Modelowanie wymagań na Dziedzinowe Systemy Bezpieczeństwa Podmiotu

dr hab. inż. Edward Kołodziński, prof. WAT
Instytut Optoelektroniki WAT

Abstracts

W pracy przedstawiono metodę wyznaczania wymagań na Dziedzinowe Systemy Bezpieczeństwa Podmiotu, bazującą na modelowaniu obiektowym z zastosowaniem języka UML. Na podstawie modelu biznesowego podmiotu określane są rodzaje zagrożeń jego funkcjonowania. Dla tak zidentyfikowanych zagrożeń opracowywane są modele biznesowe i analityczne Dziedzinowych Systemów Bezpieczeństwa Podmiotu. Na ich podstawie ustalane są pożądane właściwości tych systemów. Ich znajomość umożliwia wyznaczenie realizowalnych wymagań na te systemy dla danych nakładów i dopuszczalnego czasu jego wykonania.

Keywords:

unit, unit/individual safety, safety individual system, personal safety

podmiot, bezpieczeństwo podmiotu, system bezpieczeństwa podmiotu, wymagania na dziedzinowe systemy bezpieczeństwa podmiotu

Geneza modelowania systemów bezpieczeństwa podmiotu

Naturalnym dążeniem człowieka jest permanentna poprawa komfortu życia. Tworzy on nowe urządzenia, maszyny, środki transportu, źródła energii, systemy zaopatrzenia, usprawnia rozwiązania organizacyjne życia społecznego, doskonali metody ochrony przed zagrożeniami naturalnymi i cywilizacyjnymi. Stara się zmniejszać ich niszczycielską siłę.

Cywilizacja łagodzi skutki zagrożeń, lecz jednocześnie generuje nowe ich rodzaje.Wynika z tego, że człowiek żyje i będzie żył w środowisku potencjalnych zagrożeń bezpieczeństwa. Ich uaktywnienie wskutek niekorzystnych zmian w przestrzeni naturalnej i/lub cywilizacyjnej może powodować: powodzie, pożary, epidemie, niezadowolenia społeczne itp. Oznacza to, że stan bezpieczeństwa podmiotu (np. człowieka, obiektu, zakładu, instytucji,

aglomeracji, rejonu, grupy społecznej itp.) nie jest stanem stabilnym. Zmienia się pod wpływem niekorzystnych oddziaływań zarówno ze strony sił natury, jak i niezamierzonych, a czasem destrukcyjnych działań człowieka. Aby zapewnić bezpieczeństwo funkcjonowania podmiotu, tworzony/doskonalony jest dla niego ***System Bezpieczeństwa Podmiotu (SBP).***

Bezpieczeństwo funkcjonowania podmiotowi SBP można zapewnić poprzez skuteczne:

- *zapobieganie* powstawaniu zagrożeń,
- *reagowanie* na występujące zagrożenia, tzn. podejmowanie takich działań, które minimalizują ich niekorzystne skutki.

Skuteczność działania SBP zarówno w zakresie zapobiegania zagrożeniom, jak i reagowania w przypadku ich wystąpienia zależy od [4,5]:

- ***potencjału wykonawczego tego systemu,*** o którego wielkości stanowi, przede wszystkim:
  - stan sił podsystemu wykonawczego: liczebność, sprawność, poziom wyszkolenia, motywacja do działania, organizacja przedsięwzięć reagowania na zdarzenia itp.,
  - stan środków – wyposażenie techniczne podsystemu wykonawczego i jego dostosowanie do potrzeb wynikających z potencjalnych zagrożeń oraz wrażliwości na nie podmiotu,
  - dyslokacja sił i środków, uwzględniająca rodzaj i miejsce prognozowanych zdarzeń, ich skalę oraz pożądaną szybkość reakcji na zaistniałe zdarzenie. Możliwa do uzyskania szybkość przystąpienia do działań zadysponowanych sił i środków ratownictwa na zaistniałe zdarzenie zależy przede wszystkim od: odległości ich dyslokacji od miejsca zdarzenia, możliwości ich przemieszczania do miejsca jego wystąpienia oraz właściwości taktyczno-technicznych dysponowanych środków;
- ***potencjału informacyjno-decyzyjnego systemu,*** o wielkości którego stanowi przede wszystkim:
  - wiedza i umiejętności osób funkcyjnych zarządzających potencjałem wykonawczym;
  - organizacyjno-ergonomiczne uwarunkowania działania osób funkcyjnych systemu bezpieczeństwa,
  - zakres i poziom techniczno-programowego wspomagania procesów informacyjno- decyzyjnych wykonywanych w systemie.

Zadanie zapewnienia bezpieczeństwa funkcjonowania podmiotu realizowane jest zazwyczaj przy:

- ograniczonych nakładach,
- ograniczonym czasie na stworzenie warunków do jego zapewnienia.

W tych uwarunkowaniach jest ono trudne do wykonania, a często wręcz niemożliwe. Z analizy literatury i doświadczeń własnych autora wynika, że w znacznej części przedsięwzięć, mających na celu zapewnienie pożądanego poziomu bezpieczeństwa podmiotu, przekraczane są dopuszczalne nakłady i/lub czasy ich realizacji, a nawet przerywane są prace nad nimi z powodu bardzo znacznego ich przekroczenia. Podejmując przedsięwzięcia zapewnienia bezpieczeństwa funkcjonowania podmiotu, niezwykle istotna jest wiedza o przyczynach takiego stanu rzeczy i o tym, jaki jest w tym udział poszczególnych etapów ich realizacji. Nieznane są autorowi dane ilościowe z przedmiotowych badań. Dostępne są natomiast w literaturze wyniki badań nad przyczynami niepowodzeń w przedsięwzięciach informatycznych, które to można z dużą zasadnością odnieść do doskonalenia skuteczności działania SBP – zwłaszcza poprzez zwiększanie zakresu komputerowego wspomagania realizacji procesów informacyjno-decyzyjnych zarządzania bezpieczeństwem i kierowania ratownictwem.

Według danych literaturowych odnoszących się do systemów informatycznych:

- ponad 25% przedsięwzięć jest przerywanych z powodu bardzo znacznego przekroczenia wyasygnowanych na ten cel środków oraz limitu czasowego, a także nieuzyskiwania pożądanych ich właściwości na etapie projektowania i wdrażania,
- w ponad 50% przedsięwzięć projektowo-wdrożeniowych przekraczany jest termin i budżet ich wykonania.

Z badań nad przyczynami niepowodzeń przedsięwzięć informatycznych wynika, że w około:

- 56% ich przyczyną są niepoprawnie ustalone wymagania co do sposobu ich realizacji,
- 26% przyczyną niepowodzeń są błędy popełnione na etapie projektowania rozwiązań,
- 7% niepowodzeń przedsięwzięć wynika z błędów popełnionych na

etapie wykonawstwa,

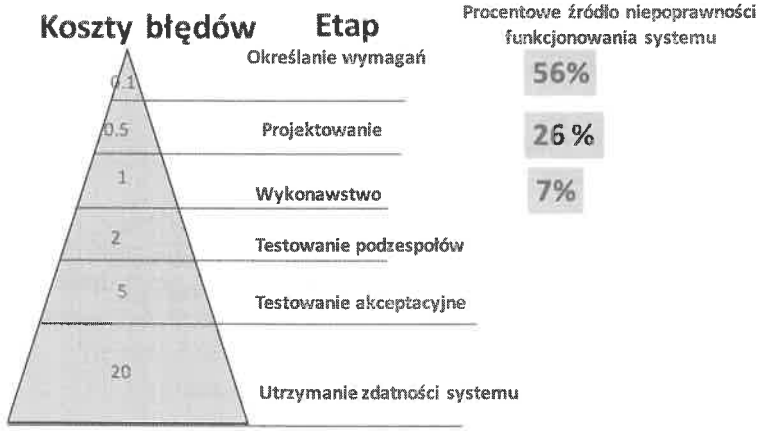
- 11% niepowodzenia wynikają z błędów popełnionych przy realizacji innych etapów.

Niezwykle ważna jest znajomość relacji między stratami w zależności od tego, w jakim etapie cyklu życia systemu wykrywane są nietrafności wymagań na jego właściwości funkcjonalne i niefunkcjonalne. Przyjmując za podstawową jednostkę straty z tytułu wykrycia niepoprawności w ustalaniu wymagań odnośnie do określonych właściwości na etapie wykonawstwa systemu, dla systemów informatycznych, szacuje się, że wynoszą one odpowiednio, dla (rys.1.):

- określania wymagań – 0.1;
- projektowania – 0.5;
- testowania podzespołów (modułów funkcjonalnych) –2.0;
- scalania podzespołów w system i przyrostowe jego testowanie akceptacyjne – 5.0;
- użytkowania – 20.

Z porównania powyższych danych wynika, że przykładowo, jeżeli określona niepoprawność wymagań na system zostanie wykryta podczas jego użytkowania, to straty będą 200 razy większe, niż gdyby została ona wykryta podczas określania wymagań.

Rys.1. Straty powodowane przez niepoprawne określenie wymagań na system w zależności od etapu cyklu życia systemu, w którym zostaną one wykryte



Źródło: opracowanie własne

Z analizy częstości występowania niepoprawności w wymaganiach na system oraz błędów popełnianych podczas jego projektowania wynika jednoznacznie potrzeba doskonalenia sposobów realizacji tych etapów cyklu życia SBP – a przede wszystkim opracowania metod i środków programowych do ustalania i weryfikacji zasadności wymagań. Takim sposobem jest modelowanie SBP i prowadzenie badań jakości ich działania na tych modelach, np. metodą symulacji cyfrowej [2].

Identyfikacja zagrożeń bezpieczeństwa funkcjonowania podmiotu

Etapy identyfikacji zagrożeń

Jednym z podstawowych uwarunkowań funkcjonowania podmiotu (rys.2.) jest jego bezpieczeństwo [2].

Rys. 2. Pojęcie podmiotu.

