RAPORT

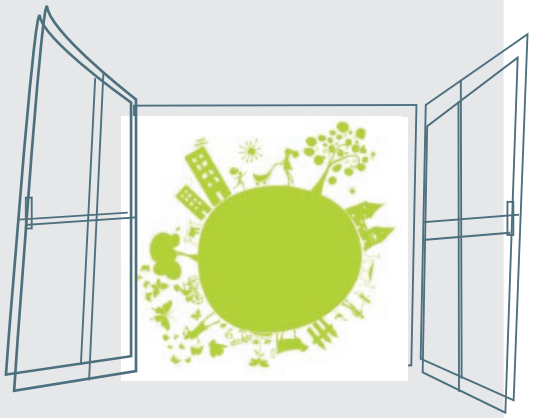
ROZWIĄZANIA FILTRUJĄCE NIEPOŻĄDANE TREŚCI w INTERNECIE

Dyżurnet.pl

Warszawa 2009

NASK s@ferinternet.pl dyżurnet.pl inhope. Internet Hotline Providers

Rozwiązania filtrujące niepożądane treści w Internecie

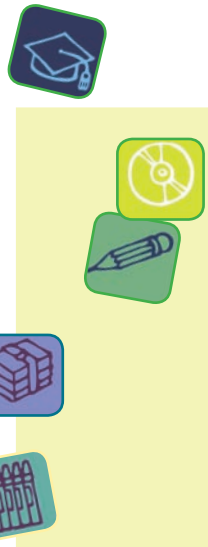


Poniższy raport został przygotowany przez specjalistów z projektu SaferInternet.pl:
Izabelę Jończyk, Marcina Mielniczka, Katarzynę Pączek, Martynę Różycką.
Pytania i sugestie proszę przesyłać na adres: ***info@dyzurnet.pl***.

Więcej informacji o zespole Dyżurnet.pl i jego działalności znajduje się na stronie ***www.dyzurnet.pl***.
Elektroniczna wersja niniejszego raportu znajduje się na stronach: ***www.dyżurnet.pl*** oraz ***www.saferinternet.pl***

Warszawa 2009

1. Wstęp



Bezpieczeństwo dzieci w Internecie jest priorytetowym celem Safer Internet – projektu Komisji Europejskiej, realizowanego w Polsce od 2005 roku przez Naukową i Akademicką Sieć Komputerową oraz Fundację Dzieci Niczyje. W 2007 roku w ramach projektu zostały przeprowadzone testy skuteczności programów filtrujących[1]. Opracowany na ich podstawie raport został bardzo pozytywnie przyjęty przez rodziców, nauczycieli oraz producentów programów filtrujących.

W ramach Polskiego Centrum Programu „Safer Internet" realizowane są 3 projekty:

- **Saferinternet.pl** – projekt, którego celem jest zwiększanie społecznej świadomości na temat zagrożeń, jakie niosą ze sobą najnowsze techniki komunikacji. Wśród podejmowanych działań priorytetem jest edukacja, zarówno dzieci, jak i rodziców, a także podnoszenie kompetencji profesjonalistów w zakresie bezpiecznego korzystania z Internetu.
  Więcej informacji: www.saferinternet.pl
- **Helpline.org.pl** – projekt, w ramach którego udzielana jest pomoc młodym internautom, rodzicom i profesjonalistom w przypadkach zagrożeń związanych z korzystaniem z Internetu oraz telefonów komórkowych przez dzieci i młodzież.
  Więcej informacji: www.helpline.org.pl
- **Dyżurnet.pl** – punkt kontaktowy, tzw. hotline, do którego można anonimowo zgłaszać przypadki występowania w Internecie treści zabronionych prawem takich, jak pornografia dziecięca, pedofilia, treści o charakterze rasistowskim i ksenofobicznym.
  Więcej informacji: www.dyzurnet.pl

Jako że producenci nieustannie udoskonalają swoje aplikacje, zaszła potrzeba przeprowadzenia kolejnej edycji testów nowych wersji programów. Oprócz typowych aplikacji filtrujących analizie zostały również poddane moduły kontroli rodzicielskiej w programach antywirusowych oraz inne rozwiązania, które mogą zwiększać bezpieczeństwo dzieci i młodzieży w Internecie.

W ramach programu Safer Internet co roku odbywa się europejska edycja testów programów i modułów kontroli rodzicielskiej SIP-Bench. Badania te mają na celu m.in. sprawdzenie:

- Czy filtrowanie oferowane przez produkt może zostać dostosowane do potrzeb różnych kategorii wiekowych, różnych języków, kultur poziomów ochrony?
- Czy produkt ma poważny wpływ na funkcjonowanie komputera użytkowanego przez dzieci?
- Czy dzieci mogą pominąć produkt lub nim manipulować?
- Czy interfejs użytkownika może być używany przez osobę, która nie mówi po angielsku?
- Czy filtrowanie może zostać dostrojone do różnorodnych języków, kultur, religii i kontekstów narodowych Europy?

Wyniki badań znajdują się na stronie www.sip-bench.eu.

[1] Więcej informacji na stronie: *http://www.dyzurnet.pl/images/stories/PDF/raport _ filtrowanie.pdf*

1.1 Nielegalne i szkodliwe treści

Wobec niedostatecznej ochrony dziecka przed nieodpowiednimi treściami, szereg firm i instytucji działa na rzecz podniesienia bezpieczeństwa. Moduły kontroli rodzicielskiej znajdują się w wielu produktach wspomagających bezpieczne surfowanie w Internecie.

Internet zawiera treści wartościowe, jak i szkodliwe dla dziecka. Nawet jeśli szuka ono serwisów z dziecięcymi grami komputerowymi online, może się zdarzyć, iż wpisując nazwę portalu zrobi literówkę i wówczas trafi na stronę zawierającą nieodpowiednie materiały. Na taką stronę dziecko może trafić wybierając nieadekwatny wynik znajdujący się w wynikach wyszukiwania czy przechodząc na link umieszczony na forum.

Niestety prawo nie jest w stanie zapewnić młodemu odbiorcy dostatecznej ochrony przed szkodliwymi treściami internetowymi. W polskim prawie istnieje tylko ograniczenie wiekowe odbiorcy treści pornograficznych.

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 pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej;
- treści publicznie propagujących 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.

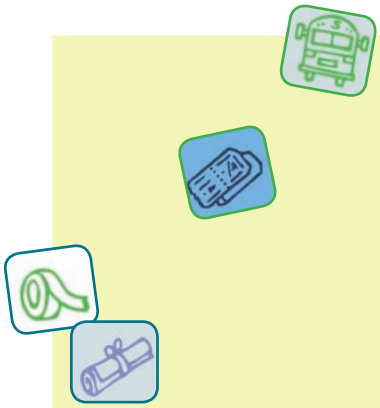
Niezgodne z prawem jest także:

- 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

Kontakt dziecka z wyżej wymienionymi treściami może sprawić, że:

– świat stanie się dla niego niezrozumiały, zagrażający i przestanie się ono czuć w nim bezpieczne
– podejmie działania przynoszące szkodę jemu samemu lub innym ludziom (w tym działania niezgodne z prawem)
– jego rozwój psychoseksualny zostanie zaburzony (w przypadku treści pornograficznych)
– będzie się zachowywało agresywnie wobec rówieśników, słabszych czy ludzi innej narodowości, wyznania itd.(w przypadku treści o charakterze rasistowskim lub zawierających przemoc)
– nawiąże relacje z osobami, które mają wobec niego złe intencje [2]

[2] Więcej informacji na stronie: *http://www.dzieckowsieci.pl/strona.php?p=82 (2009-08-01)*



Według badań[3] firmy Gemius SA (2009) 40% respondentów twierdzi, że treści pornograficzne są publikowane w Internecie w sposób łatwo dostępny dla dzieci oraz, że przynajmniej czasami, są one udostępniane najmłodszym w sposób celowy.

Innymi przykładami szkodliwych treści, z jakimi mogą się zetknąć surfujące w Internecie dzieci i młodzież, są:

- wulgaryzmy
- 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 poprzez podkreślenie ich rzekomo leczniczych właściwości czy poprzez wskazanie, że otwierają one człowieka na przeżycia duchowe;
- treści promujące środki farmaceutyczne takie jak tabletki gwałtu, dopalacze, sterydy, leki;
- drastyczne materiały – zdjęcia ofiar wypadków, samobójstw, egzekucji.

Ponadto podczas korzystania z Internetu dzieci mogą się zetknąć z niepokojącymi zjawiskami, takimi jak:

- cyberbulling – forma przemocy polegająca na wyzywaniu, ośmieszaniu, szantażowaniu czy rozprzestrzenianiu kompromitujących materiałów w Sieci przy użyciu technologii informacyjnych i komunikacyjnych (komunikatorów, czatów, stron www, blogów, SMS-ów i MMS-ów);
- grooming – 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 jej „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.

Z raportu „EU Kids Online"[4], przedstawiającego analizę wyników z 250 badań dotyczących używania Internetu przez dzieci i młodzież w Unii Europejskiej wynika, że ponad połowa rodziców obawia się: kontaktu dziecka z treściami pornograficznymi lub związanymi z przemocą (65% UE, 67% PL); uwodzenia dziecka przez nieznajomych w Sieci (60% UE, 56% PL); dostępu do informacji dotyczących samookaleczenia, samobójstwa, anoreksji (55% UE, 60% PL), dokuczania dziecku przez rówieśników (54% UE, 56% PL); społecznej izolacji dziecka ze względu na ilość czasu spędzanego przed komputerem (53% UE, 56% PL). Nieco mniej rodziców niepokoi się możliwością przekazania przez dziecko prywatnych informacji – (47% w UE, 38% PL). Warto zaznaczyć, że tylko co trzecie dziecko (w Polsce i Europie) zwraca się do rodziców o pomoc w trudnej sytuacji związanej z Internetem. W przypadku poważniejszych zagrożeń o pomoc prosi jedynie co 10 dziecko. **Jedynie połowa rodziców w Polsce zainstalowała na domowym komputerze program filtrujący lub monitorujący aktywność dziecka w Sieci.** 16% z badanych rodziców nie potrafi jednak korzystać z tego rodzaju oprogramowania. Jasno i wyraźnie kształtuje się zatem obraz polskiego rodzica, który ma stosunkowo wysoką świadomość zagrożeń, ale często nie dysponuje wystarczającą wiedzą i umiejętnościami, by zadbać o bezpieczeństwo dziecka surfującego w Internecie.

[3] Wyniki badań dostępne na stronie: *http://pliki.gemius.pl/Raporty/2009/2009 _ 06 _ Pornografia _ dziecieca _ w _ internecie.pdf (2009-08-01)*

[4] Raport dostępny na stronie *http://www.lse.ac.uk/collections/EUKidsOnline/ (2009-08-01)*

1.2 Klasyfikacje treści

Choć można się spotkać z różnymi próbami klasyfikacji stron internetowych, brakuje regulacji w zakresie międzynarodowych oznaczeń, które informowałyby o przeznaczeniu zamieszczonych treści dla danej kategorii wiekowej. Najlepszym rozwiązaniem byłoby stosowanie samoregulacji przez właścicieli serwisów internetowych.

1.2.1 Klasyfikacja ICRA

Jednym z przykładów klasyfikacji treści jest Internet Content Rating Association (ICRA)[5] – dawniej RSACI (Tab. 1 na s. 6, 7).

System został opracowany w oparciu o badania dr Donalda F. Roberta z Uniwersytetu Stanforda. Administratorzy strony dobrowolnie zgłaszają swoją witrynę do Instytutu, przypisując jej jedną z dostępnych kategorii. Następnie otrzymują wygenerowany kod, który zamieszczają na stronie. Jest on odczytywany przez przeglądarki np. Internet Explorer, co pozwala na poprawne zdefiniowanie odbiorców.

1.2.2 Klasyfikacja PEGI

W przypadku gier komputerowych takim jednolitym i stosowanym obecnie w większości krajów Europy systemem klasyfikacji (tzw. rating wiekowy) jest PEGI[6]. Został on stworzony w celu udzielenia rodzicom pomocy w podejmowaniu świadomej decyzji o zakupie gier komputerowych. Znaki ratingu PEGI znajdują się z przodu i z tyłu opakowania gry. Są to znaki 3+, 7+, 12+, 16+ i 18+. Dostarczają one wiarygodnych informacji o stosowności treści gry z punktu widzenia ochrony nieletnich. Rating wiekowy nie obejmuje poziomu trudności ani umiejętności niezbędnych do korzystania z danej gry. System PEGI jest wspierany przez głównych producentów konsol, a także wydawców i twórców gier interaktywnych.

