sekc. mgr inż. Rafał WRÓBEL
Zakład Analiz Bezpieczeństwa Cywilnego
kpt. dr inż. Paweł GROMEK
mgr inż. Magdalena GIKIEWICZ
Zakład Projektowania Systemów Bezpieczeństwa i Wspomagania Decyzji
Katedra Inżynierii Bezpieczeństwa
Wydział Inżynierii Bezpieczeństwa Cywilnego
Szkoła Główna Służby Pożarniczej

Wybrane podmioty i działania na rzecz bezpieczeństwa informacyjnego w Polsce[1]

Omówienie LEAD

Informacja jest jednym z najważniejszych aktywów każdej organizacji, także organizacji, jaką jest Państwo. Wiąże się z kondycją polityczną, ekonomiczną oraz społeczną. Jej ochrona jest nie tylko potrzeba, ale również wymagana społecznie. Istota informacji sprawia, że podmioty systemu bezpieczeństwa informacyjnego realizują ochronę na różnych płaszczyznach i w różnych formach. Zakres posiadanych kompetencji oraz realizowane działania i aktywności na rzecz bezpieczeństwa informacyjnego wymagają analizy.

Słowa kluczowe: bezpieczeństwo informacyjne, podmioty bezpieczeństwa informacyjnego, działania na rzecz bezpieczeństwa informacji.

1. Wprowadzenie do problematyki bezpieczeństwa informacji

Bezpieczeństwo informacji przybiera na znaczeniu. Jest to szczególnie widoczne na przykładzie kilku ostatnich lat, obfitujących w liczne próby wykradania, zakłócania, i przekształcania informacji, zarówno w odniesieniu do instytucji publicznych, jak i sektora prywatnego. Przykłady ataków na administracje publiczną, w tym naczelne organy państwowe mające miejsce w Argentynie czy Estonii pokazują, że walka o informacje ma nie tylko wymiar stricte fizyczny, związany z jej nieuprawnionym pozyskiwaniem, a oznacza również potrzebę ukazania światu przez wybrane grupy interesariuszy informacyjnego władztwa, potencjalizacji siły.

Termin bezpieczeństwo informacji stosowany zamiennie z pojęciem bezpieczeństwa informacyjnego można interpretować wielorako. Niejednokrotnie,

[1] Artykuł został przygotowany w ramach realizacji projektu pt. System Bezpieczeństwa Narodowego RP nr rej. O ROB/0076/03/001 realizowanego przez konsorcjum naukowo-przemysłowe AON-WSPol-UPH-SGSP-ASSECO i finansowanego ze środków Narodowego Centrum Badań i Rozwoju.

zresztą niesłusznie, w głównej mierze utożsamiany jest z ochroną informacji niejawnych. Świadczyć może o tym definicja P. Tyrały, którego zdaniem bezpieczeństwo informacyjne to „działanie zmierzające do zabezpieczenia zasobów informacyjnych w pamięci komputerów oraz sieciach teleinformatycznych – zbiór reguł i procedur dotyczących bezpieczeństwa informacji"[2]. Zaprezentowane podejście niejako siłą rzeczy zawęża tę kategorię pojęciową jedynie do branży połączonych ze sobą w układzie sieciowym komputerów, w ogóle nie odnosząc jej do bezpieczeństwa narodowego. Tymczasem bezpieczeństwo informacji jest z nim nierozerwalnie związane. Ujęcie tego typu daje się zauważyć chociażby w przyjętej w 2007 roku Strategii Bezpieczenstwa Narodowego Rzeczypospolitej Polskiej, która w rozdziale 3.8. przedstawia koncepcję bezpieczeństwa informacyjnego i telekomunikacyjnego. Zakładała ona zapobieganie próbom destruktywnego oddziaływania na infrastrukturę telekomunikacyjną państwa poprzez redukowanie jej podatności na to oddziaływanie, minimalizowanie skutków ewentualnych ataków oraz przywrócenie w krótkim czasie stanu pełnej jej funkcjonalności. Pomocnym narzędziem w tym celu miały być długofalowe plany ochrony kluczowych systemów teleinformatycznych przed:

- uzyskiwaniem dostępu do danych przez podmioty do tego niepowołane,
- zakłócaniem normalnego ich funkcjonowania,
- kradzieżą tożsamości i sabotażem.

Przywołany dokument zwracał również uwagę na cele, jakim miało służyć zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych, w tym konieczność ochrony informacji niejawnych przetwarzanych drogą elektroniczną oraz konieczność wypracowania przejrzystego mechanizmu zasad dostępu uprawnionych organów państwa do treści przesyłanych droga elektroniczną[3]. Dokument kładł nacisk na konieczność rozwoju środków, narzędzi i technologii służb ustawowo powołanych do zapobiegania zakłóceniom w tym obszarze, jak również zwiększenia zdolności do koordynacji procesów dochodzeniowych w ramach instytucji posiadających elementy rządowej infrastruktury telekomunikacyjnej.

Bezpieczeństwo informacji, będące zdaniem P. Potejko nową dziedziną bezpieczeństwa narodowego, łączy w sobie szereg cząstkowych ujęć, które odnosić należy do narzędzi i procedur ochrony danych, informacji i systemów informacyjnych, a zarazem budzi liczne kontrowersje. Zdaniem przywołanego autora objawiają się one w „zróżnicowaniu pojęciowym". Zidentyfikowane określenia to:

- Bezpieczeństwo informacji – odnosi się do ochrony danych osobowych, ich poufności, informacji niejawnych i informacji strategicznych,
- Cyberbezpieczeństwo – odnoszone do bezpieczeństwa sieci i systemów informacyjnych, nadzoru przepływu danych,

[2] P. Tyrała: Zarządzanie kryzysowe. Ryzyko – bezpieczeństwo – obronność, Toruń 2001, s. 64.
[3] Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczenstwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007, art. 78 i 79.

- Bezpieczeństwo teleinformacyjne – określa ochronę działów strategicznych, zinformatyzowanych, które są osiągalne w wyniku ich alokacji w sieci[4].