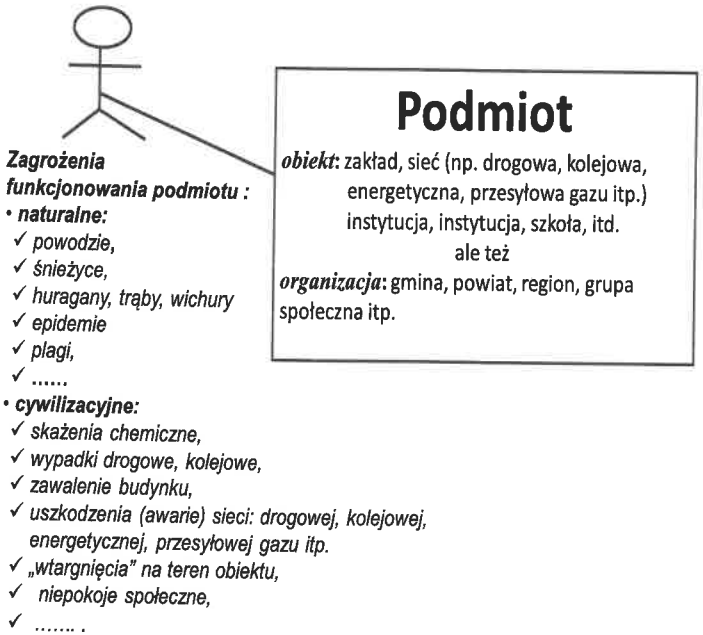
Podmiot

obiekt: zakład, sieć (np. drogowa, kolejowa, energetyczna, przesyłowa gazu itp.) instytucja, szkoła, itd.,
ale też
organizacja: gmina, powiat, region, grupa społeczna itp.

Źródło: opracowanie własne.

Bezpieczeństwo podmiotu nie jest stanem stabilnym– nie jest dobrem danym raz na zawsze. W świecie realnym występują permanentne zagrożenia jego funkcjonowania (rys.3.). Ich źródłem może być zarówno jego otoczenie, jak i sam podmiot.

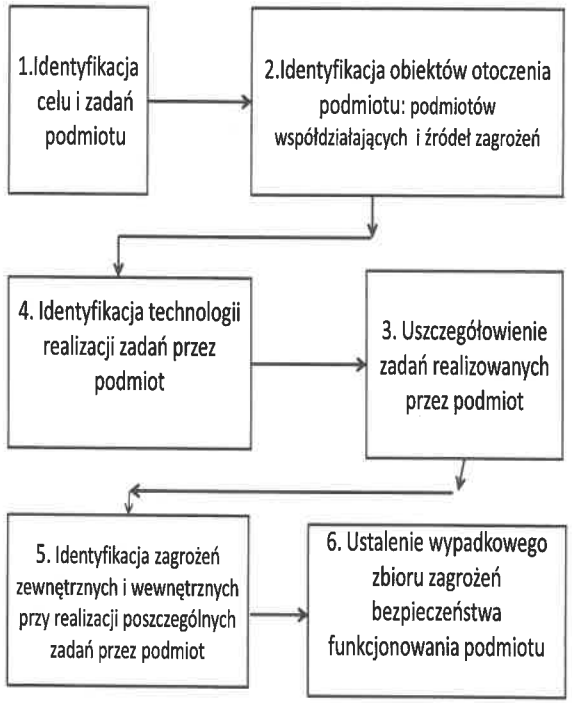
Rys.3. Zagrożenia funkcjonowania podmiotu.



Źródło: opracowanie własne.

Warunkiem koniecznym podjęcia działań nad zapewnieniem pożądanego poziomu bezpieczeństwa jego funkcjonowania jest ustalenie rodzajów zagrożeń i ich charakterystyk. Technologię identyfikacji zagrożeń przedstawiono na rys. 4.

Rys. 4. Etapy identyfikacji zagrożeń bezpieczeństwa funkcjonowania podmiotu.



Źródło: opracowanie własne.

Modelowanie dynamiki podmiotu na potrzeby identyfikacji zagrożeń bezpieczeństwa jego funkcjonowania

Podstawowe rodzaje modeli obiektowych stosowanych w identyfikacji zagrożeń bezpieczeństwa funkcjonowania podmiotu

W poprzednim punkcie, na rys. 4., przedstawiono etapy identyfikacji

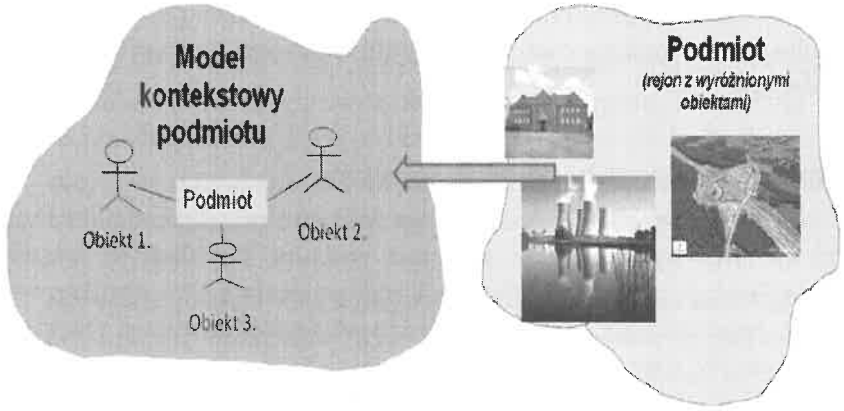
zagrożeń bezpieczeństwa funkcjonowania podmiotu. W realizacji etapu drugiego bardzo pomocny okazuje się model otoczenia podmiotu – w modelowaniu obiektowym [7,8] nazywany ***modelem kontekstowym podmiotu.*** Wykorzystywany jest on również do identyfikacji zewnętrznych zagrożeń bezpieczeństwa funkcjonowania podmiotu. W ustalaniu zbioru wewnętrznych zakłóceń i zagrożeń bezpieczeństwa funkcjonowania podmiotu przydatny jest model dynamiki jego funkcjonowania – w modelowaniu obiektowym nazywany ***modelem przypadków użycia podmiotu.*** Model przypadków użycia ułatwia również identyfikację efektywnych metod przeciwdziałania wyróżnionym zagrożeniom bezpieczeństwa funkcjonowania podmiotu.

Każdy podmiot realizuje zadania na rzecz otoczenia. Cel jego funkcjonowania określa przeznaczenie i zadania je uszczegóławiające. Jednakże technologie ich realizacji oraz wynikające z nich zapotrzebowanie na środki, materiały, różnego rodzaju media itp. generują zadania dodatkowe i potrzebę współdziałania z określonymi podmiotami, będącymi obiektami jego otoczenia. Rozszerza/modyfikuje/precyzuje to zakres zadań szczegółowych podmiotu i technologię ich realizacji. Fakt ten powoduje, że opracowywanie modelu kontekstowego i modelu przypadków użycia podmiotu odbywa się iteracyjnie.

Modelowanie otoczenia podmiotu

Każdy podmiot funkcjonuje w określonych uwarunkowaniach, wynikających ze środowiska, w szczególności zasad współdziałania z innymi podmiotami, stanowiącymi obiekty jego otoczenia. Zadania realizowane w ramach współdziałania z obiektami otoczenia mogą generować podmiotowi dodatkowe zadania do wykonania, a te z kolei również wyzwalać zagrożenia. Dlatego prace nad doskonaleniem bezpieczeństwa podmiotu powinny być rozpoczynane od opracowania modelu kontekstowego podmiotu. Przedstawia się w nim wzajemne oddziaływania podmiotu z obiektami otoczenia, w notacji umożliwiającej jednoznaczną identyfikację możliwych zagrożeń bezpieczeństwa jego funkcjonowania (rys.5.).

Rys.5. Modelowanie kontekstowe otoczenia podmiotu na potrzeby identyfikacji zagrożeń jego funkcjonowania



Źródło: opracowanie własne.

Na model kontekstowy podmiotu składa się:

1. *diagram kontekstowy*, przedstawiający podmiot w asocjacji z obiektami jego otoczenia,
2. *kontekstowa charakterystyka* tych obiektów.

Diagram kontekstowy podmiotu, w obiektowym modelowaniu jego otoczenia, graficznie przedstawia podmioty, z którymi jest on w asocjacji. Jest to komunikatywna forma prezentacji wzajemnego oddziaływania podmiotu z podmiotami będącymi obiektami jego otoczenia. Ułatwia uszczegółowienie współdziałania, a w kolejnym etapie zidentyfikowanie czynników kontekstualnych zagrożeń bezpieczeństwa jego funkcjonowania.

Kontekstowa charakterystyka obiektów otoczenia podmiotu powinna zawierać:

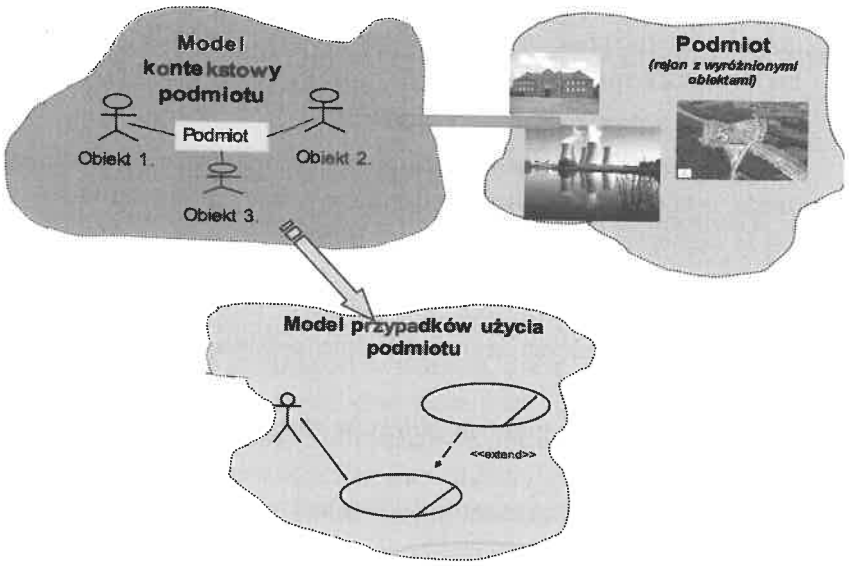
a. specyfikację zadań realizowanych w ramach współdziałania podmiotu z obiektami otoczenia,
b. częstość oraz formy i skale wzajemnych oddziaływań, a także wynikające z nich skutki zarówno dla podmiotu, jak i obiektów otoczenia,
c. informacje dotyczące wszelkich uwarunkowań mających wpływ na zakres i technologię zadań realizowanych przez podmiot.

