Lidia Więcaszek-Kuczyńska

Zagrożenia bezpieczeństwa informacyjnego

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 2(10), 210-233

2014

AUTOR
mgr Lidia Więcaszek-Kuczyńska
lidiakuczynska@neostrada.pl

ZAGROŻENIA BEZPIECZEŃSTWA INFORMACYJNEGO

Wstęp

Analiza procesu transformacji społeczeństw i gospodarek *nowego XXI wieku*[1] dokonywana przez specjalistów wielu dyscyplin naukowych określa dalszy kierunek rozwoju jako bazujący na wiedzy i informacji w społeczności globalnej[2].

Rozwój elektroniki, homogenicznych sieci teleinformacyjnych (Internet), powszechność urządzeń dostępowych, powstanie sieci społecznościowych, 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[3].

Wiek XXI, w literaturze przedmiotu nazwany wiekiem informacji, przyniósł zatem zmianę natury i kształtu zagrożeń na świecie, gdyż w czasach powszechnego dostępu do technik informatycznych, rodzą się nowe niebezpieczeństwa[4] ściśle powiązane z użytkowaniem sieci informatycznych i systemów informacyjnych np. przestępstwa wykorzystujące komputer jako narzędzie, utrata informacji związana z włamaniami komputerowymi, złośliwymi kodami i wirusami, szpiegostwem, sabotażem, wandalizmem[5], a rozpoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego staje się nieodzowne do zapewnienia przewagi konkurencyjnej podmiotów gospodarczych, ich płynności finansowej, rentowności, pozostawania w zgodzie z literą prawa[6].

[1] M. Wrzosek, *Polska, Unia Europejska, NATO wobec wyzwań i zagrożeń*, AON, Warszawa 2012, s. 7.
[2] Zob., *Świat w 2025. Scenariusze Narodowej Rady Wywiadu USA*, Alfa Sagittarius, Kraków 2009, s. 195-196.
[3] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 11-12.
[4] *Zagrożenie (…) to najbardziej klasyczny czynnik środowiska bezpieczeństwa.* Zob., S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, s. 268.
[5] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 24.
[6] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa 2010, s. 22.

Wzrost roli informacji we współczesnym świecie, powoduje wzrost zagrożeń jej bezpieczeństwa[7]. Współczesny *włamywacz*[8]*,* nie forsuje już za pomocą łomu pancernych drzwi do bankowego skarbca, ale wykorzystując swoją wiedzę informatyczną, łamie kody dostępów do kont bankowych, z których bez użycia siły fizycznej transferuje środki pieniężne na wskazane rachunki bankowe.

Czasy nam współczesne, do tradycyjnych zagrożeń informacyjnych jak np. szpiegostwo[9] dołożyły nowe, wynikające z rozwoju technologii, tj. przestępstwa komputerowe, cyberterroryzm, a kolejne wyzwania związane z postępem technologicznym mogą stać się źródłem nieznanych dotąd niebezpieczeństw. Zatem zdefiniowanie źródeł zagrożeń bezpieczeństwa informacyjnego wydaje się kluczowe dla zapewnienia bezpieczeństwa informacyjnego organizacji[10].

Definicja bezpieczeństwa informacyjnego

Podejmując próbę przybliżenia definicji bezpieczeństwa informacyjnego, należy odpowiedzieć na pytanie, jak rozumieć pojęcie *bezpieczeństwo*. W opinii T. Łoś-Nowak pojęcie to jest trudne do zdefiniowania, gdyż bezpieczeństwo to nie tylko stan możliwy do określenia jedynie w ustalonym miejscu i czasie, tu i teraz (*hic et nunc*), ale również dynamiczny, zmieniający się w czasie proces[11], zaś zdaniem R. Zięby *bezpieczeństwo można określić jako pewność istnienia i przetrwania, posiadania oraz funkcjonowania i rozwoju podmiotu. Pewność jest wynikiem nie tylko braku zagrożeń (…), ale także powstaje w skutek kreatywnej działalności danego podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego*[12]. W rozważaniach nad istotą bezpieczeństwa informacyjnego, zasadne jest odniesienie do ogólnej definicji bezpieczeństwa organizacji sformułowanej przez S. Kozieja, określającej bezpieczeństwo podmiotu jako proces, tj. *tę dziedzinę jego aktywności, która zmierza do zapewnienia możliwości prze-*

[7] A. Nowak, W. Scheffs, *Zarządzanie*…, wyd. cyt., s. 22.

[8] W. Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji*, Helion, Gliwice 2012, s. 11.

[9] Upływ czasu nie zdezaktualizował koncepcji Sun Tzu: *Tego, że się wie zawczasu, nie można uzyskać od duchów (…) ani z gwiezdnych wyliczeń. (…) Do tego trzeba szpiegów.* Zob., Sun Tzu*, Sztuka Wojenna,* przeł. Robert Stiller, Vis-a vis Etiuda, Kraków 2011, s. 127.

[10] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 7.

[11] T. Łoś-Nowak, *Bezpieczeństwo,* [w:] A. Antoszewski i R. Herbut (red.), *Leksykon politologii*, Alta 2, Wrocław 2003, s. 37-38.

[12] R. Zięba, *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 16.

trwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów[13].

Bezpieczeństwo informacyjne, w opinii K. Lidermana, jak dotąd nie doczekało się jednoznacznej wykładni i wraz z towarzyszącym mu terminem „bezpieczeństwo informacji"[14] jest używane w różnych znaczeniach[15], obejmując wszystkie formy, także werbalne, wymiany, przechowywania oraz przetwarzania informacji[16].

K. Liderman bezpieczeństwo informacyjne[17] 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*[18].

Tak definiowane bezpieczeństwo nie jest ani obiektem, ani zdarzeniem, ani procesem – *to imponderabilia z dziedziny psychologii*[19].

W opinii K. Lidermana, bezpieczeństwo informacyjne, ze względu na coraz większy udział w transmisji, przechowywaniu i przetwarzaniu informacji[20] środków technicznych, jest wrażliwe na różne postaci tzw. cyberzagrożeń, w tym związane z działaniami terrorystycznymi[21].

Bezpieczeństwo informacyjne, niejednokrotnie zatem rozważa się jako element systemu informatycznego, jako synonim bezpieczeństwa komputerowego, telekomunikacyjnego[22], czy bezpieczeństwa sieciowego[23].

---

[13] S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszaw, 2011, s. 255.

[14] Por., *Kiedy mówimy o bezpieczeństwie informacyjnym, to zawsze dotyczy to podmiotu, który jest zagrożony przez brak informacji (…). Natomiast bezpieczeństwo informacji to ochrona informacji będącej w posiadaniu tego właśnie podmiotu.* A. Nowak, W. Scheffs, *Zarządzanie…*, wyd. cyt. s. 25.

[15] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 13.

[16] Tamże, s. 22.

[17] Por., *(…) bezpieczeństwo informacji oznacza uzasadnione (…) zaufanie, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie jej obiegu.* K. Lideramn, dz.cyt.s.22.

[18] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 22.

[19] Tamże, s. 109.

[20] Informacja nie istnieje bez komunikacji, a efektywność przekazu informacyjnego w dużym stopniu zależy od telekomunikacji i teleinformatyki. Zob., B. Lent, *Bezpieczeństwo w telekomunikacji i teleinformatyce,* BBN, Warszawa 2002, s. 13.

[21] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 24.

[22] Zob. R. J. Sutton, *Bezpieczeństwo telekomunikacji*, przeł. G. Stawikowski, Wydawnictwo Komunikacji i Łączności, Warszawa 2004, s. 17.

[23] A. Nowak, W. Scheffs, *Zarządzanie…*, wyd. cyt., s. 22.

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[24].

W opinii ekspertów, bezpieczeństwo wyraża się zatem we wszystkich obszarach działalności organizacji, jego struktura jest w istocie równoważna ze strukturą funkcjonowania podmiotu, zaś bezpieczeństwo informacyjne jest umiejscawiane, obok już przywoływanego, bezpieczeństwa militarnego, ekonomicznego, czy publicznego w ramach szerszych pojęć bezpieczeństwa międzynarodowego i narodowego[25].

