie informacja o dostępnym miejscu na dysku. Aby zamknąć okno, kliknij przycisk **OK**.

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

## KROK 8. PRZYGOTOWYWANIE DO INSTALACJI

Ten krok Kreatora instalacji staje się dostępny po wybraniu instalacji niestandardowej (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)). W instalacji standardowej krok ten jest pomijany.

Proces instalacji powinien być chroniony, ponieważ Twój komputer może być zainfekowany szkodliwymi programami mogącymi mieć wpływ na instalację programu Kaspersky Anti-Virus.

Domyślnie włączona jest ochrona procesu instalacji – w oknie Kreatora zaznaczone jest pole **Chroń proces instalacji**.

Zaleca się usunięcie zaznaczenia z tego pola, gdy aplikacja nie może zostać zainstalowana (na przykład podczas instalacji zdalnej przy użyciu Zdalnego pulpitu Windows). Przyczyną takiej sytuacji może być włączona ochrona.

W tym przypadku powinieneś przerwać instalację, uruchomić ją ponownie, zaznaczyć pole **Zmień ustawienia instalacji** w kroku Kreatora Wybierz typ instalacji (sekcja "Krok 3. Wybieranie typu instalacji" na stronie [18](#)), a po przejściu do kroku Przygotowywanie do instalacji usunąć zaznaczenie z pola **Chroń proces instalacji**.

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

Podczas instalowania aplikacji na komputerze działającym pod kontrolą systemu Microsoft Windows XP przerwane zostaną aktywne połączenia sieciowe. Większość z przerwanych połączeń zostanie przywrócona.

## KROK 9. INSTALOWANIE

Instalacja programu może zająć trochę czasu. Poczekaj, aż zostanie ona zakończona.

Po zakończeniu instalacji Kreator automatycznie przejdzie do następnego kroku.

Jeśli podczas instalacji wystąpi błąd będący wynikiem działania szkodliwego programu, Kreator instalacji zaoferuje pobranie specjalnego narzędzia *Kaspersky Virus Removal Tool*, które służy do neutralizowania infekcji.

Po wyrażeniu zgody na zainstalowanie tego narzędzia Kreator pobierze je z serwera Kaspersky Lab i automatycznie zainstaluje. W przypadku, gdy Kreator nie będzie mógł pobrać narzędzia, wyświetlony zostanie odnośnik do jego ręcznego pobrania.

Po zakończeniu pracy z narzędziem należy je usunąć i ponownie rozpocząć proces instalacyjny.

## KROK 10. KOŃCZENIE DZIAŁANIA KREATORA

W ostatnim oknie Kreatora zostanie wyświetlona informacja o pomyślnym zakończeniu instalacji aplikacji. Aby uruchomić Kaspersky Anti-Virus, zaznacz pole **Uruchom Kaspersky Anti-Virus** i kliknij przycisk **Zakończ**.

W pewnych przypadkach wymagane będzie ponowne uruchomienie systemu operacyjnego. Jeżeli pole **Uruchom Kaspersky Anti-Virus 2012** jest zaznaczone, aplikacja zostanie automatycznie uruchomiona po ponownym uruchomieniu systemu operacyjnego.

Jeżeli przed zamknięciem Kreatora zaznaczenie z pola zostało usunięte, należy uruchomić aplikację ręcznie (sekcja "Ręczne uruchamianie i zatrzymywanie działania aplikacji" na stronie [37](#)).

## NIESTANDARDOWE SCENARIUSZE INSTALACJI

Ta sekcja opisuje scenariusze instalacji aplikacji inne niż instalacja standardowa lub aktualizacja z poprzedniej wersji.

### Instalowanie Kaspersky Anti-Virus i aktywowanie go później przy pomocy kodu aktywacyjnego dla Kaspersky Internet Security

Jeśli podczas instalacji Kaspersky Anti-Virus, w kroku Aktywowanie aplikacji wprowadzisz kod aktywacyjny dla Kaspersky Internet Security, wówczas również zostanie uruchomiona procedura przejścia z Kaspersky Anti-Virus do Kaspersky Internet Security.

Jeśli podczas instalacji Kaspersky Anti-Virus, w kroku Aktywowanie aplikacji wybierzesz **Aktywuj później** i aktywujesz aplikację kodem aktywacyjnym dla Kaspersky Internet Security, wówczas również zostanie uruchomiona procedura przejścia z Kaspersky Anti-Virus do Kaspersky Internet Security.

### Instalowanie Kaspersky Anti-Virus 2012 na Kaspersky Internet Security 2010 lub 2011

Jeśli uruchomisz instalację Kaspersky Anti-Virus 2012 na komputerze z zainstalowanym Kaspersky Internet Security 2010 lub 2011 z aktywną licencją, Kreator instalacji wykryje informacje o licencji i zaproponuje wybranie jednej z następujących akcji:

- Użyj bieżącej licencji Kaspersky Internet Security 2010 lub 2011. W tym wypadku uruchomiona zostanie procedura przejścia, skutkująca zainstalowaniem Kaspersky Internet Security 2012 na komputerze. Będziesz mógł używać Kaspersky Internet Security 2012 tak długo, jak licencja na Kaspersky Internet Security 2010 lub 2011 pozostaje ważna.
- Kontynuuj instalację Kaspersky Anti-Virus 2012. W tym wypadku procedura instalacji będzie kontynuowana zgodnie ze standardowym scenariuszem, począwszy od kroku Aktywowanie aplikacji.

## ROZPOCZĘCIE PRACY

Po zakończeniu instalacji aplikacja jest gotowa do użycia. W celu zapewnienia odpowiedniej ochrony Twojego komputera, po zakończonej instalacji i konfiguracji zalecamy przeprowadzić:

- Aktualizację baz danych aplikacji (sekcja "Jak aktualizować bazy danych i moduły aplikacji" na stronie [45](#)).
- Skanowanie komputera w poszukiwaniu wirusów (sekcja "Jak przeprowadzić pełne skanowanie komputera w poszukiwaniu wirusów" na stronie [48](#)) i luk (sekcja "W jaki sposób wykonać skanowanie komputera w poszukiwaniu luk" na stronie [48](#)).
- Sprawdzenie stanu ochrony Twojego komputera oraz wyeliminowanie problemów związanych z ochroną.

## DEZINSTALOWANIE APLIKACJI

Po odinstalowaniu programu Kaspersky Anti-Virus Twój komputer oraz dane osobiste nie będą chronione!

Program Kaspersky Anti-Virus jest dezinstalowany przy pomocy kreatora instalacji.

➤ *W celu uruchomienia Kreatora*

w menu **Start** wybierz **Programy** → **Kaspersky Anti-Virus 2012** → **Usuń Kaspersky Anti-Virus 2012**.

**W TEJ SEKCJI:**

Krok 1. Zapisywanie danych do ponownego użycia .....	<a href="#">26</a>
Krok 2. Potwierdzenie dezinstalacji aplikacji .....	<a href="#">26</a>
Krok 3. Dezinstalowanie aplikacji. Kończenie dezinstalacji .....	<a href="#">26</a>

**KROK 1. ZAPISYWANIE DANYCH DO PONOWNEGO UŻYCIA**

Na tym etapie możesz wskazać, które dane używane przez aplikację chcesz zachować do ponownego użycia podczas kolejnej instalacji programu (np. jego nowszej wersji).

Domyślnie aplikacja jest usuwana całkowicie.

➔ *W celu zapisania danych do ponownego użycia:*

1. Wybierz opcję **Zapisz obiekty aplikacji**.
2. Zaznacz pola obok typów danych, które chcesz zapisać:
  - **Dane aktywacyjne** – dane eliminujące potrzebę ponownej aktywacji aplikacji poprzez automatyczne użycie bieżącej licencji pod warunkiem, że nie wygaśnie ona do momentu następnej instalacji.
  - **Obiekty Kopii zapasowej i Kwarantanny** – pliki sprawdzone przez program i umieszczone w Kwarantannie oraz w miejscu przechowywania kopii zapasowych.
  - **Ustawienia wymagane do działania aplikacji** – ustawienia aplikacji zdefiniowane podczas jej konfiguracji.
  - **Dane iChecker** – pliki zawierające informacje o obiektach przeskanowanych w poszukiwaniu wirusów.

**KROK 2. POTWIERDZENIE DEZINSTALACJI APLIKACJI**

Ponieważ usunięcie aplikacji zagraża bezpieczeństwu komputera oraz Twoich danych osobistych, będziesz musiał potwierdzić jej usunięcie. W tym celu kliknij przycisk **Usuń**.

W celu zatrzymania usuwania aplikacji w dowolnym momencie użyj przycisku **Anuluj**.

**KROK 3. DEZINSTALOWANIE APLIKACJI. KOŃCZENIE DEZINSTALACJI**

Na tym etapie kreator usuwa aplikację z komputera. Zaczekaj do zakończenia procesu dezinstalacji.

Podczas dezinstalacji aplikacji wymagane będzie ponowne uruchomienie systemu operacyjnego. Jeżeli anulujesz restart komputera, zakończenie procedury dezinstalacji zostanie odroczone do czasu ponownego uruchomienia systemu operacyjnego.

# LICENCJONOWANIE APLIKACJI

Ta sekcja zawiera informacje dotyczące ogólnych zasad związanych z aktywacją aplikacji. Należy zapoznać się z informacjami zawartymi w tej sekcji, aby dowiedzieć się więcej o przeznaczeniu umowy licencyjnej, typach licencji, sposobach aktywacji aplikacji i odnawianiu licencji.

## W TEJ SEKCJI:

Informacje o Umowie licencyjnej .....	<a href="#">27</a>
Informacje o dostarczaniu danych.....	<a href="#">27</a>
Informacje o licencji.....	<a href="#">27</a>
Informacje o kodzie aktywacyjnym .....	<a href="#">28</a>

## INFORMACJE O UMOWIE LICENCYJNEJ

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

**Przed rozpoczęciem korzystania z aplikacji przeczytaj dokładnie warunki Umowy licencyjnej.**

Możesz przeczytać warunki Umowy licencyjnej podczas instalacji aplikacji firmy Kaspersky Lab.

Warunki Umowy licencyjnej są uważane za zaakceptowane w następujących przypadkach:

- Po otwarciu koperty zawierającej dysk instalacyjny (jeśli zakupiłeś aplikację w wersji pudełkowej lub u jednego z naszych partnerów).
- Po potwierdzeniu akceptacji treści Umowy licencyjnej podczas instalacji aplikacji.

Jeśli nie akceptujesz warunków Umowy licencyjnej, musisz przerwać instalację aplikacji.

## INFORMACJE O DOSTARCZANIU DANYCH

Aby zwiększyć poziom ochrony w czasie rzeczywistym, należy zaakceptować postanowienia umowy licencyjnej, co wiąże się z wyrażeniem zgody na wysyłanie w trybie automatycznym informacji o sumach kontrolnych przetworzonych obiektów (MD5), informacji niezbędnych do określenia reputacji adresów internetowych, a także danych statystycznych dla ochrony antyspamowej. Wśród dostarczanych informacji nie znajdują się żadne dane prywatne, czy inne poufne informacje. Kaspersky Lab chroni wszystkie zebrane informacje zgodnie z wymaganiami obowiązującego prawa. Więcej informacji znajdziesz na stronie pomocy technicznej: <http://support.kaspersky.com/pl/>.

## INFORMACJE O LICENCJI

*Licencja* to czasowo ograniczone prawo do korzystania z aplikacji, zgodne z Umową licencyjną. Licencja zawiera unikalny kod służący do aktywacji Twojej kopii Kaspersky Anti-Virus.

Licencja nadaje Ci prawo do korzystania z następujących usług:

- Używania aplikacji na jednym lub kilku urządzeniach.

Liczba urządzeń, na których możesz korzystać z aplikacji, jest określona w umowie licencyjnej.

- Kontakt z pomocą techniczną firmy Kaspersky Lab.
- Korzystania z pełnego zestawu usług świadczonych przez firmę Kaspersky Lab lub jej partnerów w trakcie okresu ważności licencji (sekcja "Usługi świadczone zarejestrowanym użytkownikom" na stronie [14](#)).

Zakres świadczonych usług oraz okres ważności licencji aplikacji zależą od typu licencji użytej do aktywacji aplikacji.

Dostępne są następujące typy licencji:

- Testowa - jest to darmowa licencja z ograniczonym czasem ważności, która jest udostępniana w celu zapoznania użytkowników z aplikacją.

Po skopiowaniu aplikacji ze strony <http://www.kaspersky.pl> użytkownik automatycznie staje się właścicielem licencji testowej. Po wygaśnięciu licencji wszystkie funkcje Kaspersky Anti-Virus są blokowane. Aby kontynuować korzystanie z aplikacji, musisz zakupić licencję komercyjną.

- Komercyjna - jest to płatna licencja z ograniczonym czasem ważności, która jest dostępna przy zakupie aplikacji.

Po wygaśnięciu komercyjnej licencji aplikacja działa w trybie ograniczonej funkcjonalności. Wciąż możesz skanować komputer w poszukiwaniu wirusów i używać innych składników aplikacji, ale korzystając jedynie z baz danych zainstalowanych przed wygaśnięciem licencji. Aby kontynuować korzystanie z Kaspersky Anti-Virus, musisz odnowić licencję komercyjną.

Zalecamy odnowienie licencji najpóźniej w dniu wygaśnięcia bieżącej licencji, aby zapewnić najbardziej niezawodną ochronę antywirusową komputera.

## INFORMACJE O KODZIE AKTYWACYJNYM

*Kod aktywacyjny* to kod, który otrzymasz po zakupie licencji komercyjnej dla Kaspersky Anti-Virus. Ten kod jest wymagany do aktywacji aplikacji.

Kod aktywacyjny to alfanumeryczny łańcuch znaków alfabetu łacińskiego w formacie xxxxx-xxxxx-xxxxx-xxxxx.

W zależności od sposobu zakupu aplikacji kod aktywacyjny jest dostarczany w jednej z następujących postaci:

- Jeśli zakupiłeś wersję pudełkową Kaspersky Anti-Virus, kod aktywacyjny jest podany w dokumentacji lub na kopercie zawierającej dysk instalacyjny.
- Jeżeli zakupiłeś Kaspersky Anti-Virus w sklepie internetowym, kod aktywacyjny zostanie wysłany w wiadomości e-mail na adres podany podczas składania zamówienia.

Okres ważności licencji jest liczony od momentu aktywacji aplikacji. Jeśli zakupiłeś licencję przeznaczoną do aktywacji Kaspersky Anti-Virus na kilku urządzeniach, okres ważności licencji będzie liczony od momentu wprowadzenia kodu na pierwszym z tych urządzeń.

Jeżeli po aktywacji utracono lub przypadkowo usunięto kod aktywacyjny, należy przesłać zgłoszenie do pomocy technicznej Kaspersky Lab, korzystając z usługi *Moje konto* (sekcja "Uzyskiwanie pomocy technicznej poprzez *Moje konto*" na stronie [135](#)).

Po zakończeniu aktywacji aplikacji przy pomocy kodu, zostanie Ci przydzielony identyfikator klienta. Identyfikator klienta to osobisty identyfikator użytkownika, który jest niezbędny do uzyskania pomocy technicznej poprzez telefon lub *Moje konto* (sekcja "Uzyskiwanie pomocy technicznej poprzez *Moje konto*" na stronie [135](#)).

# INTERFEJS APLIKACJI

Sekcja zawiera informacje o podstawowych elementach interfejsu graficznego aplikacji: ikonie aplikacji, menu kontekstowym ikony aplikacji, oknie głównym, oknie ustawień i oknach powiadomień.

## W TEJ SEKCJI:

Ikona obszaru powiadomień paska zadań .....	<a href="#">29</a>
Menu kontekstowe .....	<a href="#">30</a>
Okno główne Kaspersky Anti-Virus .....	<a href="#">31</a>
Okna powiadomień i wiadomości wyskakujące .....	<a href="#">32</a>
Okno ustawień aplikacji .....	<a href="#">34</a>
Gadżet Kaspersky Lab .....	<a href="#">35</a>
News Agent .....	<a href="#">36</a>

## IKONA OBSZARU POWIADOMIEŃ PASKA ZADAŃ

Po zainstalowaniu aplikacji, w obszarze powiadomień paska zadań Microsoft Windows pojawi się jej ikona.






Domyślnie w systemie operacyjnym Microsoft Windows 7 ikona aplikacji jest ukryta, ale można ją wyświetlić w celu łatwiejszego dostępu do aplikacji (zobacz dokumentację systemu operacyjnego).

Ikona posiada następujące funkcje:

- Ikona ta jest wskaźnikiem działania aplikacji.
- Ikona umożliwia uzyskanie dostępu do menu kontekstowego, okna głównego aplikacji, a także okna zawierającego najświeższe informacje.

### Wskaźnik działania aplikacji

Ikona służy jako wskaźnik działania aplikacji. Obrazuje ona również stan ochrony oraz podstawowe funkcje wykonywane przez aplikację w danym momencie:

-  – skanowanie wiadomości pocztowej;
-  – skanowanie ruchu WWW;
-  – aktualizowanie baz danych i modułów aplikacji;
-  – konieczność ponownego uruchomienia komputera w celu dokończenia aktualizacji;
-  – wystąpienie błędu w działaniu niektórych składników aplikacji.

Domyślnie ikona jest animowana: na przykład, podczas skanowania wiadomości e-mail pojawia się na niej mały pulsujący symbol listu; podczas pobierania uaktualnień pojawia się na niej obraz obracającej się kuli ziemskiej. Użytkownik może wyłączyć animację ikony (sekcja "Przenikanie okien powiadomień" na stronie [124](#)).


Jeśli animacja jest wyłączona, ikona będzie wyglądać następująco:

 (symbol kolorowy) - włączone są wszystkie lub niektóre składniki ochrony;

 (symbol czarno-biały) - wszystkie składniki ochrony są wyłączone.

## Dostęp do menu kontekstowego oraz okien aplikacji

Użytkownik może użyć tej ikony do otwarcia menu kontekstowego (strona [30](#)), klikając ją prawym przyciskiem myszy, a także do otwarcia okna głównego aplikacji (sekcja "Okno główne programu Kaspersky Anti-Virus" na stronie [31](#)), klikając ją lewym przyciskiem myszy.

Jeżeli dostępne są informacje od firmy Kaspersky Lab, na pasku zadań wyświetlona zostanie ikona . Kliknij ją dwa razy, aby otworzyć News Agent (sekcja "News Agent" na stronie [36](#)).

## MENU KONTEKSTOWE

Menu kontekstowe umożliwia szybki dostęp do różnych działań aplikacji.

Menu kontekstowe programu Kaspersky Anti-Virus zawiera następujące polecenia:

- **Menedżer zadań** – otwiera okno **Menedżer zadań**.
- **Aktualizacja** – uruchamia aktualizację baz danych i modułów aplikacji.
- **Klawiatura wirtualna** – włącza klawiaturę wirtualną.
- **Kaspersky Anti-Virus** – otwiera okno główne aplikacji.
- **Wstrzymaj ochronę / Wznów ochronę** – tymczasowe włączenie / wyłączenie komponentów ochrony w czasie rzeczywistym. Ta opcja menu nie wpływa na aktualizację aplikacji ani na wykonywanie skanowania antywirusowego.
- **Ustawienia** – otwiera okno ustawień aplikacji.
- **Informacje o** – wyświetla okno z informacjami o aplikacji.
- **Nowości** – otwiera okno News agent (sekcja "News Agent" na stronie [36](#)). Ten element menu jest dostępny, jeżeli istnieją nieprzeczytane wiadomości.

- **Zakończ** - zakończenie pracy Kaspersky Anti-Virus (w przypadku wyboru tej opcji, aplikacja zostanie usunięta z pamięci RAM komputera).



Rysunek 1. Menu kontekstowe

Jeżeli w momencie otwierania menu kontekstowego uruchomione jest zadanie skanowania lub aktualizacji, wyświetlana będzie w nim nazwa zadania oraz jego procentowy postęp. Wybranie elementu menu z nazwą zadania umożliwia przejście do okna głównego raportu zawierającego wyniki wykonywania zadania.

- ➔ *W celu otwarcia menu kontekstowego*

przesuń kursor na ikonę programu w obszarze powiadomień paska zadań i kliknij ją prawym przyciskiem myszy.

Domyślnie w systemie operacyjnym Microsoft Windows 7 ikona aplikacji jest ukryta, ale można ją wyświetlić w celu łatwiejszego dostępu do aplikacji (zobacz dokumentację systemu operacyjnego).

## OKNO GŁÓWNE PROGRAMU KASPERSKY ANTI-VIRUS

Okno główne aplikacji zawiera elementy interfejsu oferujące dostęp do wszystkich głównych funkcji programu.

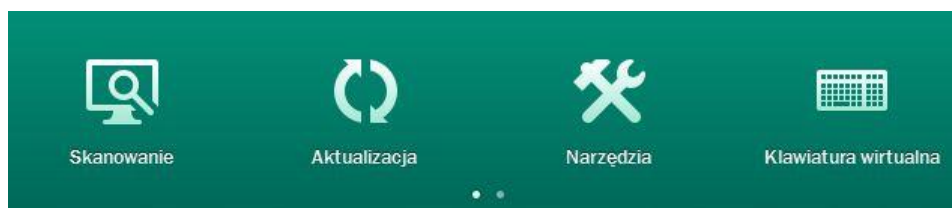
Okno główne programu można podzielić na dwie części:

- W górnej części okna dostępne są informacje o stanie ochrony Twojego komputera.



Rysunek 2. Górna część okna głównego aplikacji

- W dolnej części okna można uzyskać szybki dostęp do głównych funkcji aplikacji (na przykład, zadań skanowania antywirusowego, aktualizacji baz danych i modułów aplikacji).



Rysunek 3. Dolna część okna głównego aplikacji

Jeżeli w dolnej części okna wybrana zostanie jedna z sekcji, otwarte zostanie okno odpowiadające danej funkcji. Można wrócić do wybranej funkcji, klikając przycisk **Wstecz** znajdujący się w lewym górnym rogu okna.

Możesz również używać następujących przycisków i odnośników:

- **Ochrona "w chmurze"** – przełącza do okna z informacjami o Kaspersky Security Network (strona [127](#)).
- **Ustawienia** – otwiera okno ustawień aplikacji (sekcja "Okno ustawień aplikacji" na stronie [34](#)).
- **Raporty** – przełącza do okna raportów z działania aplikacji.
- **Nowości** – otwiera okno News Agent (sekcja "News Agent" na stronie [36](#)). Odsyłacz ten zostanie wyświetlony po otrzymaniu przez aplikację pierwszej informacji.
- **Pomoc** – otwarcie systemu pomocy Kaspersky Anti-Virus.
- **Moje konto** – przejście do panelu klienta (<https://my.kaspersky.com/pl>).
- **Pomoc techniczna** – otwiera okna zawierające informacje o systemie i odnośniki do zasobów informacyjnych Kaspersky Lab (strona pomocy technicznej, forum).
- **Zarządzaj licencją** – otwiera okno aktywacji Kaspersky Anti-Virus i odnowienia licencji.

➔ *Okno główne aplikacji może zostać otwarte przy użyciu jednej z następujących metod:*

- Klikając lewym przyciskiem myszy ikonę programu w obszarze powiadomień paska zadań.

Domyślnie w systemie operacyjnym Microsoft Windows 7 ikona aplikacji jest ukryta, ale można ją wyświetlić w celu łatwiejszego dostępu do aplikacji (zobacz dokumentację systemu operacyjnego).

- Wybierając **Kaspersky Anti-Virus** z menu kontekstowego (sekcja "Menu kontekstowe" na stronie [30](#)).
- Klikając w centrum gadżetu Kaspersky Lab ikonę Kaspersky Anti-Virus (tylko w systemie Microsoft Windows Vista i Microsoft Windows 7).

## OKNA POWIADOMIEŃ I WIADOMOŚCI WYSKAKUJĄCE

Kaspersky Anti-Virus powiadamia Cię o ważnych zdarzeniach zachodzących podczas jego działania przy pomocy *okien powiadomień* i *wiadomości wyskakujących*, które pojawiają się nad ikoną aplikacji w obszarze powiadomień paska zadań.

Okna powiadomień są wyświetlane, gdy w związku ze zdarzeniem można wykonać różne akcje: na przykład, w wypadku wykrycia szkodliwego obiektu możesz zablokować dostęp do niego, usunąć lub spróbować go wyleczyć. Aplikacja oferuje Ci wybranie jednej z dostępnych akcji. Okno powiadomień zniknie z ekranu po wybraniu jednej z akcji.



Rysunek 4. Okno powiadomienia

Wiadomości wyskakujące są wyświetlane, aby poinformować Cię o zdarzeniach niewymagających wyboru akcji. Niektóre wiadomości wyskakujące zawierają odnośniki, których można użyć w celu wykonania proponowanej przez aplikację akcji: na przykład, uruchomić aktualizację baz danych lub zainicjować aktywację aplikacji. Wiadomości wyskakujące znikają z ekranu automatycznie wkrótce po ich pojawieniu się.



Rysunek 5. Wiadomość wyskakująca

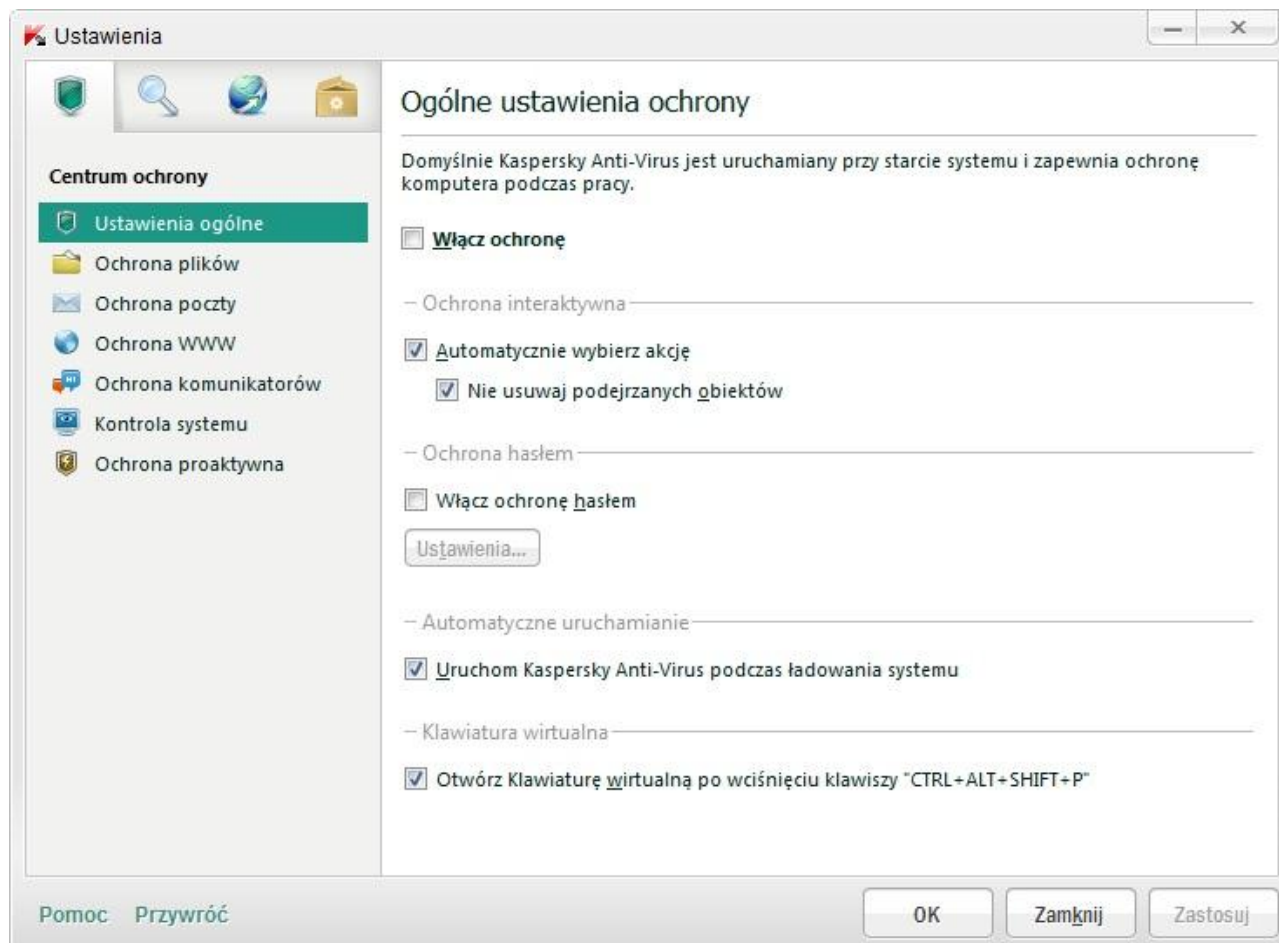
W zależności od stopnia ważności zdarzenia, powiadomienia i wiadomości wyskakujące można podzielić na trzy typy:

- Powiadomienia krytyczne - informują o zdarzeniach ważnych z punktu ochrony komputera: na przykład o wykryciu szkodliwego obiektu lub niebezpiecznej aktywności w systemie. Okna powiadomień krytycznych i wiadomości wyskakujące tego typu mają kolor czerwony.
- Ważne powiadomienia - informują o zdarzeniach potencjalnie ważnych z punktu ochrony komputera: na przykład o wykryciu potencjalnie zainfekowanego obiektu lub podejrzanej aktywności w systemie. Okna ważnych powiadomień i wiadomości wyskakujące tego typu mają kolor żółty.

- Powiadomienia informacyjne – to powiadomienia mające charakter informacyjny. Okna powiadomień i wiadomości wyskakujące tego typu mają kolor zielony.

## OKNO USTAWIEŃ APLIKACJI

Okno ustawień programu Kaspersky Anti-Virus służy do konfigurowania całej aplikacji, poszczególnych składników ochrony, zadań skanowania i aktualizacji oraz do przeprowadzania zadań zaawansowanej konfiguracji (sekcja "Zaawansowane ustawienia aplikacji" na stronie [64](#)).



Rysunek 6. Okno ustawień aplikacji

Okno ustawień aplikacji składa się z dwóch części:

- lewa część okna pozwala na wybranie składnika aplikacji, zadania lub innego elementu, który ma zostać skonfigurowany;
- prawa część okna zawiera listę ustawień dla funkcji wybranej w lewej części okna.

Składniki, zadania i inne elementy lewej części okna zostały podzielone na następujące sekcje:

 – Centrum ochrony;


 – Skanowanie;

 – Aktualizacja;



### – Ustawienia zaawansowane.

Okno ustawień może zostać otwarte przy użyciu jednej z następujących metod:

- kliknij odnośnik **Ustawienia** znajdujący się w górnej części okna głównego aplikacji (sekcja "Okno główne programu Kaspersky Anti-Virus" na stronie [31](#));
- wybierając **Ustawienia** z menu kontekstowego (sekcja "Menu kontekstowe" na stronie [30](#));
- w interfejsie gadżetu Kaspersky Lab kliknij przycisk z ikoną  **Ustawienia** (tylko w systemie Microsoft Windows Vista i Microsoft Windows 7). Do przycisku powinna być przypisana opcja otwierania okna ustawień (sekcja "Jak używać gadżetu Kaspersky Lab" na stronie [61](#)).

## GADŻET KASPERSKY LAB

Podczas używania Kaspersky Anti-Virus na komputerze działającym pod kontrolą systemu Microsoft Windows Vista lub Microsoft Windows 7 możesz używać gadżetu Kaspersky Lab (zwanego dalej *gadżet*). Gadżet umożliwia szybkie uzyskanie dostępu do głównych funkcji aplikacji: wskazania stanu ochrony, skanowania antywirusowego obiektów, raportów z działania aplikacji itd.

Po zainstalowaniu Kaspersky Anti-Virus na komputerze działającym pod kontrolą systemu Microsoft Windows 7 gadżet pojawi się na pulpicie automatycznie. Po zainstalowaniu aplikacji na komputerze z systemem Microsoft Windows Vista należy dodać gadżet do Paska bocznego Microsoft Windows ręcznie (zobacz dokumentację systemu operacyjnego).





Rysunek 7. Gadżet Kaspersky Lab

## NEWS AGENT

Kaspersky Lab będzie informował Cię przy pomocy News Agent o wszystkich ważnych zdarzeniach związanych z programem Kaspersky Anti-Virus i ochroną komputera.

Aplikacja powiadomi Cię o nowościach, wyświetlając w obszarze powiadomień paska zadań specjalną ikonę (zobacz poniżej) i wiadomość wyskakującą. Informacja na temat liczby nieprzeczytanych wiadomości jest również wyświetlana w oknie głównym aplikacji. W interfejsie gadżetu Kaspersky Lab pojawi się ikona nowości.

Możesz przeczytać informacje na jeden z następujących sposobów:

- kliknij ikonę programu  w obszarze powiadomień paska zadań;
- kliknij odnośnik **Przeczytaj wiadomości** w wyskakującej wiadomości;
- kliknij odnośnik **Nowości** znajdujący się w oknie głównym aplikacji;
- kliknij ikonę , która zostanie wyświetlona w centrum gadżetu po pojawieniu się nowości (tylko w systemie Microsoft Windows Vista i Microsoft Windows 7).

Powyższe metody otwierania okna News Agent są dostępne tylko wtedy, gdy istnieją nieprzeczytane wiadomości.

Jeżeli nie chcesz otrzymywać nowości, możesz wyłączyć ich dostarczanie.

# URUCHAMIANIE I ZATRZYMYWANIE DZIAŁANIA APLIKACJI

Ta sekcja zawiera informacje o uruchamianiu i zamykaniu aplikacji.

## W TEJ SEKCJI:

Włączanie i wyłączanie automatycznego uruchamiania.....	<a href="#">37</a>
Ręczne uruchamianie i zatrzymywanie działania aplikacji .....	<a href="#">37</a>

## WŁĄCZANIE I WYŁĄCZANIE AUTOMATYCZNEGO URUCHAMIANIA

Automatyczne uruchamianie aplikacji polega na uruchamianiu programu Kaspersky Anti-Virus po załadowaniu systemu operacyjnego. Jest to tryb domyślny.

➤ *W celu włączenia lub wyłączenia automatycznego uruchamiania aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz podsekcję **Ustawienia ogólne**.
3. Aby wyłączyć automatyczne uruchamianie aplikacji, w prawej części sekcji **Automatyczne uruchamianie** usuń zaznaczenie z pola **Uruchom Kaspersky Anti-Virus przy starcie komputera**. Zaznacz to pole, aby włączyć automatyczne uruchamianie aplikacji.

## RĘCZNE URUCHAMIANIE I ZATRZYMYWANIE DZIAŁANIA APLIKACJI

Specjaliści z firmy Kaspersky Lab zdecydowanie odradzają wyłączenie Kaspersky Anti-Virus, gdyż może to doprowadzić do zainfekowania komputera i utraty danych. Zalecane jest tymczasowe wstrzymanie ochrony komputera, bez zamykania aplikacji.

Jeśli wyłączyłeś automatyczne uruchamianie aplikacji, musisz ręcznie włączyć program Kaspersky Anti-Virus (sekcja "Włączanie i wyłączanie automatycznego uruchamiania" na stronie [37](#)).

➤ *W celu ręcznego uruchomienia aplikacji*

w menu **Start** wybierz **Programy** → **Kaspersky Anti-Virus 2012** → **Kaspersky Anti-Virus 2012**.

➤ *W celu zakończenia działania aplikacji*

kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań. Zostanie otwarte menu kontekstowe, z którego wybierz polecenie **Zakończ**.

Domyślnie w systemie operacyjnym Microsoft Windows 7 ikona aplikacji jest ukryta, ale można ją wyświetlić w celu łatwiejszego dostępu do aplikacji (zobacz dokumentację systemu operacyjnego).

# ZARZĄDZANIE OCHRONĄ KOMPUTERA

Znaleźć tu można informacje o wykrywaniu zagrożeń dla bezpieczeństwa komputera i o sposobie konfigurowania poziomu ochrony. Zapoznaj się z tą sekcją, aby dowiedzieć się więcej o włączaniu, wyłączaniu i wstrzymywaniu ochrony w trakcie pracy z aplikacją.

## W TEJ SEKCJI:

---

Diagnostyka i eliminacja problemów w ochronie komputera .....	<a href="#">39</a>
Włączanie i wyłączanie ochrony .....	<a href="#">40</a>
Wstrzymywanie i wznowianie ochrony .....	<a href="#">41</a>

## DIAGNOSTYKA I ELIMINACJA PROBLEMÓW W OCHRONIE KOMPUTERA

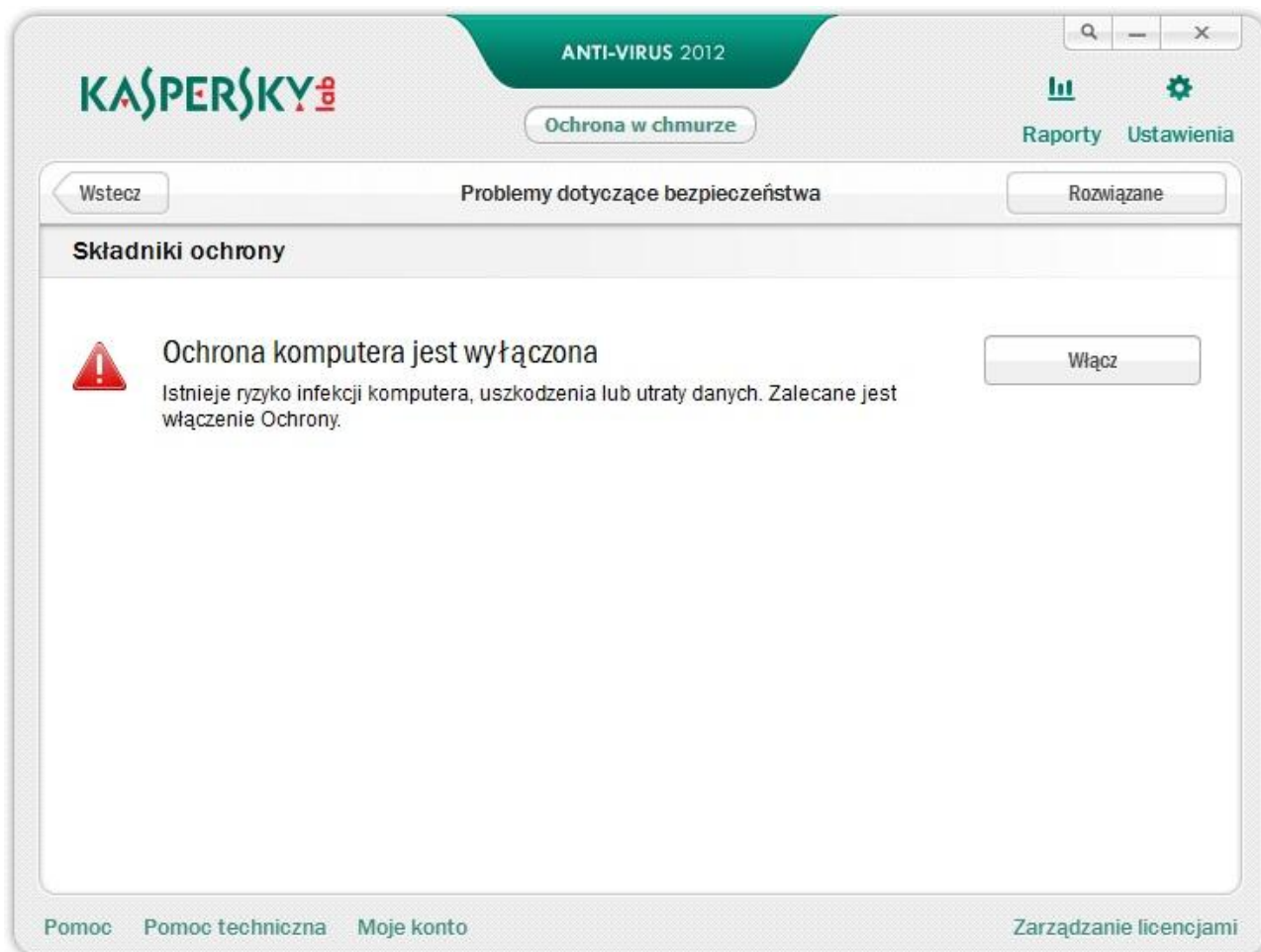
O problemach z ochroną komputera informuje wskaźnik stanu ochrony znajdujący się w lewej części okna głównego aplikacji (sekcja "Okno główne programu Kaspersky Anti-Virus" na stronie [31](#)). Kolor wskaźnika zmienia się w zależności od stanu ochrony komputera: zielony oznacza, że komputer jest chroniony, żółty wskazuje na problemy związane z ochroną, natomiast czerwony informuje o poważnych zagrożeniach dla bezpieczeństwa komputera.



Rysunek 8. Wskaźnik stanu ochrony

Zalecane jest natychmiastowe rozwiązanie problemów i zwalczanie zagrożeń bezpieczeństwa.

Po kliknięciu wskaźnika znajdującego się w oknie głównym aplikacji zostanie otwarte okno **Problemy z ochroną** (zobacz poniższy rysunek), w którym znajdują się szczegółowe informacje dotyczące stanu ochrony komputera oraz propozycje rozwiązania wykrytych problemów i wyleczenia zagrożeń.



Rysunek 9. Okno Problemy z ochroną

Problemy z ochroną są pogrupowane według kategorii. Dla każdego problemu wyświetlone są akcje, które mogą zostać użyte do jego rozwiązania.

## WŁĄCZANIE I WYŁĄCZANIE OCHRONY

Domyślnie program Kaspersky Anti-Virus jest uruchamiany podczas ładowania systemu operacyjnego i chroni Twój komputer do momentu wyłączenia go. Wszystkie składniki ochrony są uruchomione.

Możesz częściowo lub całkowicie wyłączyć ochronę realizowaną przez program Kaspersky Anti-Virus.

Specjaliści z firmy Kaspersky Lab zdecydowanie odradzają wyłączenie Ochrony, gdyż może to doprowadzić do zainfekowania komputera i utraty danych. Zalecane jest wstrzymanie ochrony na określony czas (sekcja "Wstrzymanie i wznawianie ochrony" na stronie [41](#)).

Oznaką wstrzymanej lub wyłączonej ochrony jest:

- nieaktywna (szara) ikona aplikacji w obszarze powiadomień paska zadań (sekcja "Ikona obszaru powiadomień paska zadań" na stronie [29](#));
- czerwony kolor wskaźnika ochrony znajdującego się w górnej części okna głównego programu.

W tym przypadku ochrona jest omawiana w kontekście modułów ochrony. Wyłączenie składników ochrony nie wpływa na działanie zadań skanowania i aktualizacji Kaspersky Anti-Virus.

Możesz włączyć lub wyłączyć ochronę lub pojedynczy składnik aplikacji w oknie ustawień aplikacji (sekcja "Okno ustawień aplikacji" na stronie [34](#)).

➤ *W celu całkowitego włączenia lub wyłączenia ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz podsekcję **Ustawienia ogólne**.
3. Aby wyłączyć ochronę, usuń zaznaczenie z pola **Włącz ochronę**. Aby włączyć ochronę, zaznacz to pole.

➤ *W celu wyłączenia lub włączenia składnika ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł, który ma zostać włączony / wyłączony.
3. W prawej części okna usuń zaznaczenie z pola **Włącz moduł <nazwa modułu>** dla modułu, który chcesz wyłączyć. Jeśli natomiast chcesz włączyć ten składnik, wówczas zaznacz to pole.

## WSTRZYMYWANIE I WZNAWIANIE OCHRONY

Wstrzymanie ochrony oznacza wyłączenie na określony czas wszystkich jej składników.

Oznaką wstrzymanej lub wyłączonej ochrony jest:


- nieaktywna (szara) ikona aplikacji w obszarze powiadomień paska zadań (sekcja "Ikona obszaru powiadomień paska zadań" na stronie [29](#));
- czerwony kolor wskaźnika ochrony znajdującego się w górnej części okna głównego programu.

W tym przypadku ochrona jest omawiana w kontekście modułów ochrony. Wyłączenie składników ochrony nie wpływa na działanie zadań skanowania i aktualizacji Kaspersky Anti-Virus.

Jeżeli podczas wstrzymanej ochrony podjęta zostanie próba nawiązania połączenia internetowego, na ekranie wyświetlone zostanie powiadomienie o jego przerwaniu.

Jeżeli pracujesz na komputerze z zainstalowanym systemem Microsoft Windows Vista lub Microsoft Windows 7, ochrona może zostać wstrzymana przy użyciu gadżetu Kaspersky Lab. W tym celu, do jednego z przycisków gadżetu należy przypisać opcję wstrzymywania ochrony (sekcja "Jak używać gadżetu Kaspersky Lab" na stronie [61](#)).

➤ *W celu wstrzymania ochrony komputera:*

1. Otwórz okno **Wstrzymaj ochronę** przy użyciu jednej z następujących metod:
  - wybierz **Wstrzymaj ochronę** z menu kontekstowego ikony aplikacji (sekcja "Menu kontekstowe" na stronie [30](#));
  - w interfejsie gadżetu Kaspersky Lab kliknij przycisk z ikoną  **Wstrzymaj ochronę** (tylko w systemie Microsoft Windows Vista i Microsoft Windows 7).
2. W oknie **Wstrzymaj ochronę** wybierz przedział czasu, po którym ochrona ma zostać wznowiona:
  - **Wstrzymaj na określony czas** – ochrona zostanie wznowiona po upływie przedziału czasu wybranego z poniższej listy rozwijalnej.

- **Wstrzymaj do restartu** – ochrona zostanie wznowiona po ponownym uruchomieniu systemu (o ile został włączony tryb umożliwiający ładowanie aplikacji podczas uruchomienia komputera (sekcja "Włączanie i wyłączanie automatycznego uruchamiania" na stronie [37](#))).
- **Wstrzymaj** – ochrona nie będzie wznowiana automatycznie.

➔ *W celu wznowienia ochrony komputera*

wyberz **Wznów ochronę** z menu kontekstowego ikony aplikacji (sekcja "Menu kontekstowe" na stronie [30](#)).

Możesz skorzystać z tej metody, jeśli wybrałeś opcję: **Wstrzymaj**, **Wstrzymaj na określony czas** lub **Wstrzymaj do restartu**.

# ROZWIĄZYWANIE PODSTAWOWYCH PROBLEMÓW

Ta sekcja zawiera informacje o rozwiązywaniu najpowszechniejszych problemów związanych z ochroną komputera przy pomocy aplikacji.

## W TEJ SEKCJI:

---

Jak aktywować aplikację .....	<a href="#">43</a>
Jak kupić lub odnowić licencję .....	<a href="#">44</a>
Co zrobić, gdy pojawiają się powiadomienia aplikacji .....	<a href="#">45</a>
Jak aktualizować bazy danych i moduły aplikacji .....	<a href="#">45</a>
Jak przeprowadzić skanowanie obszarów krytycznych komputera w poszukiwaniu wirusów .....	<a href="#">46</a>
Jak skanować plik, folder, dysk lub inny obiekt w poszukiwaniu wirusów .....	<a href="#">46</a>
Jak przeprowadzić pełne skanowanie komputera w poszukiwaniu wirusów .....	<a href="#">48</a>
W jaki sposób wykonać skanowanie komputera w poszukiwaniu luk.....	<a href="#">48</a>
Jak chronić dane osobiste przed kradzieżą.....	<a href="#">49</a>
Co zrobić, gdy podejrzewasz, że obiekt jest zainfekowany wirusem.....	<a href="#">51</a>
Co zrobić, gdy podejrzewasz, że komputer został zainfekowany.....	<a href="#">52</a>
Jak przywrócić plik, który został usunięty lub wyleczony przez aplikację .....	<a href="#">53</a>
Tworzenie i korzystanie z dysku ratunkowego .....	<a href="#">53</a>
Jak wyświetlić raport z działania aplikacji.....	<a href="#">56</a>
Przywracanie ustawień domyślnych programu .....	<a href="#">57</a>
Przenoszenie ustawień Kaspersky Anti-Virus do produktu zainstalowanego na innym komputerze.....	<a href="#">57</a>
Jak przejść z Kaspersky Anti-Virus do Kaspersky Internet Security.....	<a href="#">58</a>
Jak używać gadżetu Kaspersky Lab .....	<a href="#">61</a>
Jak sprawdzić reputację aplikacji .....	<a href="#">62</a>

## JAK AKTYWOWAĆ APLIKACJĘ

*Aktywacja* to procedura aktywacji licencji, która umożliwia wykorzystanie pełnej wersji aplikacji i wszystkich jej funkcji do momentu wygaśnięcia licencji.

Jeśli nie aktywowałeś aplikacji podczas instalacji, możesz zrobić to później. Kaspersky Anti-Virus powiadamia o potrzebie aktywacji aplikacji poprzez wiadomości pojawiające się w obszarze powiadomień paska zadań.

➤ *W celu uruchomienia Kreator aktywacji Kaspersky Anti-Virus:*

- Kliknij odnośnik **Aktywuj** znajdujący się w oknie powiadomień Kaspersky Anti-Virus, które pojawia się w obszarze powiadomień paska zadań.
- W dolnej części okna głównego aplikacji kliknij odnośnik **Wprowadź kod aktywacyjny**. W otwartym oknie **Zarządzaj licencją** kliknij przycisk **Aktywuj aplikację**.

