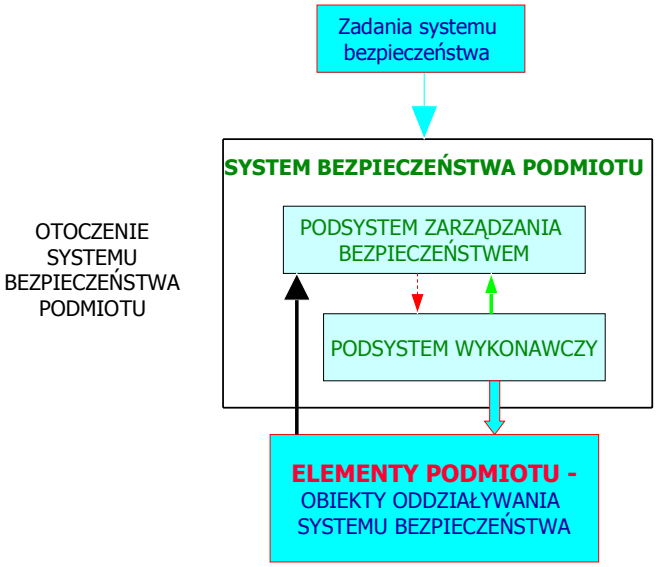
Dr hab. inż. Edward Kołodziński prof. UWM
Katedra Informatyki Stosowanej WNT
Uniwersytet Warmińsko –Mazurski w Olsztynie
www.uwm.edu.pl/kis ekolodzinski@wp.pl

ISTOTA INŻYNIERII SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM

1. Wprowadzenie

Już od najdawniejszych czasów człowiek próbuje podporządkować sobie środowisko naturalne, wprowadzając w nim zmiany umożliwiające mu nie tylko egzystencję i zapewniające komfort życia, ale również zwiększające jego bezpieczeństwo. Stara się uniezależnić od nieprzyjaznego oddziaływania na niego sił natury.

Zmiany wnoszone przez człowieka w przestrzeni naturalnej nazywane są **cywilizacją**. Określają ją wytwory, służące poprawie warunków życia oraz kontroli natury, tj. technika, organizacja życia społecznego, infrastruktura itp. Cywilizacja zmniejsza liczbę i niszczycielską siłę zagrożeń naturalnych, lecz jednocześnie generuje nowe rodzaje zagrożeń cywilizacyjnych. Z powyższego wynika, że człowiek żyje i będzie żył w środowisku **potencjalnych zagrożeń bezpieczeństwa**, które to uaktywnione wskutek niekorzystnych dla niego zmian w przestrzeni naturalnej lub cywilizacyjnej mogą zamienić się w określonego rodzaju, tj. dziedzinowe (powodziowe, pożarowe, chemiczne, epidemiologiczne itp.) **zagrożenia realne – zdarzenia** i w ich następstwie stany niekorzystne dla jego życia bądź zdrowia, czy też środowiska. Oznacza to, że stan bezpieczeństwa podmiotu (obiektu, zakładu, instytucji, aglomeracji) nie jest stanem stabilnym - nie jest dobrem danym podmiotowi raz na zawsze. W świecie realnym występują ciągłe jego zagrożenia, zarówno od sił natury jak i niezamierzonych i zamierzonych skutków działalności człowieka. Każdy podmiot musi, zatem czynić starania o zapewnienie sobie stabilności stanu bezpieczeństwa. W tym celu tworzony jest **system bezpieczeństwa podmiotu** (Rys. 1), który stanowi zespół sił i środków zapewniających akceptowalny przez niego stan bezpieczeństwa**.**



Rys. 1. Model systemu bezpieczeństwa podmiotu

2. Analiza czynników wpływających na bezpieczeństwo podmiotu

Celem działania systemu bezpieczeństwa podmiotu jest zapewnienie mu: stanu pewności, spokoju, uzasadnionego przekonania o braku istotnie szkodliwych dla niego następstw możliwych do wystąpienia zagrożeń. Poszczególne rodzaje zagrożeń mogą występować i oddziaływać na podmiot jednocześnie, zaś ich skutki nakładać się na siebie, a nawet może występować efekt ich *synergii,* która w analizie globalnego bezpieczeństwa podmiotu nie powinna być pomijana.