Strategiczny Przegląd Bezpieczeństwa Narodowego zorganizowany przez Biuro Bezpieczeństwa Narodowego i będąca jego pokłosiem Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, wskazując rolę bezpieczeństwa informacyjnego państwa precyzują, iż staje się ono nową dziedziną całościowego systemu bezpieczeństwa narodowego. Wspomniana księgą w innym miejscu konstatuje, iż owo bezpieczeństwo:

- wprowadza standardy ochrony danych i informacji oraz dobór środków i parametrów technicznych procesu przetwarzania w zależności od wymaganego stopnia poufności,
- dotyczy także bezpieczeństwa informacji przetwarzanych w strategicznych gałęziach życia kraju, takich jak przemysł, bankowość, telekomunikacja, energetyka oraz ochrona zdrowia[5].

Uczestniczy przeglądu zwracają uwagę na rolę zasobu informacyjnego, kwalifikując go do jednego z najważniejszych aktywów, jakiem dysponuje współczesne państwo. Nierozerwalnie wiąże się on bowiem z kondycją polityczną (w tym polityczno-militarną) i ekonomią państwa oraz jego sferą społeczną. Wzrost znaczenia informacji wiąże się z koniecznością stawiania czoła coraz większej liczbie zagrożeń. Wymaga to od państwa zbudowania kompleksowych pod każdym względem systemów bezpieczeństwa informacji, które pozwolą na niezakłócone gromadzenie, przetwarzanie i dystrybuowanie informacji oraz ochronę przed zagrożeniami cyberprzestrzeni.

Tworzenie polityki bezpieczeństwa informacji jest obowiązkiem jednostek administracji publicznej. Kwestię tą szczegółowo precyzują zapisy *ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne*[6]. Polityka ta powinna zostać sporządzona w formie dokumentu i zawierać ogólne zasady i wymagania, dotyczące tego, w jaki sposób dana jednostka administracyjna będzie chronić informacje, aby nie dostały się w ręce osób nieuprawnionych oraz nie zostały nielegalnie wykorzystane lub zniszczone[7]. Równocześnie polityka bezpieczeństwa informacji powinna opierać się na zasadach: poufności, integralności i dostępności. Poufność sprowadza się do tego, że dane są udostępniane i ujawniane jedynie uprawnionym do tego osobom. Integralność odnosi się do zachowania oryginalności (autoryzacji) danych rzeczywistych, zaś dostępność oznacza, że prawo skorzystania z niej mają uprawnione do tego osoby jedynie w określo-

[4] Por. P. Potejko: Bezpieczeństwo informacyjne, [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.): Bezpieczeństwo państwa, Warszawa 2009, s. 194.

[5] Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, s. 71.

[6] Ustawa z 17 maja 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r., nr 64, poz. 565).

[7] A. Gałach, R. Wójcik: Zarządzanie bezpieczeństwem informacji w sektorze publicznym, Warszawa 2009, s. 1.

nym miejscu i czasie. Wskazane podejście, preferowane przez praktyków sprawia, iż ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania, jawi się w ujęciu negatywnym skoncentrowanym na wyeliminowaniu zagrożenia dla informacji[8]. Zdaniem K. Liedela istnieje jeszcze znaczenie ważniejsze, pozytywne ujęcie bezpieczeństwa, obejmujące kształtowanie pewności przetrwania, posiadania i swobód rozwojowych podmiotu (zapewnienie kreatywnej aktywności podmiotu). W praktyce oznacza ono „wprowadzenie polityki bezpieczeństwa informacyjnego zapewniającej ochronę istniejących systemów, ale również gwarantującej państwu i podmiotom, które chroni, posiadanie, przetrwanie i swobodę rozwoju „społeczeństwa informacyjnego"[9].

2. Podmioty systemu bezpieczeństwa informacyjnego

Wśród podmiotów zajmujących się bezpieczeństwem informacyjnym w pierwszej kolejności należy wskazywać służby specjalne, ustawowo powołane do wykonywania zadań na rzecz pozyskiwania i ochrony informacji kluczowych dla zapewnienia bezpieczeństwa państwa. Jednym z takich podmiotów jest Agencja Bezpieczeństwa Wewnętrznego, znana jako ABW. Agencja Bezpieczeństwa Wewnętrznego jest służbą o szczególnym znaczeniu, toteż jej działalność nadzoruje prezes Rady Ministrów, kontroluje zaś Sejm Rzeczypospolitej Polskiej. Formacja ta została utworzona w celu ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Jej funkcjonowanie określa *ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[10]. Do zasadniczych zadań tej służby w szczególności należy rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w suwerenności i pozycję międzynarodową państwa, niepodległość i jego nienaruszalność jego terytorium oraz obronność państwa. Inne zadania Agencji Bezpieczeństwa Wewnętrznego to:

1. Rozpoznawanie, zapobieganie i wykrywanie przestępstw:
   - szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa,
   - godzących w podstawy ekonomiczne państwa,
   - korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz.U. z 2006 r. nr 216, poz. 1584, z 2008 r. nr 223, poz. 1458 oraz z 2009 r. nr 178, poz. 1375), jeśli może to godzić w bezpieczeństwo państwa,
   - w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,

[8] www.liedel.pl (dostęp: 01.06.2014 r.).
[9] www.liedel.pl (dostęp: 01.06.2014 r.).
[10] Ustawa z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r., nr 29, poz. 154 z późn. zm.).

- nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym oraz ściganie ich sprawców,

2. Realizowanie, w granicach swojej właściwości, zadań służby ochrony państwa oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych,
3. Uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego,
4. Podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

Należy zauważyć, że w uzasadnionych przypadkach (rozpoznawanie, zapobieganie i wykrywanie przestępstw określonych w ustawie o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu w art. 5, ust. 1, pkt 2) działalność Agencji Bezpieczeństwa Wewnętrznego może być prowadzona poza granicami Rzeczypospolitej Polskiej pod warunkiem, wykonywanie przez nią czynności pozostaje w związku z jej działalnością na terytorium państwa.

Organem opiniodawczo-doradczym Rady Ministrów w sprawach programowania, nadzorowania koordynowania działalności Agencji Bezpieczeństwa Wewnętrznego jest Kolegium do Spraw Służb Specjalnych (KdSSS). Szef Agencji Bezpieczeństwa Wewnętrznego jest centralnym organem administracji rządowej, powoływanym i odwoływanym przez Prezesa Rady Ministrów (Premiera). Funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego w ramach obowiązków wynikających ze służby:

- wykonują czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i analityczno-informacyjne,
- w zakresie określonym w Kodeksie Postępowania Karnego (KPK) oraz Kodeksie karnym (KK) wykonują również czynności na polecenie sądu lub prokuratora[11].

