Edyta Szczepaniuk

Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa

78375

AKADEMIA OBRONY NARODOWEJ

Edyta Szczepaniuk

Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa

78375

AKADEMIA OBRONY NARODOWEJ

Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa

AKADEMIA OBRONY NARODOWEJ

Edyta Szczepaniuk

BG-Archiwum AON
nr ewid. 78375

Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa

WARSZAWA 2016

Recenzenci
prof. dr hab. inż. Piotr Sienkiewicz
płk dr hab. inż. Piotr Dela

Projekt okładki
Genowefa Majchrowska

Redakcja
Mikołaj Adamiec-Siemiątkowski

Redakcja techniczna i skład
Małgorzata Gawłowska

Korekta
Małgorzata Sęktas

© Copyright by Akademia Obrony Narodowej 2016

ISBN 978-83-7523-517-3

Sygn. AON 6414/16

Skład, druk i oprawa Akademia Obrony Narodowej
00-910 Warszawa, al. gen. A. Chruściela 103, tel. 261-814-055, tel./fax. 261-813-752
e-mail: wydawnictwo@aon.edu.pl
Zam. nr 611/16

SPIS TREŚCI

WSTĘP

E. Yourdon stwierdził, że *jeśli lata osiemdziesiąte określano mianem dekady jakości, lata dziewięćdziesiąte – jako dekadę produktywności, to pierwsze dziesięciolecie nowego wieku będzie dekadą bezpieczeństwa*[1]. Prognoza autora książki pt. *Wojna na bity* wyraża istotę współczesnego globalnego środowiska bezpieczeństwa. Problematyka bezpieczeństwa cyberprzestrzeni jest obecnie przedmiotem analiz na arenie międzynarodowej, w wielu państwach oraz w instytucjach sektora publicznego i prywatnego.

Administracja publiczna, której jednym z podstawowych celów jest świadczenie usług publicznych, uległa na przestrzeni wieków przeobrażeniom, dlatego jej funkcjonowanie należy rozpatrywać w kontekście zmian i uwarunkowań mających miejsce w jej otoczeniu. Już od momentu ukształtowania pierwszych struktur administracyjnych powstało wiele teorii i doktryn administracji. Obecnie obserwuje się globalny trend związany z przejściem od administrowania do zarządzania sprawami publicznymi.

Współczesne środowisko administracji publicznej w Polsce ukształtowane zostało przez wiele procesów. Zmiany polityczne w Europie, które nastąpiły po upadku Związku Radzickiego, doprowadziły do decentralizacji administracji publicznej. Powstało wiele nowych form współpracy w ramach kontynentów (m.in. Unia Europejska, NAFTA). Aspekty ekonomiczne skłoniły do przekształcenia gospodarki centralnie planowanej w wolnorynkową. Zwrócono uwagę na racjonalizację wydatków publicznych i osiągnięcie efektów ekonomicznych. Wreszcie zdumiewający rozwój technologii, powstanie Internetu oraz proces globalizacji przyczyniły się do niespotykanego dotąd rozwoju komunikacji. Informacja – obok ziemi, pracy i kapitału – została podniesiona do rangi zasobu strategicznego.

Można przyjąć, choć ze świadomością daleko idącego uproszczenia zarysowanych we wstępie zmian zachodzących w otoczeniu administracji publicznej, że wymienione czynniki stały się generatorem powstania społeczeństwa informacyjnego i gospodarki opartej na wiedzy (GOW) oraz przeniesienia większości sfer aktywności ludzkiej do cyberprzestrzeni. Wyłoniła się wówczas koncepcja e-administracji, której istotę najogólniej można określić jako możliwość realizacji online usług administracji publicznej. Jednocześnie od struktur administracyjnych

1 Zob. E. Yourdon, *Wojny na bity*, Warszawa 2006.

zaczęto oczekiwać wysokiej jakości świadczenia usług publicznych, czego wyrazem stało się wdrażanie systemów zarządzania jakością.

Opisane zjawiska odnoszą się nie tylko do administracji, ale szerzej – do funkcjonowania społeczeństw, państw i społeczności międzynarodowej. Infrastruktura krytyczna państw funkcjonująca w oparciu o nowe technologie stała się wrażliwa na różnego rodzaju incydenty bezpieczeństwa. Współczesne państwa, których administracja funkcjonuje na bazie nowoczesnych technologii, stały się wrażliwe na ingerencje zakłócające procesy informacyjne – oraz działające dzięki nim bazy danych, urządzenia i sieci teleinformatyczne. Incydenty te implikują zagrożenia dla bezpieczeństwa narodowego, co w znacznym stopniu uzasadnia potrzebę ich analizy. Przykład ataków cybernetycznych na Estonię w 2007 roku obrazuje skalę możliwych skutków cyberzagrożeń.

Podjęcie problematyki wyrażonej w tytule monografii uzasadnia fakt, że jednym ze współczesnych wymiarów bezpieczeństwa narodowego jest bezpieczeństwo informacyjne. W ostatnich latach obserwuje się wzrost nowych zagrożeń dla bezpieczeństwa instytucji czy krytycznej infrastruktury państwa (KIP). Współcześnie istotnym problem stało się zapewnienie bezpieczeństwa zasobów i systemów informacyjnych. Sprawne funkcjonowanie jednostek sektora publicznego uzależnione jest m.in. od zarządzania bezpieczeństwem informacyjnym na każdym etapie działalności instytucji publicznych. W związku ze wzrostem cyberprzestępczości, przeniesieniem konfliktów do cyberprzestrzeni oraz możliwością wykorzystania jej przez terrorystów, również na arenie międzynarodowej dostrzegalne są tendencje zmierzające do budowy systemu cyberobrony. Jednocześnie należy zaznaczyć, że zagrożenia cyberprzestrzeni państwa mogą być także skutkiem zjawisk losowych (np. huraganu, pożaru), przypadkowych (nieumyślnych, np. błędu pracownika) czy też programowych (np. błędów oprogramowania). Nie brakuje także incydentów związanych z celową, zamierzoną działalnością pracowników na szkodę organizacji (instytucji, firmy).

W literaturze przedmiotu można znaleźć liczne analizy dotyczące ochrony cyberprzestrzeni państwa, które niewątpliwie stanowią oryginalne i wartościowe dzieła. Niemniej jednak trudno natrafić na opracowania zwarte dotyczące bezpośrednio tematu monografii. Bardzo często dotykają one jedynie niektórych fragmentów omawianej problematyki, np. aspektów technicznych, ochrony prawnej, penalizacji przestępstw. Dodatkowo problematyka zarządzania bezpieczeństwem teleinformatycznym struktur administracyjnych jest często analizowana w sposób separujący ją od funkcjonowania instytucji publicznej jako całości bądź też bez uchwycenia relacji między poszczególnymi elementami systemu sektora publicznego i powiązania go z bezpieczeństwem narodowym. Jednakże warto mieć na uwadze, że sektor teleinformatyczny jest współcześnie elementem spinającym wiele obszarów funkcjonowania państwa, wśród których istotne znaczenie należy

przypisać krytycznej infrastrukturze państwowej. Fakt ten ma szczególnie istotne znaczenie w razie rozprzestrzeniania się zagrożenia na zasadzie efektu domino, który jest wysoce prawdopodobny w środowisku elektronicznym.

Z zarysowanego kontekstu wynikają dwa podstawowe cele badawcze – poznawczy oraz utylitarny. Cel poznawczy dotyczy analizy obserwowanych zjawisk: funkcjonowania struktur administracyjnych, potrzeb i oczekiwań obywateli związanych z jakością świadczenia usług publicznych, zagrożeń cyberprzestrzeni państwa oraz rozwiązań prawnych, technicznych, proceduralnych i organizacyjnych wdrożonych na potrzeby zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych. Cel utylitarny wiąże się z potrzebą określenia kierunków zmian w strukturach administracyjnych, które będą sprzyjać efektywnemu zarządzaniu cyberbezpieczeństwem. Głównym celem monografii jest opracowanie modelu systemu zarządzania bezpieczeństwem struktur administracyjnych w warunkach możliwych i prawdopodobnych zagrożeń cyberprzestrzeni państwa.

Przyjęte cele wpłynęły na strukturę monografii. W rozdziale pierwszym przedstawiono aspekty ewolucji struktur administracyjnych. Przyjęto postrzeganie administracji publicznej w kategoriach systemu działania, czyli organizacji realizującej prawnie określone zadania publiczne. Teoretyczne rozważania na temat wpływu rewolucji informacyjnej na struktury administracyjne skonfrontowano z praktyczną realizacją transformacji samorządu terytorialnego. W rozdziale wykazano, że zapewnienie usług publicznych o odpowiedniej jakości jest istotą misji instytucji sektora publicznego. Zastosowanie nowoczesnych technologii w jednostkach sektora publicznego przyczyniło się do powstania koncepcji e-administracji, która stanowi narzędzie transformacji sektora publicznego. Określenie istoty elektronicznej administracji pozwoliło na zdefiniowanie warunków rozwoju elektronicznej administracji oraz na scharakteryzowanie modeli e-administracji w wybranych państwach europejskich.

Rozdział drugi poświęcono identyfikacji zagrożeń cyberprzestrzeni państwa, które mogą stanowić możliwe i prawdopodobne zakłócenia w funkcjonowaniu struktur administracyjnych, a zatem zagrożenia dla ich bezpieczeństwa oraz dla bezpieczeństwa narodowego. Charakterystyka została poprzedzona określeniem istoty oraz specyficznych cech cyberprzestrzeni, które w znacznym stopniu utrudniają kontrolę nad tym środowiskiem. Przedstawiono także techniczne elementy cyberprzestrzeni, które umożliwiają analizę poszczególnych zagrożeń oraz warunkują środki ochrony. W tym kontekście wyjaśniono istotę zagrożeń cyberprzestrzeni państwa oraz zaproponowano ich klasyfikację ze względu na przyjęte kryteria. Zgodnie z przyjętą taksonomią zidentyfikowano aktorów cyberzagrożeń oraz scharakteryzowano metody ataków w cyberprzestrzeni. Istotną kwestią jest także analiza poszczególnych zagrożeń w oparciu o kryterium podmiotu atakującego, celów i motywów oraz oczekiwanych skutków ataku.

Rozdział trzeci charakteryzuje istotę i elementy zarządzania bezpieczeństwem struktur administracyjnych oraz modele zarządzania cyberbezpieczeństwem. W procesie zarządzania każdym systemem istotną kwestię stanowi przestrzeganie przepisów prawnych, dlatego też przywołano ważniejsze uregulowania prawne w omawianym obszarze. Ponadto podano przykłady norm i standardów, ze szczególnym uwzględnieniem norm wypracowanych w wyniku współpracy Międzynarodowej Organizacji Normalizacyjnej (ISO) oraz Międzynarodowej Komisji Elektrotechnicznej (IEC). Praktyczne wdrażanie mechanizmów określonych w normach wymaga m.in. implementacji tzw. trójpoziomowego modelu odniesienia, opracowania polityki bezpieczeństwa oraz ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Przykład zarządzania ryzykiem na potrzeby bezpieczeństwa struktur administracyjnych poprzedzono rozważaniami teoretycznymi oraz wskazaniem metod ograniczenia ryzyka. W celu minimalizacji ryzyka stosowane są różnego rodzaju zabezpieczenia, w związku z czym zasadne było przedstawienie rekomendowanych środków i metod ochrony. W rozdziale dokonano także analizy modeli zarządzania cyberbezpieczeństwem w Polsce, Unii Europejskiej oraz NATO.

W ostatnim rozdziale zaprezentowano wyniki badań empirycznych. Ewaluacji wyników badań ankietowych towarzyszyła analiza zależności statystycznych między cechami społeczno-demograficznymi respondentów a udzielanymi przez nich odpowiedziami, do których oceny wykorzystano w szczególności współczynnik kontyngencji C Pearsona, który oparty jest na teście niezależności Chi-2, test U Manna-Whitneya oraz test Kruskala-Wallisa. Materiał stanowi cenną analizę na potrzeby realizacji celu głównego, który osiągnięto przez określenie rekomendacji zmian systemowych w obszarze zarządzania cyberbezpieczeństwem oraz przedstawienie propozycji modelu systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych.

Niniejsza monografia opiera się na mojej pracy doktorskiej. Pragnę w tym miejscu podziękować promotorowi Profesorowi Piotrowi Sienkiewiczowi za merytoryczne ukierunkowanie rozprawy doktorskiej, cenne rady i wskazówki, które w sposób znaczący przyczyniły się do jej powstania, a także za cierpliwość, ogromną życzliwość i wsparcie w trakcie realizacji pracy. Chcę także wyrazić swoją wdzięczność wykładowcom Akademii Obrony Narodowej, których życzliwej pomocy doświadczyłam podczas studiów doktoranckich. Specjalne podziękowania składam Rodzicom i Bratu, bez których wsparcia nie byłoby możliwe napisanie niniejszej pracy.

1. EWOLUCJA STRUKTUR ADMINISTRACYJNYCH

1.1. Teoretyczne podstawy organizacji systemu administracji publicznej

Kształtowanie współczesnych modeli administracji publicznej przebiegało w różnych warunkach politycznych, społecznych i ekonomicznych. Obecnie obserwuje się globalną tendencję przechodzenia od administrowania do zarządzania sprawami publicznymi, czego wyrazem jest powstanie i wdrażanie koncepcji *good governance* w sektorze publicznym.

Rozważania teoretyczne na temat organizacji systemu administracji publicznej warto rozpocząć od wyjaśnienia pojęcia administracji publicznej. Należy podkreślić, że w literaturze funkcjonuje wiele definicji tej kategorii, akcentujących różne jej cechy. Zmienne ujęcie administracji publicznej związane jest ze zróżnicowanym podejściem do jej roli w systemie władzy publicznej oraz ewolucją przypisywanego jej położenia w relacji ze społeczeństwem. Przykładowo w części Europy do 1989 roku dominowało funkcjonalne (czynnościowe) ujęcie administracji publicznej, traktujące ją jako organizatorską działalność państwa. Definicja ta była wynikiem m.in. zasady jednolitości władzy państwowej.

Ogólne rozumienie terminu *administracja* używane jest w znaczeniu bliskim jego łacińskiego źródłosłowu, będącego synonimem pomocy, służby, przewodnictwa, zarządzania[1]. Jedną z pierwszych definicji jest ta zaproponowana przez W. Jellinka, zgodnie z którą *administrację stanowi działalność państwa, która nie jest ani ustawodawstwem, ani wymiarem sprawiedliwości.* To ujęcie pochodzi z czasu, gdy rodziła się doktryna państwa prawnego, i nawiązuje do trójpodziału władzy w państwie.

W literaturze podkreśla się potrzebę równowagi między ujęciem przedmiotowym (działalność na rzecz interesu publicznego prowadzona na podstawie ustaw), funkcjonalnym (zespół działań, czynności i przedsięwzięć organizatorskich i wykonawczych, odbywających się w określonych prawem formach) oraz podmiotowym (różne podmioty, organy i instytucje)[2]. Administracja publiczna jest złożonym zjawiskiem, które należy do sfery organizacji i funkcjonowania

1 Łac. *administratio* – kierowanie, zarząd; *administrare* – być pomocnym.

2 H. Izdebski, M. Kulesza, *Administracja publiczna. Zagadnienia ogólne*, Warszawa 1998, s. 96.

aparatu państwowego. Powołuje się ją do realizacji zadań publicznych przez różne podmioty, funkcjonujące na podstawie przepisów prawa.

Administracja jest niewątpliwie organizacją. W zakresie definiowania organizacji dostrzegalne jest zróżnicowanie ze względu na określone jej ujęcia, np. prakseologiczne[3], cybernetyczne[4], systemowe[5], socjologiczne[6]. Zazwyczaj *organizacja* oznacza instytucję, grupę funkcjonalną oraz proces organizowania[7]. Sposób organizacji uzależniony jest od zasobów, określonych celów oraz warunków ich realizacji w rozpatrywanym systemie. Zatem organizacja stanowi wieloetapowy i złożony proces uwzględniający m.in. cele funkcjonowania, koordynację, weryfikację podjętych czynności oraz podział i specjalizację pracy[8].

Ujęcie systemowe administracji publicznej pozwala na badanie administracji w sposób holistyczny, zakładający, że rzeczywistość jest postrzegana całościowo. System definiowany jest jako *każdy złożony obiekt wyróżniony z badanej rzeczywistości, stanowiący całość tworzoną przez zbiór obiektów elementarnych (elementów) i powiązań (relacji) pomiędzy nimi*[9].

W prezentowanym ujęciu administracja publiczna jest organizacją – systemem społecznym, tworzonym przez ludzi pełniących określone funkcje w strukturach organizacyjnych, którzy za pomocą określonych sposobów działania oraz środków materialnych przyczyniają się do realizacji zamierzonych celów. Administracja publiczna wykonuje określone czynności i przedsięwzięcia na podstawie przepisów prawa i w określonych normatywnie formach. Regulatorem jej funkcjonowania są zatem czynniki prawne i polityczne. Każda jednostka administracji publicznej ma określone cele działania, które są realizowane na rzecz interesu publicznego i zaspokajania potrzeb społecznych przy wykorzystaniu dostępnych zasobów. W celu realizacji powyższych zadań administracja publiczna posiada

3 Prakseologiczne ujęcie organizacji skupia się przede wszystkim na cechach sprawności i skuteczności działania. Zob. np. J. Korczak, *Prakseologiczna interpretacja pojęcia organizacji* [w:] *Nauka organizacji i zarządzania*, Wrocław 2005, s. 174–187.

4 Cybernetyczna interpretacja organizacji opiera się na trzech etapach: wejścia, transformacji (sprzężenie zwrotne) oraz wyjścia. Zob. np. A. Chrisidu-Budnik, *Cybernetyczna interpretacja organizacji* [w:] *Nauka organizacji i zarządzania*, Wrocław 2005.

5 Ujęcie systemowe polega na analizowaniu organizacji jako systemu składającego się z celowo powiązanych elementów i relacji. Zob. np. A. Czermiński, M. Grzybowski, *Wybrane zagadnienia z organizacji i zarządzania*, Gdynia 1996, s. 18–20.

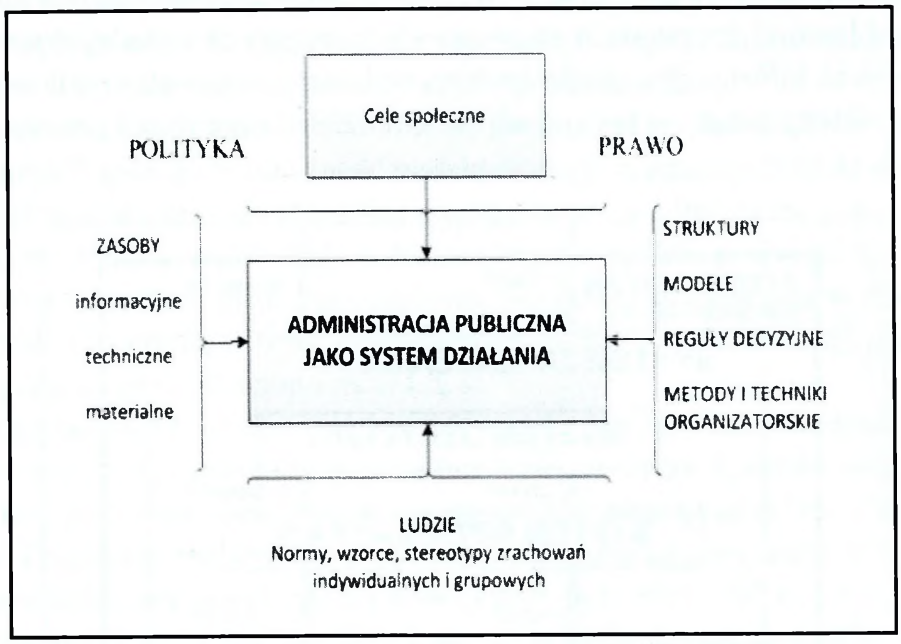
6 Socjologiczna interpretacja organizacji obejmuje swym zakresem z jednej strony badania nad organizacjami rozumianymi jako grupy celowe, z drugiej strony procesy organizacyjne zachodzące w mikro- i makroskali. Zob. np. M. Hiroszewicz, *Socjologia organizacji*, Warszawa 1967.

7 J. Szreniewski, *Wstęp do nauki administracji*, Lublin 2004, s. 30.

8 Szerzej na temat faz tworzenia struktur organizacyjnych (także w administracji): Z. Władek, *Organizacja i zarządzanie w administracji publicznej*, Warszawa 2013, s. 36–46.

9 P. Sienkiewicz, *Inżynieria systemów*, Warszawa 1983, s. 27.

określoną strukturę, która stanowi zbiór relacji zachodzących między poszczególnymi jej elementami. W systemie administracji istnieją określone reguły podejmowania decyzji i techniki organizatorskie, na które składają się określone zasady, procedury i praktyka; to na ich podstawie następuje dokonanie wyboru przyszłego funkcjonowania. Powyższa charakterystyka skłania do postrzegania administracji publicznej w kategoriach systemu działania (rys. 1.1).



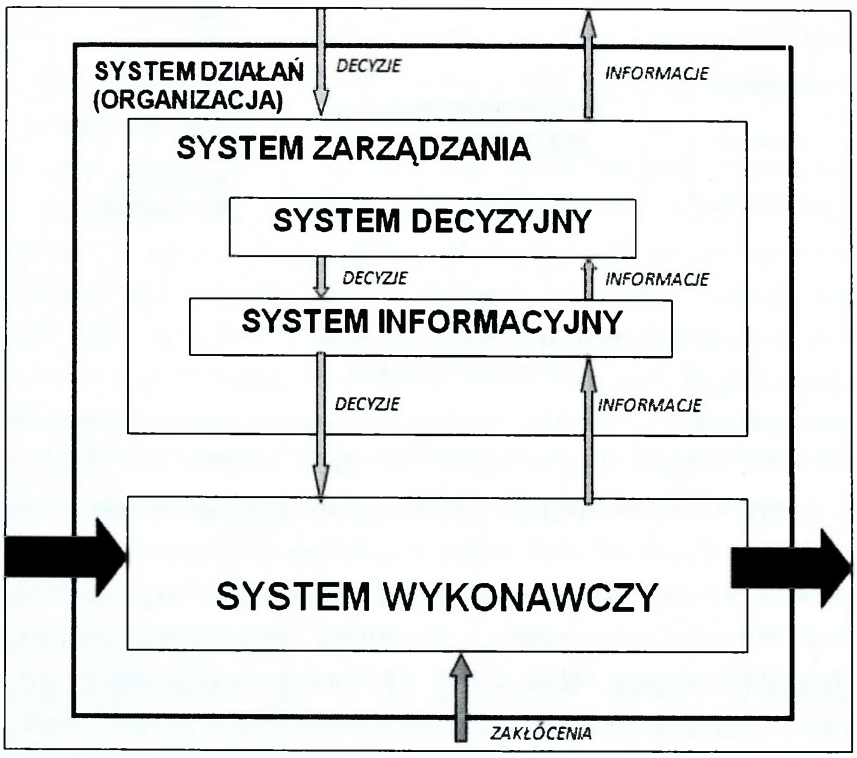
Opracowanie własne na podstawie: P. Sienkiewicz, *Systemy kierowania*, Warszawa 1989, s. 35.

Rys. 1.1. Administracja publiczna jako system działania

P. Sienkiewicz zauważa, że *systemowa koncepcja organizacji odrzuca tezę o dominacji któregokolwiek z wyróżnionych czynników organizacyjnych, co różni ja od wielu innych ujęć (koncepcji, szkół, teorii). Doskonalenie organizacji jako systemu społecznego jest równoznaczne z pożądanym kształtowaniem wszystkich rozpatrywanych czynników*[10]. W systemie administracji publicznej istotne jest racjonalne jego zachowanie polegające na współdziałaniu ze sobą poszczególnych elementów systemu. Owo współdziałanie przyczynia się do powodzenia całości, a jednocześnie zwiększa odporność na zakłócenia zewnętrzne i wewnętrzne. Obok wspomnianych formalnych uwarunkowań, na administrację publiczną oddziałują także obiektywne czynniki, takie jak wzrost oczekiwań i potrzeb społecznych związany z postępem cywilizacyjnym, rozwój nowoczesnych technologii oraz przemiany ustrojowe.

10 P. Sienkiewicz, *Systemy kierowania*, Warszawa 1989, s. 36.

W organizacji możemy wyróżnić dwa podstawowe podsystemy: wykonawczy i zarządzania. Pierwszy z nich realizuje procesy potrzeb otoczenia, czyli przetwarza określone zasoby (wejścia) w określone dobra na użytek otoczenia (wyjścia). Drugi z nich realizuje procesy zarządzania, zapewniając pożądaną realizację zadań w podsystemie wykonawczym. W tym podsystemie wyróżnia się system informacyjny, który realizuje proces przesyłania i przetwarzania informacji, oraz system decyzyjny, realizujący procesy decyzyjne polegające na rozwiązywaniu sytuacji (problemów) decyzyjnych na podstawie kompetencji i wiedzy uczestników procesów oraz informacji o stanie systemu wykonawczego i otoczenia organizacji[11]. Scharakteryzowany w ten sposób system działań organizacji przedstawiono na rys. 1.2.



Źródło: P. Sienkiewicz, *25 wykładów*, Warszawa 2014, s. 323.

Rys. 1.2. Model systemu działań organizacji

System działania administracji publicznej może być rozpatrywany w skali makro i mikro. Pierwsza obejmuje układ wszystkich jednostek organizacyjnych wykonujących zadania administracji publicznej i ich wzajemne zależności organizacyjne. Skala mikro z kolei oznacza wąski sposób postrzegania struktury organizacyjnej, koncentrujący się co do zasady na jednej jednostce organizacyj-

11 P. Sienkiewicz, *25 wykładów*, Warszawa 2014, s. 323.

nej z uwzględnieniem jej specyfikacji, układu stanowisk, komórek organizacyjnych oraz występujących między nimi relacji[12]. W skali ogólnopaństwowej administracja publiczna stanowi skomplikowany megasystem; składają się na niego różne podsystemy, między którymi trudno zidentyfikować relacje. Trudności te wynikają głównie z ogromnej złożoności aparatu administracji publicznej oraz z przemian zachodzących w strukturach administracji. Ponadto administracja publiczna w wielu aspektach funkcjonuje w powiązaniu z administracją innych państw. Wpływa to na skomplikowanie organizacji sytemu administracji zarówno w aspekcie instytucjonalnym, prawnym, jak i technicznym.

Współczesne państwa zdecydowały się na przyjęcie określonego podziału terytorialnego[13], którego konieczność podyktowana jest różnorodnością zadań, zasięgiem terytorialnym oraz stopniem skomplikowania administracji. W systemie ustrojowym Polski administrację publiczną można ogólnie podzielić na rządową (centralna i terenowa) oraz samorządową. Samorząd terytorialny w Polsce jest trójszczeblowy (gmina, powiat, województwo). Schemat administracji publicznej w skali państwa przedstawiono na rys. 1.3.

Należy zauważyć, że sprawne i efektywne funkcjonowanie administracji publicznej jest w istotnym stopniu uzależnione od jej struktury. P. Sienkiewicz definiuje strukturę jako *zbiór relacji między wzajemnie ze sobą sprzężonymi elementami systemu. Przyjmując za wyjściową definicję systemu jako pary, którą tworzy zbiór elementów oraz zbiór relacji między elementami, pierwszy z nich to skład (konfiguracja) systemu, drugi to jego struktura*[14]. Administracja stanowi niewątpliwie pewną wyodrębnioną strukturę organizacyjną, na którą składają się różnorodne jednostki wyposażone w kompetencje określone w ustawach i tworzące pewien układ organizacyjny, mający realizować zadania publiczne[15]. Strukturę administracji publicznej w Polsce można postrzegać w pięciu głównych wymiarach:

- struktura systemu administracji publicznej – układ wzajemnie powiązanych i współdziałających ze sobą jednostek administracji publicznej funkcjonujących w całym państwie;
- struktura systemu administracji rządowej – układ wzajemnie powiązanych i współdziałających jednostek administracji rządowej;

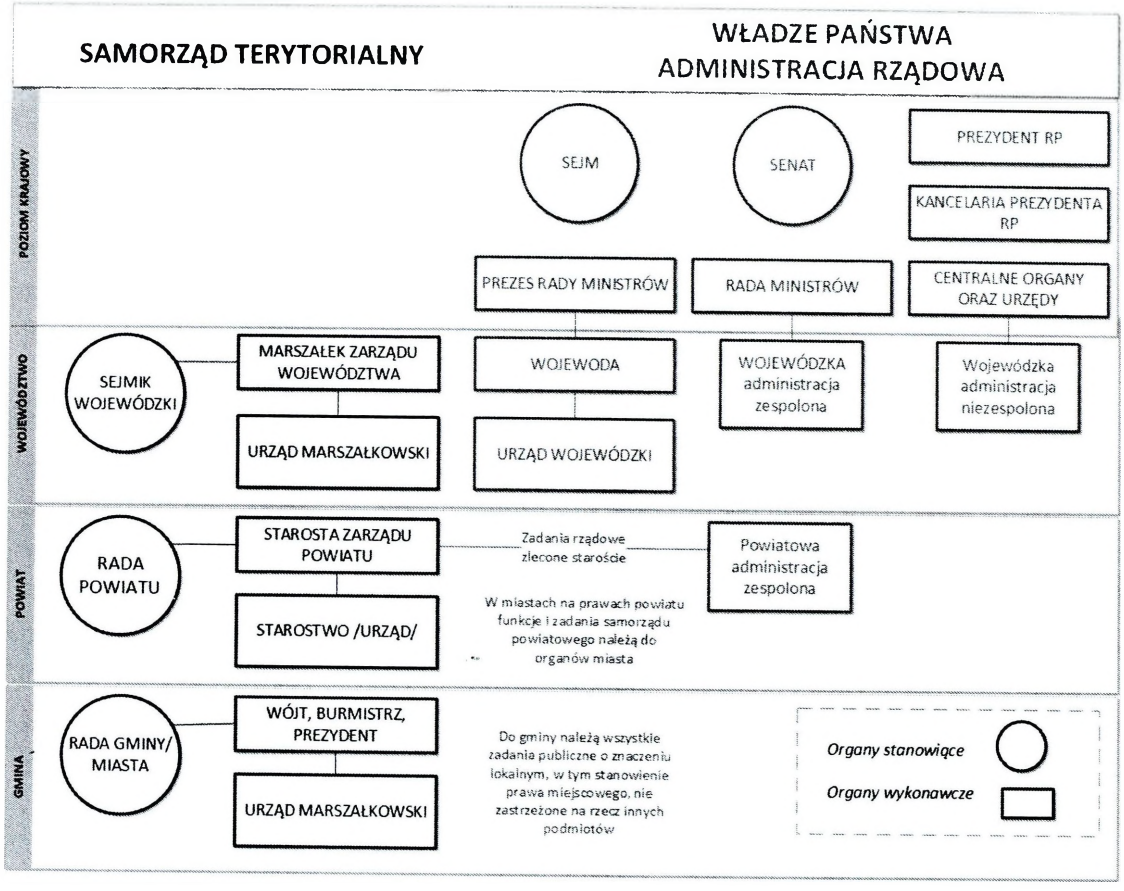
12 M. Polinceusz, *Organizacja systemu administracji publicznej* [w:] *Nauka administracji*, red. M. Karpiuk, W. Kitler, Warszawa 2013, s. 52–53.

13 Podziałów terytorialnych kraju jest wiele. W Polsce dotyczą one m.in. trójstopniowego podziału państwa (gmina, powiat, województwo), podziału na potrzeby statystyki publicznej, podziału na potrzeby ewidencji gruntów i budynków, podziału ze względu na jednostki administracji specjalnej, np. urzędy skarbowe, nadleśnictwa, regionalne zarządy gospodarki wodnej.

14 P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Warszawa 1994, s. 159.

15 J. Lang, *Zagadnienia wstępne* [w:] *Prawo administracyjne*, red. M. Wierzbowski, Warszawa 1997, s. 15.

- struktura systemu administracji samorządowej – związana z podziałem terytorialnym kraju, obejmująca układ wzajemnie powiązanych i współdziałających jednostek administracji samorządowej;
- struktura administracji ze względu na wyodrębnione działy, np. struktura administracji celnej;
- struktura pojedynczej jednostki administracji publicznej.



Opracowanie własne na podstawie: http://www.slaskie.pl/strona_n.php?jezyk=pl&grupa=3&dzi=1255957049&id_menu=285.

Rys. 1.3. Model zarządzania terytorialnego w Polsce

Jednostka administracji publicznej to całość (instytucja) wyodrębniona z systemu administracji publicznej, powołana na podstawie przepisów prawa i realizująca zadania publiczne w określonych prawnie formach. Jednostkę administracyjną można opisać jako zbiór elementów i relacji między nimi. Zdefiniowana w ten sposób jednostka administracyjna posiada następujący zbiór elementów:

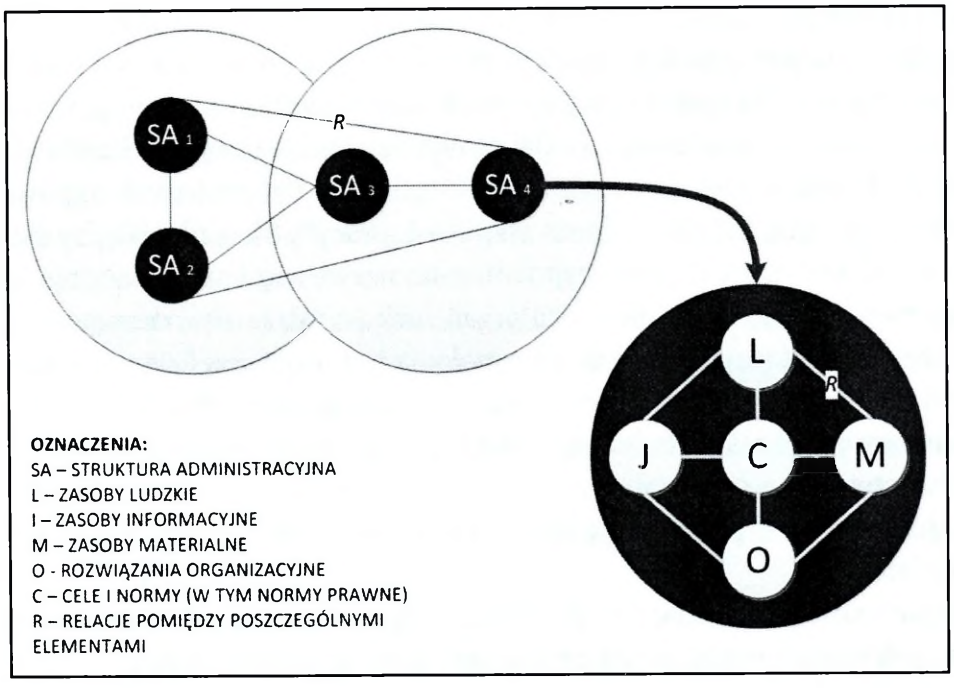
$$JA = \{L, I, M, C, O, R\}$$

gdzie:
JA – jednostka administracyjna,
L – zasoby ludzkie,
I – zasoby informacyjne,
M – zasoby materialne,
C – cele i normy (w tym prawo),
O – rozwiązania organizacyjne,
R – relacje pomiędzy poszczególnymi elementami.

Stąd struktura administracyjna to:

- układ wzajemnie powiązanych i współdziałających elementów jednostki administracyjnej;
- zbiór relacji określonych na elementach danej jednostki administracyjnej;
- układ wzajemnie powiązanych elementów systemu dla zapewnienia wysokiej skuteczności działania całego systemu lub jego części.

W prezentowanym ujęciu można wyodrębnić szereg struktur administracyjnych w administracji publicznej (rys. 1.4).



Opracowanie własne.

Rys. 1.4. Struktury administracyjne w systemie administracji publicznej

Zaproponowana interpretacja struktury administracyjnej przypomina opracowaną w latach siedemdziesiątych przez R. Pascala i A. Athosa koncepcję „7S", określającą siedem czynników przedsiębiorstwa, od których zależy jego sukces. Wśród nich znalazły się tzw. twarde S: strategia produkt – rynek (*strategy*),

formalna struktura organizacyjna (*structure*), sformalizowane systemy i procedury planowania, kierowania i kontroli (*systems*), oraz tzw. miękkie S: styl kierowania i klimat organizacyjny (*style*), obsadzanie stanowisk, rekrutacja, awanse (*staff*), fachowe i socjalne kwalifikacje i umiejętności menedżerów (*skills*). Czynnikiem integrującym pozostałe – podobnie jak w wyszczególnionych elementach struktury administracyjnej – są ogólne cele i wartości wpajane przez organizację (*superodinate goals*)[16].

Efektywność struktury administracyjnej, także w warunkach zagrożeń cyberprzestrzeni państwa, zależy od relacji między poszczególnymi elementami oraz współdziałania z innymi strukturami. W związku z tym bezpieczeństwo struktury administracyjnej może być rozpatrywane w oparciu o jej elementy składowe. W organizacji można wyróżnić relacje między ludźmi, relacje między ludźmi i zasobami oraz relacje między zasobami. Sprawą zasadniczą jest racjonalne kierowanie strukturą administracyjną. *Analiza poszczególnych form konfiguracji struktur systemu powinna doprowadzić do ujawnienia ich podstawowych zalet i wad w kontekście ogólnych celów, funkcji i warunków działania organizacji*[17]. Należy zauważyć, że rodzaj (typ) struktury determinuje jej bezpieczeństwo (niezawodność) i efektywność.

Zasadniczym elementem jednostki organizacyjnej w administracji jest organizacja stanowisk pracy. Od sposobu, w jaki zostały one ukształtowane, zależy w znacznej mierze sprawność funkcjonowania całej struktury administracyjnej. Każda jednostka administracyjna – większa czy mniejsza – powinna być zestawem odpowiednio powiązanych ze sobą indywidualnych stanowisk pracy[18]. Stosunki między stanowiskiem pracy i komórkami organizacyjnymi noszą nazwę więzi organizacyjnych, które wpływają na realizację celów. W teorii organizacji wyróżnia się cztery podstawowe rodzaje więzi organizacyjnych, których typologia jest oparta na kryterium kierunku powiązań między elementami tworzącymi strukturę organizacyjną[19]:

- służbowe – określają zależność podwładnego od przełożonego, czyli relacje zwierzchnictwa;
- funkcjonalne – przejawiają się w pomaganiu i/lub doradzaniu w wykonywaniu zadań;
- techniczne – związane z podziałem pracy, powodują, że czynności członka zespołu są determinowane przez czynności pozostałych członków;
- informacyjne – wyznaczone są przepływem informacji.

16 P. Sienkiewicz, *Systemy kierowania...*, op. cit., s. 85–86.

17 Ibidem, s. 163.

18 S. Kowalewski, *Nauka o administrowaniu*, Warszawa 1982, s. 23.

19 Zob. C. Sikorski, *Zachowania ludzi w organizacji*, Warszawa 1999, s. 38; P. Sienkiewicz, *Systemy kierowania...*, op. cit., s. 163–164; S. Kowalewski, *Nauka o administrowaniu...*, op. cit., s. 175–185.

Istotnym elementem systemu administracji publicznej jest struktura organizacyjna, określająca pewien porządek, na którym opiera się proces zarządzania. W literaturze funkcjonuje wiele taksonomii struktur organizacyjnych. Najczęściej spotykane typologie struktur organizacyjnych oraz kryteria w nich wykorzystywane[20]:

- ze względu na rozpiętość kierowania i liczbę szczebli zarządzania wyróżnia się struktury: smukłe i płaskie;
- ze względu na stopień nowoczesności wyróżnia się struktury:
  - klasyczne, to jest stworzone w początkowym okresie rozwoju nauki i zarządzania, a wśród nich, biorąc pod uwagę rodzaj więzi organizacyjnych, wyróżnia się strukturę: liniową, funkcjonalną i liniowo-sztabową;
  - podstawowe, czyli ukształtowane w okresie rozwoju nauk o zarządzaniu, a zdolność do dostosowywania się do zmiennego otoczenia pozwala wyodrębnić wśród nich następujące struktury: dywizjonalną, zadaniową (projektową), macierzową i hybrydową (mieszaną);
  - nowoczesne, to jest rozwijane w teorii i praktyce zarządzania w ostatnich latach, do których można zaliczyć struktury: procesową, sieciową, wirtualną, fraktalną i inne;
- ze względu na stopień zbliżenia do mechanistycznego lub organicznego modelu zarządzania jako kryterium można podzielić struktury na: hierarchiczne (liniową, funkcjonalną, liniowo-sztabową), pośrednie (dywizjonalną, macierzową), organiczne (zadaniową, sieciową);
- ze względu na podział zadań wyróżnia się struktury: typu U, typu M, typu H;
- biorąc pod uwagę stopień zróżnicowania części organizacji, struktury dzieli się na: proste i złożone;
- ze względu na konfigurację strukturalną wyodrębnia się: strukturę prostą, biurokrację maszynową, biurokrację profesjonalną, strukturę dywizjonalną, adhokrację, strukturę misyjną i strukturę polityczną;
- cechy struktury organizacyjnej i czynniki strukturotwórcze umożliwiają zaklasyfikowanie struktur do jednego z typów: A, B, C lub D.

Wśród różnych typów struktur organizacyjnych w administracji publicznej wymienia się najczęściej:

- strukturę funkcjonalną;
- strukturę zorientowaną na czynności administracyjne;
- strukturę zorientowaną na program/usługę;
- strukturę zorientowaną na klienta;

20 Taksonomię przywołano za: A. Zakrzewska-Bielawska, *Typy struktur organizacyjnych*, [w:] *Podstawy zarządzania. Teoria i ćwiczenia*, red. A. Zakrzewska-Bielawska, Warszawa 2012, s. 288–323.

- strukturę macierzową;
- strukturę sztabową[21].

Wymienione typy struktury organizacyjnej posiadają określone cechy charakterystyczne oraz wady i zalety. *Dla każdej organizacji o określonych celach, funkcjach i warunkach istnieje optymalna, w sensie maksymalnej efektywności działania, struktura systemu kierowania*[22]. Wybór rozwiązania determinuje wiele czynników. Są to zarówno wewnętrzne cechy, jak i czynniki znajdujące się w otoczeniu organizacji. Wśród determinantów wymienia się często strategię, wielkość organizacji, technologię, styl zarządzania czy kulturę organizacyjną.

Struktury organizacyjne odgrywają istotną rolę w organizacji. Wśród ich funkcji można wymienić m.in.:

- scalanie elementów organizacji w całość;
- synchronizację procesów realizowanych w organizacji;
- określanie ramy działań wykonawczych i zarządzających;
- regulację pracy poszczególnych pracowników oraz zespołów roboczych;
- determinowanie skuteczności i jakości realizacji celów i strategii organizacji;
- determinowanie niezawodności (bezpieczeństwa);
- koordynację współpracy z otoczeniem;
- neutralizację wpływu zmian zachodzących w otoczeniu.

Zmiana strategii w organizacji powinna modyfikować jej strukturę. Zastosowanie zaawansowanych technologii w administracji publicznej powinno wywołać zmiany polegające m.in. na powstawaniu skomputeryzowanych komórek oraz zmianie charakteru więzi strukturalnych.

1.2. Wpływ rewolucji informacyjnej na struktury administracyjne

Cechą charakterystyczną współczesnych państw jest zacieranie się granic organizacyjnych związane z procesem globalizacji, przenikaniem się systemów informacyjnych i tworzeniem globalnej przestrzeni informacyjnej. W literaturze wielokrotnie podkreśla się, że świat wkroczył w erę, w której najcenniejszym zasobem stała się informacja, podniesiona tym samym do rangi zasobu strategicz-

21 A. Pawłowska, *Struktury organizacyjne w administracji publicznej* [w:] *Administracja publiczna – zagadnienia wstępne*, red. A. Pawłowska, Lublin 1999, s. 31–48; A. Pawłowska, *Zasoby informacyjne w administracji publicznej. Problemy zarządzania*, Lublin 2002, s. 50–57.

22 P. Sienkiewicz, *Systemy kierowania...*, op. cit., s. 167.

nego[23]. Nastąpiła zmiana orientacji cywilizacyjnej związana z przechodzeniem od cywilizacji przemysłowej do społeczeństwa informacyjnego[24].

Początków rewolucji informacyjnej oraz podwalin technologicznych społeczeństwa informacyjnego należy doszukiwać się niewątpliwie w zdumiewającym rozwoju technologii, jaki miał miejsce po drugiej wojnie światowej. Era telekomunikacji rozpoczęła się jednak wcześniej. W XIX wieku wynaleziono m.in. telegraf, telefon, płytę gramofonową. Później pojawiło się radio i telewizja. Przełomowym momentem było uruchomienie ENIAC-a (1946) oraz powstanie sieci ARPANET (1969), która dała początek rozwojowi sieci komputerowych i powstaniu Internetu (1990). Nie sposób pominąć także wkładu A. Turinga (maszyna Turinga), C.E. Shannona (teoria informacji), J. von Neumanna (koncepcja maszyny cyfrowej opartej na binarnym układzie arytmetycznym), N. Wienera (twórca cybernetyki) czy też P. Barana (kierownik zespołu RAND, który opracował koncepcję sieci komputerowej ARPANET). Wymienione w krótkim zarysie osiągnięcia przyczyniły się do niespotykanego dotąd rozwoju komunikacji oraz ostatecznie do ukształtowania społeczeństwa informacyjnego.

Przyjmuje się, że twórcą pojęcia *społeczeństwo informacyjne* jest japoński socjolog T. Umesao, który po raz pierwszy użył tego sformułowania w artykule na temat ewolucyjnej teorii społeczeństwa opartego na przemysłach informacyjnych. Następnie pojęcie to zostało spopularyzowane przez K. Koyamę, uzyskując tym samym wymiar polityczny, i stało się przedmiotem analiz rządowych[25]. W Japonii istotne znaczenie w omawianym zakresie odegrał opracowany w 1972 roku plan wdrażania społeczeństwa informacyjnego opracowany przez Y. Masudę. Wzorem Japonii, w Europie czy też w Stanach Zjednoczonych zaczęto dostrzegać wzrost znaczenia innowacji, usług oraz technologii w rozwoju społeczno-gospodarczym.

23 Należy zauważyć, że informacja i działania mające na celu jej ochronę towarzyszyły człowiekowi od zarania dziejów. Tylko w oparciu o wiarygodną i aktualną informację jednostki i społeczeństwa mogły podejmować właściwe decyzje. Sprawdzona, rzetelna i dokładna informacja zawsze była także istotna przy podejmowaniu decyzji w sferze bezpieczeństwa i obronności. We współczesnych naukach wojskowych podkreśla się, że osiągnięcie złożonych celów militarnych w zmieniającym się środowisku bezpieczeństwa jest uzależnione od zdobycia tzw. dominacji informacyjnej. Warunek ten uwzględnia np. amerykańska doktryna obronna, która zakłada osiągnięcie tego celu w oparciu o przewagę technologiczną. Dominacja ta ma być wynikiem m.in. szybszego niż nieprzyjaciel pozyskiwania informacji.

24 Pojęcie społeczeństwa informacyjnego nie doczekało się powszechnie akceptowanej definicji. Przyjmuje się, że jest ono nową formą społeczno-ekonomiczną. W literaturze funkcjonuje wiele innych określeń społeczeństwa informacyjnego, np. społeczeństwo globalnej wioski (M. McLuhan), trzecia fala (A. Toffler), społeczeństwo megabitowe (S. Lem), społeczeństwo sieciowe (M. Castells), neokapitalizm (A. Gorz), społeczeństwo postindustrialne (D. Bell), wiek niepewności (J. Galbraith), społeczeństwo ryzyka (U. Beck).

25 T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 42–43.

Rezultatem tego było opracowywanie wielu narodowych i globalnych strategii rozwoju społeczeństwa informacyjnego[26].

W literaturze przedmiotu funkcjonuje wiele definicji społeczeństwa informacyjnego, akcentujących różne jego cechy: techniczne – rozwój technologiczny ma decydujące znaczenie (J. Naisbitt, J. Mączyński), ekonomiczne – wiedza i informacja ma fundamentalne znaczenie dla rozwoju społeczeństwa (D. Bell), zawodowe – społeczeństwo informacyjne wymusza elastyczną specjalizację produkcji i pracy (S. Juszczyk, M. Piore), przestrzenne – społeczeństwem informacyjnym jest każde państwo narodowe, zdolne do określenia zasobów alokacyjnych i władczych oraz do rozpoznania potrzeb własnych obywateli (M. Castells), kulturowe – kultura współczesna stała się rzeczywistością wirtualną, czyli swoistą symulacją znaczeń trudnych do rozpoznania w natłoku informacji, świat natomiast jest taki, jakim wykreują go media (J. Baudrillard)[27]. Rozwój badań nad społeczeństwem informacyjnym doprowadził do wielu konkurencyjnych ze sobą teorii, także w aspekcie możliwego i prawdopodobnego rozwoju społeczeństwa.

T. Goban-Klas i P. Sienkiewicz formułują następującą propozycję terminologiczną: *Społeczeństwo informacyjne to społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródło utrzymania większości społeczeństwa*[28]. Zgodnie z przywołaną definicją warunkiem rozwoju społeczeństwa informacyjnego z jednej strony jest odpowiednie zaplecze technologiczne, z drugiej zaś istotna jest zdolność społeczeństwa do adaptacji i wykorzystania nowych technologii.

Zmiany zachodzące w administracji publicznej następują równolegle z rozwojem społecznym. W związku z rozwojem technologii przetwarzania danych oraz z łatwością ich generowania i przesyłania rośnie zapotrzebowanie na elektroniczną postać informacji. Przeobrażenia zachodzące w otoczeniu jednostek, państw czy organizacji sprawiają, że dotychczasowe metody zarządzania informacją, a szczególności tradycyjne kanały komunikacyjne, stały się niewystarczające. Na umownej skali procesu ewolucji struktur administracyjnych, w dużym uproszczeniu i przy świadomości niejednoznaczności poglądów spotykanych w literaturze, można wyróżnić kilka etapów rozwoju administracji publicznej (tab. 1.1).

26 Powstało wiele dokumentów na temat społeczeństwa informacyjnego, np. *Europa i Społeczeństwo Globalnej Informacji – Zalecenia Rady Europy* (tzw. Raport Bangemanna, 1994), *Europejska Agenda Cyfrowa – program rozwoju społeczeństwa informacyjnego w Unii Europejskiej na lata 2010–2015.*

27 Zob. J. Lubacz (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1999, s. 30.

28 T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne...*, op. cit., s. 53.

Tab. 1.1. Etapy rozwoju struktur administracyjnych

Etap		Charakterystyka
I	Administracja publiczna tradycyjna (klasyczna, PA)	Tworzenie pierwszych funkcji administracyjnych w okresie powstawania państwa
II		Utworzenie oddzielnych stanowisk i podsystemów, które służą formułowaniu i przestrzeganiu przepisów dla regulacji członków organizacji. W rezultacie tworzy się struktura zwierzchnictwa, która jest jakościowo inna od struktury wykonywania zadań
III		Administracja oddziela się wewnątrz systemów państwowych od sądownictwa, ustawodawstwa i polityki, a w systemach gospodarczych od ich właścicieli. Administracja staje się wysoce sformalizowaną organizacją, której działania są przedmiotem udoskonalenia, badań i nauczania uniwersyteckiego[a)]
IV	Zarządzanie publiczne (*Public Management*, PM)	Okres rozkwitu struktur administracyjnych oraz samego procesu administrowania wraz z rozwojem nauk administracyjnych i wykorzystaniem naukowej organizacji i kierownictwa. Celem staje się rozwój i usprawnienie procedur. Istotą administracji IV generacji jest jej wewnętrzna efektywność
V	Nowe zarządzanie publiczne (*New Public Management*, NPM)	Po rozprzestrzenieniu się systemów demokratycznych administracja koncentruje się na wzajemnych relacjach między administrującymi a administrowanymi, a w szczególności na jakości dostarczanych usług. Powszechnie zaczyna się uznawać służebną rolę administracji wobec społeczeństwa, a administrowani zaczynają być traktowani jako klienci. Teoria NPM wywodzi się z teorii ekonomii[b)]. Reformy podejmowane w tym nurcie opierały się na mechanizmach i instrumentach charakterystycznych dla sektora prywatnego
VI	Dobre współzarządzanie/ współzarządzanie publiczne (*Good Governance/ New Public Governance*, NPG)	Etap ten przypada na przełom XX i XXI wieku. Jest to okres ukształtowania się i dalszego rozwoju społeczeństwa obywatelskiego. W tym okresie następuje dynamiczny rozwój technologii informacyjnych i Internetu, globalizacja. Powstaje koncepcja społeczeństwa informacyjnego oraz e-administracji. sprawowanie władzy publicznej w ramach wzajemnych relacji rządu, administracji i społeczeństwa, cechujące się otwartością, partnerstwem, rozliczalnością, skutecznością, efektywnością i spójnością

[a)] Prekursorami w tym zakresie byli w Europie prof. Lorenz von Stein oraz Woodrow Wilson, którzy uważani są za twórców naukowego administrowania (druga połowa XIX wieku).

[b)] Zob. K. Kernaghan, B. Marson, S. Borins, *The New Public Organization*, Toronto 2000.

Opracowanie własne na podstawie: J. Kisielewicz, *Nauka administracji*, Przemyśl–Rzeszów 2008; J. Kisielewicz, *Istota i zasady good governance*, dostęp: http://lex.pl/czasopisma/atdp/art_2_09.pdf; H. Izdebski, *Od administracji publicznej do public governance*, „Zarządzanie publiczne", 1/2007.

Kluczowym elementem zmian związanych z rewolucją informacyjną jest przejście od administrowania do zarządzania[29]. Administrowanie jest działalnością jednostek kierowniczych, która wykształciła się wcześniej niż zarządzanie. Rozwiązania dotyczące procedur związanych z administrowaniem są najczęściej uregulowane w przepisach prawa powszechnie obowiązującego oraz ograniczają się co do zasady do niektórych elementów motywowania i formalnej kontroli. Ogólnie rzecz ujmując, administrowanie związane jest z działalnością rutynową, nieuwzględniającą dynamiki zmiany w otoczeniu systemu. Natomiast zarządzanie, na gruncie teorii organizacji i zarządzania, oznacza: *Zestaw działań (obejmujący planowanie i podejmowanie decyzji, organizowanie, przewodzenie, tj. kierowanie ludźmi i kontrolowanie) skierowanych na zasoby organizacji (ludzkie, rzeczowe, finansowe i informacyjne) i wykonywanych z zamiarem osiągnięcia celów organizacji w sposób sprawny i skuteczny*[30]. Głównym zadaniem podmiotu zarządzającego jest zapewnienie rozwoju i zysku organizacji przez wypracowanie odpowiedniej strategii oddziaływania na pozostałe podmioty organizacji. W procesie zarządzania zachodzą również zmiany niezależne od wpływu podmiotów systemu zarządzania. Wobec powyższego, *proces zarządzania obejmuje ciąg określonego typu (charakteru) zmian, zależnych lub niezależnych od elementów składowych systemu zarządzania zachodzącego wewnątrz tego systemu lub wynikających z relacji łączących go z otoczeniem*[31]. W związku z tym implementacja koncepcji zarządzania wiedzą w sektorze publicznym wydaje się naturalną konsekwencją zachodzących przemian. Aparat administracyjny stanowi organizację ukierunkowaną na zmianę i uczenie się[32].

Warto wspomnieć, że jednym z założeń modelu *good governance* jest podejście sieciowe do analizowania administracji publicznej. Niemal cała ludzkość jest dominowana przez hierarchię różnego rodzaju, której zanik wydaje się w najbliższej przyszłości mało prawdopodobny. Jednakże pojawiła się nowa forma organizacji horyzontalnej – struktura sieciowa.

Sieć definiowana jest pod względem semantycznym jako złożony system lub grupa powiązanych ze sobą elementów – rzeczy bądź ludzi. Pod względem formalnym sieć to graf (rys. 1.5), czyli zbiór węzłów i łączących je łuków, dla którego

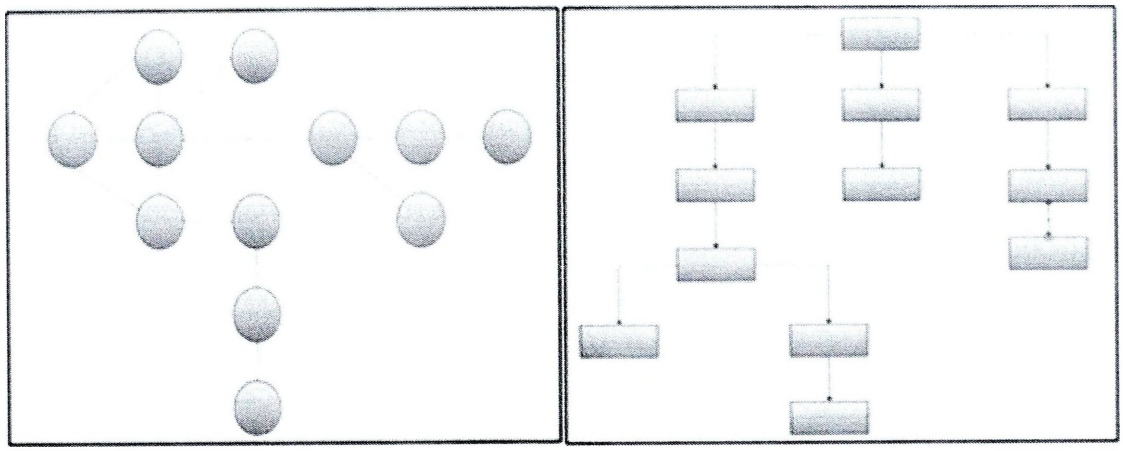
29 Por. P. Modzelewski, *System zarządzania jakością a skuteczność i efektywność administracji samorządowej*, Warszawa 2009; J. Hausner, *Zarządzanie publiczne. Podręcznik akademicki*, Warszawa 2008; K. Lisiecka, T. Papaj, E. Czyż-Gwiazda, *Public Governance koncepcją zarządzania w administracji publicznej*, Katowice 2011; Z. Władek, *Organizacja i zarządzanie w administracji publicznej*, Warszawa 2013.

30 R.W. Griffin., *Podstawy zarządzania organizacjami*, Warszawa 1998, s. 38.

31 W. Kitler, *Zarządzanie w administracji publicznej* [w:] *Nauka administracji*, red. M. Karpiuk, W. Kitler, Warszawa 2013, s. 125.

32 A. Wyroba, *Zarządzanie wiedzą w urzędzie*, Warszawa 2005, s. 5.

zostały określone funkcje na zbiorze węzłów i łuków (np. funkcja przepustowości, wydajności, niezawodności, kosztów)[33]. Strukturę sieciową definiuje się jako organizację, w której koordynację przez hierarchię zastąpiono podkreśleniem stosunków poziomych. Formalne relacje miedzy jednostkami organizacyjnymi zamieniono na powiązania między partnerami, którymi są różne organizacje. Aktywa są podzielone tak, aby wytwórcą całości nie była pojedyncza organizacja sieci, lecz sieć jako całość[34].



Opracowanie własne.

Rys. 1.5. Struktura sieciowa oraz struktura hierarchiczna

Prekursorem *governance* w stosunku do sektora publicznego był H. Cleveland, który w 1972 roku opisywał przypuszczalne zmiany w zarządzaniu publicznym. Cleveland prognozował, że organizacje publiczne nie będą zorganizowane na zasadzie hierarchicznych piramid z realną władzą na wierzchołku. Będą one ewoluować w kierunku przeplatających się sieci, charakteryzujących się mniejszą kontrolą, bardziej rozproszoną władzą oraz wieloma centrami decyzyjnymi. Podejmowanie decyzji stanie się złożonym procesem, w którym wezmą udział podmioty zarówno wewnątrz, jak i na zewnątrz organizacji. Nastąpi spłaszczenie struktur organizacyjnych związanych z rozwojem kolegialnych systemów sprawowania władzy z wykorzystaniem konsultacji społecznych[35]. Również M. Castells zauważa, że perspektywa przestrzeni przepływów modyfikuje rolę administracji. Oprócz funkcji polegających na świadczeniu usług pojawią się nowe, polegające na takiej konfiguracji czynników ekonomicznych, prawnych i społecznych, która spowoduje, że konkretne miejsce zostanie zmodyfikowane przez sieć. Nowa rola

33 P. Sienkiewicz, *25 wykładów...*, op. cit., s. 121–122.
34 H.J. Hatch, *Teoria organizacji*, Warszawa 2002, s. 195.
35 R. Wawrzyniec, *Koncepcja Governance...*, op. cit., s. 73–74.

administracji publicznej polega na umieszczeniu przestrzeni lokalnej i/lub regionalnej w przestrzeni globalnej[36].

Opisywane zmiany związane z rozwojem Internetu oraz upowszechnieniem technologii informacyjno-komunikacyjnych doprowadziły m.in. do globalizacji zjawisk społecznych, gospodarczych i politycznych. Rolą administracji publicznej w wieku informacji jest koordynowanie działań podmiotów należących do różnych sektorów oraz zarządzanie złożonymi sieciami społecznościowymi, a także dostosowanie sposobu funkcjonowania administracji publicznej do wykorzystania nowych technologii.

W Polsce, podobnie jak w innych krajach Unii Europejskiej, przyjęto założenie, że zastosowanie nowych technologii informacyjno-komunikacyjnych powinno być generatorem rozwoju społecznego i gospodarczego kraju, przy czym znaczną rolę w tym procesie przypisuje się zmianie funkcjonowania administracji publicznej opartej na przyjaznych i przejrzystych obywatelowi strukturach administracyjnych przy wykorzystaniu technologii ICT. Charakteryzując administrację publiczną w wieku informacji, należy podkreślić, że jest ona jednym z ważniejszych użytkowników nowoczesnych narzędzi i technik teleinformatycznych, albowiem funkcjonowanie administracji polega lub opiera się na przetwarzaniu informacji; dlatego też informacja jest podstawowym zasobem administracji. Istotnym aspektem jest wspomaganie procesów komunikacji państwo–obywatel, które dzięki możliwościom oferowanym przez techniki informatyczne może odbywać się na niespotykaną dotąd skalę.

Transformacje zachodzące w funkcjonowaniu administracji publicznej nie wynikają jedynie ze zmian w otoczeniu, ale także ze słabości związanych z modelem idealnej biurokracji. Z taką interpretacją nie zgodziłby się najprawdopodobniej M. Weber, który podkreślał, że biurokracja jest najbardziej racjonalną formą rządzenia państwem[37]. Od czasów Webera wiele się jednak zmieniło. Takie pojęcia jak *państwo* czy *rządzenie państwem* nabrały nowego znaczenia. Państwo w coraz mniejszym stopniu oznacza suwerena, zarówno w stosunkach wewnętrznych, jak i zewnętrznych. Jest ono jednym z elementów złożonej sieci decyzyjnej uwzględniającej zarówno interesy narodów, jak i organizacji międzynarodowych. Rządzenie państwem przekształca się natomiast w *zarządzanie publiczne*, gdzie obywatele są nie tylko biernymi odbiorcami świadczeń, ale również w coraz większym stopniu aktywnymi uczestnikami procesu ich dostarczania[38].

36 Zob. M. Castells, *Społeczeństwo sieci*, Warszawa 2011.

37 Zob. M. Weber, *Biurokracja* [w:] *Wybór tekstów z socjologii stosunków politycznych*, cz. 2, red. J. Hochfeld, Warszawa 1961, s. 126–140.

38 A. Pawłowska, *Zasoby informacyjne...*, op. cit., s. 11.

W ostatnich latach w wielu państwach istnieje tendencja do modernizacji administracji publicznej, polegająca na odchodzeniu od modelu biurokracji. Celem tych transformacji jest zwiększenie skuteczności i efektywności instytucji publicznych, także w wymiarze efektywności ekonomicznej przy wykorzystaniu nowych technologii.

Z teoretycznego punktu widzenia zasadne jest porównanie modelu biurokracji z modelem nowego zarządzania publicznego oraz modelem *good governance* przez pryzmat kluczowych elementów właściwych dla tych teorii (tab. 1.2).

Tab. 1.2. Porównanie modeli zarządzania w administracji publicznej

	Model biurokratyczny	**Nowe Zarządzanie Publiczne (NPM)**	**Dobre Współzarządzanie (NWG)**
Podstawy teoretyczne	Nauki prawne, nauki o polityce	Teoria wyboru publicznego, nauki o zarządzaniu	Teoria instytucjonalna i teoria sieci
Organizacja państwa	Dominacja układów monocentrycznych	Dominacja układów samorządowych i autonomicznych	Społeczeństwo obywatelskie
Styl kierowania	Biurokratyczny – administrowanie	Menedżerski – zarządzanie	Partnerski – konsultowanie
Mechanizm alokacji zasobów/struktury organizacyjne	Hierarchia	Rynek oraz kontrakty	Sieci powiązań i kontrakty partnerskie
Charakter relacji	Dominacja i podporządkowanie	Konkurencja i współpraca	Równość i współzależność
Cel działań	Utrwalenie porządku	Wywołanie zmian	Budowanie porozumienia społecznego
Ukierunkowanie działań	Procedury	Efekty	Potrzeby
Baza wartości	Etos sektora publicznego	Skuteczność konkurowania oraz miejsce na rynku	Rozproszona

Opracowanie własne na podstawie: J. Czaputowicz, *Zarządzanie w administracji publicznej w dobie globalizacji*, „Służba cywilna" nr 11/2005, s. 24; R. Wawrzyniec, *Rozwój zarządzania publicznego*, dostęp: http://dspace.uni.lodz.pl:8080/ xmlui/bitstream/handle/11089/821/407-418.pdf?sequence=1.

Założenia modelu NWG stały się głównym celem modernizacji wielu państw na świecie. Także unijna polityka spójności wprowadziła koncepcję *good governance* w celu wypracowania możliwości wdrożenia jej założeń do zasad funkcjonowania sektora publicznego[39]. Podstawy teoretyczne warto skonfrontować z ich praktyczną realizacją, proces transformacji administracji publicznej odbył się bowiem w Polsce i w wielu innych krajach na świecie. Analizę ewolucji struktur

39 Zob. *Promoting good governance. European Social Fund thematic paper*, European Commission, January 2014.

administracyjnych w kontekście rewolucji informacyjnej oraz praktycznej realizacji modelu NWG można rozpatrywać także w kategoriach głównych cech biurokracji, gdyż jednym z głównych założeń reform administracyjnych jest odchodzenie od rozwiązań charakterystycznych dla modelu biurokratycznego.

Należy zauważyć, że praktyczna realizacja zasad *good governance* w wielu krajach odbywa się na wzór rozwiązań z sektora prywatnego, z wykorzystaniem zasad teorii organizacji i zarządzania określających ściśle sprecyzowane metody analizy organizacyjnej, projektowania i wdrażania (np. w Kanadzie, USA, Japonii). W rozwiniętych państwach demokratycznych można zaobserwować przekształcenie sztywnej, biurokratycznej struktury w elastyczną formę rządzenia, nawiązującą do metod kierowania w wolnorynkowych organizacjach gospodarczych.

W. Kieżun podkreśla, że *elementarną zasadą budowania czy reformowania wielkiego systemu administracji publicznej jest priorytet posiadania wizji jego całości i dynamiki jego zachowań z pełną świadomością struktury wewnętrznych więzi*[40]. Trudno bowiem sprawnie modernizować organizację na podstawie wyizolowanych jej części, bez świadomości relacji między tymi częściami, które wspólnie tworzą system organizacji.

Hierarchia organizacyjna jest charakterystyczna dla struktur administracyjnych opisanych przez M. Webera. W koncepcji NWG natomiast zostaje zastąpiona siecią powiązań i kontaktów partnerskich. Wielu autorów zauważa, że wykorzystanie ICT sprzyja spłaszczeniu struktur, a więc zmniejszeniu ich hierarchiczności[41]. Spłaszczenie struktury sprzyja skutecznemu zarządzaniu jednostkami administracji publicznej, ponieważ umożliwia łatwiejszą komunikację, stwarza także możliwość mniejszego sformalizowania relacji przełożony–podwładny oraz zmniejsza możliwość wypaczenia celów organizacji.

Już w 1958 roku P. Drucker zauważył, że *każdy dodatkowy szczebel czyni trudniejszym osiąganie wspólnego kierunku wzajemnego zrozumienia. Każdy dodatkowy szczebel wypacza cele i niewłaściwie ukierunkowuje uwagę. Każde ogniwo łańcucha tworzy dodatkowe napięcie i staje się dodatkowym źródłem bezładu, tarć i zastojów*[42]. Reguła ogólnej teorii systemów głosi, że wzrost liczby elementów w systemie wymaga niewspółmiernie dużego zwiększenia liczby przetwarzanych informacji i podejmowanych decyzji[43]. Także w założeniach projektu ONZ dotyczącego reformy administracyjnej dla krajów postkomunistycznych Europy Wschodniej czytamy, że *struktura administracji państwowej i samorządowej*

40 W. Kieżun, *Patologia transformacji*, Warszawa 2013, s. 280.

41 Szerzej: L. Porębski, *Elektroniczne oblicze polityki. Demokracja, państwo, instytucje polityczne w okresie ewolucji informacyjnej*, Kraków 2001, s. 138.

42 Cyt. za: W. Kieżun, *Sprawne zarządzanie organizacją. Zarys teorii i praktyki*, Warszawa 1997, s. 68.

43 W. Kieżun, *Patologia transformacji...*, op. cit., s. 281.

winna być możliwie prosta, z tendencją do minimalizowania liczby szczebli i jednostek[44]. Zatem o sprawności struktur decyduje m.in. budowa płaskich struktur z małą liczbą szczebli organizacyjnych.

Reformy administracji przeprowadzone w Polsce i ich założenia wzbudzały od początku wiele kontrowersji. Zdaniem W. Kieżuna: *Reforma administracji publicznej była przeprowadzona w sposób spontaniczny, nieprofesjonalny, bez wstępnej wizji całości systemu i całościowego programu działania. Pierwszy etap to samorządne gminy, ale natychmiast w tym samym roku budowa nowej terenowej struktury administracji państwowej, nazwanej jednostką pomocniczą urzędu wojewódzkiego. Następnie ośmioletni okres formowania dalszej koncepcji polegającej na gigantycznej rozbudowie administracji terenowej: powiaty i podwójne urzędy wojewódzkie, w dodatku z fikcją pełnej likwidacji wszystkich urzędów wojewódzkich, a jedynie przekształcenie ich na główne i zamiejscowe*[45]. W Polsce obserwuje się systematyczny wzrost zatrudnienia w strukturach administracji publicznej, przy jednoczesnym stale pogłębiającym się wzroście długu publicznego[46].

Istotną zasadą warunkującą odchodzenie od form biurokratycznych jest decentralizacja, która wiąże się z przekazaniem zadań do kompetencji jednostek znajdujących się najbliżej obywatela. Naturalnym skutkiem tego procesu wydaje się zmniejszenie centralnego aparatu państwowego. W Polsce zaprzeczeniem tej zasady była dynamiczna budowa do końca 1998 roku aparatu centralnej administracji. Należy zauważyć, że dzięki zastosowaniu nowych technologii w sektorze publicznym *odległość przestaje być decydującym czynnikiem w budowaniu struktur organizacyjnych*[47]. Wykorzystanie nowoczesnych technologii informatycznych umożliwia zatem nadzór i koordynację działań administracyjnych z odległych centrów kierowniczych.

Decentralizację administracji publicznej należy łączyć z zasadą pomocniczości (subsydiarności), której podstawowym założeniem jest realizacja zadań publicznych przez jednostki najniższego szczebla. Na szczeblu wyższym powinny być podejmowane te działania, których przeniesienie na ten szczebel oznacza większą skuteczność i efektywność. W Polsce najbliżej obywatela znajduje się gmina, dlatego też w niej powinny być wykonywane zasadnicze zadania publiczne. Wspomniane kontrowersje wobec reformy administracji publicznej wiązały się ze sporem na temat utworzenia kolejnej po gminie jednostki podziału terytorialnego, jakim jest obecnie powiat. Przeciwnicy reformy w obecnym kształcie podkreślali, że intencja ustawy o samorządzie gminnym jest jednoznaczna – nie

44 Ibidem, s. 281.
45 Ibidem, s. 326.
46 Zob. dane Głównego Urzędu Statystycznego.
47 W. Kieżun, *Patologia transformacji...*, op. cit., s. 290.

wynika z niej potrzeba powoływania dalszych jednostek organizacyjnych między gminą a województwem[48]. W efekcie owych reform nie dostrzeżono światowych trendów związanych m.in. z koniecznością wdrożenia rozwiązań właściwych dla sektora prywatnego oraz nie uproszczono struktury administracji publicznej.

Podsumowując te wstępne rozważania na temat teorii i praktyki zastosowania nowych technologii w administracji publicznej, warto przywołać fragmenty jednego z raportów na temat wdrażania *good governance* w Polsce[49]:

- Polska w porównaniu do innych państw znajduje się na dalekich miejscach w większości rankingów opisujących stopień realizacji zasady dobrego rządzenia;
- Polska jest nadal krajem niedokończonej transformacji ustrojowej, gdzie wiele instytucji państwa nosi na sobie piętno *ancien régime*[50] (zjawisko *path dependence*[51]);
- wiele regulacji prawnych, importowanych z zewnątrz, nie jest dostosowanych do lokalnych uwarunkowań (nieudana imitacja rozwiązań instytucjonalnych);
- pierwszemu okresowi transformacji towarzyszyły przede wszystkim działania na rzecz budowy wolnego rynku i lekceważono poniekąd inicjatywy na rzecz poprawy sprawności państwa;
- najlepsze rezultaty w realizacji zasady *good governance* Polska odnosi w tych obszarach, które regulowane są przez rynek, a nie przez bezpośrednie działanie państwa;
- niepokojącym zjawiskiem jest niezdolność państwa do formułowania i realizowania długookresowych strategii rozwojowych, co może prowadzić do obniżenia konkurencyjności gospodarki.

Mamy współcześnie do czynienia z gwałtownym rozwojem technologii, który doprowadził do globalizacji w wielu sferach funkcjonowania państwa i społeczeństwa. Z teoretycznego punktu widzenia zjawiska te wpływają na spłaszczenie struktur administracyjnych. W praktyce jednak w Polsce obserwuje się wręcz od-

48 W. Kieżun, *Patologia transformacji...*, op. cit., s. 286.

49 *Badanie dotyczące stworzenia systemu wskaźników dla oceny realizacji zasady good governance w Polsce. Raport końcowy*, Warszawa 2008, dostęp: https://www.ewaluacja.gov.pl/Wyniki/Strony/Good_Gove rnance.aspx.

50 Zwrot zaczerpnięty z języka francuskiego (fr. dawny ustrój), odnoszący się do okresu sprzed rewolucji francuskiej oraz używany przenośnie na określenie starego ładu, ustroju politycznego, który należy już do przeszłości, uległ wyraźnej zmianie.

51 „Pułapka gorszego produktu" (*path dependence*) opisuje sytuację, w której niezbyt znaczące zależności początkowe, czy też różnice w rynkowych warunkach początkowych, prowadzą do wyniku, który jest nieefektywny, mimo że rozwiązanie optymalne (społecznie efektywne) było znane i osiągalne w momencie dokonywania wyboru pomiędzy dwoma rozwiązaniami. Na podstawie: R. Kowalski, *Efekty sieciowe a błędy rynku*, dostep: http://www.mikroekonomia.net/system/publication_files/1308/original/10.pdf?1315306917.

wrotną tendencję. Wyzwaniem dla polskiej administracji publicznej jest dostosowanie jej do funkcjonowania w nowych warunkach, zastosowanie rozwiązań ICT w sektorze publicznym oraz praktyczne wdrożenie modelu NWG.

1.3. Zarządzanie jakością usług publicznych

Przeobrażenia administracji publicznej w społeczeństwie informacyjnym można rozpatrywać w kontekście doskonalenia funkcjonowania i podnoszenia jakości usług publicznych. Zasadniczym wyzwaniem stało się zapewnienie sprawnej realizacji zadań publicznych. Istotnym problemem jest takie kształtowanie struktury administracyjnej, żeby jak najpełniej zaspokajać potrzeby i oczekiwania obywateli oraz optymalizować wykorzystywanie ograniczonych zasobów. Otoczenie wymusza stałe doskonalenie administracji publicznej.

Punktem wyjścia do charakterystyki jakości usług publicznych jest wyjaśnienie istoty i cech usług publicznych. Realizacja usług publicznych jest głównym zadaniem stawianym jednostkom samorządu terytorialnego. *Usługa publiczna jest świadczeniem, którego celem jest bieżące, nieprzerwane zaspokajanie zbiorowych potrzeb ludności w drodze świadczeń powszechnie dostępnych*[52]. Z przywołanej definicji wynika, że głównym celem usług publicznych jest zaspokajanie potrzeb społeczeństwa. Współcześnie zaspokajanie tych potrzeb jest podstawowym przeznaczeniem samorządu terytorialnego.

W literaturze często podkreśla się postrzeganie usług publicznych w kontekście interesu publicznego, rozumianego jako służenie celom wyższym, najważniejszym z punktu widzenia całej wspólnoty[53]. Do głównych i specyficznych cech usług publicznych można zaliczyć[54]:

- podatność na zmiany społeczno-polityczne;
- brak konkurencji w sferze usług administracyjnych;
- przymus korzystania;
- subiektywny sposób percepcji i oceny;
- finansowanie przez odbiorcę w sposób pośredni przez podatki.

Większość usług ma charakter niematerialny, co odróżnia je w istotny sposób od produktu, a jednocześnie ma znaczący wpływ na zarządzanie jakością. Problematyka jakości usług publicznych jest niewątpliwie jednym z efektów

52 U. Kobylińska, *Mierniki sprawności usług publicznych*, „Współczesne Zarządzanie" nr 2/2013, s. 133.

53 Por. B. Kożuch, A. Kożuch, *Istota współczesnych usług publicznych* [w:] *Usługi publiczne. Organizacja i zarządzanie*, red. B. Kożuch, A. Kożuch, Kraków 2011, s. 33–34.

54 M. Czerska, *Obsługa interesanta w urzędzie*, „Współczesne zarządzanie" nr 4/2005, s. 5–6.

nowego modelu zarządzania sektorem publicznym. Jednostki administracyjne traktuje się coraz częściej jako dostawcę specyficznych usług. Podstawowe funkcje urzędów są analizowane z punktu widzenia klienta zewnętrznego (obywatela) lub wewnętrznego (innej jednostki administracji, innego urzędu). Odpowiedzialność za dostarczenie usługi oznacza zapewnienie jej dostępności oraz odpowiedniego poziomu jakości. Stąd obowiązkiem administracji publicznej jest zapewnienie usługom publicznym odpowiednich standardów.

Usługę publiczną można zatem scharakteryzować w kategoriach standardu, który reguluje jego funkcjonowanie. Pojęcie standardu w *Słowniku języka polskiego* ma dwa interesujące nas znaczenia[55]: 1) poziom towarów lub usług, zwłaszcza spełniający podstawowe wymagania; 2) typowy i przeciętny model czegoś. W przywołanych określeniach można zauważyć zasadniczą różnicę: pierwsze z nich odnosi się do określonego minimum w poziomie towarów lub usług, w drugim zaś przypadku słowo to oznacza pewien typowy model.

J. Boczoń podaje kilka ujęć standardu usług[56]:

- podanie możliwie pełnego opisu usługi – od charakterystyki problemu, który wykonanie określonej usługi ma ograniczać, aż po określenie zasad ewaluacji jakości usługi;
- kryterium jakości wykonywanych usług;
- wartości docelowe, do osiągnięcia których się dąży (specyfikacja usługi – jej szczegółowy opis).

Standardy mogą wynikać z przepisów prawa lub z innych pozaprawnych przyczyn. Mogą przykładowo dotyczyć warunków umowy zawartej między jednostką samorządu terytorialnego a firmą, która wykonuje określone usługi publiczne[57]. Standard powinien zawierać określone elementy, jednak nie opracowano uniwersalnego schematu budowy standardu usługi. Powyższe rozważania skłaniają do wniosku, że usługa publiczna wymaga zaprojektowania procesu jej świadczenia, w którym można wyróżnić następujące elementy:

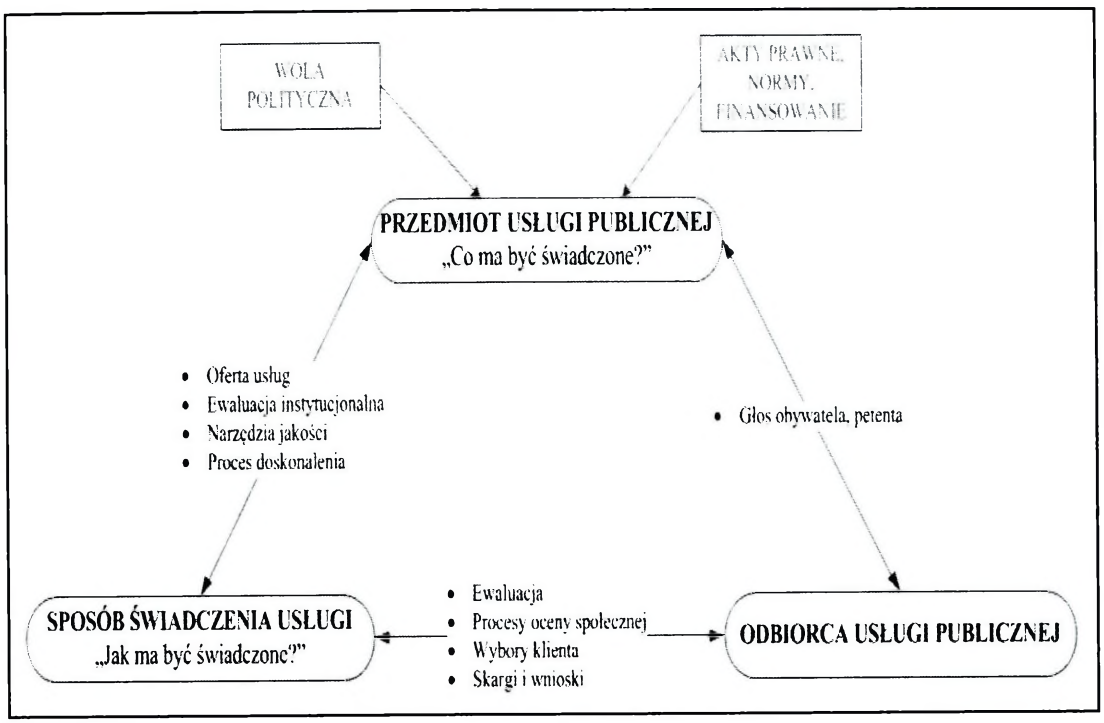
- standard usługi;
- sposób świadczenia usługi;
- doskonalenie sposobu świadczenia usługi.

55 *Słownik języka polskiego*, dostęp: http://sjp.pwn.pl/szukaj/standard.

56 J. Boczoń, *Poradnik standaryzacji usług społecznych*, Warszawa 2004, s. 18–21, cyt. za: R. Szarfenberg, *Standardy i standaryzacja pracy socjalnej i usług pomocy i integracji społecznej* [w:] *Pomoc i integracja społeczna wobec wybranych grup – diagnoza standaryzacji usług i modeli instytucji*, „Krajowy Raport Badawczy", red. R. Szarfenberg, Warszawa 2011, s. 30.

57 J. Duda, A. Jeżowski, W. Misiąg et. al., *Mierzenie ilości i jakości usług publicznych jako element programu rozwoju instytucjonalnego. Projekt naukowo-badawczy*, Instytut badań nad gospodarką, Warszawa 2014, s. 14.

Dostarczenie usług powinno uwzględniać także uwarunkowania mające wpływ na jej jakość. Wymienione elementy są istotnymi czynnikami procesu świadczenia usług publicznych (rys. 1.6).



Opracowanie własne.

Rys. 1.6. Model procesu świadczenia usług publicznych

Usługi publiczne dzieli się na usługi administracyjne, publiczne o charakterze społecznym oraz publiczne o charakterze technicznym. Zastosowanie nowoczesnych technologii w administracji publicznej przyczyniło się do powstania e-usług, dlatego przywołana taksonomia uwzględnia także e-usługi publiczne (tab. 1.3).

Tab. 1.3. Klasyfikacja usług publicznych

Kategorie usług publicznych	Przykłady usług
Usługi i e-usługi administracyjne	Wydawanie dokumentów, zezwoleń, koncesji, decyzji administracyjnych, wprowadzanie do baz danych
Usługi i e-usługi społeczne	Ochrona zdrowia, oświata i wychowanie, kultura, kultura fizyczna i rekreacja, pomoc i opieka społeczna, mieszkalnictwo, bezpieczeństwo publiczne
Usługi techniczne	Transport – usługi i infrastruktura, gospodarka odpadami oraz utrzymanie czystości i porządku, zaopatrzenie w energię, zieleń publiczna

Źródło: B. Kożuch, A. Kożuch, *Istota współczesnych usług publicznych*..., op. cit., s. 41.

Funkcjonowanie jednostek administracji publicznej ocenia się przez pryzmat uzyskiwanych rezultatów. Prawo do dobrej administracji, czyli spełniającej oczekiwania obywateli w zakresie jakości świadczonych usług, zawarto w art. 41 Karty Praw Podstawowych Unii Europejskiej[58]. Termin *jakość* posiada wiele definicji i interpretacji. Wynika to z subiektywnego charakteru postrzegania tej kategorii oraz przemian związanych z rozwojem ludzkości i zachodzących zmian jakościowych. Pojęcie jakości jest także różnie postrzegane w zależności od dziedziny nauki. Jest ono zatem wielowymiarowe i interdyscyplinarne.

Pojęcie jakości pochodzi z czasów starożytnych. Przyjmuje się, że po raz pierwszy zostało użyte przez Platona, który zdefiniował *jakość konkretnych rzeczy jako stopień osiąganych przez nie doskonałości*[59]. Przywołana definicja jest zbieżna z występującym współcześnie utożsamianiem jakości ze stopniem spełnienia przez przedmioty stawianych im wymagań.

Inaczej jakość interpretował Arystoteles – *jakością nazywał to, na mocy czego rzeczy są w pewien sposób określone*[60]. Zatem postrzegał on jakość jako zespół cech odróżniających daną rzecz od innych. Można uznać, że był zwolennikiem stworzenia obiektywnego zbioru cech opisujących dany przedmiot.

Oprócz przywołanych, przykładowych ujęć filozoficznych, można wyróżnić także jakość w ujęciu np. socjologicznym, humanistycznym, technicznym czy ekonomicznym.

M. Bugdol wyróżnia osiem podstawowych aspektów definicyjnych pojęcia jakości[61]:

- transcendentalny – jakość to coś, do czego stale dążymy, lecz znajduje się to poza naszym zasięgiem;
- produktowy – jakość jest zestawem cech decydujących o trwałości i funkcjonalności;
- użytkownika – jakość określa stopień zdolności do zaspokojenia potrzeb;
- wytwórcy – jakość jako stopień zgodności z wyspecjalizowanymi wartościami definiowanymi przez projekty i procesy technologiczne;
- wartości – stanowi różnicę pomiędzy korzyściami, jakie uzyskujemy w wyniku nabycia i użytkowania produktu, a jego ceną;
- strat społecznych – jakość występuje wtedy, kiedy wyroby nie doprowadzają do strat społecznych;

58 Zob. Karta Praw Podstawowych Unii Europejskiej, Nicea 2000.

59 A. Bielawa, *Postrzeganie i rozumienie jakości – przegląd definicji*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania" nr 21, s. 143.

60 Ibidem, s. 144.

61 M. Bugdol, *Zarządzanie jakością w urzędach administracji publicznej*, Warszawa 2008, s. 18, cyt. za: T. Skierniewski, *Diagnoza modelu zarządzania jakością w administracji rządowej. Raport z I etapu badań*, Warszawa 2008, s. 12.

- wielowymiarowe – jakość ma wiele cech, opiera się o cechy jakości usługi i modele samooceny;
- strategiczne – jakość to coś, co pozwala odróżnić jeden wyrób od innych wyrobów dostarczanych na rynek przez inne organizacje: w tym wypadku jakość stanowi element strategii, której celem jest uzyskiwanie zysków za pomocą wyrobów o wysokiej jakości.

Koncepcja zarządzania jakością w jednostkach administracji publicznej została zaczerpnięta z sektora prywatnego. Wielokrotnie jakość traktuje się jako swoiste *novum* w sektorze publicznym, jednak należy zauważyć, że odgrywała ona w administracji publicznej zawsze istotną rolę, choć jej postrzeganie zmieniało się w czasie.

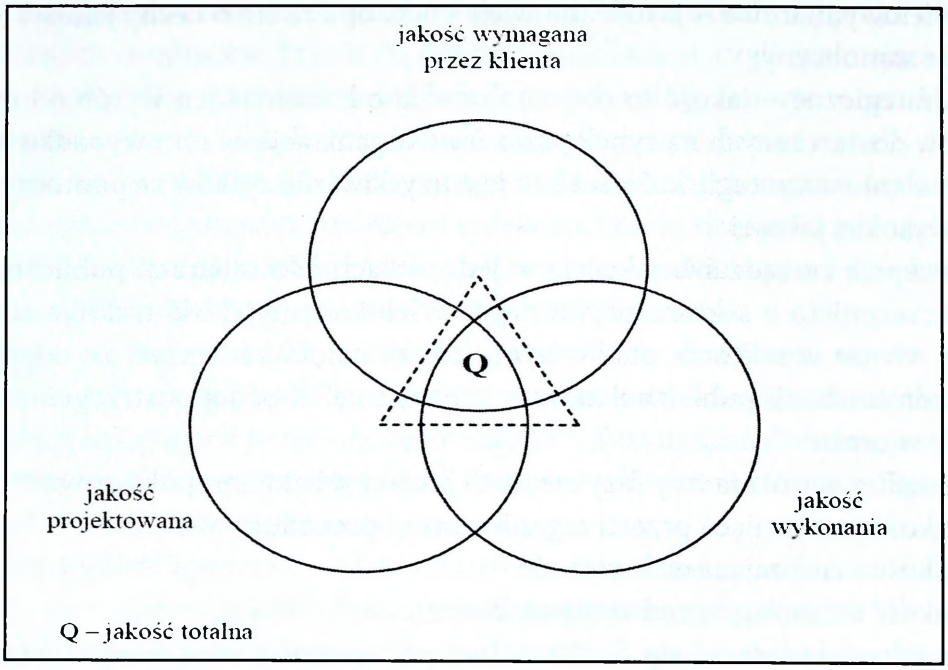
E. Loeffler wyróżnia trzy fazy ewolucji jakości w sektorze publicznym[62]:
- jakość oznaczająca przestrzeganie norm i procedur;
- jakość oznaczająca efektywność;
- jakość oznaczająca zadowolenie klienta.

Pierwsza faza odnosi się do formalnej poprawności związanej z przestrzeganiem przepisów prawa. W tym ujęciu nie ma odniesienia do odbiorcy usługi (obywatela). Druga faza związana jest z odniesieniem koncepcji zarządzania przez cele do sektora publicznego. Wówczas pojęcie jakości zaczęto postrzegać w kategoriach produktu i celu. Ostatnia faza związana jest z koncepcją kompleksowego zarządzania jakością (TQM), która w latach osiemdziesiątych ubiegłego wieku w Ameryce Północnej i Europie Zachodniej została przeniesiona z sektora prywatnego do publicznego.

Przywołane podejście – TQM – charakteryzuje się wykorzystaniem nowoczesnych technik zarządzania jakością. W prezentowanym ujęciu jakość determinowana jest funkcjonowaniem wszystkich podsystemów organizacji (instytucji) oraz jej otoczeniem. Podnoszenie jakości wiąże się z systemowym ujęciem instytucji, stałym doskonaleniem realizowanych procesów, zaangażowaniem pracowników oraz podnoszeniem ich wiedzy i umiejętności, a także podnoszeniem warunków pracy.

Syntetyczna analiza definicji i sposobu postrzegania jakości skłania do wniosku, że brak jednoznacznej i powszechnie akceptowanej definicji związany jest z jej subiektywizem i względnością (subiektywna ocena odbiorcy). Zarządzanie jakością polega nie tylko na identyfikacji oczekiwań odbiorcy usługi, ale także na monitorowaniu zadowolenia klienta. W literaturze podkreśla się, że odbiorca jest najbardziej usatysfakcjonowany, gdy jakość projektowana i jakość wykonana (faktyczna) będą zgodne z jakością przez niego oczekiwaną (rys. 1.7).

62 E. Loeffler, *Defining Quality in Public Administration*, 2002, s. 6, cyt. za: T. Skierniewski, *Diagnoza modelu zarządzania jakością...*, op. cit., s. 14.



Źródło: T. Wawak, *TQM w warunkach polskich*, materiały szkoleniowe, Mikołajki 1998, cyt. za: W. Gryncewicz, *Doskonalenie jakości informacji w jednostkach administracji skarbowej. Podejście infologiczne*, praca doktorska, Wrocław 2007, s. 74.

Rys. 1.7. Zależności między jakością projektowaną, wykonaną i wymaganą przez klienta

Poszczególne okręgi przedstawione na rys. 1.7 oznaczają jakość projektowaną, wykonaną i oczekiwaną przez odbiorcę. Najbardziej pożądana jest sytuacja, gdy wszystkie trzy wzajemnie się pokrywają. Widoczna na rysunku część wspólna będzie wtedy największa, co oznacza skuteczne wdrożenie zarządzania jakością w instytucji[63]. W praktyce jakość totalna nigdy nie zostaje osiągnięta, jednak instytucje publiczne powinny do niej dążyć w celu podnoszenia poziomu zaspokajania potrzeb odbiorców.

Wyróżnia się siedem czynników mających wpływ na jakość usług: relacje i postawy klientów, infrastrukturę techniczną, czynniki środowiskowe (obecność innych, infrastrukturę), czynniki behawioralne (np. jakość interakcji, czynniki stymulujące), czynniki sytuacyjne i organizacyjne, potrzeby i ich hierarchię, oczekiwania klientów[64]. W kontekście powyższych stwierdzeń współczesne postrzeganie jakości związane jest z wymaganiami odbiorców, czyli ze stopniem, w jakim dana usługa zaspokaja potrzeby (oczekiwania).

Jakość usług publicznych należy łączyć także z zapewnieniem bezpieczeństwa i niezawodnością usług, zdolność usługodawcy do zrealizowania usługi w sposób

63 W. Gryncewicz, *Doskonalenie jakości informacji...*, op. cit., s. 75.
64 M. Bugdol, *Zarządzanie jakością w urzędach...*, op. cit., s. 27.

niezawodny i solidny jest bowiem jednym z podstawowych wymiarów jakości. Warto zauważyć, że zagrożenia cyberprzestrzeni państwa mogą w istotny sposób obniżyć jakość usług publicznych.

Współczesna koncepcja zarządzania jakością w administracji publicznej charakteryzuje się podejściem procesowym, zorientowanym na analizę i zarządzanie wszystkimi elementami administracji. Ponadto zwraca się szczególną uwagę na konieczność opracowania mechanizmów umożliwiających stały proces doskonalenia. Zarządzanie jakością staje się wiec integralnym elementem zarządzania administracją publiczną.

Wyróżnia się wiele modeli, zasad oraz metod zarządzania jakością. Modelem, na który warto zwrócić szczególną uwagę, jest System Zarządzania Jakością według normy ISO 9000. Rodzina standardów ISO 9000 składa się z trzech głównych norm:

- ISO 9000 – Systemy zarządzania jakością. Podstawy i terminologia;
- ISO 9001 – Systemy zarządzania jakością. Wymagania;
- ISO 9004 – Systemy zarządzania jakością. Wytyczne doskonalenia.

Ponadto do tej grupy zalicza się szereg dodatkowych standardów i raportów technicznych, które dotyczą wybranych elementów zarządzania organizacją. Przykładowo[65]:

- ISO 19011 – Wytyczne dotyczące audytowania systemów zarządzania jakością i/lub zarządzania środowiskowego;
- ISO/TR 10013 – Wytyczne dotyczące dokumentacji systemu zarządzania jakością;
- ISO/TR 10017 – Wytyczne dotyczące technik statystycznych odnoszące się do ISO 9001:2000.

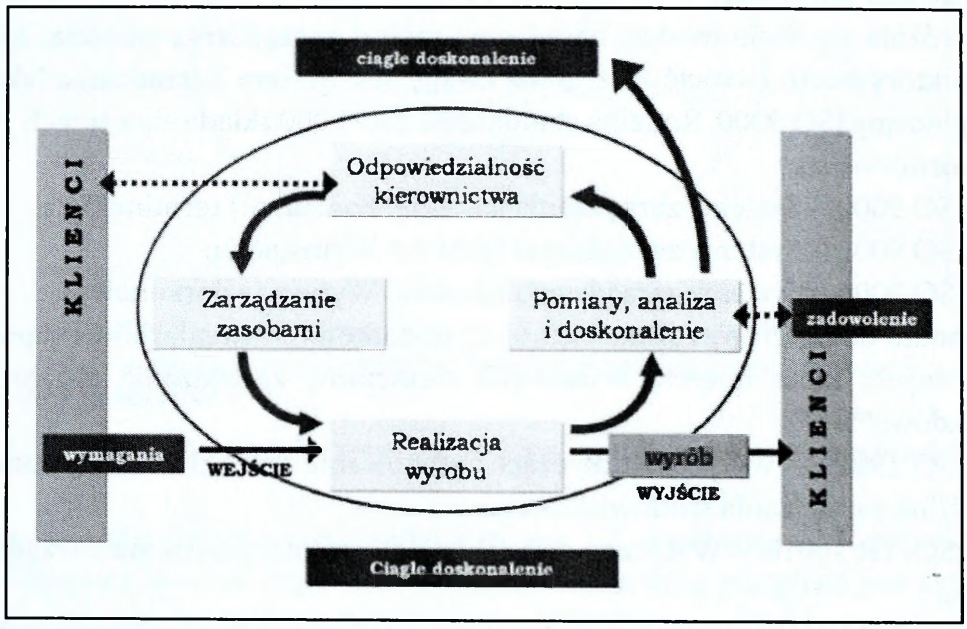
System zarządzania jakością oparty na wymaganiach normy ISO pozwala na dostosowanie działania do wymagań obywateli. Wprowadzenie normy w urzędzie zmienia jego pracę. Z organizacji nastawionej na spełnienie określonych wymagań prawnych, administracja publiczna staje się organizacją nastawioną na klienta[66]. Podstawą omawianego modelu jest podejście procesowe, które zakłada, że pożądaną jakość osiąga się z większą skutecznością, jeżeli zarządza się procesami zachodzącymi w organizacji oraz związanymi z nią zasobami. Zatem istota podejścia procesowego sprowadza się do systematycznej identyfikacji procesów zachodzących w jednostce administracji publicznej, określenia oddziaływania miedzy tymi procesami oraz zarządzania nimi. Warto zauważyć, że w omawianym

65 http://www.strefa-iso.pl/iso-podstawy.html.

66 J. Snopko, *Usługi administracyjne w świetle koncepcji zarządzania w administracji samorządowej* [w:] *Usługi publiczne. Organizacja i zarządzanie*, red. B. Kożuch, A. Kożuch, Kraków 2011, s. 128.

podejściu bardzo często wyjście jednego procesu stanowi wejście dla drugiego procesu.

Istotnym elementem wdrażania modelu jest zrozumienie roli oraz oczekiwań obywatela (klienta). Jednostka administracji publicznej funkcjonuje w powiązaniu z odbiorcami usług publicznych, dostawcami oraz innymi urzędami, dlatego też procesy powinny być planowane, realizowane, doskonalone pod kątem spełnienia wymagań odbiorcy. Rys. 1.8 przedstawia model systemu zarządzania jakością według normy ISO.



Źródło: *PN-EN ISO 9001 Systemy zarządzania jakością. Wymagania*, Warszawa: Polski Komitet Normalizacyjny 2001, punkt 0.2, dostęp: http://www.ebib.pl/2006/77/kaminska.php.

