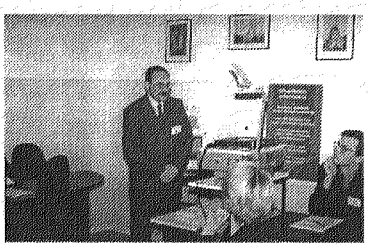
Marek Matusiak,
Krzysztof Walczewski,
Zdzisław Kajdosu
Wojskowa Akademia Medyczna, Łódź



Korzystanie z informacyjnych zasobów sieci Internet – zalety i zagrożenia

Zagadnienia wyszukiwania informacji nabierają coraz większego znaczenia, także w naukach medycznych. Niebagatelnym źródłem informacji staje się najbardziej rozległa z sieci - Internet. Zasoby tej sieci można podzielić na kilka podstawowych form:

1. Strony WWW np. http://www.wam.lodz.pl
2. Poczta elektroniczna np. marmatus@achilles.wam.lodz.pl
3. Listy dyskusyjne np. lek-med@achilles.wam.lodz.pl
4. Grupy dyskusyjne (USENET)
5. Serwisy FTP

Dostęp do konkretnych adresów można uzyskiwać poprzez:

- Specjalistyczne pozycje książkowe i periodyki oraz informacje w radiu i telewizji
- Wyszukiwarki (szperacze) internetowe oraz roboty wyszukiwawcze
- Prywatne informacje od autorów serwisów uzyskiwane np. na zjazdach naukowych

Najpopularniejsze na dzień dzisiejszy są internetowe serwisy wyszukiwawcze. Są to specjalne programy skanujące cały Internet w poszukiwaniu informacji z automatycznym jej segregowaniem tematycznym. Część z tych programów oferuje informacje podzielone wstępnie na tematyczne katalogi, powinno to pomagać w szybszym odnalezieniu poszukiwanych tematów. Jednym z popularnych szperaczy jest HotBot (*www.hotbot.com*) - amerykański program do wyszukiwania informacji w wielu płaszczyznach.
Można przeszukiwać w nim różne media Internetu:

- Sieć Web
- Grupy dyskusyjne
- Nazwy domen itd.

Wyszukiwania mogą być zawężane w aspektach:

- wyszukiwania wyrazu lub wyrażenia
- przestrzeni czasowej ukazania się informacji w Internecie
- rejonu geograficznego, w którym informacja została opublikowana

Dodatkowo umieszczono dużą kolekcję katalogów tematycznych: od biznesu przez technikę do kultury, ochrony zdrowia i nauki. Po wpisaniu w okienku poszukiwanego łańcucha tekstowego i odczekaniu niezbędnego czasu wyszukiwania otrzymamy pierwszą grupę dziesięciu (jeśli nie zmieniliśmy tej domyślnej wartości na inną) znalezionych adresów. Są to z reguły adresy WWW, ale mogą także wystąpić adresy serwisu FTP, służącego do zdalnego importowania plików. Z punktu widzenia sprawności wyszukiwania bardzo istotne jest właściwe zawężenie zakresu poszukiwań, podobnie jak przy formułowaniu zapytań do baz danych. Często jednak, mimo przemyślanego zawężenia, spotkamy się z wylistowaniem przez szperacz ogromnej ilości adresów, sięgającej wielu tysięcy. Nie daje to optymistycznej perspektywy; tak duża liczba adresów nie może być w rozsądnym czasie przejrzana w celu stwierdzenia przydatności wyszukanych informacji. Najlepszy efekt daje wtedy dalsze zawężanie zapytań do szperacza, choćby przez zawężenie obszaru geograficznego poszukiwań, użytego języka, czy też przedziału czasowego. Jeżeli uda się ograniczyć ilość otrzymanych adresów do wartości kilkuset, to można spróbować przejrzeć, co znajduje się pod wyszukanymi adresami. Niestety, nie zawsze wrażenia będą pozytywne. Przykładowo, poszukujemy autora prac naukowych o określonym nazwisku i imieniu. Otrzymaliśmy 100 adresów, z których część opisuje tego człowieka i jego twórczość, inna część opisuje zupełnie inne tematy, w których zacytowane zostało jedynie poszukiwane przez nas nazwisko. Istota Internetu jest taka, że możemy w nim szukać informacji na dosłownie każdy temat. Należy jednak pogodzić się ze smutnymi następstwami w postaci bardzo dużej ilości adresów, często niemożliwych do przetworzenia, oraz wyszukiwaniem takich informacji, które są absolutnie nieużyteczne.

Sieć komputerowa, także Internet, stanowi idealne podłoże do rozprzestrzeniania się wszelkiego rodzaju wirusów komputerowych oraz jest obszarem paraszpiegowskiej działalności. Przeglądarki ostrzegają zwykle o możliwości penetracji zagrożenia do naszego komputera, idealnego zabezpieczenia nie są w stanie jednak zagwarantować.

W ramach prewencji wirusowej należy zwracać uwagę nie tylko na wirusy w postaci plików wykonywalnych (bat, com, exe, cmd) ale w szczególności na tzw. wirusy „makro", będące skutkiem pisania procedur makroprogramowania w Winwordzie, Excelu i innych rozbudowanych programach, w których występują takie możliwości. „Makrowirusy" z racji możliwości wykonywania operacji na plikach mogą działać destrukcyjnie porównywalnie z wcześniej znanymi wirusami, ale mogą one wnikać do

komputera w bardziej zakamuflowany sposób. O podobne możliwości można podejrzewać także popularne ostatnio w dokumentach HTML znaczniki stałych klientów tzw. Cookies. Dysponując możliwie najnowszymi programami antywirusowymi, można próbować bronić się poprzez wcześniejsze przeskanowanie antywirusowe odebranego z sieci programu lub dowolnego pliku, w którym mogą wystąpić makroprogramy (np. pliki Worda, Excela czy Lotusa 123 dla Windows). Coraz większa ilość takich plików jest przekazywana jako dodatki do listów poczty elektronicznej (e-mail). Po umieszczeniu takiego pliku na własnym dysku należy przed pierwszym uruchomieniem obowiązkowo zbadać go antywirusowo lub też uruchomić ostrzeganie przed makrowirusem i nie zgadzać się na uruchomienie makra umieszczonego w pliku (możliwe w Wordzie 97).

Z racji podłączania do sieci rozległej dużej ilości instytucji i osób (poprzez modemy) obserwuje się wzrastającą tendencję do śledzenia zawartości dysków twardych ze szczególnym uwzględnieniem baz danych oraz zdalnej obserwacji aktywności występującej zarówno w sesjach połączeniowych z siecią rozległą (WAN), jak i w sieciach lokalnych (LAN). Wyniki takich obserwacji bywają przydatne w polityce gospodarczej, finansach, wdrażaniu nowych technologii, działalności naukowej itd.

W opisanych sytuacjach można się zabezpieczać, szyfrując gromadzone i przesyłane informacje (także e-mail). Sytuację poprawić mogą także specjalne programy śledzące cały ruch w sieci lokalnej i nie dopuszczające do jej penetracji przez użytkowników nie mających odpowiedniego zestawu uprawnień (oprogramowanie „firewall"). Niestety, wszystko to bardzo utrudnia życie legalnym użytkownikom danej sieci.

Wobec niekontrolowanego przyrostu informacji gromadzonej w sieci Internet, dynamicznego rozwoju nowych technologii informacyjnych i zagrożeń z tym związanych, a polegających na utracie prywatności, narażeniu na penetrację i utratę własnych danych, bardzo ważne jest wypracowanie stosownych nawyków, mających ograniczyć to niebezpieczeństwo do minimum.