PEGI 3+ – Treść gier oznaczonych w ten sposób uznaje się za odpowiednią dla wszystkich grup wiekowych. Dopuszczalna jest pewna ilość przemocy w kontekście komicznym (zwykle podobna do prezentowanej w kreskówkach w rodzaju Królika Bugsa czy Toma i Jerry'ego). Dziecko nie powinno utożsamiać postaci pojawiających się na ekranie z postaciami rzeczywistymi. Powinny one być w całości wytworem fantazji. Gra nie powinna także zawierać dźwięków ani obrazów, które mogą przestraszyć dziecko. Nie powinien się w niej ponadto pojawiać wulgarny język, sceny przedstawiające nagość ani odniesienia do aktywności seksualnej.

PEGI 7+ – Gry, które w innym przypadku zostałyby zakwalifikowane do grupy 3+, lecz zawierają dźwięki lub sceny potencjalnie przerażające najmłodszych odbiorców, mogą być uznane za odpowiednie dla tej grupy wiekowej. Dopuszczalne są sceny obejmujące częściową nagość, ale nigdy w kontekście seksualnym.

[5] Więcej na temat klasyfikacji ICRA można odnaleźć na stronie http://www.fosi.org/cms/

[6] Więcej informacji o klasyfikacji PEGI znajduje się na stronie http://www.pegi.info/pl/

PEGI 12+ – Gry wideo pokazujące przemoc o nieco bardziej realistycznym charakterze, skierowaną przeciw postaciom fantastycznym i/lub nierealistyczną przemoc wobec postaci o ludzkim lub rozpoznawalnych zwierząt, ponadto w tej kategorii wiekowej dopuszczalna jest nieco bardziej dosłowna nagość. Ewentualne wulgaryzmy muszą mieć łagodny charakter i nie mogą zawierać odwołań do seksu.

PEGI 16+ – Ten symbol jest nadawany, jeżeli przemoc lub aktywność seksualna wyglądają tak jak w rzeczywistości. Młodzież w tym wieku powinna również być odporna na brutalniejsze wulgaryzmy, sceny pokazujące używanie tytoniu lub narkotyków oraz sceny popełniania przestępstw.

PEGI 18+ – Za gry dla dorosłych uznaje się gry przedstawiające daleko posuniętą przemoc i/lub specyficzne rodzaje przemocy. Daleko posunięta przemoc jest najtrudniejsza do zdefiniowania, ponieważ w wielu przypadkach jest to pojęcie bardzo subiektywne, ale ogólnie można ją określić jako sceny przemocy powodujące u widza uczucie odrazy.

Oznaczenia zamieszczone z tyłu opakowania podają najważniejsze przyczyny zaliczenia gry do danej klasyfikacji wiekowej. Jest osiem takich oznaczeń: przemoc, wulgaryzmy, lęk, narkotyki, seks, dyskryminacja, hazard i gra w Internecie z innymi ludźmi.

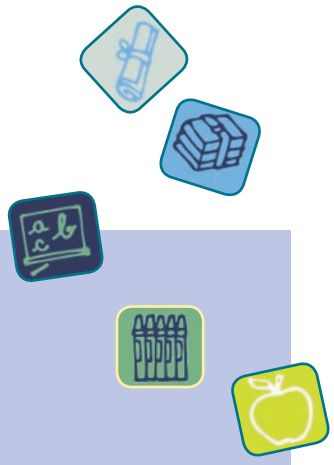
Wulgarny język – w grze jest używany wulgarny język	
Dyskryminacja – gra pokazuje przypadki dyskryminacji lub zawiera materiały, które mogą do niej zachęcać	
Używki – w grze pojawiają się nawiązania do narkotyków lub jest pokazane zażywanie narkotyków	
Strach – gra może przestraszyć młodsze dzieci	
Hazard – gry, które zachęcają do uprawiania hazardu lub go uczą	
Seks – w grze pojawiają się nagość i/lub zachowania seksualne lub nawiązania do zachowań o charakterze seksualnym	
Przemoc – gra zawiera elementy przemocy	
Online gameplay – game can be played online	

	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 ustawienia	Namawianie do dyskryminacji lub krzywdzenia i prezentowanie takich zachowań w dowolnym kontekście
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;	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 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 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 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 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 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 widoczne dotyki seksualne w kontekście sztuki, medycyny, edukacji, sportu lub wiadomości; namiętne pocałunki w dowolnym kontekście; brak zawartości jawnie seksualnej	Pośrednie i ukryte czynności seksualne, widoczne dotyki seksualne 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
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 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 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. 1 Klasyfikacja treści internetowych ICRA

2. Testy programów filtrujących



Celem drugiej edycji testów aplikacji filtrujących było:

- sprawdzenie skuteczności ochrony automatycznej dzieci i młodzieży przed szkodliwymi i nielegalnymi treściami w Internecie;
- stworzenie na podstawie otrzymanych wyników wiarygodnego i rzetelnego przewodnika po polskojęzycznych rozwiązaniach filtrujących;
- promocja idei używania rozwiązań filtrujących.

Decyzja o poddaniu ocenie programów dostępnych w polskiej wersji językowej wynika z przekonania, że wyniki testów będą miały wówczas większą przydatność dla polskich rodziców i nauczycieli (np. ze względu na lepsze zrozumienie ich funkcjonalności czy rozpoznawanie przez filtry polskich słów kluczowych).

Zamiarem autorów nie było stworzenie zestawiania rankingowego. Niniejsza publikacja może jednak pomóc rodzicom, nauczycielom i opiekunom w wyborze odpowiedniego dla ich potrzeb rozwiązania filtrującego oraz uczulić na konieczność edukacji dzieci w zakresie korzystania z zasobów internetowych.

2.1 Techniczne aspekty testów

Mając na uwadze oczekiwania opiekunów względem funkcjonalności i skuteczności rozwiązań filtrujących, badanie podzielono na trzy etapy. Na **pierwszy etap** składał się przegląd oraz testowanie funkcji, jakie posiada aplikacja. Zwrócono uwagę m.in. na: ograniczenia czasowe, możliwość modyfikacji ustawień czy informacje o tym, jakiego rodzaju strony są blokowane. Kryteria badania zostały dobrane w taki sposób, aby porównać właściwości aplikacji bez ich wartościowania.

> Niektórym opiekunom zależy na pełnej informacji o tym, co robi dziecko w Sieci – jakie odwiedza strony i ile czasu na nich spędza. Innym wystarcza jedynie informacja o stronach, które zostały zablokowane.

Drugi etap badania dotyczył skuteczności oprogramowania w filtrowaniu stron internetowych, które mogą być dla dzieci szkodliwe. Próbka badawcza zawierała strony pornograficzne, serwisy ze zdjęciami ofiar wypadków, treści ewidentnie nawołujące do zachowań rasistowskich i ksenofobicznych, strony propagujące sekty, anoreksję, bulimię, samookaleczenia, samobójstwa, różnego rodzaju używki oraz zawierające wulgarny język.

W trzecim etapie badania sprawdzano nadwrażliwość filtrów na strony internetowe zawierające określone słowa kluczowe (np. piersi, seks), na których jednak nie było zamieszczonych treści szkodliwych, a jedynie informacje medyczne (np. o raku piersi), edukacyjne (np. o dojrzewaniu płciowym) lub inne (np. o zespole Sex Pistols).

Skuteczność programów filtrujących mierzono **przy najbardziej czułym** ustawieniu filtru. Każdą aplikację testowano za pomocą programu, który na potrzeby badania został napisany przez specjalistów z zespołu CERT Polska. Dzięki przeprowadzeniu testów na jednej bibliotece stron WWW uzyskano jednorodny materiał porównawczy dla każdej z aplikacji. Każda ze stacji roboczych, na których były przeprowadzane testy, została wyposażona w system operacyjny Windows XP Professional 2002 oraz przeglądarki Internet Explorer 6.0, Firefox 3.0.12, Opera 9.02, Chrome 2.0.172.37. Wybór tego typu przeglądarek internetowych był podyktowany ich popularnością wśród polskich użytkowników oraz – w przypadku przeglądarki Chrome – zakończeniem prac nad wersją BETA i szeroką kampanią medialną produktu (Tab. 2).

Lp	Grupy przeglądarek	Użytkownicy (Cookies)
		27.07-02.08.2009
1	Internet Explorer	51.32%
2	Firefox	36.42%
3	Opera	9.11%
4	Chrome	2.11%

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

Każdy z producentów oprogramowania filtrującego był poinformowany o przeprowadzonym badaniu, a analiza każdego z produktów odbywała się tylko za wyraźną zgodą producenta.

2.2 Kryteria badania

Kryteria badawcze, według których testowano aplikacje filtrujące, podzielono na 4 grupy:

- kryteria ogólne;
- opcje filtrowania;
- wsparcie techniczne;
- sposób raportowania.

Kryteria ogólne

Kryterium	Opis
Przyjazny interfejs	Łatwość obsługi programu; zastosowanie intuicyjnych rozwiązań;klarowność komend i opisu opcji; element dodatkowy oceny – jakość graficznego opracowania interfejsu; język polski
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

Opcje filtrowania

Kryterium	Opis
Kontrola wysyłania danych osobowych	Możliwość i skuteczność kontroli przesyłania danych osobowych, np. podczas 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, nie statycznych 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.

Wsparcie techniczne

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) przez Internet
Instrukcja instalacji	Łatwość instalacji i odinstalowania, instrukcja „krok po kroku" procesu instalacji
Dostępna dokumentacja (help)	Opis ustawień programu

Sposób raportowania

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

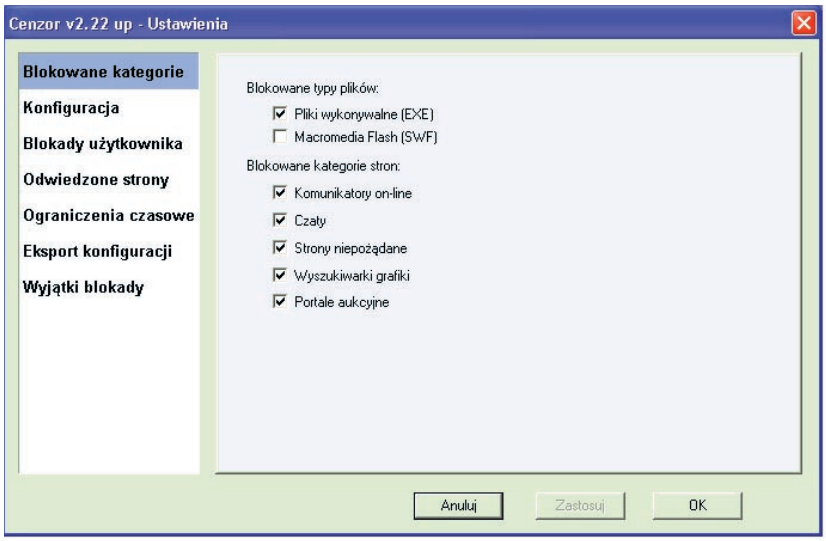
Przegląd funkcji programów 2.3

Poniżej został zamieszczony przegląd testowanych programów z wyszczególnieniem ich najważniejszych funkcji.

Cenzor 2.3.1

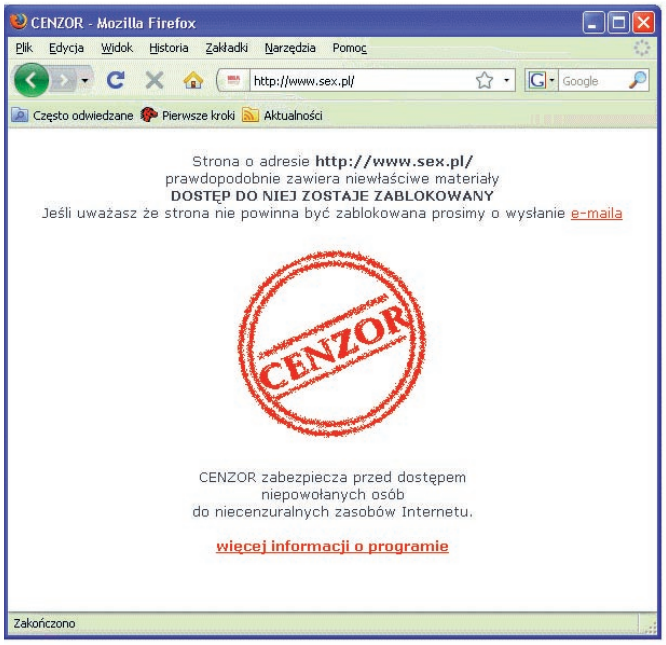
Strona producenta programu: ***http://www.cenzor.pl***

Producent oferuje 3 wersje programu: Cenzor IND – wersja jednostanowiskowa, dla indywidualnych odbiorców, Cenzor EDU – wersja wielostanowiskowa, edukacyjna przeznaczona dla placówek oświatowych oraz Cenzor BIZ – wersja biznesowa dla firm. Dla potrzeb projektu przetestowano Cenzor IND. Zgodnie z opisem producenta program blokuje dostęp do stron szkodliwych takich jak: pornografia, przemoc oraz narkomania. Posiada prosty, funkcjonalny i czytelny interfejs, przez co użytkownik w intuicyjny sposób może dowolnie go konfigurować wg własnych preferencji. Baza blokowanych stron jest automatycznie aktualizowana. Dzięki zakładce *Blokady użytkownika* można utworzyć własną listę stron zakazanych oraz poprzez zakładkę *Wyjątki blokady* można zdefiniować strony, jakie – mimo że normalnie program by je zablokował – mają się wyświetlać (Rys 1).