Rys. 1.8. Model systemu zarządzania jakością, którego podstawą jest proces

Odpowiedzialność kierownictwa sprowadza się do ustalenia misji i polityki instytucji (organizacji) oraz do określenia planów działania i przyznania odpowiednich zasobów do realizacji założonych celów. Kierownictwo odpowiada za prawidłowe funkcjonowanie organizacji, dlatego też regularnie ocenia działalność oraz wykonywanie określonych zadań i realizację założonych celów. Na podstawie przeglądu działalności organizacji przydzielane są zasoby oraz podejmowane odpowiednie działania udoskonalające.

Współcześnie ważną rolę w podnoszeniu jakości świadczenia usług publicznych odgrywa zaplecze technologiczne. Zastosowanie technologii w sektorze publicznym przyczyniło się do powstania e-administracji. Informacja jest coraz częściej przechowywana, przetwarzana i udostępniana w elektronicznych systemach przetwarzania danych. Pomimo wymienionych skrótowo zalet wykorzystania nowych technologii w sektorze publicznym, należy mieć na uwadze powstanie

nowego obszaru zagrożeń, który może wpływać negatywnie na jakość świadczonych usług. Jednym z fundamentalnych priorytetów w omawianym obszarze jest zapewnienie ciągłości i niezawodności świadczonych usług, dlatego też problematyka skutecznego zarządzania aktywami informacyjnymi przy zachowaniu standardów bezpieczeństwa ma szczególne znaczenie w kontekście jakości usług administracji publicznej.

1.4. Zasoby i systemy informacyjne

Zasoby i systemy informacyjne są współcześnie obiektem zmian spowodowanych postępem naukowo-technicznym. Zasoby informacyjne postrzega się coraz częściej przez pryzmat zarówno strategicznego zasobu, jak i czynnika warunkującego sprawność działania – zarządzania organizacją. Procesy zachodzące w strukturach administracyjnych związane są z zarządzaniem informacją oraz zapewnieniem jej odpowiedniej jakości na każdym etapie funkcjonowania jednostek sektora publicznego. Zapewnienie bezpieczeństwa zasobów i systemów informacyjnych determinuje odpowiednią jakość usług publicznych.

Literatura dotycząca pojęcia i klasyfikacji informacji jest obszerna. Od czasów sformułowania podstaw teorii informacji[67] powstało wiele różnych interpretacji omawianej kategorii, wśród których można wymienić:

- pojęcie ilości informacji według Shannona;
- pojęcie informacji według Ackoffa;
- nieprobabilistyczne ujęcia informacji (np. R. Ingardena i K. Urbanika);
- pojęcie informacji wynikłe z teorii oszacowania;
- pojęcie informacji związane z jej treścią (np. Bar-Hillela);
- pojęcie informacji związane z jej wartością (np. M. Mazura i K. Szaniawskiego)[68].

Jedną z popularnych interpretacji jest koncepcja, w której informacje są wynikiem przetwarzania danych – ich zbierania, analizy lub agregacji[69]. W systemie działania zarówno na wejściu, jak i na wyjściu różnych procesów transformacji można zidentyfikować określone kategorie zasobów informacyjnych, co oznacza, że informacja jest zasobem[70]:

67 W latach 1948–1949 C.E. Shannon ogłosił swoje prace z matematycznej teorii komunikacji, kładąc podwaliny współczesnej teorii informacji. Zob. C.E. Shannon, *The Mathematical Theory of Communication*, New York 1949.

68 P. Sienkiewicz, *Inżynieria systemów...*, op. cit., s. 63.

69 P. Beynon-Davies, *Inżynieria systemów informacyjnych*, Warszawa 1998, s. 15.

70 P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych determinantą technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" nr 9, 2013, s. 40.

- koniecznym do wytworzenia określonej wartości wyjściowej (produkt);
- powstającym w wyniku realizacji procesów transformacji, w tym procesów informacyjnych;
- posiadającym swoją wartość;
- determinującym sprawność całego systemu działania.

Nie ulega wątpliwości, że jednym z zasadniczych zadań informacji jest zwiększenie skuteczności realizacji określonego celu. Sposób tworzenia i wykorzystania informacji jest uzależniony od przeznaczenia określonego systemu. Informacja wiąże się z działaniem sprawnym i celowym, z czego niejako wynika też jej względność.

P. Sienkiewicz zauważa, że *do celów praktycznych wygodna jest następująca definicja: Informacje to zbiór faktów, zdarzeń, cech obiektów itp. zawarty w określonej wiadomości, tak ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe i fizyczne*[71]. Zdefiniowana w ten sposób informacja wpływa na decyzję lub działanie i może być klasyfikowana według dziedzin wiedzy (np. społeczna). Powiązanie informacji ze stanem niepewności wynika z konieczności podejmowania decyzji i dokonania wyboru.

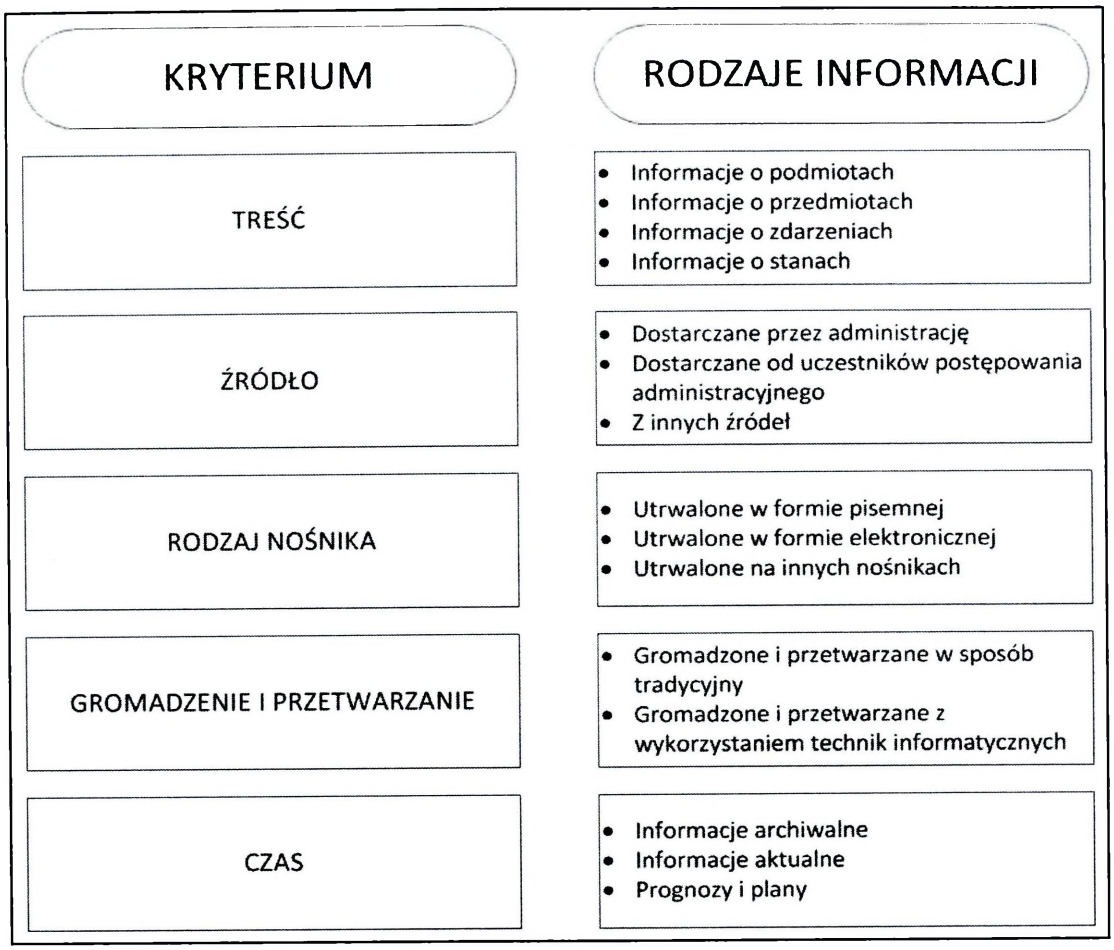
Z punktu widzenia obywatela i funkcjonowania administracji publicznej istotną kwestią jest prawo dostępu do informacji publicznej. Zgodnie z definicją ustawową, informacja publiczna to *każda informacja o sprawach publicznych*[72]. M. Luterek podkreśla, że *najlepiej identyfikowalnym jako informacja publiczna jest ten zbiór informacyjny, który odnosi się bezpośrednio do działań i zasad funkcjonowania poszczególnych instytucji*[73]. Prawo dostępu do informacji publicznej jest uznawane w państwach demokratycznych za jedną z fundamentalnych zasad konstytucyjnych. Umożliwia ono kontrolę funkcjonowania organów państwa i jednostek podejmujących decyzje oraz sprzyja realizacji celów społeczno-gospodarczych. *Dostęp do informacji publicznej jest również kluczowym czynnikiem przy zwalczaniu korupcji, będąc ściśle związany z wolnością słowa i niezależnością mediów*[74]. Informacje gromadzone przez administrację publiczną można klasyfikować według różnych kryteriów (rys. 1.9).

71 P. Sienkiewicz, *Inżynieria systemów...*, op. cit., s. 61.

72 Art. 1 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2014 r. nr 0, poz. 782 ze zm.)

73 M. Luterek, *eGovernment. Systemy informacji publicznej*, Warszawa 2010, s. 29.

74 B. Fischer, *Granice dostępu do informacji – tajemnice ustawowo chronione na przykładzie informacji publicznych, informacji niejawnych i prawa do prywatności* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007, s. 32.



Opracowanie własne.

Rys. 1.9. Klasyfikacja informacji gromadzonych w administracji publicznej

Współcześnie informacje są jednym z zasobów oraz podstawą funkcjonowania każdej organizacji[75]. W klasycznej ekonomii przyjmuje się, że na zasoby organizacji składają się zasoby materialne (fizyczne), zasoby finansowe oraz zasoby ludzkie. W latach siedemdziesiątych XX wieku do rangi zasobów podniesiono informację, a na przełomie ostatnich stuleci wiedzę. Zasoby informacyjne w połączeniu z innymi zasobami współdecydują o rozwoju społeczeństwa i gospodarki.

W rozważaniach J. Oleńskiego zasób informacyjny *stanowią wszelkie potencjalnie użyteczne zbiory informacji i metainfromacji, zgromadzone i przechowywane w czasie, w miejscu oraz przy wykorzystaniu technologii i organizacji umożliwiających ich wykorzystanie przez użytkowników finalnych informacji*[76].

75 Por. J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Warszawa 2005, s. 13.

76 J. Oleński, *Elementy ekonomiki informacji. Podstawy ekonomiczne informatyki gospodarczej*, Warszawa 2000, s. 161.

Podobne ujęcie zasobu informacyjnego prezentuje A. Pawłowska, definiując zasób informacyjny jako *wszelkie dane, informacje oraz techniki informacyjne, które mogą być użyte do produkcji określonego dobra lub usługi*[77]. Wśród przykładowych zasobów informacyjnych w administracji publicznej można wyróżnić m.in. informacje o aktach normatywnych i polityce administracyjnej, informacje dostarczone przez stronę, akta sprawy, archiwa czy też np. dzienniki urzędowe.

W funkcjonowaniu struktur administracyjnych możemy mówić o dualizmie zasobów informacyjnych. Mianowicie mogą występować jako:

- przedmiot zarządzania (to, czym się zarządza);
- narzędzie zarządzania (to, co pomaga zarządzać).

Treść i zakres zarządzania zasobami informacyjnymi rozumiane są różnie w zależności od dziedziny nauki[78]. Koncepcja zarządzania zasobami informacyjnymi związana jest ze wspomnianym już podniesieniem informacji do rangi zasobu. Zarządzanie zasobami informacyjnymi, rozumiane jako środek optymalizacji i racjonalizacji procesów informacyjnych organizacji w państwie[79], jest jednym z najistotniejszych mechanizmów służących podnoszeniu efektywności wykorzystywania zasobów informacyjnych, a tym samym zwiększeniu stopnia zaspokajania potrzeb informacyjnych administracji[80]. Konieczność pozyskiwania wartościowych informacji oraz zarządzanie zasobami informacyjnymi wymaga systematycznych i celowych działań. Dlatego też informacje oraz narzędzia służące do ich przetwarzania oraz ludzi i struktury organizuje się w systemy informacyjne.

Według J. Kisielnickiego i H. Sroki system informacyjny to wielopoziomowa struktura, pozwalająca użytkownikowi tego systemu na transformowanie określonych informacji wejścia na pożądane informacje wyjścia za pomocą odpowiednich procedur i modeli[81].

Zdefiniowany w ten sposób system informacyjny ma następujący zbiór elementów:

77 A. Pawłowska, *Zasoby informacyjne...*, op. cit., s. 76.

78 Np. w teorii organizacji i zarządzania, systemów informacyjnych, technologii informacyjnej, informacji naukowej czy bibliotekoznawstwie.

79 P. Sienkiewicz, R. Wieleba, J. Wocial, M. Kuca, M. Skoczylas, *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych*, Warszawa 2002, s. 109.

80 P. Piasecka, *Cykl analityczny jako narzędzie w zarządzaniu bezpieczeństwem* [w:] *Analiza informacji w zarządzaniu bezpieczeństwem*, red. K. Lidel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2013, s. 30

81 J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu...*, op. cit., s. 13.

$$SI = \{P, I, T, O, M, R\}$$

gdzie:
SI – system informacyjny organizacji,
P – użytkownicy systemu,
I – zasoby informacyjne,
T – narzędzia techniczne,
O – rozwiązania systemowe stosowane w danej organizacji,
M – metainformacje,
R – relacje pomiędzy poszczególnymi elementami[82].

Jednym z podstawowych zadań systemu informacyjnego jest dostarczenie informacji odpowiednim podmiotom. Cel ten może być osiągnięty, jeżeli system informacyjny realizować będzie następujące funkcje[83]:

- wspomaganie transmisji;
- przechowywanie danych;
- przetwarzanie danych;
- prezentowanie informacji;
- przesyłanie informacji.

W tab. 1.4 wymienione funkcje zostały scharakteryzowane i opisane realizacją praktyczną.

Podstawową funkcją systemu informacyjnego jest informowanie. M. Mazur, autor jakościowej teorii informacji, zauważył, że między każdymi dwoma obiektami (systemami), z których jeden jest nadawcą, a drugi odbiorcą informacji, powstaje oddziaływanie informacyjne związane z wystąpieniem określonej sytuacji informacyjnej, które dokonuje się za pomocą kanału (toru) informacyjnego[84]. Odnosząc powyższe rozważania do systemu informacyjnego w strukturze administracyjnej, można wyróżnić:

- elementy podmiotowe, będące nadawcą oraz odbiorcą informacji;
- elementy przedmiotowe, obejmujące zbiory informacji, kanały informacyjne oraz techniczne środki przetwarzania danych.

Nadawcy informacji obejmują wyodrębnione w strukturze administracyjnej jednostki organizacyjne uczestniczące w przekazie i wymianie informacji. W administracji publicznej najczęściej są to osoby z dowolnego szczebla organizacyjnego. Natomiast wśród odbiorców informacji należy wymienić:

- odbiorców wewnętrznych – komunikacja wewnątrz struktury administracyjnej;
- odbiorców zewnętrznych – obywatele i przedsiębiorcy oraz inne jednostki administracji publicznej niezwiązane podległością służbową.

82 Ibidem, s. 19.

83 K. Mikulski, *Technologia informacyjna w administracji i dla administracji*, Bydgoszcz 2008, s. 90.

84 P. Sienkiewicz, *Systemy kierowania...*, op. cit., s. 128.

Tab. 1.4. Funkcje systemu informacyjnego w administracji publicznej

Funkcja	Charakterystyka	Realizacja praktyczna
Wspomaganie transmisji	– zbieranie – ewidencjonowanie – rejestrowanie danych – notowanie komunikatów gospodarczych	– wykorzystanie dokumentów źródłowych – formularzy o sprecyzowanych poleceniach dotyczących tego, jakie informacje należy zarejestrować
Gromadzenie danych	– klasyfikacja – weryfikacja merytoryczna i formalna – konwersja danych – kodowanie danych	– klasyfikowanie danych według określonych kryteriów – przyporządkowanie danych kodom identyfikującym – wyeliminowanie danych niespełniających wymogów merytorycznych i formalnych – zmiana postaci lub nośnika – operacje przeobrażenia jawnej postaci wiadomości w formę ukrytą w celu uniemożliwienia dostępu do przekazywanych informacji osobom niepowołanym
Przechowywanie danych	– czynności wykonywane w operacjach wejściowych związane z zapisaniem danych w postaci umożliwiającej ponowne wykorzystanie	– przechowanie danych występuje na trwałych nośnikach informatycznych bądź w formie tradycyjnej (papierowej)
Przetwarzanie danych	– obliczenia – agregacja – porównanie – filtrowanie – wyszukiwanie	– wykonanie w zaplanowany sposób dowolnych operacji matematycznych – tworzenie danych sumarycznych przy wykorzystaniu danych elementarnych – porównywanie danych i określenie między nimi relacji – dopuszczenie do dalszego przetwarzania danych – wyszukiwanie danych w celu dalszej obróbki
Prezentowanie danych	– dokumenty – raporty – wynik zapytań	– zapis danych w odpowiedniej formie – informacja operacyjna dotycząca działalności instytucji w postaci wyselekcjonowanych informacji – zapytanie rozumiane jest jako zgłoszenie przez użytkownika konieczności dostępu do określonych informacji
Przesyłanie informacji	– przemieszczenie zasobów informacyjnych (wewnętrznie) lub wymiana informacji z otoczeniem (zewnętrznie)	– wykonywanie dodatkowych operacji pomocniczych: kompletowanie, porządkowanie, konwersja ze względu na dany kanał komunikacyjny, kompresja, szyfrowanie

Opracowanie własne na podstawie: K. Mikulski, *Technologia informacyjna w administracji*..., op. cit., s. 90.

Zbiory informacji będące elementem przedmiotowym systemu informacyjnego obejmują różnego rodzaju dokumenty, np.: akty prawne, akty notarialne, wnioski, regulaminy, wytyczne i zarządzenia oraz decyzje administracyjne.

Kanały (tory) informacyjne są drogami przepływu informacji, które tworzą strukturę komunikacyjną. W strukturze administracyjnej można wyróżnić następujące rodzaje kanałów informacyjnych:

- kontakt osobisty, między pracownikami a petentami oraz między pracownikami;
- tradycyjne kanały informacyjne, np. poczta tradycyjna, telefon, faks, tablica ogłoszeń;
- komunikacja wykorzystująca sieć Internet i techniczne środki przetwarzania danych, np. pobranie elektronicznych formularzy, możliwość składania elektronicznych deklaracji podatkowych.

Techniczne środki przetwarzania danych obejmują sprzęt komputerowy i oprogramowanie w poszczególnych urzędach. Zalicza się do nich także dedykowane systemy informatyczne, np. system POLTAX[85], system CELINA[86], System Informacyjny Schengen.

W społeczeństwie informacyjnym szczególnego znaczenia nabiera zastosowanie nowych technologii w administracji publicznej. Istotnym aspektem architektury systemów informacyjnych jest ułatwienie pracy osobom odpowiedzialnym za funkcjonowanie danego systemu – wprowadzanie danych i zarządzanie informacją. Często prowadzi to do powstawania barier strukturalnych, ograniczających elastyczność systemu i jego możliwości adaptacji do zmieniających się potrzeb użytkowników zewnętrznych systemu. W przypadku systemów informacji publicznej integracja systemów pozwala przełamać te bariery oraz umożliwia usunięcie sztywnych podziałów tematycznych[87]. Sprowadza się to do stworzenia takiego systemu informacyjnego, w którym użytkownik nie jest zmuszony do kilkukrotnego wprowadzania tych samych informacji. Związane jest to z koniecznością zapewnienia systemom informatycznym interoperacyjności rozumianej jako *zdolność dwóch lub więcej systemów do wymiany informacji według wzajemnego wykorzystania wymienianej informacji*[88].

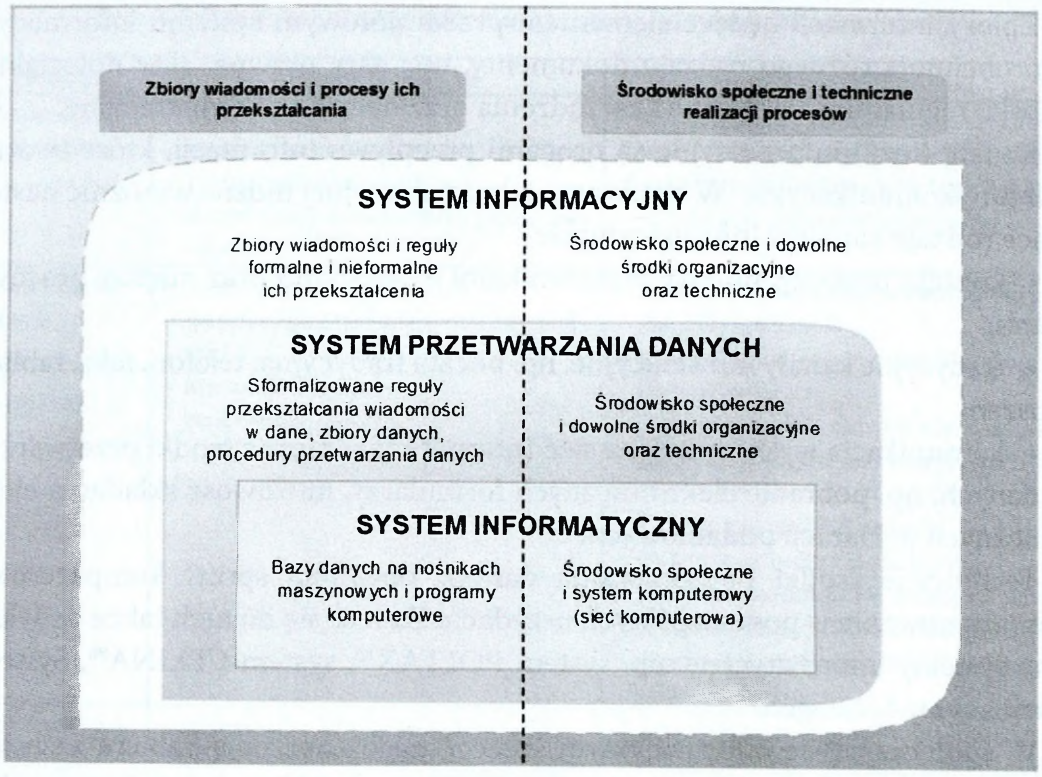
Systemu informacyjnego nie należy utożsamiać z system przetwarzania danych i system informatycznym (rys. 1–10).

85 System POLTAX – system ewidencjonowania i przetwarzania danych o podatnikach wykorzystywany w urzędach skarbowych, rozwijany i obsługiwany przez polskie Ministerstwo Finansów.

86 System CELINA – System Obsługi Deklaracji Podatkowych.

87 M. Luterek, *Systemy informacji publicznej...*, op. cit., s. 30.

88 P. Zaskórski, *Automatyzacja procesów dowodzenia*, Toruń 2001, s. 7.



Źródło: Z.J. Klonowski, *Systemy zarządzania przedsiębiorstwem. Model rozwoju i właściwości funkcjonalne*, Wrocław 2004, s. 181.

Rys. 1.10. Ogólny model relacji zachodzących między systemem informacyjnym, systemem przetwarzania danych i systemem informatycznym

System przetwarzania danych definiuje się jako złożony układ źródeł danych, zbiorów danych, kanałów przesyłania (sprzężenia), punktów gromadzenia danych, procedur ich przetwarzania oraz ludzi i środków technicznych realizujących te procesy. Natomiast przez system informatyczny rozumie się zautomatyzowany system przetwarzania danych[89]. System przetwarzania danych i system informatyczny są podzbiorami systemu informacyjnego. Obejmują one elementy, które są realizowane w systemie lub w sieci komputerowej.

Zasadniczy aspekt współczesnego funkcjonowania administracji publicznej jest realizowany w warunkach rozwoju systemów telekomunikacyjnych, systemów informatycznych i systemów masowego komunikowania. Dostępność technik informacyjnych spowodowała eksplozję informacji oraz powstanie różnego rodzaju zagrożeń dla bezpieczeństwa informacji. Stąd istotnym problem stało się zapewnienie jakości informacji. Jakość informacji wpływa na jej użyteczność rozumianą jako *cecha wyrażająca wpływ na wzrost efektywności działania*[90]. W celu

89 Z. J. Kolonowski, *Systemy zarządzania...*, op. cit., s. 181.
90 P. Sienkiewicz, *25 wykładów...*, op. cit., s. 195.

poprawy jakości informacji i usług w administracji publicznej, a także dostarczenia korzyści ekonomicznych w wielu państwach wdrażana jest koncepcja elektronicznej administracji.

1.5. Istota i warunki rozwoju elektronicznej administracji

Rozwój społeczeństwa informacyjnego oraz upowszechnienie nowoczesnych technologii przyczyniło się powstania i ciągłego rozwoju elektronicznej administracji. Rewolucyjny postęp technologiczny i powszechna komputeryzacja doprowadziły do unowocześnienia systemu informacji publicznej, opierającego się dotąd na nośnikach papierowych. Koncepcja elektronicznej administracji (e-administracji) z jednej strony zakłada umożliwienie obywatelom i przedsiębiorcom korzystanie z oferty usług publicznych za pośrednictwem Internetu; z drugiej zaś zastosowanie nowych technologii jest narzędziem transformacji struktur administracyjnych, sposobu ich działania i świadczenia usług publicznych.

W procesie transformacji struktur administracyjnych wypracowano katalog pojęciowy związany z procesem informatyzacji. Mimo to brakuje jednoznacznej definicji elektronicznej administracji, nieostre są także granice miedzy przywołanymi pojęciami. Wielokrotnie pojęcie elektronicznej administracji (e-administracji) jest utożsamiane z jej informatyzacją, koncepcją e-government czy też e-urzędem.

Koncepcja e-administracji jest odmiennie ujmowana i definiowana w państwach anglosaskich, w Unii Europejskiej, a także w organizacji Współpracy Gospodarczej i Rozwoju (OECD) oraz Organizacji Narodów Zjednoczonych[91]. Na świecie istnieją dwie podstawowe koncepcje rozwoju elektronicznej administracji – wąska i szeroka. Państwa azjatyckie (Japonia, Korea) oraz Stany Zjednoczone skupiają się na kwestii zapewnienia dostępu do usług świadczonych w formie elektronicznej. Szerzej e-administrację definiuje się w opracowaniach OECD, ONZ czy też UE.

W ujęciu Unii Europejskiej e-administracja to zintegrowane działanie zmierzające do stworzenia tańszej i skuteczniejszej administracji, co w rezultacie prowadzi do poprawy zarządzania państwem i obniżenia kosztów administracji[92]. W prezentowanym ujęciu elektroniczna administracja odnosi się nie tylko do kwestii dostępności usług świadczonych drogą elektroniczną, ale również

91 D. Grodzka, *E-administracja w Polsce* [w:] *Społeczeństwo informacyjne,* red. D. Grodzka, „Studia BAS" 2009, nr 3(19), s. 58

92 A. Dąbrowska, *Rozwój e-usług jako przejaw budowania społeczeństwa informacyjnego*, „Handel Wewnętrzny" 2009, nr 2, s. 39.

związana jest z przebudową i modernizacją struktur administracyjnych realizowanych na fundamencie nowoczesnych technologii.

W polskich opracowaniach termin e-government często tłumaczony jest jako elektroniczna administracja. Jednak interpretacja ta nie jest do końca precyzyjna. A. Dopierała zauważa, że pojęcie e-government *obejmuje nie tylko administrację rozumianą jako usługi świadczone przez instytucje publiczne, ale może też być rozszerzane na system rządów*[93]. Podobne zdania jest A. Bógdał-Brzezińska, stwierdzając, że elementami składowymi e-government jest zarówno e-administracja, jak i cyberdemokracja[94]. M. Luterek podkreśla, że e-government należy rozumieć jako elektroniczny system informacji i usług publicznych, a nie jako e-administrację[95]. Omawiany termin obejmuje także usługi oferowane przez jednostki sektora budżetowego, które wychodzą poza szeroko rozumianą administrację publiczną, np. biblioteki, uniwersytety, służbę zdrowia.

Natomiast informatyzacja administracji *oznacza działania odnoszące się do planowania, wdrażania, koordynowania i kontroli procesów związanych z wykorzystaniem nowoczesnych technologii przetwarzania informacji przez podmioty realizujące zadania publiczne*[96]. H. Izdebski i M. Kulesza zauważają, że proces informatyzacji administracji, z uwagi na liczbę i zróżnicowanie instytucji zaangażowanych w realizację funkcji państwa, jest ogromnym przedsięwzięciem pod względem organizacyjnym i finansowym i jako takie powinien przebiegać w ramach klasycznego cyklu działania organizatorskiego, obejmującego: ustalenie celu, określenie środków i metod, gromadzenie środków, działanie według zaplanowanych metod, kontrolę wyników[97]. Zatem istotnymi elementami w procesie informatyzacji są m.in. strategia informatyzacji instytucji publicznej, komórka (jednostka) ds. zarządzania zasobami informacyjnymi oraz zgodność (kompatybilność) systemu informacyjnego ze strukturą instytucji publicznej.

Kluczowym pojęciem związanym z wdrożeniem e-administracji jest cyfrowy urząd (e-urząd), rozumiany jako instytucja umożliwiająca obsługę interesanta przy pomocy technologii komputerowych on-line, tak aby złożenie wniosku, załatwienie sprawy oraz jej monitorowanie było przeprowadzone zdalnie, bezpiecznie,

93 A. Dopierała, Wywiad, „Prawo i gospodarka (dodatek), Magazyn finansowy" 2002, nr 216, s. 12.

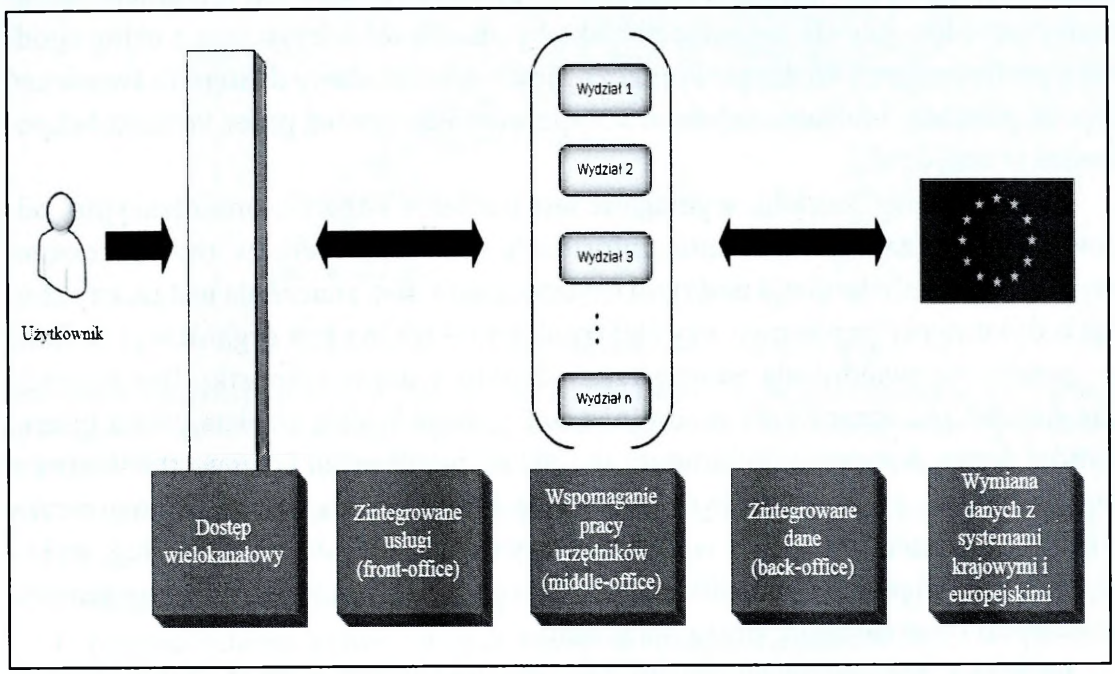
94 A. Bógdał-Brzezińska, *Społeczeństwo informacyjne a problemy rozwoju e-governmentu w Polsce* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 169.

95 Zob. M. Luterek, *eGovernment...*, op. cit.

96 P. Filgielski, *Informacja w administracji publicznej: prawne aspekty gromadzenia, udostępniania i ochrony,* Warszawa 2007, s. 164.

97 H. Izdebski, M. Kulesza, *Administracja publiczna...*, op. cit., s. 100.

terminowo oraz zgodnie z procedurami jawnymi społecznie[98]. Funkcjonowanie cyfrowego urzędu można scharakteryzować za pomocą jego części składowych: front-office, back-office oraz niekiedy wyróżniane middle-office (rys. 1.11).



Opracowanie własne na podstawie: M. Sakowicz, *Modernizacja samorządu terytorialnego w procesie integracji Polski z Unią Europejską*, Warszawa 2007, s. 155.

Rys. 1.11. Model funkcjonowania e-urzędu

Front-office to część infrastruktury urzędu odpowiedzialna za bezpośredni kontakt z obywatelem i przekazywanie (otrzymywanie) informacji, danych, dokumentów w relacjach z podmiotami zewnętrznymi. Back-office to część urzędu, na którą składają się systemy informacyjne, np. GIS (system informacji przestrzennej), rejestry, archiwa, bazy danych oraz hurtownie danych[99]. Administracja w wymiarze back-office charakteryzuje się elektroniczną komunikacją, dokumentami przesyłanymi w sposób elektroniczny, czynnościami wykonywanymi za pomocą aplikacji komputerowych i systemów teleinformatycznych, szybkim przetwarzaniem informacji, stałą aktualizacją i monitorowaniem informacji zwrotnej oraz wyspecjalizowaną kadrą urzędniczą. Natomiast middle-office to część

98 M. Sakowicz, *Zastosowanie nowych technologii informacyjno-komunikacyjnych w rządzeniu i zarządzaniu administracją publiczną* [w:] *Administracja publiczna u progu XXI wieku. Wyzwania i oczekiwania*, red. J. Osiński, Warszawa 2008, s. 80.

99 M. Sakowicz, *Modernizacja samorządu terytorialnego...*, op. cit., s. 154.

przeznaczona do bezpośredniego wspomagania pracy urzędników w generowaniu, przesyłaniu i przetwarzaniu informacji oraz w wyborze decyzji.

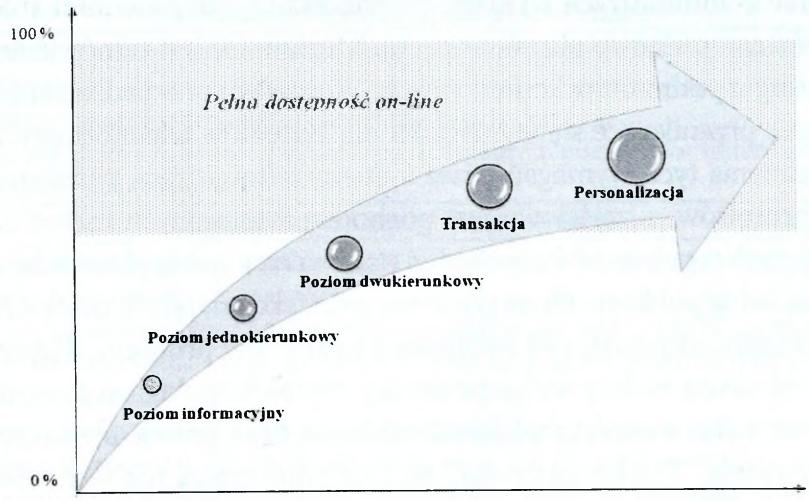
Z punktu widzenia interesanta istotne jest spełnienie dwóch wymogów w zakresie świadczenia e-usług publicznych. Po pierwsze istotna jest integracja świadczeń oraz odpowiednia organizacja, tak aby umożliwić korzystanie z usług zgodnie z preferencjami. Po drugie konieczny jest wielokanałowy dostęp do świadczeń (np. za pomocą Internetu, telefonu komputerowego czy też przez kontakt bezpośredni w urzędzie).

Niezależnie od urzędu, wymagane jest istnienie komórki organizacyjnej odpowiedzialnej za wprowadzanie informacji oraz dokumentów przy jednoczesnym zachowaniu kontroli nad tymi czynnościami. Bez znaczenia jest tu, czy chodzi o dokumenty papierowe, czy elektroniczne – ważna jest organizacja zadania w sposób odpowiedni dla wewnętrznej struktury danej jednostki. Bez względu nas stopień zaawansowania e-administracji zawsze będzie istniała grupa interesantów, która dostarcza dokumenty w postaci papierowej. Dlatego też istotnym zagadnieniem jest tu sposób dokonywania konwersji danych[100]. Zintegrowany e-urząd powinien umożliwić wielokanałowy dostęp do informacji i usług, wykorzystując rozwiązania front-office oraz informację i wymianę danych z systemami krajowymi i europejskimi przez back-office.

Jednym z podstawowych warunków umożliwiających sprawne funkcjonowanie e-administracji jest rozwiązanie problemu standaryzacji wymiany danych. Dotychczasowy proces informatyzacji administracji publicznej charakteryzował się rozwiązaniami, które nie zapewniały interopracyjności systemów, co miało niewątpliwie negatywny wpływ na realizację e-usług[101]. W tym miejscu warto wspomnieć o poziomach zaawansowania e-usług administracji publicznej. Na rys. 1.12 przedstawiona została pięciostopniowa skala zaawansowania usług e-administracji.

100 Konwersja danych oznacza zmianę jednej formy danych na inną. W prezentowanym ujęciu istotą konwersji jest zmiana postaci papierowej na elektroniczną.

101 Opracowano wiele raportów oceniających stan zaawansowania e-administracji zarówno na poziomie krajowym, jak i światowym, z których wynika, że stan zaawansowania e-usług administracji publicznej kształtuje się na wciąż zbyt niskim poziomie w stosunku do innych krajów, np. *The Global Information Technology Report 2013. Growth and Jobs in a Hyperconnected World*, Word Economic Forum and INSEAD, Geneva 2013; *E-Government Survey 2012*, United Nations, New York 2012; *Polska 2030. Wyzwania rozwojowe*, Kancelaria Prezesa Rady Ministrów, Warszawa 2009.



Opracowanie własne na podstawie: *Smarter, Faster, Better eGovernment – 8th Benchmark Measurement*, Prepared by: Capgemini, Rand Europe, IDC, Sogeti and STI for: European Commission, Directorate General for Information Society and Media, November 2009, s. 20.

Rys. 1.12. Poziomy zaawansowania e-usług administracji publicznej

Poszczególne poziomy oznaczają:

- poziom informacyjny – dostarczenie zunifikowanej informacji;
- poziom jednokierunkowy (jednokierunkowa interakcja) – możliwość pobierania formularzy, dokumentów np. z oficjalnej strony internetowej podmiotu publicznego, aby po wydrukowaniu móc rozpocząć proces związanych z daną usługą;
- poziom dwukierunkowy (dwukierunkowa interakcja) – możliwość wypełnienia formularza on-line, przekazania dokumentów, wniosków, raportów. Niezbędny system autentyfikacji (uwierzytelniania) osoby;
- poziom transakcyjny – w pełni transakcyjny system udostępniania usługi w całości przez Internet, włączając podejmowanie decyzji i dostarczenie jej. Nie jest wymagana forma papierowa na żadnym z etapów realizacji usługi;
- personalizacja – aktywne dostarczenie spersonalizowanych usług dla poszczególnych obywateli, np. instytucja wstępnie wypełnia dane w formularzu wniosku na podstawie rządowych baz danych w zakresie dozwolonym przez prawo.

Ponadto należałoby dodać „poziom 0", który oznaczałby brak jakichkolwiek stron WWW lub sytuację, gdy istniejące strony nie zawierają informacji związanych z usługami oferowanymi przez podmiot.

Miernikiem efektywności e-administracji z jednej strony jest odsetek obywateli i przedsiębiorców korzystających z e-usług administracji publicznej, zaś z drugiej interoperacyjność istniejących oraz nowych systemów teleinformatycznych, umożliwiających stworzenie sprawnego systemu informacyjnego państwa, dostarczającego usługi na poziomie wewnątrzkrajowymi i europejskim, przy jednoczesnym osiągnięciu efektywności kosztowej i jakościowej.

Powodzenie e-administracji wymaga dysponowania odpowiednim środowiskiem teleinformatycznym mającym określone cechy. Możliwe też jest zamówienie wyspecjalizowanych usług u podmiotów komercyjnych. W obydwu przypadkach obowiązywać będą wzajemnie przenikające się wymagania dla systemów teleinformatycznych. Konieczność spełnienia tych wymagań przez systemy administracji państwowej wynika częściowo z przepisów, a częściowo jest pochodną stosowanych metod zarządzania i ogólnie przyjętych reguł, nade wszystko zaś stanowi racjonalną przesłankę efektywnego świadczenia usług publicznych na poziomie satysfakcjonującym obywateli.

Informatyzacja administracji publicznej to złożony problem, dlatego też analizując to zagadnienie, należy wziąć po uwagę szerokie spektrum czynników i rozpatrywać je nie tylko z punktu widzenia techniki oraz prawa, ale także z punktu widzenia obywatela. Trzeba pamiętać, że e-administracja nie jest celem samym w sobie. Powinna ona przede wszystkim służyć społeczeństwu, sprzyjając uproszczeniu procedur administracyjnych, oraz przynosić korzyści finansowe.

Pojawienie się i rozwój elektronicznych systemów administracji publicznej powinny być rozpatrywane w szerokiej perspektywie transformacji społecznych, prawnych, technologicznych i ekonomicznych. Powodzenie koncepcji elektronicznej administracji jest uwarunkowane szeregiem osiągnięć na wielu płaszczyznach funkcjonowania państwa i społeczeństwa (tab. 1.5).

Tab. 1.5. Warunki rozwoju e-administracji

Dostosowanie regulacji prawnych
– Przeniesienie usług administracji publicznej na platformę elektroniczną wiąże się z koniecznością zdefiniowania celów działania i procesów instytucjonalnych. – Ważnym aspektem jest dostosowanie gospodarki narodowej do wymagań globalnej gospodarki elektronicznej (wpływ uregulowań wynikających z umów i porozumień międzynarodowych na ustawodawstwo krajowe). – Zapewnienie równorzędności czynności realizowanych zdalnie z czynnościami realizowanymi w sposób tradycyjny (sprawy i czynności administracyjne wykonywane on-line i w sposób tradycyjny powinny wywoływać taki sam skutek prawny). – Akty prawne powinny regulować m.in. następujące kwestie: organizacja administracji elektronicznej, instytucje odpowiedzialne za informatyzację, zdefiniowanie zasad i standardów, ustanowienie wymagań dla systemów teleinformatycznych i rejestrów publicznych, bezpieczeństwo wykonywanych czynności, sprawozdawczość i kontrola procesu informatyzacji administracji.
Rozwój i wykorzystanie technologii
– Powszechny dostęp do Internetu oraz rozwój infrastruktury teleinformatycznej. – Urzędy powinny być wyposażone w urządzenia techniczne wspierające procesy gromadzenia, przetwarzania i przechowywania informacji (komputeryzacja procesów i procedur oraz modernizacja infrastruktury urzędów). – Wymagane jest projektowanie i wdrażanie systemów informatycznych dla potrzeb administracji publicznej uwzględniających cele i zadania, grupy użytkowników, procedury bezpieczeństwa oraz integrację sieci resortowych, lokalnych i europejskich. – Efektywność wdrażania nowoczesnych rozwiązań uzależniona jest od interoperacyjności w sensie technicznym, semantycznym, organizacyjnym, prawnym oraz społecznym.

Działania organizacyjne i proceduralne
– Transformacja struktur urzędów uwzględniająca przeprojektowanie procedur administracyjnych, wprowadzenie przejrzystości i otwartości działania oraz dostosowanie do potrzeb użytkowników usług świadczonych przez różne kanały dostępu. – Wymagane jest skoordynowanie wysiłków poszczególnych podmiotów administracji publicznej związanych z informatyzacją.
Umiejętności i kompetencje społeczne
– Dynamika zmian zachodzących w dziedzinie technologii ICT powoduje konieczność ciągłego doskonalenia zawodowego pracowników. – Czynnikiem determinującym rozwój e-administracji jest poziom zdolności społeczeństwa do adaptacji wykorzystywania współczesnych technologii, środków telekomunikacji oraz systemów informatycznych. – W polskiej rzeczywistości wciąż istnieje przywiązanie do dokumentacji papierowej warunkującej przebieg procesów, dlatego też istotnym aspektem jest promowanie e-administracji zarówno wśród pracowników, jak i społeczeństwa (np. szkolenia, kampania społeczna, wspieranie programów adresowanych do osób zagrożonych wykluczeniem cyfrowym).
Koszty i efektywność ekonomiczna
– Zwiększenie środków finansowych na badania i innowacje oraz korzystanie z doświadczeń i dobrych praktyk państw europejskich sprzyja rozwojowi nowych technologii. – Funkcjonowanie e-administracji wymaga nakładów finansowych, jednak w perspektywie długookresowej przynosi korzyści finansowe zarówno dla administracji, jak i społeczeństwa. – Zastosowanie technologii informacyjnych w administracji podyktowane jest racjonalnością wydatkowania środków publicznych, zwiększeniem zaufania do sposobu gospodarowania środkami publicznymi oraz zmniejszeniem zjawisk korupcjogennych. – Wśród zadań e-administracji znaczącą rolę odgrywa ekonomizacja pracy urzędu możliwa dzięki standaryzacji danych w formie elektronicznej (oszczędność czasu pracy urzędników i petentów).
Bezpieczeństwo i ochrona zasobów administracji publicznej
– Stosowane systemy informatyczne administracji publicznej powinny minimalizować ryzyko zagrożeń dla bezpieczeństwa zasobów i transakcji (np. przez stosowanie zabezpieczeń, uwierzytelnianie transakcji, stosowanie podpisu elektronicznego). – W przypadku wystąpienia zagrożenia niezbędne jest zapewnienie informacyjnej ciągłości działania, zarówno na poziomie administracji jako całości, jak i jej elementów składowych. – Projektowaniu systemów teleinformatycznych na potrzeby administracji publicznej powinna towarzyszyć analiza zagrożeń i ryzyka (m.in. rozpoznanie zagrożeń, szacowanie prawdopodobieństwa naruszenia ochrony, rozpoznanie podatności, określenie zabezpieczeń).

Opracowanie własne.

Analiza e-administracji w ujęciu organizacyjnym wiąże się z określeniem podmiotów odpowiedzialnych za informatyzację administracji publicznej oraz podmioty świadczące e-usługi zarówno w skali makro, jak i mikro. Ujęcie funkcjonalne polega na interpretowaniu przedmiotu działania elektronicznej administracji. Celem administracji jest tworzenie warunków do wykorzystania nowoczesnych technologii, przy jednoczesnym zapewnieniu bezpieczeństwa i ochrony zasobów.

Zmiany związane z przeniesieniem funkcjonowania administracji publicznej na platformę cyfrową muszą znaleźć odzwierciedlenie w planach, koncepcjach i systemie źródeł prawa. Na system krajowego ustawodawstwa wywierają wpływ

umowy i porozumienia międzynarodowe. Niektóre przepisy są obligatoryjne, a zatem powodują potrzebę dostosowania prawa krajowego. Inne z kolei określają ogólne standardy oraz mają formę zaleceń. Zakres norm prawnych związanych z kształtowaniem elektronicznej administracji jest bardzo rozległy i rozproszony w różnych gałęziach i dziedzinach prawa. Uregulowania prawne dotyczące e-administracji można klasyfikować ze względu na obszar, którego dotyczą:

- ramy prawne społeczeństwa informacyjnego, np. *Europejska Agenda Cyfrowa, Długookresowa Strategia Rozwoju, Polska 2030. Trzecia Fala nowoczesności*;
- przepisy bezpośrednio związane z wdrożeniem e-administracji, np. ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne, *Państwo 2.0 – Nowy start dla e-administracji*;
- uregulowania dotyczące zabezpieczenia (organizacyjnego i technicznego) informatycznie przetwarzanych danych, np. normy dotyczące bezpieczeństwa informacji, m.in. ISO/IEC 27001.

1.6. Modele e-administracji na przykładzie wybranych państw

Proces informatyzacji administracji publicznej przebiega różnie w krajach europejskich. Zauważalne są dysproporcje w poziomie zaawansowania e-usług administracji publicznej. Kraje przodujące w gospodarce i konkurencyjności posiadają najlepiej funkcjonujące służby publiczne oraz najwyższe wskaźniki zaawansowania e-administracji. Wynika z tego silny związek między gospodarką, innowacyjnością, konkurencyjnością oraz jakością administracji publicznej.

Na przykładzie kilku państw scharakteryzowano funkcjonowanie elektronicznej administracji. Analiza obejmuje najistotniejsze aspekty omawianej problematyki oraz wyszczególnienie specyficznych cech w każdym z wyselekcjonowanych przypadków.

Charakterystyka rozwoju e-administracji w Wielkiej Brytanii jest uzasadniona przede wszystkim wysokim stadium zaawansowania e-usług zarówno w skali europejskiej, jak i światowej. Wyselekcjonowane przykłady obejmują również kraje skandynawskie (Finlandia) oraz bałtyckie (Estonia). W obu przypadkach obserwuje się wysoki poziom wykorzystania e-usług administracji zarówno przez obywateli, jak i przez przedsiębiorców. Charakterystyka obejmuje także Czechy ze względu na rekomendacje dotyczące wdrożenia w Polsce rozwiązań na wzór czeskiego CzechPoint. Nie ulega wątpliwości, że proces wdrażania e-usług w Polsce znajduje się wciąż w fazie wstępnej (tab. 1.6). Stąd też opis polskiego modelu e-administracji został poprzedzony analizą modeli, z których Polska mogłaby czerpać doświadczenia w omawianym obszarze.

Tab. 1.6. Polska e-administracja na tle Europy

Ranking europejski 2014	Kraj	Ranking światowy 2014	Ranking światowy 2012	Zmiana pozycji w rankingu światowym
1	Francja	4	6	2
2	Holandia	5	2	-3
3	Wielka Brytania	8	3	-5
4	Finlandia	10	9	-1
5	Hiszpania	12	23	11
6	Norwegia	13	8	-5
7	Szwecja	14	7	-7
8	Estonia	15	20	5
9	Dania	16	4	-12
10	Islandia	19	22	3
11	Austria	20	21	1
12	Niemcy	21	17	-4
13	Irlandia	22	34	12
14	Włochy	23	32	9
15	Luksemburg	24	19	-5
16	Belgia	25	24	-1
17	Rosja	27	27	0
18	Litwa	29	29	0
19	Szwajcaria	30	15	-15
20	Łotwa	31	42	13
21	Grecja	34	37	4
22	Portugalia	37	33	-4
23	Węgry	39	31	-8
24	Malta	40	35	-5
25	Słowenia	41	25	-16
26	Polska	42	47	5

Opracowanie własne na podstawie: *E-Government Survey 2014*, Department of Economic and Social Affairs New York, s. 31–34.

Przedstawiony powyżej ranking został opracowany w oparciu o trzy komponenty: 1) indeks usług dostępnych online (OSI), 2) indeks infrastruktury teleinformatycznej (TII), 3) indeks kapitału ludzkiego (HCI). Powyższe trzy składowe składają się na wskaźnik rozwoju e-administracji (EGDI).

1.6.1. Wielka Brytania

Wielka Brytania znajduje się w światowej czołówce zaawansowania i wykorzystania usług e-administracji. Według raportu e-Government Survey 2014 zajmuje ósme miejsce w światowym rankingu państw o największych wskaźnikach

rozwoju e-administracji. Natomiast w Europie zajmuje trzecie miejsce za Francją i Holandią[102].

Organem odpowiedzialnym za informatyzację w skali krajowej oraz opracowanie strategii jest Rada Ministrów. Ponadto funkcjonują jednostki odpowiedzialne za koordynację (np. Zespół ds. reform i efektywności), implementację (np. Dyrektor ds. informatyki), wsparcie (np. Dyrektor ds. technologii), audyt (np. Narodowe Biuro Audytu), bezpieczeństwo informacji (np. Biuro Komisarza ds. informacji). Zdecentralizowane administracje w Anglii, Szkocji, Walii i Irlandii Północnej mają własne podejście do polityki na rzecz administracji elektronicznej[103]. W Wielkiej Brytanii opracowano szereg aktów prawnych na rzecz budowy e-administracji, wśród których znajdują się m.in.: ustawa o ochronie danych osobowych (1998), ustawa o wolności informacji (2000), ustawa o łączności elektronicznej (2000), ustawa o gospodarce cyfrowej (2010).

Dokument programowy Rządowa Strategia Cyfrowa[104] określa 16 obszarów działań służących uproszczeniu procedur administracyjnych oraz przeciwdziałaniu wykluczeniu cyfrowemu. W strategii skupiono się głównie na usługach świadczonych przez departamenty administracji centralnej. Główne cele określone w dokumencie są następujące:

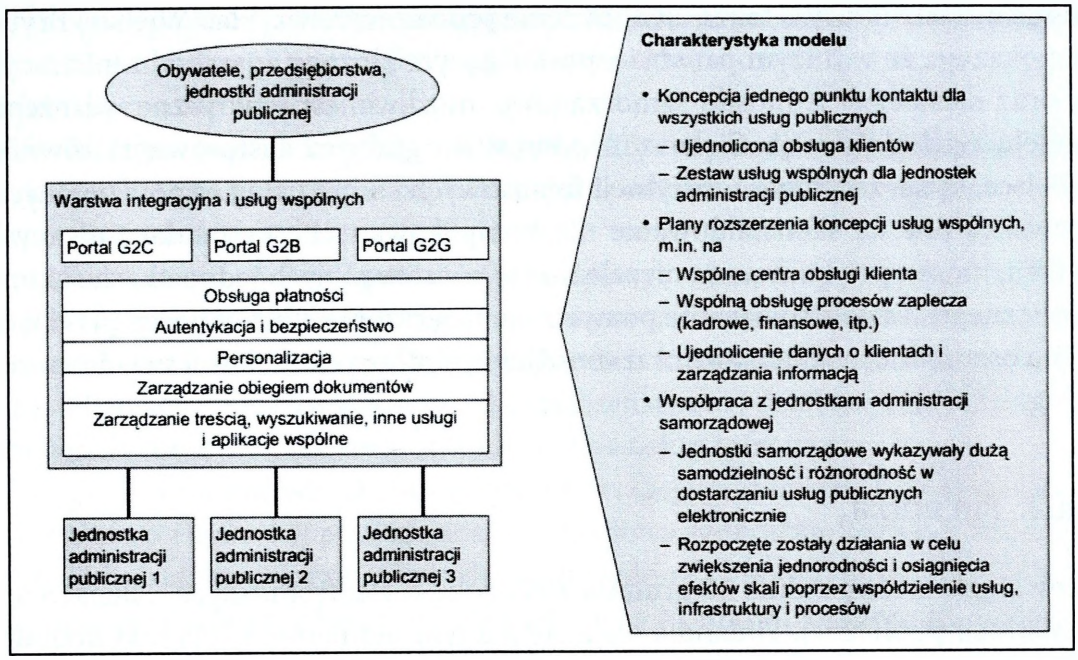
- dążenie do zapewnienia wszystkim działom odpowiedniej infrastruktury teleinformatycznej i specjalistycznych umiejętności pracowników;
- zapewnienie wsparcia ze strony Rady Ministrów;
- podniesienie świadomości i wiedzy na temat usług oferowanych przez e-administrację wśród społeczeństwa;
- zapewnienie spójnego systemu zarządzania informacjami;
- korzystanie przez kluby polityczne z narzędzi i technik cyfrowych w celu konsultacji społecznych;
- współpraca z sektorem prywatnym.

W Wielkiej Brytanii przyjęto koncepcję utworzenia jednego punktu kontaktu dla wszystkich usług publicznych, który zapewni ujednoliconą obsługę klientów oraz zestaw usług wspólnych dla jednostek administracji publicznej (rys. 1.13).

102 *E-Government Survey 2014...*, op. cit., s. 34.

103 Zob. *eGovernment in United Kingdom*, European Commission – eGovernment Practice, December 2011, s. 14–17.

104 Tekst strategii dostępny na stronie: https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy.



Źródło: *Przegląd modeli współpracy jednostek administracji w świadczeniu usług publicznych drogą elektroniczną*, dostęp: http://www.bialystok.uw.gov.pl/NR/rdonlyres/276963A6-1A26-4FE8-B787B7C1784FF B71/0/Przegl% C4%85dmodeliwsp%C3%B3%C5%82pracyjednostek.pdf, s. 12.

Rys. 1.13. Model e-administracji w Wielkiej Brytanii

Na poziomie centralnym stworzona została warstwa integracyjna i usług wspólnych, która w szczególności dostarcza usługi portalowe, obsługę płatności, uwierzytelnianie i zapewnianie bezpieczeństwa, personalizację, zarządzanie obiegiem dokumentów, zarządzanie treścią, wyszukiwanie i szereg innych usług wspólnych. Z usług tych w sposób wystandaryzowany korzystają jednostki administracji rządowej dostarczające usługi publiczne drogą elektroniczną. Jednostki administracji samorządowej do tej pory wykazywały znaczną samodzielność i niezależność w dostarczaniu usług publicznych, czego efektem była duża niejednorodność poziomu i sposobu obsługi klientów[105]. W Wielkiej Brytanii opracowana została koncepcja rozszerzenia usług wspólnych m.in. na współdzielone centra obsługi klienta i współdzieloną obsługę procesów zaplecza (takich jak np. procesy kadrowe, finansowe itp.). Dodatkowo planowane jest dalsze ujednolicane danych o klientach administracji i sposobów zarządzania informacją. Rozpoczęte zostały również działania mające na celu zwiększenie jednorodności usług świadczonych przez jednostki samorządowe oraz osiągnięcie efektów skali przez współdzielenie

105 *Przegląd modeli współpracy jednostek administracji w świadczeniu usług publicznych drogą elektroniczną*, dostęp: http://www.bialystok.uw.gov.pl/NR/rdonlyres/276963A6-1A26-4FE8-B787B7C1784FF B71/0/Przegl% C4%85dmodeliwsp%C3%B3%C5%82pracyjednostek.pdf.

usług i infrastruktury, a także ujednolicenie procesów[106]. Przykład Wielkiej Brytanii pokazuje, że w dużym państwie, posiadającym złożony aparat administracyjny oraz niezależne jednostki samorządowe, możliwe jest praktyczne wdrożenie modelu e-administracji. Ciekawym pomysłem, godnym zastosowania również w Polsce, są zaczerpnięte z instytucji finansowych centra usług współdzielonych. Pozwalają one na skonsolidowanie nieskomplikowanych, wystandaryzowanych funkcji, które są wykonywane niezależnie w poszczególnych jednostkach sektora publicznego. Takie rozwiązanie pozwala na zwiększenie efektywności, przekłada się na oszczędności finansowe oraz umożliwia podnoszenie jakości świadczonych usług.

1.6.2. Finlandia

Uchwalając ustawę z dnia 30 grudnia 1999 roku o elektronicznych usługach administracji publicznej, Finlandia stała się jednym pionierów tworzenia uregulowań e-usług w sektorze publicznym. W ciągu kilku dekad kraj ten awansował do grona krajów o najlepiej rozwiniętej infrastrukturze teleinformatycznej. Sukces ten związany jest z praktyczną realizacją teorii informacyjnego wzrostu.

Pod koniec XX wieku w Finlandii zapoczątkowano rozwój gospodarki charakteryzujący się zorientowaniem na tworzenie i stosowanie wiedzy, ściśle związanej z rozwojem przemysłu elektronicznego i usług w zakresie oprogramowania. Współcześnie podkreśla się, że w Finlandii powstał jeden z najbardziej zaawansowanych i sprawnych systemów innowacyjności, a w jego stworzeniu i kształtowaniu wiodącą rolę odgrywa państwo.

Ramy prawne e-administracji w Finlandii wyznaczają przykładowo:

- ustawa o jawności działania rządu (1999);
- ustawa o usługach i komunikacji elektronicznej w sektorze publicznym (2003);
- ustawa o podpisie elektronicznym (2003).

Długookresowa wizja strategiczna Finlandii w odniesieniu do e-administracji została określona w dokumencie *Narodowa strategia społeczeństwa wiedzy na lata 2007–2015*. Dokument koncentruje się na czterech głównych zamiarach strategicznych[107]:

- Wielokanałowe, interaktywne e-usługi dla obywateli o przedsiębiorców. Usługi te powinny działać w sposób zorientowany na klienta. Procesy aktywizacji przedsiębiorstw i administracji powinny znajdować się w elektronicznym łańcuchu zakupów i dostaw.

106 Ibidem.

107 *The National Knowledge Society Strategy 2007–2015. A renewing, human-centric and competitive Finland*, Prime Minister's office, September 2006.

• Nowe produkty, usługi i innowacje powinny być opracowane we współpracy z uniwersytetami, instytutami badawczymi, administracją publiczną, organizacjami i przedsiębiorstwami.

• Ważnym czynnikiem zapewnienia konkurencyjności w pespektywie długookresowej jest zapewnienie odpowiednich środków umożliwiających obywatelom rozwój wiedzy.

• Fundament społeczeństwa informacyjnego stanowi praktyczna realizacja interoperacyjności. Finlandia dąży do wprowadzenia solidnej infrastruktury i komunikacji, opartej na szybkich połączeniach internetowych dostępnych całą dobę. W połączeniu ze zwiększonym bezpieczeństwem i dostępnością infrastruktura będzie stanowić podstawę do świadczenia usług cyfrowych.

Organami odpowiedzialnymi za informatyzację administracji publicznej są: Ministerstwo Finansów, podlegająca mu Rządowa Jednostka Rozwoju Informatyzacji, Ministerstwo Spraw Wewnętrznych i jednostka koordynująca projekty na poziomie regionalnym i lokalnym oraz Rządowy Komitet Doradczy ds. Rozwoju Informatyzacji w Administracji Publicznej, wspierający współpracę między centralnymi i lokalnymi jednostkami w państwie[108]. W marcu 2014 roku w Ministerstwie Finansów utworzono jednostkę Government ICT Centre Valtori[109], której zadaniem jest rozwijanie e-usług w administracji i systemu informacji dla urzędów i agencji rządowych. Strategia wdrażania e-administracji w Finlandii przebiegała w kilku etapach (tab. 1.7).

Tab. 1.7. Etapy wdrażania e-administracji w Finlandii

Lp.	Etap	Charakterystyka	Realizacja praktyczna
1	Informacja	Strona internetowa, na której zostaje opublikowana informacja o usługach publicznych	Działania dotyczyły przetworzenia istniejących zbiorów informacji na formę cyfrową. Przykłady usług dostępnych w ramach pierwszego etapu: • strona internetowa instytucji publicznej, np. fińskiego Narodowego Instytutu Medycyny[a)], • informacja dostarczana użytkownikowi przez organizacje, m.in. wskaźniki i statystyki, dostarczane np. przez fiński Urząd ds. Rynku Energetycznego[b)], • zestaw odpowiedzi na najczęściej zadawane pytania (FAQ), np. na stronie internetowej Fińskiej Agencji Ochrony Konsumentów[c)]

108 A. Łuczak, A. Popowicz, M. Zieliński, *Elektroniczna administracja w Finlandii*, „Prace z Zakresu Myśli Polityczno-Prawnej oraz Elektronicznej Administracji. Studia Erasmania Wratislaviensia. Acta Studentum", Wrocław 2010, s. 185.

109 Strona oficjalna Government ICT Centre Valtori: http://www.valtori.fi/en-US.

Lp.	Etap	Charakterystyka	Realizacja praktyczna
2	Informacja interaktywna	Umożliwienie użytkownikom dostępu do baz danych instytucji publicznych (przeszukiwanie baz danych, możliwość podania informacji zwrotnej)	Przykładowe usługi informacyjne (dostępne także w języku angielskim): • Finlex – baza danych fińskiego Ministerstwa Sprawiedliwości, zawierająca przepisy prawne, prawo precedensowe oraz postanowienia traktatów międzynarodowych[d], • StatFin – baza danych fińskiego Urzędu Statystycznego, pozwalająca wyszukiwać informacje na podstawie kryteriów wybranych przez użytkownika[e]
3	Transakcja publiczna on-line	Umożliwienie użytkownikom dostępu do informacji zabezpieczonych przed dostępem osób niepowołanych oraz dokonanie bezpiecznej transakcji on-line	W obrębie transakcji on-line składających się na elementy trzeciego etapu można wyróżnić m.in. • procedurę aplikacyjną dla kandydatów na studia w Academy of Finland[f] – możliwość pobrania formularza ze strony internetowej i wysłania go po wypełnianiu pocztą elektroniczną bądź złożenia aplikacji on-line, • zbiór formularzy rejestracyjnych w zbiorach fińskiego Urzędu Patentowego i Rejestrowego[g], które można uzyskać dzięki połączeniu internetowemu, za które naliczana jest opłata z elektronicznego konta bankowego
4	Wymiana danych	Udostępnianie danych dostarczonych przez użytkownika (za jego zgodą) na potrzeby innych instytucji publicznych	Przykłady usług w ramach etapu: • The Static Finland Census Collection[h] – baza danych statystycznych gromadząca większość informacji z rejestrów centralnej administracji, w mniejszym stopniu bezpośrednio od obywateli, • system danych o ruchu drogowym[i] – zbiór informacji dotyczących pojazdów oraz kierowców, który może być wykorzystywany do celów podatkowych, statystycznych, ubezpieczeniowych, inspekcyjnych. Pod koniec 2013 roku fiński rząd przedstawił plany na wprowadzenie warstwy wymiany danych na wzór estońskiego X-Road

[a] Strona oficjalna Narodowego Instytutu Medycyny: http://www.nam.fi.
[b] Strona oficjalna Urzędu ds. Rynku Energetycznego http://www.energiavirasto.fi/en/home.
[c] Strona oficjalna Agencji Ochrony Konsumentów: http://www2.kkv.fi/en-GB/.
[d] Strona oficjalna Finlex: http://www.finlex.fi/en/.
[e] Strona oficjalna StatFin: http://www.stat.fi/index.html.
[f] Strona oficjalna Academy of Finland: http://www.aka.fi/ENG.
[g] Strona oficjalna Urzędu Patentowego i Rejestrowego: http://www.prh.fi/en/index.html
[h] Strona oficjalna The Static Finland Census Collection: http://www.stat.fi/tup/vl2010/art_2011-03-18 _001_en.html.
[i] Strona oficjalna systemu danych o ruchu drogowym: http://www2.liikennevirasto.fi/sivu_siirtynyt/sivu _siirtynyt.html.

Opracowanie własne na podstawie: M. Kowalczyk, *e-urząd w komunikacji z obywatelem*, Warszawa 2009, s. 138–143.

1.6.3. Estonia

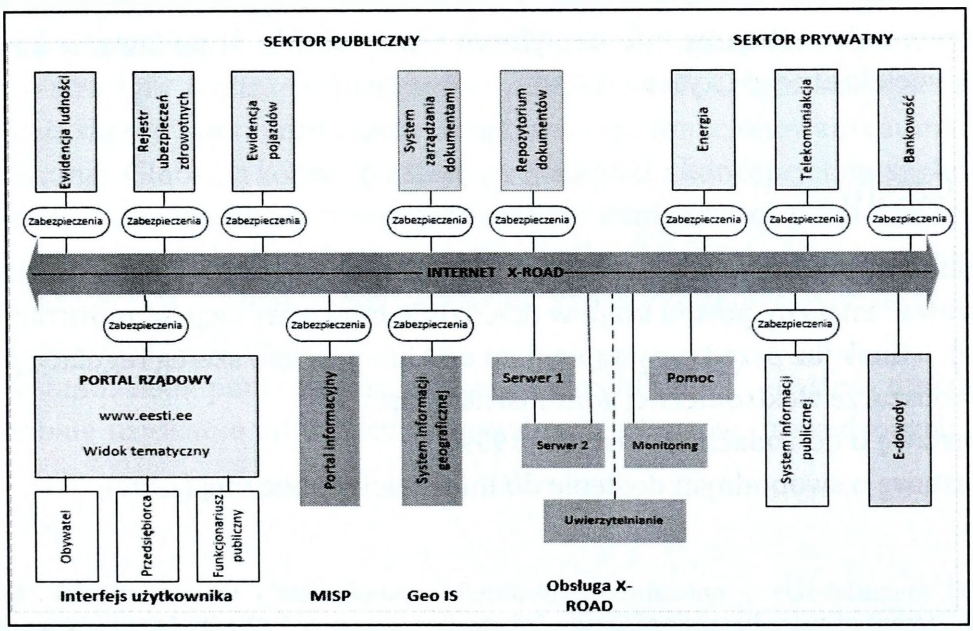
W dziedzinie wdrażania e-usług administracji publicznej Republika Estońska znajduje się w europejskiej czołówce. Ponadto większość obywateli posiada własny podpis elektroniczny oraz regularnie korzysta z elektronicznej bankowości i usług e-administracji.

Organem odpowiedzialnym za rozwój i realizację polityki informacyjnej Estonii jest przede wszystkim Ministerstwo Gospodarki i Komunikacji, a w szczególności Departament Stanu Systemów Informacyjnych. Ponadto Estońskie Centrum Informatyki rozwija główne elementy infrastruktury rządowej.

W Estonii opracowano szereg aktów prawnych na rzecz budowy e-administracji, wśród których są m.in.:

- ustawa o ochronie danych osobowych (1996);
- plan działania na rzecz budowy społeczeństw informacyjnego (1998);
- ustawa o podpisie elektronicznym (2000);
- ustawa o dostępie do informacji publicznej (2000);
- zasady polityki informacyjnej Estonii (2004–2006);
- strategia społeczeństwa informacyjnego (2007).

W latach dziewięćdziesiątych opracowano projekt X-Road, mający na celu stworzenie bezpiecznego, zestandaryzowanego otoczenia sieciowego dla systemów informacyjnych administracji publicznej. Został on uruchomiony w 2001 roku. Jest to środowisko techniczne i organizacyjne, umożliwiające bezpieczną wymianę danych pomiędzy systemami informacyjnymi państwa (rys. 1.14).



Opracowanie własne na podstawie: *X-Road. Estonian Information System's Authority*, Rävala 5, 15169 Tallinn.

Rys. 1.14. Model e-administracji w Estonii

Instytucje sektora prywatnego i publicznego mogą połączyć swój system informacyjny z X-Road, z ich własnym środowisku elektronicznym lub oferować swoje usługi za pośrednictwem X-Road. Przystąpienie do X-Road pozwala instytucjom oszczędzać zasoby, ponieważ warstwa wymiany danych już istnieje. Umożliwia to skuteczniejszą wymianę danych zarówno wewnątrz instytucji państwowych, jak i w zakresie komunikacji między obywatelem a państwem. Dodatkowo X-Road umożliwia np. przekazywanie danych ubezpieczeniowych do Estońskiego Funduszu Ubezpieczeń Zdrowotnych[110]. Aby korzystać z usługi, użytkownicy muszą najpierw uwierzytelnić się za pomocą dowodu osobistego lub za pośrednictwem banku internetowego. Autentyfikacja przedsiębiorcy następuje na podstawie danych z Rejestru Handlowego.

W latach 2000–2003 został uruchomiony portal dostępu do e-administracji przez Internet i urządzenia mobilne. W 2000 roku zaakceptowano projekt chipowych dowodów osobistych. Od stycznia do maja 2006 roku w państwie funkcjonowało ponad 850 tysięcy aktywnych dowodów w formie kart elektronicznych. Każda karta zawiera dane osobowe, zakodowane w chipie, certyfikat indentyfikacyjny oraz certyfikat podpisu elektronicznego[111]. W Estonii funkcjonuje ponadto infrastruktura klucza publicznego (PKI) umożliwiająca bezpieczne uwierzytelnianie i podpis elektroniczny. Takie rozwiązanie umożliwia przekazanie danych za pomocą pary kluczy. Technologia ta jest stosowana w związku z elektroniczną tożsamością.

W zakresie dostępu do informacji publicznej oraz zarządzania zasobami informacyjnymi w Estonii funkcjonuje Katalog Systemu Informacyjnego Państwa (RIHA). Środowisko umożliwia m.in.: 1) połączenie z X-Road; 2) rejestrację usług; 3) zastosowanie systemów informacyjnych i baz danych; 4) podawanie komponentów wielokrotnego użytku.

1.6.4. Czechy

Od momentu przystąpienia Czech do Unii Europejskiej w 2007 roku można zaobserwować znaczny postęp kraju w dziedzinie informatyzacji administracji publicznej. Jednak już przed przystąpieniem do Unii przyjęto szereg regulacji prawnych w obszarze elektronicznej administracji, np.:

- ustawę o dowodach osobistych (1999);
- ustawę o swobodnym dostępie do informacji publicznej (1999);

110 Strona oficjalna Republic of Estonia Information System of Authority: https://www.ria.ee/.

111 M. Chlewicki, A. Kedzierska, M. Oranowski, *Elektroniczna administracja w Estonii*, „Prace z Zakresu Myśli Polityczno-Prawnej oraz Elektronicznej Administracji. Studia Erasmania Wratislaviensia. Acta Studentum", Wrocław 2010, s. 204.

- ustawę o ochronie danych osobowych (2000);
- ustawę o podpisie elektronicznym (2000);
- ustawę o niektórych usługach społeczeństwa informacyjnego (2004);
- ustawę o łączności elektronicznej (2005);
- ustawę o zamówieniach publicznych (2006).

Ówczesne zasady prowadzące do rozwoju e-administracji zostały wymienione w dokumencie *Strategia rozwoju usług społeczeństwa informacyjnego na lata 2008–2015*. Zgodnie z koncepcją określoną w strategii e-administracja jest zarówno środkiem zaspokajania oczekiwań obywateli w zakresie usług publicznych, jak i sposobem modernizacji administracji publicznej umożliwiającym zapewnienie efektywności kosztowej i funkcjonalnej. Podkreśla się również istotną rolę infrastruktury oraz interoperacyjności. Strategia jest realizowana za pomocą wielu powiązanych ze sobą projektów podzielonych na pięć głównych obszarów tematycznych[112]:

- podstawowe rejestry administracji publicznej (np. ewidencja ludności) wraz z architekturą organizacyjną i techniczną umożliwiającą integrację rejestrów bez konieczności powielania informacji, przy jednoczesnym zapewnieniu procedur bezpieczeństwa;
- uniwersalny punkt kontaktu;
- bezpieczna komunikacja elektroniczna pomiędzy władzami, jak również między obywatelem a władzą;
- digitalizacja danych i ich archiwizacja;
- usługi dla społeczeństwa informacyjnego, np. opieka zdrowotna, opieka emerytalna, procedury sądowe i administracyjne.

Kolejnym istotnym dokumentem jest *Efektywna administracja i przyjazne usługi – strategia realizacji inteligentnej administracji*. Celem strategii jest zapewnienie skoordynowanego i skutecznego sposobu funkcjonowania administracji publicznej. Globalna koncepcja strategii pochodzi z koncepcji tzw. sześciokąta wzajemnie powiązanych kluczowych elementów administracji publicznej: prawo, organizacja, ludzie (społeczeństwo), służba cywilna (urzędnicy), technologie ICT, finansowanie[113]. W Czechach powstało wiele projektów centralnych na rzecz budowy e-administracji, np.:

- ustanowienie punktów kontaktowych CzechPOINT – system umożliwiający szybkie uzyskanie informacji z centralnych rejestrów prowadzonych przez

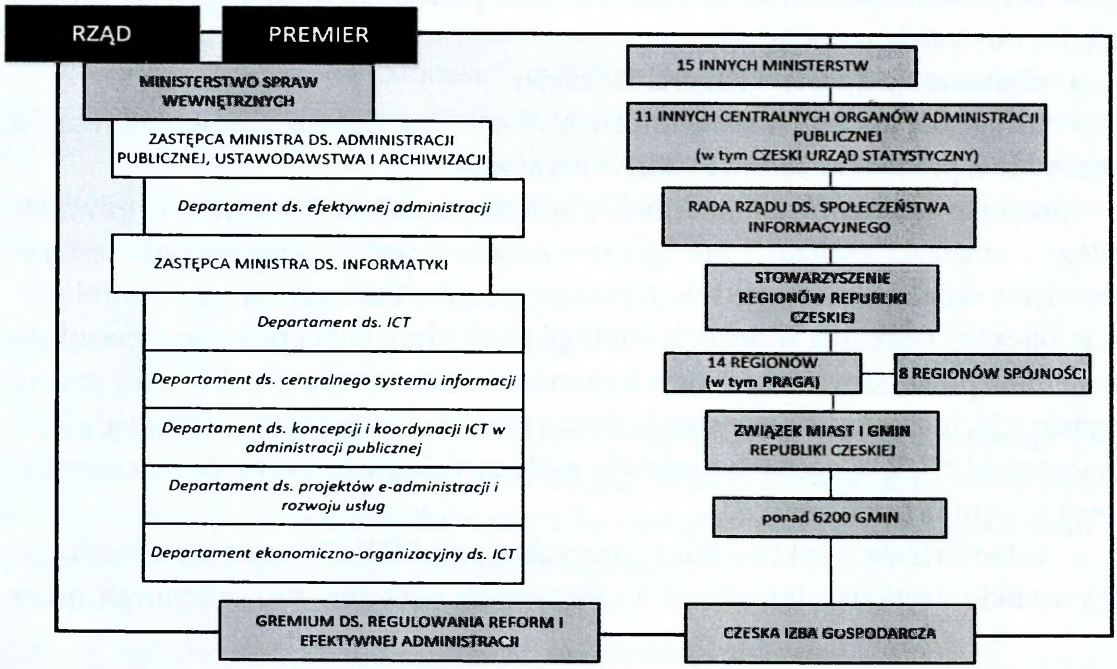
112 *eGovernment in Czech Republic*, European Commission – eGovernment Practice, November 2011, s. 9–10.

113 *Project Local Digital Agenda in the Visegrad Four countries*, Visegrad Strategic Program (May 2011), Application ID 31110019, Project coordinator: Martina Rojková, dostęp on-line: http://extranet.kr-vysocina.cz/download/odbor_informatiky/lda_v4/_an/an01_uvod.htm.

różne instytucje. Usługi CzechPOINT są adresowane do wszystkich osób fizycznych i prawnych – należą do nich m.in. rejestr podmiotów gospodarczych, rejestr spółek w stanie upadłości (wyciągi), wyciągi z rejestru karnego i rejestru karnego osób prawnych, możliwość uwierzytelnienia kopii dokumentu, możliwość złożenia podpisu urzędowo poświadczonego, autoryzowana konwersja dokumentów papierowych na elektroniczne i odwrotnie;

- podstawowe rejestry – jeden z najbardziej znaczących i skomplikowanych projektów e-government w Czechach. Podstawowe rejestry zawarte są w systemach: rejestr mieszańców ROI, rejestr osób RPO, rejestr identyfikacji terytorialnej RTIARE, rejestr praw i obowiązków RRO;
- Administracja Publiczna Portal (PAP) – głównym przeznaczeniem portalu jest stworzenie miejsca integracji i udostępniania informacji publicznej oraz ewentualnego kontaktu z władzami;
- infrastruktura komunikacyjna administracji publicznej – celem projektu jest utworzenie jednolitego sytemu sieci, aplikacji oraz bezpiecznej transmisji danych wszystkich organów władzy publicznej.

W budowę e-administracji w Czechach zaangażowanych jest wiele organów i instytucji. Ogólny model instytucjonalny zarządzania e-administracją przedstawiono na rys. 1.15.



Opracowanie własne na podstawie: D. Špaček, *E-Government management and evolution in the Czech Republic – shifts in practice?*, NISPAcee Conference 2010.

Rys. 1.15. Instytucjonalny model zarządzania e-administracją w Czechach

1.6.5. Polska

Polska wciąż jest w fazie wstępnej procesu informatyzacji administracji publicznej. W ciągu ostatnich lat powstało wiele aktów prawnych i dokumentów programowych mających na celu umożliwienie wdrożenie e-usług w sektorze publicznym (tab. 1.8).

W procesie przygotowania Polski do e-administracji zaangażowany jest szereg organów i instytucji:

- Ministerstwo Administracji i Cyfryzacji[114] – jest głównym inicjatorem polityki i strategii w obszarze e-administracji i społeczeństwa informacyjnego; do jego obowiązków należy m.in. wspieranie inwestycji w IT, promocja technologii informacyjnej, ustalenie standardów informatycznych;
- Departament Telekomunikacji – odpowiada za kwestie związane z prawnymi uregulowaniami z zakresu telekomunikacji i w tym zakresie opracowuje, opiniuje i opisuje projekty aktów prawnych oraz plany i programy strategiczne przy współpracy z organami UE i organizacjami międzynarodowymi; ponadto odpowiada za realizację i wdrożenie Narodowego Planu Szerokopasmowego[115] oraz koordynację i realizację ePUAP;
- Departament Społeczeństwa Informacyjnego – koordynuje przedsięwzięcia związane z rozwojem społeczeństwa informacyjnego oraz prowadzi sprawy związane z finansowanie inwestycji i prowadzeniem działań promocyjnych;
- Komitet Rady Ministrów ds. Cyfryzacji[116] – inicjuje, opiniuje i koordynuje między resortami prace dotyczące informatyzacji państwa;
- Centrum Projektów Informatycznych[117] – odpowiedzialne za sprawne wdrożenie sektorowych i ponadsektorowych projektów teleinformatycznych;
- Centralny Ośrodek Informatyki[118] – posiada szeroki wachlarz obowiązków, począwszy od projektowania i programowania, aż do utrzymania systemów informatycznych;
- Najwyższa Izba Kontroli[119] – organ kontrolny, którego celem jest m.in. promocja gospodarcza, efektywność i skuteczność w służbie publicznej; monitoruje przestrzeganie budżetu państwa i założeń polityki pieniężnej;

114 Strona oficjalna Ministerstwa Administracji i Cyfryzacji: https://mac.gov.pl/.

115 Zob. *Narodowy Plan Szerokopasmowy*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014.

116 Strona oficjalna Komitetu Rady Ministrów ds. Cyfryzacji: https://krmc.mac.gov.pl/.

117 Strona oficjalna Centrum Projektów Informatycznych: http://www.cpi.gov.pl/p.

118 Strona oficjalna Centralnego Ośrodka Informatyki: http://www.coi.gov.pl/.

119 Strona oficjalna NIK: http://www.nik.gov.pl/.

Tab. 1.8. Wybrane uregulowania prawne w obszarze e-administracji w Polsce

Dokument	Obszar uregulowań
Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym	Ustawa określa warunki i skutki prawne podpisu elektronicznego, zasady świadczenia usług certyfikujących oraz nadzoru nad podmiotami świadczącymi te usługi.
Ustawa z dnia 6 września 2001 roku o dostępie do informacji publicznej	Ustawa nałożyła na władze publiczne oraz inne podmioty wykonujące zadania publiczne obowiązek posiadania od 1 lipca 2003 roku Biuletynu Informacji Publicznej (BIP), w którym udostępniana jest informacja publiczna. BIP stanowi system stron internetowych służący powszechnemu dostępowi do informacji publicznej. Dostęp do BIP jest możliwy przez stronę główną BIP zawierającą podstawowe informacje wraz z odsyłaczami do stron podmiotowych[a].
Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne	Przepisy ustawy normują trzy obszary tematyczne: instytucje wspierające informatyzację, rozwiązania dotyczące zasad stosowania technik telekomunikacyjnych i informatycznych w podmiotach publicznych oraz zmiany dostosowujące zadania i czynności określone w ustawach szczególnych[b]. W ramach ustawy zmieniono 17 innych ustaw, np. kodeks postępowania administracyjnego, ustawę o dostępie do informacji publicznej, ordynację podatkową.
Strategia Rozwoju Kraju 2020	Strategia wyznacza **trzy obszary strategiczne** – *Sprawne i efektywne państwo, Konkurencyjna gospodarka, Spójność społeczna i terytorialna.*
Długookresowa Strategia Rozwoju Kraju. Polska 2030. Trzecia fala nowoczesności	Strategia określa priorytety w dziedzinie poprawy sprawności państwa oraz rozwoju społeczeństwa cyfrowego. Jednym z nich jest sprawne i efektywne państwo, gdzie celem jest przejście od administrowania do zarządzania rozwojem, m.in. przez wprowadzenie jednolitych zasad e-government w administracji.
Państwo 2.0 – Nowy start dla e-administracji	Raport przedstawia informacje na temat stanu realizacji projektów dotyczących informatyzacji i cyfryzacji wchodzących w zakres kompetencji nowo utworzonego Ministerstwa Administracji i Cyfryzacji. Ponadto prezentuje kierunki dalszych działań w obszarze informatyzacji i cyfryzacji Polski, ze szczególnym uwzględnieniem działań na rzecz rozwoju i poprawy e-administracji[c].
Program Zintegrowanej Administracji Państwa	Dokument opisuje działania rządu zmierzające do dostarczenia społeczeństwu wysokiej jakości elektronicznych usług publicznych. Celem jest stworzenie spójnego, logicznego i sprawnego systemu informacyjnego państwa dostarczającego e-usługi na poziomie krajowym i europejskim. Program zapewni współpracę istniejących oraz nowych systemów teleinformatycznych administracji publicznej, eliminując jednocześnie powielające się funkcjonalności[d].

[a] R. Przybyszewski, *Administracja publiczna wobec przemian społeczno-ekonomicznych epoki informacyjnej*, Toruń 2009, s. 294–295.

[b] G. Sibiga, *Informatyzacja administracji publicznej w Polsce*, „Edukacja prawnicza" 2011, nr 3 (123), s. 4.

[c] *Państwo 2.0 – Nowy start dla e-administracji*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.

[d] *Program zintegrowanej administracji państwa*, s. 4.

Opracowanie własne.

• Generalny Inspektor Danych Osobowych[120] – do jego obowiązków należy m.in. nadzorowanie zgodności przetwarzania danych z przepisami ustawy o ochronie danych osobowych, wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach dotyczących wykonywania przepisów ww. ustawy.

W Polsce opracowywanych jest wiele projektów w obszarze e-administracji, m.in.:

• Elektroniczna Platforma Usług Publicznych (ePUAP)[121] – realizacja projektu podzielona była na dwa etapy, w ramach których wyodrębniono ePUAP i ePUAP2. Według definicji legalnej jest to „system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci Internet"[122]. Celem zaprojektowania i wdrożenia platformy ePUAP jest stworzenie jednolitego, bezpiecznego kanału udostępniania usług publicznych przez administrację publiczną. W tym celu konieczne jest doprowadzenie do interoperacyjności systemów informatycznych w administracji publicznej, tak aby były przydatne w procesach realizacji zadań publicznych dla wszystkich jednostek administracyjnych[123].

• OST 112 – Ogólnopolska Sieć Teleinformatyczna na potrzeby obsługi numeru alarmowego 112, służąca poprawie bezpieczeństwa obywateli.

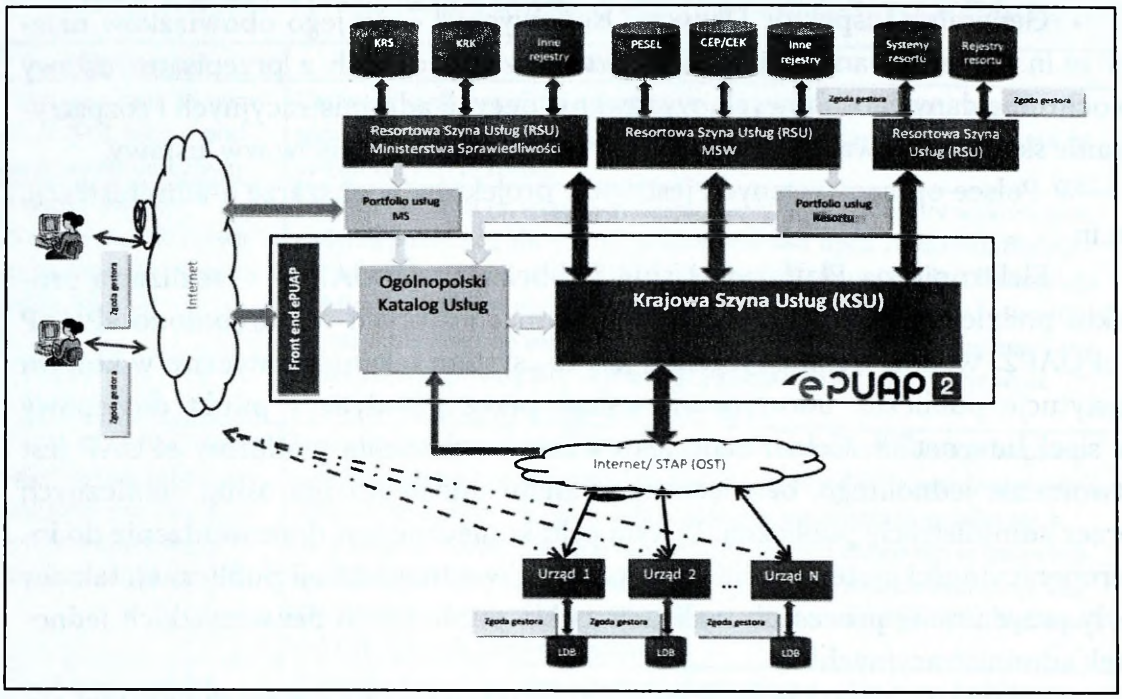
• Geoportal[124] – system pośredniczy w dostępie do usług danych przestrzennych i usług infrastrukturalnych. W ramach projektu uruchomiono i udostępniono: Portal Branżowy, Geoportal Krajowy, Geoportal Inspire.

• Chmura – celem projektu „Informatyzacja JST z zastosowaniem technologii przetwarzania w chmurze" jest umożliwienie urzędom świadczenia obywatelom i przedsiębiorcom nowych, zintegrowanych usług elektronicznej administracji. Projekt zakłada rozwój nowych i integrację już eksploatowanych[125].

• System Informatyczny Powiadamiania Ratunkowego – w ramach projektu budowana jest ogólnokrajowa platforma służąca do obsługi zgłoszeń alarmowych na potrzeby funkcjonowania Centrów Powiadamiania Ratunkowego oraz Wojewódzkich Centrów Powiadamiania Ratunkowego[126].

W procesie informatyzacji administracji publicznej podkreśla się konieczność integracji rejestrów państwowych w celu zwiększenia spójności i rzetelności informacji (rys. 1.16).

120 Strona oficjalna GIODO: http://www.giodo.gov.pl/.
121 Strona oficjalna ePUAP: http://epuap.gov.pl/.
122 Art. 3 pkt 13. Ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64, poz. 565 ze zm.).
123 S. Wrzosek, *Kompendium wiedzy administratywisty*, Lublin 2008, s. 621.
124 Strona oficjalna Geoportal: http://geoportal.gov.pl/start.
125 Strona oficjalna: http://www.cpi.gov.pl/chmura,170.html.
126 Strona oficjalna: http://www.cpi.gov.pl/si_pr,44.html.



Źródło: *Program Zintegrowanej...*, op. cit., s. 125.

Rys. 1.16. Model Platformy Integracyjnej Rejestrów Państwowych w Polsce (koncepcja)

Istotną barierą dla funkcjonowania e-administracji w Polsce jest także zbyt niski poziom wykorzystania przez obywateli dostępnych już e-usług administracji publicznej. Ponadto dotychczasowe działania w zakresie budowy infrastruktury informacyjnej państwa doprowadziły do uformowania się wielu autonomicznych rozwiązań teleinformatycznych, które odgrywają rolę rejestrów publicznych, ewidencji, wykazów. Niezgodność standardów (w tym standardów informatycznych), w szczególności w zakresie identyfikacji i klasyfikacji przedmiotowo-podmiotowych, utrudnia prawidłową identyfikację informacji, wymianę danych, możliwość weryfikacji i korekty oraz powoduje dużą nadmiarowość danych, a także problemy interpretacyjne zgromadzonych danych.

2. ZAGROŻENIA CYBERPRZESTRZENI PAŃSTWA DLA BEZPIECZEŃSTWA STRUKTUR ADMINISTRACYJNYCH

2.1. Specyfika cyberprzestrzeni

Rewolucja informacyjna, powstanie Internetu, rozwój społeczeństwa informacyjnego, globalizacja niemalże wszystkich sfer aktywności człowieka oraz towarzyszący temu błyskawiczny postęp ICT są niewątpliwie wśród głównych trendów kształtujących współczesne środowisko informacyjne.

Konwergencja technologii informatycznych, telekomunikacyjnych i mediów – a w konsekwencji infosfery, socjosfery i technosfery[1] – doprowadziła do narodzin nowej domeny ludzkiej aktywności, określonej mianem cyberprzestrzeni. Znakiem czasów stało się powszechne wykorzystanie Internetu oraz przetwarzanie ogromnych ilości danych[2].

Cyberprzestrzeń stała się środowiskiem obejmującym wiele obszarów funkcjonowania człowieka. Chociaż to pojęcie jest wciąż uznawane za swoiste *novum*, termin ten został po raz pierwszy użyty już w latach osiemdziesiątych ubiegłego wieku przez W. Gibsona, który określił ją następująco: *Konsensualna halucynacja doświadczana każdego dnia przez miliardy użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych* [...]. *Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność... Świetlne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje*

1 P. Sienkiewicz, *Bezpieczeństwo cyberprzestrzeni* [w:] *Metodologia badań bezpieczeństwa narodowego. Tom III*, red. P. Sienkiewicz, M. Marszałek, H. Świeboda, Warszawa 2012, s. 323.

2 W celu zobrazowania skali zjawiska warto posłużyć się kilkoma liczbami: 1) liczba mieszkańców na świecie wynosi ponad 7 mld, ponad 2 mld z nich korzystają z Internetu; 2) na świecie jest ponad 5 mld aktywnych numerów telefonów komórkowych; 3) liczba użytkowników Internetu w Polsce wynosi ok. 24 mln; 4) wyszukiwarka Google otrzymuje dziennie ponad miliard zapytań; 5) statystyczny użytkownik Internetu spędza w sieci 16 godzin miesięcznie, co w skali świata daje ok. 35 mld godzin w ciągu miesiąca (czyli w przybliżeniu 4 tys. lat on-line na każdy miesiąc kalendarzowy); 6) liczba kont na portalu Facebook przekracza miliard, w tym ponad 10 mln to konta użytkowników z Polski; 7) co sekundę w serwisie YouTube pojawia się kolejna godzina materiału filmowego. Dane statystyczne przywołano za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 9/13, s. 225.

danych[3]. Przywołane określenie trudno uznać za zadowalające z praktycznego punktu widzenia. Jednakże nie można odmówić mu wartości poznawczej. Gibson bowiem wskazał pewne specyficzne cechy tego środowiska – nieograniczoność w czasie i przestrzeni, wirtualność, złożoność oraz spajanie wszystkich zasobów w jedną olbrzymią bazę danych. Wizualizacja w określeniu Gibsona „graficzne odwzorowanie" stała się charakterystyczna dla nurtu określonego mianem cyberpunku[4].

Chociaż pojęcie cyberprzestrzeni nie było wcześniej używane, jego powstania należy doszukiwać się wcześniej. Sieciowość, będąca jedną ze specyficznych cech cyberprzestrzeni, łączona jest bardzo często z rewolucją informacyjną. Jednakże jak już podkreślono w rozdziale pierwszym, ludzkość od zawsze tworzyła różnego rodzaju sieci komunikacyjne, których skomplikowanie rozwijało się wraz z kolejnymi wynalazkami. Powstanie cybernetyki przedstawionej przez Norberta Wienera w 1948 roku, określonej jako *kontrola i komunikacja pomiędzy światem zwierząt a maszyn*[5], kreowało wizje cybernetycznego społeczeństwa. Skonstruowanie komputera, uruchomienie sieci ARPANET, powstanie Internetu oraz wiele innych dokonań dało początek nowej jakości w komunikacji, uwarunkowanej przez ogromną złożoność relacji i interakcji.

Wobec powyższego uzasadnione jest przyjęcie historycznej ewolucji cyberprzestrzeni zaproponowanej przez P. Sienkiewicza – począwszy od wynalazku Gutenberga do obecnie dominującej roli Internetu[6] (tab. 2.1).

Analizując istotę cyberprzestrzeni, w literaturze eksponuje się często związek między przestrzenią cybernetyczną a wirtualną rzeczywistością. Ontologia przestrzeni była przedmiotem rozważań wielu filozofów, m.in. Demokryta (*Naprawdę istnieją tylko atomy i próżnia* [...] *powszechną własnością atomów jest ruch* [...] *polega on na zmianie miejsca w przestrzeni*[7]) czy I. Kanta (*przestrzeń i czas są subiektywnymi formami zmysłowości*[8]). Leibniz natomiast określał przestrzeń jako *współistniejące rzeczy w tym samym czasie*[9] – ujęcie to rozwinął A. Einstein, wpro-

3 W. Gibson, *Neuromancer*, Katowice 2009, s. 59.

4 Cyberpunk – nurt w literaturze fantastycznej oraz kinematografii, który eksponuje relacje człowieka miedzy nim a otaczającą go zaawansowaną technologią. Cechą gatunku jest przedstawienie wizji przyszłości, w której środowiska ludzi, urządzeń i komputerów zaczynają się wzajemnie przenikać. Cyberpunk zdaje się uosobieniem postulowanej przez futurystów zasady „3M – Miasto, Masa, Maszyna". Do dzieł tego nurtu zalicza się przykładowo powieści Gibsona (np. *Graf Zero*, *Mona Liza Turbo*, *Światło wirtualne*, *Wszystkie jutra*), Bruce'a Sterlinga (np. *Schitzmatrix*, *Święty płomień*) oraz filmy, np. *John Mnemonic* i trylogię *Matrix*.

5 Przywołana definicja nawiązuje bezpośrednio do tytułu pracy – N. Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine*, New York 1948.

6 P. Sienkiewicz, *Bezpieczeństwo cyberprzestrzeni...*, op. cit., s. 324.

7 Zob. W. Tatarkiewicz, *Historia filozofii. Tom I*, Warszawa 2011, s. 50–57.

8 Zob. W. Tatarkiewicz, *Historia filozofii. Tom II*, Warszawa 2011, s. 182–209.

9 Cyt. za: P. Sienkiewicz, *25 wykładów...*, op. cit., s. 104.

wadzając pojęcie czasoprzestrzeni. Postęp, którego jesteśmy świadkami, sprawił, że informacja dostępna jest w trybie natychmiastowym. Przestrzeń kojarzona z określonymi rzeczywistymi miejscami zastąpiona została przestrzenią przepływów, o której pisał M. Castells. Dawniej przestrzeń była ograniczona geograficznie, dzisiaj – ma różne warstwy o niewyobrażalnym poziomie złożoności. Opisywana sieciowość związana jest niewątpliwie z dynamicznym rozwojem telekomunikacji oraz upowszechnieniem sieci Internet. Wirtualność postrzegana jako iluzja – w odniesieniu do cyberprzestrzeni tworzy niespotkane dotąd możliwości kreowania odwzorowania rzeczywistości. Postrzeganie cyberprzestrzeni jedynie jako świata wirtualnego nie jest do końca jednoznaczne. Od strony technicznej fundamentem jej funkcjonowania jest Internet oraz sieci, na które składają się komputery, ich komponenty oraz architektura. Przestrzeń przepływów jest zarządzana przez pewne centra, a wirtualna rzeczywistość tworzona jest przez realne osoby.