Podczas pracy z Kreatorem aktywacji aplikacji należy zdefiniować parametry ustawień.

### Krok 1. Wprowadź kod aktywacyjny

W odpowiednim polu wprowadź kod aktywacyjny i kliknij przycisk **Dalej**.

### Krok 2. Żądanie aktywacji

Jeśli żądanie aktywacji zostało przesłane pomyślnie, Kreator automatycznie przejdzie do następnego kroku.

### Krok 3. Wprowadzanie danych rejestracyjnych

Rejestracja użytkownika jest konieczna do późniejszego kontaktu z pomocą techniczną. Niezarejestrowani użytkownicy otrzymują jedynie niezbędną pomoc.

Wprowadź swoje dane rejestracyjne i kliknij przycisk **Dalej**.

### Krok 4. Aktywacja

Jeśli aktywacja aplikacji przebiegła pomyślnie, Kreator automatycznie przejdzie do następnego okna.

### Krok 5. Kończenie działania kreatora

To okno wyświetla informacje o wynikach aktywacji: typ używanej licencji i datę jej wygaśnięcia.

W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

## JAK KUPIĆ LUB ODNOWIĆ LICENCJĘ

Jeżeli zainstalowałeś Kaspersky Anti-Virus bez licencji, będziesz mógł ją zakupić w późniejszym czasie. Podczas zakupu licencji otrzymasz kod aktywacyjny, którego należy użyć do aktywacji aplikacji (sekcja "Jak aktywować aplikację" na stronie [43](#)).

Po wygaśnięciu ważności licencji można ją odnowić. Istnieje możliwość zakupu nowej licencji przed wygaśnięciem ważności bieżącego kodu aktywacyjnego. W tym celu należy dodać nowy kod jako zapasowy kod aktywacyjny. Po wygaśnięciu bieżącej licencji program Kaspersky Anti-Virus zostanie automatycznie aktywowany przy użyciu zapasowego kodu aktywacyjnego.

➤ *W celu kupienia licencji:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Zarządzaj licencją** znajdujący się w dolnej części okna.
3. W oknie, które zostanie otwarte, kliknij przycisk **Kup licencję**.

Zostaniesz przeniesiony do sklepu internetowego, w którym możesz kupić licencję.

➤ *W celu dodania zapasowego kodu aktywacyjnego:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Zarządzaj licencją** znajdujący się w dolnej części okna.  
Zostanie otwarte okno **Zarządzaj licencją**.
3. W oknie, które zostanie otwarte, w sekcji **Nowy kod aktywacyjny** kliknij przycisk **Wprowadź kod aktywacyjny**.  
Zostanie uruchomiony Kreator aktywacji aplikacji.
4. W odpowiednim polu wprowadź kod aktywacyjny i kliknij przycisk **Dalej**.  
Kaspersky Anti-Virus prześle dane na serwer aktywacji w celu ich zweryfikowania. Jeżeli weryfikacja zostanie zakończona pomyślnie, Kreator automatycznie przejdzie do następnego kroku.
5. Wybierz **Nowy kod** i kliknij przycisk **Dalej**.
6. Po zakończeniu pracy z Kreatorem kliknij przycisk **Zakończ**.

## CO ZROBIĆ, GDY POJAWIAJĄ SIĘ POWIADOMIENIA APLIKACJI

Powiadomienia, które pojawiają się w obszarze powiadomień paska zadań, informują o zdarzeniach występujących podczas działania aplikacji i wymagają Twojej uwagi. W zależności od wagi zdarzenia występują następujące rodzaje powiadomień:

- Powiadomienia krytyczne - informują o zdarzeniach ważnych z punktu ochrony komputera: na przykład o wykryciu szkodliwego obiektu lub niebezpiecznej aktywności w systemie. Okna powiadomień krytycznych i wiadomości wyskakujące tego typu mają kolor czerwony.
- Ważne powiadomienia - informują o zdarzeniach potencjalnie ważnych z punktu ochrony komputera: na przykład o wykryciu potencjalnie zainfekowanego obiektu lub podejrzanego aktywności w systemie. Okna ważnych powiadomień i wiadomości wyskakujące tego typu mają kolor żółty.
- Powiadomienia informacyjne – to powiadomienia mające charakter informacyjny. Okna powiadomień i wiadomości wyskakujące tego typu mają kolor zielony.

Jeśli takie powiadomienie zostanie wyświetlone, powinieneś wybrać jedną z sugerowanych opcji. Domyślnym wyborem jest opcja zalecana przez ekspertów z firmy Kaspersky Lab.

## JAK AKTUALIZOWAĆ BAZY DANYCH I MODUŁY APLIKACJI

Domyślnie program Kaspersky Anti-Virus automatycznie szuka nowych uaktualnień na specjalnych serwerach Kaspersky Lab. Jeżeli na serwerze znajdują się nowe uaktualnienia, program pobiera je i instaluje w tle. Proces aktualizacji może zostać uruchomiony w każdej chwili.

Aby pobrać uaktualnienia z serwerów Kaspersky Lab, konieczne jest nawiązanie połączenia z Internetem.

➤ *W celu uruchomienia aktualizacji z poziomu menu kontekstowego aplikacji,*

wybierz z niego polecenie **Aktualizacja**.

➤ *W celu uruchomienia aktualizacji z poziomu okna głównego aplikacji:*

1. Otwórz okno główne aplikacji i wybierz w jego dolnej części sekcję **Aktualizacja**.
2. W oknie **Aktualizacja**, które zostanie otwarte, kliknij przycisk **Uruchom aktualizację**.

## JAK PRZEPROWADZIĆ SKANOWANIE OBSZARÓW KRYTYCZNYCH KOMPUTERA W POSZUKIWANIU WIRUSÓW

Skanowanie obszarów krytycznych komputera to inaczej skanowanie następujących obiektów:

- obiektów uruchamianych wraz ze startem systemu operacyjnego;
- pamięci systemowej;
- sektorów startowych dysku;
- obiektów dodanych przez użytkownika (sekcja "Tworzenie listy obiektów przeznaczonych do skanowania" na stronie [69](#)).

Skanowanie obszarów krytycznych może zostać uruchomione przy użyciu jednej z następujących metod:

- korzystając z utworzonego wcześniej skrótu (strona [73](#)).
- z poziomu okna głównego aplikacji (sekcja "Okno główne Kaspersky Anti-Virus" na stronie [31](#)).

➤ *W celu uruchomienia zadania przy pomocy skrótu:*

1. Otwórz okno Eksploratora Windows i przejdź do foldera, w którym został utworzony skrót.
2. Aby uruchomić skanowanie, kliknij dwukrotnie ikonę skrótu.

➤ *W celu uruchomienia zadania skanowania z poziomu okna głównego aplikacji:*

1. Otwórz okno główne aplikacji i wybierz w jego dolnej części sekcję **Skanowanie**.
2. W oknie **Skanowanie**, które zostanie otwarte, w sekcji **Skanowanie obszarów krytycznych** kliknij przycisk



## JAK SKANOWAĆ PLIK, FOLDER, DYSK LUB INNY OBIEKT W POSZUKIWANIU WIRUSÓW

Skanowanie obiektów w poszukiwaniu wirusów możesz uruchomić:

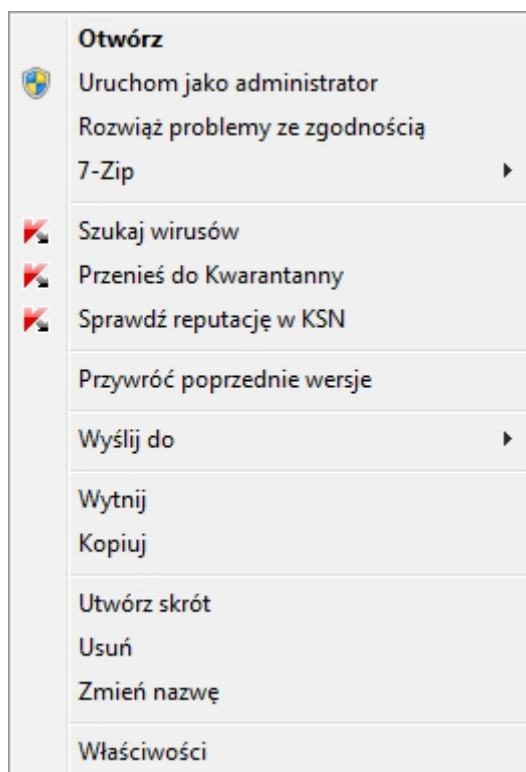
- z poziomu menu kontekstowego obiektu;
- z poziomu okna głównego aplikacji (sekcja "Okno główne Kaspersky Anti-Virus" na stronie [31](#));
- przy użyciu gadżetu Kaspersky Lab (tylko w systemie Microsoft Windows Vista i Microsoft Windows 7).

➤ *W celu uruchomienia zadania skanowania z poziomu menu kontekstowego obiektu:*

1. Otwórz Eksploratora Windows firmy Microsoft i przejdź do folderu zawierającego obiekt, który ma zostać przeskanowany.

- Otwórz menu kontekstowe (patrz rysunek poniżej), klikając obiekt prawym przyciskiem myszy, i wybierz z niego polecenie **Szukaj wirusów**.

Postęp i wyniki wykonywania zadania będą wyświetlane w oknie **Menedżer zadań**.



Rysunek 10. Menu kontekstowe obiektu w Microsoft Windows

➔ W celu uruchomienia skanowania z poziomu okna głównego aplikacji:

- Otwórz okno główne aplikacji i wybierz w jego dolnej części sekcję **Skanowanie**.
- Określ skanowany obiekt przy użyciu jednej z następujących metod:
  - W prawej części okna kliknij odnośnik **wskaż** i w oknie **Skanowanie niestandardowe** zaznacz pola przy folderach i dyskach, które chcesz skanować.

Jeśli okno nie wyświetla żadnych obiektów przeznaczonych do skanowania:

  - Kliknij przycisk **Dodaj**.
  - W oknie **Wybierz obiekt do skanowania**, które zostanie otwarte, wybierz obiekt przeznaczony do skanowania.
  - Przeciągnij obiekt, który ma być skanowany, do okna głównego aplikacji (patrz rysunek poniżej).

Postęp wykonywania zadania będzie wyświetlany w oknie **Menedżer zadań**.



Rysunek 11. Obszar okna Skanowanie, do którego powinien zostać przeciągnięty obiekt do skanowania


- W celu przeskanowania obiektu w poszukiwaniu wirusów przy pomocy gadżetu

przeciągnij na niego obiekt przeznaczony do skanowania.

Postęp wykonywania zadania będzie wyświetlany w oknie **Menedżer zadań**.

## JAK PRZEPROWADZIĆ PEŁNE SKANOWANIE KOMPUTERA W POSZUKIWANIU WIRUSÓW

Pełne skanowanie może zostać uruchomione przy użyciu jednej z następujących metod:

- korzystając z utworzonego wcześniej skrótu (strona [73](#));
- z poziomu okna głównego aplikacji (sekcja "Okno główne Kaspersky Anti-Virus" na stronie [31](#)).
- W celu uruchomienia zadania pełnego skanowania przy pomocy skrótu:
  1. Otwórz okno Eksploratora Windows i przejdź do foldera, w którym został utworzony skrót.
  2. Aby uruchomić skanowanie, kliknij dwukrotnie ikonę skrótu.
- W celu uruchomienia zadania pełnego skanowania z poziomu okna głównego aplikacji:
  1. Otwórz okno główne aplikacji i wybierz w jego dolnej części sekcję **Skanowanie**.
  2. W oknie **Skanowanie**, które zostanie otwarte, w sekcji **Pełne skanowanie** kliknij przycisk .

## W JAKI SPOSÓB WYKONAĆ SKANOWANIE KOMPUTERA W POSZUKIWANIU LUK

*Luki* to niechronione fragmenty kodu oprogramowania, które hakerzy mogą celowo wykorzystać dla własnych celów, na przykład, aby skopiować dane używane w niechronionych aplikacjach. Skanowanie komputera w poszukiwaniu luk umożliwi wykrycie słabych punktów ochrony komputera. Zalecane jest eliminowanie wykrytych luk.

Skanowanie systemu w poszukiwaniu luk możesz uruchomić:


- z poziomu okna głównego aplikacji (sekcja "Okno główne Kaspersky Anti-Virus" na stronie [31](#));

- korzystając z utworzonego wcześniej skrótu (strona [73](#)).

➤ *W celu uruchomienia zadania przy pomocy skrótu:*

1. Otwórz okno Eksploratora Windows i przejdź do foldera, w którym został utworzony skrót.
2. Kliknij dwukrotnie skrót, aby rozpocząć skanowanie systemu w poszukiwaniu luk.

➤ *W celu uruchomienia zadania z poziomu okna głównego aplikacji:*

1. Otwórz okno główne aplikacji i wybierz w jego dolnej części sekcję **Skanowanie**.
2. W oknie **Skanowanie**, które zostanie otwarte, w sekcji **Wykrywanie luk** kliknij przycisk .

## JAK CHRONIĆ DANE OSOBISTE PRZED KRADZIEŻĄ

Przy pomocy Kaspersky Anti-Virus możesz chronić swoje dane osobiste przed kradzieżą; dane takie to między innymi:

- hasła, nazwy użytkownika i inne dane rejestracyjne;
- numery kont i kart bankowych.

Kaspersky Anti-Virus zawiera następujące komponenty i narzędzia, które pomagają chronić Twoje dane osobiste:

- Anti-Phishing. Chroni przed kradzieżą danych z wykorzystaniem phishingu.
- Klawiatura wirtualna. Zapobiega przechwytywaniu danych wprowadzanych z klawiatury.

### W TEJ SEKCJI:

Ochrona przed phishingiem .....	<a href="#">49</a>
Ochrona przed przechwytywaniem danych wprowadzanych z klawiatury .....	<a href="#">50</a>

## OCHRONA PRZED PHISHINGIEM

Ochronę przed nim zapewnia moduł Anti-Phishing, który jest zaimplementowany w komponentach Ochrona WWW i Ochrona komunikatorów. Kaspersky Lab zaleca włączenie opcji sprawdzania w poszukiwaniu elementów phishingowych we wszystkich komponentach ochrony.

➤ *W celu włączenia ochrony przed phishingiem w module Ochrona WWW:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. Zostanie otwarte okno **Ochrona WWW**.
5. W oknie, które zostanie otwarte, na zakładce **Ogólne**, w sekcji **Kaspersky URL Advisor** zaznacz pole **Sprawdź, czy adresy są umieszczone w bazie adresów phishingowych**.

➤ *W celu włączenia ochrony przed phishingiem w module Ochrona komunikatorów:*

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona komunikatorów**.
3. W prawej części okna, w sekcji **Metody skanowania** zaznacz pole **Sprawdź, czy adresy są umieszczone w bazie adresów phishingowych**.

## OCHRONA PRZED PRZECHWYTYWANIEM DANYCH WPROWADZANYCH Z KLAWIATURY

Podczas pracy w Internecie zdarzają się sytuacje, gdy wymagane jest wprowadzenie danych osobowych lub nazwy użytkownika i hasła. Może do tego dojść, na przykład, podczas rejestracji konta, zakupów online lub przeprowadzania operacji finansowych.

W takich sytuacjach istnieje niebezpieczeństwo przechwycenia poufnych informacji przy użyciu keyloggerów - programów rejestrujących wciskanie klawiszy - lub programów służących do przechwytywania sprzętu.

Klawiatura wirtualna pozwala zapobiec przechwyceniu danych wprowadzanych z klawiatury.

Klawiatura wirtualna nie zabezpieczy poufnych danych w przypadku włamania się na stronę, która wymaga wprowadzenia takich danych, ponieważ w takiej sytuacji informacje zostaną zdobyte bezpośrednio przez intruzów.

Wiele aplikacji zaklasyfikowanych jako oprogramowanie spyware posiada funkcje tworzenia zrzutów ekranu, które są następnie wysyłane do hakerów do analizy i wykradania danych osobistych. Klawiatura wirtualna zapobiega przechwyceniu wprowadzanych danych przy użyciu zrzutów ekranu.

Klawiatura wirtualna chroni przed takimi sytuacjami jedynie podczas pracy z przeglądarkami Microsoft Internet Explorer, Mozilla Firefox i Google Chrome.

Klawiatura wirtualna posiada następujące funkcje:

- Do wciskania klawiszy Klawiatury wirtualnej używaj myszy.
- W przeciwieństwie do klawiatur fizycznych, na Klawiaturze wirtualnej nie możesz jednocześnie wcisnąć kilku klawiszy. Jeśli chcesz użyć kombinacji klawiszy (np. **ALT+F4**), najpierw musisz wcisnąć pierwszy klawisz (np. **ALT**), potem kolejny (np. **F4**) i ponownie pierwszy klawisz.. Drugie wciśnięcie klawisza działa podobnie do zwolnienia klawisza na klawiaturze fizycznej.
- Język Klawiatury wirtualnej można przełączyć przy użyciu kombinacji klawiszy **CTRL+SHIFT** (klawisz **SHIFT** powinien być wciśnięty przy użyciu prawego przycisku myszy) lub **CTRL+LEWY ALT** (**LEWY ALT** powinien być wciśnięty przy użyciu lewego przycisku myszy) w zależności od wprowadzonych ustawień.

Klawiatura wirtualna może zostać otwarta przy użyciu następujących metod:

- z poziomu menu kontekstowego ikony aplikacji;
- z poziomu okna głównego aplikacji;
- z poziomu okien przeglądarek internetowych Microsoft Internet Explorer, Mozilla Firefox i Google Chrome;
- przy użyciu kombinacji klawiszy.


➡ *W celu otwarcia Klawiatury wirtualnej z poziomu menu kontekstowego ikony aplikacji*

wyberz z menu kontekstowego ikony aplikacji polecenie **Klawiatura wirtualna**.

➡ *W celu otwarcia Klawiatury wirtualnej z poziomu okna głównego aplikacji*

w dolnej części okna głównego aplikacji wybierz **Klawiatura wirtualna**.

- *W celu otwarcia Klawiatury wirtualnej z poziomu okna przeglądarki*

kliknij przycisk  **Klawiatura wirtualna** znajdujący się na pasku narzędzi programu Microsoft Internet Explorer, Mozilla Firefox lub Google Chrome.

- *W celu otwarcia Klawiatury wirtualnej przy użyciu kombinacji klawiszy*

wciśnij skrót **CTRL+ALT+SHIFT+P**.

## CO ZROBIĆ, GDY PODEJRZEWASZ, ŻE OBIEKT JEST ZAINFEKOWANY WIRUSEM

Jeżeli podejrzewasz, że obiekt jest zainfekowany, przeskanuj go przy użyciu Kaspersky Anti-Virus (sekcja "Jak skanować plik, folder, dysk lub inny obiekt w poszukiwaniu wirusów" na stronie [46](#)).

Jeżeli aplikacja przeskanuje obiekt i uzna go za niezainfekowany, chociaż uważasz, że jest inaczej, możesz wykonać jedną z poniższych akcji:

- Przenieś obiekt do *Kwarantanny*. Obiekty przeniesione do Kwarantanny nie stanowią zagrożenia dla Twojego komputera. Możliwe, że po aktualizacji baz danych Kaspersky Anti-Virus wykryje i wyeliminuje to zagrożenie.
- Wyślij obiekt do *Laboratorium antywirusowego*. Specjaliści przeskanują obiekt. Jeżeli analiza wykaże, że obiekt jest zainfekowany, jego opis zostanie dodany do kolejnej wersji baz danych, która zostanie pobrana z następną aktualizacją (sekcja "Jak aktualizować bazy danych i moduły aplikacji" na stronie [45](#)).

Plik może zostać przeniesiony do Kwarantanny przy użyciu jednej z następujących metod:

- kliknij przycisk **Przenieś do kwarantanny** dostępny w oknie **Kwarantanna**;
- użyj menu kontekstowego pliku.

- *W celu przeniesienia pliku do Kwarantanny z poziomu okna Kwarantanna:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Kwarantanna** kliknij przycisk **Przenieś do kwarantanny**.
4. W otwartym oknie wybierz plik, który chcesz przenieść do Kwarantanny.

- *W celu przeniesienia pliku do Kwarantanny przy użyciu menu kontekstowego:*

1. Otwórz Eksploratora Microsoft Windows i przejdź do foldera zawierającego plik, który ma zostać przeniesiony do Kwarantanny.
2. Otwórz menu kontekstowe pliku, klikając go prawym przyciskiem myszy, i wybierz polecenie **Podaj kwarantannie**.

- *W celu wysłania pliku do Laboratorium antywirusowego:*

1. Przejdź na stronę z formularzem zgłoszenia do laboratorium antywirusowego (<http://support.kaspersky.com/virlab/helpdesk.html?LANG=pl>).
2. Aby wysłać zgłoszenie, postępuj zgodnie z instrukcjami.

## CO ZROBIĆ, GDY PODEJRZEWASZ, ŻE KOMPUTER ZOSTAŁ ZAINFEKOWANY

Jeżeli podejrzewasz, że Twój system operacyjny został uszkodzony w wyniku aktywności szkodliwego oprogramowania lub błędów systemu, użyj kreatora *Znajdź i rozwiąż problemy z systemem Windows*, który usuwa ślady szkodliwych obiektów z systemu. Eksperti firmy Kaspersky Lab zalecają uruchomienie tego Kreatora po wyleczeniu zainfekowanych obiektów w celu upewnienia się, że wszystkie zagrożenia i szkody związane z infekcją zostały naprawione.

Znajdź i rozwiąż problemy z systemem Windows sprawdza system w poszukiwaniu modyfikacji i błędów (takich, jak modyfikacje rozszerzeń plików, zablokowanie środowiska sieciowego oraz panelu sterowania). Modyfikacje oraz błędy mogą być wynikiem aktywności szkodliwego oprogramowania, nieprawidłowej konfiguracji systemu, błędów systemu lub nieprawidłowego działania oprogramowania optymalizującego.

Po sprawdzeniu systemu Kreator przeanalizuje zebrane informacje w celu sprawdzenia, czy są w systemie uszkodzenia wymagające natychmiastowego działania. W oparciu o wyniki tego wyszukiwania tworzona jest lista działań, które muszą być wykonane w celu wyeliminowania tych problemów. Działania te zostaną pogrupowane według kategorii w oparciu o priorytet wykrytego problemu.

➤ *W celu uruchomienia Kreatora przywracania systemu:*

1. Otwórz okno główne aplikacji (strona [31](#)).
2. W dolnej części okna wybierz sekcję **Narzędzia**.
3. W oknie, które zostanie otwarte, w sekcji **Znajdź i rozwiąż problemy z systemem Windows** kliknij przycisk **Uruchom**.

Zostanie otwarte okno Znajdź i rozwiąż problemy z systemem Windows.

Kreator składa się z szeregu okien (kroków) przełączanych przy pomocy przycisków **Wstecz** i **Dalej**. W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**. W celu zatrzymania kreatora w dowolnym momencie użyj przycisku **Anuluj**.

### Krok 1. Rozpoczęcie przywracania systemu

Upewnij się, że wybrana została opcja **Wyszukiwanie problemów związanych z aktywnością szkodliwego oprogramowania**, i kliknij przycisk **Dalej**.

### Krok 2. Wyszukiwanie problemów

Kreator będzie wyszukiwał problemy i uszkodzenia wymagające naprawy. Po zakończeniu wyszukiwania kreator automatycznie przejdzie do następnego kroku.

### Krok 3. Wybieranie działań służących do rozwiązywania problemów

Problemy wykryte w poprzednich krokach kreatora są pogrupowane w oparciu o typ zagrożenia, jakie mogą stwarzać. Dla każdej grupy uszkodzeń Kaspersky Lab zaleca wykonanie sekwencji działań usuwających uszkodzenia. Istnieją trzy grupy działań:

- Szczególnie zalecane działania usuwają problemy stanowiące poważne zagrożenie dla ochrony. Zalecane jest wykonanie wszystkich działań z tej grupy.
- *Zalecane działania* usuwają problemy stanowiące potencjalne zagrożenie. Zalecane jest wykonanie wszystkich działań z tej grupy.
- *Dodatkowe działania* pomagają naprawić uszkodzenia systemu, które obecnie nie stanowią zagrożenia, ale mogą stwarzać problem w przyszłości.

Aby wyświetlić listę akcji z grupy, kliknij ikonę + znajdującą się z lewej strony nazwy grupy.

Aby Kreator wykonał żądane działanie, zaznacz pole znajdujące się z lewej strony opisu odpowiedniej akcji. Domyślnie Kreator wykonuje wszystkie zalecane i szczególnie zalecane akcje. Jeżeli nie chcesz wykonywać pewnych akcji, usuń zaznaczenie z pól obok nich.

Zdecydowanie nie zaleca się usuwania zaznaczeń z pól wybranych domyślnie, gdyż zwiększy to podatność Twojego komputera na ataki.

Po zdefiniowaniu zestawu działań, które Kreator wykona, kliknij przycisk **Dalej**.

#### Krok 4. Rozwiązywanie problemów

Kreator wykona działania wskazane w poprzednim kroku. Może to chwilę potrwać. Po zakończeniu usuwania problemów Kreator automatycznie przejdzie do następnego kroku.

#### Krok 5. Kończenie działania kreatora

W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

## JAK PRZYWRÓCIĆ PLIK, KTÓRY ZOSTAŁ USUNIĘTY LUB WYLECZONY PRZEZ APLIKACJĘ

Kaspersky Lab nie zaleca przywracania usuniętych lub wyleczonych plików, ponieważ mogą one stanowić zagrożenie dla komputera.

Jeżeli chcesz przywrócić usunięty lub wyleczony obiekt, możesz użyć jego kopii zapasowej utworzonej przez aplikację podczas skanowania obiektu.

➔ *W celu przywrócenia pliku, który został usunięty lub wyleczony przez aplikację:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Miejsce przechowywania** wybierz żądany plik z listy i kliknij przycisk **Przywróć**.

## TWORZENIE I KORZYSTANIE Z DYSKU RATUNKOWEGO

Po zainstalowaniu Kaspersky Anti-Virus i wykonaniu pierwszego skanowania komputera, zaleca się utworzenie Dysku ratunkowego.

Dysk ratunkowy to inaczej aplikacja Kaspersky Rescue Disk, która jest zapisywana na nośniku wymiennym (płycie CD lub dysku USB).

Dysk ratunkowy będzie mógł zostać użyty do skanowania i leczenia zainfekowanych komputerów, które nie będą mogły być leczone w inny sposób (na przykład przez aplikacje antywirusowe).

**W TEJ SEKCJI:**

Tworzenie dysku ratunkowego.....	<a href="#">54</a>
Uruchamianie komputera z dysku ratunkowego.....	<a href="#">56</a>

**TWORZENIE DYSKU RATUNKOWEGO**

Tworzenie dysku ratunkowego obejmuje utworzenie obrazu dysku (pliku ISO) z aktualną wersją Kaspersky Rescue Disk oraz zapisanie go na nośniku wymiennym.

Oryginalny obraz dysku można pobrać z serwera Kaspersky Lab lub skopiować go ze źródła lokalnego.

Dysk ratunkowy jest tworzony przy użyciu *Kreatora tworzenia dysku ratunkowego*. Plik rescued.iso utworzony przez Kreatora zostanie zapisany na twardym dysku Twojego komputera:

- w systemie Microsoft Windows XP - w folderze: Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Data\Rdisk\;
- w systemach Microsoft Windows Vista i Microsoft Windows 7 – w następującym folderze: ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

➔ *W celu utworzenia dysku ratunkowego:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Narzędzia**.
3. W oknie, które zostanie otwarte, w sekcji **Kaspersky Rescue Disk** kliknij przycisk **Utwórz**.

Zostanie otwarte okno **Kreator tworzenia dysku ratunkowego**.

Kreator składa się z szeregu okien (kroków) przełączanych przy pomocy przycisków **Wstecz** i **Dalej**. W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**. W celu zatrzymania kreatora w dowolnym momencie użyj przycisku **Anuluj**.

Przyjrzyjmy się dokładniej krokom kreatora.

**Krok 1. Uruchamianie Kreatora. Wyszukiwanie istniejącego obrazu dysku**

W pierwszym oknie kreatora wyświetlana jest informacja o Kaspersky Rescue Disk.

Jeśli kreator wykryje w dedykowanym folderze (zobacz wyżej) istniejący plik ISO dysku ratunkowego, w pierwszym oknie kreatora zostanie wyświetlone pole **Użyj istniejącego pliku ISO**. Zaznacz to pole, aby użyć wykrytego pliku jako oryginalnego obrazu ISO i przejdź bezpośrednio do kroku **Aktualizowane obrazu dysku** (zobacz poniżej). Usuń zaznaczenie z tego pola, jeśli nie chcesz użyć odnalezionego obrazu dysku. Kreator przejdzie do okna **Wybierz źródło obrazu dysku**.

**Krok 2. Wybieranie źródła obrazu dysku ratunkowego**

Jeżeli w pierwszym oknie kreatora zaznaczyłeś pole **Użyj istniejącego pliku ISO**, krok ten zostanie pominięty.

Na tym etapie powinieneś wybrać z listy źródło pliku obrazu:

- Jeżeli posiadasz dysk ratunkowy lub jego obraz na swoim komputerze albo w zasobach sieci lokalnej, wybierz opcję **Kopiuj obraz ISO z dysku lokalnego lub sieciowego**.

- Jeżeli nie posiadasz pliku obrazu ISO dla dysku ratunkowego, wybierz opcję **Pobierz obraz ISO z serwera Kaspersky Lab** w celu pobrania go z serwera Kaspersky Lab (rozmiar tego pliku wynosi około 175 MB).

### Krok 3. Kopiowanie (pobieranie) obrazu dysku

Jeżeli w pierwszym oknie kreatora zaznaczyłeś pole **Użyj istniejącego pliku ISO**, krok ten zostanie pominięty.

Jeżeli w poprzednim kroku wybrałeś opcję **Kopiuj obraz ISO z dysku lokalnego lub sieciowego**, kliknij przycisk **Przełóżaj**. Po zdefiniowaniu ścieżki dostępu do pliku kliknij przycisk **Dalej**. Postęp kopiowania obrazu dysku będzie wyświetlany w oknie kreatora.

Jeżeli w poprzednim kroku wybrałeś opcję **Pobierz obraz ISO z serwera Kaspersky Lab**, zostanie wyświetlone okno postępu procesu pobierania obrazu dysku.

Po zakończeniu kopiowania lub pobierania obrazu ISO, Kreator automatycznie przejdzie do kolejnego kroku.

### Krok 4. Aktualizowanie pliku obrazu ISO

Aktualizacja pliku obrazu ISO składa się na następujące działania:

- aktualizację antywirusowych baz danych;
- aktualizację plików konfiguracyjnych.

Pliki konfiguracyjne określają, czy komputer może być uruchomiony z nośnika wymiennego (np. płyty CD / DVD lub dysku USB), na którym znajduje się Kaspersky Rescue Disk utworzony przez Kreator.

Podczas aktualizacji antywirusowych baz danych wykorzystywane są najnowsze uaktualnienia pobrane przez program Kaspersky Anti-Virus. Jeżeli bazy danych są bardzo stare, zalecane jest najpierw przeprowadzenie aktualizacji, a następnie ponowne uruchomienie Kreatora tworzenia dysku ratunkowego.

W celu rozpoczęcia aktualizacji pliku ISO kliknij przycisk **Dalej**. Postęp wykonywania zadania będzie wyświetlany w oknie Kreatora.

### Krok 5. Nagrywanie obrazu dysku na nośniku danych

W tym oknie kreator informuje Cię o pomyślnym zakończeniu tworzenia obrazu dysku i proponuje nagranie go na nośniku danych.

Wskaż nośnik, na którym ma zostać nagrany Kaspersky Rescue Disk:

- W celu nagrania obrazu dysku na płycie CD / DVD wybierz opcję **Nagraj na CD / DVD**, a następnie wskaż nośnik, na którym chcesz nagrać obraz dysku.
- Aby nagrać obraz dysku na dysku flash USB, wybierz opcję **Zapisz na dysku flash USB** i wskaż żądane urządzenie.

Specjaliści z Kaspersky Lab zalecają, aby nie nagrywać obrazu ISO na urządzeniach, które nie są przeznaczone do przechowywania danych, takich jak smartfony, telefony komórkowe, PDA czy odtwarzacze mp3. Nagrywanie obrazów ISO na takich urządzeniach może prowadzić do ich późniejszego nieprawidłowego funkcjonowania.

- Aby nagrać obraz ISO na dysku twardym znajdującym się na komputerze lub innym dysku dostępnym poprzez sieć, wybierz opcję **Zapisz obraz dysku do pliku na dysku lokalnym lub sieciowym** i wskaż folder, w którym chcesz zapisać obraz dysku, oraz nazwę pliku ISO.

### Krok 6. Kończenie działania kreatora

W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**. Nowo utworzony dysk ratunkowy może zostać użyty do uruchomienia komputera (strona [56](#)), jeżeli nie można tego zrobić w trybie normalnym ze względu na duże spustoszenie w komputerze, jakie spowodowały wirusy lub szkodliwe programy.

## URUCHAMIANIE KOMPUTERA Z DYSKU RATUNKOWEGO

Jeżeli fakt zainfekowania wirusem uniemożliwia normalne uruchomienie systemu operacyjnego, skorzystaj z dysku ratunkowego.

Aby uruchomić system operacyjny, należy użyć nośnika CD / DVD lub dysku USB zawierającego nagrany plik obrazu dysku ratunkowego (sekcja "Tworzenie dysku ratunkowego" na stronie [54](#)).

Uruchomienie komputera z nośnika wymiennego nie zawsze jest możliwe. W szczególności tryb ten nie jest obsługiwany przez starsze modele komputerów. Przed wyłączeniem komputera dla jego ponownego uruchomienia z dysku przenośnego upewnij się, że może to być wykonane.

➔ *W celu uruchomienia komputera z dysku ratunkowego:*

1. W ustawieniach BIOS-u włącz opcję uruchamiania z płyty CD / DVD lub urządzenia USB (szczegółowe informacje znajdziesz w instrukcji obsługi płyty głównej zainstalowanej w Twoim komputerze).
2. Włóż dysk CD / DVD do napędu lub podłącz dysk USB zawierający obraz dysku ratunkowego.
3. Uruchom ponownie komputer.


W celu uzyskania bardziej szczegółowych informacji związanych z dyskiem ratunkowym zapoznaj się z rozdziałem pomocy poświęconym temu zagadnieniu.

## JAK WYŚWIETLIĆ RAPORT Z DZIAŁANIA APLIKACJI

Kaspersky Anti-Virus tworzy raporty z działania każdego komponentu. Z raportu możesz się dowiedzieć, na przykład, ile szkodliwych obiektów zostało wykrytych i wyeliminowanych przez aplikację w określonym przedziale czasu, ile razy aplikacja została zaktualizowana, ile wiadomości zawierających spam zostało wykrytych oraz wiele innych.

Jeżeli pracujesz na komputerze z zainstalowanym systemem Microsoft Windows Vista lub Microsoft Windows 7, raporty mogą zostać otwarte przy użyciu gadżetu Kaspersky Lab. W tym celu należy tak skonfigurować gadżet, aby do jednego z jego przycisków została przypisana opcja otwierania okna raportów (sekcja "Jak używać gadżetu Kaspersky Lab" na stronie [61](#)).

➔ *W celu wyświetlenia raportu z działania aplikacji:*

1. Otwórz okno **Raporty** przy użyciu jednej z następujących metod:
  - kliknij odnośnik **Raporty** znajdujący się w górnej części okna głównego aplikacji;
  - w interfejsie gadżetu Kaspersky Lab kliknij przycisk z ikoną  **Raporty** (tylko w systemie Microsoft Windows Vista i Microsoft Windows 7).

Okno **Raporty** wyświetla raporty z działania aplikacji w formie wykresów.

2. Jeżeli chcesz wyświetlić raport szczegółowy z działania aplikacji (na przykład raport dotyczący działania pojedynczego komponentu), kliknij przycisk **Raport szczegółowy** znajdujący się w dolnej części zakładki **Raport**.

Zostanie otwarte okno **Raport szczegółowy** zawierające dane przedstawione w postaci tabeli. W zależności od potrzeb, możesz wybrać różne sposoby sortowania wpisów.

## PRZYWRACANIE USTAWIEŃ DOMYŚLNYCH PROGRAMU

W każdej chwili możesz przywrócić ustawienia domyślne programu Kaspersky Anti-Virus zalecane przez specjalistów z Kaspersky Lab. W tym celu należy uruchomić Kreator konfiguracji aplikacji.

Po zakończeniu pracy Kreatora poziom ochrony wszystkich modułów zostaje ustawiony na **Zalecany**. Podczas przywracania zalecanego poziomu ochrony można zapisać wcześniej zdefiniowane wartości dla niektórych ustawień modułów aplikacji.

◆ *W celu przywrócenia ustawień domyślnych aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. Uruchom Kreator konfiguracji aplikacji przy użyciu jednej z następujących metod:
  - w dolnej części okna kliknij przycisk **Przywróć**;
  - w lewej części okna wybierz w sekcji **Ustawienia zaawansowane**, podsekcję **Zarządzanie ustawieniami**, a następnie kliknij przycisk **Przywróć** znajdujący się w sekcji **Przywróć ustawienia domyślne**.

Przyjrzyjmy się dokładniej krokom kreatora.

### Krok 1. Uruchamianie Kreatora

Kliknij przycisk **Dalej**, aby przejść do kolejnego kroku Kreatora.

### Krok 2. Przywracanie ustawień

Kreator ten wyświetla te składniki ochrony Kaspersky Anti-Virus, których ustawienia różnią się od domyślnych, ponieważ zostały zmodyfikowane przez użytkownika. Jeżeli dla jakiegoś składnika zostały wprowadzone ustawienia specjalne, zostaną one również wyświetlone w oknie.

Zaznacz pola obok ustawień, które chcesz zapisać, i kliknij przycisk **Dalej**.

### Krok 3. Kończenie przywracania ustawień

W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**.

## PRZENOSZENIE USTAWIEŃ KASPERSKY ANTI-VIRUS DO PRODUKTU ZAINSTALOWANEGO NA INNYM KOMPUTERZE

Po skonfigurowaniu produktu możesz zastosować jego ustawienia w aplikacji Kaspersky Anti-Virus zainstalowanej na innym komputerze. W rezultacie aplikacja będzie skonfigurowana tak samo na obu komputerach. Funkcja ta jest użyteczna, jeżeli np. Kaspersky Anti-Virus jest zainstalowany na komputerze domowym i biurowym.

Ustawienia aplikacji przechowywane są w specjalnym pliku konfiguracyjnym, który możesz przesłać na inny komputer.

Ustawienia programu Kaspersky Anti-Virus można przesłać na innych komputer, wykonując następujące czynności:

1. Zapisując ustawienia aplikacji w pliku konfiguracyjnym.
2. Przenosząc plik konfiguracyjny na inny komputer (na przykład, za pośrednictwem poczty elektronicznej lub nośnika wymiennego).
3. Importując ustawienia z pliku konfiguracyjnego do programu zainstalowanego na innym komputerze.

➤ *W celu wyeksportowania bieżących ustawień programu Kaspersky Anti-Virus:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Zarządzanie ustawieniami**.
3. Kliknij przycisk **Zapisz** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, wprowadź nazwę pliku konfiguracyjnego oraz miejsce jego zapisania.
5. Kliknij przycisk **OK**.

➤ *W celu zaimportowania ustawień aplikacji z zapisanego pliku konfiguracyjnego:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Zarządzanie ustawieniami**.
3. Kliknij przycisk **Otwórz** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, wybierz plik, z którego chcesz zaimportować ustawienia Kaspersky Anti-Virus.
5. Kliknij przycisk **OK**.

## JAK PRZEJŚĆ Z KASPERSKY ANTI-VIRUS DO KASPERSKY INTERNET SECURITY

Kaspersky Anti-Virus pozwala na przełączenie do Kaspersky Internet Security bez konieczności pobierania i instalacji dodatkowego oprogramowania.

*Kaspersky Internet Security* to aplikacja utworzona w celu zapewnienia pełnej ochrony komputera. Udostępnia szeroką gamę zaawansowanych funkcji zaimplementowanych w następujących modułach:

- Kontrola aplikacji;
- Kontrola rodzicielska;
- Zapora sieciowa;
- Blokowanie ataków sieciowych;
- Filtr geograficzny;
- Blokowanie dostępu do niebezpiecznych stron internetowych;
- Monitor sieci;
- Anti-Spam;
- Blokowanie banerów reklamowych;
- Czyszczenie śladów aktywności;
- Bezpieczne uruchamianie.

Program pozwala na tymczasowe przejście do wersji testowej Kaspersky Internet Security w celu zapoznania się z jego funkcjami lub natychmiastowe rozpoczęcie korzystania z wersji komercyjnej aplikacji.

Jeśli korzystasz z licencji z subskrypcją, lub używasz z aplikacji w szczególnym regionie, Twoja kopia Kaspersky Internet Security może nie zezwalać na tymczasowe przełączenie do wersji testowej.

## W TEJ SEKCJI:

---

Przejdźcie do wersji komercyjnej .....	<a href="#">59</a>
Tymczasowe przełączenie do wersji testowej .....	<a href="#">60</a>

## PRZEJŚCIE DO WERSJI KOMERCYJNEJ

Jeśli chcesz przełączyć się do komercyjnej wersji Kaspersky Internet Security, potrzebujesz kodu aktywacyjnego dla wersji komercyjnej aplikacji, którego użyjesz do jej aktywacji (sekcja "Jak aktywować aplikację" na stronie [43](#)).

➤ *W celu zakupienia kodu aktywacyjnego dla Kaspersky Internet Security:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Aktualizacja**.
3. W oknie, które zostanie otwarte, kliknij przycisk **Kup licencję**.

Zostaniesz przekierowany na witrynę sklepu internetowego, gdzie możesz zakupić kod aktywacyjny dla Kaspersky Internet Security.

Jeśli zakupiłeś aplikację w pewnym szczególnym regionie, lub korzystasz z licencji z subskrypcją, sekcja **Aktualizacja** nie jest wyświetlana w oknie głównym aplikacji.

## TYMCZASOWE PRZEŁĄCZENIE DO WERSJI TESTOWEJ

Możesz tymczasowo przełączyć się do wersji testowej programu Kaspersky Internet Security, aby ocenić jego funkcjonalność. Następnie możesz zakupić licencję na dalsze wykorzystanie aplikacji.

➤ *W celu tymczasowego przełączenia się do Kaspersky Internet Security:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Aktualizacja**.
3. W oknie, które zostanie otwarte, kliknij przycisk **Wersja testowa**.

Zostanie uruchomiony Kreator konfiguracji aplikacji.

Jeśli zakupiłeś aplikację w pewnym szczególnym regionie, lub korzystasz z licencji z subskrypcją, sekcja **Aktualizacja** nie jest wyświetlana w oknie głównym aplikacji.

Podczas pracy z Kreatorem konfiguracji aplikacji należy zdefiniować parametry ustawień.

### Krok 1. Żądanie aktywacji wersji testowej Kaspersky Internet Security

Jeśli żądanie aktywacji dla Kaspersky Internet Security zostało przesłane pomyślnie, Kreator automatycznie przejdzie do następnego kroku.

### Krok 2. Uruchamianie Aktualizacji

W tym kroku Kreator wyświetla na ekranie wiadomość informującą o spełnieniu wszystkich początkowych wymagań aktualizacji. Aby przejść do następnego kroku, kliknij przycisk **Dalej**.

### Krok 3. Usuwanie niekompatybilnych aplikacji

W tym kroku Kreator sprawdza, czy na komputerze znajdują się jakieś aplikacje niekompatybilne z Kaspersky Internet Security. Jeśli nie wykryto takich programów, Kreator automatycznie przechodzi do następnego kroku. Jeśli wykryto takie aplikacje, Kreator wyświetla je w oknie i proponuje ich usunięcie.

Po odinstalowaniu niekompatybilnych programów, może zająć konieczność ponownego uruchomienia systemu operacyjnego. Po ponownym uruchomieniu systemu operacyjnego Kreator zostanie automatycznie otwarty, aby wznowić proces aktualizacji.

#### Krok 4. Aktualizacja

W tym kroku Kreator łączy się z modułami aktualizacji, co może zająć nieco czasu. Po zakończeniu tego procesu, Kreator automatycznie przejdzie do następnego kroku.

#### Krok 5. Ponowne uruchamianie aplikacji

W ostatnim kroku aktualizacji, aplikacja powinna zostać uruchomiona ponownie. W tym celu, w oknie Kreatora kliknij przycisk **Zakończ**.

#### Krok 6. Finalizowanie procesu aktywacji

Kreator zostanie automatycznie włączony po ponownym uruchomieniu aplikacji. Po pomyślnej aktywacji wersji testowej Kaspersky Internet Security, okno Kreatora wyświetla informacje o okresie, w trakcie którego możesz używać wersji testowej.

#### Krok 7. Analiza systemu

Na tym etapie zbierane są informacje dotyczące aplikacji systemu operacyjnego Microsoft Windows. Są one dodawane do listy zaufanych aplikacji, które nie mają ograniczeń co do akcji wykonywanych w systemie.

Po zakończeniu analizy Kreator automatycznie przejdzie do następnego kroku.

#### Krok 8. Finalizowanie aktualizacji

W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**.

Aplikacji nie można przełączyć do wersji testowej Kaspersky Internet Security drugi raz.

## JAK UŻYWAĆ GADŻETU KASPERSKY LAB

Podczas używania Kaspersky Anti-Virus na komputerze działającym pod kontrolą systemu Microsoft Windows Vista lub Microsoft Windows 7 możesz używać gadżetu Kaspersky Lab (zwanego dalej *gadżet*). Po zainstalowaniu Kaspersky Anti-Virus na komputerze działającym pod kontrolą systemu Microsoft Windows 7 gadżet pojawi się na pulpicie automatycznie. Po zainstalowaniu aplikacji na komputerze z systemem Microsoft Windows Vista należy dodać gadżet do Paska bocznego Microsoft Windows ręcznie (zobacz dokumentację systemu operacyjnego).

Wskaźnik koloru gadżetu informuje o stanie ochrony komputera, podobnie jak wskaźnik stanu ochrony w oknie głównym aplikacji (sekcja "Diagnostyka i eliminacja problemów w ochronie komputera" na stronie [39](#)). Zielony kolor oznacza, że komputer jest chroniony, żółty wskazuje na problemy związane z ochroną, a czerwony oznacza, że ochrona komputera jest zagrożona. Kolor szary wskazuje na zatrzymanie działania aplikacji.

Podczas aktualizacji baz danych i modułów aplikacji w środku gadżetu pojawia się ikona obracającego się globu.

Gadżetu możesz użyć do wykonania następujących działań:

- wznowienia działania aplikacji, jeśli zostało wstrzymane;
- otwarcia okna głównego aplikacji;
- wykonania skanowania antywirusowego określonych obiektów;
- otwarcia okna nowości.

Możliwe jest również przypisanie do przycisków gadżetu dodatkowych działań:

- uruchamianie aktualizacji;
- modyfikowanie ustawień aplikacji;
- przeglądanie raportów aplikacji;
- wstrzymywanie ochrony;
- otwieranie Klawiatury wirtualnej;
- otwieranie okna Menedżer zadań.

➔ *W celu uruchomienia aplikacji przy pomocy gadżetu*

kliknij ikonę  **Włącz** położoną w centrum gadżetu.

➔ *W celu otwarcia okna głównego aplikacji przy pomocy gadżetu*


kliknij ikonę położoną w centrum gadżetu.

➔ *W celu przeskanowania obiektu w poszukiwaniu wirusów przy pomocy gadżetu*


przeciągnij na niego obiekt przeznaczony do skanowania.

Postęp wykonywania zadania będzie wyświetlany w oknie **Menedżer zadań**.

➔ *W celu otwarcia okna nowości przy pomocy gadżetu*

kliknij ikonę  wyświetloną w jego centrum po publikacji części nowości.

➔ *W celu skonfigurowania gadżetu:*

1. Otwórz jego okno ustawień poprzez kliknięcie ikony  , która pojawi się w prawym górnym rogu bloku gadżetu po najechaniu na niego kursorem myszy.
2. Z list rozwijalnych odpowiadających przyciskom gadżetu wybierz działania, jakie powinny zostać wykonane po kliknięciu tych przycisków.
3. Kliknij przycisk **OK**.

## JAK SPRAWDZIĆ REPUTACJĘ APLIKACJI

Kaspersky Anti-Virus umożliwia poznanie reputacji aplikacji dzięki użytkownikom z całego świata. Na reputację aplikacji składają się następujące kryteria:

- nazwa producenta;
- informacje o podpisie cyfrowym (dostępne, gdy aplikacja jest podpisana cyfrowo);
- informacje o grupie, do której aplikacja została dodana przez większość użytkowników biorących udział w Kaspersky Security Network;
- liczba użytkowników biorących udział w Kaspersky Security Network, którzy używają aplikacji (dostępne, gdy aplikacja została dodana do grupy Zaufane w bazie danych Kaspersky Security Network);
- czas dodania aplikacji do Kaspersky Security Network;

- kraje, w których używanie aplikacji jest najbardziej rozpowszechnione.

Aby sprawdzić reputację aplikacji, należy zgodzić się na udział w Kaspersky Security Network (strona [127](#)) w trakcie instalacji Kaspersky Anti-Virus.

