MONITOROWANIE ZAGROŻEŃ Z WYKORZYSTANIEM SYSTEMÓW INFORMACJI GEOGRAFICZNEJ

Piotr Zaskórski

Wojskowa Akademia Techniczna

Dorota Żbik

Streszczenie. W artykule dokonano opisu możliwości wykorzystania systemów GIS do monitorowania zagrożeń w systemach zarządzania kryzysowego z uwzględnieniem kryterium ich informacyjnej ciągłości działania. Autorzy podjęli więc próbę wstępnej oceny możliwości wykorzystania systemów GIS oraz udostępniania danych i usług geoprzestrzennych jako platformy integracyjnej dla systemów zarządzania kryzysowego. Rozwój rozwiązań projektowanych i wdrażanych w ramach projektu ISOK może skutkować dalszym podnoszeniem jakości, skalowalności, dostępności oraz poziomu bezpieczeństwa w systemach zarządzania kryzysowego.
Słowa kluczowe: zarządzanie, kryzys, system, geodane, GIS.

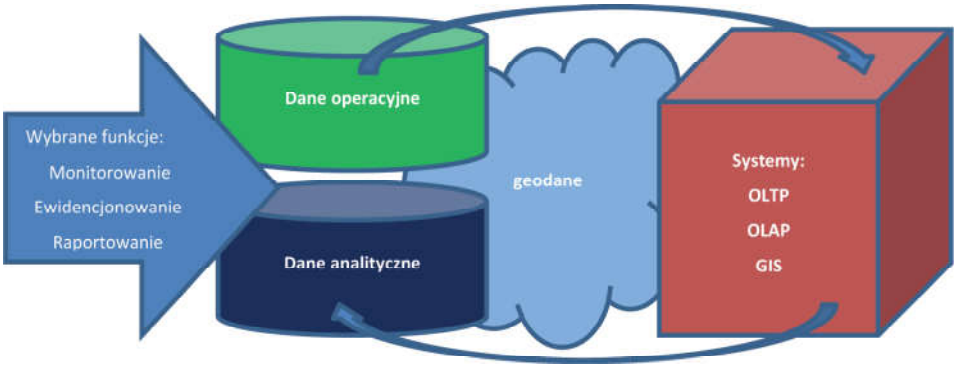
1. Wprowadzenie

Monitorowanie zagrożeń dla bezpieczeństwa państwa i jego obywateli jest stałą funkcją systemów zarządzania kryzysowego. Dotyczy to przede wszystkim zagrożeń dla infrastruktury krytycznej, którą zgodnie z ustawą o zarządzaniu kryzysowym stanowią różnorodne obiekty oraz urządzenia, instalacje i usługi tworzące podsystemy zaopatrzenia, a także podsystemy transportowe, łączności i telekomunikacji, finansowe, ochrony zdrowia i ratownictwa. Komponenty infrastruktury krytycznej zapewniają bowiem ciągłość działania systemów administracji rządowej i samorządowej[1] oraz ważnych podmiotów gospodarczych. Zapewnienie bezpieczeństwa i ciągłości działania każdej organizacji wymaga dostępu do środków koniecznych do realizacji zadań i celów statutowych. Zasoby informacyjne i środki związane z ich utrzymywaniem oraz udostępnianiem należy więc także uznać za ważny komponent infrastruktury krytycznej warunkującej realizację podstawowych funkcji oraz przetrwanie i rozwój danego podmiotu. Wśród zasobów informacyjnych istotną kategorię stanowią dane geograficzne (tzw. geodane), które wzmacniają funkcjonalność systemów zarządzania kryzysowego poprzez bieżące monitorowanie i analizę dyslokacji różnych zasobów ze szczególnym uwzględnieniem tych, które tworzą właśnie infrastrukturę krytyczną.

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

2. Zasoby informacyjne a infrastruktura krytyczna

Działanie w warunkach ryzyka oraz ograniczoności zasobów wymaga szczególnej troski o zapewnienie wysokiej skuteczności i sprawności procesów zarządzania. Poziom bezpieczeństwa każdej organizacji jest bowiem funkcją potencjału (ludzkiego, ekonomicznego, technologicznego, informacyjnego, surowcowego i in.) oraz sposobu jego wykorzystania. Problem bezpieczeństwa jest szczególnie widoczny w sytuacjach kryzysowych, wymagających podejmowania decyzji w warunkach zaskoczenia i presji czasu. Z tego wynika rosnąca rola zasobów informacyjnych warunkujących jakość planowania i podejmowania decyzji.



Rys. 1. Zasoby informacyjne w systemach zarządzania kryzysowego
Źródło: opracowanie własne

Do ważniejszych zasobów informacyjnych[2] systemu zarządzania kryzysowego (rys. 1) można ogólnie zaliczyć:

- bazy danych operacyjnych będących odzwierciedleniem/ewidencją wyników bieżącego monitorowania sytuacji;
- hurtownie danych historycznych/analitycznych odzwierciedlających sytuację i zachowania podmiotu (obiektu) w dłuższym okresie, które mogą być podstawą do normowania, prognozowania i identyfikacji trendów, związków oraz zależności w przyszłości;
- bazy danych geograficznych, tzw. geodanych, o dyslokacji zasobów, w tym o obiektach infrastruktury krytycznej, połączone z bazami/hurtowniami danych operacyjnych/historycznych.

Warto przy tym zauważyć, że dostęp oraz umiejętność przetwarzania złożonych zbiorów danych coraz częściej utożsamiana jest ze składową strategicznego potencjału organizacji.

[2] P. Zaskórski, *Asymetria informacyjna w zarządzaniu procesami*, Redakcja Wydawnictw WAT, Warszawa 2012, s. 201-282.

