

## Wstęp

Serdecznie witamy!

Strażnik AVK to produkt pakietu AntiVirenKit 8, niezmiernie przydatny do ochrony przed wirusami:

Jest stale aktywny w tle i kontroluje wywoływane pliki. Dzieje się to tak szybko, że w trakcie codziennej pracy w ogóle nie zauważymy jego obecności. Jego użycie jest bardzo proste, i możemy powierzyć mu opiekę naszego komputera !


Zaletą takiej kontroli jest fakt, że komputer nie ma dostępu do pliku w którym wykryto infekcję, niezależnie od tego, czy znajduje się na dyskietce, CD-ROMie, czy jako Attachment w e-mail lub jest załadowany przez internet. Zamyka to wirusom wiele dróg infekcji [Użycie strażnika AVK](#)

Życzymy Państwu bezpiecznej i wygodnej pracy ze Strażnikiem AVK.

G DATA Software, lipiec 1998

## **Użycie Strażnika AVK**

Strażnika AVK nie można wyłączać nigdy, bez uzasadnionej przyczyny !

Menu sterowania wywołujemy, klikając symbol  na pasku zadań. Widzimy tam ostatnio sprawdzany plik i ostatnie wykrycie wirusa. Możemy je też ukryć – wróci do paska zadań.

“Zakończ” zamyka menu, ale nie wyłącza STRAŻNIKA!! Nie ma go wtedy w pasku zadań, ale jest dostępny w grupie programowej AntiVirenKit 8.

Funkcję można wyłączyć i wyłączyć w “Konfiguracji...”. Można tu też ustalić wybrane reakcje i obiekty.

## **Konfiguracja Strażnika AVK**

W menu “Konfiguracja Strażnika AVK” ustalamy co ma kontrolować i co robić w przypadku znalezienia wirusa.


Do dyspozycji mamy następujące karty:

- Rozpoznanie
- Typ pliku
- Zapis konfiguracji
- Informacje o Strażniku AVK

## Rozpoznanie

W tej karcie możemy:

- ) Włączyć i wyłączyć funkcję strażnika. Po jej wyłączeniu symbol strażnika będzie przekreślony, dzięki czemu widzimy, że istnieje ryzyko zarażenia. **Nie wyłączajmy Strażnika AVK bez uzasadnionej przyczyny**
- ) Włączyć lub wyłączyć opcję analizy heurystycznej
- ) Ustalić rodzaj reakcji na wypadek wykrycia wirusa. Można spróbować go usunąć, usunąć zarażony plik (**ostrożnie, to oznacza nieodwołalną utratę danych, radzimy użycie innych funkcji!**) lub możemy zdecydować w oknie po wykryciu wirusa, co z nim zrobić.
- ) Poza tym możemy zlecić założenie protokołu

 [\\_powrót do menu](#)

## Typ pliku

W tej karcie wybieramy typ plików do zbadania:

- ) Pliki skompresowane – sprawdza spakowane i zarchiwizowane pliki.
- ) Automatyczne rozpoznanie plików (tryb Smart)  
kontroluje wszystkie zagrożone pliki.
- ) Pliki programowe  
kontroluje pliki programowe
- ) Wszystkie pliki  
analiza wszystkich plików. Znacznie wydłuża czas trwania analizy.
- ) Zdefiniowane przez użytkownika  
Możemy tu nakazać analizę wybranych przez nas typów plików. Wystarczy nanieść pożądane rozszerzenia.

 [\\_powrót do menu](#)

## **Zapis konfiguracji**

W karcie “Konfiguracja” możemy :

a) Importować/eksportować konfigurację jako plik “eksportuj” lub “importuj”. Jeśli zamierzamy pracować z różnymi konfiguracjami, poleca się zapisanie ustawionej raz konfiguracji i w razie potrzeby importowanie jej.

Ta cecha ułatwia konfigurowanie wielu stanowisk w sieci.

b) Chronić hasłem ustawioną konfigurację. Jeśli naniesiemy cokolwiek w oknie “Hasło”, po wywołaniu “Konfiguracji...” komputer spyta o hasło.

Ta cecha uniemożliwia zmianę konfiguracji np. administratorów przez osoby niepowołane przy pracy w sieci.

c) Ustalić, czy strażnik ma działać otwarcie, czy w tle.

 [\\_powrót do menu](#)

## **Informacje o Strażniku AVK**

W karcie “Info“ menu konfiguracji znajdziemy informacje na temat::

- ) Wersji Strażnika AVK
  - ) Wersji bazy wirusowej
  - ) Statystyki przeszukanych plików
- [powrót do menu](#)





