

MAREK BRYŁA, GRZEGORZ STEGIENIA, ALINA KOWALSKA, IRENA MANIECKA-BRYŁA

Internet jako źródło informacji o zdrowiu publicznym. Cz. III. Znaczenie informacji w zdrowiu publicznym i zagrożenia związane z pozyskiwaniem informacji z zakresu zdrowia publicznego przez Internet

Streszczenie

Za punkt wyjścia tej części opracowania przyjęto potrzeby informacyjne w zdrowiu publicznym, a więc potrzeby, które posiada każdy użytkownik informacji dotyczącej obszaru problematyki zdrowotnej, w zależności od profilu swoich zainteresowań i roli jaką pełni. Uwzględniając taki punkt widzenia, wyróżniono następujące grupy użytkowników Internetu: studentów i uczniów kierunków medycznych i pokrewnych, naukowców-nauczycieli, czynnych zawodowo lekarzy, administratorów i kierowników różnych instytucji publicznych i prywatnych, które zajmują się zdrowiem lub działają w jakimś wymiarze dotyczącym tej tematyki oraz decydentów ustalających prawo zdrowotne, a więc tych, którzy uczestniczą w budowaniu sfery zdrowia publicznego. *Gros* miejsca w opracowaniu przeznaczono charakterystyce potencjalnych zagrożeń, które mogą pojawić się podczas zdobywania informacji o zdrowiu publicznym w globalnej sieci, jaką jest Internet. Wyróżniono trzy podstawowe kierunki takich zagrożeń. Są nimi, po pierwsze, zagrożenia związane z jakością informacji (tzn. możliwość uzyskania informacji: niemerytorycznej, błędnej, nieaktualnej, bezwartościowej lub o małej wartości), po drugie, zagrożenia dotyczące legalności pozyskanej informacji (brak pewności co do statusu legalności pozyskanej informacji – np. prawa autorskie danej publikacji książkowej nie zezwalają na jej rozpowszechnianie – mimo to, publikacja ta jest dostępna w sieci), wreszcie po trzecie, zagrożenia techniczne (możliwość przechwycenia podczas wysyłania i pobierania poufnych danych przez osoby trzecie). Należy zaznaczyć, że istnieją sposoby przeciwdziałania takim zagrożeniom, co wykazano na przykładzie fundacji *Health on the Net Foundation*, która opracowała kodeks, składający się z kilku kryteriów, które jeśli są spełnione – umożliwiają wystawianie certyfikatów stronom WWW przedstawiającym informacje o zdrowiu człowieka.

Słowa kluczowe: zagrożenia w Internecie, zdrowie publiczne, informacja naukowa.

Internet as a source of information in public health. Part III. The role of information in public health and threats linked to obtaining public health information on the Internet

Summary

The paper departs from information needs in public health. These are needs of all users of information in the field of health policy, depending on their interest profile. Taking into account such a viewpoint, we distinguished the following categories of the Internet users: students of medical faculties and related faculties, academics, active doctors, administrators and managers of various public and private institutions which operate in the sphere of health as well as decision-makers creating health laws, i.e. all those who participate in building the domain of public health. We devote a lot of space to the analysis of potential threats, which may appear in the process of searching for public health information in the global network like the Internet. We distinguish three principal types of threats: 1) related to the information quality (the possibility of getting information being irrelevant, wrong outdated, useless or of little value), 2) related to the legality of obtained information (e.g. a book copyright may prevent its dissemination, and still this publication is available on a website), and 3) technical threats (the possibility of capturing confidential data by third parties while sending or receiving). It ought to be emphasised that there are ways to minimise these threats. We quote the example of the Health on the Net Foundation, which worked out a code of several criteria, which, if fulfilled, enable to award certificate to www pages presenting information on human health.

Key words: Internet threats, public health, academic information.