Ilość i złożoność informacji wykorzystywanych na potrzeby zarządzania kryzysowego wymaga zaawansowanej obsługi informatycznej. Szczególne miejsce zajmują tutaj systemy przetwarzania danych w trybie on-line, zwłaszcza w aspekcie mobilności, wielodostępności oraz bezpieczeństwa informacyjnego. Bezpieczeństwo takie należy postrzegać zarówno w wymiarze bezpieczeństwa zasobów informacyjnych, jak i infrastruktury umożliwiającej gromadzenie, przechowywanie, transfer oraz przetwarzanie danych, a także udostępnianie informacji uprawnionym podmiotom. Ważną kategorią stają się systemy informacji geograficznej GIS (Geographic Information System) powiązane z systemami OLTP (On-Line-Transaction-Processing) i z systemami analitycznymi typu OLAP (On-Line-Analytical-Processing). Bezpieczeństwo informacyjne wszystkich tych systemów i ich zasobów, a więc spełnienie kryteriów poufności, integralności, dostępności, a także autentyczności i niezaprzeczalności utrzymywanych w nich danych – w dużym stopniu determinuje sprawność informacyjną oraz niezawodność i ciągłość działania[3] infrastruktury krytycznej.

3. Dane geoprzestrzenne w systemach zarządzania kryzysowego

Współczesne systemy zarządzania i reagowania kryzysowego bazują na zaawansowanych technologiach informatycznych i teleinformatycznych. Aktualna informacja o dyslokacji i stanie posiadanych sił i środków w systemach reagowania kryzysowego jest warunkiem spójnego i skutecznego działania. Systemy GIS bazują na specyficznych modelach (normach opisu) obiektów geoprzestrzennych przeznaczonych dla potrzeb poszczególnych rozwiązań technologicznych. Normy te (przyjęte przez OGC oraz ISO[4]) umożliwiają komputerowe przetwarzanie opisów wirtualnych, operując przekształceniami typu:

- odwzorowanie świata rzeczywistego na abstrakcyjne obiekty;
- reprezentacja obiektów wykorzystanych do modelowania świata rzeczywistego (relacja świat konceptualny a świat geoprzestrzenny);
- wymiarowanie obiektów oraz ich identyfikacja w odniesieniu do Ziemi (relacja świat geoprzestrzenny a świat wymiarowany).

Modelowanie danych geoprzestrzennych normowane jest zbiorem szczegółowych specyfikacji ISO (grupy 19100) oraz odpowiadających im tematów OpenGIS utrzymywanych przez OGC i obejmujących kilkanaście perspektyw postrzegania geodanych. Modele opisu geodanych stanowią podstawę projektów geoprzestrzennych

[3] PN-ISO/IEC 27001, *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*, PKN, Warszawa 2007, pkt 3.4.

[4] OGC – *Open Geospatial Consortium Inc.*, ISO – *International Organization for Standardization.*

(np. INSPIRE[5]) oraz rozwiązań prawnych wdrażanych w Polsce[6]. W systemach reagowania kryzysowego istnieje znacząca grupa obiektów geoprzestrzennych, które są modelowane do postaci obiektów wirtualnych mogących nie mieć swoich „wizualnie podobnych" odpowiedników w świecie rzeczywistym[7]. Ważne są tu jednak właściwości operacyjne obiektów i tzw. obiekty operacyjne. W systemach reagowania kryzysowego dane geograficzne są podstawą do konstruowania map numerycznych, a dane operacyjne to kolejne warstwy informacyjne obejmujące kategorie danych o siłach i środkach, o działaniach (zadaniach), czy też dane o zdarzeniach (chemicznych, biologicznych, jądrowych, powodziach, pożarach, katastrofach technicznych, katastrofach komunikacyjnych, zamachach bombowych, aktach wandalizmu, zamieszkach itp.) lub dane operacyjne o obiektach infrastruktury.

W systemach reagowania kryzysowego opis i reprezentacja obiektów operacyjnych powinny sprowadzać się do prostego przypisania poszczególnym obiektom znaku lub symbolu wybranego z unormowanego zestawu znaków. Modelowanie obiektów operacyjnych w systemach reagowania kryzysowego[8] powinno być determinowane głównie przez techniczne możliwości wykorzystywanych narzędzi teleinformatycznych (systemów GIS). Ponadto przypisanie obiektom operacyjnym gotowych znaków wymaga centralnej weryfikacji tego procesu. Poszczególne służby budują często swoje systemy zarządzania informacją geograficzną w oparciu o różne struktury i formaty danych geoprzestrzennych. Wymaga to działań standaryzacyjnych i integracyjnych (np. STANAG[9] 2019 wersje: APP-6A, APP-6B; MIL-STD[10] 2525 wersje: A, B, C i narodowy standard wzorowany na APP-6A[11] dla SZ RP lub narodowy standard bazujący na APP-6A dla służb podległych MSW).

Jak wcześniej wspomniano, w przypadku wystąpienia sytuacji kryzysowej decydującą rolę odgrywa czas, co wiąże się z szybkością, dokładnością, wszechstronnością oraz aktualnością informacji dla procesu decyzyjnego. Te wymagania dotyczą także Systemów Informacji Geograficznej (GIS, ang. *Geographic Information Systems*). GIS jest więc systemem umożliwiającym przepływ i wykorzystanie informacji geoprzestrzennej dotyczącej lokalizacji obiektów wraz z ich charakterystyką operacyjną. Wykorzystanie jednej spójnej bazy danych geograficznych pozwala na

[5] INSPIRE – *Infrastructure for Spatial Information in Europe*.

[6] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 listopada 2011 r. w sprawie bazy danych obiektów topograficznych oraz bazy danych obiektów ogólnogeograficznych, a także standardowych opracowań kartograficznych.

[7] G. Pokorski, P. Zaskórski, *Wykorzystanie geodanych systemów dowodzenia i zarządzania w systemie bezpieczeństwa narodowego*, Konferencja naukowa nt. *Bezpieczeństwo – ujęcie kompleksowe*, Katowice – 31 maja 2012, s. 12.

[8] G. Pokorski, P. Zaskórski, W*ykorzystanie geodanych systemów dowodzenia i zarządzania w systemie bezpieczeństwa narodowego*, op. cit., s. 18/8.

