Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, 97–113
DOI: 10.17951/teka.2018.13.2.97-113

ZAGROŻENIA DLA BEZPIECZEŃSTWA ZDROWOTNEGO W SIECI

Justyna Kięczkowska
Wydział Politologii
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
ORCID ID: https://orcid.org/0000-0002-9395-2363
e-mail: justyna.kieczkowska@poczta.umcs.lublin.pl

Streszczenie: Głównym celem artykułu jest analiza zagrożeń dla bezpieczeństwa zdrowotnego wynikających z użytkowania sieci i urządzeń mobilnych. W artykule uznano również za istotne wskazanie realnych możliwości przeciwdziałania tym zagrożeniom na poziomie jednostki, państwa i innych podmiotów odpowiedzialnych za bezpieczeństwo zdrowotne.

Słowa kluczowe: cyberprzestrzeń, zagrożenia, zdrowie, bezpieczeństwo zdrowotne

W opracowaniu autor stara się przedstawić główne czynniki, które generują zagrożenia dla bezpieczeństwa zdrowotnego, jak również wpływają na ich rozwój. W artykule przedstawiono następujące tezy: zagrożenia dla bezpieczeństwa zdrowotnego wynikają przede wszystkim z rozwoju nowych technologii, a także z powszechnej dostępności urządzeń umożliwiających korzystanie z sieci; rozwój zagrożeń bierze się przede wszystkim ze zmiany modelu pracy, komunikacji społecznej i funkcjonowania w społeczeństwie, zmiana ta polega na stałym byciu online i posługiwaniu się siecią w większości obszarów życia społecznego; zagrożenia dla bezpieczeństwa zdrowotnego w sieci wynikają w dużej mierze z braku umiejętności świadomego i rozsądnego korzystania z internetu; zagrożenia te i ich rozwój są powiązane z działalnością przestępczą i często wiążą się z zamiarem wyrządzenia szkody drugiej osobie. Wszystkie z wymienionych tez zostały w artykule omówione i uzasadnione konkretnymi przykładami.

Bezpieczeństwo zdrowotne to jedna z najważniejszych kwestii, jeżeli rozpatruje się efektywne funkcjonowanie jednostki w społeczeństwie. Konieczne więc wydaje się rozpoczęcie dyskusji o wpływie sieci na poziom bezpieczeństwa zdrowotnego społeczeństwa.

PODSTAWOWE DEFINICJE

Zdefiniowanie zagrożeń wynikających z użytkowania i rozwoju internetu jest możliwe dzięki przede wszystkim dookreśleniu cyberprzestrzeni. Terminu tego użył po raz pierwszy W. Gibbson w powieści *Burnig Chrome* [Bógdał-Brzezińska, Gawrycki 2003], w której cyberprzestrzeń nazwał matrycą, obecnie tym określeniem nazywa się wirtualną przestrzeń, gdzie komputery i media cyfrowe komunikują się ze sobą za pomocą globalnego systemu komunikacji – internetu. Cyberprzestrzeń to również system powiązań internetowych, który tworzy przestrzeń komunikacyjną [Szubrycht 2005].

Wydaje się zasadne przypisanie cyberprzestrzeni kluczowego miejsca w ocenie rozwoju społeczeństwa w każdym wymiarze. To właśnie w wirtualnej rzeczywistości są realizowane zasadnicze funkcje i role jednostki, praca, komunikacja, różnego rodzaju transakcje. To również z niej wypływają niebezpieczeństwa mogące mieć znaczenie dla poziomu bezpieczeństwa zdrowotnego społeczeństw [Tadeusiewicz 2016]. Za zagrożenia dla bezpieczeństwa zdrowotnego w sieci autor uznał wszelkie działania i aktywności powodujące bądź mogące powodować realne zagrożenie dla życia i zdrowia lub trwały uszczerbek na zdrowiu.

Zdefiniowania wymagają również same pojęcia „zdrowie" i „bezpieczeństwo zdrowotne". W ujęciu szerokim samo zdrowie jest definiowane zgodnie z wytycznymi Światowej Organizacji Zdrowia jako całkowity dobrostan: „Zdrowie to nie tylko całkowity brak choroby, czy kalectwa, ale także stan pełnego, fizycznego, umysłowego i społecznego dobrostanu (dobrego samopoczucia). Definicja ta jest bardzo ważna i postępowa, ponieważ nie poprzestaje na samym negującym ujęciu, że zdrowie jest brakiem choroby, ale bardzo mocno akcentuje, że zdrowie ma w sobie aktywny aspekt, którym jest dobrostan. Oznacza to, że w kwestiach zdrowia nie mamy jedynie koncentrować się na chorobach i próbach ich zwalczania, ale powinniśmy zwłaszcza koncentrować się na samym zdrowiu – na jego wzmacnianiu" [*Holizm i zdrowie*… 2017]. Z takiego ujęcia zdrowia ujawnia się jeszcze jeden aspekt, a mianowicie kwestia dochodzenia do rzeczonego dobrostanu. W tym miejscu należy przytoczyć definicję bezpieczeństwa zdrowotnego określanego, zdaniem autora, jako proces, w którym jednostki i podmioty o charakterze rządowym, samorządowym, pozarządowym, specjalistycznym i niespecjalistycznym aktywnie dążą do zwiększenia oddziaływania na stan zdrowia w celu jego utrzymania lub poprawy, a także na wszystkie elementy systemu, którego domeną jest ochrona zdrowia. Taka definicja pozwala bowiem na podkreślenie przede wszystkim istoty zdrowia jako nadrzędnej wartości w życiu człowieka, a także roli, jaką pełnią wszystkie składowe systemu ochrony zdrowia w celu jego utrzymania, jak również zapewnienia bezpieczeństwa na najwyższym poziomie.