Zawartość i szczegółowość charakterystyki kontekstowej podmiotu z obiektami otoczenia powinny być wystarczające do opracowania modelu dynamiki funkcjonowania podmiotu, nazywanego w obiektowym modelowaniu funkcjonowania podmiotu ***modelem przypadków użycia podmiotu.***

Modelowanie funkcjonowania podmiotu

Źródłem zagrożeń bezpieczeństwa funkcjonowania podmiotu może być nie tylko jego otoczenie, ale i sam podmiot. Implikuje to potrzebę szczegółowego poznania technologii wykonywania zadań wynikających z jego przeznaczenia oraz z uwarunkowań współdziałania z obiektami otoczenia. W tym celu opracowywany jest obiektowy model biznesowy (funkcjonalny) przypadków użycia podmiotu (rys.6.)

Rys. 6. Modelowanie funkcjonowania podmiotu dla potrzeb identyfikacji zagrożeń



Źródło: opracowanie własne.

Na ***model biznesowy przypadków użycia podmiotu*** składają się:

1. ***diagram przypadków użycia podmiotu***, wraz z ich szczegółową charakterystyką,
2. ***diagramy czynności*** dla wyróżnionych w modelu przypadków użycia podmiotu, wraz z ich szczegółową charakterystyką. Prezentują one technologię realizacji przypadków użycia,
3. ***diagramy interakcji*** – stosowane do przedstawienia zasad współdziałania między realizatorami przypadków użycia podmiotu, podczas ich wykonywania.

Zawartość modelu biznesowego przypadków użycia podmiotu, szczegółowość danych w nim ujętych oraz ich notacja powinny umożliwiać jednoznaczną identyfikację potencjalnych zagrożeń i zakłóceń bezpieczeństwa funkcjonowania podmiotu.

Modelowanie biznesowe podmiotu realizowane jest przez analityka bezpieczeństwa. W procesie identyfikacji technologii wykonywania zadań przez podmiot pomocne mogą okazać się, w szczególności, następujące techniki:

- obserwacja sposobu realizacji zadań przez jego podsystemy: wykonawczy i zarządzania/kierowania;
- bezpośredni udział w realizacji zadań podmiotu – przede wszystkim tych, przy wykonywaniu których występuje, potencjalnie, największe prawdopodobieństwo wystąpienia zagrożenia bezpieczeństwa jego funkcjonowania;
- metody eksperckie, w szczególności: delficka, Crawforda itp.;

Technologia identyfikacji zagrożeń bezpieczeństwa funkcjonowania podmiotu na podstawie jego modeli obiektowych

Zagrożenia bezpieczeństwa funkcjonowania podmiotu są wypadkową jego zagrożeń zewnętrznych i wewnętrznych. Podstawę do identyfikacji możliwości powstania zagrożeń zewnętrznych stanowi przede wszystkim jego model kontekstowy, a w szczególności zawarta w nim charakterystyka współdziałania podmiotu z obiektami otoczenia. Możliwości wystąpienia zagrożeń wewnętrznych bezpieczeństwa funkcjonowania podmiotu identyfikuje się, biorąc pod uwagę:

- diagramy czynności dla przypadków użycia podmiotu oraz ich szczegółową charakterystykę,

- diagramy interakcji – przedstawiające współdziałanie między realizatorami przypadków użycia podmiotu, podczas ich wykonywania.

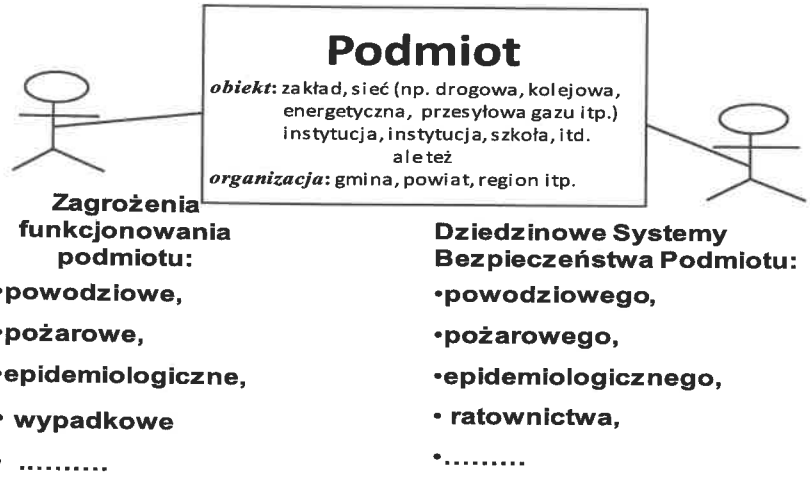
Analiza technologii wykonywania poszczególnych czynności danego przypadku użycia podmiotu oraz współdziałania między realizatorami tego przypadku użycia pozwala ustalić zbiór możliwych zagrożeń wewnętrznych w jego funkcjonowaniu. Suma zbiorów zagrożeń dla wyróżnionych przypadków użycia podmiotu stanowi wypadkowy zbiór jego zagrożeń wewnętrznych.

Bezpieczeństwo funkcjonowania podmiotu

Struktura Dziedzinowych Systemów Bezpieczeństwa Podmiotu

W celu zapewnienia stabilności stanu bezpiecznego funkcjonowania podmiotu tworzony jest ***System Bezpieczeństwa Podmiotu (SBP),*** którego składowymi są ***Dziedzinowe Systemy Bezpieczeństwa Podmiotu (DSBP)*** (rys.7.). Ich zadaniem jest zapobieganie wystąpieniu zagrożeń rodzajowych oraz reagowanie w przypadku ich wystąpienia. DSBP są systemami wirtualnymi. Tworzą je siły i środki wydzielane ze służb, inspekcji, administracji zespolonej, podmiotów itp., a także elementy składowe podmiotu. Bowiem, każdy podmiot powinien być w stanie ochraniać się do pewnego poziomu zagrożeń.

Rys.7. Diagram kontekstowy bezpieczeństwa funkcjonowania podmiotu

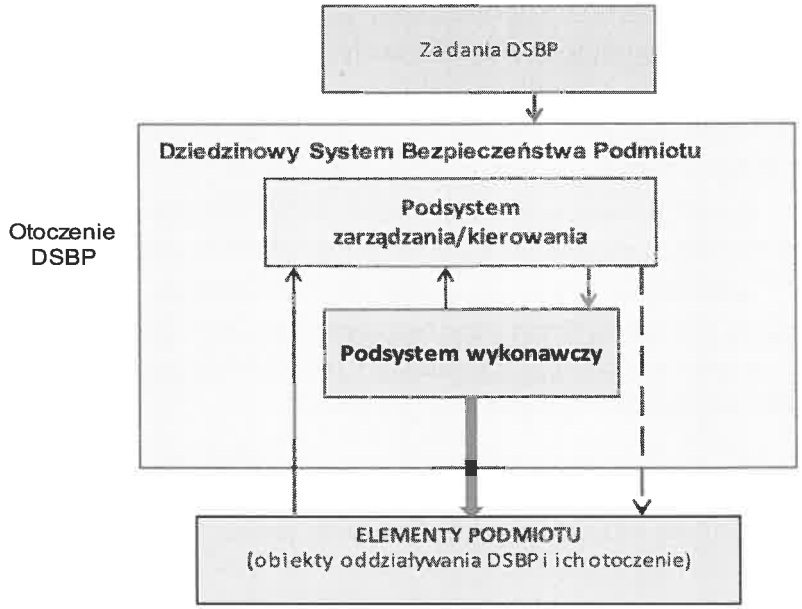


Źródło: opracowanie własne.

W cybernetycznym ujęciu DSBP (rys.8.) wyróżnia się dwa podsystemy:

- **wykonawczy**, który stanowią siły i środki realizujące procesy wykonawcze - wydzielone, np. ze straży pożarnej, ratownictwa medycznego, straży miejskiej, policji, pogotowia technicznego, itd.,
- **zarządzania/kierowania**, który realizuje procesy informacyjno-decyzyjne, stanowiące o sposobie zapewnienia podmiotowi bezpieczeństwa funkcjonowania przez podsystem wykonawczy.

Rys.8. Model Dziedzinowego Systemu Bezpieczeństwa Podmiotu.



Źródło: opracowanie własne.

Legenda do rys. 8.:

informacja robocza,

informacja sterująca,

oddziaływania wykonawcze.

