UWARUNKOWANIA CIĄGŁOŚCI DZIAŁANIA SYSTEMU ZARZĄDZANIA KRYZYSOWEGO

Krzysztof Szwarc

Wojskowa Akademia Techniczna

Streszczenie: W artykule przedstawiono uwarunkowania przeciwdziałania zagrożeniom. Podjęto próbę analizy systemu zarządzania kryzysowego w kontekście zapewniania ciągłości działania. Zaproponowano przykładowe rozwiązania organizacyjne i techniczne, ograniczające ryzyko utraty ciągłości działania. Dokonano charakterystyki więzi informacyjnych występujących w ramach systemu oraz zdiagnozowano rolę bezpieczeństwa informacji w kontekście zdolności działania.
Słowa kluczowe: zagrożenie, zarządzanie kryzysowe, ciągłość działania.

Wstęp

Zapewnianie bezpieczeństwa to złożone zagadnienie, zarówno w sferze teoretycznej, jak i praktycznej. Wychodząc od ogólnych założeń dotyczących gwarancji przetrwania i warunków rozwoju, konieczna jest wnikliwa analiza treści bezpieczeństwa, definiowanego suwerennie przez każdy podmiot.

Działania w tej sferze, poprzedzone wnikliwą analizą ryzyka, prowadzone są równolegle w dwóch wymiarach: prewencji – będącej próbą zapobiegania zagrożeniom – oraz reakcji wymagającej kreowania zdolności niwelowania skutków zakłóceń. Niedoskonałość ludzkiego postępowania, wynikająca m.in. z ograniczonej wiedzy i informacji, wskazuje na możliwość wystąpienia stanów niebezpiecznych, wpływających negatywnie na sposób funkcjonowania oraz zdolność osiągania celów.

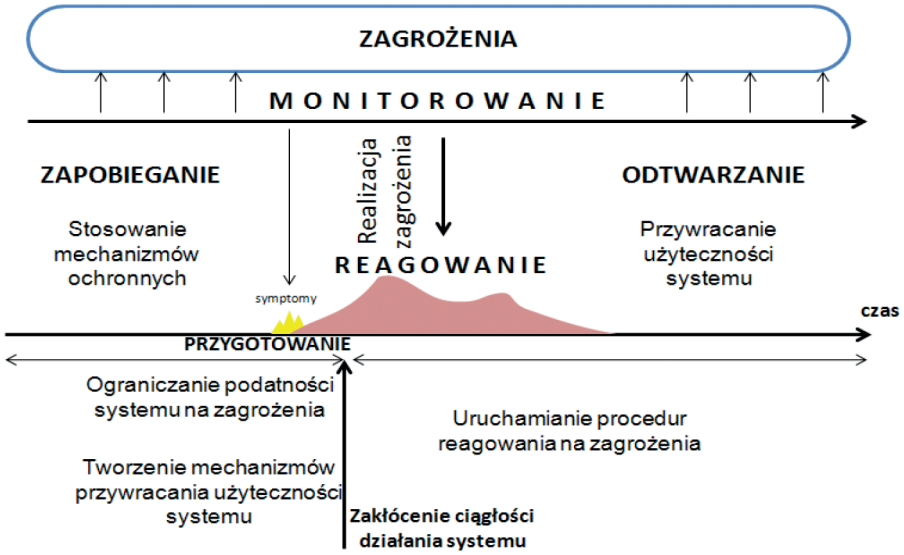
Potrzeba zapewniania ciągłości działania dotyczy zarówno organizacji, realizujących procesy w skali mikro, jak i państwa, którego zakres oddziaływania dotyczy całego społeczeństwa. Dostrzega się zatem potrzebę tworzenia dedykowanych mechanizmów na obu poziomach oraz zapewniania spójności działań w tym zakresie w oparciu o przysługujące władzy atrybuty.

Celem artykułu jest analiza systemu zarządzania kryzysowego w kontekście zapewniania ciągłości działania. W pracy odwołano się do aktów normatywnych, literatury przedmiotu, rekomendacji oraz standardów branżowych. Na podstawie przeprowadzonej kwerendy wynika, że problem ma interdyscyplinarny charakter oraz może stanowić przedmiot badań w zakresie bezpieczeństwa.

1. Uwarunkowania przeciwdziałania zagrożeniom

Zagrożenia to zjawiska, które naturalnie towarzyszą ludzkiemu życiu. Ich ignorowanie, niedostateczna wiedza i potencjał, a także zaniechania prowadzą do obniżenia wartości systemów oraz strat w otoczeniu. Dlatego ludzie powołują instytucje odpowiedzialne za zapewnianie bezpieczeństwa, których zadaniem jest ograniczanie ryzyka zagrożeń poprzez (rys. 1):

- minimalizowanie prawdopodobieństwa ich występowania;
- przejmowanie kontroli oraz ograniczanie strat – w przypadku gdy działania prewencyjne są nieskuteczne.