Analizę czynników wpływających na bezpieczeństwo podmiotu rozpatrywać będziemy poprzez ich wpływ na **poziom dziedzinowego bezpieczeństwa podmiotu**. Na jego wartość możemy wpływać przede wszystkim poprzez:

- zapobieganie powstawaniu danego rodzaju zagrożenia bezpieczeństwa;
- przygotowanie techniczno – organizacyjne podmiotu na wypadek uaktywnienia się zagrożenia jego bezpieczeństwa (tzn. zajścia zdarzenia). Do przedsięwzięć z tym związanych zaliczymy, między innymi: zapewnienie dostępności podmiotu do działań sił i środków systemu bezpieczeństwa (przejezdność dróg dojazdowych, oznakowanie i dostępność do wyłączników odcinających media, wyjścia awaryjne itp.), zapewnienie możliwości szybkiej ewakuacji ludzi i ich dobytku do miejsc uprzednio przygotowanych itd.;
- permanentne, upowszechnianie wiedzy o zagrożeniu (jego przyczynach, przebiegu, skutkach, sposobie zapobiegania mu itp.) wśród wszystkich tych, których może ono dotknąć;
- zwiększanie skuteczności sił i środków wykonawczych systemu bezpieczeństwa w przeciwdziałaniu skutkom danego zdarzenia. Osiąga się to, przede wszystkim, zapewniając odpowiednio:
  - ilościowe i jakościowe ich wyposażenie;
  - optymalne ich rozmieszczenie względem źródeł zagrożeń i elementów osłanianych;
  - permanentne doskonalenie sił [6, 9] w zakresie racjonalnego wykorzystania właściwości techniczno – taktycznych sprzętu ratowniczego itp.;
- zwiększanie skuteczności działań w usuwaniu następstw danego zdarzenia po jego opanowaniu.

Mamy, zatem możliwość kształtowania poziomu bezpieczeństwa dziedzinowego, a przez to i ogólnego. Wielkościami sterowalnymi w tym przypadku są parametry charakteryzujące czynniki wpływające na poziom bezpieczeństwa podmiotu, tj. związane z:

- zapobieganiem powstawaniu możliwych dla niego zagrożeń bezpieczeństwa;
- przygotowaniem podmiotu na wypadek uaktywnienia tych zagrożeń;
- reagowaniem w przypadku jego uaktywnienia (zajścia zdarzenia);
- usuwaniem następstw danego zdarzenia.

Z powyższych rozważań wynika możliwość **zarządzania poziomem bezpieczeństwa podmiotu**, zarówno dziedzinowego jak i ogólnego. Do jego realizacji niezbędne są następujące rodzaje informacji (Rys. 2):

- geodane infrastrukturalne obszaru podmiotu i jego otoczenia;
- dane operacyjne o siłach i środkach możliwych do użycia w przypadku wystąpienia zagrożenia bezpieczeństwa podmiotu;
- informacje o aktualnym stanie zagrożeń.

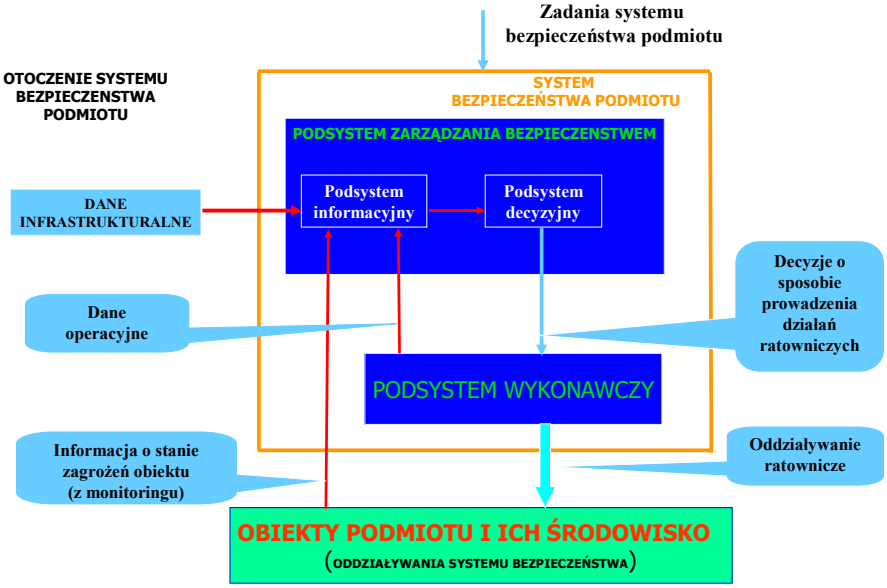
Geodane infrastrukturalne systemu bezpieczeństwa, to dane o rzeźbie i obiektach naturalnych obszaru podmiotu i jego otoczenia, infrastrukturze podziemnej i naziemnej oraz obiektach terenowych o istotnym znaczeniu dla planowania i prowadzenia działań