➔ *W celu sprawdzenia reputacji aplikacji*

otwórz menu kontekstowe pliku wykonywalnego aplikacji i wybierz z niego **Sprawdź reputację w KSN**.

#### **ZOBACZ RÓWNIEŻ:**

---

Kaspersky Security Network ..... [127](#)

# ZAAWANSOWANE USTAWIENIA APLIKACJI

Sekcja ta zawiera szczegółowe informacje dotyczące konfigurowania każdego składnika aplikacji.

## W TEJ SEKCJI:

---

Ogólne ustawienia ochrony .....	<a href="#">64</a>
Skanowanie.....	<a href="#">66</a>
Aktualizacja .....	<a href="#">74</a>
Ochrona plików .....	<a href="#">79</a>
Ochrona poczty .....	<a href="#">85</a>
Ochrona WWW .....	<a href="#">90</a>
Ochrona komunikatorów .....	<a href="#">97</a>
Ochrona proaktywna .....	<a href="#">98</a>
Kontrola systemu .....	<a href="#">100</a>
Ochrona sieci .....	<a href="#">102</a>
Strefa zaufana .....	<a href="#">106</a>
Wydajność i kompatybilność z innymi aplikacjami .....	<a href="#">108</a>
Autoochrona programu Kaspersky Anti-Virus .....	<a href="#">111</a>
Kwarantanna i Kopia zapasowa .....	<a href="#">112</a>
Dodatkowe narzędzia zwiększające bezpieczeństwo komputera .....	<a href="#">116</a>
Raporty.....	<a href="#">120</a>
Wygląd aplikacji. Zarządzanie aktywnymi elementami interfejsu .....	<a href="#">124</a>
Powiadomienia .....	<a href="#">125</a>
Kaspersky Security Network .....	<a href="#">127</a>

## OGÓLNE USTAWIENIA OCHRONY

W oknie ustawień aplikacji, w podsekcji **Ustawienia ogólne** sekcji **Centrum ochrony** możesz:

- wyłączyć wszystkie składniki ochrony (sekcja "Włączanie i wyłączanie modułów ochrony" na stronie [40](#)).
- wybrać interaktywny lub automatyczny tryb ochrony (sekcja "Wybieranie trybu ochrony" na stronie [65](#));
- ograniczyć użytkownikowi dostęp do aplikacji poprzez ustawienie hasła (sekcja "Ograniczenie dostępu do programu Kaspersky Anti-Virus" na stronie [65](#));

- włączyć lub wyłączyć automatyczne uruchamianie aplikacji przy starcie systemu operacyjnego (sekcja "Włączanie i wyłączanie automatycznego uruchamiania" na stronie [37](#));
- włączyć niestandardowy skrót do wyświetlania klawiatury wirtualnej na ekranie (sekcja "Ochrona przed przechwytywaniem danych wprowadzanych z klawiatury" na stronie [50](#)).

## W TEJ SEKCJI:

Ograniczanie dostępu do programu Kaspersky Anti-Virus.....	<a href="#">65</a>
Wybieranie trybu ochrony.....	<a href="#">65</a>

## OGRANICZANIE DOSTĘPU DO PROGRAMU KASPERSKY ANTI-VIRUS

Z komputera może korzystać kilku użytkowników posiadających różną wiedzę na temat jego bezpieczeństwa. Brak zabezpieczenia dostępu do Kaspersky Anti-Virus i jego ustawień może znacznie obniżyć poziom bezpieczeństwa.

W celu ograniczenia dostępu do aplikacji możesz ustawić hasło i określić, które akcje będą wymagać jego podania:

- zmienianie ustawień aplikacji;
- zamykanie aplikacji;
- usuwanie aplikacji.

**Hasła do ograniczania dostępu do usuwania aplikacji należy używać rozważnie. Jeśli zapomnisz hasła, usunięcie aplikacji z komputera będzie trudne.**

➤ *W celu ograniczenia dostępu do Kaspersky Anti-Virus przy pomocy hasła:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz podsekcję **Ustawienia ogólne**.
3. W prawej części okna, w sekcji **Ochrona hasłem** zaznacz pole **Włącz ochronę hasłem** i kliknij przycisk **Ustawienia**.
4. W otwartym oknie **Ochrona hasłem** wprowadź hasło i określ obszar, do którego dostęp ma być zastrzeżony.

## WYBIERANIE TRYBU OCHRONY

Domyślnie Kaspersky Anti-Virus działa w *automatycznym trybie ochrony*. W tym trybie, po wykryciu niebezpiecznego zdarzenia aplikacja będzie automatycznie wykonywała akcje zalecane przez ekspertów z Kaspersky Lab. Jeśli chcesz, aby aplikacja powiadamiała Cię o wszystkich niebezpiecznych i podejrzanych zdarzeniach zachodzących w systemie, a także pozwalała decydować o wyborze akcji przez nią zasugerowanej, włącz interaktywny tryb ochrony.

➤ W celu wybrania trybu ochrony:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz podsekcję **Ustawienia ogólne**.
3. W sekcji **Ochrona interaktywna** zaznacz lub usuń zaznaczenie z pól w zależności od wybranego trybu ochrony:
  - aby włączyć interaktywny tryb ochrony, usuń zaznaczenie z pola **Automatycznie wybierz akcję**;
  - aby włączyć automatyczny tryb ochrony, zaznacz pole **Automatycznie wybierz akcję**.

Jeżeli nie chcesz, aby w tym trybie program Kaspersky Anti-Virus usuwał podejrzane obiekty, zaznacz pole **Nie usuwaj podejrzanych obiektów**.

## SKANOWANIE

Skanowanie komputera w poszukiwaniu luk, wirusów oraz innych szkodliwych programów należy do jednych z najbardziej istotnych zadań zapewniających podstawowe bezpieczeństwo komputera.

Regularne skanowanie komputera w poszukiwaniu wirusów pomaga ograniczyć rozprzestrzenianie się szkodliwych programów, które nie zostały wykryte przez składniki ochrony (na przykład ze względu na ustawienie niskiego poziomu ochrony).

Wykrywanie luk polega na diagnostyce systemu operacyjnego oraz wykrywaniu takich cech oprogramowania, które mogą być wykorzystywane przez przestępców do rozsyłania szkodliwych obiektów i uzyskania dostępu do informacji osobistych.

Sekcja zawiera informacje o funkcjach i konfiguracji zadań skanowania, poziomach ochrony, metodach skanowania oraz technologiach skanowania.

### W TEJ SEKCJI:

Skanowanie antywirusowe .....	<a href="#">66</a>
Wykrywanie luk .....	<a href="#">74</a>
Zarządzanie zadaniami skanowania. Menedżer zadań .....	<a href="#">74</a>

## SKANOWANIE ANTYWIRUSOWE

Do wykrywania wirusów i innych szkodliwych programów Kaspersky Anti-Virus wykorzystuje następujące zadania:

- **Pełne skanowanie.** Skanowanie całego systemu. Domyślnie Kaspersky Anti-Virus skanuje następujące obiekty:
  - pamięć systemową;
  - obiekty uruchamiane wraz ze startem systemu operacyjnego;
  - kopię zapasową systemu;
  - pocztowe bazy danych;
  - nośniki wymienne, dyski twarde i sieciowe.

- **Skanowanie obszarów krytycznych.** Domyślnie Kaspersky Anti-Virus skanuje obiekty uruchamiane wraz ze startem systemu operacyjnego.
- **Skanowanie niestandardowe.** Kaspersky Anti-Virus skanuje obiekty wybrane przez użytkownika. Możesz skanować dowolny obiekt z poniższej listy:
  - pamięć systemową;
  - obiekty uruchamiane wraz ze startem systemu operacyjnego;
  - kopię zapasową systemu;
  - pocztowe bazy danych;
  - nośniki wymienne, dyski twarde i sieciowe;
  - dowolny wybrany plik lub folder.

Zadania Pełnego skanowania i Skanowania obszarów krytycznych są bardzo specyficzne. Dla tych zadań nie zaleca się modyfikowania listy obiektów przeznaczonych do skanowania.

Każde zadanie skanowania jest wykonywane w wybranym obszarze i może być uruchamiane zgodnie z wcześniej utworzonym terminarzem. Poza tym każdemu zadaniu przypisany jest poziom ochrony (kombinacja ustawień określająca szczegółowość skanowania). Domyślnie tryb używania sygnatur baz danych aplikacji do wyszukiwania zagrożeń jest zawsze włączony. Dodatkowo możesz wybrać różne metody i technologie skanowania.

Po uruchomieniu zadania pełnego skanowania lub zadania skanowania obszarów krytycznych postęp zadania jest wyświetlany w oknie **Skanowanie**, w sekcji z nazwą uruchomionego zadania, a także w Menedżerze zadań (sekcja "Zarządzanie zadaniami skanowania. Menedżer zadań" na stronie [74](#)).

Jeżeli Kaspersky Anti-Virus wykryje zagrożenie, przypisze mu jeden z następujących stanów:

- Szkodliwy program (np. *wirus* lub *trojan*).
- *Potencjalnie zainfekowany* (podejrzany) - stan przypisywany w sytuacji, gdy nie można jednoznacznie uznać obiektu za zainfekowany. Oznacza to, że aplikacja wykryła sekwencję kodu charakterystyczną dla wirusów lub zmodyfikowany kod znanego wirusa.

Aplikacja wyświetli powiadomienie (strona [125](#)) o wykrytym zagrożeniu i wykona przypisaną akcję. Możesz zmienić akcje wykonywane po wykryciu zagrożenia.

Jeżeli pracujesz w trybie automatycznym (sekcja "Wybieranie trybu ochrony" na stronie [65](#)), po wykryciu niebezpiecznych obiektów Kaspersky Anti-Virus automatycznie zastosuje akcje zalecane przez specjalistów z Kaspersky Lab. Dla szkodliwych obiektów zastosowana zostanie akcja **Wylecz. Usuń, jeżeli leczenie nie jest możliwe**, dla podejrzanych obiektów – **Podдай kwarantannie**. Jeżeli niebezpieczne obiekty zostaną wykryte podczas pracy w trybie interaktywnym (sekcja "Wybieranie trybu ochrony" na stronie [65](#)), aplikacja wyświetli okno powiadomienia, w którym można wybrać żądaną akcję.

Przed próbą wyleczenia lub usunięcia zainfekowanego obiektu Kaspersky Anti-Virus tworzy jego kopię zapasową, aby w przyszłości można było go przywrócić lub wyleczyć. Podejrzane (potencjalnie zainfekowane) obiekty są poddawane kwarantannie. Możesz włączyć automatyczne skanowanie obiektów poddanych kwarantannie po każdej aktualizacji.

Informacje o wynikach skanowania oraz o zdarzeniach zaistniałych podczas wykonywania tego zadania zostają zapisane w raporcie Kaspersky Anti-Virus (strona [120](#)).

**W TEJ SEKCJI:**

Zmianianie i przywracanie poziomu ochrony.....	<a href="#">68</a>
Tworzenie terminarza uruchamiania zadania skanowania.....	<a href="#">69</a>
Tworzenie listy obiektów przeznaczonych do skanowania.....	<a href="#">69</a>
Wybieranie metody skanowania.....	<a href="#">70</a>
Wybieranie technologii skanowania.....	<a href="#">71</a>
Zmianianie akcji wykonywanych na wykrytych zagrożeniach.....	<a href="#">71</a>
Uruchamianie skanowania z poziomu konta innego użytkownika.....	<a href="#">71</a>
Zmianianie typu obiektów przeznaczonych do skanowania.....	<a href="#">71</a>
Skanowanie plików złożonych.....	<a href="#">72</a>
Optymalizacja skanowania.....	<a href="#">73</a>
Skanowanie napędów wymiennych po ich podłączeniu.....	<a href="#">73</a>
Tworzenie skrótu do zadania.....	<a href="#">73</a>

**ZMIENIANIE I PRZYWRACANIE POZIOMU OCHRONY**

W zależności od bieżących potrzeb możesz wybrać jeden z początkowych poziomów ochrony lub ręcznie zmodyfikować ustawienia skanowania.

Po skonfigurowaniu ustawień skanowania możesz zawsze przywrócić ustawienia zalecane. Zapewniają one optymalny poziom ochrony, dlatego są zalecane przez firmę Kaspersky Lab i zostały zebrane w **Zalecanym** poziomie ochrony.

➤ *W celu zmiany poziomu ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** ustaw żądany poziom ochrony dla wybranego zadania lub kliknij przycisk **Ustawienia**, aby ręcznie modyfikować ustawienia.

Jeżeli ustawienia zostaną zmodyfikowane ręcznie, nazwa poziomu ochrony zmieni się na **Niestandardowy**.

➤ *W celu przywrócenia domyślnych ustawień skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Poziom domyślny** dla wybranego zadania.

## TWORZENIE TERMINARZA URUCHAMIANIA ZADANIA SKANOWANIA

Możesz utworzyć terminarz, według którego będą uruchamiane zadania skanowania: określ częstotliwość uruchamiania zadań, czas rozpoczęcia (jeżeli konieczne) oraz ustawienia zaawansowane.

Jeżeli z jakiegoś powodu uruchomienie zadania nie będzie możliwe (na przykład komputer nie będzie włączony o określonym czasie), można skonfigurować automatyczne uruchamianie pominiętego zadania przy najbliższej możliwej okazji. Dodatkowo skanowanie może być automatycznie wstrzymywane po wyłączeniu wygaszacza ekranu lub po odblokowaniu komputera. Powoduje to opóźnienie uruchomienia zadania do momentu, aż użytkownik skończy pracę na komputerze. Skanowanie nie będzie wówczas obciążać zasobów systemu.

Specjalny tryb Skanowania w czasie bezczynności (sekcja "Uruchamianie zadań w tle" na stronie [110](#)) umożliwia automatyczne rozpoczęcie aktualizacji podczas bezczynności komputera.

➤ *W celu zmodyfikowania terminarza uruchamiania zadań skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Wykrywanie luk**).
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W otwartym oknie, na zakładce **Tryb uruchamiania**, w sekcji **Terminarz** wybierz **Zgodnie z terminarzem** i skonfiguruj tryb uruchamiania skanowania, określając wymagane wartości dla ustawienia **Częstotliwość**.

➤ *W celu włączenia automatycznego uruchamiania pominiętego zadania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Wykrywanie luk**).
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W otwartym oknie, na zakładce **Tryb uruchamiania**, w sekcji **Terminarz** wybierz opcję **Zgodnie z terminarzem** i zaznacz pole **Uruchom pominięte zadania**.

➤ *W celu skonfigurowania uruchamiania skanowania tylko wtedy, gdy komputer nie jest używany:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Wykrywanie luk**).
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Tryb uruchamiania**, w sekcji **Terminarz** wybierz **Zgodnie z terminarzem** i zaznacz pole **Uruchom zaplanowane skanowanie po włączeniu wygaszacza ekranu lub po zablokowaniu komputera**.

## TWORZENIE LISTY OBIEKTÓW PRZEZNACZONYCH DO SKANOWANIA

Każde zadanie skanowania antywirusowego posiada domyślną listę obiektów. Mogą do nich należeć elementy systemu plików komputera, takie jak napędy logiczne i pocztowe bazy danych lub inne typy obiektów, np. dyski sieciowe. Istnieje możliwość modyfikacji listy.

Jeżeli obszar skanowania jest pusty lub nie jest wybrany żaden obiekt, zadanie skanowania nie może zostać uruchomione.

➤ W celu utworzenia listy obiektów dla skanowania niestandardowego:

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Skanowanie**.
3. W dolnej części okna kliknij odnośnik **wskaż**, aby otworzyć listę skanowanych obiektów.
4. W oknie **Skanowanie niestandardowe**, które zostanie otwarte, kliknij przycisk **Dodaj**.
5. W oknie **Wybierz obiekt do skanowania** wybierz żądany obiekt i kliknij przycisk **Dodaj**. Po dodaniu wszystkich wymaganych obiektów kliknij przycisk **OK**. Aby wykluczyć z obszaru skanowania dowolny obiekt znajdujący się na liście, usuń zaznaczenie z pola znajdującego się przy jego nazwie.

Możesz również przeciągnąć pliki, które mają być skanowane, bezpośrednio do odpowiedniego obszaru sekcji **Skanowanie**.

➤ W celu utworzenia listy obiektów dla zadań *Pełnego skanowania*, *Skanowania obszarów krytycznych* lub *Wykrywania luk*:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Wykrywanie luk**).
3. W prawej części okna kliknij przycisk **Obszar skanowania**.
4. W oknie **Obszar skanowania**, które zostanie otwarte, utwórz listę przy pomocy przycisków **Dodaj**, **Modyfikuj**, **Usuń**. Aby wykluczyć z obszaru skanowania dowolny obiekt znajdujący się na liście, usuń zaznaczenie z pola znajdującego się przy jego nazwie.

Obiekty, które domyślnie znajdują się na liście, nie mogą zostać zmodyfikowane ani usunięte.

## WYBIERANIE METODY SKANOWANIA

Podczas skanowania antywirusowego wykorzystywana jest zawsze *analiza sygnatur*. Kaspersky Anti-Virus porównuje odnaleziony obiekt z wpisami z baz danych.

W celu zwiększenia efektywności skanowania możesz użyć dodatkowych metod skanowania: analizy heurystycznej (analiza działań, jakie obiekt wykonuje w systemie) oraz wykrywania rootkitów (skanowanie w poszukiwaniu narzędzi, które mogą ukrywać szkodliwe programy w Twoim systemie operacyjnym).

➤ W celu wybrania metody skanowania:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia** dla wybranego zadania.
4. W oknie, które zostanie otwarte, na zakładce **Dodatkowe**, w sekcji **Metody skanowania** wybierz żądane metody skanowania.

## WYBIERANIE TECHNOLOGII SKANOWANIA

Oprócz różnych metod skanowania, możesz także użyć specjalnych technologii, które przyspieszą skanowanie w poszukiwaniu wirusów przez wykluczenie plików, które nie zostały zmodyfikowane od ostatniego skanowania.

➤ *W celu wybrania technologii skanowania obiektów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia** dla wybranego zadania.
4. W otwartym oknie, na zakładce **Dodatkowe**, w sekcji **Technologie skanowania** wybierz żądane wartości.

## ZMIENIANIE AKCJI WYKONYWANYCH NA WYKRYTYCH ZAGROŻENIACH

Po wykryciu zainfekowanego obiektu aplikacja wykonuje określoną akcję.

➤ *W celu zmiany akcji wykonywanej po wykryciu zagrożenia:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W prawej części okna, w sekcji **Akcja po wykryciu zagrożenia** wybierz wymaganą opcję.

## URUCHAMIANIE SKANOWANIA Z POZIOMU KONTA INNEGO UŻYTKOWNIKA

Domyślnie zadania skanowania są uruchamiane z poziomu konta systemowego. Jednak może zaistnieć potrzeba uruchomienia zadania z poziomu konta innego użytkownika. Możesz określić konto, które ma być używane przez aplikację podczas wykonywania zadania skanowania.

➤ *W celu uruchomienia skanowania z poziomu konta innego użytkownika:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Wykrywanie luk**).
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Tryb uruchamiania**, w sekcji **Konto użytkownika** zaznacz pole **Uruchom zadanie jako**. Wprowadź nazwę użytkownika i hasło.

## ZMIENIANIE TYPU OBIEKTÓW PRZEZNACZONYCH DO SKANOWANIA

Podczas wybierania typu obiektów przeznaczonych do skanowania określ formaty plików, które mają być skanowane w poszukiwaniu wirusów.

Podczas wybierania typów plików należy pamiętać, że:

- Prawdopodobieństwo wnikięcia szkodliwego kodu do pewnych formatów plików (takich, jak .txt) i jego późniejszej aktywacji jest znikome. Istnieją jednak formaty zawierające lub mogące zawierać kod wykonywalny (na przykład .exe, .dll, .doc). Ryzyko przeniknięcia i aktywacji szkodliwego kodu w takich plikach jest bardzo wysokie.

- Haker może przesłać na komputer plik wykonywalny z rozszerzeniem TXT. Jeżeli wybrałeś opcję skanowania plików według rozszerzenia, będą one pominięte podczas skanowania. Jeżeli wybrana została opcja skanowania według formatu, wówczas (bez względu na rozszerzenie) moduł Ochrona plików będzie analizował nagłówki plików i na tej podstawie określi, czy są to pliki .exe. Takie pliki będą poddawane dokładnemu skanowaniu antywirusowemu.

➤ *W celu wybrania typu skanowanych obiektów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia** dla wybranego zadania.
4. W oknie, które zostanie otwarte, na zakładce **Zakres**, w sekcji **Typy plików** zaznacz żądaną opcję.

## SKANOWANIE PLIKÓW ZŁOŻONYCH

Najczęstszą metodą ukrywania wirusów jest osadzenie ich w plikach złożonych: archiwach, pakietach instalacyjnych, osadzonych obiektach OLE i plikach wiadomości pocztowych. W celu wykrycia ukrytych w ten sposób wirusów, plik złożony musi zostać rozpakowany, co znacząco obniża prędkość skanowania.

Dla każdego typu plików złożonych możesz wybrać skanowanie wszystkich plików lub tylko nowych plików. W tym celu kliknij odnośnik znajdujący się obok nazwy obiektu. Przy każdym kliknięciu lewym przyciskiem myszy jego wartość będzie się zmieniać. Jeżeli wybrany zostanie tryb skanowania tylko nowych i zmienionych plików (strona [73](#)), niedostępne staną się odnośniki do wybrania skanowania wszystkich lub tylko nowych plików.

Możesz ograniczyć maksymalny rozmiar plików złożonych przeznaczonych do skanowania. Pliki złożone, których rozmiar przekracza zdefiniowaną wartość, nie będą skanowane.

Po wypakowaniu z archiwów plików o dużym rozmiarze będą one skanowane, nawet jeśli została wybrana opcja **Nie rozpakowuj dużych plików złożonych**.

➤ *W celu zmodyfikowania listy plików złożonych przeznaczonych do skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia** dla wybranego zadania.
4. W oknie, które zostanie otwarte, na zakładce **Zakres**, w sekcji **Skanowanie plików złożonych** zaznacz pola dla tych typów plików, które chcesz skanować.

➤ *W celu ustawienia maksymalnego rozmiaru plików złożonych przeznaczonych do skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia** dla wybranego zadania.
4. W otwartym oknie, na zakładce **Zakres**, w sekcji **Skanowanie plików złożonych** kliknij przycisk **Dodatkowe**.
5. W oknie **Pliki złożone** zaznacz pole **Nie rozpakowuj dużych plików złożonych** i w polu znajdującym się poniżej określ maksymalny rozmiar pliku.

## OPTYMALIZACJA SKANOWANIA

Możesz skrócić czas skanowania i przyspieszyć działanie Kaspersky Anti-Virus. W tym celu włącz skanowanie tylko nowych plików i plików zmienionych od czasu ostatniego skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

Możesz również wprowadzić ograniczenie czasu skanowania obiektu. Po upływie określonego czasu obiekt zostanie wykluczony z bieżącego skanowania (poza archiwami i plikami zawierającymi wiele obiektów).

➤ *W celu skanowania tylko nowych i zmienionych plików:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia** dla wybranego zadania.
4. W oknie, które zostanie otwarte, na zakładce **Zakres**, w sekcji **Optymalizacja skanowania** zaznacz pole **Skanuj tylko nowe i zmienione pliki**.

➤ *W celu wprowadzenia ograniczenia czasu skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz żądane zadanie (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie niestandardowe**).
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia** dla wybranego zadania.
4. W oknie, które zostanie otwarte, na zakładce **Zakres**, w sekcji **Optymalizacja skanowania** zaznacz pole **Pomiń obiekty skanowane dłużej niż** i określ długość skanowania pojedynczego pliku w polu obok.

## SKANOWANIE NAPĘDÓW WYMIENNYCH PO ICH PODŁĄCZENIU

Obecnie szkodliwe obiekty coraz częściej wykorzystują luki systemu operacyjnego w celu rozprzestrzeniania się poprzez Sieć oraz nośniki wymienne. Kaspersky Anti-Virus skanuje napędy wymienne po podłączeniu ich do komputera.

➤ *W celu skonfigurowania skanowania napędów wymiennych po ich podłączeniu:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz **Ustawienia ogólne**.
3. W sekcji **Skanowanie napędów wymiennych po ich podłączeniu** wybierz wymaganą akcję; w razie konieczności możesz także określić maksymalny rozmiar napędu w polu znajdującym się poniżej.

## TWORZENIE SKRÓTU DO ZADANIA

Aplikacja posiada opcję tworzenia skrótów do uruchamiania zadań pełnego skanowania, szybkiego skanowania oraz wykrywania luk. Umożliwia to uruchamianie żądanego zadania skanowania bez konieczności otwierania okna głównego aplikacji lub menu kontekstowego.

➤ *W celu utworzenia skrótu do zadania skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz **Ustawienia ogólne**.

3. W prawej części okna, w sekcji **Szybkie uruchamianie zadań skanowania** kliknij przycisk **Utwórz skrót** znajdujący się obok wybranego zadania (**Skanowanie obszarów krytycznych**, **Pełne skanowanie** lub **Wykrywanie luk**).
4. W otwartym oknie określ ścieżkę do zapisania skrótu i jego nazwę. Domyślnie skrót szybkiego uruchamiania tworzony jest z nazwą zadania w folderze *Mój komputer* obecnego użytkownika komputera.

## WYKRYWANIE LUK

Luki systemu operacyjnego mogą być wynikiem, na przykład, błędów oprogramowania, słabych haseł lub działania szkodliwych programów. Podczas skanowania w poszukiwaniu luk aplikacja analizuje system, sprawdza ustawienia systemu i przeglądarki internetowej oraz wyszukuje podatne na atak usługi.

Może to chwilę potrwać. Po zakończeniu diagnostyki wykryte problemy są analizowane do oszacowania prawdopodobieństwa zagrożenia dla systemu.

Po uruchomieniu zadania wykrywania luk (strona [48](#)) jego postęp jest wyświetlany w oknie **Skanowanie** (w sekcji **Wykrywanie luk**) i Menedżerze zadań (sekcja "Zarządzanie zadaniami skanowania. Menedżer zadań" na stronie [74](#)).

Informacje o wynikach wykonanego zadania zostają zapisane w raporcie Kaspersky Anti-Virus (strona [120](#)).

Podobnie jak w przypadku skanowania antywirusowego, dla zadania wykrywania luk można utworzyć terminarz uruchamiania, utworzyć listę skanowanych obiektów (strona [69](#)), określić konto (sekcja "Uruchamianie skanowania z poziomu konta innego użytkownika" na stronie [71](#)) oraz utworzyć skrót do jego szybkiego uruchamiania. Domyślnie aplikacje już zainstalowane na komputerze są zaznaczone jako obiekty przeznaczone do skanowania.

## ZARZĄDZANIE ZADANIAMI SKANOWANIA. MENEDŻER ZADAŃ

Menedżer zadań wyświetla informacje o ostatnich zadaniach skanowania, które były uruchamiane, lub są uruchomione obecnie (na przykład skanowanie antywirusowe, wykrywanie luk, wykrywanie rootkitów lub zaawansowane leczenie).

W Menedżerze zadań można wyświetlić postęp i wynik wykonywania zadania, a także zatrzymać zadanie. Dla niektórych zadań dostępne są również dodatkowe akcje (na przykład, po zakończeniu wykrywania luk możesz otworzyć listę wykrytych luk i je naprawić).

➔ *W celu otwarcia Menedżera zadań:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Skanowanie**.
3. W oknie **Skanowanie**, które zostanie otwarte, kliknij przycisk **Zarządzaj zadaniami** znajdujący się w jego prawym górnym rogu.

## AKTUALIZACJA

Aktualizowanie baz danych i modułów programu Kaspersky Anti-Virus zapewnia aktualny stan ochrony Twojego komputera. Codziennie na całym świecie pojawia się duża ilość nowych wirusów, trojanów i innego typu szkodliwego oprogramowania. Informacja o zagrożeniach i metodach ich neutralizacji jest przechowywana w bazach danych programu Kaspersky Anti-Virus. Aby nowe zagrożenia były wykrywane na bieżąco, należy regularnie aktualizować bazy danych i moduły aplikacji.

Do przeprowadzania regularnych aktualizacji programu potrzebna jest aktywna licencja. Jeżeli program nie posiada zainstalowanej licencji, wówczas możliwe będzie wykonanie tylko jednej aktualizacji.

Podczas aktualizacji aplikacja pobiera i instaluje na komputerze następujące obiekty:

- Bazy danych Kaspersky Anti-Virus.

Ochronę informacji zapewniają bazy danych, które zawierają sygnatury zagrożeń i ataków sieciowych, oraz metody ich zwalczania. Składniki ochrony wykorzystują te informacje do wyszukiwania i leczenia niebezpiecznych obiektów znajdujących się na komputerze. Bazy danych publikowane są co godzinę. Dodawane są do nich wpisy dotyczące najnowszych zagrożeń i metod ich zwalczania. Z tego powodu zalecamy regularnie je aktualizować.

Oprócz baz danych Kaspersky Anti-Virus aktualizowane są sterowniki sieciowe umożliwiające modułom aplikacji przechwytywanie ruchu sieciowego.

- Moduły aplikacji.

Oprócz baz danych aplikacji można także aktualizować moduły aplikacji. Uaktualnienia modułów aplikacji usuwają luki w programie Kaspersky Anti-Virus oraz dodają nowe funkcje lub ulepszają istniejące.

Podczas aktualizacji moduły aplikacji i bazy danych znajdujące się na komputerze porównywane są z tymi znajdującymi się w źródle aktualizacji. Jeśli Twoje bieżące bazy danych i moduły różnią się od tych dostępnych w najnowszej wersji programu, na Twoim komputerze zainstalowana zostanie brakująca część.

Jeśli bazy danych znajdujące się w pakiecie instalacyjnym są nieaktualne, pakiet aktualizacyjny może być duży i może powodować dodatkowy ruch internetowy (do kilkudziesięciu MB).

Przed aktualizacją baz danych Kaspersky Anti-Virus tworzy ich kopie zapasowe na wypadek, gdybyś potrzebował cofnąć aktualizację do poprzedniej wersji (sekcja "Cofanie ostatniej aktualizacji" na stronie [78](#)).

Informacje o bieżącym stanie baz danych programu Kaspersky Anti-Virus wyświetlane są w sekcji **Aktualizacja** znajdującej się w oknie głównym aplikacji.

Informacje o wynikach aktualizacji i zdarzeniach zaistniałych podczas wykonywania zadania aktualizacji zapisywane są w raporcie Kaspersky Anti-Virus (strona [120](#)).

Możesz wybrać źródło uaktualnień (strona "Wybieranie źródła uaktualnień" na stronie [75](#)) i skonfigurować automatyczne uruchamianie aktualizacji.

## W TEJ SEKCJI:

Wybieranie źródła uaktualnień .....	<a href="#">75</a>
Tworzenie terminarza uruchamiania aktualizacji .....	<a href="#">77</a>
Cofanie ostatniej aktualizacji .....	<a href="#">78</a>
Uruchamianie aktualizacji z poziomu konta innego użytkownika .....	<a href="#">78</a>
Korzystanie z serwera proxy .....	<a href="#">79</a>

## WYBIERANIE ŹRÓDŁA UAKTUALNIEŃ

Źródło uaktualnień jest zasobem zawierającym uaktualnienia baz danych oraz modułów aplikacji Kaspersky Anti-Virus.

Głównym źródłem są serwery aktualizacji Kaspersky Lab, na których przechowywane są uaktualnienia baz danych i modułów wszystkich produktów firmy Kaspersky Lab.

Aby pobrać uaktualnienia z naszych serwerów, komputer musi być połączony z Internetem. Domyślnie ustawienia połączenia internetowego są określone automatycznie. Jeśli korzystasz z serwera proxy, możliwe, że będziesz musiał dostosować ustawienia połączenia (sekcja "Konfigurowanie serwera proxy" na stronie [105](#)).

Podczas aktualizowania programu Kaspersky Anti-Virus możesz skopiować uaktualnienia bazy danych i modułów pobrane z serwera firmy Kaspersky Lab do foldera lokalnego (sekcja "Aktualizowanie aplikacji z foldera współdzielonego" na stronie [76](#)), do którego mają dostęp pozostałe komputery sieciowe. Zaoszczędza to ruch internetowy.

Jeżeli użytkownik nie ma dostępu do serwerów aktualizacji firmy Kaspersky Lab (na przykład z powodu ograniczonego dostępu do Internetu), może on skontaktować się z naszą siedzibą (<http://www.kaspersky.pl/about.html?s=contact>) w celu uzyskania informacji na temat partnerów Kaspersky Lab, którzy mogą dostarczyć mu uaktualnienia na nośniku wymiennym.

Podczas zamawiania uaktualnień na nośniku wymiennym należy zaznaczyć, czy mają się na nim znajdować również uaktualnienia modułów aplikacji.

## DODAWANIE ŹRÓDŁA UAKTUALNIEŃ

Domyślnie lista źródeł uaktualnień zawiera tylko serwery aktualizacji firmy Kaspersky Lab. Jako źródło uaktualnień można dodać folder lokalny lub inny serwer. Jeżeli jako aktywne ustawiono kilka źródeł aktualizacji, Kaspersky Anti-Virus będzie podejmował próby nawiązywania połączenia z każdym z nich, począwszy od góry listy; uaktualnienia zostaną pobrane z pierwszego dostępnego źródła.

➤ *W celu dodania źródła uaktualnień:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Źródło uaktualnień** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Źródło** kliknij przycisk **Dodaj**, aby otworzyć okno wyboru.
5. W otwartym oknie **Wybierz źródło uaktualnień** wybierz folder zawierający uaktualnienia lub w polu **Źródło** wpisz adres wskazujący serwer, z którego mają zostać pobrane uaktualnienia.

## WYBIERANIE REGIONU SERWERA UAKTUALNIEŃ

Jeżeli aktualizacja wykonywana jest z serwerów aktualizacji Kaspersky Lab, można określić optymalną lokalizację dla serwerów, z których pobierane będą uaktualnienia. Firma Kaspersky Lab posiada serwery w kilku krajach.

Korzystanie z najbliższego położonego serwera Kaspersky Lab pozwala zredukować czas potrzebny na pobranie uaktualnień oraz zwiększyć szybkość wykonywania tego zadania. Domyślnie aplikacja korzysta z informacji o bieżącej lokalizacji pobranych z rejestru systemu operacyjnego. Region może zostać wybrany ręcznie.

➤ *W celu wybrania regionu serwera:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Źródło uaktualnień** znajdujący się w prawej części okna.
4. W otwartym oknie, na zakładce **Źródło**, w sekcji **Ustawienia regionalne** wybierz opcję **Wybierz z listy** i wybierz z listy rozwijalnej kraj, który jest najbliższy Ciebie.

## AKTUALIZOWANIE Z FOLDERA WSPÓLDZIELONEGO

Aby zaoszczędzić ruch internetowy, możesz skonfigurować pobieranie aktualizacji programu Kaspersky Anti-Virus z foldera współdzielonego podczas aktualizowania aplikacji na komputerach sieciowych. Po przeprowadzeniu konfiguracji komputery sieciowe otrzymają z serwerów Kaspersky Lab lub innego zasobu sieciowego pakiet

aktualizacyjny zawierający żądany zestaw uaktualnień. Otrzymane uaktualnienia są kopiowane do foldera współdzielonego. Pozostałe komputery sieciowe pobiorą z tego foldera uaktualnienia programu Kaspersky Anti-Virus.

Jeżeli w systemie Microsoft Windows 7 zalogowałeś się na konto gościa, uaktualnienia nie będą kopiowane do foldera współdzielonego. W takiej sytuacji zalecane jest zalogowanie się na inne konto.

➤ *W celu włączenia trybu dystrybucji uaktualnień:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Zaznacz pole **Kopiuj uaktualnienia do foldera** znajdujące się w sekcji **Dodatkowe**, a następnie w polu znajdującym się poniżej określ ścieżkę do foldera publicznego, do którego będą kopiowane wszystkie pobrane uaktualnienia. Folder można również wybrać poprzez kliknięcie przycisku **Przełączaj**.

➤ *W celu skonfigurowania pobierania uaktualnień z foldera współdzielonego:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Źródło uaktualnień** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Źródło** kliknij przycisk **Dodaj**, aby otworzyć okno wyboru.
5. W oknie **Wybierz źródło uaktualnień** wybierz folder lub w polu **Źródło** wprowadź jego pełną ścieżkę dostępu.
6. Usuń zaznaczenie z pola **Serwery aktualizacji Kaspersky Lab** dostępnego na zakładce **Źródło**.

## TWORZENIE TERMINARZA URUCHAMIANIA AKTUALIZACJI

Możesz utworzyć terminarz, według którego będą uruchamiane zadania aktualizacji: określ częstotliwość, czas uruchomienia (jeżeli jest to konieczne) oraz ustawienia zaawansowane.

Jeżeli z jakiegoś powodu uruchomienie zadania nie będzie możliwe (na przykład komputer nie będzie włączony o określonym czasie), można skonfigurować automatyczne uruchamianie pominiętego zadania przy najbliższej możliwej okazji.

Możesz również odroczyć automatyczne rozpoczęcie zadania po uruchomieniu aplikacji. Należy pamiętać, że wszystkie zaplanowane zadania będą uruchamiane dopiero po minięciu określonego czasu od uruchomienia programu Kaspersky Anti-Virus.

Specjalny tryb Skanowania w czasie bezczynności (sekcja "Uruchamianie zadań w tle" na stronie [110](#)) umożliwia automatyczne rozpoczęcie aktualizacji podczas bezczynności komputera.

➤ *W celu skonfigurowania terminarza uruchamiania zadania aktualizacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W otwartym oknie, na zakładce **Tryb uruchamiania**, w sekcji **Terminarz** wybierz opcję **Zgodnie z terminarzem** i skonfiguruj tryb uruchamiania aktualizacji.

➤ *W celu włączenia automatycznego uruchamiania pominiętego zadania:*

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W otwartym oknie, na zakładce **Tryb uruchamiania**, w sekcji **Terminarz** wybierz opcję **Zgodnie z terminarzem** i zaznacz pole **Uruchom pominięte zadania**.

➤ *W celu odroczenia uruchamiania zadania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Tryb uruchamiania**, w sekcji **Terminarz** wybierz opcję **Zgodnie z terminarzem** i wypełnij pole **Odrocz uruchomienie zadania na**, aby określić czas, na jaki uruchamianie zadania ma zostać odroczone.


## COFANIE OSTATNIEJ AKTUALIZACJI

Opcja cofnięcia do poprzedniej wersji baz danych staje się dostępna po pierwszej aktualizacji Kaspersky Anti-Virus.

Funkcja cofania aktualizacji jest przydatna w sytuacji, gdy nowa wersja baz danych zawiera nieprawidłową sygnaturę powodującą blokadę bezpiecznej aplikacji.

W przypadku uszkodzenia baz danych zaleca się pobranie aktualnego zestawu baz danych.

➤ *W celu przywrócenia poprzedniej wersji bazy danych:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Aktualizacja**.
3. W oknie **Aktualizacja**, które zostanie otwarte, kliknij przycisk  i z otwartego menu wybierz **Cofnij do poprzedniej wersji baz danych**.

## URUCHAMIANIE AKTUALIZACJI Z POZIOMU KONTA INNEGO UŻYTKOWNIKA

Domyślnie zadanie aktualizacji jest uruchamiane z poziomu konta systemowego. Jednakże Kaspersky Anti-Virus może pobrać uaktualnienia ze źródła, do którego użytkownik nie ma praw dostępu (na przykład z foldera sieciowego zawierającego uaktualnienia) lub autoryzowanych uprawnień użytkownika proxy. Zadanie aktualizacji może być uruchomione z poziomu konta użytkownika posiadającego takie prawa.

➤ *W celu uruchomienia aktualizacji z poziomu konta innego użytkownika:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Tryb uruchamiania** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Tryb uruchamiania**, w sekcji **Konto użytkownika** zaznacz pole **Uruchom zadanie jako**. Wprowadź nazwę użytkownika i hasło.

## KORZYSTANIE Z SERWERA PROXY

Jeśli do połączenia internetowego używasz serwera proxy, powinieneś skonfigurować go w celu poprawnego aktualizowania programu Kaspersky Anti-Virus.

➔ *W celu skonfigurowania serwera proxy:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Kliknij przycisk **Źródło uaktualnień** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Źródło** kliknij przycisk **Serwer proxy**.
5. W otwartym oknie **Ustawienia serwera proxy** skonfiguruj ustawienia serwera proxy.

## OCHRONA PLIKÓW

Moduł Ochrona plików zapobiega zainfekowaniu systemu plików komputera. Moduł uruchamia się podczas ładowania systemu operacyjnego, pozostaje w pamięci RAM i skanuje wszystkie pliki, które są otwierane, zapisywane lub uruchamiane na Twoim komputerze, oraz wszystkie podłączone dyski.

Możesz utworzyć obszar ochrony oraz ustawić poziom ochrony (zestaw ustawień określających szczegółowość skanowania).

Podczas próby (użytkownika lub aplikacji) uzyskania dostępu do chronionego pliku, moduł Ochrona plików sprawdzi, czy bazy danych iChecker i iSwift zawierają o nim informacje, a następnie podejmie decyzję o jego ewentualnym skanowaniu.

Domyślnie zawsze włączony jest tryb analizy sygnatur - wykorzystujący wpisy z baz danych aplikacji do wykrywania zagrożeń. Ponadto do skanowania plików możesz wykorzystać analizę heurystyczną oraz inne technologie skanowania.

Jeżeli Kaspersky Anti-Virus wykryje w pliku zagrożenie, przypisze mu jeden z następujących stanów:

- Stan wskazujący na typ wykrytego szkodliwego programu (na przykład: *wirus, trojan*).
- *Potencjalnie zainfekowany (podejrzany)* - stan przypisywany w sytuacji, gdy nie można jednoznacznie uznać obiektu za zainfekowany. Oznacza to, że aplikacja wykryła sekwencję kodu charakterystyczną dla wirusów i innych szkodliwych programów lub zmodyfikowany kod znanego wirusa.

Aplikacja wyświetli powiadomienie (strona [125](#)) o wykrytym zagrożeniu i wykona akcję określoną w ustawieniach modułu Ochrona plików. Możesz zmienić akcję (strona [83](#)) podejmowaną przez aplikację po wykryciu zagrożenia.

Jeżeli pracujesz w trybie automatycznym (sekcja "Wybieranie trybu ochrony" na stronie [65](#)), po wykryciu niebezpiecznych obiektów Kaspersky Anti-Virus automatycznie zastosuje akcje zalecane przez specjalistów z Kaspersky Lab. Dla szkodliwych obiektów zastosowana zostanie akcja **Wylecz. Usuń, jeżeli leczenie nie jest możliwe**, dla podejrzanych obiektów – **Podдай kwarantannie**. Jeżeli niebezpieczne obiekty zostaną wykryte podczas pracy w trybie interaktywnym (sekcja "Wybieranie trybu ochrony" na stronie [65](#)), aplikacja wyświetli okno powiadomienia, w którym można wybrać żądaną akcję.

Przed próbą wyleczenia lub usunięcia zainfekowanego obiektu Kaspersky Anti-Virus tworzy jego kopię zapasową, aby w przyszłości można było go przywrócić lub wyleczyć. Podejrzane (potencjalnie zainfekowane) obiekty są poddawane kwarantannie. Możesz włączyć automatyczne skanowanie obiektów poddanych kwarantannie po każdej aktualizacji.

**W TEJ SEKCJI:**

Włączanie i wyłączenie modułu Ochrona plików .....	<a href="#">80</a>
Automatyczne wstrzymywanie modułu Ochrona plików .....	<a href="#">80</a>
Tworzenie obszaru ochrony modułu Ochrona plików .....	<a href="#">81</a>
Zmianie i przywracanie poziomu ochrony plików .....	<a href="#">82</a>
Wybieranie trybu skanowania plików .....	<a href="#">82</a>
Używanie analizy heurystycznej .....	<a href="#">83</a>
Wybieranie technologii skanowania plików .....	<a href="#">83</a>
Zmianie akcji podejmowanej na zainfekowanych plikach .....	<a href="#">83</a>
Skanowanie plików złożonych przez moduł Ochrona plików .....	<a href="#">84</a>
Optymalizacja skanowania plików .....	<a href="#">85</a>

**WŁĄCZANIE I WYŁĄCZANIE MODUŁU OCHRONA PLIKÓW**

Domyślnie moduł Ochrona plików jest włączony i działa w trybie zalecanym przez specjalistów z Kaspersky Lab. W razie konieczności możesz wyłączyć Ochronę plików.

➤ *W celu wyłączenia modułu Ochrona plików:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna usuń zaznaczenie z pola **Włącz moduł Ochrona plików**.

**AUTOMATYCZNE WSTRZYMYWANIE MODUŁU OCHRONA PLIKÓW**

Podczas pracy z aplikacjami wymagającymi dużej ilości zasobów komputera i systemu możesz wstrzymać działanie Ochrony plików. W celu zmniejszenia obciążenia procesora i zapewnienia szybkiego dostępu do obiektów możesz skonfigurować automatyczne wstrzymywanie pracy modułu o określonym czasie lub podczas pracy z pewnymi programami.

*Wstrzymywanie modułu Ochrona plików w sytuacji, gdy powoduje konflikty z innymi programami, jest działaniem wyjątkowym! Jeżeli podczas pracy z modułem powstaną konflikty, skontaktuj się z działem pomocy technicznej Kaspersky Lab (<http://support.kaspersky.com/pl>). Specjaliści pomogą Ci wyeliminować konflikt między aplikacją Kaspersky Anti-Virus a programami zainstalowanymi na Twoim komputerze.*

➤ *W celu wstrzymania modułu o określonym czasie:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

4. W oknie, które zostanie otwarte, na zakładce **Dodatkowe**, w sekcji **Wstrzymaj zadanie** zaznacz pole **Zgodnie z terminarzem** i kliknij przycisk **Terminarz**.
5. W oknie **Wstrzymywanie zadania** wprowadź czas (w formacie 24-godzinnym GG:MM), w którym ochrona będzie wstrzymana (pola **Wstrzymaj zadanie o** i **Wznów zadanie o**).

➤ *W celu wstrzymania modułu podczas pracy z innymi aplikacjami:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Dodatkowe**, w sekcji **Wstrzymaj zadanie** zaznacz pole **Podczas uruchamiania aplikacji** i kliknij przycisk **Wybierz**.
5. W oknie **Aplikacje** utwórz listę aplikacji, których uruchomienie spowoduje wstrzymanie działania modułu.

## TWORZENIE OBSZARU OCHRONY MODUŁU OCHRONA PLIKÓW

Obszar ochrony określa miejsce przechowywania obiektów i typy plików przeznaczonych do skanowania. Domyślnie aplikacja skanuje tylko potencjalnie infekowalne pliki uruchamiane z dowolnego dysku twardego, dysku sieciowego lub nośnika wymiennego.

➤ *W celu utworzenia obszaru ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Ogólne**, w sekcji **Typy plików** określ typy skanowanych plików:
  - Jeżeli skanowane mają być wszystkie pliki, zaznacz pole **Wszystkie pliki**.
  - Jeżeli skanowaniu mają podlegać pliki o formatach najbardziej podatnych na infekcje, wybierz opcję **Pliki skanowane według formatu**.
  - Jeżeli skanowaniu mają podlegać pliki z rozszerzeniami najbardziej podatnymi na infekcje, zaznacz pole **Pliki skanowane według rozszerzenia**.

Podczas wybierania typów plików przeznaczonych do skanowania należy pamiętać, że:

- Prawdopodobieństwo wniknięcia szkodliwego kodu do pewnych formatów plików (takich, jak .txt) i jego późniejszej aktywacji jest znikome. Istnieją jednak formaty zawierające lub mogące zawierać kod wykonywalny (na przykład .exe, .dll, .doc). Ryzyko przeniknięcia i aktywacji szkodliwego kodu w takich plikach jest bardzo wysokie.
  - Haker może przesłać na Twój komputer wirusa lub inne szkodliwe oprogramowanie w pliku wykonywalnym posiadającym rozszerzenie TXT. Jeżeli wybrałeś opcję skanowania plików według rozszerzenia, będą one pominięte podczas skanowania. Jeżeli wybrana została opcja skanowania według formatu, wówczas (bez względu na rozszerzenie) moduł Ochrona plików będzie analizował nagłówki plików i na tej podstawie określi, czy są to pliki .exe. Taki plik zostanie poddany szczegółowemu skanowaniu antywirusowemu.
5. Na liście **Obszar ochrony** należy wykonać jedną z następujących akcji:
    - Jeżeli chcesz dodać nowy obiekt do listy obiektów przeznaczonych do skanowania, kliknij odnośnik **Dodaj**.
    - Jeżeli chcesz zmienić lokalizację obiektu, wybierz go z listy i kliknij odnośnik **Modyfikuj**.

Zostanie otwarte okno **Wybierz obiekt do skanowania**.

- Jeżeli chcesz usunąć obiekt z listy, zaznacz go i kliknij odnośnik **Usuń**.

Zostanie otwarte okno potwierdzenia usunięcia.

6. Wykonaj jedną z następujących czynności:

- Jeżeli chcesz dodać nowy obiekt do listy skanowanych, wybierz go w oknie **Wybierz obiekt do skanowania** i kliknij przycisk **OK**.
- Jeżeli chcesz zmienić lokalizację obiektu, zmień ścieżkę dostępu do niego w polu **Obiekt dostępnym** w oknie **Wybierz obiekt do skanowania**, a następnie kliknij przycisk **OK**.
- Jeżeli chcesz usunąć obiekt z listy, w oknie potwierdzenia usunięcia kliknij przycisk **Tak**.

