Jak skutecznie filtrować zawartość Internetu

Raport

s@ferinternet.pl dyżurnet.pl NASK CERT POLSKA


s@ferinternet.pl

dyżurnet.pl


NASK

CERT
POLSKA

Jak skutecznie filtrować zawartość Internetu

Raport

przygotowany

przez pracowników projektu Saferinternet.pl:

Izabelę Jończyk, Martynę Różycką, Karola Kurowskiego, Adama Węgłowskiego,

we współpracy z działającym w ramach NASK zespołem CERT Polska

Spis treści

Program Safer Internet

Analiza skuteczności programów chroniących przed nielegalnymi i szkodliwymi treściami w Internecie jest jednym z elementów programu Komisji Europejskiej *Safer Internet*. Jego celem jest podnoszenie świadomości wszystkich użytkowników Internetu, szczególnie tych najmłodszych, w zakresie bezpiecznego i efektywnego korzystania z Sieci oraz nowych technik telekomunikacyjnych. W Polsce program realizowany jest od 1 stycznia 2005 roku przez konsorcjum NASK (Naukowa i Akademicka Sieć Komputerowa) i FDN (Fundacja Dzieci Niczyje). Od 2005 roku działa także powołany przy NASK punkt kontaktowy *Dyżurnet.pl*, który przyjmuje zgłoszenia dotyczące nielegalnych treści w Internecie i podejmuje działania zmierzające do ich usunięcia. Zespół *Dyżurnet.pl* współpracuje z policją, dostawcami usług internetowych, organizacjami rządowymi i pozarządowymi oraz innymi punktami kontaktowymi zrzeszonymi w stowarzyszeniu INHOPE (*The Association of Internet Hotline Providers*). W 2007 roku FDN uruchomiła Helpline.org.pl, który niesie bezpośrednią pomoc w sytuacjach zagrożenia bezpieczeństwa dzieci i młodzieży w Internecie (np. cyberprzemoc, nękanie za pomocą Internetu, kontakt ze szkodliwymi treściami).

Internetowe serwisy projektu:
www.saferinternet.pl
www.dzieckowsieci.pl
www.helpline.org.pl
www.dyzurnet.pl
www.sieciaki.pl
www.przedszkolaki.sieciaki.pl
www.dbi.pl

Nielegalne i szkodliwe treści

W przeciwieństwie do Internetu instytucje wymiaru sprawiedliwości mają ściśle określone granice oddziaływania, co wiąże się z istnieniem odmiennych definicji nielegalnych treści w różnych krajach. Zgodnie z obowiązującym w Polsce prawem zabronione jest publikowanie:

- treści pornograficznych z udziałem małoletniego, treści pornograficznych związanych z prezentowaniem przemocy lub posługiwaniem się zwierzęciem;
- treści propagujących publicznie faszystowski lub inny totalitarny ustrój państwa lub nawołujących do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość;
- treści publicznie znieważających grupę ludności albo poszczególną osobę z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości.

Niezgodne z prawem jest także:

- publiczne prezentowanie treści pornograficznych w taki sposób, że może to narzucić ich odbiór osobie, która sobie tego nie życzy;
- prezentowanie małoletniemu poniżej lat 15 treści pornograficznych lub udostępnianie mu przedmiotów o takim charakterze albo rozpowszechnianie treści pornograficznych w sposób umożliwiający małoletniemu zapoznanie się z nimi.

Zdecydowana większość psychologów jest zdania, że częsty kontakt osób nieletnich z pornografią ma na nie głęboki, wielowymiarowy i szkodliwy wpływ. Treści pornograficzne są źródłem doświadczeń, które przerastają zdolności adaptacyjne

młodych ludzi i dostarczają im wzorców patologicznych zachowań. Kształtują wypaczony i negatywny obraz świata, relacji międzyludzkich (np. instrumentalne traktowanie innych osób), utrwalają fałszywy obraz kobiecości i męskości. W wyniku kontaktu z pornografią może dojść do erotyzacji psychiki dziecka i jego przedwczesnego rozbudzenia seksualnego, a także do wzrostu poziomu niepokoju u dziecka, napięcia, nadpobudliwości psychoruchowej, wystąpienia objawów nerwicowych i depresyjnych[1].

Korelacja między częstotliwością kontaktu z przemocą i twardą pornografią a siłą ich oddziaływania jest dobrze udokumentowana. Im częściej w wieku przedszkolnym i szkolnym dziecko ma kontakt z przemocą w filmach lub grach:

- tym częściej w wieku młodzieńczym i dorosłym narusza prawo;
- tym częściej konflikt z prawem wynika ze stosowania przemocy, tym bardziej jest ona brutalna, zwłaszcza pod wpływem alkoholu;
- tym częściej stosuje ją również w przyszłej rodzinie – wobec małżonka i dzieci;
- tym większa później tendencja do alkoholizmu, rozwiązłości, trywializowania okrucieństwa;
- tym bardziej w życiu dorosłym kobiety są skłonne akceptować przemoc mężczyzn wobec siebie i włączać elementy przemocy w fantazje i zachowania seksualne.

Warto wymienić także szereg innych zagrożeń i przykładów niebezpiecznych treści, z którymi mogą się zetknąć surfujące w Internecie dzieci i młodzież:

- *cyberbulling* – to przemoc polegająca na wyzywaniu, ośmieszaniu, szantażowaniu czy rozprzestrzenianiu kompromitujących materiałów w Sieci przy użyciu technologii informacyjnych i komunikacyjnych (komunikatorów, czatów, stron WWW, blogów, SMSów i MMSów). Z badań agencji Gemius (2007) wynika, że ponad połowa nastoletnich internautów w Polsce, w wieku 12–17 lat, padła ofiarą któregoś z wymienionych aktów cyberprzemocy;
- *grooming* – to uwodzenie dzieci przez osoby dorosłe za pomocą Internetu. Do nawiązania bliskiego kontaktu z dziećmi „cyberłowcy" wykorzystują głównie komunikatory internetowe oraz czaty. Starają się oni nakłonić dzieci do rozmów o seksie, co może być wstępem do dalszego osaczania i molestowania najmłodszych użytkowników. Dorosły, często udając rówieśnika swej ofiary, stopniowo zdobywa jej zaufanie, dane osobowe, zdjęcia, a nieraz staje się „dobrym przyjacielem". Namawia dziecko do oglądania pornografii i nalega na spotkanie w świecie rzeczywistym. Gdy dojdzie do spotkania, dziecko zazwyczaj zostaje wykorzystane seksualnie i nierzadko staje się ofiarą przemysłu pornograficznego;
- treści propagujące ruchy religijne uznane za sekty;
- treści propagujące anoreksję i bulimię jako styl życia, a nie poważną chorobę;
- treści nawołujące do samobójstw lub samookaleczeń;
- treści promujące narkotyki oraz inne używki – najczęściej przez podkreślenie ich rzekomo leczniczych walorów czy wskazanie, że otwierają one człowieka na rzeczywistość duchową.

Testy programów filtrujących

Testy programów filtrujących przeprowadzono w ramach projektu Komisji Europejskiej *Safer Internet*. Celem testów było sprawdzenie skuteczności ochrony mechanicznej dzieci i młodzieży przed szkodliwymi i nielegalnymi treściami w Internecie, a także stworzenie na podstawie otrzymanych wyników wiarygodnego i rzetelnego przewodnika po polskojęzycznych aplikacjach filtrujących. Dobór takiego kryterium językowego wynika z przekonania, że testy programów w polskiej wersji językowej będą miały większą przydatność dla polskich rodziców i nauczycieli (np. ze względu na lepsze zrozumienie ich funkcjonalności).

Wyniki testów prezentujemy w formie niniejszego opracowania. Nie przedstawiamy zestawienia rankingowego, ponieważ naszym zamiarem nie jest promowanie konkretnych aplikacji i rozwiązań technicznych. Pragniemy raczej, aby nasza publikacja umożliwiła rodzicom i nauczycielom dokonanie własnego wyboru, najodpowiedniejszego dla ich wymagań i oczekiwań. Jednocześnie chcemy promować potrzebę edukacji dzieci w zakresie krytycznego korzystania z zasobów internetowych, jak i używania oprogramowania filtrującego.

---

[1] Źródło: Carr J. (2005), Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca, *Dziecko krzywdzone. Zagrożenia dzieci w Internecie,* 13, 11–27, Warszawa: FDN. ■ Kirk J.R., Showers H. R. (1998), *Szkodliwość pornografii,* Gdańsk: HLI-Europa. ■ Quayle E (2005), Pornografia dziecięca w Internecie. Działania prewencyjne i terapeutyczne wobec sprawców, *Dziecko krzywdzone. Zagrożenia dzieci w Internecie,* 13, 45–69, Warszawa: FDN. ■ Scott D. A. (1998). *Pornografia. Jej wpływ na rodzinę, społeczeństwo, kulturę.* Gdańsk: HLI-Europa.

Programy Filtrujące

Techniczne aspekty testów

Proces testowania został podzielony na dwa etapy. Pierwszy polegał na automatycznym sprawdzeniu badanych aplikacji pod względem skuteczności algorytmu filtrowania zastosowanego przez jego twórców. Narzędzie do testów technicznych zostało stworzone przez działający przy NASK zespół CERT Polska, zajmujący się bezpieczeństwem teleinformatycznym.

Testy zostały przeprowadzone na bazie jednej biblioteki stron WWW, które zawierały nielegalne treści, co pozwoliło na uzyskanie jednorodnego materiału porównawczego dla każdego programu.

Na tym etapie sprawdzono także kompatybilność oprogramowania z różnymi przeglądarkami internetowymi, jakość współpracy z systemem operacyjnym komputera i odporności na próby zmiany ustawień oraz odinstalowania przez osobę do tego nieuprawnioną.