Bezpieczeństwo informacyjne opisuje się w literaturze przedmiotu także jako stan, w którym ryzyko wystąpienia zagrożeń związanych z prawidłowym funkcjonowaniem zasobów informacyjnych jest ograniczone do akceptowalnego poziomu[26].

Szeroką definicję bezpieczeństwa informacyjnego przedstawiają E. Nowak i M. Nowak, według których bezpieczeństwo informacyjne to stan warunków zewnętrznych i wewnętrznych dopuszczających, aby państwo swobodnie rozwijało swoje *społeczeństwo informacyjne*[27], zaś za warunki osiągnięcia bezpieczeństwa informacyjnego przywołani autorzy przyjmują:

- niezagrożone strategiczne zasoby państwa;
- decyzje organów władzy podjęte na podstawie wiarygodnych, istotnych informacji;
- niezakłócony przepływ informacji pomiędzy organami państwa;
- niezakłócone funkcjonowanie sieci teleinformatycznych tworzących krytyczną infrastrukturę teleinformatyczną państwa[28];
- zagwarantowaną przez państwo ochronę informacji niejawnych i danych osobowych obywateli;

---

[24] S. Kowalkowski (red.) *Niemilitarne zagrożenia bezpieczeństwa publicznego*, AON, Warszawa 2011, s. 13-15.

[25] S. Koziej, *Teoria…*, wyd. cyt., s. 256.

[26] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa, 2010, s. 150.

[27] Zob., Ministerstwo Łączności Komitet Badań Naukowych, Raport: *Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce*, Warszawa, 28 listopada 2000 r.: *społeczeństwo informacyjne – [ang. Information society] – nowy system społeczeństwa kształtujący się w krajach o wysokim stopniu rozwoju technologicznego, gdzie zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności zarówno w przemyśle, jak i w usługach, a stopień rozwoju wymaga stosowania nowych technik gromadzenia, przetwarzania, przekazywania użytkowania informacji.* Źródło: http://kbn.icm.edu.pl [dostęp 22.02.2014].

[28] Do infrastruktury krytycznej państwa zaliczane są między innymi systemy informacyjne państw i przedsiębiorstw.

- zasadę, że prawo do prywatności obywateli jest nienaruszane przez instytucje publiczne,
- swobodny dostęp obywateli do informacji publicznej[29].

Bezpieczeństwo informacyjne staje się zatem gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego, zarówno w skali lokalnej pojedynczego państwa, jak i na arenie międzynarodowej[30], co znajduje odpowiedź w opracowanych i wdrażanych przez państwo polskie strategiach oraz programach rządowych w zakresie bezpieczeństwa informacyjnego.

Treści podkreślające wagę tej problematyki odnajdujemy w m.in. *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*[31] oraz w dokumencie: *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011*[32]*.* 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*[33]*.*

W definiowaniu terminu „bezpieczeństwo informacyjne" niezbędne wydaje się odniesienie do norm PN-ISO/IEC 27001:2007[34] oraz PN-ISO/IEC

---

[29] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Difin SA, Warszawa 2011, s. 103.

[30] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 23.

[31] Strategia Bezpieczeństwa Narodowego RP w pkt 3.8. stanowi: *Zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych ma na celu przeciwdziałanie przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjna, w tym zapobieganie atakom na elementy tej infrastruktury. Szczególne znaczenie ma ochrona informacji niejawnych przechowywanych lub przekazywanych w postaci elektronicznej. Źródło* http://www.iniejawna.pl/pomoce/przyc_pom/SBN_RP.pdf*,* [dostęp 22.02.2014].

[32] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 24.

[33] Biała Księga Bezpieczeństwa Narodowego RP, źródło http://www.spbn.gov.pl/, [dostęp: 22.02.2014].

[34] PN-ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Zakres: *przedstawiono wymagania dotyczące ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia udokumentowanego systemu zarządzania bezpieczeństwem informacji (SZBI) w całościowym kontekście ryzyk biznesowych i określono wymagania dotyczące wdrożenia*

17799:2007, posługujących się terminem bezpieczeństwo informacji, gdzie jest on opisany jako *zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.*

Norma ISO/IEC 17799[35] odnosi się do bezpieczeństwa informacji kompleksowo i dostarcza rozwiązań, dzięki którym eliminuje się nawet najczęściej marginalizowane zagadnienia w tworzeniu procedur bezpieczeństwa[36], a regulacje lokalne wszystkich państw korzystają z tego dokumentu jako pewnego rodzaju referencji[37].

Bezpieczeństwo informacyjne, prócz standaryzacji określonej w przywoływanych wyżej normach, podlega licznym regulacjom prawnym, zaś za ustawy obligujące *organizacje do zapewnienia bezpieczeństwa przetwarzanych informacji* A. Nowak i W. Scheffs przyjmują: ustawę o ochronie danych osobowych, ustawę o ochronie informacji niejawnych, ustawę o dostępie do informacji publicznej, ustawę o prawach autorskich i prawach pokrewnych[38].

Obecnie w Polsce ponad dwieście aktów prawnych odnosi się do ochrony informacji, a dla każdego obszaru działania przedsiębiorstwa[39] można rozpoznać kilka lub kilkanaście przepisów prawnych obejmujących zapisy odnoszące się do bezpieczeństwa informacji[40].

W opinii A. Żebrowskiego i W. Kwiatkowskiego za system prawnokarnej ochrony informacji należy uznać przepisy zawarte w ustawie zasadniczej – Konstytucji Rzeczypospolitej Polskiej[41], ustawie o ochronie infor-

---

zabezpieczeń dostosowanych do potrzeb pojedynczych organizacji lub ich części. Źródło: http://www.pkn.pl/, [dostęp: 22.04.2014].

[35] PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji – Zakres: *Przedstawiono zalecenia i ogólne zasady dotyczące inicjowania działań, wdrażania, utrzymania i doskonalenia zarządzania bezpieczeństwem informacji w organizacji. Cele stosowania zabezpieczeń przedstawione w normie są powszechnie akceptowanymi praktykami zarządzania bezpieczeństwem informacji.* Źródło http://www.pkn.pl/, [dostęp: 22.04.2014].

[36] A. Nowak, W. Scheffs, *Zarządzanie…,* wyd. cyt., s. 35.

[37] Tamże, s. 35-36.

[38] Tamże, s. 6.

[39] Jako przykład może posłużyć obowiązująca podmioty prowadzące księgi rachunkowe *Ustawa o Rachunkowości*, której cały rozdział ósmy dotyczy zagadnienia ochrony danych, w tym szczegółowo reguluje tematykę przechowywania danych, ich przetwarzania i udostępniania. Zob. Ustawa z 29.09.1994 r. o rachunkowości (Dz. U. z 2009 r. nr.152, poz.1223 z póz. zm.)

[40] A. Nowak, W. Scheffs, *Zarządzanie…,* wyd. cyt., s. 6.

[41] W świetle aktualnie obowiązującej ustawy zasadniczej konstytucyjny obowiązek strzeżenia tajemnicy państwowej i służbowej przez obywateli wynika z niżej wymienionych zapisów Konstytucji RP: *art. 82 „Obowiązkiem obywatela polskiego jest wierność Rzeczypospolitej Polskiej*", *art. 83 „Każdy ma obowiązek przestrzegania prawa Rzeczypospolitej Polskiej*". Zob., http://www.sejm.gov.pl/prawo/konst/polski/kon1.htm, [dostęp: 11.12.2013].

macji niejawnych[42], kodeksie karnym[43], zarządzeniach resortowych, umowach międzynarodowych, których stroną jest Polska[44].

Za J. Koniecznym można stwierdzić, *iż prawo polskie chroni sporą liczbę tajemnic*[45], ale za regulacje prawne najbardziej istotne dla menadżera w jego codziennej pracy powinno się uznać: przepisy o ochronie informacji niejawnych zawarte w *Ustawie o ochronie informacji niejawnych*, regulacje dotyczące tajemnicy przedsiębiorstwa zawarte w *Ustawie o zwalczaniu nieuczciwej konkurencji*[46] oraz zapisy *Ustawy o ochronie danych osobowych*[47].