[9] STANAG – *NATO Standardization Agreement*.

[10] MIL-STD – *United States Defense Standard*.

[11] APP-6A – *Allied Procedural Publication*.

usprawnienie podejmowania decyzji przez szybsze uzyskanie odpowiedzi na pytania i przeprowadzanie analiz. GIS pozwala na jednoczesną analizę danych geograficznych i opisowych oraz prezentację wyników tej analizy[12].

Rys. 2. Struktura zadaniowa wykorzystania GIS w procesie zarządzania kryzysowego
Źródło: opracowanie własne

Systemy GIS (rys. 2) mogą odgrywać istotną rolę w zapobieganiu, reagowaniu i minimalizowaniu skutków wystąpienia sytuacji kryzysowej. Prawidłowa realizacja zadań wymaga dostępu do aktualnych i wiarygodnych informacji o terenie. Zespoły reagowania kryzysowego mogą wykorzystywać bazy danych ogólnych (dane podstawowe, geomorfologia, klimat), demografii (dane podstawowe, wsie, miasta), komunikacji (drogi, koleje), sił i środków (zespoły reagowania, Ochotnicza Straż Pożarna, Państwowa Straż Pożarna itp.), zdarzeń (procedury, raporty) oraz zagrożeń. Większość powyższych danych to dane georeferencyjne mające odniesienie do powierzchni Ziemi. Dane te pozwalają zlokalizować na mapie zdarzenia istotne z punktu widzenia zarządzania kryzysowego m.in. dla potrzeb[13]:

- ewidencji i prezentacji obiektów niebezpiecznych na mapie,
- przeprowadzania analiz demograficznych na obszarach zagrożonych,
- ewidencji i prezentacji obiektów użyteczności i administracji publicznej,
- planowania lokalizacji punktów gromadzenia ludności, centrów dowodzenia, dróg ewakuacyjnych,
- prowadzenia symulacji skutków fali powodziowej,
- prowadzenia symulacji zalewania obszarów w przypadku uszkodzenia wałów przeciwpowodziowych,
- analizowania wariantów działań w przypadku wystąpienia sytuacji kryzysowej lub szacowania zniszczeń po jej wystąpieniu.

[12] E. Bielecka, *Systemy informacji geograficznej. Teoria i zastosowania*, Wydawnictwo PJWSTK, Warszawa 2005, s. 125-144.
[13] D. Gotlib, A. Iwaniak, R. Olszewski, *GIS. Obszary zastosowań*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 122.

Zapewnienie społeczeństwu bezpieczeństwa wymaga stworzenia sprawnego i zorganizowanego systemu ratownictwa. Dlatego w Polsce zbudowano system centrów powiadamiania ratunkowego (CPR), w którym istotną rolę powinny odgrywać systemy GIS, w tym zapewniać[14]:

- szybką i sprawną lokalizację miejsca zdarzenia, osoby powiadamiającej,
- wyszukiwanie najbliższych jednostek ratunkowych wraz z koordynacją ich pracy,
- automatyczne planowanie najlepszej trasy dojazdu do zdarzenia,
- wspomaganie planowania trasy do najbliższego szpitala, umożliwianie omijania utrudnień na trasie,
- wyszukiwanie istotnych obiektów w pobliżu zdarzenia takich jak hydranty, ujęcia wody, zbiorniki paliwa, utrudnienia dojazdu itp.

W każdym z powyższych zadań niezbędna jest informacja geograficzna o terenie, zobrazowaniu na mapie miejsca zdarzenia, miejscu znajdowania się pojazdów ratowniczych, lokalizacji szpitali (wraz z informacją o wolnych miejscach) czy też gabinetów lekarskich. GIS daje możliwość połączenia systemu z systemem GPS (ang. *Global Positioning System*) i wykorzystania technologii telekomunikacyjnych[15], na przykład TETRA (ang. *Terrestrial Trunked Radio*).

Aktualnie w Systemie Zarządzania Kryzysowego do realizacji ustawowych zadań korzysta się z wielu różnorodnych źródeł. Wykorzystywane są oprogramowanie i aplikacje przeznaczone głównie dla zadań zarządzania kryzysowego (np. ARCUS 2005, e-CZK, COREL DRAW X3 PL, InfoMed, GPS Monitor Rejestr itp.). Sprawne działanie SZK wymaga analizy informacji również z innych źródeł, takich jak ArcGIS, MapInfo Professional czy Arcus-Geo. Powyższe pakiety oprogramowania pozwalają na szeroką gamę zastosowań związanych z analizą danych przestrzennych[16]. Na potrzeby zarządzania kryzysowego wykorzystywane mogą być także bazy danych dotyczące sił i środków Szefa Obrony Cywilnej, bazy teleadresowe DTA, baza danych i system transferu komunikatów lekarza koordynatora ratownictwa medycznego LKRM czy SRK 2006 stanowiący źródło informacji dla gminnych, powiatowych i wojewódzkich CZK[17].

Wiele usług informacyjnych, w tym dostęp do geodanych, jest możliwych z wykorzystaniem usług w chmurze obliczeniowej. Wirtualizacja usług informacyjnych[18]

[14] D. Gotlib, A. Iwaniak, R. Olszewski, *GIS. Obszary zastosowań*, op. cit., s. 123.

[15] Ibidem.

[16] L . Litwin, G. Myrda, *Systemy Informacji Geograficznej. Zarządzanie danymi przestrzennymi w GIS, SIT, LIS*, Wydawnictwo Helion, Gliwice 2005, s. 230.

[17] http://www.kzgw.gov.pl/files/file/Zamowienia_publiczne/20131216-uslugi-doradcze/Zalacznik-nr-2-do-SOPZ-Studium-wykonalnosci-cz-1.pdf (24.07.2015 r.). Studium wykonalności dla projektu w ramach VII osi priorytetowej Programu Operacyjnego Innowacyjna Gospodarka, Projekt Informatyczny *System osłony kraju przed nadzwyczajnymi zagrożeniami*, s. 165.