Działania Agencji Bezpieczeństwa Wewnętrznego, podobnie jak Agencji Wywiadu wspierane są zarówno przez podmioty sektora publicznego, jak i prywatnego. Organami zobligowanymi do współdziałania z Agencjami, w szczególności do udzielania pomocy w realizacji zadań Agencji są:

- organy administracji rządowej,
- organy samorządu terytorialnego,
- instytucje państwowe,
- przedsiębiorcy prowadzący działalność w zakresie użyteczności publicznej[12].

[11] T. Serafin, S. Parszowski: Bezpieczeństwo społeczności lokalnych. Programy prewencyjne w systemie bezpieczeństwa. Wyd. Difin, Warszawa 2011, s. 140.

[12] Ustawa z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r., nr 29, poz. 154 z późn. zm.), art. 10.

Agencja Bezpieczeństwa Wewnętrznego realizuje bardzo ważne zadania w ramach ochrony infrastruktury krytycznej, szczególnie w przypadku zagrożenia terrorystycznego. Dzieje się tak z uwagi na „posiadanie przez służby specjalne rozwinięte siły i środki służące do identyfikacji zagrożeń intencjonalną działalnością człowieka”[13]. W zaprezentowanym przypadku mają zastosowanie zapisy art. 12a ustawy zarządzaniu kryzysowym, który z jednej strony przedstawia obowiązki Agencji Bezpieczeństwa Wewnętrznego, a z drugiej obowiązki organów administracji publicznej i operatorów infrastruktury krytycznej. W myśl przywołanego artykułu zadania z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym są realizowane we współpracy z organami administracji rządowej właściwymi w tych sprawach, w szczególności z Szefem Agencji Bezpieczeństwa Wewnętrznego. Organy administracji publicznej i operatorzy infrastruktur krytycznych będący w posiadaniu informacji o zagrożeniu terrorystycznym dla tej infrastruktury krytycznej (funkcjonowania systemów i sieci energetycznych, wodnokanalizacyjnych, ciepłowniczych oraz teleinformatycznych ważnych z punktu widzenia bezpieczeństwa państwa), a także działań, które mogą prowadzić do zagrożenia życia lub zdrowia ludzi, mienia w znacznych rozmiarach, dziedzictwa narodowego lub środowiska są zobligowani są do przekazania do przekazania jej Szefowi Agencji Bezpieczeństwa Wewnętrznego. Konieczność eliminowania zagrożeń dla funkcjonowania infrastruktury krytycznej, ochrony życia zdrowia ludzi, mienia na znacznych obszarach, dziedzictwa narodowego i środowiska powoduje, iż Szef Agencji Bezpieczeństwa Wewnętrznego w przypadku podjęcia informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym może udzielać zaleceń organom i podmiotom zagrożonym tymi działaniami oraz przekazywać im niezbędne informacje służące przeciwdziałaniu zagrożeniom. O działaniach tego typu Szef Agencji Bezpieczeństwa Wewnętrznego informuje dyrektora Rządowego Centrum Bezpieczeństwa. Tym samym Agencja Bezpieczeństwa Wewnętrznego swoimi działaniami wpisuje się w każdy z poziomów polskiego systemu ochrony antyterrorystycznej (PSOA):

- poziom strategiczny – realizowany przez Prezesa Rady Ministrów i podległe mu organy oraz instytucje (w tym MSW, ABW, AW),
- poziom wykonawczy – realizowany przez krajowe służby i instytucje uczestniczące w antyterrorystycznej ochronie kraju (m.in. ABW, AW, SG, Policję, Służbę Celną, GIIF, Służbę Więzienną)[14].

Zadania Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa informacyjnego związane są z: prowadzeniem działalności kontrwywiadowczej, zwalczaniem terroryzmu, zwalczaniem przestępstw, zwalczaniem przestępczości

[13] Rządowe Centrum Bezpieczeństwa, Narodowy Program Ochrony Infrastruktury Krytycznej, Warszawa 2013, s. 21.

[14] W. Skomra: Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy. Wyd. Presscom, Wrocław 2010, s. 111.

zorganizowanej, zwalczaniem korupcji, a przede wszystkim ochroną informacji niejawnej. Problematykę tej ostatniej reguluje *ustawa o ochronie informacji niejawnych*[15]. Ustawa ta nakłada na Agencję Bezpieczeństwa Wewnętrznego szereg zobowiązań. Zgodnie z art. 11 Agencja Bezpieczeństwa Wewnętrznego pełni rolę krajowej władzy bezpieczeństwa właściwej do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami i wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego (NATO), Unii Europejskiej (UE) lub innych organizacji międzynarodowych. Funkcję krajowej władzy bezpieczeństwa w stosunkach międzynarodowych w sferze cywilnej (od 2 stycznia 2011 roku) pełni Szef Agencji Bezpieczeństwa Wewnętrznego. W sferze wojskowej funkcję tę sprawuje za pośrednictwem Szefa Służby Kontrwywiadu Wojskowego. Do głównych zadań Szefa Agencji Bezpieczeństwa Wewnętrznego w tym zakresie należy:

- zapewnienie bezpieczeństwa informacji niejawnych międzynarodowych przechowywanych przez instytucje publiczne i inne jednostki organizacyjne, zarówno w kraju, jak i za granicą,
- przeprowadzanie okresowych kontroli stanu zabezpieczenia informacji klasyfikowanych międzynarodowych we wszystkich instytucjach cywilnych i wojskowych,
- wydawanie zgody na ustanowienie (lub likwidację) Kancelarii Tajnych Międzynarodowych,
- współpraca z właściwymi organami bezpieczeństwa struktur międzynarodowych;
- przeprowadzanie czynności sprawdzeniowych w stosunku do podmiotów prowadzących działalność gospodarczą i inną, ubiegających się o uzyskanie kontraktu niejawnego NATO lub UE,
- nadzór nad prawidłowym funkcjonowaniem systemów informatycznych przetwarzających informacje niejawne międzynarodowe[16].

Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego nadzorują funkcjonowanie systemu ochrony informacji niejawnych w odniesieniu do: Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (1); ataszatów obrony w placówkach zagranicznych (2); żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe inne niż wymienione (3) oraz jednostek i osób podlegających ustawie o ochronie informacji niejawnych. W ramach ochrony informacji niejawnych Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego: prowadzą kontrolę ochrony informacji nie-

[15] Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., nr 128, poz. 1228).

[16] Agencja Bezpieczeństwa Wewnętrznego, Krajowa władza bezpieczeństwa – współpraca z NATO i UE, http://www.abw.gov.pl/portal/pl/31/42/Krajowa_wladza_bezpieczenstwa__wspolpraca_z_ NATO _i_UE.html (dostęp: 01.06.2013 r.).

jawnych i przestrzegania przepisów obowiązujących w tym zakresie (1); realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych (2); prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające (3) oraz postępowania bezpieczeństwa przemysłowego (4); zapewniają ochronę informacji niejawnych wymienianych między Rzecząpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi (5); prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych (6). Wymianę informacji niejawnych międzynarodowych między Rzecząpospolitą Polską a wymienionymi stronami regulują wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi z grudnia 2010 roku[17]. Szczególnym podmiotem ochrony bezpieczeństwa informacyjnego strukturalnie ulokowanym w Departamencie Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego jest powołany w pierwszym kwartale styczniu 2008 roku Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL)[18]. Jego podstawowym zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa[19]. Do zakresu świadczonych przez CERT.GOV.PL usług należy:

- koordynacja reagowania na incydenty;
- publikacja alertów i ostrzeżeń;
- obsługa i analiza incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych);
- publikacja powiadomień (biuletynów zabezpieczeń); koordynacja reagowania na luki w zabezpieczeniach;
- obsługa zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV;
- przeprowadzanie testów bezpieczeństwa[20].

Przywołany Departament Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego wraz z Ministerstwem Obrony Narodowej (MON) i Ministerstwem Spraw Wewnętrznych i Administracji (MSWiA) jako pierwszy podjął działania zmierzające do utworzenia właściwej organizacji poli-

[17] http://www.abw.gov.pl/portal/pl/11/7/Ochrona_informacji_niejawnych.html (dostęp: 01.06.2014 r.).

[18] T. Prząda, Powstanie i działalność Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, http://www.secure.edu.pl/historia/2008/docs/Przada.pdf (dostęp: 01.06.2014 r.).

[19] Agencja Bezpieczeństwa Wewnętrznego, Raport kwartalny CERT.GOV.PL, październik–grudzień 2010, www.abw.gov.pl/download/1/875/2011_01_04_Raport_CERT_GOV_PL_za_IV_kwartal_2010.pdf (dostęp: 01.06.2014 r.).

[20] Agencja Bezpieczeństwa Wewnętrznego, Raport kwartalny CERT.GOV.PL, październik–grudzień 2010, s. 2, http://www.abw.gov.pl/portal/pl/236/575/Raporty.html (dostęp: 01.06.2014 r.).

tyki bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej[21]. Pierwszy projekt rządowego programu ochrony cyberprzestrzeni RP na lata 2008–2011 został zaprezentowany w październiku 2008 roku. Główne założenia określały, iż wiodącą rolę w jego realizacji miały spełniać Ministerstwo Spraw Wewnętrznych i Administracji jako organ odpowiedzialny za informatyzację państwa oraz Agencja Bezpieczeństwa Wewnętrznego jako podmiot odpowiedzialny za bezpieczeństwo wewnętrzne państwa[22]. Założenia tego programu przyjęte 9 marca 2009 roku przez Komitet Stały Rady Ministrów zwracały również uwagę na konieczność usprawnienia działań w sferze organizacyjno-prawnej. Główne aktywności w tym zakresie sprowadzały się do:

- wprowadzenia terminologii dotyczącej problematyki ochrony cyberprzestrzeni (cyberterroryzm; cyberprzestępstwo),
- wypracowania podstaw prawych określających obowiązki stron w ramach programu ochrony cyberprzestrzeni RP i teleinformatycznej infrastruktury krytycznej,
- określenia obowiązków sektora prywatnego reprezentowanego przez operatorów infrastruktury krytycznej,
- ustalenia prawnych ram ochrony teleinformatycznej infrastruktury krytycznej,
- ustalania sposobów i form współpracy w zakresie zapobiegania i zwalczania istotnych ataków komputerowych, wspierania działań zmierzających do ustalenia sprawców cyberterroru, itp.,
- prawnego osadzenia Rządowego Centrum Reagowania na Incydenty Komputerowe w Systemie Ochrony Teleinformatycznej Infrastruktury Krytycznej,
- zdefiniowania roli instytucji koordynującej w jednostkach organizacyjnych posiadających zasoby stanowiące elementy infrastruktury teleinformatycznej państwa,
- określenia minimalnych wymagań dla nowo powoływanych administratorów systemu w jednostkach administracyjnych.

W 2010 roku Departament Ewidencji Państwowych i Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji przygotował i przekazał do uzgodnień resortowych rządowy programu ochrony cyberprzestrzeni RP na lata 2011–2016[23]. Długotrwałe konsultacje międzyresortowe spowodowały, iż ciągle ma on status projektu, niemniej jednak jego założenia godne są zwrócenia uwagi. Wśród najważniejszych elementów tego programu znajdowały się:

- zdefiniowanie charakterystyki cyberprzestrzeni,

[21] M. Madej, M. Terlikowski: Bezpieczeństwo teleinformatyczne państwa, Warszawa 2009, s. 136.
[22] Rządowy Program Ochrony Cyberprzestrzeni na lata 2008–2011, s. 6.
[23] Rządowy Program Ochrony Cyberprzestrzeni na lata 2011–2016, Warszawa 2010, wersja 1.1., http://bip.msw.gov.pl/bip/programy/19057,dok.html (dostęp: 01.06.2013 r.).

- wskazanie podmiotów zaangażowanych w działania na rzecz ochrony cyberprzestrzeni,
- przywołanie aktualnie realizowanych inicjatyw podejmowanych na rzecz cyberbezpieczeństwa,
- wprowadzenie programów ochrony w zakresie działań legislacyjnych, proceduralno-organizacyjnych, edukacyjnych, technicznych,
- powołanie Międzyresortowego Zespołu koordynującego ds. Ochrony Cyberprzestrzeni, skupiającego jednostki administracji rządowej,
- określenie zasad współpracy w realizacji programu,
- zasady finansowania programu,
- prowadzenie oceny skuteczności programu.