ratowniczych, a także prognozowania i likwidacji skutków katastrof, klęsk żywiołowych i innych nadzwyczajnych zagrożeń. Na geodane infrastrukturalne składają się: dane graficzne zawarte w mapie numerycznej obszaru oraz dane opisowe charakteryzujące wyróżnione na niej obiekty – istotne z punkt widzenia podsystemu decyzyjnego, stanowiącego o przedsięwzięciach zapewniających bezpieczeństwo podmiotu.

Dane operacyjne o siłach i środkach dysponowanych przez system bezpieczeństwa, to dane o siłach i środkach, które potencjalnie mogą być przez niego użyte w działaniach ratowniczych oraz w eliminowaniu skutków wyzwolonego zagrożenia. Przykładowymi elementami tego zasobu mogą być dane o: stanach osobowych jednostek organizacyjnych systemu, ich wyposażeniu technicznym, parametrach sprzętu, infrastrukturze obiektów własnych, a ponadto dokumentacje jednostek, zakresy obowiązków osób funkcyjnych, procedury postępowania w określonych sytuacjach, plany ratownicze itp.

Monitorowanie zagrożeń bezpieczeństwa podmiotu. Warunkiem koniecznym przeciwdziałania zdarzeniom, powodującym zagrożenia bezpieczeństwa podmiotu, jest ich przewidywanie, wykrywanie i identyfikacja (rozpoznanie). Dotyczy to zarówno rodzaju jak i wielkości zdarzenia. Od informacji o aktualnym stanie możliwych zagrożeń bezpieczeństwa podmiotu [4] uzyskiwanej z systemów monitoringu [1] zależy rodzaj i ilość środków użytych do przeciwdziałania ich skutkom, a także sposób prowadzenia działań ratowniczych.
Sposób monitorowania rodzaju i stopnia zagrożeń oraz wykrywania i identyfikacji zdarzeń przez nie spowodowanych zależy od ich natury, tj. fizyko – chemicznego oddziaływania na człowieka i środowisko. Abstrahujemy tu od przyczyn, czy są to zagrożenia naturalne czy też cywilizacyjne, a wśród nich celowo powodowane przez określone grupy ludzi – terrorystów.

Na podstawie informacji z monitoringu zagrożeń podmiotu podsystem informacyjny, posługując się modelami matematycznymi i programowymi symulatorami, opracowuje prognozy i scenariusze możliwego rozwoju zdarzeń.



Rys. 2. Potrzeby informacyjne zarządzania bezpieczeństwem podmiotu

Jakość danych infrastrukturalnych, operacyjnych i informacji o zagrożeniach – ich kompletność, aktualność i komunikatywność udostępniania podsystemowi decyzyjnemu ma istotny wpływ na trafność podejmowanych przez niego decyzji o sposobie prowadzenia działań ratowniczych przez podsystem wykonawczy, a stąd i na skuteczność zapewnienia bezpieczeństwa podmiotowi.

Podejmowanie decyzji, zwane również **dysponowaniem sił i środków**, poprzedzane jest czynnościami przeddecyzyjnymi, tj. analizą i oceną sytuacji powstałej w wyniku zajścia

zdarzenia oraz prognozą jej rozwoju. Czas i jakość ich wykonywania (szczegółowość analizy sytuacji, liczba uwzględnianych czynników, wiarygodność prognoz itp.) zależy od zakresu i sposobu komputerowego wspomagania [7]. Sprawą niezwykle istotną jest zatem odpowiednie, techniczno – programowe wyposażenie stanowisk pracy osób funkcyjnych podsystemów zarządzania bezpieczeństwem oraz stworzenie im przyjaznego środowiska i organizacji pracy [8], zapewniających podejmowanie optymalnych decyzji.