[18] M. Serafin, *Wirtualizacja w praktyce*, Helion, Gliwice 2012; P. Zaskórski, *Wirtualizacja organizacji w „chmurze" obliczeniowej*, „Ekonomika i Organizacja Przedsiębiorstwa", Wyd. ORGMASZ,

i operowanie geodanymi w „chmurze" obliczeniowej[19] może być szczególnie efektywne w systemach reagowania kryzysowego ze względu na skalowalność, dostępność do aktualnych zasobów i ich bezpieczeństwo zapewniane poprzez dywersyfikację centrów przetwarzania danych geoprzestrzennych. Wymaga to jednak zapewnienia szybkiej i niezawodnej sieci łączności umożliwiającej użytkownikom połączenie z „chmurą". Najbardziej wrażliwym obszarem informacyjnym systemów reagowania kryzysowego jest jakość informacji, w tym geodanych z uwzględnieniem takich atrybutów jak kompletność, poprawność i aktualność. Ponadto w razie wzrostu zagrożenia możliwe jest udostępnianie wybranych zasobów systemu (danych i usług) grupom użytkowników SZK zebranym doraźnie. Tak „pozyskani" użytkownicy systemu reagowania kryzysowego mogą pełnić rolę „inteligentnych" sensorów wprowadzających do systemu informacje zdefiniowane w udostępnionych usługach (określać w trybie on-line np. zasięg powodzi, lokalizację pożarów, wypadków itp.). Podejście takie znacząco zwiększy kompletność i aktualność danych oraz może przyczynić się do zwiększenia poprawności danych. Wzmocnienie potencjału SZK może nastąpić w głównej mierze poprzez integrację współdziałania, a w szczególności integrację procesów wewnętrznych i zewnętrznych[20] na wspólnej platformie geodanych, co może być kluczem do skutecznego monitorowania zagrożeń i przeciwdziałania im w systemach reagowania kryzysowego.

4. Koncepcja monitorowania i zapewniania bezpieczeństwa z wykorzystaniem systemu ISOK

W ramach dwóch unijnych dyrektyw – powodziowej oraz INSPIRE – od 26 sierpnia 2009 roku realizowany jest projekt Informatycznego Systemu Osłony Kraju przed nadzwyczajnymi zagrożeniami ISOK. Projekt realizuje konsorcjum w składzie:

- Krajowy Zarząd Gospodarki Wodnej KZGW (lider),
- Instytut Meteorologii i Gospodarki Wodnej Państwowego Instytutu Badawczego IMGW PIB,
- Główny Urząd Geodezji i Kartografii GUGIK,
- Instytut Łączności Państwowego Instytutu Badawczego IŁ PIB oraz Rządowe Centrum Bezpieczeństwa RCB.

nr 3/2012, Warszawa 2012, s. 12.

[19] P. Zaskórski, G. Pokorski, *Chmura obliczeniowa w systemach reagowania kryzysowego w aspekcie dostępu do danych geoprzestrzennych*, Międzynarodowa Konferencja Naukowa „Polska w europejskim środowisku bezpieczeństwa", 20-22 maja 2013, Chlewiska 2013.

[20] P. Skopiński, P. Zaskórski, *CRM as integration environment of the process organization*, Federated Conference on Computer Science and Information Systems/ FedCSIS, „Informatyka Ekonomiczna", Prace Naukowe UE we Wrocławiu, Wrocław, Poland, 9-12 September 2012, s. 10/5.

Głównym celem systemu jest zwiększenie bezpieczeństwa obywateli oraz ograniczenie strat spowodowanych występowaniem zagrożeń naturalnych, technologicznych oraz synergicznych (szczególny nacisk położono na zagrożenie powodziowe). Cel ten może być osiągnięty poprzez wyszczególnienie terenów zagrożonych powodzią i ograniczenie w tych obszarach ekspansji gospodarczej. ISOK ma łączyć informacje o zagrożeniach i umieszczać je w bazach danych z możliwością ich rozpowszechniania. System powinien zapewnić dostęp do tych informacji zarówno dla administracji, jak i obywateli. ISOK docelowo ma wyeliminować problem wieloszczeblowego zarządzania kryzysowego w Polsce poprzez skuteczne i nowoczesne narzędzia efektywnego administrowania służbami, które są odpowiedzialne za bezpieczeństwo kraju w przypadku wystąpienia sytuacji kryzysowych. System składa się z:

- jednego centralnego węzła znajdującego się w Instytucie Meteorologii i Gospodarki Wodnej, który obsługuje wszystkich odbiorców danych i usług na wszystkich szczeblach administracyjnych w państwie,
- czterech Centrów Modelowania Powodziowego CMP oraz z Systemu Informatycznego Gospodarki Wodnej SIGW. Udostępnianie usług sieciowych odbywać się będzie w architekturze SOA (ang. *Service Oriented Architecture*) oraz usług zgodnych z dyrektywą INSPIRE[21].

