mks_vir – szczegółowe ustawienia pakietu mks_vir

Ochrona → Pliki:

Aktywuj ochronę antywirusową – opcja aktywuje najważniejszy moduł ochronny pakietu **mks_vir**

Po znalezieniu zagrożenia – umożliwia wybranie akcji, która ma być wykonana w przypadku znalezienia zagrożenia przez moduł ochrony antywirusowej; do wyboru są następujące możliwości:

- **Usuń zagrożenie** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowany plik
- **Skasuj plik** – kasuje zainfekowany plik
- **Przenieś plik do kwarantanny** – przenosi zainfekowany plik do folderu kwarantanny **mks_vir**
- **Pytaj użytkownika** – blokuje zainfekowany plik i wyświetla okno, gdzie można wybrać odpowiednią akcję lub wysłać plik do działu analiz **mks_vir**

Włącz powiadomienia dla akcji automatycznych – włącza wyświetlanie okien powiadomień modułu ochrony plików w przypadku znalezienia zagrożenia i wykonania wybranej akcji automatycznej (akcje automatyczne to „Usuń zagrożenie”, „Skasuj plik” i „Przenieś plik do kwarantanny”)

Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Ustawienia dodatkowe:

- **Włącz skanowanie archiwów** – włącza możliwość skanowania zawartości plików typu ZIP, RAR, 7Z itp.
- **Włącz skanowanie zasobów sieciowych** – włącza sprawdzanie podłączonych zasobów sieciowych; należy mieć na uwadze, że aktywność tej opcji może spowolnić dostęp do plików znajdujących się na podłączonych zasobach sieciowych
- **Skanuj tylko nosiciele** – opcja powoduje, że sprawdzane są tylko pliki będące domyślnymi nosicielami zagrożeń, jak np. pliki EXE, COM, JS, VBS itp.
- **Blokuj autostart na nośnikach USB** – uniemożliwia automatyczne uruchomienie z podłączanych pendrive potencjalnych zagrożeń
- **Optymalizuj dostęp do zasobów OneDrive** – optymalizuje skanowania obiektów przechowywanych w chmurze OneDrive

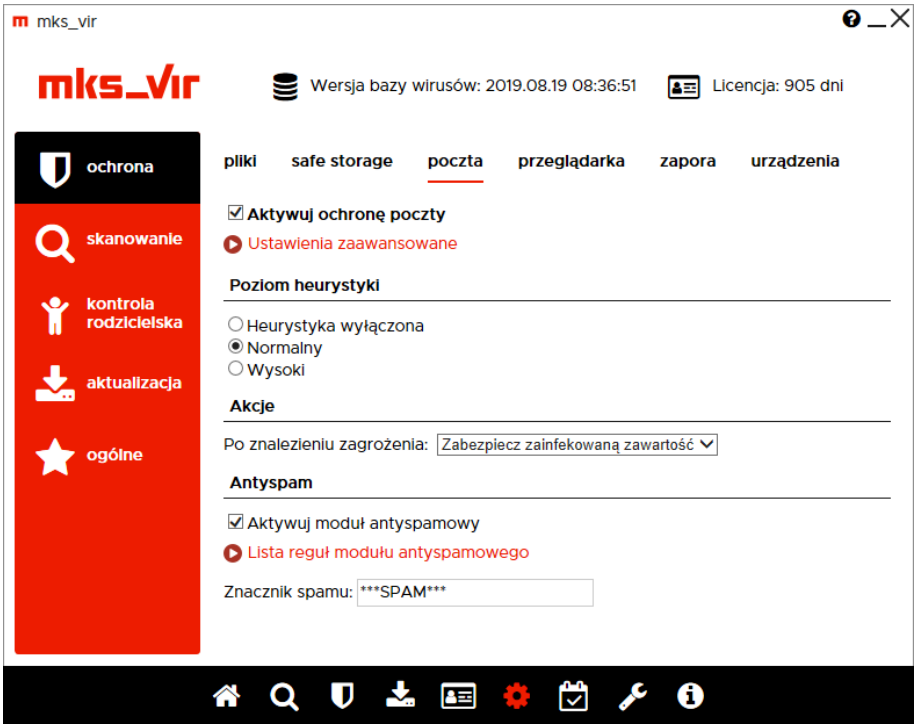
Ochrona → SafeStorage:

Włącz aktywną ochronę danych *SafeStorage* – włącza mechanizm ochrony danych, szczególnie przed zagrożeniami szyfrującymi (np. Cryptolocker)

Chroń również pliki na zasobach sieciowych – włącza ochronę danych na podłączonych zasobach sieciowych

