BEZPIECZEŃSTWO STRUKTUR ROZPROSZONYCH W SYTUACJACH KRYZYSOWYCH[1]

Jacek WOŹNIAK, Piotr ZASKÓRSKI

Wojskowa Akademia Techniczna

Streszczenie. Wiele organizacji funkcjonujących we współczesnym świecie ma charakter rozproszony. Struktury rozproszone mogą sprawnie funkcjonować dzięki technologiom informatycznym. W artykule eksponowany jest problem bezpieczeństwa struktur rozproszonych ze szczególnym uwzględnieniem bezpieczeństwa informacyjnego w sytuacjach kryzysowych. Identyfikowany jest przede wszystkim problem zapewniania i utrzymywania oczekiwanego poziomu bezpieczeństwa informacyjnego, głównie w aspekcie ciągłości działania ze szczególnym uwzględnieniem maksymalizacji użyteczności oraz wartości poszczególnych jednostek powiązanych odpowiednimi relacjami w warunkach kryzysowych. Oznacza to potrzebę dynamicznego dostosowywania struktur do zadań realizowanych w środowisku silnych ograniczeń czasowych i zasobowych. Ważną rolę można tu przypisać koncepcji X-engineeringu, która może być swoistą strategią zarządzania bezpieczeństwem organizacji rozproszonej przestrzennie i informacyjnie z uwzględnieniem technologii ICT[2]. Koncepcja ta bazuje na triadzie: proces, propozycja, partycypacja. Procesy uzyskują więc status obiektów organizacyjnych i możliwy jest wówczas dynamiczny dobór ich realizatorów. Może nastąpić zatem decentralizacja funkcji decyzyjnych stosownie do kompetencji podmiotów realizujących w rozproszeniu terytorialnym wspólne procesy. Elastyczność zmiany struktur wykonawczych w zależności od zadań i dostępności zasobów może być zapewniona przez tzw. struktury typu H-H, które uwzględniają stany dyspersji, tj. decentralizacji funkcji decyzyjnych w warunkach braku zagrożeń oraz centralizacji funkcji decyzyjnych w sytuacji kryzysowej (zagrożeń). Narzędzia informatyczne różnych klas zapewniają skuteczną realizację procesów roboczych i decyzyjnych.

Wstęp

Bezpieczeństwo należy traktować jako jeden z podstawowych atrybutów funkcjonowania każdej organizacji. Trudno bowiem rozpatrywać problem efektywnego i skutecznego oraz ciągłego działania bez uwzględniania (a tym samym zapewniania i utrzymywania) pożądanego stanu systemu organizacyjnego (również struktury rozproszonej[3] przestrzennie i informacyjnie) i jego bezpieczeństwa *sensu largo*. Ponadto bezpieczeństwo organizacji może być rozpatrywane na różnych płaszczyznach, zarówno w odniesieniu do jednostek gospodarczych, jak i administracyjnych

[1] Artykuł finansowany jest ze środków publicznych i stanowi wynik pracy badawczej nr RMN 705/2012 realizowanej na Wydziale Cybernetyki Wojskowej Akademii Technicznej w Warszawie pt. *Modelowanie procesów bezpieczeństwa*.

[2] Ang. *Information and Communication Technology*.

[3] W artykule pojęcia *struktury/organizacji sieciowej*, *struktury/organizacji rozproszonej* i *sieci zależności* traktowane są jako tożsame i stosowane zamiennie.

(publicznych). Nie można bowiem abstrahować od faktu, że określone struktury w sektorze publicznym również powinny ogniskować swoją uwagę na zapewnianiu wielowymiarowego bezpieczeństwa. Jest to o tyle istotne, że struktury te zorientowane są na zapewnianie bezpieczeństwa publicznego (często całego społeczeństwa), a sprawność działania tych struktur warunkowana jest ich bezpieczeństwem wewnętrznym. Dobrym przykładem może być reagowanie różnych typów jednostek w sytuacjach zaistnienia określonych klas zagrożeń (klęsk żywiołowych, katastrof, zagrożeń militarnych itp.), kiedy to poziom bezpieczeństwa wewnętrznego decyduje o sprawności, wiarygodności i terminowości przepływów informacyjnych. Często te przepływy mają znaczenie krytyczne dla procesów decyzyjnych. Dotyczyć to może zasobów ludzkich, finansowych, maszyn, energii elektrycznej, wody itp. Bezpieczeństwo wewnętrzne warunkuje więc poprawność wyznaczania, a także osiągania celów operacyjnych, taktycznych i strategicznych, czy też prognozowania zmian w otoczeniu oraz kontroli podejmowanych działań.

Można przyjąć, że jednym z podstawowych wymiarów bezpieczeństwa struktur rozproszonych funkcjonujących w sytuacjach kryzysowych jest bezpieczeństwo informacyjne. Ten rodzaj bezpieczeństwa jest ważną przesłanką do integracji informacyjnej całego systemu działania w pełnym cyklu zarządzania kryzysowego (zapobiegania, przygotowania, reagowania i odbudowy). Jest to swoista klasa metabezpieczeństwa obejmująca także integrację poszczególnych elementów infrastruktury krytycznej, którą – bez właściwego metodycznie ujęcia procesów informacyjno-decyzyjnych – nie można poprawnie zarządzać w sytuacjach kryzysowych.

I. ISTOTA ORGANIZACJI ROZPROSZONYCH

1. Organizacja jako system działania

Każda struktura organizacyjna jest złożonym systemem działania. Problem zapewniania jej bezpieczeństwa – zwłaszcza w wymiarze informacyjnym – powinien być więc rozwiązywany poprzez holistyczne spojrzenie na uwarunkowania. W ewaluacji i walidacji poziomu bezpieczeństwa w organizacjach rozproszonych należy dostrzegać zarówno układ sterujący/nadrzędny, jak i sterowany/podrzędny [4]. Sytuacja ta jest szczególnie istotna w układach sieciowych (jest to widoczne zwłaszcza w strukturach sieciocentrycznych) i wirtualnych [1, 5, 13, 14], jak również w konfiguracjach procesowych [21] i heterarchicznych [9, 12]. Mając bowiem na uwadze procesy zapewniania i utrzymywania stanu bezpieczeństwa organizacji w wymiarze informacyjnym, należy identyfikować jednostki (płaszczyzny zarządzania, stanowiska, komórki organizacyjne, fraktale itp.), które pełnią rolę nadrzędną (pomimo przyjętej zasady „równości" jednostek konstytuujących rozproszoną sieć), gdyż właśnie te jednostki determinują zaistnienie czynników bezpieczeństwa danej organizacji albo wzmacniają poziom bezpieczeństwa całej struktury (organizacji),

mogą go też obniżać [19]. Warto tu zauważyć, że nie każda jednostka współdziałająca (kooperant, dostawca usług, podwykonawca itp.) w równym stopniu jest istotna z punktu widzenia utrzymania ciągłości procesów głównych (o znaczeniu krytycznym) i pomocniczych lub też nie każdy pracownik danej organizacji jest w stanie w takim samym stopniu wpłynąć na wynik realizacji działań/procesów (głównie za sprawą posiadanej wiedzy ukrytej[4]). Dla organizacji rozproszonych można założyć równość szans wszystkich tworzących ją jednostek, która jest jednak determinowana potencjałem każdego elementu tej struktury w aspekcie realizacji celów całego systemu oraz celów własnych jednostek składowych. Wartość wspomnianego potencjału stymulowana jest także warunkami otoczenia, na które organizacja nie ma wpływu (np. naturą i skalą zaistniałej sytuacji kryzysowej).

