MODELOWANIE PROCESÓW ZAPEWNIANIA BEZPIECZEŃSTWA I CIĄGŁOŚCI DZIAŁANIA ORGANIZACJI ADMINISTARACJI PUBLICZNEJ[1]

Piotr ZASKÓRSKI

Wojskowa Akademia Techniczna

Krzysztof SZWARC

Wojskowa Akademia Techniczna

Streszczenie: W artykule podjęto problem identyfikacji czynników wzmacniających zapewnianie bezpieczeństwa i ciągłości działania podmiotów administracji publicznej ze szczególnym uwzględnieniem wymiaru informacyjnego. Przedstawiono tu pewne uogólnione założenia i wymagania dla modelu zapewniania ciągłości działania wraz z ramową koncepcją samego modelu wielowymiarowego tzw. „pajęczynowego" posiłkującego się dostępnymi standardami NIST/BCP.
Słowa kluczowe: bezpieczeństwo, ciągłość działania, zarządzanie bezpieczeństwem, zapewnianie bezpieczeństwa

1. Wprowadzenie

Kryzys i sytuacja kryzysowa oznacza pewien stan odstępstwa od warunków normalnych, w których funkcjonuje organizacja lub wręcz ich załamania. Można więc mówić, że bezpieczeństwo dowolnej organizacji (w tym instytucji publicznych) jest silnie determinowane poziomem ryzyka związanego z zaistnieniem wzmiankowanego stanu. Dotyczyć to może warunków, w których nastąpi obniżenie poziomu jej bezpieczeństwa a nawet utraty możliwości działania w różnych wymiarach, począwszy od finansowego, organizacyjnego, materiałowego, aż po zakłócenia dostępu do informacji[2].

Wystąpienie kryzysu jest następstwem występowania (urealniania) zagrożeń, które powinny być zidentyfikowane w procesie analizy ryzyka. Na gruncie teorii oraz z perspektywy tworzonych dokumentów, takich jak np. plan zapewniania ciągłości działania można wyprowadzić następujące twierdzenia:

---

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

[2] K. Szwarc, Uwarunkowania ciągłości działania systemu zarządzania kryzysowego, „Studia Bezpieczeństwa Narodowego", WAT, Warszawa 2014, s. 199-213.

1. system (S) posiada określone podatności (P) na zagrożenia (Z), których wykorzystanie (zaistnienie), może prowadzić do zakłócenia pracy tego systemu, a w konsekwencji braku zdolności realizacji celów (C);
2. następstwem urealnienia zagrożenia może być zdarzenie kryzysowe, którego zakres oraz atrybuty są wyspecyfikowane w planach antykryzysowych, a ich zaistnienie uzasadnia uruchomienie zapisanych procedur dotyczących postępowania z zakłóceniami oraz wznawiania pracy systemu;
3. z kryzysem jako wariantem rozstrzygnięcia sytuacji kryzysowej, związane jest ryzyko powstania dużych strat - których skala jest wartościowana w planach;
4. jednym z uniwersalnych celów systemów jest zabezpieczenie istnienia, a zatem zadaniem organizatora systemu jest umiejętne rozpoznawanie zagrożeń oraz stosowanie skutecznych mechanizmów ochronnych;
5. zagrożenia bardzo często są zjawiskami niepewnymi lub co najmniej ryzykownymi, a zatem konieczne jest tworzenie zdolności wznawiania pracy systemu po wystąpieniu zagrożenia oraz mitygowania skutków takiego zakłócenia.

Dlatego na proces zarządzania kryzysowego należy spojrzeć przez pryzmat czterech faz, począwszy od **przygotowania i zapobiegania**, kiedy dokonywana jest identyfikacja i ocena zagrożeń, tworzone plany oraz ustanawiane zabezpieczenia; fazę **reagowania**, w trakcie której implementowane są opracowane procedury postępowania, przy istniejących ograniczeniach materiałowych, czasowych i informacyjnych; oraz fazy **odtwarzania**, kiedy przywracana jest użyteczność systemu, z czasu przed zdarzeniem kryzysowym. Należy zauważyć, że w fazie reagowania weryfikacji poddawane są, opracowywane wcześniej scenariusze rozwoju sytuacji kryzysowej oraz strategie ograniczania negatywnych skutków dla ludzi, mienia, środowiska oraz samego systemu[3]. Wiele zmiennych, branych pod uwagę w trakcie konstruowania takich scenariuszów jest trudno mierzalnych lub przewidywalnych. Stąd można stwierdzić, iż bezpieczeństwo organów administracji publicznej oraz ciągłość realizowanych przez nie procesów jest silnie determinowane poziomem ryzyka. Stwierdzić można także, iż zadaniem organizatora jest ograniczanie ryzyka niedopuszczalnego, eliminowanie podatności systemu na zagrożenia oraz maksymalne skracanie czasu reakcji na ich wystąpienie. Minimalizowanie skutków powinno być jedną ze strategii zapewniania bezpieczeństwa organów administracji publicznej, z zachowaniem kryterium jakości działania.

[3] R. Grocki, Zarządzanie kryzysowe. Dobre praktyki, Difin, Warszawa 2012, s. 41-44.

2. Podstawowe założenia modelu i determinanty ciągłości działania

Bezpieczeństwo podobnie jak ciągłość działania jest kategorią systemową i może warunkować poziom zaufania do systemu oraz chęć partycypacji w realizacji różnych przedsięwzięć. Swoistym odwzorowaniem bezpieczeństwa jest ryzyko w kontekście ważności i podatności systemu na zagrożenia. Identyfikacja, analiza i ewaluacja ryzyka wiąże się ściśle z ustaleniem nie tylko źródeł zagrożeń dla poszczególnych komponentów danej organizacji, ale również z oceną jej odporności na te, częstości ich wystąpowania i potencjalnych strat oraz stopnia obniżenia podatności danej organizacji na konkretny typ zagrożenia. W ewaluacji ryzyka związanego z różnymi typami zagrożeń istotna jest trafność określania skutków takich zjawisk szczególnie dla tzw. infrastruktury krytycznej, warunkującej ciągłość działania[4].

Zapewnienie bezpieczeństwa i ciągłości działania organizacji na każdym szczeblu administracyjnym (rys. 1) wymaga przede wszystkim stałego monitorowania ryzyka i trafnej identyfikacji jego **źródeł. Należy założyć, że w inny sposób mogą rozkładać się zagrożenia i ryzyko** zakłócenia działania dla organizacji hierarchicznych (np. instytucje publiczne), w tym organizacje wpływające bezpośrednio na bezpieczeństwo ogólne, a inaczej może się to uzewnętrzniać w organizacjach gospodarczych, funkcjonujących jako organizacje procesowe, typu sieciowego, projektowego lub macierzowego. Organizacje hierarchiczne są bowiem układami silnie scentralizowanymi, choć same, mogą stanowić część bardziej złożonej całości (nadsystemu). Dlatego, bezpieczeństwo państwa jako specyficznej organizacji można traktować w pewnym uogólnieniu jako wypadkową bezpieczeństwa podmiotów administracji publicznej, a zwłaszcza dających się wyodrębnić w tym zbiorze newralgicznych ogniw sprawowania władzy wykonawczej, ustawodawczej i sądowniczej, które przez analogię można nazwać krytycznymi.

Możliwość zapewnienia bezpieczeństwa i ciągłości działania wspomnianych podmiotów wymaga permanentnego gromadzenia informacji o środowisku i otoczeniu systemu, zachodzących tam procesach oraz identyfikowanych na tej podstawie zagrożeniach (rys. 1). Równie ważna jest zdolność skutecznego przeciwdziałania zagrożeniom, a w tym poprzez podnoszenie stałej gotowości do zapobiegania i reagowania na nie, dla poszczególnych elementów danego systemu. Dodając, że działania w obu obszarach powinny być odpowiednio sterowane, można założyć, że szczególnie ważną kategorią zasobów dla zapewniania bezpieczeństwa **i ciągłości działania współczesnych organizacji (w tym organizacji publ**icznych) stanowią zasoby informacyjne, a zdolność ich gromadzenia i przetwarzania stanowi **strategiczny atrybut systemów bezpieczeństwa.**

---

[4] P. Zaskórski, Zasoby informacyjne komponentem infrastruktury krytycznej organizacji, V Międzynarodowa Konferencja Naukowa Katastrofy naturalne i cywilizacyjne. Zagrożenia i wyzwania dla bezpieczeństwa, Wro-cław–Bełchatów 2009.

Rys. 1. Ogólny schemat systemu zapewniania bezpieczeństwa i ciągłości działania OAP
Źródło: opracowanie własne

Istotna w procesie zapewniania oczekiwanego poziomu bezpieczeństwa oraz przeciwdziałania zagrożeniom, w aspekcie różnego typu zagrożeń[5] dla organizacji publicznych (w tym organizacji administracji publicznej) jest co najmniej (rys. 1)[6]:

1. analiza struktury, składu oraz otoczenia danego podmiotu działania;
2. identyfikacja i klasyfikacja zagrożeń,
3. analiza ryzyka oraz wpływu zakłócenia, według ustalonej metodyki wraz z procedurami organizacyjnymi, identyfikacja zależności a także kluczowych elementów systemu, w tym krytycznej infrastruktury (eksponowanie istotnych zjawisk/procesów/obiektów wpływających na bezpieczeństwo organizacji i realizację jej statutowych zadań), z uwzględnieniem wieloaspektowej oceny dynamiki przepływów (materialnych, finansowych, kadrowych, informacji i wiedzy);
4. opracowywanie strategii postępowania z zagrożeniami oraz jej dokumentowanie w postaci planów, procedur i instrukcji dotyczących zapobiegania i reagowania na zdarzenia kryzysowe, dla wybranych typów zasobów / komponentów danej organizacji;
5. monitorowanie środowiska i otoczenia systemu, a także doskonalenie i aktualizacja strategii postępowania, adekwatnie do zaobserwowanych zmian.

5 P. Zaskórski, *Koncepcja informatyzacji systemu reagowania kryzysowego MON*, AON, Warszawa 2002.

6 P. Zaskórski, K. Szwarc, Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania, „Zeszyty Naukowe Wyższej Warszawskiej Szkoły Informatyki" Nr 9 Rok 7, Warszawa 2013, s. 45.