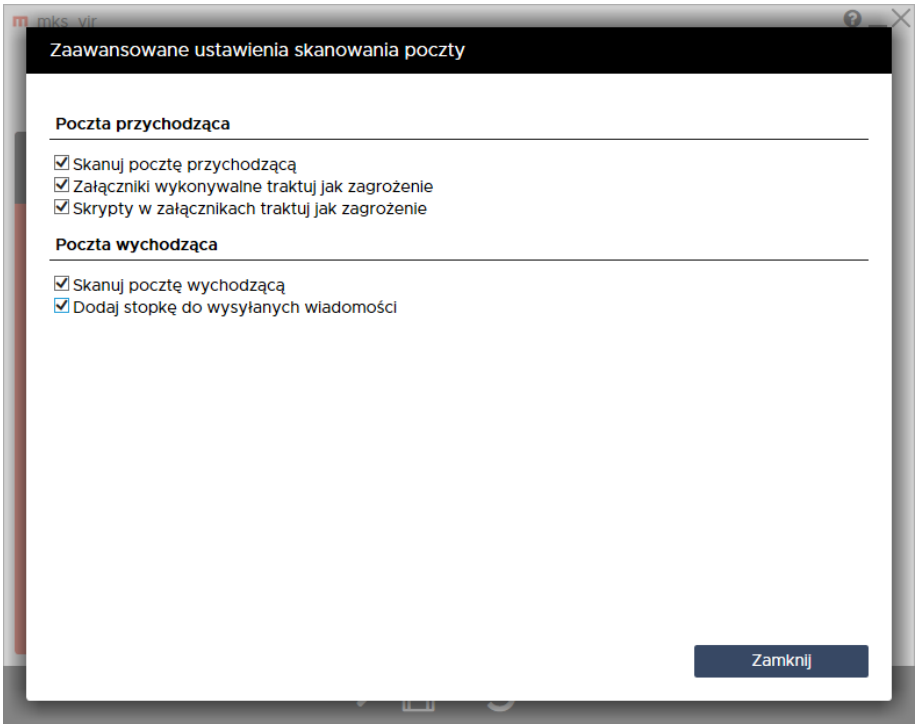
Automatycznie wybieraj foldery chronione przez *SafeStorage* – przy włączonej opcji program domyślnie chroni dane na wszystkich dyskach lokalnych dostępnych w komputerze; jej wyłączenie umożliwia wybranie, które foldery mają być chronione

Ochrona → Poczta:



Aktywuj ochronę poczty – aktywuje moduł ochrony pobieranej i wysyłanej poczty; obsługiwane protokoły to POP3, IMAP i SMTP (w wersji zwykłej i szyfrowanej)

Ustawienia zaawansowane – umożliwiają dostrojenie ustawień dla pobieranej i wysyłanej poczty:



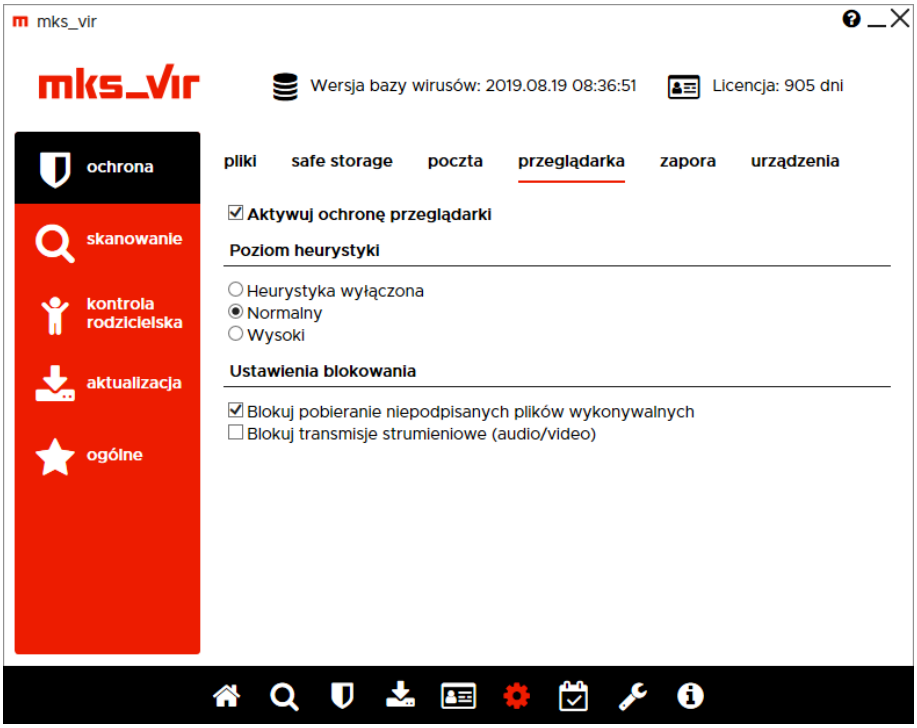
Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Akcje – umożliwia wybranie automatycznej akcji, która ma być wykonana w przypadku znalezienia zagrożenia przez moduł ochrony poczty; do wyboru są następujące możliwości:

- **Zabezpiecz zainfekowaną zawartość** – zainfekowana wiadomość zostaje obudowana dla bezpieczeństwa - orginalny email znajduje się wtedy z załączniku takiej wiadomości
- **Usuń zainfekowaną zawartość** – zawartość email, będąca nośnikiem infekcji zostaje skasowana, zaś do odbiorcy zostaje dostarczona informacja o znalezionej infekcji