W podsystemie zarządzania bezpieczeństwem podmiotu, z kolei, wyróżnia się dwa elementy składowe (rys.9.):

- podsystem informacyjny – odpowiedzialny za:

✓ wykrywanie, monitorowanie i prognozowanie zagrożeń funkcjonowania podmiotu,

✓ monitorowanie i ocenę stanu przygotowania podmiotu na wystąpienie zagrożeń,

✓ monitorowanie i ocenę stanu przygotowania podsystemu wykonawczego do przeciwdziałania zagrożeniom funkcjonowania podmiotu,

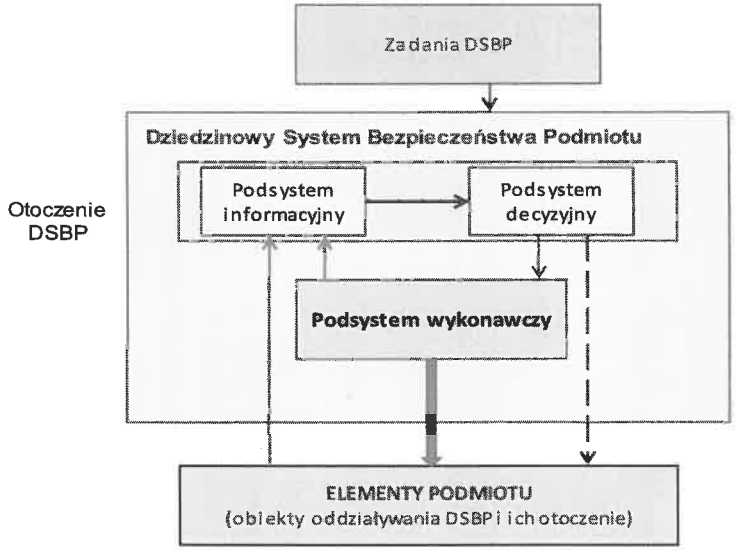
✓ opracowanie, na podstawie uzyskanych danych, obrazu stanu zagrożeń i uwarunkowań realizacyjnych niezbędnych do podejmowania decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu;

- ***podsystem decyzyjny*** – podejmujący decyzje o sposobie zapewnienia bezpieczeństwa podmiotu, na podstawie danych opracowanych przez podsystem informacyjny. Decyzje te precyzują:

✓ sposób prowadzenia działań przez podsystem wykonawczy SBP w poszczególnych etapach zarządzania bezpieczeństwem podmiotu,

✓ działania, jakie powinny podjąć obiekty podmiotu, we własnym zakresie, w celu zapewnienia sobie bezpieczeństwa funkcjonowania. Dotyczą one przede wszystkim zapobiegania zagrożeniom i przygotowania obiektów na wypadek wystąpienia tych zagrożeń.

Rys. 9. Uszczegółowienie podsystemu zarządzania bezpieczeństwem podmiotu .

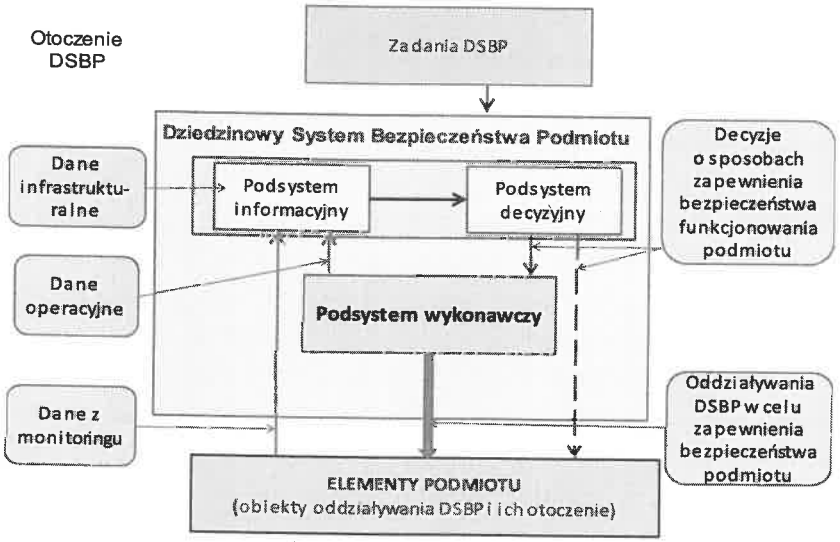


Źródło: opracowanie własne.

Wyróżnia się trzy rodzaje danych wykorzystywanych w podejmowaniu decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu (rys. 10.):

- *geodane infrastrukturalne,* to geodane (istotne z punktu widzenia zapewnienia podmiotowi bezpieczeństwa jego funkcjonowania) o i infrastrukturze i rzeźbie obszaru dyslokacji obiektów podmiotu i ich otoczenia,
- *dane operacyjne o siłach i środkach* możliwych do użycia w przypadku wystąpienia określonego rodzaju zagrożenia bezpieczeństwa podmiotu,
- *dane z monitoringu zagrożeń* bezpieczeństwa funkcjonowania podmiotu oraz czynników mających wpływ na ich stan.

Rys. 10. Przepływy danych i informacji sterującej w zarządzaniu bezpieczeństwem podmiotu



Źródło: opracowanie własne.

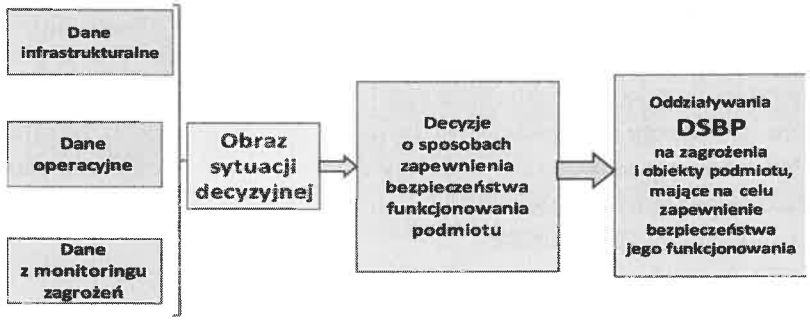
Technologia funkcjonowania Dziedzinowych Systemów Bezpieczeństwa Podmiotu

W ciągu technologicznym przedsięwzięcia zapewnienia bezpieczeństwa funkcjonowania podmiotu wyróżnia się następujące etapy (rys.11.):

1. pozyskiwanie danych niezbędnych do permanentnego opracowywania obrazu stanu bezpieczeństwa podmiotu, tj. o stanie:
   - ✓ *zagrożeń* – na podstawie danych z monitoringu,
   - ✓ *sił i środków* podsystemu wykonawczego DSBP,
   - ✓ *infrastruktury naziemnej i podziemnej* oraz o uwarunkowaniach terenowych istotnych z punktu widzenia zapewnienia bezpieczeństwa funkcjonowania podmiotu;
2. permanentne opracowywanie obrazu stanu bezpieczeństwa podmiotu na podstawie powyższych danych;
3. inicjowanie aktywności podsystemu decyzyjnego w przypadku zaistnienia stanu wymagającego działań podsystemu wykonawczego lub/ oraz podmiotu;

4. podejmowanie decyzji o sposobach zapewnienia bezpieczeństwa funkcjonowania podmiotu;
5. oddziaływania DSBP na zagrożenia i obiekty podmiotu, zapewniające bezpieczeństwo jego funkcjonowania.

Rys.11. Ilustracja ciągu technologicznego zapewnienia bezpieczeństwa funkcjonowania podmiotu



Źródło: opracowanie własne.

Warunkiem koniecznym skutecznego przeciwdziałania zdarzeniom powodującym zagrożenia bezpieczeństwa funkcjonowania podmiotu jest przewidywanie ich wystąpienia na podstawie określonych symptomów oraz ich wykrywanie i identyfikacja. Dane z monitoringu o aktualnym stanie zagrożeń stanowią podstawę do prognozowania o kierunku zmian i skutkach, jakie mogą one spowodować. Od stanu i prognozy zmian zagrożeń zależą decyzje odnośnie do sił i środków niezbędnych do przeciwdziałania im oraz o sposobie prowadzenia działań ratowniczych. Sposób monitorowania rodzaju i stopnia zagrożeń oraz wykrywania i identyfikacji zdarzeń przez nie powodowanych, a także czynników wpływających na skalę zagrożeń zależy od ich natury, tj. fizykochemicznych objawów i skutków. Abstrahuje się tu od przyczyn, czy są to zagrożenia naturalne czy też cywilizacyjne, a wśród nich celowo powodowane przez określone grupy ludzi, np. terrorystów.

Podsystem informacyjny (rys.10.), na podstawie danych z monitoringu zagrożeń bezpieczeństwa podmiotu oraz danych operacyjnych i infrastrukturalnych, posługując się modelami matematycznymi i programowy-

mi symulatorami, opracowuje prognozy i scenariusze możliwego rozwoju zdarzeń. Na ich podstawie opracowywany jest obraz sytuacji decyzyjnej, na podstawie którego podejmowana jest decyzja o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu. Jej trafność zależy od jakości danych z monitoringu zagrożeń, stanu sił i środków podsystemu wykonawczego oraz danych o infrastrukturze mającej istotne znaczenie dla bezpieczeństwa podmiotu.

Globalne bezpieczeństwo podmiotu jest wypadkową poszczególnych rodzajów bezpieczeństwa dziedzinowego. Jego zapewnienie jest problemem zazwyczaj złożonym, a stąd trudnym do rozwiązania. Zatem przed przystąpieniem do rozwiązywania problemu zapewnienia ustalonego poziomu globalnego bezpieczeństwa funkcjonowania podmiotu powinien on być zdekomponowany na problemy dziedzinowe i dla nich określone pożądane poziomy bezpieczeństwa. Ich wartości implikują właściwości, jakie powinny posiadać DSBP.

Etapy wstępnej identyfikacji pożądanych właściwości Dziedzinowych Systemów Bezpieczeństwa Podmiotu

Aktualny poziom bezpieczeństwa podmiotu zależy, przede wszystkim, od jego:

- zagrożeń zewnętrznych, generowanych przez obiekty otoczenia oraz uwarunkowania środowiskowe, w których funkcjonuje,
- zagrożeń i zakłóceń wewnętrznych, wynikających w szczególności z technologii realizacji zadań,
- wrażliwości na zagrożenia i zakłócenia, które mogą być generowane zarówno przez czynniki zewnętrzne (siły przyrody i obiekty otoczenia), jak i wewnętrzne, wynikające z procesów technologicznych działalności prowadzonej przez podmiot,
- skuteczności działania DSBP.