Procedury organizacyjne związane z zapewnianiem ochrony i ciągłości działania powinny uwzględniać najważniejsze typy zasobów warunkujące wypełnianie zadań z obszaru działalności statutowej[7]. Procedury organizacyjne stanowią podstawę zapewniania ciągłości działań poprzez zawarcie w nich opisu sposobu tworzenia struktur zapasowych (awaryjnych) lub dynamicznej zmiany w istniejących strukturach, wskazanie sposobu przesuwania kompetencji i przemieszczania zasobów, a także zasad opracowania i warunków uruchamiania planów awaryjnych. Modele wzorców procedur organizacyjnych dla zidentyfikowanych scenariuszów zagrożeń mogą bazować na strukturach zapasowych lub procesowych, a także na okresowych/specjalnych adaptacjach istniejących struktur działania.

Plany awaryjne mogą różnić się przeznaczeniem, zakresem przedmiotowym, stopniem szczegółowości, a także układem treści. Bazują bowiem na zbiorze analiz, prognoz i zamierzeń działania, gdzie opisuje się całą organizację z uwzględnieniem celu i zaangażowanych zasobów finansowych, osobowych i rzeczowych, w kontekście metod przeciwdziałania wskazanym czynnikom ryzyka. Plany tej klasy są więc dokumentami, w których na podstawie diagnozy sytuacji krytycznych określane są cele, kluczowe strategie i planowane działania[8].

Przygotowanie planu awaryjnego jako komponentu planów ciągłości działania jest procesem rozpoczynającym się diagnozą sytuacji krytycznych, w jakich może się znaleźć konkretny podmiot publiczny. Głównym zadaniem jest więc stworzenie racjonalnych przesłanek dla wyboru skutecznej i racjonalnej strategii działania bazującej na realnych ocenach ilościowo-wartościowych. Analiza i diagnoza danej organizacji powinna wykazać potencjalne możliwości działania z uwzględnieniem podstawowych kategorii zasobów, którymi dysponuje dany podmiot w układzie głównych zadań/funkcji i kompetencji (macierz koincydencji zasoby-funkcje).

Ogólnie należy przyjąć, że zapewnianie bezpieczeństwa, a w tym ciągłości działania każdego podmiotu powinno być analizowane i planowane w wymiarze logistycznym, finansowym, kadrowym, informacyjnym, czasowym i jakościowo-efektywnościowym. Istotne znaczenie dla ciągłości działania mają również determinanty techniczne i infrastrukturalne. W planach działania należy uwzględniać zarówno metody fizycznej i technicznej ochrony obiektów administracji publicznej w kontekście zakłóceń realizacji ustawowych zadań, jak również bezpieczeństwo informacyjne tych podmiotów. Ważny przy tym jest aspekt ciągłości kompetencyjno-personalnej, materiałowo-technicznej, finansowo-zasobowej oraz formalno-prawnej.

---

7 Bezpieczeństwo całej organizacji (systemu) warunkowane jest bezpieczeństwem poszczególnych jego elementów, uczestniczących w podstawowej działalności statutowej.

8 P. Zaskórski (red. nauk.), Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działa-nia, Wyd. WAT, Warszawa 2011, s. 107-144.

3. Planowanie zapewniania ciągłości działania

3.1. Standardy zakresu planowania ciągłości działania organizacji

Procesy planowania zwykle bazują na normach i standardach działania. Dla przykładu jednym z uznanych na świecie standardów z zakresu ciągłości działania w obszarze systemów informatycznych jest dokument NIST[9] „Special Publication 800-34: Contingency Planning Guide for Information Technology Systems", który zawiera pewne uniwersalne wskazania dotyczące konstrukcji planów i procedur operacyjnych w zakresie przeciwdziałania utracie nie tylko informacyjnej ciągłości działania, ale również innych zasobów, w tym infrastruktury krytycznej. Przyjmując, że systemy informacyjne są wielodziedzinowym obrazem możliwości działania każdej organizacji i monitorowania zużywania jej zasobów oraz uzyskiwanych przez nią wyników – można przez analogie przyjąć, że każdy rodzaj zagrożeń w różnych obszarach działania i dla różnych typów zasobów – będzie wymagał podobnych dokumentów. Wspomniany standard z jednej strony zawiera szereg szczegółowych informacji dotyczących wzmacniania odporności systemu informatycznego na zakłócenia (rozdz. 5), a z drugiej zawiera szereg uniwersalnych wytycznych, np. dotyczących samego procesu planowania zapewniania ciągłości działania (rozdział 3). Stąd zalecenia dotyczące zawartości wymienionych rodzajów planów (tabela 1) z powodzeniem można adaptować, w innych obszarach niż tylko systemy informacyjne.

[9] National Institute of Standards and Technology, USA.

Tabela 1. Rodzaje planów zapewniania ciągłości działania według NIST SP 800-34

PLAN	PRZEZNACZENIE	ZAKRES
Plan zapewniania ciągłości działania (BCP)	Zawiera procedury odtwarzania krytycznych procesów lub funkcji (mission/business processes) po ich przerwaniu	Dotyczy procesów realizowanych w konkretnej komórce organizacyjnej lub w całej organizacji. Jest to dokument, który dotyczy wielu wymiarów zapewniania ciągłości działania, co wymaga uzgodnień.
Continuity of Operations Plan (COOP)	Zawiera procedury i wskazania możliwości utrzymywania do 30 dni kluczowych dla organizacji funkcji (mission essential functions) w alternatywnej lokalizacji	Dotyczy krytycznych zadań dla organizacji, które zgodnie z przyjętą strategią winny być wznowione w zapasowej lokalizacji. Tworzony obligatoryjnie w urzędach administracji federalnej.
Plan komunikacji kryzysowej (CCP)	Zawiera procedury rozpowszechniania informacji dla personelu i różnych interesariuszy z otoczenia (tzw. osób trzecich)	W planie ustanawia się różne formy komunikacji adekwatnie do rodzaju incydentu oraz wskazuje podmioty odpowiedzialne za komunikację w sytuacjach kryzysowych.
Plan ochrony infrastruktury krytycznej (CIPP)	Zawiera procedury dotyczące ochrony systemów zaliczonych na podstawie niejawnych kryteriów do zbioru tzw. krytycznej infrastruktury państwa	Zawiera informacje dotyczące lokalizacji oraz struktury systemu, charakterystyki zidentyfikowanych zagrożeń, wariantów ochrony i zapewniania ciągłości działania oraz współpracy z lokalnymi organami odpowiedzialnymi za zarządzanie kryzysowe.
Plan reagowania na incydenty cybernetyczne (CIRP)	Zawiera strategie wykrywania, reagowania i ograniczania skutków ataków na systemy informacyjne organizacji.	Ukierunkowany na obsługę incydentów oraz występowanie zakłóceń w realizacji usług informacyjnych.
Plan odtwarzania po katastrofie (DRP)	Zawiera szczegółowe procedury oraz określa siły i środki do reagowania na zakłócenia, w tym sposób wznawiania pracy systemu w lokalizacji zapasowej.	Pierwotnie dotyczyły głównie obszaru techniki informacyjnej (ITDR). Wraz z ewolucją podejścia do zapewniania ciągłości działania stopniowo ewoluowało w kierunku wszystkich, innych obszarów utraty ciągłości działania (np. ciągłość zabezpieczenia materiałowego, kadrowego itp.).
Plan awaryjny dla systemów IT (ISCP)	Zawiera procedury dotyczące oceny oraz wznawiania pracy systemu informatycznego po zakłóceniu, niezależnie od miejsca i lokalizacji, z wykorzystaniem zapasowego systemu przetwarzania informacji	Wszystkie istotne informacje do wznowienia pracy systemu, a zwłaszcza role i odpowiedzialności, zasady szacowania strat, skład systemu, a także procedury wznawiania i testowania odporności na zakłócenia.
Plan fizycznej ochrony obiektów AP (OEP)	Dotyczy przeciwdziałania występowaniu strat w ludziach, zdrowiu oraz infrastrukturze na wypadek fizycznego ataku na system.	Dotyczy głownie zasobów ludzkich oraz infrastruktury biurowej i znajdującego się tam sprzętu.

Źródło: Opracowanie własne na podstawie: NIST Special Publication 800-34: *Contingency Planning Guide for Information Technology Systems*, June, 2002

Jak widać (tabela 1), istnieje wiele środków wzmacniania odporności administracji publicznej oraz wykorzystywanej przez nią systemów na zakłócenia. Niektóre z nich mają również odwzorowanie w polskim porządku prawnym, a w tym w plany ochrony infrastruktury krytycznej[10] oraz plany zarządzania kryzysowego[11]. Należy zauważyć, że Information System Contingency Plan (ISCP) oraz Disaster Recovery Plan (DRP) mogą być szerzej ukierunkowane na odtworzenie możliwości realizacji kluczowych procesów z ewentualną relokacją zasobów. Oznacza to, że w ramach organizacji może być opracowywanych i wykorzystywanych wiele DRP, jako składowych szerszego planu zapewniania ciągłości działania organizacji, przy czym mogą być wariantowane w zależności od posiadanych zasobów. Sposoby i zakresy planowania ciągłości działania można odnaleźć również w wytycznych dotyczących bezpieczeństwa systemów teleinformatycznych[12], w tym m.in. COBIT™.

Wydaje się, że bardziej precyzyjnym i dość uniwersalnym standardem, w którym uporządkowano sposób reagowania na incydenty jest opracowany przez Brytyjski Instytut Standaryzacji BS 25999: 2006, a zwłaszcza pierwsza część. Zgodnie z tym standardem, dokumentacja powinna obejmować opisanych wcześniej planów zapewniania ciągłości działania oraz odtwarzania po katastrofie również *Plany zarządzania incydentami* (IMP/*Incident Management Plans*), który może być interpretowany szerzej jako plan działania w czasie powstania incydentu/zagrożenia ze specyfikacją potrzebnych sił i środków, a także usług i działań, które należy podjąć aby skutecznie przejąć kontrolę nad zdarzeniem (rys. 2). Opis struktury rodzajów planów został zawarty w standardzie[13].