Rys 1. Panel administratora w programie Cenzor

Ponadto w ustawieniach konfiguracji można zaznaczyć, by program był niewidoczny dla użytkownika programu. Zakładka *Ograniczenia czasowe* umożliwia zarządzanie czasem korzystania z Internetu. Dzięki temu rodzic może wprowadzić limit dzienny i tygodniowy dostępu do Internetu. Cenzor zapisuje informacje o odwiedzanych stronach internetowych. Zapis podzielony jest na 3 szczegółowe kategorie: *Strony HTML*, *Wszystkie dane* oraz *Zablokowane*. W przypadku zablokowanej strony program podkreśla na czerwono adres URL, datę i czas zablokowania, aplikację, za pomocą której nastąpiło połączenie, kategorie blokowania np. strona niepożądana czy też czat oraz nazwę użytkownika. Cenzor umożliwia użytkownikowi zgłoszenie do producenta informacji o tym, że dana witryna nie powinna być blokowana lub że strona powinna a nie została zablokowana. Testowana wersja programu jest przeznaczona na jedno stanowisko komputerowe i nie ma możliwości tworzenia wielu profili.



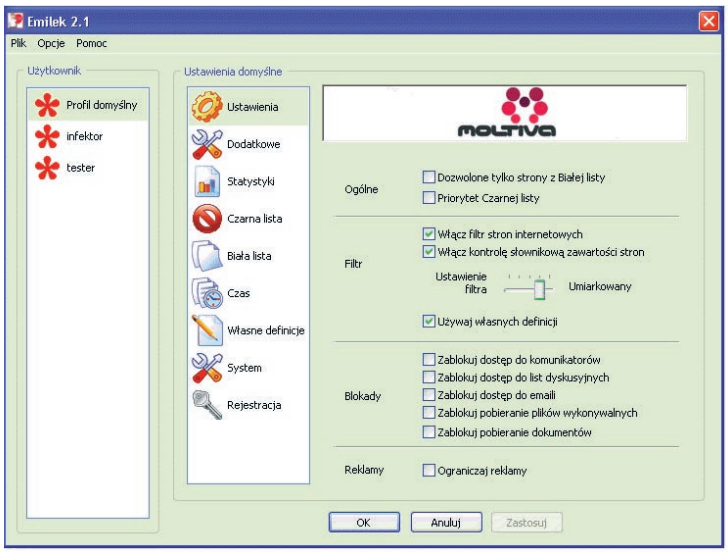
Rys 2. Komunikat zablokowania strony przez program Cenzor

Emilek 2.1

2.3.2

Strona producenta programu: *http://emilek.pl/*

Zdaniem producenta Emilek 2.1 to łatwy w obsłudze program, dzięki któremu rodzice mogą przede wszystkim blokować dostęp do stron o tematyce erotycznej i pornograficznej. Ponadto opiekunowie mogą definiować własne słowa kluczowe. Aplikacja jest przeznaczona dla użytkowników systemu Windows. Posiada intuicyjny interfejs np. duże ikonki odpowiadają symbolizowanym przez nie funkcjom. Panel administracyjny składa się z 9 zakładek: *Ustawienia, Dodatkowe, Statystyki, Czarna Lista, Biała Lista, Czas, Własne Definicje, System, Rejestracja* (Rys 3).



Rys 3. Panel administratora w programie Emilek

W zakładce *Ustawienia* administrator decyduje o zakresie filtra (dostęp do komunikatorów, list dyskusyjnych, emaili etc.). Ponadto za pomocą specjalnego suwaka może ustawić jego „czułość", czyli określić, jak restrykcyjnie filtr ma oceniać zawartość Internetu. Jeżeli program (na podstawie zdefiniowanych reguł) uzna, że strona nie powinna być zablokowana i pojawia się komunikat (Rys 4.).

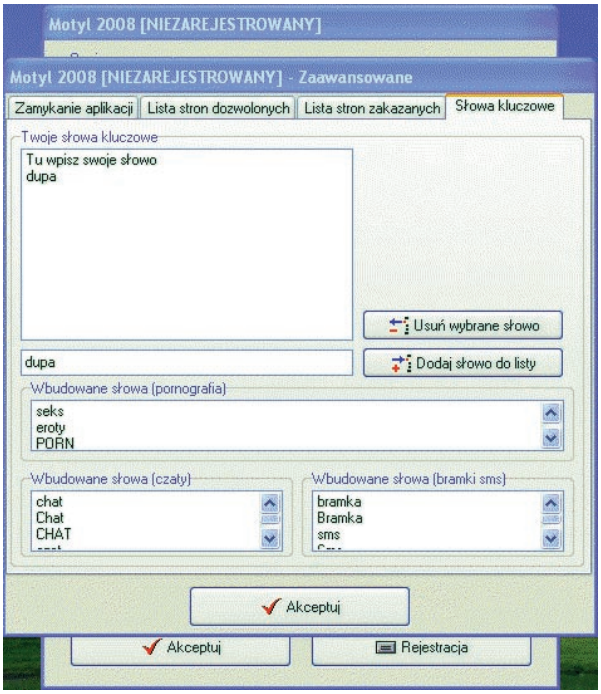
Rys 4. Komunikat zablokowania strony przez program Emilek

W dolnej części komunikatu znajduje się informacja o przyczynie zablokowania dostępu do strony, np.: *Treści erotyczne*, *Definicje użytkownika*, *Blokada reklam*. Co ciekawe, wersja Emilka 2.1 umożliwia ograniczenie dostępu dziecka do ustawień systemu Windows np. panelu sterowania, dodawania/usuwania programów, nagrywania płyt CD, zapisywania na pamięciach przenośnych USB etc. Istnieje także darmowa wersja programu dla szkół – Emilek dla Szkół 2.1.

2.3.3 Motyl

Strona producenta programu: *http://www.adalex.pl*

W panelu konfiguracyjnym użytkownik może zdefiniować opcje filtrowania w zależności od własnych preferencji. Program umożliwia blokowanie stron pornograficznych, czatów, bramek sms, komunikatorów oraz popularnych przeglądarek Opera, Firefox, Internet Explorer. Za pomocą specjalnego suwaka można zmieniać czułość programu. Producent nie opisuje jednak, co dają kolejne ustawienia suwaka i jakie są różnice w ustawieniach tej opcji. Motyl blokuje niestosowną stronę zamykając przeglądarkę i nie wyświetlając żadnego graficznego komunikatu. W przypadku gdy przeglądarka jest skonfigurowana tak, aby rozpoczynać z tymi samymi stronami co w chwili ostatniego jej zamknięcia, mogą wystąpić problemy z jej otworzeniem. Dopiero w zakładce *Raporty* można odkryć, iż dana strona nie została wyświetlona ze względu na jej nieodpowiedni charakter. Istnieje także możliwość definiowana słów czy stron dozwolonych. Służą temu zakładki: *Lista stron dozwolonych* oraz *Lista stron zakazanych* czy też *Słowa kluczowe* (Rys 5).



Rys 5. Panel administratora w programie Motyl

Program analizuje zawartość Internetu pod kątem zdefiniowanych przez użytkownika słów kluczowych bądź ich fragmentów, których pojawienie się na stronie może być powodem do jej zamknięcia. Strony jednak są zamykane zbyt wolno i to dopiero w momencie, kiedy każdy element zostanie ściągnięty. Pozwala to użytkownikowi na zapoznanie się z niestosownym charakterem strony jeszcze przed jej zablokowaniem.

Opiekun Dziecka w Internecie

2.3.4

Strona producenta programu: *www.opiekun.pl*

Producent oferuje trzy wersje programu: Opiekun Dziecka dla użytkownika domowego, Opiekun Ucznia – wersję jednostanowiskową przeznaczoną dla szkół i Opiekun Ucznia Net – wersję sieciową umożliwiającą pełną kontrolę nad całą pracownią informatyczną. Opiekun Dziecka charakteryzuje się ciekawym, kolorowym i przejrzystym interfejsem. Aplikacja zawiera opcje ograniczenia czasowego. W związku z tym rodzic ma możliwość wpływu na czas surfowania dziecka w Sieci. Program blokuje strony według kategorii: pornografia, sekty i satanizm, przemoc, narkotyki (Rys 6).

Rys 6. Panel administratora w programie Opiekun Ucznia

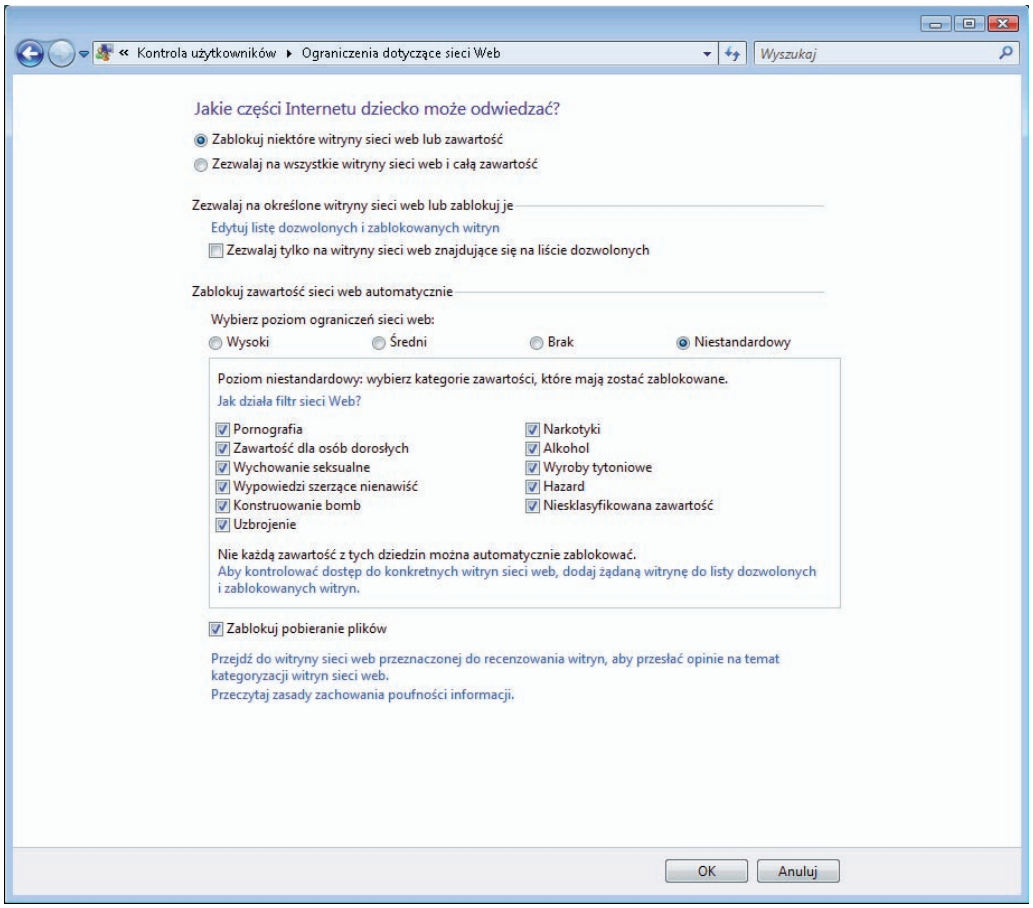
Ponadto Opiekun posiada dwie możliwości trybu pracy. Pierwszy – zaawansowany – udostępnia wszystkie funkcje programu i pozwala na stworzenie odrębnych profili ustawień dla różnych użytkowników (dzieci). Drugi – uproszczony – jest łatwiejszy w obsłudze między innymi z powodu ukrycia części zaawansowanych opcji i automatycznego wprowadzenia domyślnych ustawień. Aplikacja wyposażona jest także w funkcję raportowania rodzicom o aktywności dziecka w Sieci. Dodatkowym atutem jest możliwość zarządzania różnymi blokadami np. programów pocztowych, FTP, grup dyskusyjnych, pobierania gotowych plików typu exe. Można udostępnić dziecku wyłącznie jedną przeglądarkę. Administrator (rodzic) może również edytować listę stron zabronionych lub dozwolonych osobno dla każdego profilu. Ciekawym pomysłem jest wyposażenie programu w kalendarz, umożliwiający dokładne odczytanie stron, jakie były przeglądane w konkretnych dniach. Alert blokowania strony informuje o kategorii, wg której strona została zamknięta.