Jednym z założeń przywołanego rządowego programu ochrony cyberprzestrzeni RP na lata 2011–2016 był rozwój zespołu CERT, prowadzącego konsultacje i doradztwo dla wszystkich podmiotów administracji publicznej oraz przedsiębiorców i innych użytkowników określonych w programie, utrzymującego witryny internetowe, mające docelowo stanowić główne źródła informacji związanych z bezpieczeństwem teleinformatycznym dla szerokiego grona odbiorców, w tym żywo zainteresowanych pracowników administracji publicznej i podmiotów posiadających aktywa uznane za krytyczną infrastrukturę teleinformatyczną.

3. Działania i aktywności o charakterze formalno-prawnym

Podejmowane dotychczas inicjatywy z zakresu ochrony bezpieczeństwa informacyjnego, głównie skupione wokół ochrony informacji niejawnych narażonych na działania użytkowników cyberprzestrzeni wymagają ciągłych usprawnień. Dotyczy to zarówno kwestii prawnych, edukacyjnych, technologicznych, jak również organizacyjnych. Zagrożenia ze strony rozproszonych po całym świecie użytkowników, posiadających różne intencje i reprezentujących odmienne grupy interesów wymagają od państwa rozwiązań kompleksowych. Choć tych ciągle brakuje nieocenione w tym zakresie wydają się być aktywności i działań instytucji ochrony środowiska bezpieczeństwa informacyjnego. Jedną z kluczowych i godnych odnotowania inicjatyw zakończoną sukcesem jest przygotowanie przez Biuro Bezpieczeństwa Narodowego i podpisanie przez Prezydenta Rzeczypospolitej Polskiej ustawy z 30 sierpnia o stanie wojennym oraz o kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[24]. Zakłada ona, możliwość wprowadzenia przez Prezydenta Rzeczypospolitej Polskiej na wniosek Rady Ministrów stanu wojennego na części albo na całym tery-

[24] Ustawa z 30 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2011 r., nr 222, poz. 1323).

torium państwa, w razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji. Wprowadzanie do przytaczanej ustawy definicji cyberprzestrzeni i zdefiniowanie form przeciwdziałania jej skutkom oznacza, że ustawa odnosi się również do pozostałych dwóch stanów nadzwyczajnych (stanu wyjątkowego i stanu klęski żywiołowej) i zakłada możliwość ich wprowadzenia. Stan wyjątkowy może zostać wprowadzony na wniosek Rady Ministrów przez Prezydenta Rzeczypospolitej Polskiej w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych. Stan klęski żywiołowej wprowadzany jest przez Radę Ministrów w celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia. Katastrofę naturalną lub awarię techniczną mogą zaś wywołać również zdarzenia w cyberprzestrzeni oraz działania o charakterze terrorystycznym. Wdrożona zmiana we wszystkich ustawach o stanach nadzwyczajnych w swojej istocie polega więc na rozwinięciu niektórych pojęć, traktowanych przez Konstytucję jako przesłanki wprowadzenia stanu wojennego, stanu wyjątkowego i stanu klęski żywiołowej, dostosowuje się do pojawiających się zagrożeń w obszarze cyberprzestrzeni, mogących mieć bezpośrednie odniesienie do sfery bezpieczeństwa narodowego[25]. Należy w tym miejscu podkreślić, że procesowana ustawa nie jest pierwszym rozwiązaniem prawym odnoszącym się do problematyki cyberprzestrzeni. Ta bowiem znacznie dużej z powodzeniem funkcjonuje w:

- ustawie z 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawie – Kodeks postępowania karnego oraz ustawie – Kodeks wykroczeń[26] (implementacja zapisów Konwencja o cyberprzestępczości z 23 listopada 2001 r.),
- ratyfikowanej przez Polskę umowie między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji o współpracy w zwalczaniu terroryzmu, przestępczości zorganizowanej i innej przestępczości, podpisana w Ankarze 7 kwietnia 2003 roku (Dz.U. z 2005 r. nr 12, poz. 94)[27].

[25] M. Sumański: Uzasadnienie do ustawy z 30 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, www.sejm.gov.pl (dostęp: 01.06.2013 r.).

[26] Ustawa z 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawie – Kodeks postępowania karnego oraz ustawie – Kodeks wykroczeń (Dz.U. z 2004 r., nr 69, poz. 626).

[27] Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji o współpracy w zwalczaniu terroryzmu, przestępczości zorganizowanej i innej przestępczości, podpisana w Ankarze 7 kwietnia 2003 r. (Dz.U. z 2005 r. nr 12, poz. 94).

W tym kontekście nowelizacja ustawy o stanie wojennym ma wprawdzie jedynie charakter uzupełniający, ale stwarza możliwość wprowadzenia stanu nadzwyczajnego w przypadku negatywnej oceny stopnia zagrożenia w sferze zewnętrznego bądź wewnętrznego bezpieczeństwa państwa.

Kolejnym dokumentem o kluczowym znaczeniu dla ochrony bezpieczeństwa informacyjnego w tym przede wszystkim systemu łączności i systemu sieci teleinformatycznych jest przyjęty 26 marca 2013 roku przez Radę Ministrów w formie uchwały Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK). Zgodnie z założeniami ustawy o zarządzaniu kryzysowym Narodowy Program Ochrony Infrastruktury Krytycznej określa[28]:

- narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej,
- ministrów kierujących działami administracji i kierowników urzędów centralnych odpowiedzialnych za systemy infrastruktury krytycznej,
- szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie da funkcjonowania państwa i zaspokojenia potrzeb obywateli.

Podstawowym celem jego utworzenia jest stwarzanie warunków do poprawy bezpieczeństwa infrastruktury krytycznej zwłaszcza w zakresie:

- zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej,
- przygotowania na sytuacje kryzysowe, które mogą niekorzystnie wpływać na infrastrukturę krytyczną,
- reagowania w sytuacji zniszczenia lub zakłócenia infrastruktury krytycznej,
- odtwarzania infrastruktury krytycznej.