Rozważając problematykę bezpieczeństwa informacyjnego, bez wątpienia należy uwzględnić, iż pojęcie bezpieczeństwa informacyjnego stosuje się także do informacji spoza systemu teleinformatycznego, pojawiających się na nośnikach kiedyś standardowych, np. dokumentach papierowych, mikrofilmach, a polityka bezpieczeństwa informacji obejmuje proces korzystania z informacji bez względu na sposób jej przetwarzania i dotyka zarówno systemów prowadzonych tradycyjnie (archiwa, kartoteki, dokumenty papierowe), jak i systemów komputerowych[48].

[42] *Od 2 stycznia 2011 r. obowiązuje ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182, poz.1228), która zastąpiła dotychczasową ustawę z 1999 r. Potrzeba wprowadzenia w tej materii nowej regulacji wynikała z konieczności dostosowania przepisów do zmieniającej się rzeczywistości, uaktualnienia przestarzałych i niefunkcjonalnych uregulowań wobec dzisiejszego poziomu technologicznego oraz dostosowania polskich rozwiązań do praktyk i reguł obowiązujących w instytucjach Unii Europejskiej i NATO. Wśród uregulowań nowej ustawy istotne jest m.in. zniesienie podziału na tajemnicę państwową i służbową. Ochronie podlegają obecnie te informacje, których ujawnienie przyniosłoby szkody interesom państwa*. Źródło http://www.rp.pl/artykul/599343.html, [dostęp: 24.02.2014].

[43] Kodeks Karny Dz. U. 1997 nr 88 poz. 553 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny.

[44] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000, s. 110.

[45] Ze względu na rodzaj podmiotu lub dziedzinę gospodarki, do której odnosi się chroniona informacja możemy wyszczególnić: tajemnicę przedsiębiorstwa, tajemnicę handlową, bankową, publicznego obrotu papierami wartościowymi, zamówień publicznych, tajemnicę statystyczną, tajemnicę skarbową, tajemnicę czynności operacyjno-rozpoznawczych, lekarską i wiele innych, których szczegółowe omówienie wykracza poza ramy niniejszego opracowania. Zob., J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu*, Konsalnet, Warszawa 2004, s. 171.

[46] Por., K. Liderman, *Bezpieczeństwo…,* wyd. cyt., s. 19-22.

[47] J. Konieczny, *Wprowadzenie…*, wyd. cyt., s. 171.

[48] A. Nowak, W. Scheffs, *Zarządzanie…,* wyd. cyt., s. 40.

Zagrożenia bezpieczeństwa informacyjnego

Podejmując próbę przybliżenia problematyki zagrożeń bezpieczeństwa informacyjnego należy przede wszystkim odpowiedzieć na pytania: czym jest zagrożenie, jak rozumieć pojęcie zagrożenia?

Termin *zagrozić* możemy opisać za P. Bączkiem podającym m.in. definicję leksykalną pojęcia, jako: *postraszyć kogoś, zapowiedzieć coś złego, ostrzec pod groźba jakichś konsekwencji*, oraz *stać się niebezpiecznym, groźnym dla kogoś, czegoś*, oraz definicje politologiczne, w których *zagrożenia to wyzwania niepodejmowane lub podejmowane za późno*[49].

S. Koziej przedstawia *zagrożenie jako pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot, w podziale na zagrożenie potencjalne lub realne, subiektywne i obiektywne, zewnętrzne i wewnętrzne, militarne i niemilitarne (umiejscawiając zagrożenia informacyjne w grupie zagrożeń niemilitarnych, wraz z zagrożeniami politycznymi, ekonomicznymi, społecznymi, ekologicznymi)*[50].

Należy jednak nadmienić, iż nie wszystkie zjawiska zagrażające bezpieczeństwu są zagrożeniem: stan zagrożenia jest związany ze świadomością podmiotu będącego celem zagrożenia, a zatem możemy wnioskować, iż jedynie brak odpowiedniej wiedzy o znaczeniu i istocie zjawiska zagrożenia powoduje określony stan psychiczny. W następstwie tego poznanie oraz zrozumienie zjawiska zagrożenia prowadzi do zminimalizowania poziomu niebezpieczeństwa i wtedy zamiast pojęcia zagrożenie bardziej właściwe staje się nazwanie powstałego stanu ryzykiem[51], które należy likwidować albo wyzwaniem wartym podjęcia[52].

Lokalizacja źródeł zagrożenia pozwala wyodrębnić zagrożenia bezpieczeństwa informacyjnego wewnętrzne, powstające wewnątrz organizacji, takie jak zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu błędu jak i przypadku, zagrożenie utratą lub uszkodzeniem poprzez celowe działania nieuczciwych użytkowników, oraz zewnętrzne, powstające poza organizacją, w wyniku celowego lub przypadkowego działania ze strony osób trzecich. W stosunku do systemu, eksperci wyodrębniają także zagrożenia fizyczne, w których szkoda jest spowodowana wypadkiem, awarią, lub innym nieprzewidzianym zdarzeniem wpływającym na system informacyjny[53].

---

[49] P. Bączek, *Zagrożenia…*, wyd. cyt., s. 31.

[50] S. Koziej, *Teoria…*, wyd. cyt., s. 269.

[51] *Ryzyko to niepewność związana z własnym działaniem, z jego skutkami, to niebezpieczeństwo niepożądanych skutków własnego działania.* Zob., S. Koziej, *Teoria…*, wyd. cyt., s. 280.

[52] M. Wrzosek, *Polska…*, wyd. cyt., s. 14.

[53] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo…*, wyd. cyt., s. 65.

Za K. Lidermanem jako źródła zagrożeń bezpieczeństwa informacyjnego należy przyjąć: siły natury (pożar, powódź, huragan, trzęsienie ziemi, epidemie), błędy ludzi i ich działania wg. błędnych lub niewłaściwych procedur, celowe, szkodliwe działanie ludzi, awarie sprzętu komputerowego, awarie oprogramowania, awarie infrastruktury usługowej (zasilanie, klimatyzacja, woda, ogrzewanie)[54].

P. Bączek zagrożenia bezpieczeństwa informacyjnego klasyfikuje w podziale na[55]:

- zagrożenia losowe – klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyjnego organizacji (np. pożar budynku, w którym przechowywane są nośniki informacji);
- tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyjna lub sabotażowa, ofensywa dezinformacyjna prowadzona przez obce państwa lub osoby, podmioty, organizacje;
- zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przetwarzaniem i przekazywaniem informacji w sieciach teleinformatycznych (do takich zagrożeń zaliczamy przestępstwa komputerowe, cyberterroryzm, walkę informacyjną);
- zagrożenia odnoszące się do praw obywatelskich osób lub grup społecznych m.in. sprzedaż informacji, przekazywanie informacji podmiotom nieuprawnionym, naruszanie przez władze prywatności, bezprawne ingerencje służb specjalnych, ograniczenie jawności życia publicznego.

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[56];
- zagrożenia asymetryczne;
- szpiegostwo[57].

Z tezą P. Bączka, iż źródłem zagrożeń bezpieczeństwa informacyjnego jest człowiek, zgodne wydaje się stanowisko A. Żebrowskiego, iż za-

[54] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 155.
[55] P. Bączek, *Zagrożenia…*, wyd. cyt., s. 72-73.
[56] Zob. J. Janczak, *Zakłócenia informacyjne*, AON, Warszawa 2001, s. 11. Autor definiuje istotę i techniki prowadzenia walki informacyjnej.
[57] P. Bączek, *Zagrożenia…*, wyd. cyt., s. 86-87.

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;
- kryptoanaliza zaszyfrowanych informacji;
- przechwytywanie otwartych połączeń sieciowych[58].

Zasadne jest, aby wybrane zagrożenia bezpieczeństwa informacyjnego przedstawione w dalszej części opracowania, były rozpoznawane w świetle opinii ekspertów, iż we współczesnej organizacji jednym z najważniejszych zagrożeń bezpieczeństwa informacyjnego jest możliwość niekontrolowanego dostępu i ujawnienia informacji stanowiącej tajemnicę[59].