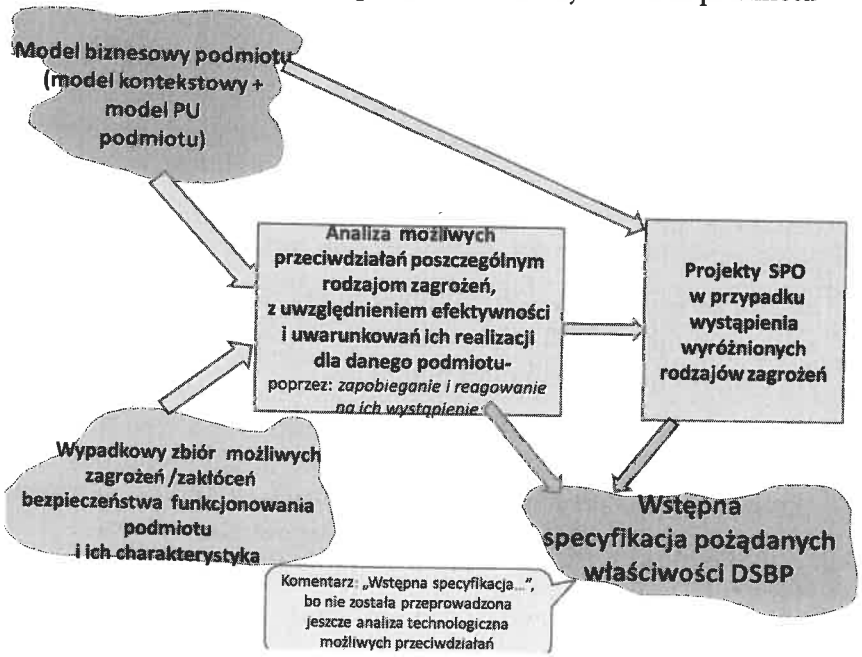
Pożądany poziom bezpieczeństwa funkcjonowania podmiotu zależy od przeznaczenia i roli, jaką ma on do spełnienia. Tego samego rodzaju podmioty mogą mieć różne wagi, np. w zależności od ich liczby w aglomeracji. W miarę jak będzie wzrastać ich liczba, można oczekiwać, że będzie maleć ich waga, a stąd i pożądany poziom bezpieczeństwa funkcjonowania każdego z nich może maleć.

Wymagania odnośnie do zapewnienia pożądanego poziomu bezpieczeństwa funkcjonowania podmiotu implikują pożądane właściwości DSBP. W celu ich ustalenia niezbędne jest:

1. określenie przeznaczenia oraz znaczenia podmiotu, np. dla społeczeństwa, gminy, powiatu, województwa, kraju, itd. i wynikających z nich wymagań odnośnie do trwałości i niezawodności jego funkcjonowania,
2. dokonanie identyfikacji zadań szczegółowych, realizowanych przez podmiot,
3. dokonanie wnikliwej analizy technologii realizacji zadań szczegółowych ukierunkowanych na identyfikację możliwości powstania zakłóceń i zagrożeń funkcjonowania podmiotu,
4. określenie zbioru podstawowych rodzajów zagrożeń bezpieczeństwa funkcjonowania podmiotu i ich skutków,
5. określenie charakterystyk zidentyfikowanych rodzajów zagrożeń, z uwzględnieniem skali i częstości ich występowania,
6. dokonanie analizy możliwości przeciwdziałania poszczególnym rodzajom zagrożeń, z uwzględnieniem uwarunkowań ich realizacji w przypadku danego podmiotu, poprzez: *zapobieganie i reagowanie na ich wystąpienie,*
7. opracowanie standardowych procedur operacyjnych (SPO) bezpieczeństwa podmiotu na wypadek wystąpienia wyróżnionych rodzajów zagrożeń.

Pożądany poziom bezpieczeństwa funkcjonowania podmiotu, możliwe zagrożenia, wrażliwości na nie podmiotu i sposób skutecznego przeciwdziałania im to podstawowe czynniki generujące pożądane właściwości DSBP. Dotyczą one zarówno zasobów podsystemu wykonawczego, jak i taktyki ich użycia oraz technologii i uwarunkowań czasowych na realizację procesów informacyjno-decyzyjnych przez podsystem zarządzania/kierowania. Wstępną identyfikację pożądanych właściwości DSBP dla ustalonego wypadkowego zbioru zagrożeń bezpieczeństwa funkcjonowania podmiotu przedstawiono na rys.11.

Rys.11. Wstępna identyfikacja pożądanych właściwości DSBP dla ustalonych zagrożeń bezpieczeństwa funkcjonowania podmiotu



Źródło: opracowanie własne.

Modelowanie Dziedzinowych Systemów Bezpieczeństwa Podmiotu na potrzeby identyfikacji pożądanych jego właściwości

Potrzeba modelowania Dziedzinowych Systemów Bezpieczeństwa Podmiotu

Bezpieczeństwo funkcjonowania podmiotu zapewnia się przez [3]:

1. ***zapobieganie*** powstawaniu poszczególnych rodzajów zagrożeń dziedzinowych (np. powodziowych, epidemiologicznych itp.),
2. ***przygotowywanie*** podmiotu i DSBP na ewentualność ich wystąpienia,
3. ***działania ratownicze*** w przypadku wystąpienia zagrożeń dziedzinowych,
4. ***likwidację*** skutków wystąpienia zagrożeń dziedzinowych.

Pożądany jego poziom można uzyskać na wiele sposobów w poszczególnych fazach zarządzania jego bezpieczeństwem. Zilustrujemy to na poniższym przykładzie [3].

Przykład

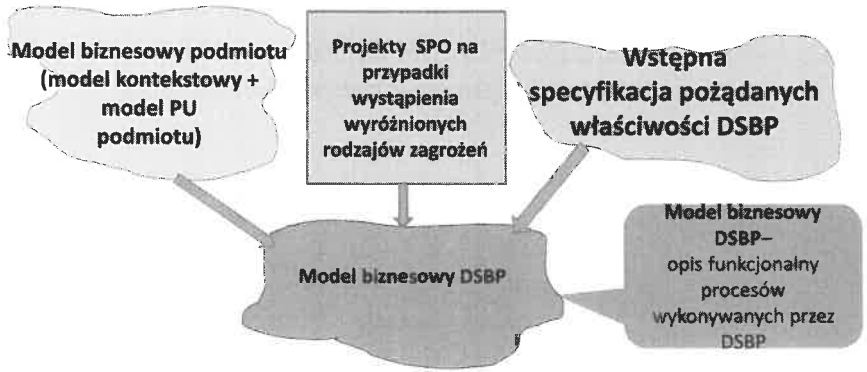
Rozpatrzone zostanie zagadnienie zapewnienia bezpieczeństwa powodziowego aglomeracji dyslokowanej w dolinie, przez którą przepływa rzeka. Można je zapewnić podejmując, między innymi, następujące działania:

1. na etapie ***zapobiegania*** powodzi:
   - budowę zbiorników retencyjnych w górnym biegu rzeki,
   - zwiększanie wysokości obwałowań rzeki przed obszarem aglomeracji i w tym obszarze ,
   - prowadzenie prac melioracyjnych;
2. na etapie ***przygotowania*** na wypadek przekraczania przez rzekę stanu alarmowego– przygotowanie:
   - obszarów zalewowych,
   - sił o odpowiednich kwalifikacjach,
   - materiałów do podwyższania poziomu obwałowania rzeki i zabezpieczenia obiektów– worków, piasku, narzędzi, środków transportu, elementów umocnień obwałowania itp.,
   - środków transportu ludności i ich dobytku – łodzi, pontonów, amfibii, samochodów itp.,
   - pomieszczeń do czasowego zakwaterowania ludności w przypadku konieczności jej ewakuowania z zalanych terenów oraz wyżywienia, wody, ubrań, środków czystości dla nich itp.;
3. na etapie ***działań ratowniczych***:
   - ratowanie ludzi, którzy nie zostali ewakuowani przed wystąpieniem powodzi,
   - ratowanie zwierząt i dobytku,
   - zaopatrywanie ludności pozostałej na obszarach zalanych w środki przetrwania, itd.;
4. na etapie ***likwidacji*** skutków powodzi:
   - przywracanie zdatności funkcjonalnej obiektów,
   - usuwanie zanieczyszczeń powodziowych, itd.

Każdy z podanych sposobów może spowodować pewien przyrost poziomu bezpieczeństwa. Jego zastosowanie wymaga poniesienia określonych nakładów. Każdy z nich może różnić się wielkością przyrostu skuteczności przypadającą na jednostkę nakładów, a zatem efektywnością. Naturalnym postępowaniem w zarządzaniu bezpieczeństwem podmiotu jest wybór rozwiązań charakteryzujących się największą efektywnością – przy spełnieniu ograniczeń (np. czasowych, społecznych, kwalifikacyjnych wykonawców i zarządzających przedsięwzięciem itp.), które to zazwyczaj występują w praktyce. Do ustalenia sposobu zapewnienia pożądanego poziomu bezpieczeństwa podmiotu niezbędne jest przeprowadzenie analizy możliwych do zastosowania rozwiązań, uwzględniając ich efektywność, a następnie wyboru najkorzystniejszego. Dokonanie tego umożliwia ***model biznesowy*** uzupełniony ***modelem analitycznym DSBP***. Model biznesowy DSBP przedstawia jego aspekty funkcjonalne, zaś analityczny sposób realizacji tych funkcjonalności. Model analityczny DSBP stanowi zatem podstawę do ustalenia niezbędnych nakładów i czasu na utworzenie przedmiotowego systemu.

Modelowanie biznesowe Dziedzinowych Systemów Bezpieczeństwa Podmiotu

Na każdy podmiot oddziałują określone zagrożenia. Do zapewnienia możliwości jego funkcjonowania musi być utworzony system bezpieczeństwa o odpowiednich właściwościach – zapewniający podmiotowi warunki do prowadzenia działalności, do której został powołany. Jeżeli warunki bezpieczeństwa funkcjonowania podmiotu w jakimś aspekcie nie są spełnione (np. komunikacyjnym, zdrowotnym, zatrudnienia itp.), to zachodzi konieczność doskonalenia tych dziedzin jego bezpieczeństwa, które nie są zadawalające. Zakres pożądanego doskonalenia bezpieczeństwa dziedzinowego podmiotu ujmuje się w postaci pożądanych właściwości DSBP. Ustala się je poprzez modelowanie biznesowe tego systemu (rys.12.).