Ujęcie cybernetyczne i teoria systemów stanowić mogą punkt wyjścia do identyfikacji i zrozumienia przepływów różnego typu zasobów oraz zależności psychospołecznych pomiędzy elementami struktur rozproszonych. W takiej sytuacji uwidacznia się bowiem swoista rozbieżność pomiędzy działaniami prowadzącymi do realizacji celów poszczególnych kooperantów/uczestników sieci a poziomem bezpieczeństwa całej organizacji/struktury, który *de facto* jest wektorem różnorodnych cech, nierzadko należących do rozłącznych zbiorów czynników (podejście to nabiera szczególnego znaczenia w przypadku kształtowania polityki bezpieczeństwa informacyjnego).

Ujęcie systemowe bezpieczeństwa organizacji rozproszonych w sytuacji kryzysowej wymaga precyzyjnej analizy przepływów czynników/zasobów podlegających transformacji w systemie organizacyjnym [3, 17]. Jednym z ważnych czynników określających wejście systemu jest informacja, która pod wpływem realizacji procesów (np. planowania działań prewencyjnych, reagowania w sytuacji wystąpienia określonego zagrożenia, usuwania skutków zagrożeń itp.) ulega zmianie (pozytywnej lub negatywnej) i staje się elementem wyjścia systemu. Uzyskana w ten sposób wiedza może stanowić dobrą informacją wejściową dla innego systemu organizacyjnego (i/lub kolejnej iteracji danego procesu) [17]. Można zatem przyjąć, iż transformacja informacji stanowi odzwierciedlenie istoty łańcucha wartości, gdyż wraz ze wzrostem stopnia zaawansowania prac w strukturze sieciowej, czyli maksymalizacji funkcji celu całego układu sieciowego, zachodzą procesy iteracyjnego przyrostu wiedzy w systemie (m.in. za pomocą mechanizmów tzw. „klienta" wewnętrznego[5]). Często

[4] Jest to wiedza posiadana tylko i wyłącznie przez konkretną osobę (pracownika organizacji, urzędnika, funkcjonariusza itp.), która jest pochodną jego doświadczeń, potencjału intelektualnego, wiedzy jawnej (tj. wiedzy rozpowszechnianej w organizacji, w której funkcjonuje) itp.

[5] Klientem wewnętrznym jest każda jednostka w danej strukturze (dział, komórka organizacyjna, a nawet pojedynczy pracownik), która jest uczestnikiem relacji wymiany (tj. przepływu środków pracy/zasobów) pomiędzy swoim poprzednikiem i następnikiem w procesie. Klient wewnętrzny odpowiada za kontrolę jakości w systemie, a tym samym także za kształtowanie i realizację polityki bezpieczeństwa informacyjnego w strukturze rozproszonej – m.in. identyfikując tzw. potrzeby informacyjne i określając poziom otrzymywanych z otoczenia i/lub od innych jednostek w strukturze

jednak w strukturze sieciowej można zaobserwować występowanie zjawiska wymuszonej (sterowanej) asymetrii informacyjnej [16] oraz dużą złożoność procesów decyzyjnych, co dodatkowo implikuje trudności (ale nie zawsze) w ocenie potencjału informacyjnego w poszczególnych iteracjach procesów w systemie działania.

Analiza systemowa daje podstawy do oceny bezpieczeństwa i sprawności procesów decyzyjnych związanych z generowaniem wiedzy przez pryzmat różnych kryteriów systemowych, takich jak np. efektywność, użyteczność, gotowość, jakość, ryzyko, spójność, kompleksowość itp. [18]. Jednym z kryteriów nierozerwalnie związanych z ryzykiem jest tutaj bezpieczeństwo warunkowane poziomem innych cech systemowych. System działania ma bowiem to do siebie, że nie deprecjonuje znaczenia nawet słabo zauważalnych zmiennych, a ponadto często dąży do łączenia faktów i zależności przyczynowo-skutkowych, rozpatrując fragment systemu (struktury rozproszonej/sieciowej) przez pryzmat całego układu [3, 11]. Tego typu mechanizmy (mające swoje bezpośrednie lub pośrednie odzwierciedlenie m.in. w identyfikacji wzorców działań i kontroli procesów decyzyjnych, wielostronnej weryfikacji informacji *ex post* itp.) mogą być podstawą do względnie precyzyjnej i wiarygodnej oceny zasobów informacyjnych w systemie, chociaż jest to proces złożony i wymaga dość znacznych nakładów. Mimo to nie powinien być pomijany lub deprecjonowany w zarządzaniu bezpieczeństwem struktur rozproszonych.

2. Decentralizacja działań w sytuacjach kryzysowych w aspekcie funkcji użyteczności

Zarządzanie bezpieczeństwem całej organizacji, w tym bezpieczeństwem informacyjnym, nie powinno być utożsamiane wyłącznie ze strukturami hierarchicznymi. Często bowiem w sytuacjach kryzysowych odwołujemy się do silnej hierarchii wyznaczanej kompetencjami i odpowiedzialnością. Tego typu podejście do realizacji procesów decyzyjnych *ex definitione* zwiększa zapewne skuteczność działań np. w zakresie egzekwowania procedur działania w stanach zagrożenia, co może mieć swoje odzwierciedlenie m.in. w usprawnianiu i udrożnianiu kanałów informacyjnych lub w skracaniu czasu realizacji poszczególnych czynności, zwłaszcza tych o krytycznym znaczeniu dla maksymalizacji użyteczności[6] danej struktury. W tym miejscu zaznaczyć należy, iż funkcja użyteczności może przyjmować różną postać[7]. Uniwersalizm tej kategorii prakseologicznej i po części aksjologicznej znajduje z powodzeniem

sieciowej danych operacyjnych/transakcyjnych lub danych analitycznych (m.in. w postaci raportów i statystyk) itp.

[6] Pod pojęciem funkcji użyteczności rozumieć należy w tym przypadku określoną kombinację pożądanych i możliwych do osiągnięcia przez daną jednostkę korzyści.