Aktem prawnym traktującym o sposobie realizacji obowiązków i współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z operatorami infrastruktury krytycznej oraz innymi organami i służbami publicznymi jest *rozporządzenie Rady Ministrów z 30 kwietnia 2010 roku w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*[29]. Skatalogowaną w jedenastu systemach infrastrukturę krytyczną należy chronić ze względu na jej kluczowy charakter dla gospodarki, bezpieczeństwa państwa, ciągłości działania administracji publicznej i przedsiębiorców, zaś zastosowane środki i formy ochrony uzależnione są od oceny ryzyka zakłócenia lub zniszczenia infrastruktury krytycznej. Pośród rekomendowanych przez Rządowe Centrum Bezpieczeństwa (organ koordynujący krajowe działania na rzecz ochrony infrastruktury krytycznej) form ochrony znajduje się ochrona teleinformatycz-

[28] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r., nr 89, poz. 590 z późn. zm.).

[29] Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. z 2010 r., nr 83, poz. 542).

na, rozumowana jako zespół przedsięwzięć, procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania infrastruktury krytycznej związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych. Stosowanie ochrony tego typu oznacza również ochronę przed cyberatakami, cyberprzestępstwami i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom[30] i w sposób nieunikniony nawiązuje do zapewnienia poufności, integralności i niezawodności danych. Oznacza wszelkie przedsięwzięcia minimalizujące ryzyko „ugodzenia" systemów infrastruktury krytycznej za pośrednictwem infrastruktury teleinformatycznej, zapewnia działania na rzecz przeciwdziałania wirtualnym atakom oraz inną działalnością cybernetyczną rodzącą zaburzenia w funkcjonowaniu infrastruktur krytycznych. Niezwykle cenną inicjatywą Rządowego Centrum Bezpieczeństwa (RCB), i odpowiedzialnego za przygotowanie Narodowego Programu Ochrony Infrastruktury Krytycznej dyrektora RCB, jest opracowanie rekomendacji i dobrych praktyk jako standardów służących zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej stanowiących załącznik nr 2 do programu głównego NPOIK. Wśród zalecanych rozwiązań z obszaru bezpieczeństwa teleinformatycznego znajduje się standard ISO/IEC 17799:2005 opublikowany przez Międzynarodową Organizację ds. Standaryzacji (ISO – International Organisation for Standarisation (ISO) i Międzynarodową Komisję Elektrotechniczną (IEC – International Electrotechnical Comission). Jego polskim odpowiednikiem jest norma z 2007 roku PN-ISO 17799:2007, znana wcześniej jako PN-ISO 17799:2003[31].

W ramach dbałości o systemy infrastruktury krytycznej, państwo sprawuje na nimi opiekę poprzez ministrów – gospodarzy systemów, odpowiedzialnych za nieformalny nadzór i animację działań na rzecz poprawy bezpieczeństwa infrastruktury krytycznej w ramach danego systemu. Minister Administracji i Cyfryzacji odpowiada za systemy i sieci teleinformatyczne administracji publicznej, technologie, techniki i standardy informatyczne oraz realizację zobowiązań międzynarodowych RP w dziedzinie informatyzacji. Są to zadania związane z bezpieczeństwem systemu sieci teleinformatycznych, w ramach systemów infrastruktury krytycznej wymienionych we wspomnianej już ustawie o zarządzaniu kryzysowym. Krytyczna Infrastruktura Teleinformatyczna (KITI) obejmuje systemy i sieci teleinformatyczne niezbędne dla prowadzenia podstawowych działań gospodarczych i funkcjonowania instytucji publicznych państwa[32], a jej ochrona i zwalczanie zagrożeń dla rządowych systemów teleinformatycznych leży także w kompetencji przywoływanej komórki Agencji Bezpieczeństwa Wewnętrznego

[30] Rządowe Centrum Bezpieczeństwa, Narodowy Program Ochrony Infrastruktury Krytycznej, s. 32.
[31] Tamże.
[32] P. Sienkiewicz, W. Błażejczyk, E. Lichocki, M. Jóźwiak, H. Świeboda: Analiza systemowa cyberterroryzmu, [w:] *Zeszyty Naukowe AON* 2006, nr 2, s. 63.

i Agencji Wywiadu[33]. Minister Administracji i Cyfryzacji (właściwy w sprawach informatyzacji) we współpracy z Agencją Bezpieczeństwa Wewnętrznego jest inicjatorem projektu dokumentu pt. Polityka Ochrony Cyberprzestrzeni RP. Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, który kładzie nacisk na wzrost świadomości użytkowników cyberprzestrzeni, przewiduje wspieranie inicjatyw naukowo-badawczych dotyczących bezpieczeństwa teleinformatycznego[34]. W ramach kampanii edukacyjno-prewencyjnej uwzględnia edukację szkolną dzieci i młodzieży mającą na celu ochronę przed zagrożeniami „płynącymi z Internetu". Celem działań zawartych w tym dokumencie jest[35]:

- zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa (w tym Krajowej Infrastruktury Teleinformatycznej),
- zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni,
- zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne,
- określenie podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni,
- stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych.

Zgodnie z założeniami Polityki ochrony Cyberprzestrzeni RP za bezpieczeństwo cyberprzestrzeni RP (CRP) odpowiada Rada Ministrów, a zadania w tym zakresie wykonuje przez Ministra Administracji i Cyfryzacji, Ministra Obrony Narodowej, Ministra Spraw Wewnętrznych, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Służby Kontrwywiadu Wojskowego, inne organy administracji rządowej[36]. W zakresie kompetencji Ministra Administracji i Cyfryzacji leży przyjmowanie sprawozdań organów administracji rządowej podsumowujących oceny ryzyka bezpieczeństwa teleinformatycznego w każdym z sektorów, w którym instytucja działa i za które odpowiada, a także opracowanie „zbiorczego" sprawozdania dla Prezesa Rady Ministrów[37]. W dokumencie uwzględniono także potrzebę stworzenia przez ministra ds. informatyzacji regulacji prawnych zapewniających bezpieczeństwo systemu sieci teleinformatycznych. Określono trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w cyberprzestrzeni. Poziom pierwszy – koordynujący – to minister właściwy ds. informatyzacji. Pozostałe poziomy to: poziom drugi – reagowania

[33] Ustawa z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz.U. z 2002 r., nr 74, poz. 676 z późn. zm.).

[34] https://mac.gov.pl/dzialania/rada-ministrow-przyjela-polityke- ochrony-cyberprzestrzeni-rzeczypospolitej-polskiej/ (dostęp: 01.06.2013 r.).

