II HETEROGENICZNE ZAGADNIENIA BEZPIECZEŃSTWA

BEZPIECZEŃSTWO INFORMACJI W ORGANIZACJI TYPU PODMIOT PUBLICZNY[1]

Krzysztof SZWARC

Wojskowa Akademia Techniczna

Streszczenie: Celem artykułu jest charakterystyka problemu zapewniania bezpieczeństwa informacyjnego w podmiotach publicznych. Na podstawie analizy aktów prawnych, dokumentów oraz literatury dokonano charakterystyki bezpieczeństwa informacyjnego jako płaszczyzny zapewniania bezpieczeństwa narodowego. Przedstawiono istotę systemowego podejścia do zapewniania bezpieczeństwa informacji w podmiotach publicznych.
Słowa kluczowe: podmiot publiczny, bezpieczeństwo informacyjne, bezpieczeństwo informacji.

Wstęp

Funkcjonowanie systemów działania w otoczeniu warunkuje ich istnienie oraz rozwój. Można dostrzec, że realizacja procesów transformacji wymaga odpowiedniego zasilania materialnego oraz niematerialnego. Występowanie losowo lub celowo zainicjowanych zakłóceń procesów ogranicza wartość systemów, jest przyczyną powstawania sytuacji kryzysowych, a w skrajnych przypadkach likwidacji systemów.

W zależności od przedmiotu działania, w każdym systemie można zidentyfikować newralgiczne funkcje/procesy, a w ślad za tym zasoby niezbędne do właściwego funkcjonowania. Na podstawie analizy definicji „organizacji"[2] oraz praw systemów[3] można przyjąć, że warunkiem koniecznym trwania systemów działania jest istnienie człowieka lub zespołu ludzkiego. Równie ważne dla przetrwania bytów zorganizowanych są zasoby informacyjne, umożliwiające właściwą percepcję, współdziałanie i oddziaływanie w środowisku oraz otoczeniu systemowym.

Informacja to strategiczny zasób w kontekście systemów bezpieczeństwa, którego obiektywna ocena w danym stanie wymaga pełnej wiedzy o istocie zagrożenia. To zasób, który decyduje o efektywności i skuteczności podejmowanych przedsięwzięć,

[1] Ten artykuł został zrealizowany w ramach pracy badawczej Nr RMN 766/2015 prowadzonej na Wydziale Cybernetyki Wojskowej Akademii Technicznej w Warszawie i jest finansowany z tego projektu.

[2] Por. R.W. Griffin, *Podstawy zarządzania organizacjami*, Wyd. Nauk. PWN, Warszawa 2009, s. 5.

[3] J. Konieczny, *Inżynieria systemów działania*, WNT, Warszawa 1983, s. 20-22.

umiejętności dotarcia do pozostałych zasobów, wynikach bitew i wojen. To także produkt stanowiący określoną wartość rynkową, podlegający specjalnej ochronie.

1. Istota bezpieczeństwa informacyjnego

Pomimo różnorodności, człowiek zawsze dąży do realizacji swoich potrzeb. Takie też były motywy tworzenia pierwszych grup i plemion – które z czasem przekształciły się w społeczności lokalne, organizacje czy państwa. Dzisiaj bardzo często mówi się o społeczeństwie informacyjnym, gospodarce opartej na wiedzy, czy kapitale niematerialnym organizacji – wskazując tym samym na szczególne znaczenie informacji jako zasobu niezbędnego do przetrwania i rozwoju[4]. Zakładając zatem, że informacja to zasób o strategicznym znaczeniu dla organizacji, szczególnie istotnym problemem pozostaje kwestia zapewnienia bezpieczeństwa zasobów informacyjnych.

Pojęcie „bezpieczeństwo" jest tradycyjnie definiowane przez pryzmat poczucia bezpieczeństwa oraz pewności – a więc stanów odnoszących się do percepcji otoczenia. Co więcej, można dostrzec relację pomiędzy obiektywnymi oraz subiektywnymi przesłankami postrzegania bezpieczeństwa podmiotu, implikującymi obiektywne lub subiektywne postrzeganie bezpieczeństwa (zagrożenia). A zatem:

- stopień spełnienia potrzeby bezpieczeństwa podlega systematycznej ocenie – zarówno przez „konsumentów" tego dobra, jak i podmioty odpowiedzialne za jego zapewnianie;
- wyniki tej oceny mogą być nieadekwatne do stanu zastanego – np. stan fałszywego bezpieczeństwa[5] czy obsesji[6];
- zapewnienie bezpieczeństwa to również działanie ukierunkowane na informowanie – dzięki temu możliwy jest właściwy opis rzeczywistości.

Dlatego istotne jest zwrócenie uwagi na kwestię **bezpieczeństwa informacyjnego**, czyli stanu zaufania (popartego obiektywnymi przesłankami) do dostępności i jakości pozyskiwanej, przechowywanej, wykorzystywanej i przekazywanej informacji. Podmiotem bezpieczeństwa informacyjnego jest zatem pośrednio (w przypadku systemów sterowania) lub bezpośrednio człowiek, którego potrzeba (dostępu do informacji) może być w takim przypadku spełniona[7]. Z przedstawionej definicji wynika, że istotnym atrybutem bezpieczeństwa informacyjnego jest jakość jako funkcja[8]:

[4] A. Toffler, *Trzecia fala*, PIW, Warszawa 1997.

[5] Gdy poziom zagrożenia jest wysoki, lecz nierozpoznany, błędnie interpretowany.

[6] Gdy nieznaczne zagrożenie postrzegane jest jako duże.

[7] K. Liderman, *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012, s. 22.

[8] H. Miller, *The multiple dimension of information quality*, [w:] "Information Systems Management", cz. 13, nr 2, Auerbach Publications, 1996, s. 79-82; B. Stafanowicz, *Informacja*, SGH, Warszawa 2010, s. 93-100.

- relewantności – miara bliskości (trafności) komunikatu ze względu na istotę problemu;
- dokładności – miara precyzji (uszczegółowienia) komunikatu w odniesieniu do jego denotacji;
- aktualności – stopień zbieżności opisywanego oraz rzeczywistego ze względu na zmianę wartości atrybutu komunikatu w czasie;
- spójności – miara zgodności (brak sprzeczności) komponentów komunikatu;
- komunikatywności – dobór adekwatnej treści i formy przekazu do zakresu pojęciowego odbiorcy oraz warunków komunikacji;
- rzetelności – stopień zaufania do wartości przekazu, m.in. ze względu na zachowanie kryteriów bezpieczeństwa czy metodyki gromadzenia i przetwarzania informacji;
- bezpieczeństwa – wynika ze spełnienia kryteriów dostępności, poufności, integralności, a także rozliczalności, autentyczności czy niezawodności.

Należy podkreślić, że scharakteryzowano wybrane kryteria ewaluacji informacji. Wang oraz Strong wymieniają 179 atrybutów jakości informacji, a także dokonują ich hierarchizacji[9].

