A C T A U N I V E R S I T A T I S N I C O L A I C O P E R N I C I
DOI: http://dx.doi.org/10.12775/AUNC_ZARZ.2018.035 ZARZĄDZANIE XLV–NR 3 (2018)

Pierwsza wersja złożona 19.05.2018
Ostatnia wersja zaakceptowana 25.06.2018

ISSN (print) 1689-8966
ISSN (online) 2450-7040

*Edyta Świnarska**

WSPÓŁCZESNE ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACYJNYM W ASPEKCIE ZAGROŻEŃ EKOLOGICZNYCH

Z a r y s t r e ś c i: Rozwój elektroniki, Internetu, wykorzystywanie sieci publicznych do przesyłania informacji dla systemów przemysłowych, powoduje, iż informacja staje się kluczowym czynnikiem wyznaczającym wiedzę, władzę, ale i decydującym o bezpieczeństwie obywateli, organizacji, całych państw. Umiejscowienie zagrożenia, w tym zagrożenia informacyjnego, w sferze świadomości społeczeństwa skłania do postawienia pytań o stopień odbierania pewnych zjawisk i o określenie, czy wszystkie zjawiska zagrażające bezpieczeństwu informacyjnemu istotnie są zagrożeniem, czy może jedynie chaosem informacyjnym.
Poniższy artykuł ma na celu scharakteryzowanie zagrożeń bezpieczeństwa informacyjnego występujących we współczesnym świecie w aspekcie bezpieczeństwa ekologicznego i działań z zakresu zarządzania bezpieczeństwem informacyjnym zmierzających do ich minimalizacji.

S ł o w a k l u c z o w e: bezpieczeństwo, informacje, zarządzanie bezpieczeństwem informacyjnym, zagrożenia ekologiczne.

Klasyfikacja YEL: Q57, L86

WSTĘP

Szybkie tempo życia i globalizacja powodują, że człowiekowi obecnie świat może kojarzyć się z chaosem, niepewnością bytu, ogromną ilością informacji, których część przestała być dla niego zrozumiała. Każdy dorosły obserwuje i analizuje otaczający go świat, ale szybki postęp w nauce i odkrywanie nowych zagrożeń ekologicznych, które kilka lat temu nie były realne powoduje, że w każdym społeczeństwie rośnie potrzeba posiadania dostępu do informacji, która nie tylko zapewnia właściwą orientację w świecie, ale przede wszystkim poszerza wiedzę człowieka i przyczynia się do rozwoju jego życia umysłowego.

* Adres do korespondencji: Wydział Humanistyczny, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Żytnia 39, 08-110 Siedlce, e-mail: edyta.swinarska@uph.edu.pl;

Potrzeba prowadzenia edukacji ekologicznej oraz jawności informacji o zagrożeniach środowiskowych wynika stąd, iż większość społeczeństwa nie ma pełnej świadomości, na czym polega chociażby ochrona środowiska, nie zna obowiązującego prawa, a także nie jest odpowiednio przygotowywana na mogące wystąpić w każdej chwili sytuacje kryzysowe.

Jednak różnica pomiędzy potrzebą nabywania nowych informacji a chaosem informacyjnym jest tak diametralna, że ich nieumiejętnie ukierunkowanie może doprowadzić do paniki społeczeństwa, a w rezultacie do tragedii. Dlatego tak istotną rolę odgrywa tu kontrola przepływu informacji oraz umiejętność zarządzania bezpieczeństwem informacyjnym.

1. BEZPIECZEŃSTWO INFORMACYJNE W UJĘCIU LITERATURY PRZEDMIOTU

Współczesne technologie informacyjno–komunikacyjne obejmują szeroką gamę technologii, tj.: technologie informacyjne, technologie komunikacyjne, nadawcze środki przekazu, przetwarzanie oraz transmisję dźwięku i obrazu, systemy zarządzania treścią, a także kontrolę sieciową, jednak obecnie to portale społecznościowe generują społeczność internetową, która tworzy wirtualne grupy oparte na wymianie informacji [Liczmańska–Kopcewicz, 2017, s. 317–318]. Konsekwencje zmian zachodzących pod wpływem technologii informatycznych są coraz bardziej zauważalne a Internet stał się podstawowym narzędziem wdrażania koncepcji zarządzania [Wiśniewska, Liczmańska, 2010, s. 132].