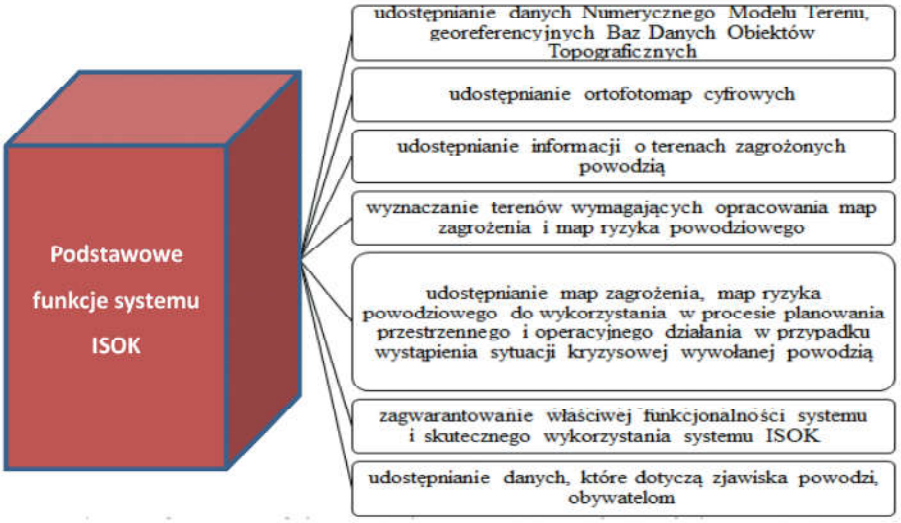
Zakłada się, że system ISOK usprawni funkcjonowanie jednostek zarządzania kryzysowego na każdym szczeblu administracji publicznej. Dodatkowo ISOK zwiększy dostęp obywateli i przedsiębiorstw do informacji w przypadku wystąpienia sytuacji kryzysowej zagrażającej zdrowiu, życiu lub mieniu obywateli, wprowadzając interoperacyjność funkcjonowania służb i jednostek administracji[22]. Praktycznym celem systemu ISOK jest stworzenie platformy systemowej do poprawy osłony obywateli, gospodarki oraz środowiska przed skutkami powodzi i innymi nadzwyczajnymi zagrożeniami. Osiągnięcie celu będzie możliwe dzięki opracowaniu produktów projektu i udostępnieniu ich obywatelom poprzez system informatyczny ISOK (rys. 3). Głównym źródłem danych topograficznych dla systemu ISOK są bazy danych prowadzone przez Główny Urząd Geodezji i Kartografii. W jego zasobach znajduje się duża ilość aktualizowanych na bieżąco danych, w tym:

- Baza Danych Ogólnogeograficzna BDO;
- Baza Danych Obiektów Topograficznych BDOT;
- Państwowy Rejestr Granic PRG;
- Ortofotomapy cyfrowe, skany map topograficznych oraz dane o charakterze katastralnym[23].

[21] http://projektisok.imgw.pl/o-projekcie/czym-bedzie-system-ISOK (26.08.2015). *Czym będzie system ISOK?*

[22] Ibidem.

[23] http://www.kzgw.gov.pl/files/file/Zamowienia_publiczne/20131216-uslugi-doradcze/Zalacznik-nr-2-do-SOPZ-Studium-wykonalnosci-cz-1.pdf (24.07.2015). Studium wykonalności dla projektu



Rys. 3. Ogólna koncepcja struktury zadaniowo-funkcjonalnej systemu ISOK
Źródło: opracowanie własne na podstawie http://www.kzgw.gov.pl/files/file/Zamowienia_publiczne/20131216-uslugi-doradcze/Zalacznik-nr-2-do-SOPZ-Studium-wykonalnosci-cz-1.pdf (24.07.2015 r.). Studium wykonalności dla projektu w ramach VII osi priorytetowej Programu Operacyjnego Innowacyjna Gospodarka, Projekt Informatyczny System Osłony Kraju przed nadzwyczajnymi zagrożeniami, s. 17

Jedną z podstawowych potrzeb obywateli jest zapewnienie poczucia bezpieczeństwa. Stąd też tylko zintegrowany i efektywny System Zarządzania Kryzysowego może zminimalizować skutki występujących zagrożeń. Poczucie bezpieczeństwa społeczeństwa można wzmocnić poprzez bieżące udostępnianie informacji o zagrożeniach zarówno organom administracji publicznej, jak i obywatelom. Sprawna organizacja oraz działania edukacyjne dotyczące sposobu korzystania z przekazywanych w tym systemie informacji mogą zaspokoić potrzeby społeczeństwa w tym zakresie. System ISOK może przyczynić się do rozwiązania wielu problemów, między innymi właściwego planowania przestrzennego w kontekście zagrożeń hydrologicznych i meteorologicznych[24]. Realizacja projektu systemu ISOK skutkuje już dziś wieloma różnorodnymi produktami, takimi jak:

1) Identyfikacja krajowych systemów informatycznych oraz baz danych umożliwiających monitorowanie, gromadzenie, przetwarzanie, analizowanie, dystrybucję i składowanie danych o zagrożeniach na potrzeby systemu ISOK.

w ramach VII osi priorytetowej Programu Operacyjnego Innowacyjna Gospodarka, Projekt Informatyczny System osłony kraju przed nadzwyczajnymi zagrożeniami.

[24] http://www.kzgw.gov.pl/files/file/Zamowienia_publiczne/20131216-uslugi-doradcze/Zalacznik-nr-2-do-SOPZ-Studium-wykonalnosci-cz-1.pdf (24.07.2015 r.), op. cit., s. 21-22.