W ujęciu dynamicznym bezpieczeństwo informacyjne będzie rozumiane przez pryzmat działań, metod i procedur podejmowanych przez uprawnione podmioty w celu zagwarantowania niezagrożonego gromadzenia, przetwarzania i przekazywania informacji w każdej formie. Jak zauważa A. Żebrowski, „jesteśmy świadkami gwałtownego rozwoju potencjałów informacyjnych, co oznacza konieczność poszukiwania odpowiedzi na pytanie: jak skutecznie oddziaływać informacyjnie na przeciwnika, dezorganizować jego systemy informacyjne, przy jednoczesnym zapewnianiu sprawności własnych systemów informacyjnych?”[10].

Zatem determinantą bezpieczeństwa informacyjnego jest **bezpieczeństwo informacji**, czyli poparte obiektywnymi przesłankami poczucie zaufania, że informacje spełniają kryteria poufności (nie będą ujawnione i wykorzystywane przez nieuprawnione osoby), integralności (poprawne, nienaruszone i niemodyfikowane) i dostępności (dla uprawnionych użytkowników zgodnie z warunkami/wymaganiami danego systemu)[11]. Informacja to zasób o szczególnej wartości – a zatem również **obiekt wymagający wyjątkowej ochrony**. To także produkt organizacji stanowiący określoną wartość rynkową. Dlatego umiejętność generowania, gromadzenia,

[9] R.Y. Wang, D.M. Strong, *Beyond Accuracy: What Data Quality Means to Data Consumers*, [w:] "Journal of Management Information Systems", cz. 12, nr 4, Wyd. M.E. Sharpe, 1996.

[10] A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, [w:] „Roczniki Kolegium Analiz Ekonomicznych", nr 29/2013, SGH, Warszawa 2013, s. 458.

[11] ISO/IEC 27000:2014 *Information technology – Security techniques – Information security management systems – Overview and vocabulary,* ISO/IEC, Geneva 2014, pkt 2.33.

przetwarzania, wymiany i bezpiecznego przechowywania informacji zajmuje szczególne znaczenie w systemie zarządzania bezpieczeństwem.

Zapewnienie bezpieczeństwa informacyjnego dotyczy podmiotu. Zakres pojęcia „podmiot publiczny" uściślono w ustawie o partnerstwie publiczno-prywatnym, gdzie przyjęto, że **podmiot publiczny to**[12]:

a) jednostka sektora finansów publicznych[13];
b) inna osoba prawna, o charakterze nieprzemysłowym i niehandlowym, świadcząca usługi publiczne oraz uzależniona od jednostek, o których mowa w pkt. a) w aspekcie:
   – finansowym – przynajmniej 50% lub
   – struktury właścicielskiej – ponad połowa udziałów lub akcji, lub
   – nadzorczym – kompetencje w stosunku do organu zarządzającego lub
   – prawa do powołania co najmniej połowy podmiotów nadzorczych lub zarządzających danym podmiotem;
c) związek podmiotów wymienionych w punktach a) i b).

Zgodnie z ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne[14], zakres ten ogranicza się do wybranych podmiotów (rys. 1).

Organy administracji rządowej, kontroli państwowej i ochrony prawa, sądy, jednostki organizacyjne prokuratury	NFZ, SPZOZ, Spółki wykonujące działalność leczniczą	ZUS, KRUS
Jednostki budżetowe i samorządowe zakładów budżetowych	Organy samorządu terytorialnego i ich organy	Państwowe lub samorządowe osoby prawne – utworzone dla realizacji zadań publicznych oraz Fundusze celowe

Rys. 1. Wybrane kategorie podmiotów publicznych
Źródło: opracowanie własne na podstawie: Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. z 2005 r., nr 64, poz. 565, art. 2

W ten sposób (rys. 1) do katalogu podmiotów objętych zasięgiem ustawy nie zalicza się m.in. przedsiębiorstw państwowych i spółek handlowych, rodzajów służb specjalnych, Kancelarii Sejmu, Senatu i Prezydenta RP, NBP, uczelni publicznych, PAN, TK, SN, NIK, czy KRRiT.

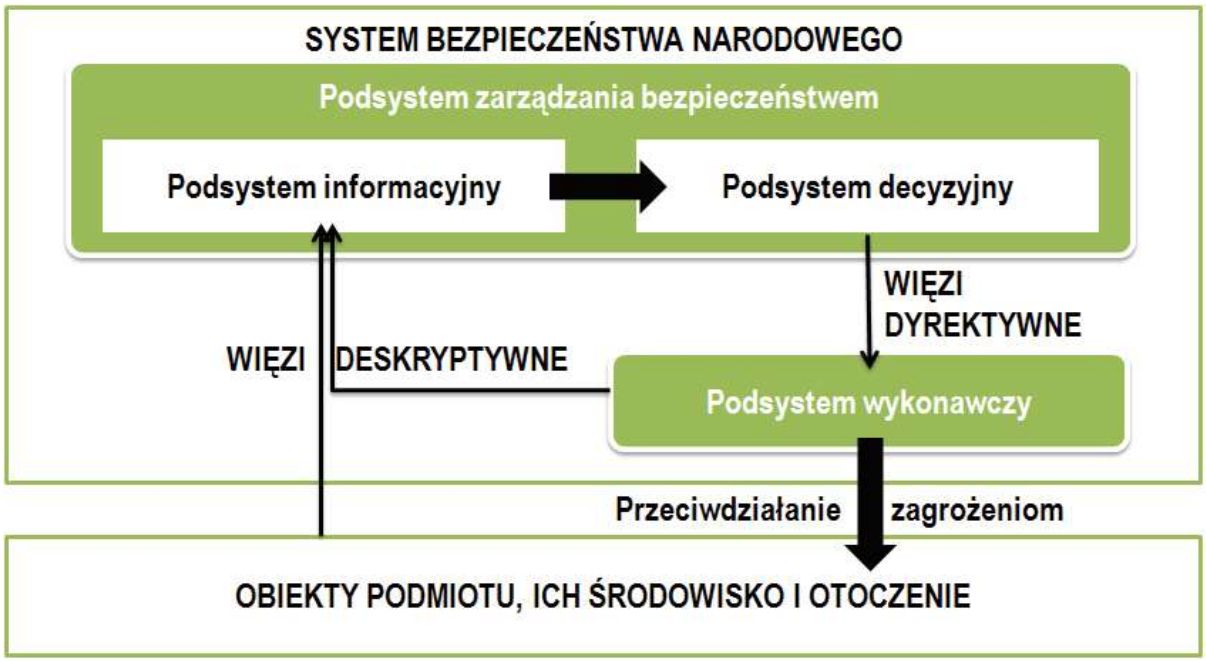
[12] Art. 2, pkt 1 ustawy z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym, Dz.U. z 2009 r., nr 19, poz. 100, z późn. zm.
[13] Zestawienie jednostek sektora finansów publicznych w: ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, Dz.U. z 2009 r., nr 157, poz. 1240-1241, z późn zm., art. 9.
[14] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. z 2005 r., nr 64, poz. 565 z późn. zm.