Z przeprowadzonej, nie w pełni wnikliwie, analizy wynika, że zapewnienie podmiotowi określonego poziomu bezpieczeństwa uwarunkowane są możliwościami techniczno – programowego **(inżynierii)** „uzbrojenia" człowieka we wszystkich fazach przeciwdziałania zagrożeniom – od wykrywania, identyfikacji, opracowywania obrazu aktualnych zagrożeń i prognozy ich rozwoju, analizy i oceny sytuacji, podejmowanie decyzji o działaniach pomniejszających ich skutki i realizację tych decyzji. Przykładowe moduły funkcjonalne biblioteki programowej systemu komputerowego wspomagania zarządzania bezpieczeństwem PREVENT, a w szczególności: analizy i oceny stanu zagrożenia podmiotu oraz podejmowania decyzji o sposobie prowadzenia działań ratowniczych i reagowania kryzysowego, podano w [5]. Zawiera ona, między innymi, moduły:

- wyznaczania miejsc ustawienia blokad drogowych;
- wyznaczania stref izolacji wokół miejsc w których występuje zagrożenie;
- wyznaczania strefy rozprzestrzeniania TŚP oraz miejsc pożądanego ustawienia blokad dostępu;
- lokalizacji zaworów które należy zamknąć w przypadku zagrożenia;
- wyznaczania obszarów zalewowych na podstawie mapy terenu;
- wyznaczania stref widoczności na podstawie mapy rzeźby terenu z uwzględnieniem rzeczywistej przejrzystości powietrza;
- optymalizacji tras dojazdu pod względem odległości lub czasu dojazdu z uwzględnieniem rodzaju pojazdu;
- oceny bezpieczeństwa dostaw gazu w warunkach zagrożeń terrorystycznych;
- itd.

3. Organizacja zapewnienia bezpieczeństwa podmiotom

System bezpieczeństwa danego podmiotu powinien być dostosowany do jego potencjalnych zagrożeń oraz pożądanego poziomu jego bezpieczeństwa. Zatem ilość i jakość sił i środków ratownictwa, niezbędnych do zapewnienia danemu podmiotowi pożądanego poziomu bezpieczeństwa, ich organizacja oraz sposób prowadzenia działań ratowniczych, po wyzwoleniu zagrożenia (zajściu zdarzenia), zależy od jego rodzaju i skali oraz prognozy możliwości implikowania przez niego wystąpienia również innych rodzajów zagrożeń. Uwzględniając powyższe wyróżnia się dwa rodzaje systemów bezpieczeństwa:

- **system ratownictwa** – to zespół sił i środków, którego zadaniem jest przeciwdziałanie skutkom określonych rodzajów zdarzeń;
- **system zarządzania kryzysowego** – to zespół sił i środków odpowiedzialny za zapewnienie podmiotowi bezpieczeństwa przy wystąpieniu zdarzeń, których skutków nie można wyeliminować siłami ratownictwa bez zastosowania nadzwyczajnych regulacji prawnych, np. wprowadzenia któregoś ze stanów nadzwyczajnych [10].