Moduł kontroli użytkowników systemu Windows Vista Ultimate

2.3.5

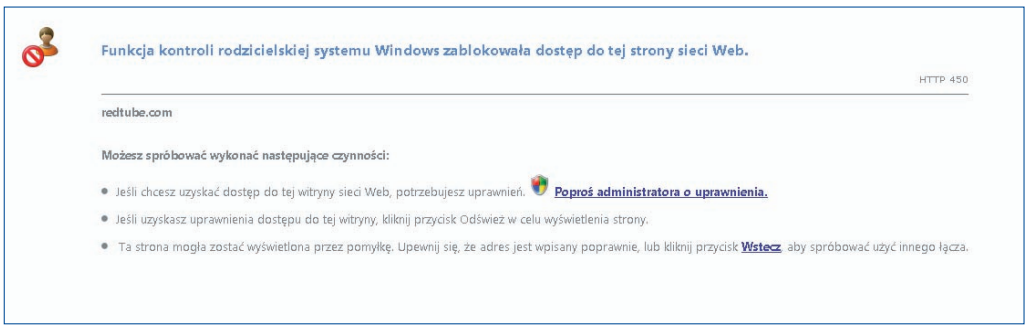
Strona producenta programu: *http://www.microsoft.com*

System operacyjny Vista pozwala na konfigurację konta dla dziecka i zdefiniowanie czynności oraz akcji, które będą dozwolone. Można ustawić ograniczenia niestandardowego filtrowania stron poprzez wybór poszczególnych kategorii treści, które powinny być blokowane (Rys 7).



Rys 7. Moduł kontroli rodzicielskiej w systemie operacyjnym Windows Vista

Istnieje możliwość dodania oraz modyfikacji czarnych i białych list. System można tak skonfigurować, aby pozwalał tylko na poruszanie się po stronach z białej listy. Korzystając z limitu czasu można określić z dokładnością do godziny w tygodniu, kiedy dziecko może używać komputera. System operacyjny kontroluje również dostęp do programów zainstalowanych na komputerze. Jest to o tyle przydatne, że na poziomie administracyjnym można zablokować np. korzystanie z komunikatorów. Podobnie można pozwolić na granie w gry zainstalowane na komputerze. Definiować można albo poszczególne gry, albo skorzystać z klasyfikacji ESRB lub PEGI przypisując dziecku jedną z wyszczególnionych kategorii.



Rys 8. Komunikat zablokowania strony przez moduł kontroli rodzicielskiej w Windows Vista

W przypadku blokady (strony www lub programu) dziecko otrzymuje informację w postaci wyświetlającego się komunikatu o przyczynie blokady (Rys 8). Ponadto dostaje wskazówkę, że może poprosić administratora komputera o odblokowanie. Istnieje możliwość zapisywania każdego zachowania dziecka w raporcie dostępnym w panelu administratora.

PANDA Internet Security 2009

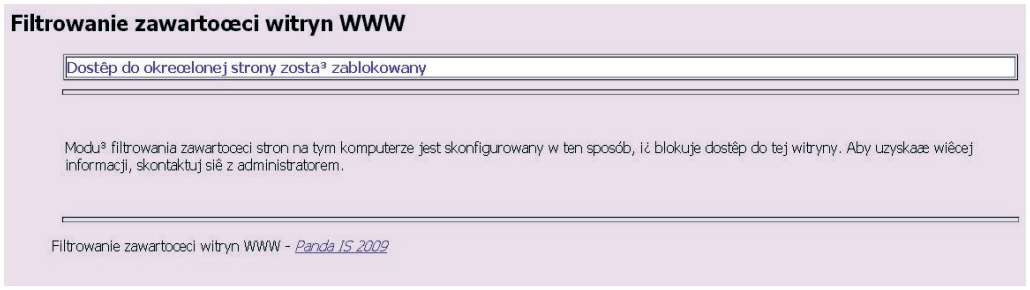
2.3.5

Strona producenta programu: ***http://www.pspolska.pl/***

Panda Internet Security 2009 jest programem antywirusowym wyposażonym dodatkowo w funkcję kontroli rodzicielskiej. Panda oferuje możliwość stworzenia niezależnych profili dla użytkowników-dzieci. Administrator może wybrać jeden ze zdefiniowanych filtrów zawartości witryn: *filtr dla dzieci, filtr dla nastolatków, filtr dla pracowników, filtr standardowy*. Filtry blokują według następujących kategorii: *Nagość, Zakupy, Społeczeństwo, Działalność przestępcza, Gry/Hazard, Rozrywka/Kultura, Informacje i komunikacje, Narkotyki, Styl Życia, Prywatne strony domowe, Praca, Finanse/Inwestycje, Broń, Medycyna, Aborcja.*

Program dość restrykcyjnie reaguje na tzw. fałszywe alarmy czyli strony zawierające edukacyjne wzmianki na temat seksu, ale nie zawierające niestosownych treści. Aplikacja umożliwia ustawienie czarnej listy stron, do których użytkownik nie będzie miał dostępu oraz białej listy stron, które zostaną wyświetlone bez względu na to, czy obejmuje je ustawiony filtr. W zakładce *Raporty* program rejestruje informacje o stronach, jakie zostały zablokowane. Choć aplikacja charakteryzuje się prostym interfejsem, brakuje czytelnego dla dziecka komunikatu o powodach zamknięcia strony (Rys 9).

Podobne funkcje – jak zapewnia producent – są dostępne w programie PANDA Global Protection 2009.



Rysunek 9. Komunikat zablokowania strony przez program PANDA Internet Security 2009

W Tab. 3 na s. 18 i 19 przedstawiono zestawienie zbiorcze funkcji, posiadanych przez badane aplikacje. Podane informacje dotyczą tylko tej wersji programu, która została wyszczególniona.

✔ *oznacza, że program spełnia dane kryterium.*

Nazwa programu	Cenzor	Emilek	Motyl	Opiekun Dziecka w Internecie	Panda	Windows Vista
Wersja programu	2.22	2.1	5.2	2.0.0.669	Internet Security 2009	ultimate
Przyjazny interfejs	✔	✔	✔	✔	✔	✔
Niezależne profile ustawień dla różnych użytkowników	brak	✔	brak	✔	✔	✔
Autom. uruchamianie się	✔	✔	✔	✔	✔	✔
Własne ustawienia	✔	✔	✔	✔	✔	✔
Możliwość czasowego wył.	✔	✔	✔	✔	brak	nie dotyczy
Ochrona hasłem	✔	✔	✔	✔	✔	✔
Opcje filtrowania						
Kontrola wysyłania danych osobowych	brak	brak	brak	brak	brak	✔
Filtrowanie/blokowanie czatów	✔	✔	✔	✔	✔	brak
Filtrowanie/blokowanie poczty	brak	✔	brak	brak	brak	brak
Filtrowanie/blokowanie usenetu	brak	brak	brak	brak	brak	✔
Filtrowanie/blokowanie komunikatorów	✔	brak	✔	✔	✔	✔
Filtrowanie przy wykorzystaniu proxy	brak	brak	✔	brak	✔	✔
Filtrowanie przy wykorzystaniu krótkiego URL	brak	✔	✔	✔	✔	✔
Filtrowanie Web 2.0	brak	brak	Nie	brak	✔	brak
Wsparcie techniczne						
Pomoc techniczna (www,tel)	✔	✔	✔	✔	✔	✔
Aktualizacje online	✔	✔	✔	✔	✔	✔
Instrukcja instalacji	✔	✔	✔	✔	✔	✔
Dostępna dokumentacja(help)	✔	✔	✔	✔	✔	✔

Sposób raportowania						
Logowanie aktywności	✔	✔	✔	✔	✔	✔
Raportowanie graficzne	✔	✔	zamknięcie przeglądarki bez raportu	✔	x/ubogi nieczytelny komunikat	✔
Wysyłanie raportów przez e-mail	brak	brak	brak	✔	✔	brak
Zapisywanie alertów	✔	brak	✔	✔	✔	✔

Tab 3. Funkcjonalność analizowanych programów

Nazwa programu	Cenzor IND	Emilek	Motyl	Opiekun Dziecka w Internecie	Panda	Windows Vista	xTerminator*
Warunki licencji	licencja 5 lat – 58,56 zł;	bezpłatny dla szkół i innych jednostek organizacyjnych systemu oświaty; wersja domowa – darmowa 30 dni; licencja roczna, na jedno stanowisko 39zł	wersja czasowa bezpłatna; licencja dla 2 komputerów 39,99 zł;	darmowe demo 30 dni; licencja roczna 49zł; przedłużenie licencji na kolejne 12 mies. – 9 zł	licencja na trzy stanowiska 209 zł	nie dotyczy**	licencja negocjowana wg warunków umowy

Tab 4. Warunki licencji programów

W powyższej tabeli zostały przedstawione warunki licencji użytkowania programu wg informacji znajdujących się na stronach producentów (dane z dnia 18-08-2009).

---

* Program jest konfigurowany wg potrzeb klienta – patrz opis programu

** Moduł jest dostępny jako część systemu operacyjnego Windows Vista

3. Wyniki testów

Testy zostały przeprowadzone na bazie 130 adresów stron WWW, przesłanych przez użytkowników Internetu do zespołu Dyżurnet.pl jako strony niepożądane, szkodliwe lub nielegalne. Za kryterium skuteczności przyjęto zamknięcie danej strony WWW (lub jej fragmentu, na którym były zamieszczone niepożądane treści) w czasie do 5 sekund po jej wyświetleniu.

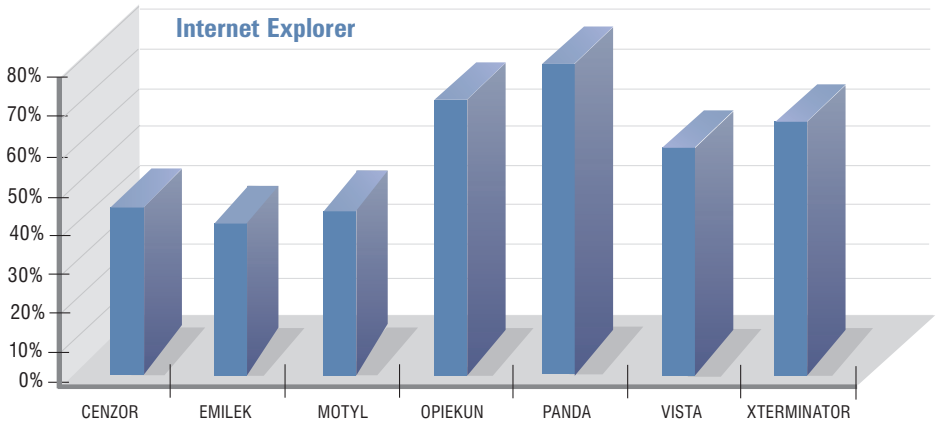
3.1. Skuteczność filtrowania

W tabeli 5 przedstawiono skuteczność aplikacji filtrujących w zależności od używanej przeglądarki internetowej. Minus (-) oznacza, że program nie działa z wykorzystaniem przeglądarki.

	Chrome	Firefox	Internet Explorer	Opera
CENZOR	-	63%	63%	66%
EMILEK	29%	48%	46%	-
MOTYL	-	45%	47%	39%
OPIEKUN	-	68%	68%	68%
PANDA	72%	77%	76%	76%
VISTA	54%	54%	55%	54%
XTERMINATOR	61%	61%	62%	61%

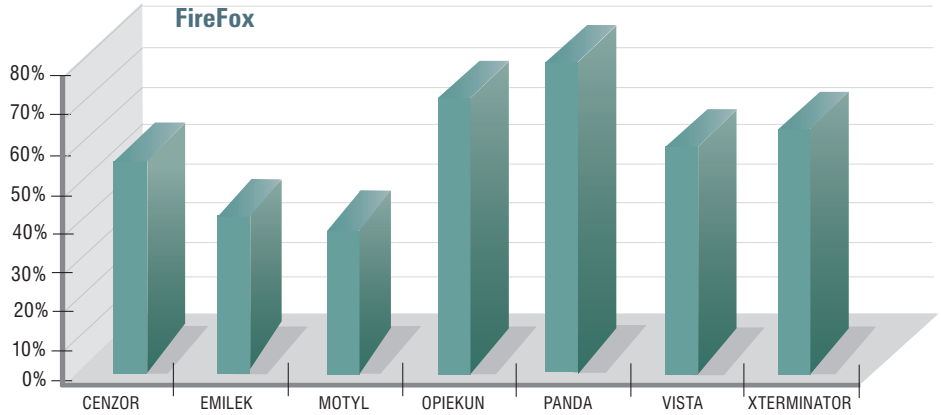
Tab 5. Skuteczność blokowania stron niepożądanych

W blokowaniu niepożądanych stron z wykorzystaniem przeglądarki Internet Explorer najskuteczniejsze są: Panda, Opiekun i Cenzor (Rys 6).