Tab. 2.1. Model ewolucji cyberprzestrzeni

Faza rozwoju	Ogólna charakterystyka
Cyberprzestrzeń – 0	– „Galaktyka Gutenberga" (M. McLuhan) – rozwój drukowanego pisma oraz początki rozwoju telegrafii, telefonii, radia, telewizji
Cyberprzestrzeń – 1	– „Galaktyka Wienera" (P. Sienkiewicz) – „społeczeństwo informacyjne" (Masuda) – cybernetyczne koncepcje rozwoju systemów społecznych, rozwój techniki cyfrowej, systemy komputerowe, łączność satelitarna (TELSTAR), sieć komputerowa (ARPANET), „boom PC" – sztuczna inteligencja
Cyberprzestrzeń – 2	– „Galaktyka Internetu" (M. Castells) – Internet (WWW), gospodarka oparta na wiedzy, globalizacja
Cyberprzestrzeń – 3	– „Galaktyka?" (?) – Internet (Web 2.0), globalizacja sieci komunikowania społecznego, nowe formy zachowań społecznych – „społeczeństwo wiedzy" (?)

Źródło: P. Sienkiewicz, *Bezpieczeństwo cyberprzestrzeni...*, op. cit., s. 324.

Rosnące wykorzystanie systemów teleinformatycznych przez społeczeństwa na całym świecie oraz ich znaczenie w infrastrukturze krytycznej doprowadziło do potrzeby legalnego definiowania cyberprzestrzeni. Konieczne było rozpoznanie tego specyficznego środowiska, które nadało nowy kształt czynnościom administracyjnym oraz określiło nowy wymiar bezpieczeństwa. Istota i bezpieczeństwo cyberprzestrzeni stały się przedmiotem badań w wielu ośrodkach naukowych.

Jedną z powszechnie cytowanych w literaturze definicji cyberprzestrzeni jest ta sformułowana przez Departament Obrony USA. Według niej cyberprzestrzeń to: *Globalna domena środowiska informacyjnego składająca się ze współzależności (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne,*

a także osadzone w nich procesory i kontrolery[10]. Przywołane określenie odnosi się jedynie do aspektu technologicznego cyberprzestrzeni. Brak jest w niej odwołania do sfery społecznej – człowieka będącego użytkownikiem cyberprzestrzeni. Ponadto definicja podkreśla sprzętową stronę infrastruktury z wiodącą rolą Internetu, pomija natomiast sferę programową.

W 2011 roku administracja Stanów Zjednoczonych zaprezentowała *Międzynarodową Strategię dla Cyberprzestrzeni*. Jest to pierwszy globalny dokument odnoszący się do ukierunkowanego rozwoju tego środowiska[11]. Podkreślono, że cyberprzestrzeń jest wszechobecna, a jej funkcjonowanie musi wiązać się z zapewnieniem swobodnego przepływu informacji, bezpieczeństwem, ochroną prywatności i zapewnieniem integralności danych. Czynniki te mają fundamentalne znaczenie dla globalnej koniunktury gospodarczej.

Na gruncie europejskim można także odnaleźć szereg definicji przyjętych w rządowych dokumentach różnych krajów, jak i Unii Europejskiej. Komisja Europejska definiuje ją następująco: *Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata*[12]. Podstawowym elementem tego ujęcia jest przestrzeń wirtualna tworząca systemy danych, do których uzyskuje się dostęp przez systemy teleinformatyczne. Interpretacja Komisji Europejskiej również pomija sferę użytkownika.

Inną, bardziej kompletną definicję cyberprzestrzeni proponuje Centrum Doskonalenia Cyberobrony NATO w Tallinie, zgodnie z którą *cyberprzestrzeń jest zależnym od czasu zbiorem połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami*[13]. Centrum w licznych opracowaniach odnosi się krytycznie do definicji cyberprzestrzeni, które eksponują jedynie aspekt techniczny, ignorując użytkownika.

W Polsce obowiązującym dokumentem planistycznym w zakresie cyberprzestrzeni jest *Doktryna Cyberbezpieczeństwa RP*, gdzie zdefiniowano omawianą kategorię w ten sposób: *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą*

10 *Dictionary of Military and Associated Terms*, "Joint Publication 1-02", Department of Defense, November 2010, s. 63. Dostęp na stronie: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni...*, op. cit., s. 227.

11 Zob. *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, May 2011. Dostęp na stronie: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

12 Cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni...*, op. cit., s. 229.

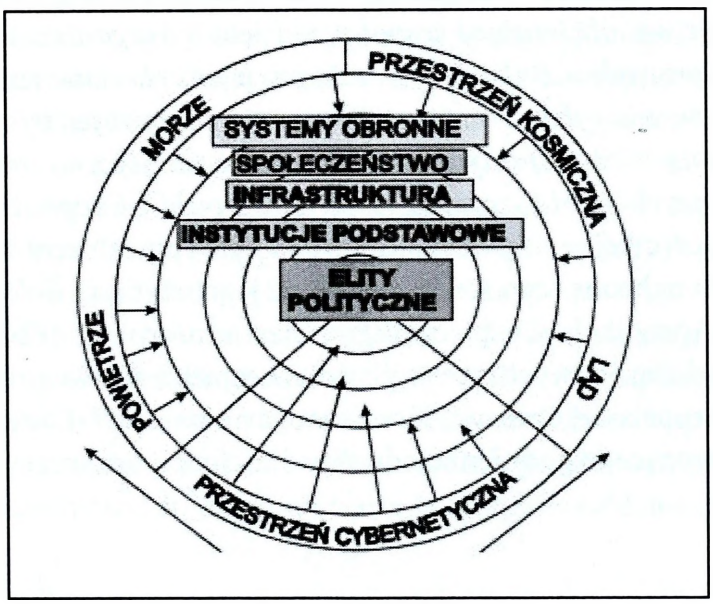
13 R. Ottis, P. Lorents, *Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence*, Tallinn. Dostęp na stronie: http://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf.

właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami[14].

Dodatkowo zdefiniowano cyberprzestrzeń RP, zawężając definicję do terytorium Polski i lokalizacji poza nim, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe). Polskie ujęcie kompleksowo obejmuje płaszczyzny cyberprzestrzeni – wymiar społeczny i techniczny oraz wirtualny.

Cyberprzestrzeń oferuje ogromne możliwości, m.in. e-learning, e-administrację, telepracę, lecz ma także swoją „ciemną stronę". W środowisku bezpieczeństwa można zaobserwować wzrost różnego rodzaju incydentów naruszających bezpieczeństwo informacyjne. Owe cyberzagrożenia mogą wywierać także destrukcyjny wpływ na infrastrukturę krytyczną państwa, której funkcjonowanie opiera się w znacznym stopniu na systemach teleinformatycznych.

Już w latach 90. ubiegłego wieku amerykański pułkownik J.A. Warden dostrzegł znaczenie cyberprzestrzeni w działaniach wojennych. Czerpiąc doświadczenia z pierwszej wojny w Zatoce Perskiej, skonstruował model, w którym określił wymiary oddziaływań na przeciwnika – ląd, morze, przestrzeń powietrzna, przestrzeń kosmiczna, cyberprzestrzeń (rys. 2.1).



Źródło: P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, red. L.H. Haber, Kraków 2003, s. 375.

Rys. 2.1. Model „pięciu wymiarów walki" Wardena

14 *Dokryna Cyberbezpieczeństwa RP*, Warszawa 2015, s. 7.

Potrzeba uregulowania kwestii związanych z bezpieczeństwem cyberprzestrzeni znalazła odzwierciedlenie w wielu dokumentach strategicznych oraz aktach prawnych. Szczegółowa ich analiza zostanie przeprowadzona w rozdziale trzecim, niemniej jednak warto wspomnieć o tym, że nowa koncepcja strategiczna NATO[15] oraz zaktualizowana polityka w dziedzinie cyberobrony w szczególnych przypadkach określa cyberzagrożenia jako potencjalny powód podjęcia obrony zbiorowej w myśl artykułu 5.

W Polsce w 2011 roku wprowadzono zmiany w ustawie o stanie wojennym, zgodnie z którymi w razie zewnętrznego zagrożenia państwa, również spowodowanego działaniami terrorystycznymi (w cyberprzestrzeni), zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa[16]. Jednym z zasadniczych celów ustawy jest wprowadzenie do systemu prawnego kategorii cyberprzestrzeni jako jednego ze składników bezpieczeństwa narodowego.

Sformułowanie definicji bezpieczeństwa cyberprzestrzeni stało się przedmiotem prac mających na celu opracowanie wspomnianej *Doktryny Cyberbezpieczeństwa RP*. W dokumencie przyjęto następującą definicję: *część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych*[17]. Przywołane określenie podkreśla aspekt funkcjonalny bezpieczeństwa cyberprzestrzeni, czyli działania mającego na celu ochronę tego środowiska oraz jego użytkowników.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) przeprowadziła przegląd narodowych strategii cyberbezpieczeństwa przyjętych przez państwa Unii Europejskiej oraz niektóre państwa na świecie[18]. Określiła w nim rekomendacje dotyczące uzgodnienia jednolitych definicji dotyczących cyberprze-

15 *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego*, Lizbona 2010.

16 Ustawa z dnia 30 sierpnia 2011 roku o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. 2002 nr 156, poz. 1301).

17 *Doktryna Cyberbezpieczeństwa RP...*, op. cit., s. 8.

18 *National Cyber Security Strategies in the World*, ENISA. Dostęp na stronie: http://www.enisa.Europa.eu/activities/Reesilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

strzeni oraz jej bezpieczeństwa, wokół których kraje powinny tworzyć narodowe strategie cyberbezpieczeństwa.

Z punktu widzenia omawianej problematyki istotna jest także techniczna strona cyberprzestrzeni. D.E. Denning definiuje cyberprzestrzeń jako *przestrzeń informacji, którą tworzą łącznie wszystkie sieci komputerowe*[19]. Podobne określenie proponuje G.T. Rattray: *Domena fizyczna będąca wynikiem utworzenia systemów informacyjnych i sieci, które umożliwiają wzajemne oddziaływania drogą elektroniczną*[20]. P. Sienkiewicz definiuje cyberprzestrzeń w wymiarze technicznym: *sieć globalna tworzona przez zmienną w czasie liczbę sieci składowych (TCP/IP) o nieograniczonych otwartych zasobach i dostępnych usługach*[21]. W przywołanych definicjach cyberprzestrzeń odnoszona jest do systemów komputerowych działających w ramach sieci komputerowych.

Systemy komputerowe są układem współdziałających ze sobą dwóch składowych: sprzętu komputerowego i oprogramowania. Technologia cyfrowa, oparta na logice binarnej[22], wykorzystuje do działań elementarnych tzw. bramki logiczne[23], które są podstawą budowy podzespołów komputerowych. Operacje są oparte na dwóch stanach logicznych – prawda, fałsz. W praktyce odpowiada to stanom napięcia: jeżeli ono nie występuje – fałsz (0), jeżeli występuje – prawda (1). Taki stan logiczny nazywany jest bitem. Wszystkie dane, na których operuje komputer, zapisane są w postaci ciągu bitów. W praktyce systemy komputerowe posługują się słowem ośmiobitowym (bajt). Struktura systemu komputerowego składa się z pięciu warstw: warstwa sprzętowa, oprogramowanie systemowe, oprogramowanie narzędziowe, oprogramowanie użytkowe oraz użytkownicy.

Podstawowym elementem, dzięki któremu funkcjonuje komputer, jest procesor, który pobiera dane z pamięci i wykonuje jako ciąg rozkazów, steruje oraz komunikuje się z innymi podzespołami. Stosuje się go nie tylko w urządzeniach komputerowych, ale także w innych urządzeniach, np. telefonie komórkowym, routerze, karcie graficznej. Procesor wykonuje polecenia zapisane m.in. w programach i systemach operacyjnych, ale również w szkodliwym oprogramowaniu, przez co może zarządzać danymi oraz sterować ich przepływem także do innych systemów informatycznych. Sformułowane w latach sześćdziesiątych ubiegłego

19 D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 24.

20 G.T. Rattray, *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004, s. 30.

21 P. Sienkiewicz, *Bezpieczeństwo cyberprzestrzeni...*, op. cit.

22 Logika binarna bazuje na algebrze Boole'a. Opisuje ona przetwarzanie informacji. Głównym osiągnięciem Boole'a było wprowadzenie do matematyki i logiki pojęcia algebry dwuwartościowej Ze względu na wagę tego pojęcia oraz jego zastosowań w informatyce i logice matematycznej Boole jest powszechnie uważany za jednego z twórców tych dziedzin nauki.

23 Bramka logiczna – elementy realizujące określone funkcje logiczne – alternatywę (OR), koniunkcję (AND), negację (NOT).

wieku prawo Moore'a wciąż się sprawdza – rozwój procesorów następuje bardzo szybko, co powoduje coraz większą ich złożoność, z którą wiąże się możliwość powstania błędów w krytycznym elemencie architektury systemów komputerowych. Niestety rozwiązania techniczne wiążą się często z powstawaniem pomyłek projektowych. Błędy te mogą umożliwić szkodliwemu oprogramowaniu dostęp do danych.

Natomiast sieci komputerowe są *systemem wzajemnych powiązań stacji roboczych, urządzeń peryferyjnych (takich jak drukarki, twarde dyski, skanery i stacje robocze) i innych urządzeń*[24]. Sieci komputerowe ze względu na swoją funkcjonalność stanowią rdzeń wszystkich systemów informatycznych. Praca w sieci komputerowej umożliwia udostępnianie danych, sprzętu i oprogramowania oraz zarządzanie z jednego komputera wszystkimi urządzeniami połączonymi w sieć.

W latach osiemdziesiątych ubiegłego stulecia Międzynarodowa Organizacja Normalizacyjna (ISO) opublikowała model sieci komputerowych (ISO/OSI). Pomimo że nie przyjął się w praktyce i pozostaje wyłącznie modelem teoretycznym, jest powszechnie traktowany jako punkt odniesienia w stosunku do mechanizmów funkcjonowania sieci komputerowych. Model składa się z siedmiu warstw (tab. 2.2).

Każda warstwa systemu jednego urządzenia komunikuje się z odpowiadającą jej warstwą drugiego urządzenia. Aby komunikacja w tej formie była możliwa, warstwy wyższe urządzenia wysyłającego muszą skorzystać z usług świadczonych przez warstwy niższe, natomiast w przypadku urządzenia odbierającego jest odwrotnie[25]. Polega to na tym, że warstwa wyższa przekazuje dane do wysyłania warstwie niższej, która przekształca dane na odpowiednią postać i przekazuje następnej niższej warstwie. Dane zostają w warstwie fizycznej przekształcone na ciąg bitów i przekazane warstwie fizycznej urządzenia odbierającego, w którym zachodzi proces odwrotny. Przy użyciu tego modelu można wyjaśnić, w jaki sposób dane są przesyłane między różnymi urządzeniami niezależnie od ich konstrukcji.

W praktyce wykorzystywany jest protokół TCP/IP, który powstał przed modelem ISO/OSI. Został on zaimplementowany w sieci ARPANET. Model TCP/IP składa się z czterech warstw. Warstwy modelu ISO/OSI wykazują wiele podobieństw w funkcjonowaniu z modelem TCP/IP (rys. 2.2).

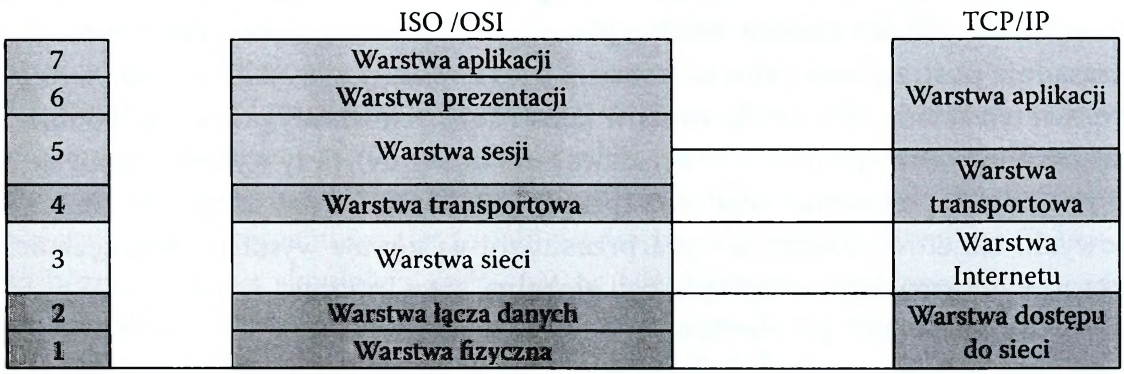
24 V. Amato, W. Lewis, *Akademia sieci CISCO. Pierwszy rok nauki*, Warszawa 2001, s. 18.

25 S. Dyrda, W. Graniszewski, G, Świątek, *Sieci komputerowe* [w:] *Informatyka gospodarcza 1*, red. J. Zawiła-Niedźwiecki, K. Rostek, A. Gąsierkiewicz, Warszawa 2010, s. 542.

Tab. 2.2. Warstwy modelu ISO/OSI

Warstwa	Charakterystyka
Warstwa aplikacji	Najbliższa użytkownikowi. Zapewnia usługi sieciowe aplikacjom użytkownika. Od pozostałych warstw różni się tym, że nie zapewnia usług innym warstwom modelu OSI, ale obsługuje aplikacje spoza zakresu modeli, np. arkusze kalkulacyjne. Warstwa aplikacji identyfikuje i sprawdza dostępność partnerów w procesie komunikowania się, synchronizuje współpracujące ze sobą aplikacje, realizuje uzgodnienia dotyczące rozpoznawania błędów i kontroli integralności danych.
Warstwa prezentacji	Sprawia, że informacja wysłana przez warstwę aplikacji w jednym systemie będzie odczytana przez warstwę aplikacji w drugim systemie. Jeżeli to konieczne, odbywa się tu translacja między różnymi formatami reprezentacji danych.
Warstwa sesji	Ustanawia, zarządza i zamyka sesje pomiędzy dwoma porozumiewającymi się ze sobą hostami.
Warstwa transportu	Odpowiedzialna jest za ustanowienie niezawodnego połączenia i przesyłania danych pomiędzy dwoma hostami. Dla zapewnienia niezawodności świadczonych usług w tej warstwie wykrywane i usuwane są błędy, a także kontrolowany jest przepływ informacji.
Warstwa sieci	Zapewnia łączność i wybór optymalnych ścieżek między dwoma dowolnymi hostami znajdującymi się w różnych sieciach. Do podstawowych funkcji tej warstwy należy: adresowanie logiczne oraz wybór najlepszych tras dla pakietów.
Warstwa łącza danych	Zapewnia niezawodne przesyłanie danych po fizycznym medium transmisyjnym. Warstwa ta jest odpowiedzialna za adresowanie fizyczne (sprzętowe), dostęp do łącza, informowanie o błędach i kontrolę przepływu danych.
Warstwa fizyczna	Definiuje elektryczne, mechaniczne, proceduralne i funkcjonalne mechanizmy aktywowania, utrzymywania i dezaktywacji fizycznego połączenia pomiędzy urządzeniami sieciowymi. Warstwa ta jest odpowiedzialna za przenoszenie elementarnych danych (bitów) za pomocą sygnałów elektrycznych, optycznych lub radiowych.

Opracowanie własne na podstawie: V. Amato, W. Lewis, *Akademia sieci CISCO...*, op. cit., s. 23–24.



Opracowanie własne na podstawie: S. Dyrda, W. Graniszewski, G. Świątek, *Sieci komputerowe...*, op. cit., s. 545.

Rys. 2.2. Porównanie modelu sieci komputerowej ISO/OSI z modelem TCP/IP

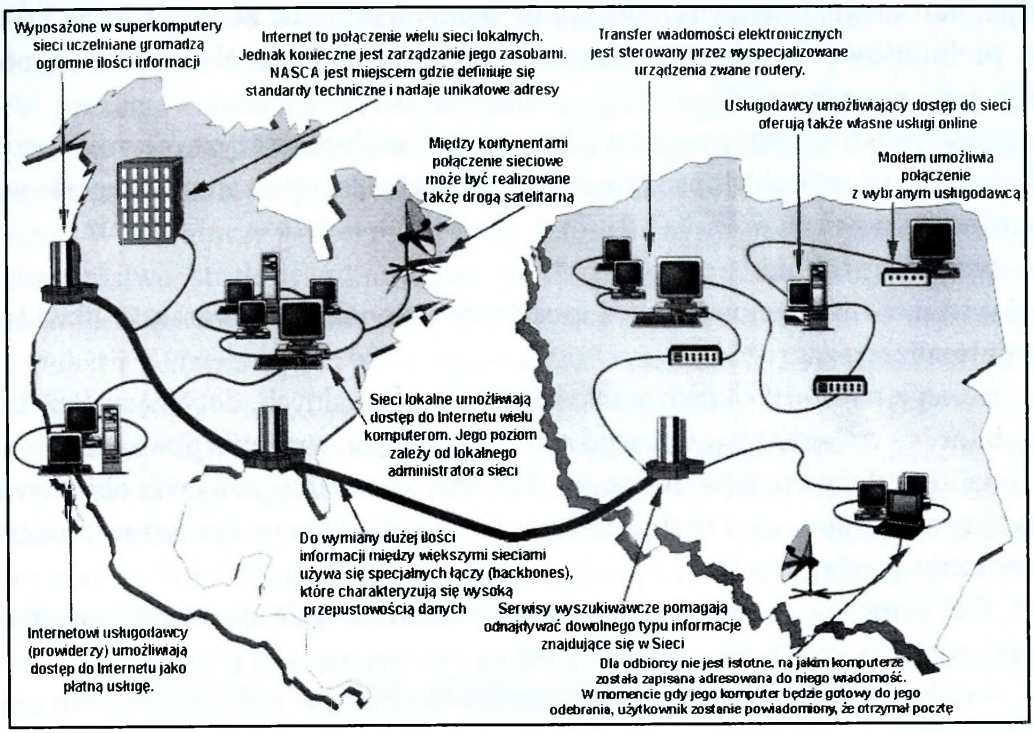
Podstawą sieci komputerowych jest sposób realizacji fizycznych połączeń między komputerami, które w zastosowaniach praktycznych opisywane są przez warstwy dostępu do sieci modelu TCP/IP. Wybór właściwego protokołu zależy bezpośrednio od wielkości obszaru geograficznego, na którym działa sieć. Ze względu na zasięg wyróżnia się trzy główne typy sieci komputerowych: sieć lokalną LAN, sieć miejską MAN, sieć rozległą WAN. Dodatkowo wyróżnia się także sieć PAN (zasięg do 10 metrów, łączy urządzenia osobiste, np. telefon komórkowy), CAN (grupa wzajemnie połączonych sieci lokalnych na ograniczonym obszarze, np. kampusie akademickim), VPN (służy do łączenia odległych sieci lokalnych z wykorzystaniem publicznej infrastruktury sieciowej, metodą tworzenia szyfrowanych tuneli komunikacyjnych między obiektami), Internetwork (jedna lub więcej sieci połączonych z zastosowaniem jednolitych zasad komunikacji w celu udostępniania wewnętrznych zasobów, np. sieć wewnętrzna organizacji).

Internet jest ogólnoświatową siecią komputerową, określaną także jako sieć sieci. Jest przykładem sieci rozległej. Pojedyncza sieć komputerowa stanowi element Internetu i posiada zdolność samodzielnego funkcjonowania. W sieci może pracować wiele komputerów połączonych za pomocą routerów. W sieci komputerów wyróżnia się dwa typy: serwer to komputer, który udostępnia swoje zasoby innym komputerom w sieci, natomiast klient to komputer, który korzysta z zasobów znajdujących się na serwerach. Na rys. 2.3 przedstawiono schemat funkcjonowania sieci Internet.

Przeprowadzona analiza skłania do wniosku, że definicje cyberprzestrzeni akcentują różne jej cechy. W wielu z nich podkreśla się, że przestrzeń cybernetyczna jest sumą fizycznych składników – sieci, oprogramowania oraz przetwarzanych w nich informacji. W innych dodatkowo uwzględnia się sumę operacji wykonywanych przez użytkowników. Wzrost znaczenia cyberprzestrzeni w funkcjonowaniu wielu obszarów państwa i społeczeństwa doprowadził do tworzenia narodowych i międzynarodowych strategii bezpieczeństwa cyberprzestrzeni.

Istotę cyberprzestrzeni stanowi koncepcja środowiska, które jest nowym wymiarem dla ludzkich działań. Analiza przeprowadzona w niniejszym podrozdziale uzasadnia postrzeganie cyberprzestrzeni jako *ewoluującego systemu złożonego*[26]. System ten składa się z użytkowników konstruujących własny przekaz lub odbierających inny (użytkownik w roli nadawcy lub odbiorcy), przy wykorzystaniu sieci połączeń, oprogramowania oraz sprzętu (np. komputerów, telefonów komórkowych, tabletów). Zatem w cyberprzestrzeni występuje wymiana i sprzężenie zwrotne informacji przy wiodącej roli globalnej sieci Internet.

26 P. Sienkiewicz, *Bezpieczeństwo cyberprzestrzeni...*, op. cit., s. 329.



Źródło: http://angraplay.republika.pl/pliki/schematinternet.htm.

Rys. 2.3. Schemat funkcjonowania sieci Internet

2.2. Aspekty bezpieczeństwa struktur administracyjnych

Rozważając pojęcie bezpieczeństwa struktur administracyjnych, warto sięgnąć do teorii bezpieczeństwa. Wraz z rozwojem nauki problematyka bezpieczeństwa absorbowała badaczy wielu dyscyplin naukowych. Kategoria bezpieczeństwa przez stulecia stosowana była zarówno w mowie potocznej, jak i publicystyce politycznej. Z czasem zostało ono zaadaptowane przez nauki wojskowe, nauki o stosunkach międzynarodowych, a od niedawna także nową dyscyplinę określaną mianem securitologii.

Ewolucja bezpieczeństwa związana jest ze stopniowym poszerzeniem zakresu wartości chronionych. Tradycyjnie (wąsko) rozumiane bezpieczeństwo narodowe odnosiło się jedynie do zagrożeń militarnych zagrażających przetrwaniu państwa, jego integralności terytorialnej oraz niezależności politycznej. Polityka bezpieczeństwa skupiała się głównie na sile militarnej oraz przewadze nad przeciwnikiem. Pod wpływem wielu czynników pojawiło się szerokie ujęcie bezpieczeństwa, które opiera się na wielu płaszczyznach funkcjonowania państwa. W teorii bezpieczeństwa i nauce o stosunkach międzynarodowych wyróżnia się różne wymiary bezpieczeństwa związane z przyjętymi kryteriami. Przykładowo ze względu na kryterium podmiotowe wyróżnia się bezpieczeństwo: jednostkowe,

lokalne, narodowe, międzynarodowe i globalne, natomiast ze względu na kryterium podmiotowe wyróżnia się bezpieczeństwo: militarne, ekonomiczne, polityczne, informacyjne itd.[27]

Bezpieczeństwo jest pojęciem złożonym i wielopłaszczyznowym, o czym może świadczyć różnorodność typologii i definicji. Jest ono zatem kategorią wieloznaczną, odnoszoną do[28]:

- braku zagrożenia;
- systemu instytucjonalnych i pozainstytucjonalnych gwarancji likwidacji lub minimalizacji zagrożeń;
- jednej z najistotniejszych wartości egzystencjonalnych, dotyczących poczucia stabilności, trwałości korzystnego stanu zagrożenia, wrażenia pewności itp.

Ponadto należy zwrócić uwagę na dwa aspekty bezpieczeństwa: obiektywny (związany z wystąpieniem realnych zagrożeń) i subiektywny (związany z odczuwaniem zagrożenia).

D. Frei zauważa, że stan bezpieczeństwa może, w zależności od jego obiektywnej i subiektywnej oceny, przybrać jedną z następujących postaci[29]:

- stan braku bezpieczeństwa – zagrożenie jest rzeczywiste, a jego postrzeganie adekwatne;
- stan obsesji – nieznaczne zagrożenie jest postrzegane jako duże;
- stan fałszywego bezpieczeństwa – zagrożenie jest poważne, a postrzegane jako niewielkie;
- stan bezpieczeństwa – zagrożenie jest mało prawdopodobne, a jego postrzeganie jest prawidłowe.

Z kolei na gruncie analizy systemowej dominują dwa ujęcia bezpieczeństwa systemów, a mianowicie[30]:

- bezpieczeństwo jako własność obiektu charakteryzująca się jego odpornością na powstawanie sytuacji niebezpiecznych (zagrożeń), przy czym uwaga koncentruje się na zawodności bezpieczeństwa obiektu, czyli jego podatności na powstawanie sytuacji niebezpiecznych;

27 Szerzej na temat typologii bezpieczeństwa: R. Zięba, *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych* [w:] *Bezpieczeństwo narodowe i międzynarodowe w schyłku XX wieku*, red. B.D. Bobrow, E. Haliżak, R. Zięba, Warszawa 1997, s. 43; J. Kukułka, *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*, Warszawa 1994, s. 40–41; J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 15–47.

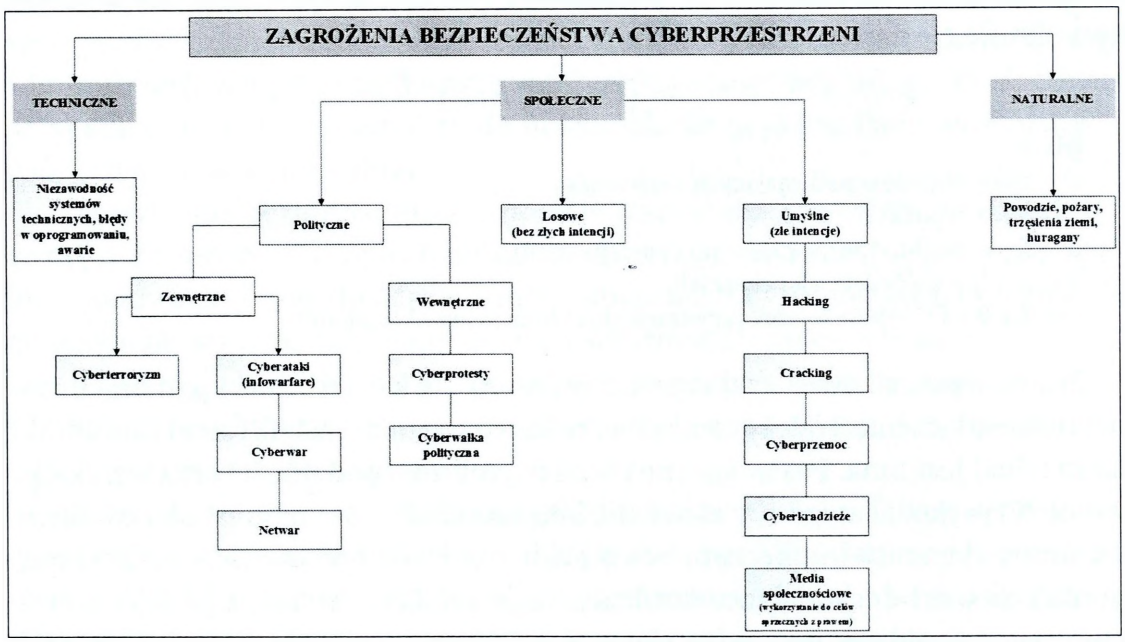
28 P. Sienkiewicz, H. Świeboda, *Perspektywy badań systemowych nad bezpieczeństwem* [w:] *Bezpieczeństwo. Wymiar współczesny i perspektywy badań*, red. M. Kwieciński, Kraków 2010, s. 13.

29 Cyt. za: R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 2004, s. 28.

30 P. Sienkiewicz, H. Świeboda, *Perspektywy badań systemowych...*, op. cit., s. 14.

• bezpieczeństwo systemu rozumiane jako zdolność do ochrony wewnętrznych wartości przed zewnętrznymi zagrożeniami.

W prezentowanym ujęciu bezpieczeństwo postrzegane jest w kategoriach cechy danego systemu, która warunkuje sprawność jego działania w przypadku wystąpienia zagrożenia. Pojęcie bezpieczeństwa jest nierozerwalnie związane z zagrożeniami. W literaturze funkcjonuje wiele definicji zagrożeń. Na potrzeby badania bezpieczeństwa struktur administracyjnych przyjęto definicję zaproponowaną przez P. Sienkiewicza: *zagrożenie to każde zjawisko (proces, zdarzenie) niepożądane z punktu widzenia niezakłóconego działania systemu*[31]. Zagrożenia mogą być wynikiem zawodności systemów technicznych (np. błędów w oprogramowaniu), katastrof naturalnych (np. pożarów) oraz działalności człowieka. W grupie zagrożeń związanych z postępowaniem człowieka można wyróżnić zagrożenia związane z działaniem celowym (np. działalność terrorystyczną) oraz z działaniem pozbawionym złych intencji (np. w wyniku niekompetencji i braku świadomości). Ogólną typologię zagrożeń dla bezpieczeństwa systemów przedstawia rys. 2.4.



Opracowanie P. Sienkiewicz.

Rys. 2.4. Ogólna typologia zagrożeń dla bezpieczeństwa systemów

Zagrożenie jest potencjalną przyczyną niepożądanego incydentu dla bezpieczeństwa systemu. Jego wystąpieniu sprzyja tzw. podatność, którą jest słabość lub luka w systemie. Taki incydent stwarza konsekwencje (skutki) dla organizacji. Relacja między zagrożeniem a podatnością, a w szczególności prawdopodobieństwo,

31 P. Sienkiewicz, *25 wykładów...*, op. cit., s. 260.

że zagrożenie wykorzysta podatność systemu, określana jest mianem ryzyka. W celu minimalizacji ryzyka wprowadza się różnego rodzaju zabezpieczenia. W związku z tym istotne dla bezpieczeństwa systemów są następujące elementy:

- identyfikacja zagrożeń;
- identyfikacja podatności;
- ocena ryzyka;
- stosowanie zabezpieczeń, aby ryzyko sprowadzić do stanu akceptowalnego.

Jednym z ogólnych modeli bezpieczeństwa jest ten opracowany przez Clementsa. Niech $Z = \{z_1, z_2, z_3, ..., z_n\}$ będzie zbiorem wszystkich zagrożeń, a $O = \{o_1, o_2, o_3, ..., o_n\}$ zbiorem wszystkich obiektów. $R \subseteq Z \times X$ opisuje oddziaływanie zidentyfikowanych zagrożeń na obiekty[32]. Na dany obiekt może oddziaływać wiele zagrożeń oraz jedno zagrożenie może oddziaływać na wiele obiektów. Z zagrożeniem można wiązać prawdopodobieństwo jego wystąpienia, choć może być ono trudne do oszacowania.

Identyfikacja zagrożeń pozwala im zapobiegać przez zorganizowanie odpowiedniego systemu ochrony. W prezentowanym ujęciu systemem bezpieczeństwa określa się następującą piątkę:

$$S = \{O, Z, B, R, P\}$$

gdzie:
O – zbiór obiektów podlegających zagrożeniu,
Z – zbiór zagrożeń,
B – zbiór środków bezpieczeństwa (zabezpieczeń),
$R \subseteq Z \times X$ – zbiór ścieżek penetracji,
$P \subseteq Z \times B \times O$ – zbiór ścieżek penetracji chronionych przed atakiem[33].

System jest całkowicie zabezpieczony, jeżeli dla każdej ścieżki penetracji istnieje zabezpieczenie. Należy zauważyć, że każda organizacja (jak i struktura administracyjna) jest inna. Posiadają one różne zagrożenia, podatności oraz wynikające z nich ryzyko. Dlatego aby zapewnić bezpieczeństwo systemu na planowanym poziomie, elementy bezpieczeństwa powinny być identyfikowane, analizowane, monitorowane i doskonalone. Realizacja tego założenia wymaga podejścia systemowego, ponieważ pomiędzy elementami bezpieczeństwa zachodzą związki przyczynowo-skutkowe oraz są one zmienne w czasie.

Wychodząc od ogólnej definicji bezpieczeństwa oraz zagrożenia, proponuje się definiowanie bezpieczeństwa struktur administracyjnych jako zdolności do ochrony przed zagrożeniami (zakłóceniami) funkcjonowania lub utraty określonych wartości. Analizując zaproponowaną definicję, warto zwrócić uwagę na dwa aspekty.

32 Cyt. za: J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Poznań 2001, s. 129.

33 J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych...*, op. cit., s. 130.

Po pierwsze bezpieczeństwo funkcjonowania struktury administracyjnej jest ściśle związane z wykonywaniem zadań publicznych. Ze specyfiki samorządu terytorialnego oraz celu powołania jednostki administracji publicznej wynika to, że część owych zadań różni się w poszczególnych jednostkach. Ogólnie można wyróżnić dwie podstawowe sfery funkcjonowania jednostek administracji publicznej:

- sferę zewnętrzną, związaną z działalnością w stosunku do podmiotów niepodporządkowanych podległością służbową danej jednostce administracji publicznej, np. świadczenie lub zapewnianie wykonania usług na rzecz mieszkańców i innych podmiotów, wydawanie decyzji administracyjnych;
- sferę wewnętrzną, oznaczającą stosunki z organami czy jednostkami podporządkowanymi bezpośrednio danej jednostce.

Po drugie istotną kwestię stanowią wartości, które mogą zostać utracone w wyniku wystąpienia zagrożenia. Funkcjonowanie administracji polega lub opiera się na gromadzeniu i przetwarzaniu informacji, dlatego też informacja jest podstawowym zasobem administracji i stanowi wartość chronioną. Incydent zagrażający bezpieczeństwu może w znacznym stopniu obniżyć poziom jakości usług administracyjnych przez zakłócenia w procesie świadczenia usługi. W skrajnym przypadku może doprowadzić to do uniemożliwienia jednostkom administracji publicznej świadczenia usługi.

Zapewnienie bezpieczeństwa procesów administracyjnych sprowadza się do dostępności usługi oraz zapewnienia bezpieczeństwa informacji na każdym etapie funkcjonowania jednostki administracji publicznej. Bezpieczeństwo informacyjne obejmuje zarówno problemy ochrony informacji wrażliwych, jak i zabezpieczenie systemów teleinformatycznych. Ze społecznego punktu widzenia istotnym przedmiotem ochrony są dane osobowe, obejmujące informacje dotyczące zidentyfikowanej lub możliwej do identyfikacji osoby.

W literaturze przedmiotu dostrzegalne są różne sposoby definiowania kategorii bezpieczeństwa informacyjnego, bezpieczeństwa informatycznego oraz bezpieczeństwa teleinformatycznego. W celu utrzymania spójności terminologicznej w monografii przyjęto następujące definiowanie wymienionych kategorii:

- Bezpieczeństwo informacyjne – ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub działaniem uniemożliwiającym jej przetworzenie.
- Bezpieczeństwo informatyczne – narzędzia i procedury ochrony danych i informacji oraz systemów informacyjnych[34].

34 P. Sienkiewicz, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka" 2009, tom 13, zeszyt II, s. 588.

• Bezpieczeństwo teleinformatyczne – zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymania atrybutów bezpieczeństwa w systemach teleinformatycznych[35].

Zgodnie z przywołanymi definicjami, bezpieczeństwo informacyjne jest pojęciem najszerszym, ponieważ obejmuje nie tylko elektroniczną postać informacji, jak to robią bezpieczeństwo teleinformatyczne czy informatyczne.

Niezależnie od postaci bezpieczeństwo informacji powinno spełnić tzw. atrybuty bezpieczeństwa, przedstawione w tabeli poniżej. Pierwsze trzy atrybuty, tj. poufność, dostępność, integralność, można odnieść do informacji niezależnie od formy (postaci). Dodatkowo w wielu opracowaniach wymienia się także: rozliczalność, autentyczność i niezawodność, które dotyczą zapewnienia bezpieczeństwa informacji w systemach teleinformatycznych.

Tab. 2.3. Atrybuty bezpieczeństwa informacji

Cecha	Charakterystyka
Poufność	dostęp do informacji musi być ograniczony tylko do kręgu użytkowników autoryzowanych
Integralność	informacja musi być zachowana w swej oryginalnej postaci, za wyjątkiem sytuacji, gdy jest aktualizowana lub usuwana przez osoby do tego uprawnione
Dostępność	informacja musi być dostępna dla osób upoważnionych na ich żądanie w każdej chwili
Rozliczalność	dotyczy możliwości identyfikacji użytkowników informacji i systemu teleinformatycznego oraz wykorzystania przez niego usług
Niezawodność	właściwość oznaczająca spójne zamierzone zachowania i skutki
Autentyczność	oznacza możliwość jednoznacznego stwierdzenia, jaki podmiot przesłał dane

Opracowanie własne na podstawie: A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Warszawa 2003, s. 246; K. Lidermann, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 19.

Interesujący standard na potrzeby analizy ryzyka (BSI-Standard 100-3) opracował niemiecki Federalny Urząd ds. Technologii Informatycznych. Suplementy dokumentu zawierają także wykaz elementarnych zagrożeń oraz ich szczegółowe definicje[36]. Zagrożenia zostały podzielone na 46 grup i dla każdej z nich określono wpływ ze względu na atrybuty bezpieczeństwa informacji:

35 A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006, s. 33.

36 Zob. *BSI-Standard 100-3. Risk analysis based on IT-Grundschutz*, Version 2.5, Bonn 2008, dostęp na stronie: https://www.bsi.bund.de/cae/servlet/contentblob/471432/publicationFile/28219/standard_100-3_e_pdf.pdf; *Supplement to BSI-Standard 100-3, Version 2.5 Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses*, Federal Office for Information Security, Bonn 2011; *Catalogue – Elementary Threats*, Federal Office for Information Security, Bonn 2011; dostęp na stronie: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/Download/download_node.html.

- poufność (P);
- integralność (I);
- dostępność (D).

Korzystając z katalogu zagrożeń, można określić wpływ zagrożeń na bezpieczeństwo informacji (tab. 2.4).

Tab. 2.4. Podział zagrożeń oraz ich wpływ na bezpieczeństwo informacji i systemów

Lp.	Nazwa podstawowego zagrożenia	Wpływ	Lp.	Nazwa podstawowego zagrożenia	Wpływ
1	Pożar	D, I	24	Niszczenie urządzeń, nośników	D
2	Niekorzystne warunki klimatyczne	D, I	25	Awaria urządzeń, systemów	D
3	Woda	D, I	26	Nieprawidłowe działanie urządzeń lub systemów	D, I, P
4	Zanieczyszczenia, pył, korozja	D, I	27	Brak zasobów	A
5	Klęski żywiołowe	D	28	Błędy, luki w zabezpieczeniach oprogramowania	D, I, P
6	Katastrofa ekologiczna	D	29	Naruszenie prawa, procedur	D, I, P
7	Ważne wydarzenie w środowisku	D, I, P	30	Nieuprawnione użycie lub administrowanie urządzeniami lub systemami	D, I, P
8	Awaria, przerwa w dostawie energii	D, I	31	Nieprawidłowe użycie lub administrowanie urządzeniami lub systemami	D, I, P
9	Awaria, przerwa w dostępie do sieci komunikacyjnych	D, I	32	Nadużycie upoważnień	D, I, P
10	Brak, utrata podstawowego zasilania	D	33	Brak personelu	A
11	Utrata, przerwa w świadczeniu usług przez usługodawców	D, I, P	34	Atak	D, I, P
12	Promieniowanie zakłócające	D, I	35	Stosowanie przymusu, wymuszenie, korupcja	D, I, P
13	Przechwytywanie emisji	P	36	Kradzież tożsamości	D, I, P
14	Przechwytywanie informacji, szpiegostwo	P	37	Zaniechanie działań	I, P
15	Podsłuchiwanie	P	38	Nadużywanie danych osobowych	P
16	Kradzież urządzeń, nośników danych, dokumentów	D, P	39	Złośliwe oprogramowanie	D, I, P
17	Utrata urządzeń, nośników danych, dokumentów	D, P	40	Odmowa świadczenia usługi	A
18	Złe planowanie, brak adaptacji	D, I, P	41	Sabotaż	A
19	Ujawnienie poufnych informacji	P	42	Inżynieria społeczna	I, P
20	Informacje z niewiarygodnego źródła	D, I, P	43	Powtarzanie wiadomości	I, P
21	Manipulacja sprzętem, oprogramowaniem	D, I, P	44	Nieautoryzowane wejście do pomieszczeń	D, I, P
22	Manipulacja informacją	I	45	Utrata danych	A
23	Nieuprawniony dostęp do systemów informatycznych	I, P	46	Utrata integralności informacji poufnych	I

Źródło: BSI, Supplement to BSI-Standard 100-3..., op. cit., s. 6, cyt. za: T. Muliński, *Zagrożenia bezpieczeństwa dla systemów e-administracji*, rozprawa doktorska, Szczytno 2014, s. 93.

Przeprowadzona analiza skłania do określenia sytuacji zagrożeń dla bezpieczeństwa struktur administracyjnych. Zakłócenia funkcjonowania administracji publicznej mogą występować na wielu płaszczyznach:

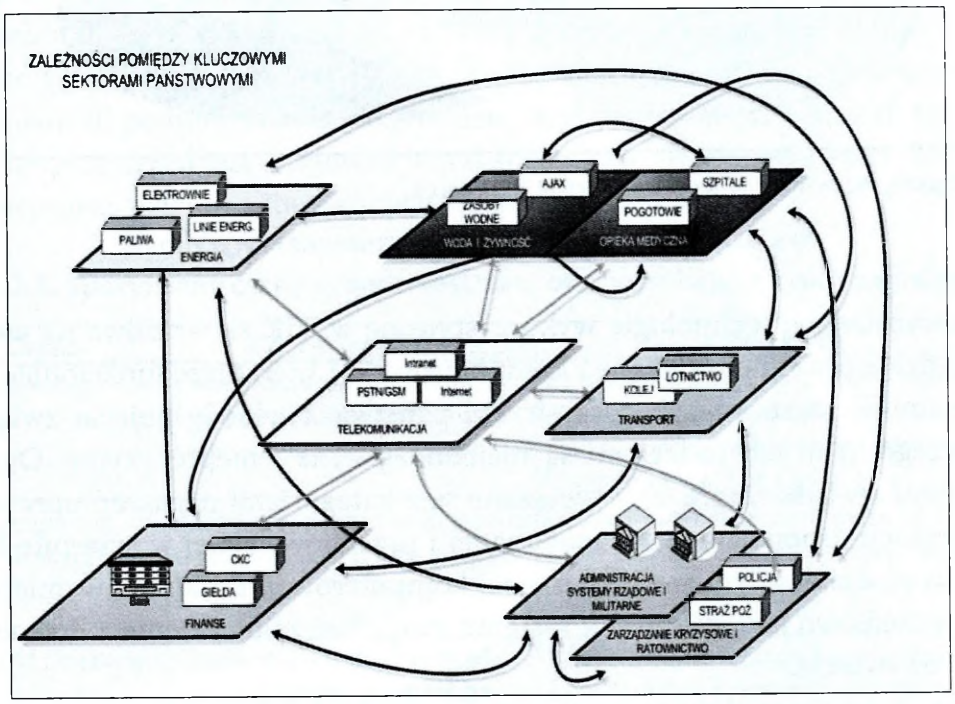
- zagrożenia naturalne związane z klęskami żywiołowymi, np. pożar budynku urzędu;
- tradycyjne zagrożenia informacyjne, związane z działaniami ukierunkowanymi na zdobycie informacji, np. szpiegostwo;
- cyberzagrożenia, obejmujące ataki na informację w systemach teleinformatycznych, które przyjmują często charakter cech właściwych np. dla cyberszpiegostwa czy cyberprzestępczości;
- zagrożenia związane z zawodnością systemów informatycznych, obejmujące przykładowo błędy w oprogramowaniu;
- zagrożenia naruszające prawa obywatelskie, związane z naruszeniem ochrony danych osobowych, przekazywaniem informacji nieuprawnionym podmiotom czy też szczególnie niebezpieczną kradzieżą tożsamości[37].
- zagrożenia związane z organizacją i procedurami wewnątrz organizacji, np. niewłaściwa koordynacja przepływu informacji czy też nieprzeszkoleni pracownicy stwarzają realne zagrożenie chociażby ze względu na łatwość ich manipulacji w związku z działaniami socjotechnicznymi.

Zastosowanie nowych technologii w sektorze publicznym przyczyniło się do powstania elektronicznej administracji, której elementy stanowią cyberprzestrzeń struktur administracyjnych. Przeniesienie części usług publicznych do cyberprzestrzeni wiąże się z ryzykiem wystąpienia zagrożeń dla systemów teleinformatycznych i przetwarzanych w nich danych. Bezpieczeństwo teleinformatyczne jest dyscypliną łączącą kilka innych: teorię organizacji i zarządzania, informatykę, prawo oraz nauki o bezpieczeństwie. Przeciwdziałanie zagrożeniom i ich złożonej naturze możliwe jest pod warunkiem skutecznego systemowego zarządzania bezpieczeństwem jednostki administracji publicznej, obejmującym kompleksowe zarządzanie posiadanymi zasobami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem ich utraty. Owo zarządzanie musi funkcjonować w graniach prawa przy odpowiednich rozwiązaniach organizacyjnych i proceduralnych. Z uwagi na problematykę monografii uzasadnione jest skoncentrowanie uwagi na identyfikacji cyberzagrożeń dla bezpieczeństwa struktur administracyjnych.

37 Kradzież tożsamości – celowe użycie danych osobowych innej osoby, najczęściej w celu osiągnięcia korzyści majątkowej.

2.3. Istota i taksonomia zagrożeń cyberprzestrzeni państwa

Zagrożenia cyberprzestrzeni można analizować w różnych wymiarach bezpieczeństwa. Z punktu widzenia bezpieczeństwa narodowego istotnym obszarem jest infrastruktura krytyczna państwa[38], na którą składają się obiekty szczególnie istotne dla bezpieczeństwa i obronności. Rozwój technologii informatycznych przyczynił się do uzależnienia infrastruktury krytycznej od sprawnego działania systemów teleinformatycznych. Powiązania między sektorami infrastruktury krytycznej są skomplikowane, a sektor telekomunikacyjny jest ogniwem spinającym je wszystkie (rys. 2.5).

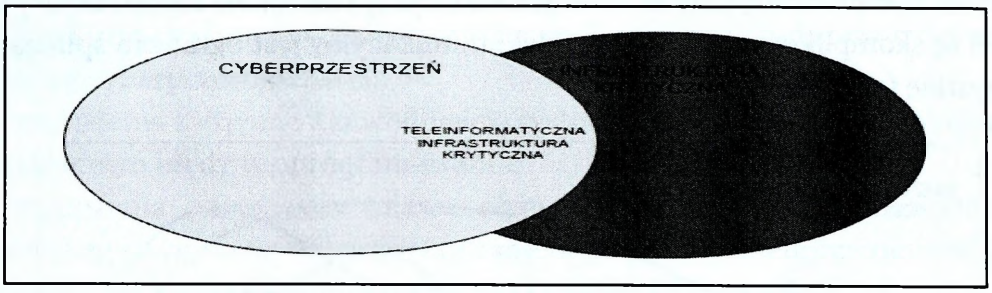


Źródło: K. Baniak, *Analiza zagrożeń telekomunikacyjnych sektora publicznego*, „Kwartalnik BBN. Tom 3 – Bezpieczeństwo w telekomunikacji i teleinformatyce", BBN, Warszawa 2007, s. 37.

Rys. 2.5. Zależności pomiędzy sektorami infrastruktury krytycznej

38 Infrastruktura krytyczna obejmuje systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Zob. art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89, poz. 5900).

Teleinformatyczna Infrastruktura Krytyczna (TIK) i cyberprzestrzeń obejmują wszystkie warstwy modelu ISO/OSI, jednakże TIK jest częścią cyberprzestrzeni o krytycznym znaczeniu dla jej funkcjonowania[39]. Administracja publiczna jest jednym z elementów właściwych w sprawach sprawnego funkcjonowania państwa i organów władzy publicznej. Kluczowe dla sprawnego funkcjonowania organów władzy publicznej, administracji, a także bezpieczeństwa państwa oraz obywateli stają się systemy teleinformatyczne stanowiące część infrastruktury krytycznej (rys. 2.6).



Źródło: *Rządowy Program Ochrony Cyberprzestrzeni RP...*, op. cit., s. 12.

Rys. 2.6. Teleinformatyczna Infrastruktura Krytyczna

Zaawansowane technologie wykorzystywane w TIK są wrażliwe na awarie, błędy ludzkie oraz ataki fizyczne i komputerowe. W literaturze funkcjonuje wiele taksonomii zagrożeń cyberprzestrzeni państwa. Niekiedy pojęcia związane z poszczególnymi ich rodzajami są niejednoznaczne i nieprecyzyjne. Ogólnie rzecz ujmując, cyberzagrożenia związane są z kategoriami naruszeń uprawnień do informacji gromadzonej, przetwarzanej i przechowywanej w systemie komputerowym, działającym w ramach sieci komputerowej. Działania wymierzone w bezpieczeństwo jakiegokolwiek systemu mogą być zainicjowane z dowolnego miejsca na świecie.

Najogólniej rzecz ujmując, wyróżnia się zagrożenia płynące z cyberprzestrzeni oraz zagrożenia wobec cyberprzestrzeni. O ile pierwsze z nich mają społeczny charakter, a ich szkodliwość jest znaczna – to nie wpływają jednak na destabilizację funkcjonowania państwa. Należą do nich np. cyberinwigilacja i cyberpornografia. Drugie natomiast stanowią realne zagrożenie bezpieczeństwa państwa – np. ataki na systemy krytycznej infrastruktury państwa.

Cyberprzestrzeń wydaje się szczególnie istotna w kontekście rozważań nad zagrożeniami asymetrycznymi[40]. Przez to pojęcie rozumie się zagrożenie, jakie stanowi strona konfliktu, która dysponuje zdecydowanie mniejszym od przeciwnika potencjałem, i z tego względu stosuje metody, środki oraz techniki rywali-

39 *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016*, Warszawa 2010, s. 12.
40 Zob. P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, Warszawa 2003.

zacji odmienne, nieprzystające do sposobów będących dla rywala zwyczajowym *modus operandi* (tzn. przez niego preferowanych, uznawanych za dopuszczalne i stosowanych rutynowo). Termin ten wiąże się przede wszystkim z aktywnością podmiotów pozapaństwowych i takimi wyzwaniami dla bezpieczeństwa państw jak terroryzm czy inne formy pozapaństwowej przemocy politycznej (rozmaite grupy zbrojne, ruchy partyzanckie itp.) albo przestępczość zorganizowana[41]. M. Madej zauważa, że *wiele z czynników, które decydowały o dotychczas większej wartości potencjałów, a co za tym idzie o przewadze ewentualnych „tradycyjnych" (prowadzonych wyłącznie lub głównie w świecie realnym) konfliktach z podmiotami pozapaństwowymi (pozbawionymi choćby odpowiedniej bazy terytorialnej i ludzkiej), wraz z przeniesieniem (częściowym lub całkowitym) rywalizacji do cyberprzestrzeni traci na znaczeniu lub też w ogóle przestaje być istotna*[42]. Rozpatrując cyberprzestrzeń jako obszar działań mamy zatem do czynienia z wyrównaniem sił podmiotów i zmniejszeniem istniejących między nimi dysproporcji. Cyberprzestrzeń jest środowiskiem o specyficznych cechach, które decydują o odmienności działań odbywających się w niej (tab. 2.5).

Tab. 2.5. Specyficzne cechy cyberprzestrzeni oraz wynikające z nich zagrożenia

Cecha	Charakterystyka	Przykłady
Anonimowość	Cyberprzestrzeń charakteryzuje się dużą możliwością zachowania anonimowości	Za pomocą usług i protokołów maskowania lub fałszowania adresu IP i innych danych umożliwiających namierzenie komputera, np. Tor, Onion
Brak ograniczeń geograficznych	Ataku cybernetycznego można dokonać z dowolnego miejsca	Działania wymierzone w podmiot lub np. w państwo mogą być zainicjowane z każdego miejsca ma świecie, brak granic politycznych
Mnogość obiektów ataku	Celem ataku może być każdy obiekt aktywny w cyberprzestrzeni	Wśród obiektów mogą być np. elementy infrastruktury krytycznej, komputery osób fizycznych, dane wrażliwe przedsiębiorstwa
Mnogość sposobów ataku	Ewolucja metod i technik ataków cybernetycznych	Obserwuje się wzrost incydentów bezpieczeństwa w cyberprzestrzeni o różnym poziomie złożoności i zaawansowania
Niejasna odpowiedzialność	Trudność w znalezieniu sprawcy oraz udowodnieniu winy	Z powodu niewykrycia sprawcy trudno ustalić, czy sprawcą incydentów były pojedyncze osoby, czy też struktury państwowe

41 Zob. M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007, s. 32–69.

42 M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa i systemu międzynarodowego* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 31.

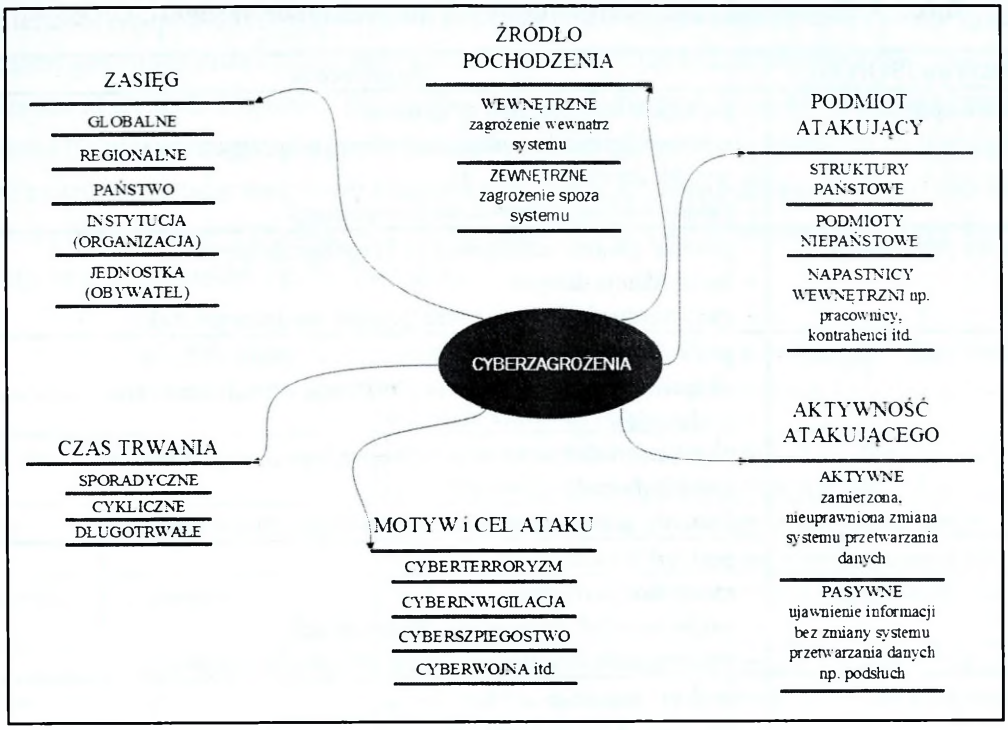
Cecha	Charakterystyka	Przykłady
Niejasne prawo	Brak przepisów prawnych, które precyzyjnie regulowałyby kwestie związane z bezpieczeństwem cyberprzestrzeni	Słabo określone przedsięwzięcia zaradcze oraz procedury postępowania w przypadku wystąpienia zagrożenia
Niskie koszty	Niskie i stale obniżające się koszty działań prowadzonych w cyberprzestrzeni	W celu przeprowadzenia ataku niezbędne jest nabycie sprzętu komputerowego, oprogramowania i dostępu do sieci
Trudności w zakwalifikowaniu czynu	Brak precyzyjnych i powszechnie przyjętych granic między poszczególnymi incydentami	Trudności w określeniu odpowiedzialności organów ścigania w przypadku braku precyzyjnego zakwalifikowania czynu, np. w Polsce Policja jest właściwym organem w przypadku ścigania sprawców przestępstw komputerowych, a ABW w przypadku ataku cyberterrorystycznego

Opracowanie własne.

Wymienione cechy utrudniają efektywną kontrolę nad przesyłaniem danych i komunikacją za pomocą Internetu. Wobec tego powstają nowe wyzwania i zagrożenia zarówno dla podmiotów stosunków międzynarodowych, jak i instytucji (organizacji) oraz społeczeństwa. Istota cyberzagrożeń sprowadza się do tego, że niewidzialny przeciwnik działający w przestrzeni wirtualnej jest trudny do zidentyfikowania. Co więcej, przewidywane skutki postępowania są trudne do oszacowania – nie wiemy, jakie umiejętności posiada strona oraz w jakim stopniu zamierza je wykorzystać. Zagrożenia mające wpływ na bezpieczeństwo infrastruktury krytycznej mogą być przeprowadzone w formie bezpośredniego fizycznego ataku na elementy infrastruktury teleinformatycznej, bądź też pośrednio przez oddziaływanie na inne elementy.

W poprzednim podrozdziale przedstawiono ogólną typologię zagrożeń dla bezpieczeństwa systemów oraz taksonomię zagrożeń dla bezpieczeństwa informacji. Podziały te obejmowały oprócz działań celowych także zagrożenia przypadkowe i spowodowane działaniami natury. Jeśli odniesie się te kwestie do cyberprzestrzeni państwa, można skonstruować ogólną klasyfikację cyberzagrożeń, przyjmując za kryteria źródło pochodzenia, czas trwania, zasięg, motyw i cel ataku, podmiot atakujący oraz jego aktywność (rys. 2.7).

Klasyfikacja przedstawiona na rys. 2.7 jest dość ogólna. W literaturze funkcjonują również klasyfikacje odnoszone do systemu informatycznego – podział ze względu na kryterium pochodzenia i losowości (tab. 2.6) oraz sieci komputerowej – analizowane w oparciu o model ISO/OSI, gdzie dla każdej z siedmiu warstw można wyróżnić zagrożenia wynikające z wykorzystywanych w nich protokołów (tab. 2.7).



Opracowanie własne.

Rys. 2.7. Ogólna klasyfikacja cyberzagrożeń

Tab. 2.6. Podział zagrożeń według kryterium pochodzenia i losowości

	Losowe	Celowe
Wewnętrzne	– niezamierzone błędy operatorów i użytkowników – wady sprzętu – wady oprogramowania	– działania własnych pracowników wynikające z chciwości, chęci rewanżu itp. – działania użytkowników wykraczające poza ich obowiązki, nadgorliwość itp. – szpiegostwo – wandalizm, chuligaństwo – terroryzm
Zewnętrzne	– zbyt wysoka temperatura lub wilgotność (pożar, zalanie) – zanieczyszczenie powietrza, kurz, pył – zakłócenia w zasilaniu – zakłócenia w procesach komunikacji – wyładowania atmosferyczne, klęski żywiołowe itp.	– działanie przestępców komputerowych podejmowane z chęci zysku – działania przedstawicieli prasy i innych mediów, szukających dostępu do informacji – szpiegostwo – wandalizm, chuligaństwo – terroryzm

Źródło: A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych*..., op. cit., s. 84.

Tab. 2.7. Zagrożenia sieci komputerowych na podstawie modelu ISO/OSI

Warstwa ISO/OSI	Zagrożenia
Warstwa aplikacji	– przejęcie kontroli nad systemem – wprowadzenie do systemu złośliwego oprogramowania – wyciek danych – zakłócenie lub przerwanie komunikacji
Warstwa prezentacji	– przełamywanie zabezpieczeń kryptograficznych – modyfikacja danych – ukrywanie złośliwego kodu/przeprowadzanego ataku
Warstwa sesji	– podszywanie się – ukrywanie funkcjonowania złośliwego oprogramowania – podsłuch – uzyskanie informacji o zainstalowanym oprogramowaniu – wyciek danych – łamanie zabezpieczeń uwierzytelniających komunikację
Warstwa transportowa	– podsłuch – modyfikacja danych – zakłócenie lub przerwanie komunikacji – wyczerpanie zasobów systemu informatycznego
Warstwa sieci	– podszywanie się – ukrywanie tożsamości – modyfikacja danych – zakłócenie lub przerwanie komunikacji – wyczerpanie zasobów systemu informatycznego
Warstwa łącza danych	– podszywanie się – podsłuch – nieuprawnione uwierzytelnienie w sieci lokalnej – uzyskanie nieuprawnionego dostępu do sieci lokalnej – zakłócanie sieci lokalnej
Warstwa fizyczna	– zakłócenie lub przerwanie komunikacji – podsłuch – modyfikacja danych

Opracowanie własne.

Identyfikacja zagrożeń ma szczególnie istotne znaczenie z uwagi na to, że jej wynik wpływa na późniejszy dobór zabezpieczeń. Należy ją realizować w oparciu wzorcowy katalog zagrożeń odpowiedni dla danego systemu. Jak dotąd nie ma przyjętej jednolitej klasyfikacji cyberzagrożeń. Symptomem zmian w tym obszarze jest opracowanie projektu *A Common Language for Computers Security Incidents*[43] autorstwa Johna D. Howarda i Thomasa A. Longstaffa. Środowiska informatyczne pozytywnie oceniły metodykę zaproponowaną w projekcie. Od 2001 roku *Common Language* jest podstawą sporządzania raportów przez CERT.

43 J.D. Howard, T.A. Longstaff, *A Common Language for Computers Security Incidents*, dostęp na stronie: http://www.osti.gov/scitech/servlets/purl/751004.

Zamierzeniem projektu jest wprowadzenie jednolitej taksonomii stosowanej na potrzeby gromadzenia i porównywania informacji na temat incydentów oraz prowadzenie statystyk. Ponadto tego typu uporządkowanie umożliwia diagnozę środowiska bezpieczeństwa badanego obiektu oraz obserwację trendów dotyczących cyberzagrożeń. Podstawą owej klasyfikacji jest atak komputerowy i jego elementy – identyfikacja atakujących, narzędzia ataku, słabość systemowa, akcja (rodzaj ataku), obiekt, rezultat i cele (tab. 2.8).

Tab. 2.8. Klasyfikacja zagrożeń według „Common Language"

Definicje atakujących		
Hackers	Hakerzy	Dokonują naruszenia bezpieczeństwa dla samego faktu i potwierdzenia swoich umiejętności technicznych
Spies	Szpiedzy	Atakujący w celu osiągnięcia informacji, którą można wykorzystać w sprawach politycznych
Terrorists	Terroryści	Próbują wywołać zagrożenie w celu osiągnięcia korzyści politycznych
Corporate raiders	Napastnicy korporacyjni	Atakujący, często pracownicy, prowadzący swą nielegalną działalność w stosunku do konkurencji w celu osiągnięcia korzyści finansowych
Professional criminals	Profesjonalni przestępcy	Atakujący komputery w celu uzyskania osobistych korzyści finansowych
Vandals	Wandale	Atakujący w celu dokonania zniszczenia
Voyeurs	Wędrownicy? Podróżnicy?	Atakujący dla samego doznania odczucia strachu związanego z faktem uzyskiwania istotnych informacji
Narzędzia		
a. Physical attack b. Information exchange c. User command d. Script or program e. Autonomous agent f. Toolkit g. Distributed tool h. Data tap		a. Atak fizyczny b. Dostęp do informacji c. Komendy systemowe d. Skrypt lub program e. Obiekt autonomiczny f. Zestaw oprogramowania służący do ataku g. Narzędzie ataku rozproszonego h. Przechwycenie danych
Słabość systemowa		
a. Design b. Implementation c. Configuration		a. Konstrukcja b. Implementacja c. Konfiguracja
Akcja		
Probe	Próbkowanie	Próba dostępu do obiektu przez zbadanie jego charakterystyki
Scan	Skanowanie	Próba dostępu do wielu obiektów naraz przez ustalenie obiektu z oczekiwaną charakterystyką
Flood	Przepełnienie	Dostęp do obiektu przez nagłe przepełnienie jego możliwości przetwarzania

Authenticate	Uwierzytelnienie	Przedstawienie się jako osoba uprawniona oraz w razie konieczności przekazanie informacji potrzebnej do poprawnego uwierzytelnienia
Bypass	Ominięcie	Ominięcie procesu zabezpieczającego przez zastosowanie alternatywnej drogi osiągnięcia obiektu
Spoof	Podszywanie	Przedstawianie się, w trakcie połączenia sieciowego, jako użytkownik posiadający prawo dostępu do zasobów
Read	Czytanie	Dostęp przez osobę nieuprawnioną do informacji z prawami czytania
Copy	Kopiowanie	Dostęp przez osobę nieuprawnioną do informacji z możliwością kopiowania
Steal	Kradzież	Przejęcie zasobów przez osobę nieuprawnioną bez pozostawienia kopii w uprawnionej lokalizacji
Modify	Modyfikacja	Zmian zawartości lub charakterystyki obiektu ataku
Delete	Usunięcie	Usunięcie (zniszczenie) obiektu ataku
Obiekt		
a. Account b. Process c. Data d. Component e. Computer f. Network g. Internetwork		a. Konto b. Proces c. Dane d. Komponenty e. Komputer f. Sieć g. Intersieć, sieć sieci
Rezultat		
a. Increased access b. Disclosure of information c. Corruption of information d. Denial of service e. Theft of resources		a. Nieautoryzowane rozszerzenie dostępu b. Ujawnienie informacji c. Fałszowanie informacji d. Odmowa dostępu e. Kradzież zasobów
Cele		
a. Challenge, status, thrill b. Political gain c. Financial gain d. Damage		a. Wyzwanie, status, emocje b. Zysk polityczny c. Zysk finansowy d. Szkoda

Opracowanie własne na podstawie: J.D. Howard, T.A. Longstaff, *A Common Language for Computers Security Incidents*, dostęp na stronie: http://www.osti.gov/scitech/servlets/purl/751004, s. 10–16.

Przywołane klasyfikacje miały na celu ukazanie złożoności charakteru cyberzagrożeń. Właściwa ich identyfikacja umożliwia skuteczne przeciwdziałanie oraz funkcjonowanie instytucji (organizacji) w przypadku sytuacji kryzysowej. Zarządzanie bezpieczeństwem systemu powinno uwzględniać identyfikację zagrożeń oraz analizę ryzyka ich wystąpienia w kontekście podatności systemu. Z uwagi na kontekst badań dotyczący cyberprzestrzeni państwa, analiza zarządzania bezpieczeństwem struktur administracyjnych zostanie ograniczona do cyberzagrożeń. Należy podkreślić, że metody i techniki stosowane przez aktorów cyberprzestrzeni podlegają ciągłej ewolucji. Jednocześnie wyszczególnione incydenty należą

często do wielu grup jednocześnie, np. atak cybernetyczny na system teleinformatyczny jest zagrożeniem spowodowanym działalnością człowieka, aktywnym, zewnętrznym, celowym i programowym. Elementy infrastruktury krytycznej oraz powiązania między nimi są szczególnie wrażliwe na nielegalną działalność w cyberprzestrzeni. Typologie przedstawione w podrozdziale nie tworzą katalogu zamkniętego. Narzędzia ataków stają się coraz bardziej powszechne. Cyberzagrożenia dla struktur administracyjnych mogą wystąpić w różnej skali nasilenia. W monografii przyjęto, że zagrożenia będą analizowane w oparciu o kryterium podmiotu atakującego, skutków, celów i motywów ataku, co pozwala wyodrębnić następujące zagrożenia: haking, haktywizm, aktywizm, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, walka informacyjna. Większość metod właściwych dla incydentów jest wspólna dla wyżej wymienionych zagrożeń, dlatego ich opis zostanie poprzedzony charakterystyką metod ataku w cyberprzestrzeni.

2.4. Metody i aktorzy ataków w cyberprzestrzeni

Właściwa analiza zagrożeń i metod ataków umożliwia skuteczne zarządzanie bezpieczeństwem struktury administracyjnej, od niej bowiem zależy wybór odpowiednich zabezpieczeń, ukierunkowanie procedury kadrowej oraz wdrażanie polityki bezpieczeństwa.

We wstępie przyjęto tezę o istotnej roli czynnika ludzkiego w przeciwdziałaniu zagrożeniom cyberprzestrzeni państwa. Nawet najdoskonalsze zabezpieczenia nie zapewnią bezpieczeństwa struktury administracyjnej, jeżeli personel nie będzie odpowiednio przeszkolony w obszarze bezpieczeństwa informacji oraz potencjalnych metod ataku. Dowodem na to są skuteczne i coraz powszechniejsze działania socjotechniczne.

Socjotechnika wiąże się z wywieraniem wpływu na ludzi i na ich postawy oraz uzyskiwaniem pożądanych reakcji. W odniesieniu do nowoczesnych technologii polega ona na wykorzystaniu narzędzi psychologicznych do zdobywania poufnych informacji, dokonywania włamań do komputerów, serwerów sieci i systemów informatycznych. Do określenia tego typu czynności stosuje się także pojęcie socjoinformatyka. Jednym z najsłynniejszych socjotechników świata jest Kevin Mitnick[44], który zdecydowaną większość ataków przeprowadził, korzystając z naiwności ludzi oraz metod socjotechniki. Mawiał on: „Łamałem ludzi, nie

44 Kevin Mitnick przy wykorzystaniu socjotechniki zdobył informacje od wielu znanych firm i agencji rządowych, takich m.in. jak FBI, Pentagon, Novell, Pacific Bell, SCO.

hasła". Dokonał wielu włamań do systemów komputerowych oraz wyprowadził setki poufnych informacji[45].

Niewiedza i łatwowierność stanowi istotny problem w omawianym obszarze. A. Suchorzewska zauważa, że *błędy użytkowników uważa się za najbardziej niebezpieczne i powodujące największe straty. Najpoważniejsze i najgłośniejsze włamania do systemów informatycznych zostały wykonane właśnie z ich wykorzystaniem*[46]. W raportach rocznych zespołu CERT[47] można zaobserwować wzrost ataków socjotechnicznych przeciwko jednostkom administracji publicznej.

Ataki socjotechniczne mogą odbywać się z wykorzystaniem technologii komputerowych lub bez nich. Przestępcy charakteryzują się umiejętnościami interpersonalnymi, łatwo wzbudzają zaufanie oraz doskonale znają metody manipulacji. Ataki tego typu są możliwe przy aktywnym udziale użytkowników, dlatego też istotną kwestię stanowi podnoszenie świadomości personelu w zakresie bezpieczeństwa systemów teleinformatycznych. Skuteczność ataków socjotechnicznych polega bowiem na słabości czynnika ludzkiego. Przy tym warto zaznaczyć, że zdarzają się błędy, które dokonywane są celowo.

Poza socjotechniką istnieje wiele technik cyberataków, których istota przejawia się w *celowym zakłóceniu prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników. Umożliwia[ją] ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu*[48]. Przestępcy dysponują szerokim wachlarzem technik oraz gotowych rozwiązań, które mogą w wysokim stopniu naruszać bezpieczeństwo cyberprzestrzeni oraz stanowić realne zagrożenie dla struktur administracyjnych. Złożoność negatywnych zjawisk powoduje, że stały się one wyzwaniem dla bezpieczeństwa narodowego.

45 Szerzej: T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013, s. 36-37.

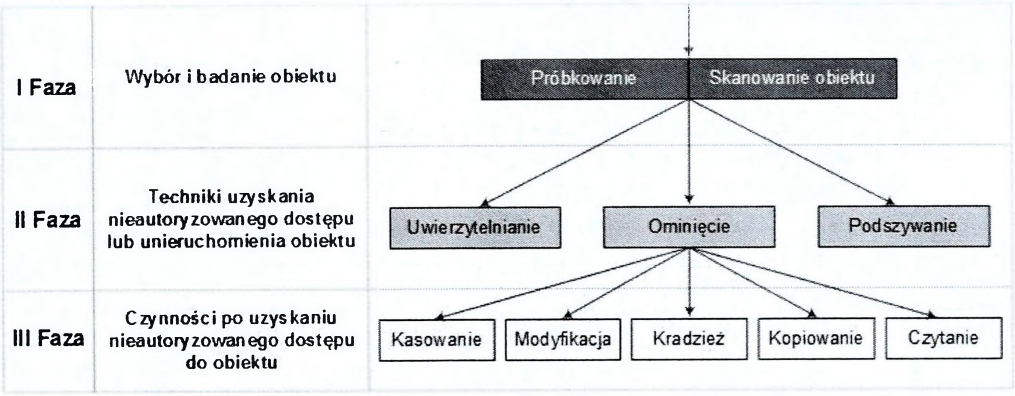
46 A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 83.

47 *Zgodnie z przyjętą Polityką Ochrony Cyberprzestrzeni RP, w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym. Podstawowym jego zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami. Realizuje on jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP. Stanowi poziom II-gi Krajowego Systemu Reagowania na Incydenty Komputerowe w CRP.* Źródło: http://www.cert.gov.pl/cer/o-nas/15,O-nas.html.

48 *Rządowy Program Ochrony Cyberprzestrzeni RP...*, op. cit., s. 5.

W typowym procesie cyberataku można wyróżnić trzy podstawowe fazy (rys. 2.8)[49]:

- pierwsza faza obejmuje próbkowanie (skanowanie), będące formą rozpoznania słabych stron obiektu (systemu);
- druga wiąże się z uzyskaniem dostępu do zasobów systemu;
- trzecia stanowi realizację właściwego celu działania (np. kradzież, kopiowanie, modyfikacja).



Źródło: P. Sienkiewicz, H. Świeboda, E. Lichocki, *Analiza systemowa zjawiska cyberterroryzmu*, „Zeszyty Naukowe AON" nr 2(63), Warszawa 2006, s. 16.

Rys. 2.8. Model cyberataku na obiekty teleinformatyczne

Na bezpieczeństwo obiektów teleinformatycznych oprócz zabezpieczeń i czynnika ludzkiego mają wpływ także zastosowane narzędzia oraz podmiot atakujący. Kombinacja tych dwóch czynników pozwala szacować prawdopodobieństwo wystąpienia cyberataku oraz prognozować konsekwencje jego wystąpienia. Wyróżnia się wiele metod ataków w cyberprzestrzeni – wybrane przedstawiono w tab. 2.9.

Tab. 2.9. Wybrane metody ataków w cyberprzestrzeni

Nazwa metody	Charakterystyka
Backdoor	Wejście do systemu z pominięciem warstwy ochronnej – programiści piszą kod, który umożliwia wykorzystanie oprogramowania np. do włamań
Bakteria	Złośliwe oprogramowanie mające na celu rozmnażanie programu, który wykładniczo zajmuje zasoby komputera, co uniemożliwia korzystanie z urządzenia
Bomba logiczna	Aktywacja funkcji elementu logicznego komputera, która prowadzi do zniszczenia lub zdeformowania sprzętu

49 E. Lichocki, *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy* [w:] *Ewolucja terroryzmu na przełomie XX i XXI wieku*, red. M. Malinowski, R. Ożarowski, W. Grabowski, Gdańsk 2009, s. 168.

Nazwa metody	Charakterystyka
Chipping	Technika polegająca na uzyskaniu dostępu do komputera przez zainstalowanie chipów
Botnet	Grupa komputerów zainfekowanych złośliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu; przejęte komputery są określane mianem zombie i mogą służyć np. do przeprowadzania zmasowanych ataków na sieci teleinformatyczne
Dialer	Oprogramowanie, które celowo łączy się przez wysokopłatne numery dostępowe zamiast przez te wybrane przez użytkownika
DoS/DDos	Ataki mające na celu zablokowanie urządzenia, usługi, serwisu sieciowego lub zawieszenie komputera przez przesyłanie dużej ilości danych z różnych źródeł
Exploit	Program wykorzystuje błędy w oprogramowaniu w celu bezpośredniego włamania się do komputera
Fastflux	Technika udostępniania nielegalnych bądź związanych z nielegalną działalnością treści przez utrzymywanie i udostępnianie wielu kopii serwisu na urządzeniach posiadających publiczne adresy IP
Hijacking	Polega na przechwyceniu transmisji odbywającej się miedzy dwoma systemami, dzięki czemu możliwe jest uzyskanie dostępu do szczególnie chronionych programów lub informacji
Keylogger	Rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika komputera
Koń trojański	Program wykonujący działania niezależnie od woli użytkownika, np. usuwanie plików, przesyłanie danych do twórcy oprogramowania
Phishing	wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne – jest to rodzaj ataku opartego na socjotechnice
Receptory van Ecka	Polega na podglądaniu i przechwytywaniu repliki obrazów wyświetlanych na monitorze komputera z wykorzystaniem specjalistycznego sprzętu
Robak	Program rozprzestrzeniający się w sieci – po zagnieżdżeniu w systemie może zachowywać się jak koń trojański, wirus albo bakteria
Rootkit	Wykorzystuje technikę maskowania procesów systemowych lub programów (wykorzystywanych przez atakującego do administracji systemem) w systemie teleinformatycznym
Sniffing	Polega na śledzeniu ruchu w sieci – programy zwane snifferami przechwytują informacje i zapisują na dysk
Spoofing	Polega na podszywaniu się pod inny element systemu; efekt ten osiągany jest przez umieszczanie w sieci preparowanych pakietów danych lub niepoprawne używanie protokołów
Spyware	Oprogramowanie stosowane w szpiegostwie cybernetycznym – programy gromadzą informacje o użytkowniku i przesyłają do twórcy programu
Wirus	Samoreplikujący się kod, który uszkadza dane lub programy, zmieniając sposób działania sprzętu

Opracowanie własne na podstawie: A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 144–158; R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2001, s. 80–88.

Przedstawione techniki pokazują złożoność i różnorodność rozwiązań, jakie może stosować podmiot atakujący. Lista nie tworzy katalogu zamkniętego oraz nie wyczerpuje wszystkich możliwych metod. Powstają coraz doskonalsze i złożone narzędzia, np. Zeus, Stuxnet, Duqu, Flame, umożliwiające dokonywanie zaawansowanych ataków.

Przeprowadzona analiza dowodzi, że przestępcy dysponują szeroką paletą możliwości ataków w cyberprzestrzeni. Ogólna ich kategoryzacja pozwala na wyodrębnienie trzech głównych grup:

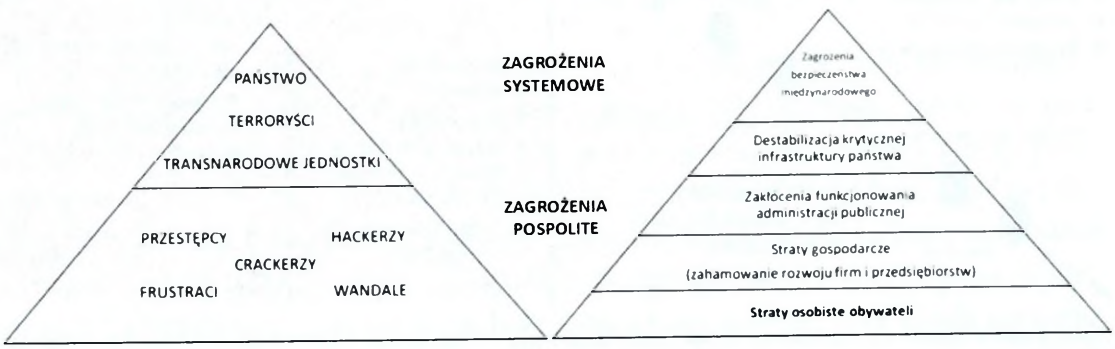
- atak na system;
- atak na informacje;
- wpieranie klasycznych form działalności przestępczej, np. jako źródło dochodów, narzędzie propagandowe.

Każda z powyższych grup stanowi istotne zagrożenie zarówno dla bezpieczeństwa osobistego obywateli, jak i struktury administracyjnej oraz bezpieczeństwa narodowego. Wszystkie wymienionych naruszenia są przestępstwami w myśl przepisów polskiego kodeksu karnego oraz prawa międzynarodowego.

Nie istnieje jedna akceptowalna taksonomia i klasyfikacja aktorów ataków w cyberprzestrzeni. P. Sienkiewicz i H. Świeboda zaproponowali interesującą klasyfikację, w której sprawcom przestępstw przyporządkowali skutki tych ataków.

Zgodnie z zaproponowanym podziałem sprawców zagrożeń można podzielić na dwie główne grupy[50]:

- sprawcy zagrożeń systemowych, do których należy zaliczyć organizacje państwowe, organizacje pospolite oraz grupy przestępcze;
- sprawcy zagrożeń tradycyjnych, np. wandale, hakerzy, przestępcy (rys. 2.9).



Źródło: P. Sienkiewicz, H. Świeboda, *Analiza systemowa zjawiska cyberterroryzmu*, „Zeszyty Naukowe AON" nr 2(63) 2006, s. 10.

Rys. 2.9. Hierarchia zagrożeń informacyjnych i ich skutków

50 H. Świeboda, *Zagrożenia informacyjne bezpieczeństwa RP...*, op. cit., s. 55.

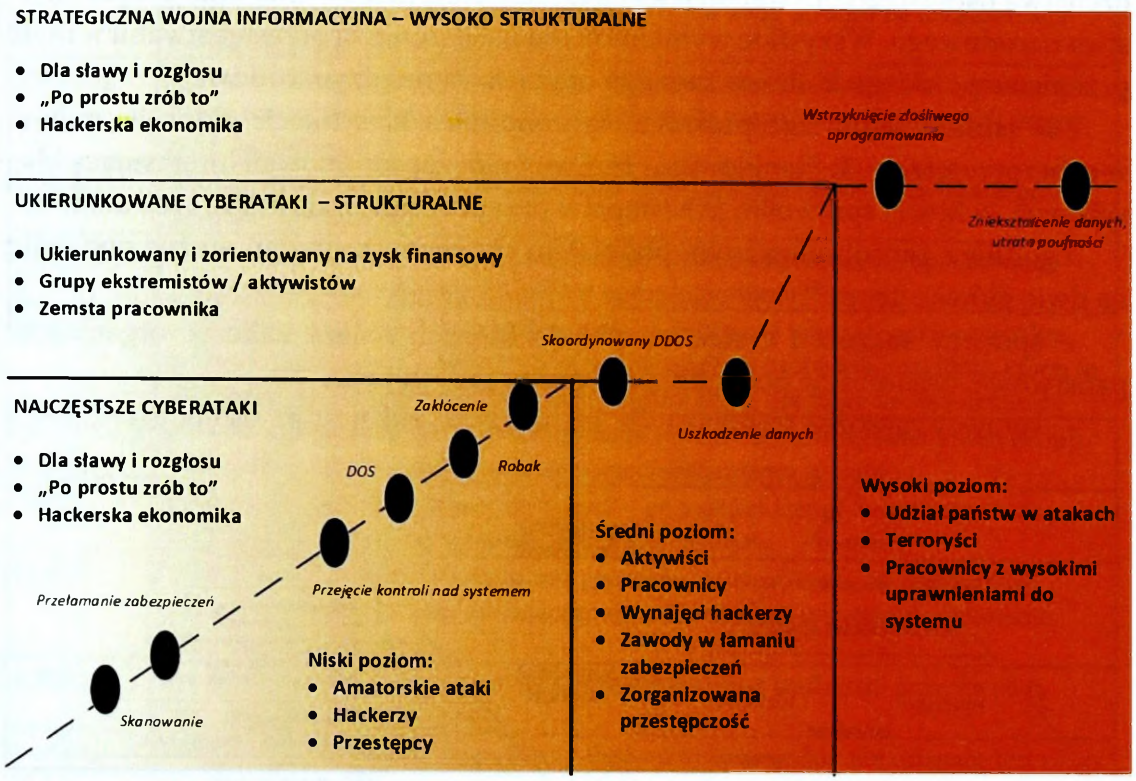
Inna klasyfikacja została przedstawiona w raporcie Cyber Attack Task Force[51] z 2012 roku opracowanym przez Północnoamerykańską Korporację ds. Niezawodności Energetycznej. Wypracowano podział na grupy aktorów zagrożeń:

- niskiego stopnia;
- średniego stopnia;
- wysokiego stopnia.

W celu określenia skutków dla systemów informatycznych zagrożenia również podzielono na trzy grupy:

- najczęstsze typy zagrożeń (niestrukturalne);
- ukierunkowane zagrożenia (strukturalne);
- zagrożenia terrorystyczne i międzypaństwowe (wysoko strukturalne).

Na rys. 2.10 przedstawiono kombinację aktorów zagrożeń i typów zagrożeń w zależności od konsekwencji oraz prawdopodobieństwa ich wystąpienia.



Opracowanie własne na podstawie: *Cyber Attack Task Force – Final Report*, North American Electric Reliability Corporation, Atlanta 2012, s. 5.

Rys. 2.10. Konsekwencje i prawdopodobieństwo wystąpienia ataków w cyberprzestrzeni w zależności od technik i aktorów zagrożeń

51 *Cyber Attack Task Force – Final Report*, North American Electric Reliability Corporation, Atlanta 2012.

Z tych wymienionych na rys. 2.10 najbardziej powszechne ataki to skanowanie, przełamanie zabezpieczeń, przejęcie kontroli nad systemem, DoS, robaki oraz zakłócenia. Aktorami są hakerzy, amatorzy oraz przestępcy niezorganizowani. Incydenty zaliczone do tej grupy stanowią zagrożenia niskiego stopnia. Kolejna grupa zagrożeń – skoordynowany DDoS i uszkodzenie danych – jest bardziej niebezpieczna pod względem potencjalnych konsekwencji. Może prowadzić np. do blokowania e-usług i niszczenia danych. Do podmiotów średniego poziomu zalicza się aktywistów, pracowników, wynajętych hakerów, przestępczość zorganizowaną. Wśród motywów wymienia się ukierunkowanie na zysk finansowy, zemstę pracownika oraz kierowanie się przesłankami ideologicznymi (np. aktywiści). Do ostatniej grupy zaliczono działania związane z zagrożeniami asymetrycznymi. Wśród stosowanych technik wymienia się wstrzyknięcie złośliwego oprogramowania, np. Flame, Stuxnet. Tego typu działania niosą poważne konsekwencje, związane chociażby ze zniekształceniem danych czy utratą poufności. Wśród sprawców wymienia się pracowników z wysokimi uprawnieniami w systemie oraz terrorystów, a także bierze się pod uwagę udział państw w atakach. Należy podkreślić, że umiejętności i wiedza są wprost proporcjonalne do złożoności ataków.

2.5. Charakterystyka cyberzagrożeń dla bezpieczeństwa struktur administracyjnych

2.5.1. Haking, aktywizm, haktywizm i cyberwojownicy

Haking jest najstarszą formą wykorzystywania luk w zabezpieczeniach systemów i sieci komputerowych[52]. Hakerzy stanowią grupę zróżnicowaną, zarówno pod względem motywacji (powodu ataku), jak i poziomu zorganizowania. Haker pierwotnie oznaczał osobę, *która dzięki dogłębnej wiedzy informatycznej i indywidualnym zdolnościom potrafiła przełamać zabezpieczenia elektroniczne systemów komputerowych i zdobywać nieuprawniony dostęp do danych w nich przechowywanych*[53]. Początkowo uważano, że haker dokonuje włamań bez złych intencji,

52 Termin *haker* pojawił się w latach osiemdziesiątych XX wieku w USA z rozpowszechnieniem urządzeń elektronicznych wśród użytkowników domowych i powstaniem pierwszych sieci komputerowych.

53 M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 98.

a przez pokonanie zabezpieczeń sprawdza jedynie swoje umiejętności oraz nabywa doświadczenia jako specjalista do spraw sieci komputerowych.

Wraz z upowszechnieniem Internetu, zwiększonym stopniem dostępności komputerów osobistych oraz rozwojem technologii ICT zjawisko hakingu zaczęło ewoluować. W latach osiemdziesiątych doszło do wykształcenia się tradycyjnej formy hakingu[54]. Przykładowo w 1987 roku grupa niemieckich hakerów dokonała włamania do serwerów NASA, komputerów w bazie wojskowej w Ramstein oraz do wielu instytucji badawczych (m.in. CERN, University of British Columbia). Pojawiły się także pierwsze przypadki hakerów opłacanych przez służby państwowe i działających z pobudek politycznych. Symboliczna była tu sprawa M. Hessa, specjalisty wynajętego przez radzieckie KGB[55]. Wówczas problem hakingu został dostrzeżony przez rządy państw, które zaczęły dostosowywać swój system prawny do zagrożeń związanych z omawianym zjawiskiem.

Na przełomie XX i XXI wieku haking był kategorią rozumianą bardzo szeroko. W tym kontekście wyodrębniły się trzy grupy hakerów: białych, czarnych oraz szarych „kapeluszy"[56]. Pierwsza grupa obejmuje osoby działające legalnie, w granicach prawa lub starające się nie popełniać szkód. Luki w zabezpieczeniach wykorzystują do sprawdzenia swoich umiejętności. W tej grupie można spotkać audytorów bezpieczeństwa, którzy działają na rzecz doskonalenia jakości pokonanych zabezpieczeń. Kolejna grupa to hakerzy, którzy działają poza granicami prawa. Znalezione luki wykorzystują w nielegalny sposób lub publikują w postaci gotowych programów, które mogą być używane także przez osoby o niskich umiejętnościach. Ostatnia grupa, tzw. szare kapelusze, przejmuje po części metody dwóch opisanych wcześniej grup. Ich działalność wykracza poza granice prawa, jednak nie zmierza do dokonania szkód, tylko podnoszenia jakości zabezpieczeń.

Haking jest zjawiskiem obejmującym łamanie zabezpieczeń komputerowych oraz uzyskanie nieuprawnionego dostępu do danych w formie elektronicznej. Główną motywacją jest sprawdzenie własnych umiejętności. Haker działa więc z pobudek pozapolitycznych, nie dokonując z reguły nieodwracalnych zniszczeń w zaatakowanych systemach i sieciach komputerowych[57]. Haking stanowi zatem zagrożenie niskiego poziomu z perspektywy bezpieczeństwa narodowego i międzynarodowego.

Haktywizm ukształtował się na przełomie lat osiemdziesiątych i dziewięćdziesiątych, kiedy cyberprzestrzeń wykorzystano do protestów przeciwko fran-

54 Z. Clarke, J. Clawson, M. Cordell, *A brief history of hacking*, November 2003, dostęp: http://steel.lcc.gatech.edu/~mcordell/lcc6316/Hacker%20Group%20Project%20FINAL.pdf.

55 M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek dla typologii*, „E-Politikon" nr 6/2013, s. 112.

56 Ibidem, s. 112.

57 M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw...*, op. cit., s. 113.

cuskiej polityce nuklearnej i próbnym wybuchom jądrowym[58]. W Polsce symbolem haktywizmu stały się protesty związane z umową ACTA. Dokonano wówczas serii ataków na polskie witryny rządowe. Wydarzenia związane z arabską wiosną potwierdziły możliwości haktywizmu na arenie międzynarodowej. Należy zauważyć, że w początkowym stadium działania haktywistów mogą doprowadzić do zakłócenia funkcjonowania Internetu, ale z reguły nie powodują poważnych strat.

W literaturze można odnaleźć szereg definicji haktywizmu. Rozróżnienia hakingu i haktywizmu można dokonać na podstawie motywu ataku. D. Denning uważa haktywizm za połączenie hakingu i aktywizmu, gdzie pod pojęciem aktywizmu rozumie gromadzenie i rozpowszechnianie informacji, koordynację działań, tworzenie stron, publikację materiałów czy też prowadzenie dyskusji. Natomiast cele haktywizmu są polityczne lub społeczne i obejmują elektroniczne nieposłuszeństwo obywatelskie[59]. Natomiast zdaniem M. Terlikowskiego współczesna forma haktywizmu ewoluuje. W ostatnich latach silniejsze są powiązania haktywistów z kryzysami i konfliktami politycznymi oraz coraz dotkliwsze stają się skutki ataków. Kwestie budzące emocje opinii publicznej i bieżące wydarzenia polityczne mogą stać się impulsem do przeprowadzania ataków, których celem będą strony internetowe konkurencyjnych partii politycznych mediów, władz i organów administracji publicznej zarówno państwa macierzystego, jak i obcych krajów[60]. Takie działania kwalifikują się wciąż jako haktywizm, jednak ataki stają się formą walki politycznej. W tym kontekście haktywizm nabiera szczególnej wagi w połączeniu z międzynarodowymi konfliktami i kryzysami politycznymi. Wówczas celami ataków są systemy teleinformatyczne instytucji reprezentujących zaangażowane w konflikt państwa lub organizacje międzynarodowe.

Z przeprowadzonej analizy wynika, że haktywizm nie jest jednorodną formą szkodliwej działalności w cyberprzestrzeni. Zwrócił na to uwagę F. Paget, który wyróżnił trzy główne grupy haktywistów[61]:

- Pierwsza grupa – obejmuje włamania na witryny internetowe, zdobywanie poufnych informacji oraz blokowanie określonych usług sieciowych. Zbierane dane mają wielokrotnie istotną wartość w kontekście bieżącej debaty publicznej. Do tej grupy zalicza się Anonymous.

58 A. Bógdał-Brzezińska, *Cyberterroryzm i problemy bezpieczeństwa...*, op. cit., s. 60.

59 D.D. Denning, *Activism, hacktivism and cyberterrorism: the internet as a tool for influencing foreign policy*, s. 241, dostęp: http://www.rand.org/content/dam/rand/pubs/monographreports/MR1382/MR1382.ch8.pdf.

60 M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa...*, op. cit., s. 105.

61 F. Paget, *Hacktivism. Cyberspace has become the new medium for political voices*, McAfee Labs White Paper, s. 4, cyt. za: M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego...*, op. cit., s. 116.

• Druga grupa – obejmuje działania w celach propagandowych lub informacyjnych. Jest to zjawisko spotykane coraz częściej, a należące tu jednostki lub grupy promują poglądy nie tylko za pomocą włamań, ale także np. na formach dyskusyjnych czy w mediach społecznościowych.

• Trzecia grupa – obejmuje tzw. cyberwojowników wchodzących w skład tzw. cyberarmii.

Cyberwojownicy stanowiący trzecią grupę w klasyfikacji Pageta określani są w literaturze także mianem aktywistów patriotycznych. O ile osoby (grupy) należące do pierwszej z wyszczególnionych kategorii działają również z pobudek politycznych, to ich działalność ma wymiar narodowy. Cyberwojownicy natomiast funkcjonują na szczeblu międzynarodowym, wielokrotnie również w trakcie konfliktów zbrojnych.

Jednym ze znanych przypadków tego typu kampanii elektronicznych motywowanych międzynarodową sytuacją polityczną była fala ataków w 2007 roku na Estonię. W tym okresie stosunki Rosji i Estonii zaostrzyły się na skutek decyzji władz estońskich o przeniesieniu pomnika ku czci żołnierzy Armii Czerwonej poległych w drugiej wojnie światowej oraz ich mogił na peryferyjny cmentarz wojskowy[62]. Sieć Internet w Estonii została kilkakrotnie sparaliżowana atakami DDoS. W wyniku ataków przestały działać m.in. witryny bankowe oraz strony administracji publicznej. Cały proceder przyniósł ogromne straty finansowe w skali kraju.

Odnosząc powyższe kwestie do bezpieczeństwa struktur administracyjnych oraz bezpieczeństwa narodowego i międzynarodowego, można wskazać na dwie odrębne kategorie zagrożeń związanych z działaniem haktywistów. W przypadku jednostkowych ataków o ograniczonej skali i skutkach mamy do czynienia ze szkodami dla wizerunku państwa, które mogą osłabić pozycję rządu w jakimś konflikcie międzynarodowym lub prowadzić do dezinformacji. Jednakże możliwość powstania znacznych zakłóceń pracy zaatakowanego systemu, jego całkowitego wyłączenia bądź rozszerzenia się skutków pierwotnego ataku na inne systemy teleinformatyczne jest minimalna. Natomiast w przypadku ataku paraliżującego funkcjonowanie całego segmentu sieci Internet jest to już poważne zagrożenie[63]. W tym przypadku należy mieć na uwadze, że Internet jest wykorzystywany nie tylko przez indywidualne osoby, ale także przez przedsiębiorców, administrację publiczną, struktury bezpieczeństwa oraz sieci specjalistyczne, np. sektor finansowy czy sieci przemysłowe. Działania takie mogą utrudnić pracę różnych podmiotów. Ponadto paraliż pewnych sektorów może destabilizować funkcjonowanie innych sektorów, które są często ze sobą połączone. Taka działalność powoduje

62 M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa...*, op. cit., s. 107.
63 Ibidem, s. 110.

bardzo poważne straty i ograniczenia życia społecznego. W skrajnym przypadku może prowadzić do szkód fizycznych, np. zniszczenia urządzeń.