[7] Nie musi być definiowana wyłącznie jako funkcja zysku netto przedsiębiorstwa.

interpretację również w zarządzaniu bezpieczeństwem narodowym *sensu largo*, np. w zakresie przeciwdziałania skutkom klęsk żywiołowych, katastrof itp.

Struktury sieciowe nie deprecjonują walorów struktur hierarchicznych, ponieważ w strukturze sieciowej można odwzorować również silną hierarchię, ale hierarchia ta ma często znaczenie chwilowe, związane ze stanem realizacji określonych zadań/procesów. W zarządzaniu bezpieczeństwem narodowym dostrzega się obecność struktur sieciowych m.in. na poziomach krajowym (np. Rządowy Zespół Zarządzania Kryzysowego) i gminnym (np. Gminny Zespół Zarządzania Kryzysowego) itp. Problemem zasadniczym jest zwykle możliwość (nawet zasadność) kształtowania zależności pomiędzy poszczególnymi jednostkami w sieci na płaszczyźnie informacyjno-decyzyjnej i egzekwowanie zasady dynamicznego powoływania jednostki koordynującej, stosownie do miejsca realizacji wybranych zadań, ale z użyciem sił i środków będących w dyspozycji różnych jednostek rozproszonych. W tym przypadku szczególnego znaczenia nabiera proces delegowania uprawnień, tj. *empowermentu*, a także określania zakresów odpowiedzialności. W obszarze zarządzania w sytuacjach kryzysowych w ujęciu bezpieczeństwa narodowego ma miejsce zwykle sytuacja, że można odwołać się do konkretnych procedur działania wspartych podstawą prawną, specyfikującą zakres i naturę współpracy pomiędzy jednostkami w strukturze sieciowej (w przypadku organizacji biznesowych brakuje takich regulacji prawnych). Ponadto struktury publiczne (uogólniając[8] – właściwe zarządzaniu bezpieczeństwem narodowym *sensu largo*) w odróżnieniu od rozproszonych/sieciowych struktur biznesowych mogą być lepiej określone, co często eliminuje możliwość zaistnienia sprzeczności w samych celach (użyteczności) działania poszczególnych partycypantów/współdziałających w całej strukturze rozproszonej. Niemniej jednak sprawność działań będąca pochodną wdrożonych procedur działania oraz sposobu ich finansowania nie musi mieć prostego i bezpośredniego przełożenia na jakość zarządzania zasobami informacyjnymi, a tym samym na kreowanie polityki bezpieczeństwa informacyjnego w strukturze sieciowej.

Zapewnienie i utrzymanie oczekiwanego poziomu bezpieczeństwa informacyjnego w strukturze rozproszonej, szczególnie w sytuacjach kryzysowych, polega w głównej mierze na celowej i racjonalnej alokacji dostępnych i utrzymywanych danych oraz informacji w sieci organizacyjnej (a także weryfikowaniu ich przydatności, wiarygodności, poufności itp.), zwłaszcza w sytuacji, kiedy szeroko rozumiana jakość działań determinowana jest reżimem czasowym. Nie bez znaczenia w tym przypadku są zatem procesy tworzenia baz wiedzy zarówno w poszczególnych jednostkach organizacyjnych konstytuujących strukturę rozproszoną, jak i w całej sieci (np. w zakresie opracowywania wzorców działania, przewidywania/zapobiegania

[8] Nie można bowiem założyć, że jednostki administracji publicznej nie są elementami sieci biznesowej (głównie za sprawą tego, iż stanowią one jeden z głównych obszarów tzw. otoczenia dalszego przedsiębiorstw) i *vice versa*, np. w zakresie partnerstwa publiczno-prywatnego.

określonym klasom zagrożeń lub minimalizacji zakresu/skali ich skutków). W strukturze scentralizowanej (tj. pionowej, hierarchicznej) mogą powstawać formalne bariery zarządzania wiedzą i dlatego struktura rozproszona/sieciowa może sprzyjać zdobywaniu i kreowaniu różnego typu zasobów wiedzy o stanie zasobów i ich bezpieczeństwie, a stąd również kreować odpowiedni poziom bezpieczeństwa informacyjnego. Nie chodzi tutaj tylko o ochronę posiadanych rozproszonych przestrzennie i informacyjnie danych przed dostępem do nich jednostek nieupoważnionych, co raczej o celowe i konstruktywne (skutkujące zaistnieniem dodatniego efektu synergii) spożytkowanie tych zasobów informacyjnych we właściwym czasie, miejscu i przez właściwe jednostki (osoby, organizacje, substruktury danej sieci zależności itp.). Warunkiem koniecznym zarządzania wiedzą w strukturach rozproszonych – szczególnie w sytuacjach kryzysowych – jest więc dążenie do uwzględniania pełnych możliwości konfiguracji sieciowych.

3. Rozproszone struktury organizacyjne a struktura typu H-H

Struktury sieciowe wykorzystywane w sytuacjach kryzysowych funkcjonują w sposób nieco odmienny niż struktury sieciowe w organizacjach komercyjnych. Związane jest to z tym, że struktury biznesowe tworzą sieci zależności na czas określony i często nie mają jasnych zasad (procedur) postępowania, zwłaszcza w zakresie zmian konfiguracyjnych w różnych stanach zagrożeń, oraz operują inną strukturą celów i sposobem ich realizacji. Tak więc rozproszone struktury biznesowe *sensu stricto* koncentrują się na maksymalizacji zarówno własnych korzyści materialnych, jak i korzyści określonych klas odbiorców (klientów zewnętrznych i wewnętrznych, tj. innych jednostek biznesowych w strukturze). Zarządzanie w warunkach zagrożenia w biznesowych strukturach rozproszonych może wymagać znacznego nakładu zasobów i czasu, a także restrykcyjnego przestrzegania przyjętych założeń dla struktury sieciowej (o ile jest to w ogóle możliwe). Powstaje wówczas problem zaufania i etyki działania. Natomiast struktury rozproszone konstruowane dla celów zarządzania kryzysowego w ujęciu bezpieczeństwa narodowego mogą nie mieć z góry określonego czasu funkcjonowania (co nie wyklucza jednak możliwości częściowej/dynamicznej modyfikacji ich funkcji użyteczności oraz funkcji użyteczności jednostek je tworzących). Ponadto struktury te – co należy wyraźnie podkreślić – odznaczają się swoistym automatyzmem w przejściu od konfiguracji hierarchicznej do konfiguracji płaskiej[9].