Ilość i złożoność planów jest według twórców standardu proporcjonalna do wielkości organizacji. Zatem działania podjęte we wszystkich fazach (rys. 2) mogą być równie dobrze opisane w ramach jednego dokumentu. Można zauważyć, że nie akcentuje się tutaj pojęcia „plan awaryjny", ale przez analogię do NIST, jest to raczej wizja obsługi incydentu (ogólniej realizacji konkretnego zagrożenia) oraz przywracania możliwości działania całej organizacji (odtwarzania) Oprócz wspomnianych planów, podstawowa dokumentacja BCM (*Business Continuity Management*) według BS 25999-1 może zawierać:

1. Politykę i strategię w zakresie BCM.
2. Analizę skutków zakłócenia (BIA/*Business Impact Analysis*).
3. Ocenę ryzyka oraz zagrożeń i ich skutków wraz z oceną podatności OAP na te zagrożenia

---

[10] *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej*, Dz.U. z 2010 r. 83, poz. 542.

[11] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. Nr 89 poz. 590 z późn. zm.

[12] *ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security controls*, ISO 2013; *NIST SP 800-100: Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology 2006.

[13] BS 25999-1: 2006: *Business continuity management. Code of practice*, BSI, London 2006.

4. Programy uświadamiania zagrożeń i szkoleń/treningów zachowań.
5. Plany zarządzania incydentami (IMP – *Incident Management Plan*).
6. Plany zachowania biznesowej (procesowej) ciągłości działania (BCP – *Business Continuity Plan*).
7. Harmonogramy ćwiczeń i zasady ich raportowania.
8. Oczekiwany/gwarantowany poziom usług wg przyjętych kryteriów jakości.

Rys. 2. Modelowy przebieg reagowania na incydent wg BS 25999-1

Źródło: BS 25999-1: 2006: *Business continuity management. Code of practice*, BSI London 2006.

Podobne, do zaprezentowanego wcześniej (rys. 2), podejście przyjęto w standardzie ISO / PAS 22399:2007, w którym zakłada się, że wspomniane rodzaje planów powinny opisywać:[14]

- zakres funkcjonalny i kompetencyjny odpowiedzialności dla stron i podmiotów zaangażowanych w reagowanie na zakłócenia oraz wyraźnie zarysowaną hierarchię;
- minimalne zasoby niezbędne do reagowania, w tym miejsce pracy.

Więcej informacji na temat zawartości planów ciągłości działania zawarto w standardzie ISO 22301:2012[15], gdzie oprócz ww. wymagane jest również:

- opis procesu uruchamiania reagowania na zakłócenie (ze zdefiniowanymi kryteriami uruchamiania procedur);
- szczegółowe wytyczne dotyczące zarządzania i mitygowania widocznych konsekwencji zakłócenia;

[14] *ISO/PAS 22399:2007 Societal security – Guideline for incident preparedness and operational continuity management*, ISO, Geneva 2007, p. 6.7.3.

[15] *ISO 22301:2012. Societal security – Business continuity management systems – Requirements*, ISO, Geneva 2012, p. 8.4.4.

- opis sposobu i warunków w jakich informowani będą interesariusze wewnętrzni i zewnętrzni oraz realizacji polityki informacyjnej z wykorzystaniem narzędzi informacyjnych organizacji;
- określenie w jaki sposób organizacja będzie kontynuować lub wznawiać krytyczne procesy przy zidentyfikowanych ograniczeniach czasowych (RTO/MTPD[16]);
- proces zmniejszania gotowości struktur po ustaniu incydentu;
- wyraźne zdefiniowanie wewnętrznych i zewnętrznych współzależności oraz zasad obiegu informacji i dokumentowania podejmowanych działań[17].

Z punktu widzenia planowania ważne są również procedury operacyjne, a w tym standardy zachowań i działań w warunkach sytuacji kryzysowych o lokalnym, regionalnym lub ogólnokrajowym zasięgu oddziaływania, które stanowić powinny tzw. minimum informacyjno-dokumentacyjne organizacji. W tym sensie należy przywołać pojęcie **Ciągłości sprawowania władzy** (ang. *Continuity of Government*), związanego z wdrażaniem polityki zapewniania ciągłości działania Rządu Federalnego Stanów Zjednoczonych, gdzie należy przez to rozumieć zdolność poszczególnych resortów rządu federalnego do niezakłóconego dostarczania newralgicznych funkcji państwa pomimo wystąpienia sytuacji kryzysowej o katastroficznych skutkach.[18] Warto podkreślić, że program jest również skierowany dla innych organów administracji, w tym stanowej[19] Zatem współczesne państwa przygotowują własne systemy zapobiegania i reagowania na tego typu zjawiska, czego przykładem jest przywoływana wcześniej ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym oraz ustawy o stanach nadzwyczajnych. Ważna, w kontekście zapewniania ciągłości działania organów administracji publicznej, jest ochrona infrastruktury krytycznej. Proces poprawy bezpieczeństwa tych, kluczowych systemów w obu państwach, został opisany w podobnych dokumentach[20].

Zagadnienie planowania bezpieczeństwa i ciągłości działania zostało opisane w wielu specjalistycznych, dziedzinowych standardach. Warty polecenia jest m.in. znany na świecie standard NFPA 1600[21], przygotowany przez Narodowy Związek Ochrony Przeciwpożarowej.

---

16 Maximum Tolerable Period of Disruption.

17 K. Szwarc, *Współzależność jako wyzwanie w aspekcie ochrony infrastruktury krytycznej*, [w:] Z. Czachór, A. Chabasińska (red. nauk.), *Bezpieczeństwo narodowe Polski. Zagrożenia i determinanty zmian*, Difin, Warszawa 2016, s. 147-160.

18 National Security Presidential Directive/NSPD-51 and Homeland Security Presidential Directive/HSPD-20 on National Continuity Policy, Washington DC 2007, pt. 2c.

19 *Continuity Guidance Circular 1. Continuity Guidance for Non-Federal Governments,* FEMA 2013.

20 Narodowy Program Ochrony Infrastruktury Krytycznej, RCB, Warszawa 2015; National Infrastructure Protection Plan, U.S. Department of Homeland Security, Washington 2013.

21 *NFPA®1600, Standard on Disaster/Emergency Management and Business Continuity Programs,* National Fire Protection Association, Technical Committee on Emergency Management and Business Continuity 2016.

Zakres, sposób i cykl opracowywania planów ciągłości działania mogą zatem wynikać z przyjętej metodyki (standardu), obowiązujących norm prawnych oraz doświadczenia podmiotu planującego. Na podstawie dokonanej kwerendy, można jednak wyodrębnić pewne uniwersalne elementy planu ciągłości działania.

3.2. Główne wymiary, parametry i wskaźniki planów ciągłości działania OAP

Struktura i zawartość Planu zapewniania ciągłości działania OAP nie posiadają odrębnych, kompleksowych uregulowań prawno-administracyjnych. Stąd wydaje się, że posiłkowanie się analogiami do norm i procedur zachowania informacyjnej ciągłości działania (tab. 1) jest w pełni uzasadnione – zwłaszcza w części dotyczącej działań odtworzeniowych, gdzie istotnymi zapisami są różne uregulowania zależności czasowych takich, jak[22]:

1. RTO (*Recovery Time Objective*) – maksymalny dopuszczalny czas od incydentu, w którym powinno zostać wznowione dostarczanie produktów, działanie systemu. Może to być jednocześnie maksymalny szacowany czas niezbędny do odtworzenia zasobów w całym systemie działania. RTO powinien być ustalany na podstawie analizy ryzyka i podlegać akceptacji przez naczelne kierownictwo danej organizacji. W ustalaniu tego wskaźnika, w kontekście organów administracji publicznej, konieczne jest uwzględnianie nie tyle ekonomicznych co społecznych konsekwencji zakłócenia (braku) sprawowania władzy na administrowanym terenie.
2. RTA (*Recovery Time Actual*) może być traktowany jako parametr określający czas (ustalany drogą eksperymentów) przywracania pracy systemu do stanu sprzed wystąpienia incydentu; zatem newralgiczne z punktu widzenia zapewniania ciągłości działania jest spełnienie warunku: RTA ≤ RTO.
3. RPO (*Recovery Point Objective*) może być traktowany jako parametr określający akceptowalne straty zasobów (przydatność i użyteczność zasobów odtworzonych po kryzysie/katastrofie) mierzone czasem od ostatniej rekonwersji zasobów do chwili powstania sytuacji kryzysowej.
4. NRO (*Network Recovery Objective*) może być traktowany jako parametr określający czas niezbędny do odtworzenia połączeń zewnętrznych danej OAP (jej relacji zewnętrznych np. z dostawcami usług, materiałów eksploatacyjnych, surowców itp.) z podmiotami otoczenia bliższego lub dalszego albo przekierowania zasobów lub usług do innych podmiotów/lokalizacji. Na NRO składają się zwykle czasy odtwarzania zasobów, niezbędnych do wznowienia działania oraz czasy niezbędne do osiągnięcia docelowego, wymaganego poziomu realizacji zadań/sług z uwzględnieniem kryterium jakości wyników działania.

22 *ISO 22301:2012. Societal security…*, op. cit., p. 3.

5. BWO (*Backup Window Objective*) jako parametr określający wymaganą długość przerwy w realizacji zadań/procesów statutowych, determinowanej czasem zabezpieczenia utrzymywanych w organizacji zasobów przed dalszą ich degradacją.
6. MDL (*Maximum Data Loss*) może być potraktowany przez analogię do poziomu utraconych danych jako parametr określający maksymalną wielkość utraconych zasobów materiałowych, sprzętowych, kadrowych, finansowych itp.) z uwzględnieniem dodatkowych możliwości odtwarzania w ramach możliwości własnych lub w relacjach zewnętrznych (w tym outsourcing).

Wskazane powyżej parametry i wskaźniki obrazujące ryzyko i margines bezpieczeństwa procesów w dowolnych organizacjach, są wyznaczana na potrzeby planowania zapewniania ciągłości działania, są często uznawane jako faktyczne zobrazowanie zjawisk występujących w sytuacji kryzysowej/kryzysie i stanowią istotną zmienną przy planowaniu zaangażowania zasobów do wznawiania lub utrzymania pracy systemów, a także wyznaczania tzw. procesów krytycznych.