[35] Polityka Ochrony Cyberprzestrzeni RP (stan na 18 września 2012 r., źródło: http://mac.bip.gov.pl/prawo-i-prace-legislacyjne/polityka-ochrony- cyberprzestrzeni-rp-resortowe-zglaszanie- uwag-do12-10-2012.html).

[36] Tamże.

[37] Tamże.

na incydenty komputerowe (Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL i Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych) i poziom trzeci – poziom realizacji (administratorzy odpowiadający za poszczególne systemy teleinformatyczne funkcjonujące w CBR)[38].

Przywoływany Minister Administracji i Cyfryzacji w ramach kierowania działem administracji rządowej łączność i informatyzacja, nadzoruje m.in. Urząd Komunikacji Elektronicznej (UKE) oraz Pocztę Polską[39]. Sprawy łączności obejmują telefonię stacjonarną i komórkową oraz łącza internetowe. Regulacje istotne z punktu widzenia ochrony infrastruktury krytycznej, które określają zadania ministra ds. łączności wynikają przede wszystkim z ustawy prawo telekomunikacyjne[40] i ustawy prawo pocztowe[41]. Minister właściwy ds. łączności uzgadnia plan działań przedsiębiorcy telekomunikacyjnego[42] w sytuacjach szczególnych zagrożeń, w tym bezpośrednich zagrożeń dla infrastruktury przedsiębiorcy w zakresie dotyczącym[43]:

- utrzymania ciągłości, a w przypadku jej utraty – odtwarzania świadczenia usług telekomunikacyjnych i dostarczania sieci telekomunikacyjnej,
- wykazu elementów sieci telekomunikacyjnej oraz sposobów ich przygotowania do zapewnienia telekomunikacji na potrzeby właściwych podmiotów i służb wraz z procedurami uruchamiania tych elementów,
- procedur współpracy przedsiębiorcy z ministrem właściwym do spraw łączności oraz Prezesem Urzędu Komunikacji Elektronicznej w zakresie sposobów wzajemnego przekazywania informacji, alarmowania i ostrzegania, dotyczących sytuacji szczególnych zagrożeń, a także powiadamiania o konieczności podjęcia lub zaprzestania działań określonych w planie.

Prezes Urzędu Komunikacji Elektronicznej jest organem regulacyjnym w zakresie działalności pocztowej, telekomunikacyjnej i gospodarki częstotliwościowej oraz kontroli spełniania wymagań dotyczących kompatybilności elektromagnetycznej. Ponadto dokonuje analizy i oceny funkcjonowania rynków usług telekomunikacyjnych i pocztowych oraz ma prawo do podejmowania interwencji w sprawach dotyczących funkcjonowania rynku usług telekomunikacyjnych

[38] Tamże.

[39] I. Kulik, R. Wróbel: Rola administracji publicznej w ochronie infrastruktury krytycznej państwa, [w:] Z. Piątek, S. Olearczyk (red.): Przygotowania obronne w działach administracji rządowej. SRWO, Warszawa 2012, s. 171.

[40] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r., nr 171, poz. 1800, z późn. zm.).

[41] Ustawa z 12 czerwca 2003 r. Prawo pocztowe (Dz.U. z 2003 r., nr 130, poz. 1188, z późn. zm.).

[42] Mowa tutaj o przedsiębiorcy ujętym w wykazie stanowiącym załącznik do Rozporządzenia Rady Ministrów z 9 listopada 2007 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym (Dz.U. z 2007 r., nr 214, poz. 1571 z późn. zm.), dla którego organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest minister właściwy do spraw łączności.

[43] Rozporządzenie Rady Ministrów z 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz.U. z 2010 r., nr 15, poz. 77).

i pocztowych oraz rynku aparatury, w tym rynku urządzeń telekomunikacyjnych. Ma także prawo nakładać na przedsiębiorców telekomunikacyjnych ograniczenia niektórych, publicznie dostępnych usług telekomunikacyjnych oraz ograniczenia zakresu lub obszaru eksploatacji sieci i urządzeń telekomunikacyjnych. Ponadto tworzy bazy danych infrastruktury telekomunikacyjnej, która może być wykorzystana na potrzeby systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa (zadanie istotne z punktu widzenia bezpieczeństwa systemu zapewnienia ciągłości działania administracji publicznej).

Ostatnim z dokumentów stanowiących przedmiot analizy niniejszego opracowania jest przygotowana przez Ministerstwo Spraw Wewnętrznych i Administracji Strategia Rozwoju Społeczeństwa Informacyjnego do roku 2013. Jej przygotowanie i wdrożenie pod koniec pierwszej dekady XXI wieku podyktowane było gwałtownym wzrostem znaczenia informacji oraz usług świadczonych drogą elektroniczną, a co za tym idzie wykorzystania technologii informacyjnych i telekomunikacyjnych w wielu obszarach życia, w gospodarce, administracji publicznej, czy w życiu codziennym. Przyjęta w grudniu 2008 roku przez Radę Ministrów w formie uchwały strategia zawierała trzy załączniki dotyczące:

- analizy aktualnej sytuacji w obszarze społeczeństwa informacyjnego w Polsce,
- dokumentów zebrane oraz stworzone podczas dyskusji środowiskowych i tematycznych,
- priorytetów rozwoju społeczeństwa informacyjnego w opinii internatów.

Jej misją było umożliwienie społeczeństwu powszechnego i efektywnego wykorzystania wiedzy i informacji do harmonijnego rozwoju w wymiarze społecznym, ekonomicznym i osobistym. Odpowiedzialność za koordynację i nadzór nad realizacją celów strategii spoczywała na Departamencie Społeczeństwa Informacyjnego ulokowanego w Ministerstwie Spraw Wewnętrznych i Administracji. Kierunki Polski do 2013 roku, określone na podstawie wizji i misji, zostały skatalogowane w trzech obszarach: człowiek – gospodarka – państwo[44]. W zakresie bezpieczeństwa informacyjnego przywołana strategia w głównej mierze odnosiła się do podnoszenia poczucia bezpieczeństwa, wykorzystania technologii informacyjnych i komunikacyjnych oraz zapewnienie bezpiecznej i zorientowane na potrzeby infrastruktury technologii informacyjnych i komunikacyjnych, niezbędnej do rozwoju społeczeństwa informacyjnego. We wrześniu 2012 roku została przyjęta nowa Strategia Rozwoju Kraju do roku 2020[45], w której z kolei duży nacisk kładzie się na wzrost wykorzystania technologii cyfrowych.