2. Bezpieczeństwo informacyjne w systemie bezpieczeństwa państwa

Bezpieczeństwo to cecha systemowa analizowana na wielu płaszczyznach. Jako kluczowe uznaje się wymiary: ekonomiczny, militarny i polityczny. Współcześnie eksponowane jest znaczenie bezpieczeństwa informacyjnego ze względu na jego transsektorowy charakter. Warto zauważyć, że każdy podmiot realizujący zadania przetwarza zasoby energetyczne, materialne i informacyjne. Możliwość realizacji zakładanych celów, definiowanych na etapie projektowania systemów działania, wymaga zasilenia w dobra pozyskiwane z otoczenia oraz środowiska organizacji.

Newralgicznym elementem każdej organizacji jest system informacyjny warunkujący kooperację elementów sterowania (kierowania) oraz wykonawczych, a także komunikację z otoczeniem. Przy czym systemy informacyjne można podzielić na[15]:

- naturalne – będące efektem procesów naturalnych, niezależnie od woli człowieka;
- sztuczne – będące wytworem ludzkiej aktywności, tworzone do realizacji procesów informacyjnych w kontekście określonych przedsięwzięć celowych (systemowych).



Rys. 2. Podsystem informacyjny w systemie bezpieczeństwa narodowego
Źródło: opracowanie własne na podstawie E. Kołodziński, *Wspomaganie decyzji w bezpieczeństwi*e, WAT, Warszawa 2014

[15] G. Nowacki, *Znaczenie informacji w obszarze bezpieczeństwa narodowego*, [w:] „Nierówności Społeczne a Wzrost Gospodarczy", zeszyt nr 36, Uniwersytet Rzeszowski, Rzeszów 2013, s. 111.

Realizacja procesów informacyjno-decyzyjnych to podstawowy atrybut systemów bezpieczeństwa narodowego (rys. 2). Co istotne, w strukturze systemu informacyjnego można wskazać pewne newralgiczne elementy umożliwiające generowanie i gromadzenie, a także ich przetwarzanie, zwłaszcza w kontekście procesów decyzyjnych. Zapewnianie ciągłości decyzyjnej, rozumiane jako podstawowe zadanie podsystemu kierowania, w różnych stanach bezpieczeństwa implikuje szczególną potrzebę ochrony informacji, również w warunkach niestabilnych[16]. Dlatego niezależnie od przedmiotu działania (ochrona zdrowia, bezpieczeństwo i porządek publiczny, gospodarka, polityka) dostęp do zasobów informacyjnych spełniających określone kryteria jakościowe warunkuje ciągłość działania systemów bezpieczeństwa.

Sposób realizacji procesów informacyjnych warunkowany jest m.in. aktualnym poziomem rozwoju technologicznego oraz dostępem do usług teleinformatycznych. W dobie „społeczeństwa informacyjnego" trudno wyobrazić sobie funkcjonowanie instytucji państwowych, finansowych, przedsiębiorstw, mediów, służb, inspekcji, straży czy konsumentów bez infrastruktury teleinformatycznej.

Nieprzypadkowo mówi się zatem o piątej przestrzeni pola walki – cyberprzestrzeni[17]. Pojęcie to wprowadzono również do porządku prawnego[18] jako potencjalny obszar zagrożenia dla suwerenności oraz konstytucjonalnego ładu państwa lub grupy państw m.in. w ramach Paktu Północnoatlantyckiego[19]. Z analizy wydarzeń ostatnich lat wynika, że takie działanie jest zasadne (wykres 1). Przejęcie kontroli nad systemami informacyjnymi przeciwnika może być znacznie tańsze oraz bardziej szkodliwe niż agresja militarna.

Zmianie wydaje się również ulegać płaszczyzna działania wywiadu gospodarczego. Nie od dzisiaj formułowane są zarzuty ze strony Stanów Zjednoczonych pod adresem Chińskiej Republiki Ludowej oraz tzw. tygrysów azjatyckich dotyczące wykradania tajemnic wojskowych i gospodarczych.

Bezpieczeństwo informacji to również istotny aspekt bezpieczeństwa wewnętrznego. Warto zaznaczyć, że wiele systemów (i ich elementów) infrastruktury krytycznej, w tym energetycznych, finansowych, transportowych, jest obsługiwanych zdalnie za pomocą sieci słabo zabezpieczonych i niewyodrębnionych ze środowiska sieci powszechnych.

---

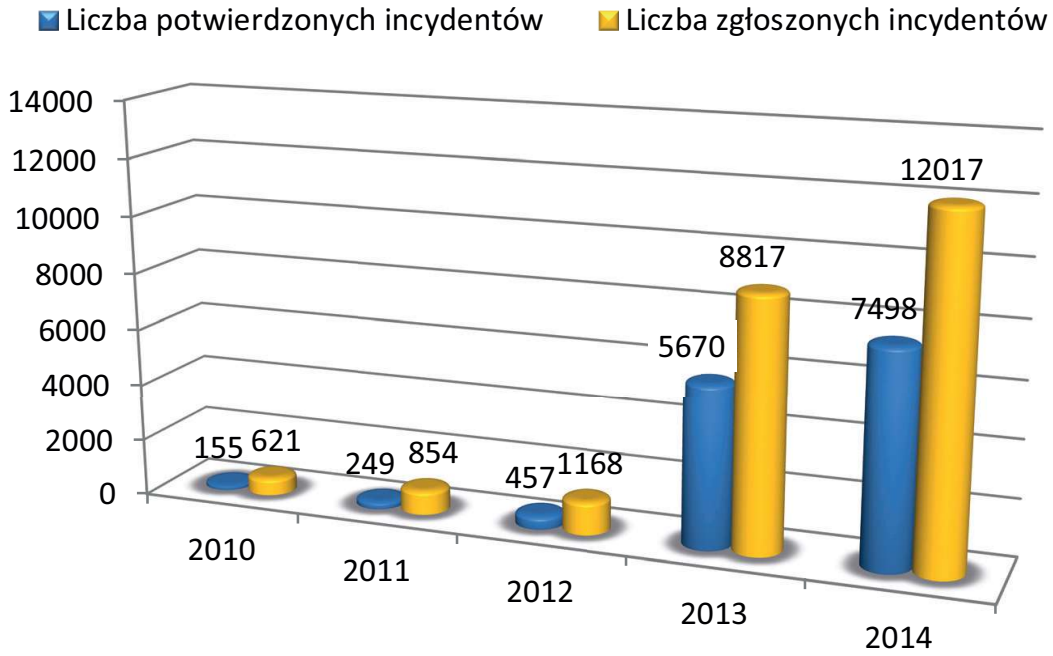
[16] Por. K. Szwarc, P. Zaskórski, *Ciągłość działania systemów zapewniania bezpieczeństwa*, [w:] B. Jagusiak (red. nauk.), *Współczesne wyzwania bezpieczeństwa Polski*, WAT, Warszawa 2015.