Podmioty pozapaństwowe nie muszą przeprowadzać ataków samodzielnie. W Internecie są rozpowszechniane narzędzia służące do ataków, jednak ich użycie jest raczej mało szkodliwe i dosyć łatwe do zneutralizowania. Poważny problem stanowią natomiast zlecone ataki cybernetyczne. Osoby działające w podziemiu internetowym posiadają bardzo specjalistyczne umiejętności. Dowodem tego jest narzędzie Duqu. Po szczegółowym przeanalizowaniu jednej z bibliotek tego trojana eksperci z Kaspersky Lab odkryli, że pewna jej sekcja, odpowiedzialna za komunikację z cyberprzestępcami, została napisana w nieznanym języku programowania.

Należy mieć na uwadze, że opisane zjawiska ewoluują. Stosunkowo najmniej szkodliwe dla bezpieczeństwa narodowego są zagrożenia hakerskie. Natomiast działania haktywistów w ramach protestów politycznych mogą prowadzić do blokady witryn stron sektora publicznego. W skrajnych przypadkach haktywiści mogą atakować również elementy infrastruktury krytycznej państwa.

2.5.2. Cyberprzestępczość

W literaturze przedmiotu oraz w prawie międzynarodowym brakuje powszechnej zgody co do określania czynów zabronionych związanych z naruszeniem dóbr prawnie chronionych przez prawo karne dokonywanych przy wykorzystaniu nowoczesnych technologii. Zatem już przy próbie kwalifikacji czynu napotyka się trudności. Jednocześnie należy podkreślić, że cyberprzestępczość jest zjawiskiem narastającym oraz przynoszącym przestępcom duże dochody, a przedsiębiorstwom i krajom niebagatelne straty. Na szczeblu międzynarodowym opracowuje się wiele raportów, w których szacuje się straty związane z tego typu przestępstwami.

W celu opisu zjawiska, w literaturze amerykańskiej używa się takich określeń jak: cyberprzestępczość (*cyber crime*), przestępczość komputerowa (*computer crime*), przestępczość związana z komputerami (*computer-related crime*) oraz przestępczość przy użyciu nowoczesnych technologii (*high-tech crime*)[64]. Stosowane są także takie pojęcia jak: przestępstwa związane z technologią cyfrową, przestępstwa związane z technologią przetwarzania informacji lub przestępstwa internetowe[65] czy też nadużycia komputerowe. W niemieckiej literaturze używa się dodatkowo takich kategorii jak przestępczość związana z nowymi mediami (*Kriminalität im Zusammenhang mit neuen Medien*) oraz przestępczość

64 M. Sawicki, *Podział i definicje cyberprzestępstw*, „Prokuratura i prawo" nr 7–8, 2012, s. 241.

65 A. Adamski, *Prawo karne komputerowe,* Warszawa 2000, s. 33; cyt za: M. Sawicki, *Podział i definicje...*, op. cit., s. 241.

związana z wykorzystaniem technik informacyjnych i komunikacyjnych (*Straftaten unter Ausnutzung der Informations- und Kommunikationstechnik*)[66]. W polskim kodeksie karnym[67] nie zdefiniowano przestępczości komputerowej czy też cyberprzestępczości, jednak w literaturze nie trudno odnaleźć próby definiowania wyżej wymienionych pojęć.

Obszerne zestawienie definicji przestępstw komputerowych oraz ich klasyfikacji – potwierdzające brak jednolitego ujęcia przestępczości komputerowej – opracował w swojej pracy B. Fischer[68]. Trudności z wypracowaniem ogólnie przyjętej definicji cyberprzestępstw związane są z ciągłym rozwojem oraz rozpowszechnianiem tego typu działalności. Brak powszechnie akceptowanej definicji cyberprzestępczości na gruncie prawa wydaje się jednak uzasadniony, pojęcie to jest bowiem związane z prawem obowiązującym w danym kraju – jedynie normy prawne danego kraju mogą kwalifikować określony czyn jako przestępstwo.

W jednej z pierwszych definicji zaproponowanej w 1973 roku przez R. von zur Mühlena przestępczość komputerowa to *każde działanie, w którym komputer stanowi albo narzędzie, albo przedmiot zamachu*[69]. Zgodnie z przywołaną definicją przestępstwo komputerowe jest czynem zabronionym przeciwko systemowi komputerowemu (komputer jest celem), jak i czynem dokonanym przy użyciu komputera (komputer jest narzędziem).

Według innej definicji przedstawionej w 1974 roku przez D.B. Parkera *przestępczość komputerowa jest czynem powodującym straty, obrażenia lub szkody, który wymaga użycia systemów przetwarzania danych*[70]. W odróżnieniu do poprzedniej definicji, Parker traktuje przestępczość komputerową jako czyn, w którym systemy komputerowe są narzędziem przestępstwa, nie są jednak jego celem, a jednocześnie podkreśla szkody powstałe w wyniku przestępstwa.

Również w Polsce podejmuje się próby zdefiniowania omawianego zjawiska. K.J. Jakubski określa przestępczość komputerową jako: *zjawisko kryminologiczne obejmujące wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz w całym systemie połączeń komputero-*

66 M. Sawicki, *Podział i definicje...*, op. cit., s. 241.

67 Ustawa z dnia 6 czerwca 1997 roku Kodeks karny (Dz.U. 1997 nr 88, poz. 553).

68 Zob. B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, s. 23.

69 R. von zur Mühlen, *Computerkriminalität. Gefahren und Abwehr*, Berlin 1973, cyt. za: M. Sawicki, *Podział i definicje...*, op. cit., s. 242.

70 Parker D.B., *Computer related crime*, „Journal of Forensic Sciences" vol. 19 nr 2 (Apr. 1974), s. 294, cyt. za: T. Muliński, *Zagrożenia bezpieczeństwa dla systemów e-adminsitracji...*, op. cit., s. 82.

wych, a także sam sprzęt komputerowy oraz prawa do programu komputerowego[71]. Powyższą definicję rozszerza A. Adamski, który w ujęciu materialnoprawnym wyróżnia zamachy na systemy, dane i programy komputerowe (np. wprowadzenie wirusa) oraz posługiwanie się elektronicznymi systemami przetwarzania danych do naruszenia dóbr tradycyjnie chronionych np. fałszerstwo dokumentów, „pranie brudnych pieniędzy". Natomiast w ujęciu karnoprocesowym przestępstwo komputerowe stanowi zarówno przedmiot, jak i narzędzie zamachu[72].

Przy analizie pojęcia przestępczości komputerowej istotne wydaje się odróżnienie dwóch kategorii czynów. Po pierwsze, przy wykorzystaniu nowoczesnych technologii mogą być popełniane czyny tradycyjnie uznawane za przestępstwa, a komputery jedynie dostarczając nowych możliwości ich popełnienia. Po drugie, wraz z rozwojem technik komputerowych oraz ich coraz szerszym zastosowaniem związane jest pojawienie się nowego rodzaju zjawisk, które zostają penalizowane i ostatecznie dochodzi do wykształcenia się nowych kategorii przestępstw[73]. Na gruncie niemieckiej doktryny orzecznictwa rozróżniono przestępstwa *stricte* komputerowe, przestępstwa związane z wykorzystaniem środków komunikacji elektronicznej do rozpowszechniania informacji zakazanych przez prawo oraz pozostałe przestępstwa związanymi z instrumentalnym wykorzystaniem Internetu[74]. Przywołana kategoryzacja rozszerza definicje, które traktowały komputery jako cel lub narzędzie ataku. W stosunku do postępu technologicznego takie ujęcie wydaje się zbyt ogólne, albowiem komputery oraz ich elementy w dzisiejszym świecie są wszechobecne, a ataki są kierowane nie tylko na komputery, ale też np. na telefony komórkowe. Ponadto przestępstwa komputerowe mogą być także związane z naruszeniem dóbr tradycyjnie chronionych przez prawo karne. Dotyczy to w szczególności rozpowszechniania informacji zakazanych przez prawo, np. pornografii dziecięcej czy też treści faszystowskich.

Rozważania na temat przestępczości komputerowej skłaniają do przyjęcia poglądu na temat ewolucji stosowanej terminologii. Wraz z ciągłym powstawaniem nowych przejawów przestępstw komputerowych, w ośrodkach naukowych przedstawia się propozycje, aby termin *przestępczość komputerowa* zastąpić terminem *cyberprzestępczość*.

71 K. J. Jakubski, *Przestępczość komputerowa – próba zdefiniowania zjawiska* [w:] *Internet – problemy prawne*, red. R. Skubisz, Lublin 1999, s. 282.

72 A. Adamski, *Nowa kodyfikacja karna. Kodeks karny. Krótkie komentarze*, „Zeszyt 17. Przestępstwa komputerowe w nowym kodeksie karnym", Warszawa 1998, s. 15–24, cyt. za: A. Zalesisńka, P. Pęcherzewski, P. Rodziewicz, *Zagrożenia związane z rozwojem nowych technologii* [w:] *Technologia informacyjna dla prawników*, A. Burdziak, R. Cieślak et al., Wrocław 2011, s. 80.

73 Por. J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1989, s. 311.

74 M. Sawicki, *Cyberprzestępczość*, Warszawa 2013, s. 14.

Cyberprzestępczość ewoluuje i dostosowuje swoje narzędzia oraz techniki do postępu technologicznego. W literaturze wymienia się ukształtowane ewolucyjnie generacje cyberprzestępczości[75]:

- pierwsza generacja – obejmowała głównie naruszenie integralności systemów komputerowych i modyfikację znajdujących się tam danych na skutek wprowadzenia programów typu robak lub wirus;
- druga generacja – związana z rozwojem sieci teleinformatycznych i atakami hakerów na bezpieczeństwo elektronicznie przetwarzanych informacji;
- trzecia generacja – związana z procesem „automatyzacji" cyberprzestępczości, będącej m.in. efektem wykorzystania złośliwego oprogramowania i botnetów;
- czwarta generacja – generacja wyróżniana w niektórych opracowaniach, związana z coraz powszechniejszym wykorzystaniem narzędzi hakerskich oraz rozwojem podziemia komputerowego.

Należy podkreślić, że rozwój cyberprzestępczości związany jest z powstawaniem coraz skuteczniejszych narzędzi przeznaczonych do celów przestępczych. Każda kolejna generacja cyberprzestępstw przynosi większą specjalizację metod ataku. Incydenty są coraz mniej losowe i chaotyczne – stają się zmasowanymi atakami na elementy infrastruktury krytycznej państwa.

Przestępstwa dokonywane w obszarze cyberprzestrzeni mają różny charakter. W związku z dynamicznym rozwojem zjawiska podział cyberprzestępstw, podobnie jak samo pojęcie, ulega ciągłej ewolucji. Wśród wielu funkcjonujących typologii w literaturze przedmiotu często można znaleźć odwołania do typologii przedstawionej przez U. Siebera, który opierając się na kryterium wyłaniania się przestępstw wraz z rozwojem nowych technologii, wyróżnił następujące rodzaje przestępstw[76]:

- przestępstwa w dziedzinie ochrony danych (naruszenie praw jednostki);
- przestępstwa gospodarcze z użyciem komputerów;
- manipulacje komputerowe, np. manipulacje bankowe;
- sabotaż i szantaż komputerowy;
- haking komputerowy;
- szpiegostwo komputerowe;
- kradzieże oprogramowania i inne formy piractwa dotyczące przemysłu komputerowego.

Istotny wkład w ujednolicenie terminologii związanej z cyberprzestępczości mają inicjatywy legislacyjne ONZ, Unii Europejskiej i Rady Europy (tab. 2.10).

75 Ibidem, s. 1–2.

76 M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, dostęp: http://www.ebib.pl/2010/113/a.php?nowak.

Tab. 2.10. Cyberprzestępczość w ujęciu ONZ, Unii Europejskiej i Rady Europy

Organizacja	Definicja/typy przestępstw
ONZ[a)]	• cyberprzestępstwo w wąskim sensie (przestępstwo komputerowe) – wszelkie nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub przetwarzanych przez te systemy danych • cyberprzestępstwo w szerokim sensie (przestępstwo dotyczące komputerów) – wszelkie nielegalne działanie, popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to m.in. nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych
Komisja Europejska[b)]	Czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom. Do cyberprzestępstw zalicza się: • przestępstwa tradycyjne w sieciach łączności elektronicznej, np. kradzież tożsamości, phishing, handel narkotykami, handel bronią • publikacja nielegalnych treści np. dziecięca pornografia, treści rasistowskie, gloryfikacja przemocy • przestępstwa typowe dla sieci łączności elektronicznej, np. ataki na masową skalę skierowane przeciwko systemom informatycznym, organizacjom i osobom prywatnym
Rada Europy[c)]	• przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych (tzw. przestępstwa *stricte* komputerowe) • przestępstwa związane z użyciem środków masowego przekazu do rozpowszechniania lub prezentowania informacji zakazanych przez prawo (tzw. przestępstwa związane z treścią informacji) • przestępstwa instrumentalnego wykorzystania elektronicznych sieci informatycznych i systemów teleinformatycznych, w tym także przestępstwa przeciwko mieniu, związane z naruszeniem praw autorskich i praw pokrewnych

a) Definicja ONZ została opracowana na X Kongresie ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców.

b) *Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady i Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości,* Bruksela 22.05.2007, KOM (2007) 267, s. 3.

c) *Konwencja Rady Europy o cyberprzestępczości*, Budapeszt 23.11.2001, CETS nr 185.

Opracowanie własne.

Jak już na wstępie wspomniano, w polskim kodeksie karnym nie zdefiniowano cyberprzestępczości oraz przestępczości komputerowej. W 2004 roku znowelizowano kodeks karny w celu ujednolicenia przepisów z Konwencją Rady Europy o cyberprzestępczości, jednakże nie zawarto w tej materii określeń definicyjnych. W *Rządowym Programie Ochrony Cyberprzestrzeni* zawarto następującą definicję:

cyberprzestępstwo – czyn zabroniony popełniony w obszarze cyberprzestrzeni[77]. Z określenia przyjętego w dokumencie wynika, że cyberprzestępstwem będzie zarówno atak cyberterrorystyczny, jak i np. cyberszpiegostwo czy hakerstwo. Takie ujęcie wydaje się zbyt ogólne z badawczego punktu widzenia, ponieważ incydenty w cyberprzestrzeni charakteryzują się różną skalą nasilenia. Ponadto wydaje się istotne odróżnienie politycznie umotywowanego ataku (haktywizm) od chociażby np. działań aktywistów. Także tendencje globalne na arenie międzynarodowej wydają się przemawiać za koniecznością odróżnienia wyżej wymienionych zjawisk.

Dokonując próby kategoryzacji cyberprzestępstw w polskim systemie prawnym, należy podkreślić, że w ujęciu systemowym przepisy prawne w obszarze cyberprzestępczości nie są zebrane w jednym akcje prawnym. Ogólnie można podzielić przestępstwa na dwie grupy:

- przestępstwa określone w przepisach kodeksu karnego;
- przestępstwa uregulowane w przepisach karnych innych ustaw.

Wobec braku powszechnie przyjętej typologii cyberprzestępstw w polskim systemie pranym, w książce przyjęto model analizy zjawiska w oparciu o podział zaproponowany w konwencji o cyberprzestępczości w powiązaniu z możliwymi sprawcami i obiektami przestępstw oraz ich praktyczną realizacją (tab. 2.11).

Tab. 2.11. Przykłady przestępstw w polskim systemie prawnym w powiązaniu ze sprawcami, obiektem ochrony oraz przykładami praktycznej realizacji

Przestępstwo i podstawa prawna	**Możliwy sprawca**	**Obiekt ochrony**	**Charakterystyka i przykłady**
Przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych			
Nielegalny dostęp do systemu komputerowego, kradzież informacji (haking) Art. 267 § 1–2 k.k.[a)]	Każda osoba nieuprawniona do dostępu do informacji, np. hakerzy, nieuprawnieni pracownicy organizacji	Poufność informacji	Nieuprawniony dostęp do informacji oznacza uzyskanie do informacji dostępu bez zgody jej dysponenta – może polegać np. na zalogowaniu się do cudzego komputera lub sieci komputerowej, uzyskanie poufnych informacji, infiltrację systemu teleinformatycznego
Podsłuch komputerowy Art. 267 § 3 k.k.	Hakerzy, szpiedzy	Dane z transmisji w systemach komputerowych (tajemnica komunikacji)	Wykorzystanie urządzenia lub oprogramowania podsłuchowego (np. snifferów, keyloggerów) w celu uzyskania informacji, do której sprawca nie jest uprawniony, np. danych o ruchu w sieci, przechwycenia adresu e-mail, numeru portu, URL

77 *Rządowy Program Ochrony Cyberprzestrzeni...*, op. cit., s. 6.

Przestępstwo i podstawa prawna	Możliwy sprawca	Obiekt ochrony	Charakterystyka i przykłady
Naruszenie integralności zapisu informacji Art. 268 k.k.	Wandale, hakerzy, pracownicy organizacji	Integralność informacji	Zniszczenie, uszkodzenie, usunięcie, zmiana zapisu istotnej informacji; działanie takie może odbywać się np. przy wykorzystaniu szkodliwego oprogramowania
Niszczenie lub utrudnienie dostępu do danych informatycznych Art. 268a k.k.	Wandale, hakerzy, pracownicy organizacji	Integralność i dostępność informacji	Utrudnienie osobie uprawnionej zapoznanie się z informacją oraz zakłócenie lub uniemożliwienie jej automatycznego przetwarzania, gromadzenia lub przesyłania, np. przez przejęcie kontroli nad systemem teleinformatycznym
Sabotaż komputerowy Art. 269 k.k.	Terroryści przestępcy zorganizowani, haktywiści, pracownicy z wysokimi uprawnieniami do systemu	Integralność, dostępność i nienaruszalność informacji mających istotne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji oraz funkcjonowania instytucji publicznych	Przestępstwo ma na celu uniemożliwienie lub utrudnienie prawidłowego funkcjonowania instytucji publicznych, często przy wykorzystaniu wyrafinowanych narzędzi, jak DDoS – tego typu czyny często związane są z szantażem komputerowym mającym na celu osiągnięcie określonej korzyści, np. finansowej
Zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej Art. 269a k.k.	Wandale, haktywiści	Poufność, integralność i dostępność danych informatycznych i systemów oraz bezpieczeństwo informacji przetwarzanych elektronicznie	Przestępstwo może być dokonane przez transmisje, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, np. ataki na serwisy internetowe uniemożliwiające korzystanie z nich
Wytwarzanie lub udostępnianie urządzeń lub programów przystosowanych do popełnienia przestępstwa Art. 269b k.k.	Osoby ze specjalistycznymi umiejętnościami, pracownicy organizacji	Informacje oraz dane znajdujące się w systemach informatycznych lub sieciach teleinformatycznych	Czyny związane z wytwarzaniem narzędzi hakerskich oraz ich posiadaniem, sprzedażą i oferowaniem oraz udostępnianie haseł, kodów dostępu
Przestępstwa związane z instrumentalnym wykorzystaniem sieci i systemów informatycznych			
Oszustwo komputerowe Art. 287 k.k.	Przestępcy, napastnicy korporacyjni	Mienie oraz zapis informacji wraz z zasadami ich automatycznego	Przestępca wpływa na automatyczne przetwarzanie, gromadzenie, przesyłanie informacji, lub zmienia czy też usuwa zapis informacji na

Przestępstwo i podstawa prawna	Możliwy sprawca	Obiekt ochrony	Charakterystyka i przykłady
		gromadzenia, przetwarzania i przesyłania	nośniku komputerowym, w celu uzyskania korzyści majątkowej lub wyrządzenia szkody innej osobie, np. oszustwo nigeryjskie[b)]
Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych Art. 116–118 PrAut.[c)]	Każda osoba, która bez wymaganego uprawnienia lub też wbrew jego warunkom upowszechnia cudzy utwór oraz wytwarza narzędzia do obchodzenia zabezpieczeń	Prawa majątkowe, własność intelektualna, prawa autorskie	Przestępstwa przejawiają się w: 1) rozpowszechnieniu utworu bez uprawnienia lub wbrew jego warunkom, 2) utrwaleniu lub zwielokrotnieniu cudzego utworu w celu rozpowszechnienia, 3) wytwarzaniu, posiadaniu, przechowywaniu i wykorzystaniu urządzeń lub ich komponentów przeznaczonych do niedozwolonego usuwania lub obchodzenia technicznych zabezpieczeń
Przestępstwa związane z treścią informacji			
Przestępstwa seksualne na szkodę małoletniego Art. 200–202 k.k.	Każda osoba dopuszczająca się przestępstw seksualnych na szkodę małoletniego	Ochrona wolności i seksualności małoletnich	Czyny zabronione przejawiające się w prezentowaniu, produkcji, rozpowszechnianiu oraz posiadaniu treści pornograficznych z udziałem małoletnich, posiadaniu pornografii pedofilskiej lub groomingu[d)]
Zniesławienie Art. 212 k.k.	Każda osoba dopuszczająca się zniesławienia – popełnienie tego czynu zabronionego nie wymaga specjalistycznych umiejętności informatycznych	Ochrona dobrego imienia osoby fizycznej, prawnej lub instytucji	Pomówienie innej osoby, grupy osób, instytucji, osoby prawnej lub jednostki organizacyjnej o takie postępowanie lub cechy, które mogą narazić na utratę zaufania publicznego, niezbędnego do wykonywanie danej działalności, zawodu itp., np. publikacja na forum internetowym nieprawdziwych treści związanych z osobą wykonująca zawód lekarza, adwokata itp.
Zniewaga Art. 216 k.k	Każda osoba dopuszczająca się zniewagi	Godność osobista	Uwłaczające lub obelżywe wypowiedzi, wizerunki lub gesty; odrębna penalizacja czynu zabronionego została przewidziana dla niektórych kategorii osób, np. zniewaga prezydenta RP (art. 135 k.k.) lub zniewaga związana z dyskryminacją rasową, wyznaniową itd. (art. 257)
Inne typy przestępstw			
Szpiegostwo komputerowe Art. 130 § 3 k.k.	Wynajęci hakerzy, szpiedzy	Bezpieczeństwo zewnętrzne	Działalność na rzecz obcego wywiadu mogąca szkodzić RP polegająca na udzielaniu wiadomości, ich gromadzeniu i przechowywaniu albo

Przestępstwo i podstawa prawna	Możliwy sprawca	Obiekt ochrony	Charakterystyka i przykłady
			wchodzeniu do systemu teleinformatycznego w celu ich uzyskania
Cyberstalking Art. 190a § 1 k.k.	Każda osoba dopuszczająca się przestępstwa cyberstalkingu	Ochrona prywatności, wolność od strachu, zdrowie fizyczne i psychiczne, nietykalność cielesna, nienaruszalność korespondencji	Prześladowanie polegające na wywołaniu uczucia strachu i zagrożenia, przez zamierzone i świadome naruszenie sfery życia prywatnego i publicznego z wykorzystaniem elektronicznych systemów przetwarzania informacji[e]
Kradzież tożsamości Art. 190 § 2 k.k.	Hakerzy, socjotechnicy	Dane osobowe	Podszywanie się pod inną osobę w celu osiągnięcia korzyści

[a] Ustawa z dnia 6 czerwca 1997 roku Kodeks karny (Dz.U. 1997 nr 88, poz. 553).
[b] Oszustwo nigeryjskie – rodzaj oszustwa polegający na wciągnięciu ofiary w fikcyjny transfer pieniędzy.
[c] PrAut. – Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24, poz. 83).
[d] Grooming – nawiązanie kontaktu z małoletnim za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej.
[e] M. Sawicki, *Cyberprzestępczość...*, op. cit., s. 274–275.

Opracowanie własne.

Analiza cyberprzestępczości potwierdza tezę dotyczącą złożoności zjawiska. Struktury administracyjne wykorzystujące systemy informatyczne są w posiadaniu ogromnej ilości informacji, które mogą być celem dla cyberprzestępców. Przeciwdziałanie tym zagrożeniom jest utrudnione z uwagi na ewolucję metod i technik wykorzystywanych do ataków oraz trudność w wykryciu sprawcy w związku z możliwością zachowania anonimowości w sieci. Oprócz napastników zewnętrznych występują także wewnętrzni, którzy mogą spowodować ogromne szkody dla bezpieczeństwa struktury administracyjnej. Wobec powyższego niezbędny jest stały nadzór nad funkcjonowaniem jednostek administracji publicznej, dokonywanie przeglądów bezpieczeństwa oraz analiza ryzyka.

2.5.3. Cyberterroryzm

Cyberterroryzm nie został jak dotąd zdefiniowany w przepisach prawa. W literaturze można jednak odnaleźć liczne próby jego określenia. Często takie kategorie jak cyberatak, cyberwojna, cyberprzestępczość i cyberterroryzm traktuje się

zamiennie. Istotną kwestią jest opracowanie interpretacji adekwatnej do opisywanego zjawiska.

Przyjmuje się, że omawiane pojęcie zostało po raz pierwszy sformułowane przez B. Collina, który w latach osiemdziesiątych użył go dla określenia połączenia terroryzmu i cyberprzestrzeni[78]. Wówczas zaczęto konstruować scenariusze dotyczące możliwych i prawdopodobnych konsekwencji cyberterroryzmu. W 1993 roku A. i H. Tofflerowie użyli sformułowania *elektroniczne Pearl Harbor* w odniesieniu do ataku na infrastrukturę krytyczną Stanów Zjednoczonych skutkującego paraliżem wielu systemów teleinformatycznych, co uniemożliwiłoby sprawne funkcjonowanie wielu obszarów państwa i społeczeństwa. Prognoza ta nie doczekała się jak dotąd realizacji, jednak nie należy jej wykluczać, gdyż wiele państw doświadczyło przejawów działalności terrorystycznej w cyberprzestrzeni z powodu wykorzystania nowoczesnych technologii w wielu obszarach funkcjonowania państwa i społeczeństwa. Publiczne zainteresowanie zjawiskiem cyberterroryzmu nasiliło się niewątpliwie po wydarzeniach z 11 września 2001 roku.

Cyberterroryzm jest zjawiskiem z pogranicza różnych obszarów: bezpieczeństwa teleinformatycznego, technologii teleinformatycznej i teleinformacyjnej, bezpieczeństwa osobowego, bezpieczeństwa fizycznego, regulacji krajowych i międzynarodowych oraz danych osobowych[79]. Odnosząc się do kwestii definicyjnych zjawiska cyberterroryzmu, należy zatem uwzględnić zróżnicowanie terminologiczne, a także określić sprawców i charakter tego typu ataku. Trudności w zdefiniowaniu cyberterroryzmu wiążą się niewątpliwie z niejednoznacznym rozumieniem terminu *terroryzm*. Ponadto niejasne są granice między cyberterroryzmem, cyberprzestępczością oraz walką informacyjną.

Jak dotąd nie opracowano jednolitej definicji cyberterroryzmu. W tab. 2.12 przedstawiono przykładowe sposoby definiowania omawianej kategorii. Najczęściej określenia sprowadzają się do definiowania jej jako terroryzmu rozszerzonego o spektrum cyberprzestrzeni.

Analiza przywołanych definicji pozwala zaobserwować pojawiającą się zasadniczą różnicę. Definicje (1) i (4) uwzględniają to, że istnieje możliwość wykorzystania systemów komputerowych lub telekomunikacyjnych do przeprowadzenia ataku w cyberprzestrzeni. Definicje (2), (3), (5) zawierają natomiast określenie, że komputery i systemy informacyjne są celem takiego ataku. Sporny charakter tych dwóch kwestii jest zauważalny w wielu definicjach omawianej kategorii.

78 A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm...*, op. cit., s. 64.

79 E. Lichocki, *Cyberterrorystyczne zagrożenia dla bezpieczeństwa teleinformatycznego Państwa Polskiego*, dostęp: http://www.csikgw.aon.edu.pl/index.php/pl/pobieranie/func-startdown/81/.

Tab. 2.12. Przykładowe definicje cyberterroryzmu

Lp.	Autor	Definicja
1.	B. Collin	Świadome wykorzystywanie systemu informacyjnego, sieci komputerowej albo jej części składowych celem wsparcia lub ułatwienia przeprowadzenia terrorystycznej akcji
2.	D. Denning	Jest to groźba lub bezprawny atak wymierzony w system informatyczny albo zgromadzone w nim dane, celem wywołania strachu czy wymuszenia na władzach państwowych i jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych działań
3.	R. Kośla	Działania blokujące, niszczące albo zniekształcające w stosunku do informacji, która jest przetwarzana, przechowywana i przekazywana w systemach teleinformatycznych, oraz obezwładniające te systemy
4.	K.C. White	Świadome wykorzystanie systemów informacyjnych, sieci komputerowych albo jej części składowych celem wsparcia lub ułatwienia terrorystycznej akcji
5.	M.M. Pollit	Cyberterroryzm to przemyślany, politycznie motywowany atak, kierowany przeciwko informacjom, systemom komputerowym, programom oraz informacjom, który prowadzi do oddziaływania na pozamilitarne cele, przeprowadzony przez ugrupowania narodowościowe bądź tajnych agentów

Opracowanie własne na podstawie: E. Lichocki, *Cyberterroryzm państwowy i niepaństwowy – początki, skutki, formy...*, op. cit., s. 165; A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm...*, op. cit., s. 63–70, cyt. za: E. Szczepaniuk, *Zagrożenia bezpieczeństwa informacyjnego RP*, praca magisterska, Siedlce 2012.

Kompromisowe ujęcie polega na rozróżnieniu wąskiego i szerokiego pojmowania zjawiska cyberterroryzmu. *W ujęciu węższym jest to działalność terrorystyczna w systemach informatycznych ukierunkowana na zniszczenie lub modyfikację danych w tych systemach, skutkująca ofiarami śmiertelnymi lub zniszczeniem mienia w znacznych rozmiarach. W szerszym znaczeniu oznacza zaś wszelką działalność terrorystyczną związaną z cyberprzestrzenią, włączając fizyczne ataki na sieci komputerowe*[80]. Niezależnie od przyjętego ujęcia, cyberterroryzm realizuje się w postaci działań blokujących, niszczących lub zniekształcających informacje w systemach teleinformatycznych.

Jak już wcześniej wspomniano, cyberterroryzm łączy w sobie dwa istotne elementy – cyberprzestrzeń i terroryzm. W podrozdziale 2.1 przywołano wiele definicji cyberprzestrzeni funkcjonujących zarówno w literaturze naukowej, jak i w dokumentach rządowych. Pomimo określonych niejasności przyjęto, że cyberprzestrzeń jest ewolucyjnym systemem złożonym, na który składają się nie tylko elementy fizyczne, m.in. sieci komputerowe i systemy informatyczne, ale także element ludzki, dzięki któremu możliwe jest ich funkcjonowanie oraz rozwój.

80 Cyt. za: R. Białoskórski, *Wyzwania i zagrożenia bezpieczeństwa XXI wieku*, Warszawa 2010, s. 60.

Wiele wątpliwości pojawia się także w definiowaniu zjawiska terroryzmu. S. Koziej określa terroryzm jako *ostentacyjne i maksymalistyczne (masowe, totalne, nieograniczone), celowe (tj. świadomie zamierzone) atakowanie niewinnych, postronnych (cywilnych) osób i dóbr publicznych (otoczenia) dla pośredniego (asymetrycznego, przez opinię publiczną) oddziaływania na rzeczywistego przeciwnika politycznego lub ideologicznego*[81]. Na ogół przyjmuje się, że terroryzm związany jest z działaniem prowadzonym w celach politycznych. Brak definicji terroryzmu na arenie międzynarodowej rodzi niejasności w odniesieniu do konkretnych aktów – np. w razie konieczności ustalenia, czy określone działanie jest przejawem walki narodowowyzwoleńczej, czy też ma ono charakter terrorystyczny. K. Liedel zauważa, że *analiza zamiaru sprawcy (sprawców) i jego (ich) celów pozwala na odróżnienie terrorystów od innych przestępców, a terroryzm od innych postaci zbrodni, przestępstw czy innych negatywnie ocenianych zjawisk społecznych. Powszechnie w literaturze przedmiotu do terroryzmu nie zalicza się aktów o charakterze kryminalnym oraz walki o charakterze narodowowyzwoleńczym*[82]. Kontrowersje pojawiają się również w odniesieniu do definicji terroryzmu państwowego, który objawia się bezprawnym użyciem siły przez władze państwowe w stosunku do innych państw, a także w wymiarze wewnętrznym – wobec własnej ludności. Terroryzm państwowy jest często kwestionowany, jednakże w odniesieniu do cyberterroryzmu takie pojęcie wydaje się użyteczne.

W cyberprzestrzeni zacierają się różnice między tym co wojskowe i cywilne oraz tym co fizyczne i wirtualne. Za atakiem cyberterrorystycznym mogą stać zarówno państwa, jak i podmioty niepaństwowe, lub też może on być przeprowadzony przez serwery pośredniczące (*proxy*). Trudności w identyfikacji sprawcy prowadzą do wniosku, że zjawisko cyberterroryzmu nie musi być kojarzone jedynie z działaniami podejmowanymi przez grupy terrorystyczne[83]; a zatem cyberterroryzm należy postrzegać jako metodę działania prowadzącą do określonych celów, której wyznacznikiem jest charakter ataku.

Przywołane w monografii szersze ujęcie cyberterroryzmu odnosi się do wszelkiej działalności terrorystów związanej z cyberprzestrzenią. Wydaje się jednak, że cyberterroryzm należy odróżnić od innych nadużyć komputerowych, takich jak np. przestępstwa komputerowe, aktywizm, haktywizm lub cyberszpiegostwo czy też walka informacyjna. Jednakże należy podkreślić, że narzędzia wykorzy-

81 S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Toruń 2006, s. 31.

82 K. Liedel, *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*, Warszawa 2010, s. 23.

83 A. Podraza, *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego XXI wieku* [w:] *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, red. A. Podraza, P. Potakowski, K. Wiak, Warszawa 2013, s. 29.

stywane w atakach są często tożsame. Różne natomiast są skutki i konsekwencje działań.

W ujęciu węższym wyklucza się z pojęcia cyberterroryzmu aktywizm, haktywizm oraz koordynację działań terrorystycznych przy pomocy Internetu, np. zdobywanie środków finansowych czy też propagandę. Takie podejście reprezentowane jest przez Dorothy Denning, która podkreśla, że działania haktywistów mogą doprowadzić do zakłócenia funkcjonowania Internetu, ale nie powodują poważnych uszkodzeń. Cyberterroryzm natomiast skutkuje przemocą przeciwko osobom lub mieniu, a co najmniej generuje strach[84]. Do aktywności haktywistów tego typu można zaliczyć np. ataki mailowe (tzw. *e-mail bombing*) czy też wirtualne blokady sieci Web.

Również K. Lidel zauważa, że *wielu badaczy zagadnienia cyberterroryzmu dzieli [go] na kolejne kategorie umożliwiające szczegółowe umiejscowienie zjawisk związanych z przemocą i atakiem w wymiarze instytucjonalnym, do których należą – aktywizm, haktywizm, cyberterroryzm. Taka kategoryzacja zjawiska oznaczałaby, że pojęcie cyberterroryzmu zawiera się samo w sobie*[85]. W celu uniknięcia niejasnej z punktu widzenia klasyfikacji zjawisk przyjęto, że wyżej wymienione zjawiska występują równolegle.

W 1999 roku opublikowano raport pt. *Cyberterror: prospect and implications*[86]. W dokumencie przedstawiono prognozę potencjalnych szkód związanych ze zjawiskiem cyberterroryzmu. W podsumowaniu dokumentu podkreślono, że cyberterroryzm może stanowić poważne zagrożenie dla bezpieczeństwa międzynarodowego – może być głównym sposobem prowadzenia walki bądź stanowić wsparcie w działaniach organizacji terrorystycznych (rys. 2.11). Ponadto w raporcie naukowcy wyróżnili trzy poziomy zagrożenia cyberterroryzmem (tab. 2.13).

Warto zaznaczyć, że zgodnie z wąskim rozumieniem cyberterroryzmu nie było do tej pory przypadku ataku cyberterrorystycznego. Natomiast jeżeli zastosuje się kryteria oparte na innym, szerszym ujęciu zjawiska – zdarzyło się już wiele przypadków takich działań. Granice między cyberzagrożeniami nie są do końca wyraźne. Ponadto aktywizm i haktywizm mogą być elementami kampanii terrorystycznej. Przykłady ataków uznanych za cyberterrorystyczne przedstawia tabela 2.14.

84 D.E. Denning, *Activism, hacktivism and cyberterrorism: the internet as a tool for influencing foreign policy*, s. 241, dostęp: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382ch8.pdf.

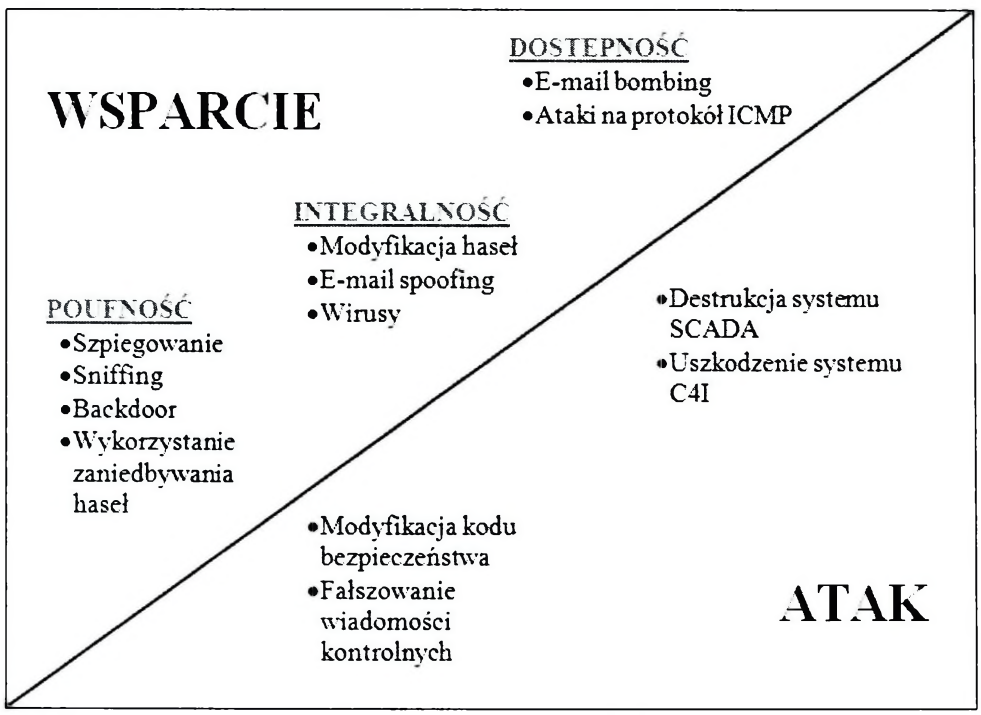
85 K. Lidel, *Bezpieczeństwo informacyjne państwa w dobie zagrożeń terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2008, s. 35.

86 B. Nelson, R. Choi, M. Iacobucci, M. Mitchell, G. Gagnon, *Cyberterror: prospect and implications*, Monterey 1999, dostęp: http://webcache.googleusercontent.com/search?q=cache:CJycB1I7ug0J:https://www. hsdl.org/%3 Fview% 26did%3D442884+&cd=1&hl=pl&ct=clnk&gl=pl.

Tab. 2.13. Poziomy zagrożenia cyberterroryzmem

Poziom	Cel	Charakterystyka	Czas
I. Prosty nieustrukturyzowany	Pojedynczy system lub sieć	Proste włamania do indywidualnych systemów przy wykorzystaniu narzędzi, które zostały skonstruowane przez kogoś innego; organizacja ma niewielką zdolność analiz celów będących przedmiotem ataku oraz uczenia się nowych metod atakowania	0–6 miesięcy
II. Zaawansowany ustrukturyzowany	Złożone systemy lub sieci	Bardziej złożone ataki na systemy i sieci komputerowe; organizacja ma zdolność modyfikacji lub tworzenia własnych narzędzi służących do cyberataków oraz zdolność uczenia się nowych metod, a także dowodzenia i kontroli	Minimum 1 rok; prawdopodobnie 2–4 lata
III. Kompleksowy skoordynowany	Złożone sieci	Terroryści dokonują skoordynowanych ataków w celu destrukcji zintegrowanego systemu obronnego; mają możliwość tworzenia własnych zaawansowanych narzędzi oraz analiz celów będących przedmiotem ataku, dowodzenia, kontroli oraz samodoskonalenia	Minimum 2 lata; prawdopodobnie 6–10 lat

Opracowanie własne na podstawie: B. Nelson, R. Choi, M. Iacobucci, M. Mitchell, G. Gagnon, *Cyberterror: prospect and implications...*, op. cit., s. 9 i 96.



Opracowanie własne na podstawie: B. Nelson, R. Choi, M. Iacobucci, M. Mitchell, G. Gagnon, *Cyberterror: prospect and implications...*, Monterey 1999, dostęp: http://webcache.googleusercontent.com/search?q=cache:CJycB1I-7ug0J:https://www. hsdl.org/%3 Fview% 26did%3D442884+&cd=1&hl=pl&ct=clnk&gl=pl, s. 11.

Rys. 2.11. Porównanie ataku i wsparcia cyberterrorystów

Tab. 2.14. Przykłady ataków uznanych za cyberterrorystyczne

Rok	Charakterystyka
1999	Cyberataki na 60 agencji rządowych w Malezji – celem były wrażliwe resorty: opieka społeczna, imigracja, skarb państwa
2000	Grupa pakistańskich hakerów zniszczyła ok. 600 indyjskich stron internetowych oraz przejściowo przejęła kontrolę nad niektórymi indyjskimi sieciami komputerowymi
2001	Blokada witryny Białego Domu i New York Times – atak z Chin
2007	Nieznani sprawcy zaatakowali i na kilka miesięcy sparaliżowali pracę systemów informatycznych jednego z biur Departamentu Handlu USA, w którym przetwarzane były informacje niejawne związane z eksportem wysoko rozwiniętych technologii
	Zorganizowany i jeden z największych w dziejach atak cyberterrorystyczny na Estonię doprowadził do paraliżu niektórych elementów infrastruktury krytycznej (m.in. systemu bankowego)
	Penetracja sieci wojskowej Pentagonu oraz atak na systemy informatyczne Departamentu Obrony Stanów Zjednoczonych techniką backdoor
	Brytyjskie służby specjalne, biuro premiera Francji oraz biuro kanclerz Niemiec oskarżyły Chiny o atakowanie ich systemów informatycznych
2008	CIA oficjalnie poinformowało o czterech znanych atakach na elektrownie jądrowe innych państw, które groziły odcięciem zasilania dla kilku miast jednocześnie
	Korea Południowa oskarżyła Chiny o próby ataku cybernetycznego na ambasadę Korei i sieci koreańskiej infrastruktury wojskowej
	Indie oskarżyły Chiny o przeprowadzenie ataków cybernetycznych na komputery rządowe, których celem było skanowanie i mapowanie danych
2010	Ataki cybernetyczne na Iran; wykrycie wirusa Stuxnet
2011	Atak na system komputerowy Komisji Europejskiej
	Zastępca sekretarza obrony USA W.J. Lynn ujawnił, że wykradziono ok. 24 tys. plików z badanych firm zaopatrujących amerykańskie siły zbrojne
2012	„Red October" – ataki na placówki dyplomatyczne

Opracowanie własne na podstawie: R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku...*, op. cit., s. 89–108, H. Świeboda, *Zagrożenia informacyjne bezpieczeństwa RP...*, op. cit., s. 60–61.

Analiza zjawiska cyberterroryzmu dowodzi, że cyberprzestrzeń pozwala w wielu wypadkach na zachowanie anonimowości. W związku z tym proponuje się postrzeganie zjawiska cyberterroryzmu jako metody działania zorientowanej na wywołanie określonych skutków. Uzasadnione są wątpliwości, czy do tej pory mieliśmy do czynienia z takimi działaniami, czy też nie. Niezależnie od przyjętej interpretacji, cyberterroryzm stanowi zagrożenie, którego nie należy bagatelizować. W związku z rosnącą liczbą cyberataków wiele państw decyduje się na budowę systemów cyberobrony.

2.5.4. Cyberszpiegostwo

Szpiegostwo w ogólnym rozumieniu jest formą działalności wywiadowczej polegającą na zdobywaniu informacji niejawnych[87]. Polski kodeks karny wyróżnia następujące typy szpiegostwa[88]:

- udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej;
- udzielanie obcemu wywiadowi wiadomości, których przekazanie może wyrządzić Polsce szkodę;
- gromadzenie lub przechowywanie wiadomości, lub wchodzenie do systemu informatycznego w celu ich uzyskania i udzielenia obcemu wywiadowi, albo zgłoszenie gotowości na rzecz działania obcego wywiadu przeciwko Polsce;
- organizowanie działalności obcego wywiadu lub kierowanie nim.

Rozwój technologii informatycznych i wykorzystanie ich w sektorach infrastruktury krytycznej przyczyniły się rozwoju cyberszpiegostwa. R. Białoskórki pod pojęciem szpiegostwa cybernetycznego (cyberszpiegostwa) rozumie *zdobywanie informacji i materiałów wywiadowczych (skutek), czyli takich, które stanowią istotną wartość z punktu widzenia działań wywiadowczych (motywacja/cel) realizowanych przez daną służbę wywiadowczą (podmiot atakujący), znajdujących się w cyberprzestrzeni (podmiot atakowany) z wykorzystaniem różnorodnych metod i technik wywiadowczych, a w szczególności cybernetycznych*[89]. Zaproponowana definicja pozawala na analizę zjawiska w oparciu o skutek, cel, wyróżnienie podmiotu atakującego i atakowanego. Należy zauważyć, że zjawisko cyberszpiegostwa jest formą szpiegostwa, która przeniosła się w środowisko elektroniczne.

Wiele informacji jest współcześnie przetwarzanych w systemach elektronicznych, co jest głównym powodem rosnącej popularności tego typu działalności w cyberprzestrzeni. W ciągu kilkunastu ostatnich lat można zaobserwować wzrost aktywności związanej z cyberszpiegostwem. Działalność szpiegowska w cyberprzestrzeni może odbywać się na zlecenie innych państw czy podmiotów. Celem mogą być plany uzbrojenia, tajemnice gospodarcze i handlowe, patenty czy też np. informacje wrażliwe.

Podstawę cyberszpiegostwa stanowią programy szpiegujące (spyware) umożliwiające instalację w atakowanym systemie komputerowym, bez wiedzy i szkody jego użytkownika, nieautoryzowanego software'u, którego zadaniem jest moni-

87 Art. 1. ust. 1. ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych stanowi, że informacje niejawne to informacje, których nieuprawnione ujawnienie spowodowałby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowania oraz niezależnie od formy i sposobu ich wyrażania.

88 Art. 130 k.k.

89 R. Białoskórski, *Cyberzagrożenia...*, op. cit., s. 66.

torowanie i zdobywanie informacji wartościowych z punktu widzenia podmiotu szpiegującego[90]. Informacje te mogą dotyczyć zasobów przechowywanych w systemie oraz akcji podejmowanych przez użytkownika. Programy szpiegujące należą do najniebezpieczniejszych rodzajów złośliwego oprogramowania. Mogą one być umieszczane na komputerze jako plik wykonywalny albo w sposób samodzielny. Dobrze zorganizowane ataki tego typu mogą pozostać nigdy nieodkryte, niezwykle trudno jest bowiem zidentyfikować sprawcę.

Dla ukazania skali zjawiska warto posłużyć się kilkoma przykładami dotyczącymi zjawiska cyberszpiegostwa. Pierwsze włamania mające na celu zdobycie poufnych informacji zdarzały się już w latach osiemdziesiątych XX wieku. Jednak dopiero na początku XXI wieku cyberszpiegostwo stało się jedną z najpopularniejszych form szkodliwej działalności w sieci[91]. W 2003 roku wykryto działania związane ze skanowaniem określane jako „Tytanowy Deszcz" (ang. *Titan Rain*), polegające na przeszukiwaniu w ciągu sekundy tysięcy komputerów instytucji pracujących na rzecz resortów obrony czy urzędów państwowych. W wyniku operacji *udało jej się uzyskać dane dotyczące m.in. planów i technologii NASA, Lockheed-Martin czy Redstone Arsenal, w tym projektu Joint Strike Fighter*[92]. W następnych latach miały miejsce incydenty związane z doskonale zorganizowanymi włamaniami do instytucji rządowych, naukowych oraz biznesowych na terytorium USA i Europy Zachodniej. Przykładowo w 2008 roku miało miejsce wyprowadzenie tajnych danych z sieci amerykańskiej armii przy wykorzystaniu socjotechniki oraz błędów personelu.

Na uwagę zasługuje powstanie globalnej sieci szpiegowskiej GhostNet, która została wykryta w 2009 roku. Podaje się, że sieć operuje głównie z terytorium Chin. W wyniku działania GhostNet zainfekowano 1295 komputerów należących do organizacji międzynarodowych oraz instytucji rządowych w 103 krajach. W raportach[93] na temat zagrożenia przedstawiono dowody na to, że motywy tego ataku miały charakter polityczny. Sieć wykorzystywała program przystosowany do wykradania danych wrażliwych w postaci poufnych lub tajnych dokumentów, przejmowania kontroli nad sieciowymi kamerami wideo oraz zainfekowanymi komputerami[94]. Przede wszystkim atakowano serwery mające duże znaczenie polityczne, ekonomiczne lub medialne.

90 Ibidem, s. 73.

91 M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw...*, op. cit., s. 128–129.

92 Ibidem, s. 128–129.

93 Zob. *Tracking GhostNet: Investigating a Cyber Espionage Network*, "Information Warfare Monitor", March 2009, dostęp: http://pl.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

94 *Szpiegowska sieć w Internecie*, dostęp: http://www.computerworld.pl/news/342832/Szpiegowska.siec.w.internecie.html.

Poziom zorganizowania, a także dobór celów ataku bywa najczęściej wysoce zaawansowany, dlatego wydaje się mało prawdopodobne, że za atakami cyberszpiegostwa stoją wyłącznie grupy przestępcze czy podmioty niepaństwowe. W tym kontekście warto zwrócić uwagę na raport przygotowany w 2013 roku przez firmę Mediant na temat chińskiej aktywności szpiegowskiej w Stanach Zjednoczonych[95]. Z danych zaprezentowanych przez autorów raportu wynika, że wchodząca w skład Chińskiej Armii Ludowo-Wyzwoleńczej jednostka 61398, będąca centralnym ogniwem chińskiego systemu wywiadu komputerowego, jest odpowiedzialna za większość ataków na firmy i rządowe agencje USA, ponieważ atakujący amerykańskie komputery hakerzy należący do grupy nazwanej APT.1 działają z rejonu geograficznego, w którym zlokalizowana jest jednostka 61398. Zdaniem autorów raportu, ze względu na wysoki poziom kontroli Internetu przez chińskie władze, jest niemożliwe, aby były one nieświadome działalności grupy – wręcz przeciwnie, prawdopodobne jest, że wysoką skuteczność w wykradaniu amerykańskich tajemnic hakerzy uzyskują dzięki współpracy z jednostką 61398 lub są jej częścią. Publikacja raportu stanowiła pierwsze publiczne oskarżenie pod adresem władz Chin o udział w procederze ataków i kradzieży własności intelektualnej należącej do amerykańskich przedsiębiorstw, organizacji oraz instytucji państwowych, a także uzyskiwanie zdolności do sterowania elementami amerykańskiej infrastruktury krytycznej[96]. Władze Chin zaprzeczyły amerykańskim oskarżeniom, podkreślając, że na terenie kraju tego typu działania są sprzeczne z prawem. Co więcej, Chiny zaliczyły siebie do kategorii ofiar hakerów z terytorium Stanów Zjednoczonych.

Na początku czerwca 2013 roku gazety „The Washington Post" oraz „The Guardian" opisały amerykański program Prism, którego celem jest inwigilacja danych gromadzonych na serwerach: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube oraz Apple. Publikując powyższe informacje, gazety powołały się na tajne dokumenty uzyskane od E. Snowdena, byłego pracownika CIA[97] oraz NSA[98]. Doniesienia dotyczące programu wywołały falę oskarżeń pod adresem USA. Jednakże władze USA podkreśliły, że jest on zgodny z prawem i nie jest używany do monitorowania obywateli lub innych osób zamieszkałych na terytorium kraju. Program koncentruje się na obcokrajowcach. Uzyskane informacje są natomiast wykorzystywane do ochrony przed zagrożeniami (m.in. terroryzmem).

95 Zob. *Exposing One of China's Cyber Espionage Units*, dostęp: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

96 M. Grzelak, *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" nr II (26), Warszawa 2013, s. 114.

97 CIA – ang. *Central Intelligence Agency*, Centralna Agencja Wywiadowcza.

98 NSA – ang. *National Security Agency*, Agencja Bezpieczeństwa Narodowego.

Podsumowując, cyberszpiegostwo należy postrzegać jako ewolucyjnie ukształtowaną formę szpiegostwa, polegającą na pozyskiwaniu informacji niejawnych przez państwa lub powiązane z nimi podmioty przy wykorzystaniu sieci teleinformatycznych. Z perspektywy bezpieczeństwa struktur administracyjnych oraz bezpieczeństwa narodowego zdobyte w ten sposób informacje stanowią poważne zagrożenie. Należy zauważyć, że do tego typu działań wykorzystuje się inne metody niż w przypadku pozostałych cyberzagrożeń, ponieważ stosowane są techniki o niskim prawdopodobieństwie wykrycia, np. keyloggery, phishing czy metody z zakresu socjotechniki. Celem działania nie jest bezpośrednie wyrządzenie szkód jak np. w przypadku cyberterroryzmu, lecz zdobycie informacji, które mają strategiczne znaczenie dla bezpieczeństwa narodowego, przez co mogą stanowić poważne zagrożenie dla instytucji rządowych czy instytutów badawczych.

2.5.5. Walka informacyjna

Chociaż za pierwszą wojnę informacyjną uznano wojnę w Zatoce Perskiej[99], a samego pojęcia zaczęto używać dopiero w połowie lat dziewięćdziesiątych XX wieku[100] – walka informacyjna była przez wieki istotnym elementem sztuki wojennej[101]. Uzyskanie dominacji informacyjnej, rozpoznanie sił wroga oraz wprowadzenie w błąd nieprzyjaciela towarzyszyło od niepamiętnych czasów działaniom wojennym[102]. Zatem już na wstępie można przyjąć tezę, że walka informacyjna nie stanowi nowego rodzaju zagrożenia, jednak zdumiewający rozwój techniki, który nastąpił między pierwszą a drugą wojną światową, przyczynił się do przeniesienia walki informacyjnej w środowisko elektroniczne.

W roku 1946 uruchomiono pierwszy komputer w ramach wojskowego „Projektu X". *W latach 50-tych pojawiły się pierwsze systemy przetwarzania danych, a w następnej dekadzie zautomatyzowane systemy dowodzenia obroną powietrzną, potem następne, coraz bardziej doskonałe, takie jak: system wczesnego ostrzegania AWACS lub lokalizacji obiektów GPS, systemy broni satelitarnej typu Fire and Forget, bądź systemy telekomunikacyjne (satelitarne, radiokomunikacji*

99 Zob. S.A. Campen (red.), *The First Information War*, Fairfax 1992.

100 P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 132.

101 Obszerne omówienie historii i ewolucji walki informacyjnej można odnaleźć w opracowaniu L. Ciborowskiego *Walka informacyjna*, Toruń 1999, s. 11–46.

102 Sun Tzu, chiński strateg wojenny żyjący ok. V w. p.n.e., dostrzegał istotną rolę niesiłowych rozstrzygnięć i strategię zmagań informacyjnych Zob. Sun Tzu, *Sztuka wojny*, Warszawa 2004.

ruchomej itp.)[103]. Rozwój techniki przyniósł jakościowe zmiany w obrębie walki informacyjnej, które na szeroką skalę zostały użyte we wspomnianej już wojnie w Zatoce Perskiej na początku lat dziewięćdziesiątych, a następnie w 2001 roku w Afganistanie i 2003 roku w Iraku.

Warto przypomnieć, że już na początku lat dziewięćdziesiątych ubiegłego stulecia J.A. Warden dostrzegł znaczenie cyberprzestrzeni w działaniach wojennych i potraktował ją jako piąty wymiar walki. Postęp technologiczny przyniósł zmiany w obrębie walki informacyjnej, związane m.in. ze wzrostem różnorodnych zagrożeń, a także potencjalnych obiektów ataku.

M. Wrzosek zauważa, że w większości opracowań (w szczególności z końca minionego wieku) pojęcie walki informacyjnej odnoszone jest w zasadzie tylko do aktywności militarnej, a więc do działań prowadzonych przez siły zbrojne stron konfliktu i służących uzyskaniu przewagi informacyjnej nad przeciwnikiem przez zniszczenie lub uszkodzenie jego zasobów informacyjnych oraz wojskowych systemów telekomunikacyjnych[104]. Pojawiły się wówczas koncepcje cyberwar, netwar oraz network-centric warfare (NCW). Równolegle do wspomnianych koncepcji walki zbrojnej następował proces informatyzacji wielu sfer funkcjonowania państwa i społeczeństwa. Istotnym problemem stała się podatność na zagrożenia informacyjne poszczególnych sektorów infrastruktury krytycznej państwa. Elementy infrastruktury krytycznej funkcjonujące w oparciu o nowoczesne technologie stały się szczególnie narażone na incydenty zagrażające bezpieczeństwu.

Wraz z rozwojem technologicznym tradycyjne zagrożenia informacyjne, m.in. szpiegostwo czy też nieuprawnione przekazywanie informacji, zyskały nową jakość oraz stały się groźniejsze, chociażby z uwagi na trudności z kontrolowaniem cyberprzestrzeni. Zagrożenia związane ze zjawiskiem walki informacyjnej są niewątpliwie zagrożeniami świadomymi, ukierunkowanymi na destrukcję bądź zmniejszenie efektywności działania elementów systemów informacyjnych lub elementów wchodzących w skład infrastruktury krytycznej państwa. Zagrożenia te stanowią wyzwanie dla podmiotów odpowiedzialnych za bezpieczeństwo narodowe (stąd także za bezpieczeństwo struktur administracyjnych). Nie istnieje powszechnie przyjęta definicja walki informacyjnej. W tab. 2.15 przedstawiono przykładowe definicje omawianego pojęcia.

103 T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne...*, op. cit., s. 92.

104 M. Wrzosek, *Zmagania o informację we współczesnych organizacjach*, „Zeszyty Naukowe AON" 2010, nr 4(81), s. 42.

Tab. 2.15. Przykładowe definicje walki informacyjnej

Autor	Definicja
L. Ciborowski	Walka informacyjna to działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron. Przedmiotem walki informacyjnej jest system informacyjno-sterujący[a)].
Departament Obrony USA	Działania podejmowane w celu uzyskania informacyjnej dominacji, przez oddziaływanie na informacje przeciwnika, jego systemy, procesy informacyjne oraz sieci komputerowe, oraz obrona własnych informacji, systemów informacyjnych oraz procesów przepływu informacji i sieci komputerowych[b)].
P. Sienkiewicz	Całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów. Istotą tak rozumianej walki jest: 1) zniszczenie bądź degradacja zasobów informacyjnych przeciwnika oraz stosowanie przez niego systemów informacyjnych; 2) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych[c)].
R. Szpyra	Walka informacyjna to zorganizowana w formie przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej informacji przed podobnym działaniem przeciwnika[d)].

a) L. Ciborowski, *Walka informacyjna...*, op. cit., s. 41.

b) S.A. Hildreth, *Cyberwarfare*, CRS Report for Congress, 2001, s. 19, dostęp: http://fas.org/irp/crs/RL30735.pdf.

c) P. Sienkiewicz, *Wizje i modele wojny informacyjnej...*, op. cit., s. 375.

d) R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych*, rozprawa habilitacyjna, Warszawa 2002, cyt. za: H. Świeboda, *Zagrożenia bezpieczeństwa informacyjnego...*, op. cit., s. 255.

Opracowanie własne.

P. Sienkiewicz i H. Świeboda zauważają, że w większości proponowanych określeń dotyczących walki informacyjnej pojawiają się wspólne treści. *Wszystkie one sprowadzą się do postrzegania walki informacyjnej jako konfliktu, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią, a zarazem obejmuje on fizyczne niszczenie infrastruktury, wykorzystywanej przez przeciwnika do działań operacyjnych*[105]. Wątpliwości pojawiają się w stosunku do pojęcia *information warfare* – termin ten jest tłumaczony na język polski zarówno jako *walka*

105 P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 80.

informacyjna, jak i *wojna informacyjna*. Pojawia się także termin *wojna informatyczna*. W tym kontekście warto przywołać pogląd R. Szpyry, który stwierdza, że wojna jest kategorią obejmującą wszystkie formy walki: zbrojną, informacyjną i ekonomiczną[106].

Interesującą analizę w ramach projektów badawczych RAND Corporation, dotyczącą nachodzących konfliktów epoki informacyjnej, przedstawili J. Arquilla i D. Ronfeldt[107]. W ramach koncepcji walki informacyjnej wyróżnili oni *netwar* i *cyberwar*.

Netwar prowadzona jest na poziomie społeczeństw oraz narodów, której celem jest zakłócenie, uszkodzenie lub modyfikacja informacji o państwie będącym celem ataku. Może skupiać się na opinii publicznej bądź też elitach rządzących[108]. Działania prowadzone w ramach opisywanego konfliktu koncentrują się na więzi łączącej państwo oraz społeczeństwo, których celem jest wpływanie na opinię publiczną. Jak słusznie zauważa K. Lidel, definicja *netwar przybliża nas do znanej z historii działań wojennych – propagandy wojennej lub też wojny propagandowej*[109]. Konflikt tego typu zakrojony na szeroką skalę wpływać ma na interesy państw oraz dezintegrację więzi łączącej państwo i społeczeństwo. Arquilla i Ronfeldt działania prowadzone w ramach *netwar* podzielili w zależności od aktorów. Mogą być nimi zarówno rządy państw oraz ich służby, jak grupy społeczne występujące przeciwko rządowi oraz aktorzy niepaństwowi.

Kolejną kategorią wyróżnioną przez badaczy RAND jest *cyberwar*, która opiera się na przeprowadzeniu operacji wojskowych związanych z traktowaniem informacji jako zasobu strategicznego. Celem działań w ramach *cyberwar* jest zakłócenie lub destrukcja systemów komunikacyjnych strony przeciwnej oraz osiągnięcie przewagi informacyjnej, przy jednoczesnym zapobieganiu uzyskania informacji na temat własnych stron. Arquilla i Ronfeldt zwrócili uwagę, że koncepcja *cyberwar* może oznaczać rozwój nowych doktryn prowadzenia walki, a co za tym idzie – zmiany organizacyjne w siłach zbrojnych, rozbudowę nowych sił i środków oraz przeobrażenia w strategii i taktyce wojennej[110]. Operacje mogą zatem być prowadzone w czasie kryzysów lub konfliktów w celu wsparcia określonych działań. Mogą one także obejmować ataki na elementy infrastruktury krytycznej czy systemy dowodzenia.

106 R. Szpyra, *Militarne operacje informacyjne*, Warszawa 2003, cyt. za: P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne...*, op. cit., s. 80.

107 J. Arquilla, D. Ronfeldt, *Cyberwar is coming!*, dostęp: http://www.rand.org/content/dam/rand/pubs /reprints /2007/RAND_RP223.pdf, s. 28.

108 Ibidem, s. 6.

109 Liedel K., *Bezpieczeństwo informacyjne państwa...*, op. cit., s. 22.

110 J. Arquilla, D. Ronfeldt, *Cyberwar is coming!*, op. cit., s. 30–31.

Obiektem tego typu działań są zasoby informacyjne oraz systemy teleinformatyczne. D. Denning zwraca uwagę na możliwość prowadzenia walki defensywnej i ofensywnej. Mianem ofensywnej wojny informacyjnej określa *takie działania, w których chodzi o zdobycie lub wykorzystanie jakiegoś szczególnego zasobu informacyjnego, w celu zwiększenia jego wartości dla gracza ofensywnego i zmniejszenia – dla gracza defensywnego*[111]. Natomiast walka defensywna według Denning *ma na celu obronę zasobów informacyjnych przed trzema rodzajami ataków: zwiększeniem dostępności dla strony ofensywnej, zmniejszeniem dostępności dla strony defensywnej lub zmniejszeniem integralności*[112]. Zatem walka defensywna jest stosowana zarówno w czasie pokoju, jak i w czasie kryzysu. Jej celem jest zabezpieczenie i obrona. Natomiast walka ofensywna ma na celu zwiększenie przewagi informacyjnej i stanowi wsparcie działań podczas konfliktu. Wykorzystanie elementów walki informacyjnej umożliwia uzyskanie określonych skutków (tab. 2.16).

Tab. 2.16. Oczekiwane skutki walki informacyjnej

Siły własne	Siły przeciwnika
Ochrona systemów dowodzenia, łączności i rozpoznania	Zakłócanie procesów informacyjno-decyzyjnych w systemach dowodzenia
Minimalizacja wpływu walki elektronicznej	Minimalizacja efektywności systemów dowodzenia, kierowania środkami walki, teleinformatyki, rozpoznania i walki elektronicznej
Minimalizacja zagrożeń informacyjnych bezpieczeństwa systemów dowodzenia i kierowania	Uniemożliwianie wykorzystania pełnej siły rażenia oraz obniżanie tempa działań (operacji)
Minimalizacja wpływu działań psychologicznych	Zwiększenie podatności na działania psychologiczne

Źródło: P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej...*, op. cit., s. 88.

W tym kontekście warto przywołać kilka przykładów zastosowania elementów walki informacyjnej, które miały miejsce w przeszłości. Wśród pierwszych prób wykorzystania przestrzeni cybernetycznej w konflikcie zbrojnym należy wymienić wydarzenia, do jakich doszło w 1991 roku w trakcie operacji „Pustynna Burza". Nieskomplikowane włamania towarzyszyły również wojnom w Czeczenii. W 1999 roku w trakcie interwencji NATO w Kosowie wykorzystano Internet do propagandy, komunikacji, dezinformacji przeciwnika oraz ataków DDoS, e-mail bombingu czy włamywania się na rządowe witryny internetowe. W sumie podczas bombardowania Jugosławii zaatakowano ok. 200 serwerów Sojuszu. Konflikt w Kosowie określany jest często jako pierwsza wojna informacyjnej. Kolejnym

111 D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 32.
112 Ibidem, s. 32.

przykładem jest przeprowadzona w 2007 roku operacja iracka „Orchard", której celem była destrukcja syryjskiego ośrodka badań nad bronią atomową. Służby Izraela zainfekowały wówczas syryjski system obrony powietrznej wirusem komputerowym, co skutkowało niewykryciem izraelskich samolotów. Warto również wspomnieć o konflikcie gruzińsko-rosyjskim w 2008 roku. Wówczas Rosja na atak gruziński zareagowała działaniami w cyberprzestrzeni. Dzięki wykorzystaniu sieci *botnet* i metod DDoS sparaliżowano witryny internetowe należące do rządu Gruzji. Zaatakowano także wiele stron komercyjnych, informacyjnych oraz naukowych.

Na podstawie powyższych rozważań można stwierdzić, że wykorzystanie cyberprzestrzeni do działań militarnych może obejmować różne formy ataków cybernetycznych. Szczególnie zagrożone są elementy infrastruktury krytycznej państwa, których paraliż może doprowadzić do destabilizacji wewnątrz państwa. Celem walki informacyjnej jest wsparcie realizacji zadania o charakterze militarnym. Należy zauważyć, że ta forma cyberzagrożeń może być stosowana jedynie przez państwa, które dysponują odpowiednim potencjałem w tym zakresie.

2.6. Wpływ cyberzagrożeń na bezpieczeństwo struktur administracyjnych

Analizując wpływ cyberzagrożeń na bezpieczeństwo struktur administracyjnych, warto sięgnąć do danych statystycznych dotyczących wszczętych postępowań karnych w obszarze przestępczości komputerowej.

W tab. 2.17 przedstawiono liczbę wszczętych postępowań dotyczących przestępczości komputerowej w Polsce w latach 2002–2011.

Na podstawie danych przedstawionych w tabeli można zaobserwować zwiększającą się liczbę przestępstw komputerowych. Największa liczba wszczętych postępowań odnosi się do udaremnienia lub utrudnienia korzystania z informacji, natomiast najmniejsza do niszczenia danych informatycznych. Należy mieć na uwadze, że cyberprzestępstwa są trudne do wykrywania i ścigania. Jedynie nikły procent spraw kończy się wyrokiem skazującym. Transgraniczny charakter tego typu przestępstw jest wyzwaniem dla organów ścigania. Niezbędne jest stałe szkolenie funkcjonariuszy, ponieważ narzędzia i techniki wykorzystywane do przestępczości komputerowej stają się coraz bardziej zaawansowane.

Statystyki Zespołu CERT.GOV.PL również pokazują wzrost ataków na systemy informatyczne. W Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku czytamy: *Rok 2013 pod względem liczby otrzymanych zgłoszeń oraz obsłużonych incydentów okazał się dla Zespołu CERT.GOV.PL rekordowy w sto-*

sunku do lat poprzednich[113]. Największą grupę zagrożeń stanowiły incydenty kategorii *Botnet*. Odnotowano 4270 incydentów związanych ze złośliwym oprogramowaniem na stacjach roboczych podłączonych do sieci jednostek administracji publicznej.

Tab. 2.17. Dane o liczbie wszczętych postępowań dotyczących przestępczości komputerowej w Polsce w latach 2002–2011

Rok	Razem	Udaremnienie lub utrudnienie korzystania z informacji Art. 268 i 268a	Niszczenie danych informatycznych Art. 269 § 1–2	Sabotaż komputerowy Art. 269a	Wytwarzanie programu komputerowego do popełnienia przestępstwa Art. 269b	Oszustwo komputerowe Art. 287 § 1–2
2011	1976	885	3	38	38	1012
2010	1592	690	7	22	35	838
2009	1291	555	6	34	23	673
2008	869	366	6	13	12	472
2007	587	244	6	11	4	322
2006	517	201	3	19	9	285
2005	487	152	2	1	6	326
2004	346	105	12	0	0	229
2003	335	114	2	0	0	219
2002	209	89	6	0	0	114
Razem		3401	53	138	127	4490

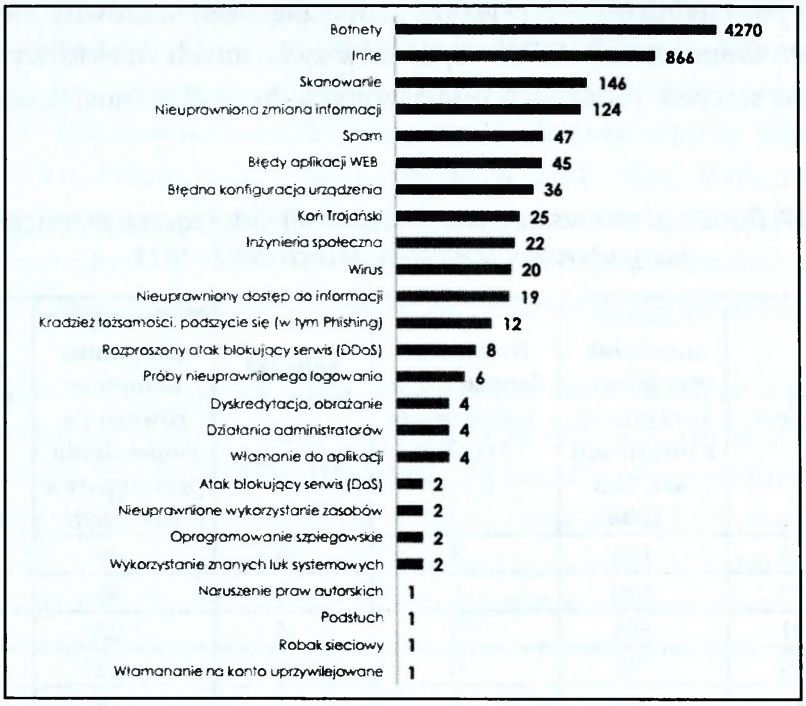
Źródło: dane statystyczne Komendy Głównej Policji, cyt. za: T. Muliński, *Zagrożenia bezpieczeństwa...*, op. cit., s. 114.

W kategorii *Inne* uwzględniono informacje o podatnościach oraz błędy konfiguracji aplikacji lub urządzeń sieciowych. Znaczący wpływ na statystykę miały w tej kategorii informacje o podatności serwerów DNS[114], dotyczące wielu podmiotów administracji publicznej oraz agend rządowych – w sumie 866 incydentów[115]. Zespół otrzymał także znaczną ilość zgłoszeń związanych ze skanowaniem sieci – 146 incydentów, oraz dotyczących nieuprawnionej zmiany informacji (np. podmiana zawartości witryn komputerowych) – 124 przypadki. Statystykę incydentów w 2013 roku z podziałem na kategorie przedstawia rys. 2.12.

113 *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*, CERT.GOV.PL, Warszawa 2014, s. 5.

114 DNS – ang. *Domain Name System*, system serwerów, protokół komunikacyjny oraz usługa obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala on na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki DNS nazwa mnemoniczna tłumaczona jest na odpowiadający jej adres IP.

115 *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*, op. cit., s. 10.



Źródło: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*, op. cit., s. 9.

Rys. 2.12. Statystyka incydentów w 2013 roku z podziałem na kategorie

Zwiększająca się liczba użytkowników sieci Internet oraz zastosowanie zaawansowanych technologii w sektorach infrastruktury krytycznej państwa determinuje potrzebę stałego doskonalenia i podnoszenia jakości rozwiązań służących ochronie cyberprzestrzeni RP. Podmioty atakujące wykorzystują nowe i coraz doskonalsze metody ataków cybernetycznych, co implikuje konieczność wdrażania nowych rozwiązań w sferze organizacyjnej oraz technicznej. Wzrastająca liczba incydentów pokazuje wysoki poziom zagrożenia dla bezpieczeństwa teleinformatycznego Polski, w tym dla administracji publicznej. Stąd niezbędne jest prowadzenia działalności informacyjnej i szkoleniowej użytkowników systemów komputerowych.

Przywołane przykłady incydentów, które miały miejsce w innych państwach, pokazują skutki związane z cyberzagrożeniami. Zagrożenia cyberprzestrzeni państwa nie odegrały jak dotąd znaczącej roli w kontekście bezpieczeństwa struktur administracyjnych, rozumianego jako zapewnienie dostępności i niezawodności usług administracyjnych o odpowiedniej jakości – przynajmniej nie zagrożenia skutkujące paraliżem wielu sektorów publicznych, jak miało to miejsce w Estonii. Nie należy jednak lekceważyć możliwości wystąpienia tego typu działań. Wydarzenia dotyczące blokowania stron rządowych w Polsce w wyniku protestu

przeciwko ACTA pokazały, że konieczny jest ciągły nadzór nad funkcjonowaniem systemów teleinformatycznych administracji publicznej. Bezpieczeństwo struktur administracyjnych w kontekście omawianej problematyki należy także postrzegać w kategoriach zapewnienia bezpieczeństwa informacji obejmującego problemy ochrony informacji w systemach teleinformatycznych. Zatem niezbędne jest zapewnienie atrybutów bezpieczeństwa informacji – przede wszystkim integralności, dostępności, niezawodności i poufności.

Obecnie w Polsce nie ma tak silnego powiązania administracji publicznej z odbiorcami usług za pośrednictwem Internetu, że brak dostępności usługi lub jej zniekształcenie wpłynęłoby w istotny sposób na funkcjonowanie państwa lub poszczególnych instytucji sektora publicznego[116]. Jednakże rozwój społeczeństwa informacyjnego oraz informatyzacja administracji publicznej w Polsce będzie sprzyjać tej formie kontaktu obywatela (przedsiębiorcy) z urzędem. Należy także mieć na uwadze bezpieczeństwo informacji w ramach komunikacji w strukturze administracyjnej oraz wymianę informacji z innymi jednostkami administracji publicznej.

Wzrost znaczenia centrów przetwarzania danych funkcjonujących od lat oraz uruchomianych w ostatnim czasie[117], spowodowany wdrażaniem centralnych systemów obsługi pracowników administracji oraz interesantów, stwarza ryzyko wystąpienia zagrożeń dla bezpieczeństwa informacji. Centra te mogą stać się potencjalnymi celami ataków cyberterrorystycznych oraz elementem walki informacyjnej[118].

Cyberzagrożenia nie wpłynęły jak dotąd na obniżenie poziomu bezpieczeństwa narodowego. Nie odnotowano istotnego przypadku braku dostępności usług publicznych czy paraliżu elementów infrastruktury krytycznej. Jednakże Polska może stać się w przyszłości celem takich ataków. Stąd warto wskazać cechy cyberzagrożeń oraz ich przypuszczalny wpływ na bezpieczeństwo narodowe i bezpieczeństwo struktur administracyjnych (tab. 2.18).

116 ePUAP posiada na dzień 26.09.2014 roku 303 776 profili zaufanych obywateli, urzędów oraz firm.

117 Do obiektów skali państwowej można zaliczyć Centrum Przetwarzania Danych Ministerstwa Finansów, Centrum Personalizacji Dokumentów MSW, serwerownie platformy ePUAP czy NBP.

118 Podobny pogląd reprezentuje T. Muliński; por. T. Muliński, *Zagrożenie bezpieczeństwa...*, op. cit., s. 122.

Tab. 2.18. Cechy cyberzagrożeń i ich wpływ na bezpieczeństwo narodowe i administrację publiczną

Zagrożenie	Podmiot atakujący	Motywacja i cele	Stopień organizacji	Stopień zagrożenia dla bezpieczeństwa narodowego	Przykłady zagrożeń dla bezpieczeństwa struktur administracyjnych
Haking	Jednostki, grupy, hakerzy	Indywidualna, rozwój własnych umiejętności	Niski	Niski	Przełamanie zabezpieczeń
Haktywizm	Jednostki, grupy, haktywiści	Społeczna, polityczna, promocja określonych wartości, postaw lub ideologii w przestrzeni publicznej	Niski z elementami koordynacji na poziomie narodowym lub międzynarodowym	Niski, czasem straty wizerunkowe dla władzy publicznej	Odmowa dostępu do usługi, przełamanie zabezpieczeń, utrudnienie dostępu do danych
„Haktywizm patriotyczny"	Jednostki, grupy, haktywiści	Polityczna, patriotyczna (narodowa), promocja określonych wartości, postaw lub ideologii związanych z państwem pochodzenia	Niski z elementami koordynacji na poziomie narodowym	Uzależniony od obiektu ataku – najczęściej są to witryny internetowe, jednak celem mogą stać się także elementy infrastruktury krytycznej	Odmowa dostępu do usługi, przełamanie zabezpieczeń, utrudnienie dostępu do danych, sabotaż komputerowy, zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej
Cyberprzestępczość	Jednostki, grupy, przestępcy, pracownicy instytucji (organizacji)	Osiągnie korzyści osobistych i materialnych	Niski z elementami koordynacji na poziomie narodowym lub międzynarodowym	Pośredni, uciążliwy przede wszystkim z punktu widzenia społecznego i gospodarczego	Nielegalny dostęp do danych, utrata atrybutów bezpieczeństwa informacji, naruszenie integralności zapisu informacji
Cyberterroryzm	Organizacje terrorystyczne, wynajęci hakerzy	Polityczna, dokonanie zniszczeń, osiągnięcie efektu psychologicznego i promocja własnej ideologii lub postulatów	Wysoki stopień koordynacji i kontroli	Wysoki – celem są elementy infrastruktury krytycznej państwa, sieci i systemy wojskowe; może się wpisywać w konflikty międzynarodowe	Odmowa dostępu do usługi, nielegalny dostęp do danych, utrata atrybutów bezpieczeństwa informacji, sabotaż komputerowy, zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej

Zagrożenie	Podmiot atakujący	Motywacja i cele	Stopień organizacji	Stopień zagrożenia dla bezpieczeństwa narodowego	Przykłady zagrożeń dla bezpieczeństwa struktur administracyjnych
Cyberszpiegostwo	Państwa i powiązane z nimi podmioty pozapaństwowe, pracownicy z wysokimi uprawnieniami do systemu	Polityczna, gospodarcza, uzyskanie niejawnych danych w różnych celach	Wysoki stopień koordynacji i kontroli	Wysoki, ponieważ celem są informacje o strategicznym znaczeniu dla bezpieczeństwa państwa; prowadzi do pogorszenia stosunków między państwami	Kradzież poufnych informacji, kradzież tożsamości, nielegalny dostęp do danych, utrata atrybutów bezpieczeństwa informacji
Walka informacyjna	Państwa	Polityczna, wojskowa, fizyczne uszkodzenia; realizacja określonego celu o charakterze militarnym	Bardzo wysoki stopień koordynacji i kontroli	Bardzo wysoki – wiąże się z operacjami o charakterze zbrojnym; może skutkować zniszczeniami lub śmiercią obywateli	Odmowa dostępu do usługi, destrukcja systemów teleinformatycznych, zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej

Opracowanie własne.

3. ZARZĄDZANIE BEZPIECZEŃSTWEM CYBERPRZESTRZENI STRUKTUR ADMINISTRACYJNYCH

3.1. Istota bezpieczeństwa cyberprzestrzeni struktur administracyjnych

Funkcjonowanie struktur administracyjnych jest uzależnione w znacznym stopniu od sprawnego działania systemów i sieci komputerowych. Współcześnie obserwuje się wzrost zapotrzebowania na informację oraz narzędzia informatyczne, które wspólnie tworzą zasoby informacyjne administracji i są elementami jej cyberprzestrzeni. Należy zauważyć, że *wiele systemów informacyjnych nie zostało zaprojektowanych tak, aby były bezpieczne. Bezpieczeństwo, które może być osiągnięte za pomocą środków technicznych, jest ograniczone i zaleca się wspieranie go przez odpowiednie normy i procedury*[1]. Dodatkowo wzrost cyberzagrożeń i incydentów bezpieczeństwa sprawia, że funkcjonowanie jednostek sektora publicznego wiąże się z ryzykiem wystąpienia zagrożeń dla bezpieczeństwa struktur administracyjnych, które generują zagrożenia dla bezpieczeństwa narodowego.

W dokumencie Polityka Ochrony Cyberprzestrzeni RP zdefiniowano bezpieczeństwo cyberprzestrzeni jako *zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego bezpieczeństwa cyberprzestrzeni*[2]. W przywołanym dokumencie czytamy także, że *w każdej jednostce organizacyjnej administracji rządowej, w ramach zapewnienia bezpieczeństwa cyberprzestrzeni, kierownik jednostki powinien ustanowić system zarządzania bezpieczeństwem informacji, w oparciu o obowiązujące przepisy i najlepsze praktyki. Zakłada się, że podmiot publiczny będzie opracowywał i modyfikował w zależności od potrzeb, a także wdrażał politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez niego do realizacji*

1 PN-ISO/IEC 17799 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zarządzanie bezpieczeństwem informacji, cyt. za: B. Szomański, *Zarządzanie bezpieczeństwem informacji – podstawy oraz znaczenie w ochronie firmy przed nieuczciwymi pracownikami, klientami i usługodawcami* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007, s. 64.

2 Polityka Ochrony Cyberprzestrzeni RP, op. cit., s. 5.

zadań publicznych[3]. Bezpieczeństwo cyberprzestrzeni jest zatem pojęciem interdyscyplinarnym, funkcjonującym na pograniczu teorii organizacji i zarządzania, informatyki, prawa oraz nauk o bezpieczeństwie.

Zdefiniowanie bezpieczeństwa cyberprzestrzeni struktur administracyjnych wymaga wyjaśnienia pewnych kwestii terminologicznych. Odwołując się do definicji zaproponowanych w monografii oraz biorąc pod uwagę rozważania związane z technicznymi aspektami cyberprzestrzeni, pojęć *bezpieczeństwo cyberprzestrzeni* i *bezpieczeństwo teleinformatyczne* można używać zamiennie. W wielu publikacjach na temat bezpieczeństwa teleinformatycznego używa się także pojęcia bezpieczeństwa informatycznego, które zawęża płaszczyznę badań, dlatego będzie ono używane w szerszym kontekście – teleinformatycznym. Kolejna kategoria – bezpieczeństwo informacji – jest pojęciem najszerszym, wykracza bowiem poza systemy teleinformatyczne (np. dokumenty papierowe). Dlatego też przyjęto używanie pojęcia bezpieczeństwa informacji w znaczeniu węższym, dotyczącym informacji przetwarzanych, przechowywanych i transmitowanych w cyberprzestrzeni.

Analiza przeprowadzona w poprzednich rozdziałach skłania do postrzegania bezpieczeństwa struktur administracyjnych w kontekście realizacji misji instytucji i zapewnienia odpowiedniej jakości świadczenia usług publicznych zarówno w wymiarze zewnętrznym, jak i wewnętrznym. Odnosząc powyższe kwestie do rozważań na temat istoty i specyfiki cyberprzestrzeni, zasadne jest analizowanie bezpieczeństwa cyberprzestrzeni struktur administracyjnych w oparciu o misję instytucji, odbiorców usług świadczonych przez instytucję, elementy tworzące cyberprzestrzeń oraz istniejące i przyszłe zagrożenia dla bezpieczeństwa cyberprzestrzeni.

Wobec powyższego proponuje się definiowanie cyberbezpieczeństwa (bezpieczeństwa cyberprzestrzeni) struktur administracyjnych jako stan, w którym:

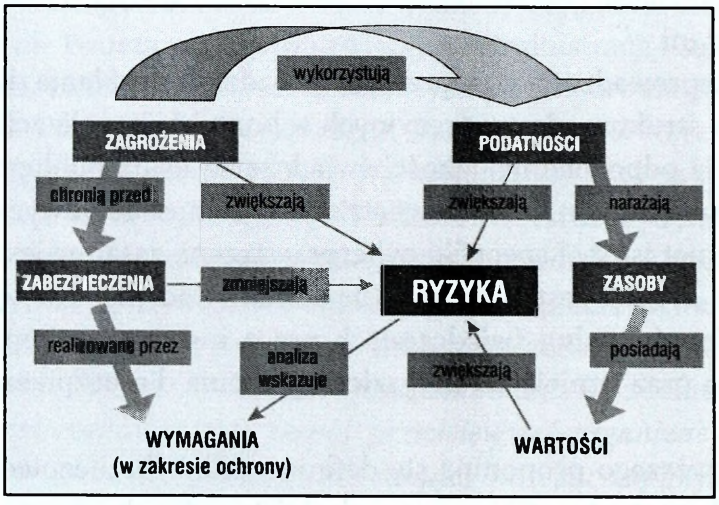
- elementy tworzące cyberprzestrzeń struktur administracyjnych cechuje zdolność do ochrony przed obecnymi i przyszłymi zakłóceniami (zagrożeniami) funkcjonowania lub utraty określonych wartości – system jest odporny na zagrożenia (wewnętrzne, zewnętrzne, przypadkowe, celowe);
- bezpieczeństwo informacji jest osiągnięte i utrzymywane na założonym poziomie poufności, integralności i dostępności;
- bezpieczeństwo świadczonych usług jest osiągnięte i utrzymywane na założonym poziomie niezawodności, dostępności i integralności usług;
- zapewniona jest autentyczność i rozliczalność podmiotów związana z autoryzacją użytkowników korzystających z określonych informacji i usług;

3 Ibidem, s. 13.

• użytkownicy informacji i usług (pracownicy zatrudnieni w strukturach administracyjnych) oraz odbiorcy informacji i usług (obywatele, przedsiębiorcy, pracownicy zatrudnieni w innych strukturach administracyjnych) mają świadomość zagrożeń bezpieczeństwa cyberprzestrzeni i nie są na nie podatni;

• aktorzy zagrożeń (także napastnicy wewnętrzni) mają małe możliwości wykorzystania cyberprzestrzeni do generowania zagrożeń przez wykorzystanie słabości, podatności i luk w systemie zabezpieczeń cyberprzestrzeni.

Realizacja wymienionych elementów wymaga przełożenia na system prawny danego państwa, instytucji i organizacji międzynarodowych. Ochrona prawna struktur administracyjnych w zakresie bezpieczeństwa cyberprzestrzeni zostanie omówiona szerzej w następnym podrozdziale. Niemniej jednak warto w tym miejscu wspomnieć, że normy dotyczące bezpieczeństwa informacji wprowadziły swoistą nomenklaturę w zakresie nazewnictwa elementów bezpieczeństwa oraz ich wzajemnych relacji (rys. 3.1).



Źródło: PN-1-13335-1..., op. cit.; cyt. za: M. Blim, *Teoria ochrony informacji (część 1)*, „Zabezpieczenia" nr 3/2007, s. 60.

Rys. 3.1. Relacje pomiędzy elementami bezpieczeństwa

Zgodnie z rysunkiem zagrożenie jest potencjalną przyczyną niepożądanego incydentu dla bezpieczeństwa systemu. Jego wystąpieniu sprzyja tzw. podatność, którą jest słabością lub luką w systemie i która naraża zasoby instytucji na utratę określonych wartości. Incydent bezpieczeństwa stwarza konsekwencje (skutki) dla organizacji. Relacja między zagrożeniem a podatnością, a w szczególności prawdopodobieństwo, że zagrożenie wykorzysta podatność systemu, określana jest mianem ryzyka. W celu minimalizacji ryzyka wprowadza się różnego rodzaju zabezpieczenia. W związku z tym z punktu widzenia bezpieczeństwa systemów istotne są następujące elementy: identyfikacja zagrożeń, identyfikacja podatności,

ocena ryzyka, stosowanie zabezpieczeń, aby sprowadzić ryzyko do stanu akceptowalnego.

W tym kontekście warto zauważyć, że w instytucji publicznej nie są chronione wszystkie informacje i usługi, lecz tylko informacje wrażliwe, czyli takie, które mają znaczenie dla realizacji zadań stawianych przed instytucją. Pojęcie wrażliwości informacji *jest pewną miarą ważności przypisaną jej przez autora lub dysponenta w celu wskazania konieczności jej ochrony*[4]. Wrażliwość informacji jest związana z jej klasyfikowaniem oraz oznaczaniem klauzul tajności wyrażających stopień jej wrażliwości. Przykładowo w strukturze administracyjnej obligatoryjną ochroną objęte będą dane osobowe, natomiast obligatoryjnym udostępnianiem objęte będą informacje publiczne.

Podobnie jest z usługami realizowanymi w instytucji przez środki teleinformatyczne. Wyodrębnia się grupę usług krytycznych, które stanowią dobro instytucji. Usługa krytyczna jest to usługa *realizowana przez system teleinformatyczny, mająca bezpośrednie znaczenie dla funkcjonowania instytucji i wskazana przez gremium odpowiedzialne za bezpieczeństwo w celu zapewnienia jej szczególnej ochrony, zwłaszcza w zakresie dostępności*[5]. W tym kontekście szczególnie istotne jest zatem zapewnienie ciągłości działania[6] i odpowiedniego poziomu jakości.

W Polsce jak dotąd nie odnotowano incydentów naruszających bezpieczeństwo cyberprzestrzeni, które w znacznym stopniu zakłóciłyby funkcjonowanie jednostek sektora publicznego. Stan bezpieczeństwa jest jednak zjawiskiem nietrwałym, który należy traktować jako proces realizowany w danym systemie. Należy mieć także na uwadze naruszenia bezpieczeństwa informacji będących w posiadaniu administracji publicznej, które z kolei nie są już zjawiskiem rzadkim. Stąd sprawne funkcjonowanie struktur administracyjnych wymaga skutecznego zarządzania bezpieczeństwem ich cyberprzestrzeni. Owo zarządzanie jest procesem umożliwiającym realizację zadań publicznych w zmieniającym się środowisku kształtowanym przez wymagania stawiane jednostkom administracji publicznej, postęp technologiczny oraz nowe formy zagrożeń.

Przeciwdziałanie zagrożeniom informacyjnym (w tym cyberzagrożeniom) możliwe jest pod warunkiem skutecznego, systemowego zarządzania bezpieczeństwem informacji jednostki administracji publicznej. Obejmuje ono kompleksowe zarządzanie posiadanymi zasobami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem ich utraty. Zarządzanie bezpieczeństwem cyberprzestrzeni podlega takim samym regułom jak każdy inny obszar zarządzania –

4 A. Białas, *Bezpieczeństwo informacji i usług...*, op. cit., s. 35.

5 Ibidem, s. 35.

6 Zob. P. Zaskórski (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, Warszawa 2011.

ma swój cel, plany, polityki, rozwiązania dotyczące wdrożenia, instrumenty kontroli (audytu), rachunek kosztów i ryzyka, programy utrzymania dotychczasowych wyników oraz ciągłego doskonalenia i poprawy jakości.

Zarządzanie bezpieczeństwem cyberprzestrzeni struktur administracyjnych jest zespołem procesów zmierzających do osiągnięcia i utrzymania ustalonego poziomu bezpieczeństwa. Jego realizacja obejmuje takie działania jak[7]:

- określenie celów (co należy chronić), strategii (w jaki sposób), i reguł polityki bezpieczeństwa zgodnie z przepisami prawa;
- identyfikowanie i analizowanie zagrożeń dla zasobów;
- identyfikowanie i analizowanie ryzyka;
- określenie adekwatnych zabezpieczeń;
- monitorowanie wdrożenia, eksploatacji (skuteczności) zabezpieczeń;
- opracowanie i wdrożenie programu szkoleń;
- wykrywanie incydentów i reakcja na nie.

Wspomniane elementy przyczyniły się do rozwoju różnego rodzaju zabezpieczeń. Jednak samo zastosowanie zabezpieczeń programowych i sprzętowych nie zapewni pożądanego poziomu bezpieczeństwa. Równie ważnym aspektami są m.in. świadomość społeczna i szkolenie personelu, opracowanie polityki bezpieczeństwa, rozpoznanie ryzyk, monitorowanie aktualnego stanu bezpieczeństwa oraz wdrożenie systemu zarządzania bezpieczeństwem informacji.

Zabezpieczenia kojarzone są najczęściej z ochroną systemów teleinformatycznych, sprzętu i oprogramowania. Norma PN-ISO/IEC 17799:2007 zawiera rekomendacje dotyczące obszarów zabezpieczeń w zakresie bezpieczeństwa informacji. Zabezpieczenia w rozumieniu przywołanej normy to nie tylko zabezpieczenia techniczne, sprzętowe czy programowe, ale również prawne, umowne, kontraktowe, proceduralne oraz szkolenia uświadamiające pracowników (tab. 3.1).

Podsumowując, zarządzanie bezpieczeństwem struktur administracyjnych na wysokim poziomie ogólności powinno być zapewnione przy wzajemnej koordynacji w następujących obszarach:

- regulacje prawne (np. ustawa, rozporządzenie, norma, wytyczne);
- rozwiązania proceduralne i organizacyjne (np. polityka bezpieczeństwa instytucji, audyt informatyczny);
- zabezpieczenia;
- zarządzanie zasobami ludzkimi w instytucji (np. polityka kadrowa, szkolenia) oraz działania na rzecz podnoszenia świadomości na temat cyberzagrożeń wśród odbiorców informacji i usług;
- doskonalenie i podnoszenie jakości.

7 T. Jemioło, *Modelowanie procesów walki informacyjnej. Model CYBERWAR*, Warszawa 2006, s. 99.

Tab. 3.1. Obszary zabezpieczeń w PN-ISO/IEC 17799: 2007

Polityka bezpieczeństwa
– Informacje o zawartości i sposobie aktualizacji
Organizacja i bezpieczeństwo informacji
– Organizacja wewnętrzna systemu – Koordynacja działań wywnętrz instytucji – Zagadnienia związane z umowami
Zarządzanie aktywami
– Identyfikacja i klasyfikacja aktywów informacyjnych
Bezpieczeństwo zasobów ludzkich
– Zakresy odpowiedzialności pracowników – Aspekt bezpieczeństwa informacji w trakcie rekrutacji, zatrudnienia i zakończenia/zamiany zatrudnienia – Uświadamianie i szkolenie pracowników – Postępowanie dyscyplinarne w przypadku naruszeń bezpieczeństwa informacji
Bezpieczeństwo fizyczne i środowiskowe
– Zabezpieczenie fizyczne instytucji – Podział na strefy, zabezpieczenie pomieszczeń i urządzeń – Bezpieczeństwo sprzętu i okablowania – Wynoszenie mienia, praca poza siecią instytucji
Zarządzanie systemami i sieciami
– Zarządzanie systemami informatycznymi – Zarządzanie sieciami
Kontrola dostępu
– Zarządzanie dostępem użytkowników do informacji – Zarządzanie przywilejami
Pozyskiwanie, rozwój i utrzymanie systemów informatycznych
– Bezpieczeństwo systemów informatycznych
Zarządzanie incydentami związanymi z bezpieczeństwem informacji
– Sposób postępowania z incydentami – Sposób zgłaszania słabości systemów – Gromadzenie materiału dowodowego
Zarządzanie ciągłością działania
– Planowanie ciągłości działania
Zgodność
– Zgodność z przepisami prawnymi – Ochrona zapisów instytucji

Opracowanie własne na podstawie: A. Sołecki, P. Sołecki, *Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007, s. 135.

Problematyka bezpieczeństwa informacji i usług, w tym systemów teleinformatycznych, znajduje obszerne odzwierciedlenie w zbiorze międzynarodowych oraz krajowych przepisów prawnych i norm. Zarządzanie cyberbezpieczeństwem struktur administracyjnych musi uwzględniać przepisy prawa. Część z tych przepisów jest obligatoryjna, inne natomiast mają formę zaleceń i dobrych praktyk.

3.2. Podstawy prawne, standaryzacja i polityka cyberbezpieczeństwa struktur administracyjnych

Prawo pełni różnorodne funkcje zarówno w stosunku do obywatela, jak jednostek sektora publicznego i prywatnego. Reguluje ono wiele sfer funkcjonowania państwa i społeczeństwa. Obok rozwiązywania problemów dogmatycznych, znaczenie szczegółowych nauk prawnych sprowadza się także do optymalizacji oddziaływania prawa na stosunki społeczne.

Przedsięwzięcia w zakresie bezpieczeństwa informacji muszą znaleźć odzwierciedlenie w systemie źródeł prawa. Zarówno w Polsce, jak i na świecie opracowuje się szereg aktów prawnych w omawianym obszarze. Niektóre przepisy są obligatoryjne, inne natomiast mają charakter norm i standardów. Przegląd zbioru polskiego prawa pozwala odnaleźć ponad 200 aktów prawnych dotyczących problematyki ochrony informacji. Również na szczeblu Unii Europejskiej, Rady Europy, NATO oraz w większości państw na świecie problematyka bezpieczeństwa cyberprzestrzeni stała się przedmiotem regulacji prawnych. Szczegółowa analiza podstaw prawnych bezpieczeństwa cyberprzestrzeni wykracza poza ramy niniejszego opracowania. W monografii wielokrotnie odwoływano się do ochrony prawnej cyberprzestrzeni, jednakże w tym miejscu warto usystematyzować obszary uregulowań prawnych dotyczących cyberbezpieczeństwa struktur administracyjnych.

Zakres norm prawnych oraz strategii związanych z cyberbezpieczeństwem jest rozległy i rozproszony w różnych gałęziach i dziedzinach prawa. W związku z tym przyjęto analizę systemu ochrony prawnej cyberprzestrzeni ze względu na obszar uregulowań. Zgodnie z przyjętym kryterium, na wysokim poziomie ogólności można wyróżnić uregulowania dotyczące następujących obszarów:

- ramy prawne bezpieczeństwa społeczeństwa informacyjnego, w których definiuje się strategię budowy społeczeństwa informacyjnego z uwzględnieniem zagrożeń w obszarze cyberprzestrzeni;
- uregulowania dotyczące ochrony bezpieczeństwa cyberprzestrzeni w wymiarze globalnym oraz narodowym, ze szczególnym uwzględnieniem ochrony infrastruktury krytycznej;
- przepisy odnoszące się do naruszeń bezpieczeństwa cyberprzestrzeni, w których klasyfikuje się przestępstwa komputerowe oraz określa instytucje i procedury związane ze ściganiem tych naruszeń;
- przepisy związane bezpośrednio z wdrożeniem elektronicznej administracji, w których określa się wymagania bezpieczeństwa;
- uregulowania dotyczące środków zabezpieczenia informatycznie przetwarzanych danych, które często mają formę norm i standardów oraz dobrych praktyk.