Antyspam – moduł do znakowania wiadomości-śmieci

Ochrona → Przeglądarka:



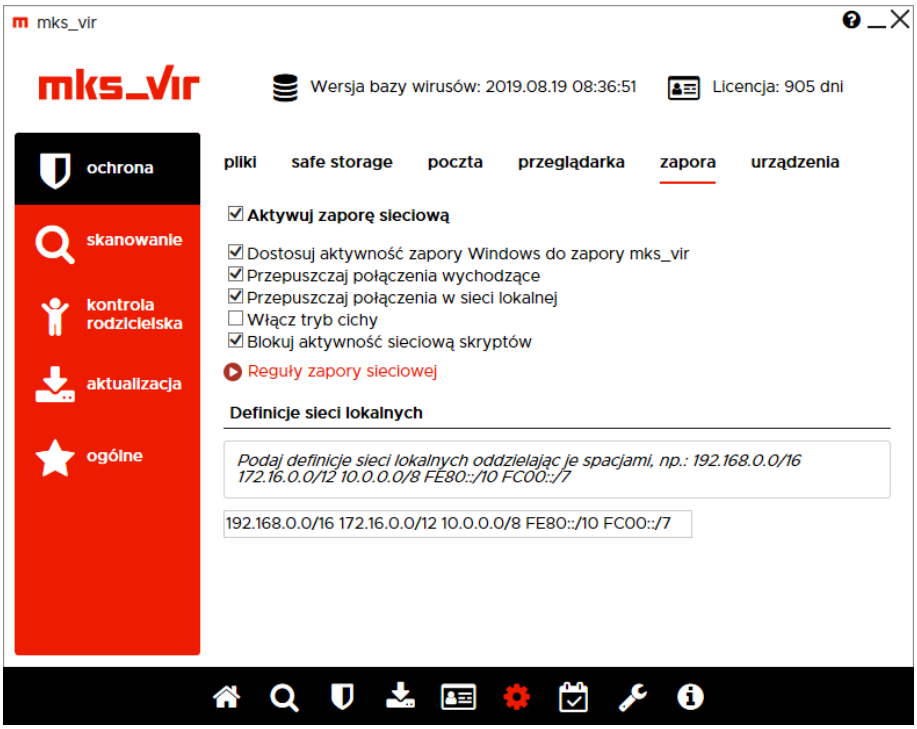
Aktywuj ochronę przeglądarki – aktywuje ochronę antywirusową dla przeglądarek; obsługiwane protokoły to HTTP i HTTPS

Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Ustawienia blokowania

- **Blokuj pobieranie niepodpisanych plików wykonywalnych** – włączenie tej opcji powoduje, że przy próbie pobrania niepodpisanych cyfrowo plików wykonywalnych (czyli takich, dla których nie da się automatycznie zweryfikować poprawności pochodzenia pliku), zostanie wyświetlone odpowiednie ostrzeżenie; użytkownik będzie mógł wtedy podjąć decyzję, czy dany plik pobrać, czy jednak nie
- **Blokuj transmisje strumieniowe (audio/video)** – włączenie tej opcji powoduje blokowanie wszelkiego rodzaju transmisji strumieniowych (co na przykład uniemożliwia słuchanie stacji radiowych przez internet)

Ochrona → Zapora:



Aktywuj zaporę sieciową – aktywuje moduł ochrony sieci

Dostosuj aktywność zapory Windows do zapory mks_vir – aktywność tej opcji umożliwia automatyczne przełączanie aktywności zapory Windows w zależności od aktywności *zapory mks_vir*; aktwacja *zapory mks_vir* wyłącza zaporę Windows, zaś dezaktywacja *zapory mks_vir* włącza zaporę Windows, dzięki czemu w systemie stale jest aktywna zapora

Przepuszczaj połączenia wychodzące – dopuszcza wszystkie połączenia wychodzące; większość połączeń sieciowych, to połączenia wychodzące (np. typowa aktywność przeglądarki w czasie surfowania po internecie) i takie połączenia są w ogromnej większości bezpieczne

Przepuszczaj połączenia w sieci lokalnej – aktywność tej opcji powoduje, że wszelkie połączenia nawiązywane w sieci lokalnej (połączenia wychodzące i przychodzące) są przepuszczane

Włącz tryb cichy – włącza tryb działania zapory eliminujący ew. zapytania o przepuszczenie lub zablokowanie połączenia; połączenia dla których pojawiałyby się zapytania będą blokowane

Blokuj aktywność sieciową skryptów – opcja ta blokuje możliwość łączenia się z różnymi witrynami lub pobierania plików, przez różnego rodzaju skrypty (JS, VBS itp.)