[17] Por. C.G. Coleman, *Aggression in Cyberspace*, [w:] S. Jasper (ed.), *Conflict and Cooperation in the Global Commons. A Comprehensive Approach for International Security*, Georgetown University Press 2012, s. 105-118.

[18] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. z 2002 r., nr 156, poz. 1301 z późn. zm.; ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. z 2002 r., nr 113, poz. 985 z późn. zm.

[19] Por. G. Kostrzewa-Zorbas, *NATO in the new strategic environment: cyber attack now covered by article 5 of the North Atlantic Treaty*, „Studia Bezpieczeństwa Narodowego", Zeszyt 6, WAT, Warszawa 2014.

Systemy informatyczne są wykorzystywane do sterowania ruchem w niektórych państwach świata. Powszechne jest również stosowanie informatycznych systemów sterowania ruchem w transporcie powietrznym. Funkcjonowanie gospodarki w środowisku globalnej sieci utrudnia kontrolę w sferze handlu. Może to być wykorzystane do rozwoju nielegalnego obrotu towarami koncesjonowanymi oraz zabronionymi.



Wykres 1. Liczba incydentów dotyczących domen rządowych w latach 2010-2014
Źródło: opracowanie własne na podstawie raportów o stanie bezpieczeństwa cyberprzestrzeni RP z lat 2010-2014. www.cert.gov.pl

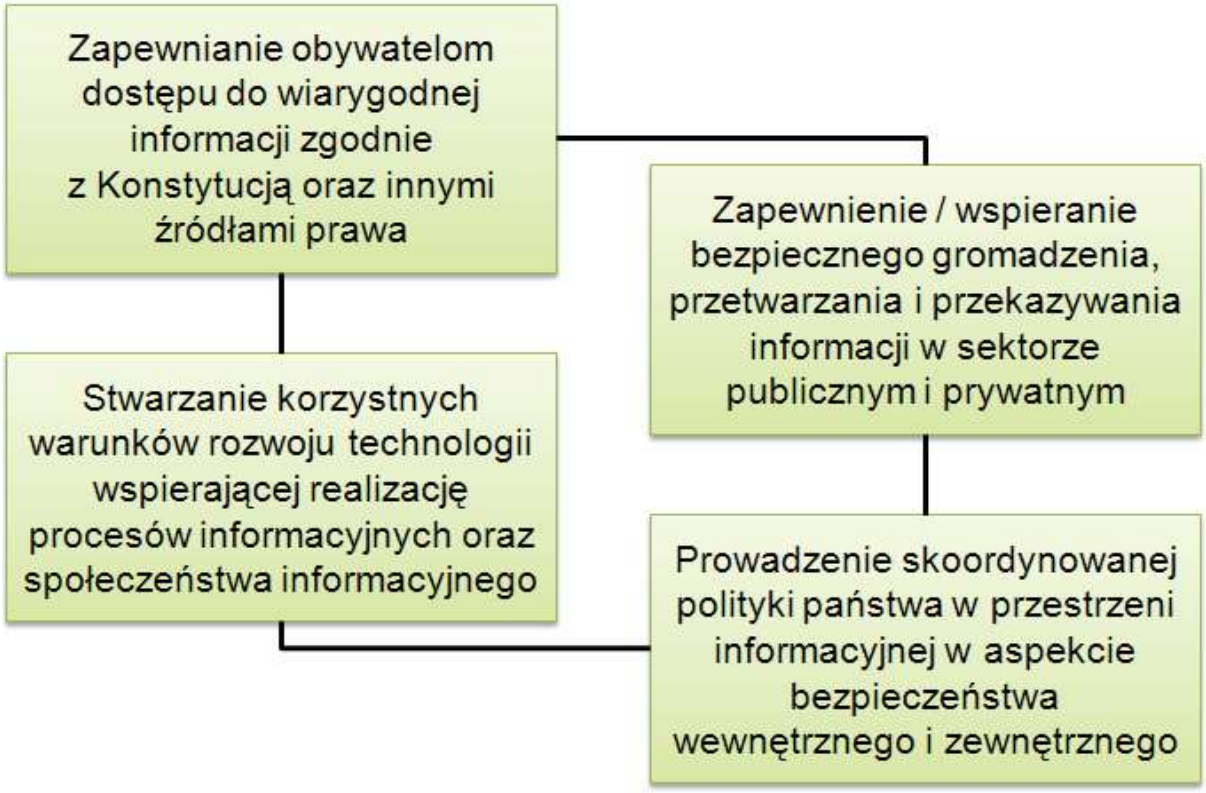
Przejęcie kontroli nad systemami sterowania to niejedyny problem. Istotnym zagrożeniem wydaje się również utrata atrybutu integralności, co może prowadzić do dezinformacji. Przedmiotem ataku mogą być zatem serwisy maklerskie, strony internetowe administracji rządowej i samorządowej, banków, mass media publikujące dane o wskaźnikach gospodarczych czy notowania giełdowe. W takich okolicznościach zagrożenie bezpieczeństwa informacyjnego może doprowadzić do destabilizacji systemu gospodarczego całego państwa. W ten sposób można również wpływać na wizerunek państwa, gdzie faktyczne straty są trudno mierzalne.

Innym istotnym problemem z punktu widzenia bezpieczeństwa personalnego i strukturalnego wydaje się wykorzystanie serwisów społecznościowych bazujących na sieci powszechnej do sterowania zachowaniami na poziomie całych narodów. Takie portale mogą być dzisiaj wykorzystywane zarówno przez organizacje terrorystyczne, jak i służby specjalne do podsycania i stymulowania działań destrukcyjnych poprzez wpływanie na starannie wyselekcjonowane osoby[20]. W ten sposób

[20] *Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013, s. 117.

można mówić o kolejnej płaszczyźnie niewidzialnej wojny – tzw. „intelektualnego terroryzmu".

Ze względu na transsektorowy charakter bezpieczeństwa informacyjnego konieczne jest systemowe podejście do jego zapewniania, wymagające zaangażowania czynnika militarnego oraz pozamilitarnego, zgodnie ze *Strategią bezpieczeństwa narodowego.* Dokumentem tego typu może być *Doktryna bezpieczeństwa informacyjnego*, w której w sposób przejrzysty i spójny powinny zostać zdefiniowane cele (rys. 3), zagrożenia, wyzwania i priorytety w tej dziedzinie, a także koncepcja realizacji.



Rys. 3. Cele bezpieczeństwa informacyjnego w aspekcie narodowym
Źródło: opracowanie własne na podstawie: A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, [w:] „Roczniki Kolegium Analiz Ekonomicznych", nr 29/2013, SGH, Warszawa 2013, s. 460

Współcześnie eksponowanym aspektem bezpieczeństwa informacyjnego jest cyberbezpieczeństwo. Biorąc pod uwagę zakres obu pojęć oraz hierarchię celów systemu bezpieczeństwa, wątpliwości może budzić wcześniejsze opracowanie i zatwierdzenie *Doktryny cyberbezpieczeństwa RP*[21] w stosunku do *Doktryny bezpieczeństwa informacyjnego RP*, której *Projekt* z dnia 24 lipca 2015 r. jest publikowany na stronach BBN.