Bezpieczeństwo informacyjne, w opinii K. Lidermana, jak dotąd nie doczekało się jednoznacznej wykładni i wraz z towarzyszącym mu terminem „bezpieczeństwo informacji" jest używane w różnych znaczeniach [Liderman, 2012, s. 13], obejmując wszystkie formy, także werbalne, wymiany, przechowywania oraz przetwarzania informacji [Liderman, 2012, s. 22]. K. Liderman [2012, s. 22] bezpieczeństwo informacyjne określa jako uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej i wykorzystywanej informacji, pojęcie bezpieczeństwa informacyjnego dotyczy zatem podmiotu (człowieka, organizacji), który może być zagrożony utratą zasobów informacyjnych albo otrzymaniem informacji o nieodpowiedniej jakości.

S. Kowalkowski, bezpieczeństwem informacyjnym określa zakres bezpieczeństwa przyjmujący wzrost znaczenia informacji w zachowaniu stabilności współczesnych międzynarodowych systemów ekonomicznych oraz uwzględniający zabezpieczenie przed atakami sieciowymi, a także skutkami ataków fizycznych i plasuje obok bezpieczeństwa politycznego, militarnego, ekonomicznego, społecznego, kulturowego i ekologicznego [Kowalkowski (red.), 2011, s. 13–15].

Treści podkreślające wagę tej problematyki można odnaleźć m.in. w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej oraz w dokumencie: Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 [Liderman, 2012, s. 24]. Należy podkreślić również, iż tematyka bezpieczeństwa informacyjnego jest regulowana przez polski system prawny, w tym Konstytucję RP. Także dokument pod nazwą Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej dotyka obszarów bezpieczeństwa informacyjnego, wskazując, iż w dobie rosnącego znaczenia bezpieczeństwa informacyjnego, w tym wzrostu znaczenia procesów gromadzenia, przetwarzania i dystrybuowania informacji w certyfikowanych systemach teleinformatycznych, rośnie (…) rola bezpieczeństwa informacyjnego w aspekcie cybernetycznym. Szczególną dziedziną bezpieczeństwa informacyjnego jest ochrona informacji niejawnych, a zatem takich, których nieuprawnione ujawnienie powoduje lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne**.**

Poufnością informacji z kolei, nazywamy zdolność do dzielenia się informacją wyłącznie z tymi instytucjami lub grupami osób, którym jest to niezbędne oraz do odmowy dostępu do informacji tym osobom, które nie są do tego powołane. Natomiast dokładność przekłada się na wiarygodność informacji, tzn. mówi o tym, że informacja pochodzi z wiarygodnego i sprawdzonego źródła i wiąże się z jej integralnością, czyli pewnością, że z upływem czasu nie została ona zniekształcona bądź nie straciła swojej pierwotnej wartości wskutek modyfikacji [Bekosty, 2017, s. 163–164].

Najistotniejszy jednak w tym wszystkim jest fakt, iż pierwszym krokiem zmierzającym do ochrony informacji jest zrozumienie, dlaczego zapewnienie jej bezpieczeństwa jest tak ważne.

2. ISTOTA SYTUACJI KRYZYSOWYCH

Sytuacje kryzysowe są nieuniknione, co oznacza, że prędzej czy później każdy z nas może się w takiej sytuacji znaleźć. Brak stosownej wiedzy i doświadczenia skutkuje tym, że w przypadku zagrożenia traci się rozsądek i możliwości racjonalnego zachowania w konkretnej sytuacji. Dlatego bardzo istotne jest poznanie charakteru zagrożenia, sposobów jego powstawania i opracowania działań zapobiegających zdarzeniu lub zmniejszających jego skutki. Sytuacjom kryzysowym wszelkiego rodzaju towarzyszą:

- emocje,
- lęk,
- trema,
- panika,

a wszystko to sprowadza się do konkretnego *zachowania ludzi* w danej sytuacji zagrożenia.