Każde racjonalne i kompleksowe działanie prowadzone w celu minimalizacji ryzyka występowania zakłóceń, obejmuje[23]:

1. działania prewencyjne, które obejmują przedsięwzięcia ukierunkowane na ograniczenie prawdopodobieństwa realizacji zagrożenia, a pośrednio również straty;
2. działania reaktywne, które wiążą się z realizacją przedsięwzięć zapisanych w procedurach oraz instrukcjach awaryjnych, a koniecznych do wykonania po wystąpieniu zdarzenia kryzysowego tak, aby zmniejszyć straty spowodowane jego wystąpieniem a także umożliwić odtworzenie działania całej organizacji i związanych z nią procesów administracyjno-biznesowych.

Nie każde wystąpienie zdarzenia kryzysowego musi prowadzić do powstania strat. W przypadku gdy istnieją właściwie przygotowane plany zapewniania ciągłości działania oraz zostały wykonane niezbędne działania prewencyjne – to procedury i instrukcje mogą doprowadzić do likwidacji jego skutków w taki sposób i w takim czasie, że OAP zachowa możliwości dalszego działania.

Struktura i zawartość planów zapewniania ciągłości działania OAP wymaga spełnienia określonych warunków takich, jak:

1. zidentyfikowanie procesów kluczowych w danej organizacji z określeniem dopuszczalnych czasów braku aktywności (przerw w działaniu),
2. określenie dla zidentyfikowanych procesów kluczowych ich wrażliwości na zakłócenia w dostępie do określonych zasobów,

[23] K. Liderman, *Model planów ciągłości działania według typów zagrożeń dla wybranych klas organizacji,* Opracowanie przygotowane w ramach zadania 5.1 projektu badawczego PBZ-MNiSW-DBO 01/1/2007; P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów…*, op. cit., s. 47.

3. wskazanie procesów krytycznych przede wszystkim z punktu widzenia minimalnej wielkości rezerwy czasowej lub wręcz jej braku[24] (ogólnie im mniejszy czas dopuszczalnej przerwy/przestoju, tym proces bardziej „krytyczny" [25)],
4. określenie: zagrożeń dla każdego z procesów krytycznych, które mogą doprowadzić do utraty zdolności wsparcia informatycznego a także odtworzenia innych zasobów niezbędnych do realizacji tych procesów,
5. wyznaczenie zakresów kompetencji i odpowiedzialności oraz zasad organizacji pracy dla kadry kierowniczej i pracowników w sytuacji kryzysowej i w warunkach kryzysu,
6. uwzględniania możliwości przeniesienia działalności biznesowej do innych lokalizacji lub do innych organizacji dublujących działanie.

Rys. 3. Struktura planów zapewniania bezpieczeństwa organu administracji publicznej
Źródło: opracowanie własne

Plany zapewniania bezpieczeństwa OAP w różnych wymiarach (rys. 3) muszą więc spełniać następujące założenia[26]**:**

1. zakres procedury dla działań prewencyjnych powinien uwzględniać cel planu (zakres ochrony);

[24] „krytyczność" może też zależeć od wrażliwości procesu na utratę tajności, integralności lub dostępności informacji.

[25] Przykładem krytycznego procesu kluczowego dla OAP może być proces dostaw materiałów eksploatacyjnych do różnych systemów technicznych, wspierających pracę organizacji w warunkach zakłóceń.

[26] P. Zaskórski (red. nauk.), Zarządzanie organizacją…, op. cit., s. 124-134.

2. procedury wznawiania działalności stanowią integralny element „Planu odtwarzania ciągłości działania" i dotyczą sposobów wznowienia działania OAP jako całości albo jej wybranych działów w takim zakresie, aby zapewnić realizację podstawowych procesów administracyjno-biznesowych w sytuacji kryzysowej,
3. procedury odtwarzania działalności uznaje się za element rutynowych, najczęściej długoterminowych, działań organizacji, w celu zapewnienie realizacji procesów administracyjno-biznesowych w podstawowej lokalizacji, w warunkach normalnej organizacji pracy,
4. plan[27] uznaje się za dobry, kiedy prowadzi do sprawnego działania, a w szczególności, gdy jest realizowalny, komunikatywny, racjonalny, kompletny, elastyczny/otwarty (dopuszczający zmiany) oraz czasowo określony (zawierający obowiązujący termin wykonania),
5. procedura musi być traktowana jako opis przebiegu procesów, w którym przedstawia się kolejne czynności i uprawnienia a także odpowiedzialność wykonawców,
6. instrukcja powinna służyć opisowi zasad działania albo przepisów postępowania w konkretnej sytuacji i może odnosić się do procedury (może być jej uzupełnieniem). Instrukcje (w odróżnieniu od procedur), przygotowywane są zwykle dla jednego wykonawcy/jednej grupy wykonawców.

Plan zapewniania bezpieczeństwa powinien być zatwierdzony do użytku przez kierownictwo organizacji, wdrożony i systematycznie aktualizowany. Plan wdrożony oznacza, że dokument ten powinien zostać wprowadzony w organizacji odpowiednim zarządzeniem kierownictwa z realizacją czynności administracyjnych (szkolenia, zakupy, czy zmiany w organizacji pracy i tp.) oraz technicznych (instalacja wyposażenia technicznego, oprogramowania i tp.). Szczególnie ważnym elementem powinny być treningi personelu zatrudnionego w OAP w realizacji planów odtwarzania ciągłości działania oraz testowanie tych planów. W tym sensie przygotowywane są bowiem zasoby kadrowe, umożliwiające mitygowania ryzyka zakłóceń wynikających np. z absencji dużej liczby pracowników. Zawarte w dokumentach planistycznych postanowienia i zadania oraz przydzielone zasoby powinny być zatwierdzone przez odpowiednie osoby z kierownictwa organizacji i być decyzją faktycznie upoważniającą do działania w warunkach szczególnych. Ponadto musi być potwierdzone przyjęcie tych postanowień do wykonania podpisem osób, których dotyczą. Aktualne egzemplarze powinny znajdować się w znanych, dostępnych miejscach[28], zapisane w różnych formatach, a z ich treścią muszą być **zapoznane wszystkie podmioty**, których postanowienia te dotyczą.

[27] T. Kotarbiński, *Traktat o dobrej robocie*, Ossolineum, Wrocław 1982.

[28] Znanych i dostępnych nie oznacza, że nie muszą być chronione przed dostępem osób nieuprawnionych.

Dla każdego wymiaru (typu zasobu) *Planu zapewniania ciągłości działania OAP* należy określić maksymalny tolerowany czas niedostępności danego zasobu (np. poziom dostępności podawany zazwyczaj w %), co może przekładać się na faktyczną ilość godzin niedostępności określonej usługi (możliwości wykonania określonego procesu/zadania). Można tu mówić o kluczowych zasobach warunkujących określone działania OAP jako całości, w tym dopuszczalny czas odtwarzania konkretnego zasobu i związane z tym elementem usługi. Ważne przy tym jest, aby kierownictwo organizacji wskazało osobę odpowiedzialną za kierowanie działaniami zapewniającymi ciągłość administracyjno-biznesową w przypadku wystąpienia zdarzeń kryzysowych. Osobie tej może podlegać *również sztab antykryzysowy.*

W przypadku utraty możliwości pracy niektórych działów administracji publicznej należy wskazać możliwości jej pracy w trybie ograniczonym, a w tym muszą być określone:

1. minimalne zapotrzebowanie na zasoby również w warunkach utraty możliwości realizacji niektórych funkcji/procesów,
2. procedury przejścia w tryb pracy ograniczonej, ze wskazaniem, jakie funkcje będą nieaktywne,
3. możliwości zastąpienia utraconych funkcji (np. poprzez ich alternatywny tryb realizacji), a w tym oszacowanie zapotrzebowania na niezbędne środki (pracowników, urządzenia, materiały, finanse i tp.) i utrzymywanie takich rezerw albo ustalenie procedur ich szybkiego pozyskiwania w sytuacji kryzysowej.

Dla zminimalizowania „wąskich gardeł" w pracy OAP jako swoistego systemu działania w trybie niestandardowym - należy możliwie wcześnie rozpoznać możliwości zastąpienia utraconych funkcji oraz zasobów. Zwykle w pierwszej kolejności należy dążyć do wykorzystania możliwości wewnętrznych (np. poprzez przeniesienie zadań do innego działu). Możliwości zewnętrzne powinny być brane pod uwagę dopiero wtedy, gdy zasoby wewnętrzne nie zapewniają wymagań operacyjnych albo rozwiązania takie nie będą uzasadnione ze społecznego i ekonomicznego punktu widzenia[29].

Jedną z zasad i wymiarów planowania ciągłości działania jest tzw. „kryzysowa organizacja pracy" dla okresu czasu od wystąpienia zdarzenia kryzysowego do pełnego odtworzenia ciągłości działania danej organizacji/firmy. W tej części planowania muszą zostać określone osoby upoważnione do ogłaszania stanu kryzysowego, jak również samodzielnie wykonywane przez jednostki i komórki organizacyjne zadania, związane z opanowaniem zaistniałej sytuacji kryzysowej.

29 T. Drewitt, *A manager's guide to ISO 22301*, IT Governance Publishing, Cambridgeshire 2013, p. 52-62; *All Hazards Risk Assesment. Methodology Guidelines 2012-2013*, Public Safety Canada, 2012, p. 25-45.

Jednym z istotnych komponentów „Planu zapewniania ciągłości działania OAP" może być plan komunikacji kryzysowej, który zawiera opis dróg i środków (np. telefon, fax, kurier, itp.) przekazywania komunikatów o zaistniałej sytuacji kryzysowej do odpowiednich osób i komórek organizacyjnych oraz procedury powiadamiania i potwierdzania alarmu. Dla różnych sytuacji kryzysowych mogą być wytwarzane różne plany alarmowania (np. w przypadku pożaru, w przypadku zniszczeń linii teletransmisyjnych itp.) i ich okresowe testy oraz aktualizacje. Innym, istotnym elementem mającym wpływ na kształtowanie „*Planu odtwarzania* zasobów oraz usług w OAP" są wspomniane wcześniej standardy działania i standardy dokumentacyjne, które mogą dotyczyć m.in. z zakresu i czasu gwarancji, możliwości zaopatrzenia w części zamienne, gwarantowanych czasów dostarczenia zamówionych elementów, gwarantowanego zakresu usług, przybycia ekipy serwisowej itp.