ZNACZENIE INFORMACJI W ZDROWIU PUBLICZNYM

Zdrowie publiczne jako interdyscyplinarna dziedzina wiedzy szczególnie potrzebuje nieustannego i bardzo efektywnego komunikowania się, wymiany oraz szybkiego dostępu do informacji: naukowej, społecznej i technicznej [1-14]. Jako że jest to dziedzina wiedzy praktyczna, w której liczy się innowacyjność i ewolucyjność – powinna ona posiadać dużą sprawność informacyjną w wymiarze dostępu i aktualizacji – zarówno w swoich strukturach (informacja dla: profesjonalistów związanych z tematyką medyczną, osób kształconych i kształcących, twórców ustaw, władzy na wszystkich szczeblach, twórców polityki zdrowotnej), jak i dla społeczeństwa, aby mogło aktywnie uczestniczyć w umacnianiu i poprawie swojego zdrowia oraz posiadać aktualną wiedzę na temat przysługujących praw związanych z opieką zdrowotną. Aby spełnić powyższe potrzeby informacyjne dla zdrowia publicznego jako całego organizmu, zaistniała potrzeba stworzenia systemu przetwarzania różnorodnych danych. W tym bardzo złożonym systemie, można wyróżnić główne ośrodki, które próbują sprostać temu zadaniu. Są to między innymi: instytucje naukowe, ośrodki informacji, biblioteki i niektóre urzędy administracji publicznej. Rozwiązaniem wielu problemów dotyczących szybkości dostępu oraz aktualności informacji, potrzebnych do usprawniania działalności zdrowia publicznego we wszystkich jego wymiarach, staje się powoli technologia, a więc informatyzacja, czyli racjonalne wykorzystanie uprzednio wprowadzonych już danych do systemów informatycznych w możliwie największym dopuszczalnym zakresie przez inne systemy informatyczne [15], która umiejętnie wykorzystana może stać się głównym ogniwem łączącym wszystkie obszary zdrowia publicznego – tym samym zapewniając szybszy rozwój tej dziedziny nauki.

POTRZEBY INFORMACYJNE W ZDROWIU PUBLICZNYM

Poprzez potrzebę informacyjną w zdrowiu publicznym, należy rozumieć potrzebę, którą posiada każdy użytkownik informacji dotyczącej obszaru problematyki zdrowotnej. Należy jednak zauważyć, że każdy z użytkowników tej wiedzy potrzebuje dostępu do różnych jej zasobów.

Studenci i uczniowie kierunków medycznych i pokrewnych, poszukują przede wszystkim informacji dotyczących podstawowych zagadnień. Osoby uczące się zazwyczaj nie poszukują kompletnej i wyczerpującej wiedzy dotyczącej konkretnego problemu. W zasięgu ich zainteresowania są ogólne publikacje, gdyż zakres wiedzy jaki muszą przyswoić podczas całego czasu trwania ich nauki zmusza ich do ciągłego poszukiwania rozmaitych źródeł obejmujących wiele tematów.

Z kolei naukowcy-nauczyciele, aby posiadać aktualne informacje muszą nieustannie kontrolować klasyfikację dostępnych pozycji naukowych, rangę i uznanie jakim w środowisku cieszy się dany tytuł oraz wiele innych wiadomości, które obecnie dzięki intensywnej wymianie informacyjnej potrafią zmieniać się szybciej niż miało to miejsce jeszcze kilka lat temu. Również muszą zwracać szczególną uwagę na metody dydaktyczne, które też podlegają zmia-

nom – choćby za sprawą rozwijającej się informatyzacji i coraz bardziej popularnej cyfryzacji wszelkich zasobów informacyjnych. Obecnie proces dydaktyczny rzadko już odbywa się *ex cathedra* – wyłącznie przez określonych nauczycieli, dlatego też zadaniem naukowców-nauczycieli staje się powoli nauczanie studentów jak użytkować i wykorzystywać wszystkie dostępne możliwości pozyskiwania informacji oraz jak odróżniać informacje nierzetelne od tych, które mają wartość naukową. Dzisiejsze kształcenie polega więc często na oswojeniu studentów z różnymi technikami informacyjnymi, które pozwalają dotrzeć do wiedzy o zdrowiu publicznym.

Innego typu potrzeby informacyjne mają czynni zawodowo lekarze. Potrzebują oni szybkiego dostępu do precyzyjnej informacji, np. dotyczącej możliwości diagnostycznych konkretnej jednostki chorobowej czy też właściwości i zastosowania nowych leków. Problem informacyjny, który w tym przypadku najczęściej występuje w tym przypadku to wiek informacji. Często jest tak, że informacje dostępne w książkach i czasopismach medycznych, pod względem aktualności, są opóźnione o około jeden rok. Zatem informacje, które nie mogą czekać na długi proces wydawniczy, powinny być umieszczane w pierwszej kolejności w specjalnych bazach informacyjnych dostępnych dla lekarzy na całym świecie przez sieć Internet.

Kolejną grupą, dla której szybki dostęp do aktualnych informacji związanych ze zdrowiem publicznym jest sprawą bardzo istotną, są:

- administratorzy i kierownicy różnych instytucji publicznych jak i prywatnych, które zajmują się zdrowiem lub działają w jakimś wymiarze dotyczącym tej tematyki;
- decydenci ustalający prawo zdrowotne, a więc wszyscy ci, którzy uczestniczą w budowaniu sfery zdrowia publicznego.