Struktury sieciowe (płaskie, procesowe) odznaczają się wyższym stopniem elastyczności operacyjnej (a także częściowo strategicznej) niż struktury hierarchiczne [7] (m.in. za sprawą stosowania na szeroką skalę nowoczesnych technologii

[9] W środowisku biznesowym wspomniany automatyzm nie występuje.

teleinformatycznych [15]), a także ukierunkowaniem na sprawne zarządzanie wiedzą [10]. Trudno jest jednak przyjąć, że atrybuty te są kluczowe i wystarczające z punktu widzenia zapewniania i utrzymywania bezpieczeństwa informacyjnego (np. w zakresie zarządzania zasobami danych transakcyjnych i analitycznych lub też kreowania asymetrii informacyjnej – a tym samym wieloaspektowego wspierania procesów decyzyjnych). Dlatego w przypadku zarządzania bezpieczeństwem struktur rozproszonych w sytuacjach kryzysowych ze szczególnym uwzględnieniem bezpieczeństwa informacyjnego, istotnego znaczenia nabiera integracja konfiguracji hierarchicznych i heterarchicznych. Powstały w ten sposób model hybrydowy nosi nazwę konfiguracji *typu H-H*.

Model *struktury H-H* wynika najczęściej z uwarunkowań otoczenia i specyfiki podejścia do realizacji celów zarówno przez całą sieć, jak i jej poszczególne jednostki organizacyjne, uwypukla także rolę i znaczenie wykorzystania potencjału rozwiązań *ICT*. Dotyczy to przede wszystkim zapewniania bezpieczeństwa informacyjnego z wykorzystaniem dostępnych technologii, w tym tzw. technologii *Cloud Computing* (CC) oraz *Zintegrowanych Systemów Informatycznych Zarządzania* (ZSIZ). Podstawową korzyścią wynikającą z integracji konfiguracji hierarchicznych i heterarchicznych, po stronie tych pierwszych, jest wsparcie procesów kontrolnych oraz automatyczne przejście do tzw. jednowładztwa w stanie zagrożenia zewnętrznego. W momencie zaistnienia sytuacji kryzysowej następuje bowiem aktywizacja tzw. *Centralnej Jednostki Decyzyjnej* (CJD), w której koncentrują się procesy decyzyjne [19]. Elementy struktury hierarchicznej wspierają tym samym m.in. działania ukierunkowane na realizację procesów decyzyjnych np. w zakresie (re)alokacji zasobów w związku z koniecznością podjęcia przez strukturę rozproszoną działań naprawczych, ratowniczych itp. i mogą sprzyjać maksymalizacji funkcji użyteczności systemowej. Natomiast struktury sieciowe – jako składowe *modelu H-H* – umożliwiają względnie swobodny przepływ (re)alokowanych zasobów, skracając czas reagowania w sytuacji zagrożenia i dostosowywanie się do dynamiki zmian w otoczeniu. Oznacza to także uwzględnianie przez jednostki decyzyjne (w momencie zaistnienia sytuacji kryzysowej podstawową jednostką decyzyjną jest CJD[10]) oraz wykonawcze (czyli wszystkie jednostki w sieci – poza CJD) kryterium wiedzy i tworzenie bazy wiedzy w systemie organizacyjnym. Uwidacznia się w ten sposób również potencjał struktury *typu H-H* w zakresie współdziałania z otoczeniem (zarówno z otoczeniem zewnętrznym całej struktury rozproszonej, jak i z otoczeniem wewnątrzsieciowym poszczególnych jednostek konstytuujących daną sieć/strukturę rozproszoną) [2, 8, 10, 13] w oparciu o platformę Internetu.

[10] W strukturach sieciocentrycznych mówimy często o tzw. Centrum Kompetencyjnym określanym potocznie jako „pełzające" centrum decyzyjne w zależności od fazy realizacji określonego procesu.

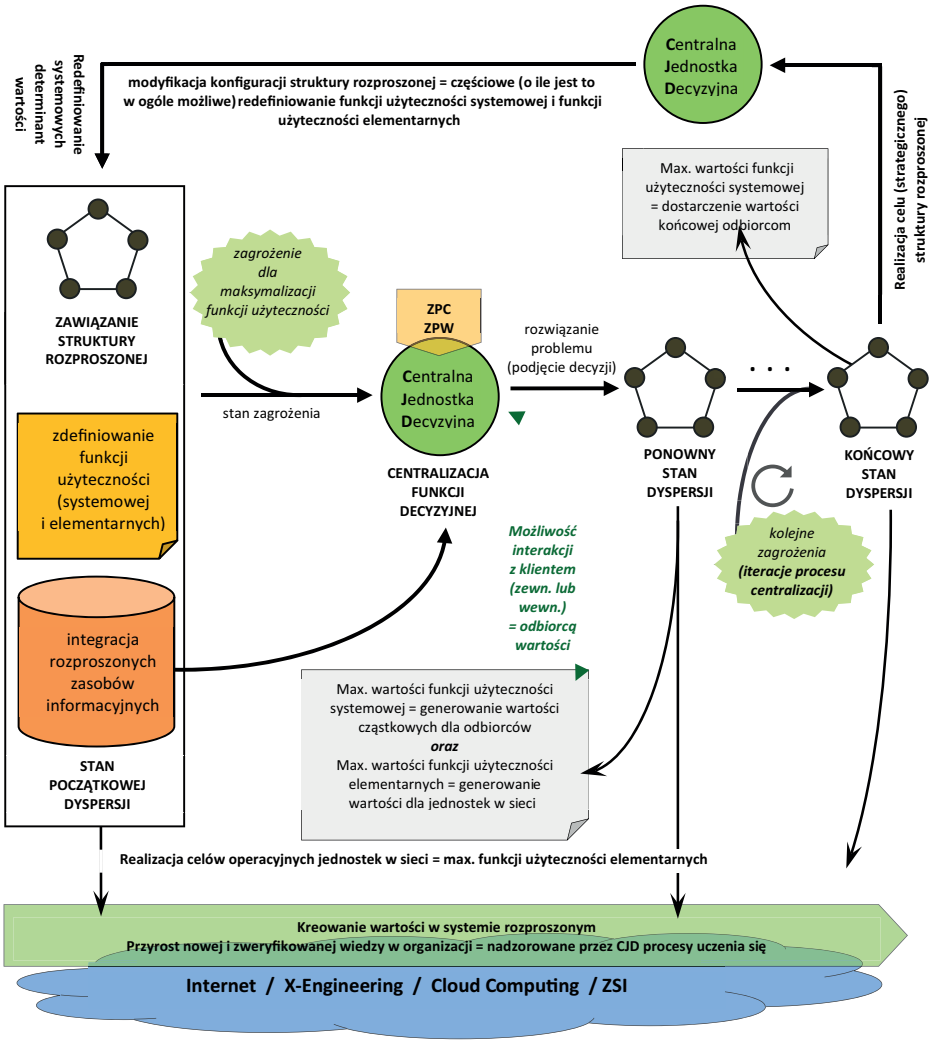
Struktura *typu H-H* jest w stanie wykorzystać potencjał do zarządzania rozproszonymi zasobami informacyjnymi z ekspozycją ich atrybutu bezpieczeństwa (zarówno w wymiarze operacyjnym, jak i strategicznym). Można więc przyjąć, że konfiguracja ta jest klasą organizacji uczącej się z silnym wsparciem funkcji planistyczno-prognostycznej oraz kontrolnej.