Przy opracowywaniu dokumentów składających się na plan zapewniania ciągłości działania należy wziąć pod uwagę obowiązujące przepisy prawa. Plany zapewniania ciągłości działania są często dokumentem niedocenianym przez kierownictwo danej organizacji. Dopiero konkretne okoliczności, a w tym przepisy prawa, współpraca z bardziej zaawansowanym partnerem (benchmarking standardów organizacyjnych), czy katastrofa/kryzys – są bodźcem do opracowania dokumentów regulujących zagadnienia zapewniania ciągłości działania. Powstaje wówczas problem braku jednolitych, ogólnie uznanych wzorców[30] tego typu dokumentów.

3.3. „Pajęczynowy" model bezpieczeństwa i ciągłości działania OAP

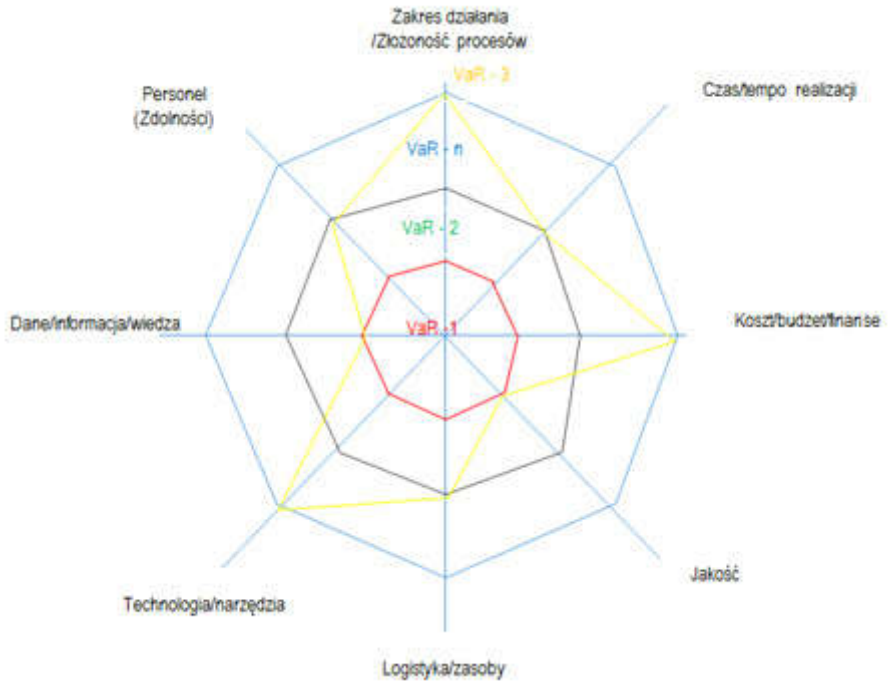
Analiza zagrożeń oraz różnych wymiarów bezpieczeństwa i ciągłości działania organizacji administracji publicznej wskazuje na wielowymiarowość i wieloaspektowość problemu. Stąd wydaje się, że dla oceny poziomu bezpieczeństwa tych organizacji i stopnia zapewniania ciągłości działania przydatnym może okazać się model wielokąta lub szerzej model „pajęczynowy". Głównym założeniem tego modelu jest próba wyznaczenia wskaźnika poziomu bezpieczeństwa OAP a zarazem stopnia spełnienia warunków ciągłości działania. Wskaźnik taki mógłby również służyć porównaniu w analizie porównawczej różnych wariantów planów ciągłości działania (rys. 4).

Na rysunku 4 pokazano czynniki ryzyka (bezpieczeństwa) będące de facto wymiarami planów bezpieczeństwa i ciągłości działania. Oznacza to tylko tyle, że pole takiej „pajęczyny" a w zasadzie pole kolejnej warstwy „pajęczyny" może być interpretowane jako i-ty poziom ryzyka (VaR-i) wyznaczanego:

a) Poziomem złożoności organizacyjno-zadaniowej (poziomem złożoności procesów) danego podmiotu administracji publicznej,

[30] Pewne wytyczne co do ich zawartości są zawarte w normach i standardach takich, jak ISO 27002:2012 oraz COBIT, ale ostateczna struktura i zawartość wytworzonej dokumentacji może się znacznie różnić w zależności od danej OAP.

b) Uwarunkowaniami czasowymi (tempem realizacji poszczególnych operacjo/ procesów),
c) Możliwościami finansowymi (budżetem),
d) Wymaganiami dla oczekiwanej jakości działania,
e) Poziomem zasobów materiałowych, eksploatacyjnych, infrastrukturalnych i tp. (zasobów logistycznych),
f) Poziomem złożoności technologicznej i narzędziowej realizacji poszczególnych procesów,
g) Poziomem zabezpieczenia informacyjnego (informatycznego) oraz potrzeb w zakresie danych i systemów przetwarzających/ wspierających funkcjonowanie OAP,
h) Potrzebami kadrowymi.



Rys. 4. Ogólny schemat modelu „pajęczynowego"
Źródło: opracowanie własne

Zaprezentowany model ośmiokąta foremnego wydaje się modelem idealnym, ponieważ oznacza, ze poszczególne wymiary są dopasowane do optymalnych możliwości i oczekiwań. Często pojęcie „optymalny" może mieć interpretację „zgodny z normą" np. czasową, kosztową, zasobową lub inną. W przypadku niepełnego dopasowania wielkości poszczególnych wymiarów (VaR – 3) do faktycznych potrzeb

organizacji i działań w warunkach zagrożeń oraz kryzysów – ośmiokąt może zostać zniekształcony i pozbawiony waloru „wypukłości". Oznacza to, że niektóre wymiary odbiegają od określonej normy i następuje rozsynchronizowanie modelu. Wyznaczony jednak relatywny poziom ryzyka jako suma pól ośmiu trójkątów opisanych wartościami względnymi poszczególnych wymiarów a więc stosunkiem wartości faktycznych, czy planowanych potrzeb do wartości optymalnej lub normatywnej tego wymiaru dla danej klasy procesów, czy całych organizacji klasy OAP np. określonego szczebla – może być wykorzystany do ewaluacji poziomu bezpieczeństwa względnego.

Wskaźnik bezpieczeństwa można wówczas wyznaczyć jako dopełnienie (np. procentowe) poziomu ryzyka. Należy jednak pamiętać, że każdy wariant planu zapewniania ciągłości działania określony w różnych wymiarach i planu całościowego bezpieczeństwa i ciągłości działania OAP – będzie opisany inną charakterystyką ilościowo-wartościową tych wymiarów. Z dość pobieżnej analizy takiego wykresu (rys. 4) wynika, w którym wymiarze dany organ jest szczególnie podatny na występowanie zakłóceń, a co za tym idzie, jakie zasoby należy gromadzić (redundować), aby ograniczyć ryzyko występowania zakłóceń. Stąd każdy wariant będzie charakteryzowany wskaźnikami ryzyka i poziomu bezpieczeństwa. Ostateczny wybór wariantu może następować na bazie ewaluacji tych wskaźników.

Warto w tym miejscu zatrzymać się nad interpretacja poszczególnych wymiarów, ponieważ można odwrócić interpretacje pola warstw „pajęczyny" jako obraz lub wskaźnik poziomu bezpieczeństwa. Oznacza to wówczas, że w wymiarach eksponowane są składowe pozytywne, a mianowicie czas może oznaczać faktyczne tolerancje czasowe, a więc im dłuższy czas do dyspozycji wykonawcy, tym wyższy poziom bezpieczeństwa poprawnego wykonania i jakości wyników. W przypadku ewaluacji wskaźnika ryzyka należy operować miarą tempa realizacji procesu i tak im wyższe tempo, tym krótszy czas realizacji przedsięwzięć, a więc wyższe ryzyko. Podobnie inne wymiary będą oznaczały poziom wzmocnienia czynników bezpieczeństwa.

Przedstawiony tutaj model jest zapewne pewną ideą łączenia różnych wymiarów bezpieczeństwa, poszukiwania i analizy zależności synergicznych między nimi a ponadto dążeniem do operowania względnie jednoznacznym a może nawet obiektywnym - miernikiem ryzyka lub bezpośrednio poziomu bezpieczeństwa. Ewaluacja poziomu bezpieczeństwa organizacji publicznych (w tym zarówno biznesowych, jak i administracji publicznej) jest wyzwaniem i problemem bardzo złożonym. Każda próba ewaluacji bezpieczeństwa wymusza porządkowanie i systematykę różnych jego determinant oraz wymiarów oraz daje podstawę do obiektywizacji analizy wartości poszczególnych organizacji i ich różnych zamiarów/wariantów działania w sytuacjach trudnych a nawet kryzysowych. Jednym z wariantów działania w sytuacjach trudnych jest strategia outsourcingu lub strategia alternatywnych zasobów, w tym alternatywnych lokalizacji (dyslokacji zasobów).

3.4. Alternatywna lokalizacja jako element strategii zapewniania ciągłości działania

Podstawowym zabezpieczeniem przed utratą ciągłości działania OAP, w przypadku katastrofy niszczącej newralgiczne elementy organizacji, jest zapasowa lokalizacja i oprzyrządowanie. Można wyróżnić różne modele lokalizacji zapasowej, a w tym zapasową lokalizację zasobów odtworzeniowych lub całościowego dublera dla prowadzenia biznesowo-administracyjnych działań operacyjnych[31]. Jest to zapewne podział uproszczony, ponieważ w praktyce budowane są modele typu mieszanego, łączące funkcje zapasowego składowania i odtwarzania zasobów, jak i prowadzenia działalności administracyjno-biznesowej, związanej z bezpośrednią obsługą interesantów w sytuacjach kryzysowych. W zależności od stopnia przygotowania lokalizacji zapasowej do przejęcia działalności operacyjnej OAP - można mówić o:

a) „wymianie usług" z inną organizacją o podobnym profilu działalności,
b) własnej (firmowej) zapasowej infrastrukturze,
c) dzierżawieniu na tzw. zasadach hostingu[32] lub kolokacji[33] (zapasowa lokalizacja zasobów i narzędzi).