Przyczyn lęków i zagrożeń jest wiele. Można je ująć w grupy np.:

- lęki katastroficzne, związane z powodziami, trzęsieniami ziemi, suszą, ostrą i długą zimą;
- lęki ekologiczne, związane z degradacją środowiska;
- lęki militarne, związane z nagromadzeniem w różnych państwach arsenałem zbrojeniowym;
- lęki wojenne, związane z walkami zbrojnymi i obawą przed ich rozprzestrzenieniem na cały świat;
- leki ekonomiczne, związane z koncentracją dużych majątków i obawa przed ich utratą;
- lęki społeczne, związane z rozszerzaniem się narkomanii, alkoholizmu, chorób;

Panika wybucha niekiedy w sytuacji braku zagrożenia, może ją spowodować złudzenie pojawienia się zagrożenia, samo hasło np.: „pożar" może wywołać panikę.

W literaturze często spotyka się informację, że napad paniki trwa 30–60 minut. Może jednak trwać znacznie dłużej gdy słabnie i nasila się. Panika, napad lęku występuje jeden raz u około 9% osób w całej populacji.

Emocje nie idą w parze z rozumem. Są przeciwstawne. Emocje zaburzają logiczne i racjonalne myślenie. Emocje często prowadzą do zachowania i myślenia nie zawsze optymalnego którego człowiek później żałuje. Mogą być szkodliwe dla danego człowieka i dla innych ludzi którzy także żyją wspólnymi emocjami w danej chwili.

Ludzie w panice przeciskają się przez zbyt wąskie przejścia, trema zaburza wykonanie czynności, nerwowość zmniejsza precyzję ruchu, a wściekłość prowadzi do dziecinnego zachowania i burzy harmonię społeczną.

Na zachowanie tłumu nie ma wpływu wykształcenie, czy stopień rozwoju umysłowego, ale zdecydowanie duży wpływ na zachowania ludzi ma grupa, które wpływają na siebie wzajemnie, doprowadzając nawet do sytuacji tragicznych w skutkach.

3. ŹRÓDŁA ZAGROŻEŃ INFORMACYJNYCH

Człowiekowi od samego początku towarzyszyły różne rodzaje zagrożeń. W miarę rozwoju cywilizacji i postępu technicznego zmienił się jednak ich charakter i skala. Można powiedzieć, iż zagrożenia naturalne nie zmieniły swojego charakteru, a trzęsienia ziemi, huragany, powodzie, wybuchy wulkanów, pożary towarzyszyły człowiekowi od zawsze i miały ten sam charakter. Zupełnie inaczej jest jednak w przypadku zagrożeń technicznych, które już niejed-

nokrotnie zmieniały swój charakter i zasięg w miarę rozwoju techniki, zagospodarowywania terenów, wykorzystywania coraz to nowych rozwiązań technologicznych.

W opinii P. Bączka zagrożenie bezpieczeństwa informacyjnego może mieć swe źródło w działalności człowieka lub organizacji i wyrażać się jako:

- nieuprawnione ujawnienie informacji tzw. wyciek lub przeciek;
- naruszenie przez władze praw obywatelskich;
- asymetria w międzynarodowej wymianie informacji;
- działalność grup świadomie manipulujących przekazem informacji;
- niekontrolowany rozwój nowoczesnych technologii bioinformatycznych;
- przestępstwa komputerowe;
- cyberterroryzm;
- walka informacyjna[1];
- zagrożenia asymetryczne;
- szpiegostwo[2].