CZYNNIKI WPŁYWAJĄCE NA ROZWÓJ ZAGROŻEŃ DLA BEZPIECZEŃSTWA ZDROWOTNEGO W SIECI

Rozwój zagrożeń w sieci nierozerwalnie jest związany z postępem technologicznym, przejawiającym się stale wzrastającą liczbą użytkowników internetu, a tym samym posiadaczy urządzeń mobilnych coraz to nowszych generacji. Nowy raport na temat stanu rynku cyfrowego, mobile i social mediów ze stycznia 2018 roku pokazuje, iż na chwilę obecną z internetu korzysta ponad 4 miliardy ludzi na całym świecie, a ponad połowa populacji na świecie jest obecnie online. Najnowsze dane ukazują, że prawie 250 mln nowych internautów pojawiło się w samym 2017 roku, co wynikało z przystępnych cen smartfonów, a także stale taniejących planów transmisji danych komórkowych [*Coraz więcej ludzi*… 2017]. Ponad połowa używanych obecnie telefonów to urządzenia „inteligentne" (smartfony), co pozwala na łatwe i niczym nieograniczone korzystanie z internetu. Automatycznie wzrostowi uległa również ilość czasu spędzona przez jednostki w internecie w ciągu ostatniego roku. Na urządzeniach mobilnych średni dzienny czas korzystania z aplikacji na jednym smartfonie wyniósł 2 godziny. Najnowsze dane z GlobalWebIndex pokazują, że przeciętny użytkownik sieci spędza obecnie około 6 godzin dziennie przy użyciu urządzeń i usług internetowych. Jeśli dodamy to do wszystkich 4 mld użytkowników internetu na świecie, w 2018 roku spędzimy online oszałamiający 1 mld lat. W przypadku Polski w 2018 roku nasze państwo zamieszkuje już 38,14 mln ludzi, z czego aż 78% korzysta z internetu (29,75 mln), prawie połowa używa aktywnie social mediów, a 37% smartfonów do korzystania z komunikacji społecznościowej. Obecnie na jednego mieszkańca Polski przypada 1,3 karty SIM [Majchrzak 2018]. Dane te pokazują pewne prawidłowości, które można uznać za czynniki generujące zagrożenia w sieci, zarówno o charakterze ogólnym, jak i te mające bezpośredni wpływ na bezpieczeństwo zdrowotne jednostek. Po pierwsze stale spadające ceny urządzeń mobilnych i transmisji danych sprawiają, że obywatel z przeciętnym wynagrodzeniem jest w stanie zapewnić sobie urządzenie w postaci smartfona (koszt około 300 zł) i abonament gwarantujący brak limitów w transmisji danych. Drugi czynnik to właśnie sam model urządzeń służących do korzystania z sieci – to już nie duży, zabierający miejsce stacjonarny czy trochę mniejszy laptop, ale urządzenie mieszczące się w dłoni, które można wykorzystać w każdym miejscu i czasie. Kolejny czynnik to zmiana modelu funkcjonowania, pracy i komunikacji społeczeństwa. Przy pomocy internetu pracujemy i szukamy pracy, nawiązujemy znajomości, rozmawiamy, przekazujemy i odczytujemy informacje, dokonujemy transakcji. Współczesny model komunikacji i pracy bez sieci i bycia online jest praktycznie niemożliwy. Wszystko to sprawia, iż używanie internetu zajmuje wiele godzin w ciągu doby, co stanowi o tym, iż czas, jaki zostaje poświęcony na bycie w sieci, staje się kolejnym czynnikiem generującym zagrożenia dla bezpieczeństwa zdrowotnego. Internet to sfera, która w dużej części nie jest regulowana i nie podlega jasnej, restrykcyjnej kontroli ze strony np. prawodawstwa państwowego, jest również obszarem, który daje możliwości zamieszczania treści czy prowadzenia

działalności, często o charakterze przestępczym – co należy również zakwalifikować jako czynnik powodujący rozwój zagrożeń w sieci. W przypadku zagrożeń dla bezpieczeństwa zdrowotnego w tym miejscu należy wskazać rozwój nielegalnego handlu medykamentami, narkotykami, działanie for internetowy zawierających niepotwierdzone informacje i zalecających niespecjalistyczne procedury lecznicze. Powszechność, niski koszt urządzeń, niczym nieograniczony dostęp i możliwość zamieszczania treści oraz prowadzenia działań to czynniki, które powodują wzrost i rozwój zagrożeń dla bezpieczeństwa zdrowotnego w sieci. Analizując dane o charakterze statystycznym, należy także podkreślić, iż w związku ze stałym wzrostem znaczenia tych czynników będą się również rozwijać zagrożenia dla bezpieczeństwa zdrowotnego w sieci.

RODZAJE ZAGROŻEŃ DLA BEZPIECZEŃSTWA ZDROWOTNEGO W SIECI

Tak zwane bycie online, czyli stałe użytkowanie sieci, jest nieodzowną częścią większości sfer życia jednostki. Pracujemy w internecie i przy jego pomocy, rozmawiamy, załatwiamy sprawy służbowe i prywatne, układamy swój czas wolny, regulujemy zobowiązania, robimy zakupy itd. Na chwilę obecną można zaryzykować stwierdzenie, iż większość społeczeństwa nie wyobraża sobie życia bez dostępu do sieci. Duża część obywateli postrzega go jako narzędzie do efektywnego funkcjonowania. Usieciowienie życia społecznego w każdym jego wymiarze niesie ze sobą również wiele zagrożeń dla życia i zdrowia jednostki, a przede wszystkim dla jej bezpieczeństwa zdrowotnego. Zagrożenia te można podzielić na zagrożenia psychiczne i fizyczne, które zostały uznane za jednostki chorobowe, jak również takie, które są w trakcie zaliczania ich do zaburzeń o charakterze chorobowym oraz takie, które posiadają znamiona bądź są czynami o charakterze przestępczym mającymi bezpośredni wpływ na poziom bezpieczeństwa zdrowotnego obywateli. Do zagrożeń uznanych za jednostki chorobowe zalicza się: dolegliwości wzroku, zespół RSI, dolegliwości układu kostno-szkieletowego, do grupy drugiej zaś przede wszystkim zespół uzależnień od internetu [*Zagrożenia cyberprzestrzeni*… 2013; Nowacki 2015]. W grupie trzeciej zdaniem autora należy umieścić zjawiska i działania, które w sposób negatywny wpływają na bezpieczeństwo zdrowotne, takie jak: użytkowanie for internetowych i stron specjalizujących się w diagnozowaniu chorób czy procesach leczenia, nielegalny handel wyrobami medycznymi, zarówno lekami dostępnymi na receptę, jak i narkotykami czy wyrobami medycznymi, kradzież, nielegalne wykorzystywanie danych medycznych i wreszcie bezpośrednie ataki na infrastrukturę medyczną służącą np. telemedycynie.

Analizując podział zagrożeń i ukazując ich grupy, należy również podkreślić, iż jednostka jest ich głównym generatorem. Stając się użytkownikiem sieci, wkracza ona bowiem na terytorium, które każdego dnia się zmienia, rzekomo dostosowując do potrzeb potencjalnego użytkownika, stanowiąc remedium na każdy problem. Takie podejście do wirtualnej rzeczywistości i możliwości inter-

netu jest przyczyną rozwoju działań, sytuacji i mechanizmów, których efektem są zagrożenia dla bezpieczeństwa zdrowotnego. W celu lepszego ukazania istoty, jak również potencjalnych, negatywnych efektów zagrożeń konieczne wydaje się zaprezentowanie krótkiej analizy poszczególnych ich przykładów.

Na pierwszym miejscu należy więc omówić zagrożenia dla bezpieczeństwa zdrowotnego w sieci uznane za jednostki chorobowe. Podkreślenia wymaga fakt, iż rozwój tych zagrożeń wynika li tylko ze sposobu funkcjonowania jednostek w obecnej rzeczywistości. Zagrożenia dla zdrowia fizycznego powstają więc w wyniku bycia użytkownikami internetu i urządzeń przeznaczonych do korzystania z sieci i innych systemów. Pierwszym najbardziej wyraźnym zagrożeniem jest wzrastająca liczba jednostek uskarżających się na tzw. *computer vision syndrome* (CVS). Pod tym terminem medycy umieszczają dolegliwości narządu wzroku najczęściej spowodowane przeciążeniem związanym ze zbyt długą pracą przy komputerze, jak również użytkowaniem urządzeń multimedialnych dla celów rozrywkowych. Medycy jednogłośnie stwierdzają, iż syndrom ten dotyka już nie tylko osoby dorosłe, ale coraz częściej z dolegliwościami wzroku do specjalistycznych poradni zgłaszają się młodzi lub mali pacjenci – 1,6 mld ludzi na świecie jest dotkniętych krótkowzrocznością; w 2050 r. połowa ludzkości będzie miała tę wadę wzroku [Grzybowski, Szajkowska 2017]. Amerykańskie Stowarzyszenie Okulistyczne opracowało listę syndromów CVS i zaliczało do niej: astenopatię, czyli przemęczenie wzroku, zmęczenie, ból głowy, utratę ostrości wzroku, diopatię, czyli podwójne widzenie, senność, trudności w czytaniu oraz koncentracji, podrażnienie oczu [*Zagrożenia cyberprzestrzeni*… 2013].