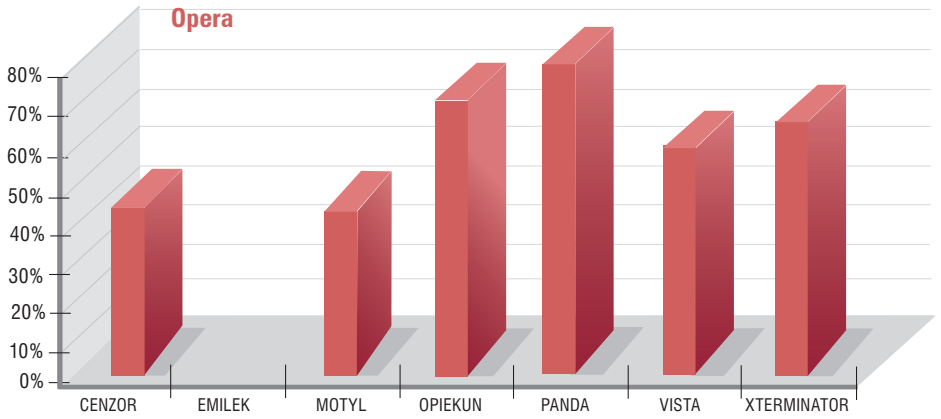
Rys 6. Skuteczność blokowania stron niepożądanych pod przeglądarką Internet Explorer

Podczas testowania pod przeglądarką Firefox, najwyższą skuteczność wykazały: Panda, Opiekun i Cenzor (Rys 7).



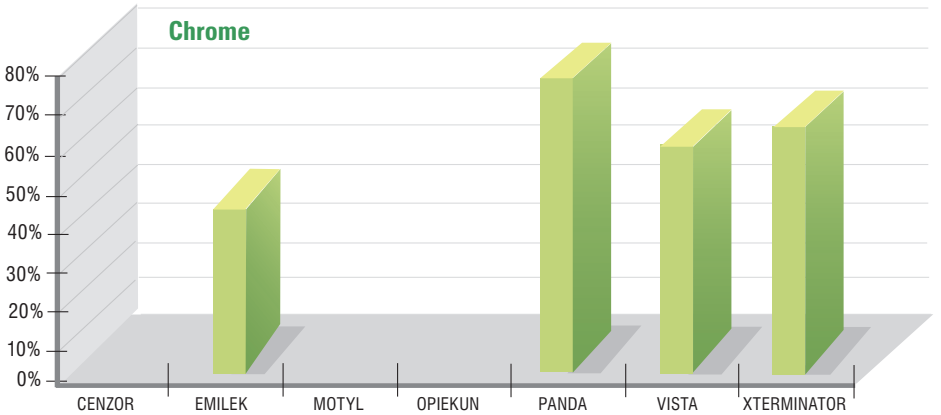
Rys 7. Skuteczność blokowania stron niepożądanych pod przeglądarką Firefox

W przypadku testów pod przeglądarką Opera wykazano, iż najwięcej stron zablokowały: Panda, Opiekun i Cenzor (Rys 8):



Rys 8. Skuteczność blokowania stron niepożądanych pod przeglądarką Opera

Jako że przeglądarka Chrome dopiero co wyszła na rynek, nie wszystkie testowane aplikacje pod nią działają (Rys 9). Najskuteczniejsze w blokowaniu niepożądanych stron okazały się: Panda, xTerminator oraz Vista.



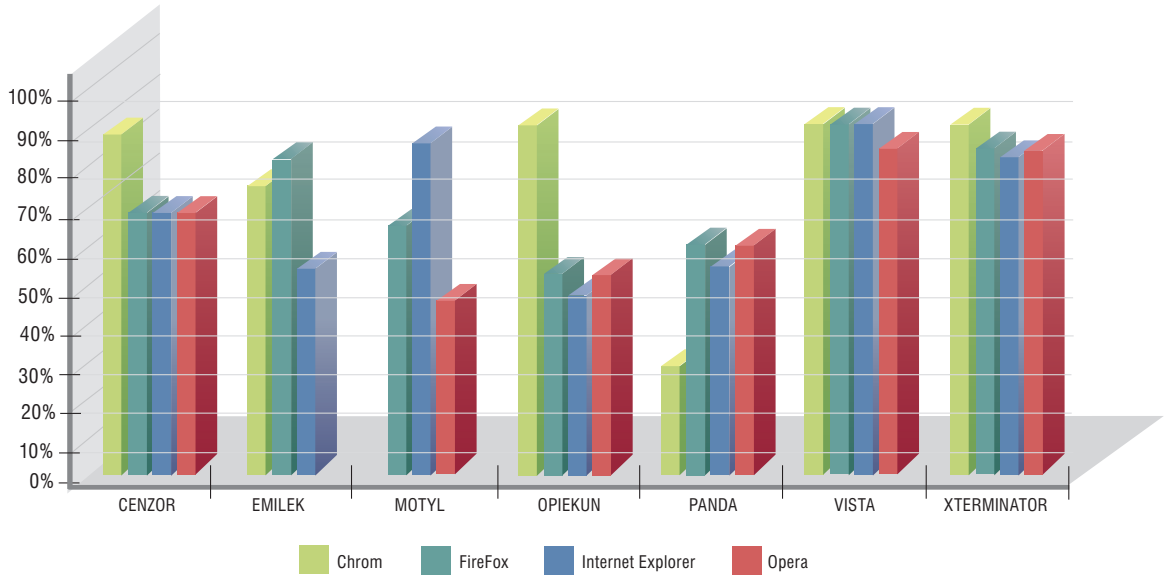
Rys 9. Skuteczność blokowania stron niepożądanych pod przeglądarką Chrome

3.2. Nadwrażliwość

W trzecim etapie badania sprawdzano nadwrażliwość filtrów na określone słowa kluczowe (np. piersi, seks, suka, penis), występujące na stronach z nieszkodliwymi treściami np. o tematyce medycznej, naukowej czy edukacyjnej.

Wszystkie programy testowano na najbardziej restrykcyjnym ustawieniu filtru.

Niezależnie od przeglądarki, najmniejszą nadwrażliwością charakteryzowały się Vista oraz xTerminator. Pozostałe programy reagowały na słowa kluczowe bez względu na charakter strony i blokowały witrynę (Rys 10).



Rys 10. Skuteczność przepuszczania stron nieszkodliwych z określonymi słowami kluczowymi

4. Podsumowanie badania

Na podstawie przeprowadzonych testów można wyciągnąć następujące wnioski:

- programy filtrujące dość skutecznie blokują dostęp do stron zawierających pornografię lub erotykę;
- aplikacje niestety pozwalają na wyświetlenie stron zawierających treści o charakterze rasistowskim propagujących używki, leki czy ryzykowne zachowania;
- w przypadku stron pornograficznych innych niż polskojęzyczne i anglojęzyczne, filtry nie spełniają swej funkcji;
- programy mają trudności ze skutecznym filtrowaniem stron zawierających wyłącznie grafikę;
- niektóre filtry zbyt wolno analizują strony i pozwalają na ich wyświetlenie. Decyzję o jej zamknięciu podejmują dopiero po kilku sekundach. Taki sposób działania stwarza zatem ryzyko, że dziecko może zapoznać się ze szkodliwymi treściami;
- w przypadku treści obojętnych/nieszkodliwych aplikacje błędnie reagują na pewne słowa kluczowe (seks, piersi, kotki), powodując zablokowanie strony;
- filtry są mało kompatybilne z nowymi lub mniej popularnymi przeglądarkami;
- mimo zapewnień producentów programy pozwalają na wysyłanie danych osobowych, korzystanie z komunikatorów, list dyskusyjnych, czatów oraz poczty WWW;
- w niedostateczny sposób rozpoznają także zawartość Web 2.0 – serwisów społecznościowych, blogów, fotoblogów oraz portali, na których udostępnia się pliki muzyczne oraz filmowe;
- większość programów nie kontroluje korzystania z gier zainstalowanych na komputerze lub dostępnych online. Niektóre pozwalają na dostęp do gier ewidentnie erotycznych;
- programy oferują możliwość dodawania własnych terminów do istniejącej bazy zakazanych słów kluczowych;
- w przypadku używania krótkiego adresu URL lub bramki proxy aplikacje słabo rozpoznają treści niepożądane (co jest popularnym wśród młodzieży sposobem na obejście blokad rodzicielskich);
- producenci na swoich stronach umieszczają dokładny opis programu oraz instrukcję jego instalacji, jak również kontakt z obsługą techniczną w przypadku ewentualnych problemów;
- alert blokady nie zawsze informuje o powodzie zamknięcia witryny i bywa niezrozumiały dla dzieci nie umiejących czytać;
- każda z aplikacja umożliwia rodzicom wgląd w aktywność dziecka w Sieci oraz ustawienie limitów korzystania z Internetu;
- większość testowanych filtrów jest wyposażona w regulację stopnia czułości;
- niemal wszystkie programy dają możliwość utworzenia i modyfikacji niezależnych profili ustawień w zależności od wieku dziecka;
- producenci programów często udostępniają licencję czasową produktu;
- przedstawione w raporcie rozwiązania filtrujące z powodzeniem mogą być stosowane w korporacjach. Co więcej, często producenci w swojej ofercie posiadają oddzielną wersję dla firm.

- **Kontrola rodzicielska wymaga świadomego użytkowania (administracji, kontroli działania, modyfikacji działania filtrów).**

5. Inne narzędzia

5.1 Wyszukiwarki dedykowane dzieciom

Alternatywą do modułów kontroli rodzicielskiej są dedykowane dzieciom wyszukiwarki internetowe. Stanowią one połączenie portalu dla dzieci z katalogiem stron, po jakich może surfować dziecko. Podczas wyszukiwania lub przeglądania kategorii wg słów kluczowych można się poruszać tylko w obszarze stron zweryfikowanych przez zespół administratorów.

5.1.1 Lupiko.pl

Wyszukiwarka dostępna pod adresem www.lupiko.pl, przeznaczona dla dzieci od 3 do 5 lat oraz ich rodziców. Wpisując słowo do wyszukiwarki, należy wybrać kategorię dla dziecka lub/oraz dla rodzica. Oprócz wyszukiwania wg wpisanego słowa istnieje możliwość przeglądania kategorii wg słów kluczowych. Każdy użytkownik może dodać stronę do katalogu, która nim jednak zostanie dodana, weryfikowana jest przez zespół psychologów i pedagogów. Co jakiś czas strony z zasobu wyszukiwarki są automatycznie skanowane i w razie wątpliwości strona jest ponownie przeglądana przez administratorów. Jeśli użytkownik ma uwagi odnośnie pozycji znajdujących się w katalogu, może dodać komentarz oraz wystawić ocenę od 1 – 5, która będzie potem widoczna dla wszystkich użytkowników.

Na stronie głównej wyszukiwarki są zamieszczone funkcje ustawienia strony jako strony startowej oraz dodania jej do ulubionych w przeglądarce. Niestety na stronie znajdują się reklamy.

5.1.2 Minigogle.pl

Wyszukiwarka dostępna pod adresem www.minigogle.pl, skierowana do dzieci poniżej 12 roku życia. Do katalogu są dodawane wartościowe strony dla dzieci oraz takie, które spełniają określone kryteria tj.:

– nie epatują przemocą;
– nie zachęcają do zmiany wyznania religijnego;
– nie promują sekt i ruchów społecznych;
– nie zawierają treści erotycznych;
– nie propagują nienawiści lub rasizmu;
– nie zawierają treści propagujących używki;
– nie zachęcają do łamania prawa.

Weryfikacją stron dodanych przez użytkowników zajmuje się administrator. Istnieje możliwość zgłoszenia naruszenia regulaminu. Na stronie głównej została zamieszczona funkcja ustawienia strony jako strony startowej. Niestety na stronie znajdują się reklamy, większość z nich znajduje się pod załamaniem ekranu.

5.2 Popularne wyszukiwarki ogólnodostępne – dla dorosłych

Także wyszukiwarki przeznaczone dla szerokiego grona użytkowników mają na uwadze bezpieczeństwo dzieci i młodzieży oraz bardziej wrażliwych odbiorców.