W przedsiębiorstwach często obserwujemy zdarzenia, które przez brak wiedzy i świadomości użytkowników prowadzą do ujawnienia bądź utraty ważnych informacji, np. tak oczywiste działania jak naklejenie na monitor kartki z hasłami dostępu, bałagan na biurku, pozostawianie bez nadzoru dokumentów firmowych finansowych lub handlowych, wyrzucanie na śmietnik korespondencji z istotnymi dla podmiotu informacjami, zagubienie laptopa lub innego nośnika danych[60].

Zagrożenia bezpieczeństwa informacyjnego, autor przywoływany w części opracowania dotyczącej definicji bezpieczeństwa informacyjnego, R. J. Sutton wiąże z przesyłaniem lub przechowywaniem informacji i iden-

[58] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo…*, wyd. cyt., s. 73.
[59] Tamże, s. 61.
[60] A. Nowak, W. Scheffs, *Zarządzanie…*, wyd. cyt., s. 6.

tyfikuje jako: podsłuchiwane, modyfikowanie, powtarzanie, penetrowanie i zakłócenie[61].

Badacz umiejscawia zagrożenia bezpieczeństwa informacyjnego w obszarze zagrożenia bezpieczeństwa komputerowego oraz poczty elektronicznej i określa jako: nieuprawniony dostęp do danych; nieuprawniona ingerencja i wykorzystanie danych, utrata danych z powodu ich usunięcia lub kradzieży, fizyczne uszkodzenie nośnika danych, monitorowanie sprzętu (atak na sprzęt zabezpieczający); ujawnienie informacji podczas przesyłania; modyfikacja wiadomości podczas przesyłania, powtarzanie zapisanych wiadomości, podszywanie się pod inną osobę, zwodzenie, pozbawianie usługi[62].

Niezwykle trafna wydaje się opinia R. J. Suttona, iż informacje poufne, które użytkownik tradycyjną pocztą przesłałby zachowując wielka ostrożność, często pocztą elektroniczną są przesyłane bez zastanowienia i refleksji. Informacje takie, jak wyniki sprzedaży, oferty, dane osobowe i finansowe, prawnie zastrzeżone szczegóły techniczne, plany podróży i transportu oraz wiele innych, których ujawnienie może spowodować szkody, są często przesyłane jako niechronione, nawet wtedy, kiedy pracownik posiada dostęp do chronionego systemu poczty elektronicznej[63].

Należy zatem zgodzić się z J. Łuczakiem, iż *niewiele sytuacji kryzysowych firmy można porównać z utratą informacji,* szczególnie, że jak dowodzi praktyka, utrata informacji to incydenty coraz bardziej powszechne i trudne do wykrycia, przynoszące konsekwencje prawne, finansowe, utratę wiarygodności podmiotu dopuszczającego do nieuprawnionego dostępu osób trzecich do swoich danych[64], a obserwowany we współczesnej rzeczywistości gospodarczej dynamiczny rozwój sieci komputerowych przyczynia się także do tego, iż zbiory danych przepływają między organizacjami w sposób nie zawsze należycie kontrolowany, zaś komputerowe przetwarzanie danych umożliwia centralizację przechowywania i przetwarzania zasobów informacyjnych, co powoduje niespotykane dotąd zagrożenie utraty zasobów informacyjnych[65].

Rozważając zagrożenia bezpieczeństwa informacyjnego należy także zaznaczyć, iż pewne informacje, stanowią w organizacji wiadomości chronione, a tajność to jeden z atrybutów ochrony informacji (obok m.in. integralności, dostępności, niezaprzeczalności i autentyczności) stanowiący

[61] R. J. Sutton, *Bezpieczeństwo…*, wyd. cyt., s. 17.
[62] Tamże, s. 278-303.
[63] Tamże, s. 303.
[64] J. Łuczak, (red.) *Zarządzanie bezpieczeństwem informacji*, Oficyna współczesna, Poznań 2004, s. 10-11.
[65] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010, s. 152.

o wymaganym stopniu ochrony informacji przed nieuprawnionym dostępem[66].

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[67].

Analiza literatury przedmiotu oraz praktyka użytkowników pozwalają stwierdzić, iż utrata danych może nastąpić nie tylko z przyczyn losowych, jako skutek działania czynników obiektywnych takich, jak m.in. uszkodzenie sprzętu elektronicznego, spadki napięcia, błędy użytkownika, ale także na skutek zamierzonego działania osób, które celowo uzyskują nieuprawniony dostęp do zasobów, aby nielegalne zawładnąć zgromadzonymi lub dystrybuowanymi danymi[68], zaś człowiek jest najsłabszym ogniwem bezpieczeństwa, gdyż urządzenia techniczne, oprogramowanie to jedynie narzędzia obsługiwane przez ludzi i przede wszystkim od użytkownika będzie zależało utrzymanie informacji z dala od dostępu osób nieuprawnionych[69].

W opinii ekspertów zagrożeniem bezpieczeństwa informacyjnego są także konflikty asymetryczne[70].

Konflikt asymetryczny[71] to pojęcie obejmujące zarówno włamania komputerowe, cyberterroryzm, wojny psychologiczne i informacyjne, jak i konwencjonalne, działania militarne, ataki terrorystyczne, sabotaż, dywersję. Typowym konfliktem asymetrycznym były działania zapoczątkowane w wyniku zamachu 11 września 2001 roku, a głównym celem terrorystów było porażenie instytucji całego świata[72], należy zatem zgodzić się z tezą, iż przewaga *asymetrycznego przeciwnika* będzie wynikać z bezsilności cywilizacji zachodniej, bezradnej w razie utraty dostępu do swoich systemów telekomunikacyjnych[73].

Ugrupowania terrorystyczne, prócz tradycyjnych form wywierania przymusu, coraz częściej będą prowadziły ataki techno-cyberterrorystyczne, a także operacje psychologiczne w środkach masowego przekazu, propagując fałszywe lub sprzeczne informacje, rozsiewa-

[66] K. Liderman, *Bezpieczeństwo…*, wyd. cyt., s. 19.
[67] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo…*, wyd. cyt. s. 78.
[68] M. Wrzosek, *Procesy*…, wyd. cyt., s.156.
[69] Tamże, s. 151.
[70] *Według niektórych naukowców faktyczna asymetria jest konsekwencją istnienia – nie tyle dysproporcji w rozwoju technologicznym pomiędzy nowoczesnym Zachodem, a słabo rozwiniętym Trzecim Światem – ale różnic cywilizacyjnych, kulturowych, aksjologicznych oraz innego pojmowania świata przez poszczególne cywilizacje.* Zob., P. Bączek, *Zagrożenia…,* wyd. cyt., s. 138.
[71] Por. K. Liedel, P. Piasecka, T. R. Aleksandrowicz (red.), *Bezpieczeństwo w XXI wieku. Asymetryczny świat,* Difin, Warszawa 2011.
[72] P. Bączek, *Zagrożenia…,* wyd. cyt. s. 138.
[73] M. Wrzosek, *Współczesne…*, wyd. cyt., s. 193.

jąc lęk, niepewność, wątpliwości, a w zglobalizowanym świecie cyfrowych technologii, w którym czynnik odległości traci znaczenie, obrazy prezentowane przez elektroniczne media często już teraz kreują specyficzne wrażenie więzi pomiędzy ofiarami ataków terrorystycznych, a odbiorcami przekazywanych informacji[74].

Zagrożenie dla bezpieczeństwa informacyjnego buduje także aktywność grup, środowisk, firm, koncernów, które w swojej działalności świadomie manipulują przekazem informacji maskując swoje prawdziwe cele, dane dotyczące oferowanych wyrobów, usług, wykorzystując techniki manipulacji, perswazji, dezinformacji[75], propagandy[76].

Sekty to szczególnie wyraźny przykład grup, w których systematycznie stosuje się taki proceder[77].