Kolejnym zagrożeniem dla użytkownika sieci i urządzeń multimedialnych jest *repetitive strain injury*, czyli zespół RSI – jest to zbiorczy termin dla schorzeń występujących w związku z koniecznością powtarzania ruchów i czynności związanych z pracą np. przy komputerze. Wśród przyczyn RSI wynikających z pracy przy komputerze wymienia się między innymi: konieczność powtarzania czynności, niestosowanie się do zasad ergonomiki pracy, długotrwałą pracą przy komputerze. W powszechnym języku medycznym w Polsce do zespołu tego najczęściej zalicza się zespół cieśni nadgarstka, jak również tzw. kciuk BlackBerry, czyli schorzenie kciuka związane z nadmiernym używaniem klawiatury dotykowej urządzeń multimedialnych. Do objawów występowania zarówno cieśni nadgarstka, jak i kciuka BlackBerry zalicza się: trudności z chwytaniem przedmiotów, bóle przy uchwycie, mrowienie kciuka, uszkodzenie nerwu pośrodkowego powodującego ból dłoni, poranne bóle lub bóle w czasie odprężenia [*Zagrożenia cyberprzestrzeni*… 2013]. Schorzenia zaliczane do zespołu RSI są jedną z najczęstszych przyczyn absencji zawodowej obywateli w Wielkiej Brytanii, gdzie corocznie ponad 1 milion pracowników udaje się na zwolnienie lekarskie w związku z RSI [The Health and Safety Executive 2013][1].

[1] Brytyjczycy cierpią w coraz większym stopniu na schorzenia nadgarstków i kciuków powodowane częstym używaniem telefonów komórkowych. Każdego dnia w Wielkiej Brytanii wysyła

Narastającym zagrożeniem wynikającym bezpośrednio z bycia użytkownikiem są dolegliwości układu kostno-szkieletowego MSD. Zgodnie z definicją Europejskiej Agencji Bezpieczeństwa i Zdrowia w Pracy z siedzibą w Bilbao za tego typu dolegliwości uznaje się choroby układu mięśniowo-szkieletowego związane z pracą, wywołujące upośledzenia struktur anatomicznych, takich jak: mięśnie, stawy, ścięgna, więzadła, nerwy, kości i miejscowy układ krążenia krwi, wywołane lub nasilone przede wszystkim na skutek wykonywania pracy oraz bezpośrednio przez odziaływanie czynników otoczenia, w którym praca jest wykonywana [*Choroby układu mięśniowo-szkieletowego*… 2013]. Choroby układu mięśniowo-szkieletowego mogą być charakteryzowane jako schorzenia o charakterze epizodycznym, ponieważ ból często znika i powraca po kilku miesiącach lub latach. Niektóre MSD jednak mogą mieć charakter chroniczny lub nieuleczalny. Grupa schorzeń zaliczana do MSD jest bardzo rozległa, jednak najpopularniejszymi występującymi wśród osób pracujących i użytkujących komputery dolegliwościami są bóle pleców, czy okolic szyi, tzw. łamanie kręgosłupa.

Wymienione zagrożenia są klasyfikowane, jak już pisano powyżej, jako jednostki chorobowe, co za tym idzie ich zdiagnozowanie u potencjalnego użytkownika sieci i urządzeń multimedialnych nierozerwalnie łączy się z zakwalifikowaniem danej jednostki do procesu leczenia, najczęściej uciążliwego, związanego z dolegliwościami bólowymi wynikłymi czy to z operacji, czy rehabilitacji. Występowanie tych zagrożeń w sposób oczywisty przekłada się również na efektywność społeczną zarówno w wymiarze zawodowym, jak i prywatnym, tym samym generuje najczęściej negatywne skutki dla gospodarki państw.

Powszechnym zagrożeniem dla użytkowników jest także zespół uzależnienia od internetu – IAD. Uzależnienie od internetu lub też, jak niektórzy określają, siecioholizm nie jest sklasyfikowane jako jednostka chorobowa według klasyfikacji zaburzeń psychicznych. Określenie listy problemów czy też objawów może jednak wskazywać na to, iż w niedalekiej przyszłości zespół uzależnień zostanie sklasyfikowany jako zaburzenie psychiczne. Do listy objawów zalicza się więc: alienację, zaburzenia rytmu dobowego (późne chodzenie spać, notoryczne spóźnianie się do szkoły czy pracy), podrażnienie, agresję, radykalizację poglądów, plany samobójcze, konflikty z prawem związane z działalnością w internecie, zaniedbywanie obowiązków zawodowych oraz rodzinnych, odczuwalne podniecenia na myśl o pracy przy komputerze, przeglądanie nielegalnych treści w internecie, radykalną zmianę zachowania [*Uzależnienie od internetu* 2018]. Analizując

się 93,5 mln wiadomości tekstowych SMS. Tej niemałej liczbie przesyłek towarzyszy zwiększająca się liczba zgłaszanych przypadków tzw. RSI, wynikająca z częstego powtarzania przez palce i nadgarstki tych samych ruchów. Ocenia się, że o około 38% więcej osób cierpi obecnie na bóle nadgarstków i kciuków spowodowane wykorzystywaniem funkcji SMS telefonów komórkowych niż miało to miejsce jeszcze pięć lat temu. W ciągu roku problemy tego typu zgłosiło 3,8 mln osób. Badania przeprowadzone dla Virgin Mobile pokazały, że ponad 12% pytanych wysyła dziennie 20 wiadomości SMS. 10% ankietowanych każdego dnia posyła do 100 takich wiadomości, Wielka Brytania – więcej przypadków RSI, http://itbiznes.pl/art18402.html [dostęp: 12.11.2017].

IAD, należy także wyznaczyć jego typ, i tu wyróżnić można: uzależnienie od gier komputerowych, które dotyka w szczególności dzieci i młodzież, erotomanię komputerową, uzależnienie od informacji [Bartosik 2014], uzależnienie od kontaktów społecznych w sieci, cyberchondrię (czyli wykorzystywanie forów internetowych w poszukiwaniu informacji dotyczących chorób), samobójstwa w sieci i samookaleczenia [*Zagrożenia cyberprzestrzeni*… 2013]. Zdiagnozowanie IAD odbywa się najczęściej za pomocą krótkich testów, z których najpopularniejszym jest test dr Kimberley Young, który po udzieleniu odpowiedzi na 8 pytań zamkniętych pozwala ocenić stopień uzależnienia od internetu [Jakubik 2017][2].