Rys. 12. Modelowanie biznesowe funkcjonowania DSBP na potrzeby identyfikacji pożądanych jego właściwości (źródło: opracowanie własne)

Modelowanie biznesowe DSBP jest sposobem *odwzorowania i dokumentowania procesów funkcjonalnych* w nim zachodzących w odpowiedniej notacji – języku modelowania. Tworzenie modeli biznesowych DSBP przyczynia się istotnie do lepszego zrozumienia sposobu jego funkcjonowania, dzięki precyzyjnemu opisowi funkcjonalnych aspektów realizowanych przez niego procesów w rozpowszechnionej ostatnio notacji UML [7,8].

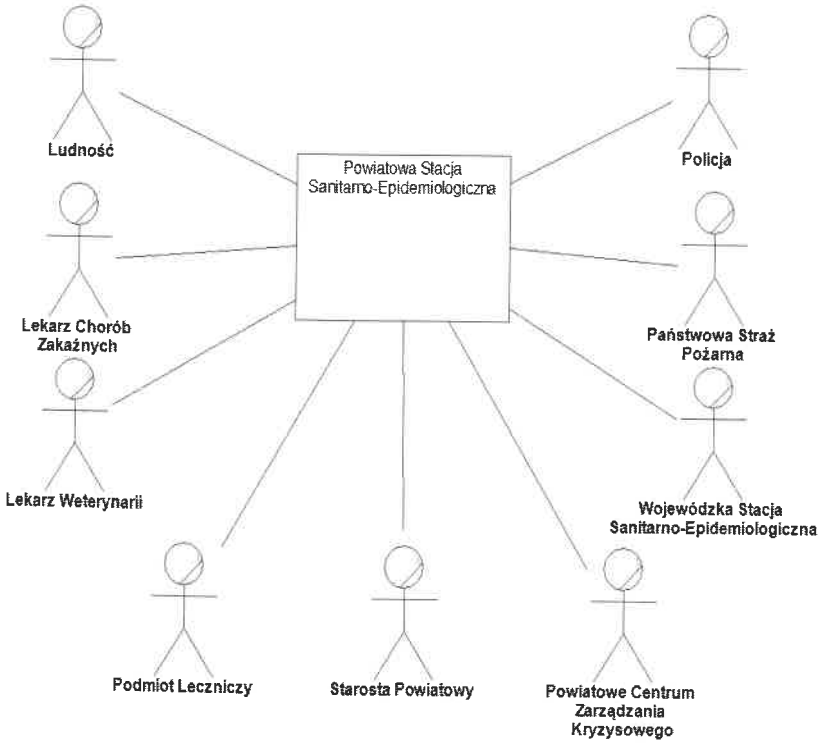
W ramach modelowania biznesowego DSBP opracowuje się:

1. ***model kontekstowy DSBP***,
2. ***model przypadków użycia DSBP***.

Elementy składowe tych modeli są analogiczne do przedstawionych w punkcie 2. modeli kontekstowego i przypadków użycia podmiotu.

Do zilustrowania elementów składowych modelu biznesowego DSBP na rys. 13. przedstawiono diagram kontekstowy Powiatowej Stacji Sanitarno-Epidemiologicznej w zakresie bezpieczeństwa epidemiologicznego, zaś na rys. 14. diagram przypadków jej użycia w tym samym zakresie oraz na rys. 15. diagram czynności dla wybranego przypadku jej użycia.

Rys. 13. Diagram kontekstowy Powiatowej Stacji Sanitarno-Epidemiologicznej w zakresie bezpieczeństwa epidemiologicznego.

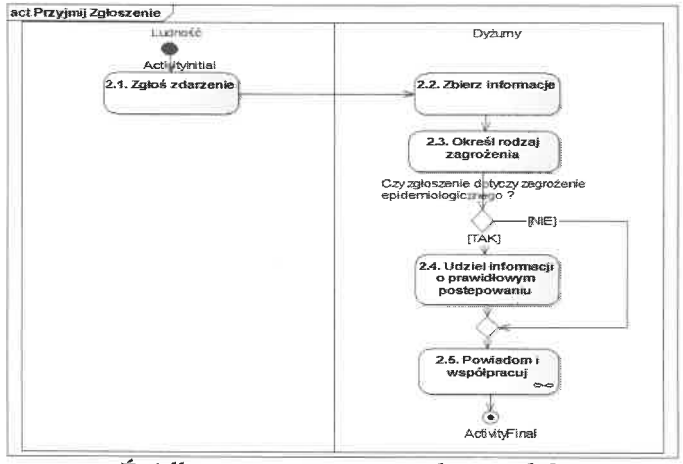


Źródło: opracowane na podstawie [6].

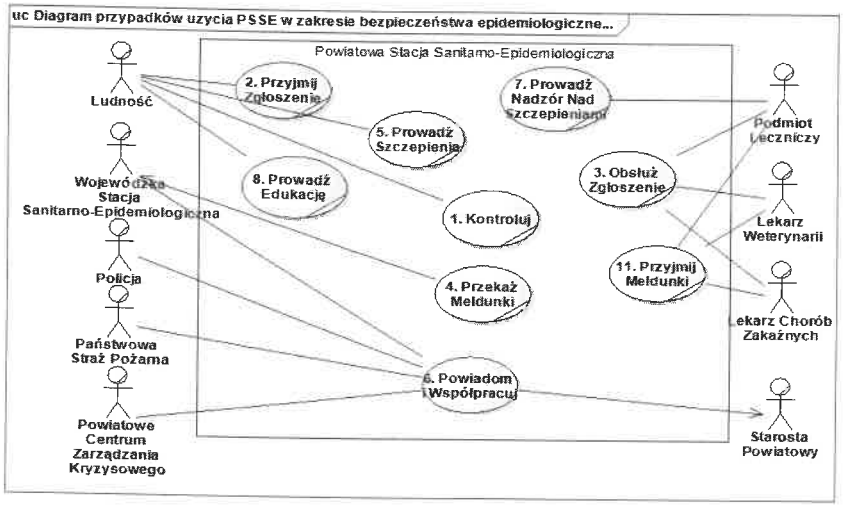
Rys. 14. Diagram przypadków użycia Powiatowej Stacji Sanitarno-Epidemiologicznej w zakresie bezpieczeństwa epidemiologicznego

Źródło: opracowane na podstawie [6].

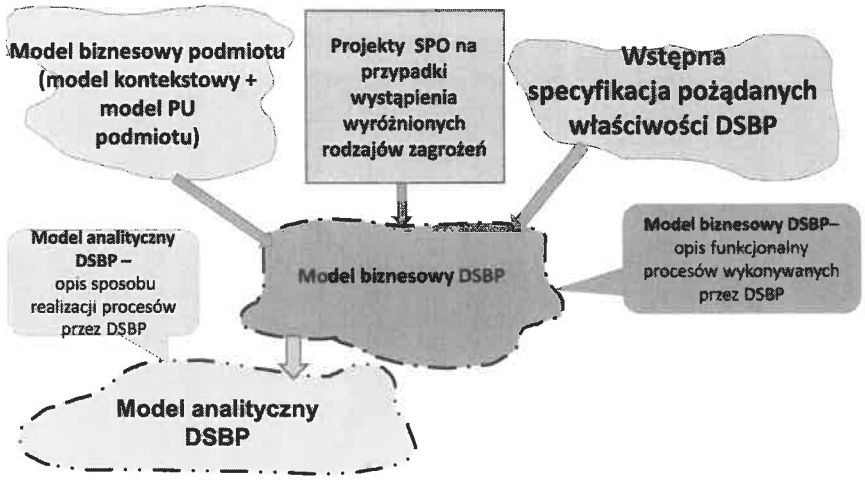
Rys. 15. Diagram czynności dla przypadku użycia „Przyjmij zgłoszenie"



Źródło: opracowane na podstawie [6].



Modelowanie analityczne to technika ustalania i dokumentowania wizji realizacyjnej DSBP. Jego wynikiem jest model analityczny DSBP (rys.16.). Przedstawia on projekt konceptualny technologii realizacji przypadków jego użycia. Można go interpretować jako wstępny projekt DSBP, który określa, jak ma być wykonany/zmodyfikowany, aby zapewnić pożądane właściwości funkcjonalne, określone w modelu biznesowym.

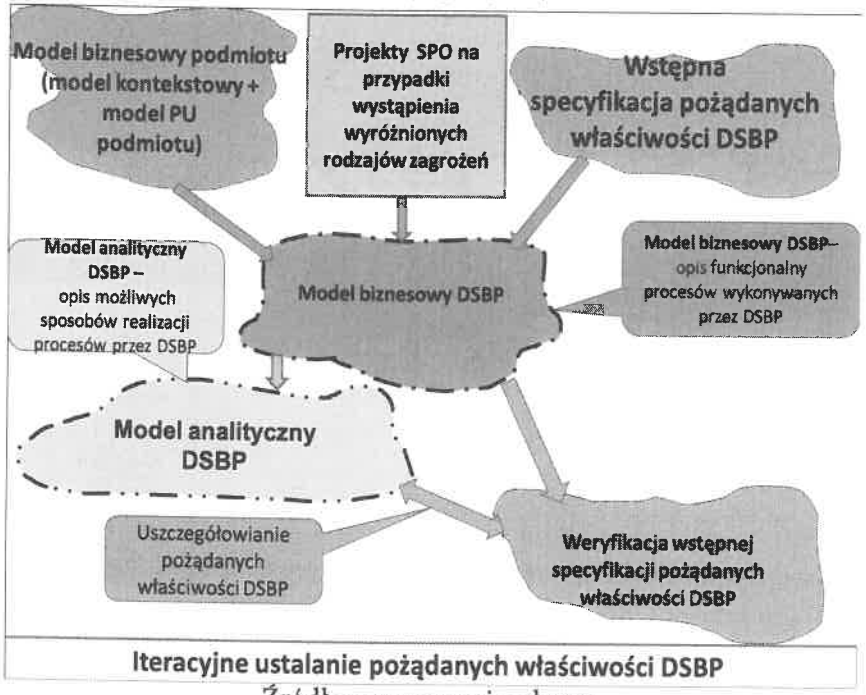


Rys. 16. Ilustracja opracowywania modelu analitycznego DSBP (źródło: opracowanie własne)

Weryfikacja wstępnej specyfikacji pożądanych właściwości DSBP

Na podstawie obiektowego modeli kontekstowego oraz przypadków użycia podmiotu określane są wstępnie pożądane właściwości DSBP – sposób określania przedstawiono w punkcie 3.3. Przy ich ustalaniu nie są uwzględniane możliwości realizacyjne. Weryfikację możliwości realizacyjnych, wstępnie zidentyfikowanych właściwości, DSBP przeprowadza się iteracyjnie, biorąc pod uwagę jego modele biznesowy i analityczny (rys. 17.). Iteracyjność weryfikacji wynika z faktu, że daną właściwość DSBP można uzyskać na więcej niż jeden sposób, z których każdy może mieć różną efektywność.