Wspomniany powyżej brak jednej i zawsze właściwej struktury organizacyjnej w systemie zarządzania kryzysowego *sensu largo* traktować można jako punkt wyjścia do konstrukcji rozwiązań hybrydowych, czego przykładem jest właśnie konfiguracja *typu H-H*. Warto jednak zauważyć, iż w stanie zagrożenia (w sytuacji kryzysowej) dla poszczególnych organizacji będących w strukturze sieciowej, funkcje użyteczności przybierają inną postać niż w stanie braku zagrożenia – postać ta determinowana jest wtedy nie strukturą zbioru celów (operacyjnych, taktycznych i strategicznych) partycypantów/jednostek współdziałających, a celami całej sieci. Na dodatek warto zauważyć, że cele te są inne w sytuacji zagrożenia (kryzysu) i w stanie braku zagrożenia. Struktura *typu H-H* niweluje jednak dysproporcje pomiędzy specyfiką funkcji użyteczności partycypantów sieci zarówno w różnych stanach zagrożenia, jak i w sytuacji kryzysowej. Związane jest to z tym, iż w stanie braku zagrożeń całej[11] sieci, struktura *typu H-H* zakłada maksymalizację celów (użyteczności) poszczególnych jej uczestników, natomiast w stanie zagrożenia następuje centralizacja funkcji decyzyjnej (dyspersja jednostek biznesowych zastępowana jest strukturą „sztywną"/hierarchiczną), a więc maksymalizowana jest w pierwszej kolejności użyteczność całego systemu (rys. 1). Odbywa to się jednak nie na zasadzie dewaluacji użyteczności uczestników sieci, ale raczej według założeń metody Zarządzania Przez Cele (ZPC).

System (a konkretniej CJD) jest świadomy tego, jakie cała sieć ma możliwości w sytuacji zagrożenia i dopiero na tej podstawie weryfikuje strukturę celów i wartość oczekiwaną użyteczności. W następnej kolejności weryfikowane są cele operacyjne i taktyczne poszczególnych jednostek w sieci. Zdolność do współdziałania, ale również do rezygnacji z własnej autonomii organizacyjnej, skłonność do poświęcenia części własnych celów i ich nowej hierarchizacji dla dobra „ogółu" (całej sieci) można traktować jako podstawowe kryteria zrównoważonego funkcjonowania struktur sieciowych – a nie tylko kryteria wiedzy, potencjału operacyjnego i intelektualnego oraz

[11] Model konfiguracji strukturalnej *typu H-H* zakłada przede wszystkim systemowe postrzeganie zależności pomiędzy poszczególnymi jednostkami w strukturze rozproszonej. Nie występuje bowiem autonomizacja *sensu stricto* celów poszczególnych partycypantów. Nawet w stanie bezpieczeństwa funkcje użyteczności powinny być odzwierciedleniem funkcji użyteczności systemu – natomiast sposób maksymalizacji użyteczności jest dowolny (o ile nie stoi w sprzeczności z obostrzeniami formalnoprawnymi oraz funkcjonowaniem całej struktury rozproszonej i nie zagraża jej bezpieczeństwu *sensu largo*). Natomiast w stanie zagrożenia (sytuacji kryzysowej) sposób maksymalizacji funkcji użyteczności (o ile w tym przypadku w ogóle można mówić o maksymalizacji – właściwszym określeniem wydaje się być „zapewnianie/utrzymywanie zadowalającego poziomu użyteczności") jest precyzyjnie zdefiniowany i nadzorowany przez CJD.

doświadczenia. Wskazane powyżej dodatkowe kryteria nie powinny być deprecjonowane na etapie zawiązywania i doskonalenia relacji w sieci, zwłaszcza że te wynikają pośrednio z kryteriów wiedzy i doświadczenia. Nie są jednak z nimi w pełni tożsame, zatem ich deprecjonowanie (lub co gorsza – ignorowanie) nie jest działaniem pożądanym dla zapewnienia i utrzymania stanu bezpieczeństwa informacyjnego w rozproszonym systemie organizacyjnym – szczególnie w sytuacji kryzysowej.



Rysunek 1. Kreowanie wartości i użyteczności w strukturze rozproszonej według założeń *modelu H-H* – jako podstawa polityki bezpieczeństwa informacyjnego
Źródło: opracowanie własne

Nie należy jednak nadmiernie rozwarstwiać różnych stanów zagrożeń, zwłaszcza w aspekcie zarządzania bezpieczeństwem informacyjnym. Takie podejście powoduje zniekształcanie działań doskonaląco-naprawczych w organizacjach rozproszonych, lawinowe nawarstwianie się konsekwencji błędnego zarządzania zasobami informacyjnymi lub też inicjowanie tego procesu dopiero w sytuacji rzeczywistego (tj. zmaterializowanego, widocznego) zagrożenia, kiedy to modyfikacje działań w jednej jednostce determinują zmiany w innych jednostkach i są nierzadko w sprzeczności zarówno z bieżącą maksymalizacją użyteczności tych jednostek, jak i użyteczności innych uczestników/partycypantów sieci, czego odzwierciedleniem może być nieprawidłowe podejście do pozyskiwania, integracji, przetwarzania, magazynowania i rozpowszechniania danych oraz informacji w strukturze, czyli innymi słowy błędne przygotowanie struktury rozproszonej do działania w sytuacji kryzysowej.

II Uwarunkowania bezpieczeństwa informacyjnego

Zapewnianie i utrzymywanie oczekiwanego poziomu bezpieczeństwa informacyjnego struktury rozproszonej wymaga podejścia holistycznego. Warto bowiem zwrócić jeszcze raz uwagę na fakt, że bezpieczeństwo informacyjne warunkowane jest z jednej strony czynnikami otoczenia zewnętrznego, a z drugiej strony mechanizmami wewnętrznymi zachodzącymi w organizacji (strukturze sieciowej, rozproszonej). Jak już wspomniano, źródeł zagrożeń dla bezpieczeństwa informacyjnego upatrywać należy na różnych płaszczyznach otoczenia struktury sieciowej. Szczególnego znaczenia nabiera w tym przypadku także operacyjne bezpieczeństwo informacyjne, sprowadzające się do utrzymania ciągłości realizowanych procesów, z czym związane jest również kreowanie wartości całego systemu (bezpieczeństwa systemowego) – co postuluje także koncepcja X-Engineeringu. Ciągłość działania (w zakresie procesów informacyjno-decyzyjnych) warunkowana jest także specyfiką otoczenia organizacji [6, 20]. Warto więc zauważyć, iż każdy z wyżej wymienionych czynników stanowi podstawę do opracowania założeń dla mechanizmów tworzenia baz wiedzy w organizacji (ze szczególnym uwzględnieniem wartości/użyteczności kreowanej/nowej wiedzy), stymulowania zjawiska asymetrii informacyjnej na wymaganym poziomie (przeciwdziałania celowemu zniekształcaniu wiedzy) oraz generowania wartości dodanej (elementarnej i systemowej) w całym systemie działania.