Wymienione zagrożenia w sposób bezpośredni wpływają na zdrowie i życie jednostki. Najczęściej są efektem złego użytkowania zarówno sieci, jak i urządzeń multimedialnych. Sam charakter tych zagrożeń, które w większości są sklasyfikowane jako jednostki chorobowe, powoduje, iż w sposób istotny wpływają one na poziom bezpieczeństwa zdrowotnego obywateli. Rozwój tych chorób i przypadłości powoduje wzrost dysfunkcjonalności społeczeństwa w każdym wymiarze życia.

Kolejną grupą zagrożeń dla bezpieczeństwa zdrowotnego w sieci są działania mające świadomie lub nieświadomie spowodować szkodę lub w sposób nieuczciwy doprowadzić inicjatora, pomysłodawcę do zysku. Do takich zagrożeń na pierwszym miejscu można zaliczyć tworzenie i upowszechnianie informacji na formach internetowych dotyczących zdrowia. Większość użytkowników internetu przyznaje się do korzystania z tzw. diagnozy „Doktor Google", polegającej na wpisaniu występujących objawów i wyszukaniu ewentualnych możliwości leczenia. Coraz większa liczba lekarzy uskarża się również na pacjentów, którzy przychodzą już tylko po leki lub po gotową terapię, gdyż w internecie znaleźli odpowiedź na wszystkie pytania dotyczące swojego stanu zdrowia i doskonale wiedzą, co im jest. Tego typu działania stanowią poważne zagrożenie dla bezpieczeństwa jednostki, która jest w stanie uwierzyć w każdą informację o zdrowiu, objawach choroby wypisanych na forum lub stronie internetowej, a także zastosować proponowaną tam terapię, pomijając etap specjalistycznej konsultacji medycznej.

Jednym z najpoważniejszych zagrożeń w sieci, które po części są związane z użytkowaniem określonych stron czy for, jest handel lekami, wyrobami medycznymi w internecie. Użytkownicy sieci, również w Polsce, coraz częściej robią

[2] Kimberley Young wyróżniła pięć typów uzależnienia związanego z komputerem: erotomanię internetową (*cybersexual addiction*), uzależnienie od internetowych kontaktów społecznych (*cyber-relationship addiction*), uzależnienie od sieci internetowej (*net compulsions*), uzależnienie od komputera (*computer addiction*) i przeciążenie informacyjne, czyli przymus pobierania informacji (*information overload*) [por. Woronowicz 2001]. Na podstawie zaadoptowanych przez siebie dla celów pracy kryteriów diagnostycznych, wywodzących się z opisu patologicznego hazardu według DSM-IV (1994), utworzyła test składający się z 8 pytań, selekcjonujący badanych na dwie grupy: uzależnionych (396 osób) i normalnych użytkowników internetu (100 osób). Tak duża dysproporcja liczbowa wynikała z faktu, iż badani byli ochotnikami, którzy zgłosili się, gdyż sami uważali się już za uzależnionych. A. Jakubik, *Zespół uzależnienia od Internetu (ZUI) – Internet Addiction Syndrome (IAS)*, http://www.psychologia.edu.pl/czytelnia/50-artykuly/235-zespol-uzaleznienia-od-internetu-zui-em-internet-addiction-syndrome-ias-em.html [dostęp: 12.11.2017].

zakupy w aptekach internetowych lub kupują np. trudno dostępne medykamenty na aukcjach. Dla potencjalnego sprzedawcy w tym przypadku najważniejszy jest zysk, na drugim miejscu jakość czy też autentyczność produktu. Wśród specyfików, którymi w sposób nielegalny handluje się w internecie, prym wiodą preparaty odchudzające, steroidy i tabletki na potencję, ale też coraz częściej pojawiają się podróbki leków na nadciśnienie, HIV, raka czy depresję [Fedorowicz 2017]. Nawet 90% leków i suplementów diety sprzedawanych w sieci może być sfałszowanych, zawierać substancje, których zażycie grozi poważnymi konsekwencjami, takimi jak utrata zdrowia, a nawet życia.

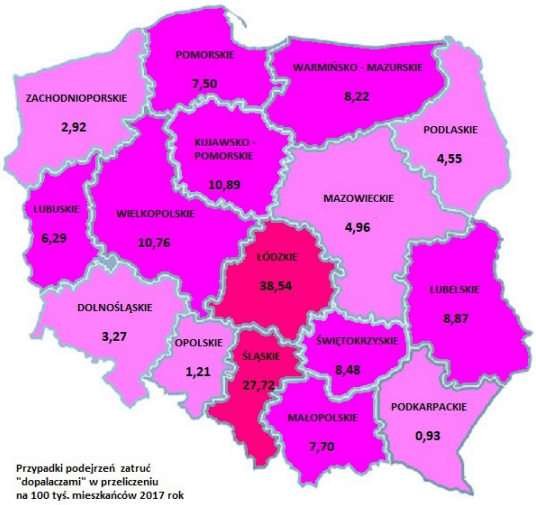
W Polsce było głośno o silnych zatruciach preparatami odchudzającymi, zawierającymi sibutraminę – specyfiki te, pod różnymi nazwami, są nadal dostępne w internecie, a możliwość ich kupna stanowi poważne zagrożenie dla życia i zdrowia. Zgodnie z prawem farmaceutycznym obowiązującym na terenie RP, handel lekami przez nieupoważnione osoby jest zabroniony i podlega karze[3]. Użytkujący internet coraz częściej jednak decydują się na zakupy wyrobów farmaceutycznych w sieci, nie licząc się z konsekwencjami. Z informacji Ministerstwa Zdrowia wynika, iż do szpitali rocznie trafia ok. 6,5 tys. osób zatrutych lekami psychotropowymi. Często też recepty na leki psychotropowe są fałszowane czy wyłudzane [*Odurzają się psychotropami…* 2017].

W sieci funkcjonują również fora internetowe, na których za pomocą specjalnie prowadzonej rozmowy można otrzymać informację, gdzie można kupić lek czy narkotyk sprzedawany w sposób legalny na receptę. Pozbawioną świadomości konsekwencji zagrożenia jest także działalność polegająca na odsprzedawaniu leków na receptę przez osoby prywatne, które chcą się pozbyć leków niewykorzystanych i w ten sposób liczą na zysk. Tego typu działalność również rozwija się w sieci, i w połączeniu z uzyskaną z for i portali zdrowotnych wiedzą może stanowić realne zagrożenie dla bezpieczeństwa zdrowotnego.