5.2.1 Google

Korzystając z wyszukiwarki Google filtr SafeSearch jest domyślnie ustawiony na umiarkowany. Istnieją trzy poziomy filtru, które można zmienić w zaawansowanych ustawieniach wyszukiwarki (podobnie jak język domyślnego wyszukiwania). Informacje zamieszczone w *Ustawieniach* wyszukiwania opisują każdy z filtrów w następujący sposób:

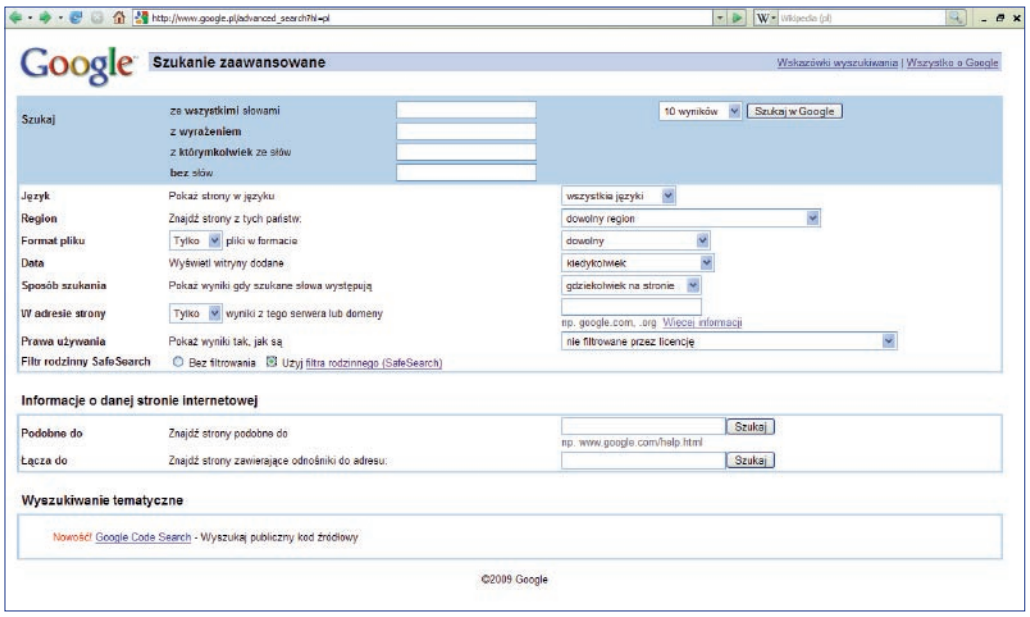
Filtrowanie umiarkowane – wyklucza jednoznacznie nieodpowiednie obrazy z wyników wyszukiwarki grafiki Google, ale nie filtruje zwykłych wyników wyszukiwania w Internecie. Jest to domyślne ustawienie filtrowania SafeSearch, czyli jeśli ustawienie nie zostanie zmienione, wyniki są filtrowane w sposób umiarkowany.

Filtrowanie ścisłe – włącza filtrowanie SafeSearch dla wszystkich wyników wyszukiwania (zarówno wyszukiwania grafiki, jak i zwykłego wyszukiwania w Internecie).

Bez filtrowania – całkowicie wyłącza filtrowanie SafeSearch.

Administratorzy korygują wyniki znajdujące się w opcji SafeSearch. Istnieje również możliwość zgłoszenia nieprawidłowości.

Wyszukiwarka Google charakteryzuje się dość prostym interfejsem i być może dlatego nie posiada żadnego graficznego odpowiednika dla dzieci.



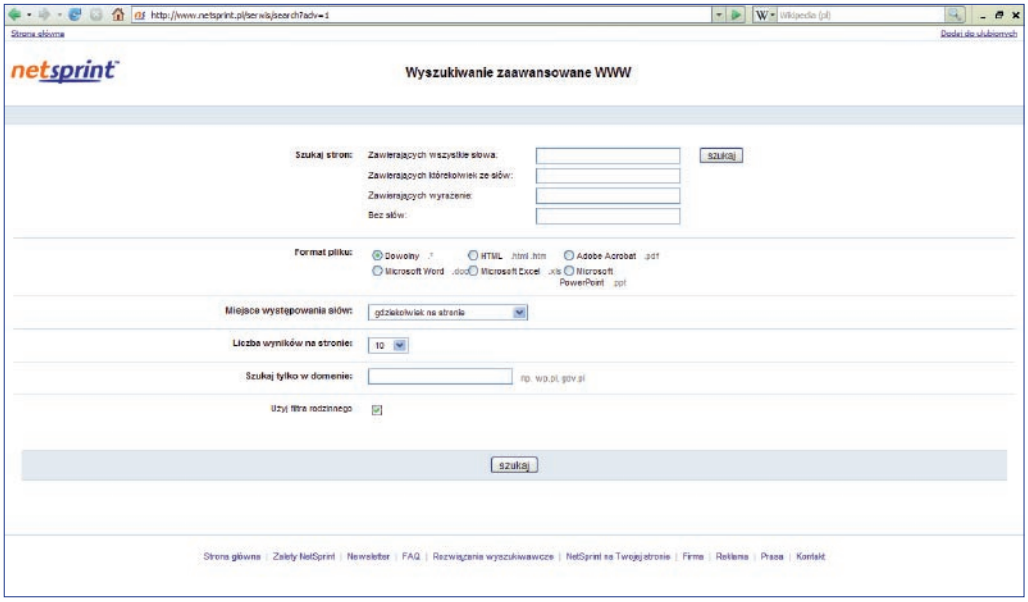
Rys 10. Zaawansowane ustawienia wyszukiwarki Google.pl z włączonym filtrem SafeSearch

5.2.2 Netsprint.pl

W wyszukiwarce NetSprint również jest dostępny filtr rodzinny. Włączenie go jest możliwe przez wejście w *Preferencje wyszukiwarki*. Wyszukując np. słowo „seks" przy włączonym filtrze rodzinnym, użytkownik może otrzymać podpowiedzi wyszukiwania – np. definicję w Wikipedii czy pozycję książkową[7].

Wyszukiwarka NetSprint charakteryzuje się prostym interfejsem i nie posiada żadnej graficznej wersji dla dzieci.

Ustawienia wyszukiwarek nie są chronione hasłem, mogą więc zostać łatwo zmienione przez każdego użytkownika.



Rys 11. Zaawansowane ustawienia wyszukiwarki netsprint.pl z włączonym filtrem rodzinnym

> Należy jednak pamiętać, że w momencie przechodzenia do wyników wyszukiwania, a potem podczas nawigacji po witrynie, dziecko może przejść na kolejne strony już nie przeznaczone dla dzieci.

5.3 Przeglądarki internetowe

Wybrane funkcje kontroli rodzicielskiej są dostępne w konfiguracji przeglądarek komputerowych. W opcjach aplikacji istnieje możliwość przeglądania historii stron, blokowania określonych witryn czy wyskakujących reklam.

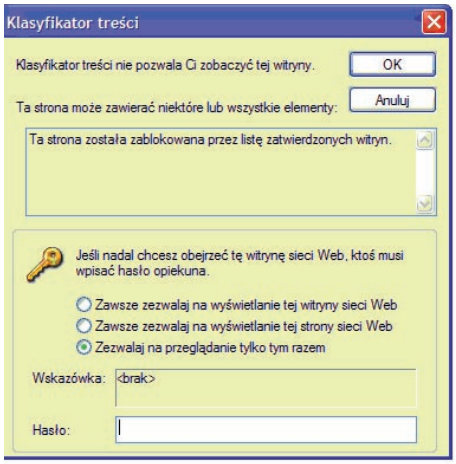
[7] Niestety w chwili opracowywania raportu filtr uwzględniał tylko niektóre słowa kluczowe

5.3.1 Internet Explorer

Strona producenta programu: *http://www.microsoft.com*

W zakładce przeglądarki Internet Explorer 7 znajduje się opcja klasyfikatora treści, która jest chroniona hasłem administratora. Za pomocą suwaka można ustawić czułość filtru posługując się kategoriami ICRA[8]. Istnieje możliwość zaimportowania innych klasyfikatorów treści. Można definiować białą i czarną listę niezależną od filtru klasyfikacji treści.

Ścieżka dostępu funkcji:
Narzędzia → opcje internetowe → zawartość



Rys 12. Komunikat zablokowania strony przez przeglądarkę Internet Explorer

5.3.2 FireFox

Strona producenta programu: *http://www.mozilla-europe.org/pl*

W wersji podstawowej przeglądarka FireFox nie posiada żadnego modułu kontroli zawartości stron internetowych. Są one dostępne w postaci dodatków ściąganych osobno. Niestety nie posiadają polskiej wersji językowej. FireFox wraz z organizacją Cybermentors przygotował przeglądarkę Firefox browser for CyberMentors, która oprócz tradycyjnych filtrów treści umożliwia bezpośredni kontakt ze specjalistami działającymi na rzecz bezpieczeństwa dzieci i młodzieży. W pasku bocznym przeglądarki są zamieszczone porady oraz materiały promujące bezpieczeństwo najmłodszych. Niestety przeglądarka ta posiada interfejs wyłącznie w języku angielskim.

Rys 13. FireFox for CyberMentors

5.3.3 Opera

Strona producenta programu: ***http://operapl.net/***

W przeglądarce Opera istnieje możliwość zdefiniowania stron, które nie powinny zostać otworzone. Po zablokowaniu nie wyświetla się żaden komunikat.

Ścieżka dostępu funkcji:
Narzędzia → zaawansowane → zablokowana zawartość

5.4. Inne rozwiązania kontroli rodzicielskiej

Również inne aplikacje posiadają moduł kontroli rodzicielskiej, które jednak ze względu na posiadanie tylko podstawowych funkcji oraz nie spełnianie wymaganych kryteriów badań nie zostały ujęte w testach skuteczności.

5.4.1 ArcaVir

Strona producenta programu: ***http://www.arcabit.pl/***

Program antywirusowy, który posiada podstawowy moduł kontroli rodzicielskiej, a w nim możliwość zdefiniowania przez administratora listy białych i czarnych stron oraz dodania fraz, które są niepożądane. Istnieje również możliwość wyboru poziomu nasycenia słowami kluczowymi analizowanego tekstu:

a) Silny, średni, słaby wpływ na blokowanie; silny, średni, słaby wpływ na zezwalanie
b) Liczona jako jedno wystąpienie, proporcjonalnie do liczby wystąpień, silniej niż proporcjonalnie.

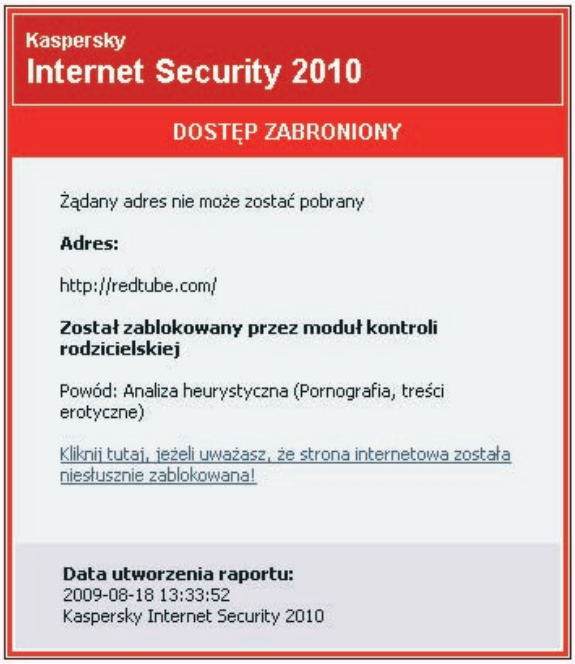
Rys 14. Komunikat blokowania strony przez program ArcaVir

Kaspersky Internet Security 2010

5.4.2

Strona producenta programu: ***http://www.kaspersky.pl/***

Moduł kontroli rodzicielskiej jest dodatkową funkcją w programie antywirusowym. Podczas tworzenia nowego profilu można wybrać w ustawieniach poziom ograniczeń z dokładnością co do pół godziny w tygodniu lub ograniczyć limit dzienny, kiedy dziecko może korzystać z Internetu. Opcja białej i czarnej listy pozwala na określenie dostępu do stron bez względu na wynik analizy programu. Istnieje możliwość wyboru kategorii, które powinny zostać zablokowane np. *pornografia, treści erotyczne, narkotyki, wulgaryzmy, broń, gry, chat, systemy płatności.* Istnieje możliwość wyboru czułości filtru spośród trzech poziomów: *niski*, *średni*, *szczegółowy*. Należy także wybrać akcję, jaką ma podjąć program – blokada dostępu do nieodpowiedniej witryny czy też tylko zapis alertu w raporcie zdarzeń. Program blokuje strony w przypadku korzystania z bramki proxy. Moduł ochrony rodzicielskiej jest chroniony hasłem. W komunikacie o zablokowaniu strony znajduje się jej adres URL oraz informacja o powodzie zamknięcia witryny. Istnieje możliwość przesłania adresu strony, która – zdaniem użytkownika – powinna zostać odblokowana.