Niestety często zdarza się, że środowiska naukowe oraz decydenci mają dostęp do zupełnie innej informacji, co skutkuje tym, że oba środowiska zamiast współpracować w rozwiązywaniu problemów dotyczących systemu opieki zdrowotnej, zajmują się odmiennymi zagadnieniami. Naukowcy w wyborze tematu do badań, zazwyczaj kierują się osobistymi zainteresowaniami, które często odbiegają od pragmatycznych potrzeb praktyków [16].

Ostatnią grupą, która również powinna mieć dostęp do określonych zasobów w zdrowiu publicznym, są osoby nie związane z tematyką medyczną zawodowo. Tę grupę można określić jako całe społeczeństwo, w którym zawierają się zarówno: zdrowi, chorzy, pacjenci, i inni potrzebujący pomocy lub wsparcia (również informacyjnego). Realizacja założeń o równym dostępie do zdrowia, a także zapewnienia bezpieczeństwa zdrowotnego danej zbiorowości, nie byłaby możliwa bez dostępu do informacji na temat zagrożeń zdrowotnych oraz możliwości zapobiegania im. Należy również pamiętać, że zasobami informacyjnymi zdrowia publicznego są wszelkiego rodzaju akcje profilaktyczne i prozdrowotne. Obecnie, kiedy metody teleinformatyczne stały się głównym sposobem przekazywania informacji, a sama informacja odgrywa decydującą rolę w odbieraniu i rozumieniu rzeczywistości, można stwierdzić, że zdrowie publiczne ze swoją misją będzie musiało zmodyfikować swój model komunikowania się ze społeczeństwem – gdyż już teraz społeczeństwo, w którym żyjemy, wielu naukowców określa jako informacyjne [17].

ZAGROŻENIA ZWIĄZANE Z POZYSKIWIANIEM INFORMACJI Z ZAKRESU ZDROWIA PUBLICZNEGO PRZEZ INTERNET

Pisząc o Internecie jako źródle wiadomości o zdrowiu publicznym, należy również wspomnieć o potencjalnych zagrożeniach, które mogą pojawić się podczas zdobywania takich informacji w globalnej sieci. Zagrożenia wstępnie można podzielić na:

- związane z jakością informacji (tzn. możliwość uzyskania informacji: niemerytorycznej, błędnej, nieaktualnej, bezwartościowej lub małowartościowej);
- dotyczące legalności pozyskanej informacji (brak pewności co do statusu legalności pozyskanej informacji – np. prawa autorskie danej publikacji książkowej nie zezwalają na jej rozpowszechnianie – mimo to, publikacja ta jest dostępna w sieci);
- techniczne (możliwość przechwycenia podczas wysyłania i pobierania poufnych danych przez osoby trzecie).

Powyżej zostały wymienione najbardziej kluczowe zagrożenia w kontekście: pozyskiwania za pomocą Internetu informacji dotyczących nauk medycznych i tematyki zdrowia publicznego oraz wymiany informacji między lekarzem a pacjentem. Należy zaznaczyć, że w sieci istnieje dużo więcej zagrożeń (np. tzw. „złośliwe” oprogramowanie i wiele innych). Uwzględniając jednak temat niniejszej pracy, poniżej zostaną opisane tylko te wcześniej wspomniane, gdyż z punktu widzenia pozyskiwania informacji o zdrowiu wydają się być najbardziej istotne.

ZAGROŻENIA DOTYCZĄCE JAKOŚCI INFORMACJI

Jakość informacji dostępnych w Internecie z zakresu medycyny i zdrowia człowieka jest skrajnie zróżnicowana. Obok rzetelnych i wartościowych materiałów, można również spotkać takie, które są nie tylko małowartościowe, ale też niebezpieczne, gdyż mogą negatywnie wpływać na zachowania zdrowotne osób z nich korzystających. Jednym z takich zagrożeń jest niekontrolowana reklama leków i paraleków, a także łatwy do nich dostęp poprzez sieć, gdyż nie jest wymagana żadna recepta przy zakupie, a co się z tym wiąże – również wizyta u lekarza. Wyjątkowo groźna jest reklama tzw. e-aptek. Nie trzeba nawet odwiedzać żadnych stron WWW poświęconym e-aptekom, gdyż reklama ta jest po prostu rozsyłana na masową skalę za pomocą poczty elektronicznej. Internetowe apteki oferują sprzedaż leków bez recepty, nawet tych, które w tradycyjnych aptekach recepty wymagają. Wiele internetowych aptek jest zarejestrowanych w krajach, w których prawo zezwala na sprzedaż leków bez recepty – po złożeniu zamówienia e-apteki wysyłają najróżniejsze medykamenty w zwykłej przesyłce. Taki stan rzeczy prowadzi do tego, że coraz więcej osób kupuje za pośrednictwem sieci leki bez zaleceń i kontroli lekarskiej. Jest to szczególnie groźne w odniesieniu do leków psychotropowych – osoby uzależnione mogą je nabywać poprzez sieć bez ograniczeń.