Przykładowo w wymiarze informacyjnej ciągłości działania można mówić o ośrodkach zapasowych dla działań odtworzeniowych np. dla odtwarzania danych niezbędnych do kontynuowania działalności administracyjno-biznesowej. Z badań amerykańskich[34] wynika, że wiodące firmy przeznaczają na szeroko pojęte bezpieczeństwo nawet do 14% budżetów IT. W wielu przypadkach część tego budżetu jest zorientowana na organizację zapasowego centrum danych, ale należy pamiętać, że własne centrum zapasowe jest przydatne tylko dla organizacji działającej w trybie 24/7 z bardzo dużą ilością zasobów i wrażliwych danych z ograniczonym dostępem trzecich firm. W innych przypadkach można stosować outsourcing i skalowalne usługi w chmurze obliczeniowej[35].

Należy zauważyć, że nadmiarowa lokalizacja stanowi uniwersalne narzędzie wzmacniające odporność systemu na zakłócenia, zwłaszcza w kontekście urealnienia zagrożeń o dużym zasięgu oddziaływania. Zabezpieczenie w postaci ośrodka zapasowego może zwiększać zaufanie do potencjalnego partycypanta, w realizacji

---

[31] Szczególnym przypadkiem tego typu modelu może być zapasowe *centrum zarządzania kryzysowego* (tzw. *alternate processing site*).

[32] Hosting – realizacja usługi (np. składowania danych) przez dostawcę usługi na jego zasobach sprzętowych i programowych, w jego centrum danych.

[33] Kolokacja – usługa polegająca na wynajęciu miejsca w centrum dostawcy usługi i umieszczeniu w nim własnych zasobów np. sprzętu komputerowego.

[34] Na grupie ponad 8 tys. firm z 62 krajów świata

[35] K. Szwarc, P. Zaskórski, *„Chmura" obliczeniowa jako usługa ograniczająca ryzyko utraty ciągłości działania*, [w:] M. Żuber (red.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i ochrona infrastruktury krytycznej*, Wrocław 2013, s. 201-212.

przedsięwzięcia, a nawet być traktowane jako warunek uczestnictwa w takowym. Taki sposób ograniczania ryzyka można traktować jako swego rodzaju gwarancję informacyjnej ciągłości działalności biznesowej na wypadek katastrofy lub poważnej awarii systemu teleinformatycznego, wspierającego kluczowe procesy biznesowe w podstawowej siedzibie organizacji albo podstawowym ośrodku obliczeniowym. Pojęcie katastrofy jest jednak pojęciem niejednoznacznym i tak przykładowo w aspekcie systemów teleinformatycznych, katastrofa następuje wtedy, gdy z jakiegoś powodu (klęski żywiołowej, awarii, itp.) przerwa w pracy systemu przekracza czas dopuszczalny.

Strategia alternatywnej lokalizacji i procesy odtworzenia mogą być odrębnymi, rozdzielonymi w czasie działaniami, ale powinny sprzyjać najogólniej ciągłości działania poprzez zminimalizowanie:

a) ilości utraconych zasobów (np. danych) wskutek katastrofy,
b) czasu niedostępności określonych usług (m.in. informatycznych), spowodowanego realizacją procedur awaryjnych i odtworzeniowych,
c) kosztów procesu odtwarzania (m.in. wykonywania kopii zapasowych dla zasobów informacyjnych).

Każdy wymiar planu zapewniania ciągłości działania wymaga odrębnej analizy. Strategia lokalizacji zapasowych/alternatywnych i procesy odtworzeniowe różnego typu zasobów mogą być kosztowne. Stąd w modelu „pajęczyny" podjęcie niektórych działań sprzyja wzrostowi poziomu bezpieczeństwa w danym wymiarze, ale osłabię jego poziom na innej współrzędnej. Naturalnym sposobem ograniczania kosztów związanych z wyznaczaniem i wyposażaniem zapasowego stanowiska pracy dla organów administracji publicznej jest wykorzystanie w tym celu potencjału terenowych jednostek administracji zespolonej (np. Państwowej Straży Pożarnej), wyposażonej zazwyczaj w inne, konieczne systemy nadmiarowe (np. agregat prądotwórczy). W takim przypadku wybór zapasowego stanowiska dyktowany jest nie tylko dostępnością określonych zasobów na miejscu ale również fizyczną lokalizacją siedziby takiego organu. Obowiązek tworzenia zapasowych stanowisk kierowania dla organów administracji publicznej do szczebla województwa wynika z przepisów prawa[36].

Zasadność wyznaczania zapasowej lokalizacji, zwłaszcza dla newralgicznych procesów realizowanych przez organa administracji publicznej, wynika z następujących przesłanek:

a) podczas odtwarzania zasobów podstawowa siedziba może być częściowo niedostępna dla pracowników lub interesariuszy,
b) niektóre zasoby w procesie odtworzenia mogą utracić swoją użyteczność lub funkcjonalność,
c) dodatkowe czynności m.in. związane z analizą strat oraz opracowaniem sposobu odzyskania utraconych zasobów mogą trwać dość długo (nawet kilka dni).

36 Zob. Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym, Dz.U. z 2004 r. nr 98, poz. 978.

W ocenach czasu niesprawności organizacji można odwołać się do parametrów wymiaru czasu, którymi operuje się w przedstawionej wcześniej klasyfikacji np. RTO i RPO. Można tu przez analogie do usług i wymiaru informacyjnego - mówić także o poziomach bezpieczeństwa. Będzie to jednak temat kolejnych badań i rozwiązań w obszarze ciągłości działania różnych organizacji. Należy jednak zauważyć, że sam proces przeniesienia na stanowisko zapasowe jest często krytycznym momentem w przejmowaniu kontroli nad sytuacjami kryzysowymi. Dlatego powinien być wcześniej odpowiednio zaplanowany i przygotowany, włącznie z określeniem minimalnych możliwości pracy, na podstawie dostępnego wyposażenia. Zmianie i utrudnieniom ulega wówczas komunikacja z interesariuszami zewnętrznymi, choćby z powodu zmiany numerów stacjonarnych numerów telefonicznych. Zatem, jak wcześniej zauważono, problem komunikacji w sytuacjach kryzysowych winien być wcześniej odpowiednio zaplanowany.

4. Wariantowanie scenariuszy monitorowania i zapewniania ciągłości działania

Wariantowanie scenariuszy działania, a w tym scenariuszy monitorowania i występowania zakłóceń to przede wszystkim możliwość operowania wspólną, jednolitą i aktualną informacją oraz narzędziami umożliwiającymi szybkie przetwarzanie zasobów informacyjnych. Stąd szczególnego znaczenia nabierają systemy zbierania i gromadzenia informacji zarówno bieżącej, jak i historycznej (statystycznej), ważnej dla każdej organizacji, w tym również dla OAP. Takie więc systemy, jak ERP II, EERP (w tym @ERP) oraz systemy OLAP a także systemy klasy AI [4] i systemy eksperckie/SE – mogą stanowić pewien standard informacyjny a jednocześnie zabezpieczać działania silnie limitowane czasem podejmowania decyzji i czasem ich realizacji.

Ciągłość działania w wymiarze informacyjnym determinowana jest dostępem do aktualnej i użytecznej informacji. Stąd systemowa (ogólna) ciągłość działania organizacji lub jej komponentu dziedzinowego (wymiaru) jest determinowana ciągłością informacyjną. Przyjmując wybrane modele i zakresy strategii zapewniania informacyjnej ciągłości działania należy stwierdzić, że w praktycznym działaniu zależnie od potrzeb i możliwości danej organizacji – stosowane są różne mechanizmy ochrony jej zasobów informacyjnych i zabezpieczania danych. Należy więc mieć na uwadze fakt, że przykładowo plan własny lub plany według NIST dotyczą działań odtworzeniowych, ale bazą ich opracowywania mogą być wyznaczone, krytyczne elementy systemów teleinformatycznych i sieci wraz z określeniem ich wagi. Można

przyjąć, że są to komponenty „Planu zapewniania ciągłości działalności organizacji/firmy" Koncepcja taka jest zgodna z podejściem proponowanym przez NIST[37].

Konfigurowanie planu wynika z możliwości wariantowania jego struktury, które mają wpływ na [9] zawartość procedur, planowaną kolejność wykonywania procedur oraz dobór procedur do planu, jak również ograniczenia i limity czasowe. Każdy wariant planu może być odniesiony do wymiaru (dziedziny planu) oraz do typu zagrożenia, takiego jak:

1. oddziaływanie sił natury,
2. awarie sprzętu i urządzeń technicznych,
3. błędy ludzi,
4. celowe działania ludzi,
5. błędne działanie systemów/oprogramowania.