Charakter bezwzględnie kwalifikowany jako przestępstwo mają aktywności polegające na wprowadzeniu na rynek sprzedaży internetowej tzw. dopalaczy. Cechą charakterystyczną „dopalaczy" jest to, że substancje w nich zawarte nie znajdują się w wykazach substancji kontrolowanych prawem. W przypadku dopalaczy nie wiadomo, jakie substancje znajdują się w ich składzie, i w jakich ilościach – skład jest stale modyfikowany tak samo jak nazwy produktów. Dlatego osobom, które zażyły te substancje, może być trudno udzielić skutecznej pomocy medycznej. Jednocześnie „dopalacze" są produkowane w niesterylnych warunkach, często w związku z tym znajdują się w nich różne zanieczyszczenia, które dodatkowo oddziałują negatywnie na organizm i przyczyniają się do utraty

[3] Zgodnie z art. 124 ustawy Prawo farmaceutyczne, „kto wprowadza do obrotu lub przechowuje w celu wprowadzenia do obrotu produkt leczniczy, nie posiadając pozwolenia na dopuszczenie do obrotu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Ustawa z dnia 6 września 2001 r. Prawo farmaceutyczne, Dz.U. 2001 nr 126, poz. 1381.

zdrowia czy życia osób, które zażyły tych narkotyków. Skalę zjawiska obrazuje mapa zamieszczona poniżej przedstawiająca liczbę podejrzeń zatruć dopalaczami.



Rycina 1. Liczba podejrzeń zatruć dopalaczami z podziałem na województwa w przeliczeniu na 100 tys. mieszkańców. Średnia krajowa w całym 2017 r. wyniosła 11,00 przypadków na 100 tys.

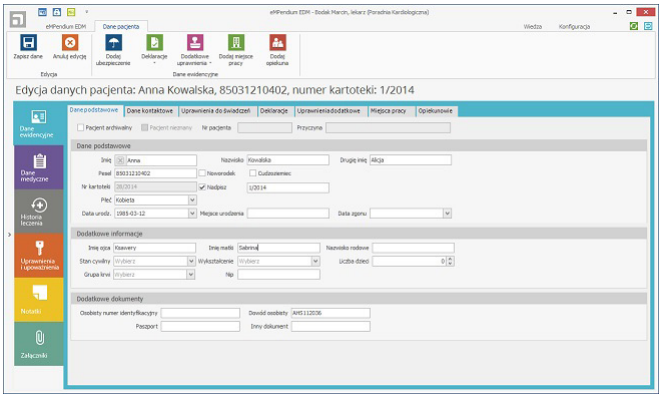
Źródło: Dane statystyczne: Wykaz środków zastępczych, nowych substancji psychoaktywnych i innych substancji, https://gis.gov.pl/bez-kategorii/dane-statystyczne/ [dostęp: 20.10.2017].

Internetowa sprzedaż leków, wyrobów medycznych, parafarmaceutyków czy wreszcie substancji psychoaktywnych jest jednym z największych zagrożeń dla bezpieczeństwa zdrowotnego. Głównym powodem wzrostu znaczenia tego zagrożenia jest w przypadku Polski na przykład społeczne niezadowolenie z funkcjonowania systemu ochrony zdrowia w państwie. Obywatel za pomocą internetowej diagnozy uzyskanej z portalu czy strony podejmuje działanie mające na celu zastąpienie wizyty u lekarza – kupuje więc leki, wdraża zalecane postępowanie. Takie aktywności finalnie najczęściej skutkują wizytą w szpitalu, coraz częściej jednak zbyt późną i niedającą gwarancji wyleczenia.

Zagrożeniem o charakterze przestępczym jest także możliwość kradzieży danych czułych z sieci. W związku z informatyzacją systemu ochrony zdrowia już od 1 stycznia 2018 roku wszystkie informacje dotyczące procesu leczniczego pacjentów są gromadzone na serwerach, za których ochronę i administrowanie są odpowiedzialne jednostki przechowujące te dane, czyli szpitale, przychodnie i gabinety. Zmiana ta będzie wywoływała poważne skutki dla podmiotów leczniczych, jak i samych pacjentów [*Elektroniczna dokumentacja medyczna*… 2017].

Głównymi korzyściami dla pacjentów, które mają wynikać z informatyzacji dokumentacji medycznej i systemu ochrony zdrowia, mają być między innymi: udostępnienie danych o zdarzeniach medycznych pacjentom w formie elektro-

nicznej, udostępnienie usługobiorcom elektronicznej historii chorób, wykonanych usług, skierowań, recept, zwolnień lekarskich, planów szczepień, zaleceń, umożliwienie elektronicznej realizacji recept, rejestracji online wizyty, zapewnienie szybkiego dostępu do elektronicznych danych medycznych w sytuacjach nagłych, umożliwienie elektronicznej obsługi zwolnień lekarskich [Ucyfrowienie.pl 2017]. W ramach ustawy o informacji w systemie ochrony zdrowia mają więc działać dwie platformy: Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych – P1, i Platforma udostępniania online przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych – P2. W praktyce w sieci będzie można zobaczyć, zweryfikować i zmodyfikować dane o pacjencie zapisane na przykładowej stronie przedstawionej na rycinie 2.



Rycina 2. Dane pacjenta.

Źródło: Dane pacjenta, https://www.mp.pl/empendium/pomoc/pomoc_edm.html?id=97679 [dostęp: 23.10.2017].

Obowiązek prowadzenia dokumentacji medycznej w formie elektronicznej stanowi część większego i docelowego projektu – informatyzacji polskiej służby zdrowia, a w szczególności jednego z jej kluczowych projektów – ogólnopolskiego systemu informacji w ochronie zdrowia. Na system ten ma się składać wiele mniejszych systemów teleinformatycznych, dzięki którym będzie możliwe przechowywanie i wymiana danych niezbędnych do świadczenia usług zdrowotnych. Dotyczy to tzw. e-recepty, e-zwolnienia, rejestru podmiotów leczniczych czy zbioru informacji o zdarzeniach medycznych i innych. W tej wymianie danych medycznych udział mają brać podmioty lecznicze, pacjenci, jak również organizatorzy systemu ochrony zdrowia w Polsce [Ucyfrowienie.pl 2017]. Informatyzacja szpitali ma przede wszystkim usprawnić działania tych placówek, poprawić dostępność i komunikację między podmiotami biorącymi udział w procesie leczenia. Problemem jest jednak samo wdrażania systemów informatycznych oraz ich zabezpieczenie. Placówki medyczne ociągają się z tymi procedurami w związku z brakiem funduszy. Wyzwaniem są również procedury i systemy zabezpieczające dokumentacje medyczne [Otwinowski 2014]. W przypadku szpitali borykających

się z zadłużeniami praktycznie niemożliwe jest zastosowanie najkorzystniejszego rozwiązania, jakim jest powierzenie zarządzania danymi specjalistycznej firmie zewnętrznej. To wszystko rodzi duże ryzyko powstania zagrożeń dla bezpieczeństwa zdrowotnego pacjentów w postaci wycieku danych czy ataków hakerskich polegających na przykład na nieuprawnionej modyfikacji informacji o procesie leczenia czy blokady dostępu do danych. Zadaniem podmiotów leczniczych jest więc zarządzanie danymi zgodnie z obowiązującymi normami prawa oraz właściwie prowadzoną polityką ochrony danych osobowych.