2) Platforma informatyczna ISOK składająca się z kilku komponentów logicznych, czyli węzła centralnego, czterech Centrów Modelowania Powodziowego oraz Systemu Informatycznego Gospodarki Wodnej.
3) Numeryczny model rzeźby i pokrycia terenu NMT będący kluczowym produktem niezbędnym do oceny ryzyka powodziowego i zarządzania nim. Produkt ten zostanie wzbogacony o dodatkowe elementy strukturalne z wykorzystaniem metod bezpośrednich (metody fotogrametryczne, metody geodezyjne), które zapewnią dokładniejsze analizy i prognozy (np. wały przeciwpowodziowe, obiekty inżynieryjne itp.).
4) System zarządzania NMT realizujący import danych, przetwarzanie danych, zarządzanie danymi, eksport danych oraz tworzenie modeli.
5) Georeferencyjna Baza Danych Obiektów Topograficznych, która jest spójną, zharmonizowaną, jednolitą, opartą na jednym modelu danych referencyjną bazą danych dla systemu ISOK i innych systemów przestrzennych niezbędnych do prawidłowego funkcjonowania organów administracji publicznej.
6) Ortofotomapa cyfrowa jako planowany produkt typu wysokorozdzielcza ortofotomapa cyfrowa, uzupełniona danymi z PZGIK, będąca źródłem danych topograficznych do wykonania map z warstwą analityczną i referencyjną w systemie ISOK.
7) Pomiar korytowych przekrojów poprzecznych rzek jako dane bazowe do analizy i modelowania transformacji wezbrania powodziowego. Dzięki temu możliwe jest monitorowanie zmian hydromorfologicznych w korytach rzek.
8) Mapy zagrożeń meteorologicznych, które zawierają zarówno analizę bieżącą, jak i historyczną. Analiza bieżącej sytuacji meteorologicznej opracowywana jest w oparciu o model prognostyczny dotyczący najbliższych sześciu, dwunastu i dwudziestu czterech godzin. Mapy te przedstawiają prawdopodobieństwo wystąpienia przekroczenia wartości w odniesieniu do danych zawartych w mapach historycznych.
9) Mapy innych zagrożeń bazujące na ocenie prawdopodobieństwa wystąpienia zagrożeń dla zdrowia i życia ludności z uwagi na warunki meteorologiczne i społeczną wrażliwość na różne zagrożenia (w tym ujęcia wód powierzchniowych i podziemnych na obszarach zagrożonych niebezpieczeństwem powodzi, zanieczyszczenie powietrza z uwagi na zagrożenia meteorologiczne, ryzyko awarii przemysłowej lub zakłóceń w sieci elektroenergetycznej z uwagi na zagrożenia meteorologiczne itp.).
10) Mapa podziału hydrograficznego Polski MPHP (rys. 4) w skali 1 : 10 000 jako podstawowa mapa położenia geometrycznego obiektów liniowych i powierzchniowych (rzeki, kanały, jeziora, zbiorniki wodne).
11) Wstępna ocena ryzyka powodziowego to dokument planistyczny, który zawiera informacje o obszarach, dla których ryzyko powodziowe na terenie

Polski jest duże lub wystąpienie powodzi jest prawdopodobne. Dokument ten zawiera: mapy obszarów dorzeczy, opis powodzi historycznych, ocenę prognozowanych prawdopodobnych negatywnych skutków powodzi, prognozę dłuższego rozwoju wydarzeń z uwzględnieniem wpływu zmiany klimatu na rozwój powodzi.

Rys. 4. Mapa podziału hydrograficznego Polski
Źródło: http://geoportal.kzgw.gov.pl/imap

12) Mapy zagrożenia powodziowego zawierają obszary o różnej intensywności zagrożeń powodzią, w tym prawdopodobieństwo niskie (co najmniej raz na 500 lat) oraz obszary z prawdopodobieństwem średnim (raz na 100 lat) i wysokim (raz na 10 lat), a także obszary między wałem przeciwpowodziowym lub naturalnym wysokim brzegiem a linią brzegu. Mapy te zostały przygotowane zgodnie z dyrektywą INSPIRE i ustawą Prawo wodne oraz innymi wytycznymi.

13) Mapy ryzyka powodziowego wykonano dla obszarów o wysokiej ocenie zagrożenia i ryzyka powodziowego, które zostały zidentyfikowane we wstępnej ocenie ryzyka powodziowego dla obszarów przedstawionych na mapach zagrożenia powodziowego. Zaznaczono na nich takie elementy jak szacunkowa liczba mieszkańców, których może dotknąć powódź, rodzaje działalności gospodarczej występujące na tych obszarach, obecność instalacji, które w przypadku wystąpienia powodzi mogą spowodować zanieczyszczenie środowiska, strefy ochronne i miejsca ujęć wody oraz obszary ochronne zbiorników wód śródlądowych, obszary Natura 2000, kąpielisk, parków narodowych, rezerwatów przyrody itp.
14) Portal internetowy przeznaczony dla społeczeństwa spełniający potrzeby szkoleniowo-informacyjne i skutecznej komunikacji ze społeczeństwem. Portal będzie pełnić funkcję edukującą społeczeństwo w zakresie wykorzystania systemu ISOK, zagrożeń, sposobów przygotowania się i reagowania na dany rodzaj zagrożenia, a także o sposobach pomagających usunąć skutki wystąpienia zagrożeń. Docelowo uruchomione zostanie forum dyskusyjne pozwalające na zbiór opinii i uwag do proponowanych rozwiązań.

Pełne wdrożenie systemu ISOK wymaga przeprowadzenia specjalistycznych szkoleń dla użytkowników systemu w zakresie wykorzystania uzyskanych produktów i ich rozwoju[25]. Projekt ISOK w latach 2009-2015 wymagał nakładów w wysokości około 300 milionów złotych. Wartość rozwiązań wynika z korzyści społecznych, które zostaną dzięki niemu osiągnięte, przede wszystkim ograniczenie ofiar w ludziach spowodowanych klęskami żywiołowymi oraz ograniczenie kosztów związanych z wystąpieniem takich zagrożeń, usprawnienie działań organów zarządzania kryzysowego czy zwiększenie poczucia bezpieczeństwa obywateli. Trudne jest całościowe zidentyfikowanie wszystkich korzyści wynikających z realizacji projektu[26], ale zaakcentowano pozytywne aspekty realizacji tego projektu i długoterminową przydatność rezultatów dla użytkowników końcowych. Jako główną i podstawową korzyść wdrożenia systemu przyjmuje się poprawę bezpieczeństwa obywateli Polski, a także zminimalizowanie gospodarczych skutków zagrożeń przez ich bieżące monitorowanie i prognozowanie oraz planowanie przeciwdziałania.