Ponadto, mnogość nierzetelnych informacji wynika z faktu, że Internet stwarza *de facto* możliwość nieograniczonego publikowania treści, bez ponoszenia odpowiedzialności za ich wiarygodność i rzetelność. Ogromna liczba publikowanych informacji powoduje, że wyodrębnienie tych istotnych jest problematyczne, nie tylko dla

przeciętnych użytkowników, ale nawet dla profesjonalistów. Problem ten został zauważony przez wiele organizacji – zarówno akademickich, rządowych, pozarządowych oraz komercyjnych. W konsekwencji, pojawiło się szereg propozycji, które mogłyby ułatwić użytkownikom Internetu ocenę jakości informacji medycznej dostępnej w globalnej sieci. Jednak zdefiniowanie jednolitych standardów jakości dla zróżnicowanych zbiorów informacji jest na tyle trudne i złożone, że do dzisiaj nie udało się stworzyć uniwersalnych narzędzi, które mogą chronić użytkowników Internetu medycznego przed informacjami złej jakości. Organizacje takie jak: *Health on the Net Foundation* (<http://www.hon.ch>) czy *American Medical Informatics Association* (<http://www.amia.org>) – zaproponowały i rozwinęły kryteria pozwalające na ocenę jakości informacji znajdujących się na stronach WWW zawierających treści związane ze zdrowiem człowieka. Ponadto, organizacje te stworzyły tzw. elektroniczne etykiety (*electronic labels*), które mogą być umieszczane na tzw. webowych stronach o tematyce zdrowotnej, spełniających wyznaczone przez te organizacje kryteria jakości.

Dla przykładu, fundacja *Health on the Net Foundation*, stworzyła logo HON Code, które wraz z certyfikatem może otrzymać każda strona WWW przedstawiająca informacje o zdrowiu człowieka, która spełni osiem poniższych kryteriów [18]:

ZASADY HON CODE

1. Wszelkie porady medyczne udzielane i prezentowane w serwisie będą przygotowane jedynie przez fachowy personel medyczny. W przypadku, kiedy autorem ich pewnej części będzie osoba bez medycznych kwalifikacji, zostanie zamieszczona czytelna informacja o tym fakcie.
2. Informacje będą umieszczane w serwisie w celu wsparcia, a nie zastąpienia tradycyjnych relacji pomiędzy pacjentem a lekarzem.
3. Prywatność danych pacjenta i osób odwiedzających strony oraz zasada poufności danych muszą być starannie przestrzegane. Zabrania się przedstawiania jakichkolwiek danych bez zgody pacjenta. Jednocześnie nakazuje się respektowanie wszelkich praw dotyczących prywatności informacji medycznej na stronach WWW i ich kopiach.
4. Informacje zawarte na stronach powinny zawierać dane dotyczące źródła ich pochodzenia, a tam, gdzie to będzie możliwe, zamieszczone będą odpowiednie HTML-owe linki do tych danych. W sposób widoczny będą przedstawione informacje o modyfikacji strony zawierające dane medyczne (np. u dołu strony).
5. Wszelkie dane dotyczące korzyści z prowadzonej terapii, sprzedaży produktów oraz usług będą poparte właściwymi dowodami przedstawionymi tak jak w zasadzie 4.
6. Projektanci serwisu będą się starali, aby informacje podawane w serwisie były jak najbardziej zrozumiałe, a także by był zamieszczony adres kontaktowy dla użytkowników poszukujących dalszych informacji wsparcia. Prowadzący serwis zamieści w widocznym miejscu strony swój adres e-mail.
7. Wymagane jest podanie informacji o instytucji/osobie sponsorującej serwis. Chodzi o wskazanie organizacji komercyjnych oraz non-profit, które dostarczyły funduszy, usług oraz materiałów dla potrzeb serwisu.

8. W przypadku, gdy źródłem finansowania serwisu będzie reklama, zostanie to wyraźnie zaznaczone. Na stronie zostanie zamieszczona informacja o polityce reklamowej prowadzącego serwis. Reklamy oraz inne materiały promocyjne będą przedstawiane użytkownikom w taki sposób i w takim kontekście, by ułatwić ich odróżnianie od oryginalnych materiałów opracowanych przez instytucję prowadzącą serwis.