Rys 15. Komunikat blokowania strony przez Kaspersky Internet Security 2010

Visikid

5.4.3

Strona producenta programu: ***http://www.visikid.pl/***

Zupełnie innym programem kontroli rodzicielskiej jest aplikacja Viskid. Jej zadaniem nie jest filtrowanie stron WWW ani blokowanie czasowego dostępu. Zapisuje natomiast: aktywność dziecka w Internecie, aplikacje, które zostały uruchomione na koncie dziecka, czas logowania oraz odwiedzane strony. Raport jest dostępny poprzez stronę WWW producenta z każdego komputera w sieci po uprzednim logowaniu. Zarówno administrator, jak i dziecko mają dostęp do wszystkich zgromadzonych informacji.

5.4.4 xTerminator

Strona producenta programu: ***http://www.guardlogic.pl***

Udostępniona wersja programu jest przeznaczona raczej dla sieci korporacyjnej niż dla użytkownika indywidualnego. Program należy do rozwiązań typu Content Filtering Proxy (CFP). Różni się od prezentowanych w poniższym raporcie o moduł analizy obrazu skoncentrowany na blokowaniu treści pornograficznych. xTerminator najpierw porównuje adres strony ze zdefiniowaną wcześniej listą białych i czarnych stron, następnie analizuje tekst strony i adres strony, a gdy te dwa etapy analizy nie dadzą jednoznacznej odpowiedzi (tj. czy zawartość strony powinna być blokowana czy nie), strona jest analizowana przez klasyfikatora obrazu. Każdy z obrazków jest analizowany indywidualnie i niezależnie od pozostałych, co skutkuje czasami zablokowaniem tych modułów strony, które zostały uznane za jednoznacznie nieodpowiednie (np. tylko obrazków). Pojawia się wtedy grafika, uprzednio zdefiniowana przez administratora systemu. Administrator otrzymuje kompletne zestawienie statystyczne z ostatnich 30 dni działania programu, prezentujące m.in. najbardziej aktywnych użytkowników, najczęściej odwiedzane witryny oraz aktywność użytkowników w poszczególnych przedziałach czasowych.

Program został poddany badaniu skuteczności i nadwrażliwości blokady ze względu na inną metodę klasyfikacji stron (*patrz Wyniki testów str. 27-30*) .

6. Wnioski końcowe

Problem ograniczenia dostępu do treści w Internecie występuje zarówno w dostępie korporacyjnym, dla pracowników zatrudnionych w firmach, jak i w dostępach domowych, gdzie użytkownikami oprócz dorosłych są także dzieci i młodzież.

Producenci oprogramowania wykorzystywanego w Internecie (wyszukiwarki, przeglądarki) oraz twórcy systemów operacyjnych wyszli naprzeciw tym zapotrzebowaniom i we wdrażanych produktach dali możliwość włączania opcji ograniczających dostęp. Ponadto pojawiły się na rynku specjalistyczne programy dedykowane wyłącznie filtrowaniu treści, jakie użytkownik (administrator, rodzic) może zainstalować na komputerze. Tę ostatnią opcję należy traktować jako najpełniejsze rozwiązanie z zakresu filtrowania i blokowania groźnych treści z poziomu komputera osobistego. Na uwagę zasługuje także fakt, iż producenci programów antywirusowych, których głównym zadaniem jest ochrona zasobów komputera przed różnego rodzaju wirusami i oprogramowaniem złośliwym, dołączają moduły, które zapewniają ochronę użytkowników tych komputerów przed szkodliwymi treściami poprzez możliwość ograniczenia dostępu do ustalonych wcześniej zasobów Internetu.

Otrzymane wyniki wskazują na bardzo zróżnicowaną skuteczność założonych przez producentów funkcji. Dodatkowo jest ona silnie zależna od rodzaju wykorzystywanej przeglądarki internetowej. Występowanie tej zależności jest istotne, gdyż przyzwyczajenie użytkowników w zakresie używania danej przeglądarki ograniczaj możliwość wyboru skutecznych programów filtrujących.

Dane zawarte w tabeli 5 powinny być podstawą do wyboru odpowiedniego programu filtrującego.

Podsumowując dwie edycje testów można dojść do wniosku, że producenci oprogramowań kontroli rodzicielskiej poważnie podchodzą do problemu filtrowania treści. Programy posiadają rozbudowane funkcje – oferują wiele opcji filtrowania (np. dostęp do czatów, poczty, komunikatorów), kontrolę czasu dostępu czy wybór własnych ustawień. Co więcej umożliwiają nadzór nad ustawieniami systemowymi komputera tj. blokują dostęp do zainstalowanych programów, panelu sterowania czy korzystania z pamięci przenośnych (np. pendrive). Posiadają też bardziej rozbudowany klucz analizy treści, co pozwala na coraz większą skuteczność w filtrowaniu zasobów internetowych.

Na swoich stronach producenci przedstawiają szczegółowy opis działania oferowanych produktów, umożliwiają aktualizację programu i kontakt z obsługą techniczną. Często też na swoich witrynach zamieszczają artykuły dotyczące dzieci w Internecie lub też prowadzą całe portale związane z tematyką bezpieczeństwa.

Mimo to należy pamiętać, że programy i rozwiązania filtrujące są tylko narzędziami i nigdy nie zastąpią rodzica. Całkowita blokada dostępu do Internetu czy też ścisły nadzór nad tym, co dziecko robi w Sieci może spowodować, że straci zaufanie do opiekuna. Niewykluczone, że na przekór będzie sięgało po to, co zakazane. Poza tym jeśli dziecko będzie chciało obejść blokadę, to wcześniej czy później znajdzie na to sposób – chociażby zacznie korzystać z Internetu poza domem.

Potrzeby dziecka zmieniają się wraz z jego wiekiem, nie można więc poprzestać na metodach raz wypracowanych. Z drugiej strony rozwiązania stosowane w programach filtrujących nie nadążają za nowymi technologiami. Aplikacje filtrujące nie są w stanie ochronić dziecka przed konsekwencjami jego własnych działań, stąd tak ważna jest rola opiekunów w kształtowaniu świadomości i samokontroli dziecka. Dzięki częstym rozmowom o bezpieczeństwie w Internecie oraz wspólnemu surfowaniu rodzic zdobywa zaufanie dziecka, a filtr rodzinny może stać się świadomym wyborem nie tylko rodzica, ale i dziecka. Jest to niezbędne wtedy, kiedy dziecko potrzebuje wsparcia i pomocy w niepokojącej sytuacji.

7. Opinie producentów

Poniżej zamieszczamy wypowiedzi kilku przedstawicieli producentów narzędzi filtrujących, z którymi współpracowaliśmy podczas przygotowywania i prowadzenia testów. Zostały one umieszczone w kolejności otrzymywania tych opinii. Zachowaliśmy oryginalną treść i układ wypowiedzi.

Guard Logic

Tworząc system xTerminator braliśmy pod uwagę takie zjawiska jak:

– dynamiczny rozwój Internetu wyrażający się wzrostem ilości stron WWW co ma bezpośredni wpływ na rozmiar baz url wykorzystywanych w systemach filtrujących koniecznych do aktualizacji. Dodatkowo różnorodność treści w obrębie jednej domeny utrudnia filtrowanie poprzez czarne i białe listy,

– techniki stosowane przez dostawców pornografii mające na celu „obejście" systemów filtrujących działających w tradycyjny sposób (np.: wykupywanie wygasłych „czystych" domen i oszukiwanie filtrów działających na podstawie list),

– częste pomijanie na stronach WWW treści tekstowych i umieszczanie jedynie elementów graficznych,

– poszukiwanie i przeglądanie pornografii przez różne wiekowo grupy użytkowników co jest potwierdzone badaniami dostawców wyszukiwarek.

Uwzględniając powyższe, w systemie filtracji stron WWW postanowiliśmy zastosować statystyczne techniki analizy tekstu oraz obrazów umożliwiające on-linową klasyfikację zawartości strony www. Opracowane klasyfikatory tekstu cechują się bardzo dobrym poziomem detekcji stron pornograficznych (klasyfikacja adresu strony, a następnie tekstu strony), przy niskiej wrażliwości na język narodowy strony.

Wykorzystywany klasyfikator obrazów uzupełnia działanie poprzednich stopni klasyfikacji, odcinając obrazy pornograficznie. W ten sposób, system filtruje również strony zawierające wyłącznie treści graficzne (np.: pojedynczy obraz). Bazując na wynikach klasyfikacji, system aktualizuje wewnętrzną bazę niepożądanych url'i, uwzględniającą specyfikę zachowań użytkowników Internetu instytucji w której pracuje.

Udostępniony do testów xTerminator ukierunkowany był na blokowanie głównie pornografii i z tego powodu wykazana w raporcie skuteczność blokowania treści niepożądanych, rozumianych szerzej niż pornografia jest niższa u innych badanych rozwiązań.

Ponieważ xTerminator jest systemem typu Content Filtering Proxy, przeznaczonym głównie dla klienta korporacyjnego, staraliśmy się by jego funkcjonowanie w sieci przedsiębiorstwa możliwie w niskim stopniu „przeszkadzało" w przeglądaniu zawartości Internetu. Takie zachowanie systemu potwierdza część raportu poświęcona nadwrażliwości.

Uważamy, że zmiany zachodzące w Internecie wymuszać będą na systemach filtrujących działanie w trybie dynamicznej klasyfikacji różnorakich treści, w tym treści multimedialnych. xTerminator wychodzi naprzeciw tym wyzwaniom.

Zespół Guard Logic

Microsoft

Microsoft przygotowując i pracując nad nowymi wersjami systemów operacyjnych bardzo dużą uwagę przykłada do bezpieczeństwa systemu operacyjnego zarówno w aspekcie ochrony użytkownika jak i również wtedy, kiedy użytkownik zwłaszcza młody sam korzystając z komputera na takie niebezpieczeństwo może się narazić. Ten drugi aspekt realizowany jest chociażby poprzez wbudowanie/wyposażenie systemu operacyjnego Windows Vista jak i również nowej wersji systemu Windows 7 w specjalny moduł Kontroli rodzicielskiej, który pozwala rodzicom uczynić z komputera nie przedmiot zagrożenia, lecz przedmiot pożądania. Rodzice posiadając już komputer często nie wiedzą, że ich codzienne narzędzie pracy wyposażone jest w specjalne funkcje, które pozwalają kontrolować czas spędzony przez dziecko przy komputerze i są integralną częścią systemu. Skorzystanie z nich nie wymaga zaawansowanych umiejętności – wystarczy tylko wpisać w Menu start – słowa kontrola rodzicielska, kliknąć Enter i można już zacząć zmieniać zasady pracy dziecka z komputerem. Moduł ten w odróżnieniu od innych programów realizujących takie zadania jest częścią systemu operacyjnego, co oznacza, że nie trzeba nic dodatkowego instalować ani konfigurować – warto z niego skorzystać, ponieważ jest. Jednym z ważniejszych elementów tej funkcjonalności jest raportowanie wszystkich aktywności dziecka, raport jest bardzo szczegółowy i bardzo przejrzysty, dzięki czemu możemy szybko i w prosty sposób zorientować się jak nasze pociechy korzystają, na co dzień z komputera. Należy jednak pamiętać by udostępniając dziecku komputer stworzyć dla niego specjalne konto – profil podstawowy bez uprawnień do zmiany ważnych ustawień komputera, takie konto administracyjne powinno być w posiadaniu rodzica – o to można poprosić już bardziej zaawansowanych użytkowników, na pewno nie odmówią. Oprogramowanie dostępne wciąż się zmienia – im nowsze tym więcej funkcji i wyższy poziom bezpieczeństwa – ta zasada odnosi się również do modułu kontroli rodzicielskiej, który dostępny będzie w nowym systemie Windows 7 jak i również do nowej wersji przeglądarki Internet Explorer w wersji 8 z nowym filtrem bezpieczeństwa Smartscreen – ta przeglądarka jest już dostępna i jest o wiele bardziej bezpiecznym produktem niż wersja 6. Dla większego bezpieczeństwa oprócz podanych programów warto skorzystać z usługi Bezpieczeństwo rodzinne usługi Windows Live (http://download.microsoft.com), która dodatkowo podnosi poziom naszego bezpieczeństwa.

Patryk Góralowski
Windows Product Marketing Lead – Consumer&Online

Opiekun

Cieszymy się z inicjatywy NASK-u, uważamy, że obiektywne i rzetelne przetestowanie programów kontroli rodzicielskiej przyczyni się do uporządkowania polskiego rynku oraz pomoże podjąć właściwą decyzję rodzicom.