7. Jeżeli to konieczne, powtórz kroki 6 – 7, aby dodać, przenieść lub usunąć obiekty z listy skanowanych.

8. Aby wykluczyć obiekt z listy skanowanych, na liście **Obszar ochrony** usuń zaznaczenie z pola znajdującego się obok niego. Obiekt zostaje wykluczony ze skanowania przez Ochronę plików, ale nadal znajduje się na liście.

## ZMIENIANIE I PRZYWRACANIE POZIOMU OCHRONY PLIKÓW

W zależności od bieżących potrzeb możesz wybrać jeden z domyślnych poziomów ochrony pliku/pamięci lub samodzielnie skonfigurować Ochronę plików.

Po skonfigurowaniu modułu Ochrona plików możesz w dowolnym momencie przywrócić ustawienia domyślne. Zapewniają one optymalny poziom ochrony, dlatego są zalecane przez firmę Kaspersky Lab i zostały zebrane w **Zalecanym** poziomie ochrony.

➤ *W celu zmiany poziomu ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** ustaw żądany poziom ochrony lub kliknij przycisk **Ustawienia**, aby ręcznie modyfikować ustawienia.

Jeżeli ustawienia zostaną zmodyfikowane ręcznie, nazwa poziomu ochrony zmieni się na **Niestandardowy**.

➤ *W celu przywrócenia domyślnego poziomu ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. Kliknij przycisk **Poziom domyślny** znajdujący się w prawej części okna, w sekcji **Poziom ochrony**.

## WYBIERANIE TRYBU SKANOWANIA PLIKÓW

*Tryb skanowania* to stan, w jakim moduł Ochrona plików skanuje pliki. Domyślnie Kaspersky Anti-Virus działa w trybie smart. W tym trybie Ochrona plików skanuje obiekt w oparciu o analizę akcji podejmowanych na obiekcie. Na przykład, jeżeli wykorzystywany jest dokument programu Microsoft Office, aplikacja skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.

➤ *W celu zmiany trybu skanowania plików:*

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Dodatkowe**, w sekcji **Tryb skanowania** wybierz żądany tryb.

Podczas wybierania trybu skanowania użytkownik powinien wziąć pod uwagę typy plików, z którymi będzie pracował przez większość czasu.

## UŻYWANIE ANALIZY HEURYSTYCZNEJ

Podczas działania Ochrony plików wykorzystywana jest *analiza sygnatur*. Kaspersky Anti-Virus porównuje odnaleziony obiekt z wpisami z baz danych.

Aby zwiększyć efektywność ochrony, możesz użyć *analizy heurystycznej* (tzn. analizy aktywności, którą obiekt wykonuje w systemie). Analiza ta umożliwia wykrywanie nowych szkodliwych obiektów, które nie zostały jeszcze opisane w bazach danych.

➤ *W celu włączenia analizy heurystycznej:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Wydajność**, w sekcji **Metody skanowania** zaznacz opcję **Analiza heurystyczna** i określ poziom szczegółowości skanowania.

## WYBIERANIE TECHNOLOGII SKANOWANIA PLIKÓW

Oprócz analizy heurystycznej możesz także użyć specjalnych technologii, które przyspieszą skanowanie plików przez wykluczenie tych, które nie zostały zmodyfikowane od ostatniego skanowania.

➤ *W celu wybrania technologii skanowania obiektów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W otwartym oknie, na zakładce **Dodatkowe**, w sekcji **Technologie skanowania** wybierz żądane wartości.

## ZMIENIANIE AKCJI PODEJMOWANEJ NA ZAINFEKOWANYCH PLIKACH

Po wykryciu zainfekowanego obiektu aplikacja wykonuje określoną akcję.

➤ *W celu zmiany akcji wykonywanych na wykrytych obiektach:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Akcja po wykryciu zagrożenia** wybierz wymaganą opcję.

## SKANOWANIE PLIKÓW ZŁOŻONYCH PRZEZ MODUŁ OCHRONA PLIKÓW

Najczęstszą metodą ukrywania wirusów jest osadzenie ich w plikach złożonych: archiwach, pakietach instalacyjnych, osadzonych obiektach OLE i plikach wiadomości pocztowych. W celu wykrycia ukrytych w ten sposób wirusów, plik złożony musi zostać rozpakowany, co znacząco obniża prędkość skanowania.

Dla każdego typu plików złożonych możesz wybrać skanowanie wszystkich plików lub tylko nowych plików. W tym celu kliknij odnośnik znajdujący się obok nazwy obiektu. Przy każdym kliknięciu lewym przyciskiem myszy jego wartość będzie się zmieniać. Jeżeli wybrany zostanie tryb skanowania tylko nowych i zmienionych plików, niedostępne staną się odnośniki do wybrania skanowania wszystkich lub tylko nowych plików.

Domyślnie, Ochrona komputera skanuje tylko osadzone pliki OLE.

W przypadku skanowania plików złożonych o dużym rozmiarze, ich wstępne rozpakowywanie może zająć dużo czasu. Czas ten może zostać skrócony przez włączenie trybu rozpakowywania plików złożonych w tle, jeśli ich rozmiar przekracza określoną wartość. Jeżeli podczas pracy z takim plikiem zostanie wykryty szkodliwy obiekt, aplikacja powiadomi Cię o tym.

Możesz ograniczyć maksymalny rozmiar plików złożonych przeznaczonych do skanowania. Pliki złożone, których rozmiar przekracza zdefiniowaną wartość, nie będą skanowane.

Po wypakowaniu z archiwów plików o dużym rozmiarze będą one skanowane, nawet jeśli została wybrana opcja **Nie rozpakowuj dużych plików złożonych**.

➤ *W celu zmodyfikowania listy plików złożonych przeznaczonych do skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Wydajność**, w sekcji **Skanowanie plików złożonych** zaznacz pola dla tych typów plików, które chcesz skanować.

➤ *W celu ustawienia maksymalnego rozmiaru plików złożonych przeznaczonych do skanowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Wydajność**, w sekcji **Skanowanie plików złożonych** kliknij przycisk **Dodatkowe**.
5. W oknie **Pliki złożone** zaznacz pole **Nie rozpakowuj dużych plików złożonych** i w polu znajdującym się poniżej określ maksymalny rozmiar pliku.

➤ *W celu rozpakowywania dużych plików złożonych w tle:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Wydajność**, w sekcji **Skanowanie plików złożonych** kliknij przycisk **Dodatkowe**.

5. W oknie **Pliki złożone** zaznacz pole **Rozpakowywanie plików złożonych w tle** i określ minimalny rozmiar pliku w polu znajdującym się poniżej.

## OPTIMALIZACJA SKANOWANIA PLIKÓW


Możesz skrócić czas skanowania i przyspieszyć działanie Kaspersky Anti-Virus. W tym celu włącz skanowanie tylko nowych plików i plików zmienionych od czasu ostatniego skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

➤ *W celu skanowania tylko nowych i zmienionych plików:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona plików**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. W otwartym oknie, na zakładce **Wydajność**, w sekcji **Optymalizacja skanowania** zaznacz pole **Skanuj tylko nowe i zmienione pliki**.

## OCHRONA POCZTY

Moduł Ochrona poczty skanuje przychodzące i wychodzące wiadomości w poszukiwaniu szkodliwych obiektów. Jest on ładowany podczas uruchamiania systemu operacyjnego i nieustannie skanuje wszystkie wiadomości elektroniczne przesyłane za pośrednictwem protokołów POP3, SMTP, IMAP, MAPI i NNTP, jak również połączeń szyfrowanych (SSL) dla protokołów POP3 i IMAP (sekcja "Skanowanie połączeń szyfrowanych" na stronie [103](#)).

Wskaźnik działania programu znajdujący się w zasobniku systemowym podczas skanowania wiadomości wygląda następująco .

Moduł Ochrona poczty przechwytuje i skanuje wszystkie wiadomości pocztowe wysyłane i odbierane przez użytkownika. Jeżeli program nie wykryje zagrożenia w wiadomości, stanie się ona dostępna dla użytkownika.

Możesz określić typy wiadomości, które będą skanowane, i wybrać poziom ochrony (strona [87](#)) (ustawienia konfiguracyjne wpływające na szczegółowość skanowania).

Domyślnie zawsze włączony jest tryb analizy sygnatur - wykorzystujący wpisy z baz danych aplikacji do wykrywania zagrożeń. Ponadto możesz użyć analizy heurystycznej. Dodatkowo możesz włączyć filtrowanie załączników (strona [88](#)), które umożliwiała automatyczną zmianę nazwy lub usuwanie określonych typów plików.

Jeżeli Kaspersky Anti-Virus wykryje w pliku zagrożenie, przypisze mu jeden z następujących stanów:

- Stan wskazujący na typ wykrytego szkodliwego programu (na przykład: *wirus, trojan*).
- *Potencjalnie zainfekowany* (podejrzany) - stan przypisywany w sytuacji, gdy nie można jednoznacznie uznać obiektu za zainfekowany. Oznacza to, że aplikacja wykryła sekwencję kodu charakterystyczną dla wirusów i innych szkodliwych programów lub zmodyfikowany kod znanego wirusa.

Aplikacja zablokuje wiadomość i wyświetli powiadomienie (strona [125](#)) o wykrytym zagrożeniu, a także wykona akcję określoną w ustawieniach modułu Ochrona poczty. Możesz zmienić akcje podejmowane po wykryciu zagrożenia (sekcja "Zmianie akcji podejmowanej na zainfekowanych wiadomościach e-mail" na stronie [88](#)).

Jeżeli pracujesz w trybie automatycznym (sekcja "Wybieranie trybu ochrony" na stronie [65](#)), po wykryciu niebezpiecznych obiektów Kaspersky Anti-Virus automatycznie zastosuje akcje zalecane przez specjalistów z Kaspersky Lab. Dla szkodliwych obiektów zastosowana zostanie akcja **Wylecz. Usuń, jeżeli leczenie nie jest możliwe**, dla podejrzanych obiektów – **Podдай kwarantannie**. Jeżeli niebezpieczne obiekty zostaną wykryte podczas pracy w trybie interaktywnym (sekcja "Wybieranie trybu ochrony" na stronie [65](#)), aplikacja wyświetli okno powiadomienia, w którym można wybrać żadaną akcję.

Przed próbą wyleczenia lub usunięcia zainfekowanego obiektu Kaspersky Anti-Virus tworzy jego kopię zapasową, aby w przyszłości można było go przywrócić lub wyleczyć. Podejrzane (potencjalnie zainfekowane) obiekty są poddawane kwarantannie. Możesz włączyć automatyczne skanowanie obiektów poddanych kwarantannie po każdej aktualizacji.

Jeżeli leczenie się powiedzie, wiadomość staje się dostępna dla użytkownika. Jeżeli próba wyleczenia nie powiedzie się, obiekt zostanie usunięty z wiadomości. Ochrona poczty dodaje do tematu wiadomości tekst informujący użytkownika o jej przetworzeniu.

Dla programu MS Outlook dostępna jest specjalna wtyczka umożliwiająca dokładną konfigurację klienta poczty.

W przypadku korzystania z programu The Bat!, program Kaspersky Anti-Virus może zostać użyty w połączeniu z inną aplikacją antywirusową. W tym wypadku reguły przetwarzania ruchu pocztowego są konfigurowane bezpośrednio w The Bat! i posiadają wyższy priorytet niż ustawienia ochrony poczty w Kaspersky Anti-Virus.

Podczas pracy z innymi popularnymi klientami pocztowymi (włączając Microsoft Outlook Express/Poczta systemu Windows, Mozilla Thunderbird, Eudora, Incredimail) moduł Ochrona poczty skanuje wiadomości na protokołach SMTP, POP3, IMAP oraz NNTP.

**Pamiętaj, że podczas pracy z klientem Thunderbird, wiadomości przesyłane przy użyciu protokołu IMAP nie będą skanowane, jeżeli używane są filtry przenoszące wiadomości z folderu **Odebrane**.**

## W TEJ SEKCJI:

Włączanie i wyłączanie modułu Ochrona poczty.....	<a href="#">86</a>
Tworzenie obszaru ochrony modułu Ochrona poczty .....	<a href="#">87</a>
Zmienianie i przywracanie poziomu ochrony.....	<a href="#">87</a>
Używanie analizy heurystycznej.....	<a href="#">88</a>
Zmienianie akcji podejmowanej na zainfekowanych wiadomościach e-mail .....	<a href="#">88</a>
Filtrowanie załączników w wiadomościach e-mail .....	<a href="#">88</a>
Skanowanie plików złożonych przez moduł Ochrona poczty .....	<a href="#">89</a>
Skanowanie poczty elektronicznej w programie Microsoft Office Outlook.....	<a href="#">89</a>
Skanowanie poczty elektronicznej w programie The Bat! .....	<a href="#">89</a>

## WŁĄCZANIE I WYŁĄCZANIE MODUŁU OCHRONA POCZTY

Domyślnie moduł Ochrona poczty jest włączony i działa w trybie zalecanym przez specjalistów z Kaspersky Lab. W razie konieczności możesz wyłączyć Ochronę poczty.

➤ *W celu wyłączenia modułu Ochrona poczty:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. W prawej części okna usuń zaznaczenie z pola **Włącz moduł Ochrona poczty**.

## TWORZENIE OBSZARU OCHRONY MODUŁU OCHRONA POCZTY

Obszar ochrony obejmuje typy skanowanych wiadomości pocztowych, protokoły, na których skanowany jest ruch pocztowy, oraz ustawienia integracji modułu Ochrona poczty z systemem.

Domyślnie Kaspersky Anti-Virus jest integrowany z programem Microsoft Office Outlook i The Bat!, skanuje wiadomości przychodzące i wychodzące oraz skanuje ruch pocztowy wykorzystujący protokoły POP3, SMTP, NNTP i IMAP.

➤ *W celu wyłączenia skanowania wiadomości wychodzących:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. W otwartym oknie, na zakładce **Ogólne**, w sekcji **Obszar ochrony** wybierz opcję **Tylko wiadomości odbierane**.

Jeżeli wybierzesz skanowanie tylko wiadomości przychodzących, przy pierwszym użyciu programu Kaspersky Anti-Virus zalecane jest przeskanowanie wiadomości wysyłanych z uwagi na możliwą obecność robaków internetowych, wykorzystujących pocztę elektroniczną jako kanał dystrybucyjny. Skanowanie wiadomości wysyłanych pozwala uniknąć problemów wynikających z niekontrolowanego wysyłania wiadomości z Twojego komputera.

➤ *W celu wybrania skanowanych protokołów i włączenia integracji modułu Ochrona poczty z systemem:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. W oknie, które zostanie otwarte, na zakładce **Dodatkowe**, w sekcji **Ustawienia skanowania** wybierz wymagane ustawienia.

## ZMIENIANIE I PRZYWRACANIE POZIOMU OCHRONY

W zależności od bieżących potrzeb możesz wybrać jeden z domyślnych poziomów ochrony poczty lub samodzielnie skonfigurować Ochronę poczty.

Specjaliści z Kaspersky Lab zalecają, aby nie konfigurować ustawień Ochrony poczty samodzielnie. W większości przypadków wystarczy wybrać inny poziom ochrony.

Po skonfigurowaniu modułu Ochrona poczty możesz w dowolnym momencie przywrócić ustawienia domyślne. Zapewniają one optymalny poziom ochrony, dlatego są zalecane przez firmę Kaspersky Lab i zostały zebrane w **Zalecanym** poziomie ochrony.

➤ *W celu zmiany poziomu ochrony poczty:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. W prawej części okna, w sekcji **Poziom ochrony** ustaw żądany poziom ochrony lub kliknij przycisk **Ustawienia**, aby ręcznie modyfikować ustawienia.

Jeżeli ustawienia zostaną zmodyfikowane ręcznie, nazwa poziomu ochrony zmieni się na **Niestandardowy**.

➤ *W celu przywrócenia domyślnych ustawień ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. Kliknij przycisk **Poziom domyślny** znajdujący się w prawej części okna, w sekcji **Poziom ochrony**.

## UŻYWANIE ANALIZY HEURYSTYCZNEJ

Podczas działania modułu Ochrona poczty wykorzystywana jest *analiza sygnatur*. Kaspersky Anti-Virus porównuje odnaleziony obiekt z wpisami z baz danych.

Aby zwiększyć efektywność ochrony, możesz użyć *analizy heurystycznej* (tzn. analizy aktywności, którą obiekt wykonuje w systemie). Analiza ta umożliwia wykrywanie nowych szkodliwych obiektów, które nie zostały jeszcze opisane w bazach danych.

➤ *W celu włączenia analizy heurystycznej:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. W prawej części okna, w sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Ogólne**, w sekcji **Metody skanowania** zaznacz opcję **Analiza heurystyczna** i określ poziom szczegółowości skanowania.

## ZMIENIANIE AKCJI PODEJMOWANEJ NA ZAINFEKOWANYCH WIADOMOŚCIACH E-MAIL

Po wykryciu zainfekowanego obiektu aplikacja wykonuje określoną akcję.

➤ *W celu zmiany akcji wykonywanej na zainfekowanych wiadomościach:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. W prawej części okna, w sekcji **Akcja po wykryciu zagrożenia** wybierz wymaganą opcję.

## FILTROWANIE ZAŁĄCZNIKÓW W WIADOMOŚCIACH E-MAIL

Szkodliwe programy mogą rozprzestrzeniać się za pośrednictwem poczty pod postacią załączników. Możliwe jest skonfigurowanie filtrowania według typu załączników, co umożliwi automatyczną zmianę nazwy lub usuwanie określonych typów plików.

➤ *W celu skonfigurowania filtrowania załączników:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.

4. W otwartym oknie wybierz zakładkę **Filtr załączników** i wybierz tryb filtrowania załączników. W przypadku wybrania dwóch ostatnich trybów, włączona zostanie lista typów plików (rozszerzenia), z której można wybrać żądane typy lub dodać maski nowych typów.

Aby dodać maskę nowego typu, należy kliknąć odnośnik **Dodaj** oraz wprowadzić żądane dane w otwartym oknie **Wprowadź maskę nazwy pliku**.

## SKANOWANIE PLIKÓW ZŁOŻONYCH PRZEZ MODUŁ OCHRONA POCZTY

Najczęstszą metodą ukrywania wirusów jest osadzenie ich w plikach złożonych: archiwach, pakietach instalacyjnych, osadzonych obiektach OLE i plikach wiadomości pocztowych. W celu wykrycia ukrytych w ten sposób wirusów, plik złożony musi zostać rozpakowany, co znacząco obniża prędkość skanowania.

Istnieje możliwość włączenia lub wyłączenia skanowania plików złożonych i ograniczenia maksymalnego rozmiaru plików złożonych przeznaczonych do skanowania.

*Jeżeli komputer nie jest chroniony przez żadne oprogramowanie zabezpieczające sieć lokalną, a podczas korzystania z Internetu nie jest wykorzystywany serwer proxy lub Zapora sieciowa, nie jest zalecane wyłączenie skanowania plików złożonych.*

➤ *W celu skonfigurowania ustawień skanowania plików złożonych:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona poczty**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. W celu określenia żądanych ustawień użyj zakładki **Ogólne** otwartego okna.

## SKANOWANIE POCZTY ELEKTRONICZNEJ W PROGRAMIE MICROSOFT OFFICE OUTLOOK

Podczas instalacji Kaspersky Anti-Virus do programu Microsoft Office Outlook dodawana jest specjalna wtyczka. Umożliwia ona szybkie przełączanie do konfiguracji Ochrony poczty z poziomu Microsoft Office Outlook, a także określenie, kiedy wiadomość ma być skanowana (przy odbieraniu, otwieraniu lub wysłaniu).

Ustawienia modułu Ochrona poczty są dostępne z poziomu programu Microsoft Office Outlook, jeżeli opcja ta została wybrana w ustawieniach obszaru ochrony modułu Ochrona poczty.

➤ *W celu przejścia w programie Microsoft Office Outlook do ustawień skanowania poczty:*

1. Otwórz okno główne aplikacji Microsoft Office Outlook.
2. Z menu aplikacji wybierz polecenie **Narzędzia** → **Opcje**.
3. W otwartym oknie **Ustawienia** wybierz zakładkę **Ochrona poczty**.

## SKANOWANIE POCZTY ELEKTRONICZNEJ W PROGRAMIE THE BAT!

Działania podejmowane przez program The Bat! po wykryciu zainfekowanych obiektów definiowane są w ustawieniach własnych programu.

Ignorowane są ustawienia Ochrony poczty określające, czy wiadomości przychodzące i wychodzące powinny być skanowane, które akcje mają być wykonywane na niebezpiecznych obiektach znalezionych w wiadomościach e-mail, oraz które wykluczenia powinny być zastosowane. The Bat! bierze pod uwagę jedynie skanowanie załączonych archiwów.

Ustawienia Ochrony poczty dotyczą wszystkich modułów antywirusowych zainstalowanych na komputerze, które współpracują z programem The Bat!

Pamiętaj, że przychodzące wiadomości są w pierwszej kolejności skanowane przez moduł Ochrona poczty, a dopiero później przez wtyczkę programu The Bat!. Jeżeli program Kaspersky Anti-Virus wykryje szkodliwy obiekt, niezwłocznie Cię o tym poinformuje. Jeżeli w oknie informacyjnym Ochrony poczty wybierzesz akcję **Wylecz (Usuń)**, będzie ona eliminować zagrożenia. Jeżeli w oknie powiadomienia wybierzesz akcję **Pomiń**, obiekt zostanie wyleczony przez wtyczkę programu The Bat!. Podczas wysyłania wiadomości e-mail skanowanie jest najpierw wykonywane przez wtyczkę, a dopiero później przez Ochronę poczty.

Ustawienia modułu Ochrona poczty są dostępne z poziomu programu The Bat!, jeżeli opcja ta została wybrana w ustawieniach obszaru ochrony modułu Ochrona poczty.

W celu skonfigurowania ustawień skanowania poczty w programie The Bat! zdefiniuj następujące kryteria:

- który strumień wiadomości (przychodzący, wychodzący) będzie skanowany;
- kiedy wykonywane będzie skanowanie obiektów pocztowych (podczas otwierania wiadomości lub przed jej zapisaniem na dysku twardym);
- jakie akcje będą podejmowane przez klienta pocztowego po wykryciu niebezpiecznych obiektów w wiadomościach e-mail. Możesz wybrać, na przykład:
  - **Spróbuj wyleczyć zarażone fragmenty** – po wybraniu tej opcji podjęta zostanie próba wyleczenia zainfekowanego obiektu; jeżeli nie powiedzie się, obiekt pozostanie w wiadomości.
  - **Usuń zarażone fragmenty** – usuwa niebezpieczne obiekty w wiadomości e-mail, bez względu na to czy są zainfekowane, czy tylko podejrzane o zainfekowanie.

Program The Bat! domyślnie poddaje kwarantannie wszystkie zainfekowane obiekty e-mail, nie podejmując próby ich wyleczenia.

Wiadomości pocztowe zawierające niebezpieczne obiekty nie są oznaczane specjalnym tematem przy skanowaniu przez wtyczkę dla The Bat!.

➤ *W celu przejścia w programie The Bat! do ustawień skanowania poczty:*

1. Otwórz okno główne programu The Bat!.
2. Z menu **Narzędzia** wybierz **Ustawienia**.
3. Z drzewa ustawień wybierz element **Ochrona antywirusowa**.

## OCHRONA WWW

Za każdym razem, gdy korzystasz z Internetu informacje przechowywane na Twoim komputerze narażone są na ryzyko zainfekowania przez wirusy lub inne szkodliwe programy. Mogą one przeniknąć do komputera podczas pobierania darmowych aplikacji lub przeglądania stron internetowych, które zostały zaatakowane przez hakerów zanim je odwiedziłeś. Robaki sieciowe mogą także przeniknąć do komputera przed otwarciem strony internetowej i pobraniem pliku - wystarczy, że nawiążesz połączenie z Internetem.

Moduł Ochrona WWW chroni dane przesyłane przez protokoły HTTP, HTTPS i FTP oraz zapobiega uruchamianiu niebezpiecznych skryptów na Twoim komputerze.

Moduł Ochrona WWW monitoruje jedynie ruch internetowy przechodzący przez porty znajdujące się na liście monitorowanych portów. Lista monitorowanych portów, które są najczęściej wykorzystywane do transmisji danych, zawarta jest w pakiecie instalacyjnym Kaspersky Anti-Virus. Jeśli używasz portów, które nie znajdują się na liście, dodaj je do listy monitorowanych portów (sekcja "Tworzenie listy monitorowanych portów" na stronie [105](#)), aby chronić dane przez nie przesyłane.

Ochrona WWW skanuje ruch internetowy przy użyciu specjalnego zestawu ustawień nazywanego poziomem ochrony. Jeżeli moduł Ochrona WWW wykryje zagrożenie, wykona odpowiednie działanie. Szkodliwe obiekty są wykrywane przy użyciu baz danych Kaspersky Anti-Virus oraz algorytmu heurystycznego.

**Specjaliści z Kaspersky Lab zalecają, aby samodzielnie nie konfigurować ustawień Ochrony WWW. W większości przypadków wystarczy wybrać odpowiedni poziom ochrony.**

## Algorytm skanowania ruchu internetowego

Każda strona internetowa lub plik, do którego użytkownik lub program uzyskał dostęp za pośrednictwem protokołu HTTP, HTTPS lub FTP, jest przechwytywany i skanowany przez Ochronę WWW w poszukiwaniu szkodliwego kodu.

- Jeżeli żądany przez użytkownika plik lub strona WWW zawiera szkodliwy kod, dostęp zostanie zablokowany. Na ekranie pojawi się komunikat informujący, że obiekt lub strona jest zainfekowana.
- Jeżeli żądany obiekt lub strona WWW nie zawiera szkodliwego kodu, następuje natychmiastowe udzielenie dostępu.

## Algorytm skanowania skryptów

Każdy skrypt uruchamiany na stronie WWW jest przechwytywany przez moduł Ochrona WWW i analizowany w poszukiwaniu szkodliwego kodu:

- Jeżeli skrypt zawiera szkodliwy kod, moduł Ochrona WWW blokuje go i wyświetla powiadomienie.
- Jeżeli w skrypcie nie zostanie wykryty szkodliwy kod, zostanie on uruchomiony.

**Ochrona WWW przechwytuje tylko skrypty używające hosta skryptów Windows.**

## W TEJ SEKCJI:

Włączanie i wyłączanie modułu Ochrona WWW .....	<a href="#">92</a>
Zmienianie i przywracanie poziomu ochrony ruchu sieciowego .....	<a href="#">92</a>
Zmienianie akcji podejmowanej na niebezpiecznych obiektach w ruchu sieciowym .....	<a href="#">92</a>
Sprawdzanie odnośników na stronach internetowych .....	<a href="#">93</a>
Używanie analizy heurystycznej.....	<a href="#">95</a>
Blokowanie niebezpiecznych skryptów .....	<a href="#">95</a>
Optymalizacja skanowania.....	<a href="#">96</a>
Tworzenie listy zaufanych adresów.....	<a href="#">96</a>

## WŁĄCZANIE I WYŁĄCZANIE MODUŁU OCHRONA WWW

Domyślnie moduł Ochrona WWW jest włączony i działa w trybie zalecanym przez specjalistów z Kaspersky Lab. W razie konieczności możesz wyłączyć Ochronę WWW.

➤ *W celu wyłączenia modułu Ochrona WWW:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. W prawej części okna usuń zaznaczenie z pola **Włącz moduł Ochrona WWW**.

## ZMIENIANIE I PRZYWRACANIE POZIOMU OCHRONY RUCHU SIECIOWEGO

W zależności od bieżących potrzeb możesz wybrać jeden z domyślnych poziomów ochrony lub samodzielnie skonfigurować Ochronę WWW.

Po skonfigurowaniu modułu Ochrona WWW możesz w dowolnym momencie przywrócić ustawienia domyślne. Zapewniają one optymalny poziom ochrony, dlatego są zalecane przez firmę Kaspersky Lab i zostały zebrane w **Zalecanym** poziomie ochrony.

➤ *W celu zmiany poziomu ochrony ruchu internetowego:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. W prawej części okna, w sekcji **Poziom ochrony** ustaw żądany poziom ochrony lub kliknij przycisk **Ustawienia**, aby ręcznie modyfikować ustawienia.

Jeżeli ustawienia zostaną zmodyfikowane ręcznie, nazwa poziomu ochrony zmieni się na **Niestandardowy**.

➤ *W celu przywrócenia domyślnego poziomu ochrony:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Poziom domyślny** znajdujący się w prawej części okna, w sekcji **Poziom ochrony**.

## ZMIENIANIE AKCJI PODEJMOWANEJ NA NIEBEZPIECZNYCH OBIEKTACH W RUCHU SIECIOWYM

Po wykryciu zainfekowanego obiektu aplikacja wykonuje określoną akcję.

Moduł Ochrona WWW zawsze blokuje akcje wykonywane przez szkodliwe skrypty i wyświetla wiadomości informujące o podjętym działaniu. Nie można zmienić akcji podejmowanych na niebezpiecznych skryptach; jedyne co można zrobić, to wyłączyć skanowanie skryptów (sekcja "Blokowanie niebezpiecznych skryptów" na stronie [95](#)).

➤ *W celu zmiany akcji wykonywanych na wykrytych obiektach:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.

3. W prawej części okna, w sekcji **Akcja po wykryciu zagrożenia** wybierz wymaganą opcję.

## SPRAWDZANIE ODNOŚNIKÓW NA STRONACH INTERNETOWYCH

Skanowanie stron internetowych w poszukiwaniu phishingu zapobiega *atakom phishingowym*. Ataki phishingowe zazwyczaj mają postać wiadomości e-mail przysłanych rzekomo przez organizacje finansowe i zawierają adresy stron internetowych tych organizacji. Treść takich wiadomości nakłania odbiorcę do kliknięcia odnośnika i wprowadzenia w otwartym oknie prywatnych informacji (np. numeru karty bankowej lub nazwy użytkownika i hasła do internetowego konta bankowego). Atak phishingowy może być zamaskowany, na przykład, pod postacią wiadomości e-mail od banku z odsyłaczem do oficjalnej strony WWW instytucji finansowej. Po kliknięciu odnośnika otwarta zostaje strona internetowa przypominająca tę należącą do danej instytucji finansowej. W rzeczywistości jednak znajdziesz się na spreparowanej stronie. Od tego momentu wszystkie Twoje działania są śledzone i mogą zostać użyte do kradzieży pieniędzy.

Odnośniki do stron typu phishing mogą być otrzymywane zarówno za pośrednictwem poczty elektronicznej, jak również z innych źródeł, takich jak wiadomości ICQ. Z tego powodu moduł Ochrona WWW monitoruje próby dostępu do stron phishingowych na poziomie ruchu internetowego oraz blokuje dostęp do takich lokalizacji.

Do skanowania stron internetowych w poszukiwaniu phishingu oprócz baz danych Kaspersky Anti-Virus można wykorzystać również analizę heurystyczną (strona [95](#)).

### W TEJ SEKCJI:

Włączanie i wyłączanie sprawdzania adresów internetowych.....	<a href="#">93</a>
Używanie Kaspersky URL Advisor.....	<a href="#">93</a>

## WŁĄCZANIE I WYŁĄCZANIE SPRAWDZANIA ADRESÓW INTERNETOWYCH

- *W celu włączenia sprawdzania adresów internetowych przy użyciu baz danych podejrzanych adresów i adresów phishingowych:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.

Zostanie otwarte okno **Ochrona WWW**.

4. Na zakładce **Ogólne** w sekcji **Kaspersky URL Advisor** zaznacz pola **Sprawdź, czy adresy są umieszczone w bazie podejrzanych adresów** i **Sprawdź, czy adresy są umieszczone w bazie adresów phishingowych**.

## UŻYWANIE KASPERSKY URL ADVISOR

Kaspersky URL Advisor jest instalowany w przeglądarce Microsoft Internet Explorer, Mozilla Firefox i Google Chrome jako wtyczka.

Kaspersky URL Advisor skanuje odnośniki na stronach internetowych w celu sprawdzenia, czy znajdują się one na liście podejrzanych adresów. Sprawdza te adresy także na obecność phishingu, podświetlając je w oknie przeglądarki.

Użytkownik może utworzyć listę stron internetowych, na których sprawdzane powinny być wszystkie adresy internetowe, wybrać sprawdzania adresów na wszystkich stronach internetowych, za wyjątkiem tych znajdujących się na liście wykluczeń, skonfigurować sprawdzanie adresów internetowych tylko w wynikach wyszukiwania lub może zdefiniować kategorie stron internetowych, których odnośniki mają być skanowane.

Kaspersky URL Advisor można konfigurować w oknie ustawień aplikacji, a także w oknie ustawień Kaspersky URL Advisor, które jest dostępne z poziomu przeglądarki internetowej.

➤ *W celu określenia stron internetowych, na których sprawdzane mają być wszystkie adresy internetowe:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. Zostanie otwarte okno **Ochrona WWW**.
5. Na zakładce **Bezpieczne surfowanie**, w sekcji **Kaspersky URL Advisor** zaznacz pole **Sprawdzaj adresy internetowe**.
6. Wybierz strony internetowe, na których skanowane mają być odnośniki:
  - a. Jeżeli chcesz utworzyć listę stron internetowych, na których skanowane mają być wszystkie adresy internetowe, wybierz opcję **Tylko na stronach internetowych z listy** i kliknij przycisk **Określ**. W oknie **Sprawdzane adresy internetowe**, które zostanie otwarte, utwórz listę sprawdzanych stron internetowych.
  - b. Jeśli chcesz sprawdzać adresy internetowe na wszystkich stronach poza tymi określonymi, wybierz **Wszystkie poza wykluczonymi** i kliknij przycisk **Wykluczenia**. W otwartym oknie **Wykluczenia** utwórz listę stron, na których odnośniki nie będą sprawdzane.

➤ *W celu sprawdzania adresów internetowych tylko w wynikach wyszukiwania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. Zostanie otwarte okno **Ochrona WWW**.
5. Na zakładce **Bezpieczne surfowanie**, w sekcji **Kaspersky URL Advisor** zaznacz pole **Sprawdzaj adresy internetowe** i kliknij przycisk **Ustawienia**.
6. W otwartym oknie **Ustawienia Kaspersky URL Advisor**, w sekcji **Tryb sprawdzania** wybierz **Tylko adresy internetowe w wynikach wyszukiwania**.

➤ *W celu wybrania kategorii stron internetowych, na których odnośniki mają być sprawdzane:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. Zostanie otwarte okno **Ochrona WWW**.
5. Na zakładce **Bezpieczne surfowanie**, w sekcji **Kaspersky URL Advisor** zaznacz pole **Sprawdzaj adresy internetowe** i kliknij przycisk **Ustawienia**.
6. W otwartym oknie **Ustawienia Kaspersky URL Advisor**, w sekcji **Kategorie stron internetowych** zaznacz pole **Pokaż informacje o kategoriach zawartości stron internetowych**.
7. Na liście kategorii zaznacz pola obok kategorii stron internetowych, na których mają być sprawdzane adresy internetowe.

➤ *W celu otwarcia okna ustawień modułu Kaspersky URL Advisor z poziomu przeglądarki*

kliknij przycisk z ikoną programu Kaspersky Anti-Virus znajdujący się na pasku narzędzi przeglądarki.

## UŻYWANIE ANALIZY HEURYSTYCZNEJ

Aby zwiększyć efektywność ochrony, możesz użyć *analizy heurystycznej* (tzn. analizy aktywności, którą obiekt wykonuje w systemie). Analiza ta umożliwi wykrywanie nowych szkodliwych obiektów, które nie zostały jeszcze opisane w bazach danych.

Jeżeli moduł Ochrona WWW jest włączony, wówczas można włączyć analizę heurystyczną oddzielnie dla skanowania ruchu internetowego i sprawdzania stron internetowych na obecność phishingu.

➤ *W celu włączenia analizy heurystycznej dla skanowania ruchu sieciowego:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.

Zostanie otwarte okno **Ochrona WWW**.

4. Na zakładce **Ogólne**, w sekcji **Analiza heurystyczna** zaznacz pole **Użyj analizy heurystycznej** i ustaw poziom szczegółowości skanowania.

➤ *W celu włączenia analizy heurystycznej dla skanowania stron internetowych w poszukiwaniu elementów phishingu:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.

Zostanie otwarte okno **Ochrona WWW**.

4. Na zakładce **Ogólne**, w sekcji **Kaspersky URL Advisor** kliknij przycisk **Dodatkowe**.
5. W otwartym oknie **Ustawienia Anti-Phishing** zaznacz pole **Użyj analizy heurystycznej podczas skanowania stron internetowych na obecność phishingu** i ustaw poziom szczegółowości skanowania.

## BLOKOWANIE NIEBEZPIECZNYCH SKRYPTÓW

Ochrona WWW skanuje wszystkie skrypty wykonywane przez Microsoft Internet Explorer oraz inne skrypty WSH (JavaScript, Visual Basic Script itp.) uruchomione podczas pracy użytkownika na komputerze. Jeżeli skrypt będzie stanowił zagrożenie dla Twojego komputera, zostanie on zablokowany.

➤ *W celu wyłączenia blokowania niebezpiecznych skryptów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.

Zostanie otwarte okno **Ochrona WWW**.

4. Na zakładce **Ogólne**, w sekcji **Dodatkowe** usuń zaznaczenie pola **Blokuj niebezpieczne skrypty w Microsoft Internet Explorer**.

## OPTIMALIZACJA SKANOWANIA

W celu efektywniejszego wykrywania szkodliwego kodu moduł Ochrona WWW buforuje obiekty pobierane przez Internet. Przy pomocy opcji buforowania moduł Ochrona WWW skanuje obiekty dopiero po ich całkowitym pobraniu na komputer.

Buforowanie zwiększa ilość czasu potrzebnego na przetworzenie obiektu i udostępnienie go dla użytkownika. Ponadto buforowanie może powodować problemy podczas pobierania lub przetwarzania obiektów o dużym rozmiarze, ponieważ może minąć czas wymagany do połączenia z klientem HTTP.

Problem ten można rozwiązać przez ograniczenie czasu buforowania fragmentów obiektów pobieranych z Internetu. Po upływie określonego czasu każdy fragmentu obiektu będzie dostępny do użycia bez przeprowadzenia jego skanowania. Po całkowitym skopiowaniu obiektu zostanie on przeskanowany. Zmniejsza to ilość czasu potrzebnego na przekazanie obiektu użytkownikowi i rozwiązuje problem związany ze zrywaniem połączenia. Poziom ochrony podczas korzystania z Internetu nie zmniejszy się.

Zniesienie ograniczeń czasu buforowania ruchu internetowego zwiększa wydajność skanowania antywirusowego, ale może wydłużać czas dostępu do obiektów.

➤ *W celu nałożenia lub zniesienia ograniczenia czasu buforowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.

Zostanie otwarte okno **Ochrona WWW**.

4. Na zakładce **Ogólne**, w sekcji **Dodatkowe** zaznacz pole **Ogranicz czas buforowania ruchu sieciowego do 1 sekundy w celu zoptymalizowania skanowania**.

## TWORZENIE LISTY ZAUFANYCH ADRESÓW

Moduł Ochrona WWW nie skanuje ruchu internetowego na obecność szkodliwych obiektów, jeżeli pochodzi on z zaufanych adresów internetowych.

➤ *W celu utworzenia listy zaufanych adresów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.

Zostanie otwarte okno **Ochrona WWW**.

4. Na zakładce **Zaufane adresy URL** zaznacz pole **Nie skanuj ruchu sieciowego z zaufanych adresów**.
5. Utwórz listę stron internetowych, którym ufasz co do zawartości. W tym celu:

- a. Kliknij przycisk **Dodaj**.

Zostanie otwarte okno **Maska adresu (URL)**.

- b. Wprowadź adres strony lub maskę adresu.
- c. Kliknij przycisk **OK**.

Nowy wpis pojawi się na liście zaufanych adresów internetowych.

6. W razie konieczności wykonaj kroki od a do c.

## OCHRONA KOMUNIKATORÓW

Moduł Ochrona komunikatorów skanuje ruch komunikatorów internetowych (tzw. pagery internetowe).

Wiadomości wysyłane za pośrednictwem komunikatorów internetowych mogą zawierać odnośniki do podejrzanych stron internetowych oraz do stron wykorzystywanych przez hakerów do ataków typu phishing. Szkodliwe programy wysyłają tą drogą spam i odnośniki do programów (albo same programy), które kradną numery ID i hasła użytkowników.

Kaspersky Anti-Virus zapewnia bezpieczne działanie różnych komunikatorów internetowych, włącznie z ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent i IRC.

Niektóre komunikatory, takie jak Yahoo! Messenger i Google Talk używają połączenia szyfrowanego. W celu skanowania ruchu generowanego przez te programy należy włączyć skanowanie połączeń szyfrowanych (strona [103](#)).

Ochrona komunikatorów przechwytuje wiadomości i sprawdza je na obecność niebezpiecznych obiektów lub adresów internetowych. Możesz wybrać typy wiadomości, które będą skanowane, oraz różne metody skanowania.

Jeżeli w wiadomości zostało wykryte zagrożenie, moduł Ochrona komunikatorów zastąpi ją wiadomością zawierającą ostrzeżenie.

Pliki wymieniane przez klienty komunikatorów internetowych są skanowane przez moduł Ochrona plików (strona [79](#)) podczas próby ich zapisania.

### W TEJ SEKCJI:

Włączanie i wyłączenie modułu Ochrona komunikatorów .....	<a href="#">97</a>
Tworzenie obszaru ochrony modułu Ochrona komunikatorów .....	<a href="#">97</a>
Sprawdzanie odnośników w wiadomościach przesyłanych poprzez komunikatory internetowe .....	<a href="#">98</a>
Używanie analizy heurystycznej.....	<a href="#">98</a>

## WŁĄCZANIE I WYŁĄCZANIE MODUŁU OCHRONA KOMUNIKATORÓW

Domyślnie moduł Ochrona komunikatorów jest włączony i działa w trybie normalnym. W razie konieczności możesz wyłączyć Ochronę komunikatorów.

➔ *W celu wyłączenia Ochrony komunikatorów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona komunikatorów**.
3. W prawej części okna usuń zaznaczenie z pola **Włącz moduł Ochrona komunikatorów**.

## TWORZENIE OBSZARU OCHRONY MODUŁU OCHRONA KOMUNIKATORÓW

Obszarem ochrony nazywa się typ wiadomości przeznaczonych do skanowania. Domyślnie aplikacja skanuje wiadomości zarówno przychodzące, jak i wychodzące. Jeżeli masz pewność, że wiadomości wysyłane przez Ciebie nie zawierają niebezpiecznych obiektów, możesz wyłączyć skanowanie ruchu wychodzącego.

➤ *W celu wyłączenia skanowania wiadomości wychodzących:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona komunikatorów**.
3. W prawej części okna, w sekcji **Obszar ochrony** wybierz opcję **Tylko wiadomości odbierane**.

## SPRAWDZANIE ODNOŚNIKÓW W WIADOMOŚCIACH PRZESYŁANYCH POPRZEC KOMUNIKATORY INTERNETOWE

➤ *W celu skanowania wiadomości na obecność podejrzanych lub phishingowych adresów internetowych:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona komunikatorów**.
3. W prawej części okna, w sekcji **Metody skanowania** zaznacz pole **Sprawdź, czy adresy są umieszczone w bazie podejrzanych adresów** i **Sprawdź, czy adresy są umieszczone w bazie adresów phishingowych**.

## UŻYWANIE ANALIZY HEURYSTYCZNEJ

Aby zwiększyć efektywność ochrony, możesz użyć *analizy heurystycznej* (tzn. analizy aktywności, którą obiekt wykonuje w systemie). Analiza ta umożliwia wykrywanie nowych szkodliwych obiektów, które nie zostały jeszcze opisane w bazach danych.

Podczas korzystania z analizy heurystycznej każdy skrypt znajdujący się w wiadomościach komunikatorów jest uruchamiany w środowisku chronionym. Jeżeli aktywność skryptu ma cechy typowe dla szkodliwych obiektów, jest on automatycznie klasyfikowany jako szkodliwy lub podejrzany. Domyślnie analiza heurystyczna jest włączona.

➤ *W celu włączenia analizy heurystycznej:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona komunikatorów**.
3. W prawej części okna, w sekcji **Metody skanowania** zaznacz opcję **Analiza heurystyczna** i określ poziom szczegółowości skanowania.

## OCHRONA PROAKTYWNA

Moduł Ochrona proaktywna zapewnia ochronę przed nowymi zagrożeniami, które nie znajdują się jeszcze w bazach danych programu Kaspersky Anti-Virus.

Podczas działania moduł Ochrona proaktywna wykorzystywane są technologie proaktywne. Technologie proaktywne umożliwiają neutralizowanie nowych zagrożeń zanim wyrządzą one jakiegokolwiek szkody na Twoim komputerze. W odróżnieniu od tradycyjnych technologii, których analiza kodu oparta jest na wpisach baz danych programu Kaspersky Anti-Virus, technologie prewencyjne rozpoznają nowe zagrożenie dzięki określonej sekwencji działań wykonywanych przez program. Jeżeli w wyniku analizy aktywności okaże się, że sekwencja działań aplikacji wzbudza jakies podejrzenia, zostanie ona zablokowana przez program Kaspersky Anti-Virus.

Na przykład, jeżeli wykryte są akcje takie jak samokopiowanie się programów do zasobów sieciowych, folderu startowego i rejestru systemowego, to bardzo prawdopodobne jest, że programem tym jest robak.

Do niebezpiecznych sekwencji działań należą również próby modyfikacji pliku HOSTS, ukryta instalacja sterowników itd. Możliwe jest wyłączenie monitorowania (strona [99](#)) dowolnej szkodliwej aktywności lub zmodyfikowanie dla niej reguły monitorowania (strona [100](#)).

Możesz utworzyć grupę zaufanych aplikacji (strona [99](#)) dla modułu Ochrona proaktywna. Wówczas nie będziesz informowany o aktywności tych aplikacji.

Jeżeli na Twoim komputerze zainstalowany jest system Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 lub Microsoft Windows 7 x64, kontrola nie będzie stosowana do wszystkich zdarzeń. Wynika to z charakterystycznych cech tych systemów operacyjnych. Na przykład, nie będzie w pełni monitorowane wysyłanie danych przez aplikacje uznane za zaufane oraz podejrzane aktywności systemu.

## W TEJ SEKCJI:

Włączanie i wyłączanie modułu Ochrona proaktywna.....	<a href="#">99</a>
Tworzenie grupy zaufanych aplikacji.....	<a href="#">99</a>
Korzystanie z listy niebezpiecznej aktywności .....	<a href="#">99</a>
Zmianie akcji wykonywanej na niebezpiecznej aktywności aplikacji .....	<a href="#">100</a>

## WŁĄCZANIE I WYŁĄCZANIE MODUŁU OCHRONA PROAKTYWNA

Domyślnie Ochrona proaktywna jest włączona i działa w trybie zalecanym przez specjalistów z Kaspersky Lab. W razie konieczności możesz wyłączyć Ochronę proaktywną.

➤ *W celu wyłączenia modułu Ochrona proaktywna:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona proaktywna**.
3. W prawej części okna usuń zaznaczenie z pola **Włącz moduł Ochrona proaktywna**.

## TWORZENIE GRUPY ZAUFANYCH APLIKACJI

Użytkownik może utworzyć grupę zaufanych aplikacji, których aktywność nie będzie monitorowana przez moduł Ochrona proaktywna. Domyślnie lista zaufanych aplikacji zawiera programy, które są podpisane cyfrowo, i aplikacje znajdujące się w bazie danych Kaspersky Security Network.

➤ *W celu zmiany ustawień grupy zaufanych aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona proaktywna**.
3. W prawej części okna, w sekcji **Zaufane aplikacje** wykonaj następujące czynności:
  - Jeśli chcesz, aby aplikacje z poprawnymi podpisami cyfrowymi były włączane do grupy zaufanych aplikacji, zaznacz pole **Aplikacje podpisane cyfrowo**.
  - Jeśli chcesz, aby aplikacje zaufane w bazie danych Kaspersky Security Network były dodawane do grupy zaufanych aplikacji, zaznacz pole **Zaufane w bazie danych Kaspersky Security Network**.

## KORZYSTANIE Z LISTY NIEBEZPIECZNEJ AKTYWNOŚCI

Nie można modyfikować listy zawierającej akcje typowe dla niebezpiecznej aktywności. Można natomiast wyłączyć monitorowanie wybranej niebezpiecznej aktywności.

➤ *W celu wyłączenia monitorowania wybranej niebezpiecznej aktywności:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona proaktywna**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. W oknie **Ochrona proaktywna** usuń zaznaczenie z pola obok typu aktywności, której monitorowanie chcesz wyłączyć.

## ZMIENIANIE AKCJI WYKONYWANEJ NA NIEBEZPIECZNEJ AKTYWNOŚCI APLIKACJI

Nie można modyfikować listy zawierającej akcje typowe dla niebezpiecznej aktywności. Można natomiast zmienić akcję wykonywaną przez program Kaspersky Anti-Virus po wykryciu niebezpiecznej aktywności aplikacji.