Koncepcja X-Engineeringu wspiera procesy kształtowania polityki bezpieczeństwa informacyjnego organizacji rozproszonych, głównie za sprawą dekompozycji i ewaluacji procesów realizowanych w danej strukturze oraz ich integracji i bieżącej, wieloaspektowej ocenie otrzymanych wyników (również na płaszczyźnie informacyjnej). Warte podkreślenia jest wsparcie integracji procesów poprzez wieloaspektową analizę danych i informacji w sytuacji kryzysowej w obszarze np. zarządzania relacjami z poszczególnymi partycypantami procesów (zewnętrznymi

i wewnętrznymi), subsystemu podstawowego i pomocniczego/zabezpieczającego działania, w tym zaopatrzenia materiałowego, dystrybucji materiałów, zarządzania finansami oraz zasobami ludzkimi itp. Dzięki wdrożeniu koncepcji X-Engineeringu może wystąpić dodatni efekt synergii w zakresie rozproszonych informacyjnie i przestrzennie baz danych (tzw. „wysp" informacyjnych) [17]. Czynnikiem kluczowym w usprawnianiu procesów informacyjno-decyzyjnych, jako zmiennej funkcji bezpieczeństwa ogólnego struktury rozproszonej, jest możliwość wykorzystania potencjału Internetu, m.in. w zakresie pozyskiwania z otoczenia informacji odpowiadających specyfice tzw. potrzeb informacyjnych jednostek w strukturze rozproszonej (dla określonej klasy działania) zgłaszanych przez poszczególne grupy wykonawców procesów oraz odbiorców[12]. Ważne przy tym są korzyści uzyskiwane na wyjściu systemu w sytuacji kryzysowej uwzględniające naturę procesów i możliwość ich integracji w generowaniu decyzji zbiorczych w strukturze rozproszonej. Usprawnianie procesów informacyjno-decyzyjnych powinno zmierzać do uwzględniania specyfiki działań ukierunkowanych na wsparcie procesów tworzenia baz wiedzy, komunikacji oraz dzielenia się wiedzą z zachowaniem zasad tzw. sterowanej asymetrii informacyjnej.

Zarządzanie bezpieczeństwem informacyjnym organizacji rozproszonej wspierane jest również innymi – komplementarnymi względem X-Engineeringu – koncepcjami zarządzania[13], np. outsourcingiem (informacyjnym i informatycznym), benchmarkingiem, strategią Lean Management czy też Time-Based Management itp. [17, 19, 22]. W związku z powyższym **procesy, propozycje i partycypacje** (czyli tzw. **trójkąt X-Engineeringu**) przebiegają według ustalonych formalnie zasad i poprzedzone są procesami planistycznymi i prognostycznymi oraz szczegółową dekompozycją każdego procesu. Ponadto wieloaspektowe wzajemne wsparcie działań ukierunkowane jest w głównej mierze na utrzymanie oczekiwanego poziomu operacyjnego bezpieczeństwa informacyjnego (głównie w czasie zaistnienia sytuacji kryzysowej), a także – w długim okresie – na wzrost wartości zarówno systemowo postrzeganej struktury rozproszonej, jak i jej elementów składowych (tj. na zwiększenie potencjału[14] danej struktury i tym samym doskonalenie realizowanych przez nią działań w przyszłości).

Każda jednostka organizacyjna w *stanie dyspersji*[15] (równoznacznym z delegowaniem funkcji decyzyjnej wybranym jednostkom tworzącym sieć) ma możliwość:

[12] Czyli ogółu lub części społeczeństwa.

[13] W tym przypadku należy dokonać transpozycji biznesowego wymiaru tych koncepcji zarządzania na specyfikę procesów zarządzania w sytuacjach kryzysowych.

[14] Między innymi w wyniku przyrostu wiedzy jawnej i wiedzy ukrytej.

[15] Równoznacznym w *modelu H-H* ze *stanem bezpieczeństwa* (tj. stanem braku bezpośrednich zagrożeń /sytuacji kryzysowej).

- identyfikacji procesów (jednakże zgodnych z początkowym planem strategicznym, taktycznym lub operacyjnym konstruowanym przez CJD w strukturze *typu H-H*),
- zgłaszania własnych propozycji wspólnych działań z określonymi jednostkami w sieci[16] oraz częściowej specyfikacji skali partycypacji (w zakresie przewidzianym w odpowiednich aktach normatywnych).

Tym samym zarządzanie bezpieczeństwem informacyjnym determinowane jest wypełnianiem kryteriów systemowych, takich jak kompletność, kompleksowość, gotowość, spójność, żywotność itp. Warto także podkreślić szczególną rolę CJD, która ma możliwość – zgodnie z przyjętymi procedurami bezpieczeństwa informacyjnego – częściowej modyfikacji zakresu działania z uwzględnieniem całej triady: *proces*, *propozycja*, *partycypacja* oraz stanu wejściowego systemu działania w momencie zaistnienia sytuacji kryzysowej, co ma na celu zwiększenie elastyczności, efektywności, niezawodności i finalnie skuteczności operacyjnego działania struktury rozproszonej. Centralizacja funkcji decyzyjnej, uwzględniana w modelu strukturalnym *typu H-H*, stanowi więc podstawę zarządzania zorientowanego na możliwie szybkie przywrócenie stanu równowagi i utrzymanie odpowiedniego poziomu bezpieczeństwa całej organizacji poprzez wsparcie/usprawnianie procesów kompleksowego zarządzania zasobami informacyjnymi.

III Kreowanie wartości organizacji w sytuacji kryzysowej

Wartość systemu organizacyjnego wyznaczana jest wartością jego elementów, a w szczególności szacowana jest jako suma wartości osiąganych wyników [17]. Mogą to być wskaźniki ekonomiczne lub inne skwantyfikowane wartości, np. użyteczności, które odzwierciedlają określoną klasę korzyści[17] dla danego systemu organizacyjnego (także w sektorze publicznym) lub odbiorców rezultatów działania tej struktury. Jednostką inicjującą procesy kreowania wartości jest CJD, która realizuje w tym przypadku funkcję analogiczną jak firma-integrator (kreator sieci[18]), pełniąc m.in. rolę technologicznego (w aspekcie technologii teleinformatycznych) opiekuna jednostek całej organizacji rozproszonej, koordynatora przedsięwzięć czy też dys-

[16] Zalecane jest także zgłaszanie propozycji dołączania określonych nowych jednostek do już istniejącej struktury sieciowej, np. jednostek z sektora pozarządowego (fundacji, stowarzyszeń itp.), które mogą wspierać działania struktury scentralizowanej (w sytuacji kryzysowej) w zakresie dostarczania żywności i wody, udostępniania miejsc noclegowych, zbierania środków pieniężnych, odbudowy zniszczonych domów i obiektów gospodarczych itp.