Klasy organizacji (zarówno organizacje hierarchiczne i płaskie) mogą mieć wpływ na objętość i rodzaj przesyłanych/odtwarzanych danych oraz na ich rozmieszczenie, a także na część techniczno-komponentową systemów i sieci teleinformatycznych. Każde działanie wymaga dostosowania do odpowiednich procedur. Ogólna struktura procedury bezpieczeństwa i ciągłości działania powinna wskazywać na konkretną organizację (jednostkę organizacyjną) i cel (cele), który dzięki zastosowaniu tej procedury można uzyskać oraz oczekiwane efekty jej zastosowania. Ponadto tej klasy procedura powinna mieć ustalone:

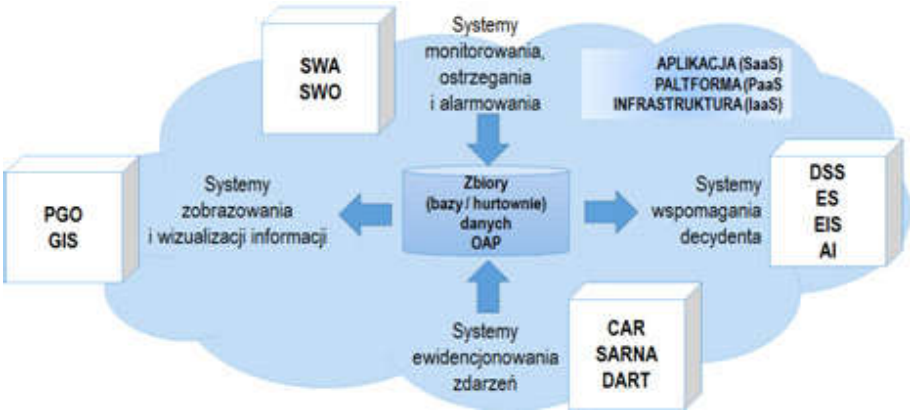
1. Zakres stosowania , a w tym opisany tok postępowania, kogo dotyczy (jednostki organizacyjne, stanowiska itp.), a także sposób uruchamiana w danej sytuacji (dla różnych wariantów zagrożeń);
2. Terminologię i definicje ważnych pojęć występujących w procedurze;
3. Osoby odpowiedzialne za realizację zadań wskazanych w procedurze;
4. Sposób realizacji zadań w poszczególnych fazach (np. odebranie sygnału, powołanie zespołu, analiza, powiadomienie i tp. Sposób realizacji można przedstawić w formie swoistego algorytmu kolejno podejmowanych działań, w formie werbalnej lub w formie prezentacji graficznej);
5. Typowe zagrożenia spotykane w czasie realizacji tej procedury;
6. Główne zasoby materialne (np. techniczne) i niematerialne (np. technologiczne);
7. Podmioty współpracujące (w niektórych specyficznych procedurach może wystąpić konieczność wariantowania współpracy z podmiotami zewnętrznymi lub też wręcz określenia zespołów wielopodmiotowych);
8. Podstawę prawną działań (w tym regulacje zewnętrzne lub wewnętrzne, w tym plan reagowania, instrukcje itp.)

[37] NIST Special Publication 800-34: *Contingency Planning Guide for Information Technology Systems*. June. 2002; NIST Special Publication 800-82 (SECOND PUBLIC DRAFT): *Guide to Industrial Control Systems (ICS) Security*. September 2007.

9. Zasady dokumentowania działań (zapisy, raporty, sprawozdania itp.);
10. Załączniki w tym formularze, rejestry, pokwitowania itp.).

Tworząc model/strukturę planów i procedur organizacyjnych oraz ustalając zasady ich wariantowania dla określonych klas organizacji kreuje się podstawę do wyboru i implementacji narzędzi wspomagających generowanie poszczególnych wariantów planu ciągłości działania. Z uwagi na to jednak, że bezpieczeństwo organizacji wyznaczane jest przez poziom ryzyka utraty informacyjnej ciągłości działania – w dalszej części zostaną przedstawione zagadnienia biznesowej/administracyjnej ciągłości działania organizacji (OAP) ze szczególną ekspozycją wybranych klas zintegrowanych systemów informatycznych zarządzania. Ważne bowiem staje się operowanie własnymi, bogatymi zasobami (rzeczowymi, informacyjnymi, finansowymi, energetycznymi, czy ludzkimi), ale jednym z ważnych uwarunkowań staje się aktualna informacja o tych zasobach i ich dyslokacji również w relacji z otoczeniem zewnętrznym. Duże znaczenie ma tutaj współodpowiedzialność i poziom świadomości pracowników oraz samokontrola. Innym, równie ważnym z punktu widzenia zachowania ciągłości działania, rozwiązaniem jest szeroko rozumiana decentralizacja podejmowania decyzji oraz odpowiedzialność decyzyjna w uwarunkowaniach zewnętrznych i kryzysowych.

Można stwierdzić, że na potrzeby oceny ryzyka, formułowania strategii przeciwdziałania zagrożeniom oraz bieżącego zarządzania i zapewniania bezpieczeństwa, każda organizacja (w tym administracja publiczna) powinna zadbać o utrzymanie repozytoriów danych transakcyjnych i analitycznych (rys. 5). Zasoby transakcyjne odzwierciedlają bieżące możliwości oraz potrzeby administracji publicznej w wymiarze procesów roboczych. Analityczne zaliczyć można do zasobów strategicznych, które mogą być obrazem długiego okresu funkcjonowania organizacji i podstawą realizacji procesów decyzyjnych szczególnie w wymiarze strategicznym



Rys. 5. Zasoby informacyjne jako determinanta skutecznego decydowania
Źródło: opracowanie własne

(programowanie strategii przeciwdziałania zakłóceniom w wymiarach prewencyjnym i reaktywnym). Tak więc całościowy proces zarządzania OAP i zapewnienie jej ciągłości działania jest następstwem wykorzystania rozwiązań informatycznych/ systemów teleinformatycznych np. przez możliwość szybkiej oceny sytuacji, przeglądu dostępnych sił i środków oraz angażowania ich zgodnie z opracowanymi planami / procedurami.

Problem zapewnienia ciągłości działania organizacji i jej wpływu na procesy zachodzące w jej wnętrzu i w otoczeniu - wiąże się dość często z możliwością odwołania się do historii i tzw. analitycznych zasobów informacyjnych. Gromadzone dane transakcyjne mogą dotyczyć wymiaru ogólnego (otoczenia dalszego, w tym określonych norm, wskaźników społeczno-ekonomicznych oraz prawno-politycznych). W wymiarze otoczenia bliższego ważna jest informacja o różnych podmiotach limitujących działania OAP (np. dostawcy, dystrybutorzy, pośrednicy, itp.) oraz klienci i pozostali interesariusze. Zwykle dane opisujące związki gospodarcze (organizacyjne) pomiędzy organizacją a otoczeniem bliższym (dane „wewnętrzne") można uznać za unikatowe. Mogą służyć tworzeniu wielowariantowych zestawień i analiz w celu lepszego zrozumienia zmian zachodzących w otoczeniu i elastycznego dopasowania się do nich – zwłaszcza w sytuacji z dużym poziomem ryzyka. Można na tych zasobach danych zdefiniować procesy integracji i agregacji a wtedy staną się danymi analitycznymi magazynowanymi m.in. w hurtowniach danych (HD)[38].

W procesie planowania i podejmowania decyzji główną bazą są zasoby analityczne (hurtownie danych z systemami klasy OLAP i procedurami DM[39]), które umożliwiają prowadzenie wieloaspektowych (wielowymiarowych) złożonych analiz i konstruowanie na ich podstawie wielowariantowych (wielodziedzinowych) raportów (w tym np. planów rzeczowo-finansowych)[40]. Dane te mogą stanowić bazę do generowania wiedzy (wzorców i modeli zachowań). Kierownicy OAP mogliby więc na tej podstawie np. przewidywać wystąpienie określonych zagrożeń (głównie natury informacyjno-decyzyjnej), ale również przeciwdziałać ich negatywnym skutkom, zapewniając tym samym ogólną lub dziedzinową (dla określonego wymiaru/ obszaru działania i zasobów z tym związanych) ciągłość działania swojej organizacji w momencie zaistnienia zagrożenia. Należy przy tym pamiętać, że ciągłość jest silnie determinowana dynamiką działań i procesowym modelem zarządzania, w tym bieżącego monitorowania zasobów organizacji w kontekście zagrożeń. Stąd możliwość

[38] Hurtownie danych w szczególnych sytuacjach można uznać za magazyny/repozytoria danych warunkujące procesy odtwarzania danych, a zarazem będące podstawa wdrażania i użytkowania zaawansowanych funkcji klasy Business Intelligence (BI).

[39] Data Mining – „zgłębianie" danych, „odkrywanie" wiedzy

[40] P. Zaskórski, *Asymetria informacyjna w zarządzaniu procesami*, WAT, Warszawa 2012.

zapewniania przede wszystkim informacyjnej ciągłości działania poprzez dostęp do sieci powszechnej typu Internet, a ogólniej do usług w chmurze obliczeniowej[41].

Procesy decyzyjne w strukturach procesowych są warunkowane bezpośrednim dostępem do systemów OLTP i mechanizmów systemów OLAP/DM w dłuższej perspektywie czasowej. Dzięki temu możliwa jest kompleksowa analiza zagrożeń oraz monitorowane i wieloaspektowe analizowanie sytuacji i w ślad za tym wspomaganie działań zgodnie z przyjętą polityką zapewniania bezpieczeństwa, w tym ciągłości działania organizacji.

Wybór i nadzorowanie realizacji wariantu planu bezpieczeństwa i zapewniania ciągłości działania wymaga koordynowania działań. W trakcie ich realizacji następuje gromadzenie oraz przetwarzanie danych bieżących i analitycznych pozyskiwanych także z otoczenia poprzez nawiązywanie współzależności pomiędzy poszczególnymi realizatorami procesów/działami. Eliminuje się bariery w komunikacji, które często uniemożliwiają (lub w znacznym stopniu utrudniają) utrzymanie ciągłości działania. Szybka identyfikacja źródeł ryzyka pozwala na właściwe i skuteczne działanie. Dążąc do wzrostu skuteczności działań prewencyjno-naprawczych w aspekcie ryzyka utraty ciągłości działania, należy przede wszystkim:

a) zbudować trwałe zespoły wykonawcze dla poszczególnych, kluczowych procesów oraz wzmacniać ich wiedzę i potencjał;
b) kształtować efektywność i skuteczność działania w związku z reagowaniem na możliwość obniżenia bezpieczeństwa OAP i zakłóceń ciągłości działania.

Właściwe organizowanie i koordynowanie różnych procesów w OAP wymaga odpowiednich narzędzi dla nadzorowania realizacji różnych wariantów planów i zapewnienia ciągłości funkcjonowania całej organizacji.

Procesy kontroli działań umożliwiają zlokalizowanie i wyeliminowanie słabych ogniw systemu bezpieczeństwa i ciągłości działania wobec realnych zagrożeń. Kontrola jest bowiem niezbędnym elementem procesu utrzymania lub odtwarzania ciągłości działania zarówno w wymiarze organizacyjno-kadrowym, jak i zasobowo-czasowym.