Należy zauważyć, że wymienione obszary często przenikają się wzajemnie. Ponadto jak już wspominano, uregulowania prawne można także klasyfikować ze względu na kryterium zasięgu – międzynarodowe, regionalne, krajowe, lokalne, oraz ze względu na moc obowiązywania – obligatoryjne i fakultatywne[8].

Do pierwszej z wymienionych grup można zaliczyć strategię na rzecz bezpiecznego społeczeństwa informacyjnego[9] opracowaną przez Komisję Europejską. W dokumencie zaprezentowano zintegrowane podejście do problematyki bezpieczeństwa społeczeństwa informacyjnego, obejmujące wszystkie zainteresowane podmioty i oparte na dialogu, partnerstwie i przejmowaniu inicjatywy[10]. Kolejnym dokumentem, o którym należy wspomnieć, jest europejska agenda cyfrowa[11], w którym podkreślono konieczność przeciwdziałania cyberprzestępczości, naruszeniu prywatności w sieci i danych osobowych. Ponadto zaproponowano rekomendacje na temat przeprowadzenia symulacji ataków cybernetycznych. W Polsce Strategia Rozwoju Kraju 2020[12] będąca elementem nowego systemu zarządzania rozwojem kraju czytamy, że *ważnym systemowym czynnikiem rozwoju będą korzyści – dla gospodarki, społeczeństwa i państwa – płynące ze zwiększonego i coraz efektywniejszego dostępu do zasobów teleinformatycznych i wykorzystania możliwości cyberprzestrzeni, przy zapewnieniu odpowiednio wysokiego poziomu bezpieczeństwa dla wszystkich jej użytkowników*[13]. Dostrzeżono zatem uzależnienie rozwoju kraju od rozwoju technologicznego oraz zapewnienia odpowiedniego poziomu bezpieczeństwa. Wyrazem tego jest także Program Zintegrowanej Informatyzacji Państwa[14], w którym wśród standardów tworzących warunki dla e-administracji wymieniono bezpieczeństwo teleinformatyczne oraz ochronę cyberprzestrzeni.

Z drugiej grupy uregulowań należy wymienić opracowaną przez USA Międzynarodową Strategię dla Cyberprzestrzeni[15]. *Nowa, opracowana we współpracy z 18 amerykańskimi departamentami i agencjami strategia nie jest dokumentem*

8 Szerzej na temat źródeł prawa: B. Banaszak, *Prawo konstytucyjne*, Warszawa 2012.

9 Komunikat Komisji do Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy", 31 maja 2006.

10 A. Suchorzewska, *Ochrona prawna systemów informatycznych...*, op. cit., s. 39.

11 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Europejska agenda cyfrowa", 19 maja 2010.

12 Strategia Rozwoju Kraju 2020. Aktywne społeczeństwo, konkurencyjna gospodarka, sprawne państwo, Warszawa, wrzesień 2012.

13 Strategia Rozwoju Kraju 2020..., op. cit., s. 14.

14 Program Zintegrowanej Informatyzacji Państwa, Warszawa, marzec 2013.

15 *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, May 2011, dostęp: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

technicznym i nie prezentuje gotowego rozwiązania, ale opisuje raczej wizję przyszłości cyberprzestrzeni, zaproponowaną przez prezydenta Baracka Obamę. Zawiera również propozycje działań, które mają pomóc w urzeczywistnieniu tej wizji[16]. Jest to pierwszy globalny dokument odnoszący się do ukierunkowanego rozwoju tego środowiska. Podkreślono, że cyberprzestrzeń jest wszechobecna, a jej funkcjonowanie musi wiązać się z zapewnieniem swobodnego przepływu informacji, bezpieczeństwem, ochroną prywatności i zapewnieniem integralności danych. Czynniki te mają fundamentalne znaczenie dla globalnej koniunktury gospodarczej. Na gruncie europejskim opracowano Europejską Strategię Bezpieczeństwa Cybernetycznego[17], która składa się z pięciu strategicznych priorytetów:

- osiągnięcie odporności w dziedzinie bezpieczeństwa cybernetycznego;
- radykalne ograniczenie cyberprzestępczości;
- opracowanie polityki obrony cybernetycznej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO);
- rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego;
- ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE.

W Polsce problematyka bezpieczeństwa cyberprzestrzeni znalazła odzwierciedlenie zarówno w Strategii Bezpieczeństwa Narodowego[18], jak i w Białej Księdze[19]. Szczególnie istotną rolę w omawianym obszarze odgrywa przywoływany Rządowy Program Ochrony Cyberprzestrzeni RP[20], który jednak nie został przy-

16 M. Grzelak, *Międzynarodowa strategia USA dla cyberprzestrzeni*, „Bezpieczenstwo Narodowe" nr II-2011, s. 140.

17 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.02.2013, dostęp: http://eeas. europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

18 Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

19 Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013.

20 Pierwotnie dokument został opracowany pod kierownictwem Radcy Ministra w Departamencie Ewidencji Państwowych i Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji. Po uzgodnieniach resortowych, międzyresortowych i społecznych podjęto decyzję o zmianie formy dokumentu na mający cechy polityki. Polityka Bezpieczeństwa Cyberprzestrzeni RP została w dniu 16 czerwca 2011 roku przyjęta przez Komitet Rady Ministrów z rekomendacją Radzie Ministrów. W wyniku wyborów parlamentarnych dokument nie został wniesiony pod obrady Rady Ministrów, w związku z czym nie został również zatwierdzony. Ostatecznie, decyzją Komitetu Rady Ministrów ds. Cyfryzacji, został powołany zespół ds. ochrony portali rządowych. W trakcie jego prac powstał dokument (bazujący na wyżej wskazanym o tej samej nazwie): Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Dokument został poddany uzgodnieniom międzyresortowym i społecznym i w dniu 25 czerwca 2013 roku został zatwierdzony przez Radę Ministrów.

jęty. Ostatecznie przyjęto dokument Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej oraz Doktrynę Cyberprzestrzeni RP.

Kolejna grupa przepisów odnosi się do uregulowania kwestii związanych z klasyfikacją czynów zabronionych w obszarze cyberprzestrzeni. Problematyka ta była przedmiotem szczegółowej analizy w rozdziale drugim, niemniej jednak w nawiązaniu do zaproponowanych obszarów uregulowań prawnych należy wymienić: Konwencję Rady Europy o zwalczaniu cyberprzestępczości, Komunikat Komisji Europejskiej – do Parlamentu Europejskiego, Rady i Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości oraz ustawę z dnia 6 czerwca 1997 roku Kodeks karny. Do tej grupy należą również przepisy odnoszące się do praw obywatelskich, związanych m.in. z ochroną prywatności, ochroną własności intelektualnej i praw autorskich.

Czwarta grupa określa wymagania bezpieczeństwa związane z wdrożeniem e-administracji. Na gruncie europejskim w deklaracji ministerialnej z Malmö zapisano, że *działania powinny bazować na zobowiązaniach w ramach legislacji krajowej i europejskiej, w szczególności dotyczących ochrony prywatności i danych osobowych oraz procedur administracyjnych. Działania te powinny również bazować i rozwijać istniejące inicjatywy na wszystkich szczeblach, uwzględniając wagę bezpieczeństwa informacji i sieci ponad granicami*[21]. W ramach deklaracji przyjęto Europejski Plan Działania na rzecz administracji elektronicznej. W Polsce wdrażanie bezpiecznych rozwiązań teleinformatycznych w sektorze publicznym zostało określone w dokumentach strategicznych i raportach, m.in. w przywoływanym już Programie Zintegrowanej Informatyzacji Państwa, w raporcie Państwo 2.0 – Nowy start dla e-administracji, a także w ustawach, m.in. w ustawie Prawo telekomunikacyjne, ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne, oraz wielu szczegółowych rozporządzeniach, m.in. rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 roku w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Przepisy prawne wyróżnione w tej grupie odnoszą się do bezpieczeństwa systemów teleinformatycznych stosowanych w administracji publicznej. Nie są one strategią (wizją), tylko zawierają praktyczne rozwiązania dotyczące implementacji w sektorze usług publicznych.

Ostatni punkt stanowią uregulowania dotyczące metod zabezpieczenia informatycznie przetwarzanych danych. Do aktów prawnych tego typu można zaliczyć m.in. rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

21 Pkt 7 deklaracji ministerialnej w sprawie administracji elektronicznej, Malmö, 18 listopada 2009.

Do tej grupy zalicza się także normy i standardy, które są szczególnie ważne na etapie wyboru zabezpieczeń, dlatego też zasługują na odrębną analizę.

Problematyka standaryzacji bezpieczeństwa systemów teleinformatycznych podlega ciągłej ewolucji[22]. K. Lidermann wyróżnia dwie grupy standardów z zakresu bezpieczeństwa teleinformatycznego[23]: standardy, na podstawie których można przeprowadzać certyfikacje systemów i produktów teleinformatycznych, np. ISO 15408 (*Common Criteria*), ITSEC[24], TCSEC[25]; oraz standardy stanowiące tzw. dobre praktyki[26], np. BS 77991.

A. Białas proponuje inną klasyfikację, w której wyróżnia dwa rodzaje standardów[27]:

- oficjalne, zwane standardami *de iure*, tworzone przez gremia standaryzacyjne, wśród których wyróżnia się:
  - międzynarodowe, np. ISO[28], IEC[29], ITU-T[30], ONZ;

22 Jako jedne z pierwszych standardów wymienia się najczęściej: 1) kryteria techniczno-technologiczne – skierowane na produkt – wywodzą się z USA i prac nad TCSEC (lata 1945–1983) dla potrzeb systemów informatycznych wojska i rządu; 2) kryteria organizacyjno-zarządcze – skierowane na system i zarządzanie systemem – wywodzą się z Wielkiej Brytanii i prac nad BS 7799 (lata 1993–1999) dla potrzeb środowiska biznesowego. Źródło: A. Wójcik, *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Część 1*, „Zabezpieczenia" nr 2/2008, s. 72.

23 K. Lidermann, *Standardy w ocenie bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" nr 17/2002, s. 99–100.

24 ITCES – zbiór kryteriów oceny bezpieczeństwa systemów teleinformatycznych wprowadzony w latach 90. XX w. Certyfikację według kryteriów ITSEC prowadzi w Polsce m.in. Jednostka Certyfikująca Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego. Po roku 2000 ITSEC jest stopniowo wypierane przez Common Criteria.

25 TSCEC – tzw. Orange Book, dokument powstały z inicjatywy Agencji Bezpieczeństwa Narodowego Departamentu Obrony USA oraz Narodowego Biura Standaryzacji. Wydany w 1983 roku w postaci pomarańczowej książeczki, której zawdzięcza swoją nieoficjalną nazwę. Dokument ten opisuje podstawowe wymagania, jakie muszą spełnić środki ochrony w systemie komputerowym do przetwarzania informacji podlegającej ochronie. Dokument został zaktualizowany w roku 1985, a następnie zastąpiony przez międzynarodowy standard Common Criteria.

26 Dobre praktyki, rozumiane jako powtarzalne stosowanie – z dobrym skutkiem, choć w różnych okolicznościach – rozwiązań praktycznych, są niczym innym jak odwołaniem się do pozytywnych doświadczeń. Źródło: M. Blim, *Teoria ochrony informacji...*, op. cit., s. 60.

27 A. Białas, *Bezpieczeństwo informacji i usług...*, op. cit., s. 45.

28 Międzynarodowa Organizacja Normalizacyjna, ang. *International Organization for Standardization.*

29 Międzynarodowa Komisja Elektrotechniczna, ang. *International Electrotechnical Commission.*

30 Sektor Normalizacji Telekomunikacji, ang. *International Telecommunication Union – Telecommunication Standardization Sector.*

– regionalne, np. CEN[31], ETSI[32], NAFTA[33], APEC[34];

– krajowe, np. ANSI[35], BSI[36], NIST[37] – publikujący normy FIPS[38], lub polski PKN[39] – publikujący polskie normy[40];

• pozostałe, w tym tzw. standardy *de facto*, obejmujące zalecenia firm, organizacji i stowarzyszeń branżowych, np. ISACA[41], lub obejmujące rozwiązania powszechnie stosowane, promowane przez różne firmy, które nie były dotąd przedmiotem prac oficjalnych organizacji standaryzacyjnych.

Szczególne znaczenie mają dokumenty dotyczące zarządzania bezpieczeństwem informacji, powstałe w wyniku współpracy Międzynarodowej Organizacji Normalizacyjnej (ISO) i Międzynarodowej Komisji Elektrotechnicznej (IEC). W wyniku działalności instytucji powstały standardy dotyczące: zarządzania bezpieczeństwem informacji i systemów teleinformatycznych, stosowania kryptografii i bezpieczeństwa sieciowego, oceny zabezpieczeń teleinformatycznych.

W praktyce konstruowanie bezpieczeństwa w instytucji często odnosi się do tzw. trójpoziomowego modelu odniesienia opracowanego przy współpracy ISO i IEC. Model ten jest szczególnie istotny z punktu widzenia kompleksowego ujęcia problematyki ochrony instytucji oraz przedstawia ogólną architekturę bezpieczeństwa. Budowany jest w oparciu o hierarchię celów instytucji, jej strategię oraz politykę (rys. 3.2).

31 Europejski Komitet Normalizacyjny, ang. *European Committee for Standardization.*

32 Europejski Instytut Norm Telekomunikacyjnych, ang. *European Telecommunications Standards Institute.*

33 Północnoamerykański Układ Wolnego Handlu lub Północnoamerykańska Strefa Wolnego Handlu, ang. *North American Free Trade Agreement.*

34 Wspólnota Gospodarcza Azji i Pacyfiku, ang. *Asia-Pacific Economic Co-operation.*

35 Amerykański Narodowy Instytut Normalizacyjny, ang. *American National Standards Institute.*

36 Brytyjski Instytut Normalizacyjny, ang. *British Standards Institution.*

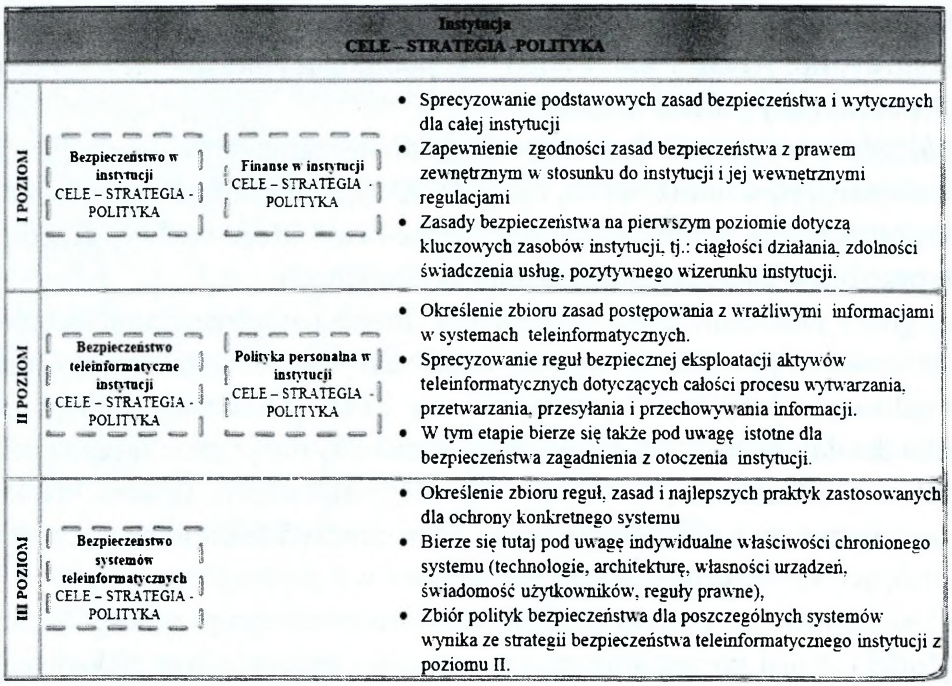
37 Instytut Standaryzacji i Technologii, ang. *National Institute of Standards and Technology.*

38 Federalny Standard Przetwarzania Informacji, ang. *Federal Information Processing Standard.*

39 Polski Komitet Normalizacyjny.

40 Do 31 grudnia 1993 roku stosowanie PN było obowiązkowe i pełniły one funkcję przepisów. Nieprzestrzeganie postanowień PN było naruszeniem prawa. Od 1 stycznia 1994 roku stosowanie PN jest dobrowolne, przy czym do 31 grudnia 2002 istniała możliwość, przez właściwych ministrów i w pewnych przypadkach, nakładania obowiązku stosowania PN. Od 1 stycznia 2003 stosowanie PN jest już całkowicie dobrowolne, z wyjątkiem działań wykonywanych ze środków publicznych, podlegających ustawie Prawo zamówień publicznych, która nakłada obowiązek ich uwzględnienia, oraz innych ustaw i rozporządzeń ministrów.

41 Międzynarodowe stowarzyszenie osób zajmujących się zawodowo zagadnieniami audytu, kontroli, bezpieczeństwa oraz innymi aspektami zarządzania systemami informatycznymi.



Opracowanie własne na podstawie: A. Białas, *Bezpieczeństwo informacji...*, op. cit., s. 166.

Rys. 3.2. Trójpoziomowy model odniesienia

Przywołany model opiera się na identyfikacji potrzeb wynikających z zadań realizowanych przez instytucję, jej systemów teleinformatycznych oraz struktury organizacyjnej. Takie podejście umożliwia uporządkowanie w sposób hierarchiczny kwestii prawnych, organizacyjnych, personalnych, technologicznych oraz fizycznych. Podstawowym dokumentem związanym z zarządzaniem bezpieczeństwem informacji w instytucji jest polityka bezpieczeństwa informacyjnego.

W Polskiej Normie PN-ISO/IEC 02000:2002, zawierającej terminologię stosowaną w technikach informatycznych, można znaleźć następujące definicje polityki bezpieczeństwa[42]:

- polityka bezpieczeństwa – plan lub sposób postępowania przyjęty w celu zapewnienia bezpieczeństwa systemu informatycznego;
- polityka bezpieczeństwa (polityka bezpieczeństwa systemu) – zestaw reguł określających wykorzystanie informacji, łącznie z jej przetwarzaniem, przechowywaniem, prezentacją i dystrybucją, niezależnie od wymagań dotyczących bezpieczeństwa i celów bezpieczeństwa;

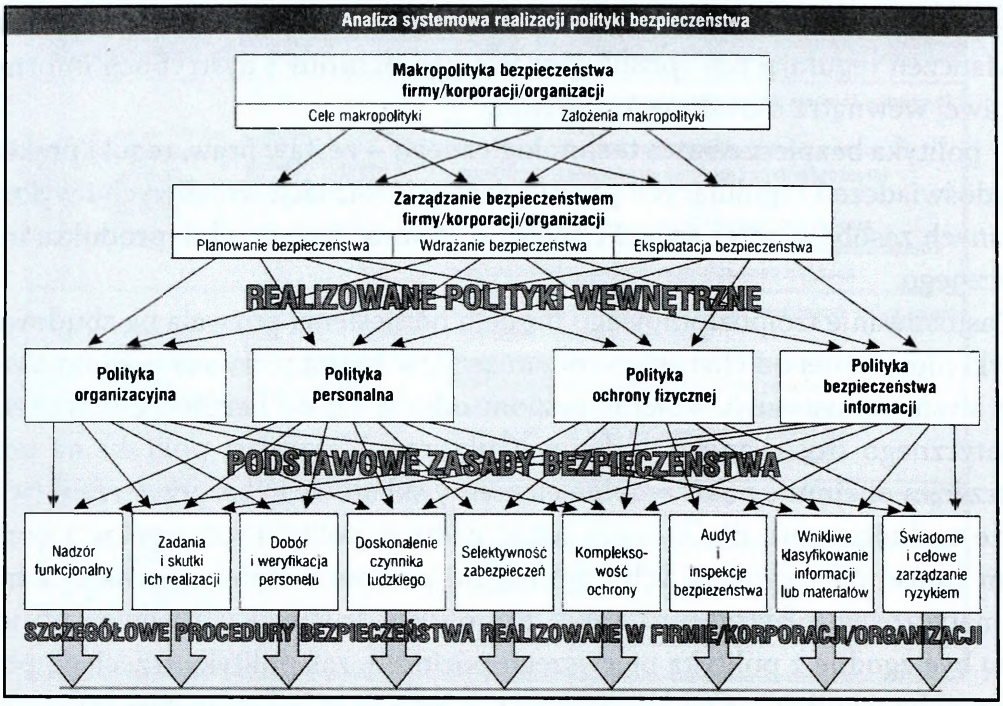
42 Norma PN-ISO/IEC 02000:2002 – Technika Informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia, Polski Komitet Normalizacyjny, Warszawa 2002; cyt za: T. Muliński, *Zagrożenia bezpieczeństwa...*, op. cit., s. 124.

- polityka bezpieczeństwa informacji – zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu;
- polityka bezpieczeństwa technologicznego – zestaw praw, reguł i praktycznych doświadczeń regulujących przetwarzanie informacji wrażliwych i wykorzystywanych zasobów przez sprzęt i oprogramowanie systemu lub produktu informatycznego.

Zastosowanie trójpoziomowego modelu odniesienia pozwala na zbudowanie polityki niezależnej od charakteru organizacji, w której pierwszy poziom określa cele i strategię instytucji. Kolejny poziom odnosi się do bezpieczeństwa teleinformatycznego stosowanego w danej strukturze. Natomiast polityka na poziomie trzecim obejmuje poszczególne elementy składowe cyberprzestrzeni (w wymiarze technicznym), dla których poziom drugi polityki jest ogólny i brakuje w nim zapisów zapewniających odpowiedni poziom bezpieczeństwa systemów informatycznych. Należy podkreślić, że polityki drugiego i trzeciego poziomu muszą być zgodne z polityką pierwszego poziomu, zaś polityka trzeciego poziomu powinna wynikać z polityki poziomu drugiego. Polityka bezpieczeństwa jest dokumentem spisanym, z którym powinni zapoznać się wszyscy pracownicy organizacji. Użytkownicy systemów ITC muszą rozumieć zapisy zawarte w polityce i przestrzegać ich[43]. Polityka bezpieczeństwa powinna być dostosowana do potrzeb urzędu. Działania prowadzone w ramach polityki bezpieczeństwa informacji powinny być prowadzone w racjonalny sposób tak, aby osiągnąć zamierzone cele, zminimalizować koszty i, jeżeli to możliwe, osiągnąć pewien stopień zwrotu poniesionych inwestycji[44]. Polityka bezpieczeństwa stanowi podstawę do zarządzania bezpieczeństwem struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa. Na podstawie określonych w niej zasad buduje się i utrzymuje procesy zarządzania. Dokument ten określa sposoby wykorzystania metod oraz środków, dostępnych narzędzi i zgromadzonych danych w celu przeciwdziałania zagrożeniom bezpieczeństwa. Polityka bezpieczeństwa powinna być dokumentem spinającym uregulowania odnoszące się do poszczególnych polityk wewnętrznych oraz zasad bezpieczeństwa (rys. 3.3).

43 M. Molski, M. Łacheta, *Bezpieczeństwo i audyt systemów informatycznych*, Bydgoszcz 2009, s. 47.

44 K. Lisiecka, T. Papaj, *Bezpieczeństwo informacji w urzędach terytorialnej administracji publicznej* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007, s. 109.



Źródło: M. Blim, *Teoria ochrony informacji. Część 1*..., op. cit., s. 59.

Rys. 3.3. Makropolityka bezpieczeństwa jako strategia wieloetapowego i wielopoziomowego działania

Jednostki administracji publicznej w Polsce zostały zobligowane do opracowania polityki bezpieczeństwa na mocy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Rozporządzenie MSWiA określa minimalne wymagania, które powinna zawierać polityka:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- opis struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- sposób przepływu danych pomiędzy poszczególnymi systemami;
- określenie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Przywołane rozporządzenie w sposób minimalistyczny wymienia elementy w polityce bezpieczeństwa, dlatego zasadne jest sięgnięcie do Polskiej Normy PN-ISO/IEC 17799:2005, która wskazuje, jakie niezbędne zapisy powinny być za-

warte w polityce. Powyższe wymagania zostały opisane także przez Generalnego Inspektora Danych Osobowych w opracowanych przez niego wytycznych[45].

Odnosząc powyższe rozważna do wdrożonych polityk bezpieczeństwa w instytucjach publicznych, wykorzystano wyszukiwarkę Google i zastosowano popularne filtry wyszukiwania[46] (tab. 3.2).

Tab. 3.2. Dostępność w Internecie pojęcia „polityka bezpieczeństwa informacji" (na dzień 1.10.2014)

Poszukiwany ciąg znaków	Liczba wyników[a)]		Filtr
	wyszukiwania	dostępnych	
Polityka bezpieczeństwa informacji	2 990 000	446	brak
„Polityka bezpieczeństwa informacji"	243 000	310	brak
„Polityka bezpieczeństwa informacji"	21 100	248	filetype:pdf
„Polityka bezpieczeństwa informacji"	19 500	233	site:pl filetype:pdf
„Polityka bezpieczeństwa informacji"	2 320	76	site:gov.pl filetype:pdf
„Polityka bezpieczeństwa informacji"	74	15	site:eu filetype:pdf
„Polityka bezpieczeństwa informacji"	2 220	34	filetype:doc
„Polityka bezpieczeństwa informacji"	1 930	33	site:pl filetype:doc
„Polityka bezpieczeństwa informacji"	77	22	site:gov.pl filetype:doc
„Polityka bezpieczeństwa informacji"	1	1	filetype:doc

a) Wyszukiwarka Google pokazuje znacznie większą liczbę wyników wyszukiwania, lecz jedynie niewielka część wyników jest możliwa do przejrzenia.

Opracowanie własne na podstawie: M. Muliński, *Zagrożenia bezpieczeństwa*..., op. cit., s. 128.

Powyższa tabela przedstawia dostępność sformułowania *polityka bezpieczeństwa informacji*. Zastosowanie filtrów wyszukiwania umożliwiło wyszukanie udostępnionych polityk bezpieczeństwa informacji przez administrację publiczną. Analiza otrzymanych wyników dowodzi, że opracowane polityki nie zawsze uwzględniają wytyczne rozporządzenia MSWiA. Można wyróżnić dokumenty:

- krótkie i lakoniczne (np. Centralne Biuro Antykorupcyjne, Ministerstwo Sprawiedliwości);
- niespełniające wszystkich wytycznych rozporządzenia MSWiA (np. Wojskowy Instytut Medycyny Lotniczej, Świętokrzyski Urząd Wojewódzki w Kielcach);
- zgodne z wytycznymi MSWiA (np. Urząd Gminy Podegrodzie, Urząd Marszałkowski Województwa Lubelskiego).

45 Zob. opracowanie Biura GIODO – A. Kaczmarek, *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Warszawa 2007.

46 Zastosowano filtry filetype:pdf (format pliku Adobe Acrobat Document) i filetype: doc (format pliku Microsoft Word) oraz filtry site:pl (polska domena internetowa), site:gov. pl (domena internetowa polskich organizacji rządowych), site:eu (domena internetowa Unii Europejskiej).

3.3. System Zarządzania Bezpieczeństwem Informacji

Bezpieczeństwo cyberprzestrzeni w instytucjach sektora publicznego budowane jest w oparciu o politykę bezpieczeństwa informacji oraz instrukcję zarządzania system informatycznym. Elementem scalającym te elementy jest System Zarządzania Bezpieczeństwem Informacji (SZBI), który definiuje się jako: *część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanowienia, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji*[47]. Wdrażanie SZBI jest zatem złożonym procesem, którego podstawowym elementem jest zarządzanie ryzykiem.

Krajowe Ramy Interoperacyjności nakładają na podmioty publiczne obowiązek opracowania, ustanowienia, wdrożenia, eksploatacji oraz doskonalenia SZBI[48]. W przywołanym dokumencie określono sposób współpracy systemów informatycznych stosowanych w jednostkach sektora publicznego oraz zawarto wytyczne dotyczące bezpieczeństwa informatycznego odwołującego się bezpośrednio do norm PN-ISO/IEC 20000[49] oraz PN-ISO/IEC 27000[50]. Zatem jednostki administracji są zobowiązane do zastosowywania wymagań zawartych w rozporządzeniu[51]. W praktyce oznacza to, że przywołane normy stały się obowiązujące dla systemów zarządzania bezpieczeństwem informacji oraz e-usługami w stosunku do podmiotów realizujących zadania publiczne.

47 PN ISO/IEC 270001..., op. cit., cyt. za: B. Szomański, *Zarządzanie bezpieczeństwem informacji...*, op. cit., s. 63.

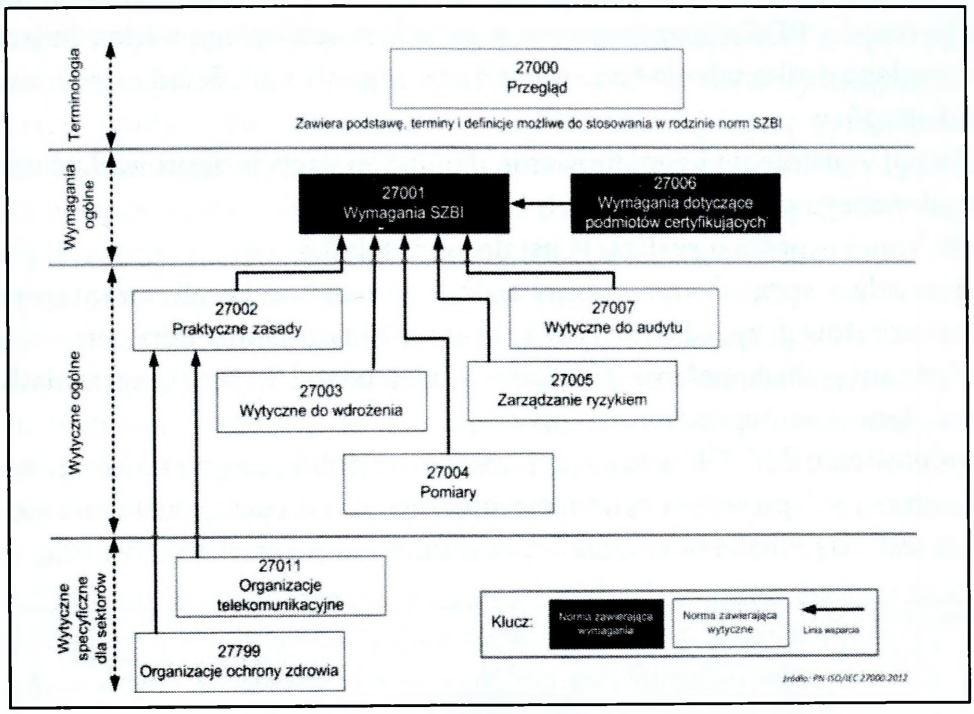
48 § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów informatycznych.

49 PN-ISO/IEC 20000-1:2014-01 Technika informatyczna – Zarządzanie usługami – Część 1: Wymagania dla systemu zarządzania usługami, i PN-ISO/IEC 20000-2:2007 – Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania.

50 PN-ISO/IEC 27000:2012 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia.

51 W przepisach końcowych określono termin obligatoryjnego dostosowania funkcjonowania jednostek publicznych do wymogów określonych w rozporządzeniu: 1) systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań określonych w § 19 (wymagania WCAG 2.0 z uwzględnieniem poziomu AA) nie później niż w ciągu 3 lat od dnia wejścia w życie rozporządzenia; 2) systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów należy dostosować do wymagań określonych w rozdziale IV rozrządzania(*Minimalne wymagania dla systemów informatycznych*) nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia.

Polska Norma PN-ISO/IEC 27000 wprowadza pojęcie rodziny norm, oznaczające zbiór norm odnoszących się do organizacji zarządzania bezpieczeństwem informacji (rys. 3.4).



Źródło: E. Andrukiewicz, *Norma PN-ISO/IEC 27000:2012 Technika informatyczna – Techniki bezpieczeństwa – System zarządzania bezpieczeństwem informacji – Przegląd i terminologia*, „Wiadomości PKN" nr 9/2012, s. 8.

Rys. 3.4. Relacje w ramach rodziny norm SZBI

Istotą funkcjonowania SZBI jest zapewnienie bezpiecznego i efektywnego funkcjonowania oraz eliminacja potencjalnych zagrożeń. Ustanowienie i zarządzanie SZBI powinno obejmować następujące działania[52]:

- zdefiniowanie zakresu i granic systemu przy uwzględnieniu charakterystyki prowadzonej działalności, organizacji, lokalizacji, aktyw i technologii wraz z dokładnym opisem oraz uzasadnieniem każdego wyłączenia z zakresu;
- zdefiniowanie polityki SZBI;
- określenie ryzyka;
- analizę i ocenę ryzyka;
- zdefiniowanie i ocenę wariantów postępowania z ryzykiem;
- wybór zabezpieczeń;
- uzyskanie akceptacji kierownictwa dla proponowanych ryzyk szczątkowych;

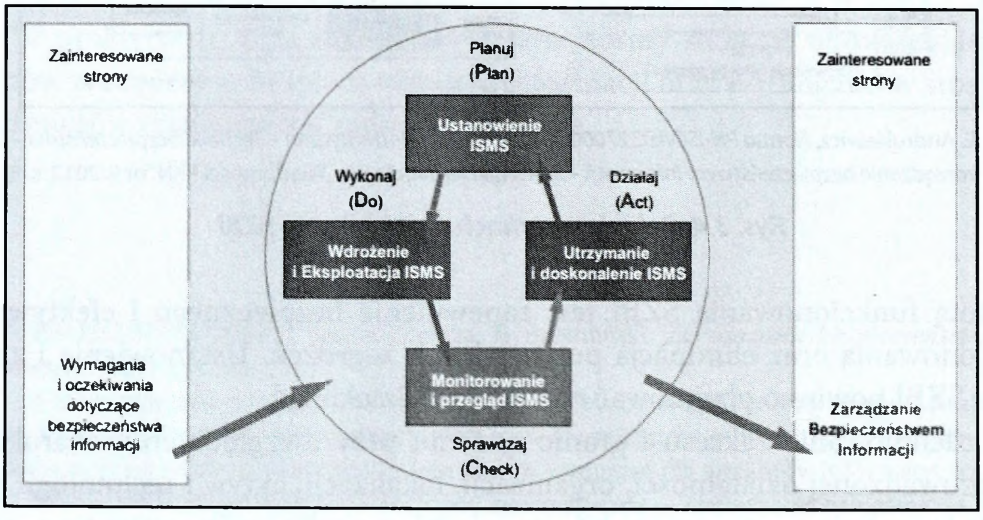
52 A. Wysokińska-Senkus, P. Senkus, *Systemy zarządzania w świetle nowych wyzwań. Bezpieczeństwo, informacja, integracja, model doskonalenia*, Warszawa 2013, s. 123–124.

- uzyskanie autoryzacji do wdrażania i eksploatacji SZBI;
- przygotowanie deklaracji stosowania (dokument opisujący, jakie zabezpieczenia posiada instytucja, który powinien być szczególnie chroniony).

W normach dotyczących SZBI w całej strukturze procesów zastosowano cykl Deminga (model PDCA), opracowany w latach 50. ubiegłego wieku, ilustrujący proces ciągłego doskonalenia firmy (instytucji, organizacji). Składa się on z następujących etapów:

- Planuj – ustalenie i zaplanowanie działań mających doprowadzić do uzyskania założonego celu;
- Wykonuj – próbna realizacja ustalonych działań;
- Sprawdź – sprawdzenie poprawności i skuteczności realizowanego procesu oraz rezultatów przy jednoczesnej analizie możliwości doskonalenia;
- Zastosuj – doskonalenie procesów i działalności, które się sprawdziły, lub poprawa błędów w niepoprawnym procesie.

W odniesieniu do SZBI w instytucjach sektora publicznego model ten stanowi cykl następujących po sobie czynności zmierzających do osiągnięcia celu głównego, jakim jest osiągniecie bezpieczeństwa informacji w instytucji (rys. 3.5).



Źródło: A. Wójcik, *Model PDCA w procesach SZBI (ISMS)*, „Zabezpieczenia" nr 6/2008, s. 70.

Rys. 3.5. Model PDCA stosowany w procesach SZBI (ang. ISMS)

Istotna w zarządzaniu bezpieczeństwem informacji jest kwestia zarządzania ryzykiem, która odnoszona jest do: 1) minimalizacji lub redukcji negatywnych skutków pojawiającego się ryzyka w różnych obszarach działalności organizacji; 2) szukania szans rozwoju dzięki przedsięwzięciom podejmowanym w sferach

podwyższonego ryzyka[53]. Zarządzanie ryzykiem opiera się na kilku etapach: analiza ryzyka, opracowanie planu postępowania ryzykiem oraz akceptacji ryzyka szczątkowego.

SZBI powinien zapewniać także informacyjną ciągłość działania, za pomocą przedsięwzięć organizacyjnych i technicznych. Do pierwszej grupy zalicza się m.in. wdrożone plany zapewnienia ciągłości działania, przećwiczoną kryzysową organizację pracy, szkolenia, właściwą eksploatację (sprzętu, oprogramowania i obiektów infrastruktury), użytkowanie sprzętu i oprogramowania spełniającego odpowiednie standardy jakości. Grupa działań technicznych obejmuje: kopie bezpieczeństwa, system kontroli dostępu (fizycznego i logicznego), ośrodek zapasowy (przetwarzania danych, biznesowy), rezerwę sprzętową (komputery i urządzenia sieciowe), zapasową infrastrukturę usługową (łącza, zasilanie, łączność, woda, gaz)[54]. Informacyjna ciągłość działania jest zbiorem działań jakie, podejmuje instytucja publiczna w celu zapewnienia użytkownikom dostępności jej usług w przypadku wystąpienia zagrożenia (sytuacji kryzysowej). Jest to proces mający na celu zapobieganie sytuacji awaryjnej oraz utrzymanie gotowości do reakcji, gdyby taka sytuacja zaistniała.

Zachowaniu bezpieczeństwa informacji nie sprzyja brak świadomości znaczenia informacji oraz brak standardów i zasad przekazywania informacji. Błędy w zabezpieczeniu informacji mogą spowodować ogromne straty w działalności każdej organizacji[55]. Dlatego też istotną częścią SZBI są szkolenia pracowników, mające na celu podnoszenie świadomości o zagrożeniach, ich wpływie na funkcjonowanie instytucji oraz o odpowiedzialności prawnej. Ponadto obowiązkowym szkoleniem powinny być objęte zasady funkcjonowania SZBI.

Ważną kwestią przy tworzeniu i utrzymaniu SZBI jest odpowiedzialność kierownictwa. Zgodnie z wymaganiami normy, najważniejsze kierownictwo powinno nieustannie angażować się w doskonalenie systemu, monitorować realizację założonych celów i zadań, określić odpowiedzialność poszczególnych pracowników w odniesieniu do bezpieczeństwa informacji, przeprowadzać przeglądy oraz zapewniać niezbędne zasoby[56]. Koniecznym warunkiem powodzenia wdrożonych rozwiązań jest ciągłe doskonalenie, mające na celu podejmowanie działań korygujących oraz eliminowanie niezgodności.

Norma PN-ISO/IEC umożliwia budowę zintegrowanego systemu zarządzania bezpieczeństwem informacji z system zarządzania jakością zgodnym ze standardem

53 P. Sienkiewicz (red.), *Zarządzanie ryzykiem w sytuacjach kryzysowych*, AON, Warszawa 2006, s. 47.

54 K. Liderman, *Bezpieczeństwo informacyjne...*, op. cit., s. 158.

55 R. Borowiecki, M. Kwieciński, *Informacja i wiedza w zintegrowanym systemie zarządzania*, Kraków 2004, s. 25.

56 A. Wysokińska-Senkus, P. Senkus, *Systemy zarządzania...*, op. cit., s. 125.

ISO 9001:2000, który dość powszechnie wdrażany jest w jednostkach sektora publicznego. Obie normy zawierają liczne podobieństwa i wspólne elementy, które ułatwiają integrację systemu zarządzania jakością i systemu zarządzania bezpieczeństwem informacji.

Praktyczne wdrożenie zintegrowanych systemów przynosi organizacji wiele korzyści, do których według B. Szomańskiego należą przede wszystkim[57]:

- jednolite zasady przeprowadzania audytów;
- jednolita podstawowa terminologia i dokumentacja;
- usprawnienie zarządzania organizacją (informacją i jakością) oraz standaryzacja pracy w sytuacjach kryzysowych – odpowiedzialność i uprawnienia są jednoznaczne, pracownicy znają wagę przetwarzanych informacji (znaczenie jakości), zapobiega się nieświadomym zachowaniom pracowników, mającym negatywny wpływ na funkcjonowanie, bezpieczeństwo i wizerunek organizacji;
- niższe koszty funkcjonowania zintegrowanego systemu zarządzania;
- objęcie systemem całej sfery działalności instytucji, w tym np. księgowości, ochrony fizycznej, sieci teleinformatycznych itp.;
- prosta i przejrzysta dokumentacja;
- prowadzenie analizy ryzyka i zarządzanie ryzykiem;
- redukcja ryzyka utraty kontroli nad bezpieczeństwem informacji;
- rozwój planowania jako elementu zapewnienia ciągłości działania organizacji;
- wdrożony system jako element zwiększający konkurencyjność w marketingu wyrobu/usługi;
- zapewnienie, że odpowiednie i kompletne informacje trafią do upoważnionych osób;
- zastosowanie podejścia procesowego, ciągłego doskonalenia jako podstawy funkcjonowania organizacji;
- zwrócenie uwagi na znaczenie jakości i informacji jako ważnej wartości w organizacji.

3.4. Zarządzanie ryzykiem

Bezpieczeństwo struktur administracyjnych budowane w oparciu o politykę bezpieczeństwa oraz SZBI, wymaga wdrożenia zarządzania ryzykiem z uwzględnie-

57 B. Szomański, *Systemy zarządzania bezpieczeństwem informacji – założenia i projektowanie*, „Problemy jakości" 2004, nr 4, cyt. za: J. Radwan, *Zarządzanie bezpieczeństwem informacji w świetle wymagań normy ISO 9001: 2000* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, Bielsko-Biała 2007, s. 95.

niem PN-ISO/IEC 27001:2007[58] oraz norm z nią związanych[59]. *Zarządzanie ryzykiem jest podstawowym elementem profesjonalnego podejścia do bezpieczeństwa informacji i stanowi kluczowy element SZBI*[60]. Proces ten odgrywa zatem znaczącą rolę w procesie zapewnienia bezpieczeństwa jednostek sektora publicznego.

Ryzyko jest pojęciem wieloznacznym i różnie klasyfikowanym. P. Sienkiewicz definiuje je jako *szczególną relację między czynnikiem zewnętrznym (źródłem zagrożeń) a podmiotem (obiektem zagrożeń) o określonej wartości i podatności na zagrożenia (lub inne czynniki wpływające na obniżenie albo całkowitą utratę wartości). Wartością mogą być oczekiwane korzyści (zysk, użyteczność) podmiotu (obiektu), jednakże zagrożenia powodują, że korzyści te mogą być niższe niż oczekiwane lub mogą wystąpić po prostu straty*[61]. Natomiast w Polskiej Normie ryzyko jest prawdopodobieństwem określającym możliwość wykorzystania określonej podatności przez dane zagrożenie w celu spowodowania straty lub zniszczenia zasobu albo grupy zasobów, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na instytucję[62]. Ryzyko odnosi się zatem do niepewności wystąpienia niepożądanego zdarzenia i stanowi immanentną cechę sytuacji decyzyjnych, w których istnieje konieczność wyboru między alternatywnymi wariantami działania, zaś dla możliwych ich skutków brane są pod uwagę prawdopodobieństwa ich wystąpienia. W takich sytuacjach mówi się o ryzyku dobrowolnym, będącym przedmiotem teorii decyzji[63]. W tym sensie ryzyko odnoszone jest do wyboru (decyzji).

Liczne klasyfikacje i typologie ryzyka wyróżniają następujące jego odmiany: ekonomiczne (gospodarcze, inwestycyjne), polityczne, prawne, produkcyjne (handlowe, rynkowe), logistyczne, finansowe, kredytowe, organizacyjne, ekologiczne, technologiczne (przemysłowe, chemiczne), transportowe (komunikacyjne),

58 Wcześniejsza wersja normy to PN-I-07799-2:2005 – Systemy zarządzania bezpieczeństwem informacji – polskie tłumaczenie normy ISO/IEC 17799 (wcześniej znanej jako brytyjska norma BS7799-2). 4 stycznia 2007 roku opublikowano normę PN-ISO/IEC 27001:2007, która ją zastępuje.

59 PN-ISO/IEC 27005 – Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji; PN-ISO/IEC 24762 – Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.

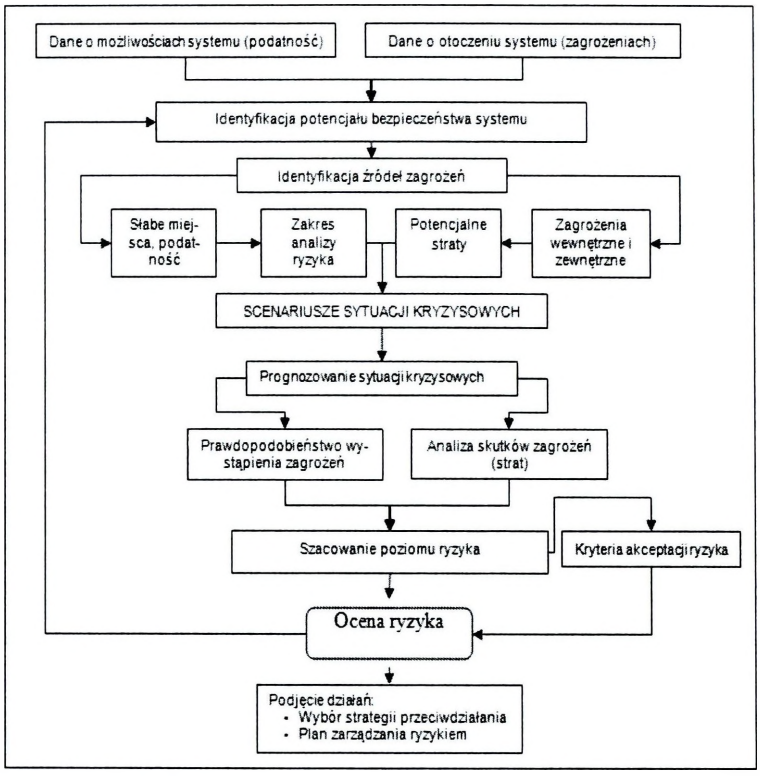
60 A. Guzik, *Ryzyko w bezpieczeństwie informacji...*, op. cit., s. 72.

61 P. Sienkiewicz, *25 wykładów...*, op. cit., s. 351.

62 Polska Norma PN-I-13335-1:1999 *Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, Warszawa 1999 [cyt. za:] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008, s. 70.

63 P. Sienkiewicz, H. Świeboda, *Efektywność i niezawodność organizacji sieciowej, Tom II – Metody oceny efektywności, niezawodności i bezpieczeństwa organizacji sieciowej*, Warszawa 2010, s. 61.

informacyjne, medyczne i epidemiologiczne, farmaceutyczne, zdrowotne, psychologiczne, socjologiczne, kulturowe itp. Wyróżnionym wyżej przedmiotowym odmianom ryzyka bez trudu można przyporządkować odpowiadające im odmiany bezpieczeństwa odpowiednich obiektów[64]. Niezależnie od przeznaczenia instytucji, analiza ryzyka przebiega według uniwersalnego schematu (rys. 3.6).



Źródło: P. Sienkiewicz (red.), *Zarządzanie ryzykiem w sytuacjach kryzysowych*, Warszawa 2006, s. 43 [cyt. za:] H. Świeboda, *Zagrożenia informacyjne bezpieczeństwa RP...*, op. cit., s. 196.

Rys. 3.6. Model oceny ryzyka w sytuacjach kryzysowych

Istnieje wiele metodyk zarządzania ryzykiem. Przykładowo amerykański rządowy instytut NIST[65] opracował metodykę zarządzania ryzykiem[66], w której zwrócił uwagę, że proces ten służy przede wszystkim instytucji i realizowanej przez nią misji. Metodyka NIST jest stosowana w wielu instytucjach prywatnych i publicznych na świecie. W Polsce jednostki sektora publicznego zostały zobligowane do stosowania w tym zakresie Polskich Norm.

64 P. Sienkiewicz, *25 wykładów...*, op. cit., s. 351.

65 Instytut Standaryzacji i Technologii, ang. *National Institute of Standards and Technology.*

66 Zob. G. Stoneburner, A. Goguen, A. Feringa, *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*, NIST, July 2002, dostęp: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Dla osoby zajmującej się ryzykiem w instytucji publicznej ryzyko związane z bezpieczeństwem teleinformatycznym będzie jednym z wielu ryzyk mogących mieć wpływ na realizację misji struktur administracyjnej. Należy bowiem pamiętać, że usługi publiczne obejmują nie tylko usługi administracyjne. Natomiast dla osoby odpowiedzialnej za bezpieczeństwo teleinformatyczne ryzyko związane z przetwarzaniem informacji w systemach teleinformatycznych i bezpieczeństwem e-usług jest najważniejsze i ma wpływ na zarządzanie ryzykiem.

K. Liderman podkreśla, że gdy mowa jest o analizie ryzyka w kontekście bezpieczeństwa teleinformatycznego, należy mieć na uwadze związki takiej analizy z analizą ryzyka biznesowego firmy oraz zależności i zakresy odpowiedzialności pomiędzy osobami zaangażowanymi w ocenę (i zarządzanie) ryzyka biznesowego firmy i ryzyka związanego z bezpieczeństwem informacji przetwarzanych, przesyłanych i przechowywanych w firmowych systemach teleinformatycznych[67]. Odnosząc powyższe rozważania do bezpieczeństwa struktur administracyjnych, za cele zarządzania ryzykiem można uznać:

- wykazanie, których ryzyk i w jaki sposób można uniknąć, stosując rozwiązania organizacyjne, techniczne i proceduralne w zakresie zapewnienia bezpieczeństwa informacji i usług;
- zminimalizowanie ryzyka szczątkowego[68] tak, aby stało się ryzykiem akceptowalnym;
- zapewnienie optymalnego, ze względu na koszty i ograniczenia, stanu ochrony informacji i usług.

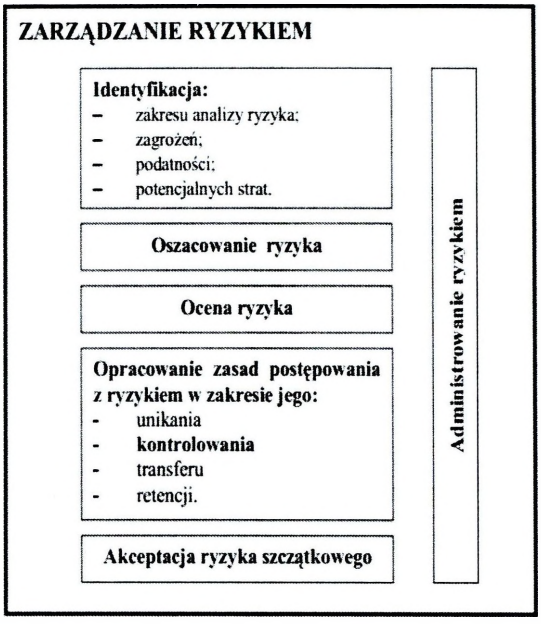
W tym kontekście można wyróżnić kilka etapów etapy zarządzania ryzykiem (rys. 3.7).

Zgodnie z rysunkiem czynności zmierzające do identyfikacji zakresu, zagrożeń, podatności i potencjalnych strat oraz oszacowania i oceny ryzyka nazywane są analizą ryzyka. Natomiast wynikiem rozpoznania zagrożeń i środowiska (podatności i wymagań) jest opisanie ryzyka, tzn. przedstawienie cech zagrożeń w sposób strukturalny oraz pozwalający na ich porównanie.

Wstępną czynnością analityczną w analizie ryzyka jest identyfikacja zagrożeń i podatności. W przypadku obiektów mających szczególne znaczenie należy także przeprowadzić analizę otoczenia instytucji, ma to bowiem istotne znaczenie w przypadku rozprzestrzeniania się ryzyka (efekt domina).

67 K. Liderman, *Zarządzanie ryzykiem jako element zapewniania odpowiedniego poziomu bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" nr 23, 2006, s. 44–45.

68 Ryzyko szczątkowe – ryzyko pozostające po wprowadzeniu mechanizmu zabezpieczenia.



Źródło: K. Liderman, *Zarządzanie ryzykiem jako element zapewniania odpowiedniego poziomu bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" nr 23, 2006, s. 49.

Rys. 3.7. Podstawowe elementy procesu zarządzania ryzykiem

Zagrożenia struktur administracyjnych na potrzeby zarządzania ryzykiem z punktu widzenia realizacji misji można przyporządkować do następujących grup[69]:

- strategiczne, wpływające na długoterminowe cele struktur administracyjnych;
- operacyjne, wpływające na krótkoterminowe cele struktur administracyjnych;
- finansowe, związane z bezpośrednimi działaniami finansowymi struktur administracyjnych;
- informacyjne, wpływające na bezpieczeństwo zbiorów informacji, zgodności, wpływające na utrzymanie zgodności z obowiązującymi przepisami prawa.

Identyfikując zagrożenia dla bezpieczeństwa cyberprzestrzeni struktur administracyjnych na potrzeby zarządzania ryzykiem przyjęto klasyfikację zagrożeń zaproponowaną w rozdziale drugim. Ujęcie zagrożeń w formie tabelarycznej umożliwia powiązanie zasobów instytucji publicznej z podatnościami oraz skutkiem na bezpieczeństwo – atrybuty bezpieczeństwa informacji i usług (tab. 3.3).

69 K. Liderman, *Zarządzanie ryzykiem...*, op. cit., s. 49.

Tab. 3.3. Przykład analizy zagrożeń dla cyberbezpieczeństwa struktur administracyjnych na potrzeby zarządzania ryzykiem

Grupa zagrożeń	Przykłady zagrożeń	Przykład zagrożonego zasobu	Podatność	Skutek	ID
Katastrofy naturalne	Powodzie, pożary, trzęsienia ziemi	Budynek	Uwarunkowania naturalne	Dostępność, integralność, niezawodność	Z_1
Działania nieuprawnione i przestępcze	Cyberszpiegostwo	Baza danych	Wykorzystanie luk w systemie operacyjnym, brak programów antywirusowych – wykorzystanie programów szpiegujących	Poufność	Z_2
	Cyberterroryzm	System komputerowy, sieć teleinformatyczna, aplikacje uwierzytelniania	Ataki na urządzenia firewall, wykorzystanie błędów oprogramowania, wykorzystanie luk w systemie operacyjnym, przełamanie zabezpieczeń	Poufność, integralność, rozliczalność, autentyczność, dostępność, niezawodność	Z_3
	Haking	Sieć komputerowa	Wykorzystanie błędów oprogramowania, wykorzystanie luk w systemie operacyjnym	Poufność	Z_4
	Nieuprawnione działania personelu	Bazy danych, sieci komputowe, urządzenia, nośniki danych	Nieprawidłowy dobór personelu, kradzież urządzeń, nośników danych	Integralność, poufność	Z_5
Błędy personelu i zła organizacja pracy	Udostępnianie haseł	Sieć komputerowa, bazy danych	Niedbalstwo, brak świadomości i szkoleń	Autentyczność, rozliczalność	Z_6
	Brak programów antywirusowych	Bazy danych	Zaniedbanie ze strony administratora, możliwość wykorzystania braku zabezpieczeń przez aktorów zagrożeń	Poufność, integralność, dostępność, niezawodność	Z_7
Awarie i uszkodzenia sprzętu, wady software	Awarie zasilania sieci informatycznej	Zasilenie systemu informatycznego	Brak zastosowania zasilaczy awaryjnych niwelujących nieprawidłowości sieci elektrycznej	Dostępność, niezawodność	Z_8

Opracowanie własne.

Przechodząc do analizy ryzyka, konieczne jest określenie możliwości wystąpienia zagrożeń. Metod szacowania ryzyka jest wiele i ogólnie można je podzielić na:

- jakościowe – polegają na ocenie przez ekspertów zagrożeń poziomu ryzyka i wynikających z nich ewentualnych strat, a wyniki otrzymuje się w postaci opisowej, np. metoda HAZOP;
- ilościowe – w ramach których próbuje się skwantyfikować i wyrazić liczbowo, na podstawie danych statystycznych, poziom występujących ryzyk, np. metoda Courtneya, modele Markowa;
- ilościowo-jakościowe – które łączą w sobie elementy dwóch poprzednich grup, np. metoda FMEA.

Ryzyko określa się jako uporządkowaną trójkę:

$$R \equiv (S, P, C)$$

gdzie:
S – scenariusz sytuacji, zwykle opisany jako ciąg następujących po sobie zdarzeń,
P – prawdopodobieństw zajścia S,
C – odpowiednia miara skutków (strat) wywołanych przez S[70].

Wobec powyższego szacowanie poziomu ryzyka następuje na podstawie iloczynu P –prawdopodobieństwa zajścia zagrożenia (przez wykorzystanie podatności) i C – strat określenia podatności:

$$R = P \times C$$

Odwołując się do identyfikacji zagrożeń (tab. 3.3) i metodyki NIST, która umożliwia wyrażenie następstw w sposób jakościowy i ilościowy[71], można wyróżnić poziomy prawdopodobieństwa zagrożeń, związane z prawdopodobieństwem wystąpienia podatności. A. Białas zaleca stosowanie nieparzystej liczby poziomów zagrożeń, gdyż ułatwia to zdefiniowanie równomiernego podziału na poziomy ryzyka[72], dlatego wyróżniono trzy poziomy prawdopodobieństwa (P):

- wysokie (1) – czynnik sprawczy o wysokiej motywacji i potencjale rażenia, a zabezpieczenia przed wykorzystaniem podatności są niewystarczające;
- średnie (0,5) – czynnik sprawczy posiada motywację i możliwości realizacji, ale zabezpieczenia są w stanie przeciwstawić się wykorzystaniu podatności;
- niskie (0,1) – czynnik sprawczy nie ma motywacji lub wystarczającego potencjału, albo zabezpieczenia były skuteczne.

70 P. Sienkiewicz, *25 wykładów...*, op. cit., s. 359.
71 Szerzej na temat metodyki NIST Zob. A. Białas, *Bezpieczeństwo informacji i usług...*, op. cit., s. 108–117.
72 A. Białas, *Bezpieczeństwo informacji i usług...*, op. cit., s. 35.

Podobną skalę należy stosować przy określaniu skutków (S):

- wysokie (100) – wykorzystanie podatności może spowodować najwyższe możliwe straty dla zasobów i usług krytycznych oraz może zakłócić ciągłość działania funkcjonowania instytucji publicznej i realizację jej misji;
- średnie (50) – wykorzystanie podatności może spowodować duże straty dla zasobów i usług krytycznych oraz może w istotny (zauważalny) sposób zakłócić realizację celów instytucji;
- niskie (10) – wykorzystanie podatności może spowodować stratę niektórych zasobów, ale nie wpływa w znaczący sposób na realizację misji instytucji – ciągłość działania jest zachowana.

W oparciu o ustalone poziomy prawdopodobieństwa (P) i skutków (S) można zbudować macierz poziomu ryzyka (tab. 3.4).

Tab. 3.4. Przykład macierzy poziomu ryzyka do określonego prawdopodobieństwa oraz skutków

		(S)		
		Niskie (10)	**Średnie (50)**	**Wysokie (100)**
(P)	**Niskie (0,1)**	0,1 X 10 = 1	0,1 X 50 = 5	0,1 X 100 = 10
	Średnie (0,5)	0,5 X 10 = 5	0,5 X 50 = 25	0,5 X 100 = 50
	Wysokie (1)	1 X 10 = 10	1 X 50 = 50	1 X 100 = 100

Opracowanie własne.

W tabeli uzyskano wartość ryzyka wyrażoną ilościowo w skali od 1 do 100. Otrzymane wyniki można wyrazić jakościowo, stosując przyjętą skalę, co z kolei decyduje o podjęciu określonych działań w procesie redukcji (tab. 3.5).

Tab. 3.5. Przykład poziomów ryzyka na podstawie macierzy ryzyka

Poziom	**Przedział**	**Interpretacja i zalecane działania według NIST**[a)]
Niski	<1, 10>	Osoba odpowiedzialna za akredytację systemu powinna niezwłocznie podjąć decyzję od podjęciu działań korygujących lub akceptacji ryzyka i dopuszczeniu systemu do eksploatacji
Średni	<11, 50>	Działania korygujące są konieczne. Plan zabezpieczeń powinien być wdrożony w rozsądnym horyzoncie czasowym
Wysoki	<51, 100>	Silna potrzeba redukcji, potrzeba działań korygujących wdrożenie systemu zabezpieczeń. System może kontynuować pracę, jednak plan zabezpieczeń powinien być niezwłocznie skorygowany

[a)] A. Białas, *Bezpieczeństwo informacji i usług...*, op. cit., s. 116.

Opracowanie własne.

Do wyróżnionych zagrożeń (tab. 3.3) określa się prawdopodobieństwo ich wystąpienia (P) i szkodę (S). Poziom ryzyka jest iloczynem oszacowanych poziomów prawdopodobieństwa i skutków. Otrzymany wynik przyporządkowuje się do poziomu ryzyka (tab. 3.5). Ocenę ryzyka zidentyfikowanych zagrożeń przedstawia tabela 3.6.

Tab. 3.6. Ocena ryzyka zidentyfikowanych zagrożeń

ID zagrożenia	P	S	Wyliczone ryzyko	Poziom ryzyka
Z_1	0,1	100	0,1 x 100 =10	niski
Z_2	1	50	1 x 50 = 50	średni
Z_3	0,1	100	0,1 x 100 = 10	niski
Z_4	1	50	1 x 50 = 50	średni
Z_5	1	100	1 x 100 = 100	wysoki
Z_6	0,1	100	0,1 x 50 = 10	niski
Z_7	1	100	1 x 100 = 100	wysoki
Z_8	0,1	100	0,1 x 100 =10	niski

Opracowanie własne.

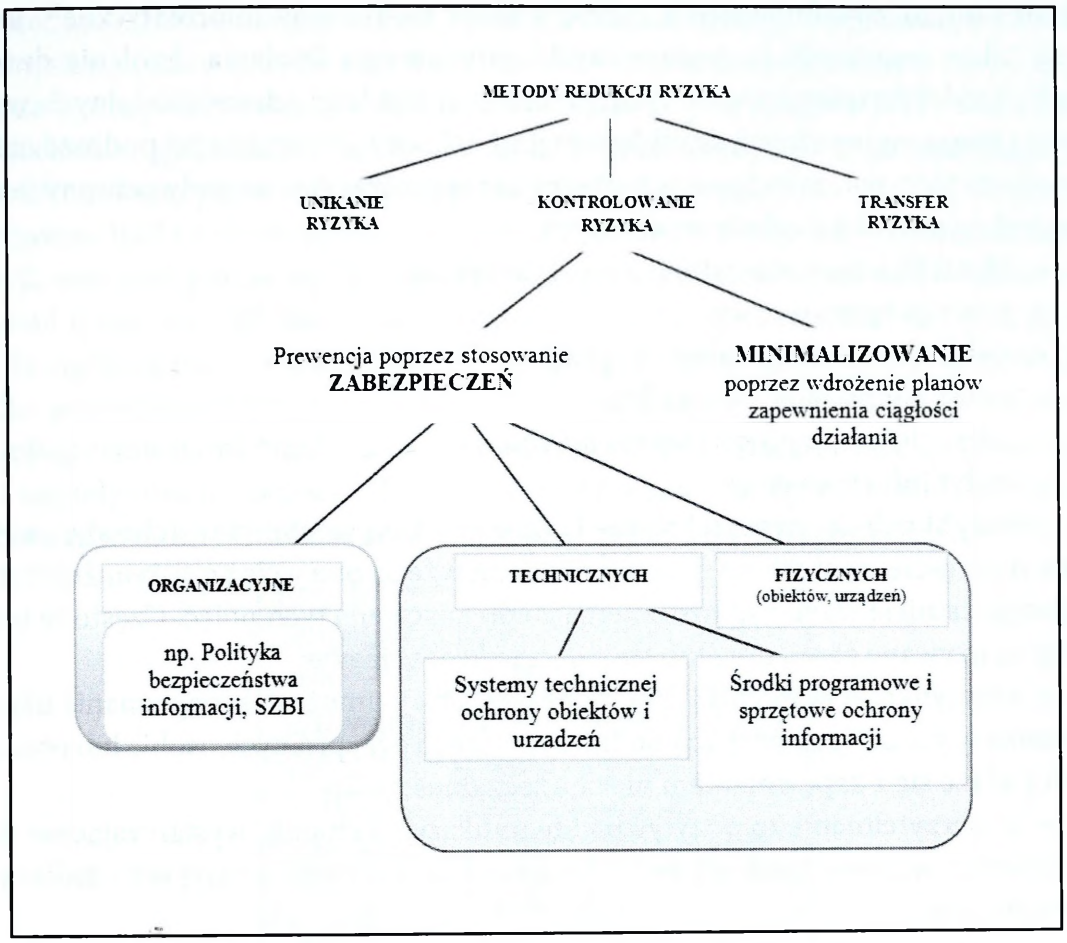
Podejmowanie działań redukujących (ograniczających) ryzyko sprowadza się do uszeregowania rekomendowanych zabezpieczeń według priorytetów, wdrożenia tych zabezpieczeń i przeprowadzenia oceny ich skuteczności[73]. W procesie ograniczania ryzyka można podjąć decyzję w zakresie tolerowania ryzyka, unikania ryzyka, transferu ryzyka, kontrolowania ryzyka (stosowanie zabezpieczeń, minimalizowanie ryzyka).

Transferowanie ryzyka polega na zapewnieniu rekompensaty od ubezpieczenia w sytuacji wystąpienia zdarzeń prowadzących do następstw[74]. Unikanie ryzyka związane jest z ignorowaniem ryzyka albo eliminowaniem potencjalnych skutków, np. odłączenia od sieci. K. Liderman podkreśla, że takiej strategii należy unikać. Kontrolowanie ryzyka związane jest ze stosowaniem zabezpieczeń. Do zabezpieczeń organizacyjnych należy przykładowo: polityka bezpieczeństwa, SZBI, system zarządzania jakością. Techniczne aspekty bezpieczeństwa struktur administracyjnych stanowią istotne zagadnienie zarządzania bezpieczeństwem, dlatego też poświęcono im następny podrozdział.

Scharakteryzowana metoda zarządzania ryzykiem została zaprezentowana w sposób uproszczony. Rekomenduje się, aby pełna analiza była bardziej złożona. W praktyce zalecane jest posługiwanie się większymi i dokładniejszymi macierzami ryzyka. Rozważania zawarte w niniejszym podrozdziale miały na celu uchwycenie istoty zarządzania ryzykiem na potrzeby zarządzania cyberbezpieczeństwem struktur administracyjnych.

73 Ibidem, s. 117.

74 A. Białas, *Bezpieczeństwo informacji...*, s. 117.



Opracowanie własne na podstawie: K. Liderman, *Bezpieczeństwo informacji...*, op. cit., s. 32.

Rys. 3.8. Sposoby redukcji ryzyka

3.5. Techniczne i organizacyjne aspekty bezpieczeństwa cyberprzestrzeni struktur administracyjnych

Największą grupę problemów związanych z bezpieczeństwem cyberprzestrzeni struktur administracyjnych stanowią problemy stwarzane przez ludzi. To ludzie włamują się do systemów, niszczą dane, wprowadzają wirusy, zaniedbują swoje obowiązki lub w sposób świadomy przyczyniają się do obniżenia poziomu bezpieczeństwa[75]. Wachlarz środków zabezpieczeń jest szeroki. Należy zauważyć, że ewoluują one wraz z rozwojem coraz doskonalszych urządzeń elektronicznych, powstawaniem coraz bardziej zaawansowanych systemów teleinformatycznych,

75 J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych...*, op. cit., s. 19.

a tym samym wyrafinowanych metod ataków na systemy informatyczne[76]. Istnieją także zagrożenia niebędące skutkiem celowego działania. Istnienie dużej liczby źródeł bezpieczeństwa cyberprzestrzeni struktur administracyjnych wymusza stosowanie różnych środków i metod ochrony. W niniejszym podrozdziale przedstawiono rekomendowane techniczne i organizacyjne metody ochrony bezpieczeństwa struktur administracyjnych:

- identyfikacja, uwierzytelniane i autoryzacja;
- kopie bezpieczeństwa;
- zwiększenie niezawodności sprzętu;
- zabezpieczenia kryptograficzne;
- zabezpieczenia programowe i sprzętowe;
- audyt informatyczny.

Identyfikacja, uwierzytelnianie i autoryzacja są elementami ochrony, z którymi najczęściej spotyka się użytkownik, jednakże są one wciąż częstym źródłem nadużyć. Istnieje wiele niezrozumienia co do znaczenia tych pojęć. Często te terminy są używane zamiennie lub traktowane jako tożsame:

- identyfikacja (autentyfikacja) to proces, który umożliwia rozpoznanie użytkownika w systemie za pomocą unikatowych cech przypisanych osobie lub obiektowi i wiąże się z zapewnieniem niezaprzeczalności;
- uwierzytelnianie to pozytywna identyfikacja w stopniu wystarczającym do przyznania odpowiednich uprawnień osobie lub procesowi pozytywnie zidentyfikowanemu;
- autoryzacja to nadanie osobie, programowi lub procesowi uprawnień (praw dostępu lub do korzystania z zasobów).

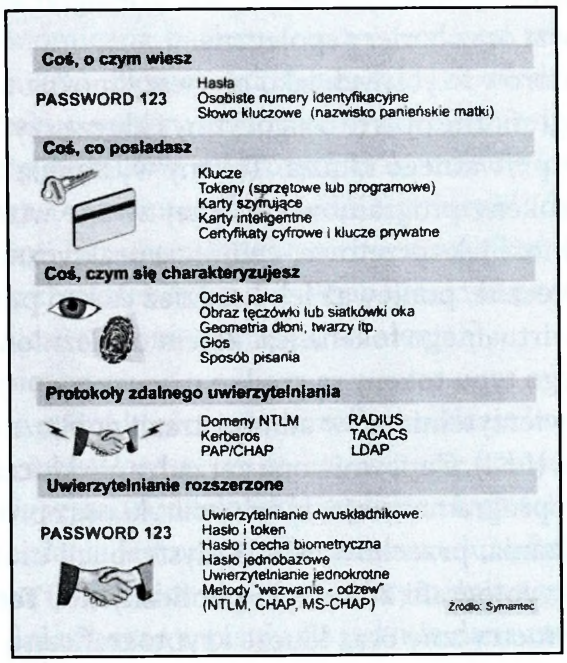
Wyróżnia się wiele metod uwierzytelniana. Najczęściej stosowane schematy przedstawia rys. 3.9.

Hasła należą do najpowszechniejszych metod autoryzacji. Podstawową zaletą ich stosowania jest prosta implementacja. Zapewnienie poziomu bezpieczeństwa wymaga przestrzegania zasad stosowania haseł. Powinno ono być długie – co najmniej ośmioznakowe, mieć duży stopień skomplikowania – składać się z wielkich i małych liter, cyfr i znaków, oraz nie mieć znaczenia w żadnym języku.

Hasła najczęściej łamane są metodą słownikową lub tzw. *brute force*. Obie metody polegają na sprawdzaniu kolejnych haseł, przy czym metoda słownikowa pobiera je ze zdefiniowanych słowników, zaś *brute force* generuje je przez kombinacje wszystkich dostępnych znaków. Choć są one nieoptymalne, to zarazem najbardziej

76 E. Szczepaniuk, *Zarządzanie bezpieczeństwem informacji w urzędach administracji publicznej* [w:] *Inżyniera systemów bezpieczeństwa*, red. P. Sienkiewicz, Warszawa 2015, s. 87.

skuteczne[77]. Dobre hasło powinno być zatem dostatecznie skomplikowane. Warto uzmysłowić sobie fakt, że kod ASCII zawiera 256 znaków, z których ponad 200 może być wykorzystanych w haśle. Wykorzystując przykładowo tylko małe litery łacińskie, ograniczamy się do używania jedynie 26 znaków. Natomiast używając kombinacji cyfr oraz wielkich i małych liter, mamy już do dyspozycji 62 znaki. Wówczas hasło ośmioliterowe daje ponad tysiąckrotnie więcej możliwych kombinacji, więc czas potrzebny do złamania hasła przywołanymi metodami wydłuża się ponad tysiąc razy. W haśle można użyć także znaków specjalnych, np. @, $, które komplikują hasło w jeszcze większym stopniu. Należy pamiętać, że hasło służy tylko posiadaczowi. Istotnym problemem wśród pracowników wielu instytucji jest udostępnianie haseł. Najsłabszym ogniwem stosowania haseł jest człowiek Dążenie do wygody oraz podatność człowieka na ataki socjotechniczne sprawia, że jest on potencjalnym źródłem informacji o sposobie dostępu do danego systemu.



Źródło: http://itpedia.pl/index.php/Dost%C4%99p_do_zasob%C3%B3w:_identyfikacja,_uwierzytelnianie_i_autoryzacja.

Rys. 3.9. Metody uwierzytelniania

Kolejną kategorią uwierzytelniania są techniki biometryczne, opierające się na pomiarach unikatowych cech człowieka. A. Bertillon w 1879 roku jako pierwszy opracował metodę identyfikacji przestępców na podstawie pomiarów kilkunastu

77 P. Jaroszerwski, *Jak skonstruować dobre hasło?*, CERT Polska, dostęp: http://www.cert.pl/PDF/dobre_ haslo.pdf.

cech, m.in. wzrostu, długości palców, obwodu głowy[78]. Do cech wykorzystywanych w technikach biometrycznych należą: linie papilarne, kształt twarzy i dłoni, głos, siatkówka i tęczówka oka, sposób pisania na klawiaturze, DNA.

Uwierzytelnianie za pomocą biometrii jest procesem kilkuetapowym. Rozpoczyna się od pomiaru cech użytkownika. Czujnik pomiarowy przekazuje do systemu sygnały analogowe reprezentujące wyniki pomiaru, które następnie są przetwarzane do odpowiedniego formatu. W dalszej kolejności następuje weryfikacja, czyli porównanie wyniku pomiaru z zapamiętanym wzorcem danego użytkownika[79]. Wzorce cech użytkowników i wyniki pomiarów powinny być chronione.

Wiarygodność technik biometrycznych jest charakteryzowana przez trzy wskaźniki: FAR (fałszywej akceptacji nieuprawnionej osoby), FRR (fałszywego odrzucenia uprawnionej osoby) i EER (równowagi)[80]. Rozwój technik biometrycznych w administracji publicznej jest jak na razie ograniczony ze względu na standardy, wysoki koszt oraz bariery społeczne.

Wśród identyfikatorów fizycznych jako pierwszy można wymienić token. Jest to urządzenie kryptograficzne oparte o algorytmy i klucze szyfrujące. Generuje on ciąg cyfr przy użyciu prywatnego klucza. Tokeny występują w wersji sprzętowej oraz programowej. Tokeny programowe, inaczej zwane wirtualnymi, posiadają taką samą funkcjonalność jak sprzętowe – emulują praktycznie działanie sprzętu, są jednak mniej bezpieczne, ponieważ ich kradzież często pozostaje nieujawniona. Bezpieczeństwo wirtualnego tokena jest zatem uzależnione od ochrony komputera. Dlatego też tego typu tokeny są rzadko używane.

Ważną metodą uwierzytelniania w administracji publicznej jest infrastruktura klucza publicznego (PKI). Zapewnia ona zarządzanie kluczami i certyfikatami. Jest to zbiór sprzętu, oprogramowania, ludzi, polityki oraz procedur niezbędnych do tworzenia, zarządzania, przechowywania, dystrybucji oraz odbierania certyfikatów opartych na kryptografii z kluczem publicznym[81]. Technologia ta oparta jest o szyfrowanie asymetryczne oraz klucze kryptograficzne. W Polsce kluczem o najwyższym poziomie zaufania jest certyfikat kwalifikowany wydawany przez podmioty, które świadczą usługi certyfikacyjne. Narodowe Centrum Certyfikacji prowadzi rejestr podmiotów kwalifikowanych.

78 T. Witczak, *Początki indentyfikacji*, dostęp: http://www.e-detektyw.pl/Magazyn_Detektyw/Wydanie_S pecjalne/Wydanie_Specjalne_042006/Poczatki_Identyfikacji/?id=676.

79 J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych...*, op. cit., s. 19.

80 Szerzej: M. Plucińska, J. Wójtowicz, *Analiza technik biometrycznych do uwierzytelniania osób*, „Elektronika" nr 4/2014, s. 65–66.

81 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Network Working Group, May 2008.

Kopie bezpieczeństwa (zapasowe) są obligatoryjnym wymaganiem bezpieczeństwa informatycznego struktur administracyjnych[82]. Ze względu na cele kopiowania zasobów danych można wyróżnić: kopie bezpieczeństwa (zapasowe), kopie archiwalne zasobów informacyjnych oraz kopie „transportowe" do przenoszenia danych i oprogramowania pomiędzy systemami komputerowymi[83]. Dla zapewnienia informacyjnej ciągłości działania struktur administracyjnych w zakresie systemów teleinformatycznych główne znaczenie ma kopia bezpieczeństwa, której proces wykonywania określany jest słowem *backup*.

Przeznaczenie kopii bezpieczeństwa to zachowanie istotnych danych czy też programów, w celu odtworzenia danych czy oprogramowania w przypadku zniszczenia czy utraty oryginału. Backup ma także swoje zastosowanie w informatyce śledczej oraz analizie powłamaniowej.

Ze względu na konieczność częstego powtarzania czynności zapisu kolejnych stanów informacyjnych systemu komputerowego, bardzo ważnym zagadnieniem jest efektywność ekonomiczna backupu. Zależy ona od jakości wykorzystywanych urządzeń i nośników. Biorąc pod uwagę fakt, że zwykle występują ograniczenia nakładów na zakup sprzętu i materiałów eksploatacyjnych, istnieje potrzeba optymalizacji liczby nośników, na których dokonuje się kopii bezpieczeństwa. Jest to możliwe przy zastosowaniu odpowiedniej strategii[84]. Sposób wykonywania i przechowywania kopii bezpieczeństwa powinien wynikać z zapisów zawartych w planie zapewnienia ciągłości działania. Wymagania te przekładają się na określone działania techniczne, które wymagają ustalenia[85]:

1. Co ma być kopiowane.
2. W jaki sposób ma być kopiowane, możliwe rodzaje kopii:

a) kopia pełna – w ustalonym czasie zapisuje się całość informacji, zgodnie z ustaloną specyfikacją wymian ustalonych w planie ciągłości działania. Podstawową wadą tego typu działania jest zapotrzebowanie na dużą ilość nośników danych;

b) kopia różnicowa (tygodniowa) – w wybranym dniu zapisuje się komplet danych, a w pozostałe dni robocze zapisuje się jedynie dane zmienione od ostatniego kopiowania pełnego. Przechowuje się jedynie kopie pełne. Nośniki z kopiami różnicowymi są kasowane i używane ponownie;

c) kopia przyrostowa (tygodniowa) – w wybranym dniu zapisuje się komplet danych, natomiast w pozostałe dni robocze zapisuje się jedynie dane zmienione

82 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100, poz. 1024).

83 K. Liderman, *Bezpieczeństwo informacyjne...*, op. cit., s. 159.

84 A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów...*, op. cit., s. 122.

85 K. Liderman, *Bezpieczeństwo informacyjne...*, op. cit., s. 159.

od ostatniej kopii przyrostowej. Przechowywane są jedynie kopie pełne. Nośniki z kopiami przyrostowymi są kasowane i używane ponownie.

3. Jak daleko wstecz ma istnieć możliwość odtwarzania stanu systemu – podstawowe strategie rotacji i przechowywania kopii zapewniające takie możliwości to:

a) prosta – 2 nośniki stosowane naprzemiennie;

b) podstawowa – 6 nośników: 4 dla kopii codziennych, 2 kopie tygodniowe;

c) dziadek-ojciec-syn – jest to rozszerzenie strategii podstawowej o wytworzenie i przechowywanie kopii tygodniowych przez miesiąc oraz wytworzenie kopii miesięcznych i przechowywanie ich przez ustalony okres (np. 6 miesięcy).

4. Czy wymagana jest automatyzacja procesu wykonywania kopii – tzn. czy ma być ona wykonywana ręcznie (przez operatora), czy automatycznie (przez oprogramowanie, według ustalonego harmonogramu, bez udziału operatora).

5. Czy pożądane jest scentralizowane zarządzanie procesem wykonywania i przechowywania kopii bezpieczeństwa – proces ten może być:

a) zdecentralizowany – każdy użytkownik wykonuje kopie bezpieczeństwa, bez przenoszenia ich do wskazanego, centralnego punktu systemu;

b) scentralizowany – przeprowadzony jest przez wyznaczoną osobę, z jednego miejsca w systemie komputerowym, dla danych wszystkich użytkowników.

6. Czy i jak kopiowane dane mają być kompresowane.

7. Jak często należy wymieniać nośniki używane do wytwarzania kopii bezpieczeństwa na nowe. Podstawowa przyczyna konieczności wymiany nośników to ich zużycie.

Wyróżnia się także zdalne kopie bezpieczeństwa, które są jednak rzadziej używane w administracji publicznej. Kopie bezpieczeństwa zapewniają minimalizację ryzyka utraty danych w przypadku zdarzeń katastrofalnych.

Zwiększenie niezawodności sprzętu ma na celu minimalizowanie prawdopodobieństwa awarii związanych m.in. z zanikiem lub zakłóceniem zasilania, wyładowaniami elektrostatycznymi, zmianami temperatury otoczenia. *Niezawodność systemu jako całości podnosi się przez redundancję: zwielokrotnienie dysków, źródeł zasilania, niekiedy całych systemów*[86]. W celu zwiększenia niezawodności sprzętu jednostki administracji publicznej zostały zobligowane m.in. do ochrony przez awariami zasilania.

Rozporządzenie MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzanych danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, wprowadziło obowiązek stosowania w jednostkach sektora publicznego rozwiązań minimalizujących skutki awarii zasilania. W załączniku do rozporządzenia zapisano, że *system informatyczny służący do przetwarzania*

86 J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych...*, op. cit., s. 34.

danych osobowych zabezpiecza się, w szczególności przed: utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. W sferze sprawności technicznej urządzeń elektronicznych utrzymanie parametrów zasilania jest zagadnieniem niezwykle ważnym, sprzęt komputerowy jest bowiem szczególnie wrażliwy na niekontrolowane skoki napięć: przepięcia, spadki i zaniki. Jak wskazują statystyki urządzeń sprzętu elektronicznego, ogromna ich część jest powodowana gwałtownymi skokami napięć zasilających[87]. Awarie zasilania wiążą się zatem z parametrami napięcia zasilającego dostarczanego za pośrednictwem sieci energetycznej, które charakteryzują się niestabilnością.

W celu wyeliminowania problemów wynikających z zakłóceń i zaników zasilania pomiędzy komputerami a siecią energetyczną instaluje się filtry oraz zasilacze awaryjne (UPS) lub spalinowe generatory prądotwórcze. Te ostatnie wykorzystuje się najczęściej w systemach o szczególnym znaczeniu (wojsko, banki, szpitale, centrale telefoniczne)[88]. Rozporządzenie MSWiA zobowiązuje jednostkę administracji publicznej do stosowania zasilaczy awaryjnych typu UPS.

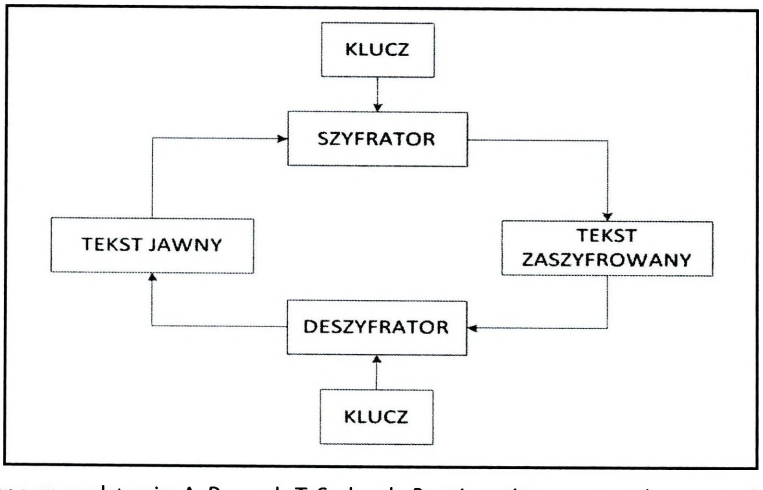
Niezawodność dysków zwiększa się przez stosowanie systemów zwielokrotnionych – macierzy RAID. Macierz RAID to zestaw kilku magnetycznych dysków fizycznych traktowanych przez system operacyjny jak jeden dysk logiczny. Macierze te są stosowane w celu powiększenia pojemności, zwiększenia bezpieczeństwa danych i poprawności efektywności systemu[89]. Macierze są sposobem zwiększenia dostępności danych w wypadku awarii dysków twardych. Właściwości macierzy RAID obejmują[90]:

- pierwszy stopień zabezpieczenia danych przed ich utratą w wyniku awarii dysku twardego, co pozwala na nieprzerwaną pracę systemu w wypadku awarii pojedynczego urządzenia oraz łatwość odbudowy po awarii podczas ciągłej jego pracy, a także możliwość zdalnego monitorowania pracy macierzy;
- zwiększenie wydajności całego systemu, wynikające ze zwiększenia strumienia danych zapisywanych i odczytywanych równolegle na kilku dyskach, przekazania sterowania nad zapisem/odczytem specjalizowanemu kontrolerowi (odciążenie procesora) oraz zaimplementowanie algorytmu buforowania (*cache*) operacji zapisu i odczytu;
- uzyskanie z wielu dysków twardych bardzo dużej ciągłej przestrzeni w jednym logicznym woluminie;
- łatwość rozbudowy systemu przez powiększenie pojemności macierzy w trakcie jego nieprzerwanej pracy.

87 A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów...*, op. cit., s. 109.
88 J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych...*, op. cit., s. 35.
89 Ibidem s. 34.
90 A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów...*, op. cit., s. 127.

Wyróżnia się kilka poziomów architektury macierzy dyskowych RAID[91]. Wybór macierzy wiąże się ze znalezieniem proporcji pomiędzy dostępnością, wydajnością i kosztem. W jednostkach administracji publicznej zastosowanie macierzy RAID wymaga złożenia zamówienia u firmy zewnętrznej, poprzedzonego ogłoszeniem przetargu nieograniczonego w myśl przepisów ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych.

Zabezpieczenia kryptograficzne są jednym z najbardziej efektywnych sposobów zabezpieczenia informacji przed dostępem osób nieupoważnionych. Proces szyfrowania polega na takim przekształceniu, aby dane mogły być odczytane tylko przez osoby upoważnione. Szyfrowanie odbywa się zgodnie z przyjętym algorytmem matematycznym, a efektywność szyfrowania, której miarą może być np. prawdopodobieństwo odczytania zaszyfrowanej wiadomości przez podmioty nieuprawnione, zależy od metody oraz zastosowania tzw. klucza[92]. Celem kryptografii jest przekształcenie tekstu jawnego w tekst zaszyfrowany; działanie to nazywa się szyfrowaniem, zaś proces odwrotny – deszyfrowaniem. Jak już wspominano, w procesie szyfrowania i deszyfrowania używa się kluczy kryptograficznych – są to *ciągi danych służące do przekształcenia tekstu jawnego w kryptogram i kryptogramu w tekst jawny za pomocą, odpowiednio, algorytmu szyfrowania i algorytmu deszyfrowania*[93]. Ogólny schemat szyfrowania i deszyfrowania przedstawiono na rys. 3.10.



Opracowanie własne na podstawie: A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów...*, op. cit., s. 140.

Rys. 3.10. Idea szyfrowania i deszyfrowania informacji

91 Zob. A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów...*, op. cit., s. 138.
92 A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów...*, op. cit., s. 138.
93 Ibidem, s. 140.

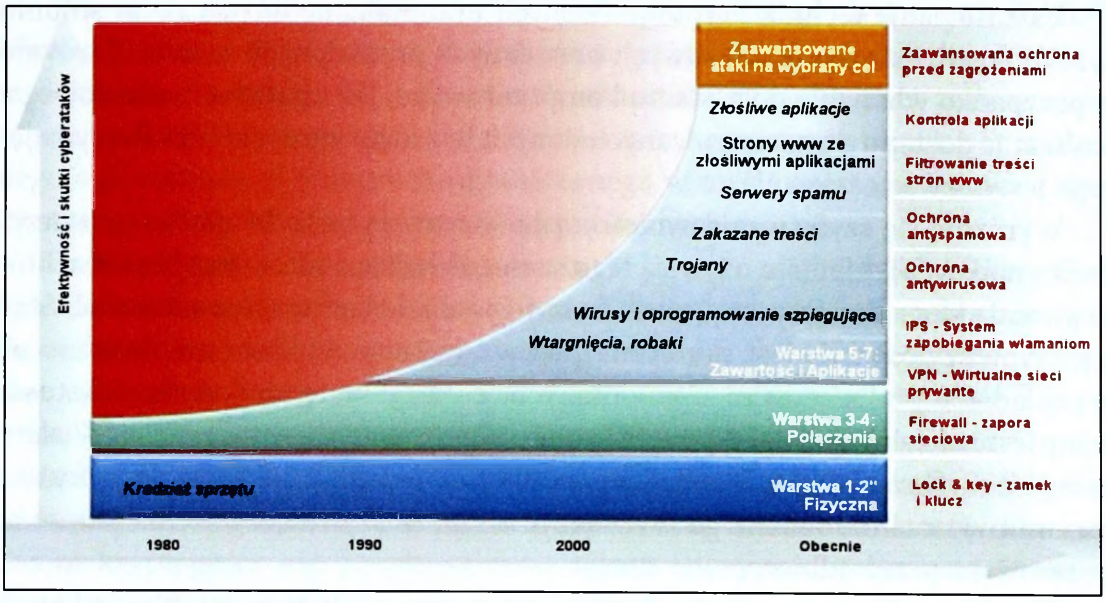
Zastosowanie technik kryptograficznych minimalizuje w znacznym stopniu ryzyko utraty informacji wrażliwych oraz danych przesyłanych w sieci. Zarówno w przypadku włamania do systemu komputerowego, jak i podsłuchu sieciowego, uzyskanie dostępu do zaszyfrowanych danych bez algorytmu i klucza deszyfrującego jest bezwartościowe.

Wyróżnia się szyfrowanie symetryczne i asymetryczne. W pierwszym przypadku nadawca i odbiorca używają tego samego klucza, a zatem każda osoba, która posiada klucz symetryczny, może zaszyfrować i odszyfrować wiadomość. Stąd tego typu szyfrowanie jest skuteczne pod warunkiem, że klucz nie znajdzie się w posiadaniu podmiotów nieuprawnionych. Z uwagi na te niedogodności stosowany jest najczęściej drugi typ szyfrowania – szyfrowanie asymetryczne. W algorytmach szyfrowania klucz szyfrujący (publiczny) jest inny niż klucz deszyfrujący (prywatny) oraz nie można go wyznaczyć z klucza szyfrującego. Oba klucze są generowane przez odbiorcę.

W celu zapewnienia wiarygodności kluczy wprowadzono certyfikację kluczy publicznych, za którą odpowiadają centra certyfikacji. W administracji publicznej stosowanie podpisu elektronicznego uregulowała ustawa o podpisie elektronicznym z 2001 roku. W wyniku ustawy znowelizowano kodeks postępowania administracyjnego[94], co zapewniło równorzędność czynności realizowanych w formie papierowej i elektronicznej.

Zabezpieczenia programowe i sprzętowe należą do kluczowych elementów ochrony systemu teleinformatycznego. Zabezpieczenia te są związane ze stroną techniczną cyberprzestrzeni i obejmują wszystkie warstwy modelu ISO/OSI. Należy zauważyć, że wraz z przechodzeniem przez kolejne warstwy, od sprzętu do warstwy aplikacji, ochrona i zabezpieczenia stają się coraz bardziej złożone, ale też coraz bardziej zawodne[95]. Wynika to z coraz większej złożoności wbudowanej w systemy teleinformatyczne, które zależą w znacznej mierze od umiejętności osób implementującej zabezpieczenia[96]. W poprzednim rozdziale wykazano, że rozwój technologii informatycznych jest związany z powstawaniem coraz doskonalszych metod ataków na systemy teleinformatyczne. Fakt ten determinował konieczność tworzenia nowych rozwiązań dotyczących ochrony systemów teleinformatycznych. Rys. 3.11 przedstawia zależności między rozwojem metod ataków a powstawaniem zabezpieczeń.

94 Ustawa z dnia 25 czerwca 1960 roku Kodeks postępowania administracyjnego.
95 R. Anderson, *Inżynieria zabezpieczeń*, Warszawa 2005, s. 60.
96 Ibidem, s. 83.



Źródło: High Performance Network Security, Fortinet Inc., Sunnyvale 2013, s. 3, dostęp: http://www.fortinet.com/sites/default/files/basicfiles/FortinetBroch.pdf; cyt za: M. Muliński, *Zagrożenia bezpieczeństwa...*, op. cit., s. 153.

Rys. 3.11. Sprzętowa i programowa ochrona systemu teleinformatycznego

Zgodnie z rysunkiem, za ochronę warstwy trzeciej i czwartej odpowiada firewall (zapora sieciowa). Zapewnia on ochronę sieci przed nieautoryzowanym dostępem. Znajduje się pomiędzy siecią prywatną a publiczną. Przez zespół reguł decyduje, który ruch sieciowy zostanie przepuszczony, a który zablokowany lub zawrócony. W niektórych dużych organizacjach zapory stosowane są w celu odseparowania wrażliwych i czułych obszarów organizacji od reszty pracowników. Za pomocą list dostępu kontrolowane jest oddzielenie stref zaufanych od niezaufanych. Decydują one, czy transmisja może być przepuszczona, porzucona lub odrzucona[97]. Wyróżnia się trzy podstawowe typy zapór sieciowych:

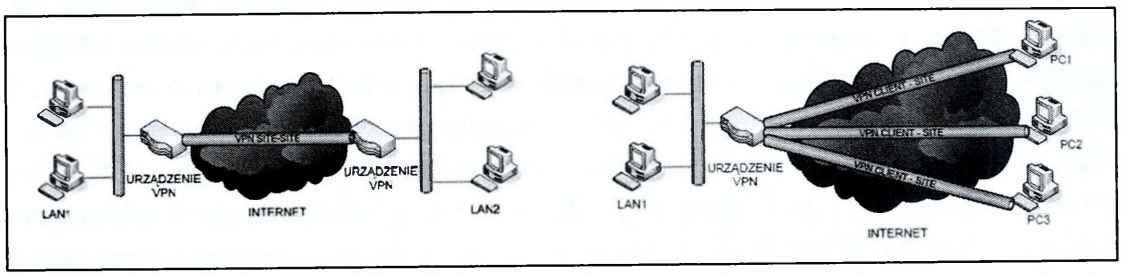
- zapory sieciowe na poziomie sieci/pakietu (filtry pakietów), które monitorują przepływające przez nie pakiety sieciowe oraz przepuszczają te, które są zgodne z regułami ustalonymi na danej zaporze;
- zapory sieciowe na poziomie aplikacji/usługi (bramy pośredniczące, *proxy*), które wykonują połączenia z serwerem w imieniu użytkownika;
- translacja adresów sieciowych (maskowanie), która polega na dokonywaniu zamiany adresu IP hosta wewnętrznego, aby ukryć go przez zewnętrznym monitorowaniem.

97 P. Nowak, A. Majka, D. Kościelniak, *Firewall. Metody filtracji*, Kraków 2002, s. 7.

Kolejnym typem zabezpieczeń jest koncepcja funkcjonowania wirtualnych sieci prywatnych (VPN). Polega na tworzeniu wydzielonych logicznych kanałów transmisji danych w ramach sieci rozległej, tak aby dane przesyłane tymi kanałami zostały zabezpieczone w zakresie poufności, integralności i autentyczności. Zabezpieczenie danych w sieci VPN realizowane jest za pomocą technik kryptograficznych[98]. Oznacza to, że ruch w ramach sieci prywatnej pomiędzy użytkownikami końcowymi płynie przez tunel za pośrednictwem sieci publicznej. Pakiety przechwytywane w sieci są nierozpoznawalne bez kluczy szyfrowania.

Wyróżnia się dwa podstawowe rodzaje architektury sieci VPN:

- *site-to-site* – kanał zestawiony między dwoma odległymi fizycznie sieciami LAN. Urządzeniem VPN może być serwer firmowy lub odpowiednio skonfigurowany router z obsługą sieci VPN;
- *client-to-site* – kanał VPN zestawiany między komputerem zdalnego użytkownika a odległą siecią LAN.



Źródło: http://reset.ath.bielsko.pl/systemy-operacyjne/artykuly/windows/2010/vpn.aspx.

Rys. 3.12. Architektura prywatnych sieci wirtualnych – VPN

Ochrona systemu teleinformatycznego obejmuje także systemy wykrywania i zapobiegania włamaniom. Są to urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym. W hierarchii zabezpieczenia infrastruktury teleinformatycznej powinny one być lokowane jako kolejne po zaporze systemy ochrony. IDS służy do monitorowania zagrożeń i incydentów naruszenia bezpieczeństwa oraz do powiadamiania o nich. Z kolei IPS podejmuje dodatkowo działania mające na celu powstrzymanie ataku, minimalizację jego skutków lub aktywną odpowiedź na naruszenie bezpieczeństwa[99]. Zatem systemy te zwiększają bezpieczeństwo przez wzmocnienie kontroli komunikacji w sieci.

98 R. Rekut, P. Skalski, *Wirtualne Sieci Prywatne – bezpieczne sieci korporacyjne przez Internet*, http://seminarium.zielman.pl/zielman99/pdf/VPN.pdf.

99 M. Wrzesień, Ł. Olejnik, P. Ryszawa, *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, „Pomiary Automatyka Robotyka" nr 2/2013, s. 167.

Kolejną metodą zapewnienia bezpieczeństwa systemów teleinformatycznych jest ochrona antywirusowa. Zapewnienie pełnego bezpieczeństwa w ten sposób jest praktycznie niemożliwe, jednakże stosowanie programów antywirusowych pozwala w znacznym stopniu ograniczyć liczbę wirusów dostających się do systemu.

Programy antywirusowe wykorzystują wiele metod wykrywania wirusów[100]:

- poszukiwanie sygnatur – zawartość testowanego pliku jest porównywana ze zbiorem sygnatur (charakterystycznych ciągów bitów) różnych wirusów. W bardziej zaawansowanego programach wykrywanie jest wspomagane przez sieci neuronowe czy systemy ekspertowe;
- sprawdzenie integralności – aktualne cechy charakterystyczne testowanego pliku są porównywalne z wartościami zapamiętanymi w bazie danych, w czasie gdy plik jest „czysty";
- analiza heurystyczna – badanie zachowania się programów i poszukiwanie prób infekowania systemu (np. wywołania przerwań systemowych).