Reguły zapory sieciowej – umożliwia definiowanie własnych reguł przepuszczających lub blokujących ruch sieciowy różnych aplikacji

Definicje sieci lokalnych – domyślnie podane są tu standardowe definicje adresów i masek dla sieci lokalnych; jeśli używana jest inna definicja własnej sieci lokalnej, należy ją tu podać, aby wszelkie reguły dotyczące sieci (w tym rozróżnienie – sieć lokalna czy nie) miały zastosowanie; definicje podajemy używając skróconego formatu maski, krótki opis jak korzystać z takich masek jest podany tu:

`https://pl.wikipedia.org/wiki/Maska_podsieci`

Ochrona → Urządzenia:

Aktywuj kontrolę urządzeń USB – aktywuje moduł kontroli urządzeń USB

Ustawienia – umożliwia konfigurację modułu kontroli urządzeń USB

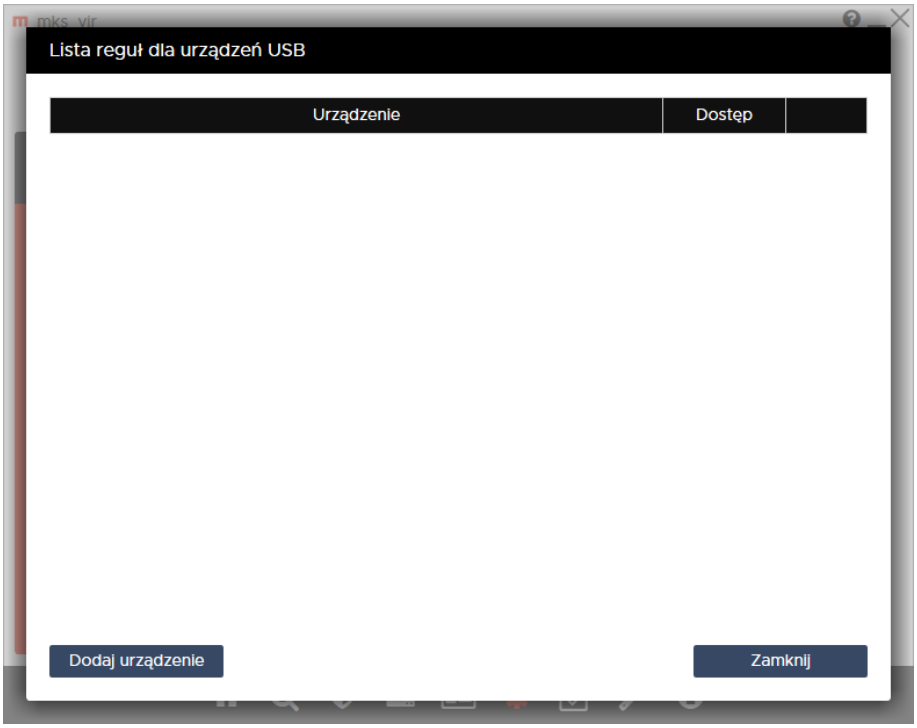
- **Gdy brak reguły** – umożliwia wybranie akcji, która ma być wykonana w przypadku podłączenia nowego urządzenia USB, czyli takiego dla którego nie jest zdefiniowana odpowiednia reguła (dopuszczająca lub blokująca); do wyboru są następujące możliwości:
  - **Blokuj** – blokuje każde nowe podłączane urządzenie USB
  - **Dopuść** – dopuszcza każde nowe podłączane urządzenie USB
  - **Pytaj użytkownika** – wyświetla okno z pytaniem o zablokowanie lub dopuszczenie nowo podłączanego urządzenia USB; wybranie jednej lub drugiej możliwości tworzy odpowiednią regułę dla danego urządzenia USB
- **Dopuszczaj urządzenia podłączone przy pierwszej aktywacji** – automatycznie dopuszcza urządzenia USB podłączone do komputera w momencie aktywacji modułu kontroli urządzeń USB
- **Twórz raporty o dopuszczonych urządzeniach** – włącza tworzenie raportów o podłączanych do komputera urządzeniach USB, dla których istnieją reguły dopuszczające lub wybraną akcją jest „Dopuść” (przy podłączaniu nowych urządzeń USB)

Reguły – umożliwia definiowanie lub modyfikację reguł blokujacych lub dopuszczajacych podłączane urządzenia USB

