Prace Instytutu Mechaniki Górotworu PAN
Tom 10, nr 1-4, (2008), s. 131-140
© Instytut Mechaniki Górotworu PAN

Uwagi o czynnikach efektywnego sterowania ryzykiem

Tadeusz Cyrul

Instytut Mechaniki Górotworu PAN, ul. Reymonta 27, 30-059 Kraków

Streszczenie

Prezentowana praca stanowi kolejny etap badań związanych z problematyką ryzyka w projektach górniczych. W pracy przedstawiono rozważania na temat sterowania ryzykiem w kopalni czy grupie kopalń traktowanych jako system. Opracowano model zagrożenia bezpieczeństwa systemu umożliwiający analizę bezpiecznych i niebezpiecznych scenariuszy działalności, model bezpieczeństwa systemu pozwalający na sterowanie poziomem bezpieczeństwa systemu oraz zaproponowano model zarządzania bezpieczeństwem systemu umożliwiający efektywne dysponowanie zasobów „centralnych" na sterowanie bezpieczeństwem obiektów składowych systemu.

Słowa kluczowe: bezpieczeństwo, niezawodność, ryzyko, zagrożenie, system, zarządzanie ryzykiem

1. Wprowadzenie

Zakład górniczy, a tym bardziej grupa zakładów górniczych jak np. Spółka Węglowa nie tylko prowadzą działalność gospodarczą w obszarze tzw. podwyższonego ryzyka ale również dysponują majątkiem dużej wartości zarówno w postaci mienia jak i technologii oraz miejsc pracy dla dużej liczby osób czy wreszcie zasobów ludzkich. W tej sytuacji zarządzanie ryzykiem odgrywa szczególnie ważną rolę, gdyż w procesie działalności zakładu może dochodzić do szkód znacznej wartości i niewłaściwe zarządzanie ryzykiem może generować istotne straty w działalności gospodarczej zakładu.

Nie ma jednolitej i powszechnie akceptowalnej definicji zarządzania ryzykiem. Można je zatem określić jako proces poszukiwania i podejmowania działań, które powinny zabezpieczyć decydenta przed poniesieniem strat większych niż te, które dopuszcza przyjęty przez niego poziom bezpieczeństwa. Zarządzanie ryzykiem w przedsiębiorstwie można podzielić na pewne etapy jak:

- Identyfikacja zagrożeń
- Analiza i ocena ryzyka
- Sterowanie ryzykiem.

Identyfikacja zagrożeń jest procesem systematycznego rozpoznania środowiska w jakim dana organizacja gospodarcza prowadzi działalność. Celem tych działań jest gromadzenie informacji na temat źródeł ryzyka, zagrożeń i podatności na straty. Niezwykle pomocnym w tym etapie jest odpowiednie skonstruowanie list kontrolnych czy kwestionariuszy oceny ryzyka, które obejmowałyby wszystkie istotne obszary działalności przedsiębiorstwa, w których pojawić się mogą zalążki start (Cyrul, 2004). W przypadku zakładu górniczego do takich obszarów zaliczyć należy:

- zagrożenia naturalne
- zagrożenia społeczne
- zagrożenia polityczne
- zagrożenia działalności operacyjnej
- zagrożenia ekonomiczne (rynkowe).

Analiza i ocena ryzyka koncentruje się na przetwarzaniu danych zgromadzonych w kwestionariuszach oceny ryzyka, tworzeniu scenariuszy zdarzeń szkodowych, określaniu wielkości możliwych strat oraz

prawdopodobieństwa ich zajścia. Pomocnym w tym etapie są techniki drzewa zdarzeń i drzewa awarii oraz analizy udokumentowanych zdarzeń szkodowych z przeszłości, wizje lokalne, modelowanie ryzyka itp.