Zastosowanie nowoczesnych rozwiązań teleinformatycznych w projekcie ISOK[27] zapewni rozwojowość jego produktów. Dzięki udostępnianiu usług sieciowych

[25] http://www.kzgw.gov.pl/files/file/Zamowienia_publiczne/20131216-uslugi-doradcze/Zalacznik-nr-2-do-SOPZ-Studium-wykonalnosci-cz-1.pdf (24.07.2015). Studium wykonalności dla projektu w ramach VII osi priorytetowej Programu Operacyjnego Innowacyjna Gospodarka, Projekt Informatyczny System osłony kraju przed nadzwyczajnymi zagrożeniami.
[26] Ibidem, s. 17.
[27] Ibidem, s. 139-144.

w architekturze SOA (ang. *Service Oriented Architecture*) oraz usług zgodnych z dyrektywą INSPIRE uzyska się elastyczność oraz większą dostępność systemu i większą odporność na awarie[28]. System ISOK przetwarza dane tekstowe, liczbowe, bitmapowe (pliki w formacie TIFF, JPG), wektorowe oraz geoprzestrzenne przy założeniu wydajnego przetwarzania wszystkich zasadniczych typów danych w jednym czasie, co zapewnia architektura SOA. Koncepcja ISOK jako systemu otwartego może być wzorcem projektowym systemu zintegrowanego monitorowania innych zagrożeń, zapewniającego ciągłość działania[29].

5. Warunki i standardy ciągłości działania w środowisku GIS

Ciągłość działania[30] jest jednym z atrybutów bezpieczeństwa państwa i społeczeństwa. Ciągłość procesu monitorowania zagrożeń należy więc uznać za bazową determinantę sprawności i skuteczności systemów zarządzania kryzysowego, przy czym ciągłość informacyjna jest istotnym warunkiem ciągłości działania tych systemów. Stały dostęp do zasobów utrzymywanych w systemach klasy GIS podnosi poziom funkcjonalności systemów zarządzania kryzysowego. Zapewnianie informacyjnej ciągłości działania wymaga stałego monitorowania stanu (rys. 5):

- zasobów organizacyjnych oraz „produktów" zarządzania (plany, procedury, formalna struktura działania);
- zasobów ludzkich, które stanowią najbardziej newralgiczny i podatny na zagrożenia element systemu informacyjnego, a ich znaczenie należy postrzegać przede wszystkim w kontekście sposobu definiowania i bieżącej oceny realizacji zadań;
- zasobów techniczno-ekonomicznych, które determinują sposób działania i zapewniania bezpieczeństwa przy efektywnym wykorzystaniu potencjału techniczno-technologicznego i bieżącego monitorowania jego stanu;
- procedur prawnych określających prawa i ograniczenia systemu zarządzania kryzysowego w uwarunkowaniach zewnętrznych i wewnętrznych oraz normy i standardy dostępu do danych i innych systemów (np. GIS).

[28] http://projektisok.imgw.pl/o-projekcie/czym-bedzie-system-ISOK (26.08.2015). *Czym będzie system ISOK?*, op. cit.

[29] D. Żbik, *Koncepcja monitorowania zagrożeń z wykorzystaniem systemów informacji geograficznej*, WAT, praca magisterska pod kier. P. Zaskórskiego, Warszawa 2016.

[30] P. Zaskórski (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, Wyd. WAT, Warszawa 2011, s. 229.

Rys. 5. Uwarunkowania zapewnienia informacyjnej ciągłości działania w organizacji. Opracowanie własne

Problem informacyjnej ciągłości działania wiąże się bezpośrednio z bezpieczeństwem informacyjnym/informatycznym i należy odnieść to także do systemów klasy GIS oraz uwzględnić standardy i normy typu:

- ISO 22301:2012 jako normę opisującą System zarządzania ciągłością działania, w której dokonano uporządkowania i wyszczególnienia kluczowych czynników ryzyka oraz uprządkowania procedur odtwarzania i przywracania możliwości realizacji kluczowych procesów po wystąpieniu zakłócenia ciągłości działania;
- British Standard BS 25999 *Business Continuity Management* jako normę bazującą na dobrych praktykach oraz specyfikującą zawartość programu zarządzania ciągłością działania[31], a w szczególności ujęcie systemowe zapewnienia ciągłości działania z opisem zasad planowania, wdrażania, wykorzystania, rozwijania, testowania i dokumentacji programu utrzymania ciągłości działania;
- ISO/PAS 22399:2007, *Societal security – Guideline for incident preparedness and operational continuity management*, gdzie definiuje się podstawy budowy kompleksowego systemu zarządzania w aspekcie wystąpienia incydentów;
- PN-ISO/IEC 17799:2005, *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji*, gdzie przedstawia się zalecenia i zasady w zakresie zarządzania bezpieczeństwem informacji, w tym założenia dotyczące polityki bezpieczeństwa informacji, zasad organizacji systemu z uwzględnieniem uwarunkowań personalnych, fizycznych i środowiskowych oraz infrastrukturalnych, zarządzania incydentami oraz pozyskiwania, rozwijania i utrzymania systemów informacyjnych (w tym GIS);
- NIST *Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems*, gdzie kluczowym elementem tego standardu

[31] *BS 25999-1:2006. Code of Practice, BS 25999-2:2007. Specification for Business Continuity Management.*

są założenia dotyczące tworzenia planów ciągłości działania oraz innych planów awaryjnych;
- NFPA 1600. *Standard on Disaster / Emergency Management and Business Continuity Programs*. 2010 Edition, czyli amerykański standard tworzony przez Narodowe Stowarzyszenie ds. Ochrony Przeciwpożarowej (NFPA). Istnieją tu obligatoryjne zapisy dotyczące polityki utrzymania ciągłości działania dla instytucji państwowych oraz organizacji typu non profit. Podobnie jak w przypadku BS 25999, omawiany standard określa również zasady implementacji, testowania, weryfikacji i doskonalenia programu ciągłości działania.

Należy zaznaczyć, że przedstawiony katalog stanowi jedynie część unormowań w rozważanym zakresie. W tym miejscu warto wspomnieć o normie PN-IEC 62198:2005 *Zarządzanie ryzykiem przedsięwzięcia. Wytyczne stosowania* – gdzie dokonano uporządkowania treści związanych z problematyką zarządzania ryzykiem, a także wielu innych publikacji w tym Zbiorze Dobrych Praktyk w zakresie Zarządzania Ciągłością Działania – opracowanym przez Business Continuity Institute. W przedmiotowym obszarze rozważań należy uwzględnić ciągłość procesów monitorowania zagrożeń z wykorzystaniem systemów GIS jako platformy współdziałania systemów informatycznych wspomagających procesy zarządzania kryzysowego.