Kolejna część testów polegała na badaniach manualnych, przeprowadzonych na podstawie stałego zestawu kryteriów badawczych, które omawiamy szczegółowo w punkcie „Kryteria badania". Każda aplikacja została sprawdzona przez dwa zespoły, na oddzielnych stanowiskach testowych. Ustawienia i oprogramowanie stanowisk testowych miało stwarzać symulację środowiska komputera domowego średniej klasy.

Na stanowiskach testowych zainstalowano system operacyjny Microsoft Windows XP 2002, który należy do grupy systemów najczęściej używanych przez polskich internautów (~99%) (Tab. 1).

Kompatybilność, skuteczność i funkcjonalność aplikacji filtrujących sprawdzano pod trzema przeglądarkami internetowymi: Internet Explorer 6, Firefox 2.0.0.2, Opera 9.2. Są one najczęściej wykorzystywane przez polskich internautów do przeglądania zawartości Internetu.

Lp.	Grupy systemów	Użytkownicy (cookies)					
		24.IV.2007 -30.IV.2007		1.V.2007 – 7.V.2007		8.V.2007 -14.V.2007	
1	Windows	18 639 535	98.9%	16 962 725	99.0%	19 423 286	98.9%
2	Unix	192 669	1.0%	160 760	0.9%	199 816	1.0%
3	MacOS	39 627	0.2%	28 598	0.2%	41 692	0.2%

Tab. 1 Systemy operacyjne używane przez internautów łączących się z polskimi witrynami z obszaru Polski (Źródło: Gemius SA, gemiusTraffic. Więcej na www.ranking.pl)

Lp.	Grupy przeglądarek	Użytkownicy (cookies)					
		24.IV.2007 – 30.IV.2007		1.V.2007 – 7.V.2007		8.V.2007 -14.V.2007	
1	Internet Explorer	12 704 143	67.3%	11 352 942	66.2%	13 214 294	67.2%
2	Firefox	4 937 567	26.2%	4 622 475	26.9%	5 178 436	26.3%
3	Opera	1 057 444	5.6%	1 028 832	6.0%	1 094 053	5.6%

Tab. 2 Przeglądarki używane przez internautów łączących się z polskimi witrynami z obszaru Polski (Źródło: Gemius SA, gemiusTraffic. Więcej na www.ranking.pl)

Kryteria badania

Kryteria badawcze, według których testowano aplikacje filtrujące, zostały podzielone na pięć grup: kryteria ogólne, opcje filtrowania, wsparcie techniczne, sposób raportowania, dostępność (licencja płatna-bezpłatna, możliwość pobrania z Internetu).

Kryterium	Opis
Przyjazny interfejs	Łatwość obsługi programu; zastosowanie intuicyjnych rozwiązań; klarowność komend i opisu opcji; element dodatkowy oceny – jakość graficznego opracowanie interfejsu
Niezależne profile ustawień dla różnych użytkowników	Możliwość ustawienia niezależnych profili dla więcej niż jednego użytkownika; podział na profile administrator (np. rodzic) – zwykły użytkownik (np. dziecko); funkcjonalność profilu administratora i użytkownika
Automatyczne uruchamianie się	Uruchamianie się aplikacji filtrującej bezpośrednio po zainstalowaniu
Własne ustawienia	Dostępność własnych ustawień dla opcji filtrowania/ blokowania zawartości Internetu – np. dostosowanie przez administratora ustawień do wieku dziecka
Możliwość czasowego wyłączenia	Możliwość czasowej rezygnacji z działania programu bez konieczności jego odinstalowania
Ochrona hasłem	Ochrona panelu administracyjnego przed dostępem niepowołanych użytkowników

Tab. 3 Kryteria ogólne

Kryterium	Opis
Kontrola wysyłania danych osobowych	Możliwość i skuteczność kontroli wysyłania do Internetu danych osobowych, np. rejestracji/wypełniania formularzy online
Filtrowanie/blokowanie czatów	Możliwość i skuteczność filtrowania i/lub blokowania serwisów umożliwiających prowadzenie w czasie rzeczywistym rozmów online z innymi internautami za pomocą specjalnych serwisów lub programów
Filtrowanie/blokowanie poczty	Możliwość i skuteczność filtrowania zawartości poczty elektronicznej oraz blokowania serwisów oferujących tę usługę
Filtrowanie/blokowanie usenetu	Możliwość i skuteczność filtrowania grup dyskusyjnych – usenetu
Filtrowanie/blokowanie komunikatorów	Możliwość i skuteczność filtrowania programów służących do konwersacji z innymi internautami (komunikatorów)
Filtrowanie przy wykorzystaniu proxy	Skuteczność filtrowania/blokowania zawartości Internetu podczas łączenia się z Siecią przy wykorzystaniu serwerów pośredniczących – sprawdzenie efektywności filtrów przy rozbudowanych, niestatycznych adresach stron internetowych
Filtrowanie przy zastosowaniu krótkiego URL	Skuteczność filtrowania/blokowania zawartości Internetu przy zastosowaniu skróconego adresu URL: sprawdzenie efektywności filtrów przy zamianie adresu strony WWW na krótki adres
Filtrowanie Web 2.0	Skuteczność filtrowania/blokowania zawartości serwisów Web 2.0: serwisów społecznościowych, blogów, fotoblogów, etc.

Tab. 4 Opcje filtrowania

Kryterium	Opis
Pomoc techniczna	Jakość relacji producent–użytkownik; strona WWW, kontakt do obsługi technicznej: e-mail, telefon
Aktualizacje online	Aktualizowanie aplikacji filtrującej przez producenta, możliwość uzupełnienia bazy (np. zakazanych słów i adresów) za pomocą Internetu
Instrukcja instalacji	Łatwość instalacji i odinstalowania, instrukcja „krok po kroku" procesu instalacji
Dostępna dokumentacja (help)	Opis ustawień programu

Tab. 5 Wsparcie techniczne

Kryterium	Opis
Logowanie aktywności	Zapisywanie aktywności w Internecie; w przypadku istnienia kilku profili – odrębne zapisywanie dla każdego z nich
Raportowanie graficzne	Wyświetlanie komunikatu graficznego w przypadku zablokowania dostępu do określonej strony internetowej; robienie zrzutów ekranu alertu
Wysyłanie raportów przez e-mail	Możliwość wysyłania alertów do administratora (np. rodzica przebywającego w pracy)
Zapisywanie alertów	Wyszczególnianie połączeń z witrynami, których zawartość uznana została za nielegalną lub szkodliwą

Tab. 6 Sposób raportowania

Jak właściwie używać programów filtrujących

Należy pamiętać, że oprogramowanie filtrujące nie zastąpi rodziców i nauczycieli w procesie wychowania dzieci (szczególnie tych najmłodszych). Jest ono przydatnym narzędziem, umożliwiającym większą skuteczność ochrony przed negatywnym wpływem szkodliwej zawartości Internetu.

Dobry program filtrujący powinien spełniać dwa podstawowe kryteria: skutecznie blokować niepożądane treści internetowe oraz ograniczać niebezpieczne zachowania najmłodszych, takie jak podawanie swoich danych osobowych. Jednocześnie aplikacje filtrujące powinny służyć jedynie do filtrowania treści, a nie do całkowitej kontroli nad aktywnością dziecka w Internecie. Warto postawić na jawność i nie logować w ukryty sposób wszystkiego, co dziecko pisze na klawiaturze i wysyła do Sieci. Taki zapis pozwala na uzyskanie przejrzystego obrazu miejsc odwiedzanych w Internecie i rodzaju wyszukiwanych informacji, ale przez dostęp do zapisu korespondencji pocztowej czy prowadzonej za pośrednictwem komunikatorów dokonuje się ingerencja w życie osobiste dziecka. Może to wywołać efekt odwrotny od zamierzonego – dziecko straci zaufanie do rodziców/opiekunów i przeniesie swą aktywność sieciową poza dom.

Wystarczy, że rodzice i dziecko wspólnie stworzą zestaw dobrych praktyk korzystania z Sieci, które pomogą kształtować pozytywne nawyki, np. informowanie rodziców o przykrych sytuacjach doświadczonych w Internecie, krytyczne podejście do zawartości stron internetowych, ostrożność w kontaktach z osobami poznanymi online.

Opcje przeglądarek

Przeglądarki internetowe wyposażone są w podstawowe narzędzia, umożliwiające ochronę najmłodszych użytkowników Internetu przed szkodliwymi treściami. Najpopularniejsze w Polsce przeglądarki pozwalają na blokowanie pop-up'ów. Pop-up – nazywany również „wyskakującym okienkiem" – jest jedną z funkcji stron internetowych, pozwalającą na automatyczne uruchomienie nowej karty z określoną treścią. Wyskakujące okienka zawierają głównie przekaz reklamowy, ale często za ich pomocą promowane są serwisy posiadające zawartość nieodpowiednią dla surfujących w Internecie dzieci (Tab. 7).

Internet Explorer 6	Narzędzia ➳ Blokowanie wyskakujących okienek ➳ Wyłącz blokowanie wyskakujących okienek/Ustawienia blokowania wyskakujących okienek (*Możliwość określania witryn dozwolonych)*
Firefox 2.0.0.2	Narzędzia ➳ Opcje ➳ Treść ➳ Zablokuj wyskakujące okienka (*Istnieje możliwość definiowania wyjątków od reguły*)
Opera 9.2	Narzędzia ➳ Szybka konfiguracja ➳ Blokuj niechciane wyskakujące okienka/Blokuj wszystkie wyskakujące okienka

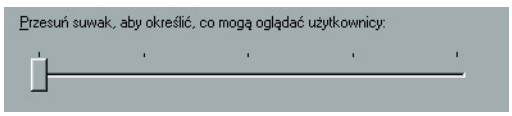
Tab. 7 Aktywowanie blokowania wyskakujących okienek

Przeglądarka Opera 9.2 daje także możliwość blokowania określonych stron internetowych. Nie jest to jednak opcja zabezpieczona hasłem, stąd też każdy użytkownik danego stanowiska komputerowego może dowolnie edytować listę zablokowanej zawartości. Do panelu edycji listy można się dostać w dwojaki sposób:
Narzędzia ➳ Preferencje ➳ Zaawansowane ➳ Zawartość ➳ Zablokowana zawartość
Narzędzia ➳ Zaawansowane ➳ Zablokowana zawartość

Opcja blokady witryn internetowych w przeglądarce Opera 9.2

Wbudowany w przeglądarkę IE 6 (i kolejne wersje) klasyfikator treści oparty o system etykietowania ICRA (dawniej RSACi) oferuje bardziej zaawansowany system blokowania określonej zawartości Internetu. System powstał w oparciu o badania i prace dr. Donalda F. Roberta z Uniwersytetu Stanforda, który przez prawie dwadzieścia lat badał skutki oddziaływania mediów i nowoczesnych technik telekomunikacyjnych na dzieci[2].