Korzystanie z procesowego modelu zarządzania jednostką administracji publicznej w warunkach kryzysów i zagrożeń stwarza wiele szans, umożliwiających zapewnienie informacyjnej ciągłości działania organizacji lub szybką rekonstrukcję jej działań głównie poprzez: delegowanie uprawnień decyzyjnych, działanie zespołowe oraz systematyczne doskonalenie. Czynnikiem poprawy poziomu bezpieczeństwa mogą stać się w wielu przypadkach dobrze chronione i selektywnie udostępniane analityczne zasoby informacyjne (OLAP), umożliwiające dynamiczne wspomaganie analiz i procesów podejmowania decyzji w warunkach określonych zagrożeń i wdrażania alternatywnych planów przeciwdziałania im.

---

[41] Rosenberg J., Mateos A., *Chmura obliczeniowa. Rozwiązania dla biznesu*, Helion S.A., Warszawa 2011. K. Szwarc, P. Zaskórski, *„Chmura" obliczeniowa jako usługa*, op. cit., s. 201-212.

Ważnym czynnikiem warunkującym skuteczność zapewnienia ciągłości działania OAP jest szeroko rozumiana infrastruktura w różnych jej wymiarach. Nie można jednak zapomnieć o tym, że repozytoria określonych kategorii zasobów informacyjnych szczególnie o elementach infrastruktury krytycznej organizacji przyczyniają się w znacznym stopniu do zapewnienia ogólnego bezpieczeństwa całej organizacji. Chcąc zachować ich wysoką wartość merytoryczną, niezbędne jest zapewnienie im atrybutu aktualności i poufności.

5. Zakończenie

Autorzy podnieśli problem silnego związku wielowymiarowej (ogólnej/systemowej) ciągłości działania organizacji administracji publicznej i poziomu jej bezpieczeństwa z informacyjną ciągłością działania i możliwością operowania aktualną informacją o stanie realizacji zadań/procesów oraz o bieżącym poziomie zasobów niezbędnych do ich realizacji. W obecnych czasach dostosowuje się struktury kierowania do nowych realiów politycznych, technicznych i organizacyjnych. Z doświadczeń różnych sytuacji kryzysowych i z ostatnich kryzysów wynika, że współczesne działania kryzysowe nie mogą być skutecznie prowadzone bez rozbudowanego wsparcia informacyjnego i teleinformatycznego.

Procesowe modele zarządzania uznaje się za rozwiązania wzmacniające poziom bezpieczeństwa organizacji oraz za możliwość uelastyczniania i uodporniania organizacji na różne zakłócenia na gruncie zapewniania informacyjnej ciągłości procesów w organizacji. Tym samym może być utrzymywany względnie stabilny system informacji o poszczególnych typach zasobów warunkujących systemową ciągłość działania OAP.

Rozwój Internetu i szeroko pojmowanych usług w chmurze obliczeniowej[42] powoduje, że następuje wirtualizacja całych systemów zarządzania i dowodzenia z ekspozycją podmiotów zewnętrznych. Ważnym, a może bazowym czynnikiem wartości organizacji, w tym szczególnie typu OAP jest de facto informatyzacja procesów podstawowych (krytycznych) a do szczególnie newralgicznych należą procesy zbierania, syntezy, uogólniania i prognozowania skutków z wykorzystaniem metod i środków informatyki. Współczesne systemy kierowania ewoluują w ślad za rozwojem bazy techniczno-technologicznej informatyki[43] oraz ujednolicają swoje reguły działania poprzez standaryzację rozwiązań, co jest ważnym atrybutem usług w chmurze obliczeniowej.

---

[42] P. Zaskórski, *Wirtualizacja organizacji w „chmurze" obliczeniowej*, Ekonomika i Organizacja Przedsiębiorstwa, Warszawa 2012, s. 24-33; P. Zaskórski, D. Pałka, P. Zaskórski, *Cloud computing jako środowisko integracji usług informatycznych*, „Zeszyty Naukowe WWSI", Warszawa 2013.

[43] M. Maleszak, P. Zaskórski, *Systemy i modele sztucznej inteligencji w zarządzaniu współczesną organizacją*, Wyd. SGGW, Warszawa 2015.

Uproszczenie i automatyzacja działania z wykorzystaniem ICT uzależnia podmioty administracji publicznej od tej klasy systemów, od których sprawności, zależy coraz częściej zdolność działania. Tym bardziej zasadne jest zatem ustanawianie kompleksowych zabezpieczeń, wymaganych przepisami prawa[44], w tym w zakresie zapewniania ciągłości działania[45].

BIBLIOGRAFIA:

[1] *All Hazards Risk Assessment. Methodology Guidelines 2012-2013*, Public Safety Canada, 2012.

[2] BS 25999-1: 2006: *Business continuity management. Code of practice,* BSI, London 2006.

[3] *Continuity Guidance Circular 1. Continuity Guidance for Non-Federal Governments*, FEMA 2013.

[4] Drewitt T., *A manager's guide to ISO 22301*, IT Governance Publishing, Cambridgeshire 2013.

[5] Grocki R., *Zarządzanie kryzysowe. Dobre praktyki*, Difin, Warszawa 2012.

[6] *ISO 22301:2012. Societal security – Business continuity management systems – Requirements,* ISO, Geneva 2012.

[7] *ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security controls*, ISO 2013;

[8] *ISO/PAS 22399:2007 Societal security – Guidline for incident preparedness and operational continuity management,* ISO, Geneva 2007.

[9] Kotarbiński T., *Traktat o dobrej robocie*, Ossolineum, Wrocław 1982.

[10] Liderman K.:, *Model planów ciągłości działania według typów zagrożeń dla wybranych klas organizacji,* Opracowanie przygotowane w ramach zadania 5.1. projektu badawczego PBZ-MNiSW-DBO 01/1/2007

[11] Maleszak M., Zaskórski P., *Systemy i modele sztucznej inteligencji w zarządzaniu współczesną organizacją.* Wyd. SGGW, Warszawa 2015.

[12] Narodowy Program Ochrony Infrastruktury Krytycznej, RCB, Warszawa 2015.

[13] National Infrastructure Protection Plan, U.S. Department of Homeland Security, Washington 2013.

[14] National Security Presidential Directive/NSPD-51 and Homeland Security Presidential Directive/HSPD-20 on National Continuity Policy, Washington DC 2007.

[15] *NFPA®1600, Standard on Disaster/Emergency Management and Business Continuity Programs,* National Fire Protection Association, Technical Committee on Emergency Management and Business Continuity 2016.

[16] *NIST SP 800-100: Information Security Handbook: A Guide for Managers,* National Institute of Standards and Technology 2006.

[17] NIST Special Publication 800-34: *Contingency Planning Guide for Information Technology Systems.* June 2002.

[44] Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* Dz.U. z 2014 poz. 1114; Obwieszczenie Prezesa Rady Ministrów z dnia 14 stycznia 2016 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2016 poz. 113.

[45] K. Szwarc, *Bezpieczeństwo informacji w organizacji typu „Podmiot publiczny"*, „Studia Bezpieczeństwa Narodowego", Zeszyt 8, WAT, Warszawa 2015, s. 126-144.

[18] NIST Special Publication 800-82 (SECOND PUBLIC DRAFT): *Guide to Industrial Control Systems (ICS) Security*. September 2007.

[19] Obwieszczenie Prezesa Rady Ministrów z dnia 14 stycznia 2016 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2016 poz. 113.

[20] Rosenberg J., Mateos A., *Chmura obliczeniowa. Rozwiązania dla biznesu*, Helion S.A., Warszawa 2011.

[21] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym, Dz.U. z 2004 r. Nr 98 poz. 978.

[22] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz.U. z 2010 r. 83 poz. 542.

[23] Szwarc K., *Bezpieczeństwo informacji w organizacji typu „Podmiot publiczny"*, „Studia Bezpieczeństwa Narodowego", Zeszyt 8, WAT, Warszawa 2015.

[24] Szwarc K., *Uwarunkowania ciągłości działania systemu zarządzania kryzysowego*, „Studia Bezpieczeństwa Narodowego", WAT, Warszawa 2014.

[25] Szwarc K., *Współzależność jako wyzwanie w aspekcie ochrony infrastruktury krytycznej*, [w:] Z. Czachór, A. Chabasińska (red. nauk.), *Bezpieczeństwo narodowe Polski. Zagrożenia i determinanty zmian*, Difin, Warszawa 2016.

[26] Szwarc K., Zaskórski P., *„Chmura" obliczeniowa jako usługa ograniczająca ryzyko utraty ciągłości działania*, [w:] M. Żuber (red.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i ochrona infrastruktury krytycznej*, Wrocław 2013.

[27] Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*, Dz.U. z 2014 poz. 1114.

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

[29] Zaskórski P. (red. nauk.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, Wyd. WAT, Warszawa 2011.

[30] Zaskórski P., *Koncepcja informatyzacji systemu reagowania kryzysowego MON*, AON, Warszawa 2002.

[31] Zaskórski P., Pałka D., Zaskórski P., *Cloud computing jako środowisko integracji usług informatycznych*, „Zeszyty Naukowe WWSI", Warszawa 2013.

[32] Zaskórski P., Szwarc K., *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Wyższej Warszawskiej Szkoły Informatyki" Nr 9 Rok 7, Warszawa 2013.

[33] Zaskórski P., *Wirtualizacja organizacji w „chmurze" obliczeniowej*, Ekonomika i Organizacja Przedsiębiorstwa, Warszawa 2012.

[34] Zaskórski P., *Zasoby informacyjne komponentem infrastruktury krytycznej organizacji*, V Międzynarodowa Konferencja Naukowa, Katastrofy Naturalne i Cywilizacyjne. Zagrożenia i wyzwania dla bezpieczeństwa. Wrocław–Bełchatów 2009.

MODELING OF SECURITY AND CONTINUITY OF GOVERNMENT PROCESSES

Summary: Article identifies the factors that strengthen the public administration security and continuity, especially in informational dimension. It presents the basic assumptions and requirements

for continuity of government model, the framework of "spider's web" risk analysis tool. The system is based on the NIST 800-34 standard, as described.
Keywords: security, continuity of government, security management, ensuring security.