[44] Ministerstwo Spraw Wewnętrznych i Administracji, Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013 r., Warszawa 2008.

[45] Uchwała nr 157 Rady Ministrów z 25 września 2012 r. w sprawie przyjęcia Strategii Rozwoju Kraju 2020 (M. P. poz. 882, dn. 22.11.2012 r.).

4. Podsumowanie

W czasach, gdy informacja stanowi kluczowy zasób władzy, ochrona bezpieczeństwa informacyjnego ma szczególne znaczenie. Wspomniany obszar zgodnie z konkluzjami Białej Księgi Bezpieczeństwa Narodowego Rzeczypospolitej Polskie z 2013 roku jako nowa dziedzina całościowego systemu bezpieczeństwa narodowego, w zależności od wymaganego stopnia poufności wprowadza standardy ochrony danych oraz dobór środków i parametrów technicznych. Wśród podmiotów wykonujących działania i aktywności na rzecz bezpieczeństwa informacyjnego znajdują się zarówno przedstawiciele administracji publicznej, służb specjalnych, jak sektora prywatnego. Ochrona bezpieczeństwa informacji niejednokrotnie bowiem wiąże się nie tylko z ochroną przed zagrożeniami, ale również warunkuje rozwój zarówno małych grup, jednostek, a także państwa. Określaniu warunków i ram działalności podmiotów na w tym zakresie służyć mają między innymi programy, polityki i strategie działania stylizowane na te, które stanowiły przedmiot rozważań niniejszego opracowania[46].

Literatura

Akty prawne

[1] Ustawa z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r., nr 29, poz. 154 z późn. zm.).

[2] Ustawa z 12 czerwca 2003 r. Prawo pocztowe (Dz.U. z 2003 r., nr 130, poz. 1188, z późn. zm.).

[3] Ustawa z 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawie – Kodeks postępowania karnego oraz ustawie – Kodeks wykroczeń (Dz.U. z 2004 r., nr 69, poz. 626).

[4] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r., nr 171, poz. 1800, z późn. zm.).

[5] Ustawa z 17 maja 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r., nr 64, poz. 565).

[6] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r., nr 89, poz. 590 z późn. zm.).

[7] Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., nr 128, poz. 1228).

[8] Ustawa z 30 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2011 r., nr 222, poz. 1323).

[9] Rozporządzenia Rady Ministrów z 9 listopada 2007 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym (Dz.U. z 2007 r., nr 214, poz. 1571 z późn. zm.)

[46] Niniejsze opracowanie powstało dzięki uprzejmości Pani Ilony Kulik (AON).

[10] Rozporządzenie Rady Ministrów z 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz.U. z 2010 r., nr 15, poz. 77).

[11] Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. z 2010 r., nr 83, poz. 542).

[12] Uchwała nr 157 Rady Ministrów z 25 września 2012 r. w sprawie przyjęcia Strategii Rozwoju Kraju 2020 (M. P. poz. 882, dn. 22.11.2012 r.).

Publikacje i artykuły naukowe

[13] Gałach A, Wójcik R.: Zarządzanie bezpieczeństwem informacji w sektorze publicznym. Warszawa 2009.

[14] Madej M, Terlikowski M.: „Bezpieczeństwo teleinformatyczne państwa". Warszawa 2009.

[15] Kulik I., Wróbel R.: Rola administracji publicznej w ochronie infrastruktury krytycznej państwa, [w:] Piątek Z., Olearczyk S. (red.): Przygotowania obronne w działach administracji rządowej. SRWO, Warszawa 2012.

[16] Potejko P.: Bezpieczeństwo informacyjne, [w:] Wojtaszczyk A.K., Materska-Sosnowska A. (red.): Bezpieczeństwo państwa. Warszawa 2009.

[17] Tyrała P.: Zarządzanie kryzysowe. Ryzyko – bezpieczeństwo – obronność. Toruń 2001.

[18] Sienkiewicz P., Błażejczyk W., Lichocki E., Jóźwiak M., Świeboda H.: Analiza systemowa cyberterroryzmu. [w:] *Zeszyty Naukowe AON* 2006, nr 2.

[19] Skomra W.: Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy. Wyd. Presscom, Wrocław 2010.

Dokumenty, polityki i strategie

[20] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

[21] Narodowy Program Ochrony Infrastruktury Krytycznej. Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

[22] Polityka Ochrony Cyberprzestrzeni RP (stan na 18 września 2012 r.).

[23] Raport kwartalny CERT.GOV.PL, październik – grudzień 2010.

[24] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku, Warszawa 2013.

[25] Rządowy Program Ochrony Cyberprzestrzeni na lata 2008–2011, Warszawa 2008.

[26] Rządowy Program Ochrony Cyberprzestrzeni na lata 2011–2016, Warszawa 2010, wersja 1.1.

[27] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Biuro Bezpieczeństwa Narodowego, Warszawa 2007.

[28] Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013 r., Warszawa 2008.

[29] Sumański M.: Uzasadnienie do ustawy z 30 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw.
[30] Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji o współpracy w zwalczaniu terroryzmu, przestępczości zorganizowanej i innej przestępczości, podpisana w Ankarze 7 kwietnia 2003 r. (Dz. U. z 2005 r. nr 12, poz. 94).

Strony internetowe

[31] www.liedel.pl
[32] www.abw.gov.pl
[33] www.abw.gov.pl
[34] www.cert.gov.pl
[35] www.secure.edu.pl
[36] www.bip.msw.gov.pl
[37] ww.sejm.gov.pl
[38] www.mac.bip.gov.pl
[39] www.mac.gov.pl

Rafał WRÓBEL
Paweł GROMEK
Magdalena GIKIEWICZ

Selected Entities and Actions for Information Safety in Poland

SUMMARY

Information is one of the most important assets of any organization, including the organization, which is State. Associated with a condition of political, economic and social. Its protection is not only necessary, but also socially required. The essence of this information causes that the entities of system safety information implements protection at different levels and in different forms. The scope of their competences and the actions and activities on the security of the information required analysis.

Keywords: information safety, information safety entities, measures for information safety.