W starszej wersji systemu etykietowania – RSACi – zostały wyszczególnione cztery kategorie potencjalnie szkodliwych treści, jakie można zablokować: język, nagość, przemoc, seks. Skuteczność i „siła" filtrowania uzależnione są od ustawienia suwaka:



Dla każdej kategorii istnieją cztery poziomy ustawień suwaka – od najbardziej restrykcyjnego do najbardziej liberalnego. Ustawienia są chronione hasłem. Można wymagać podania hasła również wtedy, kiedy chcemy odwiedzić witrynę zablokowaną przez system.

Aplikacje filtrujące powinny służyć jedynie do filtrowania treści, a nie do całkowitej kontroli nad aktywnością dziecka w Internecie. Warto postawić na jawność i nie logować w ukryty sposób wszystkiego, co dziecko pisze na klawiaturze i wysyła do Sieci.

[2] http://www.microsoft.com/poland/windows/ie/using/howto/contentadv/config.mspx.

	Poziom 0	Poziom 1	Poziom 2	Poziom 3	Poziom 4
Język	Nieobraźliwy żargon	Łagodne inwektywy lub odniesienia do fizjologii	Umiarkowane inwektywy (inwektywy, aseksualne odniesienia anatomiczne)	Obsceniczne gesty (mocny, wulgarny język, obsceniczne gesty, używanie epitetów)	Dosadny lub wulgarny język (wypowiedzi pełne nienawiści lub wulgarny język, dosadne odniesienia seksualne)
Nagość	Bez nagości	Skąpy strój	Częściowa nagość	Pełna nagość	Prowokacyjna pełna nagość
Przemoc	Bez przemocy (bez agresji i przemocy, bez gwałtownych zdarzeń naturalnych lub losowych)	Walka (zadawanie ran lub zabijanie żywych stworzeń, niszczenie realistycznie wyglądających obiektów)	Zabójstwo (zadawanie ran lub zabijanie stworzeń lub ludzi, zadawanie ran stworzeniom nie stanowiącym zagrożenia)	Krwawe zabójstwo (zadawanie ran, zabijanie ludzi)	Bezlitosna i bezduszna przemoc
Seks	Bez pokazywania seksu. Romans	Namiętne pocałunki	Dotyk erotyczny bez nagości	Niebezpośrednie pokazywanie dotyku erotycznego	Bezpośrednie pokazywanie zachowań erotycznych

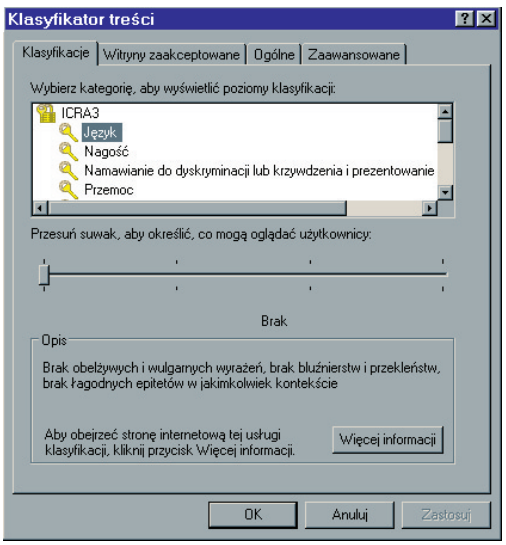
Tab. 8 System klasyfikacji treści RSACi

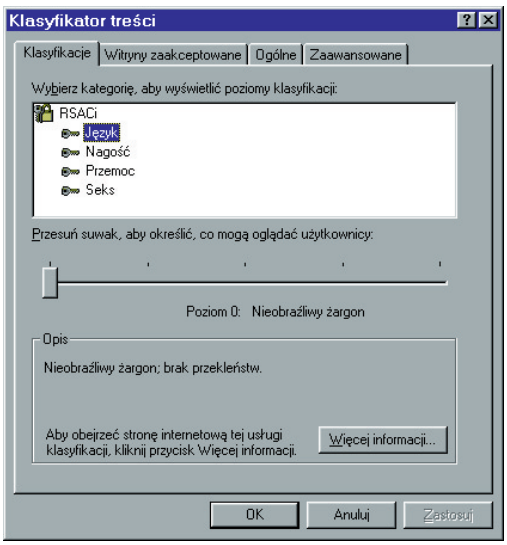
	Brak	Ograniczone	Niektóre	Bez ograniczeń
Język	Brak obelżywych i wulgarnych wyrażeń, brak bluźnierstw i przekleństw, brak łagodnych epitetów w jakimkolwiek kontekście	Brak obelżywych i wulgarnych wyrażeń w jakimkolwiek kontekście; bluźnierstwa, przekleństwa i łagodne epitety tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	Obelżywe i wulgarne wyrażenia tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości; wulgarne słowa, bluźnierstwa i łagodne epitety w dowolnym kontekście	Obelżywe i wulgarne wyrażenia, bluźnierstwa, przekleństwa i łagodne epitety w dowolnym kontekście (ta reguła nie obejmuje języka seksualnego, który opisano osobno)
Nagość	Brak obnażonych pośladków, biustów i genitaliów w jakimkolwiek kontekście	Obnażone pośladki i/lub biusty w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości; brak genitaliów w jakimkolwiek kontekście	Obnażone pośladki i/lub biusty w dowolnym kontekście, genitalia tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	Nagość dowolnego rodzaju w dowolnym kontekście (ta reguła nie dotyczy seksu, który opisano osobno)
Namawianie do dyskryminacji lub krzywdzenia i prezentowania takich zachowań	Brak namawiania do dyskryminacji lub krzywdzenia i prezentowania takich zachowań w jakimkolwiek kontekście	Namawianie do dyskryminacji lub krzywdzenia i prezentowanie takich zachowań tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Namawianie do dyskryminacji lub krzywdzenia i prezentowanie takich zachowań w dowolnym kontekście

	Brak	Ograniczone	Niektóre	Bez ograniczeń
Przemoc	Brak przemocy/gwałtu; brak uszkodzeń ciała, torturowania, zabijania i krwi albo rozczłonkowywania ludzi, zwierząt lub postaci fikcyjnych (włączając w to animację) w dowolnym kontekście	Zadawanie ran, torturowanie, zabijanie lub krwawienie i ćwiartowanie postaci fikcyjnych tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości; żadna z wymienionych czynności wykonywana	Zadawanie ran, torturowanie, zabijanie lub krwawienie i ćwiartowanie postaci fikcyjnych w dowolnym kontekście; wymienione czynności wykonywane na ludziach lub zwierzętach tylko w kontekście sztuki medycyny, edukacji, sportu lub wiadomości; brak przemocy/gwałtu	Przemoc dowolnego rodzaju w dowolnym kontekście, w tym napaści/gwałty
Sceny przedstawiające hazard	Brak scen przedstawiających hazard w jakimkolwiek kontekście	Sceny przedstawiające hazard tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Sceny przedstawiające hazard w dowolnym kontekście
Sceny używania alkoholu	Brak scen używania alkoholu w jakimkolwiek kontekście	Sceny używania alkoholu tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Sceny używania alkoholu w dowolnym kontekście
Sceny używania broni	Brak scen używania broni w jakimkolwiek kontekście	Sceny używania broni tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Sceny używania broni w dowolnym kontekście
Sceny używania narkotyków	Brak scen używania narkotyków w jakimkolwiek kontekście	Sceny używania narkotyków tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Sceny używania narkotyków w dowolnym kontekście
Sceny używania tytoniu	Brak scen używania tytoniu w jakimkolwiek kontekście	Sceny używania tytoniu tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Sceny używania tytoniu w dowolnym kontekście
Seks	Brak namiętnych pocałunków, pośrednich i ukrytych czynności seksualnych, widocznych dotyków seksualnych, otwartego języka dotyczącego seksu, erekcji, jawnych czynności seksualnych lub erotyki w jakimkolwiek kontekście	Pośrednie i ukryte czynności seksualne oraz widoczny dotyk seksualny w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości; namiętne pocałunki w dowolnym kontekście; brak zawartości jawnie seksualnej	Pośrednie i ukryte czynności seksualne, widoczny dotyk seksualny oraz namiętne pocałunki w dowolnym kontekście; jawny seks i erotyka tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	Seks dowolnego rodzaju w dowolnym kontekście (ta reguła nie obejmuje przemocy na tle seksualnym, którą opisano osobno)