➤ *W celu zmiany akcji wykonywanej przez program Kaspersky Internet Security po wykryciu niebezpiecznej aktywności innej aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Ochrona proaktywna**.
3. Kliknij przycisk **Ustawienia** znajdujący się w prawej części okna.
4. W oknie **Ochrona proaktywna**, w kolumnie **Zdarzenie** wybierz zdarzenie, dla którego chcesz zmodyfikować regułę.
5. Skonfiguruj ustawienia dla wybranego zdarzenia przy użyciu odnośników znajdujących się w sekcji **Opis reguły**. Na przykład:
  - a. Kliknij odnośnik z domyślną akcją i wybierz odpowiednie działanie w oknie **Wybierz akcję**.
  - b. Kliknij odnośnik **Włączono / Wyłączono** w celu wskazania, czy ma zostać utworzony raport z wykonywania działania.

## KONTROLA SYSTEMU

Kontrola systemu gromadzi dane o działaniach aplikacji na Twoim komputerze i dostarcza informacje pozostałym modułom, co zwiększa ochronę.

W oparciu o informacje zebrane przez moduł Kontrola systemu program Kaspersky Anti-Virus może cofnąć akcje wykonane przez szkodliwe programy.

Cofanie akcji wykonanych przez szkodliwe programy może zostać zainicjowane przez jeden z modułów:

- Kontrola systemu - w oparciu o wzorce niebezpiecznej aktywności;
- Ochrona proaktywna;
- Ochrona plików;
- podczas wykonywania skanowania antywirusowego.

Jeśli w systemie zostaną wykryte podejrzane zdarzenia, moduły ochrony programu Kaspersky Anti-Virus zażądadają dodatkowych informacji od modułu Kontrola systemu. W interaktywnym trybie ochrony Kaspersky Anti-Virus (sekcja "Wybieranie trybu ochrony" na stronie [65](#)) możesz przeglądać dane zebrane przez moduł Kontrola systemu

i zaprezentowane pod postacią raportu historii niebezpiecznej aktywności. Dane te pomogą podjąć decyzję podczas wybierania akcji w oknie powiadomienia. Po wykryciu szkodliwego programu odnośnik do raportu Kontroli systemu jest wyświetlany w górnej części okna powiadomienia (strona [149](#)) wraz z możliwością wyboru akcji.

## W TEJ SEKCJI:

Włączanie i wyłączanie modułu Kontrola systemu .....	<a href="#">101</a>
Używanie schematów niebezpiecznej aktywności (BBS) .....	<a href="#">101</a>
Cofanie działań szkodliwego programu .....	<a href="#">102</a>

## WŁĄCZANIE I WYŁĄCZANIE MODUŁU KONTROLA SYSTEMU

Domyślnie moduł Kontrola systemu jest włączony i działa w trybie zalecanym przez specjalistów z Kaspersky Lab. W razie konieczności możesz wyłączyć Kontrolę systemu.

**Zaleca się unikanie wyłączenia modułu, pomijając sytuacje wyjątkowe, ponieważ wpływa to na wydajność Ochrony proaktywnej i innych modułów ochrony, które mogą wymagać danych zebranych przez Kontrolę systemu w celu zidentyfikowania wykrytego zagrożenia.**

➤ *W celu wyłączenia modułu Kontrola systemu:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Kontrola systemu**.
3. W prawej części okna usuń zaznaczenie z pola **Włącz moduł Kontrola systemu**.

## UŻYWANIE SCHEMATÓW NIEBEZPIECZNEJ AKTYWNOŚCI (BBS)

Schematy niebezpiecznej aktywności (BSS – Behavior Stream Signatures) zawierają sekwencje działań typowych dla aplikacji zaklasyfikowanych jako niebezpieczne. Jeśli aktywność aplikacji odpowiada schematowi niebezpiecznej aktywności, Kaspersky Anti-Virus wykona przypisane działanie.

Aby zapewnić ochronę w czasie rzeczywistym na odpowiednim poziomie, podczas aktualizacji bazy danych program Kaspersky Anti-Virus dodaje schematy niebezpiecznej aktywności, które są używane przez Kontrolę systemu.

Domyślnie, jeśli program Kaspersky Anti-Virus działa w trybie automatycznym a aktywność aplikacji odpowiada schematowi niebezpiecznej aktywności, moduł Kontrola systemu przeniesie tę aplikację do Kwarantanny. Podczas działania w trybie interaktywnym moduł Kontrola systemu zapyta użytkownika o działanie. Możesz zdefiniować akcję, którą moduł wykona po wykryciu aktywności aplikacji odpowiadającej schematowi niebezpiecznej aktywności.

Moduł Kontrola systemu wykrywa aktywności aplikacji dokładnie odpowiadające wzorcom niebezpiecznej aktywności oraz takie, które pokrywają się z nimi w pewnym stopniu i dodatkowo zostały uznane za podejrzane na podstawie analizy heurystycznej. Po wykryciu niebezpiecznej aktywności Kontrola systemu pyta użytkownika o akcję bez względu na tryb działania.

➤ *W celu wybrania akcji, która zostanie wykonana po wykryciu aktywności aplikacji odpowiadającej schematowi niebezpiecznej aktywności:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Kontrola systemu**.
3. W prawej części okna, w sekcji **Analiza heurystyczna** zaznacz pole **Użyj schematów niebezpiecznej aktywności (BSS) możliwych do zaktualizowania**.

4. Kliknij **Wybierz akcję**, a następnie z listy rozwijalnej wybierz żądane działanie.

## COFANIE DZIAŁAŃ SZKODLIWEGO PROGRAMU

Możliwe jest użycie funkcji cofania działań wykonanych w systemie przez szkodliwe oprogramowanie. Kontrola systemu zapisuje historię aktywności programu w celu umożliwienia cofnięcia akcji. Można ograniczyć ilość informacji przechowywanych przez Kontrolę systemu dla cofania działań.

Domyślnie Kaspersky Anti-Virus automatycznie cofa działania po wykryciu przez Ochronę proaktywną szkodliwej aktywności. Podczas działania w trybie interaktywnym moduł Kontrola systemu zapyta użytkownika o działanie. Użytkownik może określić akcje podejmowane w przypadku, gdy możliwe jest cofnięcie działań szkodliwego oprogramowania.

Procedura cofania działań szkodliwego oprogramowania oddziałuje na ściśle określony zestaw danych. Nie wpływa to negatywnie na system operacyjny ani na integralność danych.

➤ *W celu wybrania akcji podejmowanej w przypadku, gdy możliwe jest cofnięcie działań szkodliwego oprogramowania:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Kontrola systemu**.
3. W prawej części okna, w sekcji **Cofanie działań szkodliwego oprogramowania** wybierz **Wybierz akcję**, a następnie z listy rozwijalnej wybierz żądaną akcję.

➤ *W celu ograniczenia ilości informacji przechowywanych przez moduł Kontrola systemu dla cofania działań:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Centrum ochrony** wybierz moduł **Kontrola systemu**.
3. W prawej części okna, w sekcji **Cofanie działań szkodliwego oprogramowania** zaznacz pole **Ograniczenie danych przechowywanych dla wycofywania** i określ maksymalną ilość danych przechowywanych dla wycofywania działań.

## OCHRONA SIECI

Narzędzia oraz ustawienia programu Kaspersky Anti-Virus wspólnie zapewniają bezpieczeństwo i kontrolę Twojej aktywności sieciowej.

Poniższe sekcje zawierają szczegółowe informacje o weryfikowaniu połączeń sieciowych, ustawieniach serwera proxy i monitorowaniu portów sieciowych.

### W TEJ SEKCJI:

Skanowanie połączeń szyfrowanych.....	<a href="#">103</a>
Konfigurowanie serwera proxy .....	<a href="#">105</a>
Tworzenie listy monitorowanych portów.....	<a href="#">105</a>

## SKANOWANIE POŁĄCZEŃ SZYFROWANYCH

Nawiązywanie połączeń za pośrednictwem protokołów SSL / TLS chroni dane wymieniane przez Internet. Protokoły SSL / TLS umożliwiają identyfikację stron wymieniających dane przy użyciu certyfikatów elektronicznych, szyfrowanie przesyłanych danych oraz zapewnia ich integralność podczas przesyłania.

Wymienione cechy protokołu często są wykorzystywane przez hakerów do rozsyłania szkodliwych programów, ponieważ większość programów antywirusowych nie skanuje ruchu przechodzącego przez SSL / TLS.

Kaspersky Anti-Virus skanuje połączenia szyfrowane wykorzystując certyfikat Kaspersky Lab.

Jeżeli podczas połączenia z serwerem wykryto nieprawidłowy certyfikat (na przykład, gdy jest zamieniony przez hakera), zostanie wyświetlone powiadomienie z zapytaniem o jego akceptację lub odrzucenie.

Jeśli jesteś pewien, że połączenie ze stroną internetową jest zawsze bezpieczne pomimo nieprawidłowego certyfikatu, możesz dodać stronę do listy zaufanych adresów internetowych. Kaspersky Anti-Virus nie będzie skanować zaszyfrowanego połączenia z tą stroną.

Do zainstalowania certyfikatu możesz użyć Kreatora instalacji certyfikatu, co umożliwi skanowanie połączeń szyfrowanych w trybie częściowo zautomatyzowanym w programie Microsoft Internet Explorer, Mozilla Firefox (jeśli nie jest uruchomiony) i Google Chrome, a także umożliwi otrzymanie instrukcji dotyczących instalacji certyfikatu w przeglądarce Opera.

➤ *W celu włączenia skanowania połączeń szyfrowanych oraz zainstalowania certyfikatu Kaspersky Lab:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz moduł **Sieć**.
3. W oknie, które zostanie otwarte, zaznacz pole **Skanuj połączenia szyfrowane**. Przy pierwszym włączeniu tej opcji uruchomiony zostanie Kreator instalacji certyfikatu.
4. Jeśli kreator się nie uruchomi, kliknij przycisk **Zainstaluj certyfikat**. Zostanie uruchomiony kreator, który pomoże Ci zainstalować certyfikat.

### W TEJ SEKCJI:

Skanowanie połączeń szyfrowanych w przeglądarce Mozilla Firefox ..... [103](#)

Skanowanie połączeń szyfrowanych w przeglądarce Opera ..... [104](#)

## SKANOWANIE POŁĄCZEŃ SZYFROWANYCH W PRZEGLĄDARCE MOZILLA FIREFOX

Przeglądarka Mozilla Firefox nie używa funkcji Microsoft Windows do przechowywania certyfikatów. W celu skanowania połączeń SSL podczas korzystania z tej przeglądarki należy ręcznie zainstalować certyfikat Kaspersky Lab.

Jeśli przeglądarka nie jest uruchomiona, możesz skorzystać z Kreatora instalacji certyfikatu.

➤ *W celu zainstalowania certyfikatu Kaspersky Lab:*

1. Z menu przeglądarki wybierz polecenie **Narzędzia** → **Ustawienia**.
2. W oknie, które zostanie otwarte, wybierz sekcję **Dodatkowe**.
3. W sekcji **Certyfikaty** przejdź na zakładkę **Ochrona** i kliknij przycisk **Przeglądaj certyfikaty**.

4. W oknie, które zostanie otwarte, przejdź na zakładkę **Ośrodki certyfikacji** i kliknij przycisk **Przywróć**.
5. W otwartym oknie wybierz plik certyfikatu Kaspersky Lab. Ścieżka dostępu do pliku z certyfikatem Kaspersky Lab jest następująca:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
6. W otwartym oknie zaznacz pola w celu wybrania akcji, które będą skanowane z użyciem zainstalowanego certyfikatu. Aby zapoznać się z informacjami o certyfikacie, kliknij przycisk **Wyświetl**.

➤ W celu zainstalowania certyfikatu Kaspersky Lab dla przeglądarki Mozilla Firefox w wersji 3.x:

1. Z menu przeglądarki wybierz polecenie **Narzędzia** → **Opcje**.
2. W oknie, które zostanie otwarte, wybierz zakładkę **Zaawansowane**.
3. Na zakładce **Szyfrowanie** kliknij przycisk **Wyświetl certyfikaty**.
4. W oknie, które zostanie otwarte, przejdź do zakładki **Organy certyfikacji** i kliknij przycisk **Importuj**.
5. W otwartym oknie wybierz plik certyfikatu Kaspersky Lab. Ścieżka dostępu do pliku z certyfikatem Kaspersky Lab jest następująca:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
6. W otwartym oknie zaznacz pola w celu wybrania akcji, które będą skanowane z użyciem zainstalowanego certyfikatu. Aby zapoznać się z informacjami o certyfikacie, kliknij przycisk **Wyświetl**.

Jeżeli na Twoim komputerze zainstalowany jest system Microsoft Windows Vista lub Microsoft Windows 7, ścieżka dostępu do pliku certyfikatu Kaspersky Lab jest następująca:  
`%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`

## SKANOWANIE POŁĄCZEŃ SZYFROWANYCH W PRZEGLĄDARCE OPERA

Przełęczarka Opera nie używa funkcji Microsoft Windows do przechowywania certyfikatów. W celu skanowania połączeń SSL podczas korzystania z tej przeglądarki należy ręcznie zainstalować certyfikat Kaspersky Lab.

➤ W celu zainstalowania certyfikatu Kaspersky Lab:

1. Z menu przeglądarki wybierz polecenie **Narzędzia** → **Ustawienia**.
2. W oknie, które zostanie otwarte, wybierz zakładkę **Zaawansowane**.
3. W lewej części okna przejdź do sekcji **Zabezpieczenia** i kliknij przycisk **Zarządzaj certyfikatami**.
4. W oknie, które zostanie otwarte, przejdź do zakładki **Ośrodki certyfikacji** i kliknij przycisk **Importuj**.
5. W otwartym oknie wybierz plik certyfikatu Kaspersky Lab. Ścieżka dostępu do pliku z certyfikatem Kaspersky Lab jest następująca:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
6. W oknie, które zostanie otwarte, kliknij przycisk **Instaluj**. Spowoduje to zainstalowanie certyfikatu Kaspersky Lab. W celu zapoznania się z informacjami o certyfikacie i wybrania działań, które będą monitorowane z użyciem certyfikatu, wybierz go z listy i kliknij przycisk **Wyświetl**.

➤ W celu zainstalowania certyfikatu Kaspersky Lab dla przeglądarki Opera wersja 9.x:

1. Z menu przeglądarki wybierz polecenie **Narzędzia** → **Ustawienia**.
2. W oknie, które zostanie otwarte, wybierz zakładkę **Zaawansowane**.

3. W lewej części okna przejdź do sekcji **Zabezpieczenia** i kliknij przycisk **Zarządzaj certyfikatami**.
4. W oknie, które zostanie otwarte, przejdź do zakładki **Ośrodki certyfikacji** i kliknij przycisk **Importuj**.
5. W otwartym oknie wybierz plik certyfikatu Kaspersky Lab. Ścieżka dostępu do pliku z certyfikatem Kaspersky Lab jest następująca:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert(fake)Kaspersky Anti-Virus personal root certificate.cer.`
6. W oknie, które zostanie otwarte, kliknij przycisk **Instaluj**. Spowoduje to zainstalowanie certyfikatu Kaspersky Lab.

Jeżeli na Twoim komputerze zainstalowany jest system Microsoft Windows Vista lub Microsoft Windows 7, ścieżka dostępu do pliku certyfikatu Kaspersky Lab jest następująca:  
`%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert(fake)Kaspersky Anti-Virus personal root certificate.cer.`

## KONFIGUROWANIE SERWERA PROXY

Jeśli połączenie Twojego komputera z Internetem odbywa się przez serwer proxy, konieczna może się okazać zmiana ustawień dotyczących jego połączeń. Program Kaspersky Anti-Virus używa tych ustawień do pewnych komponentów ochrony, jak również do uaktualniania baz danych i modułów aplikacji.

Jeżeli Twoja sieć zawiera serwer proxy używający niestandardowego portu, należy dodać jego numer do listy monitorowanych portów (sekcja "Tworzenie listy monitorowanych portów" na stronie [105](#)).

➔ *W celu skonfigurowanie połączenia nawiązywanego poprzez serwer proxy:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz moduł **Sieć**.
3. W sekcji **Serwer proxy** kliknij przycisk **Ustawienia serwera proxy**.
4. W oknie **Ustawienia serwera proxy**, które zostanie otwarte, określ wymagane ustawienia dla połączenia z serwerem proxy.

## TWORZENIE LISTY MONITOROWANYCH PORTÓW

Komponenty ochrony, takie jak Ochrona poczty, Ochrona WWW i Ochrona komunikatorów (strona [90](#)), monitorują strumienie danych przesyłane z użyciem określonych protokołów i przechodzące przez poszczególne otwarte porty TCP Twojego komputera. Na przykład Ochrona poczty skanuje informacje przesyłane z użyciem protokołu SMTP, podczas gdy Ochrona WWW skanuje informacje przesyłane przez protokoły HTTP, HTTPS i FTP.

Możesz włączyć monitorowanie wszystkich portów sieciowych lub tylko wybranych. Jeśli w produkcie skonfigurujesz monitorowanie tylko wybranych portów, będziesz mógł utworzyć listę aplikacji, dla których wszystkie porty będą monitorowane. Zalecamy rozszerzenie tej listy o aplikacje otrzymujące lub przesyłające dane poprzez FTP.

➔ *W celu dodania portu do listy monitorowanych portów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Sieć**.
3. W sekcji **Monitorowane porty** wybierz **Monitoruj tylko wybrane porty** i kliknij przycisk **Wybierz**.

Zostanie otwarte okno **Porty sieciowe**.

4. Kliknij odnośnik **Dodaj** umieszczony pod listą portów w górnej części okna. Zostanie otwarte okno **Port sieciowy**, w którym należy wprowadzić numer i opis portu.

➔ *W celu wykluczenia portu z listy monitorowanych portów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Sieć**.
3. W sekcji **Monitorowane porty** wybierz **Monitoruj tylko wybrane porty** i kliknij przycisk **Wybierz**.  
Zostanie otwarte okno **Porty sieciowe**.
4. Z listy portów znajdującej się w górnej części okna wybierz ten, który chcesz wykluczyć, przez usunięcie zaznaczenia z pola obok jego opisu.

➔ *W celu utworzenia listy aplikacji, dla których chcesz monitorować wszystkie porty:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Sieć**.
3. W sekcji **Monitorowane porty** wybierz **Monitoruj tylko wybrane porty** i kliknij przycisk **Wybierz**.  
Zostanie otwarte okno **Porty sieciowe**.
4. Zaznacz pole **Monitoruj wszystkie porty dla wskazanych aplikacji** i na liście aplikacji znajdującej się poniżej zaznacz pola obok nazw tych aplikacji, dla których wszystkie porty powinny być monitorowane.
5. Jeśli wymagana aplikacja nie znajduje się na liście, dodaj ją w następujący sposób:
  - a. Kliknij odnośnik **Dodaj** znajdujący się pod listą aplikacji, aby otworzyć menu, z którego wybierz odpowiedni element:
    - Aby określić lokalizację pliku wykonywalnego aplikacji, wybierz **Przełącznik** i określ lokalizację pliku na komputerze.
    - Aby wybrać aplikację z listy obecnie uruchomionych aplikacji, wybierz **Aplikacje**. W otwartym oknie **Wybierz aplikację** wybierz wymaganą aplikację.
  - b. W oknie **Aplikacja** wprowadź opis dla wybranej aplikacji.

## STREFA ZAUFANA

*Strefa zaufana* jest listą obiektów, których aplikacja nie będzie monitorować. Innymi słowy, jest to zestaw wykluczeń z obszaru ochrony.

Strefa zaufana jest tworzona w oparciu o listę zaufanych aplikacji (sekcja "Tworzenie listy zaufanych aplikacji" na stronie [107](#)) i reguły wykluczeń (sekcja "Tworzenie reguł wykluczeń" na stronie [107](#)) w zależności od funkcji obiektów, z którymi pracujesz, i aplikacji zainstalowanych na komputerze. Umieszczenie obiektów w strefie zaufanej może być przydatne, gdy na przykład Kaspersky Anti-Virus blokuje dostęp do obiektu lub aplikacji, które według Ciebie są nieszkodliwe.

Jeżeli uważasz, że obiekty używane przez Notatnik firmy Microsoft Windows są nieszkodliwe i nie wymagają skanowania, dodaj ten program do listy zaufanych aplikacji w celu wykluczenia tych obiektów ze skanowania.

Pewne działania zaklasyfikowane jako niebezpieczne mogą być traktowane przez inne aplikacje jako nieszkodliwe. Przykładem mogą być tutaj aplikacje, które automatycznie przełączają układ klawiatury (np. Punto Switcher) i regularnie przechwytywać tekst wpisywany z klawiatury. Aby korzystać z właściwości takich aplikacji i wyłączyć monitorowanie ich aktywności, dodaj je do listy zaufanych aplikacji.

Po dodaniu aplikacji do listy zaufanych jej plik i aktywności sieciowe (także te podejrzane) nie będą kontrolowane. Może próbować uzyskać dostęp do rejestru systemu. Należy pamiętać, że pliki wykonywalne oraz procesy zaufanych aplikacji będą skanowane w poszukiwaniu szkodliwych programów, tak jak wcześniej. W celu całkowitego wykluczenia programu ze skanowania użyj reguł wykluczeń.

Wykluczenie zaufanych aplikacji ze skanowania pozwala uniknąć problemów ich kompatybilności z innymi programami (np. podwójne skanowanie ruchu sieciowego przez Kaspersky Anti-Virus i przez inną aplikację antywirusową), jak również zwiększyć wydajność komputera, która w wypadku korzystania z aplikacji serwerowych osiąga wartość krytyczną.

Reguły wykluczeń strefy zaufanej zapewniają możliwość pracy z legalnymi aplikacjami, które mogą być wykorzystywane przez hakerów do uszkodzenia komputera lub danych. Aplikacje te nie posiadają szkodliwych funkcji, ale mogą zostać wykorzystane jako pomocnicze moduły szkodliwego programu. Do tej kategorii zaliczają się aplikacje zdalnej administracji, klienci IRC, serwery FTP, różne narzędzia używane do zatrzymywania lub ukrywania procesów, keyloggery, aplikacje służące do łamania haseł, dialery itd. Takie aplikacje mogą być blokowane przez program Kaspersky Anti-Virus. Aby uniknąć blokowania, możesz skonfigurować reguły wykluczeń.

*Reguła wykluczeń* jest zestawem warunków określających, które obiekty nie będą skanowane przez program Kaspersky Anti-Virus. W innym przypadku, obiekt będzie skanowany przez wszystkie moduły ochrony zgodnie z ich ustawieniami.

Reguły wykluczeń dla strefy zaufanej mogą być wykorzystywane przez kilka modułów aplikacji, takich jak Ochrona plików (sekcja "Ochrona plików" na stronie [79](#)), Ochrona poczty (sekcja "Ochrona poczty" na stronie [85](#)), Ochrona WWW (sekcja "Ochrona WWW" na stronie [90](#)) lub podczas wykonywania zadań skanowania antywirusowego.

## W TEJ SEKCJI:

Tworzenie listy zaufanych aplikacji .....	<a href="#">107</a>
Tworzenie reguł wykluczeń .....	<a href="#">107</a>

## TWORZENIE LISTY ZAUFANYCH APLIKACJI

Domyślnie, Kaspersky Anti-Virus skanuje obiekty otwierane, uruchamiane lub zapisywane przez proces dowolnego programu i monitoruje aktywność wszystkich programów oraz ruchu sieciowego będącego wynikiem ich działania. Jeśli dodasz aplikację do listy zaufanych, Kaspersky Anti-Virus wykluczy ją ze skanowania.

➔ *W celu dodania aplikacji do listy zaufanych:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Zagrożenia i wykluczenia**.
3. W sekcji **Wykluczenia** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Zaufane aplikacje** kliknij przycisk **Dodaj**, aby otworzyć menu wyboru.
5. W otwartym menu wybierz aplikację z listy **Aplikacje** lub wybierz **Przeglądaj**, aby zdefiniować ścieżkę dostępu do pliku wykonywalnego żądanej aplikacji.
6. W otwartym oknie **Wykluczenia dla aplikacji** zaznacz pola dla typów aktywności aplikacji, które będą wykluczone ze skanowania.

## TWORZENIE REGUŁ WYKLUCZEŃ

Jeżeli używasz aplikacji rozpoznanych przez Kaspersky Anti-Virus jako legalne, które mogą zostać wykorzystane przez hakerów do uszkodzenia komputera lub danych, zalecamy utworzenie dla nich reguł wykluczeń.

➔ W celu utworzenia reguły wykluczenia:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Zagrożenia i wykluczenia**.
3. W sekcji **Wykluczenia** kliknij przycisk **Ustawienia**.
4. W oknie, które zostanie otwarte, na zakładce **Reguły wykluczeń** kliknij przycisk **Dodaj**.
5. W otwartym oknie **Reguła wykluczeń** zmodyfikuj ustawienia reguły wykluczeń.

## WYDAJNOŚĆ I KOMPATYBILNOŚĆ Z INNYMI APLIKACJAMI

Wydajność programu Kaspersky Anti-Virus to zakres wykrywanych zagrożeń oraz zużycie energii i intensywność korzystania z zasobów komputera.

Kaspersky Anti-Virus umożliwia wybranie różnych typów zagrożeń (sekcja "Wybieranie kategorii wykrywanych zagrożeń" na stronie [108](#)), które aplikacja powinna wykrywać.

Zużycie energii jest bardzo istotne w przypadku komputerów przenośnych. Skanowanie komputera w poszukiwaniu wirusów i aktualizacja baz danych programu Kaspersky Anti-Virus często wymagają dużej ilości zasobów. Specjalny tryb laptopa programu Kaspersky Anti-Virus (sekcja "Oszczędzanie baterii" na stronie [109](#)) umożliwia automatyczne odrzucanie zaplanowanych zadań skanowania i aktualizacji podczas pracy na bateriach. W wyniku tego oszczędzana jest energia baterii, a tryb Skanowania w czasie bezczynności (sekcja "Uruchamianie zadań w tle" na stronie [110](#)) umożliwia uruchamianie zadania wymagającego dużej ilości zasobów w sytuacji, gdy komputer nie jest używany.

Zużywanie zasobów komputera przez Kaspersky Anti-Virus może wpływać na działanie innych aplikacji. Aby rozwiązać problem równoczesnego wykonywania działań wymagających dużego obciążenia procesora i podsystemów dysku, Kaspersky Anti-Virus może wstrzymać zadania skanowania i udostępnić zasoby innym aplikacjom (sekcja "Zarządzanie zasobami komputera podczas skanowania antywirusowego" na stronie [109](#)) uruchomionym na Twoim komputerze.

W Trybie gracza (strona [111](#)) aplikacja automatycznie wyłącza wyświetlanie powiadomień o aktywności programu Kaspersky Anti-Virus podczas uruchamiania innych aplikacji w trybie pełnoekranowym.

W przypadku aktywnej infekcji w systemie, procedura zaawansowanego leczenia wymagała będzie ponownego uruchomienia komputera, co również może wpłynąć na działanie innych aplikacji. W razie konieczności możesz wyłączyć technologię zaawansowanego leczenia (strona [109](#)) w celu uniknięcia ponownego uruchomienia komputera.

### W TEJ SEKCJI:

Wybieranie kategorii wykrywanych zagrożeń.....	<a href="#">108</a>
Oszczędzanie baterii.....	<a href="#">109</a>
Technologia zaawansowanego leczenia.....	<a href="#">109</a>
Zarządzanie zasobami komputera podczas skanowania antywirusowego.....	<a href="#">109</a>
Uruchamianie zadań w tle.....	<a href="#">110</a>
Tryb pełnoekranowy. Profil gracza.....	<a href="#">111</a>

## WYBIERANIE KATEGORII WYKRYWANYCH ZAGROŻEŃ

Zagrożenia wykryte przez program Kaspersky Anti-Virus podzielone są w oparciu o różne cechy na kategorie. Aplikacja zawsze wykrywa wirusy, trojany oraz szkodliwe narzędzia. Programy te mogą wyrządzić istotne szkody na Twoim komputerze. Aby zapewnić pewniejszą ochronę komputera, możesz poszerzyć listę wykrywanych zagrożeń, włączając

kontrolę akcji wykonywanych przez legalne aplikacje, które hakerzy mogą wykorzystać do uszkodzenia komputera i danych.

➤ *W celu wybrania kategorii wykrywanych zagrożeń:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Zagrożenia i wykluczenia**.
3. W prawej części okna kliknij przycisk **Ustawienia** umieszczony pod listą **Włączone jest wykrywanie następujących rodzajów zagrożeń**
4. W otwartym oknie **Zagrożenia** zaznacz pola przy kategoriach zagrożeń, które powinny zostać wykryte.

## OSZCZĘDZANIE BATERII

W celu oszczędzenia energii komputera przenośnego, wykonywanie zadań skanowania antywirusowego i aktualizacji może zostać odroczone. Jeżeli jest to wymagane, możesz ręcznie uaktualnić program lub uruchomić skanowanie antywirusowe.

➤ *W celu włączenia trybu oszczędzania energii podczas pracy na bateriach:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Oszczędzanie energii**.
3. W prawej części okna zaznacz pole **Wyłącz zaplanowane zadania skanowania podczas pracy na bateriach**.

## TECHNOLOGIA ZAAWANSOWANEGO LECZENIA

Obecnie szkodliwe oprogramowanie może wnikać do najniższych poziomów systemu operacyjnego, co praktycznie uniemożliwia jego usunięcie. W momencie wykrycia aktywnego zagrożenia w systemie aplikacja wyświetla zapytanie dotyczące uruchomienia technologii zaawansowanego leczenia, która umożliwia wyeliminowanie zagrożenia i usunięcie go z komputera.

Po zakończeniu procedury zaawansowanego leczenia nastąpi ponowne uruchomienie komputera. Po ponownym uruchomieniu komputera zalecamy wykonać pełne skanowanie (sekcja "Jak przeprowadzić pełne skanowanie komputera w poszukiwaniu wirusów" na stronie [48](#)).

➤ *W celu włączenia wykorzystywania przez Kaspersky Anti-Virus technologii zaawansowanego leczenia:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Zgodność**.
3. Zaznacz pole **Włącz technologię zaawansowanego leczenia**.

## ZARZĄDZANIE ZASOBAMI KOMPUTERA PODCZAS SKANOWANIA ANTYWIRUSOWEGO

Wykonywanie zadań skanowania antywirusowego zwiększa obciążenie procesora komputera oraz podsystemów dyskowych, co spowalnia działanie innych programów. W przypadku zaistnienia takiej sytuacji program domyślnie wstrzyma wykonywanie zadań antywirusowych oraz udostępni zasoby systemowe dla aplikacji użytkownika.

Jednak istnieją takie aplikacje, które uruchamiają się podczas udostępniania zasobów procesora i działają w tle. Aby skanowanie antywirusowe nie zależało od takich programów, nie należy z nimi współdzielić zasobów systemowych.

➔ *W celu włączenia odraczania przez Kaspersky Anti-Virus zadań skanowania, gdy powodują wolniejsze działanie innych aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Zgodność**.
3. Zaznacz pole **Współdziel zasoby z innymi aplikacjami**.

## URUCHAMIANIE ZADAŃ W TLE

Aby zoptymalizować wykorzystanie zasobów komputera, Kaspersky Anti-Virus wykonuje regularne skanowanie w poszukiwaniu rootkitów w tle i uruchamia zadania wymagające dużej ilości zasobów, kiedy komputer jest beczynny.

Regularne skanowanie w poszukiwaniu rootkitów jest przeprowadzane podczas Twojej pracy na komputerze. Skanowanie trwa co najwyżej 5 minut i wykorzystuje minimalną ilość zasobów komputera.

W czasie beczynności komputera uruchomione mogą zostać następujące zadania:

- automatyczna aktualizacja antywirusowych baz danych oraz modułów programu;
- skanowanie pamięci systemu, obiektów startowych oraz partycji systemu.

Zadania skanowania w czasie beczynności będą uruchamiane, jeśli komputer jest zablokowany przez użytkownika lub jeżeli wygaszacz jest aktywny dłużej niż 5 minut.

Jeśli komputer zasilany jest przez baterie, podczas jego beczynności program nie uruchomi żadnych zadań.

Gdy zadania są uruchomione w tle ich postęp jest wyświetlany w Menedżerze zadań (sekcja "Zarządzanie zadaniami skanowania. Menedżer zadań" na stronie [74](#)).

### W TEJ SEKCJI:

Skanowanie w poszukiwaniu rootkitów w tle .....	<a href="#">110</a>
Skanowanie w czasie beczynności .....	<a href="#">110</a>

## SKANOWANIE W POSZUKIWANIU ROOTKITÓW W TLE

Domyślnie, Kaspersky Anti-Virus wykonuje regularne skanowanie w poszukiwaniu rootkitów. W razie konieczności możesz wyłączyć skanowanie w poszukiwaniu rootkitów.

➔ *W celu wyłączenia regularnego skanowania w poszukiwaniu rootkitów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz podsekcję **Ustawienia ogólne**.
3. W prawej części okna usuń zaznaczenie pola **Wykonuj regularne skanowanie w poszukiwaniu rootkitów**.

## SKANOWANIE W CZASIE BECZYNNOŚCI

W pierwszym etapie skanowania w czasie beczynności sprawdzana jest aktualność baz danych i modułów aplikacji. Jeżeli po skanowaniu wymagana jest aktualizacja, uruchamia się zadanie automatycznej aktualizacji. W drugim etapie aplikacja sprawdza datę i stan ostatniego uruchomienia skanowania w czasie beczynności. Jeżeli skanowanie to nie

zostało jeszcze uruchomione, minęło od niego więcej niż 7 dni lub zostało przerwane, aplikacja uruchamia zadanie skanowania pamięci systemu, obiektów startowych i rejestru systemu.

Skanowanie w czasie bezczynności jest wykonywane z użyciem szczegółowego poziomu analizy heurystycznej, co zwiększa prawdopodobieństwo wykrycia zagrożenia.

Po wznowieniu pracy przez użytkownika zadanie skanowania w czasie bezczynności zostaje automatycznie przerwane. Zauważ, że aplikacja pamięta etap, w którym zostało przerwane skanowanie i wznowi je w przyszłości od tego momentu.

Jeżeli skanowanie w czasie bezczynności zostało przerwane podczas pobierania pakietu uaktualnień, aktualizacja rozpocznie się od początku.

➤ *W celu wyłączenia trybu skanowania w czasie bezczynności:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Skanowanie** wybierz podsekcję **Ustawienia ogólne**.
3. W prawej części okna usuń zaznaczenie pola **Wykonuj skanowanie w trybie bezczynności**.

## TRYB PEŁNOEKRANOWY. PROFIL GRACZA

Pewne programy (w szczególności gry wideo) działające w trybie pełnoekranowym nie są wystarczająco kompatybilne z niektórymi funkcjami Kaspersky Anti-Virus, takimi jak powiadomienia wyskakujące. Dodatkowo, aplikacje tego typu często pochłaniają znaczną część zasobów systemowych, zatem wykonywanie pewnych zadań przez Kaspersky Anti-Virus może spowolnić ich działanie.

Kaspersky Anti-Virus posiada specjalną opcję czasowej modyfikacji ustawień, z której można korzystać podczas używania trybu gracza. Pozwala ona uniknąć ręcznego wyłączenia powiadomień i zatrzymywania zadań za każdym razem, gdy włączasz aplikacje o trybie pełnoekranowym. Gdy Profil gracza jest aktywny, przełączenie na tryb pełnoekranowy automatycznie zmienia ustawienia wszystkich modułów produktu, aby zapewnić optymalne działanie systemu w tym trybie. Przy wyjściu z trybu pełnoekranowego ustawienia produktu wracają do wartości wprowadzonych przed przejściem do trybu pełnoekranowego.

➤ *W celu włączenia profilu gracza:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Profil gracza**.
3. Zaznacz pole **Użyj Profilu gracza** i w sekcji **Opcje profilu** znajdującej się poniżej określ wymagane ustawienia trybu gracza.

## AUTOCHRONA PROGRAMU KASPERSKY ANTI-VIRUS

Ponieważ Kaspersky Anti-Virus zapewnia Twojemu komputerowi ochronę przed szkodliwym oprogramowaniem, aplikacje tego typu przenikające do Twojego komputera mogą próbować blokować jego działania, a nawet usuwać go z Twojego komputera.

Stabilne działanie systemu ochrony komputera utrzymane jest dzięki funkcjom autoochrony i ochrony przed zdalnym dostępem, będących częścią programu Kaspersky Anti-Virus.

Autoochrona zapobiega modyfikacji i usuwaniu plików programu Kaspersky Anti-Virus, procesów w pamięci oraz wpisów w rejestrze systemu. Ochrona przed zdalnym dostępem umożliwia blokowanie wszelkich prób zdalnej kontroli aplikacji.

Na komputerach działających pod kontrolą 64-bitowych systemów operacyjnych oraz systemu Microsoft Windows Vista autoochrona chroni tylko przed modyfikacją lub usunięciem plików programu zapisanych na dyskach lokalnych oraz wpisów rejestru.

**W TEJ SEKCJI:**

Włączanie i wyłączanie autoochrony.....	<a href="#">112</a>
Ochrona przed kontrolą zewnętrzną .....	<a href="#">112</a>

**WŁĄCZANIE I WYŁĄCZANIE AUTOOCHRONY**

Domyślnie autoochrona programu Kaspersky Anti-Virus jest włączona. W razie konieczności możesz ją wyłączyć.

➤ *W celu wyłączenia autoochrony programu Kaspersky Anti-Virus:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Autoochrona**.
3. W prawej części okna usuń zaznaczenie pola **Włącz autoochronę**.

**OCHRONA PRZED KONTROLĄ ZEWNĘTRZNĄ**

Domyślnie ochrona przed kontrolą zewnętrzną jest włączona. W razie konieczności możesz ją wyłączyć.

Jeśli chcesz korzystać z aplikacji do zdalnej administracji (takich jak RemoteAdmin) musisz dodać je do listy Zaufane aplikacje (sekcja "Strefa zaufana" na stronie [106](#)) przy włączonej Zewnętrznej kontroli usługi i włączyć dla nich ustawienie **Nie monitoruj aktywności aplikacji**.

➤ *W celu wyłączenia ochrony przed kontrolą zewnętrzną:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Autoochrona**.
3. W sekcji **Kontrola zewnętrzna** usuń zaznaczenie z pola **Wyłącz możliwość zewnętrznej kontroli usługi**.

**KWARANTANNA I KOPIA ZAPASOWA**

*Kwarantanna* jest specjalnym obszarem, w którym przechowywane są potencjalnie zainfekowane pliki oraz pliki, które nie mogły zostać wyleczone w momencie wykrycia.

Potencjalnie zainfekowany plik może zostać wykryty i umieszczony w folderze kwarantanny podczas skanowania antywirusowego oraz przez moduł Ochrona plików, Ochrona poczty lub Ochrona proaktywna.

Obiekty poddawane są kwarantannie w następujących przypadkach:

- Kod pliku przypomina znane zagrożenie lub ma strukturę podobną do szkodliwego obiektu, ale nie jest zarejestrowany w bazie danych. W tym przypadku plik zostaje przeniesiony do Kwarantanny po przeprowadzeniu analizy heurystycznej przez Ochronę plików lub Ochronę poczty lub podczas skanowania antywirusowego. Analiza heurystyczna generuje bardzo mało fałszywych alarmów.
- Sekwencja działań wykonanych przez obiekt wygląda podejrzanie. W tym wypadku plik zostaje przeniesiony do Kwarantanny po przeanalizowaniu jego zachowania przez moduł Ochrona proaktywna.

Pliki w Kwarantannie nie stanowią zagrożenia. Wraz z upływem czasu pojawiają się informacje o nowych zagrożeniach i sposobach ich neutralizowania, co może umożliwić wyleczenie przez Kaspersky Anti-Virus pliku umieszczonego w Kwarantannie.

*Miejsce przechowywania kopii zapasowej* zostało zaprojektowane do przechowywania kopii zapasowych plików, które w wyniku procesu leczenia zostały usunięte lub zmodyfikowane.

## W TEJ SEKCJI:

Przechowywanie obiektów Kwarantanny i Kopii zapasowej.....	<a href="#">113</a>
Pracowanie z plikami poddanymi kwarantannie.....	<a href="#">113</a>
Pracowanie z obiektami w Kopii zapasowej.....	<a href="#">115</a>
Skanowanie plików w Kwarantannie po aktualizacji.....	<a href="#">115</a>

## PRZECHOWYWANIE OBIEKTÓW KWARANTANNY I KOPII ZAPASOWEJ

Domyślnie maksymalny czas przechowywania obiektów wynosi 30 dni. Po tym czasie obiekty zostaną usunięte. Możesz wyłączyć ograniczenie czasu przechowywania obiektu lub zmienić jego maksymalną wartość.

Dodatkowo możesz zdefiniować maksymalny rozmiar Kwarantanny i Kopii zapasowej. Gdy maksymalny rozmiar zostanie osiągnięty, zawartość Kwarantanny i Kopii zapasowej zostanie zastąpiona nowymi obiektami. Domyślnie ograniczenie maksymalnego rozmiaru jest wyłączone.

### ➤ *W celu zmiany maksymalnego czasu przechowywania obiektów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Przechowywanie obiektów kwarantanny i kopii zapasowej** zaznacz pole **Przechowuj obiekty nie dłużej niż** i zdefiniuj maksymalny czas przechowywania obiektów znajdujących się w kwarantannie.

### ➤ *W celu skonfigurowania maksymalnego rozmiaru Kwarantanny i Kopii zapasowej:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Przechowywanie obiektów kwarantanny i kopii zapasowej** zaznacz pole **Maksymalny rozmiar** i zdefiniuj maksymalny rozmiar kwarantanny i kopii zapasowej.

## PRACOWANIE Z PLIKAMI Poddanymi Kwarantannie

Kwarantanna Kaspersky Anti-Virus umożliwia wykonywanie następujących akcji:

- poddawanie kwarantannie plików, które uważasz za zainfekowane;
- skanowanie plików w Kwarantannie przy pomocy bieżącej wersji baz danych Kaspersky Anti-Virus;
- przywracanie plików do oryginalnych folderów, z których zostały przeniesione do Kwarantanny;
- usuwanie wybranych plików z Kwarantanny;
- wysyłanie plików poddanych kwarantannie do analizy do firmy Kaspersky Lab.

Możesz wykorzystać następujące sposoby, aby przenieść plik do Kwarantanny:

- używając przycisku **Przenieś do kwarantanny** dostępnego w oknie **Kwarantanna**;
- użyj menu kontekstowego pliku.

➤ *W celu przeniesienia pliku do Kwarantanny z poziomu okna Kwarantanna:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Kwarantanna** kliknij przycisk **Przenieś do kwarantanny**.
4. W otwartym oknie wybierz plik, który chcesz przenieść do Kwarantanny.

➤ *W celu przeniesienia pliku do Kwarantanny przy użyciu menu kontekstowego:*

1. Otwórz Eksploratora Microsoft Windows i przejdź do foldera zawierającego plik, który ma zostać przeniesiony do Kwarantanny.
2. Otwórz menu kontekstowe pliku, klikając go prawym przyciskiem myszy, i wybierz polecenie **Poddaj kwarantannie**.

➤ *W celu przeskanowania pliku poddanego kwarantannie:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Kwarantanna** wybierz plik, który chcesz przeskanować.
4. Kliknij przycisk **Skanowanie**.

➤ *W celu przywrócenia obiektu poddanego kwarantannie:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Kwarantanna** wybierz plik, który chcesz przywrócić.
4. Kliknij przycisk **Przywróć**.

➤ *W celu usunięcia obiektu poddanego kwarantannie:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Kwarantanna** wybierz plik, który chcesz usunąć.
4. Kliknij plik prawym przyciskiem myszy, aby otworzyć jego menu kontekstowe, i wybierz **Usuń**.

➤ *W celu wysłania obiektu poddanego kwarantannie do analizy do firmy Kaspersky Lab:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Kwarantanna** wybierz plik, który chcesz przesłać do analizy.

4. Otwórz menu kontekstowe pliku, klikając go prawym przyciskiem myszy, i wybierz polecenie **Wyślij plik do analizy**.

## PRACOWANIE Z OBIEKTAMI W KOPII ZAPASOWEJ

Kopia zapasowa Kaspersky Anti-Virus pozwala wykonywać następujące akcje:

- przywracać pliki do określonych folderów lub folderów pierwotnych, w których plik znajdował się przed przetworzeniem go przez Kaspersky Anti-Virus;
- usuwać wybrane pliki lub wszystkie pliki z Kopii zapasowej.

### ➤ *W celu przywrócenia obiektu z Kopii zapasowej:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Miejsce przechowywania** wybierz plik, który chcesz przywrócić.
4. Kliknij przycisk **Przywróć**.

### ➤ *W celu usunięcia pliku z Kopii zapasowej:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Miejsce przechowywania** wybierz plik, który chcesz usunąć.
4. Kliknij plik prawym przyciskiem myszy, aby otworzyć jego menu kontekstowe, i wybierz **Usuń**.

### ➤ *W celu usunięcia wszystkich plików z Kopii zapasowej:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Kwarantanna**.
3. Na zakładce **Miejsce przechowywania** kliknij przycisk **Wyczyść miejsce przechowywania**.

## SKANOWANIE PLIKÓW W KWARRANTANNIE PO AKTUALIZACJI

Jeśli aplikacja przeskanuje plik i nie rozpozna dokładnie typu szkodliwego programu, podda go kwarantannie. Możliwe, że po aktualizacji baz danych Kaspersky Anti-Virus wykryje i wyeliminuje to zagrożenie. Możesz włączyć automatyczne skanowanie obiektów poddanych kwarantannie po każdej aktualizacji.

Zalecamy okresowe przeglądanie plików poddanych kwarantannie. Skanowanie może spowodować zmianę ich stanu. Możliwe może okazać się przywrócenie niektórych tego typu plików do poprzedniej lokalizacji oraz kontynuowanie pracy z nimi.

### ➤ *W celu włączenia skanowania plików poddanych kwarantannie po aktualizacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Aktualizacja** wybierz składnik **Ustawienia aktualizacji**.
3. Zaznacz pole **Przeskanuj kwarantannę po aktualizacji** znajdujące się w sekcji **Dodatkowe**.

## DODATKOWE NARZĘDZIA ZWIĘKSZAJĄCE BEZPIECZEŃSTWO KOMPUTERA

Do rozwiązywania konkretnych problemów dotyczących zabezpieczeń komputera służą następujące kreatory i narzędzia wchodzące w skład Kaspersky Anti-Virus:

- Kreator tworzenia dysku ratunkowego został zaprojektowany do tworzenia obrazu dysku ISO i zapisywania go na nośniku wymiennym. Dysk ratunkowy umożliwi przywrócenie działania systemu po ataku wirusa, gdy zostanie załadowany z nośnika wymiennego. Dysk ratunkowy może zostać wykorzystany, jeżeli infekcji nie można wyleczyć przy użyciu programów antywirusowych lub narzędzi do usuwania szkodliwego oprogramowania.
- Kreator czyszczenia śladów aktywności wyszukuje i eliminuje ślady aktywności użytkownika w systemie oraz ustawienia systemu, które umożliwiają uzyskanie informacji o działaniach użytkownika.
- Kreator przywracania systemu służy do eliminowania śladów obecności szkodliwych obiektów w systemie.
- Kreator konfiguracji przeglądarki analizuje i dostosowuje ustawienia programu Microsoft Internet Explorer w celu wyeliminowania potencjalnych luk.

Wszystkie problemy wykryte przez Kreatory (za wyjątkiem Kreatora tworzenia dysku ratunkowego) są pogrupowane w oparciu o typ zagrożenia, jakie stanowią dla systemu operacyjnego. Dla każdej grupy Kaspersky Lab oferuje zestaw akcji, które mają na celu pomoc w wyeliminowaniu luk i słabych punktów ustawień systemu. Rozróżniane są trzy grupy problemów oraz odpowiednio trzy grupy podejmowanych akcji:

- *Szczególnie zalecane działania* pomogą wyeliminować problemy stwarzające poważne zagrożenie dla systemu. Zaleca się bezzwłoczne wykonanie wszystkich akcji z tej grupy w celu wyeliminowania zagrożenia.
- *Zalecane działania* pomogą wyeliminować problemy stwarzające potencjalne zagrożenie. W celu zapewnienia optymalnego poziomu ochrony zaleca się wykonywanie wszystkich akcji tej grupy.
- *Dodatkowe działania* pomagają naprawić uszkodzenia systemu, które obecnie nie stanowią zagrożenia, ale mogą stwarzać problem w przyszłości. Wykonywanie tych działań zapewnia odpowiednią ochronę Twojego komputera. Jednak, w pewnych przypadkach, mogą one prowadzić do usuwania pewnych ustawień użytkownika (np. pliki cookie).

### W TEJ SEKCJI:

Czyszczenie śladów aktywności .....	<a href="#">116</a>
Konfigurowanie ustawień przeglądarki dla bezpiecznej pracy.....	<a href="#">118</a>
Cofanie zmian dokonanych przez kreatory .....	<a href="#">119</a>

## CZYSZCZENIE ŚLADÓW AKTYWNOŚCI

W systemie rejestrowane są różne czynności użytkownika wykonywane podczas pracy na komputerze. Należą do nich zapytania dla wyszukiwarek, odwiedzane strony internetowe, uruchamiane programy, otwierane i zapisywane pliki, wpisy w dzienniku zdarzeń systemu Microsoft Windows, pliki tymczasowe itd.