W odpowiedzi na rosnącą liczbę incydentów bezpieczeństwa stworzono zaawansowane zabezpieczenia posiadające wielowymiarowe mechanizmy bezpieczeństwa, które określono mianem urządzeń klasy UMT[101]. Termin ten po raz pierwszy został przedstawiony i szeroko opisany przez C.J. Kolodgy'ego, dyrektora działu badań w zakresie zabezpieczeń internetowych w firmie IDC. Aby produkt był zgodny z technologią UTM, musi posiadać co najmniej wbudowany firewall, sondę IDS/IDP, silnik antywirusowy i antyspamowy oraz filtry treści URL. Podstawowym składnikiem UMT jest firewall. Jeżeli ruch sieciowy zostanie przepuszczony przez zaporę, jest analizowany w kolejnym ogniwie, czyli w filtrze pracującym w warstwie aplikacji. W tej warstwie następuje filtrowanie ruchu, który odbywa się na porcie przypisanym do danej usługi.

Audyt informatyczny jest ostatnim z wymienionych elementów wspomagających zapewnienie bezpieczeństwa cyberprzestrzeni struktur administracyjnych, ale nie ostatnim w ogóle. Ogólnie pojęcie audytu oznacza *postępowanie dla oceny zgodności audytowanego obiektu z wzorcem (normą, wzorcem proceduralnym lub arbitralnie ustanowionym wektorem wartości pewnych cech) prowadzone przez stronę niezależną (firmę, osobę lub zespół)*[102]. W literaturze funkcjonuje wiele sprzecznych definicji dotyczących audytu informatycznego. Niekiedy jest on także utożsamiany z audytem bezpieczeństwa. K. Liderman podkreśla, że audyt bezpieczeństwa teleinformatycznego jest częścią audytu informatycznego.

100 J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych...*, op. cit., s. 33.

101 Ang. *Unified Threat Management.*

102 K. Liderman, *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"*, „Biuletyn Instytutu Automatyki i Robotyki" nr 21/2004, s. 93.

Podczas przeprowadzania audytu informatycznego stosowane są standardy audytowania systemów informatycznych. Do modeli wspomagających audyt informatyczny zalicza się: COBIT, ITIL i Val IT, BS 7799, TCSEC[103]. Model COBIT jest obecnie na świecie uznawany za standard budowy ładu informatycznego, czyli *IT Governance* w organizacjach. Ład organizacyjny w IT ma spowodować, że wykorzystywanie informatyki w instytucjach będzie wspierało osiąganie ich celów i realizację ich strategii[104]. K. Liderman wyróżnia następujące obszary audytu informatycznego[105]:

1. infrastruktura:

a) fizyczna (płoty, zamki, drzwi itp.),

b) techniczna (alarmy ppoż., systemy monitoringu wizyjnego, systemy uwierzytelniania itp.),

c) informatyczna (routery, firewalle, IDS, serwery, komputery, sieć teledacyjna itp.);

2. oprogramowanie (systemy operacyjne, oprogramowanie antywirusowe, zapory sieciowe, aplikacje biznesowe, systemy uwierzytelniające itp.);

3. informacje (struktury organizacyjne, polityki bezpieczeństwa, procedury itp.);

4. zasoby ludzkie.

W metodyce standardu COBIT wyróżnia się 302 szczegółowe wymagania przypisane do 34 procesów zachodzących w systemach teleinformatycznych. Do każdego z procesów określone zostały kryteria, które muszą spełniać informacje: efektywność, wydajność, poufność, integralność, dostępność, zgodność, rzetelność. W trakcie przeprowadzania audytu wypełniana jest lista audytowa, która pozwala na zakwalifikowane poszczególnych punktów audytu do jednej z kategorii: spełnione, spełnione częściowo, niespełnione, nie dotyczy.

Krajowe Ramy Interoperacyjności[106] w jednostkach sektora publicznego wprowadziły obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Należy mieć świadomość, że żadna z wymienionych metod nie jest doskonała oraz nie eliminuje całkowicie zagrożeń. Zapewnienie pełnego bezpieczeństwa

103 M. Pańkowska, *Audyt informatyczny w jednostkach sektora finansów publicznych* [w:] *Komputerowo zintegrowane zarządzanie*, red. R. Knosala, Opole 2005, s. 278.

104 A. Kaczorowska, *Audyt o kontrole systemów teleinformatycznych oraz projektów IT w sektorze administracji publicznej* [w:] *Komputerowo zintegrowane zarządzanie*, red. R. Knosala, Opole 2011, s. 452.

105 K. Liderman, A.E. Patkowski, *Metodyka LP–A przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, WAT, Warszawa 2004, s. 112, cyt za: T. Muliński, *Zagrożenia bezpieczeństwa...*, op. cit., s. 149.

106 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

w praktyce nie jest możliwe. Dlatego też istotnym czynnikiem jest poprawne stosowanie środków ochrony w celu minimalizacji ryzyka. Zarządzanie cyberbezpieczeństwem struktur administracyjnych powinno opierać się na koordynacji wszystkich elementów składowych jednostek administracji publicznej.

3.6. Modele zarządzania cyberbezpieczeństwem struktur administracyjnych

3.6.1. Zarządzanie na szczeblu krajowym w Polsce

Odpowiedzialność za bezpieczeństwo oraz ochronę cyberprzestrzeni RP (w tym struktur administracyjnych) jest rozproszona. W Polsce nie funkcjonuje jeden podmiot koordynujący działania w obszarze zarządzania bezpieczeństwem cyberprzestrzeni. W związku z tym poszczególne instytucje odpowiadają za ochronę w obszarze cyberbezpieczeństwa administracji państwowej, ochronę użytkowników prywatnych oraz sferę obrony narodowej. W wymienionych obszarach bezpieczeństwo może obejmować zarówno jawne, jak i niejawne systemy teleinformatyczne.

W Polsce nie funkcjonuje akt prawny rangi ustawowej regulujący kwestie odpowiedzialności instytucji publicznych związanych z cyberbezpieczeństwem. Dokumentem strategicznym w tym obszarze jest Polityka Bezpieczeństwa Cyberprzestrzeni RP, w której ustanowiono trójpoziomowy Krajowy System Reagowania na Incydenty Komputerowe w cyberprzestrzeni RP[107]:

1. poziom koordynacji – minister właściwy ds. informatyzacji;
2. poziom reagowania na incydenty komputerowe:

a) Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL – realizujący jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP;

b) Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizujące zadania w sferze militarnej;

3. poziom administracji – administratorzy odpowiadający za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni.

Zgodnie z ustawą o działach administracji rządowej[108], Ministerstwo Administracji i Cyfryzacji (MAC) jest głównym resortem zajmującym się informatyzacją państwa. Ponadto Polityka Bezpieczeństwa Cyberprzestrzeni RP

107 *Polityka Bezpieczeństwa Cyberprzestrzeni RP...*, op. cit., s. 18.

108 Art. 12a ustawy z dnia 4 września 1997 roku o działach administracji rządowej.

wskazuje na ministra ds. informatyzacji jako podmiot koordynujący jej realizację, z zastrzeżeniem, że podmiotem nadzorującym wdrażanie dokumentu jest Rada Ministrów[109]. Należy zauważyć, że minister nie posiada żadnych kompetencji władczych związanych z bezpieczeństwem cyberprzestrzeni, ponieważ zadania i uprawnienia w przypadku jawnych systemów teleinformatycznych nie mają podstaw prawnych w przepisach ustawowych. Stąd możliwości w zakresie egzekwowania wymagań i zaleceń cyberbezpieczeństwa wynikają jedynie z Polityki Bezpieczeństwa Cyberprzestrzeni RP, która ma charakter strategii i nie jest dokumentem rangi ustawowej. Minister ds. informatyzacji przy pomocy zespołu zadaniowego ds. ochrony cyberprzestrzeni[110] zapewnia koordynację i spójność działań realizowanych przez poszczególne urzędy państwowe.

W obszarze reagowania na incydenty komputerowe związane z bezpieczeństwem cyberprzestrzeni RP Rządowy Zespół Reagowania na Incydenty Komputerowe CERT. GOV.PL pełni funkcję głównego zespołu CERT w obszarze administracji rządowej i w obszarze cywilnym[111]. Do nałożonych na niego zadań należy[112]:

- kreowanie polityki w zakresie ochrony przed cyberzagrożeniami;
- koordynowanie przepływu informacji pomiędzy podmiotami w tym zakresie;
- wykrywanie cyberzagrożeń, rozpoznawanie ich i przeciwdziałanie im;
- współpraca z krajowymi instytucjami, organizacjami oraz podmiotami resortowymi w zakresie ochrony cyberprzestrzeni;
- reprezentacja RP w kontaktach międzynarodowych;
- gromadzenie wiedzy dotyczącej stanu bezpieczeństwa dla krytycznej infrastruktury teleinformatycznej;
- reagowanie na incydenty bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem krytycznej infrastruktury krytycznej państwa;
- prowadzenie analiz powłamaniowych;
- tworzenie polityki ochrony systemów i sieci teleinformatycznych;
- szkolenie i podnoszenie świadomości odnośnie do zagrożeń komputerowych;
- przygotowanie okresowych raportów w zakresie bezpieczeństwa teleinformatycznego państwa;
- konsulting i doradztwo w zakresie cyberbezpieczeństwa.

109 *Polityka Bezpieczeństwa Cyberprzestrzeni RP...*, op. cit., s. 18.

110 Zespół Zadaniowy ds. ochrony cyberprzestrzeni został powołany 13.06.2014 roku decyzją Ministra Administracji i Cyfryzacji. Zespół jest odpowiedzialny jest za koordynację działań dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni RP oraz za przygotowywanie rekomendacji z tym związanych. Zespół funkcjonuje przy Komitecie Rady Ministrów ds. informatyzacji (KRMC).

111 *Polityka Bezpieczeństwa Cyberprzestrzeni RP...*, op. cit., s. 8.

112 M. Młotek, M. Siedlarz, *Rządowy Zespół Reagowania na Incydenty Komputerowe CERT. GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 4/11, s. 158.

W 2012 roku w ramach CERT powołane zostały zespoły dyżurujące, które pełnią funkcję całodobowego punktu kontaktowego dla administratorów sieci teleinformatycznych. Zespół CERT działa w obszarze jawnych i niejawnych systemów teleinformatycznych i funkcjonuje od 2008 roku w ramach Agencji Bezpieczeństwa Wewnętrznego (ABW). Zgodnie z ustawą o ochronie informacji niejawnych[113] ABW jest odpowiedzialna za realizację zadań w zakresie bezpieczeństwa systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych.

W Polsce nie istnieje jeden zespół reagowania na incydenty komputerowe. Oprócz CERT.GOV.PL funkcjonuje także Centrum Zarządzania Bezpieczeństwem Usług i Sieci Teleinformatycznych MON oraz zespoły utworzone przez środowisko telekomunikacyjne, np. CERT POLSKA – funkcjonujący w ramach NASK, CERT OPL – monitorowanie zagrożeń bezpieczeństwa dla systemów podłączonych do sieci Orange Polska, PIONIER-CERT – grupa reagowania na incydenty bezpieczeństwa dla użytkowników Polskiej Szerokopasmowej Sieci Naukowej PIONIER.

W resorcie obrony narodowej również ustanowiono trójstopniową strukturę Systemu Reagowania na Incydenty Komputerowe (SRnIK), w skład której wchodzą[114]:

- Centrum Koordynacyjne SRnIK, którego funkcję spełnia właściwa komórka wewnętrzna Narodowego Centrum Kryptologii;
- Centrum Techniczne SRnIK, którego funkcję spełnia właściwa komórka wewnętrzna Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych;
- administratorzy systemów teleinformatycznych w jednostkach i komórkach organizacyjnych.

Poza wymienionymi podmiotami ważnym elementem bezpieczeństwa cyberprzestrzeni działającym w sferze publicznych sieci telekomunikacyjnych jest Urząd Komunikacji Elektronicznej (UKE), który jest organem krajowym właściwym w sferze telekomunikacji. Zgodnie z ustawą Prawo telekomunikacyjne[115] przedsiębiorcy telekomunikacyjni mają obowiązek niezwłocznie powiadomić prezesa UKE w przypadku naruszenia bezpieczeństwa lub integralności sieci lub usług, mających istotny wpływ na ich działanie, a także podjętych w tym celu środkach zapobiegawczych.

113 Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. nr 182, poz. 1228).

114 Decyzja nr 24/MON Ministra Obrony Narodowej z dnia 18 czerwca 2014 roku w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz.Urz. MON nr 243, poz. 203).

115 Art. 175a ust. 1 ustawy z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Dz.U. 2004 nr 171, poz. 1800).

Analogicznie dostawca dostępnych usług publicznych zawiadamia Generalnego Inspektora Ochrony Danych Osobowych (GIODO) o naruszeniu danych osobowych, przez które w myśl przepisów ustawy Prawo telekomunikacyjne rozumie się *przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych*[116]. GIODO jest zatem istotnym organem w obszarze ochrony danych osobowych.

Kolejną instytucją, którą należy wskazać, jest Rządowe Centrum Bezpieczeństwa (RCB), które rozpoczęło działalność w 2008 roku na postawie ustawy o zarządzaniu kryzysowym[117]. RCB pełni zadania w obszarze zarządzania kryzysowego oraz budowy systemu ochrony infrastruktury krytycznej[118]. W sferze infrastruktury krytycznej Minister Administracji i Cyfryzacji jest odpowiedzialny za systemy łączności, systemy sieci teleinformatycznych, systemy zapewniające ciągłość działania.

Do instytucji realizujących w Polsce zadania z zakresu bezpieczeństwa informacji i sieci należy także zaliczyć: Ministerstwo Skarbu, Ministerstwo Spraw Zagranicznych, Ministerstwo Spraw Wewnętrznych, Ministerstwo Finansów, Kancelarię Prezesa Rady Ministrów, Komendę Główną Policji, Narodowe Centrum Kryptologii.

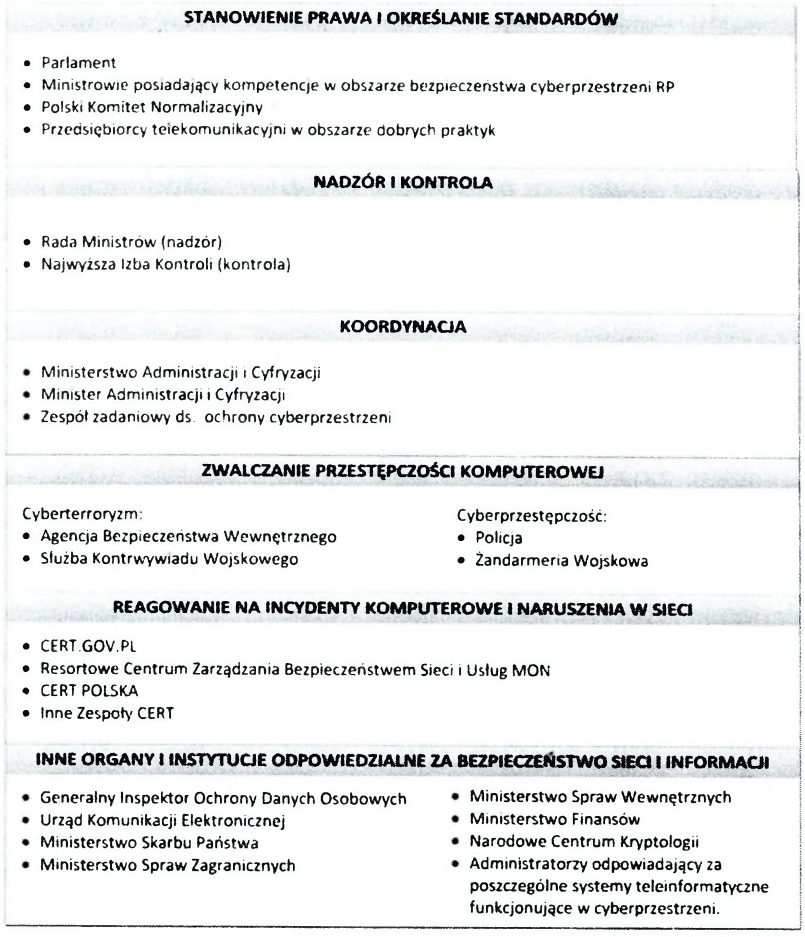
W zapewnieniu bezpieczeństwa cyberprzestrzeni RP duże znaczenie mają instytucje odpowiedzialne za zwalczanie przestępczości w cyberprzestrzeni (Policja, Żandarmeria Wojskowa). Agencja Bezpieczeństwa Wewnętrznego współpracuje z pozostałymi organami odpowiedzialnymi za bezpieczeństwo RP (MON, SKW) oraz zwalczanie przestępczości komputerowej o charakterze kryminalnym. Na rys. 3.13 przedstawiono podstawowe instytucje właściwe w obszarze zarządzania cyberbezpieczeństwem struktur administracyjnych na szczeblu krajowym.

W zaprezentowanym modelu stanowienie prawa oraz określanie standardów ma istotną rolę w zapewnieniu bezpieczeństwa cyberprzestrzeni, organy i instytucje działają bowiem w granicach i na podstawie prawa. Prawne uregulowanie uprawnień i kompetencji jest wymogiem koniecznym w sferze praktycznej możliwości stworzenia systemu bezpieczeństwa cyberprzestrzeni RP. Normy, standardy i dobre praktyki dają rekomendacje w obszarze już zastosowanych, efektywnych rozwiązań systemowych.

116 Art. 174a ust. 2 ustawy z dnia 16 lipca 2004 roku Prawo telekomunikacyjne..., op. cit.

117 Art. 10 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89, poz. 590).

118 *Narodowy Program Ochrony Infrastruktury Krytycznej*, Warszawa 2013, s. 13.



Opracowanie własne.

Rys. 3.13. Model instytucjonalny zarządzania cyberbezpieczeństwem struktur administracyjnych na szczeblu krajowym w Polsce

3.6.2. Zarządzanie na szczeblu samorządowym w Polsce

Analizując problematykę zarządzania bezpieczeństwem teleinformatycznym na szczeblu samorządowym, należy zauważyć, że poszczególne instytucje publiczne charakteryzują się odmiennością w obszarze ich misji, potencjalnych zagrożeń czy też wykorzystywanych systemów teleinformatycznych. Postrzeganie administracji publicznej w kategoriach systemu pozwala na wyodrębnienie jego elementów oraz uchwycenie relacji między tymi elementami.

Zakres oddziaływania Polityki Bezpieczeństwa Cyberprzestrzeni RP został określony w instytucjach rządowych. Natomiast jednostkom samorządu terytorialnego rekomenduje się założenia polityki. W celu określenia odpowiedzialności instytucji publicznych w obszarze zarządzania bezpieczeństwem struktur administracyjnych niezbędne jest zatem powołanie się na inne uregulowania prawne.

Zgodnie z ustawą o zarządzaniu kryzysowym tworzy się wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego, w skład których powinny wchodzić następujące elementy[119]:

1. Plan główny, zawierający:

a) charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej, oraz mapy ryzyka i mapy zagrożeń;

b) zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa;

c) zestawienie sił i środków planowanych do wykorzystania w sytuacji kryzysowej;

d) Zadania określone planami działań krótkookresowych.

2. Zespół przedsięwzięć na wypadek sytuacji kryzysowych, zawierający:

a) zadania w zakresie monitorowania zagrożeń;

b) tryb uruchamiania niezbędnych sił i środków;

c) procedury reagowania kryzysowego.

3. Załączniki funkcjonalne planu głównego, zawierające m.in.:

a) procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną infrastruktury krytycznej;

b) organizację łączności;

c) organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania;

d) zasady informowania ludzi o zagrożeniach i sposobach postępowania na wypadek zagrożeń;

e) organizację ewakuacji z obszarów zagrożonych;

f) organizację ratownictwa, opieki medycznej, pomocy społecznej oraz pomocy psychologicznej;

g) organizację ochrony przed zagrożeniami charakterystycznymi dla danego obszaru;

h) wykaz zawartych umów i porozumień związanych z realizacją zadań w obszarze zarządzania kryzysowego;

i) zasady oraz tryb dokumentowania szkód;

j) zasady uruchamiania rezerw państwowych;

k) wykaz infrastruktury krytycznej objętej planem;

l) priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej.

W celu analizy zarządzania cyberbezpieczeństwem struktur administracyjnych warto zwrócić uwagę na fakt, czy plany zarządzania kryzysowego uwzględniają cyberzagrożenia oraz w jakim stopniu spełnione są ustawowe wymagania

119 Art. 5 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, op. cit.

dotyczące zawartości owych planów. W tab. 3.7 przedstawiono analizę wojewódzkich planów zarządzania kryzysowego pod kątem uwzględnienia zagrożeń bezpieczeństwa teleinformatycznego.

Tab. 3.7. Analiza wojewódzkich planów zarządzania kryzysowego w kontekście zagrożeń cyberprzestrzeni państwa[120]

Województwo	C	Czy zawiera obligatoryjne elementy?			Instytucje
		1	2	3	
dolnośląskie	Nieudostępniony				
kujawsko-pomorskie	Nieudostępniony				
lubelskie	Nieudostępniony				
lubuskie	NIE	–	–	–	–
łódzkie	NIE	–	–	–	–
małopolskie	NIE	–	–	–	–
mazowieckie	NIE	–	–	–	–
opolskie	TAK	TAK	TAK	TAK	Wojewoda, Wydział Bezpieczeństwa i Zarządzania Kryzysowego, WCZK, WZZK, Straż Pożarna, Policja, wojsko, przedsiębiorcy telekomunikacyjni
podkarpackie	Nieudostępniony				
podlaskie	Nieudostępniony				
pomorskie	NIE	–	–	–	–
śląskie	Nieudostępniony				
świętokrzyskie	TAK	TAK	TAK	TAK	Wojewoda, System Pomocy Społecznej
warmińsko-mazurskie	NIE	–	–	–	–
wielkopolskie	Nieudostępniony				
zachodniopomorskie	Nieudostępniony				

Opracowanie własne na podstawie planów zamieszczonych w Internecie.

Powyższa tabela przedstawia dostępność wojewódzkich planów zarządzania kryzysowego (WPZK) w Internecie oraz określa, czy uwzględniają one cyberzagrożenia. W ośmiu województwach nie udostępniono w sieci WPZK. Spośród analizowanych planów jedynie dwa zawierają informacje na temat możliwości wystąpienia zagrożeń dla bezpieczeństwa teleinformatycznego – województwa świętokrzyskiego i opolskiego. W planach tych zawarto obligatoryjne elementy WPZK zgodnie z ustawą o zarządzaniu kryzysowym.

120 Oznaczenia zastosowane w tabeli: C – Czy w planie uwzględniono cyberzagrożenia?; Czy zawiera obligatoryjne elementy: 1 – plan główny, 2 – zespół przedsięwzięć na wypadek sytuacji kryzysowych, 3 – załączniki funkcjonalne?

Analogiczną analizę przeprowadzono dla powiatowych planów zarządzania kryzysowego. Ze względu na dużą liczbę powiatów ograniczono się jedynie do wybranych. W tab. 3.8 przedstawiono analizę powiatowych planów zarządzania kryzysowego pod kątem uwzględnienia zagrożeń bezpieczeństwa teleinformatycznego.

Tab. 3.8. Analiza powiatowych planów zarządzania kryzysowego w kontekście zagrożeń cyberprzestrzeni państwa [121]

Powiat	C	Czy zawiera obligatoryjne elementy?			Instytucje
		1	2	3	
prudnicki	TAK	TAK	TAK	TAK	Starosta, Wydział Organizacyjny, Programów i Zarządzania Kryzysowego, PCZK, PZZK, Zespół Radców Prawnych, Straż Pożarna, Policja, WKU, PKP
namysłowski	TAK	TAK	TAK	TAK	Starosta, Wydział Zarządzania Kryzysowego i Spraw Obywatelskich, PCZK, PZZK, Wydział Organizacyjny, Straż Pożarna, Policja, WKU
drawski	TAK	TAK	TAK	TAK	Starosta, Wydział Zarządzania Kryzysowego, PCZK, Wydział Organizacyjny, Wydział Finansowy, Policja, Straż Pożarna
cieszyński	TAK	TAK	TAK	TAK	Burmistrz, Koordynator programów kryzysowych, Koordynator porządku publicznego i przeciwdziałania terroryzmowi, Koordynator ochrony obiektów urzędu, Policja, Straż Miejska
lipski	NIE	–	–	–	–
oleski	TAK	TAK	TAK	TAK	Starosta, Wydział Promocji i Rozwoju, Wydział Zarządzania Kryzysowego, PCZK, PZZK, Wydział Organizacyjny
krapkowicki	TAK	TAK	TAK	TAK	Starosta, PCZK, PZZK, Policja, Straż Pożarna
opoczyński	NIE	–	–	–	–
brzeski	TAK				Starosta, Zespół ds. Zarządzania Kryzysowego, Spraw Wojskowych i Obronnych, PCZK, PZZK, Wydział Organizacyjno-Prawny, Straż Pożarna, Policja

Opracowanie własne na podstawie planów zamieszczonych w Internecie.

W tab. 3.8 przestawiono analizę wybranych powiatowych planów zarządzania kryzysowego (PPZK) w kontekście zagrożeń cyberprzestrzeni państwa oraz zawartości w nich wymogów ustawowych. Z wybranych powiatów jedynie

121 Oznaczenia zastosowane w tabeli: C – Czy w planie uwzględniono cyberzagrożenia?; Czy zawiera obligatoryjne elementy: 1 – plan główny, 2 – zespół przedsięwzięć na wypadek sytuacji kryzysowych, 3 – załączniki funkcjonalne?

w powiecie lipskim i opoczyńskim nie odniesiono się do problemu cyberzagrożeń. Pozostałe PPZK uwzględniają zagrożenia bezpieczeństwa teleinformatycznego oraz zawierają kompletne informacje na temat odpowiedzialności instytucji w poszczególnych fazach zarządzania kryzysowego (zapobieganie, przygotowanie, reagowanie, odbudowa).

Analiza gminnych planów zarządzania kryzysowego również wymaga ograniczenia ich liczby, ponieważ w Polsce działa 2479 gmin. W tab. 3.9 przedstawiono analizę gminnych planów zarządzania kryzysowego w kontekście uwzględnienia zagrożeń bezpieczeństwa teleinformatycznego.

Tab. 3.9. Analiza gminnych planów zarządzania kryzysowego w kontekście zagrożeń cyberprzestrzeni państwa[122]

Gmina	C	Czy zawiera obligatoryjne elementy?			Instytucje
		1	2	3	
Wilków	TAK	TAK	TAK	TAK	Wójt, Sekretarz Gminy, Stanowisko ds. Obrony Cywilnej, Obronności i Spraw Wojskowych, Gminny Zespół Zarządzania Kryzysowego, Policja
Kielce	TAK	NIE	TAK	TAK	Wójt, System Pomocy Społecznej
Paczków	TAK	TAK	TAK	TAK	Burmistrz, Gminny Zespół Zarządzania Kryzysowego
Kluczbork	TAK	TAK	TAK	TAK	Burmistrz, Wydział Spraw Obywatelskich i Obronnych, Gminny Zespół Zarządzania Kryzysowego, Wydział Organizacyjny, Zastępca Burmistrza, Straż Pożarna, Policja, WKU
Gogolin	TAK	TAK	TAK	TAK	Gminne Centrum Reagowania, Gminny Zespół Zarządzania Kryzysowego, Naczelnik Wydziału Finansowego, Naczelnik Spraw Administracyjnych, Naczelnik Wydziału ds. Informatyki, PKP, przedsiębiorcy telekomunikacyjni
Lubrza	TAK	TAK	TAK	TAK	Wójt, Referat Spraw Obywatelskich, Gminny Zespół Zarządzania Kryzysowego, Sekretarz Gminy, Stanowisko ds. inwestycji, Policja, Straż Pożarna
Malechowo	TAK	TAK	TAK	TAK	Wójt, Sekretarz Gminy, Kierownik Referatu Organizacyjnego, Policja, Straż Pożarna
Jakubów	NIE	–	–	–	–
Wyszków	NIE	–	–	–	–

Opracowanie własne na podstawie planów zamieszczonych w Internecie.

122 Oznaczenia zastosowane w tabeli: C – Czy w planie uwzględniono cyberzagrożenia?; Czy zawiera obligatoryjne elementy: 1 – plan główny, 2 – zespół przedsięwzięć na wypadek sytuacji kryzysowych, 3 – załączniki funkcjonalne?

Powyższa tabela przedstawia analizę wybranych gminnych planów zarządzania kryzysowego. W większości badanych jednostek samorządu terytorialnego uwzględnia się zagrożenia bezpieczeństwa teleinformatycznego. Jedynie w gminie Jakubów oraz Wyszków nie odniesiono się do problematyki zagrożeń cyberprzestrzeni państwa.

3.6.3. Zarządzanie w jednostce organizacyjnej administracji publicznej w Polsce

Zarządzanie bezpieczeństwem cyberprzestrzeni w poszczególnych jednostkach administracji publicznej wynika głównie z obowiązków nakładanych na jednostki samorządu terytorialnego w związku z koniecznością zapewnienia bezpieczeństwa danych zgromadzonych i przetwarzanych w urzędzie oraz z różnego rodzaju wymagań, jakie muszą spełniać systemy bezpieczeństwa informatycznego, ze szczególnym uwzględnieniem wymagań ogólnych, technicznych oraz prawnych[123]. Istotną rolę w zarządzaniu cyberbezpieczeństwem odgrywają również wymagania organizacyjne i proceduralne, które określają podział zadań i kompetencji związanych z bezpieczeństwem teleinformatycznym, procedury związane z zapobieganiem i minimalizacją ryzyka wystąpienia zagrożeń oraz postępowanie w przypadku wystąpienia zakłócenia.

W dobie społeczeństwa informacyjnego i wykorzystania technologii informatycznych w sektorze publicznym instytucje publiczne są szczególnie narażone na wystąpienie zagrożeń cyberprzestrzeni państwa. Witryny internetowe, usługi oraz aplikacje powinny być zabezpieczone przez utratą danych, atakami cybernetycznymi oraz skutkami działania szkodliwego oprogramowania. Brak właściwego zabezpieczenia dla informacji i usług publicznych może skutkować brakiem zaufania użytkowników, co w rezultacie może przekładać się na spowolnienie informatyzacji i upowszechniania się elektronicznych usług w tym sektorze.

W jednostkach organizacyjnych administracji publicznej, dla zapewnienia bezpieczeństwa teleinformatycznego, kierownik danej jednostki powinien ustanowić system zarządzania bezpieczeństwem informacji z uwzględnieniem obowiązujących przepisów prawnych oraz najlepszych praktyk. *W celu zapewnienia spójności polityk bezpieczeństwa informacji jednostek organizacyjnych, zakłada się, że minister właściwy ds. informatyzacji w porozumieniu z Ministrem Obrony Narodowej i Szefem Agencji Bezpieczeństwa Wewnętrznego może przygotować wytyczne dotyczące*

123 D. Gacoń (kierownik projektu), *Model bezpieczeństwa informatycznego i ochrony e-Urzędu terenowej jednostki administracji publicznej przed zagrożeniami związanymi z elektroniczną łącznością multimedialną*, Instytut Łączności. Państwowy Instytut Badawczy, Warszawa–Miedzeszyn 2008, s. 51.

systemów zarządzania bezpieczeństwem informacji[124]. *Przy opracowaniu polityki bezpieczeństwa niezbędne jest uwzględnienie obligatoryjnych wymagań wynikających z ustawy o informatyzacji*[125] oraz rozwiązań dotyczących minimalnych wymagań dla systemów teleinformatycznych[126] w omawianym obszarze. W tab. 3.10 przedstawiono wymagania bezpieczeństwa teleinformatycznego w jednostkach organizacyjnych administracji publicznej zgodne z wymienionymi przepisami prawnymi.

Tab. 3.10. Wymagania bezpieczeństwa teleinformatycznego w jednostkach organizacyjnych administracji publicznej

Nazwa wymogu	Typ wymogu
Opracowanie polityki bezpieczeństwa	obligatoryjny
Opracowanie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	obligatoryjny
Opracowanie systemu zarządzania bezpieczeństwem informacji	obligatoryjny
Kontrola dostępu do obiektów i pomieszczeń, w których zainstalowane serwery przetwarzające dane osobowe	obligatoryjny
Utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację	obligatoryjny
Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko	obligatoryjny
Sprzętowy moduł bezpieczeństwa HSM (Hardware Security Module)	obligatoryjny
Wyposażenie w instalację alarmową klasy SA3	warunkowy
Ochrona przed awariami zasilania	obligatoryjny
Ochrona przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	obligatoryjny
Kopie zapasowe	obligatoryjny
Ochrona przed zagrożeniami pochodzącymi z sieci publicznej	obligatoryjny
Ochrona kryptograficzna dla danych wykorzystywanych do uwierzytelniania przy przesyłaniu danych w sieci publicznej	obligatoryjny
Wysoki poziom bezpieczeństwa	obligatoryjny
Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji	obligatoryjny
Monitorowanie dostępu do informacji	obligatoryjny
Bezzwłoczne zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących	obligatoryjny
Zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok	obligatoryjny

Opracowanie własne.

124 Polityka bezpieczeństwa cyberprzestrzeni RP..., op. cit., s. 13.

125 Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64, poz. 565).

126 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526).

Przedstawione wymagania można ogólnie podzielić na wymagania proceduralne, organizacyjne oraz techniczne. Tworzenie bezpiecznych rozwiązań dla jednostek sektora publicznego powinno uwzględniać możliwość przystosowania się na bieżąco do zmieniających się warunków bezpieczeństwa (np. dostosowanie zabezpieczeń do zmieniających się zagrożeń) oraz dodatkowe uwarunkowania związane m.in. z wprowadzeniem nowych usług elektronicznych, zachowaniem atrybutów bezpieczeństwa.

Ochrona informacji i usług wymaga zaangażowania ze strony instytucji publicznej jako całości. W kształtowaniu cyberbezpieczeństwa niezwykle istotne jest uwzględnienie misji instytucji oraz realizowanych zadań. Często kompetencje struktur administracyjnych są różne, również wykorzystywane systemy teleinformatyczne są charakterystyczne dla danej działalności.

W praktyce funkcjonowania elektronicznej administracji publicznej w Polsce wiodącą rolę przypisuje się Elektronicznej Platformie Usług Publicznych (ePUAP). Z portalu będącego częścią systemu ePUAP mogą korzystać wszyscy użytkownicy posiadający dostęp do Internetu. Operacje chronione mogą być wykonywane przez uwierzytelnione osoby, natomiast znaczna liczba operacji i dostępów przez autoryzowanych użytkowników. W celu korzystania z ePUAP możliwe są dwa sposoby uwierzytelniania:

- hasło – wykorzystanie losowego identyfikatora użytkownika, który generowany jest podczas zakładania konta, oraz statycznego hasła;
- certyfikat kwalifikowany – wykorzystanie losowego identyfikatora oraz certyfikatu kwalifikowanego posiadanego przez użytkownika.

System korzysta z platformy sprzętowej zlokalizowanej w dwóch ośrodkach, pomiędzy którymi dokonywana jest bieżąca replikacja danych. W przypadku wystąpienia awarii lub z innych powodów (np. zniszczenie fizyczne działającego ośrodka) możliwe jest przełączenie systemu, tak aby działał on na drugim ośrodku bez utraty danych[127]. Podsystemami operującymi na danych są: podsystem bezpieczeństwa[128], podsystem front-end[129] oraz profil zaufany[130]. W ePUAP rejestruje się operacje na danych osobowych. Mechanizmy zabezpieczające w postaci rejestru zdarzeń zapewniają atrybuty bezpieczeństwa.

127 Zakres Systemu Zarządzania Bezpieczeństwem Informacji ePUAP, dostęp: http://e-dziennik.mswia.gov.pl/DUM_MSW/2011/9/45/Zalacznik2.DOC.

128 W ramach tego podsystemu gromadzone są dane osobowe: dane użytkownika i podmiotu, w kontekście którego użytkownik pracuje.

129 W ramach tego podsystemu dokonywane są operacje na danych osobowych pochodzących z danych gromadzonych w podsystemie bezpieczeństwa – pobranie danych użytkownika i podmiotu oraz przechowywane dokumenty xml z danymi osobowymi, np. dane adresata, dane odbiorcy.

130 W ramach tego podsystemu gromadzone są potwierdzone podpisem kwalifikowanym dane osobowe użytkownika, wykorzystywane do generowania podpisów cyfrowych.

ePUAP może być wykorzystywany przez instytucje publiczne jako wsparcie architektury bezpieczeństwa systemów tych instytucji. W tym zakresie wyróżnia się trzy podstawowe modele wsparcia[131]:

- model, w którym instytucja udostępnia swoje zasoby (systemy) z wykorzystaniem własnych łącz (np. do Internetu albo do innych instytucji publicznych), jednocześnie korzystając ze wsparcia pewnych usług bezpieczeństwa ePUAP, np. wykorzystując profile użytkowników ePUAP oraz mechanizmy identyfikacji i uwierzytelnienia użytkowników;
- model, w którym wszelka komunikacja z zasobami (systemami) instytucji będzie realizowana za pośrednictwem ePUAP. W tym modelu instytucja może czerpać pełnię korzyści z infrastruktury bezpieczeństwa ePUAP, wykorzystując nie tylko profile użytkowników i mechanizmy identyfikacji i uwierzytelnienia, ale także np. mechanizmy autoryzacji dostępu do zasobów oraz zapewniania bezpieczeństwa sieciowego (firewall, IPS itp.; w takim modelu, z perspektywy systemu instytucji, ePUAP można potraktować jako wyrafinowany firewall chroniący przed atakami z Internetu i innych sieci); instytucja może wtedy rozważyć rezygnację z własnych urządzeń zapewniania bezpieczeństwa sieciowego takiej klasy, jaka wymagana byłaby podczas udostępniania zasobów bezpośrednio np. w Internecie;
- model, w którym instytucja wykorzystuje wybrane usługi związane z podpisem elektronicznym, takie jak np. weryfikacja podpisu, archiwizacja podpisu. Jest to model o charakterze komplementarnym wobec dwóch powyższych (nie stoi z nimi w sprzeczności).

W praktyce wykorzystanie ePUAP jest na niskim poziomie. Niedawne doniesienia na temat błędów w systemie nie sprzyjają zaufaniu użytkowników oraz ograniczają kontakt obywatela z użytkownikiem z pomocą Internetu. Społeczna świadomość na temat e-usług administracji publicznej[132] oraz zainteresowanie tego typu usługami jest wciąż marginalne.

3.6.4. Zarządzanie w Unii Europejskiej

Na szczeblu Unii Europejskiej opracowuje się szereg aktów prawnych w obszarze bezpieczeństwa cybernetycznego. Przedmiotem prac jest obecnie dyrektywa w sprawie bezpieczeństwa sieci i informacji[133]. Polityka międzynarodowa Unii Eu-

131 http://www.bialystok.uw.gov.pl/NR/rdonlyres/B813FAC3-EC5C-474A-A297-FAF89DA349A4/0/ePUA Pwsp%C3%B3%C5%82pracainstytucjipublicznych.pdf.

132 Szerzej A. Grudzińska-Kuna, J. Papińska-Kacperek, *Usługi elektronicznej administracji dla obywateli w Polsce – wybrane problemy*, „Roczniki Kolegium Analiz Ekonomicznych SGH" nr 24, Warszawa 2012, s. 119–131.

133 Zaproponowana dyrektywa jest kluczowym elementem ogólnej strategii i nakładałaby na wszystkie państwa członkowskie, podmioty świadczące kluczowe usługi internetowe i ope-

ropejskiej w kontekście cyberprzestrzeni wspiera przestrzeganie podstawowych wartości, definiuje normy zachowania, promuje przestrzeganie istniejących już przepisów międzynarodowych w dziedzinie cyberprzestrzeni, a jednocześnie pomaga państwom, które nie są jej członkami w zakresie budowy zdolności obronnych i propaguje współpracę międzynarodową w kwestiach bezpieczeństwa cybernetycznego[134]. Istotną rolę w zapewnieniu bezpieczeństwa odgrywają instytucje unijne powołane na rzecz ochrony cyberprzestrzeni.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA)[135] powołana w 2004 roku rozporządzeniem Parlamentu Europejskiego i Rady[136] jest agencją funkcjonującą na potrzeby Unii oraz jej członków. Jej celem jest zwiększenie możliwości w obszarze ochrony oraz reagowania na zagrożenia bezpieczeństwa teleinformatycznego. Instytucja oferuje Komisji Europejskiej oraz jej członkom pomoc i doradztwo, może także wspierać Komisję w pracach przygotowawczych dotyczących aktualizacji ustawodawstwa unijnego.

ENISA ma następujące kompetencje i zadania[137]:

- zbiera właściwe informacje w celu analizowania ryzyka bieżącego oraz powstającego, a wyniki przekazuje państwom UE oraz Komisji;
- oferuje doradztwo, a w stosownych przypadkach pomoc Parlamentowi Europejskiemu, Komisji oraz właściwym europejskim i krajowym organom;
- rozszerza współpracę między różnymi instytucjami w sektorze (np. przez konsultacje i tworzenie sieci kontaktów);
- ułatwia współpracę między Komisją a państwami UE w zakresie rozwoju wspólnych metodologii, w celu zapobiegania problemom dotyczącym bezpieczeństwa;
- przyczynia się do wzrostu świadomości i dostępności aktualnych, celowych i wszechstronnych informacji na temat bezpieczeństwa sieci i informacji w stosunku do wszystkich użytkowników (m.in. przez promowanie wymiany najlepszych praktyk, w tym metod ostrzegania użytkowników, oraz poszukiwanie współdziałania między inicjatywami w sektorze publicznym i prywatnym);
- wspiera Komisję i państwa UE w ich dialogu z przemysłem, w celu określania problemów dotyczących bezpieczeństwa sprzętu i oprogramowania;

ratorów infrastruktury krytycznej, platformy handlu elektronicznego, portale społecznościowe oraz przedsiębiorstwa z sektora energetycznego, sektora transportu, sektora bankowego i opieki zdrowotnej obowiązek zapewnienia bezpiecznego i wiarygodnego środowiska cyfrowego dla całej Unii Europejskiej.

134 G. Furgał, *Strategia cyberbezpieczeństwa według UE*, dostęp: http://www.e-kirp.pl/Aktualnosci/Strategia-cyberbezpieczenstwa-wedlug-UE.

135 Strona internetowa ENISA: http://www.enisa.europa.eu/.

136 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji.

137 Ibidem.

- śledzi rozwój norm bezpieczeństwa w zakresie produktów i usług oraz promuje działania z zakresu oceny ryzyka i zarządzania nim;
- wyraża własne wnioski i porady;
- uczestniczy w wysiłkach UE zmierzających do współpracy z krajami trzecimi i organizacjami międzynarodowymi, w celu promowania globalnej propozycji dotyczącej bezpieczeństwa.

W Strategii Bezpieczeństwa Wewnętrznego Unii Europejskiej określono zamiar ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3). Zgodnie z zapisami strategii centrum miało umożliwić państwom członkowskim i instytucjom UE budowanie zdolności operacyjnych i analitycznych do prowadzenia dochodzeń oraz pogłębienie współpracy z partnerami międzynarodowymi[138]. Centrum utworzono w 2013 roku w ramach Europejskiego Urzędu Policji (Europolu) w Hadze.

Centrum w obszarze cyberbezpieczeństwa spełnia cztery podstawowe funkcje[139]:

- służy jako europejski punkt kontaktowy w zakresie informacji dotyczących cyberprzestępczości;
- gromadzi dostępną w Europie wiedzę specjalistyczną na temat cyberprzestępczości potrzebną do budowania potencjału państw członkowskich w zakresie walki z tym zjawiskiem;
- wspiera krajowe dochodzenia dotyczące cyberprzestępstw;
- zapewnia wspólne stanowisko służbom ścigania i służbom sądowniczym zaangażowanym w europejskie dochodzenia w zakresie cyberprzestępczości.

Kolejnym osiągnięciem Unii jest powołanie w 2012 roku Zespołu Reagowania na Incydenty Komputerowe Unii Europejskiej – CERT.EU. W skład zespołu wchodzą eksperci pochodzący z instytucji unijnych – Komisji Europejskiej, Parlamentu Europejskiego i Komitetu Regionów. Głównym zdaniem CERT jest wspieranie innych instytucji unijnych w obszarze cyberbezpieczeństwa oraz wykrywanie, prewencja, odpowiedź i regeneracja uszkodzonej infrastruktury[140]. Powołanie CERT stanowiło realizację zapisów Europejskiej Agendy Cyfrowej.

W Polityce Bezpieczeństwa Cyberprzestrzeni RP podkreślono konieczność współpracy krajowych struktur odpowiedzialnych za cyberbezpieczeństwo z inicjatywami tworzonymi na poziomie europejskim. W celu wypracowania sku-

138 Komunikat Komisji Europejskiej i Rady. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy, Bruksela, dnia 22.11.2010, KOM(2010) 673, s. 11.

139 Komunikat Komisji do Rady i Parlamentu Europejskiego. Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością, Bruksela, dnia 28.3.2012, COM(2012) 140 final, s. 5–7.

140 M. Lakomy, *Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego – zarys problemu*, „Rocznik Integracji Europejskiej" nr 7/2013, s. 139.

tecznej ochrony niezbędna jest wymiana doświadczeń oraz koordynacja działań przedstawicieli Polski w ENISA, EC3 oraz CERT.EU. Cenne wskazówki i dobre praktyki mogą także wynikać z zaimplementowanych rozwiązań w innych państwach UE. W tab. 3.11 przedstawiono elementy zarządzania bezpieczeństwem cyberprzestrzeni w wybranych państwach unijnych.

Tab. 3.11. Zarządzanie cyberbezpieczeństwem w wybranych krajach Unii Europejskiej

Państwo	Charakterystyka
Wielka Brytania (UK)	Dokumentem programowym jest Strategia Cyberbezpieczeństwa Wielkiej Brytanii[a)], która określa, jak UK będzie wspierać dobrobyt gospodarczy, ochronę bezpieczeństwa narodowego i społeczeństwa w kontekście środowiska cyfrowego. Priorytety w kształtowania środowiska cyberbezpieczeństwa sprowadzają się do wyznaczenia trzech głównych obszarów: 1) ludzie – zasoby ludzkie powinny być kluczowym elementem budowania zdolności obronnych w UK. W tym sensie istotną rolę odgrywają nie tylko wojsko i sektor publiczny, ale także obywatele; 2) partnerstwa – efektywne partnerstwa z podmiotami sektora prywatnego, które dostarczają technologiczną bazę dla sieciowej obrony oraz wieloletnią ekspertyzę w zakresie przeciwdziałania atakom w cyberprzestrzeni; 3) obrona sieciowa – oparta na systemie ochrony zasobów cybernetycznych państwa[b)]. W 2010 roku działalność rozpoczęły dwie komórki zajmujące się cyberbezpieczeństwem: 1) Office Cyber Security (OCS), które uczestniczy w doradztwie strategicznym w obszarze bezpieczeństwa cyberprzestrzeni dla rządu UK oraz odpowiada za tworzenie i nadzór na osiąganiem priorytetowych celów strategicznych bezpieczeństwa; 2) Cyber Security Operations Centre (CSOC), które monitoruje oraz reaguje na incydenty bezpieczeństwa.
Finlandia (FI)	Dokumentem programowym jest Strategia Cyberbezpieczeństwa[c)], zgodnie z którą wizja bezpieczeństwa cybernetycznego sprowadza się do trzech elementów: 1) zapewnienie ochrony przed zagrożeniami sieciowymi; 2) obywatele, instytucje publiczne oraz przedsiębiorcy mogą bezpiecznie korzystać z domen internetowych, a środki bezpieczeństwa wynikają z uregulowań krajowych i międzynarodowych; 3) do 2016 FI będzie prekursorem w globalnej identyfikacji zagrożeń i w zarządzaniu zakłóceniami spowodowanymi przez te zagrożenia. Za bezpieczeństwo cybernetyczne w Finlandii odpowiada przede wszystkim Urząd Regulacji Łączności (FICORA) oraz utworzone na początku 2014 roku Narodowe Centrum Bezpieczeństwa Cybernetycznego (NCSC). FICORA przyjmuje opłaty licencyjne i telewizyjne, wydaje krótkoterminowe licencje dla telewizji i radia, monitoruje treści programów telewizyjnych i radiowych oraz reklamy. Kontroluje również poziom i jakość ogólnych usług pocztowych. Zarządza centralnie częstotliwościami radiowymi. Ta istotna odpowiedzialność krajowa i międzynarodowa zapewnia skuteczne i wolne od zakłóceń wykorzystywanie częstotliwości. Ponadto FICORA kontroluje sytuację w sieciach komunikacyjnych i czuwa nad bezpieczeństwem informacji. Informuje ministerstwo i opinię publiczną o wykroczeniach[d)]. Centrum dokonuje przeglądu funkcjonalności sieci i łączności elektronicznej i bezpieczeństwa informacji i sprawozdań z ewentualnych zagrożeń dla bezpieczeństwa informacyjnego. Celem działania NCSC jest także zwiększenie świadomości na temat bezpieczeństwa wśród użytkowników. Natomiast Urząd Regulacji Łączności funkcjonuje w ramach Ministerstwa Transportu i Komunikacji.

Państwo	Charakterystyka
Estonia (EST)	Dokumentem programowym w Estonii w obszarze bezpieczeństwa cyberprzestrzeni jest Strategia Bezpieczeństwa Cybernetycznego Estonii[e]. Cele strategiczne w obszarze bezpieczeństwa cybernetycznego to: 1) zastosowanie środków bezpieczeństwa; 2) rozwój wiedzy i świadomości na temat bezpieczeństwa informacji; 3) opracowanie odpowiednich ram regulacyjnych i prawnych; 4) promowanie współpracy międzynarodowej. Na potrzeby bezpieczeństwa wdrożono system ISKE, którego celem jest zapewnienie wysokiego poziomu bezpieczeństwa przez wprowadzenie rozwiązań organizacyjnych, infrastrukturalnych oraz fizycznych i technicznych środków bezpieczeństwa. ISKE jest standardem bezpieczeństwa informacji opartym na standardzie niemieckim[f]. W Estonii działa CERT-EE, który obsługuje incydenty komputerowe. Ważną instytucją jest także Estońskie Centrum Informatyczne zajmujące się utrzymaniem bezpieczeństwa informatycznego w sektorze prywatnym i publicznym. Centrum ma także prawo nadzoru. Wydział ochrony Infrastruktury Informatycznej (CIIP) ocenia bezpieczeństwo systemów informatycznych oraz przeprowadza ocenę ryzyka. W Estonii każdy dostawca usług jest odpowiedzialny za bezpieczeństwo swojego systemu, a CIIP udziela im porad na temat oceny ryzyka i bezpieczeństwa.
Czechy (CZ)	Dokumentem programowym jest Strategia Bezpieczeństwa Cybernetycznego na lata 2011–2015[g].W 2011 roku utworzono Narodowe Centrum Cyberbezpieczeństwa (NCSC), które koordynuje współpracę na poziomie krajowym i międzynarodowym w celu minimalizacji ryzyka cyberzagrożeń. Ponadto NCSC opracowuje standardy bezpieczeństwa, prowadzi badania oraz wspiera edukację. W ramach NCSC działa zespół GovCERT.cz, reagujący na incydenty komputerowe[h].
Niemcy (DE)	Dokumentem regulującym kwestie bezpieczeństwa teleinformatycznego jest Strategia Bezpieczeństwa Cybernetycznego[i], której celem jest zapewnienie bezpieczeństwa: 1) teleinformatycznej infrastruktury krytycznej; 2) systemów informatycznych, które są wykorzystywane przez obywateli; 3) administracji. W 2011 roku utworzono Centrum Bezpieczeństwa Cybernetycznego, którego celem jest koordynacja współpracy urzędów federalnych odpowiedzialnych za bezpieczeństwo cyberprzestrzeni. Priorytetem CBC jest skoordynowane i efektywne zapobieganie atakom cybernetycznym o podłożu kryminalnym, terrorystycznym i wywiadowczym. Pełnomocnik Rządu Federalnego ds. Technologii Informatycznych jest głównym punktem kontaktowym dla landów i sektora prywatnego w obszarze bezpieczeństwa IT. Ważną instytucją jest Federalny Urząd ds. Bezpieczeństwa Informatycznego, którego celem jest wydawanie certyfikatów bezpieczeństwa.

[a] *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, November 2011, dostęp: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[b] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" nr I – 2011/17, s. 25.

[c] *Finland´s Cyber security Strategy*, Government Resolution 24.1.2013, dostęp: http://www.defmin.fi/files /2378/Finland_s_Cyber_Security_Strategy.pdf.

[d] A. Dragan, D.M. Korzeniewska, A. Krasnowolski, *Organy ochrony prawnej w wybranych krajach Unii Europejskiej*, Kancelaria Senatu, Warszawa 2011, s. 15.

[e] *Cyber Security Strategy*, Tallinn 2008, dostęp: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf.

[f] *Three-level IT baseline security system ISKE*, dostęp: https://www.ria.ee/iske-en/.

g) Cyber Security Strategy of the Czech Republic for the 2011–2013, dostęp: https://www.enisa.europa. eu/media/news -items/CZ_Cyber_Security_Strategy_20112015.PDF.

h) https://www.govcert.cz/en/.

i) *Cyber Security Strategy for Germany*, Berlin 2011, dostęp: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

Opracowanie własne.

Analiza zarządzania bezpieczeństwem cyberprzestrzeni w wybranych państwach Unii Europejskiej wykazała tendencję do tworzenia strategii cyberbezpieczeństwa, które wskazują główne priorytety oraz planowane przedsięwzięcia. We wszystkich państwach tworzone są instytucje odpowiedzialne za bezpieczeństwo teleinformatyczne oraz instytucje koordynujące ochronę informacji i usług w sektorze publicznym.

3.6.5. Zarządzanie w NATO

Podczas szczytu praskiego w 2002 roku wydano deklarację szefów państw i rządów, w której dokonano pierwszej próby przeciwdziałania zagrożeniom cybernetycznym. Uzgodniono wówczas, że program ochrony cyberprzestrzeni będzie realizowany w trzech etapach[141]:

- utworzenie NCIRC[142], czyli podmiotu odpowiedzialnego za bezpieczeństwo infrastruktury teleinformatycznej Sojuszu;
- rozwój systemu i wprowadzanie poprawek mających doprowadzić system do optymalnego działania;
- analiza zdarzeń i wniosków wypływających z dwóch poprzednich etapów oraz unowocześnienie systemu tak, aby był w stanie sprostać zagrożeniom wynikającym z rozwoju nowych technologii.

Instytucjonalizacja działalności Sojuszu w obszarze przeciwdziałania cyberzagrożeniom wiąże się z utworzeniem w 2008 roku Centrum Kompetencyjnego ds. Obrony Teleinformatycznej (CCD COE)[143] w Tallinie, po atakach cybernetycznych na Estonię. Misją CCD COE jest stworzenie wymiany informacji między NATO, państwami członkowskimi i innymi partnerami w obszarze cyberobrony

141 P. Borkowski, *NATO a zjawisko cyberterroryzmu* [w:] M. Pietraś, J. Olchowski (red.), *NATO w pozimnowojennym środowisku (nie)bezpieczeństwa*, Lublin 2011, s. 355.

142 Ang. *NATO Computer Incident Response Capability.*

143 Ang. *Cooperative Cyber Defence Centre of Excellence.*

przez szkolenia, wymianę doświadczeń i konsultacje[144]. W 2011 roku Polska stała się członkiem Centrum.

W 2010 roku powołano jednostkę Międzynarodowego Sztabu NATO – Dział Nowych Wyzwań dla Bezpieczeństwa. *Cyberobrona stała się tym samym statutowym zadaniem nowej struktury organizacyjnej. Formalizowanie mechanizmów przeciwdziałania zagrożeniom dla cyberbezpieczeństwa świadczy o tym, iż postrzegane są one jako zjawiska, które będą stanowić stały element środowiska bezpieczeństwa państw NATO*[145]. Powstanie działu związane jest z szerzej pojmowanymi zmianami w zakresie priorytetów bezpieczeństwa oraz dostrzeżeniem konieczności reagowania na wyzwania bezpieczeństwa w takich dziedzinach jak terroryzm, proliferacja broni masowego rażenia, cyberterroryzm oraz bezpieczeństwo energetyczne.

W 2011 roku NATO przedstawiło Politykę Cyberobrony oraz Plan Działania, gdzie uregulowano następujące kwestie[146]:

- planowanie w celu wspólnej obrony i zarządzania kryzysowego;
- prewencja, odporność i obrona krytycznych zasobów cyfrowych NATO i sojuszników;
- wypracowanie solidnych zdolności obronnych;
- opracowanie minimalnych krajowych wymagań dla obrony elementów teleinformatycznej infrastruktury krytycznej;
- udzielanie pomocy w celu osiągnięcia minimalnego poziomu ochrony przed atakami cybernetycznymi;
- współdziałanie z partnerami organizacji międzynarodowych, sektora prywatnego i środowiska ekonomicznego.

W dokumentach zawarto definicję centralnej struktury odpowiedzialnej za ochronę wszystkich struktur Sojuszu (rys. 3.14).

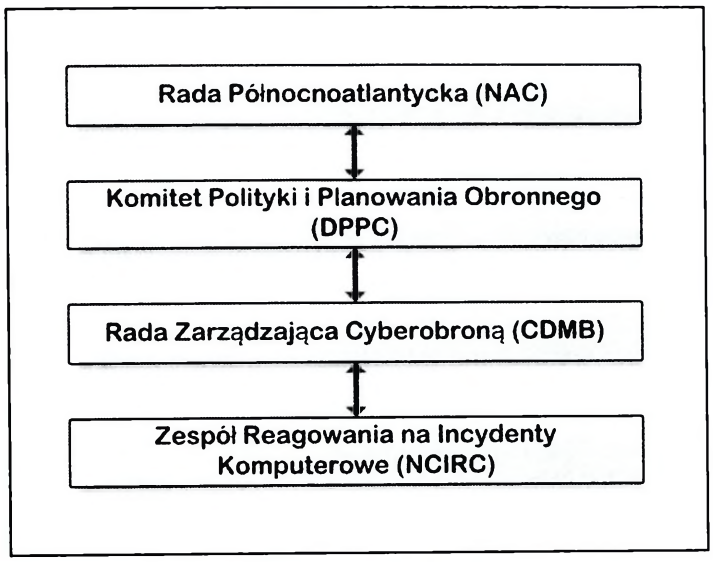
W obszarze zarządzania bezpieczeństwem cyberprzestrzeni NATO warto zwrócić uwagę na funkcje poszczególnych instytucji. Rada Północnoatlantycka jest organem decyzyjnym Sojuszu. Doradztwo i koordynacja w zakresie cyberobrony odbywa się przez Komitet Polityki i Planowania Obronnego (DPPC). Rada Zarządzająca Cyberobroną (CDMB) odpowiada natomiast za koordynację instytucji wojskowych i cywilnych. NCIRC jest odpowiedzialne za techniczną koordynację działań w obszarze:

144 B. Grenda, *Cyber-bezpieczeństwo operacji powietrznych NATO* [w:] R. Czulda, R. Łoś, J. Reginia-Zacharski (red.), *NATO wobec wyzwań współczesnego świata*, Warszawa–Łódź 2013, s. 209.

145 K. Liedel, *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej* [w:] *Bezpieczeństwo w XXI wieku: asymetryczny świat*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2011, s. 441.

146 *NATO has constituted Cyber Response Teams*, dostęp: http://securityaffairs. co/wordpress/20705/cyber-warfare-2/nato-attack-response-teams. html.

- udzielania pomocy zaatakowanym strukturom,
- minimalizacji ryzyka kradzieży lub utraty informacji,
- reagowania w obszarze sprawdzonych procedur.



Opracowanie własne na podstawie: Defending the networks. The NATO Policy on Cyber Defence, http://www.nato. int/nato_ static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

Rys. 3.14. Model zarządzania cyberbezpieczeństwem NATO

W koncepcji NCIRC przyjęto trójwarstwową strukturę zarządzania. Istotną kwestią jest współpraca narodowych zespołów CERT z NCIRC, która może się odbywać na zasadzie koordynacji lub wsparcia technicznego.

Również w 2011 roku opracowano w USA pierwszą Międzynarodową Strategię Cyberbezpieczeństwa[147]. W dokumencie podkreślono konieczność budowy sieci międzynarodowych partnerstw w celu utworzenia globalnej „cyberkoalicji". Zaproponowano, aby decyzje w ramach struktury podejmowano na zasadzie konsensusu. USA chce określić odpowiedzialność za poszczególne elementy globalnej sieci, aby uniknąć dublowania zadań poszczególnych podmiotów.

Wizja określona w strategii sprowadza się do siedmiu priorytetowych obszarów działań[148]:

- gospodarka – wspieranie międzynarodowych standardów, wolnego rynku oraz ochrona własności intelektualnej;
- ochrona sieci – zwiększenie poziomu bezpieczeństwa, niezawodności i odporności, usprawnienie procedur reagowania kryzysowego, tworzenie partnerstw oraz jednolitych norm zachowania w sprawie cyberobrony;

147 *International Strategy for Cyberspace...*, op. cit.
148 M. Grzelak, *Międzynarodowa strategia USA dla cyberprzestrzeni...*, op. cit., s. 140–141.

- egzekwowanie prawa – tworzenie międzynarodowej polityki walki z cyberprzestępczością, harmonizacja prawa w tym obszarze w celu zgodności z konwencją z Budapesztu[149], zmniejszenie możliwości wykorzystania Internetu do działań przestępczych (np. odcinanie wsparcia finansowego terrorystów);
- współpraca wojskowa – dostosowanie sił zbrojnych do zapewnienia bezpieczeństwa sieci wojskowych oraz rozszerzenie współpracy kolektywnej cyberobrony;
- zarządzanie globalną siecią – wsparcie dla otwartości i innowacji, tworzenie bezpiecznej i niezawodnej infrastruktury oraz prowadzenie wielostronnych dyskusji w obszarze rozwoju Internetu;
- rozwój międzynarodowy – tworzenie globalnej społeczności odpowiadającej za rozwój cyberprzestrzeni, wymiana doświadczeń, wiedzy i umiejętności, dobrych praktyk, przeprowadzanie szkoleń dla organów ścigania, prawników i prawodawców oraz rozwój relacji na szczeblu politycznym i eksperckim;
- wolność Internetu – wspieranie społeczeństwa obywatelskiego, wolności wypowiedzi, prawa do stowarzyszania, ochrona danych i prywatności, współpraca z organizacjami pozarządowymi oraz zapewnienie wolnego przepływu informacji (np. zapobieganie cenzurze w Internecie).

Obszary te mają być podzielone między departamenty i agencje amerykańskie przy współpracy z partnerami sektora publicznego i prywatnego. Ich realizacja jest przedsięwzięciem, które łączy elementy dyplomacji, obronności oraz działania na rzecz rozwoju Internetu.

W 2013 roku zatwierdzono pierwszy etap integracji celów i zdolności cyberobrony do procesu planowania obronnego sojuszników i ustanowienia minimalnego zestawu cyberobrony i gotowości. NATO zwróciło się wówczas do państw członkowskich o określenie krajowych polityk cyberbezpieczeństwa oraz organów właściwych w tym obszarze i tworzenie zdolności reagowania na cyberzagrożenia[150]. Wspólny wysiłek państw członkowskich jest niezbędny do obrony teleinformatycznej infrastruktury krytycznej Sojuszu.

Również w 2013 roku z inicjatyw pięciu państw członkowskich (Holandii, Danii, Norwegii, Rumunii, Kanady) powstał projekt wielonarodowych zdolności do cyberobrony (*Multinational Cyber Defence Capability Development Project*, MCDCDP)[151]. Projekt powstał w celu rozwoju wielonarodowych zdolności związanych z cyberobroną. Istotną reformą w ramach Sojuszu jest możliwość powołania się na artykuł piąty traktatu waszyngtońskiego w przypadku ataku na sieci teleinformatyczne. W ramach harmonizacji prawa Polska znowelizowała ustawę o stanie wojennym w omawianym obszarze.

149 Konwencja o cyberprzestępczości..., op. cit.

150 *NATO has constituted...*, op. cit.

151 R. Czulda, *Atak w wirtualu*, http://www.polska-zbrojna.pl/home/articleinmagazineshow/10171?t= ATA K-W-WIRTUALU.

4. EWALUACJA SYSTEMU ZARZĄDZANIA CYBERBEZPIECZEŃSTWEM STRUKTUR ADMINISTRACYJNYCH

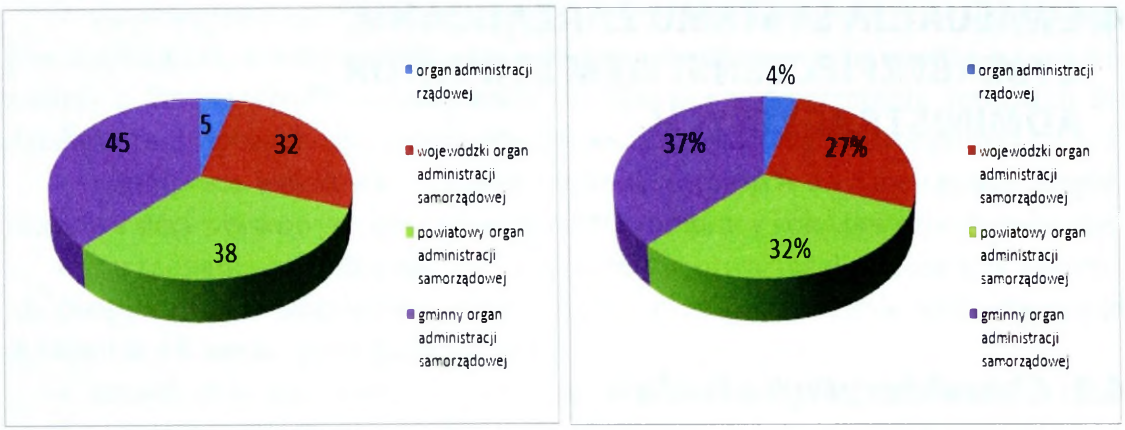
4.1. Charakterystyka badań

Niniejszy rozdział poświęcono ocenie systemu zarządzania bezpieczeństwem struktur administracyjnych w oparciu o wyniki badań ankietowych oraz przedstawieniu rekomendacji dotyczących zmian w funkcjonującym systemie. Problematyka badań wyrażona w tytule monografii determinowała wybór obiektów analiz empirycznych, czyli osób zatrudnionych w strukturach administracyjnych w Polsce.

Kwestionariusz ankiety rozesłano łącznie do 250 jednostek administracji publicznej. Odpowiedź uzyskano z 47 jednostek, co stanowi 18% jednostek, do których rozesłano kwestionariusz. Łącznie w badaniu wzięło 120 pracowników zatrudnionych w strukturach administracyjnych. Podczas doboru próby badawczej starano się zbadać populacje należące do różnych szczebli administracji publicznej. Uzyskane wyniki wskazują jednak na tendencję, zgodnie z którą jednostki niższego szczebla w strukturze administracji publicznej chętniej udzielały odpowiedzi.

Pytania zawarte w kwestionariuszu ankiety miały sprzyjać realizacji celu założonego we wstępie. Problematyka pytań w ankiecie została sformułowana z uwzględnieniem rozważań zawartych w poprzednich rozdziałach, uwzględniała także cechy społeczno-demograficzne respondentów. Wśród tych zmiennych znalazły się: typ jednostki administracji publicznej, w której są zatrudnieni respondenci, wiek, płeć, poziom i typ wykształcenia, zajmowane stanowisko oraz staż pracy. Przeprowadzone badania wykazały, że ankietowani są w istotnym stopniu zróżnicowani pod względem cech społeczno-demograficznych.

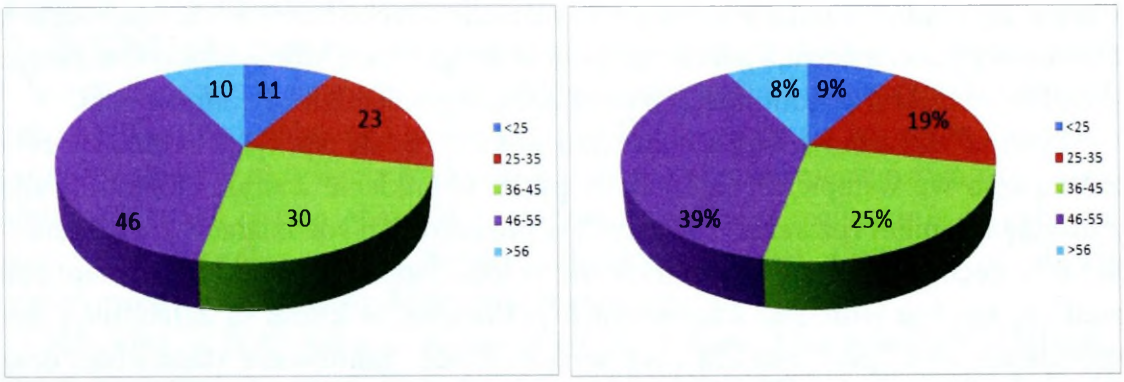
Pod względem struktury administracyjnej, w której zatrudnieni są ankietowani, rozkład procentowy uzyskanych odpowiedzi zgodnie z uszeregowaniem malejącym przedstawia się następująco: gminne organy samorządowe – 37%, powiatowe organy samorządowe – 32%, wojewódzkie organy samorządowe – 27%. Najmniejszą liczbę odpowiedzi uzyskano ze struktur administracji rządowej. Wśród jednostek, do których rozesłano ankiety, znalazły się zarówno naczelne i centralne organy, jak i terenowe jednostki administracji rządowej. Niemniej jednak w wyniku prowadzonych badań uzyskano jedynie wyniki na poziomie 4% w stosunku do jednostek administracji samorządowej. Szczegółowy rozkład ilościowy i procentowy osób biorących udział w badaniu ze względu na typ jednostki administracji publicznej przedstawia rys. 4.1.



Opracowanie własne.

Rys. 4.1. Rozkład ilościowy i procentowy osób biorących udział w badaniu ze względu na typ jednostki administracji publicznej

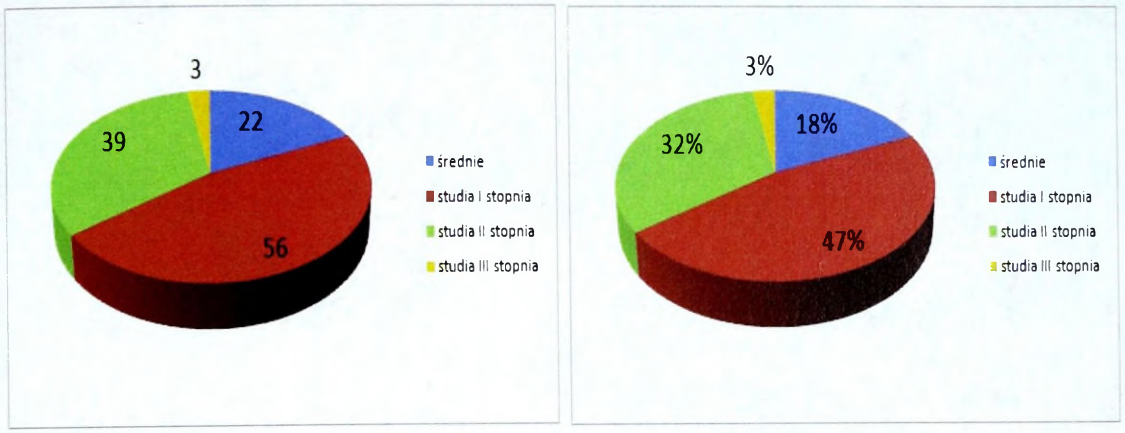
Wśród badanych znalazły się 82 kobiety i 38 mężczyzn, co stanowi odpowiednio udział procentowy 68% i 32%. Jeśli chodzi o przedziały wiekowe respondentów, najwięcej osób znalazło się w przedziale 46–55 lat, natomiast najmniej poniżej 25 lat. Szczegółowy rozkład ilościowy i procentowy wieku ankietowanych przedstawia rys. 4.2.



Opracowanie własne.

Rys. 4.2. Rozkład ilościowy i procentowy wieku osób biorących udział w badaniu

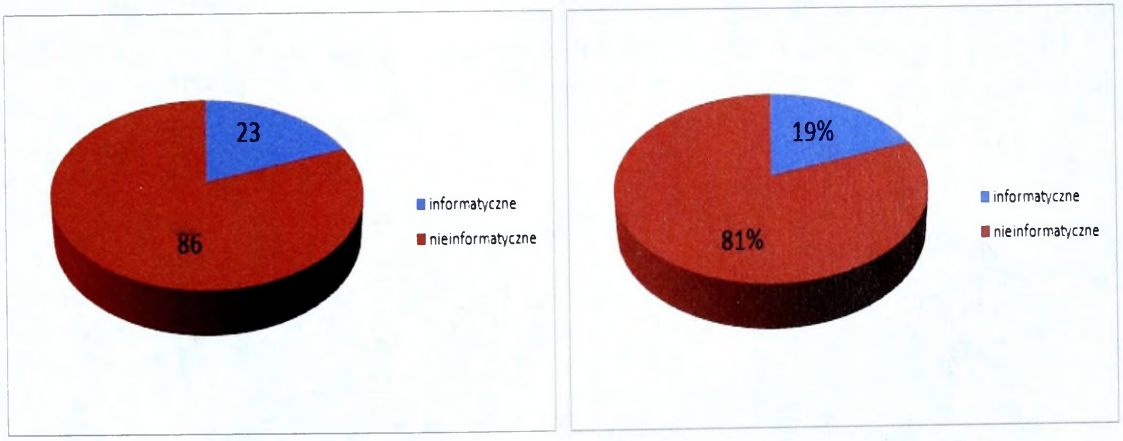
Respondenci charakteryzują się istotnym zróżnicowaniem pod względem posiadanego wykształcenia (średnie, studia I stopnia, studia II stopnia, studia III stopnia). Na podstawie odpowiedzi ankietowanych największy odsetek osób posiada ukończone studia I stopnia – 47% próby badawczej. Najmniej osób posiada ukończone studia III stopnia – 3%. Szczegółowy rozkład ilościowy i jakościowy respondentów pod kątem posiadanego wykształcenia przedstawia rys. 4.3.



Opracowanie własne.

Rys. 4.3. Rozkład ilościowy i procentowy wykształcenia osób biorących udział w badaniu

Wśród pytań w kwestionariuszu ankiety znalazło się także pytanie dotyczące typu posiadanego wykształcenia ze względu na podział – studia informatyczne i studia nieinformatyczne. Większość respondentów, ponad 80%, posiada wykształcenie nieinformatyczne. Szczegółowy rozkład ilościowy i procentowy przedstawiono na rys. 4.4.



Opracowanie własne.

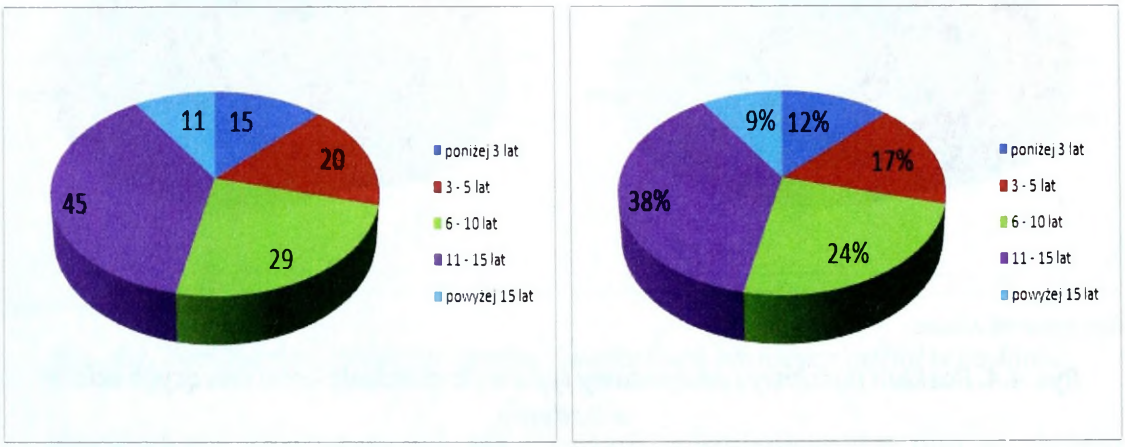
Rys. 4.4. Rozkład ilościowy i procentowy typu wykształcenia osób biorących udział w badaniu

Kolejne pytanie w kwestionariuszu dotyczyło stanowiska zajmowanego w strukturach administracyjnych. Pod tym względem największy odsetek stanowią osoby pracujące na stanowisku pracownika biurowego – 63%, natomiast najmniejszy osoby z kadry zarządzającej – 3%. Procentowy i ilościowy podział ze względu na zajmowane stanowisko przedstawiono na rys. 4.5.

Opracowanie własne.

Rys. 4.5. Rozkład ilościowy i procentowy zajmowanego stanowiska osób biorących udział w badaniu

Istotne zróżnicowanie ankietowanych wykazały odpowiedzi udzielane na temat stażu pracy w strukturach administracyjnych. Wśród możliwych odpowiedzi podano pięć przedziałów: poniżej 3 lat, 3–5 lat, 6–10 lat, 11–15 lat, powyżej 15 lat. Analiza odpowiedzi udzielanych przez respondentów wykazała, że największą grupę stanowią osoby pracujące od 11 do 15 lat, natomiast najmniejszą osoby ze stażem poniżej 3 lat. Szczegółowy rozkład ilościowy i jakościowy stażu pracy ankietowanych przedstawia rys. 4.6.



Opracowanie własne.

Rys. 4.6. Rozkład ilościowy i procentowy stażu pracy osób biorących udział w badaniu

Charakterystyka próby badawczej miała na celu prezentację cech społeczno-demograficznych osób biorących udział w badaniu. Ponadto ilościowa prezentacja danych niezbędna jest do określenia zależności między zmiennymi zależnymi i niezależnymi w dalszych etapach opracowania wyników badań. Zgodnie z zasadami analizy danych statystycznych zastosowano ilościową i jakościową prezentację wyników badań. Ponadto istotną kwestią jest określenie relacji między udzielanymi odpowiedziami a cechami społeczno-demograficznymi ankietowanych, do których oceny wykorzystano w szczególności współczynnik kontyngencji C Pearsona, test niezależności Chi-2, test U Manna-Whitneya oraz test Kruskala-Wallisa. Badanie relacji przy pomocy wymienionych modeli matematycznych pozwala wnioskować o problemach występujących w danych grupach społecznych. Zebrane wyniki umożliwiają także dostrzeżenie nieprawidłowości w funkcjonowaniu badanego systemu.

W związku z celami monografii wyodrębniono obszary określające kierunki oraz zakres badań:

- ewolucja struktur administracyjnych,
- zagrożenia cyberprzestrzeni państwa dla bezpieczeństwa struktur administracyjnych,
- zarządzanie bezpieczeństwem cyberprzestrzeni struktur administracyjnych.

Z uwagi na fakt rosnącej liczby stwierdzonych naruszeń bezpieczeństwa istnieje potrzeba zmian w systemie zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych, z wiodącą rolą czynnika ludzkiego. Pożądane jest zatem określenie słabych i mocnych stron w funkcjonującym systemie zarządzania cyberbezpieczeństwem struktur administracyjnych, z uwzględnieniem rozważań zawartych w poprzednich rozdziałach oraz wyników badań empirycznych. Ponadto istotną kwestią jest przedstawienie rekomendacji dotyczących zmian w systemie sprzyjających zapewnieniu bezpieczeństwa w kontekście możliwych i prawdopodobnych zagrożeń cyberprzestrzeni państwa w postaci modelu systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych.

4.2. Ewolucja struktur administracyjnych

Wśród przyjętych obszarów badawczych pierwszy dotyczył ewolucji struktur administracyjnych. W kwestionariuszu ankiety zawarto pytania dotyczące tego zakresu (tab. 4.1).

Tab. 4.1. Pytania ankietowe dotyczące ewolucji struktur administracyjnych

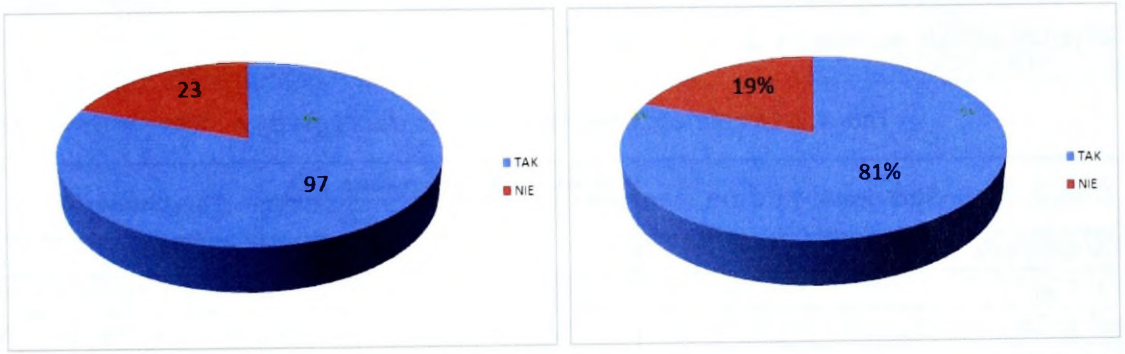
W jaki sposób rewolucja informacyjna wpłynęła na system zarządzania administracją publiczną?		
Nr[a)]	**Treść pytania w kwestionariuszu ankiety**	**Możliwe odpowiedzi**
1	Według Pani/Pana, czy rewolucja informacyjna wpłynęła na system zarządzania administracją publiczną?	– tak – nie
2	Według Pani/Pana, które z wymienionych elementów są następstwem rewolucji informacyjnej dla struktur administracyjnych: – e-administracja, – podnoszenie jakości usług, – zmiana organizacji pracy w instytucji, – uprawnienie działania organizacji, – komplikacja procedur administracyjnych, – wzrost cyberzagrożeń? Proszę podać wagę.	– nieistotne – mało istotne – umiarkowanie istotne – istotne – istotne – bardzo istotne
Od jakich czynników zależy bezpieczeństwo struktur administracyjnych oraz w jakiej relacji pozostaje ono z jakością świadczonych usług?		
Nr	**Treść pytania w kwestionariuszu ankiety**	**Możliwe odpowiedzi**
3	Czy według Pani/Pana wymienione zagrożenia wpływają na bezpieczeństwo struktur administracyjnych: – katastrofy naturalne, – niezwiązane z postępowaniem człowieka (np. awarie zasilania, błędy w oprogramowaniu), – błędy i pomyłki ludzkie, – celowe, szkodliwe działania pracowników, – cyberzagrożenia?	– tak – nie
4	Według Pani/Pana, w jakim stopniu zagrożenia dla bezpieczeństwa administracji publicznej wpływają na jakość świadczonych usług? Proszę zaznaczyć jedną odpowiedź.	– znikomym – niskim – średnim – poważnym – krytycznym
Od jakich czynników zależy efektywność wdrażania e-administracji?		
Nr	**Treść pytania w kwestionariuszu ankiety**	**Możliwe odpowiedzi**
5	Według Pani/Pana, które z wymienionych elementów stanowią największą barierę w korzystaniu z usług e-administracji? – brak umiejętności w zakresie korzystania z e-usług administracji, – zbyt mała liczba usług, których całkowita transakcja jest możliwa za pośrednictwem Internetu, – brak zaufania obywateli do e-administracji, – odnotowane przypadki naruszeń bezpieczeństwa informacji danych osobowych, – inne?	– wybór jednej odpowiedzi

6	Czy zgadza się Pani/Pan z tym, że organy administracji publicznej wywiązują się ze swoich obowiązków w zakresie informatyzacji administracji publicznej? Proszę zaznaczyć jedną odpowiedź.	– zdecydowanie się nie zgadzam – raczej się nie zgadzam – nie mam zdania – raczej się zgadzam – zdecydowanie się zgadzam

[a] Numer pytania w kwestionariuszu ankiety.

Opracowanie własne.

Odpowiedź twierdząca na pytanie nr 1 przeważała w większości przypadków – aż 81%. Rozkład procentowy oraz ilościowy odpowiedzi na pytanie nr 1 przedstawiono na rys. 4.7.



Opracowanie własne.

Rys. 4.7. Ocena wpływu rewolucji informacyjnej na model zarządzania administracją publiczną

W stosunku do odpowiedzi na pytanie nr 1 zawarte w kwestionariuszu ankiety zachodzą bardzo istotne zależności statystyczne pomiędzy cechami społeczno-demograficznymi respondentów a udzielanymi przez nich odpowiedziami. Osoby z dłuższym stażem pracy znacznie częściej odpowiadały twierdząco na pytanie dotyczące oceny wpływu rewolucji informacyjnej na struktury administracyjne.

W celu określenia siły zależności między uzyskanymi odpowiedziami a stażem pracy ankietowanych wykorzystano współczynnik kontyngencji C Pearsona, który oparty jest na teście niezależności Chi-2 (inaczej x^2 albo Ch-kwadrat niezależności). Wartość testu niezależności Chi-2 jest równa kwadratowi różnicy między wartością zaobserwowaną a oczekiwaną w każdej klasie, podzielonemu przez wartość oczekiwaną dla danej grupy. Wzór na test niezależności ma zatem następującą postać:

$$x^2 = \sum_{j=1}^{k} \frac{(O_j - E_j)^2}{Ej}$$

gdzie:
x^2 – test niezależności Chi-2,
O_j – liczebność obserwowana dla danej grupy,
E_j – liczebność oczekiwana dla danej grupy.

Badania zależności pomiędzy zmiennymi dotyczą dwóch czynników – A i B. W przypadku testów wielowymiarowych określa się hipotezę zerową i alternatywną. Na potrzeby badań empirycznych zostały określone następujące hipotezy:

H_0 – czynniki A i B są niezbieżne,

H_1 – czynniki A i B są zbieżne.

W badaniu otrzymano dwie grupy zmiennych A – staż pracy, B – odpowiedzi. Wyniki zostały przedstawione w tab. 4.2.

Tab. 4.2. Liczebność obserwowana dla danej grupy o_j

Staż pracy	Wartość obserwowana – O_j		Suma
	Tak	Nie	
poniżej 3 lat	4	11	15
3–5 lat	15	5	20
6–10 lat	27	2	29
11–15 lat	41	4	45
powyżej 15 lat	10	1	11
SUMA	97	23	120

Opracowanie własne.

Na podstawie otrzymanych wyników wylicza się liczebność oczekiwaną, czyli wartość odpowiadającą liczbie jednostek (n), które powinny znaleźć się w danym przedziale, gdyby były one sobie równe. W badaniu mamy dwie możliwe do udzielenia odpowiedzi, dlatego wartość oczekiwana wynosi 50% i 50%. Wobec powyższego wartości oczekiwane będą odpowiadały liczbom przedstawionym w tab. 4.3.

Tab. 4.3. Liczebność oczekiwana dla danej grupy E_j

Staż pracy	Wartość oczekiwana – E_j		Suma
	Tak	Nie	
poniżej 3 lat	7,5	7,5	15
3–5 lat	10	10	20
6–10 lat	14,5	14,5	29
11–15 lat	22,5	22,5	45
powyżej 15 lat	5,5	5,5	11

Opracowanie własne.

Znając wartości liczebności obserwowanej i oczekiwanej można obliczyć wartość testu niezależności Chi-2 (tab. 4.4).

Tab. 4.4. Obliczenia dla testu niezależności Chi-2

A	B	O_i	E_i	$O_i - E_i$	$(O_i - E_i)^2$	$\frac{(O_i - E_i)^2}{Ej}$
TAK	poniżej 3 lat	4	7,5	-3,5	12,25	1,633333333
	3–5 lat	15	10	5	25	2,5
	6–10 lat	27	14,5	12,5	156,25	10,77586207
	11–15 lat	41	22,5	18,5	342,25	15,21111111
	powyżej 15 lat	10	5,5	4,5	20,25	3,681818182
NIE	poniżej 3 lat	11	7,5	3,5	12,25	1,633333333
	3–5 lat	5	10	-5	25	2,5
	6–10 lat	2	14,5	-12,5	156,25	10,77586207
	11–15 lat	4	22,5	-18,5	342,25	15,21111111
	powyżej 15 lat	1	5,5	-4,5	20,25	3,681818182
Wynik testu niezależności Chi-2						**67,60424939**

Opracowanie własne.

Wynik testu niezależności stanowi wartość empiryczną statystyki Chi-2. W celu weryfikacji hipotezy zerowej i alternatywnej niezbędne jest wyznaczenie wartości krytycznej dla testu niezależności Chi-2. Jeżeli wartość empiryczna Chi-2 jest większa lub równa wartości krytycznej statystyki Chi-2, wówczas cechy pomiędzy badanymi czynnikami są zbieżne, a szansa pomyłki jest mniejsza lub równa poziomowi istotności (α)[1]. Poziom istotności został określony na poziomie 0,05. Jest to wartość przyjmowana bardzo często w analizach statystycznych, ponieważ przyjęcie niskiego poziomu istotności pozwala na ograniczenie błędu.

Poza znajomością poziomu istotności, w celu oszacowania wartości krytycznej należy wyznaczyć stopień swobody, który dla testu niezależności Chi-2 oblicza się według wzoru $(r - 1) \times (p - 1)$, gdzie r i p oznaczają liczbę kategorii dla pierwszej i drugiej zmiennej. W badanym przypadku występuje $r = 5$ (dwie możliwe odpowiedzi dla zmiennej A) oraz $p = 2$ (dwie możliwe odpowiedzi dla zmiennej B). Podstawiając te wartości do wzoru, otrzymujemy liczbę stopni swobody: $(5 - 1) \times (2 - 1) = 4$.

Znając poziom istotności oraz stopień swobody, wartość krytyczną testu Chi-2 można odczytać z tablic statystycznych. Na potrzeby monografii został jednak wykorzystany program MS Excel, gdzie wartość krytyczną testu niezależności można wyznaczyć za pomocą następującej formuły: ROZKŁAD.CHI.ODW(POZIOM ISTOTNOŚCI; POZIOM SWODODY). W rozpatrywanym przypadku

1 B. Pułaska-Turyna, *Statystyka dla ekonomistów*, Warszawa 2011, s. 285.

otrzymano wartość krytyczną testu niezależności Chi-2 równą 9,487729037. Wartość ta jest mniejsza od wartości empirycznej statystyki Chi-2, co oznacza zgodnie z przyjętymi wcześniej założeniami, że badane cechy są zbieżne.

Wykazana zbieżność cech pozwoliła na ocenę związku między dwoma cechami jakościowymi, który została wyznaczona za pomocą współczynnika kontyngencji C Pearsona. Współczynnik ten wskazuje na siłę relacji pomiędzy badanymi czynnikami i przyjmuje dla przyjętych przedziałów określoną interpretację. Gdy współczynnik C wynosi:

0–0,2 – występuje bardzo słaby związek między zmiennymi,
0,2–0,4 – występuje słaby związek,
0,4–0,6 – występuje umiarkowany związek,
0,6–0,8 – występuje silny związek,
0,8–1,0 – występuje bardzo silny związek.

Współczynnik C Pearsona obliczany jest według następującego wzoru:

$$C = \sqrt{\frac{x^2}{x^2 + n}}$$

gdzie:
C – współczynnik kontyngencji C Pearsona,
x^2 – test niezależności Chi-2,
n – liczebność próby badawczej.

Podstawiając wartości do wzoru, otrzymujemy współczynnik kontyngencji C = 0,60, co oznacza, że występuje silny związek między badanymi zmiennymi. Podsumowując, w prowadzonych badaniach otrzymano wyniki przedstawione w tab. 4.5.

Tab. 4.5. Relacje zachodzące pomiędzy oceną wpływu rewolucji informacyjnej na system zarządzania administracją publiczną a stażem pracy ankietowanych

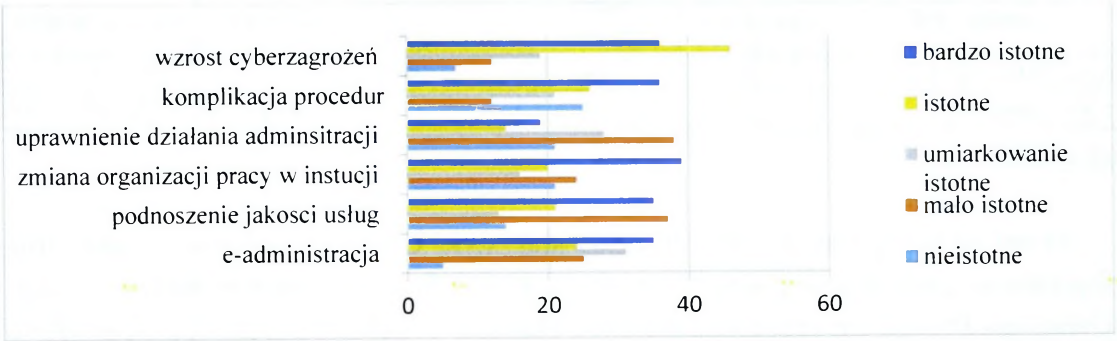
Określenie badanych zmiennych		**Wartość empiryczna Ch-2**	**Poziom istotności**	**Liczba stopni swobody**	**Współczynnik kontyngencji C Pearsona**	**Siła zależności**
Ocena wpływu...	Staż pracy	67,6042	0,05	4	0,98	Bardzo silny związek

Opracowanie własne.

Badania wykazały bardzo silną korelację między oceną wpływu rewolucji informacyjnej na system zarządzania administracją publiczną a stażem pracy. Przy obliczaniu testu niezależności Chi-2 oraz współczynnika kontyngencji C Pearsona w dalszych etapach badań postępowanie odbywa się zgodnie z zaprezentowanym

przykładem. Ze względu na zastosowanie analogicznego schematu w następnych etapach, zostaną przedstawione jedynie wyniki owych obliczeń.

Pytanie nr 2 dotyczyło określenia następstw rewolucji informacyjnej w stosunku do następujących elementów: e-administracji, podnoszenia jakości usług, zmiany organizacji pracy w jednostce, usprawnienia działania administracji, komplikacji procedur administracyjnych, wzrostu zagrożeń. Zaproponowano pięciostopniową skalę dla przyporządkowania wymienionych czynników do określonych wag według schematu: 1 – nieistotne, 2 – mało istotne, 3 – umiarkowanie istotne, 4 – istotne, 5 – bardzo istotne. Otrzymane wyniki przedstawiono na rys. 4.8.



Opracowanie własne.

Rys. 4.8. Wpływ rewolucji informacyjnej na model zarządzania administracją publiczną

Odpowiedź na pytanie nr 2 polegała na uszeregowaniu wymienionych elementów zgodnie z przyjętą skalą. W przypadku zmiennych nienależących do typu nominalnego w celu zbadania korelacji pomiędzy badanymi cechami stosuje się inne modele matematyczne niż test niezależności Chi-2. Odpowiedzi wskazane w pytaniu nr 2 są danymi typu porządkowego, ponieważ można je uszeregować według skali nasilenia określonego zjawiska.

Analizując odpowiedzi respondentów, można zauważyć zachodzące zależności statystyczne między cechami społeczno-demograficznymi a udzielonymi odpowiedziami. Osoby z wykształceniem informatycznym częściej oceniają e-administrację jako bardzo istotne następstwo rewolucji informacyjnej.

W celu określenia związku miedzy typem wykształcenia a odpowiedziami udzielanymi przez respondentów zastosowano test U Manna-Whitneya. Badanie zależności między dwoma czynnikami A i B wymaga określenia hipotezy zerowej i alternatywnej:

H_0 – czynniki A i B są niezbieżne,

H_1 – czynniki A i B są zbieżne.

W badaniu otrzymano dwie grupy zmiennych: zmienną zależną A (e-administracja, podnoszenie jakości usług, zmiana organizacji pracy w instytucji, usprawnienie działania administracji, komplikacja procedur, wzrost cyberzagrożeń) i zmienną niezależną B (typ wykształcenia).

W omawianym przypadku ograniczono się do zobrazowania metody wykorzystania testu U Manna-Whitneya dla pierwszej podgrupy cech: A (e-administracja), B (typ wykształcenia). Weryfikacja hipotez dla kolejnych podgrup przebiega według tego samego schematu,dlatego zostaną przedstawione jedynie wyniki tego testu. W badanym przypadku otrzymano odpowiedzi przedstawione w tab. 4.6.

Tab. 4.6. Liczebność grupy A i B

Typ wykształcenia – zmienna A	Odpowiedzi – zmienna B				
	nieistotne	mało istotne	umiarkowanie istotne	istotne	bardzo istotne
nieinformatyczne	5	24	28	15	25
informatyczne	0	1	3	9	10

Opracowanie własne.

Przed przystąpieniem do obliczenia statystyki U należy dokonać rangowania obserwacji, czyli uszeregowania uzyskanych wyników od najmniejszego do największego. Proces ten przebiega w trzech etapach: 1) zebranie wyników ze względu na badane grupy; 2) sortowanie rosnące danych dla obu grup i przypisanie im rang w kolejności rosnącej zaczynając od 1; 3) sortowanie rosnące rang w ramach grup. Schemat procesu rangowania dla otrzymanych wyników przedstawia tab. 4.7.

Tab. 4.7. Rangowanie grup

I etap		II etap		Ranga	III etap		
nieistotne	5	nieistotne	0	1	nieistotne	5	4
mało istotne	24	mało istotne	1	2	istotne	15	7
umiarkowanie istotne	28	umiarkowanie istotne	3	3	mało istotne	24	8
istotne	15	nieistotne	5	4	bardzo istotne	25	9
bardzo istotne	25	istotne	9	5	umiarkowanie istotne	28	10
nieistotne	0	bardzo istotne	10	6	nieistotne	0	1
mało istotne	1	istotne	15	7	mało istotne	1	2
umiarkowanie istotne	3	mało istotne	24	8	umiarkowanie istotne	3	3
istotne	9	bardzo istotne	25	9	istotne	9	5
bardzo istotne	10	umiarkowanie istotne	28	10	bardzo istotne	10	6

Opracowanie własne.

Kolejnym etapem jest obliczenie sumy rang dla obydwu grup (R_1, R_2) oraz liczebności tych grup (n_1, n_2). W stosunku do prowadzonego badania otrzymujemy następujące wyniki (tab. 4.8).

Tab. 4.8. Suma rang i liczebność grup

	Suma rang	Liczebność
nieinformatyczne	$R_1 = 38$	$n_1 = 5$
informatyczne	$R_2 = 17$	$n_2 = 5$

Opracowanie własne.

Otrzymane wyniki podstawiamy do wzoru na test U Manna-Whitneya, który ma następującą postać[2]:

$$U = R_{\min(k)} - \frac{n_k(n_k + 1)}{2}$$

gdzie:
U – wynik testu U Manna-Whitneya,
$R_{min(k)}$ – suma rang dla grupy, w której suma jest mniejsza,
n_k – liczba obserwacji w grupie z mniejszą sumą rang.

W badanym przypadku otrzymujemy:

$$U = 17 - \frac{5 \times (5 + 1)}{2} = 2$$

Uzyskany wynik należy porównać z wartościami krytycznymi z tabel statystycznych dla testu U Manna-Whitneya. W przypadku gdy wartość obliczona jest mniejsza lub równa wartości krytycznej, odrzucamy hipotezę zerową. Na rys. 4.9 przedstawiono fragment tablic statystycznych dla badanych grup.

Otrzymany wynik testu U jest równy wartości krytycznej. Należy wiec odrzucić hipotezę zerową. Badania prowadzą do wniosku, że istnieje zależność między udzielaniem odpowiedzi w przypadku e-administracji a typem wykształcenia. Wyniki obliczeń testu dla pozostałych zmiennych przedstawia tab. 4.9.

2 Wzór wykorzystuje się dla małej próby. Dla większej liczby obserwacji statystykę przybliża się rozkładem normalnym, zatem do obliczenia wykorzystuje się test Z. Oblicza się wartość oczekiwaną i wariancję dla testu U Manna-Whitneya. Następnie wykorzystuje się wzór na test U Manna-Whitneya, z wykorzystaniem testu Z.

n		Wielkość największej grupy (n_2)																			
		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
(n_1)	3	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10
	4	1	2	3	4	4	5	6	7	8	9	10	11	11	12	13	14	15	16	17	17	18
	5	2	3	5	6	7	8	9	11	12	13	14	15	17	18	19	20	22	23	24	25	27
	6		5	6	8	10	11	13	14	16	17	19	21	22	24	25	27	29	30	32	33	35
	7			8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44

Źródło: http://www.naukowiec.org/tablice/statystyka/rozklad-wartosci-u-manna-whitneya_345.html.