Rys. 1. Istota zapewniania bezpieczeństwa systemu
Źródło: opracowanie własne

Systemy posiadają określone podatności, które mogą być wykorzystywane przez zagrożenia (rys. 1). Stąd podstawowym celem działań zapobiegawczych jest identyfikacja słabości oraz stosowanie mechanizmów ochronnych. Realizacja procesów zapewniania bezpieczeństwa wymaga zaangażowania pewnych sił i środków. Potencjał zagregowany oraz wykorzystywany na te potrzeby stanowi koszt alternatywny:

- w aspekcie otoczenia systemu bezpieczeństwa, a więc podziału dochodu danego podmiotu (państwa, organizacji), np. inwestycji rozwojowych;
- w ramach samego systemu, np. dysponowanie karetkami pogotowia ratunkowego, budowa obiektów ochronnych, edukacja dla bezpieczeństwa.

Istotne znaczenie ma zatem unikanie marnotrawstwa oraz skuteczność działań związanych z zapewnianiem bezpieczeństwa. Warto przy tym wskazać na trzy

zagadnienia. Pierwszym z nich jest subiektywny charakter bezpieczeństwa, wynikający z samej definicji tego pojęcia[1]. Błędna percepcja zagrożenia może prowadzić zarówno do stanu obsesji, jak i pozornego bezpieczeństwa. Istnieje zatem potrzeba wskazania uniwersalnych kryteriów, które umożliwiają obiektywną ocenę zjawisk, potencjalnie mogących wpływać negatywnie na funkcjonowanie danego podmiotu.

Kolejnym problemem jest rosnący przedmiotowy zakres procesów zapewniania bezpieczeństwa. Transformacja systemu politycznego na przełomie lat 80. i 90. doprowadziła do znaczących zmian doktryny bezpieczeństwa w wielu państwach. Brak jasno zdefiniowanego wroga wpływa na stopniową marginalizację zagrożeń militarnych oraz akcentowanie kwestii związanych z ochroną przed skutkami katastrof i awarii, bezpieczeństwa socjalnego, ale również zagrożeń paramilitarnych, jak terroryzm[2]. Można przypuszczać, że wydarzenia w bezpośrednim otoczeniu NATO oraz dostrzegalna redukcja amerykańskiej obecności w Europie[3] wymuszają rewizję strategii bezpieczeństwa państw starego kontynentu[4].

Warto również zwrócić uwagę na podmiotowe ujęcie bezpieczeństwa. Występowanie zagrożeń negatywnie oddziałuje na ludzi, ich mienie oraz środowisko. Zagrożenia wpływają na możliwość osiągania celów przez organizacje, instytucje, przedsiębiorstwa – ustanawiające dedykowane systemy zarządzania bezpieczeństwem. Newralgiczne znaczenie dla bezpieczeństwa państwa oraz obywateli mają systemy infrastruktury krytycznej, które podlegają szczególnej ochronie. Wśród nich znajdują się systemy zapewniające ciągłość działania administracji publicznej odpowiedzialnej za zarządzanie bezpieczeństwem. Jak już wcześniej zauważono, systemy bezpieczeństwa również posiadają określone podatności, stąd istnieje ryzyko utraty użyteczności systemów oraz zasobów niezbędnych do zapobiegania oraz przejmowania kontroli nad przebiegiem zagrożeń.

Ochrona infrastruktury krytycznej to złożone przedsięwzięcie, wymagające holistycznego podejścia. Współzależność składających się na nią podsystemów jest szczególnie widoczna w sytuacjach kryzysowych, gdy awaria jednego komponentu zakłóca ciągłość działania pozostałych systemów (rys. 2), a w konsekwencji struktur odpowiedzialnych za zarządzanie bezpieczeństwem[5]. Konsekwencją utraty zdolności przejmowania kontroli nad przebiegiem takiego zjawiska są rosnące straty.

---

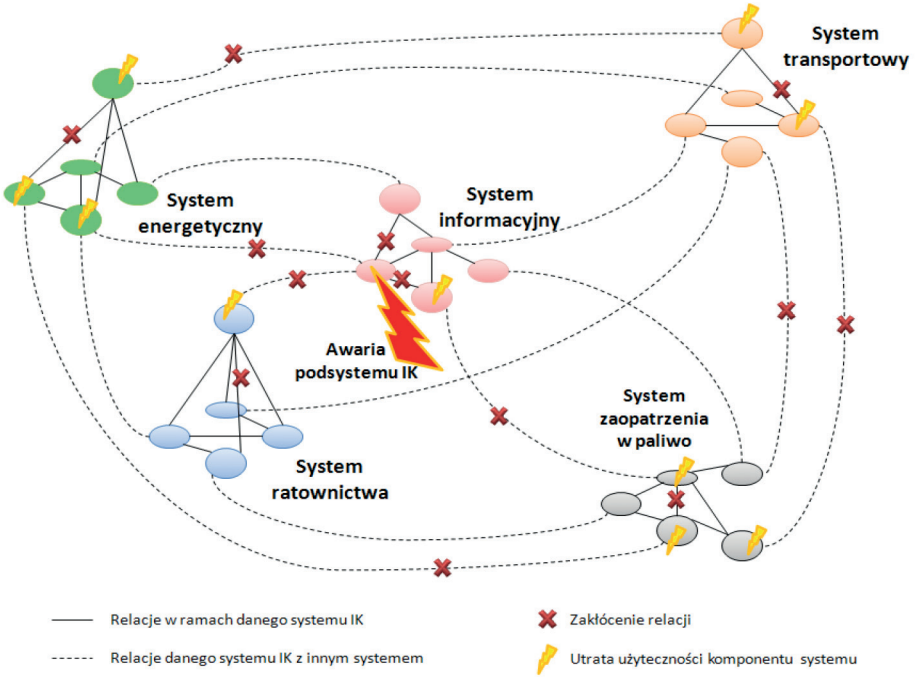
1 Zob.: J. Pawłowski (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002, s. 12; L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, European Association for Security, Kraków 2008, s. 33.