W opinii badaczy, także niekontrolowany rozwój technologii bioinformatycznych może doprowadzić w przyszłości do powstania nowych zagrożeń, także w obszarze zagrożeń bezpieczeństwa informacyjnego, zagrożeń, które ostatecznie mogą okazać się znacznie poważniejsze od obecnie zidentyfikowanych i prowadzić do konfliktu wynalazków z zakresu inżynierii neuroinformatycznej z istniejącym systemem etyczno-moralnym (przykład prac nad tzw. sztuczną inteligencją)[78]. Naukowcy przewidują, iż komputery nowych generacji *będą zdolne komunikować się samodzielnie, a żyjąca własnym elektronicznym sygnałem sieć komunikacyjna* ogarnie całą naszą planetę[79].

Czy to tylko wizje z naukowych laboratoriów? Rozwój Internetu świadczy, że *informacyjna superautostarda*[80] staje się faktem, a nieuprawniony dostęp do zasobów informatycznych stwarza realne zagrożenie ataku na sieci informacyjne dezorganizującego działanie sektora publicznego, a nawet całego społeczeństwa.

---

[74] R. Borkowski, *Fabryki strachu – obraz terroryzmu jako kicz w medialnej popkulturze. Zagrożenia bezpieczeństwa międzynarodowego,* [w:] K. Liedel, P. Piasecka, T. R. Aleksandrowicz (red.), *Bezpieczeństwo…*, wyd. cyt., s. 113.

[75] Dezinformacja (osobowa lub techniczna) często utożsamiana jest z zakłóceniami dezinformującymi stanowiącymi formę walki informacyjnej. Zob., J. Janczak, *Zakłócenia informacyjne*, AON, Warszawa 2001, s. 17-25.

[76] P. Bączek, *Zagrożenia…,* wyd. cyt., s. 116.

[77] *Po kilku latach spokoju uaktywniła się w Polsce sekta Moona (…). Poszukiwane są osoby aktywne zawodowo, posiadające rodziny, a także studenci. Po zdobyciu namiarów po kilku tygodniach pojawiają się telefony i e-maile zapraszające do współpracy, a w końcu atrakcyjna oferta zagranicznego wyjazdu. Wszystko to prowadzi do psychicznego i finansowego uzależnienia najczęściej młodych ludzi od sekty. Osoby wciągnięte przez sekty bardzo trudno później odnaleźć, ponieważ zrywają wszelkie więzi łączące je z rodziną i znajomymi. Wyjeżdżają nawet na kilka lat, przekazując cały swój majątek sekcie.* http://www.rmf24.pl/fakty/polska/news-uwaga-sekta-moona-znow-dziala-w-polsce,nId,597548, [dostęp: 28.01.2014].

[78] P. Bączek, *Zagrożenia…,* wyd. cyt., s. 121.

[79] M. Wrzosek, *Współczesne…*, wyd. cyt., s. 201.

[80] Tamże, s. 201.

Zagrożenie bezpieczeństwa informacji to jednak nie tylko zagrożenia związane z rozwojem technologicznym współczesnego świata, ale także znane już od tysiącleci szpiegostwo, rozumiane jako działanie przestępcze dokonywane na szkodę danego państwa, przez podjęcie pracy na rzecz obcego wywiadu, a szczególnie przekazywanie informacji stanowiących tajemnice państwową lub wojskowa obcemu wywiadowi[81].

W opinii ekspertów, postępujący rozwój informatyzacji wraz z uzależnieniem większości aspektów działalności człowieka od systemów informatycznych i informacyjnych sprawi, iż powiększy się katalog zagrożeń informatycznych, a *wiele krajów europejskich oraz organizacji rządowych podejmuje działania* zawierające elementy współczesnej *walki informacyjnej*[82].

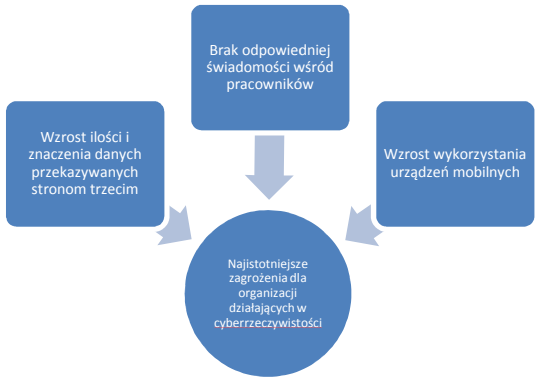
Zagrożenia bezpieczeństwa informacji: aspekty praktyczne

Obserwując codzienną praktykę rzeczywistości gospodarczej, śledząc doniesienia medialne, stajemy się świadkami, a często uczestnikami zdarzeń świadczących, iż zagrożenie bezpieczeństwa informacyjnego jest zagrożeniem realnym, a utrata informacji może naruszyć żywotne interesy podmiotu, narazić bezpieczeństwo osobowe oraz podstawowe wartości życia społecznego, o czym świadczą zaprezentowane w tej części opracowania przykłady wybranych incydentów.

Współcześni przedsiębiorcy, aktywnie działając na płaszczyźnie biznesowej w otoczeniu rynkowym opartym na nowoczesnych technikach przetwarzania informacji widzą i identyfikują zagrożenia z tym związane umiejscawiając je w trzech obszarach, które obrazuje rys.1.

[81] P. Bączek, *Zagrożenia…,* wyd. cyt., s. 147.

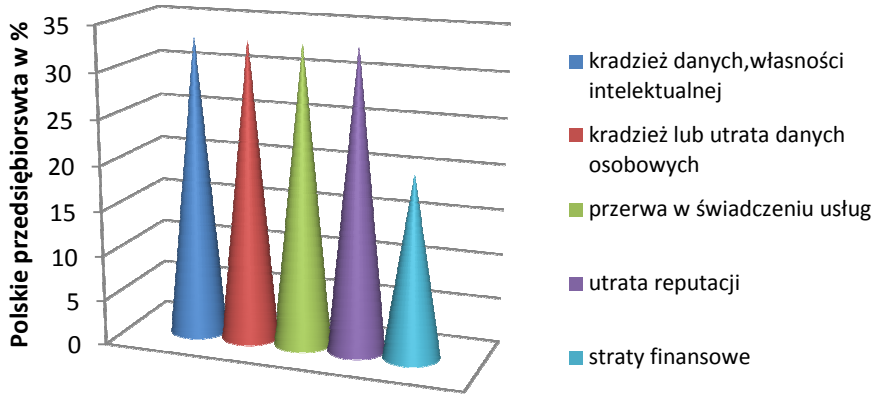
[82] Pojęcie walki informacyjnej nie jest jednoznaczne, wśród badaczy dominuje jednak teza, iż walkę informacyjną należy postrzegać jako konflikt, w którym informacja jest zasobem, obiektem ataku i zarazem bronią, obejmując fizyczne niszczenie infrastruktury wykorzystywanej przez przeciwnika do działań operacyjnych. Zob., K. Liedel, P. Piasecka, T. R. Aleksandrowicz*, Analiza informacji. Teoria i Praktyka,* Difin SA, Warszawa 2012, s. 19.



Źródło: https://www.pwc.pl/pl/publikacje/PwCCrime_Survey_2011.pdf [dostęp: 22.02.2014].

Rys. 1. Zagrożenia dla organizacji działających w cyberrzeczywistości

Największy niepokój polskich przedsiębiorców w odniesieniu do cyberprzestępczości wywołują zagrożenia kradzieży własności intelektualnej, w tym kradzieży danych, kradzieży lub utraty danych osobowych, przerwy w świadczeniu usług, a także zagrożenie utraty reputacji, straty finansowe.



Źródło: http://www.deloitte.com/view/pl_PL/pl/dla-prasy/Raporty/, [dostęp: 10.01.2014].