[17] Wartością w tym znaczeniu może być już nawet sama maksymalizacja funkcji użyteczności systemowej (ale wartość może mieć też znaczenie szersze lub może dotyczyć wyłącznie procesów kreowania wiedzy w systemie).

[18] CJD nie musi (ale może) być jednostką występującą z inicjatywą kreowania struktury sieciowej lub jej modyfikacji.

ponenta/gestora zasobów i ich przepływów [10]. Należy jednak zaznaczyć, że CJD w strukturze *typu H-H* nie powinna pełnić roli archiwizatora wiedzy i informacji.

Problem kreowania wartości w strukturze rozproszonej związany jest silnie z dopasowaniem organizacji o strukturze rozproszonej do możliwości i ograniczeń wynikających z własności narzędzi IT, czyli z takim doborem technologii teleinformatycznych (ICT), które umożliwią w pełni realizację celów operacyjnych i strategicznych nie tylko poszczególnych uczestników struktury rozproszonej, lecz także całego systemu działania. Istotną rolę pełni w tym przypadku właściwie zaplanowana i realizowana integracja danych rozproszonych. Jest to ważne zadanie, gdyż wartość działań podejmowanych przez jednostkę będącą w strukturze rozproszonej ma swoje istotne odzwierciedlenie w wartości funkcji użyteczności systemu działania w sytuacji kryzysowej.

W strukturze *typu H-H* kreowana jest wartość w wymiarze (rys. 1):

- **maksymalizacji wartości funkcji użyteczności systemowej** (czyli następuje generowanie wartości cząstkowych dla społeczeństwa *sensu largo*, jako wynik działania całego systemu rozproszonego);
- **maksymalizacji wartości funkcji użyteczności elementarnych** (czyli odbywa się generowanie wartości dla poszczególnych jednostek tworzących strukturę rozproszoną).

W kreowaniu wartości organizacji w stanie dyspersji (w tym jej poziomu bezpieczeństwa informacyjnego) wiodącą rolę pełnią zasoby danych bieżących/operacyjnych (OLTP[19]), ze szczególnym uwzględnieniem ich gromadzenia i wymiany na platformie sieci powszechnej (Internet, usługi *Cloud Computing*), jak również danych historycznych/analitycznych (OLAP[20]), gdyż te umożliwiają realizację procesów prognostyczno-planistycznych (na wzór metody Zarządzania Przez Wyjątki – ZPW).

W sytuacji zagrożenia, kiedy wiodącą rolę pełni CJD, kreowanie wartości bazuje przede wszystkim na danych operacyjnych (eksponowane są bowiem wtedy bieżące mechanizmy decyzyjne), jednak przydatność zasobów danych analitycznych nie jest wówczas kwestionowana. Warto również zaznaczyć, że ważnym etapem w procesie kreowania wartości organizacji o strukturze rozproszonej (w tym także w strukturze *typu H-H*) jest możliwość dynamicznego redefiniowania funkcji użyteczności systemowej oraz elementarnych funkcji użyteczności (w ramach kompetencji CJD) (rys. 1). Jest to założenie bazowe, gdyż warunkuje nie tylko reorganizację relacji w strukturze rozproszonej (a tym samym swobodnego pozyskiwania i wymiany zasobów informacyjnych w strukturze sieciowej), lecz także determinuje założenia asymetrii informacyjnej i wpływa na potencjał organizacji do utrzymania ciągłości procesów podstawowych, pomocniczych i zarządczych. Wpływa tym samym na poziom bezpieczeństwa informacyjnego poprzez elastyczne i iteracyjne kształtowanie

[19] Ang. *On-Line Transaction Processing*.
[20] Jak wyżej.

polityki bezpieczeństwa. Modyfikacji mogą ulec cele operacyjne i strategiczne, a więc zmienić się może także struktura i zakres dopasowania samej organizacji do infrastruktury IT. Fakt ten oznacza konieczność zmiany aktualnie stosowanej i rozwijanej technologii, np. w zakresie rozbudowy ZSIZ, lub też konieczność rozbudowy infrastruktury telekomunikacyjnej i platform integracyjnych. W sytuacjach kryzysowych są to integralne elementy infrastruktury krytycznej.

PODSUMOWANIE

W ocenie struktur rozproszonych kryterium ich bezpieczeństwa należy uznać za dominujące. Jedną z ważnych składowych tego kryterium jest bezpieczeństwo informacyjne warunkujące ciągłość działania organizacji w warunkach zagrożeń i kryzysów. Ocena bezpieczeństwa informacyjnego struktur rozproszonych w sytuacji kryzysowej jest działaniem wieloaspektowym, wymagającym znajomości specyfiki zarówno wnętrza struktury, jak i jej otoczenia. Bezpieczeństwo informacyjne jest pochodną zbioru zasad zarządzania zasobami informacyjnymi, ze szczególnym uwzględnieniem poprawnej metodycznie i celowej (re)alokacji zasobów danych i informacji pomiędzy strukturą i otoczeniem, a także pomiędzy jednostkami tworzącymi tę strukturę – w celu zwiększenia skuteczności działań operacyjnych i strategicznych. Płaszczyzna operacyjna bezpieczeństwa informacyjnego przenika płaszczyznę strategiczną (oraz taktyczną), głównie w aspekcie dostarczania danych oraz wniosków będących elementami wyjścia kolejnej iteracji działania systemu (struktury sieciowej) w stanie zagrożenia/sytuacji kryzysowej.

Zarządzanie bezpieczeństwem informacyjnym w sytuacjach kryzysowych sprowadza się do umiejętnego kształtowania konfiguracji strukturalnej. Szczególnego znaczenia nabiera więc model struktury *typu H-H*, ponieważ stanowi pomost pomiędzy decentralizacją i centralizacją funkcji decyzyjnej. Strukturalizacja funkcji decyzyjnych w znacznym stopniu determinuje skuteczność zarządzania zasobami informacyjnymi w różnych stanach zagrożeń i powinna uwzględniać specyfikę wszystkich etapów zarządzania zasobami tej kategorii. Zarządzanie bezpieczeństwem informacyjnym struktur rozproszonych warunkowane jest w szczególności złożonością samej struktury sieciowej oraz rozbieżnością w definiowaniu i kształtowaniu funkcji użyteczności zarówno poszczególnych jednostek, jak i całej sieci. Ważnym czynnikiem tego procesu jest również nieregularność (nieprzewidywalność)[21] występowania określonych klas sytuacji kryzysowych oraz ich niejednorodność. Powstają więc problemy z identyfikacją potrzeb informacyjnych, pozyskiwaniem danych, ich integracją, przetwarzaniem w systemach informatycznych oraz z udostępnianiem samych zasobów itp. Ponadto kryterium bezpieczeństwa informacyj-

[21] Oczywiście z określonymi wyjątkami.

nego powinno być skojarzone z kryteriami wiarygodności, spójności i poufności pozyskiwanych i przetwarzanych danych. Jak zatem widać, działanie w warunkach ryzyka i niepewności determinuje szeroko rozumianą jakość procesów zarządzania bezpieczeństwem informacyjnym struktur rozproszonych w sytuacji kryzysowej – nie wszystko zależy bowiem wyłącznie od działań podejmowanych przez człowieka.