Według A. Żebrowskiego, za grożenie bezpieczeństwa informacyjnego może wystąpić jako skutek działania człowieka, który może wykorzystywać różnorakie techniki włamań do systemów informacyjnych, będących cennym źródłem informacji stanowiących tajemnicę państwową lub służbową, a przykłady takich technik to:

- zmowa kilku sprawców;
- celowe inicjowaniu awarii;
- wywoływanie fałszywych alarmów (uśpienie czujności);
- przeszukiwanie śmietników położonych w pobliżu firmy (pozyskanie pozornie nieważnych informacji);
- szantaż, korupcja;
- rozsyłanie do firm ankiet, zapytań, propozycji;
- rozkodowywanie hasła dostępu;
- atak słownikowy;
- podsłuch sieciowy;
- wirusy, robaki, konie trojańskie, oraz inne groźne aplikacje destabilizujące sprawność sytemu;
- wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego;
- techniki obchodzenia zabezpieczeń np. programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym;

[1] J. Janczak, Zakłócenia informacyjne, AON, Warszawa 2001, s. 11.

[2] P. Bączek, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2006, s. 86-87.

- krypto analiza zaszyfrowanych informacji;
- przechwytywanie otwartych połączeń sieciowych.[3]

Mając świadomość tego, jak wiele istnieje zagrożeń bezpieczeństwa informacji, należy wyselekcjonować najistotniejsze potencjalne obszary ich występowania. Trzeba opracować i wdrożyć procedury mające na celu ochronę tych obszarów, wprowadzić procedury ograniczające (uprawniony) dostęp, przeprowadzić szkolenia oraz kontrolować.

Schemat 1. Zagrożenia informacyjne

Źródło: Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30.

Bez wątpienia, za najbardziej wrażliwe na zagrożenia nieuprawnionym ujawnieniem informacji (wyciek lub przeciek) uznaje się obszary działalności takie, jak: planowanie polityczne, zarządzanie w skali makroekonomicznej, polityka obronna, wywiad i kontrwywiad wojskowy[4].

Obecnie największe niebezpieczeństwo stanowią jednak prawie nieograniczone możliwości manipulowania informacjami, prowadzące do chaosu informacyjnego.

[3] A. Żebrowski, W. Kwiatkowski, Bezpieczeństwo informacji III Rzeczypospolitej, Oficyna Wydawnicza ABRYS, Kraków 2000, s. 73.

[4] A. Żebrowski, W. Kwiatkowski, Bezpieczeństwo informacji III Rzeczypospolitej, Oficyna Wydawnicza ABRYS, Kraków 2000, s 78.

Dlatego w przypadku sytuacji kryzysowych dotyczących m.in bezpieczeństwa ekologicznego, a co za tym idzie, bezpieczeństwa publicznego, warto zastanowić się nad istotą braku informacji oraz chaosu informacyjnego i odpowiedzieć na kilka podstawowych pytań:

1. Czy zachowania osób, które zdają sobie sprawę z powagi sytuacji i pomimo to wolą milczeć, zamiast przekazywać tą wiedzę dalej i budować świadomość społeczną, są istotnym elementem braku świadomości ogółu społeczeństwa?
2. Czy są korzyści z bycia nieświadomym/niepoinformowanym?
3. Co jest gorsze – brak informacji, czy chaos informacyjny?

Wszechobecność i nadmiar informacji wymaga przygotowania do krytycznego ich odbioru, a upowszechnienie Internetu sprawia, że umiejętność twórczego i aktywnego wykorzystania sieci w zdobywaniu informacji ma wręcz kluczowe znaczenie. Niestety, na obecną chwilę w polskim społeczeństwie zauważyć można brak systemowych rozwiązań, które zapewniałyby minimalny poziom umiejętności ważnych dla świadomego korzystania z informacji.