Rys.17. Iteracyjna identyfikacja pożądanych właściwości DSBP



Źródło: opracowanie własne.

Ustalanie wymagań na Dziedzinowe Systemy Bezpieczeństwa Podmiotu

Wielkościami charakteryzującymi przedsięwzięcie zapewnienia dziedzinowego bezpieczeństwa funkcjonowania podmiotu są:

1. pożądane właściwości DSBP,
2. koszt wytworzenia DSBP o pożądanych właściwościach,
3. czas wytworzenia DSBP o pożądanych właściwościach.

Zwrot „wytworzenie DSBP o pożądanych właściwościach" użyty jest w szerokim znaczeniu. Obejmuje on nie tylko wytwarzanie nowego DSBP, ale również doskonalenie jego właściwości ukierunkowane na zwiększanie skuteczności działania.

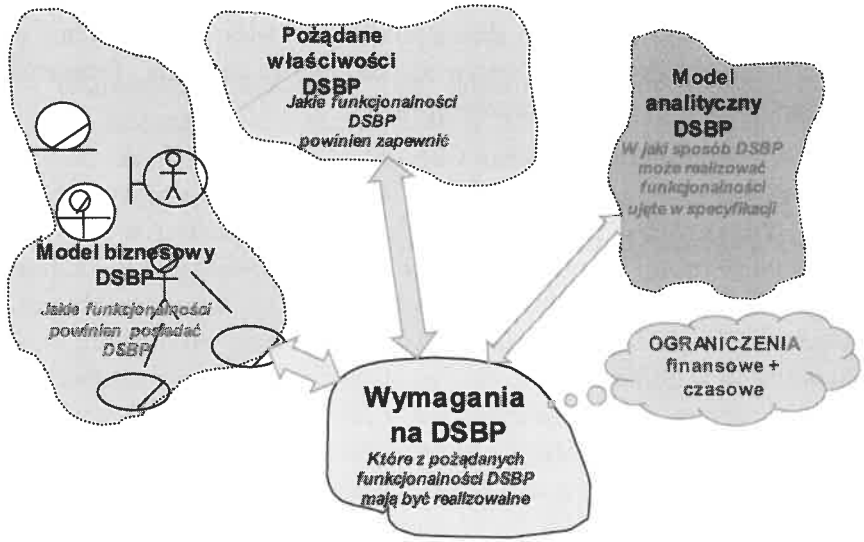
W praktyce zadanie zapewnienia dziedzinowego bezpieczeństwa funkcjonowania podmiotu realizowane jest przy ograniczeniach na dopuszczalne koszty i czas wykonania. W przeważającej części przypadków

tak sformułowane zadanie jest niewykonalne. Dopuszczalne koszty i czas ograniczają możliwość bezpośredniej zamiany pożądanych właściwości funkcjonalnych DSBP na wymagania na ten system.

Zatem danymi wyjściowymi do ustalenia wymagań na DSBP są (rys.18.):

1. pożądane jego właściwości, których sposób identyfikacji przedstawiono w poprzednich punktach;
2. ograniczenia na:
   a) możliwe do poniesienia nakłady na zapewnienie bezpieczeństwa funkcjonowania podmiotu;
   b) dopuszczalny czas na zrealizowanie przedsięwzięcia zapewniającego bezpieczeństwo funkcjonowania podmiotu.

Rys.18. Ustalanie wymagań na DSBP na podstawie jego modeli biznesowego i analitycznego z uwzględnieniem ograniczeń na dopuszczalne koszty i czas wykonania



Źródło: opracowanie własne.

Przy ustalaniu, które z pożądanych właściwości DSBP mogą być uwzględnione przy jego tworzeniu, należy zdekomponować je do funkcjonalności autonomicznych, tzn. takich, które mogą być realizowane za

pomocą wyodrębnianego jego elementu o cechach komponentu. Komponent może mieć postać: urządzenia, zespołu wykonawczego, modułu programowego itp. Jego charakterystykę stanowić będą trzy wielkości:

1. nakłady, jakie muszą być poniesione na jego wytworzenie i wdrożenie – aby system mógł posiadać daną funkcjonalność;
2. czas niezbędny na jego wytworzenie i wdrożenie;
3. efektywność danej funkcjonalności.

Efektywność funkcjonalności rozumiana jest jako relacja między przyrostem skuteczności systemu w wyniku jej wdrożenia a nakładami poniesionymi na opracowanie komponentu ją realizującego i jego wdrożenie.

Dobre praktyki w specyfikacji wymagań na Dziedzinowe Systemy Bezpieczeństwa Podmiotu

Uwzględniając fakt, że w praktyce występują ograniczenia budżetowe i czasowe na realizację przedsięwzięć zwiększających skuteczność działania DSBP, wskazane jest dokonanie hierarchizacji pożądanych jego właściwości. Kryterium podziału zbioru pożądanych właściwości systemu na podzbiory powinien być ich wpływ na skuteczność działania . Proponuje się wyróżnienie trzech podzbiorów (rys.19.):

- koniecznych do spełnienia,
- wskazanych do spełnienia,
- usprawniających działanie systemu.

Rys. 19. Ilustracja hierarchizacji pożądanych właściwości DSBP w celu określenia wymagań na sposób doskonalenia skuteczności jego działania.

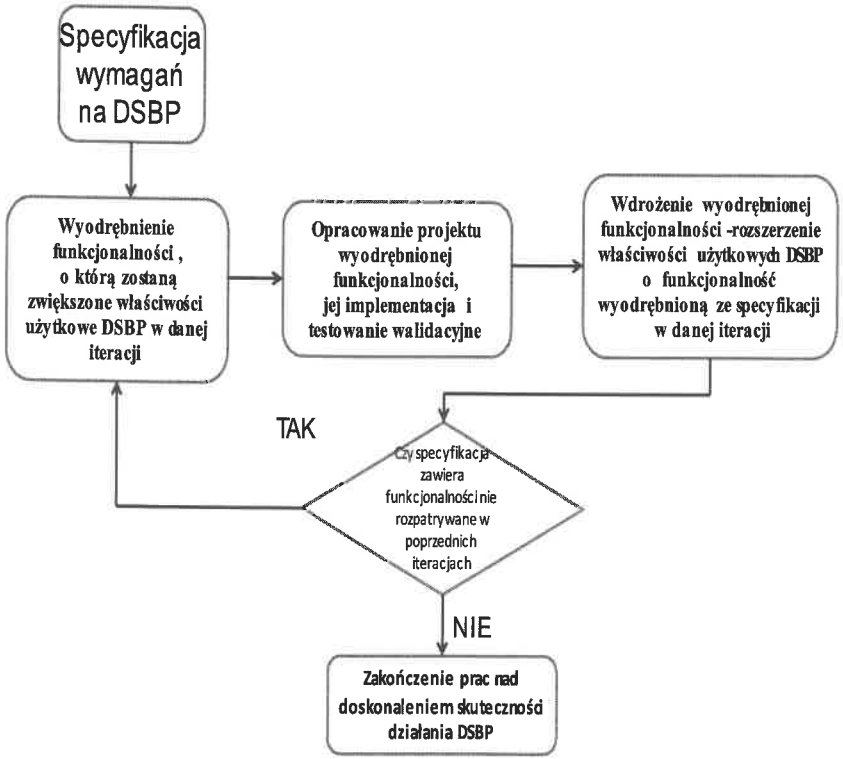
Źródło: opracowanie własne.

Właściwości „konieczne" do spełnienia przez DSBP powinny być bezwzględnie uwzględnione w specyfikacji wymagań na ten system. W drugiej kolejności powinna być rozpatrywana możliwość rozszerzenia ich zakresu o właściwości z podzbioru „wskazanych" i w trzeciej „usprawniających". Podzbiory właściwości „wskazanych" i „usprawniających" zazwyczaj nie są jednoelementowe. Uzasadnione staje się zatem, aby właściwości przyporządkowane do tych podzbiorów uszeregować z uwzględnieniem ich efektywności. Z tak zhierarchizowanych pożądanych właściwości DSBP w podzbiorach „wskazane" i „usprawniające", w wymaganiach na ten system powinny być uwzględniane te, które mogą być realizowalne ze względu na dysponowane środki na ten cel, oraz/i których czas wykonania nie przekracza dopuszczalnego.

Jedną z podstawowych cech dobrej praktyki w ustalaniu wymagań na DSBP jest umożliwienie zarządzania nimi [1,7]. W tym celu wskazane jest, aby pożądane właściwości funkcjonalne systemu były zdekomponowane do poziomu autonomicznych. Pozwala to na zastosowanie przyrostowej metody zwiększania skuteczności jego działania. Ideę tej metody

przedstawiono na rys. 20. Zdekomponowanie pożądanych właściwości funkcjonalnych DSBP do poziomu, aby wyróżnioną funkcjonalność mógł autonomicznie realizować wyodrębniony element systemu, znakomicie usprawnia prowadzenie prac projektowych i implementacyjnych nad danym systemem.

Rys. 20. Przyrostowa metoda zwiększania skuteczności działania DSBP.



Źródło: opracowanie własne.