W przypadku kiedy strona z interesującymi nas informacjami dotyczącymi zdrowia, nie jest stroną zarządzaną przez ośrodek naukowy lub rządowy i nie posiada żadnego certyfikatu przyznawanego przez takie organizacje jak *Health on the Net Foundation* czy *American Medical Informatics Association*, wtedy istnieje większe prawdopodobieństwo, że informacje tam zawarte mogą być nierzetelne. Wtedy taką stronę WWW należałoby przeanalizować pod kątem podanych wyżej 8 zasad – im więcej taka strona będzie spełniała kryteriów według HON Code, tym większe prawdopodobieństwo, że podane tam informacje są rzetelne. Dobrze jest również, za pomocą zapytania skierowanego do wyszukiwarki Google, w postaci: link: adres URL strony, sprawdzić na jakich stronach umieszczony został link do strony, którą analizujemy pod kątem wiarygodności. Jeśli ów link odnajdziemy na stronach zaufanych, tzn.: należących do organizacji rządowych lub ośrodków akademickich, wtedy wiarygodność takiej strony wzrasta. Im więcej stron zaufanych powołuje się lub nawet tylko umieszcza taki link na swoich stronach, oznacza to, że strona taka została zakwalifikowana jako wiarygodna. Oczywiście należy wtedy dokładnie przeczytać w jakim kontekście ów link został podany – należy upewnić się, że nie jest on podawany w negatywnym kontekście.

ZAGROŻENIA DOTYCZĄCE LEGALNOŚCI POZYSKANEJ INFORMACJI

Internauta pobierając z Internetu materiały naukowe, czyli jakiegokolwiek utwory (w rozumieniu prawa polskiego, wszystko co posiada prawa autorskie nazywane jest utworem), narażony jest na nieświadome pobranie np. dzieła, którego autor nie zezwolił na powielanie w jakiegokolwiek formie – gdyż każdy utwór zamieszczony w Internecie podlega ochronie, zaś zakres dostępu do utworów zależy od właścicieli praw, które precyzuje i reguluje ustawa o prawie autorskim. Innymi słowy: każdy kto korzysta z globalnej sieci powinien mieć świadomość, że korzystanie (czyli pobieranie danych) z ogólnodostępnych zasobów Internetu może wiązać się z popełnianiem przestępstwa w świetle obowiązującego prawa polskiego. Wynika to z faktu, że internauta nie może tłumaczyć się nieznajomością prawa, ani tym, że był nieświadomy tego co pobierał z sieci. Dlatego też, aby definitywnie uniknąć zagrożenia polegającego na nielegalnym pobraniu jakiegoś utworu, należałoby wprawdzie przed pobraniem, upewnić się, że prawa autorskie tego utworu pozwalają na jego pobranie. Jednak jeśli nawet prawa autorskie danego utworu zezwalają na jego pobranie, to należy również pamiętać, że taki utwór można wykorzystywać wyłącznie w sposób, na jaki zgodził się właściciel praw.

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. nr 24, poz. 83 z późn. zm.), w rozdziale 1., w art. 1. w punkcie 2., stwierdza, że [19]:

„W szczególności przedmiotem prawa autorskiego są utwory:

- 1) wyrażone słowem, symbolami matematycznymi, znakami graficznymi (literackie, publicystyczne, naukowe, kartograficzne oraz programy komputerowe);
- 2) plastyczne;
- 3) fotograficzne;
- 4) lutnicze;
- 5) wzornictwa przemysłowego;
- 6) architektoniczne, architektoniczno-urbanistyczne i urbanistyczne;
- 7) muzyczne i słowno-muzyczne;
- 8) sceniczne, sceniczno-muzyczne, choreograficzne i pantomimiczne;
- 9) audiowizualne (w tym filmowe).”

Natomiast w art. 3., ustawa dodaje również, że:

„Zbiory, antologie, wybory, bazy danych spełniające cechy utworu są przedmiotem prawa autorskiego, nawet jeżeli zawierają niechronione materiały, o ile przyjęty w nich dobór, układ lub zestawienie ma twórczy charakter, bez uszczerbku dla praw do wykorzystanych utworów.”

Ta sama ustawa w art. 4., definiuje również, co nie podlega prawu autorskiemu:

„Nie stanowią przedmiotu prawa autorskiego:

- 1) akty normatywne lub ich urzędowe projekty;
- 2) urzędowe dokumenty, materiały, znaki i symbole;
- 3) opublikowane opisy patentowe lub ochronne;
- 4) proste informacje prasowe.”