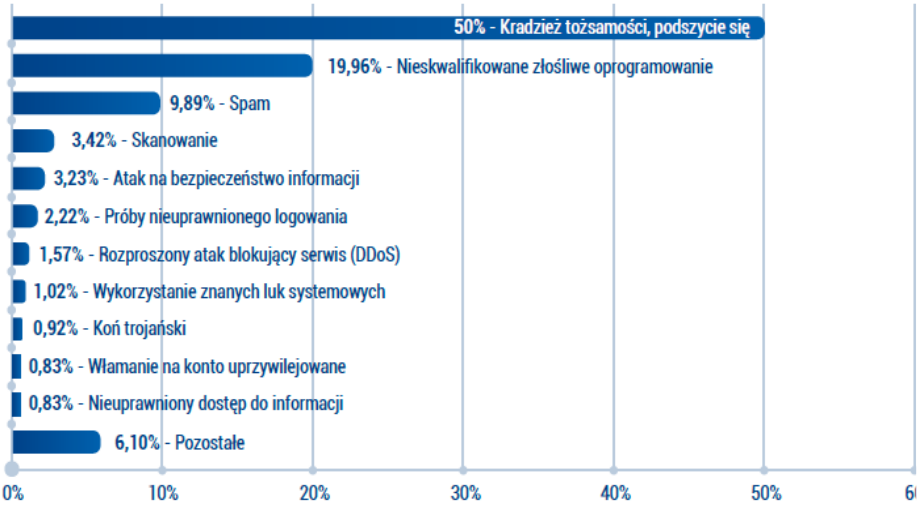
Rys. 2. Niepokój polskich przedsiębiorców w odniesieniu do cyberprzestępczości

Skalę zagrożeń bezpieczeństwa informacyjnego we współczesnej organizacji, które mogą skutkować utratą zasobów informacyjnych podmiotu obrazują wyniki raportu CERT[83] za rok 2012 w zakresie, na jaki pozwala

[83] CERT Polska (Computer Emergency Response Team Polska (http://www.cert.pl/) jest zespołem działającym w ramach Naukowej i Akademickiej Sieci Komputerowej

warunek ograniczenia tematyki opracowania jedynie do zasygnalizowania najważniejszych treści.

W roku 2012 najwięcej odnotowanych przez CERT incydentów dotyczyło przestępstw komputerowych określonych jako kradzież tożsamości i tzw. podszycie się, a także dokonanych przy użyciu złośliwego oprogramowania.



Źródło: http://www.cert.pl/PDF/Raport_CP_ 2012.pdf, s. 31, [dostęp: 28.01.2014].

Rys. 3. Rozkład procentowy podtypów incydentów

Jednym z najważniejszych zagrożeń w obszarze bezpieczeństwa informacyjnego w roku 2012, według raportu CERT, była seria ataków na serwisy rządowe, związanych z protestami przeciwko zapowiedziom podpisania przez Polskę porozumienia ACTA.

Do ataków tych nawoływała za pośrednictwem mediów społecznościowych grupa Anonymous Polska, nakłaniając do blokowania dostępu do witryn resortów odpowiedzialnych za prace nad ACTA, czyli Ministerstwa Administracji i Cyfryzacji, Ministerstwa Spraw Zagranicznych, Sejmu RP i Kancelarii Premiera.

O realnym wymiarze zagrożenia wyciekiem danych świadczą odnotowane w grudniu 2013 roku w prasie krajowej doniesienia, iż *dane setek*

(http://www.nask.pl/) zajmującym się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie. Zobacz szerzej: *Analiza incydentów naruszających bezpieczeństwo teleinformatyczne,* http://www.cert.pl/PDF/Raport_CP_ 2012.pdf, s. 32-40, [dostęp: 28.01.2014].

tysięcy użytkowników firmy Orange można było kupić w Internecie od kilku miesięcy[84].

Kradzieży danych dopuścił się jeden z pracowników firmy zewnętrznej, która wykonywała prace na rzecz Orange Polska. W momencie zatrzymania pracownik ten miał przy sobie laptop i inne nośniki zawierające skradzione dane, takie jak imiona i nazwiska, numery telefonów, PESEL, NIP i numery dokumentów tożsamości oraz adresy tradycyjne i e-mail.

Z kolei lekceważenie wewnętrznych procedur organizacji było przyczyną utraty danych trzech tysięcy klientów przez koncern Virgin Media (rok 2008). Pracownik koncernu zgubił płytę CD z niezaszyfrowanymi danymi dotyczącymi nowych klientów, a rzecznik Virgin Media przyznał, iż transport niezaszyfrowanych danych na dysku CD był wyraźnym naruszaniem zasad firmy[85].

Należy także zwrócić uwagę na przypadek nieuprawnionego ujawnienia tajnych informacji odnotowany przez media brytyjskie, który poruszył środki przekazu w roku 2008:

Podróże pociągami muszą wprowadzać brytyjskich urzędników w bardzo beztroski nastrój. (…) pisaliśmy o supertajnych dokumentach brytyjskiego rządu, dotyczących Iraku i Al-Kaidy, które znaleziono w pociągu podmiejskim w Londynie. Zostawił je tam (…) wysoki rangą przedstawiciel rządu (…). Tego samego dnia zgubiono drugi komplet tajnych dokumentów(…). W dokumentach można między innymi wyczytać jak system bankowy może być wykorzystany do finansowania programu budowy broni masowego rażenia w Iranie (…)[86].

Przykładem nieuprawnionego ujawnienia informacji (rok 2013) jest postępowanie zainicjowane zawiadomieniami szefa Centralnego Biura Antykorupcyjnego: *Prokuratura Okręgowa w Lublinie zdecydowała się wszcząć śledztwo po doniesieniu szefa CBA w sprawie „bezpieczeństwa funkcjonariuszy oraz Biura". (…) Chodzi o bezprawne ujawnienie informacji, które uzyskało się w związku z pełnioną funkcją czy wykonywaną pracą*[87].

Kolejny incydent to umorzone w roku 2013 postępowanie *dotyczące ewentualnego ujawnienia – w postaci przecieku do mediów – informacji ze śledztwa w sprawie domniemanych tajnych więzień CIA w Polsce. Jak wyjaśnił (…) naczelnik wydziału śledczego Prokuratury Okręgowej*

[84] http://www.tvn24.pl/lodz,69/zarzuty-ws-kradziezy-danych-setek-tysiecy-klientow-orange,380344.html, [dostęp: 27.01.2014].

[85] http://www.theregister.co.uk/2008/06/20/virgin_media_banking_loss/, [dostęp: 27.01.2014].

[86] http://wiadomosci.dziennik.pl/swiat/artykuly/77131,tajne-do-wgladu-tylko-w-pociagu.html, [dostęp: 27.01.2014].

[87] http://m.wiadomosci.gazeta.pl/wiadomosci/1,117915,13257248,Jest_sledztwo_ws__ujawnienia__Gazecie_Wyborczej__niejawnych.html, [dostęp: 28.01.2014].

w Gdańsku, w śledztwie badano sprawę (…) wykorzystania informacji niejawnych o klauzuli „tajne" lub „ściśle tajne"[88].

Przestępstwa komputerowe, niekontrolowany rozwój nowoczesnych technologii: o takich zagrożeniach świadczą incydenty ujawnione przez Adobe, firmę o zasięgu globalnym, oferującą rozwiązania i produkty cyfrowe dla biznesu i osób fizycznych:

Zespół ds. zabezpieczeń firmy Adobe wykrył niedawno złożone ataki na naszą sieć, obejmujące między innymi nielegalny dostęp do informacji o klientach oraz do kodu źródłowego wielu produktów Adobe. Przypuszczamy także, że włamywacze usunęli z naszego systemu dane odnoszące się do 2,9 miliona klientów Adobe. Są to nazwiska klientów, zaszyfrowane numery kart kredytowych i płatniczych, daty ważności i inne dane dotyczące zamówień klientów[89].

W USA jednym z największych przestępstw (w opinii mediów) był atak na dane gromadzone w firmie Global Payments. Hakerzy wykradli dane około 1,5 miliona kart. Global Payments obsługiwało wszystkie największe koncerny produkujące karty kredytowe, w tym VISA, American Express, MasterCard. Według wstępnych informacji, problem wycieku danych miał dotyczyć jedynie mieszkańców Stanów Zjednoczonych, jednak dalsze zgłoszenia od osób poszkodowanych, których danych użyto do dokonania transakcji bez ich wiedzy świadczyły, iż przestępstwo miało zasięg globalny[90].