Sterowanie ryzykiem to część procesu zarządzania ryzykiem, przeprowadzana w sposób scentralizowany na szczeblu strategicznym przedsiębiorstwa. Do najbardziej znanych metod sterowania ryzykiem zalicza się:

- *unikanie ryzyka*, które zalicza się do negatywnych metod sterowania ryzykiem gdyż przeważnie wiąże się z zaniechaniem podejmowania przez przedsiębiorstwo działań obarczonych ryzykiem co hamuje inicjatywę i przedsiębiorczość.
- *prewencja*, która zmierza do podejmowania działań zmniejszających lub eliminujących ryzyko lub minimalizujących straty
- *transfer ryzyka* na inny podmiot. Najbardziej rozpowszechnioną metodą transferu ryzyka jest jego ubezpieczenie w firmie ubezpieczeniowej. W takim przypadku ryzyko traktowane jest jak towar, którego sprzedaż ubezpieczycielowi jest równoznaczna z zakupem gwarancji rekompensaty poniesionej szkody w wyniku zdarzenia losowego. W przypadku dużych przedsiębiorstw działających w warunkach znacznego ryzyka cena ubezpieczenia może być znaczna, dlatego też kluczową rolę w jej negocjacji odgrywać mogą dane zgromadzone w procesie identyfikacji ryzyka i jego analizy. Udokumentowane działania prewencyjne są również ważnym czynnikiem obniżającym koszty ubezpieczenia.

Istotnym składnikiem procesu sterowania ryzykiem jest monitoring ryzyka, który koncentruje się na obserwacji i kontroli planowych działań przedsiębiorstwa, reakcji na nowe nieprzewidziane wcześniej zagrożenia, realizację działań prewencyjnych, opracowywanie i wdrażanie planów awaryjnych itp.

Przedmiotem tej pracy jest koncepcyjna analiza procesu sterowania ryzykiem w kopalniach spółek węglowych, jako element systemu zarządzania bezpieczeństwem.

2. Pojęcie ryzyka i pojęcia pokrewne

Pojęcie ryzyka i szeregu wyrażeń pochodnych jak zarządzanie ryzykiem, analityk ryzyka i wiele innych stały się modne w ostatnich dziesięcioleciach po części za sprawą udokumentowanej przydatności tych pojęć w procesie decyzyjnym, szczególnie w projektach tzw. wysokiego ryzyka jak np. projekty kosmiczne, projekty w dziedzinie energetyki jądrowej czy przemyśle naftowym. Aby ryzyko taką rolę przydatną w procesie decyzyjnym spełniało musi posiadać cechy dopuszczające sensowne jego uporządkowanie. Mamy tutaj na myśli binarną relację porządku czy preferencji

$$A \succeq B$$

oznaczającą fakt, że alternatywa A jest co najmniej tak ryzykowna jak B i spełniającą dwa warunki tj. zupełności i przechodniości (Brachinger i Weber, 1997). Uporządkowanie ryzyka wynikające z jego oceny nie powinno mieć jednak wyłącznie znamion preferencji osobistych. Aby tak było potrzebujemy pewnych funkcji R, których wartości liczbowe spełnia naszą relację porządku $\succeq$ czyli funkcji R o własnościach

$$A \succeq B \Leftrightarrow R(A) \succeq R(B)$$

Każda taka funkcja jest nazywana miarą ryzyka.

W praktycznych zastosowaniach technicznych dominuje utożsamianie ryzyka z oczekiwaną szkodą w postaci iloczynu wartości prawdopodobieństwa zdarzenia szkodowego oraz wartości powstałej szkody.

$$R = P_x \times S_x$$

gdzie: R – oznacza ryzyko, p_x jest prawdopodobieństwem zdarzenia x, zaś s_x jest wielkością straty jaka towarzyszy wystąpieniu zdarzenia x.