	Brak	Ograniczone	Niektóre	Bez ograniczeń
Zawartość powodująca strach, onieśmielenie, etc.	Brak zawartości powodującej uczucie strachu, onieśmielenia, itp. w jakimkolwiek kontekście	Zawartość powodująca uczucie strachu, onieśmielenia, itp. tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Zawartość powodująca uczucie strachu, onieśmielenia, itp. w dowolnym kontekście
Zawartość stanowiąca zły przykład dla dzieci	Brak zawartości stanowiącej zły przykład dla dzieci, uczącej lub zachęcającej dzieci do wykonywania szkodliwych czynności lub naśladowania niebezpiecznych zachowań w jakimkolwiek kontekście	Zawartość stanowiąca zły przykład dla dzieci, ucząca lub zachęcająca dzieci do wykonywania szkodliwych czynności lub naśladowania niebezpiecznych zachowań tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	*Brak tego ustawienia*	Zawartość stanowiąca zły przykład dla dzieci, ucząca lub zachęcająca dzieci do wykonywania szkodliwych czynności lub naśladowania niebezpiecznych zachowań w dowolnym kontekście
Zawartość wygenerowana przez użytkowników	Brak zawartości wygenerowanej przez użytkowników, takiej jak pokoje rozmów i tablice dyskusyjne, w jakimkolwiek kontekście	Moderowana zawartość wygenerowana przez użytkowników, taka jak pokoje rozmów i tablice dyskusyjne, w dowolnym kontekście	Moderowana zawartość wygenerowana przez użytkowników w dowolnym kontekście; niemoderowana zawartość wygenerowana przez użytkowników tylko w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości	Niemoderowana zawartość wygenerowana przez użytkowników, taka jak pokoje rozmów i tablice dyskusyjne, w dowolnym kontekście

Tab. 9 System klasyfikacji treści ICRA (w przeglądarce Internet Explorer 7)





Klasyfikator treści w przeglądarce Internet Explorer – system ICRA oraz RSACi

Wyniki testów

Nazwa programu	Wersja	Producent	WWW
Beniamin	1.4.186	AKKORP	www.beniamin.pl
Cenzor	1.62	ANCOM	www.cenzor.pl
Motyl	2.0	Adalex	www.adalex.alpha.pl
Ochraniacz	1.2.0	BENAROM	www.benarom.k7.pl
Opiekun Dziecka w Internecie	2.0.0.537	SoftStory	www.opiekun.com
Strażnik Ucznia	3.0.0.8	Adalex	www.adalex.alpha.pl
Weblock	1.3	AKKORP	www.chrondziecko.pl
X-Guard II	X Guard II	PROINVEST Group	www.x-guard.pl

Tab. 10 Wykaz programów poddanych testom

Testy skuteczności programów filtrujących przeprowadzono na bazie trzystu adresów stron WWW, przesłanych przez użytkowników Internetu do Zespołu Dyżurnet.pl. Za kryterium skuteczności przyjęto zamknięcie danej strony WWW przez program w czasie do 5 sekund po jej wyświetleniu. Raport bazuje na testach przeprowadzonych w okresie od maja do lipca 2007 r. W celu uzyskania informacji na temat aktualizacji programów, prosimy o kontakt z producentami.

Porównanie skuteczności filtrowania

W Tab. 11 przedstawiono skuteczność programów filtrujących. Krzyżyk oznacza, że program pod daną przeglądarką internetową nie działa.

	Firefox	Opera	Internet Explorer
Beniamin	77 %	77 %	78 %
Cenzor	91 %	91 %	91 %
Motyl	82 %	85 %	81 %
Ochraniacz	40 %	x	24 %
Opiekun	76 %	82 %	75 %
Weblock	82 %	82 %	82 %
X-Guard II	72 %	68 %	65 %
Strażnik	x	x	80 %

Tab. 11 Skuteczność programów filtrujących

Skuteczność programów filtrujących

Poniżej prezentujemy skuteczność programów filtrujących pod przeglądarkami internetowymi Firefox, Opera i Internet Explorer.

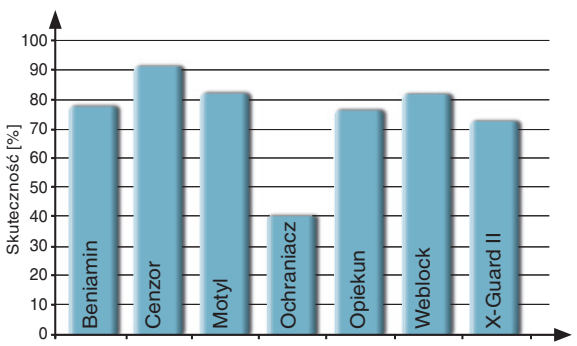
Spośród wszystkich programów filtrujących najwyższą skutecznością blokowania niepożądanych stron pod przeglądarką Firefox odznacza się Cenzor – 90%.

Ponad 80% skuteczności osiągnęły oprogramowania Motyl i Weblock. Najmniej stron zablokował Ochraniacz (Ryc. 1).

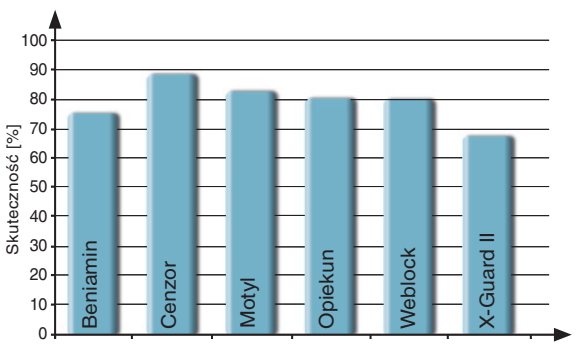
Podczas testowania pod przeglądarką Opera stwierdzono, że największą skuteczność wykazuje Cenzor – 91%. Równie wysoką skuteczność osiągnęły Opiekun i Weblock – 82%, a najmniej stron zablokował X-Guard II (Ryc. 2).

W przypadku testów pod przeglądarką Internet Explorer wykazano, iż najwięcej stron zablokował program Cenzor – 91% skuteczności. Nieco niższą skutecznością charakteryzowały się Motyl i Weblock. Najmniej stron zablokował Ochraniacz (Ryc. 3).

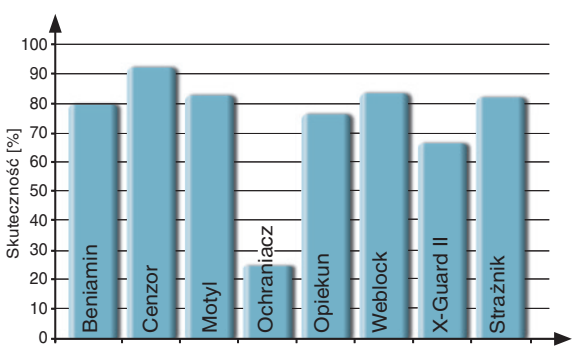
Podsumowując, najwyższą skutecznością blokowania niepożądanych stron internetowych charakteryzuje się Cenzor, najniższą zaś – Ochraniacz (Ryc. 4).



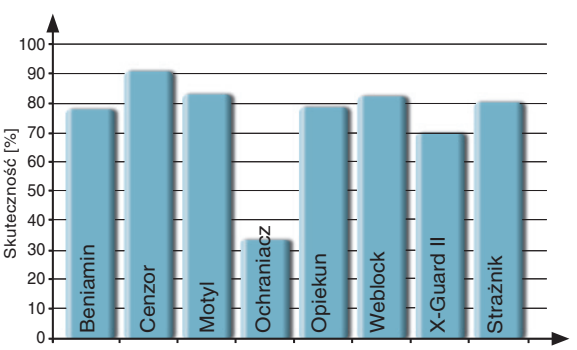
Ryc. 1 Skuteczność programów filtrujących pod przeglądarką Firefox



Ryc. 2 Skuteczność programów filtrujących pod przeglądarką Opera



Ryc. 3 Skuteczność programów filtrujących pod przeglądarką Internet Explorer



Ryc. 4 Skuteczność programów filtrujących – wyniki ogólne

Opis funkcjonalności programów poddanych testom

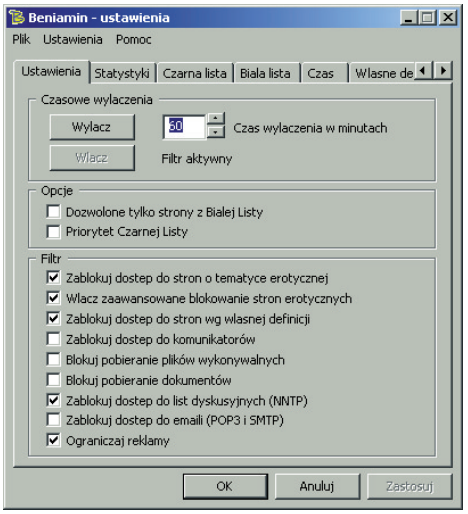
Nazwa programu	Beniamin	Cenzor	Motyl	Ochraniacz	Opiekun Dziecka w Internecie	Strażnik Ucznia	Weblock	X-Guard II
Wersja	1.4.186	1.62	2.0	1.2.0	2.0.0.537	3.0.0.0	1.3	X Guard II
Kryteria ogólne								
Polska wersja językowa	X	X	X	X	X	X	X	X
Przyjazny interfejs	X	X	X	X	X	X	X	X
Niezależne profile		X			X			X
Autom. uruchamianie się	X	X	X	X	X	X	X	X
Własne ustawienia	X	X	X	X	X	X	X	X
Możliwość czasowego wył.	X	X		X			X	X
Ochrona hasłem	X	X	X	X	X	X	X	X
Opcje filtrowania								
Kontrola wysył. danych osob.	X						X	
Filtrowanie/blokowanie czatów	X	X	X	X	X	X	X	X
Filtrowanie/blokowanie poczty	X		X			X	X	
Filtrowanie/blokowanie usenetu	X		X	X	X	X	X	
Filtr./blokowanie komunikatorów	X	X	X	X	X	X	X	X
Filtrowanie przy proxy	X	X	X	X	X/-	X	X	X
Filtrowanie przy krótkim URL	X	X	X	X	X	X	X	X
Filtrowanie Web 2.0	X/-	X/-	X/-	X/-	X/-	X/-	X/-	X/-
Wsparcie techniczne								
Pomoc techniczna (www, tel.)	X	X	X	X	X	X	X	X
Aktualizacja online		X	X	X	X	X	X	X
Instrukcja instalacji	X	X	X	X	X	X	X	X
Dostępna dokumentacja	X	X	X	X	X	X	X	X
Sposób raportowania								
Logowanie aktywności	X	X		X	X	X/-	X	X
Raportowanie graficzne	X	X		X	X	X	X	X
Wysyłanie raportów przez email								
Zapisywanie alertów		X		X	X	X		X
Rodzaj reakcji na zdarzenie	z+k	z+k	z	z+k+e	z+k	możliwość wyboru	z+k	z+k

z – zamknięcie, k – komunikat, e – zrzut ekranu (opcje)