[21] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, BBN, Warszawa 22 stycznia 2015 r.

W kontekście integracji obu dokumentów w *Projekcie* stwierdza się, że: „W przyszłości należałoby scalić obydwa dokumenty w jeden”[22].

3. Ochrona informacji w organizacji typu podmiot publiczny

Z powyższych przesłanek wynika potrzeba tworzenia zintegrowanego systemu ochrony informacji w organizacjach, którego celem jest zapewnianie realizacji statutowych funkcji podmiotu, również w przypadku wystąpienia incydentów związanych z bezpieczeństwem informacji. W zależności od typu podmiotu, w którym jest wdrażany i utrzymywany, powinno się uwzględniać specyficzne uwarunkowania środowiskowe i otoczenia, w tym prawnego – określające wymagania w stosunku do funkcjonalności projektowanego systemu.

Zakres pojęcia „zintegrowany” odnosi się zatem do trzech kwestii:

- tworzenia systemów wewnętrznie spójnych;
- zgodności systemu zarządzania bezpieczeństwem informacji z pozostałymi systemami związanymi z zapewnieniem bezpieczeństwa organizacji – a zwłaszcza bezpieczeństwa i higieny pracy, zarządzania ryzykiem, kadrami i logistyką;
- zgodności założeń systemu z uwarunkowaniami środowiskowymi i otoczeniem funkcjonowania danego podmiotu – zwłaszcza w aspekcie prawnym i kulturowym.

Kompleksowy system ochrony informacji w organizacji powinien z jednej strony ograniczać możliwość wystąpienia negatywnych zjawisk – poprzez zmniejszanie podatności systemu na zagrożenia, a z drugiej umożliwiać przywracanie zdolności działania – gdy zabezpieczenia okażą się niewystarczające. Poziom bezpieczeństwa podmiotu publicznego będzie warunkowany potencjałem tej organizacji, w tym kadrowym, finansowym, technicznym, infrastrukturalnym, organizacyjnym. Przyjmując, że zagrożenia mogą prowadzić do zmniejszenia wartości zasobów informacyjnych dowolnego podmiotu, działania związane z ograniczeniem ryzyka ich wystąpienia powinny być poparte m.in. rachunkiem ekonomicznym.

Integralnym, a współcześnie kluczowym aspektem bezpieczeństwa informacyjnego podmiotów publicznych jest bezpieczeństwo teleinformatyczne. Za A. Białasem można przyjąć, że **system bezpieczeństwa teleinformatycznego instytucji** to „ogół spójnych środków i skoordynowanych przedsięwzięć zastosowanych w celu zapewnienia właściwego poziomu atrybutów bezpieczeństwa w systemach teleinformatycznych instytucji traktowanych jako całość”[23].

---

[22] *Doktryna bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej. Projekt*, BBN, Warszawa 24 lipca 2015 r., pkt 3.

[23] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2007, s. 183.

W akcie wykonawczym do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne określono Krajowe Ramy Interoperacyjności (KRI) jako wytyczne określające sposób integracji informacyjnej podmiotów publicznych – „zapewniających zdolność (…) do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych”[24]. Można w ten sposób przyjąć, że istotą ustanowienia takiego aktu prawnego było dostosowanie wykorzystywanych systemów do ogólnie uznanych, międzynarodowych standardów bezpieczeństwa informacyjnego – w celu dalszego zwiększania zakresu usług świadczonych drogą elektroniczną zgodnie z *Programem zintegrowanej informatyzacji państwa do 2020 r.*[25]

W dalszej kolejności, w rozdziale IV rozporządzenia[26], definiuje się minimalne wymagania dla systemów teleinformatycznych. Zgodnie z § 20 ust. 1 na podmioty realizujące zadania publiczne nałożono obowiązek tworzenia, wdrożenia i utrzymywania systemów zarządzania bezpieczeństwem informacji, a także sprecyzowano (ust. 2) zakres działań. Przyjęto, że wymagania są spełnione, jeżeli system ten będzie tworzony zgodnie z wytycznymi normy PN-ISO/IEC 27001, a także:

- PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;
- PN-ISO/IEC 27005 – w obszarze zarządzania ryzykiem;
- PN-ISO/IEC 24762 – w odniesieniu do założeń zarządzania ciągłością działania.

W tym aspekcie należy zauważyć, że:

1) normy PN-ISO/IEC 27001:2007 oraz PN-ISO/IEC 27005 zostały zaktualizowane i zastąpione odpowiednio normami PN-ISO/IEC 27001:2014-12 oraz PN-ISO/IEC 27005:2014-01;
2) norma PN-ISO/IEC 17799 została zastąpiona normą PN-ISO/IEC 27002:2014-12.

Z analizy powyższych norm wynika, że projektowanie systemów bezpieczeństwa powinno opierać się na triadzie problemowej: ryzyko – prewencja – terapia (rys. 4)[27]. Zatem system ochrony informacji dla podmiotów publicznych powinien tworzyć

[24] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów…, op. cit., art. 3, pkt 18.

[25] https://mac.gov.pl/files/pzip_ostateczny.pdf - dostęp z dnia 15.10.2015 r.