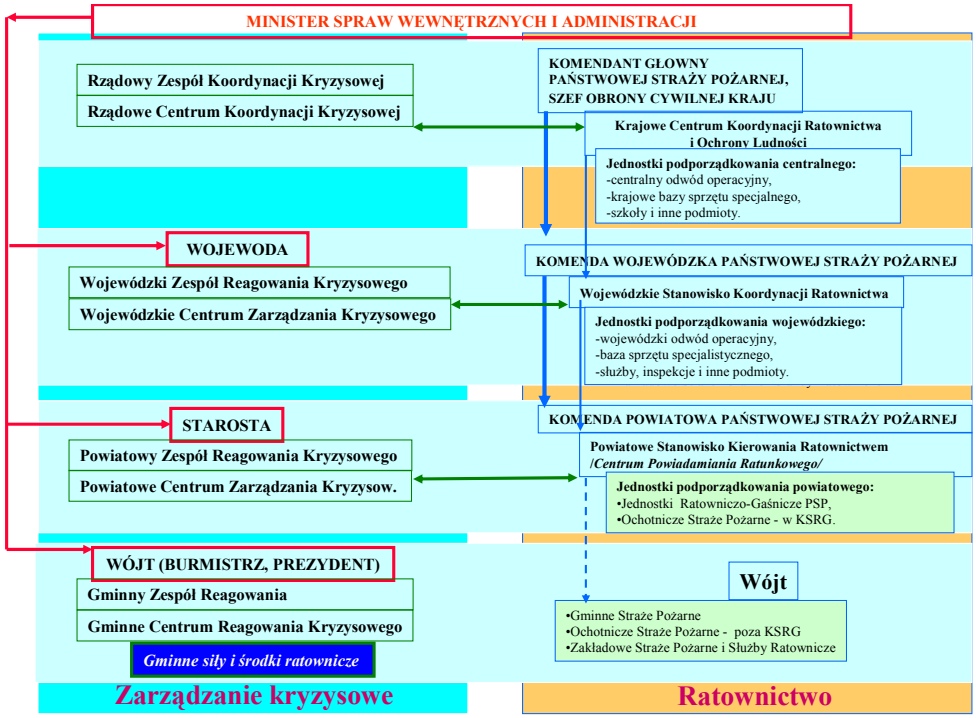
Zatem w zależności od wielkości zdarzenia mamy do czynienia z ratownictwem bądź reagowaniem kryzysowym. Możliwe sytuacje przedstawiono na Rys. 3.

Krajowy system bezpieczeństwa jest systemem dziedzinowym. Wyróżniamy takie systemy dziedzinowe jak: system ratowniczo – gaśniczy, ratownictwo medyczne, ratownictwa specjalistyczne itp. Systemy dziedzinowe mają strukturę hierarchiczną – w większości

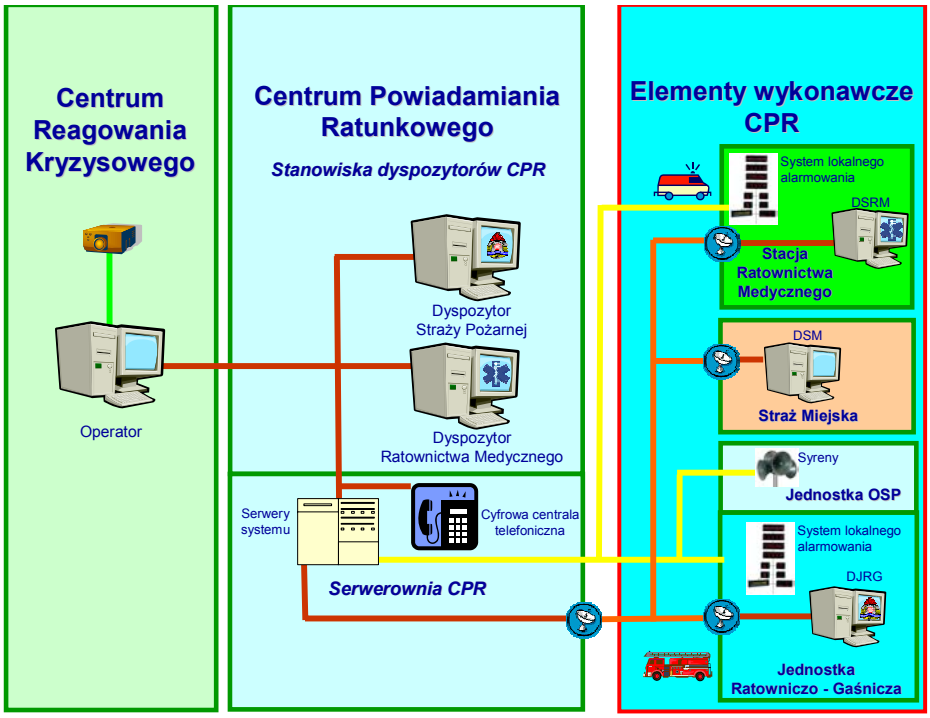
przypadków dostosowaną do struktury administracyjnej kraju. Model systemu bezpieczeństwa z wyróżnieniem ratownictwa (realizowanego przez Państwową Straż Pożarną) i zarządzania kryzysowego przedstawiono na Rys. 4. Elementem spinającym te dwa systemy jest Centrum Powiadamiania Ratunkowego (Rys. 5). Potrzeby informacyjne kierowania ratownictwem i zarządzania kryzysowego przedstawiono na Rys. 6 i Rys. 7.