2 Np. terroryzm. Zob. T. Szczurek, *Od deskrypcji do antycypacji wykorzystania potencjału militarnego w kształtowaniu bezpieczeństwa nowoczesnych wspólnot państwowych wobec rozwoju zagrożeń niemilitarnych*, WAT, Warszawa 2012, s. 101-110.

3 *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013, s. 120-128.

4 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014.

5 P. Pederson i in., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory, Idaho 2006.



Rys. 2. Współzależności pomiędzy systemami infrastruktury krytycznej w kontekście zapewniania ogólnej sprawności systemu
Źródło: opracowanie własne

Ogólna niezawodność systemów jest pochodną niezawodności elementarnej (wszystkich elementów tworzących dany system), którą można oceniać na podstawie zagregowanych charakterystyk oraz struktury (równoległej, szeregowej, hybrydowej). W zależności od typu struktury wykorzystywane są adekwatne strategie wzmacniania ogólnej niezawodności systemu, odpowiednio poprzez:[6]

- redundancję elementów/ podsystemów:
- jako wzmocnienie aktualnej struktury, funkcjonują równolegle z istniejącymi komponentami i jako takie narażone są na zmianę stanu zdatności;
- jako rezerwa wykorzystywana do zastępowania uszkodzonych komponentów;
- ograniczanie liczby elementów lub dobór elementów o większej niezawodności.

[6] E. Pająk, *Zarządzanie produkcją: produkt, technologia, organizacja*, Wyd. Nauk. PWN, Warszawa 2007, s. 76.

A zatem niezawodność kosztuje. Celowe w kontekście racjonalizowania i określania priorytetów wydatków jest identyfikowanie elementów, których:[7]

- zmiana stanu zdatności, przy stałości stanów pozostałych elementów, powoduje zmianę stanu całego systemu – elementy krytyczne;
- stan nie ma wpływu na stan systemu – tzw. elementy pasywne.

W aspekcie procesów zapewniania bezpieczeństwa systemów działania można mówić o ryzyku decyzji wynikających z:[8]

- ograniczonego dostępu do informacji umożliwiającej właściwą ocenę stanów zagrożenia oraz chronionego systemu;
- niewłaściwej percepcji zagrożeń (wynikającej z błędów na etapie identyfikowania i analizy ryzyka);
- różnych uwarunkowań działania na etapach: planowania oraz realizacji założeń;
- ograniczonych możliwości prognozowania przyszłych zdarzeń oraz błędów prognozy.

W konsekwencji, obok środków prewencyjnych, konieczne jest przygotowywanie planów na wypadek zakłócenia stabilności systemu. Zwłaszcza funkcjonowanie w zmiennych warunkach determinuje konieczność planowania ciągłości działania systemów oraz gromadzenia potencjału niezbędnego do ich wdrażania. Jednym ze sposobów ograniczania ryzyka niepowodzenia takich przedsięwzięć jest wykorzystanie sprawdzonych wzorców, standardów i praktyk.

2. Problem zapewniania ciągłości działania systemu zarządzania kryzysowego

Możliwość powstania strat wynikających z czasowego ograniczenia użyteczności systemów determinuje zainteresowanie problematyką zapewniania ciągłości działania. Analiza współczesnych uwarunkowań biznesowych wskazuje, że zakłócenia realizacji procesów gospodarczych prowadzą do istotnych strat finansowych, wizerunkowych czy utraty kluczowych zasobów (np. informacji).

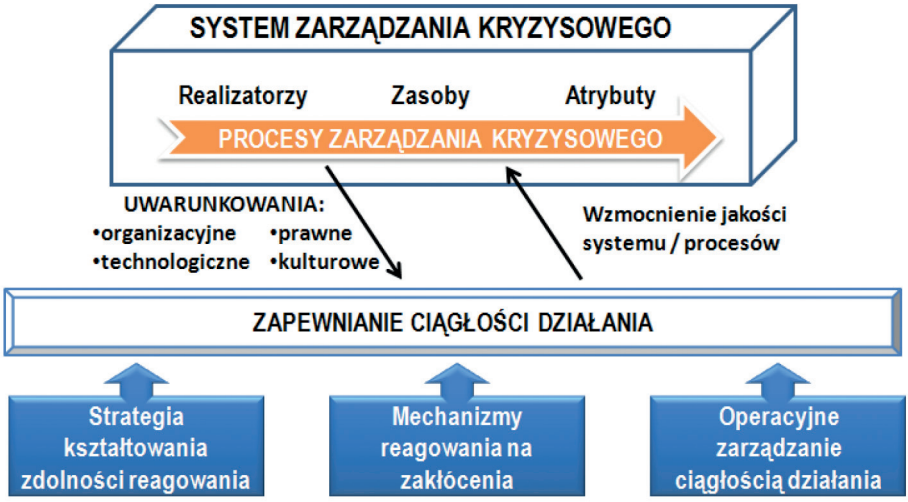
Problem ten w równej mierze dotyczy instytucji sektora publicznego realizujących zadania zarządzania kryzysowego. W tym przypadku zakłócenia realizacji procesów mogą prowadzić do:

- ograniczenia zdolności przejmowania kontroli nad przebiegiem sytuacji kryzysowej, a tym samym potencjalnie większych strat;
- powstawania niebezpiecznych stanów systemu oraz otoczenia, np. wskutek utraty kontroli nad wybranymi siłami i środkami;

[7] F. Grabski, J. Jaźwiński, *Funkcje o losowych argumentach w zagadnieniach niezawodności, bezpieczeństwa i logistyki*, WKŁ, Warszawa 2009, s. 132-145.

[8] E. Kołodziński (red. nauk.), *Wspomaganie decyzji w bezpieczeństwie*, WAT, Warszawa 2014, s. 24.

– błędnej percepcji aktualnego stanu bezpieczeństwa/ zagrożenia (w tym występowania stanu obsesji);
– osłabienia zaufania do instytucji państwa.



Rys. 3. Istota zapewniania ciągłości realizacji procesów zarządzania kryzysowego
Źródło: opracowanie własne na podstawie: J. Zawiła-Niedźwiecki, Ciągłość działania *organizacji, PW, Warszawa 2008*

W kontekście każdej organizacji można mówić o specyficznych uwarunkowaniach (rys. 3) determinujących sposób realizacji statutowych funkcji oraz możliwość reagowania na zakłócenia. Z analizy systemu zarządzania kryzysowego wynika, że:[9]

– na każdym szczeblu istnieje organ decyzyjny, który posiada wyłączne kompetencje kierowania w sytuacjach kryzysowych oraz zastępcę. Analizowana problematyka stanowi jeden z wielu obszarów kompetencji podmiotu, który realizuje swoje zadania m.in. przy pomocy wyspecjalizowanej jednostki organizacyjnej (np. wydział, departament, komórka) w ramach podmiotu, któremu przewodzi;
– merytoryczne wsparcie realizacji zadań dla decydenta stanowi kolegialny organ opiniodawczo-doradczy, skupiający przedstawicieli administracji zespolonej, wybrane podmioty administracji niezespolonej, przedstawicieli władzy samorządowej, wybranych pracowników administracji oraz zaproszonych do współpracy ekspertów. W zależności od okoliczności tryb pracy zespołu może mieć charakter cykliczny (posiedzenia zgodnie z przyjętym

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

harmonogramem) lub doraźny (w sytuacjach kryzysowych). Miejsce pracy zazwyczaj stanowi siedziba urzędu, na czele którego stoi organ decyzyjny – wskazywane są również alternatywne lokalizacje;
- tworzone są wyspecjalizowane jednostki organizacyjne[10] zapewniające bieżącą koordynację działań oraz całodobowy, sprawny przepływ informacji pomiędzy podmiotami ZK. Oprócz szczebla krajowego (RCB) oraz wojewódzkiego (urząd wojewódzki), miejscem pracy centrum może być siedziba organu decyzyjnego (np. starostwo powiatowe) lub podległa/ nadzorowana jednostka organizacyjna (np. Dowództwo Operacyjne RSZ, KP PSP);
- instytucją zapewniającą spójność działań jest Rządowe Centrum Bezpieczeństwa, które koordynuje przepływ informacji pomiędzy podmiotami oraz odpowiada m.in. za nadzór nad realizacją zadań związanych z ochroną infrastruktury krytycznej;
- jest to integralny element systemu bezpieczeństwa narodowego, zapewniający sprawne wykorzystanie jednostek interwencyjno-ratowniczych do reagowania w sytuacjach wykraczających poza rutynową działalność służb, straży i inspekcji;
- na właścicielach i posiadaczach systemów IK spoczywa obowiązek tworzenia mechanizmów zapobiegania i reagowania na zakłócenia (w tym planów zapewniania ciągłości funkcjonowania oraz odtwarzania IK[11]), odtwarzanie tych systemów w przypadku zniszczenia i utrzymywanie alternatywnych rozwiązań do podtrzymania funkcjonowania infrastruktury, do czasu odtworzenia[12]. Istnieją branżowe standardy w tym zakresie.

Realizacja procesów zarządzania kryzysowego wymaga wykorzystania określonego potencjału:
- ludzkiego, w ramach podsystemu kierowania i wykonawczego;
- techniczno-technologicznego, na który składają się obiekty budowlane[13], urządzenia oraz systemy wykorzystywane do ich obsługi/ sterowania;

[10] Na szczeblu gminnym (miasta) tworzenie centrum zarządzania kryzysowego ma charakter fakultatywny. Stąd jedynie w sytuacjach kryzysowych zapewnia się tutaj pełnienie całodobowego dyżuru na potrzeby skutecznego przepływu informacji. Realizację pozostałych standardowych zadań takiego podmiotu zapewnia organ decyzyjny.

[11] § 2 ust. 3 rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz.U. z 2010 r. Nr 83, poz. 543.