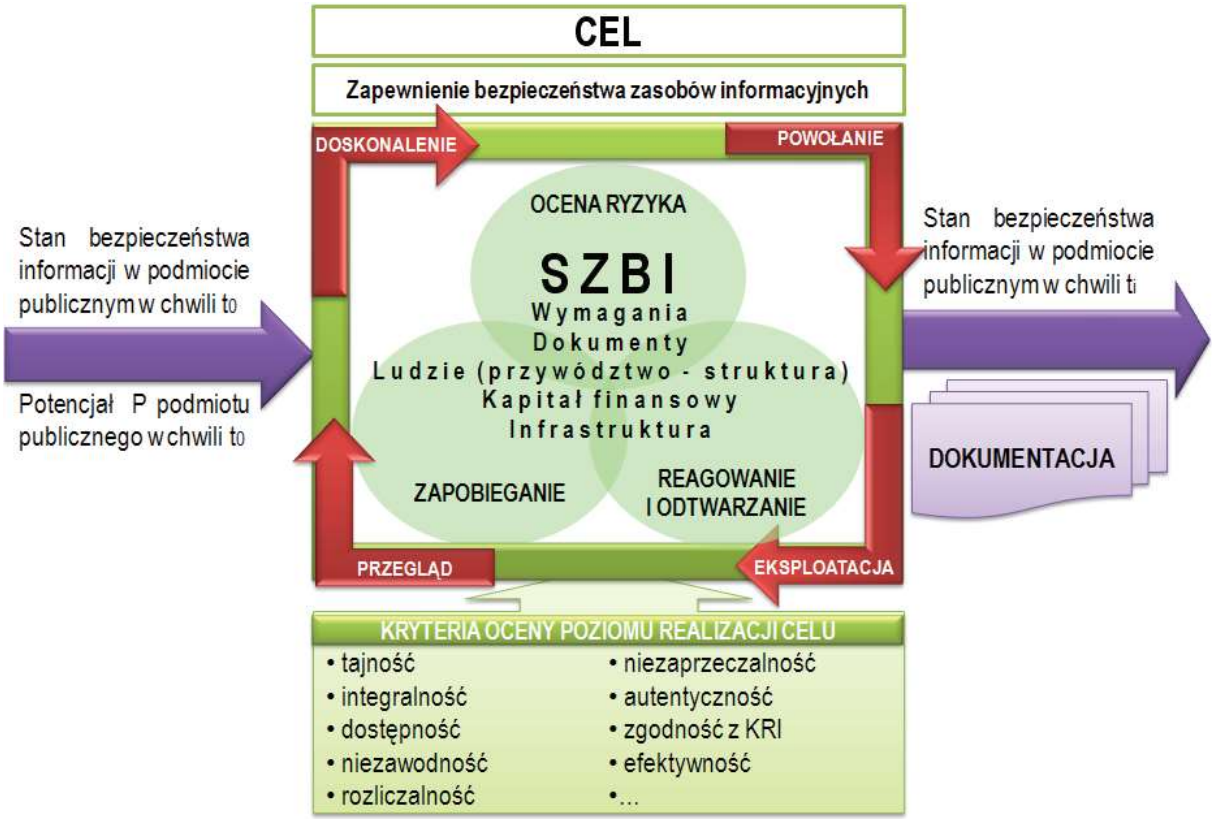
[26] *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*, Dz.U. z 2012 r., nr 0, poz. 526.

[27] J. Zawiła-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, edu-Libri, Kraków 2013.

zintegrowany zbiór rozwiązań prewencyjno-reaktywnych spełniających kryterium **kompleksowości**, rozumianej poprzez[28]:

- wykorzystanie różnych typów zabezpieczeń;
- zapewnienie ciągłości działania w przypadku przełamania części lub wszystkich zabezpieczeń;
- spełnienie warunków spójności i niesprzeczności.

Nadrzędnym kryterium oceny systemu jest skuteczność, rozumiana generalnie jako stopień realizacji zakładanych celów. W tym przypadku chodzi zatem o zachowanie integralności, dostępności i tajności chronionych zasobów w przypadku próby penetracji systemu. Ta zdolność systemu powinna być dowiedziona w oparciu o ocenę *ex ante* (poprzez audyty teleinformatyczne) oraz *ex post* – po wykryciu zakłócenia.



Rys. 4. Model systemu zapewniania bezpieczeństwa informacji
Źródło: opracowanie własne

Zarówno analizowane w tym artykule przepisy prawne, jak i wymogi racjonalnego stawiania zadań oraz kontroli ich realizacji wymagają, aby system bezpieczeństwa

[28] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008, s. 15.

informacji funkcjonował w oparciu o przejrzyste dokumenty (rys. 4). Należą do nich[29]:

- polityka bezpieczeństwa informacyjnego – dokument będący zestawieniem najistotniejszych (ogólnych) zasad i deklaracji najwyższego kierownictwa dotyczących bezpieczeństwa informacyjnego podmiotu. Zawiera m.in. cele tworzenia takiego systemu w organizacji, opis zasobów będących przedmiotem ochrony, zakres kompetencji i odpowiedzialności członków organizacji, które dotyczą bezpieczeństwa informacji, w tym zasad nadawania dostępu do informacji i ich przetwarzania, zasady ochrony i sprawowania kontroli nad tym procesem. Jest to dokument jawny;
- plan bezpieczeństwa informacyjnego – będący dokumentem wykonawczym do polityki, określający przyjętą w podmiocie publicznym koncepcję systemu ochrony informacji wraz z przyjętymi rozwiązaniami osiągania zakładanych celów w ujęciu organizacyjnym, technicznym, fizycznym i prawnym. Istotnym elementem planów są procedury, traktowane jako wzorzec postępowania w kontekście spełnienia określonych przesłanek warunkujących ich wdrożenie;
- instrukcje bezpieczeństwa informacyjnego – czyli dyspozycje przypisywane konkretnym osobom będące uzupełnieniem procedur;
- plany zapewniania ciągłości działania – w których opisany jest sposób postępowania, reagowania oraz odtwarzania realizacji procesów informacyjnych w wypadku występowania ich zakłóceń.

Projektowanie systemu bezpieczeństwa informacji podmiotu publicznego wymaga uwzględniania wymagań normatywnych, w tym zawartych w ustawie o ochronie informacji niejawnej. Stąd wynika obowiązek uwzględniania w dokumentacji systemu[30]:

- szczegółowych wymagań bezpieczeństwa – definiowanych w razie potrzeby we współpracy z ABW lub SKW;
- procedur bezpiecznej eksploatacji.

Konstatując, przyjęto, że:

- zarządzanie bezpieczeństwem zasobów informacyjnych stanowi integralny element ogólnego bezpieczeństwa organizacji;
- jego funkcjonowanie wymaga zabezpieczenia określonego potencjału, a zwłaszcza: kadrowego, finansowego, technicznego, infrastrukturalnego;
- celem systemu jest ochrona informacji gromadzonej, przechowywanej i przetwarzanej w podmiotach publicznych oraz przekazywanej między nimi.

[29] K. Liderman, *Bezpieczeństwo informacyjne*, op. cit., s. 121-136.

[30] Art. 49 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. z 2010 r., nr 182, poz. 1228 z późn. zm.

Zadaniem podmiotów publicznych jest ustanawianie/dostosowanie polityki bezpieczeństwa informacji do zmian powstałych w wyniku wydania rozporządzania oraz jego nowelizacji. Sam kształt i eksploatacja systemu będą warunkowane:

- potencjałem organizacji – stanem i jakością kadry (w tym osób odpowiedzialnych za bezpieczeństwo informacji w instytucji), środkami finansowymi (budżetem instytucji), dostępną infrastrukturą;
- formalnymi wymogami działania – wewnętrznymi i zewnętrznymi;
- stopniem zaangażowania podmiotów odpowiedzialnych za administrowanie daną instytucją w proces zapewniania bezpieczeństwa zasobów informacyjnych.