4. PRZYKŁADY ZAGROŻEŃ SPOWODOWANYCH CHAOSEM INFORMACYJNYM W ASPEKCIE BEZPIECZEŃSTWA EKOLOGICZNEGO

Chaos informacyjny po każdej katastrofie to norma, a nie wyjątek. Ktoś do kogoś dzwoni o 8.56 że była katastrofa. Ten następnie dzwoni do kogoś innego, że o 8.56 dostał informację o katastrofie. A tamten na antenie zapodaje, że o 8.56 doszło do katastrofy. Podchwytują to inne media i mamy fakt medialny, nijak się mający do rzeczywistości, ale wywołujący szerzącą się z każdą chwilą panikę. Śledztwo zawsze obejmuje szerokie spektrum założeń, które po kolei się eliminuje, do niektórych również się czasem wraca, gdy wychodzą na jaw nowe okoliczności. Dlatego oficjalne komunikaty z jego przebiegu siłą rzeczy są mało konkretne i enigmatyczne.

Należy pamiętać, iż mówiąc o zagrożeniach bezpieczeństwa ekologicznego mamy na uwadze nie tylko zagrożenie środowiska, ale także tych elementów materialnego otoczenia człowieka, które decydują o jego dalszej egzystencji, a co za tym idzie, zdrowia oraz życia ludzkiego. Sytuacja zagrożenia występuje najczęściej w połączeniu z innego rodzaju sytuacjami trudnymi, takimi jak: przeciążenia, utrudnienia, sytuacje stresowo oraz konfliktowe. Bywa też, że mamy do czynienia z zagrożeniem urojonym, ale jego wpływ na zachowanie człowieka jest mniejszy niż podczas zagrożenia realnego.

Jedna z najstarszych, najgłośniejszych, ale też najbardziej barwnych historii sięga 30 października 1938 r., kiedy to amerykański reżyser Orson Welles przygotował radiowe słuchowisko na podstawie książki „Wojna światów”

Herberta George'a Wellsa. O godz. 20.00 kilka milionów Amerykanów włączyło radioodbiorniki, by wysłuchać wieczornej audycji i kompletnie zaskoczone opowieścią o ataku Marsjan na ziemię… uwierzyło, że dzieje się to naprawdę. Bez wątpienia sprzyjała temu dynamika kilkugodzinnej(!) akcji, przerywane sceny, dobra gra aktorska… i pewnie słabe jeszcze obycie społeczeństwa z mediami. Część słuchaczy przeoczyła zresztą wprowadzającą zapowiedź audycji, a reszta – nawet jeśli początkowo zdawała sobie sprawę, iż jest to fikcja – uległa nastrojom sąsiadów. Koniec końców późnym wieczorem wielu Amerykanów ze spakowanym dobytkiem życia opuściło swoje domy znacząco degradując przy tym środowisko i zaczęło gromadzić się w miejscach publicznych. Reżyserski eksperyment spowodował histerię tłumu… która na szczęście nie skończyła się tragicznie.

Uczestnicy piwnego święta w Mińsku (na Białorusi) 30 maja 1999 roku nie mieli jednak tyle szczęścia. Nagła zmiana warunków atmosferycznych i gwałtowny opad deszczu z gradem w czasie koncertu rockowego na wolnym powietrzu (niedaleko Pałacu Sportu), spowodował panikę słuchaczy doprowadzając do tragedii. Ludzie obecni na koncercie chcąc schować się przed niespodziewanym załamaniem pogody ruszyła do przejścia podziemnego na stacji metra „Niamiha". Niestety, zniszczenia środowiska były w tym przypadku najmniejszą stratą, bowiem z powodu deszczu schody zrobiły się bardzo śliskie i wiele osób przewracało się, a potem nie mogło się podnieść. W wyniku stratowania zginęły 53 osoby, ponad 250 zostało rannych. Większość ofiar to nastolatki. Większość zmarła w wyniku uduszenia i ran. Mnóstwo ofiar miało głębokie rany kłute na ciele, zadane butami na wysokich obcasach.