Mimo iż wyniki Opiekuna w teście były bardzo dobre to porównanie z innymi programami jest dla nas również bodźcem do wytężonej pracy – aby w kolejnych testach program wypadł jeszcze lepiej. Jeśli chodzi o sam test to chcielibyśmy go uzupełnić informacją, że Opiekun współpracuje już z przeglądarką Chrome. Nowa wersja programu pojawiła się już w trakcie przeprowadzania testów.

Mamy nadzieję, że inicjatywa NASK-u rozpowszechni ideę kontroli rodzicielskiej w dostępie dzieci do Internetu gdyż gro rodziców nie widzi takiej potrzeby lub nie wie jak się z problemem zmierzyć. Z tego punktu widzenia przedstawiony raport jest bardzo techniczny, zabrakło nam w nim informacji o tym jak program kontroli rodzicielskiej do domu „wprowadzić".

Chodzi przede wszystkim o pewną formę konsensusu między rodzicami a dziećmi, aby te ostatnie nie miały poczucia, że program jest przeciwko nim. Zwłaszcza nastolatki są bardzo wrażliwe w tej kwestii. Jeśli program wprowadzi się niejako na siłę to może się okazać, że wszystko, co udało nam się osiągnąć to fakt, że nasze dzieci przeglądają niedozwolone strony u znajomych lub w kafejce internetowej.

Kolejnym krokiem, do którego niniejszym zachęcamy NASK jest przeprowadzenie testów programów filtrujących przeznaczonych dla szkół.

Praktycznie wszystkie dzieci w Polsce mają dostęp w szkołach do Internetu i aktywnie z tej możliwości korzystają. Szkoły mają obowiązek dbać o bezpieczeństwo swoich podopiecznych, zatem w większości z nich działa któryś z programów filtrujących. Jestem przekonany, że przeprowadzenie rzetelnego testu ułatwiłoby podjęcie decyzji bardzo wielu nauczycielom i opiekunom pracowni informatycznych.

Krzysztof Jeż
Opiekun

Kaspersky Lab Polska

Przygotowanie raportu zawierającego tak wiele informacji w obrębie jednego dokumentu z pewnością było bardzo trudnym zadaniem. Tym bardziej zespołowi SaferInternet.pl oraz CERT Polska przygotowującemu zestawienie należą się wyrazy uznania. W Kaspersky Lab kładziemy bardzo duży nacisk na działalność edukacyjną i doceniamy takie inicjatywy, w szczególności gdy dotyczą one tych najbardziej bezbronnych użytkowników Internetu, czyli dzieci. Raport kompleksowo przedstawia tematykę filtrowania zawartości i może znacznie ułatwić dobór rozwiązania, które będzie pełnić rolę kontroli rodzicielskiej, zarówno w komputerach domowych, jak i w firmowej infrastrukturze IT.

Ze względu na rzeczowe przedstawienie informacji dotyczących klasyfikacji treści z raportem powinien zapoznać się każdy rodzic.

Piotr Kupczyk
Dyrektor działu prasowego Kaspersky Lab Polska

Panda Security Polska

Twórcy raportu podjęli ważny temat, często pomijany przez specjalistyczne media. Większość opracowań i testów koncentruje się na wirusach, włamaniach i kradzieżach tożsamości, SPAM-ie lub wydajności aplikacji ochronnych. Zapomina się jednak, że Internet z racji swojej dostępności i otwartości wpływa na rozwój i edukację wielu młodych ludzi. Obok bez wątpienia pozytywnej roli niesie też za sobą liczne zagrożenia. Wiele z nich wymienili autorzy raportu – warto też dodać, że strony o treściach niedozwolonych mogą być wykorzystywane do nawiązania fizycznego kontaktu. Umożliwiają cyber – przestępcom atak na zasoby informatyczne zgromadzone na komputerze oraz domowej sieci. To właśnie tego typu strony są najczęściej źródłem infekcji. Bardzo niebezpieczna może być np. pozornie nie szkodliwa prośba o ściągnięcie specjalnej „wtyczki" lub kodeku, niezbędnych do odtworzenia filmu umieszczonego na stronie WWW. Jeśli prośba taka pochodzi z nieznanej witryny, zgadzając się na zainstalowanie tego typu produktu narażamy się na ogromne niebezpieczeństwo.

Młodzież jest w centrum uwagi Panda Security od blisko 20 lat. Staramy się aby nasze produkty skierowane do użytkowników domowych były proste i łatwe w obsłudze. Zdajemy sobie sprawę, że większość ludzi traktuje komputer jako narzędzie pracy i rozrywki. Programy chroniące system powinny być więc z jednej strony skuteczne, a z drugiej niezauważalne dla użytkownika. Samo oprogramowanie niestety nie wystarcza. Bardzo ważna jest świadomość internautów. Blisko 8 lat temu powstał m.in. specjalny program edukacyjny Panda's Kids Protection, którego celem jest edukacja zarówno młodzieży jak i rodziców. Staramy się w blisko 200 krajach dzielić naszą wiedzą o zagrożeniach i o tym jak ich unikać. Wagę jaką Panda Security przywiązuje do ochrony dzieci i młodzieży, pokazują też wyniki testu, w których rozwiązania naszej firmy osiągnęły najwyższą skuteczność wśród analizowanych produktów.

Dariusz Kostanek
Dyr. Ds. Marketingu Panda Security Polska

8. Summary

In August 2009 there was the second edition of the tests of applications filtering undesirable contents on the Internet. Tests were performed on the Polish language filtering solutions – Emilek 2.1., Cenzor, Motyl, Opiekun Dziecka w Internecie, PANDA Internet Security 2009, xTerminator.

The first stage of the examination included the review of the application's functions. The attention was paid, among others, to: time limits, the possibility of settings modifications or information on the type of websites being blocked.

The second stage of the examination regarded the effectiveness of blocking websites which may be harmful to children. The tests were performed on the basis of 130 WWW website addresses, sent by the Internet users to the Dyzurnet.pl team within the notifications regarding illegal contents. The effectiveness criterion applied was a closure of a given WWW website (or its part where the undesirable contents were placed) within no more than 5 seconds after its display. The examination sample contained pornography websites, websites with the pictures of accident victims, contents obviously calling for racist and xenophobic behaviours, websites promoting sects, anorexia, bulimia, self-mutilation, suicides, various kinds of stimulants and websites with vulgar language.

At the third stage of the examination the hypersensitivity of the filters to the websites containing specified key words was checked (e.g. breast, sex), however without harmful contents, but only medical information (e.g. regarding breast cancer), educational (e.g. regarding pubescence) or other (e.g. regarding Sex Pistols band).

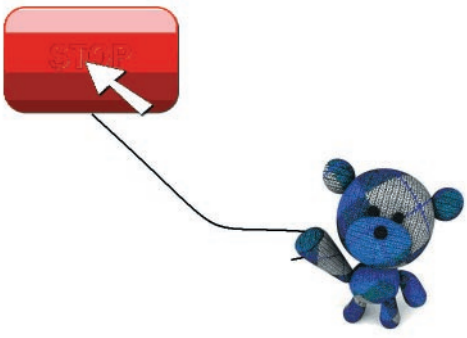
The effectiveness of the filtering programmes was measured at the most sensitive setting of the filter. Each application was tested using the programme which was written for the purpose of the examination by the specialists from the CERT Poland team. Thanks to the tests on one WWW websites library, homogenous reference material for any application was obtained. Each of the working stations, which was subject to testing, was equipped with the Windows XP Professional 2002 operating system and the browsers: Internet Explorer 6.0., Firefox 3.0.12, Opera 9.02., Chrome 2.0.172.37. The reason for choosing this kind of internet browsers was their popularity among the Polish users and – in the case of the Chrome browser – the end of works on BETA version and the vast product media campaign.

On the basis of the performed testes one may draw the following conclusions:

- in blocking undesirable websites under the Internet Explorer, the most effective were: Panda, Opiekun and Cenzor, in the case of the Firefox browser – Panda, Opiekun and Cenzor, in the case of the Opera browser – Panda, Opiekun and Cenzor, and in the case of the Chrome browser – Panda, xTerminator and Windows Vista
- Vista and xTerminator had the least hypersensitivity to the specified key words (e.g. breast, sex, bitch, penis), which appear on the websites with harmless contents. Other programmes reacted to the key words irrespective of the nature of the website and blocked the site
- none of the tested applications guarantees 100 % protection against harmful contents

the filtering programmes effectively block the access to the websites with pornography or erotic contents

- unfortunately the applications allow displaying websites with racist contents, promoting stimulants, drugs or risky behaviour
- in the case of pornography websites other than in Polish and English language, the filters fail to perform their function
- the programmes have difficulties in effective filtering of the websites with graphics only
- some filters analyse websites too slowly and allow their display. The decision on its closure is made no sooner than after several seconds. This kind of activity increases the risk that a child may become acquainted with the harmful contents
- in the case of the neutral/harmless contents, the applications incorrectly react to some key words (sex, breast, kitties), causing the website blockage
- the filters are not very compatible with the new or less popular browsers
- in spite of the producers assurances, the programmes allow sending personal data, using electronic communicators, electronic mailing lists, chats and www mail
- also insufficiently recognize Web 2.0 – social network services, blogs, photo blogs and web portals, which make music and film files available
- the majority of programmes do not control the use of games installed on a computer or available online. Some of them allow access to games which are obviously erotic
- the programmes offer the possibility of adding own terms to the existing base of the forbidden key words
- in case of using *short URL address or a proxy frame*, the applications hardly recognize undesirable contents (which is a popular, among young people, manner to evade parents blockages)
- the producers place on their websites a precise description of a programme and the instruction of its installation, as well as a contact to helpdesk in case of possible problems
- the blockage alert not always alarms about the reason for the site closure and sometimes it is unintelligible for children who cannot read
- each of the applications enables parents to look into the child's activity on the Net and set the limits for the Internet use
- the majority of tested filters is equipped with a regulation of the sensitivity level
- almost all of the programmes enable to create and modify independent setting profiles in relation to the child's age
- the producers of the programmes often make the temporary product license available
- the filtering solutions presented in the report may apply in corporations. What is more, the producers' offer often contains separate version for the companies.



W ramach
Polskiego Centrum Programu „Safer Internet"
realizowane są 3 projekty:

Saferinternet.pl

– projekt, którego celem jest zwiększanie społecznej świadomości na temat zagrożeń, jakie niosą ze sobą najnowsze techniki komunikacji. Wśród podejmowanych działań priorytetem jest edukacja, zarówno dzieci, jak i rodziców, a także podnoszenie kompetencji profesjonalistów w zakresie bezpiecznego korzystania z Internetu.

Projekt realizowany przez FDN i NASK we współpracy z Fundacją Orange.

Więcej informacji: *www.saferinternet.pl*

Helpline.org.pl

– projekt, w ramach którego udzielana jest pomoc młodym internautom, rodzicom i profesjonalistom w przypadkach zagrożeń związanych z korzystaniem z Internetu oraz telefonów komórkowych przez dzieci i młodzież.

Projekt realizowany przez FDN oraz Fundację Orange.

Więcej informacji: *www.helpline.org.pl*

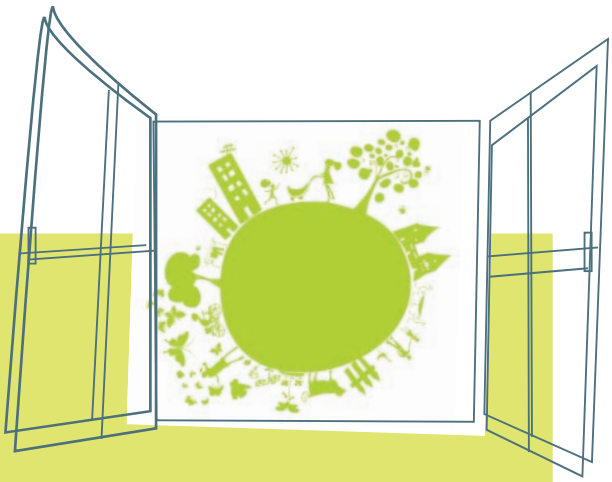
Dyżurnet.pl

– punkt kontaktowy, tzw. hotline, do którego można anonimowo zgłaszać przypadki występowania w Internecie treści zabronionych prawem takich, jak pornografia dziecięca, pedofilia, treści o charakterze rasistowskim i ksenofobicznym.

Projekt realizowany przez NASK.

Więcej informacji: *www.dyzurnet.pl*

Projekt i opracowanie graficzne ASP Grafik. Wykorzystano materiały © *NL shop* i © *lapie Fotolia.com*



Informacje
o nielegalnych treściach
napotkanych w Internecie
można zgłaszać do Dyżurnet.pl:

- poprzez formularz
  na stronie **www.dyzurnet.pl**
- mailem na adres:
  dyzurnet@dyzurnet.pl
- telefonicznie:
  0 801 615 005