Wydawać by się mogło, że ustawa o prawie autorskim i prawach pokrewnych, jest tak restrykcyjna, że jej przestrzeganie jest wręcz niemożliwe, gdyż każdy internauta, który chciałby pobrać cokolwiek z sieci, musiałby przed pobraniem zawsze sprawdzać jak zostały sformułowane prawa autorskie do konkretnego utworu (według części prawników, właśnie tak powinno się robić). Jednak można spotkać również inne interpretacje prawne tej ustawy. Mianowicie, obok restrykcyjnych przepisów, ta sama ustawa wprowadza również pojęcie dozwolonego użytku chronionych utworów, pozwalającego na nieodpłatne korzystanie z artykułów, plików muzycznych i filmów nie tylko posiadaczowi oryginalnego nagrania, ale także osobom, które pozostają z nim w bliskim związku osobistym. Ustawa nie precyzuje jednak warunków, które decydują o tym, że dany sposób korzystania z utworu jest użytkowaniem osobistym. Ustawa o prawie autorskim nie precyzuje również stopnia pokrewieństwa i powinowactwa, który ogranicza dopuszczalność dozwolonego użytku. Dlatego też, wielu prawników interpretuje to w taki sposób, że cel używania może być w związku z tym różnorodny (naukowy, kolekcjonerski, rozrywkowy). W konsekwencji dozwolone jest kopiowanie z Internetu takich utworów jak np.: artykuły, książki, całe strony WWW (z technicznego punktu widzenia otwarcie strony za pomocą przeglądarki jest również jej skopiowaniem) w celu tworzenia prywatnego zbioru, który jest wykorzystywany w celach naukowych albo edukacyjnych.

Ustawa o prawie autorskim i prawach pokrewnych jest tak skonstruowana, że wiele punktów w niej zawartych może być różnie rozumianych w zależności od interpretacji prawnej. Należy jednak pamiętać, że internauci, którzy pobierają utwory objęte prawem autorskim nie zezwalającym na kopiowanie są narażeni na odpowiedzialność cywilną względem twórcy – może on zażądać od takiego internauty odszkodowania finansowego. Natomiast rozpowszechnianie

i zwielokrotnienie w Internecie wbrew zasadom dozwolonego użytku utworów posiadających prawa autorskie może zostać potraktowane jako przestępstwo, zagrożone karą grzywny lub pozbawienia wolności do lat 5. Osoby, które dodatkowo przy zwielokrotnieniu utworów objętych prawami autorskimi czerpią korzyści finansowe, mogą podlegać pozbawieniu wolności na dłużej niż 5 lat [20].

ZAGROŻENIA TECHNICZNE

Korzystając z Internetu należy pamiętać, że zawsze wysyłamy i pobieramy dane. Jeśli wysyłamy poufne dane, to należy minimalizować ryzyko ich przechwycenia. Należy upewnić się, że miejsce, w którym podłączamy się do Internetu jest godne zaufania. Kafejka internetowa, publiczny tzw. hotspot, inne miejsce publiczne z dostępem do Internetu nie są miejscami bezpiecznymi jeśli chcemy minimalizować ryzyko przechwycenia wysyłanych i odbieranych przez nas informacji. Miejsca godne zaufania, to takie, kiedy wiemy dokładnie kto jest dostarczycielem usług internetowych (providerem). Jeśli nie jest to połączenie bezpośrednie do Internetu (np. poprzez firmę telekomunikacyjną, itp.) tylko połączenie za pośrednictwem sieci LAN, to należy zwrócić szczególną uwagę na to kto jest administratorem tej sieci – czy jest to osoba zaufana i w jaki sposób dba o bezpieczeństwo tej sieci. Następnie należy upewnić się, że oprogramowanie, którego używamy jest pozbawione wirusów, programów szpiegujących (ang. *spyware*), etc. W tym celu najlepiej zaopatrzyć się w program antywirusowy, który co pewien czas skanuje nasz komputer w poszukiwaniu złośliwego oprogramowania, i który codziennie pobiera aktualizacje o bazie najnowszych wirusów oraz automatycznie analizuje pod kątem obecności wirusów każdy pobrany przez nas plik z Internetu. Kolejną rzeczą zapewniającą nam dodatkowe bezpieczeństwo to instalacja *firewall'a*, najlepiej takiego, który pobiera z Internetu informacje o numerach IP niebezpiecznych stron WWW i blokuje je, kiedy chcemy na nie wejść lub kiedy zostaniemy na takie strony przekierowani. *Firewall* pozwoli nam również zablokować nieużywane porty w komputerze oraz usługi i programy, które mogą zostać wykorzystane przez osoby trzecie z zewnątrz – jako tzw. tylne wejścia (ang. *backdoors*). Należy cyklicznie (najlepiej automatycznie) aktualizować aplikacje internetowe, które wykorzystujemy do łączenia się z Internetem – takie jak: przeglądarka internetowa, komunikatory internetowe, itp. Podczas wysyłania i odbierania poufnych danych, należy wykorzystywać wyłącznie oprogramowanie i protokoły, które szyfrują dane. W przypadku poczty elektronicznej należy stosować bezpieczne połączenie SSL. Jeśli wypełniamy formularz na stronie WWW to upewnijmy się, że używany jest do tego celu bezpieczny protokół HTTPS. Natomiast jeśli poufne informacje mają zostać przesłane za pomocą komunikatora internetowego, to należy upewnić się, że ów komunikator szyfruje rozmowy wychodzące i przychodzące – zarówno te w trybie tekstowym jak i głosowym. Wykorzystując wirtualne sieci prywatne (VPN – ang. *virtual private network*) poprzez Internet trzeba upewnić się, że oprogramowanie, które je obsługuje, szyfruje przesył danych w obu kierunkach (np. programem VPN wyposażonym w szyfrowanie sesji jest Hamachi). Używając oprogramowania umożliwiającego zdalną pracę na odległych komputerach (potocznie: zdalny pulpit), powinno się wykorzystywać wyłącznie opro-