W wielu dziedzinach określenie prawdopodobieństwa przebiega typowo zgodnie ze znanymi schematami opartymi na tradycji i doświadczeniu. W niektórych innych istnieją naturalne modele probabilistyczne, które opisują badaną sytuację. W takich przypadkach odpowiednie prawdopodobieństwa mogą być przypisane szybko i obiektywnie ponieważ panuje powszechna zgodność co do prawidłowości stosowania określonych rozkładów do pewnych typów problemów.

Niestety większość sytuacji związanych eksploatacją podziemną cechuje niepowtarzalność i w takich warunkach określenie prawdopodobieństw prognozowanych zdarzeń przez analityka (osobę lub zespół) musi być wysoce subiektywne, odzwierciedlając w zasadzie jego własne informacje i przekonania.

Zarówno wielkość obiektu jakim jest kopalnia, a tym bardziej grupa kopalń, jak i zakres prowadzonej działalności i złożoność relacji pomiędzy różnymi elementami tego obiektu sugeruje podejście systemowe do problematyki zarządzania ryzykiem, które jest jednym z elementów problematyki zarządzania bezpieczeństwem kopalni, czy grupy kopalń.

Zapewne właśnie taka natura otaczającej nas rzeczywistości jest jednym z powodów, że we współczesnych naukach stosowanych kładzie się nacisk na podejście systemowe, holistyczne w opisie tej rzeczywistości (Sienkiewicz, 2003). Ponieważ system to zbiór synergicznie połączonych elementów tworzących całość, w analizie czy opisie dużych systemów, do których niewątpliwie zaliczyć należy kopalnię czy grupę kopalń, kluczową rolę odgrywa system człowiek-technika-środowisko (C-T-O). Te trzy elementy są ze sobą ściśle powiązane, a ich stan zależy w dużym stopniu od charakteru oddziaływań między sobą, a te z kolei mogą być przyczyną zdarzeń niepożądanych, które mogą powodować straty materialne w postaci utraty zdrowia lub życia ludzi oraz inne straty mające wymiar ekonomiczny.

Tak więc zdarzenie niepożądane to takie zdarzenie, którego zajście w systemie C-T-O wywołuje zagrożenie dla chronionych dóbr.

Z kolei pojęcie zagrożenia możemy zdefiniować jako warunkową możliwość powstania strat, w wyniku pojawienia się zdarzenia niepożądanego w systemie C-T-O.

Ponieważ każdy z tych podsystemów jest bytem wielce złożonym więc badanie konsekwencji pojawiania się zdarzeń niepożądanych w tych obszarach kreuje specyficzną terminologię czy kryteria, pomimo tego, że stosowane tam metody badawcze są podobne. I tak w obszarze „człowiek" zamiast pojęcia ryzyko dominuje pojęcie bezpieczeństwo, a więc stan pewności, spokoju i braku zagrożeń, a tym samym i wypadków czyli szkód. Pozostając w obszarze określeń werbalnych, wysokie bezpieczeństwo kojarzy nam się z niskim ryzykiem. Podobnie jest w obszarze technika, gdzie substytutem pojęcia ryzyko jest pojęcie niezawodności, a więc takiej własności urządzenia, która powoduje jego bezawaryjną pracę. Podobnie więc wysoka niezawodność danego obiektu to również wysokie bezpieczeństwo a niskie ryzyko.

Analiza systemowa bezpieczeństwa dowolnych obiektów ma sens, gdy istnieje niebezpieczeństwo, czyli istnieją zagrożenia mogące spowodować bądź zakłócenia funkcjonowania (egzystencji, rozwoju) tych obiektów, bądź możliwość utraty przez obiekty określonych wartości. Bezpieczeństwo jest pojęciem wieloznacznym, odnoszącym się do:

1) braku zagrożenia;
2) systemu instytucjonalnych i pozainstytucjonalnych gwarancji likwidacji lub minimalizacji zagrożeń;
3) jednej z istniejących wartości egzystencjonalnych, wiążącej się z poczuciem stabilności, trwałości korzystnego stanu rzeczy, wrażeniem pewności.