[12] Art. 6 ust. 5 ustawy o zarządzaniu kryzysowym, op. cit.

[13] W rozumieniu ustawy z dnia 7 lipca 1994 r., prawo budowlane, Dz.U. 1994, Nr 89, poz. 414 ze zm. W załączniku do ustawy wyróżniono 30 kategorii obiektów budowlanych, w tym: budynki administracji publicznej, obiekty budowlane SZ (12), służby zdrowia, opieki społecznej i socjalnej (11), sieci (np. elektroenergetyczne, telekomunikacyjne) (26), budowle hydrotechniczne (27).

- informacyjnego, obejmującego dane i informacje o charakterze operacyjnym i analitycznym – gromadzone, przetwarzane i udostępniane zgodnie z istniejącymi standardami;
- finansowego, który stanowią środki własne oraz dotacje celowe.

Dostępność elementów w ramach wskazanych zbiorów w różnym stopniu determinuje zdolność realizacji procesów. Dlatego dokonując analizy wpływu zmian wartości atrybutów tych elementów na zdolność realizacji procesów zarządzania kryzysowego, można wskazać elementy krytyczne, a także określić strategię postępowania z ryzykiem utraty ciągłości działania poprzez:[14]

- tolerowanie zakłóceń, których występowanie jest rzadkie, a potencjalne konsekwencje znikome. Pomimo małej istotności instytucja powinna kształtować zasady postępowania z takimi zakłóceniami, np. poprzez zawarcie odpowiednich adnotacji w podpisywanych umowach;
- unikanie poprzez świadomą rezygnację z zasobów/usług/funkcji, interpretowanych jako potencjalne źródło ryzyka, których eliminacja nie ogranicza zdolności realizacji celów;
- zapobieganie poprzez stosowanie zabezpieczeń (ograniczających prawdopodobieństwo wystąpienia) i oddziaływanie na podatności. Strategia preferowana dla zakłóceń o wysokim prawdopodobieństwie wystąpienia oraz potencjalnie wysokich (destrukcyjnych) konsekwencjach wystąpienia;
- redukowanie strat poprzez tworzenie, aktualizowanie planów odtwarzania ciągłości działania oraz zapewnianie środków do ich implementacji;
- transfer ryzyka zakłócenia na podmioty, które ze względu na posiadane kompetencje i potencjał mogą uczestniczyć w przeciwdziałaniu zakłóceniom/ reagowaniu na nie.

Istotne jest monitorowanie ryzyka zakłóceń, tak aby przyjęta strategia przystawała do rzeczywistego poziomu zagrożenia. Wybór strategii postępowania determinowany jest w znacznej mierze ograniczeniami budżetowymi. Rozwiązania mogą mieć charakter organizacyjny (np. delegowanie uprawnień, nadawanie dodatkowych kompetencji), prawny (zawieranie formalnych umów, porozumień) oraz techniczny (fizyczny lub programowy, np. dublowanie wybranych elementów, systemy replikacji danych). Na podstawie analizy planów zarządzania kryzysowego można dostrzec pewne działania związane z ograniczaniem ryzyka utraty ciągłości działania we wszystkich wspomnianych obszarach (rys. 4).

[14] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008, s. 102-114.

Rys. 4. Wybrane działania ukierunkowane na ograniczanie ryzyka zakłóceń
Źródło: opracowanie własne na podstawie analizy planów zarządzania kryzysowego

Zdolność reagowania na zakłócenia wymaga ustanawiania i doskonalenia odpowiednich mechanizmów (rys. 3), na które składają się:[15]

- formalna struktura – na podstawie której określane są role, zakres kompetencji (w tym prawo dysponowania zasobami) podmiotów odpowiedzialnych za zapewnianie ciągłości działania, będącej uzupełnieniem ogólnej struktury organizacyjnej systemu;
- regulacje określające relacje pomiędzy elementami struktury;
- procedury oraz dobre praktyki określające sposób postępowania w przypadku wystąpienia zakłócenia.

Jako zasadne należy zatem uznać próby odpowiedzi na pytania:

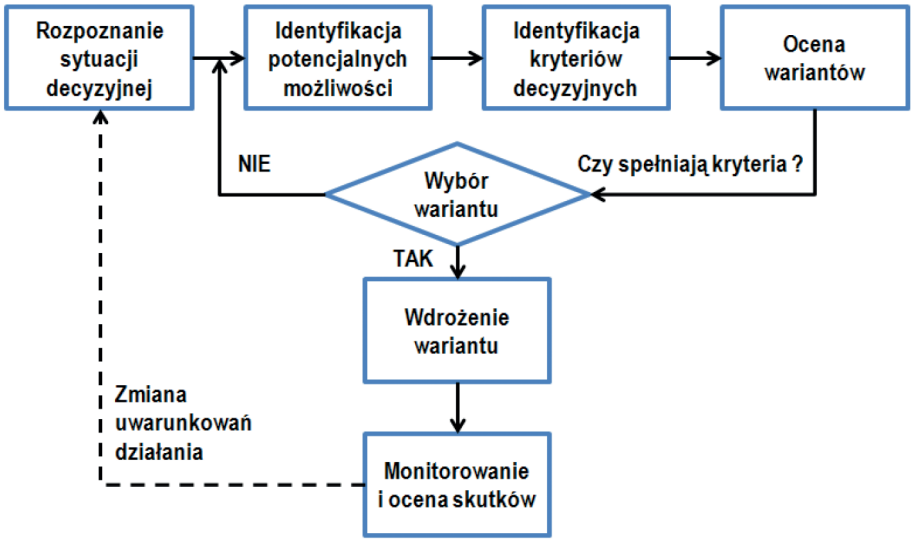
- kto powinien odpowiadać za tworzenie mechanizmów zapewniania ciągłości działania systemu zarządzania kryzysowego?
- jak zapewnić spójność tworzonego rozwiązania ze stanem zastanym, w tym regulacjami prawnymi oraz standardami branżowymi?