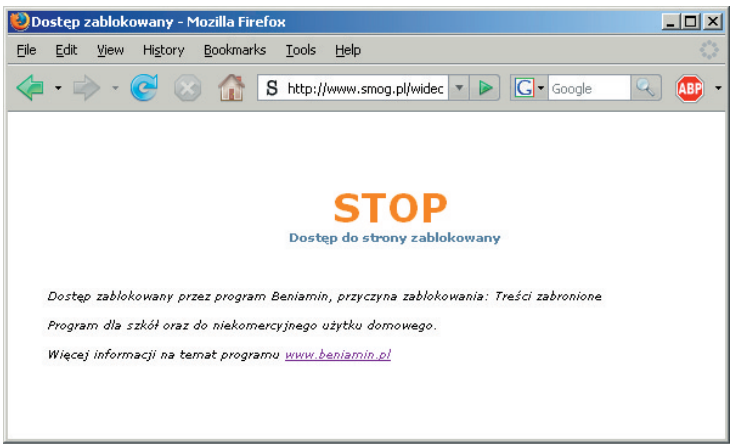
Beniamin

Program posiada prosty, funkcjonalny interfejs. Panel administracyjny składa się z sześciu zakładek: Ustawienia, Statystyki, Czarna lista, Biała lista, Czas, Własne definicje. Administrator ma możliwość wprowadzania zmian w ustawieniach, korzystając z szeregu opcjonalnych funkcji: blokowanie stron o tematyce erotycznej, zaawansowane blokowanie stron erotycznych, blokowanie komunikatorów, blokowanie pobierania plików wykonywalnych (EXE), blokowanie pobierania dokumentów, blokowanie list dyskusyjnych (protokół do obsługi usenetu NNTP), blokowanie dostępu do poczty elektronicznej (protokoły POP3 i SMTP), ograniczanie reklam. Ponadto może ustawić własne definicje określeń (słów lub ich fragmentów), których pojawienie się na stronie spowoduje jej zamknięcie (zablokowanie). Dodatkową opcją jest możliwość wprowadzenia wyższego priorytetu dla stron, które można oglądać niezależnie od ich zawartości (Biała lista) lub których nie można odwiedzić niezależnie od tego, co się na nich znajduje (Czarna lista). Program Beniamin pozwala na wprowadzenie limitów czasowych w dostępie do Internetu lub korzystanie z niego tylko w określonych godzinach.

W zakładce Statystyki prowadzona jest historia odwiedzanych stron WWW. Aplikacja zapisuje jedynie adresy domenowe nie odnotowując np. faktu odwiedzin podstron określonej witryny. Brak jest również zapisu dnia i godziny wejścia na stronę. Nie są zapisywane alerty, czyli sytuacje, kiedy program wyświetla komunikat o zablokowaniu dostępu do strony.



Ustawienia programu Beniamin 1.4.186



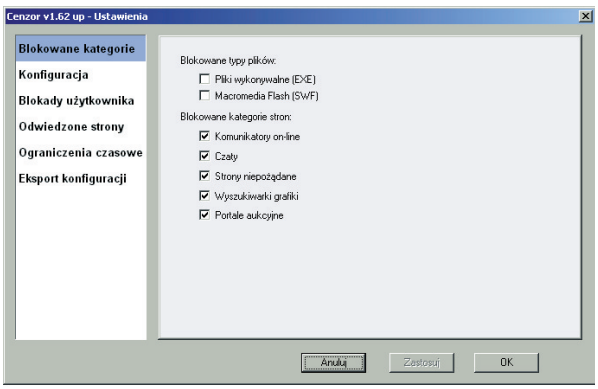
Komunikat programu Beniamin o zablokowaniu dostępu do strony

Cenzor

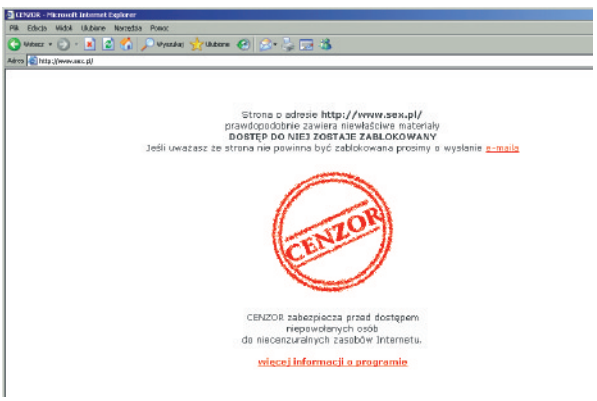
Cenzor – „Program filtrujący zasoby Internetu" – posiada przejrzysty, prosty panel administracyjny z sześcioma zakładkami ustawień: Blokowane kategorie, Konfiguracja, Blokady użytkownika, Odwiedzane strony, Ograniczenia czasowe, Eksport konfiguracji. Pierwsze z wymienionych ustawień pozwala na wybór przeznaczonych do zablokowania usług (pliki wykonywalne, Macromedia Flash, komunikatory on-line, czaty, strony niepożądane, wyszukiwarki grafiki np. images.google.pl, portale aukcyjne). Nie wiadomo jednak, co kryje się pod hasłem „strony niepożądane". W pliku pomocy znajduje się opis wcześniejszej wersji programu, w której zamiast opcji blokowania „stron niepożądanych" występowała opcja blokady „stron pornograficznych". Pozwala to przypuszczać, że zakres pojęciowy tej kategorii został rozszerzony, choć brakuje informacji o rodzaju treści uznanych za szkodliwe. Aplikacja umożliwia ustawienie stałej blokady lub

zezwolenie na odwiedziny wybranych stron niezależnie od ich treści. Pozwala także na wprowadzenie limitów czasowych na korzystanie z Internetu. Cenzor zapisuje informacje o odwiedzanych stronach internetowych. Zapis ten jest czytelny, można go również sortować według trzech kategorii: Strony (HTML), Wszystkie dane, Zablokowane. Program odnotowuje URL odwiedzonej witryny, datę odwiedzin, aplikację, za pomocą której nastąpiło połączenie, a w przypadku zablokowania strony – podświetla adnotację na czerwono i opatruje kategorią „Strony niepożądane".

Ciekawym rozwiązaniem jest umożliwienie użytkownikowi programu zgłoszenia do producenta informacji o tym, że dana witryna nie powinna być blokowana (np. portale edukacyjne posiadające informacje na temat rozwoju płciowego człowieka). Jest to przydatne w sytuacji, kiedy aplikacja stosowana jest w miejscach publicznych, takich jak szkoły, i nie ma możliwości bezpośredniego kontaktu z administratorem.



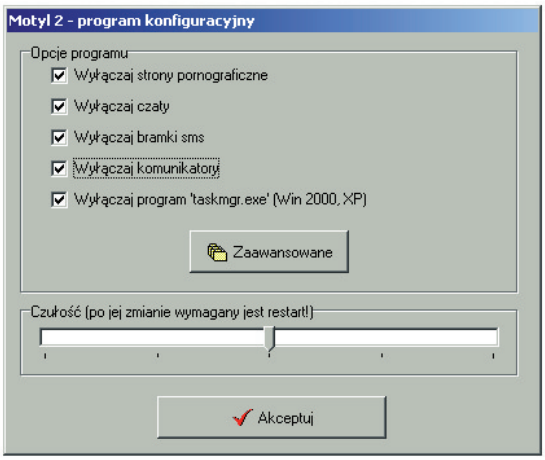
Ustawienia programu Cenzor 1.62



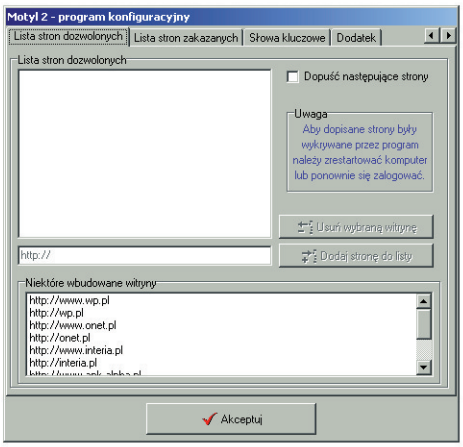
Komunikat programu Cenzor o zablokowaniu dostępu do strony

Motyl

Panel konfiguracyjny programu nie jest skomplikowany i umożliwia wprowadzenie szybkich zmian w ustawieniach. Uciążliwa może jedynie być konieczność ponownego uruchomienia komputera w przypadku zmiany ustawień. Opcje podstawowe pozwalają na wyłączanie stron pornograficznych, czatów, bramek SMS, komunikatorów oraz procesu taskmgr.exe – menedżera zadań systemu operacyjnego Windows (pozwala on np. na zamknięcie programu Motyl). Za pomocą specjalnego suwaka można zmienić „czułość" programu, czyli sprawić, że będzie on bardziej lub mniej restrykcyjnie oceniał zawartość Internetu. Producent nie opisuje jednak dokładniej, co dają kolejne ustawienia suwaka i jakie są różnice w ustawieniach tej opcji. Panel opcji zaawansowanych posiada cztery zakładki funkcyjne (Zamykanie aplikacji, Lista stron dozwolonych, Lista stron zakazanych, Słowa kluczowe) i jedną informacyjną (Dodatek). Korzystając z tych ustawień administrator programu może blokować



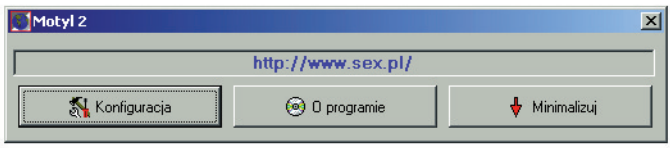
Opcje podstawowe programu Motyl 2.0



Opcje zaawansowane programu Motyl 2.0

określone procesy lub witryny, ustalać zawartość „białej listy", a także samodzielnie definiować słowa lub ich fragmenty, których pojawienie się na stronie spowoduje jej zamknięcie. Program skutecznie analizuje zawartość Internetu pod kątem zdefiniowanych w panelu konfiguracyjnym słów kluczowych i zamyka okno przeglądarki nawet wtedy, kiedy niedopuszczone słowa pojawią się np. w treści pisanego listu elektronicznego.