Wszystkie te źródła informacji o aktywności użytkownika mogą zawierać poufne dane (także hasła) i mogą być dostępne dla osób niepowołanych. Użytkownik często nie posiada wystarczającej wiedzy, jak zapobiec kradzieży informacji z tych źródeł.

Aplikacja Kaspersky Anti-Virus zawiera Kreator czyszczenia śladów aktywności. Jego zadaniem jest wyszukiwanie nagromadzonych śladów aktywności użytkownika w systemie oraz ustawień systemu operacyjnego.

Należy pamiętać, że informacje związane z aktywnością użytkownika są cały czas rejestrowane w systemie. Uruchomienie dowolnego pliku lub otwarcie dowolnego dokumentu jest zapisywane w historii. Dziennik systemu Microsoft Windows rejestruje także wiele zdarzeń występujących w systemie. Z tego powodu powtórne uruchomienie Kreatora czyszczenia śladów aktywności może spowodować wykrycie takich śladów aktywności, które nie zostały usunięte podczas jego poprzedniego uruchomienia. Niektóre pliki mogą być wykorzystywane przez system w czasie, gdy kreator próbuje je usunąć (na przykład plik dziennika zdarzeń systemu Microsoft Windows). W celu usunięcia tych plików Kreator zasugeruje ponowne uruchomienie systemu. Jednak podczas restartu mogą one zostać odtworzone i powtórnie wykryte jako ślady aktywności.

Kreator składa się z szeregu okien (kroków) przełączanych przy pomocy przycisków **Wstecz** i **Dalej**. W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**. W celu zatrzymania kreatora w dowolnym momencie użyj przycisku **Anuluj**.

➤ *W celu usunięcia śladów aktywności użytkownika w systemie:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Narzędzia**.
3. W otwartym oknie, w sekcji **Czyszczenie śladów aktywności** kliknij przycisk **Uruchom**.

Przyjrzyjmy się dokładniej krokom kreatora.

### Krok 1. Uruchamianie Kreatora

Upewnij się, że wybrana została opcja **Wykonaj diagnostykę śladów aktywności użytkownika** i kliknij przycisk **Dalej**, aby uruchomić Kreator.

### Krok 2. Wyszukiwanie śladów aktywności

Kreator wyszukuje ślady szkodliwej aktywności na komputerze. Skanowanie może zająć trochę czasu. Po zakończeniu wyszukiwania kreator automatycznie przejdzie do następnego kroku.

### Krok 3. Wybieranie akcji Kreatora czyszczenia śladów aktywności

Po zakończeniu wyszukiwania Kreator wyświetli wykryte ślady aktywności i metody ich usunięcia.

Aby wyświetlić listę akcji z grupy, kliknij ikonę **+** znajdującą się z lewej strony nazwy grupy.

Aby Kreator wykonał żądane działanie, zaznacz pole znajdujące się z lewej strony opisu odpowiedniej akcji. Domyślnie Kreator wykonuje wszystkie zalecane i szczególnie zalecane akcje. Jeżeli nie chcesz wykonywać pewnych akcji, usuń zaznaczenie z pól obok nich.

**Zdecydowanie nie zaleca się usuwania zaznaczeń z pól wybranych domyślnie, gdyż zwiększy to podatność Twojego komputera na ataki.**

Po zdefiniowaniu zestawu działań, które Kreator wykona, kliknij przycisk **Dalej**.

### Krok 4. Czyszczenie śladów aktywności

Kreator wykona działania wskazane w poprzednim kroku. Może to zająć chwilę czasu. Czyszczenie niektórych śladów aktywności może wymagać ponownego uruchomienia komputera. Jeżeli będzie to konieczne, kreator wyświetli odpowiedni komunikat.

Po zakończeniu czyszczenia Kreator automatycznie przejdzie do następnego kroku.

## Krok 5. Kończenie działania kreatora

Jeśli chcesz, aby ślady aktywności były czyszczone automatycznie po każdym zakończeniu pracy programu Kaspersky Anti-Virus, w ostatnim ekranie Kreatora zaznacz pole **Usuń ślady aktywności po zamknięciu Kaspersky Anti-Virus**. Jeżeli zamierzasz ręcznie czyścić ślady aktywności, nie zaznaczaj tego pola.

W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

## KONFIGUROWANIE USTAWIEŃ PRZEGLĄDARKI DLA BEZPIECZNEJ PRACY

W niektórych przypadkach wymagane jest przeprowadzenie analizy przeglądarki Microsoft Internet Explorer oraz jej skonfigurowanie, gdyż niektóre domyślne ustawienia lub te wprowadzone przez użytkownika mogą prowadzić do problemów z ochroną.

Poniżej znajdują się przykłady obiektów i ustawień używanych w przeglądarce oraz ich powiązanie z potencjalnym zagrożeniem ochrony:

- **Pamięć podręczna Microsoft Internet Explorer.** Pamięć podręczna przechowuje dane pobierane z Internetu, co zapobiega ich późniejszemu ponownemu pobieraniu. Przyspiesza to otwieranie stron oraz zmniejsza ruch internetowy. Dodatkowo pamięć podręczna zawiera poufne dane, co umożliwia sprawdzenie, jakie strony użytkownik odwiedzał. Niektóre szkodliwe programy skanują pamięć podręczną i pobierają z niej np. adresy e-mail. Zaleca się czyścić pamięć podręczną wraz z każdym zamykaniem przeglądarki internetowej.
- **Wyświetlanie rozszerzeń plików znanych typów.** Aby łatwo modyfikować nazwy plików, możesz wyłączyć pokazywanie ich rozszerzeń. Niemniej jednak, wyświetlanie rozszerzeń plików może być czasem przydatne. Nazwy wielu szkodliwych plików zawierają dodatkowe kombinacje symboli znajdujące się przed prawdziwym rozszerzeniem (np. example.txt.com). Jeżeli prawdziwe rozszerzenie nie jest wyświetlane, użytkownik może zobaczyć tylko nazwę pliku z fałszywym rozszerzeniem i tym samym zidentyfikować szkodliwy obiekt jako nieszkodliwy. Aby zwiększyć ochronę, zaleca się włączenie wyświetlania znanych formatów plików.
- **Lista zaufanych adresów internetowych.** Aby niektóre strony internetowe mogły działać poprawnie, powinieneś dodać je do listy zaufanych. Warto pamiętać, że szkodliwe obiekty również mogą dodać do tej listy odnośniki do stron utworzonych przez hakerów.

Konfiguracja przeglądarki dla trybu Bezpieczne uruchamianie może powodować problemy podczas wyświetlania niektórych stron (na przykład, gdy używają elementów ActiveX). W celu rozwiązania tych problemów dodaj takie strony do strefy zaufanej.

Analiza i konfiguracja przeglądarki wykonywane są w Kreatorze konfiguracji przeglądarki. Kreator sprawdza, czy zainstalowane są ostatnie aktualizacje przeglądarki oraz czy jej ustawienia nie sprawiają, że system jest podatny na ataki. Po zakończeniu pracy Kreatora wygenerowany zostanie raport, który możesz wysłać do firmy Kaspersky Lab w celu poddania go szczegółowej analizie.

Kreator składa się z szeregu okien (kroków) przełączanych przy pomocy przycisków **Wstecz** i **Dalej**. W celu zamknięcia kreatora po zakończeniu jego działania kliknij przycisk **Zakończ**. W celu zatrzymania kreatora w dowolnym momencie użyj przycisku **Anuluj**.

Przed uruchomieniem diagnostyki zamknij wszystkie okna przeglądarki Microsoft Internet Explorer.

➔ *W celu skonfigurowania przeglądarki dla bezpiecznej pracy:*

1. Otwórz okno główne aplikacji.
2. W dolnej części okna wybierz sekcję **Narzędzia**.
3. W oknie, które zostanie otwarte, w sekcji **Konfiguracja przeglądarki** kliknij przycisk **Uruchom**.

Przyjrzyjmy się dokładniej krokom kreatora.

### Krok 1. Uruchamianie Kreatora

Aby uruchomić Kreator, upewnij się, że wybrana została opcja **Wykonaj diagnostykę dla Microsoft Internet Explorer** i kliknij przycisk **Dalej**.

### Krok 2. Analiza ustawień programu Microsoft Internet Explorer

Kreator analizuje ustawienia programu Microsoft Internet Explorer. Może to zająć chwilę czasu. Po zakończeniu wyszukiwania kreator automatycznie przejdzie do następnego kroku.

### Krok 3. Wybieranie akcji dla konfiguracji przeglądarki

Po zakończeniu wyszukiwania Kreator wyświetli wykryte problemy i metody ich usunięcia.

Aby wyświetlić listę akcji z grupy, kliknij ikonę **+** znajdującą się z lewej strony nazwy grupy.

Aby Kreator wykonał żądane działanie, zaznacz pole znajdujące się z lewej strony opisu odpowiedniej akcji. Domyślnie Kreator wykonuje wszystkie zalecane i szczególnie zalecane akcje. Jeżeli nie chcesz wykonywać pewnych akcji, usuń zaznaczenie z pól obok nich.

Zdecydowanie nie zaleca się usuwania zaznaczeń z pól wybranych domyślnie, gdyż zwiększy to podatność Twojego komputera na ataki.

Po zdefiniowaniu zestawu działań, które Kreator wykona, kliknij przycisk **Dalej**.

### Krok 4. Konfiguracja przeglądarki

Kreator wykona działania wskazane w poprzednim kroku. Konfiguracja przeglądarki może zająć trochę czasu. Po zakończeniu konfiguracji Kreator automatycznie przejdzie do następnego kroku.

### Krok 5. Kończenie działania kreatora

W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

## COFANIE ZMIAN DOKONANYCH PRZEZ KREATORY

Niektóre zmiany wykonane przez Kreatora czyszczenia śladów aktywności (sekcja "Czyszczenie śladów aktywności" na stronie [116](#)), Kreatora przywracania systemu (sekcja "Co zrobić, gdy podejrzewasz, że komputer został zainfekowany" na stronie [52](#)) i Kreatora konfiguracji przeglądarki (sekcja "Konfigurowanie ustawień przeglądarki dla bezpiecznej pracy" na stronie [118](#)) mogą zostać wycofane.

➤ *W celu wycofania zmian dokonanych przez kreatory:*

1. Otwórz okno główne aplikacji i wybierz w jego dolnej części sekcję **Narzędzia**.
2. W prawej części okna kliknij przycisk **Uruchom**, znajdujący się w sekcji z nazwą kreatora, dla którego chcesz wycofać wykonane zmiany:
  - **Czyszczenie śladów aktywności** – aby wycofać zmiany wykonane przez Kreatora Czyszczenia śladów aktywności;
  - **Znajdź i rozwiąż problemy z systemem Windows** – aby wycofać zmiany wykonane przez Kreatora przywracania systemu;

- **Konfiguracja przeglądarki** – aby wycofać zmiany wykonane przez Kreatora konfiguracji przeglądarki.

Przyjrzyjmy się krokom kreatora wykonywanym podczas cofania zmian.

### Krok 1. Uruchamianie Kreatora

Wybierz **Cofnij zmiany** i kliknij przycisk **Dalej**.

### Krok 2. Wyszukiwanie zmian

Kreator wyszukuje możliwe do cofnięcia zmiany, które wcześniej wprowadził. Po zakończeniu wyszukiwania kreator automatycznie przejdzie do następnego kroku.

### Krok 3. Wybieranie zmian, które mają zostać cofnięte

Po zakończeniu wyszukiwania kreator informuje użytkownika o wykrytych zmianach.

Aby kreator cofnął wcześniej podjęte działania, zaznacz pole znajdujące się z lewej strony nazwy wybranego działania.

Po wybraniu działań, które mają być cofnięte, kliknij przycisk **Dalej**.

### Krok 4. Wycofywanie zmian

Kreator cofa zmiany, które zostały wskazane w poprzednim kroku. Po zakończeniu cofania zmian kreator automatycznie przejdzie do kolejnego kroku.

### Krok 5. Kończenie działania kreatora

W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

## RAPORTY

Zdarzenia pojawiające się w trakcie działania modułów ochrony lub uruchomionych zadań programu Kaspersky Anti-Virus rejestrowane są w raportach.

### W TEJ SEKCJI:

Tworzenie raportu dla wybranego modułu ochrony.....	<a href="#">121</a>
Filtrowanie danych .....	<a href="#">121</a>
Wyszukiwanie zdarzeń.....	<a href="#">122</a>
Zapisywanie raportu do pliku.....	<a href="#">122</a>
Przechowywanie raportów .....	<a href="#">123</a>
Czyszczenie raportów aplikacji .....	<a href="#">123</a>
Zapisywanie w raporcie zdarzeń informacyjnych .....	<a href="#">123</a>
Konfigurowanie powiadamiania o dostępności raportu .....	<a href="#">124</a>

## TWORZENIE RAPORTU DLA WYBRANEGO MODUŁU OCHRONY

Możesz uzyskać raport szczegółowy o zdarzeniach, które zaistniały podczas działania każdego modułu ochrony Kaspersky Anti-Virus lub podczas wykonywania zadań.

Aby ułatwić pracę z raportami, możesz dostosować wyświetlanie danych na ekranie: pogrupować zdarzenia według różnych parametrów, wybrać okres raportu, posegregować zdarzenia według kolumny lub znaczenia, a także ukryć kolumny.

➤ *W celu utworzenia raportu dla modułu lub zadania:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Raporty** znajdujący się w górnej części okna.
3. W oknie **Raporty**, które zostanie otwarte, kliknij przycisk **Raport szczegółowy**.
4. W lewej części okna **Raport szczegółowy**, które zostanie otwarte, wybierz moduł lub zadanie, dla którego chcesz utworzyć raport. Po wybraniu elementu **Centrum ochrony** raport zostanie utworzony dla wszystkich składników ochrony.

## FILTROWANIE DANYCH

Zdarzenia z raportów programu Kaspersky Anti-Virus możesz filtrować według jednej lub kilku wartości z kolumn, możesz również określić złożone warunki filtrowania danych.

➤ *W celu filtrowania zdarzeń według wartości:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Raporty** znajdujący się w górnej części okna.
3. W oknie **Raporty**, które zostanie otwarte, kliknij przycisk **Raport szczegółowy**.
4. W prawej części otwartego okna **Raport szczegółowy** przesunij wskaźnik myszy na lewy górny róg kolumny i kliknij go w celu otwarcia menu filtra.
5. Z otwartego menu wybierz wartość, która ma zostać użyta do filtrowania danych.
6. Jeśli to konieczne, powtórz procedurę dla innej kolumny.

➤ *W celu określenia złożonego warunku filtrowania:*

1. Otwórz okno główne aplikacji.
2. W celu otwarcia okna raportów kliknij odnośnik **Raporty** znajdujący się w górnej części okna.
3. W oknie, które zostanie otwarte, na zakładce **Raport** kliknij przycisk **Raport szczegółowy**.
4. W prawej części otwartego okna **Raport szczegółowy** kliknij prawym przyciskiem myszy odpowiednią kolumnę raportu, aby wyświetlić jej menu kontekstowe, z którego wybierz opcję **Niestandardowy**.
5. W otwartym oknie **Filtr niestandardowy** ustaw warunki filtrowania:
  - a. W prawej części okna zdefiniuj ograniczenia wyszukiwania.
  - b. W lewej części okna, z listy rozwijalnej **Warunek** wybierz żądany warunek wyszukiwania (np. jest większy lub mniejszy, równy lub nierówny wartości zdefiniowanej jako ograniczenie wyszukiwania).

- c. Jeśli to konieczne, dodaj drugi warunek przy użyciu iloczynu logicznego (ORAZ) lub sumy logicznej (LUB). Jeśli chcesz, aby Twoje zapytanie spełniało oba warunki, wybierz **ORAZ**. Jeśli wymagany jest tylko jeden z dwóch warunków, wybierz **LUB**.

## WYSZUKIWANIE ZDARZEŃ

Żądane zdarzenie możesz odszukać w raporcie poprzez wpisanie słowa kluczowego w polu wyszukiwania lub specjalnym oknie.

➔ *W celu odnalezienia zdarzenia, korzystając z pola wyszukiwania:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Raporty** znajdujący się w górnej części okna.
3. W oknie **Raporty**, które zostanie otwarte, kliknij przycisk **Raport szczegółowy**.
4. W polu wyszukiwania znajdującym się w prawej części otwartego okna **Raport szczegółowy** wpisz słowo kluczowe.

➔ *W celu odnalezienia zdarzenia, korzystając z okna wyszukiwania:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Raporty** znajdujący się w górnej części okna.
3. W oknie **Raporty**, które zostanie otwarte, kliknij przycisk **Raport szczegółowy**.
4. W prawej części okna **Raport szczegółowy**, które zostanie otwarte, kliknij prawym przyciskiem myszy odpowiedni nagłówek kolumny. Z otwartego menu kontekstowego wybierz opcję **Szukaj**.
5. W oknie **Wyszukiwanie**, które zostanie otwarte, określ kryteria wyszukiwania:
  - a. W polu **Tekst** wprowadź słowo kluczowe, które ma być wyszukiwane.
  - b. Z listy rozwijalnej **Kolumna** wybierz nazwę kolumny, w której ma być wyszukiwane żądane słowo kluczowe.
  - c. Jeśli to konieczne, zaznacz pola obok dodatkowych parametrów wyszukiwania.
6. Uruchom wyszukiwanie przy użyciu jednej z następujących metod:
  - Jeżeli chcesz odszukać zdarzenie spełniające określone kryteria wyszukiwania i będące jednocześnie kolejnym po zaznaczonym na liście, kliknij przycisk **Znajdź następny**.
  - Jeśli chcesz odnaleźć wszystkie zdarzenia spełniające określone kryterium wyszukiwania, kliknij przycisk **Zaznacz wszystko**.

## ZAPISYWANIE RAPORTU DO PLIKU

Uzyskany raport może zostać zapisany do pliku tekstowego.

➔ *W celu zapisania raportu do pliku należy:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Raporty** znajdujący się w górnej części okna.
3. W oknie **Raporty**, które zostanie otwarte, kliknij przycisk **Raport szczegółowy**.

4. W oknie **Raport szczegółowy**, które zostanie otwarte, utwórz wymagany raport i kliknij odnośnik **Zapisz**, aby wybrać lokalizację dla pliku, który chcesz zapisać.
5. W otwartym oknie wybierz folder, do którego chcesz zapisać raport i wprowadź nazwę pliku.

## PRZECHOWYWANIE RAPORTÓW

Domyślnie maksymalny czas przechowywania raportów wynosi 30 dni. Po tym czasie raporty zostaną usunięte. Możesz wyłączyć ograniczenie czasu przechowywania raportu lub zmienić jego maksymalną wartość.

Ponadto możesz zdefiniować maksymalny rozmiar pliku raportu. Domyślnie wynosi on 1024 MB. Gdy raport osiągnie ten rozmiar, zawartość pliku zostanie nadpisana przez nowy wpis. Możesz anulować ograniczenie rozmiaru raportu lub wpisać inną wartość.

➤ *W celu zmiany maksymalnego czasu przechowywania raportów:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Przechowywanie raportów** zaznacz pole **Przechowuj raporty nie dłużej niż** i zdefiniuj okres przechowywania raportów.

➤ *W celu skonfigurowania maksymalnego rozmiaru pliku raportu:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Przechowywanie raportów** zaznacz pole **Maksymalny rozmiar plików** i zdefiniuj maksymalny rozmiar pliku raportu.

## CZYSZCZENIE RAPORTÓW APLIKACJI

Możesz wyczyścić raporty zawierające dane, których już nie potrzebujesz.

➤ *W celu wyczyszczenia raportów aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Czyszczenie raportów** kliknij przycisk **Wyczyść**.
4. W otwartym oknie **Czyszczenie raportów** zaznacz pola dla raportów, które chcesz wyczyścić.

## ZAPISYWANIE W RAPORCIE ZDARZEŃ INFORMACYJNYCH

Domyślnie aplikacja nie zapisuje w swoich raportach zdarzeń: informacyjnych, systemu plików i operacji na rejestrze. Można dodawać do raportu wpisy dotyczące tych zdarzeń.


➤ *W celu zapisania w raporcie zdarzeń informacyjnych:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Raporty i pliki danych**.
3. W prawej części okna zaznacz pole **Zapisuj zdarzenia informacyjne**.

## KONFIGUROWANIE POWIADAMIANIA O DOSTĘPNOŚCI RAPORTU

Możesz utworzyć terminarz, zgodnie z którym program Kaspersky Anti-Virus będzie przypominał o gotowości raportu.

➤ *W celu skonfigurowania powiadamiania o gotowości raportu:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Raporty** znajdujący się w górnej części okna.
3. W oknie **Raporty**, które zostanie otwarte, kliknij przycisk .
4. W otwartym oknie **Powiadomienia** zdefiniuj ustawienia terminarza.

## WYGLĄD APLIKACJI. ZARZĄDZANIE AKTYWNYMI ELEMENTAMI INTERFEJSU

Kaspersky Anti-Virus umożliwia dostosowanie ustawień wyświetlania tekstu na ekranie logowania w Microsoft Windows oraz aktywnych elementów interfejsu (takich, jak ikona aplikacji w obszarze powiadomień paska zadań, okna powiadomień oraz wiadomości wyskakujące).

### W TEJ SEKCJI:

Przenikanie okien powiadomień .....	<a href="#">124</a>
Animacja ikony aplikacji w obszarze powiadomień .....	<a href="#">124</a>
Tekst na ekranie logowania Microsoft Windows .....	<a href="#">125</a>

### PRZENIKANIE OKIEN POWIADOMIEŃ

➤ *W celu włączenia przenikania okien powiadomień:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Wygląd**.
3. W sekcji **Ikona zasobnika systemowego** zaznacz pole **Włącz przenikanie okien**.

### ANIMACJA IKONY APLIKACJI W OBSZARZE POWIADOMIEŃ

Animacja ikony jest wyświetlana w obszarze powiadomień paska zadań podczas aktualizacji lub skanowania.

Domyślnie animacja ikony aplikacji jest włączona.

➤ *W celu wyłączenia animacji ikony aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Wygląd**.

3. W sekcji **Ikona zasobnika systemowego** usuń zaznaczenie pola **Animuj ikonę programu podczas wykonywania zadań**.

## TEKST NA EKRANIE LOGOWANIA MICROSOFT WINDOWS

Domyślnie, gdy program Kaspersky Anti-Virus jest włączony i chroni Twój komputer, na ekranie logowania podczas ładowania systemu Microsoft Windows wyświetlany jest tekst "Protected by Kaspersky Lab".

Tekst "Protected by Kaspersky Lab" wyświetlany jest tylko w systemie Microsoft Windows XP.

➤ *W celu włączenia wyświetlania tego tekstu podczas ładowania systemu Microsoft Windows:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Wygląd**.
3. W sekcji **Ikona zasobnika systemowego** usuń zaznaczenie pola **Wyświetl napis "Protected by Kaspersky Lab" w oknie logowania Microsoft Windows**.

## POWIADOMIENIA

Domyślnie, jeśli podczas pracy Kaspersky Anti-Virus wystąpią jakieś zdarzenia, zostaniesz o nich powiadomiony. Jeśli konieczne będzie wybranie dalszych akcji, na ekranie pojawiają się okna powiadomień (sekcja "Okna powiadomień i wiadomości wyskakujące" na stronie [32](#)). Aplikacja powiadamia o zdarzeniach, które nie wymagają wybrania akcji, za pośrednictwem sygnału dźwiękowego, wiadomości e-mail, a także wiadomości wyskakujących w obszarze powiadomień paska zadań (sekcja "Okna powiadomień i wiadomości wyskakujące" na stronie [32](#)).

Kaspersky Anti-Virus zawiera moduł News Agent (strona [36](#)), przy pomocy którego firma Kaspersky Lab powiadamia Cię o nowościach. Jeżeli nie chcesz otrzymywać nowości, możesz wyłączyć ich dostarczanie.

### W TEJ SEKCJI:

Włączanie i wyłączanie powiadomień .....	<a href="#">125</a>
Konfigurowanie metody powiadamiania .....	<a href="#">126</a>
Wyłączanie otrzymywania nowości .....	<a href="#">127</a>

## WŁĄCZANIE I WYŁĄCZANIE POWIADOMIEŃ

Domyślnie Kaspersky Anti-Virus wykorzystuje różne metody powiadamiania o ważnych zdarzeniach związanych z działaniem aplikacji (sekcja "Konfigurowanie metody powiadamiania" na stronie [126](#)). Możesz wyłączyć wyświetlanie powiadomień.

Bez względu na to, czy dostarczanie powiadomień jest włączone czy wyłączone, informacje o zachodzących w trakcie działania Kaspersky Anti-Virus zdarzeniach są zapisywane w raporcie z działania aplikacji (strona [120](#)).

Wyłączenie dostarczania powiadomień nie wpływa na wyświetlanie okien powiadomień. Aby zminimalizować liczbę wyświetlanych na ekranie okien powiadomień, skorzystaj z automatycznego trybu ochrony (sekcja "Wybieranie trybu ochrony" na stronie [65](#)).

➤ *W celu wyłączenia otrzymywania powiadomień:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Powiadomienia**.

3. W prawej części okna usuń zaznaczenie z pola **Włącz powiadomienie o zdarzeniach**.

## KONFIGUROWANIE METODY POWIADAMIANIA

Aplikacja powiadamia Cię o zdarzeniach na następujące sposoby:

- poprzez komunikaty wyskakujące w obszarze powiadomień paska zadań;
- poprzez powiadomienia dźwiękowe;
- przy użyciu wiadomości e-mail.

Możesz skonfigurować odrębny zestaw metod dostarczania powiadomień dla każdego typu zdarzenia.

Domyślnie powiadomieniom krytycznym i powiadomieniom o błędach w działaniu aplikacji towarzyszy sygnał dźwiękowy. Jako źródło efektów dźwiękowych wykorzystywany jest schemat dźwięków Microsoft Windows. Możesz zmodyfikować bieżący schemat lub całkowicie wyłączyć dźwięk.

Aby zezwolić aplikacji Kaspersky Anti-Virus na powiadomianie o zdarzeniach poprzez wiadomości pocztowe, dostosuj ustawienia dostarczania powiadomień za pośrednictwem poczty elektronicznej.

➤ *W celu wybrania metody dostarczania powiadomień dla różnych typów zdarzeń:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Powiadomienia**.
3. W prawej części okna zaznacz pole **Włącz powiadomianie o zdarzeniach** i kliknij przycisk **Ustawienia** umieszczony pod polem.
4. W oknie **Powiadomienia**, które zostanie otwarte, zaznacz pola w zależności od sposobu, w który chcesz być powiadamiany o różnych zdarzeniach: poprzez wiadomości e-mail, wiadomość wyskakującą lub przy pomocy sygnału dźwiękowego.

➤ *W celu zmiany ustawień wysyłania powiadomień za pośrednictwem wiadomości e-mail:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Powiadomienia**.
3. W prawej części okna zaznacz pole **Włącz powiadomianie przy użyciu e-mail** i kliknij przycisk **Ustawienia**.
4. W oknie **Ustawienia powiadomień e-mail**, które zostanie otwarte, określ ustawienia dostarczania powiadomień poprzez e-mail.

➤ *W celu skonfigurowania schematu dźwięków wykorzystywanego podczas wyświetlania powiadomień:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Powiadomienia**.
3. W prawej części okna usuń zaznaczenie z pola **Włącz powiadomienia dźwiękowe**.

Jeżeli dla powiadomień o zdarzeniach Kaspersky Anti-Virus chcesz użyć schematu dźwięków Microsoft Windows, zaznacz pole **Użyj domyślnego schematu dźwięków Windows**. Jeżeli pole nie jest zaznaczone, użyty będzie schemat dźwięku z poprzedniej wersji aplikacji Kaspersky Anti-Virus.

## WYŁĄCZANIE OTRZYMYWANIA NOWOŚCI

➤ *W celu wyłączenia otrzymywania nowości z poziomu okna ustawień aplikacji:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Wygląd**.
3. W prawej części okna usuń zaznaczenie z pola **Powiadamiaj o nowościach**.

## KASPERSKY SECURITY NETWORK

Aby zwiększyć efektywność ochrony komputera, Kaspersky Anti-Virus używa danych zebranych od użytkowników z całego świata. Usługa Kaspersky Security Network została zaprojektowana do gromadzenia tych danych.

Kaspersky Security Network (KSN) jest usługą sieciową oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky Lab zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Anti-Virus po wykryciu nowego zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów.

Twoja zgoda na uczestnictwo w Kaspersky Security Network ułatwi firmie Kaspersky Lab zbieranie w czasie rzeczywistym informacji o typach nowych zagrożeń, rozwinięcie metod ich neutralizacji, a także zmniejszenie liczby fałszywych alarmów.

Ponadto uczestnictwo w Kaspersky Security Network oferuje dostęp do informacji o reputacji różnych aplikacji i stron internetowych.

Jeżeli uczestniczysz w Kaspersky Security Network, zbierane są pewne statystyki programu Kaspersky Anti-Virus, które następnie są automatycznie wysyłane do Kaspersky Lab.

Żadne dane użytkowników nie są gromadzone, przetwarzane, ani przechowywane przez Kaspersky Lab.

Uczestnictwo w Kaspersky Security Network nie jest obowiązkowe. O uczestnictwie w Kaspersky Security Network można zdecydować podczas instalowania programu Kaspersky Anti-Virus lub w późniejszym terminie.

### W TEJ SEKCJI:

Włączanie i wyłączanie uczestnictwa w Kaspersky Security Network.....	<a href="#">127</a>
Sprawdzanie połączenia z Kaspersky Security Network.....	<a href="#">128</a>

## WŁĄCZANIE I WYŁĄCZANIE UCZESTNICTWA W KASPERSKY SECURITY NETWORK

➤ *W celu uczestniczenia w Kaspersky Security Network:*

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Gromadzenie danych**.
3. W prawej części okna zaznacz pole **Zgadzam się na uczestnictwo w Kaspersky Security Network**.

## SPRAWDZANIE POŁĄCZENIA Z KASPERSKY SECURITY NETWORK

Nawiązanie połączenia z Kaspersky Security Network może być niemożliwe, gdy:

- Twój komputer nie jest połączony z Internetem;
- nie zgodziłeś się na uczestnictwo w Kaspersky Security Network;
- Twoja licencja na Kaspersky Anti-Virus jest ograniczona.

➡ *W celu sprawdzenia połączenia z Kaspersky Security Network:*

1. Otwórz okno główne aplikacji.
2. W górnej części okna kliknij przycisk **Ochrona w chmurze**.
3. W lewej części okna, które zostanie otwarte wyświetlany jest stan połączenia z Kaspersky Security Network.

# TESTOWANIE DZIAŁANIA APLIKACJI

Dostępne są tu informacje dotyczące sposobu sprawdzania, czy aplikacja wykrywa wirusy i ich modyfikacje i wykonuje na nich odpowiednie akcje.

## W TEJ SEKCJI:

Informacje o pliku testowym EICAR .....	<a href="#">129</a>
Testowanie działania aplikacji przy pomocy pliku testowego EICAR .....	<a href="#">129</a>
Informacje o typach pliku testowego EICAR .....	<a href="#">131</a>

## INFORMACJE O PLIKU TESTOWYM EICAR

Możesz upewnić się, że aplikacja wykrywa wirusy i leczy zainfekowane pliki, korzystając z *pliku testowego EICAR*. Plik testowy EICAR został opracowany przez European Institute for Computer Antivirus Research (EICAR) w celu testowania funkcjonalności aplikacji antywirusowych.

Testowy plik EICAR nie jest wirusem. Nie zawiera on szkodliwego kodu, który mógłby uszkodzić Twój komputer. Jednak większość aplikacji antywirusowych wykrywa plik testowy EICAR jako wirusa.

Plik testowy EICAR nie służy do testowania funkcjonalności analizy heurystycznej ani wykrywania szkodliwego oprogramowania na poziomie systemu (rootkity).

**Do testowania funkcjonalności aplikacji antywirusowych nie używaj prawdziwych wirusów! Może to uszkodzić Twój komputer.**

**Nie zapomnij włączyć ochrony antywirusowej ruchu internetowego i plików po zakończeniu testowania plikiem EICAR.**

## TESTOWANIE DZIAŁANIA APLIKACJI PRZY POMOCY PLIKU TESTOWEGO EICAR

Plik testowy EICAR może zostać użyty do przetestowania ochrony ruchu internetowego, ochrony antywirusowej plików, a także skanowania komputera.

**Nie zapomnij włączyć ochrony antywirusowej ruchu internetowego i plików po zakończeniu testowania plikiem EICAR.**

➤ *W celu przetestowania ochrony ruchu internetowego przy użyciu pliku EICAR:*

1. Plik testowy możesz pobrać z oficjalnej strony EICAR, dostępnej pod adresem [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).
2. Spróbuj zapisać plik testowy EICAR w dowolnym folderze na swoim komputerze.

Kaspersky Anti-Virus poinformuje Cię, że w zażądanym adresie internetowym zostało wykryte zagrożenie i zablokuje próbę zapisu obiektu na komputerze.

3. W razie konieczności, możesz użyć różnych rodzajów pliku testowego EICAR (sekcja "Informacje o typach pliku testowego EICAR" na stronie [131](#)).

➤ *W celu sprawdzenia ochrony antywirusowej plików przy użyciu pliku testowego EICAR lub jego modyfikacji:*

1. Wstrzymaj ochronę antywirusową ruchu internetowego oraz ochronę plików komputera.

Podczas wstrzymanej ochrony nie jest zalecane łączenie komputera z sieciami lokalnymi, a także używanie nośników wymiennych w celu uniknięcia przedostania się szkodliwego oprogramowania do Twojego komputera.

2. Plik testowy możesz pobrać z oficjalnej strony EICAR, dostępnej pod adresem [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

3. Zapisz plik testowy EICAR w dowolnym folderze na swoim komputerze.

4. Dodaj jeden z przedrostków na początku pliku testowego EICAR (sekcja "Informacje o typach pliku testowego EICAR" na stronie [131](#)).

Możesz wykorzystać dowolny edytor tekstu lub htmla, na przykład program Notatnik. Aby otworzyć Notatnik, wybierz **Start** → **Wszystkie programy** → **Akcesoria** → **Notatnik**.

5. Zapisz plik wynikowy pod nazwą odzwierciedlającą modyfikację pliku EICAR: na przykład, dodaj przedrostek DELE- i zapisz plik jako eicar\_dele.com.

6. Wznów ochronę antywirusową ruchu internetowego oraz ochronę plików komputera.

7. Spróbuj uruchomić plik, który zapisałeś.

Kaspersky Anti-Virus poinformuje o wykryciu zagrożenia na dysku twardym komputera i wykona akcję określoną w ustawieniach ochrony antywirusowej plików.

➤ *W celu sprawdzenia skanowania antywirusowego przy użyciu pliku testowego EICAR lub jego modyfikacji:*

1. Wstrzymaj ochronę antywirusową ruchu internetowego oraz ochronę plików komputera.

Podczas wstrzymanej ochrony nie jest zalecane łączenie komputera z sieciami lokalnymi, a także używanie nośników wymiennych w celu uniknięcia przedostania się szkodliwego oprogramowania do Twojego komputera.

2. Plik testowy możesz pobrać z oficjalnej strony EICAR, dostępnej pod adresem [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

3. Dodaj jeden z przedrostków na początku pliku testowego EICAR (sekcja "Informacje o typach pliku testowego EICAR" na stronie [131](#)).

Możesz wykorzystać dowolny edytor tekstu lub htmla, na przykład program Notatnik. Aby otworzyć Notatnik, wybierz **Start** → **Wszystkie programy** → **Akcesoria** → **Notatnik**.

4. Zapisz plik wynikowy pod nazwą odzwierciedlającą modyfikację pliku testowego EICAR: na przykład, dodaj przedrostek DELE- i zapisz plik jako eicar\_dele.com.

5. Uruchom skanowanie pliku, który zapisałeś.

Kaspersky Anti-Virus poinformuje o wykryciu zagrożenia na dysku twardym komputera i wykona akcję określoną w ustawieniach skanowania antywirusowego.

6. Wznów ochronę antywirusową ruchu internetowego oraz ochronę plików komputera.

## INFORMACJE O TYPACH PLIKU TESTOWEGO EICAR

Możesz przetestować funkcje aplikacji przy użyciu różnych modyfikacji pliku testowego EICAR. Aplikacja wykrywa plik EICAR (lub jego modyfikację) i w zależności od wyników skanowania przypisuje mu określony stan. Aplikacja podejmuje określone działania na pliku "wirusa" testowego EICAR, jeżeli zostały wybrane w ustawieniach modułu, który go wykrył.

Pierwsza kolumna tabeli (patrz poniższa tabela) zawiera prefiksy, których można użyć do tworzenia modyfikacji pliku "wirusa" testowego EICAR. Druga kolumna zawiera wszystkie możliwe stany przypisane do pliku na podstawie wyników skanowania wykonanego przez aplikację. Trzecia kolumna zawiera informacje na temat przetwarzania przez aplikację plików z określonym stanem.

Tabela 2. Modyfikacje pliku testowego EICAR

Przedrostek	Stan pliku	Informacje dotyczące przetwarzania pliku
Brak przedrostka, standardowy "wirus" testowy.	<b>Zainfekowany.</b> Plik zawiera kod znanego wirusa. Plik nie może zostać wyleczony.	Aplikacja rozpoznaje ten plik jako zawierający wirusa, którego nie można wyleczyć. Zastosowana zostanie akcja określona dla zainfekowanych plików. Domyślnie aplikacja wyświetla powiadomienie zawierające informację o braku możliwości wyleczenia obiektu.
CURE-	<b>Zainfekowany.</b> Plik zawiera kod znanego wirusa. Plik może zostać wyleczony.	Plik zawiera wirusa, który może zostać wyleczony lub usunięty. Aplikacja wyleczy plik; treść ciała wirusa zostanie zastąpiona słowem CURE. Aplikacja wyświetli powiadomienie o wykryciu wyleczonego pliku.
DELE-	<b>Zainfekowany.</b> Plik zawiera kod znanego wirusa. Plik nie może zostać wyleczony.	Aplikacja rozpoznaje ten plik jako wirusa, którego nie można wyleczyć i którego usuwa. Aplikacja wyświetli powiadomienie o usunięciu wyleczonego pliku.
WARN-	<b>Potencjalnie zainfekowany.</b> Plik zawiera kod nieznanego wirusa. Plik nie może zostać wyleczony.	Plik jest potencjalnie zainfekowany. Aplikacja zastosuje akcję określoną dla potencjalnie zainfekowanych plików. Domyślnie aplikacja wyświetli powiadomienie o wykryciu potencjalnie zainfekowanego pliku.
SUSP-	<b>Potencjalnie zainfekowany.</b> Plik zawiera zmodyfikowany kod znanego wirusa. Plik nie może zostać wyleczony.	Aplikacja wykryła, że część kodu znajdującego się w pliku jest taka sama jak fragment kodu znanego wirusa. W momencie wykrycia potencjalnie zainfekowanego pliku bazy danych aplikacji nie zawierały opisu pełnego kodu wirusa. Aplikacja zastosuje akcję określoną dla potencjalnie zainfekowanych plików. Domyślnie aplikacja wyświetli powiadomienie o wykryciu potencjalnie zainfekowanego pliku.
CORR-	<b>Uszkodzony.</b>	Aplikacja nie skanuje tego typu pliku, gdyż jego struktura jest uszkodzona (na przykład format pliku jest nieprawidłowy). Informacje o postępowaniu z plikiem możesz znaleźć w raporcie z działania aplikacji.
ERRO-	<b>Błąd skanowania.</b>	Wystąpił błąd podczas skanowania pliku. Aplikacja nie mogła uzyskać dostępu do pliku: naruszona została integralność pliku (na przykład, fragment wieloczęściowego archiwum jest uszkodzony) lub nie można nawiązać z nim połączenia (jeżeli skanowany plik znajduje się na dysku sieciowym). Informacje o postępowaniu z plikiem możesz znaleźć w raporcie z działania aplikacji.

# KONTAKT Z DZIAŁEM POMOCY TECHNICZNEJ

Sekcja zawiera informacje o sposobach uzyskania pomocy technicznej i warunkach, które należy spełnić, aby uzyskać tę pomoc.

## W TEJ SEKCJI:

Jak uzyskać pomoc techniczną .....	<a href="#">132</a>
Korzystanie z pliku śledzenia i skryptu AVZ .....	<a href="#">132</a>
Pomoc techniczna za pośrednictwem telefonu .....	<a href="#">135</a>
Uzyskiwanie pomocy technicznej poprzez Moje konto .....	<a href="#">135</a>

## JAK UZYSKAĆ POMOC TECHNICZNĄ

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji dla aplikacji lub w jednym z dodatkowych źródeł informacji o aplikacji (sekcja "Źródła informacji o aplikacji" na stronie [11](#)), zalecamy kontakt z działem pomocy technicznej firmy Kaspersky Lab. Eksperti z działu pomocy technicznej odpowiedzą na wszelkie pytania związane z instalacją i użytkowaniem aplikacji. Jeśli komputer jest zainfekowany, nasi specjaliści pomogą rozwiązać problemy wywołane przez szkodliwe oprogramowanie.

Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej (<http://support.kaspersky.com/pl/support/rules>).

Możesz skontaktować się z działem pomocy technicznej na jeden z następujących sposobów:

- Telefonicznie. Metoda ta pozwala na skonsultowanie się ze specjalistami z naszej pomocy technicznej w języku polskim.
- Przesyłając zapytanie z usługi Moje konto na stronie pomocy technicznej. Metoda ta pozwala na kontakt z naszymi specjalistami za pośrednictwem formularza zgłoszeniowego.

Aby uzyskać pomoc techniczną, musisz być zarejestrowanym użytkownikiem komercyjnej wersji Kaspersky Anti-Virus. Pomoc techniczna nie jest dostępna dla użytkowników testowych wersji aplikacji.

## KORZYSTANIE Z PLIKU ŚLEDZENIA I SKRYPTU AVZ

Po powiadomieniu specjalistów z działu pomocy technicznej o wystąpieniu problemu, mogą oni poprosić o utworzenie raportu, zawierającego informacje o Twoim systemie operacyjnym, i wysłanie go do pomocy technicznej. Specjaliści pomocy technicznej mogą również poprosić o utworzenie specjalnego pliku śledzenia. Plik śledzenia pozwala na śledzenie procesu wykonywania poleceń aplikacji krok po kroku, w celu sprawdzenia, w którym momencie działania aplikacji wystąpił błąd.

Po przeanalizowaniu otrzymanych danych specjaliści utworzą skrypt AVZ, który pomoże wyeliminować problemy i prześlą Ci go. Uruchamianie skryptów AVZ pozwala na przeanalizowanie aktywnych procesów w poszukiwaniu szkodliwego kodu, skanowanie systemu w poszukiwaniu szkodliwego kodu, leczenie / usuwanie zainfekowanych plików i tworzenie raportów z wyników skanowania systemu.

## TWORZENIE RAPORTU O STANIE SYSTEMU

➤ *W celu utworzenia raportu o stanie systemu:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Pomoc techniczna** znajdujący się w dolnej części okna głównego. Zostanie otwarte okno **Pomoc techniczna**, w którym kliknij odsyłacz **Narzędzia pomocy technicznej**.
3. W otwartym oknie **Narzędzia pomocy technicznej** kliknij przycisk **Utwórz raport o stanie systemu**.

Zostanie on utworzony w formatach HTML oraz XML i zapisany w archiwum sysinfo.zip. Po zakończeniu procesu zbierania informacji możliwe jest przejrzanie raportu.

➤ *W celu przejrzania raportu:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Pomoc techniczna** znajdujący się w dolnej części okna głównego. Zostanie otwarte okno **Pomoc techniczna**, w którym kliknij odsyłacz **Narzędzia pomocy technicznej**.
3. W otwartym oknie **Narzędzia pomocy technicznej** kliknij odnośnik **Pokaż**.
4. Otwórz archiwum sysinfo.zip zawierające pliki raportu.

## TWORZENIE PLIKU ŚLEDZENIA

➤ *W celu utworzenia pliku śledzenia:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Pomoc techniczna** znajdujący się w dolnej części okna głównego. Zostanie otwarte okno **Pomoc techniczna**, w którym kliknij odsyłacz **Narzędzia pomocy technicznej**.
3. W oknie **Narzędzia pomocy technicznej** wybierz poziom śledzenia przy użyciu listy rozwijalnej znajdującej się w sekcji **Śledzenie**.  
  
Zalecane jest określenie poziomu śledzenia przez specjalistę pomocy technicznej. Jeżeli nie zostały przekazane żadne zalecenia, należy ustawić poziom śledzenia na **500**.
4. W celu uruchomienia procesu śledzenia należy kliknąć przycisk **Włącz**.
5. Odtwórz sytuację, która spowodowała wystąpienie problemu.
6. W celu zatrzymania procesu śledzenia kliknij przycisk **Wyłącz**.

Możesz przejść do wysyłania wyników śledzenia (sekcja "Wysyłanie plików danych" na stronie [133](#)) na serwer firmy Kaspersky Lab.

## WYSYŁANIE PLIKÓW DANYCH

Po utworzeniu plików śledzenia oraz raportu o stanie systemu należy przesłać je specjalistom z działu pomocy technicznej firmy Kaspersky Lab.

Aby przesłać pliki danych na serwer pomocy technicznej, musisz posiadać numer zgłoszenia. Jeżeli żądanie jest aktywne, numer ten znajduje się w usłudze Moje konto na stronie pomocy technicznej.

➤ *W celu przesłania plików danych na serwer działu pomocy technicznej:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Pomoc techniczna** znajdujący się w dolnej części okna głównego. Zostanie otwarte okno **Pomoc techniczna**, w którym kliknij odsyłacz **Narzędzia pomocy technicznej**.
3. W oknie **Narzędzia pomocy technicznej**, które zostanie otwarte, w sekcji **Akcje** kliknij przycisk **Prześlij na serwer informacje dla działu pomocy technicznej**.

Zostanie otwarte okno **Przesyłanie na serwer informacji dla pomocy technicznej**.

4. Zaznacz pola obok tych plików śledzenia, które chcesz przesłać na serwer działu pomocy technicznej, a następnie kliknij przycisk **Wyślij**.

Zostanie otwarte okno **Numer zgłoszenia**.

5. Wprowadź numer przypisany do Twojego zgłoszenia po skontaktowaniu się z działem pomocy technicznej za pośrednictwem usługi Moje konto, a następnie kliknij przycisk **OK**.

Wybrane pliki danych zostaną spakowane i przesłane na serwer działu pomocy technicznej.

Jeśli z jakiegoś powodu nie można skontaktować się z działem pomocy technicznej, pliki danych będą przechowywane na komputerze w celu ich późniejszego wysłania za pośrednictwem usługi Moje konto.

➤ *W celu zapisania plików danych na dysku:*

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Pomoc techniczna** znajdujący się w dolnej części okna głównego. Zostanie otwarte okno **Pomoc techniczna**, w którym kliknij odsyłacz **Narzędzia pomocy technicznej**.
3. W oknie **Narzędzia pomocy technicznej**, które zostanie otwarte, w sekcji **Akcje** kliknij przycisk **Prześlij na serwer informacje dla działu pomocy technicznej**.

Zostanie otwarte okno **Przesyłanie na serwer informacji dla pomocy technicznej**.

4. Zaznacz pola obok tych plików śledzenia, które chcesz przesłać na serwer działu pomocy technicznej, a następnie kliknij przycisk **Wyślij**.

Zostanie otwarte okno **Numer zgłoszenia**.

5. Kliknij przycisk **Anuluj** i w otwartym oknie potwierdź zapisanie plików na dysku, klikając przycisk **Tak**.

Zostanie otwarte okno zapisywania archiwów.

6. Wprowadź nazwę archiwum i potwierdź zapisanie.

Utworzone archiwum może być wysłane na serwer działu pomocy technicznej za pośrednictwem usługi Moje konto.

## WYKONYWANIE SKRYPTU AVZ

Nie zalecamy zmieniać treści skryptu otrzymanego od ekspertów firmy Kaspersky Lab. Jeżeli podczas wykonywania skryptu wystąpi problem, skontaktuj się z działem pomocy technicznej (sekcja "Jak uzyskać pomoc techniczną" na stronie [132](#)).

➤ W celu uruchomienia skryptu AVZ:

1. Otwórz okno główne aplikacji.
2. Kliknij odnośnik **Pomoc techniczna** znajdujący się w dolnej części okna głównego. Zostanie otwarte okno **Pomoc techniczna**, w którym kliknij odsyłacz **Narzędzia pomocy technicznej**.
3. W otwartym oknie **Narzędzia pomocy technicznej** kliknij odnośnik **Wykonaj skrypt AVZ**.

Po pomyślnym wykonaniu skryptu kreator zostanie zamknięty. Jeżeli podczas wykonywania skryptu wystąpi błąd, Kreator wyświetli odpowiedni komunikat.

## POMOC TECHNICZNA ZA POŚREDNICTWEM TELEFONU

W przypadku naglącego problemu możesz zadzwonić do specjalistów z pomocy technicznej (<http://www.kaspersky.pl/services.html?s=support>).