Maksymalizacja funkcji użyteczności z zachowaniem poziomu bezpieczeństwa informacyjnego struktur rozproszonych sprowadza się do takiego kształtowania struktury celów (poszczególnych jednostek oraz całej sieci), aby nie występowała sprzeczność w postrzeganiu jakości (m.in. potencjału i zawartości merytorycznej, kompletności itp.) udostępnianych informacji. Wartością szczególną dla jednostki i całej sieci w sytuacjach kryzysowych – w warstwie procesów decyzyjnych – jest możliwość maksymalizacji stopnia spełnienia celów statutowych danej jednostki, czyli zapewnienia bezpieczeństwa w określonym obszarze działania systemu. Zarządzanie bezpieczeństwem informacyjnym nierozerwalnie związane jest więc z **użytecznością** i **wartością** oraz **efektywnością**, **niezawodnością**, a także **jakością całej organizacji** i **jej zasobów** zarówno w krótkiej, jak i długiej perspektywie czasowej.

LITERATURA:

1. M. Brzozowski, *Organizacja wirtualna*, PWE, Warszawa 2010.
2. W. Czakon, *Sieci w zarządzaniu strategicznym*, Wolters Kluwer, Warszawa 2012.
3. K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, BEL Studio, Warszawa 2007.
4. Z. Gomółka, *Cybernetyka w zarządzaniu*, Placet, Warszawa 2000.
5. A. Jaruga, *Technologia teleinformatyczna w organizacji wirtualnej*, Wydawnictwo Politechniki Poznańskiej, Poznań 2010.
6. T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu a ciągłość działania: Business Continuity Management*, Difin, Warszawa 2009.
7. S. Kasiewicz, *Elastyczność przedsiębiorstwa w koncepcjach zarządzania procesowego*, (w:) *Metody osiągania elastyczności przedsiębiorstw: od zarządzania zasobowego do procesowego*, S. Kasiewicz i in., SGH, Warszawa 2009.
8. S. Łobejko, *Przedsiębiorstwo sieciowe: zmiany uwarunkowań i strategii w XXI wieku*, SGH, Warszawa 2010.
9. A. Mrożek, *Zarządzanie bezpieczeństwem organizacji o strukturze heterarchicznej*, http://bezpieczna.uek.krakow.pl/artykol.pdf (25.09.2013).
10. K. Perechuda, *Dyfuzja wiedzy w przedsiębiorstwie sieciowym: wizualizacja i kompozycja*, Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu, Wrocław 2007.
11. A. Piekarczyk, K. Zimniewicz, *Myślenie sieciowe w teorii i praktyce*, PWE, Warszawa 2010.
12. P. Płoszajski, *Organizacja przyszłości: przerażony kameleon*, http://www.allternet.most.org.pl/SOD/Heterarchia%20prof._Ploszajski_-_Organizacja_przyszlosci.pdf (24.09.2013).

13. K. Polańska, *Ewolucja przedsiębiorstwa w środowisku wirtualnym*, „Kwartalnik Nauk o Przedsiębiorstwie", 2013, nr 1(26).
14. A. Sankowska, *Organizacja wirtualna: koncepcja i jej wpływ na innowacyjność*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009.
15. W. Urban, *Narzędzia służące zwiększaniu elastyczności*, (w:) *Metody osiągania elastyczności przedsiębiorstw: od zarządzania zasobowego do procesowego*, S. Kasiewicz i in., SGH, Warszawa 2009.
16. J. Woźniak, P. Zaskórski, *Asymetria informacyjna w zarządzaniu bezpieczeństwem organizacji procesowych*, „Nowoczesne Systemy Zarządzania", 2009, z. 4.
17. P. Zaskórsk i in., *Zarządzanie projektami w ujęciu systemowym*, WAT, Warszawa 2013.
18. P. Zaskórski, *Asymetria informacyjna w zarządzaniu procesami*, WAT, Warszawa 2012.
19. P. Zaskórski, W. Gonciarski, *Struktury i strategie zarządzania organizacją*, (w:) *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, P. Zaskórski (red.), WAT, Warszawa 2011.
20. P. Zaskórski, J. Woźniak, *Ciągłość informacyjno-decyzyjna warunkiem bezpieczeństwa organizacji gospodarczej*, (w:) *Wybrane koncepcje i metody zarządzania początku XXI wieku*, W. Gonciarski, P. Zaskórski (red.), WAT, Warszawa 2009.
21. P. Zaskórski, J. Woźniak, G. Pieniążek, *Procesowe modele zarządzania w aspekcie ryzyka utraty informacyjnej ciągłości działania*, (w:) *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, P. Zaskórski (red.), WAT, Warszawa 2011.
22. K. Zimniewicz, *Współczesne koncepcje i metody zarządzania*, PWE, Warszawa 2009.

SECURITY OF THE DISPERSED ARRANGEMENTS IN CRISIS SITUATIONS

Abstract. In the contemporary world many of its functional organizations are dispersed. The dispersed structures can function efficiently thanks to the ICT technology. In presented article the focus is placed on security of the dispersed structures, with a particular regard to the information security, mainly with respect to the crisis situation management. There is a special consideration given to methods providing and maintaining desired level of an information security, mainly in terms of the operations' continuity and with reference to maximization of the utility and value of each units connected by assumed relationships in the crisis circumstances. This presentation highlights the need of dynamic adaptation of the structures to the tasks taken under conditions of strong restrictions because of time and resources. Special importance can be given in this case to the concept of X-Engineering, which can stimulate a specific kind of a security management strategy of the spatially and informationaly dispersed organization with the use of the ICT technology. This concept is based on the triad: process, proposal, participation. The processes obtain a status of the organizational objects what makes possible to select their executers dynamically. Therefore, there may be observed the decentralization of the decision-making functions in accordance to the provinces of the units that execute the common processes in a territorial dispersion of a particular situation. The flexibility of changing the executive structures depends on tasks and resources' availability and can be ensured *by* the *H-H type* structure, which identifies the *dispersion states* – i.e. the decentralization of a decision-making function – under the conditions of a lack of threats, and the centralization of the decision-making functions – in an emergency/crisis situation (or the situation under threat). The different classes' of ICT tools ensure the effective implementation of the operating and decision-making processes.