Warto zauważyć, że tworzenie zdolności reagowania na zakłócenia to istotny element zapewniania bezpieczeństwa podmiotu, którego wartość jest szczególnie dostrzegana, gdy stosowane zabezpieczenia okazują się nieskuteczne.

[15] J. Zawiła-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania*, Wyd. edu-Libri, Warszawa 2013, s. 56.

3. Informacja jako zasób determinujący ciągłość zarządzania kryzysowego

Ograniczenie marnotrawstwa oraz zapewnienie skutecznej realizacji zakładanych celów wskazuje na potrzebę zarządzania procesami zapewniania bezpieczeństwa. Realizacja klasycznych funkcji (planowania, organizowania, przewodzenia i kontroli) wymaga podejmowania zarówno rutynowych, jak i niestandardowych decyzji (rys. 5). Dlatego jak zauważają P. Sienkiewicz i P. Górny, zarządzanie kryzysowe można utożsamiać z procesem decyzyjnym, którego celem ma być wybór strategii przeciwdziałania realnym i potencjalnym sytuacjom kryzysowym, a także wykorzystania dostępnych zasobów, co umożliwi utrzymanie/przywrócenie stabilnego stanu systemu[16].



Rys. 5. Etapy procesu decyzyjnego
Źródło: opracowanie własne na podstawie: R.W. Griffin,
Podstawy zarządzania organizacjami, PWN, Warszawa 2009, s. 288-293

Jak widać (rys. 5), podstawowym zasobem przetwarzanym w procesach decyzyjnych są informacje. Dlatego istotnym elementem zarządzania bezpieczeństwem jest podsystem informacyjny zapewniający gromadzenie, przechowywanie, przetwarzanie, transfer oraz udostępnianie informacji uprawnionym podmiotom. Wartość tych zasobów jest szczególnie dostrzegana w nadzwyczajnych warunkach,

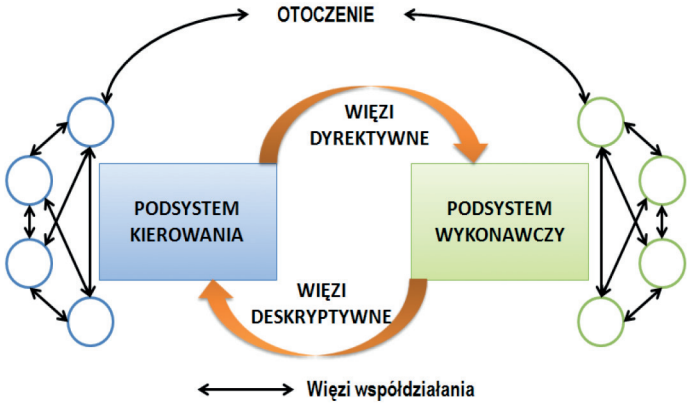
[16] P. Sienkiewicz, P. Górny, *Analiza systemowa sytuacji kryzysowych*, „Zeszyty Naukowe AON", Nr 4 (45), Warszawa 2001, s. 32.

które cechuje presja czasu, skrócenie cyklu decyzyjnego, duża dynamika zmian środowiska działania, niepewność, niewystarczające środki do realizacji celów. Jak zauważa T. Waściński, źródłem wartości informacji jest jej użyteczność w kontekście podejmowanych decyzji[17].

Immanentną cechą zarządzania kryzysowego jest potrzeba gromadzenia i przetwarzania dużej ilości danych. Obecny stan techniki, ilość, a także wymagania jakościowe uzasadniają wykorzystanie teleinformatycznej infrastruktury jako środowiska realizacji procesów informacyjnych.

Informację można traktować jako istotny wkład do procesów decyzyjnych oraz ich rezultat (efekt). W ten sposób można wskazać na występujące w organizacji więzi informacyjne o charakterze (rys. 6):[18]

- pionowym, które odzwierciedlają relacje służbowe i zapewniają zasilanie podmiotów decyzyjnych w informację operacyjną (deskryptywne) oraz przekazywanie decyzji/ rozkazów dla podmiotów wykonawczych (dyrektywne);
- poziomym, zapewniające współdziałanie podmiotów w ramach systemu (np. w ramach wspólnej specjalności), w tym pomiędzy różnymi szczeblami, z pominięciem więzi służbowych oraz otoczenia.