O zachowaniu ludzi w sytuacji zagrożenia decydują uczucia i instynkty. Tłum kieruje się uczuciami, a nie rozumem. Tłum wykazuje niezwykłą łatwość ulegania wpływom. Uczucia rozchodzą się z niezwykłą szybkością. Ludzie w tłumie wykazują instynkt stadny i kierują się bezmyślnie zachowaniem innych osób. Nie poszukują drogi ucieczki na własną rękę, podążają za innymi. Dążenie do szybkiego opuszczenia zagrożonego miejsca jest silniejsze niż dążenie niż dążenie do unikania kolizji z innymi. Ludzie zaczynają się tratować wzajemnie podczas gdy inne wyjścia ewakuacyjne są nieużywane.

Sytuacje kryzysowe są nieuniknione, jednak brak stosownej wiedzy i doświadczenia skutkuje tym, że w przypadku zagrożenia traci się rozsądek i możliwości racjonalnego zachowania.

Pojawia się zatem pytanie, czy warto przedwcześnie ogłaszać ryzyko wystąpienia katastrofy ekologicznej? Należy zawsze zadać sobie to pytanie, bowiem skutki takich decyzji mogą być mieć ogromne konsekwencje, zarówno zdrowotne, polityczne, ekonomiczne, czy ekologiczne, a wymienić można wśród nich:

- możliwość paniki wśród ludności oraz zagrożenie zakłócenia porządku publicznego,
- utrudnienia w dostępie do żywności i wody pitnej,
- okresowe utrudnienia w przemieszczaniu się w tym przez granicę państwową,
- możliwy wzrost przestępczości o charakterze kryminalnym oraz zwiększona liczba przestępstw i wykroczeń pospolitych (kradzieże z włamaniem, rozboje, niszczenie mienia),
- zakłócenia w funkcjonowaniu administracji jak również gospodarki wynikające z nieobecności kadry przedsiębiorstw i instytucji, w tym obsługujących infrastrukturę krytyczną,
- izolacja znacznych terenów, długoterminowe zablokowanie szlaków/ węzłów komunikacyjnych powodującym unieruchomienie lub utrudnienia w transporcie oraz utrudnienia komunikacyjne,
- Konieczność dużych nakładów z budżetu państwa związaną z likwidacją powstałego chaosu,
- Możliwość miejscowego skażenia środowiska (w przypadku braku zachowania wymogów z zakresu bezpieczeństwa sanitarna – epidemiologicznego i weterynaryjnego,
- Możliwe zniszczenia środowiska naturalnego (skala zniszczeń uzależniona od skali i zasięgu zaistniałego zjawiska) w tym straty w populacji zwierząt dziko żyjących,
- Zniszczenia obiektów użyteczności publicznej/lokali mieszkalnych/ miejsc pracy,
- wrist can product żywnościowych,
- możliwość upadku gospodarstw oraz zakładów przetwórczych.

Według najnowszych badań aż 40% ludności świata jest zagrożone skutkami degradacji gleby. Przyczyny stanowią przede wszystkim zanieczyszczenia środowiska, ekstremalne warunki pogodowe, postępujące wylesianie oraz nadmierna eksploatacje gleb na potrzeby rolnictwa. Już dziś eksperci ostrzegają, że nawet 700 mln ludzi może być w niedalekiej przyszłości zmuszonych do migracji z powodu pogorszenia się właściwości fizycznych, biologicznych oraz chemicznych ziemi.[5] Już sama taka informacja jest w stanie wywołać strach, a u niektórych nawet panikę. Do czego więc może dojść, kiedy faktycznie sytuacja zacznie stanowić realne zagrożenie? Jak zachowają się i do czego posuną przerażeni ludzie uciekający przed katastrofa ekologiczną i walczący o przetrwanie? Niestety, dotychczasowa historia pokazuje, że ludzie w sytuacji zagrożenia zdrowia, ale także w celach konsumpcyjnych oraz eksportowych

[5] https://zmianynaziemi.pl/wiadomosc/ludzkosc-czekaja-potezne-migracje-ludnosci-nawet-700-mln-ludzi-bedzie-musialo-uciekac-aby, (16.05.2018r.).

lub życia bezmyślnie potrafią degradować środowisko, nie zważając, że i tak ostatecznie dotknie to ich samych.