Środowiska i narzędzia programowe wykorzystywane w modelowaniu obiektowym przy ustalaniu wymagań na Dziedzinowe Systemy Bezpieczeństwa Podmiotu

Opracowanie modelu biznesowego podmiotu, dla którego opracowywany jest system bezpieczeństwa, jak i modeli biznesowych i analitycznych DSBP w celu ustalenia pożądanych ich właściwości, wymaga, przede wszystkim:

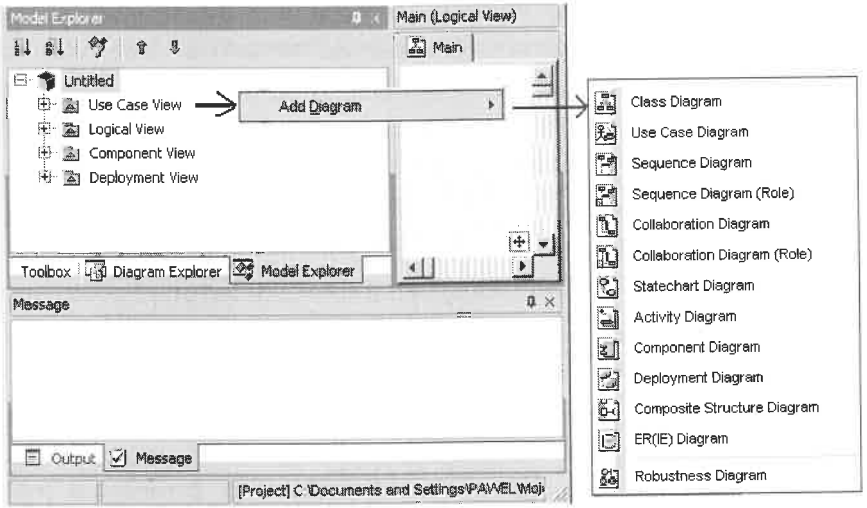
1. umiejętności modelowania obiektowego w wybranym języku,
2. szczegółowego poznania technologii realizacji zadań przez podmiot,
3. umiejętności identyfikacji zagrożeń zewnętrznych i wewnętrznych bezpieczeństwa funkcjonowania podmiotu.

Modelowanie na potrzeby identyfikacji zagrożeń bezpieczeństwa funkcjonowania podmiotu i ustalenia pożądanych właściwości DSBP jest przedsięwzięciem bardzo złożonym i pracochłonnym. Pomocne w jego realizacji mogą być istniejące środowiska i narzędzia programowe, które ułatwiają panowanie nad złożonością przedsięwzięcia, a przede wszystkim odciążają od niezwykle czasochłonnego dokumentowania elementów składowych modeli. Istnieje wiele narzędzi programowych wykorzystywanych do modelowania obiektowego z użyciem języka UML. Najpopularniejsze z nich to:

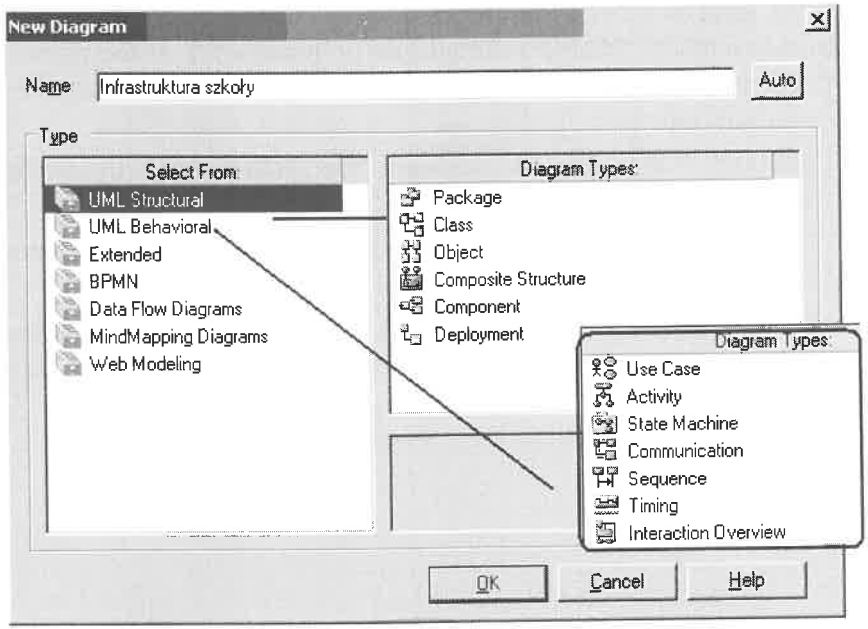
- StarUML – dostępny pod adresem: http://sourceforge.net/projects/whitestaruml – darmowe;
- Enterprise Architect, na użytkowanie którego licencja jest stosunkowo niedroga, a miesięczna wersja testowa darmowa.

Środowiska te dostarczają przede wszystkim narzędzi do tworzenia wszystkich rodzajów diagramów wyróżnianych w UML (rys. 21. i rys. 22.)

Rys. 21. Rodzaje diagramów dostępnych w StarUML



Rys. 22. Rodzaje diagramów dostępnych w Enterprise Architect



Wybrane narzędzia wspierają prawie cały cykl projektowania systemów (zwłaszcza informatycznych), a w szczególności tworzenie diagramów kontekstowych i przypadków użycia, które to są istotne w modelowaniu systemów bezpieczeństwa.

Cenną zaletą środowisk i narzędzi wspomagających modelowanie obiektowe jest to, że podpowiadają analitykowi kolejność, jaką należy zachować przy tworzeniu projektu. Pokazano to na rys. 21., który przedstawia interfejs po utworzeniu nowego projektu.

Podsumowanie

W artykule przedstawiono zastosowanie modelowania obiektowego do wspomagania określania wymagań na przedsięwzięcia zapewniające podmiotowi pożądany poziom bezpieczeństwa jego funkcjonowania. Realizowane jest ono w filozofii i notacji UML. W pierwszej kolejności opracowywany jest model biznesowy podmiotu, ograniczony do jego modelu kontekstowego i przypadków użycia. Wykorzystywane są one do identyfikacji zagrożeń bezpieczeństwa jego funkcjonowania – ustalania możliwych rodzajów zagrożeń i ich charakterystyk, ze szczegółowością niezbędną do określenia pożądanych właściwości i opracowania wizji realizacyjnej DSBP. Wizja realizacyjna DSBP przedstawiana jest za pomocą jego modelu analitycznego – wykonana jest również w filozofii i notacji UML.

Model analityczny DSBP zawiera sposoby uzyskiwania pożądanych jego właściwości i pozwala oszacować koszt i czas ich osiągnięcia. Koszt i czas osiągnięcia każdej z pożądanej właściwości DSBP stanowią ich charakterystyki, które uwzględniane są przy ustalaniu wymagań na DSBP.

References

Dean Leffingwell i inni: *Zarządzanie wymaganiami.* Seria: Inżynieria oprogramowania, WNT, Warszawa 2003.

Kołodziński E.: *Symulacyjne metody badania systemów*, PWN, Warszawa 2002.

Kołodziński E.: Wprowadzenie do zarządzania bezpieczeństwem podmiotu, w pracy zbiorowej pod redakcją Zygmunta Mierczyka i Romana Ostrowskiego pt. *Ochrona przed skutkami nadzwyczajnych zagrożeń Tom 2.*, Warszawa

Kołodziński E.: O problemie oceny bezpieczeństwa podmiotu oraz skuteczności i efektywności działania Dziedzinowego Systemu Bezpie-

czeństwa Podmiotu, w monografii *Bezpieczeństwo –wymiar współczesny i perspektywy badań* pod redakcją Mirosława Kwiecińskiego, Kraków 2010 s. 71–86.

Kołodziński E., Ropiak R., Tomczyk Ł.: Analiza skuteczności działania Wojewódzkiego Systemu Ratownictwa w przypadku zdarzeń masowych, w monografii pod redakcją Juliusza Jakubaszki pt. 20 lat zimowych spotkań medycyny ratunkowej w Karpaczu, Wrocław 2011.

Kubica D.: Model obiektowy teleinformatycznego systemu wspomagania zarządzania bezpieczeństwem epidemiologicznym w powiecie, praca inżynierska, wykonana pod kierunkiem dra hab. inż. Edwarda Kołodzińskiego, prof. WAT, WAT, 2013.

Śmiałek M.: *Zrozumieć UML 2.0 – metody modelowania obiektowego*, Helion, Gliwice 2005.

Wrycza S. i inni: *Język UML 2.0 w modelowaniu systemów informatycznych*, Helion, Gliwice 2005.

Audyt personalny czynnikiem wspomagającym bezpieczeństwo personelu w organizacji

dr Aleksandra Szejniuk

Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie

a.szejniuk@gmail.com

Abstracts

Audyt personalny dotyczy kapitału ludzkiego, który razem z kapitałem finansowym i rzeczowym stanowi o sile firmy. Jego zadaniem jest ocena umiejętności zawodowych pracowników. Ponadto poszukuje czynników powodujących zadowolenie lub jego brak w pracy zawodowej.

Dziedziny, którymi zajmuje się audyt personalny, to przede wszystkim rekrutacja i selekcja. Uzyskane informacje na temat umiejętności, zdolności i doświadczenia powinny być bezpiecznie przechowywane. Zapewnienie bezpieczeństwa danych personalnych i bezpieczeństwa pracy powinno być priorytetem dla każdego przedsiębiorstwa, warunkującym jego funkcjonowanie na rynku.

Keywords:

audit, personnel audit, safety audit, security data audit

audyt, audyt personalny, audyt bezpieczeństwa, audyt bezpieczeństwa pracy, audyt bezpieczeństwa danych

Wstęp

Współczesne organizacje zwracają szczególną uwagę na zasoby ludzkie, które określają ich sukces. Pracownicy przyczyniają się do wzrostu efektywności nie tylko swoją wiedzą, lecz także sposobem radzenia sobie w sytuacjach kryzysowych.

Konieczne i uzasadnione wydaje się stosowanie audytu personalnego, który dotyczy kultury organizacyjnej i jej wpływu na efektywność przedsiębiorstwa. Powodem takich działań jest globalizacja rynku.

Przejawem kultury organizacyjnej w Polsce są normy, zachowania, filozofia, polityka i systemy motywacyjne stosowane w firmach. Rozwój