Przed skontaktowaniem się z pomocą techniczną należy zebrać informacje (<http://support.kaspersky.com/pl/support/details>) o komputerze i zainstalowanej na nim aplikacji antywirusowej. Umożliwi to specjalistom szybkie rozwiązanie problemu.

## UZYSKIWANIE POMOCY TECHNICZNEJ POPRZECZ MOJE KONTO

*Moje konto* to Twoja osobista sekcja (<https://my.kaspersky.com/pl>) na stronie działu pomocy technicznej.

Aby uzyskać dostęp do Mojego konta, musisz przejść procedurę rejestracji na stronie rejestracyjnej (<https://my.kaspersky.com/en/registration?LANG=pl>). Wprowadź swój adres e-mail oraz hasło do systemu *Moje konto*.

Przy użyciu Mojego konta możesz wykonać następujące czynności:

- skontaktować się z działem pomocy technicznej i laboratorium antywirusowym;
- skontaktować się z działem pomocy technicznej bez konieczności używania poczty;
- śledzić stan swojego zapytania w czasie rzeczywistym;
- przeglądać szczegółową historię Twoich zgłoszeń wysyłanych do działu pomocy technicznej;
- uzyskać kopię pliku klucza w wypadku jego zgubienia lub utraty.

### Pomoc techniczna za pośrednictwem poczty elektronicznej

Możesz wysłać zgłoszenie do działu pomocy technicznej w języku polskim.

W polach formularza internetowego zgłoszenia należy określić następujące dane:

- typ zapytania;
- nazwa aplikacji i numer wersji;
- opis zgłoszenia;
- identyfikator klienta i hasło;
- adres e-mail.

Eksperti z działu pomocy technicznej odpowiedzą na Twoje pytanie na Moje konto oraz wyślą odpowiedź na adres e-mail podany w zapytaniu.

### Zgłoszenie internetowe do Laboratorium antywirusowego

Niektóre pytania należy wysłać do laboratorium antywirusowego, a nie do pomocy technicznej.

Do laboratorium antywirusowego możesz wysłać zgłoszenia następujących typów:

- Nieznany szkodliwy program – podejrzewasz, że plik zawiera wirusa, ale Kaspersky Anti-Virus nie rozpoznał go jako zainfekowanego.

Specjaliści laboratorium antywirusowego przeanalizują przysłany szkodliwy kod. Jeśli wykryją oni nieznanego wirusa, dodadzą odpowiedni opis do bazy danych, która stanie się dostępna przy aktualizacji aplikacji antywirusowych.

- *Fałszywy alarm* – Kaspersky Anti-Virus błędnie klasyfikuje plik jako wirus;
- *Prośba o opis szkodliwego programu* – chcesz uzyskać opis wirusa wykrywanego przez Kaspersky Anti-Virus, podając nazwę wirusa.

Możesz również wysłać zgłoszenie do Laboratorium antywirusowego ze strony z formularzem zgłoszenia (<http://support.kaspersky.com/virlab/helpdesk.html?LANG=pl>), nie rejestrując się w usłudze Moje konto. Na tej stronie nie musisz określać kodu aktywacyjnego aplikacji.

# DODATEK

Sekcja ta zawiera dodatkowe informacje uzupełniające niniejszy dokument.

## W TEJ SEKCJI:

---

Pracowanie z aplikacją z poziomu wiersza poleceń..... [137](#)

Lista powiadomień programu Kaspersky Anti-Virus ..... [147](#)

## PRACOWANIE Z APLIKACJĄ Z POZIOMU WIERSZA POLECEŃ

Możesz pracować z aplikacją Kaspersky Anti-Virus przy użyciu wiersza poleceń. Możliwe jest:

- aktywowanie aplikacji;
- uruchamianie i zatrzymywanie działania aplikacji;
- uruchamianie i zatrzymywanie działania modułów aplikacji;
- uruchamianie i zatrzymywanie zadań;
- uzyskiwanie informacji o bieżącym stanie modułów oraz zadań, jak również statystyk dla nich;
- uruchamianie i zatrzymywanie zadań skanowania antywirusowego;
- skanowanie wybranych obiektów;
- aktualizowanie baz danych oraz modułów programu, jak również cofanie aktualizacji;
- eksportowanie i importowanie ustawień ochrony;
- otwieranie plików pomocy przy użyciu składni wiersza poleceń ogólnie lub dla wybranego polecenia.

Składnia wiersza poleceń:

```
avp.com <polecenie> [opcje]
```

Dostęp do programu można uzyskać z wiersza poleceń z foldera instalacyjnego programu lub poprzez określenie pełnej ścieżki dostępu do pliku avp.com.

Lista poleceń używanych do zarządzania programem Kaspersky Internet Security i jego modułami dostępna jest w tabeli poniżej.

<b>START</b>	Uruchamia moduł lub zadanie.
<b>STOP</b>	Zatrzymuje moduł lub zadanie. Polecenie może być wykonane tylko po wprowadzeniu hasła przydzielonego przez interfejs programu.
<b>STATUS</b>	Wyświetla na ekranie bieżący stan modułu lub zadania.
<b>STATISTICS</b>	Wyświetla na ekranie statystyki dla modułu lub zadania.
<b>HELP</b>	Wyświetla informacje dla listy poleceń oraz składni poleceń.
<b>SCAN</b>	Skanuje obiekty w poszukiwaniu wirusów.
<b>UPDATE</b>	Rozpoczyna aktualizację programu.
<b>ROLLBACK</b>	Cofa ostatnią aktualizację programu. Polecenie może być wykonane tylko po wprowadzeniu hasła przydzielonego przez interfejs programu.
<b>EXIT</b>	Zamyka aplikację. Polecenie może być wykonane tylko po wprowadzeniu hasła ustawionego z poziomu interfejsu programu.
<b>IMPORT</b>	Importuje ustawienia ochrony. Polecenie może być wykonane tylko po wprowadzeniu hasła przydzielonego przez interfejs programu.
<b>EXPORT</b>	Eksportuje ustawienia ochrony.

Każde polecenie posiada własny zestaw ustawień.

## W TEJ SEKCJI:

Aktywowanie aplikacji.....	<a href="#">139</a>
Uruchamianie aplikacji .....	<a href="#">139</a>
Zatrzymywanie działania aplikacji .....	<a href="#">139</a>
Zarządzanie składnikami i zadaniami programu .....	<a href="#">139</a>
Skanowanie antywirusowe .....	<a href="#">141</a>
Aktualizowanie aplikacji.....	<a href="#">143</a>
Cofanie ostatniej aktualizacji .....	<a href="#">144</a>
Eksportowanie ustawień ochrony .....	<a href="#">144</a>
Importowanie ustawień ochrony .....	<a href="#">145</a>
Tworzenie pliku śledzenia .....	<a href="#">145</a>
Przeglądanie pomocy.....	<a href="#">146</a>
Kody zwrotne wiersza poleceń.....	<a href="#">146</a>

## AKTYWOWANIE APLIKACJI

Program Kaspersky Anti-Virus może zostać aktywowany przy użyciu pliku klucza.

Składnia polecenia:

```
avp.com ADDKEY <nazwa_pliku>
```

Poniższa tabela opisuje ustawienia wykonywania polecenia.

<nazwa_pliku>	Plik klucza aktywacji z rozszerzeniem *.key.
---------------	--

### **Przykład:**

```
avp.com ADDKEY 1AA111A1.key
```

## URUCHAMIANIE APLIKACJI

Składnia polecenia:

```
avp.com
```

## ZATRZYMYWANIE DZIAŁANIA APLIKACJI

Składnia polecenia:

```
avp.com EXIT /password=<twoje_hasło>
```

Opis parametrów znajduje się w tabeli poniżej.

<twoje_hasło>	Hasło aplikacji wprowadzone w interfejsie.
---------------	--

Tego polecenia nie można wykonać bez podania hasła.

## ZARZĄDZANIE SKŁADNIKAMI I ZADANIAMI PROGRAMU

Składnia polecenia:

```
avp.com <polecenie> <profil|nazwa_zadania> [/R[A]:<plik_raportu>]
```

```
avp.com STOP <profil|nazwa_zadania> /password=<twoje_hasło> [/R[A]:<plik_raportu>]
```

Opisy poleceń i ustawienia znajdują się w tabeli poniżej.

<polecenie>	<p>Przy użyciu następujących poleceń można zarządzać zadaniami i składnikami programu Kaspersky Anti-Virus z poziomu wiersza poleceń:</p> <p>START – uruchom moduł lub zadanie ochrony w czasie rzeczywistym.</p> <p>STOP – zatrzymaj działanie modułu lub zadanie ochrony w czasie rzeczywistym.</p> <p>STATUS – wyświetl bieżący stan modułu lub zadania ochrony w czasie rzeczywistym.</p> <p>STATISTICS – wyświetl statystyki dotyczące działania modułu lub zadania ochrony w czasie rzeczywistym.</p> <p>Pamiętaj, że polecenie STOP wymaga podania hasła.</p>
<profil nazwa_zadania>	<p>Dla wartości &lt;profil&gt; możliwe jest określenie dowolnego składnika ochrony w czasie rzeczywistym, modułów składników, zadań skanowania na żądanie lub aktualizacji (standardowe wartości wykorzystywane w programie znajdują się w poniższej tabeli).</p> <p>Jako wartość dla &lt;nazwa_zadania&gt; możliwe jest określenie nazwy dowolnego zadania skanowania na żądanie lub aktualizacji.</p>
<twoje_haslo>	Hasło aplikacji wprowadzone w interfejsie.
/R[A]:<plik_raportu>	<p>/R:&lt;plik_raportu&gt; – rejestrowanie w raporcie tylko ważnych zdarzeń.</p> <p>/RA:&lt;plik_raportu&gt; – rejestrowanie w raporcie wszystkich zdarzeń.</p> <p>Możesz podać bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli ustawienie nie zostanie zdefiniowane, rezultaty skanowania oraz wszystkie zdarzenia będą wyświetlane na ekranie.</p>

W ustawieniu <profil> należy określić jedną z wartości znajdujących się w tabeli poniżej.

RTP	<p>Wszystkie składniki ochrony.</p> <p>Polecenie <b>avp.com START RTP</b> uruchamia działanie wszystkich składników ochrony, gdy ochrona jest całkowicie wyłączona.</p> <p>Jeżeli komponent został wyłączony z poziomu wiersza poleceń przy użyciu polecenia <b>STOP</b>, uruchomienie go za pomocą polecenia <b>avp.com START RTP</b> nie jest możliwe. Moduł ten można uruchomić za pomocą polecenia <b>avp.com START &lt;profil&gt;</b>, wpisując w polu &lt;profil&gt; wartość dla określonego składnika ochrony, na przykład <b>avp.com START FM</b>.</p>
pdm	Ochrona proaktywna.
FM	Ochrona plików.
EM	Ochrona poczty.
WM	<p>Ochrona WWW.</p> <p>Wartości dla komponentów modułu Ochrona WWW:</p> <p><b>httpscan (HTTP)</b> – skanowanie ruchu http;</p> <p><b>sc</b> – skanowanie skryptów.</p>
IM	Ochrona komunikatorów.
Updater	Aktualizacja.
Rollback	Cofanie ostatniej aktualizacji.
Scan_My_Computer	Skanowanie.
Scan_Objects	Skanowanie obiektów.

<b>Scan_Quarantine</b>	Skanowanie Kwarantanny.
<b>Scan_Startup (STARTUP)</b>	Skanowanie obiektów startowych.
<b>Scan_Vulnerabilities (SECURITY)</b>	Wykrywanie luk.

Moduły i zadania uruchomione z poziomu wiersza poleceń działają z ustawieniami skonfigurowanymi w interfejsie programu.

#### **Przykłady:**

➤ *W celu włączenia działania modułu Ochrona plików wprowadź następujące polecenie:*

```
avp.com START FM
```

➤ *W celu zatrzymania skanowania komputera wprowadź następujące polecenie:*

```
avp.com STOP Scan_My_Computer /password=<twoje_hasło>
```

## SKANOWANIE ANTYWIRUSOWE

Uruchamianie skanowania wybranego obszaru w poszukiwaniu wirusów i przetwarzanie szkodliwych obiektów z poziomu wiersza poleceń wygląda następująco:

```
avp.com SCAN [<obiekt skanowany>] [<akcja>] [<typy plików>] [<wykluczenia>] [<plik konfiguracyjny>] [<ustawienia raportu>] [<ustawienia zaawansowane>]
```

Do skanowania obiektów możesz również użyć zadań utworzonych w aplikacji, uruchamiając żądane zadanie z poziomu wiersza poleceń. Zadanie zostanie uruchomione z ustawieniami określonymi w interfejsie programu Kaspersky Anti-Virus.

Opis parametrów znajduje się w tabeli poniżej.

<b>&lt;obiekt skanowany&gt;</b> – ten parametr określa listę obiektów, które będą skanowane w poszukiwaniu szkodliwego kodu. Parametr może zawierać wiele wartości z dostarczonej listy, oddzielonych spacjami.	
<b>&lt;pliki&gt;</b>	<p>Lista ścieżek dostępu do plików i / lub folderów przeznaczonych do skanowania.</p> <p>Możesz określić bezwzględną lub względną ścieżkę dostępu do pliku. Obiekty na liście oddzielone są spacją.</p> <p>Komentarze:</p> <ul style="list-style-type: none"> <li>• jeśli nazwa obiektu zawiera spację, musi być umieszczona w cudzysłowach;</li> <li>• jeśli występuje odniesienie do określonego katalogu, wszystkie pliki w tym katalogu zostaną przeskanowane.</li> </ul>
<b>/MEMORY</b>	Obiekty pamięci RAM.
<b>/STARTUP</b>	Obiekty startowe.
<b>/MAIL</b>	Skrzynki pocztowe.
<b>/REMDRIVES</b>	Wszystkie dyski i nośniki wymienne.
<b>/FIXDRIVES</b>	Wszystkie dyski wewnętrzne.
<b>/NETDRIVES</b>	Wszystkie dyski sieciowe.
<b>/QUARANTINE</b>	Obiekty poddane kwarantannie.

<b>/ALL</b>	Pełne skanowanie komputera.
<b>/@:&lt;listaplików.lst&gt;</b>	<p>Ścieżka dostępu do pliku zawierającego listę obiektów i folderów przeznaczonych do skanowania. Możesz określić bezwzględną lub względną ścieżkę dostępu do pliku zawierającego listę. Ścieżka dostępu nie może być umieszczona w cudzysłowach, nawet jeśli zawiera spację.</p> <p>Plik zawierający listę obiektów powinien być w formacie tekstowym. Każdy obiekt przeznaczony do skanowania powinien znajdować się w oddzielnym wierszu.</p> <p>Zaleca się zdefiniowanie bezwzględnej ścieżki dostępu do obiektów przeznaczonych do skanowania. Przy określaniu ścieżki względnej należy określić ścieżkę względem pliku wykonywalnego aplikacji, a nie względem pliku z listą skanowanych obiektów.</p>
<p><b>&lt;akcja&gt;</b> – parametr ten określa, jakie działanie będzie wykonane na szkodliwych obiektach wykrytych podczas skanowania. Jeśli ten parametr nie został zdefiniowany, wówczas domyślnym działaniem stanie się to o wartości <b>/i8</b>.</p> <p>Jeżeli pracujesz w trybie automatycznym, po wykryciu niebezpiecznego obiektu Kaspersky Anti-Virus będzie automatycznie wykonywał akcję zalecaną przez specjalistów z Kaspersky Lab. Akcja odpowiadająca wartości parametru <b>&lt;akcja&gt;</b> będzie ignorowana.</p>	
<b>/i0</b>	Na obiekcie nie są podejmowane żadne akcje; informacje o obiekcie zapisywane są w raporcie.
<b>/i1</b>	Leczenie zainfekowanych obiektów lub ich pomijanie w przypadku braku możliwości wyleczenia.
<b>/i2</b>	Leczenie zainfekowanych obiektów lub ich pomijanie w przypadku braku możliwości wyleczenia; nie usuwanie zainfekowanych plików z obiektów złożonych; usunięcie zainfekowanych obiektów złożonych z wykonywalnymi nagłówkami (archiwa sfx).
<b>/i3</b>	Leczenie zainfekowanych obiektów lub ich pomijanie w przypadku braku możliwości wyleczenia; całkowite usunięcie wszystkich złożonych obiektów, jeżeli nie można usunąć plików osadzonych.
<b>/i4</b>	Usuń zainfekowane obiekty. Całkowicie usuń obiekty złożone, jeśli zainfekowane części nie mogą zostać usunięte.
<b>/i8</b>	Zapytaj użytkownika o działanie, jeśli zostanie wykryty zainfekowany obiekt.
<b>/i9</b>	Zapytaj użytkownika o działanie po zakończeniu skanowania.
<p><b>&lt;typy plików&gt;</b> – parametr ten definiuje typy plików, które będą poddane skanowaniu antywirusowemu. Domyślnie, jeśli ten parametr nie jest zdefiniowany, skanowaniu według zawartości poddawane są tylko pliki możliwe do zainfekowania.</p>	
<b>/fe</b>	Skanuj tylko pliki, które mogą zostać zainfekowane według rozszerzenia.
<b>/fi</b>	Skanuj tylko pliki, które mogą zostać zainfekowane według zawartości.
<b>/fa</b>	Skanuj wszystkie pliki.
<p><b>&lt;wykluczenia&gt;</b> – parametr ten definiuje obiekty, które zostaną wykluczone ze skanowania. Parametr może zawierać wiele wartości z dostarczonej listy, oddzielonych spacjami.</p>	
<b>-e:a</b>	Nie skanuj archiwów.
<b>-e:b</b>	Nie skanuj pocztowych baz danych.
<b>-e:m</b>	Nie skanuj wiadomości zawierających czysty tekst.
<b>-e:&lt;maska_pliku&gt;</b>	Nie skanuj obiektów, które zgadzają się z maską.

<b>&lt;e:&lt;sekundy&gt;</b>	Pomiń obiekty, które są skanowane dłużej niż czas określony parametrem <b>&lt;sekundy&gt;</b> .
<b>&lt;es:&lt;rozmiar&gt;</b>	Pomiń obiekty o rozmiarze (w MB) przekraczającym wartość określoną przez parametr <b>&lt;rozmiar&gt;</b> .  Ustawienie to dostępne jest tylko dla plików złożonych (takich jak archiwa).
<b>&lt;plik konfiguracyjny&gt;</b> – definiuje ścieżkę dostępu do pliku konfiguracyjnego, który zawiera ustawienia aplikacji dla zadania skanowania.  Plik konfiguracyjny jest plikiem w formacie tekstowym i zawiera zestaw parametrów wiersza poleceń dla skanowania antywirusowego.  Możesz określić bezwzględną lub względną ścieżkę dostępu do pliku. Jeśli ten parametr nie zostanie zdefiniowany, wówczas używane są wartości ustawione w interfejsie aplikacji.	
<b>/C:&lt;nazwa_pliku&gt;</b>	Użyj wartości ustawień określonych w pliku konfiguracyjnym <b>&lt;nazwa_pliku&gt;</b> .
<b>&lt;ustawienia raportu&gt;</b> – ten parametr określa format raportu wyników skanowania.  Możesz podać bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli ustawienie nie zostanie zdefiniowane, rezultaty skanowania oraz wszystkie zdarzenia będą wyświetlane na ekranie.	
<b>/R:&lt;plik_raportu&gt;</b>	Zapisuj w tym pliku tylko ważne zdarzenia.
<b>/RA:&lt;plik_raportu&gt;</b>	Zapisuj wszystkie zdarzenia w tym pliku.
<b>&lt;ustawienia zaawansowane&gt;</b> – ustawienia, które definiują użycie technologii skanowań antywirusowych.	
<b>/iChecker=&lt;on off&gt;</b>	Włącz / wyłącz używanie technologii iChecker.
<b>/iSwift=&lt;on off&gt;</b>	Włącz / wyłącz używanie technologii iSwift.

**Przykłady:**

- *Rozpoczęcie skanowania pamięci, programów autostartu, skrzynek pocztowych, folderów Moje dokumenty i Program Files oraz pliku test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\Moje dokumenty" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Skanowanie obiektów umieszczonych w pliku object2scan.txt, z wykorzystaniem pliku konfiguracyjnego scan\_setting.txt. Użycie pliku konfiguracyjnego scan\_settings.txt. Po zakończeniu skanowania nastąpi utworzenie pliku raportu z zapisem wszystkich zaistniałych zdarzeń:*

```
avp.com SCAN /MEMORY /@:object2scan.txt /C:scan_settings.txt /RA:scan.log
```

Przykładowy plik konfiguracyjny:

```
/MEMORY /@:object2scan.txt /C:scan_settings.txt /RA:scan.log
```

**AKTUALIZOWANIE APLIKACJI**

Składnia polecenia aktualizacji modułów oraz baz danych Kaspersky Anti-Virus z poziomu wiersza poleceń jest następująca:

```
avp.com UPDATE [<źródło_uaktualnień>] [/R[A]:<plik_raportu>] [/C:<nazwa_pliku>]
```

Opis parametrów znajduje się w tabeli poniżej.

<b>&lt;źródło_uaktualnień&gt;</b>	Serwer HTTP, FTP lub folder sieciowy, z którego pobierane są uaktualnienia. Wartością tego parametru może być pełna ścieżka dostępu do źródła uaktualnień lub adres internetowy. Jeżeli ścieżka nie zostanie podana, program pobierze źródło uaktualnień z ustawień aplikacji.
<b>/R[A]:&lt;plik_raportu&gt;</b>	<b>/R:&lt;plik_raportu&gt;</b> – rejestrowanie w raporcie tylko ważnych zdarzeń.

	<p><b>/RA:&lt;plik_raportu&gt;</b> – rejestrowanie w raporcie wszystkich zdarzeń.</p> <p>Możesz podać bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli ustawienie nie zostanie zdefiniowane, rezultaty skanowania oraz wszystkie zdarzenia będą wyświetlane na ekranie.</p>
<b>/C:&lt;nazwa_pliku&gt;</b>	<p>Ścieżka dostępu do pliku konfiguracyjnego, który zawiera ustawienia aktualizacji Kaspersky Anti-Virus.</p> <p>Plik konfiguracyjny to plik tekstowy zawierający listę parametrów wiersza poleceń dla aktualizacji aplikacji.</p> <p>Możesz określić bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli parametr ten nie został zdefiniowany, użyte zostaną wartości ustawień znajdujące się w interfejsie aplikacji.</p>

**Przykłady:**

- Aktualizacja baz danych aplikacji i zapisywanie wszystkich zdarzeń w raporcie:

```
avp.com UPDATE /RA:avbases_upd.txt
```

- Aktualizacja modułów programu Kaspersky Anti-Virus przy użyciu parametrów pliku konfiguracyjnego updateapp.ini:

```
avp.com UPDATE /C:updateapp.ini
```

Przykładowy plik konfiguracyjny:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

**COFANIE OSTATNIEJ AKTUALIZACJI**

Składnia polecenia:

```
avp.com ROLLBACK [/R[A]:<plik_raportu>] [/password=<twoje_hasło>]
```

Opis parametrów znajduje się w tabeli poniżej.

<b>/R[A]:&lt;plik_raportu&gt;</b>	<p><b>/R:&lt;plik_raportu&gt;</b> – rejestrowanie w raporcie tylko ważnych zdarzeń.</p> <p><b>/RA:&lt;plik_raportu&gt;</b> – rejestrowanie w raporcie wszystkich zdarzeń.</p> <p>Możesz podać bezwzględną lub względną ścieżkę dostępu do pliku. Jeżeli ustawienie nie zostanie zdefiniowane, rezultaty skanowania oraz wszystkie zdarzenia będą wyświetlane na ekranie.</p>
<b>&lt;twoje_hasło&gt;</b>	Hasło aplikacji wprowadzone w interfejsie.

Tego polecenia nie można wykonać bez podania hasła.

**Przykład:**

```
avp.com ROLLBACK /RA:rollback.txt /password=<twoje_hasło>
```

**EKSPORTOWANIE USTAWIEŃ OCHRONY**

Składnia polecenia:

```
avp.com EXPORT <profil> <nazwa_pliku>
```

Poniższa tabela opisuje ustawienia wykonywania polecenia.

<profil>	Moduł lub zadanie, którego ustawienia są eksportowane. Dla ustawienia <profil> możesz użyć wartości opisanych w sekcji pomocy zatytułowanej "Zarządzanie składnikami i zadaniami programu".
<nazwa_pliku>	Ścieżka dostępu do pliku, do którego wyeksportowane zostaną ustawienia programu Kaspersky Anti-Virus. Możesz podać ścieżkę względną lub bezwzględną.  Plik konfiguracyjny zapisywany jest w formacie binarnym (.dat), jeśli żaden inny format nie został sprecyzowany lub nie wybrano formatu w ogóle; może być użyty później do eksportowania ustawień aplikacji na inne komputery. Plik konfiguracyjny może zostać zapisany również jako plik tekstowy. W tym celu należy w nazwie pliku dodać rozszerzenie .txt. Należy pamiętać, że nie można importować ustawień ochrony z pliku tekstowego. Plik ten może zostać użyty jedynie do określenia głównych ustawień działania programu Kaspersky Anti-Virus.

**Przykład:**

```
avp.com EXPORT RTP c:\settings.dat
```

**IMPORTOWANIE USTAWIEŃ OCHRONY**

Składnia polecenia:

```
avp.com IMPORT <nazwa_pliku>[/password=<twoje_hasło>]
```

Poniższa tabela opisuje ustawienia wykonywania polecenia.

<nazwa_pliku>	Ścieżka dostępu do pliku, z którego importowane będą ustawienia programu Kaspersky Anti-Virus. Możesz podać ścieżkę względną lub bezwzględną.
<twoje_hasło>	Hasło do programu Kaspersky Anti-Virus wprowadzone w interfejsie aplikacji. Parametry bezpieczeństwa mogą zostać zaimportowane tylko z pliku binarnego.

Tego polecenia nie można wykonać bez podania hasła.

**Przykład:**

```
avp.com IMPORT c:\settings.dat /hasło=<twoje_hasło>
```

**TWORZENIE PLIKU ŚLEDZENIA**

Utworzenie pliku śledzenia może być konieczne w przypadku problemów z działaniem programu Kaspersky Anti-Virus. Pomoże to specjalistom z pomocy technicznej bardziej dokładnie zdiagnozować problem.

Pliki śledzenia zalecamy tworzyć tylko w celu rozwiązania określonego problemu. Ciągłe tworzenie plików śledzenia może doprowadzić do spowolnienia pracy komputera i zapełnienia dysku twardego.

Składnia polecenia:

```
avp.com TRACE [file] [on|off] [<poziom_śledzenia>]
```

Opis parametrów znajduje się w tabeli poniżej.

[on off]	Włączenie / wyłączenie tworzenia plików śledzenia.
[file]	Zapisanie śledzenia do pliku.
<poziom_śledzenia>	Ustawienie to może przyjmować wartość całkowitą od 0 (poziom minimalny, tylko krytyczne komunikaty) do 700 (poziom maksymalny, wszystkie komunikaty).  Specjaliści z działu pomocy technicznej poinformują Cię, jaki poziom śledzenia należy ustawić. Jeżeli poziom nie zostanie zdefiniowany, zalecamy ustawienie wartości na 500.

**Przykłady:**

- ➔ *W celu wyłączenia tworzenia plików śledzenia:*

```
avp.com TRACE file off
```

- ➔ *W celu utworzenia pliku śledzenia wysyłanego do działu pomocy technicznej z maksymalnym poziomem śledzenia o wartości 500:*

```
avp.com TRACE file on 500
```

## PRZEGLĄDANIE POMOCY

Polecenie to służy do przeglądania pomocy na temat składni wiersza poleceń:

```
avp.com [ /? | HELP ]
```

Jeśli chcesz przejrzeć pomoc na temat składni danego polecenia, możesz użyć jednego z następujących poleceń:

```
avp.com <polecenie> /?
```

```
avp.com HELP <polecenie>
```

## KODY ZWROTNE WIERSZA POLECEŃ

Sekcja ta opisuje kody zwrotne wiersza poleceń (zobacz tabelę poniżej). Kody ogólne mogą być zwracane przez dowolne polecenie z wiersza poleceń. Kody zwracane przez program obejmują kody ogólne oraz kody specyficzne dla konkretnego typu zadania.

<b>OGÓLNE KODY ZWROTNE</b>	
<b>0</b>	Działanie zakończone pomyślnie.
<b>1</b>	Błędna wartość parametru.
<b>2</b>	Nieznany błąd.
<b>3</b>	Błąd podczas zakończenia wykonywania zadania.
<b>4</b>	Zadanie anulowane.
<b>KODY ZWRACANE PRZEZ ZADANIE SKANOWANIA ANTYWIRUSOWEGO</b>	
<b>101</b>	Wszystkie niebezpieczne obiekty zostały przetworzone.
<b>102</b>	Wykryto niebezpieczne obiekty.

# LISTA POWIADOMIEŃ PROGRAMU KASPERSKY ANTI-VIRUS

Sekcja ta zawiera informacje o powiadomieniach, które są wyświetlane na ekranie przez Kaspersky Anti-Virus.

## W TEJ SEKCJI:

---

Powiadomienia w dowolnym trybie ochrony.....	<a href="#">147</a>
Powiadomienia w interaktywnym trybie ochrony .....	<a href="#">152</a>

## POWIADOMIENIA W DOWOLNYM TRYBIE OCHRONY

Sekcja ta zawiera informacje o powiadomieniach, które są wyświetlane na ekranie zarówno w automatycznym, jak i w interaktywnym trybie ochrony (sekcja "Wybieranie trybu ochrony" na stronie [65](#)).

## W TEJ SEKCJI:

---


Wymagane jest specjalne przetwarzanie .....	<a href="#">147</a>
Podłączono dysk wymienny .....	<a href="#">148</a>
Wykryto niezauwany certyfikat.....	<a href="#">148</a>
Wykryto aplikację, która może zostać użyta przez hakerów do uszkodzenia komputera lub danych.....	<a href="#">149</a>
Plik poddany kwarantannie nie jest zainfekowany .....	<a href="#">149</a>
Dostępna jest nowa wersja produktu .....	<a href="#">150</a>
Dostępne jest nowe uaktualnienie techniczne.....	<a href="#">150</a>
Pobrano uaktualnienie techniczne .....	<a href="#">150</a>
Pobrane uaktualnienie techniczne nie jest zainstalowane .....	<a href="#">151</a>
Licencja wygasta .....	<a href="#">151</a>
Przed wykonaniem skanowania zalecane jest zaktualizowanie baz danych.....	<a href="#">151</a>

## WYMAGANE JEST SPECJALNE PRZETWARZANIE

W przypadku wykrycia zagrożenia, które jest obecnie aktywne w systemie (na przykład szkodliwy proces wykryty w pamięci RAM lub w obiektach startowych), wyświetlone zostaje powiadomienie z zapytaniem dotyczącym potwierdzenia użycia technologii zaawansowanego leczenia.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Typ zagrożenia i nazwę szkodliwego obiektu zgodną z Encyklopedią Wirusów Kaspersky Lab.

Obok nazwy szkodliwego obiektu wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o obiekcie. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje o zagrożeniu, jakie stwarza obiekt.

- Nazwę pliku szkodliwego obiektu oraz jego ścieżkę dostępu.

Możesz wybrać jedno z następujących działań:

- **Tak, wylecz po ponownym uruchomieniu** – wykonuje specjalną procedurę leczenia (zalecane).

Podczas trwania leczenia wszystkie aplikacje poza zaufanymi są zablokowane. Po zakończeniu procedury leczenia system operacyjny zostanie ponownie uruchomiony, dlatego też przed rozpoczęciem leczenia zalecamy zapisanie wprowadzonych zmian i zamknięcie wszystkich aplikacji. Po ponownym uruchomieniu komputera zalecane jest wykonanie pełnego skanowania antywirusowego.

- **Nie uruchamiaj** – wykryty obiekt lub proces zostanie przetworzony zgodnie z wybraną akcją.

Aby zastosować wybraną akcję automatycznie przy każdym następnym wystąpieniu tej sytuacji, zaznacz pole **Zastosuj do wszystkich obiektów**.

## PODŁĄCZONO DYSK WYMIENNY

Po podłączeniu dysku wymiennego do komputera na ekranie pojawi się powiadomienie.

Możesz wybrać jedno z następujących działań:

- **Szybkie skanowanie** – skanuje tylko te pliki na dysku wymiennym, które mogą stanowić potencjalne zagrożenie.
- **Pełne skanowanie** – skanuje wszystkie pliki znajdujące się na dysku wymiennym.
- **Nie skanuj** – nie skanuje dysku wymiennego.

Aby zastosować wybraną akcję do wszystkich dysków wymiennych, które mogą być podłączone w przyszłości, zaznacz pole **Zawsze wykonuj taką akcję**.

## WYKRYTO NIEZAUFANY CERTYFIKAT

Kaspersky Anti-Virus sprawdza połączenie nawiązywane za pośrednictwem protokołu SSL przy użyciu zainstalowanego certyfikatu. Jeżeli podczas próby połączenia z serwerem wykryto nieprawidłowy certyfikat (na przykład, jeżeli został podmieniony przez hakera), na ekranie wyświetlony zostanie odpowiedni komunikat.

Powiadomienie zawiera następujące informacje:

- opis zagrożenia;
- odnośnik do wyświetlenia certyfikatu;
- możliwy powód błędu;
- adres zasobu sieciowego.

Możesz wybrać jedno z następujących działań:

- **Tak, zaakceptuj niezaufany certyfikat** – kontynuuje łączenie z zasobem sieciowym.
- **Odrzuć certyfikat** – przerywa połączenie ze stroną.

## WYKRYTO APLIKACJĘ, KTÓRA MOŻE ZOSTAĆ UŻYTA PRZEZ HAKERÓW DO USZKODZENIA KOMPUTERA LUB DANYCH

Po wykryciu przez Monitor aktywności aplikacji, która może zostać użyta przez hakerów do uszkodzenia komputera lub danych, na ekranie wyświetlane jest powiadomienie.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Typ i nazwa aplikacji, która może zostać wykorzystana przez hakera do uszkodzenia komputera lub danych.  
Obok nazwy aplikacji wyświetlona jest ikona ⓘ. Kliknij ją, aby wyświetlić okno z informacjami o aplikacji.
- Identyfikator procesu i nazwę pliku aplikacji wraz z jego ścieżką dostępu.
- Odnośnik do okna z raportem uruchamiania aplikacji.

Możesz wybrać jedno z następujących działań:

- **Zezwól** – zezwala na uruchomienie aplikacji.
- **Kwarantanna** – zamyka aplikację, przenosi plik programu do Kwarantanny, gdzie nie stwarza on żadnego zagrożenia dla bezpieczeństwa komputera.

Podczas późniejszych skanowań Kwarantanny stan obiektu może się zmienić. Na przykład, obiekt może się okazać zainfekowany z możliwością przetworzenia przy użyciu zaktualizowanych baz danych. Stan obiektu może się także zmienić na *niezainfekowany* i jego przywrócenie będzie możliwe.

Podczas kolejnego skanowania stan pliku przeniesionego do Kwarantanny może się zmienić na *niezainfekowany* pod warunkiem, że skanowanie odbyło się przynajmniej trzy dni po przeniesieniu go do Kwarantanny.

- **Zakończ aplikację** – przerywa wykonywanie aplikacji.
- **Dodaj do wyjątków** – zezwala aplikacji na wykonywanie takich akcji w przyszłości.

## PLIK PODDANY KWARRANTANNIE NIE JEST ZAINFEKOWANY

Domyślnie, Kaspersky Anti-Virus skanuje pliki w kwarantannie po każdej aktualizacji baz danych. Jeżeli skanowanie antywirusowe pliku poddanego kwarantannie wykaże, że nie jest on zainfekowany, na ekranie pojawi się powiadomienie.

Powiadomienie zawiera następujące informacje:

- zalecenie przywrócenia pliku z kwarantanny;
- nazwę pliku, łącznie ze ścieżką do folderu, w którym się znajdował przed przeniesieniem do kwarantanny.

Możesz wybrać jedno z następujących działań:

- **Przywróć** – przywraca plik, usuwając go z kwarantanny i przenosząc go do folderu, gdzie znajdował się przed przeniesieniem do kwarantanny.
- **Anuluj** – pozostawia plik w Kwarantannie

## DOSTĘPNA JEST NOWA WERSJA PRODUKTU

Po pojawieniu się nowej wersji Kaspersky Anti-Virus, gdy jest ona dostępna do pobrania na serwerach Kaspersky Lab, na ekranie zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- odnośnik do okna zawierającego szczegółowe informacje o nowej wersji aplikacji;
- rozmiar pakietu instalacyjnego.

Możesz wybrać jedno z następujących działań:

- **Tak, pobierz** – pobiera pakiet instalacyjny nowej wersji aplikacji do wybranego folderu.
- **Nie** – anuluje pobieranie pakietu instalacyjnego.

Jeśli w przyszłości nie chcesz otrzymywać powiadomień o nowej wersji aplikacji, zaznacz pole **Nie informuj o tej aktualizacji**.

## DOSTĘPNE JEST NOWE UAKTUALNIENIE TECHNICZNE

Po pojawieniu się technicznej aktualizacji Kaspersky Anti-Virus, gdy jest ona dostępna do pobrania na serwerach Kaspersky Lab, na ekranie zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- numer wersji aplikacji zainstalowanej na komputerze;
- numer wersji aplikacji po oczekiwanej aktualizacji technicznej;
- odnośnik do okna zawierającego szczegółowe informacje o nowym uaktualnieniu technicznym;
- rozmiar pliku aktualizacji.

Możesz wybrać jedno z następujących działań:

- **Tak, pobierz** – pobiera plik aktualizacji do wybranego folderu.
- **Nie** – anuluje pobieranie uaktualnienia. Ta opcja jest dostępna, jeżeli zaznaczone jest pole **Nie informuj o tej aktualizacji** (patrz poniżej).
- **Nie, przypomnij później** – anuluje pobieranie i wyświetli przypomnienie o aktualizacji w późniejszym terminie. Ta opcja jest dostępna, gdy nie jest zaznaczone pole **Nie informuj o tym uaktualnieniu** (patrz poniżej).

Jeśli nie chcesz otrzymywać w przyszłości tego powiadomienia, zaznacz pole **Nie informuj o tej aktualizacji**.

## POBRANO UAKTUALNIENIE TECHNICZNE

Gdy pobieranie uaktualnień technicznych Kaspersky Anti-Virus z serwerów Kaspersky Lab zostanie zakończone, na ekranie pojawi się powiadomienie.

Powiadomienie zawiera następujące informacje:

- numer wersji aplikacji po aktualizacji technicznej;
- odnośnik do pliku aktualizacji.

Możesz wybrać jedno z następujących działań:

- **Tak, zainstaluj** – instaluje aktualizację.

Po zainstalowaniu aktualizacji wymagane będzie ponowne uruchomienie systemu operacyjnego.

- **Odrocz instalację** – anuluje instalację, by wykonać ją później.

## POBRANE UAKTUALNIENIE TECHNICZNE NIE JEST ZAINSTALOWANE

Jeśli uaktualnienie techniczne Kaspersky Anti-Virus zostało pobrane, ale nie jest zainstalowane na komputerze, na ekranie zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- numer wersji aplikacji po aktualizacji technicznej;
- odnośnik do pliku aktualizacji.

Możesz wybrać jedno z następujących działań:

- **Tak, zainstaluj** – instaluje aktualizację.

Po zainstalowaniu aktualizacji wymagane będzie ponowne uruchomienie systemu operacyjnego.

- **Odrocz instalację** – anuluje instalację, by wykonać ją później.

Jeśli nie chcesz otrzymywać w przyszłości powiadomienia o tej aktualizacji, zaznacz pole **Nie pytaj, aż do nowej wersji**.

## LICENCJA WYGASŁA

Po wygaśnięciu licencji testowej, Kaspersky Anti-Virus wyświetla na ekranie powiadomienie.

Powiadomienie zawiera następujące informacje:

- długość okresu testowego;
- informacje o wynikach działania aplikacji (może zawierać odnośnik do szczegółów).

Możesz wybrać jedno z następujących działań:

- **Tak, kup** – wybranie tej opcji otwiera okno przeglądarki i łączy stronę internetową sklepu, w którym możesz zakupić licencję komercyjną.
- **Anuluj** – zrezygnuj z korzystania z aplikacji. Jeśli wybierzesz tę opcję, aplikacja przestanie wykonywać swoje główne funkcje (skanowanie antywirusowe, aktualizację, ochronę w czasie rzeczywistym itd.).

## PRZED WYKONANIEM SKANOWANIA ZALECANE JEST ZAKTUALIZOWANIE BAZ DANYCH

Jeśli zainicjujesz zadania skanowania przed lub w trakcie pierwszej aktualizacji baz danych, na ekranie jest wyświetlane powiadomienie.

Zawiera ono zalecenie dotyczące aktualizacji baz danych lub zaczekania do zakończenia aktualizacji przed wykonaniem pierwszego skanowania.

Możesz wybrać jedno z następujących działań:

- **Zaktualizuj bazy danych przed uruchomieniem skanowania** – uruchamiana jest aktualizacja baz danych, po której następuje automatyczne uruchomienie skanowania. Opcja ta jest niedostępna, gdy uruchomiłeś skanowanie przed pierwszą aktualizacją baz danych.
- **Uruchom skanowanie po aktualizacji** – poczekaj na zakończenie aktualizacji baz danych i uruchom zadanie skanowania automatycznie. Opcja ta jest niedostępna, gdy uruchomiłeś skanowanie podczas pierwszej aktualizacji baz danych.
- **Uruchom skanowanie teraz** – uruchamia zadanie skanowania bez oczekiwania na zakończenie aktualizacji baz danych.

## POWIADOMIENIA W INTERAKTYWNYM TRYBIE OCHRONY

Sekcja ta zawiera informacje o powiadomieniach, które są wyświetlane na ekranie w interaktywnym trybie ochrony (sekcja "Wybieranie trybu ochrony" na stronie [65](#)).

### W TEJ SEKCJI:

Wykryto podejrzany / szkodliwy obiekt.....	<a href="#">152</a>
Wykryto lukę.....	<a href="#">153</a>
Wykryto niebezpieczną aktywność w systemie .....	<a href="#">154</a>
Cofanie zmian dokonanych przez aplikację, która może zostać użyta przez hakerów do uszkodzenia komputera lub danych.....	<a href="#">154</a>
Wykryto szkodliwą aplikację.....	<a href="#">155</a>
Wykryto aplikację, która może zostać wykorzystana przez hakerów .....	<a href="#">156</a>
Wykryto podejrzany / szkodliwy odnośnik .....	<a href="#">156</a>
Wykryto niebezpieczny obiekt w ruchu sieciowym .....	<a href="#">157</a>
Wykryto próbę dostępu do strony typu phishing.....	<a href="#">157</a>
Wykryto próbę uzyskania dostępu do rejestru systemowego.....	<a href="#">158</a>
Obiekt nie może zostać wyleczony .....	<a href="#">158</a>
Wykryto ukryty proces.....	<a href="#">159</a>


## WYKRYTO PODEJRZANY / SZKODLIWY OBIEKT

Podczas działania modułu Ochrona plików i Ochrona poczty, a także wykonywania skanowania antywirusowego, wyświetlony może zostać komunikat o wykryciu:

- szkodliwego obiektu;
- obiektu zawierającego kod nieznanego wirusa.
- obiektu zawierającego zmodyfikowany kod nieznanego wirusa.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Typ zagrożenia i nazwę szkodliwego obiektu zgodną z Encyklopedią Wirusów Kaspersky Lab.

Obok nazwy szkodliwego obiektu wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o obiekcie. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje o zagrożeniu, jakie stwarza obiekt.

- Nazwę pliku szkodliwego obiektu oraz jego ścieżkę dostępu.

Na obiekcie możesz wykonać następujące akcje:

- **Wylecz** – próba wyleczenia szkodliwego obiektu. Opcja ta jest zalecana, jeśli zagrożenie jest znane.

Przed wyleczeniem obiektu tworzona jest jego kopia zapasowa.

- **Kwarantanna** – przenosi obiekt do Kwarantanny, gdzie nie będzie stwarzać żadnego zagrożenia dla komputera. Opcja ta jest zalecana, jeśli nie jest znane zagrożenie oraz sposoby wyleczenia obiektu.

Podczas późniejszych skanowań Kwarantanny stan obiektu może się zmienić. Na przykład, obiekt może się okazać zainfekowany z możliwością przetworzenia przy użyciu zaktualizowanych baz danych. Stan obiektu może się także zmienić na *niezainfekowany* i jego przywrócenie będzie możliwe.

Podczas kolejnego skanowania stan pliku przeniesionego do Kwarantanny może się zmienić na *niezainfekowany* pod warunkiem, że skanowanie odbyło się przynajmniej trzy dni po przeniesieniu go do Kwarantanny.

- **Usuń** – usuwa obiekt. Przed usunięciem obiektu tworzona jest jego kopia zapasowa.
- **Ignoruj / Blokuj** – blokuje dostęp do obiektu, ale nie wykonuje na nim żadnych akcji; po prostu zapisuje informacje o nim w raporcie.

Możesz powrócić do przetwarzania pominiętych obiektów w oknie raportu. Pomijanie przetwarzania obiektów wykrytych w wiadomościach e-mail nie jest możliwe.

Wybrana akcja może zostać zastosowana do wszystkich zagrożeń tego samego typu, które zostały wykryte w bieżącej sesji modułu ochrony lub zadania. W tym celu należy zaznaczyć opcję **Zastosuj do wszystkich obiektów**. Bieżąca sesja to czas liczony od uruchomienia składnika aż do zatrzymania jego pracy lub ponownego uruchomienia Kaspersky Anti-Virus. Czas ten może być również liczony od rozpoczęcia do zakończenia skanowania.


Jeżeli masz pewność, że klasyfikacja wykonana przez program jest błędna, dodaj nieprawidłowo wykrywany obiekt do strefy zaufanej w celu uniknięcia fałszywych alarmów.

## WYKRYTO LUKĘ

W przypadku wykrycia luki na ekranie wyświetlane jest powiadomienie.

Powiadomienie zawiera następujące informacje:

- Opis luki.
- Nazwę obiektu zgodną z klasyfikacją Encyklopedii Wirusów Kaspersky Lab.

Obok nazwy wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o luce. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje o tej luce.

- Nazwę pliku obiektu zawierającego lukę oraz jego ścieżkę dostępu.


Na obiekcie możesz wykonać następujące akcje:

- **Tak, napraw** – eliminuje lukę.
- **Ignoruj** – nie wykonuje żadnych akcji na obiekcie zawierającym lukę.

## WYKRYTO NIEBEZPIECZNĄ AKTYWNOŚĆ W SYSTEMIE

Jeżeli Ochrona proaktywna wykryje niebezpieczną aktywność aplikacji w Twoim systemie, na ekranie zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Typ zagrożenia i nazwę szkodliwego obiektu zgodną z Encyklopedią Wirusów Kaspersky Lab.  
 Obok nazwy szkodliwego obiektu wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o obiekcie. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje o zagrożeniu, jakie stwarza obiekt.
- Identyfikator procesu i nazwę pliku aplikacji wraz z jego ścieżką dostępu.

Możesz wybrać jedno z następujących działań:

- **Zezwól** – zezwala na uruchomienie aplikacji.
- **Kwarantanna** – zamyka aplikację, przenosi plik programu do Kwarantanny, gdzie nie stwarza on żadnego zagrożenia dla bezpieczeństwa komputera.

Podczas późniejszych skanowań Kwarantanny stan obiektu może się zmienić. Na przykład, obiekt może się okazać zainfekowany z możliwością przetworzenia przy użyciu zaktualizowanych baz danych. Stan obiektu może się także zmienić na *niezainfekowany* i jego przywrócenie będzie możliwe.

Podczas kolejnego skanowania stan pliku przeniesionego do Kwarantanny może się zmienić na *niezainfekowany* pod warunkiem, że skanowanie odbyło się przynajmniej trzy dni po przeniesieniu go do Kwarantanny.

- **Zakończ aplikację** – przerywa wykonywanie aplikacji.
- **Dodaj do wyjątków** – zezwala aplikacji na wykonywanie takich akcji w przyszłości.

Jeżeli masz pewność, że klasyfikacja wykonana przez program Kaspersky Anti-Virus jest błędna, dodaj nieprawidłowo wykrywany obiekt do strefy zaufanej w celu uniknięcia fałszywych alarmów.

## COFANIE ZMIAN DOKONANYCH PRZEZ APLIKACJĘ, KTÓRA MOŻE ZOSTAĆ UŻYTA PRZEZ HAKERÓW DO USZKODZENIA KOMPUTERA LUB DANYCH

Zalecamy wycofanie (anulowanie) zmian dokonanych przez aplikację, która może zostać użyta przez hakerów do uszkodzenia komputera lub danych. Po zakończeniu działania takiej aplikacji, na ekranie wyświetlone zostanie powiadomienie zawierające żądanie wycofania zmian.

Powiadomienie zawiera następujące informacje:

- Żądanie wycofania zmian dokonanych przez aplikację, która może zostać użyta przez hakerów do uszkodzenia komputera lub danych.
- Typ i nazwę aplikacji.

Obok nazwy aplikacji wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o aplikacji.

- Identyfikator procesu i nazwę pliku aplikacji wraz z jego ścieżką dostępu.

Możesz wybrać jedno z następujących działań:

- **Ignoruj** – anulowanie cofania zmian.
- **Tak, cofnij** – wycofanie zmian dokonanych przez aplikację.