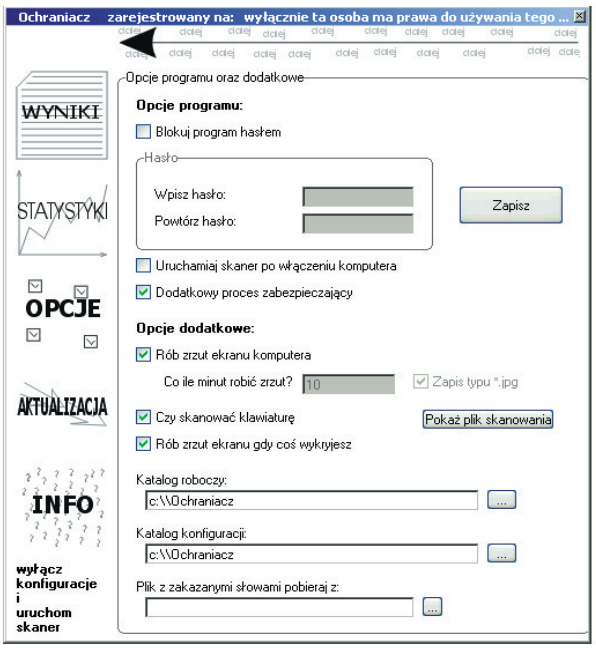
Aplikacja w specjalnym panelu przechwytuje adres zamkniętej strony. Jest to jednak funkcja niezrozumiała, ponieważ nie towarzyszy jej jednoczesny zapis historii przechwyconych witryn. Adres nowo zablokowanej strony zastępuje miejsce starego wpisu, przez co administrator (np. rodzic) nie ma klarownego obrazu aktywności użytkowników (np. dzieci) w Internecie. Poważnym mankamentem jest również brak kompatybilności programu z przeglądarkami innymi niż Internet Explorer.



Okno programu Motyl z polem przechwyconego adresu zamkniętej witryny

Ochraniacz

Aplikacja posiada rozbudowany system ustawień i funkcjonalności. Opcje internetowe pozwalają na ustawienie częstości skanowania Internetu (częstotliwość sprawdzania otwartych witryn pod kątem zakazanych słów), skanowanie w poszukiwaniu konkretnych stron (brak informacji, o jakie strony chodzi), blokowanie czatów, serwisów pocztowych i grup dyskusyjnych, sprawdzanie dozwolonych adresów („biała lista", czyli strony otwierane bez względu na to, co zawierają) oraz skanowanie zawartości stron internetowych. Opcje aplikacji określają, w jaki sposób ma działać program Ochraniacz. Umożliwiają ustawienie częstości skanowania okien wszystkich otwartych programów, wyświetlanie i edycję treści komunikatu, jaki pojawi się po zamknięciu strony, sprawdzanie dozwolonych słów, zamykanie okien programów zawierających zakazane słowa, skanowanie procesów, blokowanie komunikatorów internetowych oraz programów P2P, a także skanowanie tylko aktywnego okna. Z testów wynika, że mniej doświadczeni użytkownicy mogą mieć



Ustawienia programu Ochraniacz 1.2.0

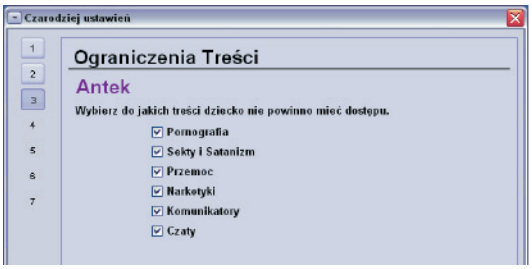
trudności z ustawieniem pożądanej częstotliwości skanowania, jak i z określeniem różnicy między skanowaniem Internetu i aplikacji (w pliku pomocy obie funkcje zdefiniowano w ten sam sposób). Opcje dodatkowe pozwalają na włącznie dodatkowego procesu zabezpieczającego (można zachować ciągłość skanowania w przypadku prób wyłączenia aplikacji przez nieuprawnionego użytkownika), robienie zrzutów ekranu (w tym alertów) oraz skanowanie klawiatury (logowanie wszystkiego, co jest pisane na danej klawiaturze).

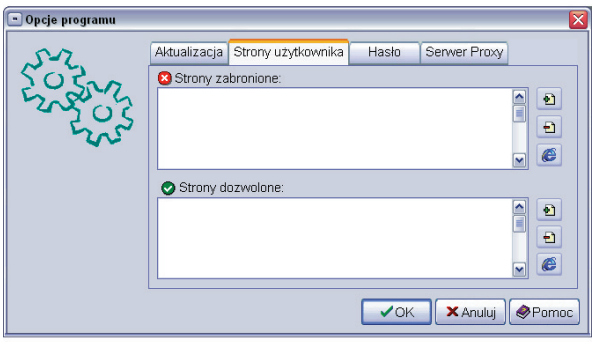
Program Ochraniacz udostępnia szereg edytowalnych baz danych, dając uprawnionym użytkownikom możliwość znacznej ingerencji w sposób działania skanera. Można zmieniać (dodawać lub usuwać) zawartość pliku z zakazanymi słowami i adresami serwisów, można edytować listę stron, dozwolonych słów oraz bazę zakazanych procesów, nazw komunikatorów internetowych oraz programów P2P, a także adresów portów (z wyszczególnieniem portów wykorzystywanych przez serwisy oferujące usługę czatów). Dodatkowo istnieje możliwość wyboru jakości zabezpieczeń – najlepszej, średniej lub słabej – ale producent nie opisał, czym się one między sobą różnią. Ochraniacz pozwala na ustawienie przedziałów czasowych na korzystanie z Internetu. Prowadzi również standardowy zapis odwiedzanych witryn, nie informując o wykrytych alertach.

Trzeba jednak zauważyć, że aplikacja niekiedy zachowuje się niestabilnie, a skaner wyłącza się samoczynnie. Nie zawsze poprawnie działają statystyki. Program nie działa pod przeglądarką Opera.

Opiekun Dziecka w Internecie

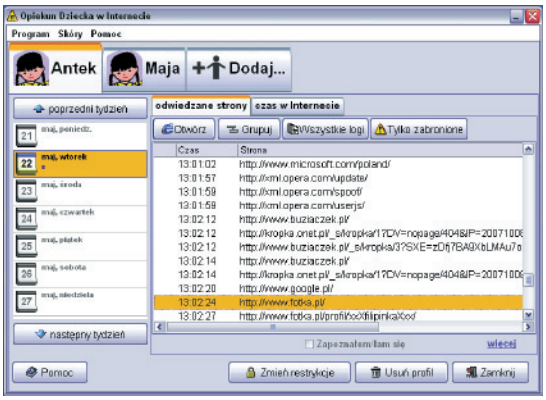
Program wywołuje dobre wrażenie przemyślanym, klarownym i estetycznie wykonanym interfejsem. Po uruchomieniu aplikacji istnieje możliwość wyboru między dwoma trybami pracy. Pierwszy – zaawansowany – udostępnia wszystkie funkcje programu i pozwala na stworzenie odrębnych profili ustawień dla różnych użytkowników (dzieci), drugi – uproszczony – jest łatwiejszy w obsłudze między innymi z powodu ukrycia części zaawansowanych opcji i automatycznego wprowadzenia domyślnych ustawień. Przy korzystaniu z pierwszego z wymienionych trybów, administrator-rodzic samodzielnie ustawia „profil ograniczeń dziecka". Aplikacja pozwala na blokowanie stron zawierających wiele rodzajów treści, które mogą mieć szkodliwy wpływ na rozwój dziecka: pornografii, przemocy, promocji narkotyków i sekt. Umożliwia także blokowanie czatów i komunikatorów oraz pobierania plików z Internetu (wykonywalnych EXE lub plików dokumentów, np. doc czy mp3). Daje możliwość wprowadzenia limitów czasowych na korzystanie z Internetu. Administrator może także edytować listę stron zabronionych lub dozwolonych dla użytkownika konkretnego profilu.



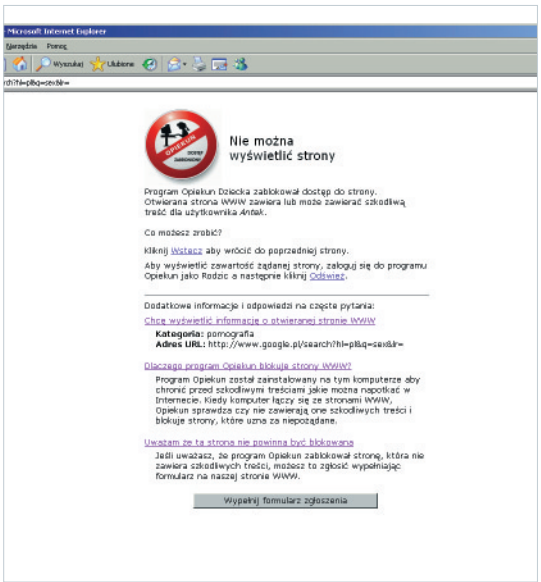


Funkcje programu Opiekun Dziecka w Internecie 2.0.0.537

Panel profilu użytkownika jest przejrzysty i funkcjonalny. Posiada zakładki Odwiedzone strony i Czas w Internecie informujące o internetowej aktywności dziecka. Informacje o zdarzeniach opatrzone są ikonką popularnego znaku ostrzegawczego i żółtym podkreśleniem. Ciekawym pomysłem jest wprowadzenie możliwości odznaczenia przez administratora faktu zapoznania się z historią przeglądanych stron WWW. Dopóki użytkownik nie zaloguje się do swojego profilu, program nie pozwala na połączenie z Internetem. Aplikacja filtruje słowa wpisywane do wyszukiwarki i blokuje wyniki



Podgląd profilu użytkownika i jego aktywności w Internecie



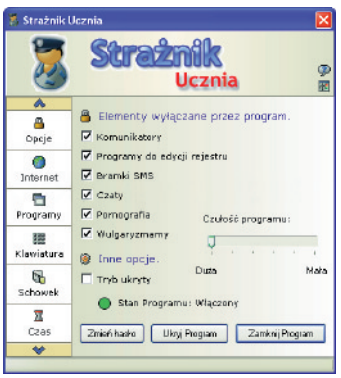
Szczegółowy komunikat o zamknięciu strony

wyszukiwania, jeśli zostaną użyte wyrażenia pochodzące z wbudowanej w program „czarnej listy". W momencie zamknięcia strony wyświetla się szczegółowy komunikat informujący o tym, dlaczego program zabronił dostępu do danej witryny. Wątpliwości dotyczące niewłaściwej, zdaniem użytkownika, klasyfikacji strony można zgłaszać producentowi za pomocą formularza.