Rys. 6. Więzi informacyjne w systemie zarządzania kryzysowego
Źródło: *opracowanie własne na podstawie:* J. W. Michniak, *Dowodzenie w operacjach antykryzysowych i połączonych*, AON, Warszawa 2003, s. 53-59

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

[18] G. Sobolewski, J. Stępień, K. Żwirek, *Model zarządzania przepływem informacji w sytuacjach kryzysowych: praca naukowo-badawcza*, AON, Warszawa 2013, s. 42-46.

Można zatem zauważyć (rys. 6), że zakłócenia procesów informacyjnych determinują ryzyko utraty ciągłości działania systemu[19]. Zagrożeniami warunkującymi powstanie takich stanów są:[20]

- oddziaływanie siły wyższej, w tym klęski żywiołowe, luki powstałe w wyniku zmian w systemie prawnym;
- niezamierzone działanie użytkownika systemu;
- celowa działalność użytkowników lub podmiotów z otoczenia systemu;
- awarie lub absencja elementów systemu informacyjnego;
- błędy na etapie projektowania systemów informacyjnych oraz zabezpieczeń tych systemów.

O bezpieczeństwie zasobów informacyjnych decyduje zwłaszcza spełnienie kryteriów poufności, integralności oraz dostępności, a także autentyczności, rozliczalności, niezawodności i niezaprzeczalności[21]. A zatem przyczyną zakłócenia procesów zarządzania kryzysowego może być zarówno brak informacji, jak i dostęp do zasobu niespełniającego wymagań jakościowych. Zgodnie z zaleceniami normy ISO/IEC 27002 zapewnianie ciągłości informacyjnej powinno być integralnym elementem systemu zarządzania ciągłością działania w organizacji[22]. Dlatego odwołania do problematyki zapewniania informacyjnej ciągłości można dostrzec w kontekście innych systemów infrastruktury krytycznej, a zwłaszcza w sektorze bankowym[23]. Do podobnych wniosków prowadzi analiza *Białej Księgi Bezpieczeństwa Narodowego RP*, gdzie dostrzega się transsektorowy charakter bezpieczeństwa informacyjnego[24].

[19] P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe WWSI", Rok 7 Nr 9, Warszawa 2013, s. 49-50.

[20] K. Liderman, op. cit., s. 42.

[21] ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, Switzerland 2014.

[22] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*, Switzerland 2013, pt. 17.

[23] Zgodnie z Rekomendacją M wydaną przez Komisję Nadzoru Finansowego banki powinny tworzyć i aktualizować plany zarządzania ciągłością działania oraz plany awaryjne, zapewniające utrzymanie podstawowych funkcji tych podmiotów, w których należy uwzględniać ryzyko wynikające m.in. z awarii lub zniszczenia infrastruktury teleinformatycznej. Zob. *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*, KNF, Warszawa 2012, rekomendacja 11.

[24] *Biała Księga…*, op. cit., s. 248.

Tabela 1. Wybrane metody ograniczania skutków zakłóceń

OGRANICZENIE SKUTKÓW ZAKŁÓCEŃ	
ORGANIZACYJNE	**TECHNICZNE**
• tworzenie planów zapewniania ciągłości działania/ planów awaryjnych • decentralizacja uprawnień decyzyjnych (ograniczanie asymetrii informacyjnej) • definiowanie ról i kompetencji • uwzględnianie stosownych zapisów w podpisywanych umowach • wyznaczanie alternatywnych lokalizacji i ich wyposażanie • dublowanie wybranych usług informacyjnych (np. outsourcing) • szkolenia pracowników dotyczące sposobu postępowania w przypadku zakłócenia	• tworzenie kopii zapasowych na nośnikach fizycznych • utrzymanie i konserwacja elementów infrastruktury teleinformatycznej (w tym zapasowych i alternatywnych) • montowanie urządzeń szybkiego reagowania na incydenty (zraszacze, pompy, systemy zasilania awaryjnego) • nadmiarowe gromadzenie wybranych elementów infrastruktury • systemy przywracania danych oraz ich konfiguracja • replikacja baz danych

Źródło: opracowanie własne

Podejmowane są zatem różne przedsięwzięcia natury organizacyjnej i technicznej ukierunkowane na ograniczenie strat powstałych w wyniku zakłócenia informacyjnej ciągłości działania (tabela 1). Specyfika systemu zarządzania kryzysowego sprzyja implementacji wybranych rozwiązań bazujących na wykorzystaniu potencjału podmiotów wykonawczych, np. PSP czy Policji[25]. Ciekawym rozwiązaniem może być dublowanie wybranych usług informacyjnych w oparciu o własne[26] lub dzierżawione (outsourcing) ośrodki obliczeniowe, np. w ramach „chmury obliczeniowej"[27].

ZAKOŃCZENIE

Zapewnianie bezpieczeństwa to złożony proces, realizowany w zmiennych warunkach. Jak zauważa F. Bastiat, laika od specjalisty odróżnia to, że ten drugi

[25] J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego. Część 1. Zarządzanie kryzysowe w administracji publicznej*, Krakowska Akademia im. A.F. Modrzejewskiego, Kraków 2010, s. 113-114.

[26] Np. w formie prywatnej chmury obliczeniowej resortu spraw wewnętrznych, administracji i cyfryzacji lub podmiotu międzyresortowego (RCB). W zależności od usytuowania, rozwiązanie takie mogłoby wzmacniać ogólną niezawodność administracji publicznej w realizacji usług informacyjnych.