Zwraca się uwagę, że dla wyróżnionych poziomów hierarchicznych systemów ratownictwa i zarządzania kryzysowego zasoby informacji (geodanych) infrastrukturalnej i operacyjnej (Rys. 6 i Rys. 7) nie są tożsame. Praktycznie potrzeby informacyjne zarządzania kryzysowego są większe niż ratownictwa.

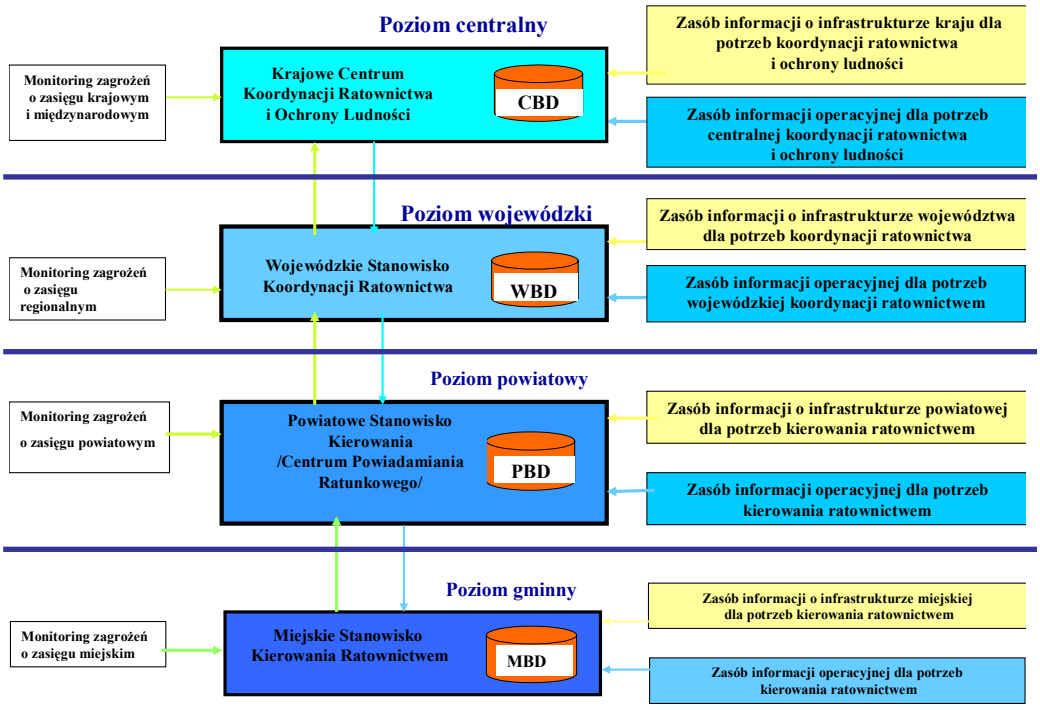
Rys. 3. Możliwe sposoby reagowania na zajście zdarzenia wymagającego prowadzenia działań ratowniczych