Strażnik Ucznia

W estetyczny interfejs programu zostało wkomponowanych 11 zakładek funkcyjnych i informacyjnych: Opcje, Internet, Programy, Klawiatura, Schowek, Czas, Zrzuty, Zdarzenia, Aktualizacja, Pomoc, O programie. Pierwsza z nich udostępnia opcje wyłączania komunikatorów, programów do edycji rejestru, bramek SMS, czatów, stron zawierających pornografię oraz wulgaryzmy. Skuteczność działania aplikacji można ustawić za pomocą specjalnego suwaka – brak jednak informacji, jaka jest różnica między dużą i małą czułością filtrowania (plik pomocy informuje jedynie, że blokowanie następuje po przekroczeniu na stronie limitu zakazanych słów). Administrator posiada możliwość edytowania listy dozwolonych witryn i zabronionych wyrażeń, a także blokowania określonych programów. Co ciekawe, można również edytować listę „zabronionych słów w programie". Ich pojawienie się w oknie otwartej aplikacji spowoduje jej wyłączenie. Strażnik Ucznia pozwala na filtrowanie słów wpisywanych z klawiatury (np. do wyszukiwarki). Kontroluje również zawartość schowka systemowego, czyli przestrzeni komputera przeznaczonej do zapisywania danych wskazanych przez użytkownika (tekstu lub grafiki). Program daje możliwość wykonywania zrzutów ekranu oraz wprowadzenia ograniczeń na korzystanie z komputera.

O zdarzeniach administrator powiadamiany jest w odrębnej zakładce. Składa się ona z trzech pól: „znaleziono w'", „treść", „data". Aplikacja ma również dwie opcje dodatkowe,

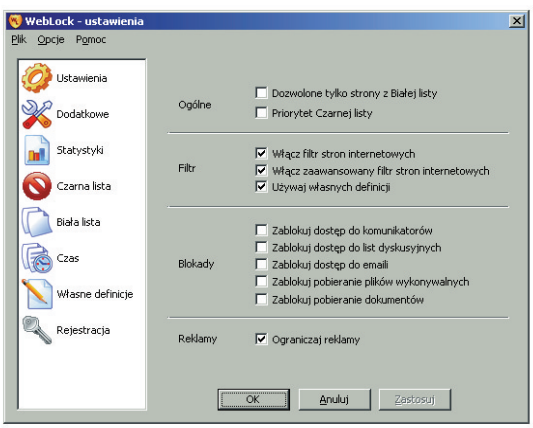


Ustawienia programu Strażnik Ucznia 3.0.0.0

za pomocą których można włączyć zaawansowaną kontrolę Internetu (brak szczegółów) oraz ustalić listę dozwolonych przeglądarek. Program posiada kilka interesujących funkcjonalności, takich jak informacja o sile wybranego przez administratora hasła czy możliwość wyboru reakcji na zdarzenie (zamknięcie systemu, ponowne uruchomienie komputera, wylogowanie, wyświetlenie komunikatu, zamknięcie przeglądarki czy brak reakcji). Każda z zakładek funkcyjnych posiada własny wybór sposobu reagowania na alert. Nie zawsze jednak użytkownik otrzymuje informację o tym, dlaczego aplikacja/komputer zachowały się w określony sposób. Kłopotliwy jest również fakt zamykania wszystkich otwartych okien przeglądarki, nawet jeśli tylko w jednym pojawiły się niedozwolone treści.

Weblock

Weblock został wprowadzony na rynek przez producenta programu Beniamin, dlatego między obiema aplikacjami występuje wiele zbieżności. Jego interfejs jest równe prosty i funkcjonalny, choć graficznie został lepiej opracowany. Panel administracyjny posiada siedem zakładek, za pomocą których można określić sposób działania programu. Ustawienia dzielą się na cztery podkategorie: ogólne (ustawienie priorytetu czarnej listy lub zezwolenie na otwieranie stron tylko z białej listy), filtr (możliwość włączenia filtru stron internetowych, zaawansowanego filtru stron internetowych i używania własnych definicji), blokady (blokowanie dostępu do komunikatorów, list dyskusyjnych, serwisów poczty elektronicznej, pobierania plików wykonywalnych i dokumentów), reklama (wprowadzenie ograniczeń na wyświetlanie reklam).

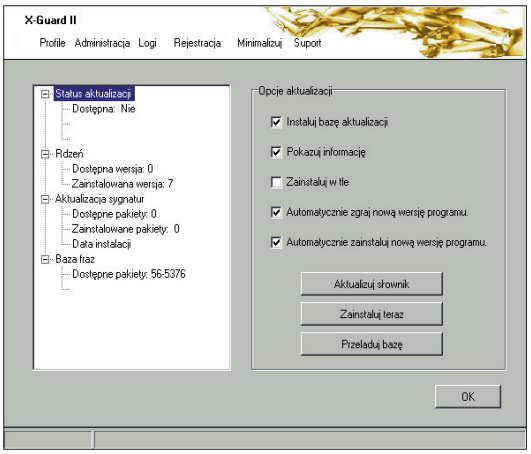


Ustawienia programu Weblock 1.3

Można edytować białą i czarną listę adresów stron internetowych oraz wprowadzać własne definicje zabronionych słów lub ich fragmentów (Weblock filtruje słowa wpisywane do wyszukiwarki). Program pozwala na wprowadzenie limitów czasowych w dostępie do Internetu lub korzystanie z niego tylko w określonych godzinach. Administrator może przejrzeć statystkę odwiedzonych stron, ale aplikacja loguje jedynie URL witryny, nie zapisując dodatkowych informacji (data, alerty). Komunikat informujący o zamknięciu strony jest identyczny jak informacja wyświetlana przez program Beniamin.

X Guard II

X Guard II (Internetowy Strażnik) posiada wiele funkcji, które użytkownik może dowolnie zestawiać. Program pozwala na tworzenie niezależnych profili ustawień. Co więcej, dla każdego profilu – za pomocą specjalnego suwaka – można odrębnie ustalić poziom restrykcji (od niskiego do wysokiego). Skuteczność działania aplikacji jest modyfikowana poprzez ustawienie ograniczeń „podstawowych" lub/i „dodatkowych" (poza informacją, że opierają się na analizie treści, brak szczegółowego opisu wymienionych funkcji) oraz bazy zabronionych słów i wyrażeń. Ponadto istnieje możliwość ustalenia preferencji dla konkretnych przeglądarek internetowych (przeglądarki niewybrane z listy zostaną zablokowane). Aplikacja X Guard II pozwala na filtrowanie zawartości Internetu pod kątem trzech kategorii (wybór opcjonalny): pornografii, wulgaryzmów i używek. Dodatkowo można ograniczać użytkownikom dostęp do czatów i komunikatorów. Szybkość analizy stron pozwala zwiększyć opcja „Szybka reakcja", ale producent uprzedza, że może się to wiązać z obciążeniem pracy procesora. Dla każdego profilu program prowadzi zestawienie ilości stron otwartych oraz zablokowanych. Aplikacja loguje adresy odwiedzanych stron, informując o rodzaju podjętej akcji (wyświetlona lub zamknięta). W panelu wyświetlanych jest 250 ostatnio otwieranych witryn. Program nie filtruje słów wpisywanych do wyszukiwarki, ale sprawnie zamyka strony z wynikami wyszukiwania dotyczącymi



Podgląd profilu użytkownika i jego aktywności w Internecie

niepożądanych treści (pornografia, używki, wulgaryzmy). Bardzo ciekawą funkcją jest możliwość wysłania informacji o zdarzeniach (np. na temat nielegalnych lub szkodliwych treści znalezionych w Internecie) do hotline'u – punktu kontaktowego prowadzonego przez Fundację dla Śląska *(http://www.dlaslaska.pl/)*.

Dostępność testowanych aplikacji

Tab. 12 prezentuje dostępność oprogramowań filtrujących poddanym testom – przykładowo, w pełni funkcjonalne wersje Ochraniacza i X Guard II są bezpłatne i można je pobrać z Internetu.