Incydentem, który miał miejsce w roku 2013 i był szeroko komentowany w środkach masowego przekazu stanowi przypadek wykradzenia przez hakerów ze znanej międzynarodowej grupy Anonymous danych z Ministerstwa Gospodarki. W sieci można było znaleźć zeskanowane dokumenty, w tym paszporty cudzoziemców zapraszanych do Polski, dane ze skrzynek mailowych pracowników ministerstwa wraz z ich testowymi hasłami, przez co Polska stała się kolejną ofiarą ataku hakerów z tej grupy po Grecji i Organizacji Bezpieczeństwa i Współpracy w Europie[91].

W dzisiejszych czasach, tzw. *zmagania o informacje* są prowadzone w celu pozyskania komercyjnych tajemnic przedsiębiorstw i korporacji prowadzących do wyeliminowania z rynku konkurenta, a walka informacyjna, stanowiąca zagrożenie bezpieczeństwa informacyjnego, może być prowadzona także w skali globalnej[92].

---

[88] http://www.tvn24.pl/pomorze,42/umorzono-sprawe-przeciekow-ws-domniemanych-wiezien-cia,302943.html, [dostęp: 28.01.2014].

[89] http://helpx.adobe.com/pl/x-productkb/policy-pricing/customer-alert.html, [dostęp: 29. 01.2014].

[90] http://natemat.pl/8709,z-globalnej-firmy-wycieklo-1-5-mln-numerow-kart-kredytowych-co-zrobic-kiedy-hakerzy-ukradna-twoje-pieniadze, [dostęp: 27.01.2014].

[91] http://wyborcza.biz/biznes/1106928,14788057,Hakerzy_wykradli_dane_z_Ministerstwa_Gospodarki.html, [dostęp: 27.01.2014].

[92] M. Wrzosek, *Współczesne…*,wyd. cyt., s. 192.

Ujawnienie i wykorzystanie poufnej informacji dotyczącej wyników finansowych przedsiębiorstwa Polskie Górnictwo Naftowe i Gazownictwo (PGNiG) za II kwartał 2008 r. miało wpływ na kurs akcji spółki na Giełdzie Papierów Wartościowych. Opinia biegłego w zakresie obrotu papierami wartościowymi wykazała, iż wykorzystana informacja poufna rzutowała na wysokość kursu akcji PGNiG, a Urząd Komisji Nadzoru Finansowego (UKNF) wszczął z tego tytułu dziesięć postępowań administracyjnych wraz z warszawską prokuraturą, która prowadzi śledztwo w sprawie ujawnienia informacji poufnej dotyczącej wyników finansowych PGNiG. 6 sierpnia 2008 r., na tydzień przed opublikowaniem oficjalnych wyników PGNiG za II kwartał, cena papierów spółki spadła o 7,73 proc. UKNF ustalił, że w tym dnia sprzedający otrzymali tajne informacje, iż wyniki firmy będą gorsze od oczekiwanych. Rozmowy na ten temat prowadziło 18 pracowników firm inwestycyjnych. Zdaniem UKNF większość sprzedających akcje spółki tego dnia stanowili inwestorzy instytucjonalni z 4 grup finansowych, z tego 73,34 proc. łącznego wolumenu sprzedaży akcji spółki stanowiły transakcje na rachunkach jednej grupy finansowej[93].

Za przykład walki informacyjnej można uznać z kolei prowadzone równolegle do działań zbrojnych, w czasie konfliktu między Gruzją i Rosją w 2008 roku, zmasowane ataki na gruzińskie strony internetowe. Po rozpoczęciu działań wojennych, podmieniona została strona prezydenta Gruzji. Następnie ta i wiele innych oficjalnych gruzińskich stron rządowych, policji, agencji prasowych, stacji telewizyjnych, a nawet najpopularniejsze gruzińskie forum hackerskie zostały sparaliżowane atakami przez DDoS (ang. *Distributed Denial of Service* – rozproszona odmowa usługi)[94].

Jak wspomniano w części opracowania poświęconej próbie zdefiniowania zagrożeń bezpieczeństwa informacyjnego, zagrożenia te mogą obejmować obszary odnoszące się także do praw obywatelskich osób lub grup społecznych w postaci m.in. naruszania przez władze prywatności, bezprawne ingerencje służb specjalnych, ograniczenie jawności życia publicznego: *W drugiej połowie 2011 roku koncern Google otrzymał od władz różnych krajów ponad 1000 żądań usunięcia rozmaitych treści z rezultatów wyszukiwań, bądź materiałów wideo z portalu YouTube. Koncern informuje, że wspomniane żądania dotyczyły ok. 12 tys. pozycji – ok. 25 proc. więcej niż w poprzednim półroczu. Wiele z tych żądań dotyczyło wystąpień politycznych. Zagrożona jest wolność słowa, (…) niektóre z tych żądań nadeszły z krajów, których by się o to nie podejrzewało – z zachodnich demokracji*[95].

[93] http://www.wprost.pl/ar/209024/Wyciek-tajnych-informacji-wplynal-na-kurs-akcji-PGNiG/, [dostęp: 27.01.2014].

[94] http://www.cert.pl/news/866 [dostęp: 28.01.2014].

[95] http://www.wprost.pl/ar/328964/Google-wolnosc-slowa-zagrozona-Zachodnie-demokracje-cenzuruja-internet/ [dostęp: 30.01.2014].

Przedsiębiorstwa w odpowiedzi na zagrożenia bezpieczeństwa informacyjnego, których praktyczny wymiar autorka niniejszego opracowania starała się przybliżyć, szkicując powyższe przykłady, podjęły wysiłki, aby wdrożyć i udoskonalić swoje środki zapewnienia bezpieczeństwa informacyjnego, opracowując ogromne ilości zaleceń, norm, technologii powiązanych z bezpieczeństwem informacyjnym.

Wielorakość i niesymetryczność tych rozwiązań przyczyniła się do tego, iż organizacje zaczęły poszukiwać jednorodnego systemu ochrony informacji. W odpowiedzi na te poszukiwania Międzynarodowa Organizacja Normalizacyjna – ISO (International Organization for Standarization) opracowała i wprowadziła normalizację procesów dotyczących bezpieczeństwa informacji w postaci pierwszej wersji normy ISO/IEC 17799, w roku 2007 przemianowanej na normę ISO/IEC/27002, a Polski Komitet Normalizacyjny opublikował zmienioną normę ISO/IEC 17799 pod nazwą PN-ISO/IEC 17799. Norma wspomaga zatem procesy w przedsiębiorstwie, zapewniając realne podniesienie bezpieczeństwa informacji, kładąc nacisk na sferę organizacyjną oraz monitorując obszary szczególnego ryzyka, np. dostęp do informacji, zabezpieczenia na poziomie organizacyjnym, kontrolę zasobów, działanie urządzeń informatycznych, przestrzeganie prawa i obowiązujących procedur, zabezpieczenie fizyczne organizacji i otoczenia[96].

Fizyczny proces budowy i ochrony dostępu do informacji należących do organizacji i jednoczesne zwiększanie świadomości użytkowników co do wartości posiadanych zasobów informacyjnych przedsiębiorstwa to realizowanie polityki bezpieczeństwa informacji[97].

Nie podejmując szczegółowych analiz dotyczących modeli ochrony informacji w organizacji[98] i technicznej strony ochrony danych w przedsiębiorstwie, co wykroczyłoby poza ramy niniejszego opracowania, należy podkreślić, iż świadomość zagrożeń bezpieczeństwa informacyjnego wśród wszystkich pracowników, a w szczególności najwyższej kadry zarządzającej ma kluczowe znaczenie dla skutecznego wdrożenia i przestrzegania zasad określonych w polityce bezpieczeństwa informacji i uzupełniających ją dokumentach, a zachowanie dobrze pojętej czujności wydaje się wpierać wszystkie, najbardziej zaawansowane technologicznie metody zapobiegające utracie informacji.