Rozwój informatyzacji i nowych technologii w medycynie najlepiej uwidacznia się także w sukcesach, jakie odnoszą rozwiązania stosowane w ramach telemedycyny[4]. Zastosowanie najnowszych technologii w procesach leczniczych stanowi również pole do popisu dla działań o charakterze przestępczym, hakerskich. Można uznać, że wzrost i rozwój takich inicjatyw w obecnej rzeczywistości jest równorzędny. Hakerzy coraz częściej atakują wymagające i dobrze zabezpieczone systemy, nie licząc się z możliwością wystąpienia tragicznych skutków dla życia i zdrowia obywateli. Myślenie o ataku hakerskim w trakcie precyzyjnej operacji przeprowadzanej na podstawie możliwości telemedycyny jest na razie tylko fikcją, ale nie jest niemożliwe. Potwierdzają to zdarzenia między innymi z Wielkiej Brytanii, gdzie w maju 2017 roku doszło do ataku hakerskiego, w wyniku którego zablokowano komputery w 25 szpitalach. W komunikatach przekazanych lekarzom można było przeczytać, że komputery zostaną odblokowane po zapłaceniu okupu w elektronicznej walucie bitcoin. Najpoważniejszym skutkiem ataku mającym bezpośredni wpływ na poziom bezpieczeństwa zdrowotnego było odwołanie zabiegów, które nie wymagały ratowania życia. W szpitalach dotkniętych atakiem hakerów osoby potrzebujące pilnej pomocy medycznej zostały przewiezione do innych placówek [*Potężny atak hakerski*… 2017]. Innym przykładem ukazującym skalę zagrożenia jest raport z maja 2017 roku ekspertów amerykańskiej firmy WhiteScope dotyczący rozruszników serca. Autorzy podkreślają, że również na tego typu urządzenia medyczne istnieje ryzyko ataku hakerskiego. Problemem są nie tyle same rozruszniki, co cały ich „ekosystem", np. oprogramowanie, monitory, programatory. Ustalono między innymi, że w 4 programatorach od 4 różnych dostawców było aż 8 tysięcy znanych luk wynikających ze stosowania przesta-

[4] Telemedycyna (medycyna na odległość) – forma świadczenia usług medycznych i opieki zdrowotnej łącząca w sobie elementy telekomunikacji, informatyki oraz medycyny. Dzięki wykorzystaniu nowych technologii pozwala ona przełamywać geograficzne bariery, pozwalając na wymianę specjalistycznych informacji, przesyłając obrazy statyczne oraz dynamiczne (przesyłanie najwyższej jakości zdjęć EKG, USG, MRI). Pozwala przeprowadzić diagnozę na odległość. Duże zastosowanie telemedycyna znajduje w środowisku chirurgicznym, które wykorzystuje ją do prowadzenia operacji „na odległość". Nowoczesna technologia, korzystająca z szybkich procesorów i algorytmów do cyfrowego przetwarzania i kompresji sygnałów, umożliwia przesyłanie obrazów o wysokiej rozdzielczości, a także interaktywną transmisję audiowizualną z wyjątkową dokładnością i w czasie rzeczywistym. Systemy wideokomunikacyjne (wideokodery) pracują na ogólnodostępnych cyfrowych liniach transmisyjnych ISDN, w ogólnoświatowej sieci internet, a także na liniach satelitarnych.

rzałych bibliotek w oprogramowaniu. Rozruszniki dostępne na rynku są wyposażone w interfejsy bezprzewodowej komunikacji, jest to rozwiązanie przyjęte w celu wygody pacjentów, jednak obarczone wieloma wadami. Rozrusznik może nawiązywać połączenie z większością domowych monitorów, a także programatorami i to właśnie one mogą stanowić narzędzie ataku w nieodpowiednich rękach. Urządzenie służy do programowania rozrusznika w gabinecie lekarskim, ale programatory można kupić również w internecie. Firmy produkujące urządzenia nie mają w planach prowadzania dodatkowych zabezpieczeń, dopóki nie otrzymają potwierdzonych informacji o celowych atakach, tymczasem jeśli hakerom udałoby się uzyskać zdalny dostęp do rozrusznika, byliby w stanie zmienić ustawienia zaprogramowanej terapii i nawet doprowadzić do śmierci posiadacza urządzenia [*USA: eksperci przestrzegają*… 2018].

Sieć, internet, korzystanie z urządzeń multimedialnych niosą ze sobą wiele korzyści ułatwiających komunikację, pozyskiwanie informacji, wdrażanie nowych rozwiązań. W przypadku bezpieczeństwa zdrowotnego skutkuje również wieloma zagrożeniami, których występowanie wynika w dużej mierze z poziomu świadomości i wiedzy samych użytkowników, a także szczelności systemu i skutecznych rozwiązań prawnych na poziomie państwa.

SKUTECZNE METODY ZAPOBIEGANIA ZAGROŻENIOM DLA BEZPIECZEŃSTWA ZDROWOTNEGO W SIECI

Analizując zagrożenia dla bezpieczeństwa zdrowotnego w sieci związane z występowaniem jednostek chorobowych, należy zwrócić uwagę na tzw. dobre praktyki, które powinny być uznawane za priorytetowe przez każdego użytkownika internetu i urządzeń multimedialnych. W przypadku wszelkiego rodzaju schorzeń opisanych wcześniej, takich jak CVS, RSI czy MSD, właściwych dla potencjalnych użytkowników, dobre praktyki polegają przede wszystkim na spełnieniu i zastosowaniu wymogów technicznych. W miejscu pracy czy stanowisku służącym do korzystania z internetu należy więc stosować konkretne wytyczne, takie jak: odpowiednie monitory i odpowiednie ich ustawienie, właściwe krzesła/fotele i biurka, stosowanie przerw w pracy i odpowiednich ćwiczeń, właściwego oświetlenia, a przede wszystkim przestrzeganie czasu pracy przed komputerem. Kilka państw członkowskich Unii Europejskiej sformułowało specyficzną politykę i programy zmierzające do zapobiegania urazom wynikającym z chronicznego przeciążenia organizmu. Inicjatywy te przyjmują różne formy. Są to m.in.: działania prewencyjne skierowane do specyficznych sektorów gospodarki, poprawa systemów sprawozdawczości, finansowanie badań lub specyficznych studiów naukowych, wydawanie materiałów informacyjnych, wytycznych itd., protokoły monitorowania zdrowia, ustalanie planów działania i celów zmierzających do ograniczenia przypadków występowania chorób RSI [*Urazy wynikające z chronicznego*… 2017]. W przypadku IAD, nieuznanego za jednostkę chorobową, nie ma jeszcze wytycznych do