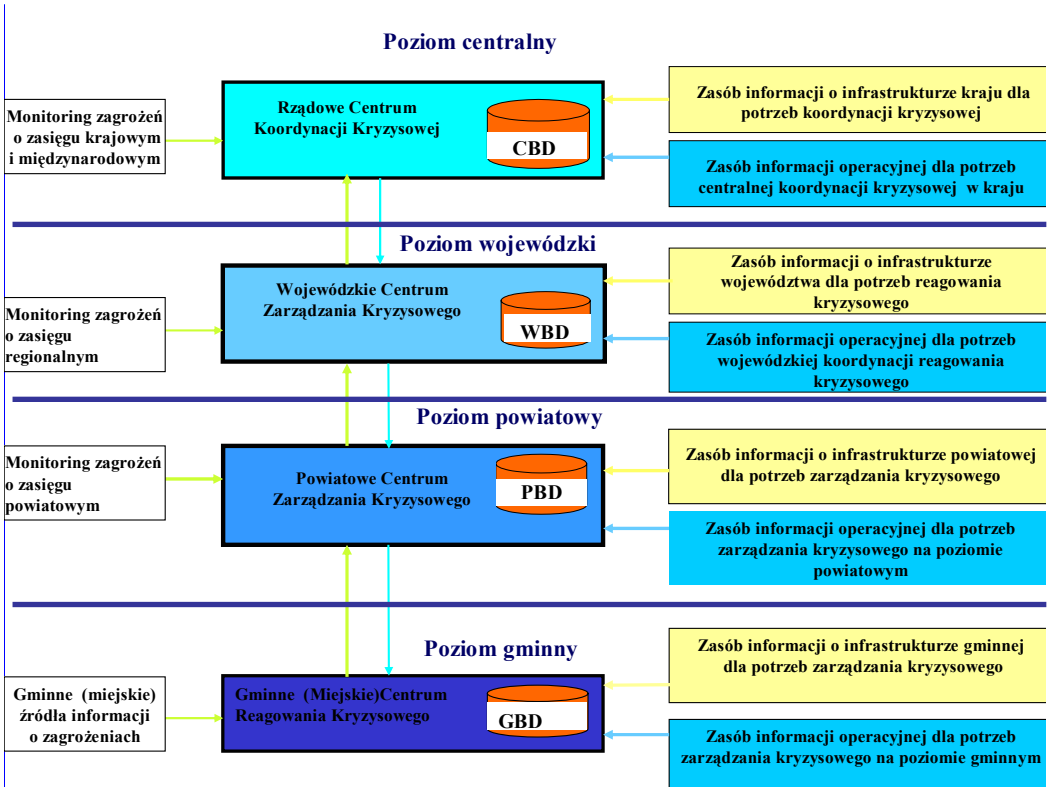
Rys. 4. Model struktury organizacyjnej krajowego systemu ratownictwa i zarządzania kryzysowego



Rys. 5. Model Zintegrowanego Systemu Miejskiego (Powiatowego) Centrum Ratownictwa i Reagowania Kryzysowego



Rys. 6. Potrzeby informacyjne hierarchicznego systemu kierowania ratownictwem



Rys. 7. Potrzeby informacyjne hierarchicznego systemu zarządzania kryzysowego

4. Podsumowanie

Bezpieczeństwo podmiotu (obiektu, zakładu, instytucji, aglomeracji, itd.) zależy od wielu czynników, które agregując można ująć, jako:

- zagrożenia;
- przygotowanie na nie podmiotu;
- system bezpieczeństwa – rozumiany jako zespół sił i środków zapewniających akceptowalny przez podmiot stan bezpieczeństwa.

Możliwość zapewnienia podmiotowi akceptowalnego przez niego stanu bezpieczeństwa wymaga, między innymi, wiedzy a priori: o naturze zagrożeń i możliwościach ich rozpoznawania za pomocą aktualnie dostępnych środków, które to mogą być użyte do tworzenia podsystemu monitoringu w systemie bezpieczeństwa. Podsystem monitoringu jest źródłem informacji dla podsystemu informacyjnego (Rys. 2) o aktualnym stanie zagrożeń podmiotu. Informacja ta uzupełniona geodanymi o infrastrukturze podmiotu i jego otoczenia oraz danymi operacyjnymi podsystemu wykonawczego stanowi podstawę do podejmowania decyzji o sposobie przeciwdziałania zdarzeniu.

Wymieniona, przyczynowo-skutkowa, sekwencja operacji informacyjno – decyzyjnych wskazuje na potrzebę kompleksowego podejścia do doskonalenia procesów realizowanych przez podsystem zarządzania, poprzez racjonalną ich automatyzację. Drogą do jej ustalenia jest tzw. modelowanie biznesowe, zaś narzędziem do jego realizacji może być język UML [11]. Analiza przypadków użycia jest doskonałym sposobem ustalenia poziomu i zakresu komputerowego wspomagania zarządzania bezpieczeństwem podmiotu.