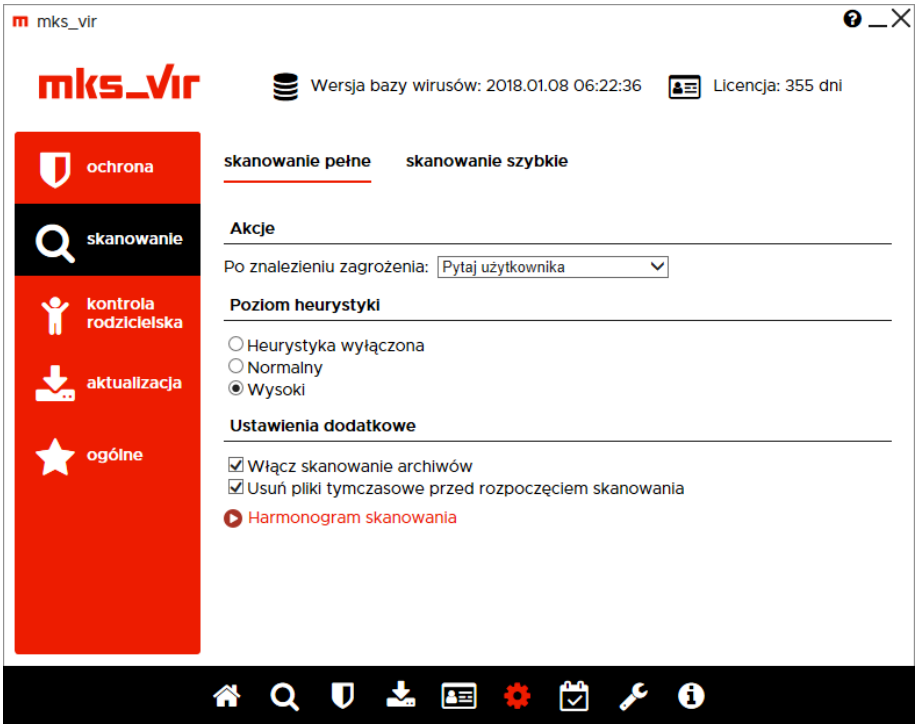
- **Dopuszczaj myszy i klawiatury** – automatycznie dopuszcza podłączane do komputera nowe klawiatury USB lub myszy USB

- **Dopuszczaj drukarki** – automatycznie dopuszcza podłączane do komputera nowe drukarki USB
- **Dopuszczaj karty sieciowe/Bluetooth** – automatycznie dopuszcza podłączane do komputera nowe karty sieciowe USB lub karty Bluetooth USB

Pokaż listę reguł dla urządzeń USB – umożliwia definiowanie lub modyfikację własnych reguł blokujących lub dopuszczających dla podłączanych do komputera urządzeń USB:



Skanowanie → Skanowanie pełne:



Akcje – umożliwia wybranie akcji, która będzie wykonywania po zakończeniu pełnego skanowania komputera, do wyboru są następujące możliwości:

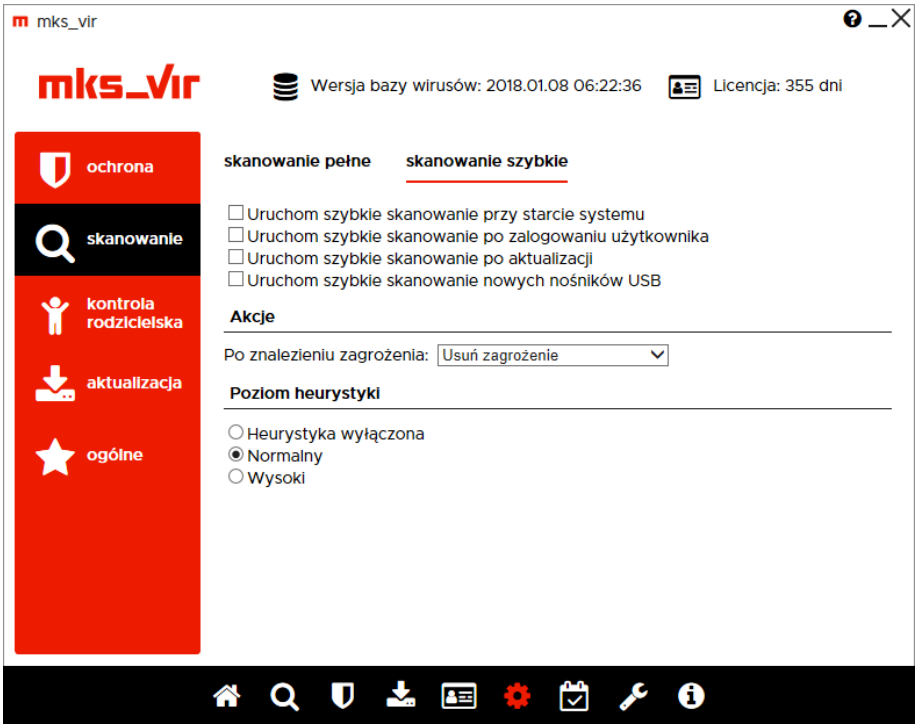
- **Usuń zagrożenia** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- **Skasuj plik** – kasuje zainfekowane pliki
- **Przenieś do kwarantanny** – przenosi zainfekowane pliki do folderu kwarantanny **mks_vir**
- **Pytaj użytkownika** – po zakończeniu skanowania ew. znalezione zagrożenia zostaną wyświetlone w tabeli z możliwością wyboru akcji, które dla nich będą miały być wykonane

Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Ustawienia dodatkowe:

- **Włącz skanowanie archiwów** – włącza możliwość skanowania zawartości plików typu ZIP, RAR, 7Z itp.
- **Usuń pliki tymczasowe przed rozpoczęciem skanowania** – usuwa pliki znajdujące się w folderach tymczasowych systemu i użytkowników przed rozpoczęciem skanowania
- **Harmonogram skanowania** – umożliwia określenie, kiedy ma się automatycznie rozpocząć skanowanie dysków komputera

Skanowanie → Skanowanie szybkie:



Skanowanie szybkie, które skanuje zawartość pamięci uruchomionych procesów i serwisów, może być automatycznie wykonywane w następujących przypadkach:

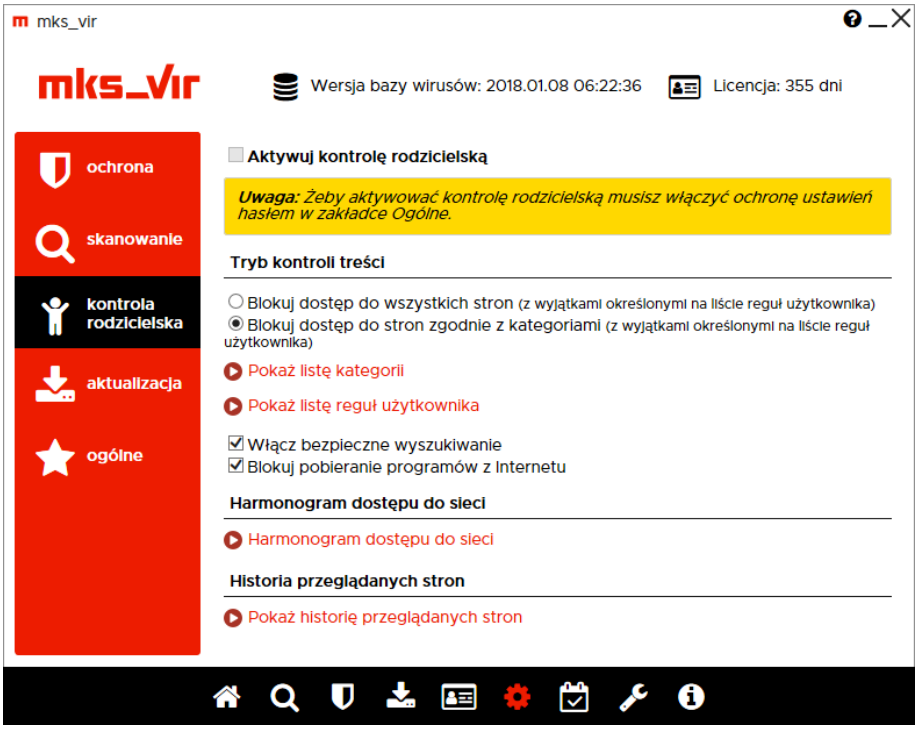
- **przy starcie systemu**
- **po zalogowaniu użytkownika**
- **po aktualizacji programu mks_vir**
- **po podłączeniu nośnika USB** – skanowana jest wtedy zawartość takiego nośnika

Akcje – umożliwia wybranie akcji, która będzie wykonywania po znalezieniu zagrożenia w czasie szybkiego skanowania, do wyboru są następujące możliwości:

- **Usuń zagrożenia** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- **Skasuj plik** – kasuje zainfekowane pliki
- **Przenieś do kwarantanny** – przenosi zainfekowane pliki do folderu kwarantanny **mks_vir**
- **Pytaj użytkownika** – po zakończeniu skanowania ew. znalezione zagrożenia zostaną wyświetlone w tabeli z możliwością wyboru akcji, które dla nich będą miały być wykonane

Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

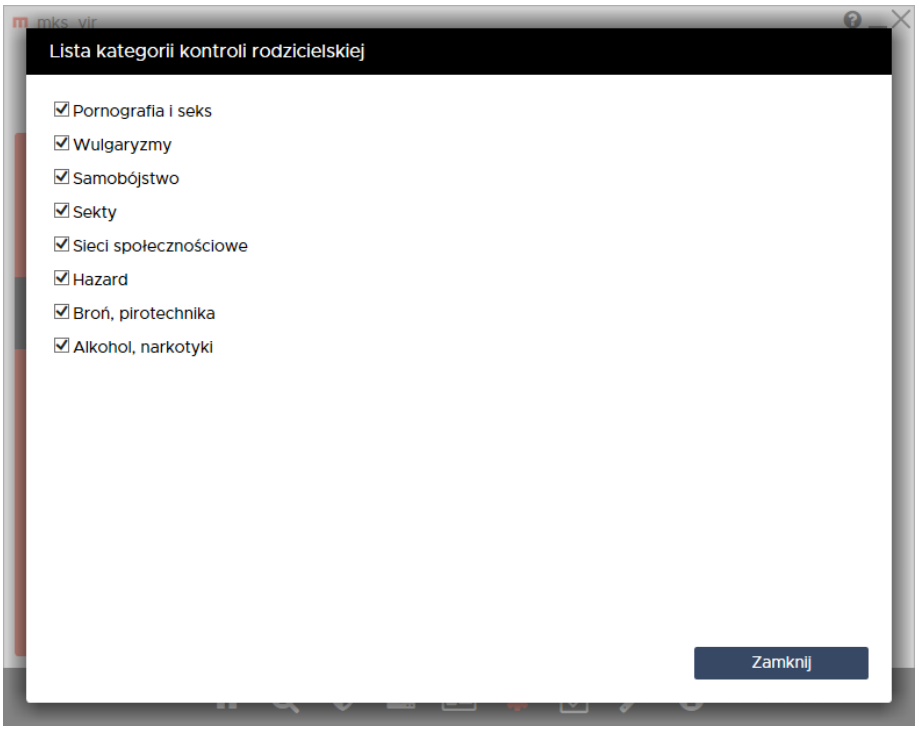
Kontrola rodzicielska:



Aktywuj kontrolę rodzicielską – uaktywnia moduł kontroli rodzicielskiej; aktywacja kontroli rodzicielskiej wymaga wcześniejszego ustawienia ochrony ustawień za pomocą hasła (w sekcji „Ogólne” ustawień)

Tryb kontroli treści – umożliwia określenie sposobu działania modułu kontroli rodzicielskiej:

- **Blokuj dostęp do wszystkich stron** – w tym trybie blokowane będą wszystkie strony internetowe, za wyjątkiem tych podanych w regułach użytkownika
- **Blokuj dostęp do stron zgodnie z kategoriami** – w tym trybie strony będą blokowane lub przepuszczane zależnie od analizy zawartości stron zgodnie z regułami zdefiniowanymi dla poszczególnych kategorii, aktywność poszczególnych kategorii można zmieniać po wybraniu „Pokaż listę kategorii”:

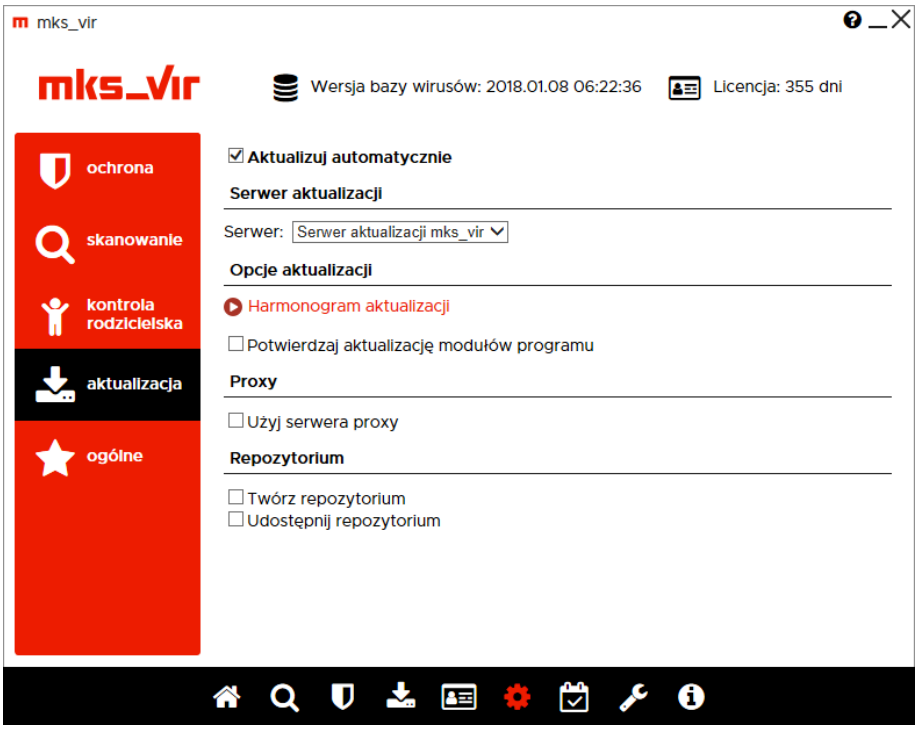


- **Pokaż listę reguł użytkownika** – umożliwia zdefiniowane własnych reguł przepuszczających lub blokujących w oparciu o adresy lub frazy (słowa kluczowe)
- **Włącz bezpieczne wyszukiwanie** – wymusza włączenie trybu bezpiecznego wyszukiwania (*SafeSearch*) w wyszukiwarkach
- **Blokuj pobieranie programów z Internetu** – uniemożliwia pobieranie programów z witryn internetowych

Harmonogram dostępu do sieci – umożliwia określenie, kiedy użytkownicy mają mieć dostęp do Internetu, a kiedy nie; aktywność tej opcji nie ma wpływu na dostępność zasobów w sieciach lokalnych

Pokaż historię przeglądanych stron – umożliwia przejrzenie adresów stron przeglądanych przez użytkowników oraz zbudowanie na ich podstawie reguł przepuszczających lub blokujących dane strony

Aktualizacja:



Aktualizuj automatycznie – wymusza sprawdzanie co jakiś czas (jest on określany częściowo losowo w granicach kilkudziesięciu minut) dostępności aktualizacji i przy ich dostępności aktualizuje program **mks_vir**

Serwer – umożliwia wybranie źródła aktualizacji, do wyboru są następujące możliwości:

- **Serwer aktualizacji mks_vir** – aktualizacje odbywają się bezpośrednio z serwerów aktualizacyjnych **mks_vir**
- **Inny serwer HTTP** – aktualizacje będą się odbywały z udostępnionego za pomocą protokołu HTTP repozytorium (np. tworzonego, aktualizowanego i udostępnianego przez program **mks_vir** nie zarządzany z poziomu programu **mks_vir administrator**)
- **Zasób lokalny** – aktualizacje będą się odbywały z repozytorium dostępnego na lokalnym nośniku, np. na pendrive; opcja może mieć znaczenie dla sieci całkowicie odciętych od Internetu

Opcje aktualizacji:

- **Harmonogram aktualizacji** – umożliwia określenie, kiedy ma być bezwzględnie wymuszana aktualizacja programu **mks_vir**
- **Potwierdzaj aktualizację modułów programu** – włączenie tej opcji powoduje, że na stacjach w przypadku konieczności aktualizacji modułów programowych (a więc innych niż bazy antywirusowe i silniki skanujące) pojawi się pytanie, czy tego dokonać; w niektórych przypadkach samoczynna aktualizacja takich elementów programu może chwilowo zaburzać działanie innych programów

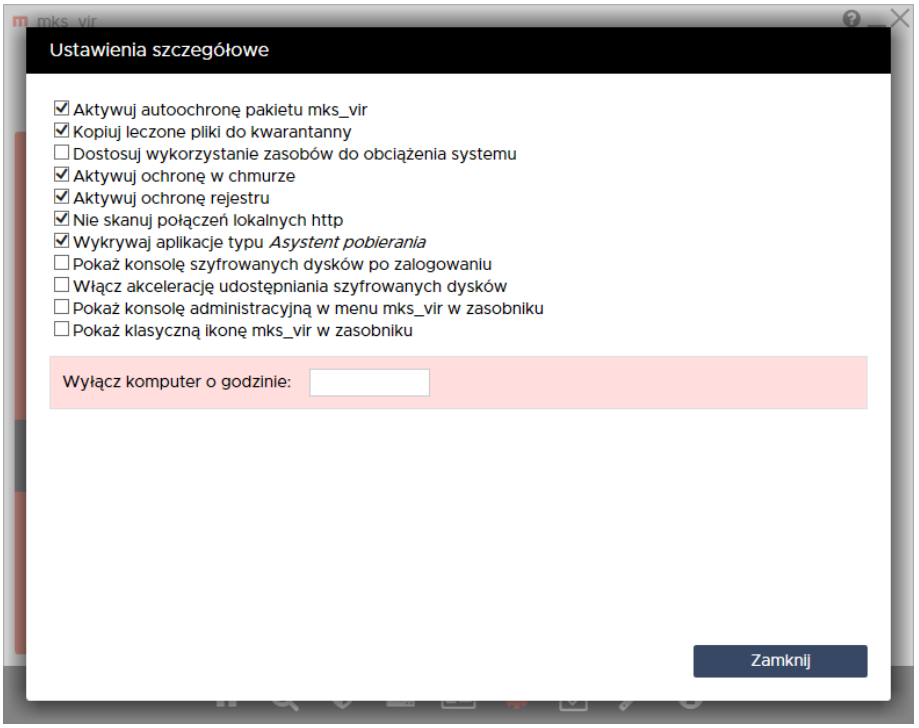
Proxy – umożliwia automatyczne wykorzystanie serwerów proxy, jeśli te są dostępne

Repozytorium – umożliwia tworzenie, aktualizację i udostępnienie repozytorium w sieci za pomocą protokołu HTTP

- **Twórz repozytorium** – tworzy i aktualizuje repozytorium
- **Udostępnij repozytorium** – umożliwia udostępnienie repozytorium po protokole HTTP na wybranym porcie, który podaje się po włączeniu tej opcji

Ogólne:

Ustawienia szczegółowe – umożliwiają dostrojenie niektórych elementów programu **mks_vir**, a także ustalenie o której godzinie stacje powinny zostać wyłączone:



Globalne wykluczenia ochrony – umożliwia zdefiniowanie obiektów, dla których nie będzie działała żadna ochrona, korzystanie z tych ustawień wymaga dużej rozwagi:

- **Lista wykluczonych domen internetowych** – umożliwia zdefiniowane adresów, dla których nie będą działały moduły ochrony przeglądarki i kontroli rodzicielskiej programu **mks_vir**
- **Lista wykluczonych plików i folderów** – umożliwia zdefiniowane obiektów (plików lub folderów), dla których nie będzie działał moduł ochrony plików programu **mks_vir**

Porty i protokoły – umożliwia zdefiniowane dla których portów mają działać moduły ochrony poczty, ochrony przeglądarki i kontroli rodzicielskiej oraz jakie porty mają być w ogóle wyłączone spod kontroli, również w zaporze programu **mks_vir**; definiuje się je w **Tabeli skanowanych i wykluczonych portów i protokołów**

Folder danych – umożliwia określenie innego niż domyślny folderu dla dużych ilości danych (kwarantanna, *SafeStorage*, kopie zapasowe, szyfrowane dyski); zdefiniowanie innego niż domyślny folderu wymaga, by dysk twardy na którym ma się znajdować, był dostępny w komputerze

Przywróć ustawienia domyślne – *przywraca domyślną konfigurację*