Istotą tworzenia takich systemów jest ograniczanie ryzyka utraty postulowanych atrybutów informacji oraz zapewnianie „informacyjnej" ciągłości działania[31]. Ograniczanie podatności podmiotów publicznych na zagrożenia wymaga wyboru odpowiedniej strategii postępowania z ryzykiem, która może polegać na:

- akceptacji występowania pewnych zjawisk ze względu na ich znikomą szkodliwość;
- rezygnacji z aktywności/środków realizacji celu – przy założeniu, że ich wycofanie nie obniży (przynajmniej w stopniu znacznym) wartości funkcji celu;
- podejmowaniu przedsięwzięć ukierunkowanych na ograniczanie podatności instytucji na zagrożenia, w wymiarze[32]:
  - ochrony fizycznej – ograniczanie ryzyka bezpośredniego kontaktu z chronionymi zasobami przez nieuprawnione osoby. Działanie w tym zakresie będzie polegało m.in. na analizie i ocenie aktualnego stanu zabezpieczeń oraz ich ewentualnej modyfikacji;
  - ochrony technicznej i logicznej – związanej z utrzymaniem sprawności elementów systemów teleinformatycznych, ze szczególnym uwzględnieniem sprzętu oraz aktualizacji oprogramowania, a także stosowania odpowiednich systemów i programów, w tym aktualizacja oprogramowania, stosowanie mechanizmów kryptograficznych, monitorowanie ruchu w sieciach, tworzenie kopii zapasowych;

[31] Istotne jest podejście holistyczne do oceny bezpieczeństwa informacji. Eksponowane w aspekcie ciągłości działania kryterium dostępności ma znaczenie jedynie wtedy, gdy informacja stanowi wartość, a więc np. nie została celowo zmodyfikowana (integralność) lub ujawniona nieuprawnionym stronom (poufność). Zob. również: P. Zaskórski (red. nauk.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, WAT, Warszawa 2011.

[32] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności…, op. cit. § 20 ust. 2; PN-ISO/IEC 17799: 2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*, PKN, Warszawa 2007; *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Standardy służące zapewnianiu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, RCB, Warszawa 2015.

- ochrony osobowej – ograniczanie ryzyka utraty atrybutów bezpieczeństwa informacji w wyniku szkodliwego działania pracownika organizacji, obejmuje przedsięwzięcia podejmowane od etapu rekrutacji do ustania stosunku pracy, a także doskonalenie ich kompetencji poprzez systematyczne szkolenia;
- ochrony prawnej – związanej ze środowiskiem instytucji (ustanawianie i aktualizacja wewnętrznych regulacji) oraz otoczeniem – w kontekście zawieranych umów (np. dotyczących zakupu lub świadczenia usług przez podmioty zewnętrzne);

– podziale i transferze ryzyka – między innymi poprzez outsourcing wybranych procesów zapewniania bezpieczeństwa oraz ubezpieczeń.

Ponadto istotnym komponentem systemów bezpieczeństwa informacyjnego podmiotów publicznych jest wzmacnianie ich odporności na zakłócenia. Tworzone w tym celu plany ciągłości działania precyzują:

– zasady organizacji i postępowania (reagowania) w sytuacjach kryzysowych;
– plan i procedury przywracania częściowej[33] oraz pełnej funkcjonalności systemu informacyjnego;
– plan i procedury odtwarzania utraconych zasobów informacyjnych.

W tym kontekście ważnym wymogiem jest także definiowanie wymagań bezpieczeństwa informacji dla stanowisk zastępczych – w przypadku niemożności realizacji statutowych funkcji w siedzibie podmiotu. Warto przy tym zauważyć, że narzucony w KRI stopień standaryzacji sprzyja organizacji pracy w lokalizacji zapasowej przy wykorzystaniu potencjału podmiotów, których to rozporządzenie dotyczy.

Sieci teleinformatyczne to istotny komponent infrastruktury krytycznej państwa. Z art. 6 ustawy o zarządzaniu kryzysowym wynika obowiązek ochrony tych systemów poprzez tworzenie planów oraz procedur uruchamianych w sytuacjach kryzysowych oraz utrzymywanie systemów nadmiarowych, wzmacniających ich niezawodność i ograniczających ryzyko zakłóceń. Można domniemywać, że celem ustawodawcy jest ustanowienie realnych zabezpieczeń oraz unikanie niespójności dokumentacji[34].

Eksponowanie kryterium dostępności wymaga zwrócenia uwagi na zjawisko asymetrii informacyjnej, które dotyczy:

– środowiska podmiotów publicznych, gdzie dostęp do repozytorium danych jest uzależniony od pełnionej funkcji[35];
– otoczenia podmiotów publicznych, zgodnie z aktualnym stanem prawnym[36].

[33] Ograniczonej do newralgicznych funkcji systemu.

[34] Art. 6 ust. 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r., nr 89, poz. 590 z późn. zm.

[35] P. Zaskórski (red. nauk.), *Zarządzanie organizacją w warunkach…*, op. cit., s. 162-166.

[36] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997, nr 133, poz. 883 z późn. zm.; Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010, nr 182, poz.

Istotę oraz metody organizacji dostępu do zasobów informacyjnych w sposób wyczerpujący przedstawił K. Liderman[37].

Analizowane w tym artykule restrykcje wzmacniają standaryzację projektowania, ustanawiania oraz wdrażania systemów bezpieczeństwa informacji w instytucjach publicznych. Proces wdrażania wymagań opisanych w rozporządzeniu[38] w urzędach miejskich zbadała w 2014 r. NIK. Zgodnie z opublikowanym raportem zastrzeżenia może/mogą budzić[39]:

- stopień zaangażowania w proces przygotowania podstawowego dokumentu: polityki bezpieczeństwa informacyjnego (w 15 z 24 nie sporządzono dokumentu);
- błędy i braki związane z pisemnymi procedurami zarządzania uprawnieniami dostępu do pracy w systemach informatycznych, polegające m.in. na nieograniczonych możliwościach instalowania dowolnego oprogramowania, a także z wdrażaniem tych procedur (np. aktywne konta byłych pracowników);
- brak odpowiednich wytycznych dotyczących pracy na komputerach przenośnych oraz poprawnego formułowania umów na zakup lub usługi dotyczące sprzętu komputerowego, gwarantujących poufność informacji zawartych w umowach;
- niewykonanie audytu bezpieczeństwa informacji[40] w 9 urzędach.

Należy również odnotować, że:

+ w 19 z 23 podmiotów poprawnie prowadzono inwentaryzację zasobów informacyjnych;
+ w 17 z 24 urzędów zorganizowano szkolenia dotyczące bezpieczeństwa informacji;
+ w 20 z 24 urzędów we właściwy sposób były tworzone, przechowywane oraz testowane kopie zapasowe danych.

Ze względu na liczebność i małe zróżnicowanie próby badawczej prezentowane wyniki w ograniczony sposób umożliwiają dokonanie oceny systemów bezpieczeństwa informacyjnego w podmiotach publicznych. Biorąc pod uwagę konieczność

1228 z późn. zm.

37 Zob. K. Liderman, *Bezpieczeństwo informacyjne*, op. cit., s. 67-127.

38 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności…, op. cit.

39 *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu*, Departament Administracji Publicznej NIK, Warszawa 2015.

40 Czas objęty kontrolą to: 31.05.2012-24.10.2014. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności…, op. cit., audyt powinien być przeprowadzany nie rzadziej niż raz na rok.

doskonalenia systemów bezpieczeństwa, równie istotne wydaje się monitorowanie zmian będących następstwem postępowania kontrolnego.