Nie bez powodu zresztą mówi się, że rzeczywistym celem terrorystów nie są konkretne przeprowadzane akty terrory, a zastraszenie ludzkości. Bo zastraszonych ludzi łatwiej wpędzić w przerażenie, chaos, destabilizację… I w panikę, która potrafi zebrać całkiem spore żniwa. Dlatego tak ważne jest, aby zachować bezpieczeństwo informacyjne i w przypadku zagrożeń lub katastrof ekologicznych zachować wszelkie procedury zarządzania bezpieczeństwem informacyjnym.

4. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACYJNYM

Zdobywanie wiadomości pewnych i najświeższych jest dziś działaniem wyjątkowo ambitnym i pożytecznym. Stanowią one rosnącą wciąż lawinę komunikatów, które nieustannie bombardują psychikę człowieka. Wcześniejsze źródła informacji, jak prasa, radio i telewizja, wsparte zostały Internetem i telefonią komórkową.

Obecnie jednak coraz więcej mówi się o „szybkim przyroście informacji", który może się stać nawet barierą poznania. Specjaliści przestrzegają w związku z tym przed „przeciążeniem informacyjnym", które z kolei wyklucza poprawne przetwarzanie informacji, niezbędne do ich praktycznego zastosowania. Ktoś może dowiadywać się bardzo wiele i z różnych źródeł, ale nie radzi sobie z natłokiem wiadomości. Nic dziwnego więc, że ich presja nazywana jest „bombą I", gdyż uniemożliwia zebranie zdobywanych informacji, ich segregację i wykorzystanie w różnych sektorach aktywności człowieka.

Informacja staje się szkodliwa także wtedy, gdy jest niepełna, nieprawdziwa i ukazuje fałszywy obraz pewnej rzeczywistości. Jest to informacja zmanipulowana, wskutek czego jednostka żyje w świecie iluzji, z której nie zdaje sobie sprawy, dlatego tak istotne jest zarządzanie bezpieczeństwem informacyjnym, szczególnie w sytuacjach dotyczących bezpieczeństwa publicznego.

Polityka bezpieczeństwa powinna zatem obejmować stały dostęp do informacji, zaś zarządzanie nią przyczyniać się do ciągłego aktualizowania zmian i procedur systemu bezpieczeństwa. Nie bez znaczenia są także pracownicy, którzy powinni ponosić odpowiedzialność za wyznaczony im zakres bezpieczeństwa informacji.

Może się jednak okazać, że system wykryje działania niepożądane lub dojdzie do próby włamania. Wtedy kluczowa okazuje się reakcja. W celu jak najszybszej reakcji opracowuje się plan awaryjny, w którym definiuje się, jaki powinien być odzew na zaistniały atak, dokumentuje się, a następnie testuje daną odpowiedź, aby w czasie kryzysu nie budzić paniki i postępować według planu.

Sposób ogłoszenia alarmu lokalnego lub ewakuacji, powinien być znany całej społeczności. Poznaniu sposobów ogłaszania oraz zasad zachowania się w sytuacji ogłoszenia alarmu służy ścieżka edukacyjna Obrona Cywilna, jednak mimo obowiązku realizacji tego ważnego zagadnienia nie wszyscy obywatele wiedzą jak prawidłowo należy zachować się w razie w sytuacji ogłoszenia ewakuacji.

Ostatnim etapem, nie mniej istotnym, jest refleksja. Po zażegnaniu niebezpieczeństwa przychodzi czas na podjęcie wszelkich kroków mogących udoskonalić plan ochrony informacji, ocenę dokonanych działań i dalszy rozwój. Dlatego tak ważne jest, aby opracować sprawnie funkcjonujący system zarządzania bezpieczeństwem informacyjnym i koordynować wszelkie procedury i zasady z nim związane.