5. Literatura

1. Bielecki Z.: Monitoring zagrożeń bezpieczeństwa. XIII Konferencja Naukowa nt. „Automatyzacja dowodzenia", Kraków 11-13 maja 2005 rok http://www.infocorp.com.pl/html/zarz_monitoring.htm
2. Kołodziński E.: Zabezpieczenie informacyjne ratownictwa i reagowania kryzysowego. XII Konferencja Naukowa nt. „Automatyzacja dowodzenia", Gdynia-Jurata 02-04 czerwca 2004 rok http://www.infocorp.com.pl/html/zarz_7.htm
3. Kołodziński E., Betliński G.: Wykorzystanie map numerycznych we wspomaganiu kierowania działaniami ratowniczymi. Przegląd Pożarniczy nr 3/2004 rok http://www.infocorp.com.pl/html/zarz_10.htm
4. Kołodziński E.: Zagrożenie bezpieczeństwa i organizacja przeciwdziałania ich skutkom XII Konferencja Naukowa nt. „Automatyzacja dowodzenia", Gdynia-Jurata 02-04 czerwca 2004 rok http://www.infocorp.com.pl/html/zarz_8.htm
5. Kołodziński E.: Inżynieria systemów zarządzania bezpieczeństwem. Wykład. http://www.infocorp.com.pl
6. Kołodziński E. i inni: Zastosowanie e-learningu do doskonalenia zawodowego służb dyżurnych ratownictwa na stanowiskach pracy. III Międzynarodowa Konferencja Naukowa Zarządzanie Kryzysowe nt. „Bezpieczeństwo i ochrona statków morskich" , Akademia Morska w Szczecinie, Szczecin 24-25 czerwca 2005 rok, http://www.infocorp.com.pl/html/zarz_elearning.htm
7. Kołodziński E.: Komputerowe wspomaganie procesów informacyjno-decyzyjnych ratownictwa. II Konferencja Naukowa Zarządzanie Kryzysowe nt. "Ratownictwo w sytuacjach kryzysowych", Akademia Morska w Szczecinie, Szczecin 18 czerwca 2004 rok. http://www.infocorp.com.pl/html/zarz_11.htm
8. Kołodziński E., Donigiewicz A.: Ergonomiczne aspekty w projektowaniu zautomatyzowanych systemów zarządzania bezpieczeństwem. XIII Konferencja Naukowa nt. „Automatyzacja dowodzenia", Kraków 11-13 maja 2005 rok http://www.infocorp.com.pl/html/zarz_ergo.htm
9. Kołodziński E. Kowalski A.: Zastosowanie symulatorów programowych do szkolenia i doskonalenia zawodowego osób funkcyjnych stanowisk kierowania ratownictwem. XI Warsztaty Naukowe PTSK Symulacja w Badaniach i Rozwoju, Białystok 1-4 września 2004 rok, http://www.infocorp.com.pl/html/zarz_6.htm
10. Kołodziński E. Inżynieria systemów zarządzania bezpieczeństwem. Opracowanie wewnętrzne. PPW INFOKART S.A. Warszawa 2005 rok
11. Schmuller J.: UML dla każdego. Helion. 2003 rok

Streszczenie

W referacie dokonano analizy czynników wpływających na bezpieczeństwo podmiotu i możliwości wpływania na jego poziom, między innymi, poprzez doskonalenie: monitoringu zagrożeń i procesów informacyjno – decyzyjnych realizowanych przez podsystem zarządzania bezpieczeństwem. Sposobem doskonalenia jest wdrażanie do systemów monitoringu zagrożeń [1] czujników i urządzeń pomiarowych o coraz lepszych właściwościach użytkowych oraz zwiększanie poziomu i zakresu komputerowego wspomagania zarządzania bezpieczeństwem.

Referat ma charakter przeglądowy. Wskazuje pozycje literaturowe, w których poszczególne zagadnienia są przedstawione bardziej szczegółowo.

Abstract

The paper covers an analysis of factors influencing the security of the subject and possibility of it's level changing by , among others, mastering of hazards monitoring and information – decisive processes done by a security management subsystem [1]. The mastering is the introducing of "state of the art" sensors and measurement devices, as well as, the computer aided security management level and scope increasing. The paper is a review mostly, pointing literature describing in detail specific topics mentioned here in.