W świetle powyższych rozważań, w opinii autorki niniejszego opracowania, uzasadnione jest podjęcie problematyki zagrożeń bezpieczeństwa informacyjnego. Należy zatem przyjąć, iż przedmiotem badań w tym przypadku będzie wybrana organizacja postrzegana w kontekście zagrożeń

[96] A. Nowak, W. Scheffs, *Zarządzanie…*, wyd. cyt., s. 36.
[97] Tamże, s. 37-38.
[98] Modele ochrony informacji zostały szczegółowo opisane przez K. Lidermana w cytowanej publikacji.

bezpieczeństwa informacyjnego. Zatem na gruncie dotychczasowych dociekań, analizy literatury przedmiotu i aktywnego uczestnictwa w życiu organizacji, wydaje się zasadne podjęcie badań, których celem jest rozwinięcie i uzupełnienie charakterystyki oraz specyfiki zagrożeń bezpieczeństwa informacyjnego w organizacji. Osiągnięcie tak określonego celu teoretycznego winno przyczynić się do realizacji celu praktycznego, jakim będą praktyczne rozwiązania w zakresie zapewnienia optymalnego poziomu bezpieczeństwa informacji w organizacji.

Sytuacja problemowa, której próbę zarysowania przedstawia niniejsze opracowanie, przedmiot badań i cel określają główny problem badawczy, sprowadzający się do odpowiedzi na pytanie: jakie zagrożenia bezpieczeństwa informacyjnego występują we współczesnym przedsiębiorstwie i jakie działania zmierzające do ich minimalizacji można zaproponować w organizacji? Ze względu na złożoność problemu głównego pomocne staje się sformułowanie celów szczegółowych, prowadzących do odpowiedzi na pytania: jaka jest rola informacji we współczesnym przedsiębiorstwie? Jak rozumieć pojęcie bezpieczeństwa informacyjnego? Na czym polega specyfika zagrożeń bezpieczeństwa informacyjnego? Czy pracownicy, a szczególnie kadra zarządzająca mają świadomość zagrożeń, jakie niesie utrata informacji? Czy polityka bezpieczeństwa, w obszarze bezpieczeństwa informacyjnego, jest częścią całej polityki zarządzania firmą, czy obowiązkiem formalnym i dokumentem opracowywanym jedynie na potrzeby spełnienia wymogów prawa?

W opinii autorki niniejszego opracowania na podstawie obserwacji aktywności gospodarczej wybranych organizacji, mimo realnych zagrożeń bezpieczeństwa informacyjnego i często wyraźnej obecności polityki bezpieczeństwa w obszarze zarządzania całym przedsiębiorstwem, obszar bezpieczeństwa informacyjnego jest „złem koniecznym" opracowywanym doraźnie na potrzeby spełnienia wymogów organów kontrolnych, a polityka bezpieczeństwa informacji ogranicza się tylko do powierzenia określonych obowiązków wybranym pracownikom np. ochrony fizycznej.

Podsumowanie

Gwałtowny postęp cywilizacyjny, powstanie zbiorów olbrzymich zasobów informacji oraz rozwój środków komunikowania jako zjawiska charakterystyczne dla czasów nam współczesnych[99], niosą szczególne zagrożenia dla bezpieczeństwa informacyjnego, a katalog tych zagrożeń jest katalogiem otwartym, gdyż wraz z rozwojem społeczeństwa informacyjnego pojawiają się nowe możliwości i wyzwania.

[99] M. Wrzosek, *Współczesne…,* wyd. cyt., s. 179.

Zagrożenia bezpieczeństwa informacyjnego jest definiowane w różnorakich obszarach zagrożeń, szczególnie wyraźnie w obszarze zagrożeń technologicznych jako następstwo rozwoju technologicznego, jednak choć to systemy informatyczne przetwarzają dane, człowiek bogaty w wiedzę, ale przecież niedoskonały, stwarza potencjalne zagrożenie dla bezpieczeństwa informacyjnego.

Umiejscowienie zagrożenia, w tym zagrożenia informacyjnego, w sferze świadomości podmiotu skłania do postawienia pytań o stopień odbierania pewnych zjawisk przez ten podmiot i o określenie, czy wszystkie zjawiska zagrażające bezpieczeństwu informacyjnemu istotnie są zagrożeniem, czy może jedynie biznesowym wyzwaniem.

Zagrożenia bezpieczeństwa informacyjnego są zagrożeniami realnymi, obecnymi w codziennej rzeczywistości życia podmiotu, zatem rozpoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego staje się nieodzowne do zapewnienia przewagi konkurencyjnej organizacji, płynności finansowej, rentowności, pozostawania w zgodzie z literą prawa.

Bibliografia

1. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.
2. Janczak J., *Zakłócenia informacyjne*, AON, Warszawa 2001.
3. Kodeks Karny Dz. U. 1997 nr 88 poz. 553 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny.
4. Konieczny J., *Wprowadzenie do bezpieczeństwa biznesu*, Konsalnet, Warszawa 2004.
5. Kowalkowski S. (red.), *Niemilitarne zagrożenia bezpieczeństwa publicznego,* AON, Warszawa 2011.
6. Koziej S., *Teoria sztuki wojennej*, Bellona, Warszawa 2011.
7. Lent B., *Bezpieczeństwo w telekomunikacji i teleinformatyce,* BBN, Warszawa 2002.
8. Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.
9. Liedel K., Piasecka P., Aleksandrowicz T. R., *Analiza informacji. Teoria i Praktyka.* Difin SA*,* Warszawa 2012.
10. Liedel K., Piasecka P., Aleksandrowicz T. R. (red.), *Bezpieczeństwo w XXI wieku. Asymetryczny świat,* Difin SA, Warszawa 2011.
11. Łoś-Nowak T., *Bezpieczeństwo*, [w:] Antoszewski A., Herbut R. (red.), *Leksykon politologii*, Alta2, Wrocław 2003.
12. Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Oficyna Współczesna, Poznań 2004.

13. Nowak A., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Difin SA, Warszawa 2011.
14. Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa 2010.
15. Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji*, Helion, Gliwice 2012.
16. Sun Tzu, *Sztuka wojenna*, przeł. Robert Stiller, Vis-a-Vis Etiuda, Kraków 2011.
17. Sutton R. J., *Bezpieczeństwo telekomunikacji*, przeł. G. Stawikowski, Wydawnictwo Komunikacji i Łączności, Warszawa 2004.
18. *Świat w 2025. Scenariusze Narodowej Rady Wywiadu USA*, Alfa Sagittarius, Kraków 2009.
19. Ustawa z 29 września 1994 r. o rachunkowości (Dz. U. z 2009 r. nr.152, poz.1223 z póz. zm.).
20. Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182, poz.1228).
21. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (Dz. U. 1997 nr 133 poz. 883).
22. Wrzosek M., *Dezinformacja – skuteczny element walki informacyjnej*, Zeszyty Naukowe AON nr 2(87), Warszawa 2012.
23. Wrzosek M., *Polska, Unia Europejska, NATO wobec wyzwań i zagrożeń*, AON, Warszawa, 2012.
24. Wrzosek M., *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010.
25. Wrzosek M., *Współczesne zagrożenia w obszarze bezpieczeństwa europejskiego,* Wydawnictwo Menedżerskie PTM, Warszawa 2013.
26. Zięba R. (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.
27. Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000.
28. Żukrowska K. (red.), *Bezpieczeństwo międzynarodowe. Przegląd aktualnego stanu*, IUSatTAX, Warszawa 2011.

Strony internetowe

1. http://helpx.adobe.com/pl.
2. http://kbn.icm.edu.pl.
3. http://m.tokfm.pl.
4. http://m.wiadomosci.gazeta.pl.
5. http://natemat.pl.
6. http://wiadomosci.dziennik.pl.
7. http://www.cert.pl.

8. http://www.pkn.pl/.
9. http://www.rmf24.pl.
10. http://www.rp.pl.
11. http://www.spbn.gov.pl/.
12. http://www.theregister.co.uk.
13. http://www.tvn24.pl.
14. http://www.wprost.pl.
15. http://wyborcza.biz.

ABSTRACT
THREATS TO INFORMATION SECURITY

The article presents information security problems in an organization. As the importance of information is growing in the contemporary world, and the fact that it is accompanied by the development of information techniques generating new threats connected particularly with the loss of information and its direct negative impact on the entity's security, it seems justified to research this area in order to define and complement characteristic and specific character of information security threats in an organization and present practical solutions to ensure optimal level of information security.