gramowanie, które potrafi szyfrować zdalne sesje. Ponadto, należy pamiętać, że używając innego niż własnego sprzętu komputerowego, istnieje większe prawdopodobieństwo, że informacje, które wysyłamy i odbieramy mogą być przez osoby trzecie przechwytywane – gdyż to nie my jesteśmy administratorami takiego sprzętu i nie mamy wpływu jakie oprogramowanie jest na takim sprzęcie zainstalowane (dot. szczególnie takich miejsc jak kafejki internetowe).

Powyższe zalecenia powinny być szczególnie kierowane do personelu zatrudnionego w organizacjach i instytucjach funkcjonujących w obszarze zdrowia publicznego. Organizacje takie są zmuszone do starannego przestrzegania ustawy o ochronie danych osobowych, szczególnie wtedy gdy przesyłają poufne dane (np. o pacjentach) poprzez Internet. Opisując kwestie technicznych zagrożeń w kontekście przesyłania i przetwarzania poufnych danych w organizacjach, które takimi danymi dysponują, nie można zapomnieć również o tzw. czynniku ludzkim. Żaden doskonale zabezpieczony system informatyczny nie będzie systemem bezpiecznie chroniącym dane, jeśli użytkownicy tego systemu (infrastruktury informatycznej) nie będą odpowiednio przeszkoleni w zakresie zagadnień informatycznych i socjotechnicznych. Obecnie większość wycieków poufnych danych w dużych przedsiębiorstwach i organizacjach nie jest spowodowana tylko i wyłącznie lukami w systemach bezpieczeństwa. Zdarzenia takie wynikają najczęściej z powodu nieuświadomienia pracownikom, że z pozoru nieistotne informacje, które są przez tych pracowników przekazywane osobom z zewnątrz w konsekwencji mogą posłużyć do zdobycia kolejnych informacji – tym razem bardziej istotnych. To właśnie takie czynniki jak nieuświadomiony personel na okoliczność możliwości wystąpienia niebezpieczeństw informatycznych i zagrożeń socjotechnicznych (mogących wystąpić ze strony osób trzecich), najczęściej przyczynia się do tego, że osoba z zewnątrz (np. haker) może zebrać dzięki pracownikom (nieświadomym potencjalnych zagrożeń) potrzebne informacje, które potem posłużą do poważnego w skutkach ataku przeprowadzonego z Internetu, np. na serwer należący do tej organizacji. Dlatego też, oprócz wprowadzania norm i standardów pozwalających chronić bezpieczeństwo danych, ważna jest również edukacja pracowników wszelkich organizacji, które dysponują poufnymi danymi i cennymi informacjami. Edukacja informatyczna – np. w celu uświadomienia niebezpieczeństw wynikających z nieodpowiedzialnego korzystania z Internetu i psychologiczna – np. w celu rozpoznawania technik socjotechnicznych mających na celu wydobycie informacji. Edukacja, której celem powinno być umacnianie najsłabszego ogniwa w zabezpieczeniach systemów informatycznych gromadzących liczne dane – czyli pracowników obsługujących te systemy [21].

PIŚMIENNICTWO

1. Czy Internet może być źródłem informacji o usługach medycznych: <http://www.federacja-konsumentow.org.pl/story.php?story=109>, 28.09.2009.
2. Fulmański P, Sobieski Ś. Wstęp do informatyki. Łódź: Wyd. Uniwersytetu Łódzkiego; 2005. s. 229-33.
3. Getzen T. Informacja. W: *Ekonomia zdrowia*. Warszawa: Wydawnictwo Naukowe PWN; 2000. s. 412-15.
4. Gil R, Dziedziczko A. Pojęcie świadomości zdrowotnej, zdrowia i choroby. *Zdr Publ*. 2004;114(2):250-5.
5. <http://pl.wikipedia.org/wiki/Informacja>, 28.09.2009.