Rys. 4.9. Rozkład wartości krytycznych dla testu U Manna-Whitneya dla poziomu istotności p = 0,05

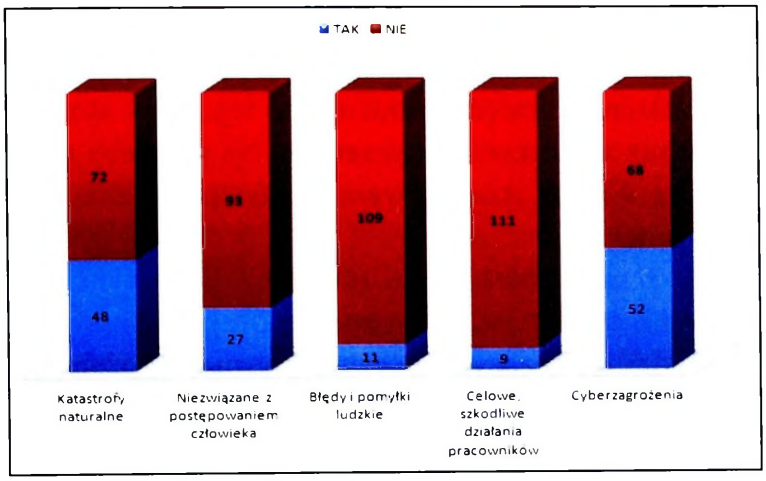
Tab. 4.9. Relacje zachodzące między zmiennymi A i B

Zmienna		Wynik testu U	Wartość krytyczna	Weryfikacja hipotezy
A	B			
Podnoszenie jakości usług	Typ wykształcenia	1	2	Odrzucenie hipotezy zerowej H_0. Istnieje zależność między zmiennymi A i B.
Zmiana organizacji pracy w instytucji		1	2	Odrzucenie hipotezy zerowej H_0. Istnieje zależność między zmiennymi A i B.
Usprawnienie działania		4	2	Przyjęcie hipotezy zerowej H_0. Zmienne A i B są niezbieżne.
Komplikacja procedur		2	2	Odrzucenie hipotezy zerowej H_0. Istnieje zależność między zmiennymi A i B.
Wzrost cyberzagrożeń		1	2	Odrzucenie hipotezy zerowej H_0. Istnieje zależność między zmiennymi A i B.

Opracowanie własne.

Przeprowadzona analiza wykazała, że istnieje zależność miedzy typem wykształcenia a określeniem wpływu rewolucji informacyjnej na następujące zmienne: podnoszenie jakości usług, zmiana organizacji pracy w instytucji, komplikacja procedur i wzrost cyberzagrożeń. Osoby z wykształceniem informatycznym wskazywały bardzo istotny wpływ rewolucji informacyjnej na e-administrację, podnoszenie jakości usług oraz wzrost cyberzagrożeń. Natomiast osoby nieposiadające wykształcenia informatycznego wskazywały istotny wpływ rewolucji informacyjnej na zmianę organizacji pracy w instytucji oraz komplikację procedur.

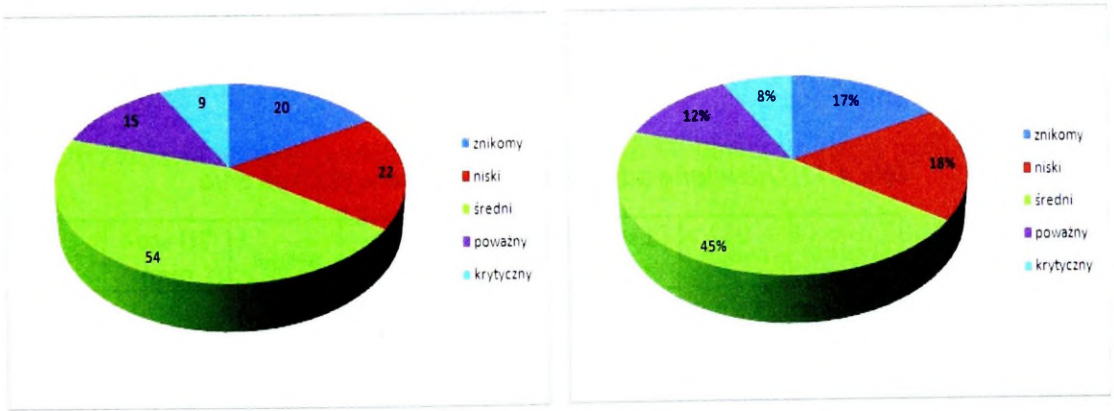
Pytanie nr 3 dotyczyło oceny wpływu wymienionych zagrożeń na bezpieczeństwo struktur administracyjnych. Największą grupę zagrożeń dla bezpieczeństwa struktur administracyjnych według ankietowanych stanowią cyberzagrożenia – 17,33% twierdzących odpowiedzi. Pozostałe grupy zagrożeń kształtują się na następującym poziomie: 16% – katastrofy naturalne, 9% – zagrożenia niezwiązane z postępowaniem człowieka, 3,67% – błędy i pomyłki ludzkie oraz 3% – celowe, szkodliwe działania pracowników. Rozkład ilościowy odpowiedzi respondentów przedstawiono na rys. 4.10.



Opracowanie własne.

Rys. 4.10. Rozkład ilościowy oceny wpływu zagrożeń na bezpieczeństwo struktur administracyjnych

Pytanie nr 4 dotyczyło oceny wpływu zagrożeń dla bezpieczeństwa administracji publicznej na jakość świadczonych usług. Najwięcej osób uznało, że zagrożenia mają średni wpływ na jakość świadczonych usług. Kolejna według wielkości grupa wskazała na niski wpływ zagrożeń na jakość usług. Jedynie 8% ankietowanych uznało, że wystąpienie zagrożeń ma krytyczny wpływ na jakość usług. Odpowiedzi respondentów przedstawiono na rys. 4.11.



Opracowanie własne.

Rys. 4.11. Rozkład ilościowy i procentowy oceny wpływu zagrożeń na jakość usług

Analizując odpowiedzi respondentów, można zauważyć zachodzące zależności statystyczne między cechami społeczno-demograficznymi a udzielonymi odpowiedziami. Przeprowadzone badania wykazały zależność między udzielanymi odpowiedziami a poziomem wykształcenia. Należy zauważyć, że pierwsza grupa zmiennych (A – udzielane odpowiedzi) jest typu porządkowego, natomiast

druga grupa zmiennych (B) ma więcej niż dwie podgrupy, tzn. średnie, I stopień, II stopień, III stopień.

Do określenia zależności między zmiennymi tego typu stosuje się inne modele matematyczne niż wykorzystane wcześniej. Na potrzeby monografii zastosowano test Kruskala-Wallisa. Analiza wymaga sformułowania hipotezy zerowej i hipotezy alternatywnej:

H_0 – czynniki A i B są niezbieżne, tzn. nie różnicują otrzymanego wyniku,

H_1 – czynniki A i B są zbieżne, tzn. różnicują otrzymany wynik.

Liczbę odpowiedzi dotyczących oceny wpływu zagrożeń na jakość usług z uwzględnieniem posiadanego wykształcenia prezentuje tab. 4.10.

Tab. 4.10. Udzielane odpowiedzi a poziom wykształcenia

	średnie	I stopień	II stopień	III stopień
znikomy	7	6	7	0
niski	6	7	9	0
średni	5	34	15	0
poważny	3	3	8	1
krytyczny	1	4	0	2

Opracowanie własne.

Przed przystąpieniem do obliczenia statystyki testu Kruskala-Wallisa należy dokonać rangowania obserwacji. Wyniki rangowania przedstawia tab. 4.11. W badanym przypadku występują rangi wiązane, tzn. cechy o tej samej wielkości. Wówczas wartość rangi stanowi iloraz sumy rang (które zostałyby przypisane kolejno) i liczby rang.

Tab. 4.11. Udzielane odpowiedzi a poziom wykształcenia

	średnie	ranga	I stopień	ranga	II stopień	ranga	III stopień	ranga
znikomy	7	15	6	12,5	7	15	0	2,5
niski	6	12,5	7	15	9	18	0	2,5
średni	5	11	34	20	15	19	0	2,5
poważny	3	8,5	3	8,5	8	17	1	2,2
krytyczny	1	2,2	4	10	0	2,5	2	7

Opracowanie własne.

Po przypisaniu rang można przystąpić do obliczenia wartości statystyki testu Kruskala-Wallisa, którą oblicza się z wzoru:

$$T = \frac{12}{N(N+1)} \times \sum_{i=1}^{p} \frac{R_i^2}{n_i} - 3(N+1)$$

gdzie:
T – wynik testu Kruskala-Wallisa,
N – liczba wszystkich obserwacji,
p – liczba porównywanych grup,
R_i – suma rang w danej grupie,
n_i – liczba obserwacji w grupie.

Obliczenia testu Kruskala-Wallisa dla uzyskanych odpowiedzi udzielanych przez respondentów zostały przedstawione w tab. 4.12.

Tab. 4.12. Obliczenia dla testu Kruskala-Wallisa

	Średnie	**I stopień**	**II stopień**	**III stopień**
n_i	5	5	5	5
N	5 x 4 = 20			
R_i	49,2	66	71,5	16,7
R_i^2	2420,64	4356	5112,25	278,89
$\frac{R_i^2}{n_i}$	484,128	871,2	1022,45	55,778
$\sum_{i=1}^{p} \frac{R_i^2}{n_i}$	2433,356			

Opracowanie własne.

Otrzymane wyniki podstawiamy do wzoru. W badanym przypadku otrzymujemy:

$$T = \frac{12}{20 \times (20+1)} \times 2433{,}356 - 3 \times (20+1) = 6{,}53$$

W celu weryfikacji hipotezy zerowej należy porównać otrzymany wynik z wartością krytyczną. W tym celu należy wyznaczyć stopień swobody, dla testu Kruskala-Wallisa, który oblicza się według wzoru k – 1, gdzie k to liczba badanych grup. Zatem stopień swobody wynosi 4 – 1 = 3. Ponadto poziom istotności został określony na poziomie 0,05. Jest to wartość przyjmowana bardzo często w analizach statystycznych, gdyż przyjęcie niskiego poziomu istotności pozwala na ograniczenie błędu. Wówczas w tablicach statystycznych rozkładu wartości krytycznych dla testu Kruskala-Wallisa odczytujemy wartość krytyczną dla poziomu istotności p = 0,05 oraz stopnia swobody 3. W tym przypadku wartość krytyczna testu wynosi 7,81473. Gdy wartość obliczona jest mniejsza lub równa wartości krytycznej, odrzucamy hipotezę zerową. Porównując wyliczony wynik

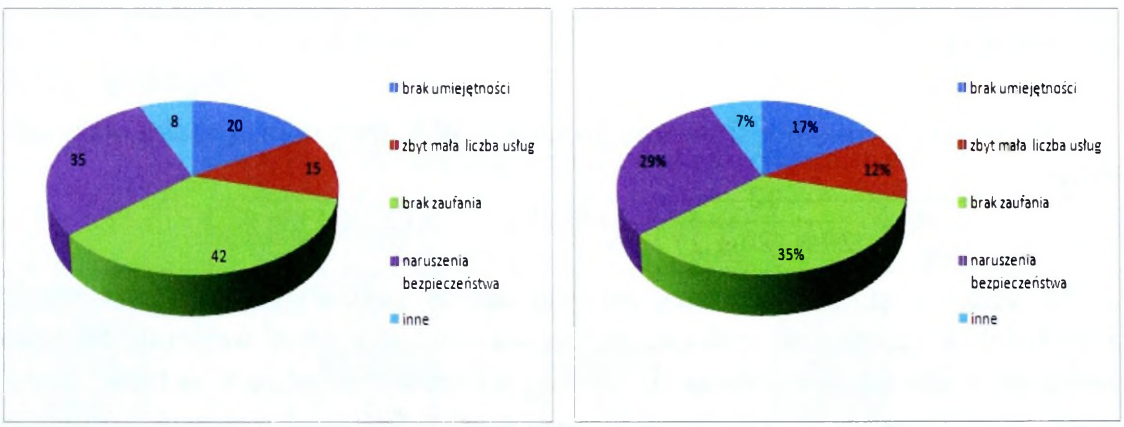
z wartością krytyczną testu, wnioskuje się, że badane cechy są zbieżne i występuje między nimi zależność. Siłę związku między zmiennymi w badanej grupie obliczamy według wzoru:

$$\varepsilon = \frac{T(N+1)}{N^2 - 1}$$

Gdy współczynnik wynosi:
0–0,2 – występuje bardzo słaby związek między zmiennymi,
0,2–0,4 – występuje słaby związek,
0,4–0,6 – występuje umiarkowany związek,
0,6–0,8 – występuje silny związek,
0,8–1,0 – występuje bardzo silny związek.

W badanym przypadku otrzymujemy: $\varepsilon = \frac{6{,}53 \times (20+1)}{20^2 - 1} = 0{,}29$. Uzyskany wynik świadczy o słabym związku między udzielanymi odpowiedziami a poziomem wykształcenia.

Pytanie nr 5 dotyczyło wyrażenia opinii na temat barier korzystania z usług e-administracji. Wśród zaproponowanych odpowiedzi znalazły się: 1) brak umiejętności w zakresie korzystania z e-usług administracji; 2) zbyt mała liczba usług, których całkowita transakcja jest możliwa za pośrednictwem Internetu; 3) brak zaufania obywateli do elektronicznej administracji; 4) odnotowane przypadki naruszeń bezpieczeństwa informacji danych osobowych; 5) inne. Rozkład udzielonych odpowiedzi przedstawiono na rys. 4.12.

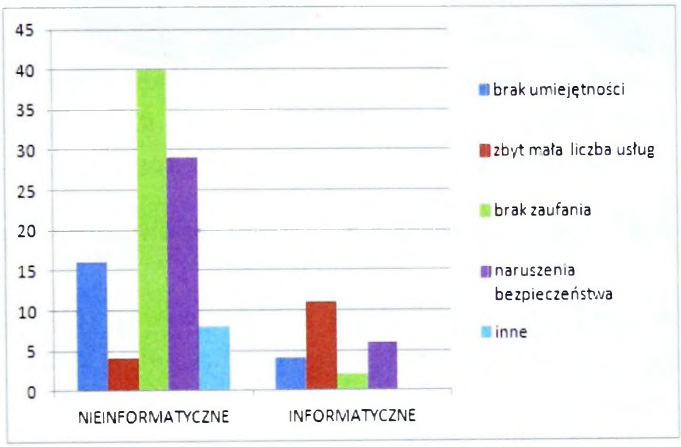


Opracowanie własne.

Rys. 4.12. Rozkład ilościowy i procentowy oceny barier rozwoju e-administracji

Przeprowadzone badania wykazały, że w opinii ankietowanych największą barierę stanowi brak zaufania obywateli do elektronicznej administracji. Wśród otrzymanych wyników można zaobserwować zależność między udzielanymi odpowiedziami a typem wykształcenia (rys. 4.13). Uzyskane wyniki wskazują, że wśród osób o wykształceniu nieinformatycznym najczęściej udzielaną odpowie-

dzią był brak zaufania do e-administracji. Najrzadziej zaznaczaną odpowiedzią była zbyt mała liczba usług. W przypadku osób z wykształceniem informatycznym najwięcej osób podawało, że zbyt mała liczba usług jest największą barierą rozwoju e-administracji. Natomiast najrzadziej wystąpiła odpowiedź brak zaufania.



Opracowanie własne.

Rys. 4.13. Zależność między oceną barier rozwoju e-administracji a wykształceniem

Między typem wykształcenia a udzielonymi odpowiedziami istnieje zależność statystyczna, którą oszacowano Testem Chi-2 oraz oceniono za pomocą współczynnika C Pearsona (tab. 4.13).

Tab. 4.13. Relacje zachodzące pomiędzy oceną barier rozwoju e-administracji a typem wykształcenia

Określenie badanych zmiennych		Wartość empiryczna Chi-2	Poziom istotności	Liczba stopni swobody	Współczynnik kontyngencji C Pearsona	Siła zależności
Bariery rozwoju e-administracji	Typ wykształcenia	67,96	0,05	4	0,60	Silny związek

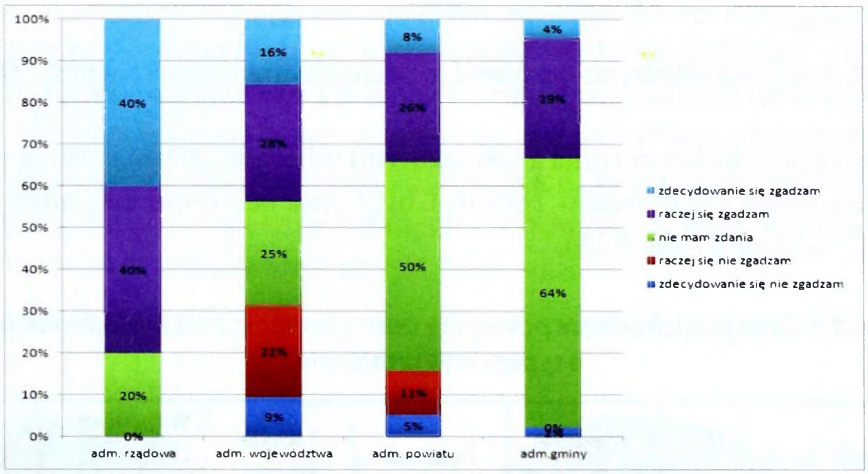
Opracowanie własne.

Pytanie nr 6 dotyczyło oceny organów administracji w obszarze informatyzacji administracji publicznej. Ankietowanych zapytano, czy zgadzają się z tym, że organy administracji publicznej wywiązują się ze swoich obowiązków w zakresie informatyzacji administracji publicznej. Jak wynika z analizy uzyskanych odpowiedzi, najwięcej osób nie ma zdania na ten temat (48%). Kolejną co do wielkości grupą jest odpowiedź „raczej się zgadzam" (28%). Najmniej ankietowanych udzieliło odpowiedzi „zdecydowanie się nie zgadzam" (5%). Rozkład ilościowy i procentowy wszystkich odpowiedzi udzielanych przez ankietowanych przedstawiono na rys. 4.14.

Opracowanie własne.

Rys. 4.14. Rozkład ilościowy i procentowy oceny organów administracji publicznej

Wśród otrzymanych wyników można zaobserwować zależność między uzyskanymi wynikami a jednostką administracji publicznej, w której zatrudniony jest respondent (rys. 4.15).



Opracowanie własne.

Rys. 4.15. Rozkład ilościowy i procentowy oceny organów administracji publicznej

W celu zbadania zależności miedzy tego typu zmiennymi wykorzystano test Kruskala-Wallisa, którego wyniki prezentuje tab. 4.14.

Tab. 4.14. Wyniki testu Kruskala-Wallisa

Określenie badanych zmiennych		Test Kruskala-Wallisa	Poziom istotności	Liczba stopni swobody	Wartość krytyczna testu	Współczynnik ε	Siła zależności
Ocena	Miejsce pracy	11,83	0,05	3	9,48	0,04	Umiarkowany związek

Opracowanie własne.

Podsumowując wyniki badań, można zauważyć, że odpowiedzi udzielone przez ankietowanych wskazują na wpływ rewolucji informacyjnej na system zarządzania administracji publicznej. Zależność między oceną a cechami demograficzno-społecznymi pokazuje związek między odpowiedziami a stażem pracy. Pozwala to wnioskować, że osoby z dłuższym stażem pracy, a co za tym idzie większym doświadczeniem lepiej dostrzegają dynamikę zmian. Jako istotne następstwo podawano najczęściej zmianę organizacji pracy, komplikację procedur, powstanie elektronicznych systemów administracji publicznej oraz powstanie cyberzagrożeń. Zmienną zależną w tym wypadku był typ posiadanego wykształcenia. Osoby nie posiadające wykształcenia informatycznego znacznie częściej wskazywały na takie następstwa jak komplikacja procedur. Respondenci o wykształceniu informatycznym łączyli często rewolucję informacyjną z powstaniem e-administracji, podnoszeniem jakości usług oraz usprawnieniem działań administracji. W obydwu grupach na podobnym poziomie kształtuje się stosunek do cyberzagrożeń jako istotny skutek rozwoju nowych technologii.

Odpowiedzi udzielone przez ankietowanych pozwalają na sformułowane następującego wniosku – bezpieczeństwo struktur administracyjnych jest współcześnie determinowane różnego rodzaju zagrożeniami. Najczęściej wybieranymi odpowiedziami były cyberzagrożenia oraz katastrofy naturalne. Respondenci uznali, że błędy i pomyłki ludzkie oraz celowe, szkodliwe działania pracowników w najmniejszym stopniu wpływają na bezpieczeństwo jednostek administracji publicznej. Takie wyniki mogą świadczyć o tym, że w badanych jednostkach pracownicy niechętnie przyznają się do popełnianych błędów czy też szkodliwego działania na rzecz instytucji. Z drugiej zaś strony udzielane odpowiedzi mogą wiązać się z rzadkością występowania tego typu zjawisk w badanej instytucji. W obszarze określenia relacji zachodzących między jakością a bezpieczeństwem ankietowali odpowiadali najczęściej, że występuje średnia zależność miedzy tymi dwoma czynnikami. W próbie badawczej odpowiedzi w tym obszarze są warunkowane w znacznym stopniu poziomem wykształcenia. Osoby z wyższym poziomem wykształcenia znacznie część łączyły zagrożenia z osłabieniem jakości usług administracji publicznej.

Efektywność informatyzacji administracji publicznej zależy od wielu czynników. Ankietowani ocenili, że największą barierą w korzystaniu z usług e-administracji jest brak zaufania do tego typu usług oraz odnotowane naruszenia bezpieczeństwa informacji i usług. Istotnym czynnikiem wskazywanym przez respondentów był także brak umiejętności i wiedzy na temat tego typu usług. Otrzymane wyniki pozwalają wnioskować, że pożądane jest przeprowadzenie kampanii społecznej na temat usług elektronicznej administracji oraz podnoszenie poziomu bezpieczeństwa tych usług. Największy odsetek ankietowanych wskazał, że nie ma zdania na temat realizacji zadań przez organy administracji

publicznej w obszarze informatyzacji. Dlatego istotne wydaje się informowanie obywateli o rozwiązaniach związanych z e-administracją oraz powstawaniem kolejnych e-usług administracji publicznej.

4.3. Zagrożenia cyberprzestrzeni państwa dla struktur administracyjnych

W ramach drugiego obszaru badań sformułowano pytania w kwestionariuszu ankiety przedstawione w tab. 4.15.

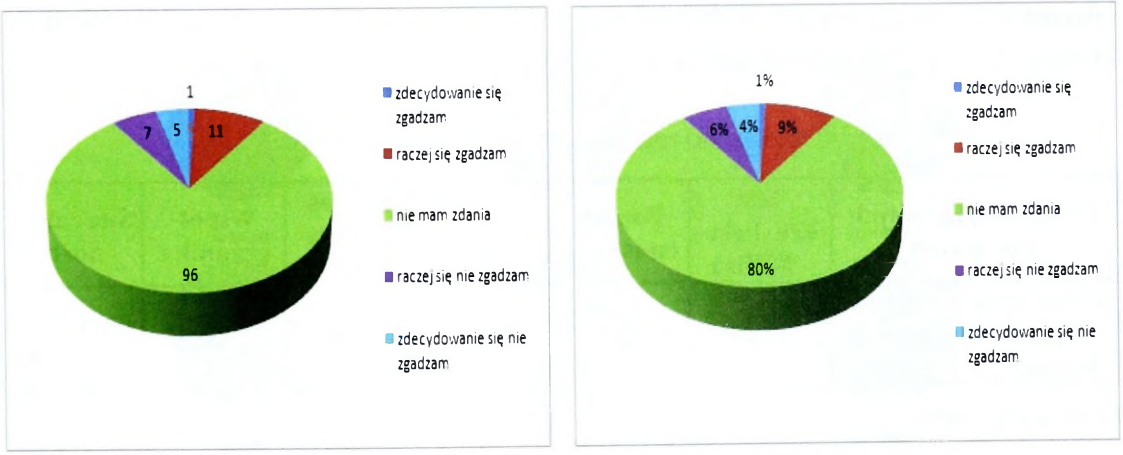
Tab. 4.15. Pytania ankietowe dotyczące zagrożeń cyberprzestrzeni państwa

Jaka jest istota i taksonomia zagrożeń cyberprzestrzeni państwa oraz jaka jest skala świadomości tych zagrożeń wśród pracowników jednostek sektora publicznego?		
Nr	**Treść pytania w kwestionariuszu ankiety**	**Możliwe odpowiedzi**
7	Czy zgadza się Pani/Pan z tym, że wykorzystywanie socjotechniki w atakach na systemy informatyczne struktur administracyjnych ma istotny wpływ na obniżenie ich bezpieczeństwa?	– zdecydowanie się nie zgadzam – raczej się nie zgadzam – nie mam zdania – raczej się zgadzam – zdecydowanie się zgadzam
8	Według Pani/Pana, jaka jest waga poniższych zagrożeń dla bezpieczeństwa informacji i usług w jednostkach administracji publicznej: – działania legalnych wewnętrznych użytkowników (np. ujawnienie danych przez pracownika), – haking, – działania „aktywistów" przeciwko systemom informatycznym, – cyberprzestępczość, – cyberszpiegostwo, – cyberterroryzm, – wojna w cyberprzestrzeni?	– nieistotne – mało istotne – umiarkowanie istotne – istotne – bardzo istotne
9	Jak Pani/Pan ocenia wpływ poniższych cyberzagrożeń na bezpieczeństwo teleinformatyczne: – złośliwe oprogramowanie, – koń trojański, – DoS/DDoS, – spoofing, – phishing, – spyware, – botnet, – backdoor, – keylogger, – rootkit, – chipping?	– duży – mały – nie mam zdania

W jakim zakresie cyberzagrożenia struktur administracyjnych wpływają na poziom bezpieczeństwa narodowego RP?		
Nr	**Treść pytania w kwestionariuszu ankiety**	**Możliwe odpowiedzi**
10	Czy zgadza się Pani/Pan z tym, że wykorzystywanie w atakach na systemy informatyczne e-administracji niekonwencjonalnych środków i technik utrudnia ocenę zagrożenia bezpieczeństwa?	– zdecydowanie się nie zgadzam – raczej się nie zgadzam – nie mam zdania – raczej się zgadzam – zdecydowanie się zgadzam
11	Według Pani/Pana, w jakim stopniu cyberzagrożenia dla bezpieczeństwa struktur administracyjnych mogą osłabić bezpieczeństwo narodowe? Proszę zaznaczyć jedną odpowiedź.	– znikomym – niskim – średnim – poważnym – krytycznym

Opracowanie własne.

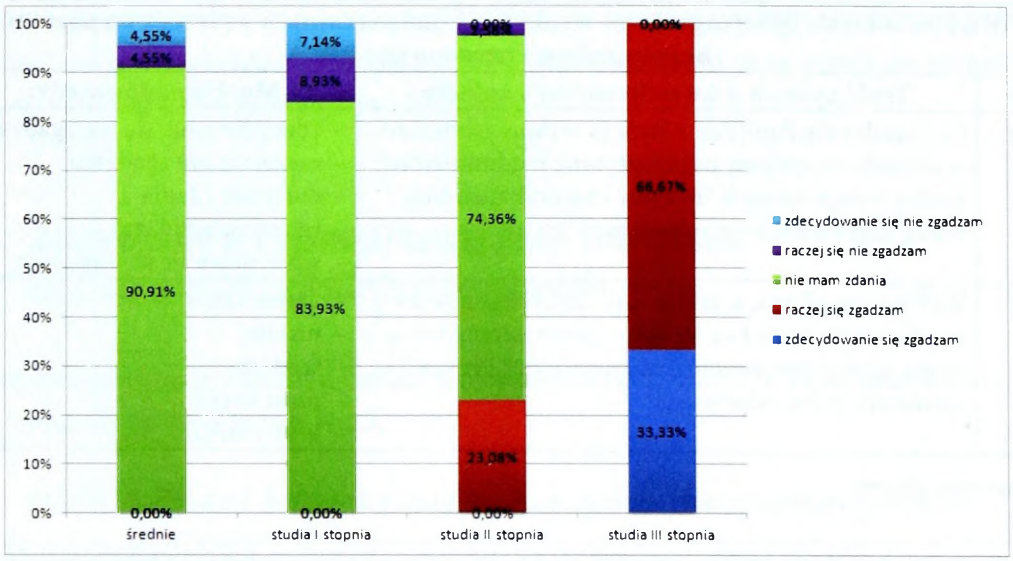
Pytanie nr 7 dotyczyło oceny wpływu socjotechniki na bezpieczeństwo systemów informatycznych e-administracji. Ankietowani w przeważającej większości uznali, że nie mają zdania na ten temat. Jedynie 10 osób udzieliło twierdzącej odpowiedzi na to pytanie. Rozkład procentowy i ilościowy otrzymanych wyników przedstawiono na rys. 4.16.



Opracowanie własne.

Rys. 4.16. Rozkład ilościowy i procentowy oceny wpływu socjotechniki na bezpieczeństwo informatyczne systemów administracji publicznej

Analizując odpowiedzi udzielone przez ankietowanych, można zaobserwować istotną zależność między udzielonymi odpowiedziami a stopniem wykształcenia. Osoby z wykształceniem II i III stopnia w przeważającej liczbie wypadków odpowiadały twierdząco na zadane pytanie. Osoby z wykształceniem średnim najczęściej nie miały zdania na ten temat. Rozkład procentowy udzielanych odpowiedzi w stosunku do posiadanego wykształcenia przedstawia rys. 4.17.



Opracowanie własne.

Rys. 4.17. Rozkład ilościowy i procentowy oceny wpływu socjotechniki na bezpieczeństwo informatyczne systemów administracji publicznej

W celu określenia siły zależności między wymienionymi zmiennymi – udzielanymi odpowiedziami i wykształceniem, wykorzystano test Kruskala-Wallisa, którego wyniki prezentuje tab. 4.16.

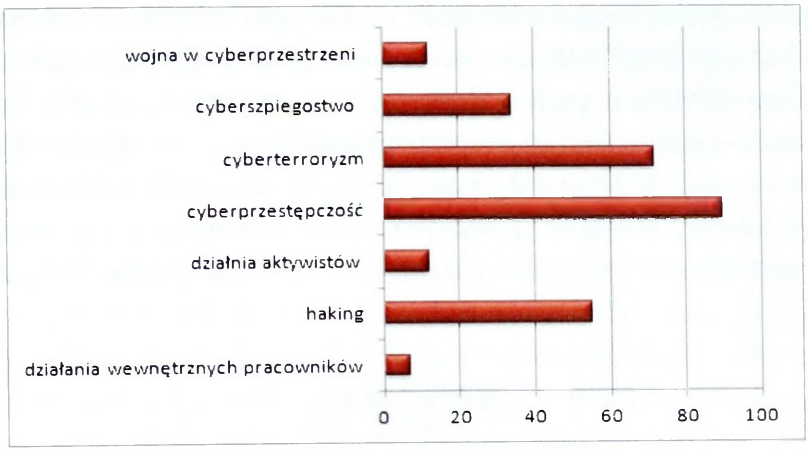
Tab. 4.16. Wyniki testu Kruskala-Wallisa (pytanie nr 7)

Określenie badanych zmiennych		Test Kruskala-Wallisa	Poziom istotności	Liczba stopni swobody	Wartość krytyczna testu	Współczynnik ε	Siła zależności
Ocena wpływu socjotechniki ...	Wykształcenie	17,49	0,05	3	9,48	0,83	Bardzo silny związek

Opracowanie własne.

Otrzymane wyniki pozwalają wnioskować, że dużej grupie respondentów brakuje wiedzy na temat zagrożeń socjotechnicznych. W tym miejscu warto przypomnieć statystyki publikowane m.in. przez CERT.GOV, które wskazują, że działania socjotechniczne są obecnie istotnym problemem w obszarze bezpieczeństwa teleinformatycznego systemów administracji publicznej.

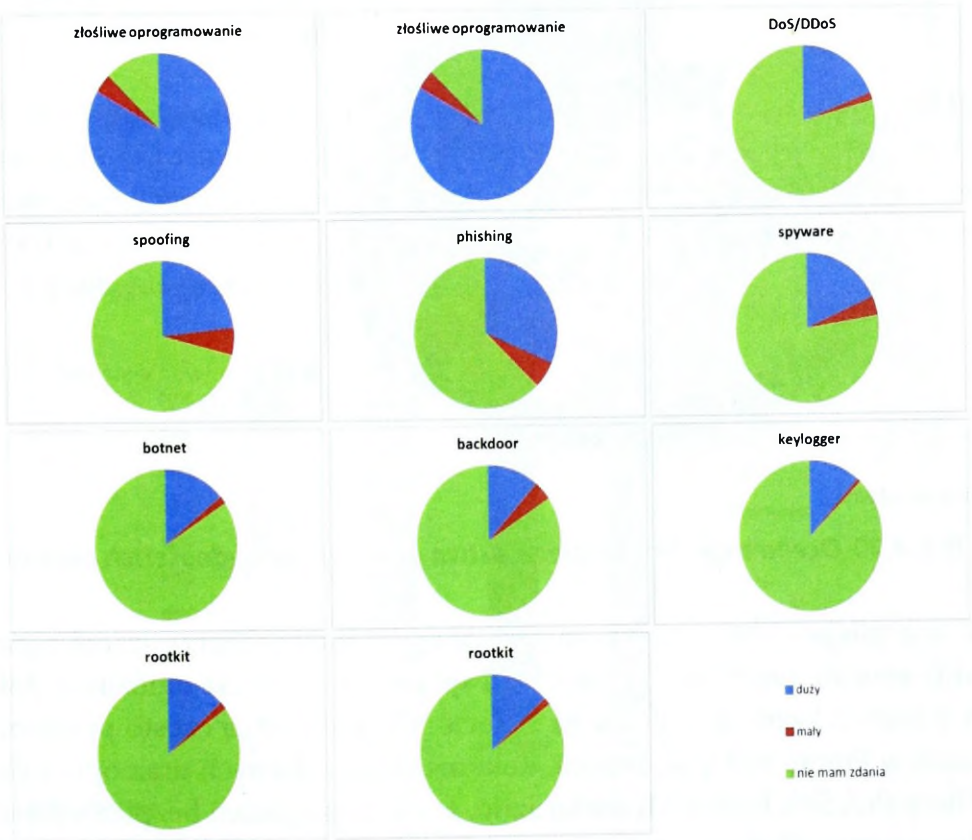
Odpowiedź na pytanie nr 8 wiązała się z dokonaniem wyboru (co najmniej dwóch i maksymalnie czterech) najpoważniejszych zagrożeń dla cyberbezpieczeństwa administracji publicznej. Ankietowani najczęściej wskazywali, że najpoważniejszym zagrożeniem jest obecnie cyberprzestępczość, następnie cyberterroryzm. Jedynie siedem osób wybrało działania wewnętrznych pracowników. Rozkład ilościowy udzielonych odpowiedzi przedstawiono na rys. 4.18.



Opracowanie własne.

Rys. 4.18. Ocena wpływu zagrożeń na bezpieczeństwo informacji i usług

Pytanie nr 9 dotyczyło oceny wpływu wymienionych w pytaniu zagrożeń na bezpieczeństwo teleinformatyczne administracji publicznej. Wśród możliwych odpowiedzi znalazły się: duży wpływ, mały wpływ oraz brak zdania. Liczebność uzyskanych odpowiedzi przedstawia rys. 4.19.

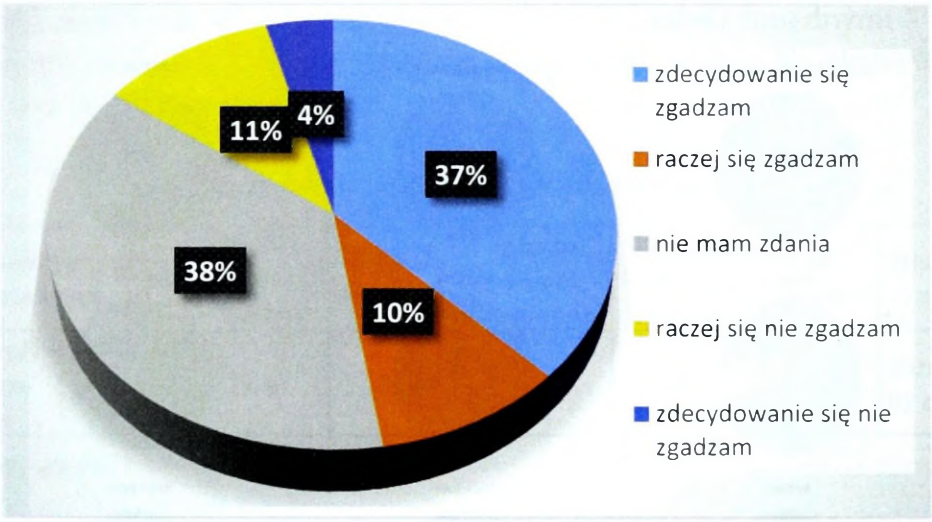


Opracowanie własne.

Rys. 4.19. Ocena wpływu cyberzagrożeń na bezpieczeństwo teleinformatyczne

Najczęściej respondenci stwierdzali, że nie mają zdania na ten temat, co pozwala wnioskować, że ankietowani posiadają małą wiedzę na temat zagrożeń teleinformatycznych. W przypadku złośliwego oprogramowania oraz konia trojańskiego badani stwierdzili, że stanowią one poważne zagrożenie dla bezpieczeństwa teleinformatycznego. W pozostałych przypadkach ponad 75% odpowiedzi to brak opinii na dany temat. Nawet w przypadku – zdaniem autorki – powszechnie używanych w mediach czy też w witrynach internetowych banków terminów, takich jak np. phishing, respondenci nie wykazali się wiedzą w tym zakresie. Między udzielanymi odpowiedziami a typem wykształcenia istnieje istotna statystycznie zależność. Osoby z wykształceniem informatycznym znacznie rzadziej odpowiadały, że nie mają zdania na ten temat.

Pytanie nr 10 z kwestionariusza ankiety brzmiało: Czy zgadza się Pani/Pan z tym, że wykorzystywanie w atakach na systemy informatyczne e-administracji niekonwencjonalnych środków i technik utrudnia ocenę zagrożenia bezpieczeństwa? Analizując odpowiedzi ankietowanych, można dostrzec dwie dominujące pod względem liczebności grupy odpowiedzi – „zdecydowanie się zgadzam" oraz „nie mam zdania". Szczegółowe wyniki przedstawia rys. 4.20.

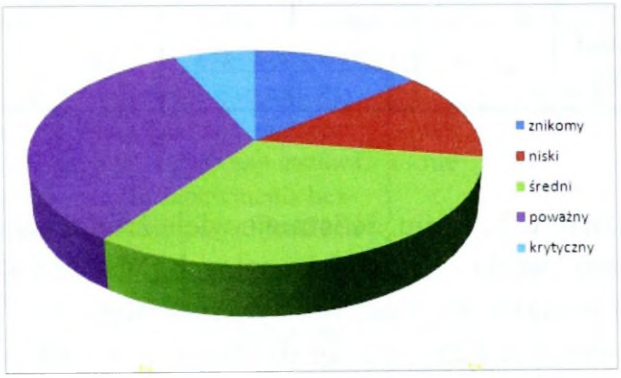


Opracowanie własne.

Rys. 4.20. Ocena zagrożeń bezpieczeństwa pod kontem trudności ich analizy

W tym miejscu warto przypomnieć, że specyfika cyberprzestrzeni ogranicza w istotny sposób możliwość identyfikacji sprawcy czynu oraz umożliwia dokonywanie ataków z każdego miejsca na świecie. Czynniki te są często przedmiotem rozważań w literaturze przedmiotu, dokumentach prawnych oraz opinii ekspertów. Niespełna 50% badanych stwierdziło, że ocena zagrożeń bezpieczeństwa jest utrudniona ze względu na stosowanie niekonwencjonalnych metod i technik.

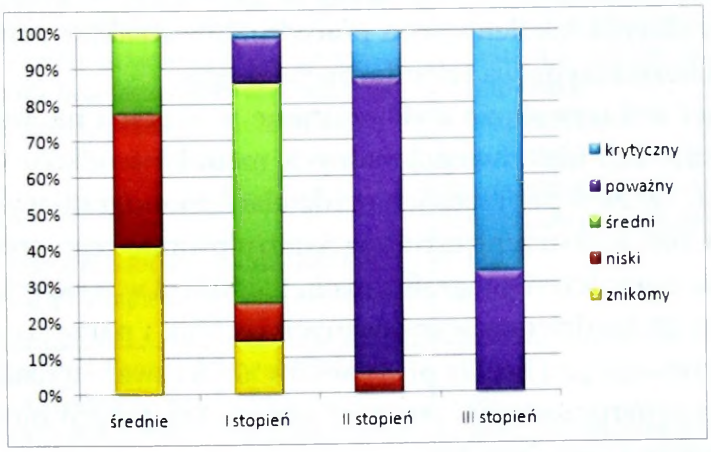
W pytaniu nr 11 ankietowani oceniali wpływ cyberzagrożeń bezpieczeństwa struktur administracyjnych na bezpieczeństwo narodowe. Możliwe odpowiedzi były typu porządkowego: znikomy, niski, średni, poważny, krytyczny. W przeważającej liczbie przypadków respondenci uznali, że cyberzagrożenia dla bezpieczeństwa struktur administracyjnych mają średni wpływ na bezpieczeństwo narodowe. Druga co do wielkości grupa ankietowanych uznała, że zagrożenia te mają poważny wpływ na bezpieczeństwo narodowe. Rozkład ilościowy udzielonych odpowiedzi przedstawiono na rys. 4.21.



Opracowanie własne.

Rys. 4.21. Ocena wpływu zagrożeń bezpieczeństwa teleinformatycznego na struktury administracyjne

Między odpowiedziami udzielanymi na pytanie nr 10 a posiadanym wykształceniem zachodzą istotne statystycznie zależności. Osoby z wyższym poziomem wykształcenia znacznie częściej oceniały wpływ cyberzagrożeń jako poważny bądź krytyczny. Szczegółowy rozkład uzyskanych wyników w stosunku do poziomu wykształcenia przedstawia rys. 4.22.



Opracowanie własne.

Rys. 4.22. Ocena wpływu zagrożeń bezpieczeństwa teleinformatycznego na struktury administracyjne według stopnia wykształcenia

W celu określenia siły zależności między wymienionymi zmiennymi (udzielane odpowiedzi i wykształcenie) zastosowano test Kruskala-Wallisa, którego wyniki prezentuje tab. 4.17.

Tab. 4.17. Wyniki testu Kruskala-Wallisa (pytanie nr 10)

Określenie badanych zmiennych		Test Kruskala-Wallisa	Poziom istotności	Liczba stopni swobody	Wartość krytyczna testu	Współczynnik ε	Siła zależności
Ocena wpływu socjotechniki ...	Wykształcenie	22,44	0,05	3	9,48	1	Bardzo silny związek

Opracowanie własne.

Ankietowani uznali w badaniu, że istnieje wiele źródeł zagrożeń bezpieczeństwa cyberprzestrzeni struktur administracyjnych. Wśród najczęściej występujących odpowiedzi znalazły się działania cyberprzestępców i cyberterrorystów. Najrzadziej respondenci wskazywali, że działania wewnętrznych pracowników stanowią poważne zagrożenie dla bezpieczeństwa. Odpowiedzi na bardziej szczegółowe pytania, np. dotyczące metod ataków – pytanie nr 10 oraz działań socjotechnicznych – pytanie nr 7, wykazały istotny brak wiedzy na ten temat wśród pracowników struktur administracyjnych. Osoby z wykształceniem informatycznym oraz wyższym poziomem wykształcenia wykazywały się znacznie większą wiedzą w omawianym zakresie. Należy zauważyć, że powszechne korzystanie z e-usług administracji w Polsce występuje w ograniczonym zakresie. Także poziom informatyzacji tych usług – pełna realizacja usługi za pośrednictwem Internetu – jest niski. Niemniej jednak wysoce prawdopodobne wydaje się przeobrażenie sektora publicznego w tym obszarze. Pozwala to wnioskować o konieczności przeprowadzenia szkoleń wśród pracowników struktur administracyjnych na temat zasad bezpieczeństwa teleinformatycznego.

Respondenci wskazywali, że wykorzystanie w atakach na systemy informatyczne e-administracji niekonwencjonalnych metod i środków utrudnia ocenę bezpieczeństwa. Także w poprzednich rozdziałach monografii wykazano, że istota i specyfika cyberprzestrzeni utrudnia kontrolowanie tego środowiska, m.in. z powodu braku ograniczeń geograficznych, trudności w wykryciu sprawcy oraz powstawania coraz bardziej zaawansowanych technik i narzędzi ataku cybernetycznego. W przeważającej liczbie przypadków ankietowani uznali, że zagrożenia bezpieczeństwa cyberprzestrzeni struktur administracyjnych mogą obniżyć poziom bezpieczeństwa narodowego.

4.4. System zarządzania bezpieczeństwem struktur administracyjnych

Odnośnie systemu zarządzania bezpieczeństwem struktur administracyjnych sformułowano pytania w kwestionariuszu ankiety zaprezentowane w tab. 4.18.

Tab. 4.18. Pytania ankietowe dotyczące systemu zarządzania bezpieczeństwem

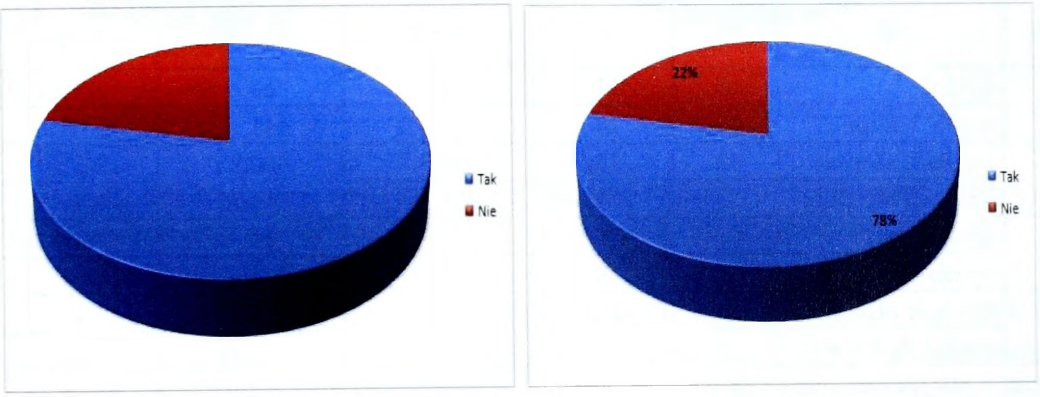
W jakim stopniu rozwiązania prawne wpływają na poziom bezpieczeństwa struktur administracyjnych?		
Nr[a)]	**Treść pytania w kwestionariuszu ankiety**	**Możliwe odpowiedzi**
12	Czy zgadza się Pani/Pan z tym, że konieczne jest tworzenie regulacji prawnych (np. ustawa, rozporządzenie itp.) w celu zapewnienia bezpieczeństwa informacji i usług w jednostkach administracji publicznej?	– tak – nie
13	Według Pani/Pana, jaki wpływ na cyberbezpieczeństwo struktur administracyjnych mają regulacje prawne?	– znikomy – niski – średni – poważny – krytyczny
14	Według Pani/Pana, jaka jest waga poniższych regulacji prawnych dotyczących bezpieczeństwa cyberprzestrzeni struktur administracyjnych: – ustawa, – norma, – rozrządzenie, – wytyczne?	– nieistotne – mało istotne – istotne – umiarkowanie istotne – bardzo istotne
Jakie rozwiązania proceduralne i organizacyjne sprzyjają zapewnieniu cyberbezpieczeństwa struktur administracyjnych?		
15	Według Pani/Pana, jakie rozwiązania w największym stopniu przeciwdziałają cyberzagrożeniom dla bezpieczeństwa administracji publicznej? Proszę zaznaczyć minimum 2 i maksimum 4 odpowiedzi.	– Polityka Bezpieczeństwa Informacji – System Zarządzania Bezpieczeństwem Informacji – analiza ryzyka – audyt informatyczny – procedury i rozwiązania techniczne – szkolenia pracowników
16	Czy w jednostce ustalono strukturę organizacyjną związaną z bezpieczeństwem informacji?	– tak – nie – nie wiem
17	Czy znane są Pani/Panu dokumenty Polityka Bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznym oraz ich założenia?	– tak – nie – wiem, że takie dokumenty istnieją, ale nie znam ich założeń
18	Czy w jednostce wdrożono System Zarządzania Bezpieczeństwem Informacji?	– tak – nie – nie wiem

19	Czy w jednostce przeprowadza się analizę ryzyka?	– tak – nie – nie wiem
20	Czy w jednostce opracowano procedury obsługi incydentów naruszeń bezpieczeństwa informacji?	– tak – nie – nie wiem
Jaka jest znaczenie rozwiązań programowych i sprzętowych w przeciwdziałaniu zagrożeniom dla cyberbezpieczeństwa struktur administracyjnych?		
21	Czy zgadza się Pani/Pan z tym, że konieczne jest stosowanie zabezpieczeń programowych oraz sprzętowych chroniących systemy informatyczne administracji publicznej?	– zdecydowanie się nie zgadzam – raczej się nie zgadzam – nie mam zdania – raczej się zgadzam – zdecydowanie się zgadzam
22	Które z wymienionych rozwiązań są stosowane w jednostce: – firewall, – program antywirusowy, – mechanizmy szyfrowania danych, – wydzielona sieć wirtualna (VPN), – system wykrywania włamań i podatności, – kopie bezpieczeństwa, – zasilanie awaryjne, – audyt informatyczny, – inne (jakie)?	– tak – nie – nie wiem
23	Czy w jednostce stosuje się kontrolę dostępu do zasobów informacyjnych? Jeśli tak, proszę podać, w jaki sposób: – logowanie do komputerów, – logowanie do zasobów sieciowych, – karty elektroniczne/tokeny, – system monitoringu i kontroli haseł, – zabezpieczenia biometryczne?	– tak – nie
Jakie jest znaczenie czynnika ludzkiego w zarządzaniu bezpieczeństwem struktur administracyjnych?		
24	Czy w jednostce przeprowadzono szkolenia pracowników w zakresie bezpieczeństwa informacji?	– tak – nie
25	Według Pani/Pana, w jakim stopniu przestrzeganie zasad bezpieczeństwa przez pracowników wpływa na bezpieczeństwo teleinformatyczne administracji publicznej?	– znikomy – niski – średni – poważny – krytyczny

[a] Numer pytania w kwestionariuszu ankiety

Opracowanie własne.

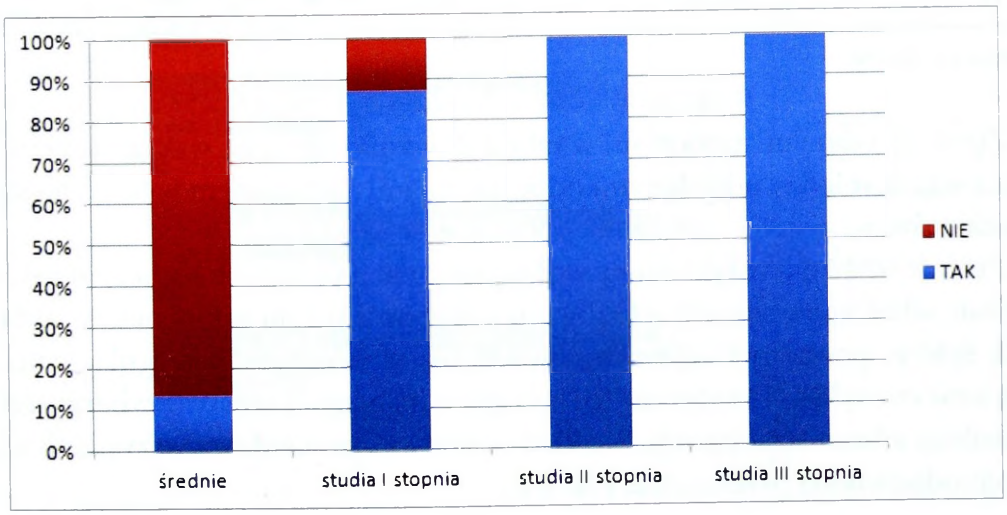
Pytanie nr 12 i 13 w kwestionariuszu ankiety dotyczyły oceny wpływu regulacji prawnych na zapewnienie bezpieczeństwa cyberprzestrzeni struktur administracyjnych. W pytaniu 12 poproszono o wyrażenie opinii na temat konieczności tworzenia regulacji prawnych w celu zapewnienia bezpieczeństwa informacji i usług w jednostkach administracji publicznej. Rozkład ilościowy i procentowy udzielnych odpowiedzi przedstawiono na rys. 4.23.



Opracowanie własne.

Rys. 4.23. Ocena konieczności tworzenia regulacji prawnych w celu zapewnienia bezpieczeństwa informacji i usług w jednostkach administracji publicznej

W stosunku do odpowiedzi na pytanie nr 12 zachodzą bardzo istotne zależności statystyczne pomiędzy cechami społeczno-demograficznymi respondentów a udzielanymi przez nich odpowiedziami. Osoby z wyższym stopniem wykształcenia znacznie częściej odpowiadały twierdząco na zadane pytanie. Szczegółowy rozkład uzyskanych wyników w stosunku do poziomu wykształcenia przedstawia rys. 4.24.



Opracowanie własne.

Rys. 4.24. Ocena konieczności tworzenia regulacji prawnych w celu zapewnienia bezpieczeństwa informacji i usług w jednostkach administracji publicznej

W celu określenia siły zależności między uzyskanymi odpowiedziami (zmienna A) a poziomem wykształcenia ankietowanych (zmienna B) wykorzystano test niezależności Chi-2 oraz współczynnik kontyngencji C Pearsona. Wyniki obliczeń przedstawiono w tab. 4.19 i 4.20.

Tab. 4.19. Obliczenia dla testu niezależności Chi-2

A	B	O_j	E_j	$O_j - E_j$	$(O_j - E_j)^2$	$\frac{(O_j - E_j)^2}{E_j}$
TAK	średnie	3	11	-8	64	5,818182
	studia I stopnia	49	28	21	441	15,75
	studia II stopnia	39	19,5	19,5	380,25	19,5
	studia III stopnia	3	1,5	1,5	2,25	1,5
NIE	średnie	19	11	8	64	5,818182
	studia I stopnia	7	28	-21	441	15,75
	studia II stopnia	0	19,5	-19,5	380,25	19,5
	studia III stopnia	0	1,5	-1,5	2,25	1,5
Wynik testu niezależności Chi-2						85,14

Opracowanie własne.

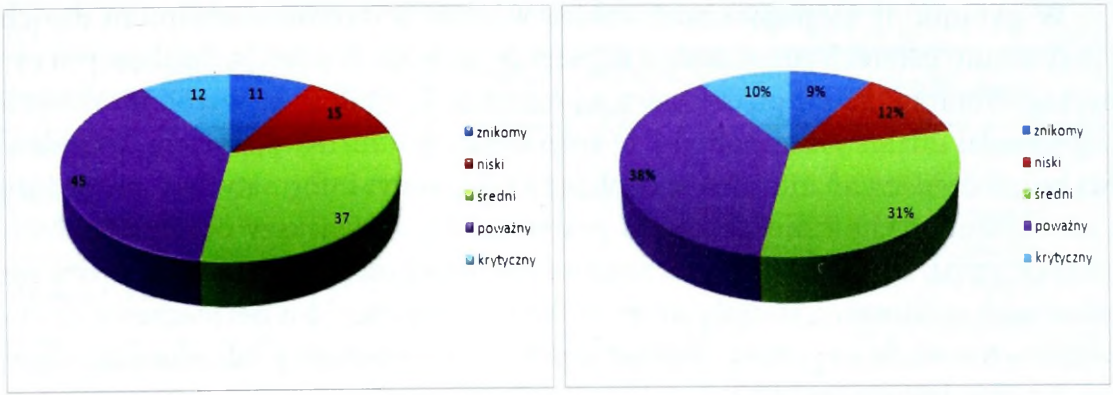
Tab. 4.20. Relacje zachodzące pomiędzy oceną konieczności tworzenia regulacji prawnych w celu zapewnienia bezpieczeństwa informacji i usług a poziomem wykształcenia

Określenie badanych zmiennych		Wartość empiryczna Ch-2	Wartość krytyczna Ch-2	Poziom istotności	Liczba stopni swobody	Współczynnik kontyngencji C Pearsona	Siła zależności
A	B	85,14	7,81	0,05	3	0,99	Bardzo silny związek

Opracowanie własne.

Zgodnie z danymi zawartymi w tabelach wyniki obliczeń wskazują na bardzo silny związek między udzielanymi odpowiedziami a poziomem wykształcenia respondentów.

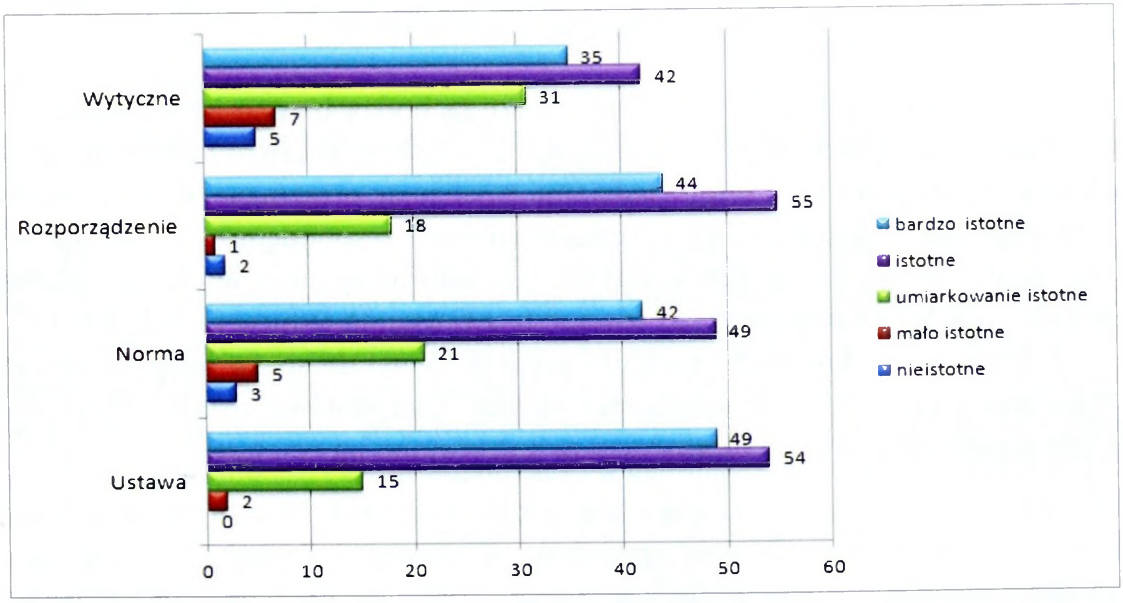
Pytanie nr 13 dotyczyło oceny wpływu regulacji prawnych na bezpieczeństwo struktur administracyjnych. Możliwy był wybór z pięciu odpowiedzi: znikomy, niski, średni, poważny i krytyczny. Najwięcej osób uznało, że regulacje prawne mają poważny (38%) i krytyczny (31%) wpływ na bezpieczeństwo cyberprzestrzeni struktur administracyjnych. Rozkład ilościowy i procentowy wszystkich udzielonych odpowiedzi przedstawia rys. 4.25.



Opracowanie własne.

Rys. 4.25. Ocena konieczności tworzenia regulacji prawnych w celu zapewnienia bezpieczeństwa informacji i usług w jednostkach administracji publicznej

Ankietowani w pytaniu nr 14 oceniali wagę rozwiązań prawnych dotyczących bezpieczeństwa cyberprzestrzeni struktur administracyjnych. Najistotniejszą regulacją prawną według respondentów jest ustawa (49 osób), rozporządzenie (44 osoby) i norma (42 osoby). Uzyskane odpowiedzi pozwalają wnioskować, że ankietowani doceniają wagę poszczególnych rozwiązań prawnych. Za mało istotne i nieistotne respondenci uznali wytyczne (łącznie 12 osób; 10%), rozporządzenie (łącznie 3 osoby; 2,5%), norma (łącznie 8 osób; 6,67%), ustawa (łącznie 2 osoby; 1,67%). Szczegółowy rozkład ilościowy odpowiedzi udzielonych na pytanie nr 14 zawarte w kwestionariuszu ankiety przedstawiono na rys. 4.26.



Opracowanie własne.

Rys. 4.26. Waga regulacji prawnych dotyczących cyberbezpieczeństwa struktur administracyjnych

W pytaniu nr 15 poproszono ankietowanych o wybranie minimum dwóch i maksimum czterech rozwiązań w największym stopniu przeciwdziałających cyberzagrożeniom dla bezpieczeństwa administracji publicznej. Wśród możliwych odpowiedzi znalazły się: polityka bezpieczeństwa informacji, system zarządzania bezpieczeństwem informacji, analiza ryzyka, audyt informatyczny, procedury i rozwiązania techniczne, szkolenia pracowników. Największy odsetek ankietowanych uznał, że polityka bezpieczeństwa i system zarządzania bezpieczeństwem informacji w istotnym stopniu przeciwdziałają zagrożeniom bezpieczeństwa cyberprzestrzeni. Szczegółowy rozkład ilościowy i procentowy udzielonych odpowiedzi przedstawia rys. 4.27.

Opracowanie własne.

Rys. 4.27. Ocena wpływu rozwiązań proceduralnych i organizacyjnych sprzyjających zapewnieniu cyberbezpieczeństwa

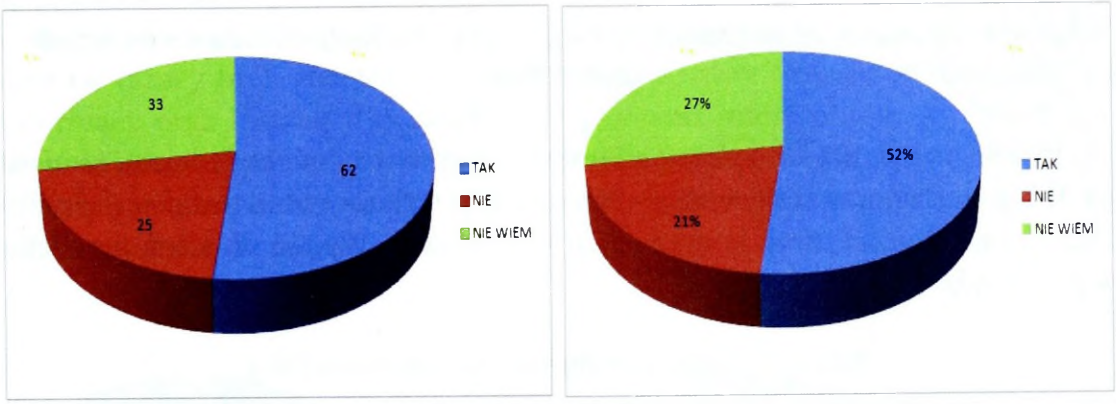
W stosunku do uzyskanych odpowiedzi zachodzą bardzo istotne zależności statystyczne pomiędzy cechami społeczno-demograficznymi respondentów a udzielanymi przez nich odpowiedziami. Analizując otrzymane wyniki, można zaobserwować zależność między odpowiedziami respondentów (zmienna A) oraz typem wykształcenia (informatyczne, nieinformatyczne). W celu określenia związku między zmiennymi zastosowano test U Manna-Whitneya (tab. 4.21).

Pytanie nr 16 dotyczyło struktury organizacyjnej do spraw bezpieczeństwa cyberprzestrzeni struktur administracyjnych. Szczegółowy rozkład ilościowy i procentowy udzielonych odpowiedzi przedstawiono na rys. 4.28.

Tab. 4.21. Wyniki testu U Manna-Whitneya dla pytania nr 15

Zmienna		Wynik testu U	Wartość krytyczna	Weryfikacja hipotezy
A	B			
Polityka bezpieczeństwa informacji	Typ wykształcenia	2	5	Odrzucenie hipotezy zerowej H_0. Zmienna A i B są zależne.
System zarządzania bezpieczeństwem informacji		6	5	Przyjęcie hipotezy zerowej H_0. Zmienne A i B są niezależne.
Analiza ryzyka		5	5	Przyjęcie hipotezy zerowej H_0. Zmienne A i B są niezbieżne.
Audyt informatyczny		2	5	Odrzucenie hipotezy zerowej H_0. Zmienna A i B są zależne.
Procedury i rozwiązania techniczne		1	5	Odrzucenie hipotezy zerowej H_0. Zmienna A i B są zależne.
Szkolenia pracowników		6	5	Przyjęcie hipotezy zerowej H_0. Zmienne A i B są niezależne.

Opracowanie własne.

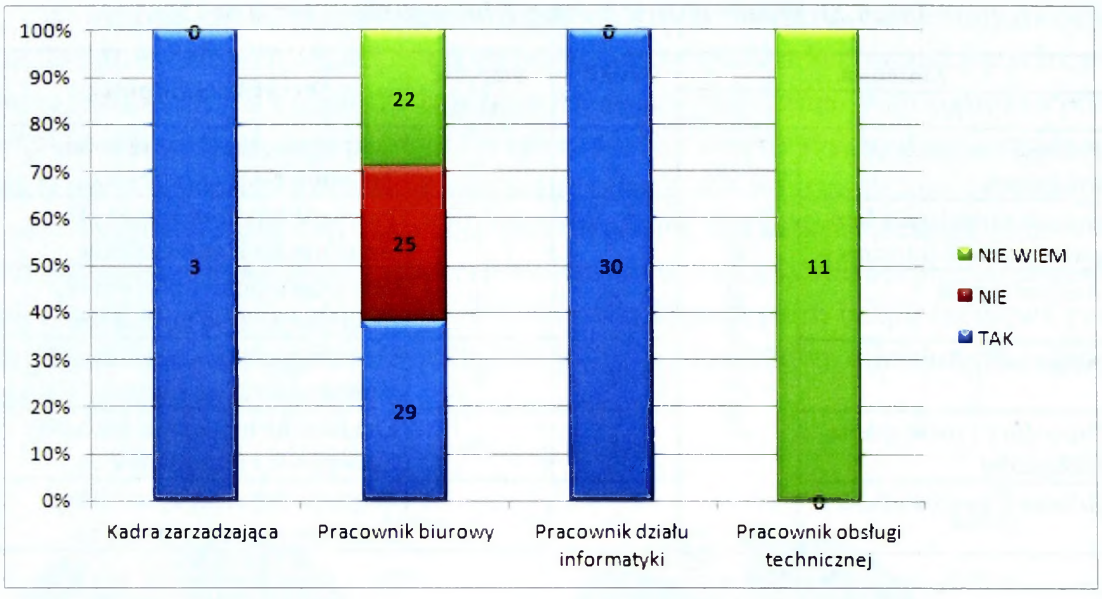


Opracowanie własne.

Rys. 4.28. Struktura organizacyjna ds. bezpieczeństwa cyberprzestrzeni w badanych jednostkach

Zgodnie z rys. 4.28 w przeważającej liczbie przypadków udzielono twierdzącej odpowiedzi. Zaskakujące wydaje się, że ponad jedna czwarta respondentów przyznała, że nie wie, czy istnieje struktura organizacyjna związana z bezpieczeństwem cyberprzestrzeni w ich miejscu pracy. Fakt ten pozwala przypuszczać, że w badanych jednostkach struktura organizacyjna jest określana inną nazwą niż zawarta w pytaniu „struktura organizacyjna ds. bezpieczeństwa cyberprzestrzeni". Być może pytanie nie było sformułowane adekwatnie do rozwiązań funkcjonujących w badanych jednostkach administracji publicznej. Niemniej jednak udzielone odpowiedzi wskazują na fragmentaryczną wiedzę badanych osób na temat bezpieczeństwa cyberprzestrzeni struktur administracyjnych.

W stosunku do otrzymanych wyników można zaobserwować zależność statystyczną między udzielonymi odpowiedziami a zajmowanym stanowiskiem (rys. 4.29).



Opracowanie własne.

Rys. 4.29. Struktura organizacyjna ds. bezpieczeństwa cyberprzestrzeni w badanych jednostkach

W celu określenia siły zależności między uzyskanymi odpowiedziami (zmienna A) a zajmowanym stanowiskiem (zmienna B) wykorzystano test niezależności Chi-2 oraz współczynnik kontyngencji C Pearsona. Wyniki obliczeń przedstawiono w tab. 4.22 i 4.23.

Tab. 4.22. Obliczenia dla testu niezależności Chi-2

A	B	O_i	E_i	$O_i - E_i$	$(O_i - E_i)^2$	$\frac{(O_i - E_i)^2}{E_i}$
TAK	Kadra zarządzająca	3	1	2	4	4
	Pracownik biurowy	29	25,33	3,67	13,4689	0,531737
	Pracownik działu informatyki	30	10	20	400	40
	Pracownik obsługi technicznej	0	3,67	-3,67	13,4689	3,67
NIE	Kadra zarządzająca	0	1	-1	1	1
	Pracownik biurowy	25	25,33	-0,33	0,1089	0,004299
	Pracownik działu informatyki	0	10	-10	100	10
	Pracownik obsługi technicznej	0	3,67	-3,67	13,4689	3,67
NIE WIEM	Kadra zarządzająca	0	1	-1	1	1
	Pracownik biurowy	22	25,33	-3,33	11,0889	0,437777
	Pracownik działu informatyki	0	10	-10	100	10
	Pracownik obsługi technicznej	0	11	-11	121	11
Wynik testu niezależności Chi-2						85,31

Opracowanie własne.

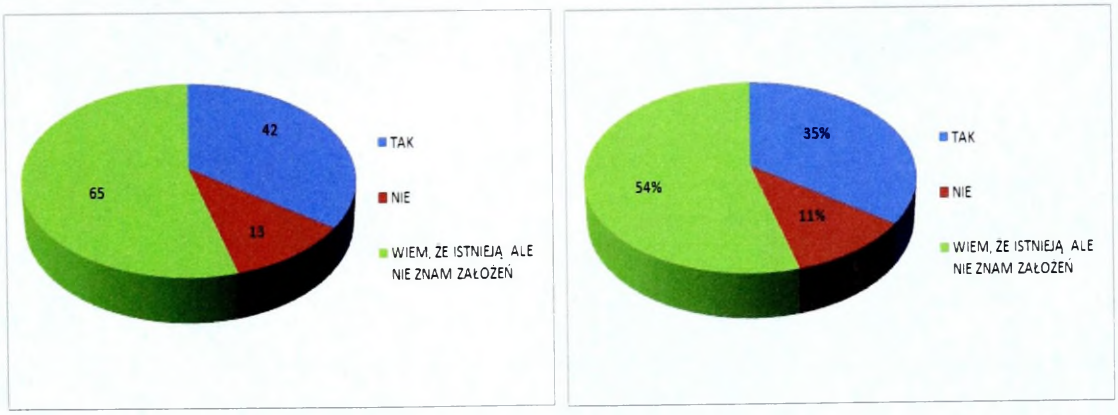
Tab. 4.23. Relacje zachodzące pomiędzy udzielanymi odpowiedziami a zajmowanym stanowiskiem

Określenie badanych zmiennych		Wartość empiryczna Chi-2	Wartość krytyczna Chi-2	Poziom istotności	Liczba stopni swobody	Współczynnik kontyngencji C Pearsona	Siła zależności
A	B	85,31	12,59	0,05	6	0,99	Bardzo silny związek

Opracowanie własne.

Zgodnie z danymi zawartymi w tabelach wyniki obliczeń wskazują na bardzo silny związek między udzielanymi odpowiedziami a zajmowanym stanowiskiem.

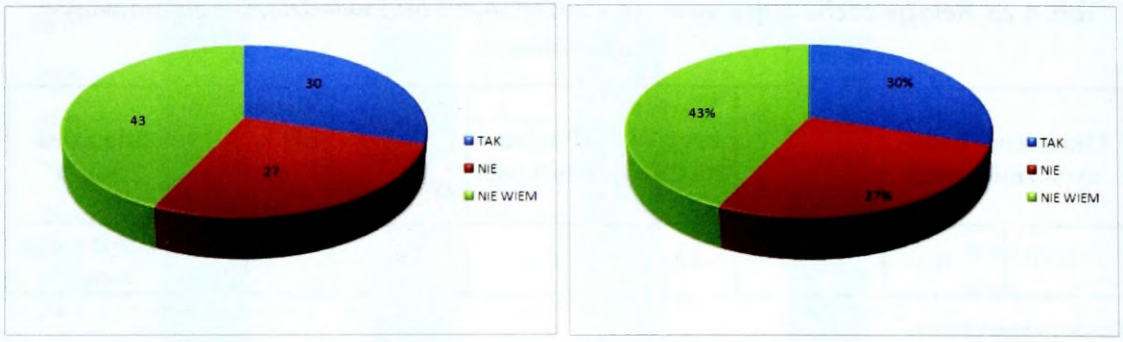
Pytanie nr 17 w kwestionariuszu ankiety dotyczyło znajomości u ankietowanych dokumentu Polityka Bezpieczeństwa Informacji oraz Instrukcja Zarządzania Systemem Informatycznym i ich założeń. W tym miejscu warto przypomnieć, że jednostki administracji publicznej zostały zobligowane przepisami prawa do opracowania wymienionych dokumentów. Opracowanie wyników ankiety wskazało na rażący brak znajomości wśród respondentów Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym. Ponad połowa ankietowanych odpowiedziała, że wie o istnieniu tych dokumentów, ale nie zna ich założeń. Na rys. 4.30 przedstawiono rozkład ilościowy i procentowy udzielonych odpowiedzi.



Opracowanie własne.

Rys. 4.30. Znajomość polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemem informatycznym

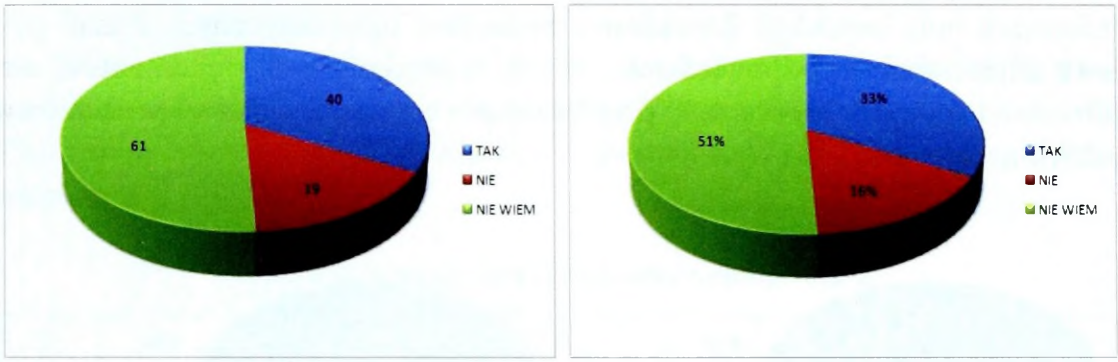
Pytanie nr 18 w kwestionariuszu ankiety dotyczyło wdrożenia w jednostce Systemu Zarządzania Bezpieczeństwem Informacji. 43% respondentów odpowiedziało, że nie wie, czy w jednostce wdrożono SZBI. Jedynie 30% ankietowanych odpowiedziało twierdząco na zadane pytanie. Rozkład ilościowy i procentowy odpowiedzi przedstawia rys. 4.31.



Opracowanie własne.

Rys. 4.31. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

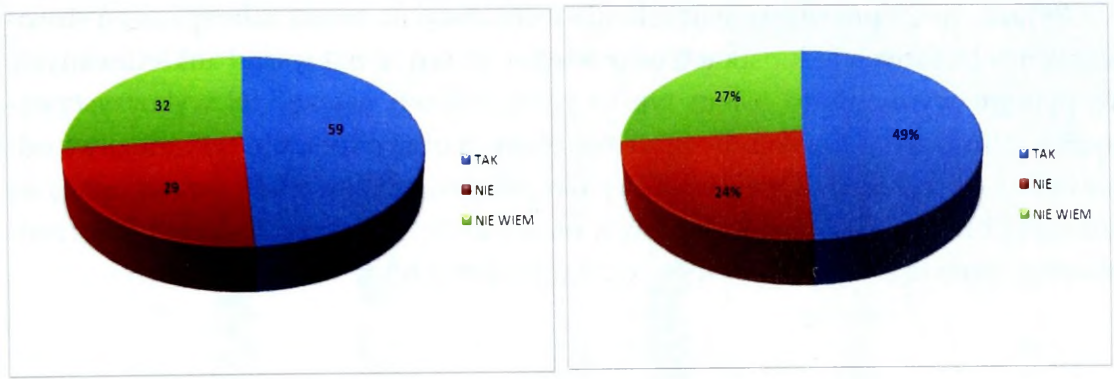
Ankietowani w pytaniu nr 19 udzielali informacji na temat analizy ryzyka w jednostkach administracji publicznej. Ponad połowa ankietowanych przyznała, że nie wie, czy w jednostce przeprowadzana jest analiza ryzyka. Twierdzącej odpowiedzi udzieliło 33% respondentów. Rozkład ilościowy i procentowy odpowiedzi przedstawia rys. 4.32.



Opracowanie własne.

Rys. 4.32. Analiza ryzyka w badanych jednostkach administracji publicznej

Pytanie nr 20 dotyczyło procedur obsługi incydentów naruszających bezpieczeństwo informacji w jednostce. Blisko 50% ankietowanych potwierdziło opracowanie takich procedur. Jedna czwarta respondentów udzieliła przeczącej odpowiedzi. Szczegółowy rozkład ilościowy i procentowy zebranych wyników przedstawia rys. 4.33.



Opracowanie własne.

Rys. 4.33. Procedura obsługi incydentów w badanych jednostkach administracji publicznej

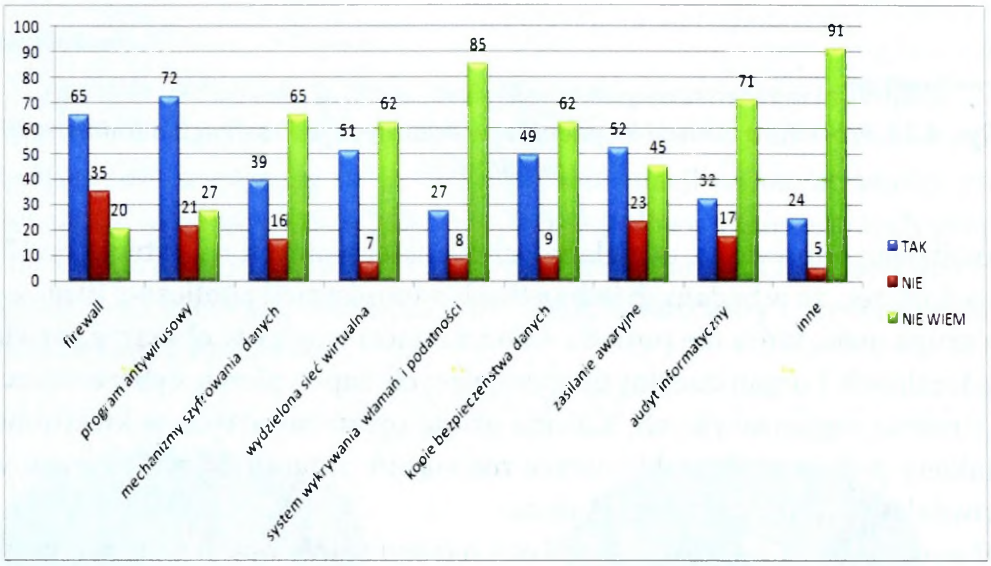
Analizując odpowiedzi udzielane przez ankietowanych na pytania nr 17–20, można dostrzec, że w badanych jednostkach administracji publicznej istnieje znacząca grupa osób, która nie posiada wystarczającej wiedzy w obszarze rozwiązań proceduralnych i organizacyjnych sprzyjających zapewnieniu cyberbezpieczeństwa struktur organizacyjnych. Kolejną grupę pytań zawartych w kwestionariuszu ankiety poświęcono problematyce rozwiązań programowych i sprzętowych przeciwdziałających cyberzagrożeniom.

W pytaniu nr 21 poproszono badanych o wyrażenie opinii na temat konieczności stosowania zabezpieczeń programowych oraz sprzętowych chroniących systemy informatyczne administracji publicznej. Udzielone odpowiedzi pozwalają wnioskować o świadomości ankietowanych na temat konieczności stosowania tego typu zabezpieczeń. Zdecydowana większość osób odpowiedziała, że raczej się zgadza – 49% i zdecydowanie się zgadza – 32% (łącznie 81%). Szczegółowy rozkład ilościowy i procentowy zebranych wyników przedstawiono na rys. 4.34.

Opracowanie własne.

Rys. 4.34. Procedura obsługi incydentów w badanych jednostkach administracji publicznej

Pytanie nr 22 poświęcono uzyskaniu informacji na temat zabezpieczeń stosowanych w badanych jednostkach oraz wiedzy na ten temat wśród ankietowanych. W pytaniu wymieniono osiem typów zabezpieczeń najczęściej wykorzystywanych w celu ochrony systemów informatycznych oraz określono trzy możliwe odpowiedzi – tak, nie oraz nie wiem. Wyniki przeprowadzonych badań wskazują na znaczący brak wiedzy respondentów w omawianym obszarze. Na rys. 4.35 przedstawiono rozkład ilościowy odpowiedzi udzielonych przez ankietowanych.

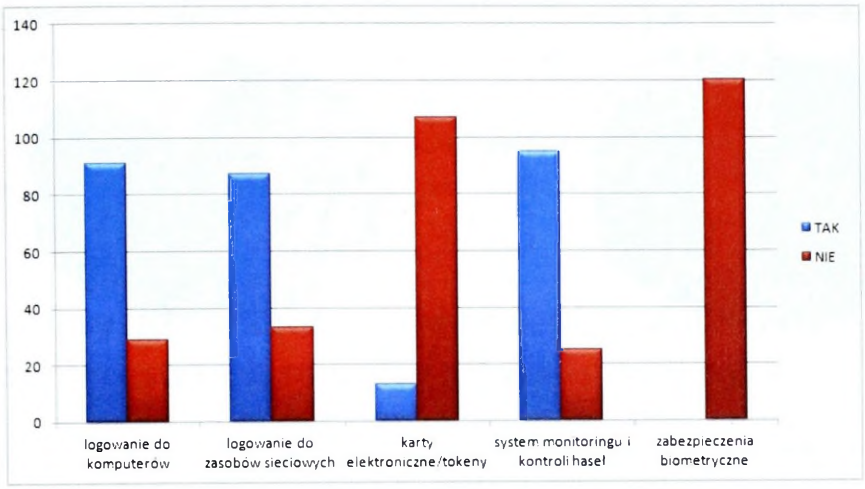


Opracowanie własne.

Rys. 4.35. Ochrona systemów informatycznych stosowana w badanych jednostkach

W stosunku do otrzymanych wyników można zaobserwować zależność statystyczną między udzielanymi odpowiedziami a posiadanym typem wykształcenia. Osoby z wykształceniem informatycznym znacznie częściej odpowiadały na pytanie „tak" lub „nie", natomiast osoby z wykształceniem innym niż informatyczne najczęściej wybierały odpowiedź „nie wiem".

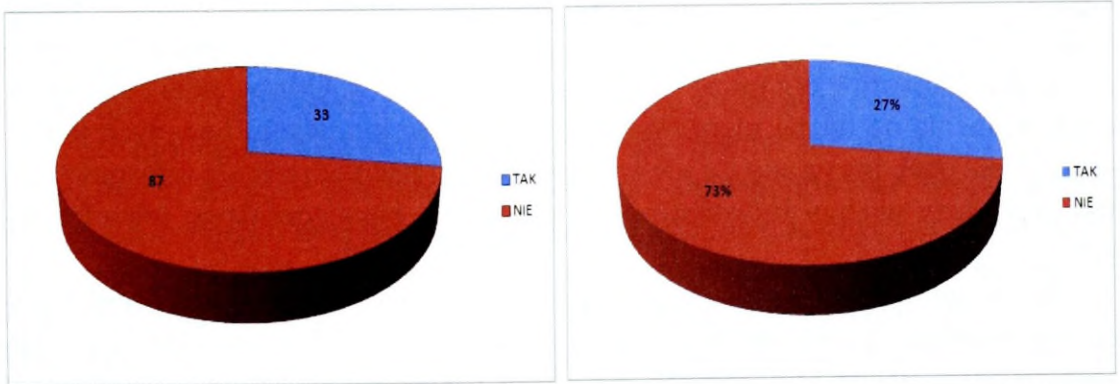
Pytanie nr 23 zawarte w kwestionariuszu ankiety dotyczyło uzyskania informacji na temat sposobów i metod kontroli dostępu do zasobów informacyjnych. Wśród możliwych odpowiedzi znalazły się: logowanie do komputerów, logowanie do zasobów sieciowych, karty elektroniczne/tokeny, system monitoringu i kontroli haseł, zabezpieczenia biometryczne. Odpowiedzi udzielane przez respondentów wskazują, że najczęściej stosowane są: system monitoringu i kontroli haseł, logowanie do komputerów oraz logowanie do zasobów sieciowych. Rys. 4.36 przedstawia rozkład ilościowy odpowiedzi udzielonych przez ankietowanych.



Opracowanie własne.

Rys. 4.36. Kontrola dostępu do zasobów informacyjnych w badanych jednostkach

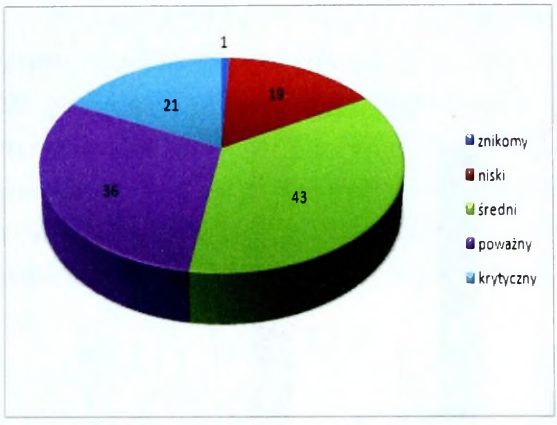
Pytanie nr 24 dotyczyło szkoleń przeprowadzonych w obszarze bezpieczeństwa informacji. W tym miejscu warto przypomnieć, że w Krajowych Ramach Interoperacyjności zawarto wskazanie, że osoby przetwarzające informacje powinny posiadać wiedzę z zakresu bezpieczeństwa informacji oraz że należy zapewnić takim osobom szkolenia. W blisko 75% badanych jednostek ankietowani przyznali, że nie przeprowadzono szkolenia w zakresie bezpieczeństwa informacji. Rozkład ilościowy i procentowy odpowiedzi ankietowanych przedstawia rys. 4.37.

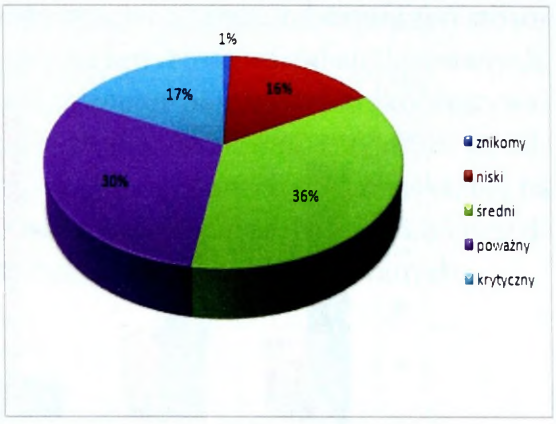


Opracowanie własne.

Rys. 4.37. Kontrola dostępu do zasobów informacyjnych w badanych jednostkach

Pytanie nr 25 w kwestionariuszu ankiety poświęcono wyrażaniu opinii ankietowanych na temat wpływu przestrzegania zasad bezpieczeństwa przez pracowników na bezpieczeństwo teleinformatyczne administracji publicznej.





Opracowanie własne.

Rys. 4.38. Wpływ przestrzegania zasad bezpieczeństwa przez pracowników na bezpieczeństwo teleinformatyczne administracji publicznej

Odpowiedzi udzielane przez ankietowanych wskazują, że system prawny jest istotnym elementem bezpieczeństwa cyberprzestrzeni struktur administracyjnych. Jednostki samorządu terytorialnego funkcjonują w granicach i na podstawie prawa. Dlatego też stanowienie odpowiednich przepisów prawnych jest warunkiem niezbędnym skutecznego zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych oraz realizacji misji instytucji w warunkach możliwych i prawdopodobnych zagrożeń cyberprzestrzeni państwa.

Organizacja i procedury w istotnym stopniu determinują przeciwdziałanie zagrożeniom cyberprzestrzeni państwa. Niemniej jednak analiza wyników badań wykazała istotne braki w wiedzy pracowników administracji publicznej w obszarze wielu elementów organizacyjnych i proceduralnych. Odpowiedzi ankietowanych wskazują na liczne nieprawidłowości w funkcjonowaniu badanych jednostek. Wiele osób przyznaje, że nie zna np. polityki bezpieczeństwa informacji czy też procedury obsługi incydentów naruszających bezpieczeństwo teleinformatyczne.

Rozwiązania programowe i sprzętowe są podstawową barierą ochronną systemów informatycznych administracji publicznej. Na podstawie odpowiedzi ankietowanych można wnioskować, że wśród pracowników istnieje świadomość konieczności stosowania różnego rodzaju zabezpieczeń. Gorzej przedstawia się natomiast stan wiedzy respondentów na temat tych zabezpieczeń. Osoby z wykształceniem informatycznym posiadają znacznie szerszą wiedzę w omawianym obszarze.

Bezpieczeństwo jednostek administracji publicznej jest w istotnym stopniu determinowane przestrzeganiem zasad bezpieczeństwa przez pracowników jednostek administracji publicznej. Dlatego ważne są szkolenia w obszarze bezpieczeństwa informacji. Wyniki badań wskazują na istotne nieprawidłowości w ilości przeprowadzanych szkoleń w badanych jednostkach.

4.5. Ocena systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych

Rozważania zawarte w poprzednich rozdziałach monografii wykazały, że istotnym problemem w obszarze bezpieczeństwa narodowego są współcześnie zagrożenia cyberprzestrzeni państwa. W strukturach administracyjnych obserwuje się wzrost tego typu zagrożeń o różnej skali nasilenia. Informatyzacja sektora publicznego w wielu państwach na świecie, oprócz generowania korzyści z tym związanych, implikuje powstanie obszarów mogących stanowić cel cyberataku. Z perspektywy bezpieczeństwa narodowego szczególnie narażone są elementy infrastruktury krytycznej państwa, które są współcześnie w istotnym stopniu uzależnione od technologii ICT.

W tym kontekście większość państw na świecie zdecydowała się na budowę, utrzymanie oraz doskonalenie zdolności do cyberobrony. Instytucje sektora publicznego zostały także zobligowane do zapewnienia bezpieczeństwa teleinformatycznego. W Polsce jak dotąd możliwość pełnej realizacji usługi on-line jest wciąż na ograniczonym poziomie. Niemniej jednak wysoce prawdopodobna jest transformacja sektora publicznego w Polsce, także w obszarze e-administracji.

Celem monografii była ewaluacja istniejącego systemu zarządzania cyberbezpieczeństwem struktur administracyjnych oraz zaproponowanie zmian sprzyjających zapewnieniu bezpieczeństwa struktur administracyjnych w warunkach możliwych i prawdopodobnych zagrożeń cyberprzestrzeni państwa. Realizacji badań w jednostkach administracji publicznej towarzyszyła analiza aktów prawnych i literatury, dobrych praktyk oraz skutecznych rozwiązań wdrożonych na świecie w celu zapewnienia bezpieczeństwa informacji. Badania empiryczne wskazały obszary problemowe oraz zalety funkcjonującego systemu zarządzania cyberbezpieczeństwem struktur administracyjnych w Polsce, których rezultat przedstawiono w tab. 4.24.

Tab. 4.24. Analiza SWOT[3] systemu zarządzania cyberbezpieczeństwem struktur administracyjnych na podstawie badań empirycznych

Mocne strony	Słabe strony
– logowanie do komputerów – logowanie do zasobów sieciowych – system monitoringu i kontroli haseł – kopie bezpieczeństwa danych – zasilanie awaryjne – świadomość części pracowników na temat zasad bezpieczeństwa informacji – świadomość pracowników na temat konieczności stosowania zabezpieczeń programowych i sprzętowych – świadomość pracowników na temat konieczności tworzenia przepisów prawnych w obszarze bezpieczeństwa cyberprzestrzeni	– przyzwyczajenie do tradycyjnej (papierowej) realizacji spraw administracyjnych – nieprzestrzeganie przepisów prawa – brak świadomości pracowników na temat zagrożeń bezpieczeństwa cyberprzestrzeni oraz typowych metod ataków – brak polityki bezpieczeństwa informacji i SZBI – brak powszechnych szkoleń w zakresie bezpieczeństwa informacji – brak szkoleń na temat korzystania z oprogramowania – brak przeprowadzanej analizy ryzyka – brak procedur obsługi incydentów naruszających bezpieczeństwo informacji – brak programów antywirusowych – brak świadomości co do stosowania analiz w zarządzaniu bezpieczeństwem cyberprzestrzeni
Szanse	**Zagrożenia**
– rozwój e-administracji – ponoszenie jakości usług administracji publicznej – zwiększenie zatrudnienia specjalistów w obszarze bezpieczeństwa teleinformatycznego – stworzenie struktury organizacyjnej do spraw bezpieczeństwa cyberprzestrzeni – pozyskiwanie, rozwój i utrzymanie systemów informatycznych – wykorzystanie technik biometrycznych – przestrzeganie zasad bezpieczeństwa – opracowanie polityki bezpieczeństwa i SZBI – przeprowadzanie analizy ryzyka i audytu informatycznego – monitorowanie wiedzy – zgodność z przepisami prawnymi – zarządzanie systemami i sieciami – zarządzanie ciągłością działania	– brak świadomości pracowników na temat zasad bezpieczeństwa teleinformatycznego sprzyja występowaniu zagrożeń – możliwość wykorzystania socjotechniki w celu pozyskiwania informacji – brak zastosowania zabezpieczeń programowych i sprzętowych zwiększa podatność systemu na zagrożenia

Opracowanie własne.

3 Analiza SWOT jest heurystyczną techniką analityczną służącą do porządkowania informacji. Bywa często stosowana we wszystkich obszarach planowania strategicznego. Dzięki zastosowaniu analizy SWOT można zidentyfikować silne i słabe strony, a także istniejące i potencjalne szanse oraz zagrożenia.

Podsumowując, w ostatnich latach wprowadzono szereg zmian legislacyjnych, organizacyjnych i technicznych w celu przeciwdziałania zagrożeniom cyberprzestrzeni państwa. Pomimo tych zabiegów w systemie zarządzania cyberbezpieczeństwem struktur administracyjnych w Polsce wciąż istnieją liczne dysfunkcjonalności. Pożądane jest przedstawienie rekomendacji sprzyjających zapewnieniu cyberbezpieczeństwa w strukturach administracyjnych z uwzględnieniem następujących kwestii:

- elementy tworzące cyberprzestrzeń struktur administracyjnych cechuje zdolność ochrony przed istniejącymi oraz przyszłymi zagrożeniami;
- bezpieczeństwo informacji gromadzonych, przechowywanych oraz przetwarzanych w jednostkach sektora publicznego jest osiągnięte i utrzymywane na założonym poziomie poufności, integralności i dostępności;
- bezpieczeństwo świadczonych usług administracji publicznej jest osiągnięte i utrzymywane na założonym poziomie niezawodności, dostępności i integralności usług;
- zapewniona jest autentyczność i rozliczalność podmiotów związana z autoryzacją użytkowników korzystających z określonych informacji i usług;
- użytkownicy informacji i usług (pracownicy zatrudnieni w strukturach administracyjnych) oraz odbiorcy informacji i usług (obywatele, przedsiębiorcy, pracownicy zatrudnieni w innych strukturach administracyjnych) mają świadomość i nie są podatni na zagrożenia bezpieczeństwa cyberprzestrzeni;
- aktorzy zagrożeń (także napastnicy wewnętrzni) mają małe możliwości wykorzystania cyberprzestrzeni do generowania zagrożeń przez wykorzystanie słabości, podatności i luk w systemie zabezpieczeń cyberprzestrzeni;
- system zarządzania cyberbezpieczeństwem struktur administracyjnych jest zorganizowany z uwzględnieniem utrzymywania oraz doskonalenia zdolności do cyberobrony.

Realizacja głównego celu – opracowanie modelu systemu zarządzania cyberbezpieczeństwem struktur administracyjnych – wymaga uwzględnienia powyżej określonych elementów oraz rozważań zawartych w poprzednich rozdziałach monografii. W tym kontekście w kolejnym podrozdziale zaprezentowano autorski model systemu zarządzania cyberbezpieczeństwem cyberprzestrzeni struktur administracyjnych, uwzględniający obszary problemowe, jak i rekomendowane rozwiązania systemowe.

4.6. Proponowany model systemu zarządzania cyberbezpieczeństwem struktur administracyjnych

4.6.1. Rozwiązania prawne i instytucjonalne

Analiza przeprowadzona w poprzednich rozdziałach wykazała liczne dysfunkcjonalności w systemie prawnym zarządzania bezpieczeństwem cyberprzestrzeni RP. Wobec powyższego pożądane jest krytyczne podejście do wdrożonych rozwiązań oraz przedstawienie rekomendacji sprzyjających skutecznemu przeciwdziałaniu możliwym i prawdopodobnym zagrożeniom cyberprzestrzeni państwa.

W Polsce nie funkcjonuje akt prawny rangi ustawowej regulujący kwestie odpowiedzialności instytucji publicznych związane z cyberbezpieczeństwem. Dokumentem strategicznym w tym obszarze jest Polityka Bezpieczeństwa Cyberprzestrzeni RP.

Jedną z podstawowych wad przywołanego dokumentu jest ograniczenie obszaru funkcjonowania polityki. Teoretycznie dokument adresowany jest do wszystkich użytkowników cyberprzestrzeni państwa. W praktyce jednak uszczegółowiono, że dokument obowiązuje administrację rządową. Natomiast dla administracji samorządowej jest rekomendowany, a dla pozostałych użytkowników jest jedynie wskazówką. Wydaje się, że takie zdefiniowanie adresatów dokumentu nie będzie sprzyjać zapewnieniu akceptowalnego poziomu bezpieczeństwa. Struktury administracyjne pozostają ze sobą w bardzo złożonych relacjach, związanych m.in. z przepływem informacji na potrzeby realizacji zadań publicznych oraz realizacji misji instytucji. Zatem zastosowanie niższych standardów w jednostkach administracji samorządowej oraz w przedsiębiorstwach prywatnych zwiększa ryzyko wystąpienia zagrożeń bezpieczeństwa cyberprzestrzeni, które mogą mieć negatywny wpływ na bezpieczeństwo narodowe. Wobec powyższego rekomenduje się objęcie obligatoryjnym obowiązkiem przestrzegania zapisów polityki wszystkich jednostek administracji publicznej oraz przedsiębiorców. W tym zakresie polityka powinna skupiać się na strategii komunikacji w sprawach cyberzagrożeń oraz na wypracowaniu standardów i procedur.