procesu leczenia tego schorzenia. Stworzono jednak listę możliwych rozwiązań, do których zaliczono: alternatywne metody spędzania wolnego czasu, np. poprzez zwiększenie aktywności fizycznej, stosowanie specjalnych oprogramowań, które automatycznie skracają czas użytkowania komputera, terapie psychologiczne oraz terapie behawioralne [*Uzależniony od komputera*… 2017]. Znacznie trudniejsze wydaje się wdrażanie procedur czy praktyk ograniczających możliwość wystąpienia zagrożeń dla bezpieczeństwa zdrowotnego w sieci, które mają znamiona przestępstw lub po prostu nimi są. W przypadku korzystania z for, portali internetowych służących stawianiu diagnoz lub zlecających leczenie rozsądnym rozwiązaniem na poziomie państwa wydałoby się stworzenie akredytacji ministerialnej (dodanie gov do adresu), a tym samym wprowadzenie kontroli nad takimi stronami, które potwierdzałaby wiarygodność informacji na nich zawartych. Szukając rozwiązań eliminujących zagrożenia dla bezpieczeństwa zdrowotnego spowodowane nielegalnym handlem lekami, należy podkreślić funkcjonowanie regulacji prawnych, których podmiot sprzedający musi przestrzegać. Apteka prowadząca sprzedaż wysyłkową musi działać przede wszystkim na podłożu apteki stacjonarnej. Jeśli prowadzi sprzedaż wyłącznie przez internet, wówczas powinna wzbudzić podejrzenie potencjalnego klienta. Każda apteka internetowa na swojej stronie WWW winna umieścić dane właściwego Wojewódzkiego Inspektoratu Farmaceutycznego (w tym: nazwę organu, adres fizyczny, adres e-mail, numer telefonu lub faksu). Apteka zobligowana jest także do posiadania zezwolenie na prowadzenie działalności i informowania o tym na swojej stronie. Na witrynie legalnej e-apteki musi się znaleźć odesłanie do Krajowego Rejestru zezwoleń na prowadzenie aptek ogólnodostępnych, punktów aptecznych oraz Rejestru Udzielonych Zgód na Prowadzenie Aptek Szpitalnych i Zakładowych. Zgodnie z najnowszymi przepisami, które weszły w życie z dniem 3 maja 2015 roku, apteka internetowa powinna zamieścić na swojej stronie wspólny logotyp Unii Europejskiej podlinkowany do rekordu w wykazie aptek w Centrum Systemów Informacyjnych Ochrony Zdrowia (CSIOZ), gdzie znajdują się informacje o prowadzonej aptece i jej zgłoszeniu do WIF [*Legalna Apteka internetowa*… 2017].

Rycina 3. Wspólny logotyp UE.

Źródło: http://www.eapteki.info/legalna-apteka-internetowa-jak-ja-rozpoznac-poradnik-dla-kupujacych-infografika/ [dostęp: 23.10.2017].

Na stronie apteki internetowej powinno się również znaleźć odesłanie do Biuletynu Informacji Publicznej GIF, gdzie znajdują się informacje o przepisach regulujących sprzedaż wysyłkową w Polsce, o wspólnym logotypie oraz o ryzyku związanym z zakupem produktów leczniczych w internecie. Legalna apteka musi zapewnić pacjentowi telefoniczny dyżur farmaceuty w godzinach pracy apteki oraz 2 godziny po przewidywanym terminie dostawy przesyłki, czyli w praktyce w godzinach 9.00–19.00. Apteka internetowa nie sprzedaje swoich produktów przez ogłoszenia na forach internetowych lub w serwisach ogłoszeniowych oraz zakazana jest sprzedaż przez internet leków na potencję (np. viagra, cialis, maxigra, levitra, kamagra), preparatów na odchudzanie (np. zelixa, adipex, meridia) oraz steroidów anabolicznych [*Legalna apteka internetowa*… 2017].

Zabezpieczenie systemu informacji medycznej, a tym samym czułych danych dotyczących pacjentów jest kwestią zastosowania skutecznych rozwiązań informatycznych, odpowiednich programów antywirusowych, zapór czy procedur związanych z weryfikacją dostępu, które w najwyższym stopniu zabezpieczałyby dane i weryfikowały ewentualne możliwości modyfikacji danych. Konieczne jest również stałe analizowanie zagrożeń i ciągłe wdrażanie nowych rozwiązań zabezpieczających na poziomie firm, które są wytwórcami zarówno urządzeń, jak i oprogramowania dla systemu ochrony zdrowia. Przepisy prawa, takie jak ustawa o ochronie danych osobowych, wchodzące w życie regulacje dyrektywy RODO, powoływanie Zespołów Reagowania na Incydenty Komputerowe czy doktryna cyberbezpieczeństwa RP [Żuk, Żuk 2016] doskonale wpisują się w mechanizm konieczny do realizacji na poziomie państwa i instytucji specjalistycznych, takich jak np. szpitale, w celu zabezpieczenia danych osobowych pacjentów [Jędrzejczyk-Kuliniak 2015]. Pozostaje mieć nadzieję ze rozwój systemów zabezpieczających procedury wykonywane za pomocą sieci będzie nadążał za pomysłowością i ambicjami hakerów i innych podmiotów dążących do wyrządzenia szkody za pomocą i przy użyciu danych czy technologii stosowanych w procesie leczenia.

KONKLUZJE

Rozwój usług internetowych i najnowszych technologii całkowicie i dogłębnie przearanżował mechanizm pracy i funkcjonowania jednostek w każdym obszarze ich życia. Zmienił się sposób pracy, przekazywania informacji, realizowania transakcji, kontaktów społecznych. Usieciowienie życia przyniosło wiele ułatwień i pożytecznych innowacji, jak również dostarczyło nowych zagrożeń i niebezpieczeństw. Tymi mało analizowanymi są zagrożenia dla bezpieczeństwa zdrowotnego. Większość zagrożeń wynika z bezrefleksyjnego i mało rozsądnego użytkowania internetu. Ci, którzy życie zawodowe i prywatne nierozerwalnie łączą z nowymi technologiami, a tym samym z siecią, często zapominają o własnym bezpieczeństwie i zdrowiu. Łatwość i prostota dostępu do wszystkiego

i wszędzie stwarza realne zagrożenie dla prawidłowego funkcjonowania jednostki. Konieczność stałego bycia online wymusza formę życia z i przy komputerze, co bardzo często skutkuje rozwojem jednostek chorobowych wymienionych powyżej, powoduje też nieodwracalne zmiany w sposobie życia i funkcjonowania społecznego, które wykluczają kontakty interpersonalne czy rodzinne. Możliwość sprawdzenia wszystkiego pozwala na osiągnięcie dostępu do wiedzy często niesprawdzonej, niepotwierdzonej, obfitującej w przekłamania czy uogólnionej, co w przypadku poszukiwania diagnozy możne skutkować źle wyciągniętymi wnioskami, złym procesem leczniczym lub jego brakiem na poziomie specjalistycznym. Sieć to również obszar funkcjonowania i aktywności tych podmiotów, które działają często bezprawnie, z nastawieniem na własną korzyść. Działania takich jednostek skutkują najczęściej sytuacją zagrażającą życiu i zdrowiu tych, którzy, mówiąc wprost, dali się nabrać. Internet to również pole dla tych, których umiejętności mogą zagrozić najlepszym systemom zabezpieczającym i którzy dla rozrywki i żartu potwierdzenia swoich ambicji będą robić wszystko, aby złamać zapory, szyfry, pozyskać chronione informacje, zablokować system czy nawet przerwać operację. Skuteczną metodą przeciwdziałania zagrożeniom dla bezpieczeństwa zdrowotnego w sieci jest przede wszystkim rozsądek i stosowanie zasady ograniczonego zaufania wobec tego, co czytamy, kupujemy i sprawdzamy sieci, a także w jaki sposób z niej korzystamy i w jakim wymiarze. Metodą może być również niezaspokojona ciekawość, która powinna być ukierunkowana na ciągłe sprawdzanie i weryfikację tego, co możemy w sieci uzyskać.