Na gruncie analizy systemowej dominują dwa ujęcia bezpieczeństwa systemów, a mianowicie (Sienkiewicz, 2007):

a) bezpieczeństwo rozumiane jako własność obiektu charakteryzująca jego odporność na powstanie sytuacji niebezpiecznych (zagrożeń), przy czym uwaga koncentruje się na zawodności bezpieczeństwa obiektu, czyli jego podatności na powstanie sytuacji niebezpiecznych;
b) bezpieczeństwo systemu rozumiane jako jego zdolność do ochrony wewnętrznych wartości przed zewnętrznymi zagrożeniami.

Ponadto należy dostrzec dwa aspekty bezpieczeństwa: obiektywny – istnieją warunki wystąpienia realnych zagrożeń, subiektywny – wyraża poczucie bezpieczeństwa (zagrożeń).

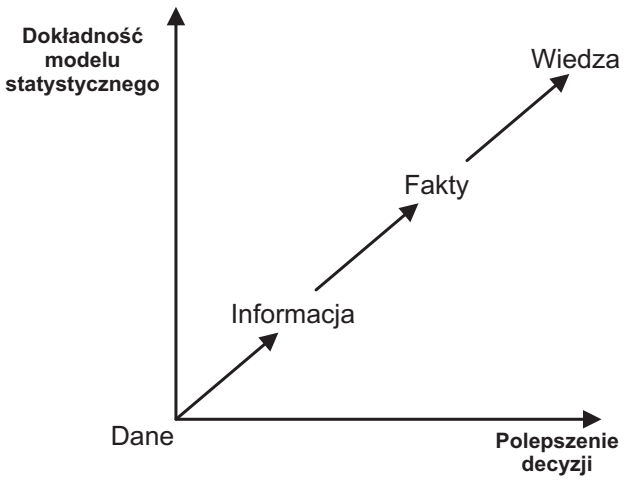
2.1. Ryzyko a zagrożenie

Termin zagrożenie jest niewątpliwie najczęściej używanym terminem w tekstach na tematy górnicze. Zagrożenie wybuchem, tąpaniami czy ocena stanu zagrożeń skojarzonych to tylko nieliczne przykłady fragmentów tytułów artykułów ukazujących się w literaturze naukowej na tematy górnicze. Systematycznej klasyfikacji zagrożeń podejmował się m.in. Ryncarz (Ryncarz, 1983) zaś próbę sformalizowanego opisu zagrożeń z perspektywy teorii decyzji w warunkach niepewności i ryzyka przedstawił Kortas (Kortas, 1982).

Ryzyko i zagrożenie w ogólności odnoszą się do tego samego zjawiska naturalnego lub sztucznego wytworu jednakże treść tych pojęć jest zasadniczo odmienna, chociaż w literaturze często jest ze sobą utożsamiana (Krzemień, 1992), (Sobala i Rosmus 1997). Zagrożenie jest stanem natury o takiej własności, która w wyobrażalnych okolicznościach może wygenerować szkodę materialną. Np. wysoka metanonośność pokładu węgla stanowi zagrożenie wyrzutem gazu i skał, pożarem, wybuchem mieszaniny gazu i powietrza czyli ogólnie stanowi potencjał do wygenerowania zdarzenia niebezpiecznego (ZN) tj. wyrzutu, wybuchu czy pożaru. Zdarzenia te (wybuch, pożar, wyrzut) określamy terminem zdarzenia niebezpieczne (ZN), gdyż ich wystąpienie następuje zwykle w sposób niekontrolowany, nieprzewidziany i wbrew intencjom osób lub procesu technologicznego ingerujących w stan natury określany mianem „zagrożenie metanowe" oraz powoduje szkody materialne (uszkodzenie obudowy, zniszczenie maszyn, śmierć lub okaleczenie ludzi). Zagrożenie jako stan natury sam w sobie nie powoduje szkody tj. nie generuje ZN. Jest niejako wewnętrzną własnością rozważanego systemu, rozumianego jako świadomie i celowo wyodrębniony fragment otaczającej rzeczywistości. Pojawienie się ZN jest reakcją natury na ingerencję człowieka lub innego obiektu zewnętrznego względem obiektu określanego mianem zagrożenie.