## WYKRYTO SZKODLIWĄ APLIKACJĘ

Po wykryciu przez Kontrolę systemu aplikacji, której zachowanie jest takie jak zachowanie szkodliwych programów, na ekranie wyświetlone zostanie powiadomienie.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Typ i nazwę szkodliwej aplikacji.

Obok nazwy aplikacji wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o aplikacji.

- Identyfikator procesu i nazwę pliku aplikacji wraz z jego ścieżką dostępu.
- Odnośnik do okna z raportem uruchamiania aplikacji.

Możesz wybrać jedno z następujących działań:

- **Zezwól** – zezwala na uruchomienie aplikacji.
- **Kwarantanna** – zamyka aplikację, przenosi plik programu do Kwarantanny, gdzie nie stwarza on żadnego zagrożenia dla bezpieczeństwa komputera.

Podczas późniejszych skanowań Kwarantanny stan obiektu może się zmienić. Na przykład, obiekt może się okazać zainfekowany z możliwością przetworzenia przy użyciu zaktualizowanych baz danych. Stan obiektu może się także zmienić na *niezainfekowany* i jego przywrócenie będzie możliwe.

Podczas kolejnego skanowania stan pliku przeniesionego do Kwarantanny może się zmienić na *niezainfekowany* pod warunkiem, że skanowanie odbyło się przynajmniej trzy dni po przeniesieniu go do Kwarantanny.


- **Zakończ aplikację** – przerywa wykonywanie aplikacji.
- **Dodaj do wyjątków** – zezwala aplikacji na wykonywanie takich akcji w przyszłości.

## WYKRYTO APLIKACJĘ, KTÓRA MOŻE ZOSTAĆ WYKORZYSTANA PRZEZ HAKERÓW

Jeśli Ochrona plików, Ochrona poczty lub zadanie skanowania antywirusowego wykryje aplikację, którą mogą wykorzystać hakerzy, zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Rodzaj zagrożenia i nazwę obiektu zgodną z klasyfikacją Encyklopedii Wirusów Kaspersky Lab.

Obok nazwy obiektu wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o obiekcie. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje.

- Nazwę pliku obiektu oraz jego ścieżkę dostępu.

Na obiekcie możesz wykonać następujące akcje:

- **Kwarantanna** – przenosi obiekt do Kwarantanny, gdzie nie będzie stwarzać żadnego zagrożenia dla komputera. Opcja ta jest zalecana, jeśli nie jest znane zagrożenie oraz sposoby wyleczenia obiektu.

Podczas późniejszych skanowań Kwarantanny stan obiektu może się zmienić. Na przykład, obiekt może się okazać zainfekowany z możliwością przetworzenia przy użyciu zaktualizowanych baz danych. Stan obiektu może się także zmienić na *niezainfekowany* i jego przywrócenie będzie możliwe.

Podczas kolejnego skanowania stan pliku przeniesionego do Kwarantanny może się zmienić na *niezainfekowany* pod warunkiem, że skanowanie odbyło się przynajmniej trzy dni po przeniesieniu go do Kwarantanny.

- **Usuń** – usuwa obiekt. Przed usunięciem obiektu tworzona jest jego kopia zapasowa.
- **Usuń archiwum** - usunięcie szkodliwego archiwum chronionego hasłem.
- **Ignoruj / Blokuj** – blokuje dostęp do obiektu, ale nie wykonuje na nim żadnych akcji; po prostu zapisuje informacje o nim w raporcie.

Możesz powrócić do przetwarzania pominiętych obiektów w oknie raportu. Pomijanie przetwarzania obiektów wykrytych w wiadomościach e-mail nie jest możliwe.

- **Dodaj do wykluczeń** - tworzy regułę wykluczeń dla tego typu zagrożeń.

Wybrana akcja może zostać zastosowana do wszystkich zagrożeń tego samego typu, które zostały wykryte w bieżącej sesji modułu ochrony lub zadania. W tym celu należy zaznaczyć opcję **Zastosuj do wszystkich obiektów**. Bieżąca sesja to czas liczony od uruchomienia składnika aż do zatrzymania jego pracy lub ponownego uruchomienia Kaspersky Anti-Virus. Czas ten może być również liczony od rozpoczęcia do zakończenia skanowania.

Jeżeli masz pewność, że klasyfikacja wykonana przez program jest błędna, dodaj nieprawidłowo wykrywany obiekt do strefy zaufanej w celu uniknięcia fałszywych alarmów.

## WYKRYTO PODEJRZANY / SZKODLIWY ODNOŚNIK

Po wykryciu przez Kaspersky Anti-Virus próby otwarcia strony internetowej zawierającej podejrzaną lub szkodliwą treść, na ekranie zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- opis zagrożenia;

- nazwę aplikacji (przeglądarki), która otwiera stronę;
- adres internetowy strony ze szkodliwą lub podejrzaną treścią.

Możesz wybrać jedno z następujących działań:

- **Zezwól** – kontynuuje otwieranie strony.
- **Blokuj** – blokuje otwieranie strony.


Wybrana akcja może zostać zastosowana do wszystkich zagrożeń tego samego typu, które zostały wykryte w bieżącej sesji modułu ochrony. W tym celu należy zaznaczyć opcję **Zastosuj do wszystkich obiektów**. Bieżąca sesja to czas od momentu uruchomienia modułu do momentu jego zatrzymania lub ponownego uruchomienia Kaspersky Anti-Virus.

## WYKRYTO NIEBEZPIECZNY OBIEKT W RUCHU SIECIOWYM

Jeżeli moduł Ochrona WWW wykryje w ruchu sieciowym szkodliwy obiekt, na ekranie wyświetlony zostanie specjalny komunikat.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia lub akcji wykonanych przez aplikację.
- Nazwę aplikacji, która wykonuje akcję.
- Typ zagrożenia i nazwę szkodliwego obiektu zgodną z Encyklopedią Wirusów Kaspersky Lab.

Obok nazwy szkodliwego obiektu wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o obiekcie. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje o zagrożeniu, jakie stwarza obiekt.

- Lokalizację obiektu (adres internetowy).

Możesz wybrać jedno z następujących działań:

- **Zezwól** – kontynuuje pobieranie obiektu.
- **Blokuj** – blokuje pobranie obiektu.

Wybrana akcja może zostać zastosowana do wszystkich zagrożeń tego samego typu, które zostały wykryte w bieżącej sesji modułu ochrony lub zadania. W tym celu należy zaznaczyć opcję **Zastosuj do wszystkich obiektów**. Bieżąca sesja to czas od momentu uruchomienia modułu do momentu jego zatrzymania lub ponownego uruchomienia Kaspersky Anti-Virus.

## WYKRYTO PRÓBĘ DOSTĘPU DO STRONY TYPU PHISHING

Po wykryciu przez Kaspersky Anti-Virus próby dostępu do strony internetowej należącej lub mogącej należeć do stron typu phishing, na ekranie pojawi się powiadomienie.

Powiadomienie zawiera następujące informacje:

- opis zagrożenia;
- adres strony internetowej.

Możesz wybrać jedno z następujących działań:

- **Zezwól** – kontynuuje otwieranie strony.
- **Blokuj** – blokuje otwieranie strony.

Wybrana akcja może zostać zastosowana do wszystkich zagrożeń tego samego typu, które zostały wykryte w bieżącej sesji programu Kaspersky Anti-Virus. W tym celu należy zaznaczyć opcję **Zastosuj do wszystkich obiektów**. Bieżąca sesja to czas od momentu uruchomienia modułu do momentu jego zatrzymania lub ponownego uruchomienia Kaspersky Anti-Virus.

## WYKRYTO PRÓBĘ UZYSKANIA DOSTĘPU DO REJESTRU SYSTEMOWEGO

Gdy moduł Ochrona proaktywna wykryje próbę uzyskania dostępu do kluczy rejestru systemowego, na ekranie wyświetlone zostanie specjalne powiadomienie.

Powiadomienie zawiera następujące informacje:

- klucz rejestru, do którego uzyskiwany jest dostęp;
- nazwę pliku procesu, który zainicjował próbę uzyskania dostępu do kluczy rejestru, łącznie ze ścieżką dostępu do niego.

Możesz wybrać jedno z następujących działań:

- **Zezwól** – jednorazowo zezwala na wykonanie niebezpiecznej akcji;
- **Blokuj** – jednorazowo blokuje niebezpieczną akcję.

Aby wybrana akcja stosowana była do każdej próby uzyskania dostępu do kluczy rejestru, zaznacz pole **Utwórz regułę**.


Jeżeli masz pewność, że każda aktywność aplikacji próbującej uzyskać dostęp do kluczy rejestru systemu jest bezpieczna, dodaj tę aplikację do listy zaufanych.

## OBIEKT NIE MOŻE ZOSTAĆ WYLECZONY

W niektórych przypadkach obiekt nie może zostać wyleczony: na przykład, jeśli plik jest uszkodzony w tak dużym stopniu, że aplikacja nie może usunąć z niego szkodliwego kodu i przywrócić jego integralności. Procedura leczenia nie może być stosowana do niektórych typów szkodliwych obiektów, takich jak trojany. Jeżeli nie będzie można wyleczyć obiektu, na ekranie zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Typ zagrożenia i nazwę szkodliwego obiektu zgodną z Encyklopedią Wirusów Kaspersky Lab.

Obok nazwy szkodliwego obiektu wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o obiekcie. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje o zagrożeniu, jakie stwarza obiekt.

- Nazwę pliku szkodliwego obiektu oraz jego ścieżkę dostępu.

Możesz wybrać jedno z następujących działań:

- **Usuń** – usuwa obiekt. Przed usunięciem obiektu tworzona jest jego kopia zapasowa.
- **Ignoruj / Blokuj** – blokuje dostęp do obiektu, ale nie wykonuje na nim żadnych akcji; po prostu zapisuje informacje o nim w raporcie.

Możesz powrócić do przetwarzania pominiętych obiektów w oknie raportu. Pomijanie przetwarzania obiektów wykrytych w wiadomościach e-mail jest możliwe.

- **Dodaj do wykluczeń** - tworzy regułę wykluczeń dla tego typu zagrożeń.


Wybrana akcja może zostać zastosowana do wszystkich zagrożeń tego samego typu, które zostały wykryte w bieżącej sesji modułu ochrony lub zadania. W tym celu należy zaznaczyć opcję **Zastosuj do wszystkich obiektów**. Bieżąca sesja to czas liczony od uruchomienia składnika aż do zatrzymania jego pracy lub ponownego uruchomienia Kaspersky Anti-Virus. Czas ten może być również liczony od rozpoczęcia do zakończenia skanowania.

## WYKRYTO UKRYTY PROCES

Jeśli moduł Ochrona proaktywna wykryje w systemie ukryty proces, na ekranie zostanie wyświetlone powiadomienie.

Powiadomienie zawiera następujące informacje:

- Opis zagrożenia.
- Typ i nazwę zagrożenia zgodną z klasyfikacją Encyklopedii Wirusów Kaspersky Lab.

Obok nazwy wyświetlona jest ikona . Kliknij ją, aby wyświetlić okno z informacjami o zagrożeniu. Kliknięcie w tym oknie odnośnika [www.viruslist.pl](http://www.viruslist.pl) otwiera stronę internetową Encyklopedii Wirusów, na której znajdują się szczegółowe informacje o tym zagrożeniu.

- Nazwę pliku procesu oraz jego ścieżkę dostępu.

Możesz wybrać jedno z następujących działań:

- **Kwarantanna** – zamyka proces, przenosi plik procesu do Kwarantanny, gdzie nie będzie stanowił żadnego zagrożenia dla bezpieczeństwa komputera.

Podczas późniejszych skanowań Kwarantanny stan obiektu może się zmienić. Na przykład, obiekt może się okazać zainfekowany z możliwością przetworzenia przy użyciu zaktualizowanych baz danych. Stan obiektu może się także zmienić na *niezainfekowany* i jego przywrócenie będzie możliwe.

Podczas kolejnego skanowania stan pliku przeniesionego do Kwarantanny może się zmienić na *niezainfekowany* pod warunkiem, że skanowanie odbyło się przynajmniej trzy dni po przeniesieniu go do Kwarantanny.

- **Zakończ** – kończy proces.
- **Zezwól** – zezwala na wykonanie procesu.

Wybrana akcja może zostać zastosowana do wszystkich zagrożeń o danym typie wykrytych w bieżącej sesji Ochrony proaktywnej. W tym celu należy zaznaczyć opcję **Zastosuj do wszystkich zdarzeń tego typu**. Bieżąca sesja to czas od momentu uruchomienia modułu do momentu jego zatrzymania lub ponownego uruchomienia Kaspersky Anti-Virus.

Jeżeli masz pewność, że klasyfikacja wykonana przez program Kaspersky Anti-Virus jest błędna, dodaj nieprawidłowo wykrywany obiekt do strefy zaufanej w celu uniknięcia fałszywych alarmów.

# SŁOWNIK

## A

### **AKTUALIZACJA**

Procedura zastępowania/dodawania nowych plików (baz danych i modułów aplikacji) otrzymywanych z serwerów aktualizacji firmy Kaspersky Lab.

### **AKTUALIZACJA BAZ DANYCH**

Jedną z funkcji aplikacji firmy Kaspersky Lab umożliwiającą zapewnienie aktualnej ochrony. W tym celu z serwerów aktualizacji firmy Kaspersky Lab na komputer pobierane są bazy danych, które są następnie automatycznie dodawane do aplikacji.

### **AKTYWNA LICENCJA**

Bieżąca licencja używana do działania programu firmy Kaspersky Lab. Licencja definiuje okres, w którym produkt posiada pełną funkcjonalność oraz zasady, na jakich on może być użytkowany. Aplikacja może posiadać tylko jedną aktywną licencję.

### **AKTYWOWANIE APLIKACJI**

Przełączanie aplikacji do trybu pełnej funkcjonalności. Do aktywacji aplikacji niezbędna jest licencja.

### **ALTERNATYWNE STRUMIENIE NTFS**

Strumienie danych NTFS (alternatywne strumienie danych) zostały utworzone w celu uzyskania dodatkowych atrybutów lub informacji o pliku.

Każdy plik w systemie plików NTFS jest zbiorem strumieni. Jeden z nich zawiera plik, którego zawartość będzie można przeglądać po jego otwarciu; inne strumienie (zwane alternatywnymi) zawierają metainformacje i zapewniają, na przykład, kompatybilność NTFS z innymi systemami, takimi jak starszy system plików zwany przez firmę Macintosh Hierarchicznym Systemem Plików (HFS). Strumienie mogą być tworzone, usuwane, osobno przechowywane, przemianowane lub nawet uruchomione jako proces.

Strumienie alternatywne mogą być wykorzystywane przez hakerów do przesyłania poufnych danych lub do wykradania ich z komputera.

### **ANALIZA HEURYSTYCZNA**

Technologia polegająca na wykrywaniu zagrożeń, które nie mogą zostać zidentyfikowane przy pomocy baz danych aplikacji Kaspersky Lab. W wyniku działania heurystyki możliwe jest wykrywanie obiektów, które prawdopodobnie zawierają nieznane wirusy lub modyfikacje znanych wirusów.

Analizator heurystyczny pozwala na wykrywanie do 92% zagrożeń. Mechanizm ten jest bardzo efektywny i rzadko generuje fałszywe alarmy.

Pliki wykryte przez analizator heurystyczny są uznawane za podejrzane.

### **ARCHIWUM**

Plik "zawierający" jeden lub większą liczbę innych obiektów, które także mogą być archiwami.

## B

### **BAZA ADRESÓW STRON ZAWIERAJĄCYCH PHISHING**

Lista adresów internetowych, które są oznaczone przez specjalistów z Kaspersky Lab jako phishingowe. Baza danych jest regularnie aktualizowana i jest częścią aplikacji Kaspersky Lab.

## **BAZA PODEJRZANYCH ADRESÓW INTERNETOWYCH**

Lista adresów internetowych o potencjalnie niebezpiecznej zawartości. Jest ona tworzona przez specjalistów z Kaspersky Lab. Lista ta jest regularnie aktualizowana oraz znajduje się w pakiecie instalacyjnym Kaspersky Lab.

## **BAZY DANYCH**

Bazy danych utworzone przez ekspertów z Kaspersky Lab zawierają szczegółowe opisy wszystkich dotychczas poznanych zagrożeń, a także metody wykorzystywane do ich wykrycia i wyleczenia. Natychmiast po pojawieniu się nowego zagrożenia bazy danych zostają zaktualizowane przez firmę Kaspersky Lab.

## **BLOKOWANIE OBIEKTU**

Odmowa dostępu do obiektu z zewnętrznych aplikacji. Zablokowany obiekt nie może zostać odczytany, wykonany, zmodyfikowany, ani też usunięty.

## **BRAMA DWUKIERUNKOWA**

Komputer posiadający dwie karty sieciowe (każda jest podłączona do innych sieci) przesyłający dane z jednej sieci do innej.

## **C**

### **CERTYFIKAT SERWERA ADMINISTRACYJNEGO**

Certyfikat, który umożliwia autoryzację Serwera administracyjnego podczas połączenia do niego Konsoli administracyjnej oraz podczas wymiany danych między użytkownikami komputerów. Certyfikat serwera administracyjnego jest tworzony podczas instalacji serwera administracyjnego i jest przechowywany w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminikit\1093\cert.

### **CZARNA LISTA PLIKÓW KLUCZY**

Baza danych zawierająca informacje o dodanych do czarnej listy plikach kluczy Kaspersky Lab. Zawartość pliku czarnej listy jest aktualizowana wraz z bazami danych.

## **D**

### **DODATKOWA LICENCJA**

Licencja, która została dodana do działania programu firmy Kaspersky Lab, ale nie została aktywowana. Licencja zapasowa zostanie automatycznie aktywowana po wygaśnięciu obecnie wykorzystywanej.

### **DOSTĘPNE UAKTUALNIENIA**

Zestaw uaktualnień dla modułów aplikacji firmy Kaspersky Lab łącznie z uaktualnieniami krytycznymi nagromadzonymi podczas pewnego okresu oraz zmianami w architekturze aplikacji.

## **E**

### **EPIDEMIA WIRUSA**

Seria celowych prób zainfekowania komputera wirusem.

## **F**

### **FALSZYWY ALARM**

Sytuacja, gdy aplikacja firmy Kaspersky Lab identyfikuje niezainfekowany obiekt jako zainfekowany z powodu podobieństwa jego kodu do kodu wirusa.

**I****INSTALACJA W OPARCIU O SKRYPT LOGOWANIA**

Metoda zdalnej instalacji aplikacji Kaspersky Lab, która umożliwi przypisanie uruchomienia zadania zdalnej instalacji indywidualnemu kontu użytkownika (lub różnym kontom użytkowników). Po zarejestrowaniu użytkownika w domenie podejmowana jest próba instalacji aplikacji na komputerze klienckim, na którym użytkownik został zarejestrowany. Ta metoda jest zalecana w przypadku instalowania aplikacji firmy Kaspersky Lab na komputerach z systemami Microsoft Windows 98 / ME.

**K****KASPERSKY SECURITY NETWORK**

Kaspersky Security Network (KSN) jest usługą sieciową oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky Lab zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Anti-Virus po wykryciu nowego zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów.

**KWARANTANNA**

Folder, w którym umieszczane są potencjalnie zarażone obiekty wykryte podczas skanowania lub przez ochronę w czasie rzeczywistym.

**L****LECZENIE OBIEKTU**

Metoda używana do przetwarzania zainfekowanych obiektów, której efektem jest całkowite lub częściowe przywrócenie danych lub informacja, że obiekty nie mogą zostać wyleczone. Obiekty są leczone przy użyciu wpisów z bazy danych. Podczas procesu leczenia część danych może zostać utracona.

**LICZNIK EPIDEMII WIRUSA**

Szablon, na podstawie którego generowane jest powiadomienie o zagrożeniu epidemią wirusa. Licznik epidemii wirusa zawiera ustawienia określające próg aktywności wirusa, sposób jego rozprzestrzeniania oraz treść wysyłanych wiadomości.

**LISTA BLOKOWANYCH ADRESÓW INTERNETOWYCH**

Lista masek i adresów zasobów sieciowych, do których dostęp będzie blokowany przez aplikację Kaspersky Lab. Lista adresów jest tworzona przez użytkownika podczas konfiguracji ustawień aplikacji.

**LISTA DOZWOLONYCH ADRESÓW INTERNETOWYCH**

Lista masek i adresów zasobów sieciowych, do których dostęp nie będzie blokowany przez aplikację Kaspersky Lab. Lista adresów jest tworzona przez użytkownika podczas konfiguracji ustawień aplikacji.

**LISTA SPRAWDZANYCH ADRESÓW INTERNETOWYCH**

Lista masek i adresów zasobów sieciowych, które będą obowiązkowo skanowane przez aplikację Kaspersky Lab na obecność szkodliwych obiektów.

**LISTA ZAUFANYCH ADRESÓW INTERNETOWYCH**

Lista masek i adresów zasobów sieciowych, których treść jest uważana za zaufaną. Aplikacja Kaspersky Lab nie skanuje na obecność szkodliwych obiektów stron internetowych znajdujących się na liście.

**M****MASKA PLIKU**

Reprezentacja nazwy i rozszerzenia pliku przy użyciu symboli wieloznacznych. Dwa standardowe symbole wieloznaczne wykorzystywane w maskach plików to \* i ?, gdzie \* zastępuje dowolną liczbę dowolnych znaków, a ? oznacza dowolny

pojedynczy znak. Przy użyciu tych symboli możliwa jest reprezentacja dowolnego pliku. Należy pamiętać, że nazwa i rozszerzenie zawsze są rozdzielone kropką.

### **MASKA PODSIECI**

Maska podsieci (zwana również maską sieci) oraz adres sieci określają adresy komputerów w sieci.

### **MODUŁ PRZECHWYTUJĄCY**

Składnik aplikacji odpowiedzialny za skanowanie określonych typów wiadomości e-mail. Zestaw modułów przechwytyjących dla Twojej instalacji zależy od tego, do wykonywania jakiej roli lub ich kombinacji jest wdrażana aplikacja.

### **MODUŁY APLIKACJI**

Pliki znajdujące się w pakiecie instalacyjnym Kaspersky Lab, odpowiedzialne za wykonywanie jego głównych zadań. Określony moduł wykonywalny odpowiada każdemu rodzajowi zadania wykonywanego przez aplikację (ochrona w czasie rzeczywistym, skanowanie na żądanie, aktualizacja). Poprzez uruchomienie pełnego skanowania komputera z poziomu okna głównego można rozpocząć wykonanie modułu tego zadania.

### **MONITOROWANY OBIEKT**

Plik przechodzący przez protokoły HTTP, FTP oraz SMTP jak również przez zaporę sieciową i wysyłany do aplikacji firmy Kaspersky Lab w celu przeskanowania.

## **N**

### **NAGŁÓWEK**

Informacje na początku pliku lub wiadomości zawierające dane niskiego poziomu dotyczące statusu i przetwarzania pliku (lub wiadomości). Nagłówek wiadomości e-mail zawiera głównie takie dane, jak informacje o nadawcy i odbiorcy oraz datę.

### **NEUTRALIZOWANIE OBIEKTÓW PO RESTARCIE**

Metoda przetwarzania zainfekowanych obiektów, które w momencie leczenia są wykorzystywane przez inne aplikacje. Polega na tworzeniu kopii zainfekowanego obiektu, leczeniu tej kopii i zastąpieniu pierwotnego zainfekowanego obiektu wyleczoną kopią po kolejnym powtórnym uruchomieniu systemu.

### **NIEBEZPIECZNY OBIEKT**

Obiekt zawierający wirusa. Nie zalecamy korzystania z tych obiektów, ponieważ może to skutkować zainfekowaniem komputera. Po wykryciu zainfekowanego obiektu zalecamy przeprowadzenie jego leczenia przy użyciu jednej z aplikacji Kaspersky Lab lub usunięcie, gdy nie jest to możliwe.

### **NIEKOMPATYBILNA APLIKACJA**

Aplikacja antywirusowa innego producenta lub aplikacja firmy Kaspersky Lab, którą nie można zarządzać za pomocą Kaspersky Anti-Virus.

### **NIEZNANY WIRUS**

Nowy wirus, o którym informacje nie zostały uwzględnione w bazach danych. Zwykle nieznanne wirusy są wykrywane przez aplikację w obiektach przy użyciu analizy heurystycznej i są one klasyfikowane jako potencjalnie zainfekowane.

## **O**

### **OBIEKT OLE**

Obiekt załączony lub osadzony w innym pliku. Aplikacja Kaspersky Lab umożliwia skanowanie obiektów OLE w poszukiwaniu wirusów. Na przykład, gdy dokument Microsoft Office Word zawiera tabelę Microsoft Office Excel, będzie ona skanowana jako obiekt OLE.

## **OBIEKTY STARTOWE**

Zestaw programów niezbędnych do uruchomienia i poprawnego działania systemu operacyjnego i oprogramowania zainstalowanego na Twoim komputerze. Obiekty te są wykonywane za każdym razem, gdy uruchamiany jest system operacyjny. Istnieją wirusy potrafiące infekować takie obiekty, co może doprowadzić między innymi do zablokowania uruchamiania systemu operacyjnego.

## **OCHRONA W CZASIE RZECZYWISTYM**

Tryb działania aplikacji, w którym obiekty są skanowane w celu wykrycia szkodliwego kodu w czasie rzeczywistym.

Aplikacja przechwytuje wszystkie próby otwarcia dowolnego obiektu (do odczytu, zapisu, wykonania) i skanuje go w poszukiwaniu zagrożeń. Niezainfekowane obiekty są przekazywane użytkownikowi; obiekty zawierające zagrożenia lub podejrzane o zawieranie takich zagrożeń są przetwarzane zgodnie z ustawieniami zadania (są leczone, usuwane lub umieszczane w kwarantannie).

## **OKRES WAŻNOŚCI LICENCJI**

Okres, w którym możesz wykorzystywać wszystkie funkcje aplikacji firmy Kaspersky Lab. Okres ważności licencji zwykle wynosi jeden rok kalendarzowy, począwszy od daty instalacji. Po wygaśnięciu licencji aplikacja będzie posiadała ograniczoną funkcjonalność. Nie będziesz mógł aktualizować baz danych aplikacji.

## **P**

### **PAKIET AKTUALIZACYJNY**

Pakiet plików wykorzystywany do aktualizowania oprogramowania. Jest pobierany z Internetu i instalowany na Twoim komputerze.

### **PHISHING**

Rodzaj oszustwa internetowego, które polega na wysyłaniu wiadomości elektronicznych w celu kradzieży poufnych informacji - przeważnie danych związanych z bankowością online.

### **PLIK KLUCZA**

Plik z rozszerzeniem KEY, który stanowi Twój osobisty "klucz" niezbędny do korzystania z aplikacji firmy Kaspersky Lab. W przypadku zakupu aplikacji u dystrybutora firmy Kaspersky Lab, klucz dostarczany jest wraz z produktem, natomiast w przypadku zakupu online - wysyłany w e-mailu.

### **PLIK SKOMPRESOWANY**

Plik zarchiwizowany zawierający program dekompresujący oraz instrukcje do wykonania przez system operacyjny.

### **PODEJRZANA WIADOMOŚĆ**

Wiadomość, która podczas skanowania wydaje się podejrzana, jednak nie może być jednoznacznie określona jako spam (np. niektóre rodzaje wiadomości i reklam).

### **PODEJRZANY OBIEKT**

Obiekt zawierający zmodyfikowany kod znanego wirusa lub kod przypominający wirusa, który nie został jeszcze wykryty przez specjalistów z Kaspersky Lab. Podejrzane obiekty są wykrywane przy użyciu analizy heurystycznej.

### **PORT SIECIOWY**

Parametr TCP oraz UDP określający lokalizację docelową pakietów danych w formacie IP przesyłanych do hosta za pośrednictwem sieci i umożliwiający różnym programom działającym na jednym hoście otrzymywanie danych niezależnie od siebie. Każdy program przetwarza dane otrzymywane za pośrednictwem określonego portu (czasami mówi się, że program "nasłuchuje" na tym porcie).

Dla niektórych popularnych protokołów sieciowych istnieją standardowe numery portów (na przykład serwery sieciowe zazwyczaj otrzymują żądania HTTP na porcie TCP numer 80); zwykle jednak program może wykorzystywać dowolny protokół na dowolnym porcie. Możliwe wartości: od 1 do 65535.

**PORT SPRZĘTOWY**

Gniazdo w komputerze, do którego może być podłączony kabel lub wtyczka (port LPT, port szeregowy, port USB).

**PORT WEJŚCIA/WYJŚCIA**

Wykorzystywany w procesorach (np. firmy Intel), obsługuje wymianę danych między składnikami sprzętu. Port wejścia / wyjścia skojarzony jest z pewnym składnikiem sprzętu oraz jest wykorzystywany przez aplikacje do wymiany danych.

**POTENCJALNIE INFEKOWALNY OBIEKT**

Obiekt, który ze względu na swoją strukturę lub format może zostać użyty przez hakerów jako "kontener" do przechowywania i rozprzestrzeniania szkodliwego obiektu. Są to pliki wykonywalne, na przykład pliki z rozszerzeniami COM, EXE, DLL itp. Ryzyko uaktywnienia szkodliwego kodu w takich plikach jest bardzo wysokie.

**POTENCJALNIE ZAINFEKOWANY OBIEKT**

Obiekt zawierający zmodyfikowany kod znanego wirusa lub kod przypominający wirusa, który nie został jeszcze wykryty przez specjalistów z Kaspersky Lab. Potencjalnie zainfekowane pliki są wykrywane przy użyciu analizy heurystycznej.

**POZIOM OCHRONY**

Poziom ochrony jest to początkowa konfiguracja modułu.

**POZIOM PRIORYTETU ZDARZENIA**

Opis zdarzenia rejestrowanego podczas działania aplikacji firmy Kaspersky Lab. Istnieją cztery poziomy priorytetu:

- Zdarzenie krytyczne.
- Błąd w funkcjonowaniu.
- Ostrzeżenie.
- Informacja.

Zdarzenia tego samego typu mogą posiadać różne poziomy priorytetu w zależności od sytuacji, w której wystąpiły.

**POZIOM ZALECANY**

Poziom bezpieczeństwa oparty na ustawieniach aplikacji zalecanych przez ekspertów firmy Kaspersky Lab jako optymalny poziom ochrony Twojego komputera. Poziom ten jest ustawiony domyślnie.

**PROTOKÓŁ**

Wyraźnie zdefiniowany i znormalizowany zestaw reguł określających interakcję pomiędzy klientem a serwerem. Do najbardziej znanych protokołów i usług z nimi skojarzonych należą HTTP (WWW), FTP oraz NNTP (nowość).

**PROTOKÓŁ INTERNETOWY (IP)**

Podstawowy protokół dla Internetu wykorzystywany w niezmienionej postaci od czasu stworzenia go w 1974 roku. Wykonuje podstawowe operacje transmisji danych z jednego komputera do innego i służy jako podstawa dla protokołów wyższego poziomu, takich jak TCP i UDP. Zarządza przetwarzaniem połączeń i błędów. Technologie, takie jak NAT i maskowanie, umożliwiają ukrywanie wielu prywatnych sieci przy pomocy niewielkiej liczby adresów IP (lub nawet jednego adresu), co pozwala spełnić potrzeby nieustannie rozrastającego się Internetu przy użyciu stosunkowo ograniczonej przestrzeni adresowej IPv4.

**PRÓG AKTYWNOŚCI WIRUSA**

Maksymalny dopuszczalny poziom określonego typu zdarzenia w ograniczonym czasie, po przekroczeniu którego można mówić o nadmiernej aktywności wirusa i zagrożeniu epidemią wirusa. Funkcja ta jest istotna podczas epidemii wirusów i umożliwia administratorom szybką reakcję na pojawiające się zagrożenie epidemią wirusów.

## PRZENOSZENIE OBIEKTÓW DO KWARANTANNY

Metoda przetwarzania potencjalnie zainfekowanego obiektu poprzez blokowanie dostępu do pliku i przenoszenie go z jego pierwotnej lokalizacji do foldera kwarantanny. Jest on przechowywany tam w postaci zaszyfrowanej, co eliminuje ryzyko infekcji.

## PRZYWRACANIE

Przenoszenie oryginalnego obiektu z Kwarantanny lub foldera Kopii zapasowej do foldera, w którym znajdował się zanim został przeniesiony do Kwarantanny, wyleczony lub usunięty, lub do innego foldera wskazanego przez użytkownika.

## R

### ROOTKIT

Aplikacja lub zestaw aplikacji, których celem jest ukrywanie śladów hakera lub szkodliwego oprogramowania w systemie.

W przypadku systemów operacyjnych Microsoft Windows nazwa rootkit zazwyczaj odnosi się do programów, które przenikają do systemu i przechwytyują funkcje systemu (Windows API). Przechwytywanie i modyfikowanie funkcji API niskiego poziomu umożliwia tym programom zamaskowanie ich obecności w systemie. Rootkit może maskować obecność dowolnych procesów, folderów i plików przechowywanych na dysku, a także kluczy rejestru, jeżeli są opisane w konfiguracji rootkitu. Wiele rootkitów instaluje w systemie własne sterowniki i usługi (które również pozostają "niewidoczne").

## S

### SEKTOR STARTOWY DYSKU

Sektor startowy jest określonym obszarem na dysku twardym komputera, dyskietce lub innym urządzeniu do przechowywania danych. Zawiera informacje dotyczące systemu plików dysku oraz programu rozruchowego odpowiedzialnego za uruchamianie systemu operacyjnego.

Istnieje wiele wirusów infekujących sektory startowe, zwanych wirusami sektora startowego. Aplikacja firmy Kaspersky Lab umożliwia skanowanie sektorów startowych w celu wykrycia wirusów oraz ewentualnego wyleczenia infekcji.

### SERWER PROXY

Usługa sieciowa komputera, która umożliwia użytkownikom tworzenie pośrednich zapytań do innych usług sieciowych. W pierwszej kolejności użytkownik łączy się z serwerem proxy i wysyła zapytanie o zasób (np. plik) umieszczony na innym serwerze. Następnie serwer proxy także łączy się z określonym serwerem i uzyskuje z niego zasób lub zwraca go ze swojej pamięci podręcznej (jeżeli jest w nią wyposażony). W niektórych przypadkach zapytanie użytkownika lub odpowiedź serwera mogą zostać zmodyfikowane przez serwer proxy.

### SERWERY AKTUALIZACJI KASPERSKY LAB

Lista serwerów HTTP oraz FTP firmy Kaspersky Lab, z których aplikacja pobiera na Twój komputer aktualizacje baz danych oraz modułów.

### SKANOWANIE RUCHU SIECIOWEGO

Skanowanie w czasie rzeczywistym obiektów przesyłanych za pośrednictwem protokołów (np. HTTP, FTP itd.) przy użyciu informacji zawartych w najnowszej wersji baz danych.

### SKRYPT

Mały program komputerowy lub niezależna część programu (funkcja), która służy do wykonywania drobnego i specjalistycznego zadania. W większości przypadków są one osadzone w dokumentach hipertekstowych. Skrypty mogą być uruchamiane, na przykład, podczas otwierania strony internetowej.

Jeżeli ochrona w czasie rzeczywistym jest włączona, aplikacja będzie śledziła uruchamianie skryptów, przechwytywała je i skanowała w poszukiwaniu wirusów. W zależności od wyników skanowania użytkownik może zablokować skrypt lub zezwolić na jego wykonanie.

## SOCKS

Protokół serwera proxy pozwalający na nawiązanie połączenia punkt-punkt między komputerami w sieciach wewnętrznych i zewnętrznych.

## STAN OCHRONY

Aktualny stan ochrony podsumowujący stopień bezpieczeństwa komputera.

## SZABLON POWIADOMIENIA

Szablon, na podstawie którego generowane jest powiadomienie o wykryciu zainfekowanego obiektu podczas skanowania. Szablon powiadamiania zawiera ustawienia dotyczące trybu powiadamiania, sposobu rozsyłania oraz treści wysyłanej wiadomości.

## Ś

### ŚLEDZENIE

Uruchamianie aplikacji w trybie diagnostycznym; po wykonaniu każdego polecenia działanie aplikacji jest wstrzymywane i wyświetlany jest wynik wykonania tego polecenia.

## T

### TECHNOLOGIA ICHECKER

iChecker to technologia, która zwiększa szybkość skanowania antywirusowego poprzez wykluczenie obiektów, które nie były modyfikowane od ostatniego skanowania bez zmiany parametrów skanowania (antywirusowa baza danych oraz ustawienia). Informacja o każdym pliku jest przechowywana w specjalnej bazie danych. Technologia ta jest używana zarówno w ochronie w czasie rzeczywistym, jak i podczas skanowania na żądanie.

Na przykład, do archiwum skanowanego przez aplikację Kaspersky Lab został przypisany stan niezainfekowane. Następnym razem aplikacja pominie to archiwum, chyba że zostało ono zmodyfikowane lub zmieniono ustawienia skanowania. Program powtórnie przeskanuje archiwum, jeżeli na skutek dodania nowego obiektu zmieniła się jego struktura, zmieniono ustawienia skanowania lub zostały zaktualizowane bazy danych aplikacji.

Ograniczenia technologii iChecker:

- nie obsługuje dużych plików, ponieważ przeskanowanie pliku zajmuje mniej czasu niż sprawdzenie, czy został on zmodyfikowany od ostatniego skanowania;
- działa ona tylko z niektórymi formatami (**EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR**).

## U

### UAKTUALNIENIA KRYTYCZNE

Uaktualnienia krytyczne modułów aplikacji firmy Kaspersky Lab.

### USŁUGA NAZWY DOMENOWEJ (DNS)

Rozproszony system konwertowania nazw hosta (komputer lub inne urządzenie sieciowe) na adresy IP. Usługa DNS działa w sieciach TCP/IP. DNS może również przechowywać i przetwarzać zapytania odwrotne, poprzez określenie nazwy hosta po jego adresie IP (wpis PTR). Rozwiązanie nazw DNS jest często wykonywane przez aplikacje sieciowe, nie przez użytkowników.

### USTAWIENIA APLIKACJI

Ustawienia aplikacji, które są wspólne dla wszystkich typów zadań, odpowiadające za działanie aplikacji jako całości, np. ustawienia wydajności aplikacji, raportów, przechowywania kopii zapasowej.

## USTAWIENIA ZADANIA

Ustawienia aplikacji, które są określone dla każdego typu zadania.

## USUWANIE OBIEKTU

Metoda przetwarzania obiektów, która skutkuje jego fizycznym usunięciem z pierwotnej lokalizacji (dysku twardego, foldera, zasobu sieciowego). Zalecamy stosowanie tej metody do obiektów, które z jakiegoś powodu nie mogą zostać wyleczone.

## W

### WIADOMOŚĆ WULGARNĄ

Wiadomość e-mail zawierająca obraźliwy język.

### WIRUS SEKTORA STARTOWEGO

Wirus infekujący sektory startowe dysku twardego komputera. Wirus wymusza na systemie, aby załadował go do pamięci podczas powtórnego uruchomienia oraz przekazał kontrolę kodowi wirusa zamiast kodowi pierwotnego programu rozruchowego.

### WYKLUCZENIE

Wykluczenie to obiekt wykluczony ze skanowania przez aplikację firmy Kaspersky Lab. Możliwe jest wykluczanie z obszaru skanowania określonych formatów plików, użycie masek plików, wykluczanie określonych obszarów (na przykład: folderu lub programu), wykluczanie procesów programu lub obiektów według stanu przydzielonego do nich podczas skanowania. Do każdego zadania można przydzielić zestaw wykluczeń.

## Z

### ZADANIE

Funkcje wykonywane przez aplikację Kaspersky Lab zaimplementowane są w postaci zadań, na przykład: **Ochrona plików w czasie rzeczywistym**, **Pełne skanowanie komputera**, **Aktualizacja baz danych**.

### ZAINFEKOWANY OBIEKT

Obiekt zawierający szkodliwy kod. Zostaje on rozpoznany, gdy część kodu pokrywa się z częścią kodu znanego zagrożenia. Kaspersky Lab nie zaleca korzystania z takich obiektów, ponieważ mogą prowadzić do zainfekowania komputera.

### ZAUFAANY PROCES

Proces programu, którego operacje plikowe nie są monitorowane przez aplikację firmy Kaspersky Lab w trybie ochrony w czasie rzeczywistym. Innymi słowy, nie będą skanowane żadne obiekty uruchomione, otwarte lub zapisane przez zaufany proces.

### ZRZUT PAMIĘCI

Zawartość pamięci uruchomionego procesu lub całej pamięci RAM systemu w określonym czasie.

# KASPERSKY LAB ZAO

Kaspersky Lab jest znaną na całym świecie firmą zajmującą się tworzeniem oprogramowania do ochrony komputerów przed wirusami, szkodliwymi programami, spamem, atakami sieciowymi i hakerskimi oraz innymi zagrożeniami.

W 2008 roku firma Kaspersky Lab zajęła miejsce wśród czwórki czołowych producentów światowej klasy oprogramowania do ochrony danych (według rankingu IDC Worldwide Endpoint Security Revenue by Vendor). Według badań rynkowych TGI-Russia 2009 zrealizowanych przez agencję badawczą COMCON, Kaspersky Lab jest preferowanym dostawcą oprogramowania chroniącego komputery w Rosji.

Firma Kaspersky Lab została założona w 1997 roku w Rosji. Obecnie Kaspersky Lab jest międzynarodową grupą firm z główną siedzibą w Moskwie i pięcioma regionalnymi oddziałami zarządzającymi aktywnością firmy w Rosji, Europie Zachodniej i Wschodniej, na Bliskim wschodzie, w Afryce, Ameryce Północnej i Południowej, Japonii, Chinach i innych krajach Dalekiego wschodu. Firma zatrudnia ponad 2000 wykwalifikowanych specjalistów.

**Produkty.** Produkty firmy Kaspersky Lab zapewniają ochronę wszystkich systemów—począwszy od komputerów domowych aż po sieci dużych korporacji.

Linia produktów dla domu i małych biur obejmuje oprogramowanie antywirusowe dla komputerów stacjonarnych, laptopów, PDA oraz smartfonów i innych urządzeń mobilnych.

Ponadto firma oferuje także aplikacje i usługi do ochrony stacji roboczych, serwerów plików i serwerów sieciowych, bram pocztowych oraz zapór sieciowych. W połączeniu ze scentralizowanym systemem zarządzania Kaspersky Lab rozwiązania te zapewniają firmom i organizacjom efektywną ochronę przed zagrożeniami komputerowymi. Produkty Kaspersky Lab posiadają certyfikaty głównych laboratoriów testujących, są kompatybilne z wieloma programami komputerowymi oraz są zoptymalizowane z myślą o działaniu na wielu platformach sprzętowych.

Analitycy wirusów Kaspersky Lab pracują przez dwadzieścia cztery godziny na dobę. Każdego dnia odkrywają oni tysiące nowych zagrożeń oraz tworzą narzędzia do ich wykrywania i leczenia, które następnie umieszczają w bazach danych wykorzystywanych przez aplikacje firmy Kaspersky Lab. *Firma Kaspersky Lab uaktualnia antywirusowe bazy danych raz na godzinę, a antyspamowe bazy danych co 5 minut.*

**Technologie.** Wiele technologii, które są obecnie nieodłączną częścią nowoczesnych narzędzi antywirusowych, zostało stworzonych przez Kaspersky Lab. To nie przypadek, że wielu innych producentów oprogramowania używa w swoich produktach silnika Kaspersky Anti-Virus. Należą do nich: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Izrael), Clearswift (Wielka Brytania), CommuniGate Systems (USA), Critical Path (Irlandia), D-Link (Tajwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Francja), NETGEAR (USA), Parallels (Rosja), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Tajwan). Wiele innowacyjnych technologii naszej firmy zostało opatentowanych.

**Osiągnięcia.** Przez lata firma Kaspersky Lab otrzymała setki nagród i wyróżnień za swoje zasługi w walce z zagrożeniami komputerowymi. Na przykład w 2010 roku program Kaspersky Anti-Virus otrzymał kilka najwyższych nagród Advanced+ w teście przeprowadzonym przez AV-Comparatives, szanowane austriackie laboratorium antywirusowe. Jednakże największym osiągnięciem Kaspersky Lab jest zaufanie i lojalność użytkowników na całym świecie. Nasze produkty i technologie chronią ponad 300 milionów użytkowników oraz ponad 200,000 klientów korporacyjnych.

Oficjalna strona Kaspersky Lab:

<http://www.kaspersky.pl>

Encyklopedia Wirusów:

<http://www.viruslist.pl>

Laboratorium antywirusowe:

[nowywirus@kaspersky.pl](mailto:nowywirus@kaspersky.pl) (tylko do wysyłania podejrzanych plików w archiwach)

<http://support.kaspersky.com/virlab/helpdesk.html?LANG=pl> (do wysyłania pytań do analityków wirusów)

Forum internetowe Kaspersky Lab

<http://forum.kaspersky.com>

# INFORMACJE O KODZIE FIRM TRZECICH

Informacje o kodzie firm trzecich znajdują się w pliku o nazwie legal\_notices.txt przechowywanym w folderze instalacyjnym aplikacji.

# INDEKS

## A

Aktualizacja	
cofanie ostatniej aktualizacji .....	78
serwer proxy .....	79
ustawienia regionalne .....	76
źródło uaktualnień .....	75
Aktualizowanie	
z foldera lokalnego .....	76
Analiza heurystyczna	
Ochrona plików .....	83
Ochrona poczty .....	88
Ochrona WWW .....	95
Autoochrona programu .....	111

## B

Baza adresów phishingowych	
Ochrona komunikatorów .....	98
Ochrona WWW .....	93

## D

Dezinstalacja	
aplikacja .....	25
Dysk ratunkowy .....	53

## E

EICAR .....	129
-------------	-----

## F

Folder instalacyjny .....	19
---------------------------	----

## I

Ikona obszaru powiadomień paska zadań .....	29
---	----

## K

Kaspersky URL Advisor	
Ochrona WWW .....	93
Klawiatura wirtualna .....	50
Konfiguracja przeglądarki .....	118
Kwarantanna i Kopia zapasowa .....	112

## L

Licencja	
aktywowanie aplikacji .....	43
Umowa licencyjna .....	27

## M

Menu kontekstowe .....	30
------------------------	----

## O

Obszar ochrony	
Ochrona komunikatorów .....	97

Ochrona plików .....	81
Ochrona poczty .....	87
Ochrona WWW .....	96
Ochrona komunikatorów	
baza adresów phishingowych .....	98
obszar ochrony .....	97
Ochrona plików	
analiza heurystyczna .....	83
obszar ochrony .....	81
optymalizacja skanowania .....	85
poziom ochrony .....	82
reakcja na zagrożenie .....	83
skanowanie plików złożonych .....	84
technologia skanowania .....	83
tryb skanowania .....	82
wstrzymywanie .....	80
Ochrona poczty	
analiza heurystyczna .....	88
filtrowanie załączników .....	88
obszar ochrony .....	87
poziom ochrony .....	92
reakcja na zagrożenie .....	88
skanowanie plików złożonych .....	89
Ochrona proaktywna	
grupa zaufanych aplikacji .....	99
lista niebezpiecznej aktywności .....	99
reguła monitorowania niebezpiecznej aktywności .....	100
Ochrona WWW	
analiza heurystyczna .....	95
baza adresów phishingowych .....	93
Kaspersky URL Advisor .....	93
obszar ochrony .....	96
optymalizacja skanowania .....	96
poziom ochrony .....	92
reakcja na zagrożenie .....	92
Odnawianie licencji .....	44
Ograniczanie dostępu do aplikacji .....	65
Okno główne aplikacji .....	31
<b>P</b>	
Powiadomienia .....	45
dostarczanie powiadomień przy użyciu e-mail .....	126
typy powiadomień .....	126
wyłączanie .....	125
wyłączanie sygnału dźwiękowego .....	126
Poziom ochrony	
Ochrona plików .....	82
Ochrona poczty .....	92
Ochrona WWW .....	92
Przywracanie ustawień domyślnych .....	57
<b>R</b>	
Raporty	
filtrowanie .....	121
wybieranie składnika lub zadania .....	121
wyszukiwanie zdarzeń .....	122
zapisywanie do pliku .....	122
Reakcja na zagrożenie	
Ochrona plików .....	83
Ochrona poczty .....	88
Ochrona WWW .....	92
skanowanie antywirusowe .....	71

**S**

Sieć	
monitorowane porty .....	105
połączenia szyfrowane .....	103
Skanowanie	
automatyczne uruchamianie pominiętego zadania .....	69
działanie podejmowane na wykrytym obiekcie .....	71
konto użytkownika .....	71
optymalizacja skanowania .....	73
poziom ochrony .....	68
skanowanie plików złożonych .....	72
skanowanie w poszukiwaniu luk .....	74
technologie skanowania .....	71
terminarz .....	69
typy obiektów przeznaczonych do skanowania .....	71
Śledzenie	
przesyłanie wyników śledzenia .....	133
tworzenie pliku śledzenia .....	133
Strefa zaufana	
reguły wykluczeń .....	107
zaufane aplikacje .....	107

**T**

Terminarz	
aktualizacja .....	77
skanowanie antywirusowe .....	69

**W**

Wydajność komputera .....	109
Wyłączanie / włączanie ochrony w czasie rzeczywistym .....	40