6. Katalog Rozproszony Bibliotek Polskich, <http://karo.umk.pl/Karo>, 28.09.2009.
7. Przyłuska J. Efektywność wykorzystywania źródeł informacji naukowej a potrzeby edukacyjne użytkowników, <http://www.ebib.info/publikacje/matkonf/25kpbm/przyluska.php>, 28.09.2009
8. Richardson E. Złożoność struktur zdrowia publicznego w krajach Unii Europejskiej – Raport porównawczy. W: Zdrowie publiczne w krajach europejskich – wybrane zagadnienia etyczne. Włodarczyk C, Shickle D, Czabanowska K, red. Kraków: Wyd. Uniwersytetu Jagiellońskiego; 2007. s. 35-61.
9. Ryś E. Źródła informacji w zdrowiu publicznym. W: Informacja naukowa w zdrowiu publicznym. Franaszek P, red. Kraków: Wyd. Uniwersytetu Jagiellońskiego; 2001. s. 73-90.
10. Staniszewski A, Bujnowska-Fedek MM. Korzystanie z Internetu medycznego i usług z zakresu e-zdrowia w opinii publicznej Polaków w 2007 roku. *Przew Lek.* 2008;1:287-9.
11. Wdowiak L, Czubek A, Bojar I, Steć A. Kierunki rozwoju opieki zdrowotnej w Polsce a koncepcja społeczeństwa informacyjnego. *Zdr Publ.* 2006;116(4):543-7.
12. Wdowiak L. Dziś i jutro medycyny społecznej i zdrowia publicznego. *Zdr Publ.* 2004;114(2):125-6.
13. Właśniak K, Marcinkowski JT. Ocena sposobów wyszukiwania informacji o zdrowiu w Internecie przez młodzież. *Zdr Publ.* 2007;117(2): 164-70.
14. Zöllner H. WHO's Vision and Strategy of Public Health In Europe. *Zdr Publ.* 2001;111(5-6):422-5.
15. Ryś E, Stachura-Chatłas M. Informacja naukowa w zdrowiu publicznym. W: Zdrowie publiczne – wybrane zagadnienia. Tom I. Czupryna A, Poździej S, red. Kraków: Uniwersyteckie Wydawnictwo Medyczne Vesalius; 2000. s. 229-64.
16. <http://pl.wikipedia.org/wiki/Informatyzacja>, 28.09.2009.
17. Niedźwiedzka B. Rozpowszechnianie wyników badań naukowych i wdrażanie innowacji. W: Informacja naukowa w zdrowiu publicznym. Franaszek P, red. Kraków: Wyd. Uniwersytetu Jagiellońskiego; 2001. s. 127-51.
18. Marcinkowski JT, Właśniak K. Jakość dostępnych w Internecie informacji o zdrowiu. *Zdr Publ.* 2007;117(2):220-4.
19. http://www.prawo.ngo.pl/files/prawo.ngo.pl/public/akty_prawne_obowiazujace/ustawa_o_prawie_autorskim.pdf 28.09.2009
20. Makosz A. Prawa autorskie w Internecie. <http://www.infor.pl/temat-dnia/48867,Prawa-autorskie-w-internecie.html>, 28.09.2009.
21. Mitnick K, Simon L. Sztuka podstępu: łamałem ludzi, nie hasła. Gliwice Wydawnictwo Helion, 2003, s. 282-357.

Informacja o Autorach

Dr n. ekonom. MAREK BRYŁA – adiunkt, Zakład Medycyny Społecznej, Katedra Medycyny Społecznej i Zapobiegawczej, Uniwersytet Medyczny w Łodzi; mgr GRZEGORZ STEGIENTA, dr n. med. ALINA KOWALSKA – adiunkt, Zakład Medycyny Społecznej, Katedra Medycyny Społecznej i Zapobiegawczej, Uniwersytet Medyczny w Łodzi; dr hab. n. med. IRENA MANIECKA-BRYŁA – kierownik, Zakład Epidemiologii i Biostatystyki, Katedra Medycyny Społecznej i Zapobiegawczej, Uniwersytet Medyczny w Łodzi.

Adres do korespondencji

Dr n. ekonom. Marek Bryła
Zakład Medycyny Społecznej
Katedra Medycyny Społecznej i Zapobiegawczej
Uniwersytetu Medycznego w Łodzi
ul. Żeligowskiego 7/9, 90-752 Łódź, tel. (42) 639-32-73