[27] K. Szwarc, P. Zaskórski, *„Chmura" obliczeniowa jako usługa ograniczająca ryzyko utraty ciągłości działania*, [w:] M. Żuber (red. nauk.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i ochrona infrastruktury krytycznej*, Wrocław 2013, s. 208-211.

potrafi analizować zarówno bezpośrednie, jak i odległe, trudno dostrzegalne skutki[28]. Dlatego obok prewencji tworzone są zdolności przywracania ciągłości działania systemów, traktowane jako zabezpieczenie, implikowane ryzykiem nieskuteczności mechanizmów ochronnych.

W artykule dokonano analizy uwarunkowań zapewniania ciągłości działania systemu zarządzania kryzysowego. Dążąc do ograniczania zjawiska suboptymalizacji, można jednak przyjąć, że proponowane w tym zakresie rozwiązania organizacyjne i techniczne mogą przyczyniać się do usprawnienia całego systemu bezpieczeństwa narodowego – lub szerzej, administracji państwowej realizującej swoje zadania z wykorzystaniem systemów infrastruktury krytycznej.

Szczególną uwagę poświęcono analizie informacji, jako zasobu warunkującego ciągłość realizacji procesów zarządzania kryzysowego. W organizacjach XXI wieku szereg procesów realizowanych jest z wykorzystaniem technologii teleinformatycznej. Należy zatem dostrzegać transsektorowy charakter bezpieczeństwa informacyjnego oraz jego wpływ na możliwość przetrwania i rozwoju jednostki, społeczeństwa i organizacji.

LITERATURA:

1. F. Bastiat, *Co widać i czego nie widać*, Fijorr Publishing, Warszawa 2005.
2. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013.
3. F. Grabski, J. Jaźwiński, *Funkcje o losowych argumentach w zagadnieniach niezawodności, bezpieczeństwa i logistyki*, WKŁ, Warszawa 2009.
4. R.W. Griffin, *Podstawy zarządzania organizacjami*, PWN, Warszawa 2009.
5. ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, Switzerland 2014.
6. ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*, Switzerland 2013.
7. E. Kołodziński (red. nauk.), *Wspomaganie decyzji w bezpieczeństwie*, WAT, Warszawa 2014.
8. L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, European Association for Security, Kraków 2008.
9. K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.
10. J.W. Michniak, *Dowodzenie w operacjach antykryzysowych i połączonych*, AON, Warszawa 2003.
11. E. Pająk, *Zarządzanie produkcją: produkt, technologia, organizacja*, Wyd. Nauk. PWN, Warszawa 2007.

[28] F. Bastiat, *Co widać i czego nie widać*, Fijorr Publishing, Warszawa 2005.

12. J. Pawłowski (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002.
13. P. Pederson i in., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory, Idaho 2006.
14. *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*, KNF, Warszawa 2012.
15. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w *sprawie planów ochrony infrastruktury krytycznej*, Dz.U. z 2010 r. Nr 83, poz. 543.
16. P. Sienkiewicz, P. Górny, *Analiza systemowa sytuacji kryzysowych*, „Zeszyty Naukowe AON", Nr 4 (45), Warszawa 2001.
17. G. sobolewski, J. Stępień, K. Żwirek, *Model zarządzania przepływem informacji w sytuacjach kryzysowych*, Praca naukowo-badawcza, AON, Warszawa 2013.
18. T. Szczurek, *Od deskrypcji do antycypacji wykorzystania potencjału militarnego w kształtowaniu bezpieczeństwa nowoczesnych wspólnot państwowych wobec rozwoju zagrożeń niemilitarnych*, WAT, Warszawa 2012.
19. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. Nr 89, poz. 590, ze zm.
20. Ustawa z dnia 7 lipca 1994 r. prawo budowlane, Dz.U. 1994, Nr 89, poz. 414 ze zm.
21. T. Waściński, *Finansowa diagnoza procesów restrukturyzacji przedsiębiorstwa w aspektach ekonomicznej wartości wiedzy*, Dom Wydawniczy Elipsa, Warszawa 2010.
22. P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe WWSI", Rok 7, Nr 9, Warszawa 2013.
23. J. Zawiła-Niedźwiecki, *Ciągłość działania organizacji*, PW, Warszawa 2008.
24. J. Zawiła-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania*, Wyd. edu-Libri, Warszawa 2013.
25. J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego. Część 1. Zarządzanie kryzysowe w administracji publicznej*, Krakowska Akademia im. A.F. Modrzejewskiego, Kraków 2010.
26. M. Żuber (red. nauk.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i ochrona infrastruktury krytycznej*, Wrocław 2013.

CONDITIONS FOR CRISIS MANAGEMENT SYSTEM CONTINUITY

Abstract: The author of article presents an overview of issues pertaining to the conditions of threat counteracting. The subject of analysis is a crisis management system as a field of continuity ensurance. Based on this, the proposition on some organizational and technical solutions is given, that may reduce continuity disruptions risk. Whole article has been summarized by a debate of information security impact on crisis management process continuity.
Keywords: threat, crisis management, continuity of functioning.