PODSUMOWANIE

Gwałtowny postęp cywilizacyjny, powstanie zbiorów olbrzymich zasobów informacji oraz rozwój środków komunikowania stanowią zjawiska charakterystyczne dla współczesnych czasów, jednak niosą szczególne zagrożenia dla bezpieczeństwa informacyjnego, bowiem te informacje coraz częściej stanowią wciąż rosnącą lawinę komunikatów, które nieustannie bombardują psychikę człowieka. Dlatego dostęp informacji dotyczących sytuacji kryzysowych w społeczeństwie powinien być szczególnie chroniony, aż do momentu wystąpienia realnego zagrożenia bezpieczeństwa, w tym ekologicznego, bowiem skutki „przecieku" informacji bądź przedwczesnego zaalarmowania mogą być nawet tragiczne w skutkach.

Zarządzanie bezpieczeństwem informacyjnym w obecnych warunkach stanowi zatem poważne wyzwanie i powinno być zagadnieniem stale poruszanym przy omawianiu problematyki zmieniającego się świata. Ogrom przepływu informacji jest zjawiskiem powszechnym i pożądanym, ale także niebezpiecznym, jeżeli nie podejmuje się działań wspierających politykę bezpieczeństwa.

Należy także pamiętać, iż sprawnie działający system zarządzania bezpieczeństwem informacji powinien obejmować, poza odpowiednim oprogramowaniem, sprzętem i zasobami materialnymi, także pracowników, których odpowiednie przeszkolenie oraz przygotowanie w zakresie ochrony informacji znacznie zwiększa szansę na opanowanie sytuacji kryzysowych, mających wpływ na bezpieczeństwo ekologiczne oraz publiczne.

LITERATURA

Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2006.

Beskosty M., *Zarządzanie bezpieczeństwem informacji*, Studia nad Bezpieczeństwem, Nr 2/2017, Wyd. Naukowe Akademii Pomorskiej w Słupsku, Słupsk 2017.

https://zmianynaziemi.pl/wiadomosc/ludzkosc-czekaja-potezne-migracje-ludnosci-nawet-700-mln-ludzi-bedzie-musialo-uciekac-aby, (16.05.2018r.).

Janczak J., Zakłócenia informacyjne, AON, Warszawa 2001.

Kowalkowski S. (red.) Niemilitarne zagrożenia bezpieczeństwa publicznego, AON, Warszawa 2011.

Liczmańska-Kopcewicz K., *Uczestnictwo konsumentów w tworzeniu innowacji poprzez media społecznościowe,* Przedsiębiorczość i Zarządzanie, t. 18, z. 4, cz. 2 Agile Commerce - technologie przyszłości, Społeczna Akademia Nauk, Łódź-Warszawa 2017.

Liderman K., Bezpieczeństwo informacyjne, Wydawnictwo Naukowe PWN, Warszawa 2012.

Wiśniewska A. M., Liczmańska K., *Tworzenie wartości dla klientów w erze technologii informatyczno–komunikacyjnych*, Roczniki Ekonomiczne Kujawsko-Pomorskiej Szkoły Wyższej w Bydgoszczy, Nr 3/2010, Bydgoszcz 2010.

Żebrowski A., W. Kwiatkowski, Bezpieczeństwo informacji III Rzeczypospolitej, Oficyna Wydawnicza ABRYS, Kraków 2000.

CONTEMPORARY INFORMATION SECURITY MANAGEMENT IN THE ASPECT OF ECOLOGICAL HAZARDS

Abstract: The development of electronics, the Internet, the use of public networks to send information for industrial systems, makes information become a key factor determining knowledge and power, but also decisive for the safety of citizens, organizations, and even entire countries. The location of the threat, including the information threat, in the area of public awareness prompts questions about the degree of reception of certain phenomena and the determination of whether all phenomena threatening information security are indeed a threat or only information chaos.

The following article aims to characterize the contemporary threats to information security occurring in the modern world in the aspect of ecological security and activities in the field of information security management aimed at minimizing them.

Keywords: security, information, information security management, ecological threats.