Podsumowanie

Zapewnienie bezpieczeństwa jest procesem wielowymiarowym oraz uniwersalnym celem każdego systemu działania. Świadomość istnienia źródeł ryzyka, zarówno w środowisku, jak i otoczeniu organizacji, powinna być podstawą do podejmowania racjonalnych przedsięwzięć zmierzających do ograniczania prawdopodobieństwa występowania negatywnych zjawisk, a także ich konsekwencji. Zakres działania analizowanych w artykule podmiotów, zwłaszcza w obszarze szeroko rozumianego bezpieczeństwa narodowego, implikuje potrzebę profesjonalnego podejścia do ich ochrony na wielu płaszczyznach.

W artykule skupiono się na zagadnieniu bezpieczeństwa informacyjnego. Za sprawą powszechnego dostępu do technologii informacyjno-komunikacyjnych (*ICT*) pojęcie to zazwyczaj ograniczane jest do problemu bezpieczeństwa teleinformatycznego. Należy jednak pamiętać, że niezależnie od przyjętego podejścia, zasadniczym przedmiotem ochrony jest informacja – dobro, którego wartość można szacować w ujęciu *ex post* – jako wartość użyteczną informacji w kontekście efektów decyzji oraz w ujęciu *ex ante* – jako zakres wiedzy koniecznej do podjęcia decyzji[41].

Ochrona zasobów informacyjnych jest zespołem przedsięwzięć organizacyjnych, technicznych i formalnoprawnych realizowanych w celu zapewnienia niezakłóconego dostępu do informacji spełniającej określone indywidualnie przez konsumenta wymagania jakościowe. Obowiązujące oraz scharakteryzowane w artykule podstawy prawne należy traktować jako istotny krok w kierunku profesjonalizacji i standaryzacji podejścia do zapewniania bezpieczeństwa informacji przetwarzanej w systemach informatycznych przez podmioty publiczne. To z kolei stanowi przesłankę do wzmacniania ogólnej sprawności systemu, również w warunkach niestabilnych. Potrzeba wzmacniania odporności na zakłócenia wynika bezpośrednio z zapewniania zdolności reagowania na nie zarówno w aspekcie zarządczym, jak i wykonawczym. Dlatego scharakteryzowane w artykule rozwiązania należy oceniać pozytywnie, zwłaszcza w kontekście wzmacniania takich atrybutów jak niezawodność, ryzyko czy ciągłość działania – warunkujących ogólne bezpieczeństwo systemu.

[41] T. Waściński, *Finansowa diagnoza procesów restrukturyzacji przedsiębiorstwa w aspektach ekonomicznej wartości wiedzy*, Dom Wydawniczy Elipsa, Warszawa 2010, s. 31-32.

BIBLIOGRAFIA:

1. *Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013.
2. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2007.
3. Coleman C.G., *Aggression in Cyberspace*, [w:] S. Jasper (ed.), *Conflict and Cooperation in the Global Commons. A Comprehensive Approach for International Security*, Georgetown University Press 2012.
4. *Doktryna bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej. Projekt*, BBN, Warszawa, 24 lipca 2015 r.
5. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, BBN, Warszawa, 22 stycznia 2015 r.
6. Griffin R.W., *Podstawy zarządzania organizacjami*, Wyd. Nauk. PWN, Warszawa 2009.
7. https://mac.gov.pl/files/pzip_ostateczny.pdf (dostęp 15.10.2015).
8. ISO/IEC 27000:2014 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*, ISO/IEC, Geneva 2014.
9. Kołodziński E., *Wspomaganie decyzji w bezpieczeństwie*, WAT, Warszawa 2014.
10. Konieczny J., *Inżynieria systemów działania*, WNT, Warszawa 1983.
11. Kostrzewa-Zorbas G., *NATO in the new strategic environment: cyber attack now covered by article 5 of the North Atlantic Treaty*, „Studia Bezpieczeństwa Narodowego", Zeszyt 6, WAT, Warszawa 2014.
12. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.
13. Liderman K., *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012.
14. Miller H., *The multiple dimension of information quality*, [w:] „Information Systems Management", cz. 13, nr 2, Auerbach Publications, 1996.
15. *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Standardy służące zapewnianiu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, RCB, Warszawa 2015.
16. Nowacki G., *Znaczenie informacji w obszarze bezpieczeństwa narodowego*, [w:] „Nierówności Społeczne a Wzrost Gospodarczy", Zeszyt Nr 36, Uniwersytet Rzeszowski, Rzeszów 2013.
17. PN-ISO/IEC 17799: 2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*, PKN, Warszawa 2007.
18. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2012 r., nr 0, poz. 526.
19. Stefanowicz B., *Informacja*, SGH, Warszawa 2010.
20. Szwarc K., Zaskórski P., *Ciągłość działania systemów zapewniania bezpieczeństwa*, [w:] B. Jagusiak (red. nauk.), *Współczesne wyzwania bezpieczeństwa Polski*, WAT, Warszawa 2015.
21. Toffler A., *Trzecia fala*, PIW, Warszawa 1997.

22. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. z 2005 r., nr 64, poz. 565 z późn. zm.
23. Ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym, Dz.U. z 2009 r., nr 19, poz. 100 z późn. zm.
24. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. z 2002 r., nr 113, poz. 985 z późn. zm.
25. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r., nr 89, poz. 590 z późn. zm.
26. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, Dz.U. z 2009 r., nr 157, poz. 1240-1241 z późn. zm.
27. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997, nr 133, poz. 883 z późn. zm.
28. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. z 2002 r., nr 156, poz. 1301 z późn. zm.
29. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. z 2010 r., nr 182, poz. 1228 z późn. zm.
30. Wang R.Y., Strong D.M., *Beyond Accuracy: What Data Quality Means to Data Consumers*, [w:] „Journal of Management Information Systems", cz. 12, nr 4, Wyd. M.E. Sharpe, 1996.
31. Waściński T., *Finansowa diagnoza procesów restrukturyzacji przedsiębiorstwa w aspektach ekonomicznej wartości wiedzy*, Dom Wydawniczy Elipsa, Warszawa 2010.
32. *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu*, Departament Administracji Publicznej NIK, Warszawa 2015.
33. www.cert.gov.pl (dostęp 20.10.2015).
34. Zaskórski P. (red. nauk.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, WAT, Warszawa 2011.
35. Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, edu-Libri, Kraków 2013.
36. Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, [w:] „Roczniki Kolegium Analiz Ekonomicznych", nr 29/2013, SGH, Warszawa 2013.

INFORMATION SECURITY ISSUE IN PUBLIC INSTITUTIONS

Abstract: Intention of the article is a presentation of the information assurance issue in public entities. The following article is an analysis of the legislation, documents and literature regarding to information assurance as a sensitive domain of current national security assurance. The main focus of the article has been on systemic approach to information security issue in public entities.
Keywords: public entity, information assurance, information security.