Title: Threats to Health Security in the Internet

Summary: The aim of the article is to present threats in the health security system which originate from the use of the Internet. The development of the new technologies as well as the widespread availability of mobile devices and information makes these types of threats an important issue which receives a lot of coverage in the current social reality. The constantly increasing number of Internet users also generates a change in the model of the unit's operation in both the professional and private areas. Being off line is virtually impossible. We spend time searching, talking or dealing with most things in the Internet, and consequently we spend more time in front of computers. This creates conditions for the development of threats that directly affect our health and safety. Internet users may become victims of criminal activity as a result of ill-advised use of the computer and the Internet. The number, type and power of threats to health security, in the same way as cyberspace, is virtually unlimited and is not subject to full control.

Keywords: cyberspace, threats, health, health security

BIBLIOGRAFIA

1. Bartosik P. (2014), *Bezpieczeństwo w globalnej wiosce – zagrożenia czyhające na dzieci i seniorów w Intrenecie*, [w:] *Nowe zagrożenia bezpieczeństwa*, K. Hennlga (red.), Sieradz.
2. Bógdał-Brzezińska A., Gawrycki M. (2013). *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa.
3. *Choroby układu mięśniowo-szkieletowego w sektorze Horeca*, (2013), Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy, http://osha.europaeu/pl/publications/e-facts/efact24 [dostęp: 25.10.2017].
4. *Coraz więcej ludzi korzysta z sieci. Już blisko 4 miliardy osób ma dostęp do Internetu*, (2017), https://publicrelations.pl/coraz-wiecej-ludzi-korzysta-z-sieci-juz-blisko-4-miliardy-osob-ma-dostep-do-internetu/ [dostęp: 23.10.2017].
5. *Dane pacjenta*, (2017), https://www.mp.pl/empendium/pomoc/pomoc_edm.html?id=97679 [dostęp: 30.10.2017].
6. *Elektroniczna dokumentacja medyczna w ramach systemu informacji medycznej*, 2017, https://www.zdrowie.abc.com.pl/narzedzia-i-materialy/komentarze-praktyczne/elektroniczna-dokumentacja-medyczna-w-ramach-systemu-informacji-medycznej,107810.html [dostęp: 02.10.2017].
7. Fedorowicz M. (2017), *W Internecie kwitnie handel nielegalnymi lekami*, http://www.nto.pl/wiadomosci/opolskie/art/4590319,w-internecie-kwitnie-handel-nielegalnymi-lekami,id,t.html [dostęp: 25.10.2017].
8. Grzybowski A., Szajkowska M. (2017), *Epidemiologia i leczenie krótkowzroczności na świecie*, „Ophtha Therapy", vol. 4, nr 3 (15), s. 129–135, file:///C:/Users/user/Downloads/1.OPT_3-2017_Epidemiologia%20i%20leczenie%20krótkowzroczno%20ci.pdf [dostęp: 01.10.2018].
9. *Holizm i zdrowie. Współczesna definicja zdrowia WHO*, (2017), http://www.seremet.org/who_zdrowie.html [dostęp: 24.10.2017].
10. Jędrzejczyk-Kuliniak K. (2015), *Globalne wyzwania i zagrożenia bezpieczeństwa międzynarodowego w XXI wieku*, Poznań.
11. *Legalna apteka internetowa – jak ją rozpoznać? Poradnik dla kupujących + infografika*, (2017), http://www.eapteki.info/legalna-apteka-internetowa-jak-ja-rozpoznac-poradnik-dla-kupujacych-infografika/ [dostęp: 30.10.2017].
12. Majchrzak Ł. (2018), *Mobile i digital w 2018 roku w Polsce i na świecie*, https://mobirank.pl/2018/02/02/mobile-i-digital-w-2018-roku-w-polsce-i-na-swiecie/ [dostęp: 23.10. 2018].
13. *Narkotyki A–Z*, http://dopalaczeinfo.pl/strony/co_to_sa_dopalacze#nowe-narkotyki [dostęp: 26.10.2017].
14. Nowacki G. (2015). *Zagrożenia informacyjne oraz sposoby ich zwalczania*, [w:] B. Jagusiak, *Zagrożenia bezpieczeństwa państwa – geneza i charakter uwarunkowań*, Warszawa.
15. *Odurzają się psychotropami. Kwitnie nielegalny handel lekami. Coraz więcej ofiar*, (2017), https://www.fakt.pl/wydarzenia/polska/niebezpieczny-handel-lekami-w-internecie-sluza-do-odurzania/e7hytp6 [dostęp: 26.10.2017].
16. Otwinowski W. (2014). *Wybrane zagrożenia bezpieczeństwa państwa i człowieka*, Poznań.
17. *Potężny atak hakerski w Anglii i Szkocji. Zaatakowane zostały komputery wielu szpitali*, (2017), Polish express.uk, https://www.polishexpress.co.uk/potezny-atak-hakerski-w-anglii-i-szkocji-zaatakowane-zostaly-komputery-wielu-szpitali [dostęp: 01.10.2018].
18. Szubrycht T. (2005). *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1.

19. Tadeusiewicz R., *Zagrożenia w cyberprzestrzeni*, http://www.pan.poznan.pl/nauki/N_410_05_Tadeusiewicz.pdf 2016 [dostęp: 25.10.2017].
20. *The Health and Safety Executive*, (2013), http://www.hse.gov.uk/statistic/tables/thorgp02.htm, [dostęp: 25.10.2017].
21. Ucyfrowienie.pl, (2017), http://ucyfrowienie.pl/informatyzacja/ [dostęp: 23.10.2017].
22. *Urazy wynikające z chronicznego przeciążenia organizmu (RSI) w państwach Unii Europejskiej*, file:///C:/Users/user/Downloads/Factsheet_6_-_Urazy_wynikajace_z_chronicznego_przeciazenia_organizmu_-RSI-_ [dostęp: 30.10.2017].
23. Ustawa z dnia 6 września 2001 r. *Prawo farmaceutyczne*, Dz.U. 2001 nr 126, poz. 1381.
24. *USA: eksperci przestrzegają przed ryzykiem ataku hakerskiego na rozruszniki serca*, http://www.rynekzdrowia.pl/Po-godzinach/USA-eksperci-przestrzegaja-przed-ryzykiem-ataku-hakerskiego-na-rozruszniki-serca,188978,10.html [dostęp: 01.10.2018].
25. *Uzależnienie od Internetu*, (2018), http://www.uzaleznieniabehawioralne.pl/siecioholizm/uzalaznienie-od-internetu/ [dostęp: 26.10.2018].
26. *Uzależniony od komputera. Dowiedz się jak walczyć z nałogiem*, (2017), https://www.chip.pl/2013/11/uzalezniony-od-komputera-poznaj-sposoby-obrony-przed-nalogiem/ [dostęp: 30.10.2017].
27. *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, (2013), https://cyberprzestrzen.wspkorczak.eu/download/dokumenty/podrecznik_zagrozenia_cyberprzestrzeni.pdf [dostęp: 24.10.2017].
28. Żuk J., Żuk M. (2016), *Zagrożenia w cyberprzestrzeni a bezpieczeństwo jednostki*, „Rozprawy Społeczne", t. 10, nr 3.