Beniamin	Program dostępny bezpłatnie w pełnej wersji. Możliwość pobrania z Internetu.
Cenzor	Wersja pełna dostępna po wykupieniu licencji (licencja indywidualna na 5 lat – 48 zł netto).
Motyl	Wersja demonstracyjna aktywna przez 15 dni. Pełna wersja dostępna po wykupieniu licencji (licencja indywidualna na 2 stanowiska komputerowe – 42 zł lub 49 zł – w zależności od formy płatności).
Ochraniacz	W pełni funkcjonalna wersja dla użytkowników indywidualnych jest dostępna bezpłatnie w Internecie (wersja płatna jest przeznaczona dla firm oraz instytucji).
Opiekun Dziecka w Internecie	Wersja demonstracyjna aktywna przez 30 dni. Pełna wersja dostępna po wykupieniu licencji (licencja indywidualna na 1 stanowisko – 49 zł. Po upływie pierwszego roku należy wykupić abonament na kolejny rok).
Strażnik Ucznia	Wersja demonstracyjna daje możliwość 50-krotnego otwarcia programu. Wersja pełna dostępna po wykupieniu licencji (Licencja Personal na komputer domowy – 55 zł lub 65 zł – w zależności od formy płatności).
Weblock	Wersja demonstracyjna możliwa do pobrania z Internetu (brak np. ochrony hasłem). Informacji na temat wersji pełnej i opłat licencyjnych nie udało sie uzyskać.
X Guard II	Wersja testowa możliwa do pobrania z Internetu. Pełna wersja do otrzymania po wypełnieniu formularza rejestracyjnego.

Dostępność testowanych programów

Podsumowanie wyników

Wyniki przeprowadzonych testów pozwalają na sformułowanie kilku ogólnych wniosków:

1) Aplikacje filtrujące nie są w stanie monitorować całej zawartości Internetu. Ich konstrukcja opiera się na rozwiązaniach statycznych, podczas gdy Internet jest medium podlegającym nieustannym zmianom. Skutecznie można jedynie filtrować pewien wycinek globalnej Sieci. Podstawowym ograniczeniem jest wielojęzyczność serwisów internetowych – jakość filtrowania zależy między innymi od zbioru stałych kryteriów (słów kluczowych), których liczba jest praktycznie nieograniczona.

2) Filtry nie są w stanie dokonać inteligentnego rozpoznania kontekstu i grafiki. Nielegalne lub szkodliwe treści mogą zostać mylnie otagowane, umieszczone w neutralnym kontekście, bądź opisane za pomocą neutralnych słów-kluczy. Jednocześnie aplikacja filtrująca może blokować portale edukacyjne czy encyklopedie ze względu na to, że hasła odnoszące się do rozwoju płciowego człowieka będą przez nią identyfikowane jako treści zabronione.

3) Programy filtrujące w niedostateczny sposób rozpoznają także zawartość Web 2.0 – serwisów społecznościowych, blogów, fotoblogów oraz portali zawierających pliki muzyczne i filmowe.

4) Większość aplikacji nie zawiera wykazu blokowanych kategorii, co może utrudnić administratorom (rodzicom, opiekunom, nauczycielom) właściwą i pożądaną ze względu na dobro rozwoju dziecka konfigurację programu.

5) Dobrą praktyką jest tworzenie niezależnych profili ustawień dla różnych użytkowników, co daje administratorowi możliwość ich modyfikacji (np. dostosowania do wieku dziecka) i pozwala mu na lepszą kontrolę aktywności poszczególnych użytkowników.

6) Nie istnieje powszechne, doskonałe rozwiązanie techniczne, które mogłoby zastąpić rodzica/nauczyciela w procesie wychowania dziecka i nauce rozważnego korzystania z Internetu; przy braku odpowiedniej edukacji skuteczność działania aplikacji filtrującej znacznie się obniża – szczególnie w przypadku starszych dzieci.

7) Program filtrujący nie jest w stanie nakłonić użytkownika Internetu do unikania niebezpiecznych bądź niefrasobliwych zachowań online, ponieważ młody internauta niekoniecznie musi uświadamiać sobie skalę potencjalnych zagrożeń.

8) Ważnym elementem działania aplikacji filtrujących jest prawidłowy opis komunikatu o zablokowaniu strony, który powinien pełnić nie tylko funkcję odstraszającą, ale i edukacyjną.

Korzystanie z aplikacji filtrujących może pomóc w lepszej ochronie dzieci przed niechcianymi i niepożądanymi treściami w Internecie. Rodzice powinni stosować programy filtrujące

i jednocześnie mieć świadomość, na jakie treści lub ludzi może natrafić ich dziecko podczas surfowania. Dlatego to właśnie na nich spoczywa największa odpowiedzialność za internetową edukację dzieci. Rodzice powinni towarzyszyć dzieciom w procesie poznawania Internetu, uwrażliwiać je na zagrożenia, uczyć odpowiedzialnego i etycznego zachowania. Mogą zawrzeć z dzieckiem rodzaj „umowy" na korzystanie z Internetu, która będzie podstawą do kształtowania dobrych nawyków (przykładowe umowy można znaleźć na stronie www.dzieckowsieci.pl). Rodzice nie powinni jednak nadmiernie ingerować w sposób korzystania przez dziecko z Sieci. Trzeba również pamiętać, że zalety Internetu przewyższają jego wady, a ciekawość dziecka jest rzeczą naturalną.

Skuteczna ochrona dzieci i młodzieży przed szkodliwymi i nielegalnymi treściami wymaga wsparcia ze strony instytucji rządowych, szkół, a także dostawców usług internetowych. 11 kwietnia 2007 r. Sejm przyjął nową ustawę, która przewiduje m.in. wprowadzenie regulacji dotyczących problemu ochrony dzieci przed treściami mogącymi stanowić zagrożenie dla ich prawidłowego rozwoju psychicznego i moralnego.

Do działań na rzecz bezpieczeństwa dzieci i młodzieży w Internecie warto włączyć również kawiarenki internetowe. Stworzenie odpowiednich stanowisk dla młodych internautów (posiadających np. oprogramowanie filtrujące, ale również dające możliwość korzystania z różnych gier online) może pomóc w kształtowaniu odpowiedniej wrażliwości społecznej i upowszechnieniu świadomości, w jaki sposób najlepiej korzystać z jego zasobów.

Serwisy związane z programem Safer Internet:
www.saferinternet.pl
www.dzieckowsieci.pl
www.helpline.org.pl
www.dyzurnet.pl
www.sieciaki.pl
www.przedszkolaki.sieciaki.pl
www.dbi.pl

"Art. 4a. 1. Rada Ministrów, w drodze rozporządzenia, nałoży na szkoły i placówki zapewniające uczniom korzystanie z usługi dostępu do Internetu na ich terenie obowiązek zainstalowania i aktualizowania oprogramowania zabezpieczającego przed dostępem do treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju psychicznego uczniów, oraz określi minimalne wymagania, jakie powinno spełniać to oprogramowanie.

2. W rozporządzeniu, o którym mowa w ust. 1, zostanie określony szczegółowy zakres treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju psychicznego i moralnego uczniów, w szczególności pornograficznych, eksponujących brutalność i przemoc, zawierających zachowania naruszające normy obyczajowe, propagujących nienawiść i dyskryminację.

3. Minister właściwy do spraw oświaty i wychowania zapewni szkołom i placówkom możliwość nieodpłatnego korzystania z oprogramowania zabezpieczającego przed dostępem do treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju psychicznego i moralnego uczniów, spełniającego minimalne wymagania, o których mowa w ust. 1, w wersjach działających w systemach operacyjnych powszechnie użytkowanych na obszarze kraju, z uwzględnieniem zasady równego traktowania różnych platform systemowych.

4. Szkoły i placówki mogą, w celu realizacji obowiązku, o którym mowa w ust. 1, wykorzystywać inne oprogramowanie spełniające minimalne wymagania, o których mowa w ust. 1."

Od początku 2007 r. przy Fundacji Dzieci Niczyje działa Helpline.org.pl – punkt kontaktowy, do którego można zgłaszać przypadki zagrożenia bezpieczeństwa dzieci i młodzieży w Internecie.

Z pracownikami „Helpline"
można skontaktować się
za pomocą komunikatora online
(ze strony **www.helpline.org.pl**),
e-maila **helpline@helpline.org.pl**
lub telefonu **0800 100 100** (połączenie bezpłatne).
Helpline doradza także rodzicom i osobom
zawodowo pracującym z dziećmi.

**Jeśli w Internecie
coś Cię zaniepokoiło,
ktoś nęka Ciebie
lub Twoich kolegów,
wypytuje o nazwisko, wiek, adres,
zadaje krępujące pytania,
skontaktuj się
z Helpline.org.pl.**

Zestaw dobrych praktyk korzystania z Internetu

- Rodzic jest pierwszym przewodnikiem dziecka po Internecie.
- Należy wspólnie z dzieckiem ustalić zasady korzystania z Internetu.
- Rodzic powinien wspólnie z dzieckiem odkrywać i tworzyć bazę przyjaznych stron WWW (szczególnie w przypadku najmłodszych użytkowników Internetu).
- Należy uwrażliwić dziecko na potencjalne zagrożenia w Sieci związane z:
  - nawiązywaniem nowych znajomości w Internecie,
  - podawaniem danych osobowych,
  - odbieraniem i otwieraniem poczty elektronicznej pochodzącej z niewiadomego źródła i od obcych osób,
  - ściąganiem plików.
- Należy uczyć dziecko krytycznego podejścia do informacji znalezionych w Internecie i konieczności ich weryfikacji z informacjami zawartymi w słownikach, encyklopediach, etc.
- Należy przekonać dziecko, aby zgłaszało rodzicom fakt napotkania nieprzyjemnych, szkodliwych lub nielegalnych treści. Poinformuj je o istnieniu specjalnych punktów kontaktowych, takich jak dyzurnet.pl czy helpline.org.pl.
- Należy nauczyć dziecko właściwego zachowania w Sieci (tzw. netykiety), aby:
  - nie spamowało (nie wysyłało innym internautom niechcianych wiadomości, linków, plików, etc.),
  - nie rozsyłało tzw. „łańcuszków szczęścia”,
  - nie nadużywało emotikonów (graficznej ilustracji stanów emocjonalnych), które mają być dodatkiem do tekstu, a nie główną treścią komunikatu,
  - nie nagabywało osób, które sobie tego nie życzą,
  - nie wyzywało i obrażało innych internautów i nie dało się do tego sprowokować,
  - nie nękało i nie kompromitowało innych internautów (treści umieszczone w Internecie mają dużą siłę oddziaływania i nie da się ich ostatecznie usunąć).