6. Zakończenie

Współpraca systemów wszystkich służb zaangażowanych w procesy zarządzania kryzysowego ujawnia różne ograniczenia w możliwościach integracji informacyjnej systemów przetwarzania informacji geoprzestrzennej. Duża grupa systemów przetwarzających jedynie dane geograficzne może stanowić podstawę do przenoszenia tej klasy usług do chmury obliczeniowej. Jako zasadnicza grupa danych obejmujących informacje operacyjne, istotne z punktu widzenia systemów reagowania kryzysowego, wymaga dodatkowego przygotowania do procesów integracyjnych. Jak wykazują badania – przy zachowaniu i przestrzeganiu standardów modelowania obiektów operacyjnych – istnieje możliwość ujednolicenia modeli stosowanych dla obiektów geograficznych i wykorzystania ich dla obiektów operacyjnych. W ten sposób można posiłkować się wspólnymi standardami do przetwarzania danych geoprzestrzennych, czego przykładem może być system ISOK.

Dynamiczny rozwój usług w chmurze obliczeniowej[32] umożliwia dostęp do różnych systemów GIS. Dla systemów zarządzania kryzysowego jest to ważne wyzwanie, biorąc pod uwagę mobilność i skalowalność usług oraz możliwość adaptacyjnego

[32] P. Zaskórski, G. Pokorski, *Chmura obliczeniowa w systemach reagowania kryzysowego w aspekcie dostępu do danych geoprzestrzennych*, Międzynarodowa konferencja naukowa *Polska w europejskim środowisku bezpieczeństwa*, 20-22 maja 2013, Chlewiska 2013.

dopasowywania adekwatnych technologii informatycznych do potrzeb użytkowników[33] z zachowaniem kryterium ciągłości monitorowania zagrożeń.

LITERATURA

1. Bielecka E., *Systemy informacji geograficznej. Teoria i zastosowania*, Wydawnictwo PJWSTK, Warszawa 2005.
2. Gotlib D., Iwaniak A., Olszewski R., *GIS. Obszary zastosowań*, Wydawnictwo Naukowe PWN, Warszawa 2007.
3. http://www.kzgw.gov.pl/files/file/Zamowienia_publiczne/20131216-uslugi-doradcze/Zalacznik-nr-2-do-SOPZ-Studium-wykonalnosci-cz-1.pdf (24.07.2015). Studium wykonalności dla projektu w ramach VII osi priorytetowej Programu Operacyjnego Innowacyjna Gospodarka, Projekt Informatyczny System osłony kraju przed nadzwyczajnymi zagrożeniami.
4. http://projektisok.imgw.pl/o-projekcie/czym-bedzie-system-ISOK (26.08.2015 r.). Czym będzie system ISOK?
5. Litwin L., Myrda G., *Systemy Informacji Geograficznej. Zarządzanie danymi przestrzennymi w GIS, SIT, LIS*, Wydawnictwo Helion, Gliwice 2005.
6. PN-ISO/IEC 27001, *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania,* PKN, Warszawa 2007, pkt 3.4.
7. Pokorski G., Zaskórski P., *Wykorzystanie geodanych systemów dowodzenia i zarządzania w systemie bezpieczeństwa narodowego*, Konferencja naukowa nt. *Bezpieczeństwo – ujęcie kompleksowe*, Katowice – 31 maja 2012 r., s. 12, 18/8.
8. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 listopada 2011 r. w sprawie bazy danych obiektów topograficznych oraz bazy danych obiektów ogólnogeograficznych, a także standardowych opracowań kartograficznych.
9. Serafin M., *Wirtualizacja w praktyce*, Helion, Gliwice 2012.
10. Skopiński P., Zaskórski P., *CRM as integration environment of the process organization*, Federated Conference on Computer Science and Information Systems/ FedCSIS, „Informatyka Ekonomiczna" Prace Naukowe UE we Wrocławiu, Wrocław, Poland, 9-12 September 2012, s. 10/5.
11. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. nr 89, poz. 590 z późn. zm.
12. Zaskórski P., *Asymetria informacyjna w zarządzaniu procesami*, Redakcja Wydawnictw Wojskowej Akademii Technicznej, Warszawa 2012, s. 285.
13. Zaskórski P., *Wirtualizacja organizacji w „chmurze" obliczeniowej*, „Ekonomika i Organizacja Przedsiębiorstwa", nr 3/2012, Wyd. ORGMASZ, Warszawa 2012, s. 12.
14. Zaskórski P. (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, Redakcja Wydawnictw Wojskowej Akademii Technicznej, Warszawa 2011, s. 229.

[33] P. Zaskórski, *Asymetria informacyjna w zarządzaniu* procesami, op. cit.

15. Zaskórski P., Pokorski G., *Chmura obliczeniowa w systemach reagowania kryzysowego w aspekcie dostępu do danych geoprzestrzennych*, Międzynarodowa Konferencja Naukowa *Polska w Europejskim Środowisku Bezpieczeństwa*, 20-22 maja 2013, Chlewiska 2013.
16. Żbik D., *Koncepcja monitorowania zagrożeń z wykorzystaniem systemów informacji geograficznej*, WAT, praca magisterska pod kier. P. Zaskórskiego, Warszawa 2016.

THREAT MONITORING BY USING GEOGRAPHICAL INFORMATION SYSTEMS

Abstract. The article discusses the ability of using GIS systems to monitor threats in crisis management systems within meeting the information continuity criteria. Authors are trying to judge ability of using GIS systems (data and geolocation services) as a integration platform for crisis management systems operations. Development of ISOK system may result in quality, scalability, accessibility and security improvement of crisis management systems.
Keywords: management, crisis management, system, geodata.