Kolejną istotną nieprawidłowością w polityce jest brak systemowej analizy zagrożeń bezpieczeństwa cyberprzestrzeni RP. Identyfikacja zagrożeń powinna uwzględniać ich przyczyny oraz prawdopodobne następstwa dla gospodarki, przedsiębiorców, bezpieczeństwa obywateli oraz dla stabilności państwa i bezpieczeństwa narodowego. Zdolność przeciwdziałania zagrożeniom cyberprzestrzeni państwa wiąże się nie tylko z zastosowaniem technicznych i organizacyjnych metod ochrony, ale również musi uwzględniać rozpoznanie zagrożeń oraz zmniejszenie podatności na ich wystąpienie. W opinii Stowarzyszenia Euro-Atlantyckiego (SEA), *penalizowanie zagrożeń z cyberprzestrzeni powinno opierać się przede*

wszystkim o sprawdzone klauzule generalne. Tendencja wymiaru sprawiedliwości do uszczegóławiania norm prawa karnego nie nadąża za inwencją cyberprzestępców i cyberterrorystów[4]. Zastosowanie klauzul generalnych sprzyja zastosowaniu pewnego stopnia dowolności w wykładni prawa, w celu umożliwienia stosowniejszej – w zależności od przypadku – kwalifikacji czynu podejmowanego przez organ orzekający[5]. Trudno się nie zgodzić z opinią wyrażoną przez ekspertów SEA. Analiza przepisów prawnych polskiego kodeksu karnego skłania do wniosku, że znamiona niektórych przestępstw przenikają się wzajemnie. Stąd można napotkać trudności już przy próbie klasyfikacji czynu.

Znaczącym niedostatkiem polityki jest brak prawidłowego umocowania instytucjonalnego podmiotów odpowiedzialnych za realizację zadań, czasu ich wykonania oraz przybliżonych środków finansowych – zgodnie z podstawowymi i stosowanym na świecie zasadami cyklu projektowego. Ponadto poszczególne obszary, w ramach których realizowane mają być zadania, stanowią jedynie formę zaleceń. Związane to jest niewątpliwie z charakterem i statusem polityki, która nie jest dokumentem rangi ustawowej. Dlatego też na etapie analizy napotyka się trudności w określeniu odpowiedzialności za bezpieczeństwo oraz ochronę cyberprzestrzeni RP. Wobec powyższego proponuje się opracowanie planu działania uwzględniającego podmioty odpowiedzialne za realizację poszczególnych zadań w omawianym obszarze. W sferze organizacyjnej i funkcjonalnej zaleca się racjonalizację struktury systemu podejmowania decyzji strategiczno-politycznych w kontekście możliwych i prawdopodobnych zagrożeń bezpieczeństwa w cyberprzestrzeni oraz konsolidację struktur w poszczególnych resortach i na szczeblu rządowym[6]. W tym względzie wymagane jest określenie podziału odpowiedzialności za obszary cyberprzestrzeni. Proponuje się wprowadzenie zmian prawnych w celu precyzyjnego zdefiniowania kompetencji, uprawnień i odpowiedzialności przez instytucje państwowe oraz przedsiębiorstwa. Istotną kwestią jest wypracowanie zasad wymiany informacji oraz współpracy pomiędzy wymienionymi podmiotami. Wydaje się, że istotną rolę należy tu przypisać współpracy z przedsiębiorstwami telekomunikacyjnymi oraz z dostawcami usług informatycznych.

W następnej kolejności warto zauważyć, że wiedza na temat zagrożeń oraz środków zaradczych jest często poza zasięgiem oddziaływania administracji publicznej. Dowodem na to są wyniki badań empirycznych przedstawione w poprzednich podrozdziałach. Wobec powyższego pożądane jest przeprowadzenie

4 *Rekomendacje Stowarzyszenia Euro-Atlantyckiego dotyczące cyberprzestrzeni RP*, dostęp: http://sea.org.pl/?q= pl/node/915.

5 Szerzej: A. Korybski, L. Leszczyński, A. Pieniążek, *Wstęp do prawoznawstwa*, Lublin 2005, s. 138.

6 *Bezpieczeństwo cyberprzestrzeni. Rekomendacje towarzyszenia Euro-atlantyckiego*, dostęp: http://sea.org.pl/sites/default/files/rek_cyber.pdf.

powszechnych szkoleń w jednostkach administracji publicznej, skierowanych do obywateli, urzędników oraz funkcjonariuszy. W celu zwiększenia możliwości systemu cyberobrony wskazane jest opracowanie programu w obszarze edukacji dla cyberbezpieczeństwa. Ważnym elementem takiego programu powinno być określenie podmiotów odpowiedzialnych oraz mechanizmów nadzoru i kontroli realizacji programu. Współcześnie w Polsce wiele urzędów nie korzysta w pełni z serwisów transakcyjnych, np. ePUAP. Niemniej jednak wysoce prawdopodobna wydaje się transformacja sektora publicznego w omawianym obszarze. Stąd rekomenduje się przygotowanie wymagań dotyczących wdrażania poszczególnych zabezpieczeń oraz metod praktycznej oceny ich skuteczności, np. testów penetracyjnych. Monitorowanie bezpieczeństwa teleinformatycznego wymaga aktywnego podejścia, procedury reagowania wymagają bowiem ciągłej i bieżącej weryfikacji oraz aktualizacji. Kwestie wdrożenia zabezpieczeń powinny określać także zalecenia dotyczące zamawiania usług u firm zewnętrznych.

W obszarze uregulowań prawnych pożądane jest także określenie zasad wykorzystania mechanizmów ochrony cyberprzestrzeni oraz stworzenie możliwości wykorzystania tych mechanizmów w działaniach zapobiegawczych. Zmiany wprowadzone w polskim ustawodawstwie przewidują możliwość stosowania środków nadzwyczajnych w postaci wprowadzenia stanu wojennego. Może się to wiązać z m.in. z naruszeniem prawa do prywatności, prawa do własności intelektualnej czy też przykładowo ograniczyć swobodę obrotu gospodarczego. Wymagane jest umocowanie prawne powyższych kwestii oraz wprowadzenie procedur niwelowania skutków zastosowania przez służby państwowe środków nadzwyczajnych.

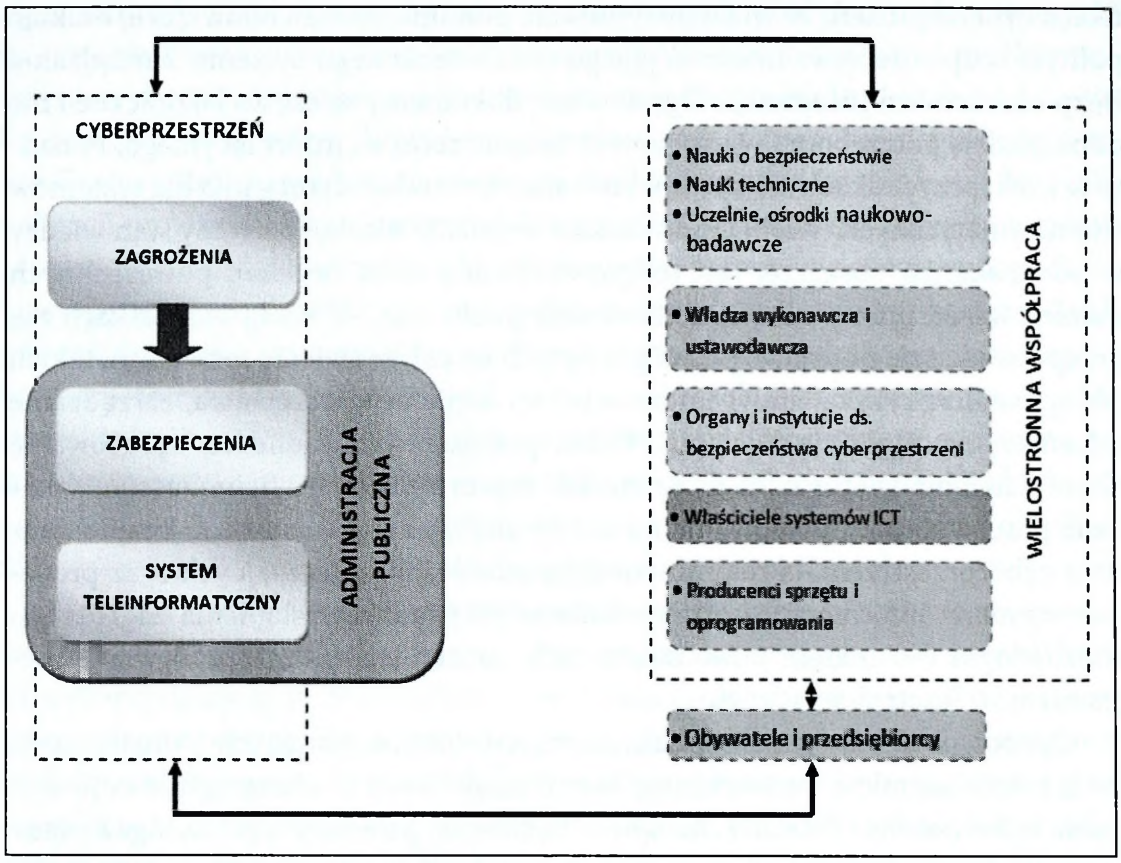
Jedną ze specyficznych cech cyberprzestrzeni jest jej ponadterytorialny charakter, dlatego też współpraca międzynarodowa stanowi istotną szansę dla cyberobrony. Ministerstwo Spraw Zagranicznych powinno uczestniczyć w wymianie informacji i doświadczeń z instytucjami międzynarodowymi w celu wypracowania procedur i standardów. W 2013 roku powstało w ramach Europolu Europejskie Centrum ds. Cyberprzestępczości. Zaleca się współpracę wyselekcjonowanych podmiotów z centrum. Działania podejmowane w ramach polityki powinny uwzględniać także skuteczne i sprawdzone rozwiązania innych państw.

Jak już wcześniej wspomniano, polityka jest jedynie rekomendowana w stosunku do jednostek samorządowych w Polsce. Dlatego też w poprzednich rozdziałach analiza zarządzania cyberbezpieczeństwem na szczeblu samorządowym została przeprowadzona w oparciu o szczegółowe rozwiązania prawne. W Polsce wprowadzono wiele wymagań w obszarze bezpieczeństwa teleinformatycznego. Pomimo tych zabiegów, wciąż istnieją nieprawidłowości, czego dowodem są wyniki badań empirycznych. Już w obszarze planowania zarządzania kryzysowego w wielu jednostkach administracji publicznej nie uwzględnia się analizy i identy-

fikacji cyberzagrożeń. W wielu instytucjach, pomimo takiego obowiązku, brakuje polityki bezpieczeństwa informacyjnego oraz wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji. Opracowane dokumenty są często lakoniczne i nie odpowiadają potrzebom i wymaganiom bezpieczeństwa informacyjnego. Ponadto w wielu przypadkach nie są respektowane minimalne wymagania dla systemów teleinformatycznych. Wielu pracowników wyróżnia nieakceptowany stan wiedzy w obmawianym obszarze. Jest to spowodowane m.in. brakiem powszechnych szkoleń wśród pracowników administracji publicznej. W wielu jednostkach nie przeprowadza się podstawowych i przyjętych na całym świecie rozwiązań, takich jak np. analiza ryzyka, audyt informatyczny, kopie bezpieczeństwa, zarządzanie informacyjną ciągłością działania. Wobec powyższego zasadne jest opracowanie planu działania w stosunku do jednostek samorządowych obejmującego: szkolenia pracowników, opracowanie metodyki analizy ryzyka zagrożeń bezpieczeństwa cyberprzestrzeni, określenie mechanizmów zabezpieczających oraz procedur wymiany informacji i postępowania w przypadku wystąpienia zagrożenia. Niezbędnym warunkiem powodzenia tych założeń jest także opracowanie mechanizmów kontroli i nadzoru.

Oprócz proponowanych zmian prawnych, instytucjonalnych i organizacyjnych zaleca się także intensyfikację badań naukowych w obszarze rozwoju systemu cyberobrony. Ośrodki naukowo-badawcze powinny być zaangażowane w prowadzenie badań nad rozwojem technologii bezpieczeństwa czy też np. powinny uczestniczyć w opracowaniu metodyk analiz i oceny bezpieczeństwa cyberprzestrzeni RP. W tym zakresie niezbędne jest wdrożenie mechanizmów umożliwiających praktyczne wykorzystanie wyników badań w jednostkach administracji publicznej. Ponadto proponuje się rozwijanie programów nauczania pod kątem budowania powszechnej świadomości na temat bezpieczeństwa cyberprzestrzeni oraz bezpiecznej eksploatacji systemów informatycznych. W programach nauczania wielu kierunków humanistycznych i społecznych nie odnosi się do kwestii bezpieczeństwa teleinformatycznego. Należy mieć na uwadze, że wielu studentów kończących studia na kierunku administracja nie jest przygotowanych do pracy w strukturach administracyjnych pod kątem bezpieczeństwa teleinformatycznego. Rozwój e-administracji jest obecnie warunkiem niezbędnym rozwoju społeczeństwa informacyjnego. Zastosowanie nowych technologii będzie najprawdopodobniej generatorem dalszych zmian strukturalnych w sektorze publicznym.

Rozważania zawarte w monografii skłaniają do zaproponowania modelu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych, który został przedstawiony na rys. 4.39.



Opracowanie własne.

Rys. 4.39. Proponowany model systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych

Zaproponowany model zarządzania bezpieczeństwem struktur administracyjnych uwzględnia zagrożenia cyberprzestrzeni państwa, które mogą oddziaływać destrukcyjnie na administrację publiczną. W systemie administracji publicznej niezbędne jest tworzenie zabezpieczeń chroniących informacje przetwarzane, przechowywane i transmitowane w systemach teleinformatycznych. Owe zabezpieczenia zostały szczegółowo omówione w poprzednich rozdziałach. Minimalizują one w znacznym stopniu ryzyko wystąpienia zagrożeń dla bezpieczeństwa informacji i usług administracji publicznej. Proponuje się prowadzenie wielostronnej współpracy organów i instytucji zaangażowanych w zarządzanie bezpieczeństwem struktur administracyjnych. Pożądane jest, aby ośrodki naukowe i uczelnie prowadziły badania naukowe w obszarze rozwoju cyberobrony. Istotne jest opracowanie mechanizmów umożliwiających wykorzystanie wyników badań w jednostkach administracji publicznej. Władza ustawodawcza i wykonawcza w proponowanym modelu odpowiada za rozwój, implementację oraz nadzór nad przestrzeganiem przepisów prawa w omawianym zakresie. Organy i instytucje ds. bezpieczeństwa cyberprzestrzeni wraz z właścicielami systemów IT powinny

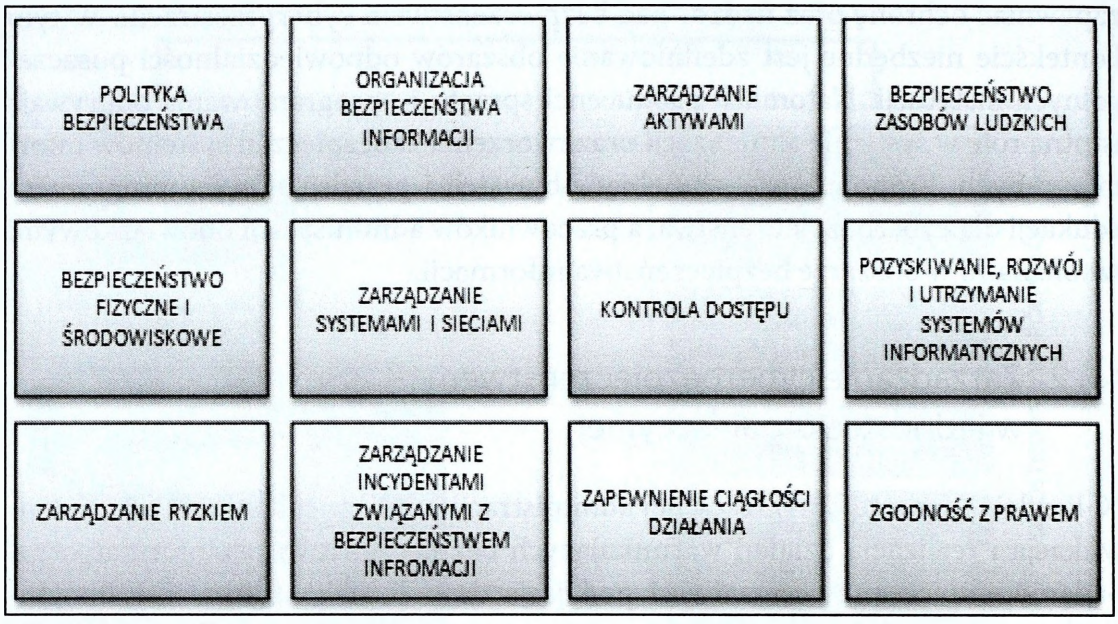
zapewniać ochronę oraz nadzór nad bezpieczeństwem cyberprzestrzeni. W tym kontekście niezbędne jest zdefiniowanie obszarów odpowiedzialności poszczególnych instytucji. Natomiast producenci sprzętu i oprogramowania odgrywają istotną rolę w systemie aktualizacji oraz tworzenia zabezpieczeń systemów informatycznych. Proponuje się, aby objąć obywateli i przedsiębiorców programem edukacji dla cyberbezpieczeństwa, a pracowników administracji obowiązkowymi szkoleniami w obszarze bezpieczeństwa informacji.

4.6.2. Zarządzanie cyberbezpieczeństwem w jednostce organizacyjnej

W każdej jednostce organizacyjnej administracji publicznej konieczna jest identyfikacja i realizacja działań warunkujących bezpieczeństwo teleinformatyczne. Badanie empiryczne wykazały, że podejścia do ochrony informacji w instytucjach publicznych bywają różne – występują prowizoryczne próby stosowania zabezpieczeń czy też nieskoordynowane działania pojedynczych wydziałów. Aby zapewnić pożądany poziom bezpieczeństwa cyberprzestrzeni jednostki organizacyjnej, niezbędne jest opracowanie, stosowanie oraz doskonalenie systemu zarządzania bezpieczeństwem informacji zintegrowanego z systemem zarządzania urzędu. Zapewnienie bezpieczeństwa informacji jest złożonym procesem, który powinien być realizowany przy wzajemnej koordynacji w wielu obszarach. Stąd bezpieczeństwo informacyjne w administracji publicznej powinno być realizowane w oparciu o ujęcie systemowe skoncentrowane na zarządzaniu wszystkimi elementami systemu bezpieczeństwa informacji. Organizując system zarządzania cyberbezpieczeństwem instytucji publicznej, należy mieć na uwadze cechy specyficzne danej instytucji. Konstruowanie polityki bezpieczeństwa informacji nie powinno występować w oderwaniu od misji instytucji oraz ogólnej polityki bezpieczeństwa. Zarządzanie bezpieczeństwem informacji w administracji publicznej powinno uwzględniać wiele obszarów (rys. 4.40).

Uwzględniając rozważania zawarte w poprzednich rozdziałach oraz wyniki badań empirycznych, proponuje się, aby system zarządzania bezpieczeństwem jednostki organizacyjnej, wdrażany był z uwzględnieniem następujących elementów:

1. Podsystem ds. organizacji bezpieczeństwa informacji oraz nadzoru i kontroli realizacji zadań – podsystem ten powinien odpowiadać za praktyczną organizację całości systemu, opracowywać politykę bezpieczeństwa informacji, System Zarządzania Bezpieczeństwem Informacji, odpowiadać za podział zadań i kompetencji w ramach systemu oraz posiadać uprawnienia w obszarze nadzoru i kontroli zadań przez pozostałe podsystemy. Podsystem ten powinien być także gwarantem jakości usług świadczonych przez daną jednostkę oraz ciągłego doskonalenia instytucji.



Opracowanie własne na podstawie: A. Sołecki, P. Sołecki, *Wdrożenie SZBI w Urzędzie* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007, s. 134–135.

Rys. 4.40. Obszary zarządzania bezpieczeństwem informacji w administracji publicznej

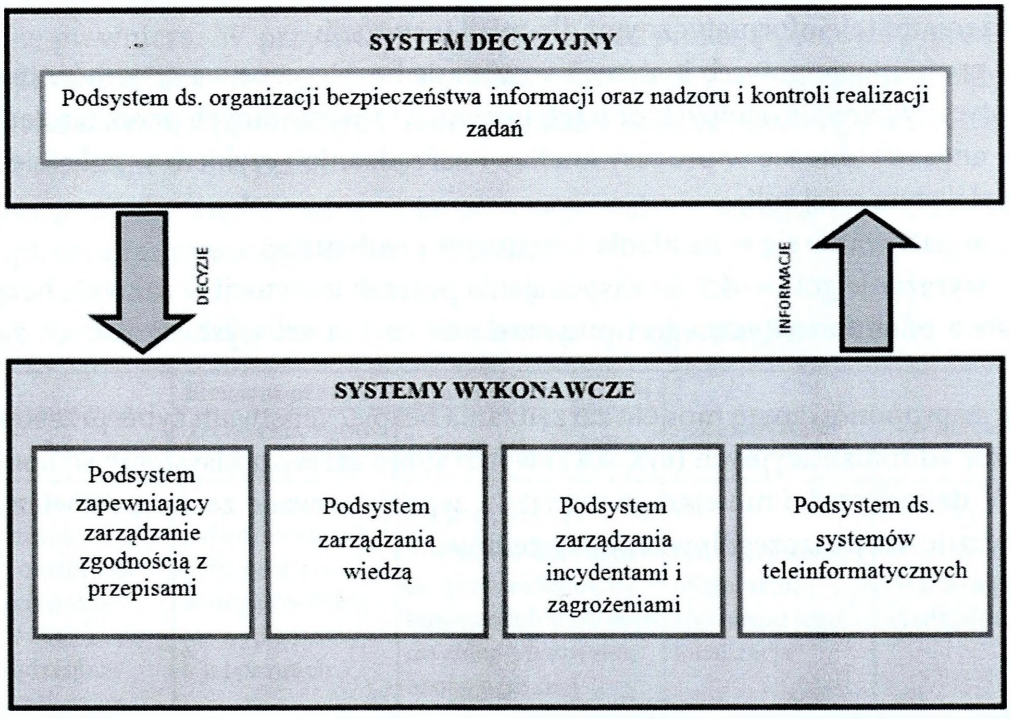
2. Podsystem zapewniający zarządzanie zgodnością z przepisami – proponuje się wspomaganie pracy pracowników struktur administracyjnych przez wykorzystanie oprogramowania prawniczego, takiego jak np. LEX Omega czy LexPolonica. Należy mieć na uwadze, że przywołane oprogramowanie zawiera akty prawne oraz ich interpretacje. Podsystem wspomagający zapewnienie zgodności z przepisami powinien także obejmować dokumenty wewnętrzne danej instytucji publicznej oraz umowy z kontrahentami związane z bezpieczeństwem informacji. Podsystem powinien spełniać następujące funkcje: umożliwienie wprowadzania nowych dokumentów, nowelizacja i aktualizacja istniejących dokumentów oraz prezentacja dokumentów.

3. Podsystem zarządzania wiedzą – do skutecznego zarządzania bezpieczeństwem cyberprzestrzeni jednostki organizacyjnej administracji publicznej niezbędne jest przeprowadzenie obowiązkowych szkoleń, obejmujących wszystkich pracowników struktur administracyjnych. Warunkiem niezbędnym skutecznego funkcjonowania danego podsystemu jest realizacja następujących funkcji: dostarczanie wiedzy, kontrola wiedzy, identyfikacja pracowników wymagających dodatkowego szkolenia. Zaleca się, aby szkolenia były przeprowadzane także w przypadku implementacji nowych rozwiązań w jednostce administracji publicznej. Istotną kwestią jest wypracowanie nie tylko teoretycznych, ale także praktycznych umiejętności pracowników administracji w obszarze bezpieczeństwa informacji.

4. Podsystem do spraw systemów teleinformatycznych – powinien odpowiadać za aktywa teleinformatyczne danej instytucji publicznej (sprzętowe i programowe – aplikacje i zbiory danych). W tej komórce powinno się zatrudniać osoby posiadające wykształcenie techniczne oraz specjalistyczną wiedzę na temat bezpieczeństwa teleinformatycznego. Zadania powinny obejmować m.in. zabezpieczenia, np. programy antywirusowe, kopie bezpieczeństwa danych, VPN, szyfrowanie informacji, kontrolę dostępu do zasobów.

5. Podsystem zarządzania incydentami i zagrożeniami – powinien swym zakresem działania obejmować identyfikację zagrożeń, zarządzanie ryzykiem, pozyskiwanie informacji o podatnościach, opracowanie procedur postępowania w przypadku wystąpienia cyberzagrożenia (m.in. rejestracja incydentów, reakcja na podatności i incydenty). W tym podsystemie powinno się uwzględniać informacje zgłaszane przez pracowników oraz dane publikowane przez organizacje ds. bezpieczeństwa informacji (np. CERT.GOV).

System zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych powinien funkcjonować w oparciu o przepisy prawa oraz dobre praktyki z zakresu bezpieczeństwa informacji. Ponadto pożądane jest, aby system był zorientowany na ciągłe doskonalenie i podnoszenie jakości usług publicznych. Proponowany model systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych przedstawiono na rys. 4.41.



Opracowanie własne.

Rys. 4.41. Proponowany model systemu zarządzania bezpieczeństwem cyberprzestrzeni jednostki organizacyjnej administracji publicznej

Organizacja systemu zarządzania bezpieczeństwem cyberprzestrzeni jednostki organizacyjnej administracji publicznej powinna być procesem obejmującym ciąg logicznie powiązanych czynności, zmierzających do zapewnienia bezpieczeństwa zasobów informacyjnych oraz usług krytycznych realizowanych w instytucji.

System decyzyjny w zaproponowanym modelu spełnia istotną funkcję w organizacji systemu zarządzania ochroną informacji. A. Białas zwraca uwagę na fakt, że struktury zarządzające rozwijane są ewolucyjnie. Oznacza to, że szczególnie złożona jest sytuacja instytucji, w której dopiero porządkowane są sprawy z zakresu bezpieczeństwa teleinformatycznego. Natomiast w innych instytucjach system zarządzania cyberbezpieczeństwem jest jedynie doskonalony[7]. Stąd istotną kwestią jest diagnoza cyklu życia systemu bezpieczeństwa instytucji oraz jego efektywności w omawianym względzie.

Badania empiryczne wykazały, że wiele instytucji znajduje się wciąż w fazie przygotowań organizacji systemu zarządzania bezpieczeństwem teleinformatycznym. Jak już podkreślono, za organizację systemu odpowiadają osoby pełniące funkcje systemu decyzyjnego w instytucji publicznej. Dlatego też istotne jest spełnienie przez osoby zarządzające określonych kryteriów, do których można zaliczyć[8]:

- posiadanie wysokiego poziomu świadomości relacji między niezakłóconym funkcjonowaniem instytucji a różnymi aspektami bezpieczeństwa, w tym zagrożeniami teleinformatycznymi dla misji instytucji;
- zrozumienie potrzeb instytucji w zakresie bezpieczeństwa systemów teleinformatycznych na tle ogólnych potrzeb instytucji i realizowanych przez nią zadań;
- angażowanie się w procesy analizy i zarządzania ryzykiem w zakresie odpowiadającym swej roli;
- angażowanie się w działania korygujące i nadzorcze;
- wyrażanie gotowości do zaspokajania potrzeb instytucji w zakresie bezpieczeństwa teleinformatycznego i przydzielanie na ten cel wystarczających zasobów.

W zaproponowanym modelu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych (rys. 4.41) wyróżniono cztery podsystemy wykonawcze. W dalszej części niniejszego rozdziału zaproponowane zostaną rozwiązania praktyczne dla poszczególnych podsystemów.

7 A. Białas, *Bezpieczeństwo informacji i usług...*, op. cit., s. 173.
8 Ibidem.

4.6.3. Podsystem zapewniający zarządzanie zgodnością z przepisami

Funkcjonowanie zgodnie z przepisami prawnymi stanowi obligatoryjny obowiązek wszystkich jednostek sektora publicznego. Systemy teleinformatyczne administracji publicznej podlegają często bardziej restrykcyjnym regulacjom prawnym niż systemy komercyjne. Niepoświęcenie należytej uwagi kwestiom zgodności z przepisami w obszarze bezpieczeństwa teleinformatycznego może wiązać się z przyniesieniem organizacji szeregu niebezpieczeństw. Zrozumienie i przestrzeganie wymogów prawnych jest niezbędną wiedzą dla każdej organizacji.

Oprócz istniejących już od kilku lat przepisów prawnych (np. ustawa o ochronie danych osobowych) można zaobserwować nieustannie rosnącą liczbę zmian w przepisach prawnych w obszarze bezpieczeństwa teleinformatycznego (np. minimalne wymagania dla systemów teleinformatycznych). Konieczność ochrony z mocy prawa informacji wrażliwych jest rozproszona w kilkudziesięciu aktach prawnych. Istotną kwestię stanowią także uwarunkowania prawne dotyczące możliwości współdzielenia informacji przez jednostki administracji publicznej. Także umowy wzajemne z partnerami czy zleceniobiorcami oraz zarządzenia wewnętrzne (np. polityka bezpieczeństwa informacji) w instytucji powinny być opracowywane z przestrzeganiem przepisów prawnych.

Zaleca się, aby w omawianym podsystemie zatrudniać osoby posiadające wiedzę prawniczą. W przypadku trudności z interpretacją przepisów prawnych pożądane jest korzystanie z pomocy doświadczonych i wykwalifikowanych specjalistów do spraw prawniczych. Nowe przepisy prawne powinny być na bieżąco interpretowane w instytucji.

Na potrzeby analizy otoczenia prawnego zaleca się korzystać z szablonu LE_tpl, zaprezentowanego w tab. 4.25.

Tab. 4.25. Szablon LE_tpl – otoczenie prawne instytucji (przykład)

Podstawa prawna	Element otoczenia prawnego instytucji		Lokalizacja	Właściciel
	Działania zgodne z prawem	Informacje wrażliwe		
Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych wraz z rozporządzeniem wykonawczym	Rejestrowanie danych osobowych wymaga poinformowania osoby o jej prawach	Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej	Nazwa systemu teleinformatycznego i jego lokalizacja	Osoba odpowiedzialna

Opracowanie własne na podstawie: A. Białas, *Bezpieczeństwo informacji i usług*..., op. cit., s. 225.

Należy zauważyć, że identyfikacja elementów otoczenia prawnego powinna być wykorzystywana w analizie ryzyka, ponieważ informacje wrażliwe są zasobami instytucji, dlatego stanowią krytyczną dla niej wartość.

Do funkcji realizowanych przez podsystem zapewniający zarządzanie zgodnością z przepisami należy śledzenie nowelizacji w obowiązujących przepisach oraz ustanawianych aktów prawnych. Dodatkowym atutem sprawnie funkcjonującego podsystemu jest także analiza przepisów prawnych, które mają wejść w życie w przyszłości[9]. Akty wewnętrzne opracowywane w instytucji oraz umowy zewnętrzne (np. umowa zlecenia wykonania usługi) powinny również być opracowywane zgodnie z obowiązującymi przepisami prawa. Analiza przeprowadzona w opracowaniu wykazała niezgodności w realizacji przez jednostki administracji publicznej wymogów prawnych w obszarze bezpieczeństwa informacji, np. w obszarze opracowania polityki bezpieczeństwa informacji urzędu.

4.6.4. Podsystem zarządzania wiedzą

Istotę zarządzania wiedzą można rozpatrywać w kilku aspektach. W ujęciu funkcjonalnym jest to proces polegający na realizacji funkcji zarządzania skoncentrowanych na zasobach wiedzy i procesach. W ujęciu procesowym jest postępowaniem normującym i dyspozycyjnym, mającym na celu stworzenie odpowiedniego środowiska, które umożliwi realizację zadań z zakresu zarządzania wiedzą. W ujęciu instrumentalnym oznacza dobór i wykorzystanie instrumentów przyczyniających się do przebiegów głównych procesów z udziałem wiedzy na wszystkich poziomach i obszarach organizacji. Natomiast w sensie instytucjonalnym oznacza system stanowisk i zespołów pracowniczych realizujących funkcje z zakresu zarządzania wiedzą[10]. Warunkiem koniecznym dla sprawnego funkcjonowania instytucji publicznych jest zarządzanie wiedzą pracowników na temat bezpieczeństwa teleinformatycznego. Determinowane jest to miedzy innymi oczekiwaniami obywateli w zakresie podnoszenia jakości usług publicznych.

9 Akty prawne są obowiązujące po upływie okresu vacatio legis. Termin ten oznacza okres między publikacją aktu a jego wejściem w życie. Celem vacatio legis jest umożliwienie wszystkim zainteresowanym zapoznania się z nowymi przepisami oraz przygotowania do ewentualnych zmian, jakie mogą wynikać z ich obowiązywania. Terminy wejścia w życie aktów normatywnych zostały uregulowane ustawą z dnia 20 lipca 2000 roku o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych.

10 B. Mikuła, *Istota zarządzania wiedzą w organizacji* [w:] *Komunikacja w procesach zarządzania wiedzą*, red. A. Potocki, Kraków 2011, s. 17.

Zgodnie z Krajowymi Ramami Interoperacyjności[11] osobom zaangażowanym w proces przetwarzania informacji powinno być zapewnione szkolenie ze szczególnym uwzględnieniem następujących zagadnień:

- zagrożenia bezpieczeństwa informacji;
- skutków naruszeń zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej;
- stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizujących ryzyko błędów ludzkich.

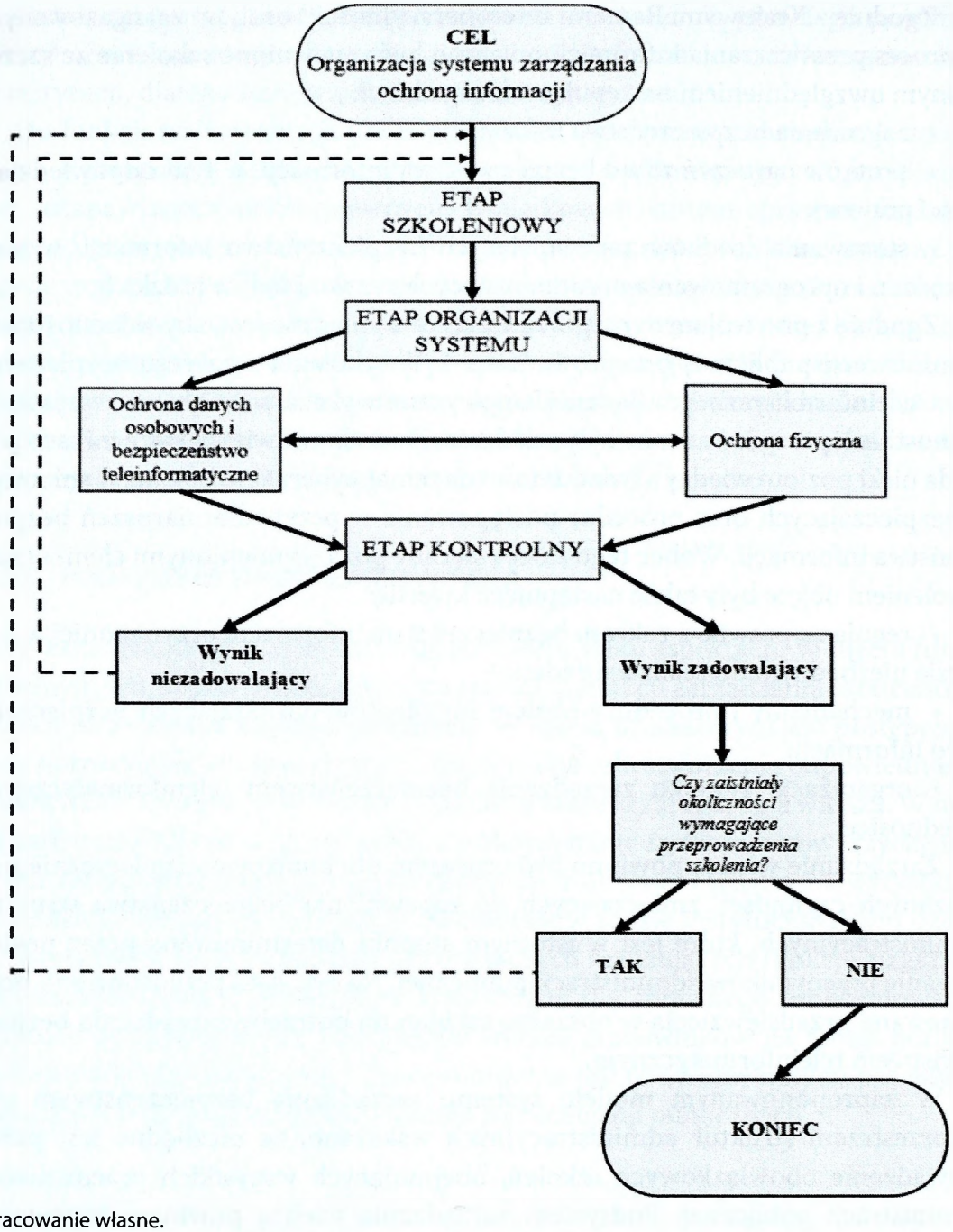
Zgodnie z przywołanym rozporządzeniem wymagane jest, aby w jednostkach administracji publicznej przeprowadzane były szkolenia z zakresu bezpieczeństwa teleinformatycznego. Badania empiryczne wykazały, że nie we wszystkich jednostkach przeprowadzane były szkolenia. Dodatkowo wielu pracownikach posiada niski poziom wiedzy i świadomości na temat cyberzagrożeń, mechanizmów zabezpieczających oraz procedur postępowania w przypadku naruszeń bezpieczeństwa informacji. Wobec tego zaleca się, aby poza wymienionymi elementami szkoleniem objęte były także następujące kwestie:

- regulacje prawne z zakresu bezpieczeństwa informacji, przynajmniej w zakresie niezbędnym do realizacji zadań;
- mechanizmy i procedury obsługi incydentów naruszających bezpieczeństwo informacji;
- organizacja systemu zarządzania bezpieczeństwem teleinformatycznym w jednostce.

Zarządzanie wiedzą powinno być procesem obejmującym ciąg logicznie powiązanych czynności, zmierzających do zapewnienia bezpieczeństwa struktur administracyjnych, które jest w istotnym stopniu determinowane przez postępowanie pracowników administracji publicznej. Na rys. 4.42 przedstawiono proponowane przedsięwzięcia w obszarze szkoleń na potrzeby zarządzania bezpieczeństwem teleinformatycznym.

W zaproponowanym modelu systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych wskazano, że niezbędne jest przeprowadzenie obowiązkowych szkoleń, obejmujących wszystkich pracowników administracji publicznej. Podsystem zarządzania wiedzą powinien zapewniać dostarczenie wiedzy, kontrolę wiedzy oraz identyfikację pracowników wymagających dodatkowego szkolenia. Materiałem szkoleniowym mogą być studia przypadków incydentów, które niekoniecznie miały miejsce w danej instytucji sektora publicznego, ale są wysoce prawdopodobne ze względu na możliwe analogie.

11 § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności..., op. cit.



Opracowanie własne.

Rys. 4.42. Algorytm przedsięwzięć w obszarze szkoleń na potrzeby zarządzania cyberbezpieczeństwem

4.6.5. Podsystem zarządzania incydentami i zagrożeniami

Zarządzanie incydentami i zagrożeniami powinno stanowić istotny element systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych. Potrzebę tą uzasadnia fakt, że bezpieczeństwo nie jest stanem trwałym.

Współczesne instytucje publiczne funkcjonują w zmieniającym się środowisku bezpieczeństwa. W ostatnich latach obserwuje się wzrost coraz bardziej zaawansowanych metod i narzędzi cyberataku. Ponadto wraz z procesem informatyzacji jednostek administracji publicznej następuje wzrost funkcjonalności oferowanych w ramach e-usług administracji.

Zarządzanie incydentami polega na permanentnym gromadzeniu i analizowaniu wszelkiego typu zdarzeń dotyczących naruszeń bezpieczeństwa w celu ciągłego jego doskonalenia[12]. Proces zarządzania incydentami naruszającymi bezpieczeństwo informacji stanowi o efektywności systemu bezpieczeństwa instytucji. Efekty pracy zespołu osób realizujących funkcje w podsystemie powinny wspierać analizę ryzyka. Pożądane jest, aby w każdej instytucji administracji publicznej zostały opracowane i wdrożone mechanizmy postępowania na wypadek wystąpienia incydentu naruszającego bezpieczeństwo informacji.

Proponuje się, aby podsystem zarządzania incydentami i zagrożeniami realizował następujące zadania:

- gromadzenie informacji o incydentach, które miały miejsce w przeszłości, oraz analiza możliwości powtórzenia tego incydentu w przyszłości;
- identyfikacja zagrożeń (gromadzenie informacji o zdarzeniach, które stanowią możliwe i prawdopodobne zagrożenia bezpieczeństwa teleinformatycznego – przyczyny, źródła i skutki);
- bieżąca analiza zagrożeń w kontekście wyników analizy ryzyka;
- implementacja zaleceń i dobrych praktyk dotyczących reagowania na incydenty;
- wspieranie działań zabezpieczających i dostarczanie środków zaradczych;
- współpraca z podsystemem zarządzania wiedzą w celu umieszczenia w materiałach szkoleniowych wniosków z analizy incydentów i mechanizmów postępowania na okoliczność wystąpienia zagrożenia;
- dostarczanie informacji dla zespołów reagowania kryzysowego;
- opracowanie planów postępowania na wypadek wystąpienia zagrożeń;
- pozyskiwanie informacji o podatnościach oraz reakcja na nie;
- gromadzenie materiałów dowodowych;
- zapewnienie właściwej reakcji na zdarzenie ze szczególnym uwzględnieniem ochrony informacji wrażliwych i usług krytycznych;
- zapewnienie ciągłości działania;
- pozyskiwanie i wymiana informacji z innymi instytucjami na temat zagrożeń.

Zarządzanie incydentami powinno odbywać się według ustalonego planu postępowania. Przykład planu zarządzania incydentami przedstawiono w tab. 4.26.

12 A. Białas, *Bezpieczeństwo informacji i usług...*, op. cit., s. 173.

Tab. 4.26. Elementy planu zarządzania incydentami

Lp.	Zawartość planu
I	**Działania przygotowawcze zmierzające do osiągnięcia gotowości do wykrywania i reagowania na incydenty**
	– przygotowanie procedur postępowania, szkolenia i opracowania instrukcji zarządzania incydentami – ustalenie ogólnych zasad postępowania – zgromadzenie podręcznej dokumentacji systemu bezpieczeństwa związanej z zarządzaniem incydentami lub wskazanie jej lokalizacji, umożliwiające szybki do niej dostęp – korelacja z planem ciągłości działania – ogólne zasady gromadzenia i zabezpieczenia materiału dowodowego – szczególne zasady dotyczące utrzymania dzienników zdarzeń – ustalenie sposobów i zasad dotyczących udzielania informacji na zewnątrz instytucji – szkolenia i działania uświadamiające w zakresie zarządzania incydentami
II	**Wykrywanie zdarzeń wskazujących na możliwość wystąpienia incydentu i pierwsza reakcja**
	– wykrywanie symptomów, anomalii według wypracowanych w instytucji kryteriów definiowania incydentów oraz wykrywanie dotychczas nieznanych zdarzeń, które mogą okazać się incydentami – powiadomienie według schematu powiadamiania – rozpoczęcie działań służących gromadzeniu materiału dowodowego – raportowanie
III	**Procedury oceny zdarzeń, służące realizacji następujących czynności:**
	– wyjaśnienie przyczyn incydentu – ustalenie stopnia jego powagi – wybór środków zaradczych
IV	**Reagowanie, ograniczenie następstw i powiadamianie kierownictwa**
	– odpieranie ataku – ograniczenie szkód – dalsze gromadzenie i zabezpieczenie materiału dowodowego – powiadomienie najwyższego kierownictwa – ustalenie treści informacji przekazywanej na zewnątrz instytucji
V	**Odtwarzanie po incydencie**
	– przywrócenie stanu sprzed incydentu – powrót do normalnego działania według planu odtwarzania, skorelowanego z planem organizacji
VI	**Wyciągniecie wniosków z incydentów**
	– ustalenie przyczyn wystąpienia incydentu – oszacowanie poniesionych szkód, w tym skutków prawnych – konfrontacja incydentu z prognozami jego wystąpienia, wynikającymi z analizy ryzyka – wyciągniecie wniosków na przyszłość – wdrożenie działań korygujących system bezpieczeństwa (modyfikacja procedur lub zabezpieczeń)
VII	**Doskonalenie systemu zarządzania incydentami**
	– analiza trendów występowania różnego typu incydentów na świecie i w instytucjach o podobnym charakterze – wnioskowanie – przegląd procedur i doskonalenie własnego systemu prewencji – wymiana informacji dotyczących analizy incydentów z innymi instytucjami – współpraca z centrami reagowania – współpraca instytucji w zakresie wzajemnego ostrzegania się

Źródło: A. Białas, *Bezpieczeństwo informacji i usług*..., op. cit., s. 406–407.

Wyróżnione w tabeli siedem obszarów zawartości planu zarządzania incydentami stanowi kluczowe elementy sprawnego funkcjonowania omawianego podsystemu. Dla każdego z wymienionych elementów niezbędne jest: ustalenie zbiorów zasad postępowania oraz określonych działań, wyznaczenie środków potrzebnych do realizacji poszczególnych elementów planu oraz określenie zasad odpowiedzialności personelu.

4.6.6. Podsystem ds. bezpieczeństwa systemów teleinformatycznych

W systemie zarządzania bezpieczeństwem cyberprzestrzeni powinien funkcjonować podsystem ds. systemów teleinformatycznych odpowiadający za aktywa teleinformatyczne danej instytucji publicznej. Bezpieczeństwo infrastruktury i usług określane jest jako osiąganie i utrzymywanie pewnych podstawowych cech, którymi powinien charakteryzować się system przekazu komunikatów.

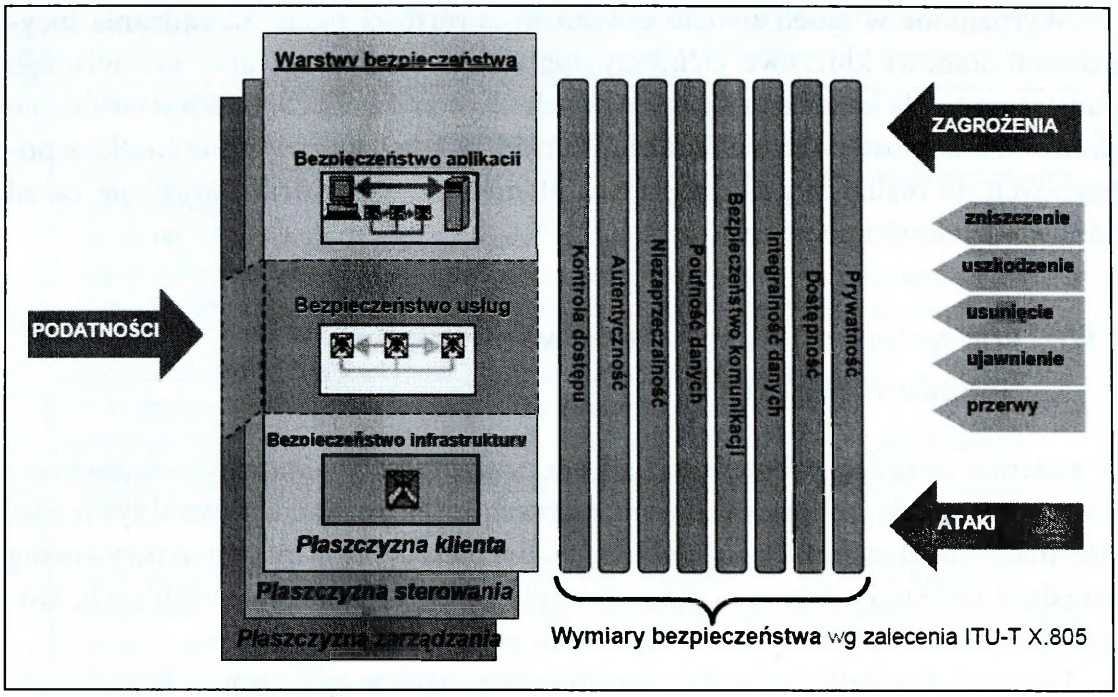
Elementem niezbędnym do zapewnienia pożądanego poziomu bezpieczeństwa jest stosowanie zabezpieczeń, które klasyfikowane są według różnych kryteriów. A. Barczak i T. Sydoruk wymieniają następujące rodzaje zabezpieczeń[13]:

- zabezpieczenia wewnętrzne systemu informacyjnego,
- zabezpieczenia zewnętrzne obejmujące ochronę dostępu i ochronę fizyczną,
- szyfrowanie informacji.

Na rys. 4.43 przedstawiono model bezpieczeństwa infrastruktury teleinformatycznej urzędu.

Zagwarantowanie bezpieczeństwa informacji znajdującej się w sieci informatycznej urzędu jest obowiązkiem każdego administratora sieci. Prawo nakłada na urzędy oraz inne instytucje obowiązek podjęcia szeregu działań o charakterze organizacyjnym i technicznym w celu ochrony przechowywania i przetwarzania danych. Wymogi ochrony informacji o strategicznym znaczeniu dla funkcjonowania urzędów administracji publicznej wynikają z przepisów prawa. Natomiast wymogi w stosunku do innych informacji – ważnych z punktu widzenia funkcjonowania urzędów – powinny być określone przez kierownictwo urzędów. W projektowaniu bezpieczeństwa systemów teleinformatycznych niezbędne jest uwzględnienie potrzeb oraz wymagań informatycznych urzędów (tab. 4.27).

13 A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów...*, op. cit., s. 245.



Źródło: W. Szczęsny et al., *Metody wspomagania decyzji budowy infrastruktury teleinformatycznej dla komunikacji elektronicznej urząd – obywatel: praca naukowo-badawcza*, Warszawa 2007, s. 51.

Rys. 4.43. Model bezpieczeństwa infrastruktury teleinformatycznej urzędu

Tab. 4.27. Potrzeby i wymagania w obszarze bezpieczeństwa systemów teleinformatycznych

Potrzeby	Wymagania
– potrzeby związane z obsługą danych objętych poufnością – potrzeby wynikające z różnorodności kanałów komunikacji z urzędem – potrzeby związane z bezpieczeństwem zasobów i danych – potrzeby związane z bezpieczeństwem transmisji danych – potrzeby związane ze świadczeniem usług w formie elektronicznej – potrzeby związane z archiwizacją dokumentów	– wymagania techniczne wobec systemu bezpieczeństwa – wymagania wobec systemu bezpieczeństwa informatycznego wynikające z obowiązujących przepisów: • wymóg dotyczący opracowania polityki bezpieczeństwa • wymóg dotyczący opracowania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych • wymóg dotyczący kontroli dostępu do obiektów i pomieszczeń, w których są zainstalowane serwery przetwarzające dane osobowe • wymóg dotyczący zainstalowania sprzętowego modułu bezpieczeństwa HSW • wymóg dotyczący wyposażenia pomieszczenia serwerowni w instalację alarmową klasy SA3 ochrony przed awariami zasilania • wymóg dotyczący ochrony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

	• wymóg dotyczący tworzenia kopii zapasowych • wymóg dotyczący ochrony przed zagrożeniami pochodzącymi z sieci publicznej • wymóg dotyczący ochrony kryptograficznej danych wykorzystywanych do uwierzytelniania przy przesyłaniu danych w sieci publicznej • wymóg dotyczący zapewnienia wysokiego poziomu bezpieczeństwa

Opracowanie własne.

W komórce ds. bezpieczeństwa systemów teleinformatycznych powinno się zatrudniać osoby posiadające wykształcenie techniczne oraz specjalistyczną wiedzę na temat bezpieczeństwa teleinformatycznego.

W celu zapewnienia bezpieczeństwa systemów teleinformatycznych pożądane jest korzystanie z różnego typu zabezpieczeń, omówionych szerzej w poprzednich rozdziałach, np. ochrony antywirusowej, zwiększania niezawodności sprzętu czy też kopii bezpieczeństwa. Należy zauważyć, że techniki zabezpieczeń ewoluują wraz z rozwojem coraz doskonalszych urządzeń elektronicznych, powstawaniem coraz bardziej zaawansowanych systemów teleinformatycznych, a tym samym wyrafinowanych metod ataków na systemy informatyczne.

ZAKOŃCZENIE I KIERUNKI DALSZYCH BADAŃ

Głównym celem monografii było przedstawienie koncepcji modelu systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych. Przy opracowaniu modelu wykorzystano wnioski z analizy literatury przedmiotu, danych statystycznych, aktów prawnych oraz uwzględniono wyniki przeprowadzonych badań empirycznych. Zaprezentowane rozwiązania mogą wspomagać procesy decyzyjne przy planowaniu bezpieczeństwa cyberprzestrzeni jednostek administracji publicznej. Ponadto materiał może stanowić cenne źródło edukacji na kierunkach studiów związanych z bezpieczeństwem cyberprzestrzeni oraz określa kierunki kontynuowania badań.

Analiza przeprowadzona w pierwszym rozdziale wykazała, że administracja publiczna stanowi skomplikowany megasystem, który uległ w ostatnich latach istotnemu przeobrażeniu. Zmiany związane z rozwojem nowych technologii i powstaniem społeczeństwa informacyjnego wpływają na koncepcję administracji publicznej. Wśród istotnych elementów można wymienić transformację sektora publicznego, wdrożenie systemów zarządzania jakością w administracji publicznej, powstanie elektronicznej administracji oraz nowych typów zagrożeń. Owe zagrożenia mogą w istotny sposób wpływać na obniżenie jakości usług publicznych. Stąd wdrożenie elektronicznej administracji wymaga spełnienia szeregu warunków. Sprawne funkcjonowanie struktury administracyjnej jest w coraz większym stopniu uzależnione od nowoczesnych technologii. Administracja publiczna jest elementem infrastruktury krytycznej państwa, dlatego też podjęta problematyka jest szczególnie istotna z punktu widzenia bezpieczeństwa narodowego. Dane statystyczne oraz odnotowane przypadki incydentów bezpieczeństwa dowodzą, że współczesne środowisko bezpieczeństwa stwarza szereg możliwych i prawdopodobnych zagrożeń cyberprzestrzeni państwa dla bezpieczeństwa struktur administracyjnych.

Rozdział drugi dowodzi, że zagadnienie zagrożeń cyberprzestrzeni państwa jest złożone, m.in. z uwagi na cechy specyficzne cyberprzestrzeni, dynamicznie rozwijające się metody cyberataków, a także dylematy naukowe, związane z klasyfikacją i typologią zagrożeń oraz z istotą i definicją bezpieczeństwa struktur administracyjnych. Wystąpienie incydentów zagrażających bezpieczeństwu struktur administracyjnych może w istotny sposób zakłócić funkcjonowanie instytucji oraz wpływać na obniżenie bezpieczeństwa narodowego. Należy podkreślić, że istnieje szeroki wachlarz metod i środków, którym dysponują podmioty atakują-

ce. Stąd niezbędne są dalsze badania nad omawianym zjawiskiem. Z perspektywy nauk społecznych problematyka ta jest obszarem interdyscyplinarnym, dlatego wysoce skomplikowanym i wielowymiarowym. Świadomość zagrożeń wśród pracowników jednostek sektora publicznego kształtuje się na zbyt niskim poziomie, dlatego też pożądane jest przeprowadzenie szkoleń edukacyjnych w zakresie bezpieczeństwa teleinformatycznego.

Rozdział trzeci dotyczył elementów systemu zarządzania cyberbezpieczeństwem struktur administracyjnych. Rozważania w omawianym obszarze poprzedzono zaproponowaniem definicji zarządzania bezpieczeństwem struktur administracyjnych. Pogłębiona analiza problematyki wykazała, że uregulowania prawne są jednym z filarów chroniących administrację publiczną przez zagrożeniami dla bezpieczeństwa informacji. Rozwiązania proceduralne, organizacyjne oraz zabezpieczenia techniczne są kolejnym elementem wspomagającym zarządzanie cyberbezpieczeństwem w jednostkach sektora publicznego. Od niedawna administracja publiczna została zobligowana do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), którego jednym z kluczowych elementów jest zarządzanie ryzykiem. Wiodącą rolę mają także techniczne aspekty zapewnienia bezpieczeństwa teleinformatycznego, m.in. zabezpieczenia kryptograficzne, programy antywirusowe. Ponadto przy konstruowaniu polityki bezpieczeństwa informacji zaleca się stosowanie dobrych praktyk i sprawdzonych rozwiązań. W tym obszarze warto zwrócić uwagę na modele zarządzania bezpieczeństwem cyberprzestrzeni stosowane przez NATO, Unię Europejską czy też ich poszczególnych członków. Należy podkreślić, że czynnik ludzki stanowi kluczowy element w procesie zarządzania cyberbezpieczeństwem struktur administracyjnych. Błędy ludzkie, brak świadomości i nieprzestrzeganie procedur to istotne kwestie niniejszej problematyki.

Wyniki badań empirycznych zaprezentowane w rozdziale czwartym wykazały, że jednostki administracji publicznej w sposób niedostateczny chronią przetwarzane przez siebie dane. Część wymagań prawnych dotyczących bezpieczeństwa informacji jest niespełniona, a pracownicy struktur administracyjnych posiadają stosunkowo niską wiedzę na temat zasad bezpieczeństwa teleinformatycznego. Sytuacja ta stanowiła jedną z przyczyn podjęcia w niniejszej monografii badań nad identyfikacją kluczowych elementów zarządzania bezpieczeństwem cyberprzestrzeni w jednostkach administracji publicznej.

Należy podkreślić, że środowisko bezpieczeństwa struktur administracyjnych zmienia się dynamicznie. Ponadto zarówno na świecie, jak i w Polsce można zaobserwować globalną tendencję związaną ze zmianą modelu zarządzania administracją publiczną, który opiera się przede wszystkim na dostarczeniu usług publicznych o odpowiedniej jakości przy jednoczesnym osiągnięciu efektywności ekonomicznej. Wykorzystanie nowoczesnych technologii w sektorze publicznym

powinno m.in. przyczynić się do spłaszczenia struktur administracyjnych, przenieść wymierne korzyści finansowe oraz dalszy rozwój e-administracji. Wobec tego wysoce prawdopodobne są dalsze transformacje samorządu terytorialnego w Polsce, ukierunkowane na wdrożenie sprawdzonych rozwiązań zaimplementowanych w innych państwach. W tym kontekście niezbędne jest ciągłe doskonalenie systemu zarządzania bezpieczeństwem cyberprzestrzeni struktur administracyjnych.

Skuteczne zarządzanie bezpieczeństwem instytucji publicznych powinno uwzględniać ryzyko wystąpienia cyberzagrożeń, mogących skutkować utratą bezpieczeństwa informacji i usług oraz w skrajnym przypadku uniemożliwić realizację misji instytucji. W Polsce jak dotąd nie ma tak silnego powiązania administracji publicznej z odbiorcami usług za pośrednictwem Internetu, że brak dostępności usługi lub jej zniekształcenie wpłynęłoby w istotny sposób na funkcjonowanie państwa lub poszczególnych instytucji sektora publicznego. Niemniej jednak wszystko wskazuje na to, że informatyzacja administracji publicznej w Polsce będzie sprzyjać tej formie kontaktu obywatela (przedsiębiorcy) z urzędem oraz stanowić kolejną przyczynę transformacji sektora administracji publicznej. Amatorskie ataki hakerskie, których przykładem był protest przeciwko podpisaniu międzynarodowej umowy handlowej dotyczącej zwalczania obrotu towarami podrabianymi (ACTA), uwidoczniły słabości w zakresie ochrony cyberprzestrzeni struktur administracyjnych. Incydenty te wskazują, że bezpieczeństwo narodowe może być w istotny sposób osłabione, gdyby zostały przeprowadzone bardziej zorganizowane ataki na systemy posiadające krytyczne znaczenie dla Polski, co w znacznym stopniu uzasadnia potrzebę kontynuowania badań w niniejszym obszarze tematycznym.

Problematyka bezpieczeństwa cyberprzestrzeni struktur administracyjnych wymaga dalszego kontynuowania badań. Potrzebę tę uzasadnia fakt, że bezpieczeństwo nie jest stanem trwałym. Analiza środowiska bezpieczeństwa pozwala wnioskować, że zagrożenia będą ewoluowały oraz będą powstawać coraz doskonalsze i bardziej zaawansowane metody ataków. Ponadto administracja publiczna w Polsce będzie uczestnikiem dalszego procesu informatyzacji, a samorząd terytorialny ulegnie najprawdopodobniej kolejnej transformacji. Niewątpliwie doprowadzi to do wielu zmian prawnych, technologicznych, organizacyjnych, finansowych, funkcjonalnych strukturalnych oraz innych. Omawiany problem jest interdyscyplinarny, dlatego istnieje potrzeba badań wspomaganych współpracą ośrodków naukowych oraz uczelni wyższych. Dodatkowo konieczność kontynuowania badań uzasadniają wyniki badań empirycznych, które wskazują na liczne dysfunkcjonalności w systemie zarządzania cyberbezpieczeństwem administracji publicznej.

Stąd wynika potrzeba badań systemowych i konieczność doskonalenia:

- systemu prawnego i instytucjonalnego;
- środków technicznych, organizacyjnych i proceduralnych;
- metod identyfikacji zagrożeń cyberprzestrzeni państwa;
- metod oceny podatności obiektów na zagrożenia;
- metod oszacowania szkód (strat) obiektów spowodowanych zagrożeniami informacyjnymi;
- metod oceny ryzyka zagrożeń cyberprzestrzeni państwa dla bezpieczeństwa struktur administracyjnych;
- metod i modeli systemu zarządzania cyberbezpieczeństwem struktur administracyjnych;
- integracji systemów monitoringu, wczesnego ostrzegania i analizy zagrożeń;
- programów zawierających praktyczne wskazówki dla jednostek sektora publicznego w obszarze bezpieczeństwa teleinformatycznego;
- metod szkolenia pracowników struktur administracyjnych;
- programów nauczania na kierunkach kształcących studentów będących potencjalnymi pracownikami struktur administracyjnych;
- stałej współpracy międzynarodowej w obszarze bezpieczeństwa teleinformatycznego.

Autorka ma świadomość ograniczeń wynikających z interdyscyplinarności tematyki monografii oraz dynamicznie zmieniającego się środowiska bezpieczeństwa. Pomimo wspomnianych ograniczeń dołożono wszelkich starań sprzyjających realizacji przyjętych celów monografii. Zagrożenia bezpieczeństwa w obszarze cyberprzestrzeni mogą przynieść skutki o różnej skali nasilenia zarówno dla instytucji państwowych i bezpieczeństwa narodowego, jak i dla przedsiębiorstw gospodarczych oraz jednostek społecznych. Brak ograniczeń w cyberprzestrzeni powoduje, że ataki cybernetyczne mogą być wykonywane z dowolnego miejsca, co może rodzić konsekwencje także dla bezpieczeństwa międzynarodowego. W tej sytuacji wzrasta konieczność skoordynowanych wysiłków w celu zapewnienia akceptowalnego poziomu bezpieczeństwa.

LITERATURA

Adamski A., *Nowa kodyfikacja karna. Kodeks karny. Krótkie komentarze*, „Zeszyt 17. Przestępstwa komputerowe w nowym kodeksie karnym", Warszawa 1998.

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Amato V., Lewis W., *Akademia sieci CISCO. Pierwszy rok nauki*, Warszawa 2001.

Anderson R., *Inżynieria zabezpieczeń*, Warszawa 2005.

Andrukiewicz E., *Norma PN-ISO/IEC 27000:2012 Technika informatyczna – Techniki bezpieczeństwa –system zarządzania bezpieczeństwem informacji – Przegląd i terminologia*, „Wiadomości PKN" nr 9/2012.

Arquilla J., Ronfeldt D., *Cyberwar is coming!*, http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf.

Badanie dotyczące stworzenia systemu wskaźników dla oceny realizacji zasady good governance w Polsce. Raport końcowy, Warszawa 2008, dostęp: https://www.ewaluacja.gov.pl/Wyniki/Strony/Good_ Governance.aspx.

Banaszak B., *Prawo konstytucyjne*, Warszawa 2012.

Baniak K., *Analiza zagrożeń telekomunikacyjnych sektora publicznego*, „Kwartalnik BBN. Tom 3 – Bezpieczeństwo w telekomunikacji i teleinformatyce", BBN, Warszawa 2007.

Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Warszawa 2003.

Barta J., Markiewicz R., *Internet a prawo*, Kraków 1989.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006.

Beck U., *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Warszawa 2004.

Beynon-Davies P., *Inżynieria systemów informacyjnych*, Warszawa 1998.

Bezpieczeństwo cyberprzestrzeni. Rekomendacje Stowarzyszenia Euro-Atlantyckiego, dostęp: http://sea.org.pl/sites/default/files/rek_cyber.pdf.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2001.

Białoskórski R., *Wyzwania i zagrożenia bezpieczeństwa XXI w.*, Warszawa 2010.

Bielawa A., *Postrzeganie i rozumienie jakości – przegląd definicji*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania" nr 21.

Blim M., *Teoria ochrony informacji (część 1)*, „Zabezpieczenia" nr 3/2007.
Boczoń J., *Poradnik standaryzacji usług społecznych*, Warszawa 2004.
Borkowski P., *NATO a zjawisko cyberterroryzmu* [w:] M. Pietraś, J. Olchowski (red.), *NATO w pozimnowojennym środowisku (nie)bezpieczeństwa*, Lublin 2011.
Borowiecki R., Kwieciński M., *Informacja i wiedza w zintegrowanym systemie zarządzania*, Kraków 2004.
Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.
Bógdał-Brzezińska A., *Społeczeństwo informacyjne a problemy rozwoju e-governmentu w Polsce* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.
BSI-Standard 100-3. Risk analysis based on IT-Grundschutz, Version 2.5, Bonn 2008; dostęp: https://www.bsi.bund.de/cae/servlet/contentblob/471432/publicationFile/28219/standard_100-3_e_pdf.pdf.
Bugdol M., *Zarządzanie jakością w urzędach administracji publicznej*, Warszawa 2008.
Campen S.A. (red.), *The First Information War*, Fairfax 1992.
Castells M., *Społeczeństwo sieci*, Warszawa 2011.
Catalogue – Elementary Threats, Ferderal Office for Information Security, Bonn 2011; dostęp: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/Download/ download_ node.html.
Chlewicki M., Kedzierska A., Oranowski M., *Elektroniczna administracja w Estonii*, „Prace z Zakresu Myśli Polityczno-Prawnej oraz Elektronicznej Administracji. Studia Erasmania Wratislaviensia. Acta Studentum", Wrocław 2010.
Chrisidu-Budnik A., *Cybernetyczna interpretacja organizacji* [w:] *Nauka organizacji i zarządzania*, Wrocław 2005.
Ciborowski L., *Walka informacyjna*, Toruń 1999.
Clarke Z., Clawson J., Cordell M., *A brief history of hacking*, November 2003, dostęp: http://steel.lcc.gatech.edu/~mcordell/lcc6316/Hacker%20Group%20Project%20FINAL.pdf.
Cyber Attack Task Force – Final Report, North American Electric Reliability Corporation, Atlanta 2012.
Cyber Security Strategy for Germany, Berlin 2011, dostęp: https://www.bsi.bund.de/SharedDocs/ Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.
Cyber Security Strategy of the Czech Republic for the 2011–2013, dostęp: https://www.enisa. europa.eu/media/newsitems/CZ_Cyber_Security_Strategy_20112015.PDF.
Cyber Security Strategy, Tallinn 2008, dostęp: http://www.enisa.europa.Eu/activities/Resilience-and-CIIP/national-cyber-security-strategiesncsss/Estonia_ Cyber_s ecurity_Strategy.pdf.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, dostęp: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_co mm_en.pdf.

Czaputowicz J., *Zarządzanie w administracji publicznej w dobie globalizacji*, „Służba Cywilna" nr 11/2005.

Czechowicz R., Sienkiewicz P., *Przestępcze oblicza komputerów*, Warszawa 1993.

Czermiński A., Grzybowski M., *Wybrane zagadnienia z organizacji i zarządzania*, Gdynia 1996.

Czerska M., *Obsługa interesanta w urzędzie*, „Współczesne Zarządzanie" nr 4/2005.

Czulda R., *Atak w wirtualu*, http://www.polska-zbrojna.pl/home/articleinmagazineshow/10171?t=ATA K-W-WIRTUALU.

Dąbrowska A., *Rozwój e-usług jako przejaw budowania społeczeństwa informacyjnego*, „Handel Wewnętrzny" 2009, nr 2.

Decyzja nr 24/MON Ministra Obrony Narodowej z dnia 18 czerwca 2014 roku w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz.Urz. Min. Obr. Nar. nr 243, poz. 203).

Defending the networks The NATO Policy on Cyber Defence, dostęp: http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

Deklaracja ministerialna w sprawie administracji elektronicznej, Malmö, 18 listopada 2009.

Dela P., Strzoda, M., Wisz M., *Systemy teleinformatyczne na potrzeby kierowania reagowaniem kryzysowym: praca naukowo-badawcza*, Warszawa 2007.

Dela P., *Sieci komputerowe stanowisk dowodzenia*, Warszawa 2007.

Denning D.D., *Activism, hacktivism and cyberterrorism: the internet as a tool for influencing foreign policy*, dostęp: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382ch8.pdf.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

Dictionary of Military and Associated Terms, "Joint Publication 1-02", Department of Defense, November 2010, dostęp: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Długookresowa Strategia Rozwoju Kraju – Polska 2030. Trzecia fala nowoczesności, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.

Długookresowa Strategia Rozwoju Kraju. Polska 2030. Trzecia fala nowoczesności.

Dopierała A., Wywiad, „Prawo i Gospodarka (dodatek), Magazyn Finansowy" 2002, nr 216.

Dragan A., Korzeniewska D.M., Krasnowolski A., *Organy ochrony prawnej w wybranych krajach Unii Europejskiej*, Kancelaria Senatu, Warszawa 2011.

Duda J., Jeżowski A., Misiąg W. et al., *Mierzenie ilości i jakości usług publicznych jako element programu rozwoju instytucjonalnego. Projekt naukowo-badawczy*, Instytut Badań nad Gospodarką, Warszawa 2014.

Dyrda S., Graniszewski W., Świątek G, *Sieci komputerowe* [w:] *Informatyka gospodarcza 1*, red. J. Zawiła-Niedźwiecki, K. Rostek, A. Gąsierkiewicz, Warszawa 2010.

E-Government Survey 2014, Department of Economic and Social Affairs, New York.

E-government in Czech Republic, European Commission – e-government Practice, November 2011.

E-government in United Kingdom, European Commission – e-government Practice, December 2011.

E-Government Survey 2012, United Nations, New York 2012.

Europa i Społeczeństwo Globalnej Informacji – Zalecenia Rady Europy (tzw. Raport Bangemanna), 1994.

Europejska Agenda Cyfrowa – program rozwoju społeczeństwa informacyjnego w Unii Europejskiej na lata 2010–2015.

Exposing One of China's Cyber Espionage Units, dostęp: http://intelreport.mandiant.com/Mandiant AP T1_Report.pdf.

Filgielski P., *Informacja w administracji publicznej: prawne aspekty gromadzenia, udostępniania i ochrony*, Warszawa 2007.

Finland´s Cyber Security Strategy, Government Resolution 24.1.2013, dostęp: http://www.defmin.fi/files /2378/Finland_s_Cyber_Security_Strategy.pdf.

Fischer B., *Granice dostępu do informacji – tajemnice ustawowo chronione na przykładzie informacji publicznych, informacji niejawnych i prawa do prywatności* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007.

Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000.

Furgał G., *Strategia cyberbezpieczeństwa według UE*, dostęp: http://www.e-kirp.pl/Aktualnosci/Strategia-cyberbezpieczenstwa-wedlug-UE.

Gacoń D. (kierownik projektu), *Model bezpieczeństwa informatycznego i ochrony e-Urzędu terenowej jednostki administracji publicznej przed zagrożeniami związanymi z elektroniczną łącznością multimedialną*, Instytut Łączności, Państwowy Instytut Badawczy, Warszawa–Miedzeszyn 2008.

Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Warszawa 2003.

Gibson W., *Neuromancer*, Katowice 2009.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999.

Grenda B., *Cyber-bezpieczeństwo operacji powietrznych NATO* [w:] *NATO wobec wyzwań współczesnego świata*, red. R. Czulda, R. Łoś, J. Reginia-Zacharski, Warszawa–Łódź 2013.

Griffin. R.W., *Podstawy zarządzania organizacjami*, Warszawa 1998.

Grodzka D., *E-administracja w Polsce* [w:] *Społeczeństwo informacyjne*, red. D. Grodzka, „Studia BAS" 2009, nr 3(19).

Grudzińska-Kuna A., Papińska-Kacperek J., *Usługi elektronicznej administracji dla obywateli w Polsce – wybrane problemy*, „Roczniki Kolegium Analiz Ekonomicznych SGH" nr 24, Warszawa 2012.

Gryncewicz W., *Doskonalenie jakości informacji w jednostkach administracji skarbowej. Podejście infologiczne*, praca doktorska, Wrocław 2007.

Grzelak M., *Międzynarodowa strategia USA dla cyberprzestrzeni*, „Bezpieczeństwo Narodowe" nr 2/2011.

Grzelak M., *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" nr 2(26), Warszawa 2013.

Hatch H.J., *Teoria organizacji*, Warszawa 2002.

Hausner J., *Zarządzanie publiczne. Podręcznik akademicki*, Warszawa 2008.

High Performance Network Security, Fortinet Inc., Sunnyvale 2013, dostęp: http://www.fortinet.com/sites /default/files/basicfiles/FortinetBroch.pdf.

Hildreth S.A., *Cyberwarfare*, CRS Report for Congress, 2001, dostęp: http://fas.org/irp/crs/ RL30735.pdf.

Hiroszewicz M., *Socjologia organizacji*, Warszawa 1967.

Howard J.D., Longstaf T.A., *A Common Language for Computers Security Incidents*, dostęp: http://www.osti.gov/scitech/servlets/purl/751004.

International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, May 2011, dostęp: http://www.whitehouse.gov /sites/default/files/rss_viewer/international_strategy _for_cybers pace.pdf.

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group, May 2008.

Izdebski H., Kulesza M., *Administracja publiczna. Zagadnienia ogólne*, Warszawa 1998.

Izdebski H., *Od administracji publicznej do public governance*, „Zarządzanie Publiczne", 1/2007.

Jakubski K.J., *Przestępczość komputerowa – próba zdefiniowania zjawiska* [w:] *Internet – problemy prawne*, red. R. Skubisz, Lublin 1999.

Jaroszerwski P., *Jak skonstruować dobre hasło?*, CERT Polska, dostęp: http://www.cert.pl/PDF/dobre_ haslo.pdf.

Jemioło T., *Modelowanie procesów walki informacyjnej. Model CYBERWAR*, Warszawa 2006.

Jemioło T., *Wyzwania i zagrożenia dla globalnego bezpieczeństwa informacyjnego w pierwszych dekadach XXI wieku* [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioło, J. Kisielnicki, K. Rajchel, Warszawa 2009.

Kaczmarek A., *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Warszawa 2007.

Kaczorowska A., *Audyt o kontrole systemów teleinformatycznych oraz projektów IT w sektorze administracji publicznej* [w:] *Komputerowo zintegrowane zarządzanie*, red. R. Knosala, Opole 2011.

Karta Praw Podstawowych Unii Europejskiej, Nicea 2000.

Kernaghan K., Marson B., Borins S., *The New Public Organization*, Toronto 2000.

Kieżun W., *Patologia transformacji*, Warszawa 2013.

Kieżun W., *Sprawne zarządzanie organizacją. Zarys teorii i praktyki*, Warszawa 1997.

Kisielewicz J., *Istota i zasady good governance*, dostęp: http://lex.pl/czasopisma/atdp/art_2_09.pdf.

Kisielewicz J., *Nauka administracji*, Przemyśl–Rzeszów 2008.

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Warszawa 2005.

Kitler W., *Zarządzanie w administracji publicznej* [w:] *Nauka administracji*, red. M. Karpiuk, W. Kitler, Warszawa 2013.

Klonowski Z.J., *Systemy zarządzania przedsiębiorstwem. Model rozwoju i właściwości funkcjonalne*, Wrocław 2004.

Kobylińska U., *Mierniki sprawności usług publicznych*, „Współczesne Zarządzanie" nr 2/2013.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 19 maja 2010 r., „Europejska agenda cyfrowa".

Komunikat Komisji do Rady i Parlamentu Europejskiego. Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością, Bruksela, dnia 28.3.2012 roku COM(2012) 140 final.

Komunikat Komisji do Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przyjmowanie inicjatywy", 31 maja 2006.

Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady i Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości, Bruksela 22.05.2007, KOM(2007) 267.

Komunikat Komisji Europejskiej i Rady. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy, Bruksela, dnia 22.11.2010 KOM(2010) 673.

Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, Lizbona 2010.

Konwencja Rady Europy o cyberprzestępczości, Budapeszt 23.11.2001, CETS nr 185.

Korczak J., *Prakseologiczna interpretacja pojęcia organizacji* [w:] *Nauka organizacji i zarządzania*, Wrocław 2005.

Korybski A., Leszczyński L., Pieniążek A., *Wstęp do prawoznawstwa*, Lublin 2005.

Kowalczyk M., *e-urząd w komunikacji z obywatelem*, Warszawa 2009.

Kowalewski S., *Nauka o administrowaniu*, Warszawa 1982.

Kowalski R., *Efekty sieciowe a błędy rynku*, dostęp: http://www.mikroekonomia.net/system/publication _files/1308/original/10.pdf?1315306917.

Koziej S., *Między piekłem a rajem: Szare Bezpieczeństwo na progu XXI wieku*, Toruń 2006.

Kozielecki J., *Rozwiązywanie problemów*, Warszawa 1969.

Kożuch B., Kożuch A., *Istota współczesnych usług publicznych* [w:] *Usługi publiczne. Organizacja i zarządzanie*, red. B. Kożuch, A. Kożuch, Kraków 2011.

Kukułka J., *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*, Warszawa 1994.

Lakomy M., *Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego – zarys problemu*, „Rocznik Integracji Europejskiej" nr 7/2013.

Lakomy M., *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek dla typologii*, „E-Politikon" nr 6/2013.

Lang J., *Zagadnienia wstępne* [w:] *Prawo administracyjne*, red. M. Wierzbowski, Warszawa 1997.

Lichocki E., *Cyberterrorystyczne zagrożenia dla bezpieczeństwa teleinformatycznego Państwa Polskiego*, dostęp: http://www.csikgw.aon.edu.pl/index.php/pl/pobieranie/func-startdown/81/.

Lichocki E., *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy* [w:] *Ewolucja terroryzmu na przełomie XX i XXI wieku*, red. M. Malinowski, R. Ożarowski, W. Grabowski, Gdańsk 2009.

Lidel K., *Bezpieczeństwo informacyjne państwa w dobie zagrożeń terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2008.

Liderman K., Patkowski A.E., *Metodyka LP–A przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, WAT, Warszawa 2004.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Liderman K., *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"*, „Biuletyn Instytutu Automatyki i Robotyki" nr 21/2004.

Liderman K., *Standardy w ocenie bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" nr 17/2002.
Liderman K., *Zarządzanie ryzykiem jako element zapewniania odpowiedniego poziomu bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" nr 23, 2006.
Liedel K., *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej* [w:] *Bezpieczeństwo w XXI w: asymetryczny świat*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2011.
Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" nr I – 2011/17.
Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*, Warszawa 2010.
Lisiecka K., Papaj T., *Bezpieczeństwo informacji w urzędach terytorialnej administracji publicznej* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007.
Lisiecka K., Papaj T., Czyż-Gwiazda E., *Public Governance koncepcją zarządzania w administracji publicznej*, Katowice 2011.
Löffler E., *Defining Quality in Public Administration*, 2002.
Lubacz J. (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1999.
Luterek M., *e-government. Systemy informacji publicznej*, Warszawa 2010.
Łobocki M., *Metody nadań pedagogicznych*, Warszawa 1982.
Łuczak A., Popowicz A., Zieliński M., *Elektroniczna administracja w Finlandii*, „Prace z zakresu myśli polityczno-prawnej oraz elektronicznej administracji. Studia Erasmania Wratislaviensia. Acta Studentum", Wrocław 2010.
Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa i systemu międzynarodowego* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.
Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.
Mazur S. (red.), *Rozwój instytucjinalny. Poradnik dla samorządów*, Kraków 2004.
Mikulski K., *Technologia informacyjna w administracji i dla administracji*, Bydgoszcz 2008.
Mikuła B., *Istota zarządzania wiedzą w organizacji* [w:] *Komunikacja w procesach zarządzania wiedzą*, red. A. Potocki, Kraków 2011.
Młotek M., Siedlarz M., *Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 4/11.
Modzelewski P., *System zarządzania jakością a skuteczność i efektywność administracji samorządowej*, Warszawa 2009.
Molski M., Łacheta M., *Bezpieczeństwo i audyt systemów informatycznych*, Bydgoszcz 2009.

Muliński T., *Zagrożenia bezpieczeństwa dla systemów e-adminsitracji*, rozprawa doktorska, Szczytno 2014.

Narodowy Plan Szerokopasmowy, Ministerstwo Administracji i Cyfryzacji, styczeń 2014 r.

Narodowy Program Ochrony Infrastruktury Krytycznej, Warszawa 2013.

National Cyber Security Strategies in the World, ENISA, dostęp: http://www.enisa.Europa.eu/activities/Reesilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

NATO has constituted Cyber Response Teams, dostęp: http://securityaffairs.co/wordpress/20705/cyber-warfare-2/nato-attack-response-teams.html.

Nelson B., Choi R., Iacobucci M., Mitchell M., Gagnon G., *Cyberterror: prospect and implications*, Monterey 1999, dostęp: http://webcache.googleusercontent.com/search?q=cache:CJycB1I7ug0J.

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne*, dostęp: http://www.ebib.pl/2010 /113/a.php?nowak.

Nowak P., Majka A., Kościelniak D., *Firewall. Metody filtracji*, Kraków 2002.

Oleński J., *Elementy ekonomiki informacji. Podstawy ekonomiczne informatyki gospodarczej*, Warszawa 2000.

Ottis R., Lorents P., *Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence*, Tallinn, dostęp: http://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf.

Paget F., *Hacktivism. Cyberspace has become the new medium for political voices*, McAfee Labs White Paper.

Pańkowska M., *Audyt informatyczny w jednostkach sektora finansów publicznych* [w:] *Komputerowo Zintegrowane Zarządzanie*, red. R. Knosala, Opole 2005.

Państwo 2.0. – Nowy start dla e-administracji, Warszawa 2012.

Parker D.B., *Computer related crime*, „Journal of Forensic Sciences", vol. 19 nr 2 (Apr. 1974).

Pawłowska A., *Struktury organizacyjne w administracji publicznej* [w:] *Administracja publiczna – zagadnienia wstępne*, red. A. Pawłowska, Lublin 1999.

Pawłowska A., *Zasoby informacyjne w administracji publicznej. Problemy zarządzania*, Lublin 2002.

Pawłowska B., Seredocha I., *Wybrane metody doskonalenia jakości usług publicznych*, dostęp: http://dlibra.bg.ajd.czest.pl:8080/Content/1103/Pragmata_6-35.pdf.

Pelc M., *Wybrane problemy metodologiczne wojskowych badań naukowych*, Warszawa 1998.

Piasecka P., *Cykl analityczny jako narzędzie w zarządzaniu bezpieczeństwem* [w:] *Analiza informacji w zarządzaniu bezpieczeństwem*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2013.

Plucińska M., Wójtowicz J., *Analiza technik biometrycznych do uwierzytelniania osób*, „Elektronika" nr 4/2014.

PN-EN ISO 9001 Systemy zarządzania jakością. Wymagania, Warszawa: Polski Komitet Normalizacyjny 2001. Punkt 0.2.

Podraza A., *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego XXI wieku* [w:] *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, red. A. Podraza, P. Potakowski, K. Wiak, Warszawa 2013.

Polinceusz M., *Organizacja systemu administracji publicznej* [w:] *Nauka administracji*, red. M. Karpiuk, W. Kitler, Warszawa 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013.

Polska 2030. Wyzwania rozwojowe, Kancelaria Prezesa Rady Ministrów, Warszawa 2009.

Porębski L., *Elektroniczne oblicze polityki. Demokracja, państwo, instytucje polityczne w okresie ewolucji informacyjnej*, Kraków 2001.

Program Operacyjny Polska Cyfrowa na lata 2014–2020, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.

Program Zintegrowanej Administracji Państwa, Warszawa 2013 r.

Project Local Digital Agenda in the Visegrad Four countries, Visegrad Strategic Program (May 2011), Application ID 31110019, Project coordinator: Martina Rojková, dostęp: http://extranet.kr-vysocina.cz/download/odbor_informatiky/lda_v4/_an/an01_uvod.htm.

Promoting good governance. European Social Fund thematic paper, European Commission, January 2014.

Przegląd modeli współpracy jednostek administracji w świadczeniu usług publicznych drogą elektroniczną, dostęp: http://www.bialystok.uw.gov.pl/NR/rdonlyres/276963A6-1A26-4FE8-B787B7C1784FFB71/0/Przegl% C4%85dmodeliwsp%C3%B3%C5%82pracyjednostek.pdf.

Przybyszewski R., *Administracja publiczna wobec przemian społeczno-ekonomicznych epoki informacyjnej*, Toruń 2009.

Pułaska-Turyna B., *Statystyka dla ekonomistów*, Warszawa 2011.

Radwan J., *Zarządzanie bezpieczeństwem informacji w świetle wymagań normy ISO 9001:2000* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, Bielsko-Biała 2007.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku, CERT.GOV.PL, Warszawa 2014.

Rattray G.T., *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004.

Rekomendacje Stowarzyszenia Euro-Atlantyckiego dotyczące cyberprzestrzeni RP, dostęp: http://sea.org.pl/?q= pl/node/915.

Rekut R., Skalski P., *Wirtualne Sieci Prywatne – bezpieczne sieci korporacyjne przez Internet*, http://seminarium.zielman.pl/zielman99/pdf/VPN.pdf.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100, poz. 1024).

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016, Warszawa 2010.

Sakowicz M., *Modernizacja samorządu terytorialnego w procesie integracji Polski z Unią Europejską*, Warszawa 2007.

Sakowicz M., *Zastosowanie nowych technologii informacyjno-komunikacyjnych w rządzeniu i zarządzaniu administracją publiczną* [w:] *Administracja publiczna u progu XXI wieku. Wyzwania i oczekiwania*, red. J. Osiński, Warszawa 2008.

Sawicki M., *Cyberprzestępczość*, Warszawa 2013.

Sawicki M., *Podział i definicje cyberprzestępstw*, „Prokuratura i Prawo" nr 7–8, 2012.

Shannon C., *The Mathematical Theory of Communication*, New York 1949.

Sibiga G., *Informatyzacja administracji publicznej w Polsce*, „Edukacja Prawnicza" 2011, nr 3(123).

Sienkiewicz P. (red.), *Metody badań nad bezpieczeństwem i obronnością*, Warszawa 2010.

Sienkiewicz P. (red.), *Zarządzanie ryzykiem w sytuacjach kryzysowych*, AON, Warszawa 2006.

Sienkiewicz P., *25 wykładów*, Warszawa 2014.

Sienkiewicz P., *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka" 2009, tom 13, zeszyt II.

Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Warszawa 1994.

Sienkiewicz P., *Bezpieczeństwo cyberprzestrzeni* [w:] *Metodologia badań bezpieczeństwa narodowego. Tom III*, red. P. Sienkiewicz, M. Marszałek, H. Świeboda, Warszawa 2012.

Sienkiewicz P., *Inżynieria systemów*, Warszawa 1983.

Sienkiewicz P., *Metody systemowe* [w:] *Metody matematyczne w wojskowych badaniach naukowych*, red. J. Kaczmarek, Warszawa 1987.

Sienkiewicz P., *Systemy kierowania*, Warszawa 1989.

Sienkiewicz P., Świeboda H., *Analiza systemowa zjawiska cyberterroryzmu*, „Zeszyty Naukowe AON" nr 2(63) 2006.
Sienkiewicz P., Świeboda H., *Efektywność i niezawodność organizacji sieciowej. Tom II – Metody oceny efektywności, niezawodności i bezpieczeństwa organizacji sieciowej*, Warszawa 2010.
Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, „Zeszyty Naukowe AON" nr 2(63), Warszawa 2006.
Sienkiewicz P., Świeboda H., *Perspektywy badań systemowych nad bezpieczeństwem* [w:] *Bezpieczeństwo. Wymiar współczesny i perspektywy badań*, red. M. Kwieciński, Kraków 2010.
Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.
Sienkiewicz P., *Teoria i inżynieria bezpieczeństwa systemów*, „Zeszyty Naukowe AON" nr 1(66), Warszawa 2007.
Sienkiewicz P., Wieleba R., Wocial J., Kuca M., Skoczylas M., *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych*, Warszawa 2002.
Sienkiewicz P., *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, red. L.H. Haber, Kraków 2003.
Sikorski C., *Zachowania ludzi w organizacji*, Warszawa 1999.
Skierniewski T., *Diagnoza modelu zarządzania jakością w administracji rządowej. Raport z I etapu badań*, Warszawa 2008.
Słownik języka polskiego, dostęp: http://sjp.pwn.pl/szukaj/standard.
Smarter, Faster, Better e-government – 8th Benchmark Measurement, Prepared by: Capgemini, Rand Europe, IDC, Sogeti and STI for: European Commission, Directorate General for Information Society and Media, November 2009.
Snopko J., *Usługi administracyjne w świetle koncepcji zarządzania w administracji samorządowej* [w:] *Usługi publiczne. Organizacja i zarządzanie*, red. B. Kożuch, A. Kożuch, Kraków 2011.
Sołecki A., Sołecki P., *Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007.
Špaček D., *E-Government management and evolution in the Czech Republic – shifts in practice?*, NISPAcee Conference 2010.
Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.
Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, Poznań 2001.
Stoma M., *Modele i metody pomiaru jakości usług*, Lublin 2012.

Stoneburner G., Goguen A., Feringa A., *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*, NIST, July 2002, dostęp: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

Strategia Rozwoju Kraju 2020. Aktywne społeczeństwo, konkurencyjna gospodarka, sprawne państwo, Warszawa, wrzesień 2012.

Strategia Rozwoju Kraju 2020, Warszawa 2012.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.

Sun Tzu, *Sztuka wojny*, Warszawa 2004.

Supplement to BSI-Standard 100-3, Version 2.5 Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses, Ferderal Office for Information Security, Bonn 2011.

Szarfenberg R. (red.), *Pomoc i integracja społeczna wobec wybranych grup – diagnoza standaryzacji usług i modeli instytucji, Krajowy raport badawczy*, Warszawa 2011.

Szarfenberg R., *Standardy i standaryzacja pracy socjalnej i usług pomocy i integracji społecznej* [w:] *Pomoc i integracja społeczna wobec wybranych grup – diagnoza standaryzacji usług i modeli instytucji, Krajowy raport badawczy*, red. R. Szarfenberg, Warszawa 2011.

Szczepaniuk E., *Zagrożenia bezpieczeństwa informacyjnego RP*, praca magisterska, Siedlce 2012.

Szczepaniuk E., *Zarządzanie bezpieczeństwem informacji w urzędach administracji publicznej* [w:] *Inżyniera systemów bezpieczeństwa*, red. P. Sienkiewicz (w druku).

Szczęsny W. et al., *Metody wspomagania decyzji budowy infrastruktury teleinformatycznej dla komunikacji elektronicznej urząd – obywatel: praca naukowo-badawcza*, Warszawa 2007.

Szomański B., *Systemy zarządzania bezpieczeństwem informacji – założenia i projektowanie*, „Problemy Jakości" 2004, nr 4.

Szomański B., *Zarządzanie bezpieczeństwem informacji – podstawy oraz znaczenie w ochronie firmy przed nieuczciwymi pracownikami, klientami i usługodawcami* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, red. T. Wawak, Bielsko-Biała 2007.

Szpiegowska sieć w Internecie, dostęp: http://www.computerworld.pl/news/342832/Szpiegowska.siec. w.internecie.html.

Szpyra R., *Militarne operacje informacyjne*, Warszawa 2003.

Szpyra R., *Operacje informacyjne państwa w działaniach sił powietrznych*, rozprawa habilitacyjna, Warszawa 2002.

Szreniewski J., *Wstęp do nauki administracji*, Lublin 2004.
Świeboda H., *Zagrożenia informacyjne bezpieczeństwa RP*, rozprawa doktorska, Warszawa 2009.
Tatarkiewicz W., *Historia filozofii. Tom I*, Warszawa 2011.
Tatarkiewicz W., *Historia filozofii. Tom II*, Warszawa 2011.
Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.
The Global Information Technology Report 2013. Growth and Jobs in a Hyperconnected World, World Economic Forum and INSEAD, Geneva 2013.
The National Knowledge Society Strategy 2007–2015. A renewing, human-centric and competitive Finland, Prime Minister's office, September 2006.
The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, November 2011, dostęp: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/ukcybersecr -strategy-final.pdf.
Three-level IT baseline security system ISKE, dostęp: https://www.ria.ee/iske-en/.
Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor, March 2009, dostęp: http://pl.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.
Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013.
Ustawa z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Dz.U. 2004 nr 171, poz. 1800).
Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2005 nr 64, poz. 565 z późn. zm.).
Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym.
Ustawa z dnia 25 czerwca 1960 roku Kodeks postępowania administracyjnego.
Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89, poz. 590).
Ustawa z dnia 30 sierpnia 2011 roku o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. 2002 nr 156, poz. 1301).
Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24, poz. 83).
Ustawa z dnia 4 września 1997 roku o działach administracji rządowej.
Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. nr 182, poz. 1228).
Ustawa z dnia 6 czerwca 1997 roku Kodeks karny (Dz.U. 1997 nr 88, poz. 553).
Ustawa z dnia 6 września 2001 roku o dostępie do informacji publicznej (Dz.U. 2014 nr 0, poz. 782 z późn. zm.).

Wańkowicz W., *Wskaźniki realizacji usług publicznych*, Kraków 2004.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 9/13.
Wawak T., *TQM w warunkach polskich, materiały szkoleniowe*, Mikołajki 1998.
Wawrzyniec R., *Rozwój zarządzania publicznego*, dostęp: http://dspace.uni.lodz.pl:8080/xmlui/bitstream /handle/11089/821/407-418.pdf?sequence=1.
Weber M., *Biurokracja* [w:] *Wybór tekstów z socjologii stosunków politycznych, cz. 2*, red. J. Hochfeld, Warszawa 1961.
Wiener N., *Cybernetics: or Control and Communication in the Animal and the Machine*, New York 1948.
Wiener N., *Cybernetyka i społeczeństwo*, Warszawa 1960.
Witczak T., *Początki indentyfikacji*, dostęp: http://www.e-detektyw.pl/Magazyn_Detektyw/Wydanie_Specjalne/Wydanie_Specjalne_042006/Poczatki_Identyfikacji/?id=676.
Władek Z., *Organizacja i zarządzanie w administracji publicznej*, Warszawa 2013.
Wójcik A., *Model PDCA w procesach SZBI (ISMS)*, „Zabezpieczenia" nr 6/2008.
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Część 1*, „Zabezpieczenia" nr 2/2008.
Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, „Pomiary Automatyka Robotyka" nr 2/2013, Przemysłowy Instytut Automatyki i Pomiarów, Warszawa 2013.
Wrzosek M., *Zmagania o informację we współczesnych organizacjach*, „Zeszyty Naukowe AON" 2010, nr 4(81).
Wrzosek S., *Kompendium wiedzy administratywisty*, Lublin 2008.
Wspólna metoda oceny (CAF). Doskonalenie organizacji przez samoocenę, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2011, dostęp: http://caf.kprm.gov.plsites/default/files/caf2006_ dr_ matla.pdf.
Wyroba A., *Zarządzanie wiedzą w urzędzie*, Warszawa 2005.
Wysokińska-Senkus A., Senkus P., *Systemy Zarządzania w świetle nowych wyzwań. Bezpieczeństwo, informacja, integracja, model doskonalenia*, Warszawa 2013.
X-Road Estonian Information Systems's Authority, Rävala 5, 15169 Tallinn.
Yourdon E., *Wojny na bity*, Warszawa 2006.
Zacher L., *Transformacje i perspektywy społeczeństw informacyjnych*, „Nierówności Społeczne a Wzrost Gospodarczy" nr 32/2013.
Zakrzewska-Bielawska A., *Typy struktur organizacyjnych* [w:] *Podstawy zarządzania. Teoria i ćwiczenia*, red. A. Zakrzewska-Bielawska Warszawa 2012.

Zalesisńka A., Pęcherzewski P., Rodziewicz P., *Zagrożenia związane z rozwojem nowych technologii* [w:] *Technologia informacyjna dla prawników*, A. Burdziak, R. Cieślak et al., Wrocław 2011.
Zaskórski P. (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, Warszawa 2011.
Zaskórski P., *Automatyzacja procesów dowodzenia*, Toruń 2001.
Zaskórski P., *Strategie informacyjne w zarządzaniu organizacjami gospodarczymi*, Warszawa 2005.
Zaskórski P., Szwarc K., *Bezpieczeństwo zasobów informacyjnych determinantą technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", nr 9, 2013.
Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 2004.
Zięba R., *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych* [w:] B.D. Bobrow, E. Haliżak, R. Zięba (red.), *Bezpieczeństwo narodowe i międzynarodowe w schyłku XX wieku*, Warszawa 1997.
Zur-Mühlen von R., *Computerkriminalität. Gefahren und Abwehr*, Berlin 1973.
http://epuap.gov.pl/.
http://www.strefa-iso.pl/iso-podstawy.html.
http://www.ebib.pl/2006/77/kaminska.php.
https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy.
http://www.valtori.fi/en-US.
http://www.nam.fi.
http://www.energiavirasto.fi/en/home.
http://www2.kkv.fi/en-GB/.
http://www.finlex.fi/en/.
http://www.stat.fi/index.html.
http://www.aka.fi/ENG.
http://www.prh.fi/en/index.html.
http://www.stat.fi/tup/vl2010/art_2011-03-18 _001_en.html.
http://www2.liikennevirasto.fi/sivu_siirtynyt/sivu _siirtynyt.html.
https://www.ria.ee/.
https://mac.gov.pl/.
https://krmc.mac.gov.pl/.
http://www.cpi.gov.pl/.
http://www.coi.gov.pl/.
http://www.nik.gov.pl/.
http://www.giodo.gov.pl/.
http://epuap.gov.pl/.

http://geoportal.gov.pl/start.
http://www.cpi.gov.pl/chmura,170.html.
http://www.cpi.gov.pl/si_pr,44.html.
http://angraplay.republika.pl/pliki/schematinternet.htm.
http://www.cert.gov.pl/cer/o-nas/15,O-nas.html.
http://itpedia.pl/index.php/Dost%C4%99p_do_zasob%C3%B3w:_identyfikacja,_uwierzytelnianie_i_autoryzacja.
http://reset.ath.bielsko.pl/systemy-operacyjne/artykuly/windows/2010/vpn.aspx.
https://www.govcert.cz/en/.
http://www.efqm.pl/index.php/model-doskonalosci-efqm/uklad-logiczny-radar.
http://www.pri.msap.pl/.
http://wawak.pl/pl/content/ciagle-doskonalenie.

SPIS RYSUNKÓW

SPIS TABEL

BG - Archiwum AON
nr ewid. 78375

WYDAWNICTWO
AON

WYDAWNICTWO

e-mail: wydawnictwo@aon.edu.pl

tel. 261 813 671, tel./fax 261 813 752

KSIĘGARNIA

e-mail: ksiegarnia.akademicka@aon.edu.pl

261 814 608
261 814 055

SKLEP INTERNETOWY

www.ksiegarnia.aon.edu.pl

al. gen. A. Chruściela 103, 00-910 Warszawa

WYDAWNICTWO
AON

Oferujemy następujące usługi:

– przygotowanie projektów graficznych
– opracowanie redakcyjne i korektę
– usługi introligatorskie
– skład komputerowy
– drukowanie

Nasze atuty:

– długoletnie doświadczenie
– kompleksowa obsługa
– konkurencyjne ceny
– wysoka jakość
– krótkie terminy

ISBN 978-83-7523-517-3

WYDAWNICTWO
AON