Z kolei treść pojęcia ryzyko wyraża oczekiwany bilans świadomej ingerencji człowieka lub innego obiektu w naturę będącą w stanie zagrożenia. Tak więc bilans ten zależy nie tylko od zagrożenia samego w sobie ale również, a nawet przede wszystkim od sposobu ingerencji w stan zagrożenia. Uzasadnione jest w tym momencie założenie, że ingerencja człowieka w stan zagrożenia jest racjonalna, a miarą racjonalności jest minimalizowanie strat wywołanych tą ingerencją. Podstawą racjonalnego działania jest wiedza o środowisku, w którym działanie ma być przeprowadzone, w naszym przypadku chodzi o górotwór, a właściwie fragment górotworu wydzielony fizycznie lub myślowo do realizacji planowanych zadań (eksploatacji kopaliny). Wiedza jest tym co dobrze wiemy. Jedną z podstawowych form utylizacji posiadanej wiedzy jest jej przekazywanie innym podmiotom. Przekazywanie wiedzy jest informacją. Informację można klasyfikować, przetwarzać czy modyfikować. Surową formą informacji są dane, które same w sobie nie są wiedzą. Na drodze od surowych danych do wiedzy o analizowanym systemie pojawia się najpierw informacja, w którą przekształcają się dane jeśli okazują się one odpowiednie do rozważanego problemu decyzyjnego. Informacja z kolei staje się faktem jeśli posiadane dane ją potwierdzają. W związku z tym, że dane o badanym obiekcie/procesie mają zwykle charakter prób, dlatego też wiedza stosowna jaką uzyskujemy o badanym obiekcie tą drogą nie może być uznana za wiedzę pełną, a raczej za wiedzę o określonym statystycznym poziomie ufności.

Fakty stają się wiedzą, kiedy pozwalają skonstruować kompletny proces decyzyjny zakończony sukcesem. Poniższy rysunek, Rys. 1, obrazuje proces wnioskowania statystycznego bazujący na danych wykorzystywanych do konstrukcji modelu dla potrzeb decyzji w warunkach niepewności. Należy sobie uświadomić, że o ile opis matematyczny zagrożenia może być nawet bardzo skomplikowany to i tak nie ma możliwości wyrażenia go w kategoriach ilościowych. Taki opis jest jedynie modelem pewnego obiektu, który konstruujemy w naszej wyobraźni na podstawie posiadanej wiedzy.



Rys. 1. Schemat transformacji danych w wiedzę

Model ten wygeneruje dane liczbowe, jeśli poddamy go warunkom wynikającym z planowanego i przemyślanego działania na obiekt będący w stanie zagrożenia, który ten model opisuje. Np. rozpoczęcie wykonywania wyrobiska górniczego w modelowanej partii złoża wywoła zmianę naprężeń, przepływ gazu ze złoża do przestrzeni wyrobiska i wiele innych zmian w pierwotnym stanie natury, który został zakwalifikowany do klasy obiektów określanych mianem zagrożenie.

Innymi słowy zagrożenie opisuje warunki podczas gdy dla wystąpienia ryzyka wymagana jest decyzja o podjęciu działania. Aby z kolei kwantyfikować ryzyko określonych konsekwencji podjętego działania, musimy oprócz modelu „obiektu – zagrożenia" dobrze określić czasowo przestrzenny scenariusz tego działania. Tak więc z definicji ryzyko jest zawsze wyrażone liczbowo. Pytanie czy ryzyko wyrażone jest ilościowo czy jakościowo to pytanie o wielkość błędu oszacowania ryzyka. Jeżeli błąd oszacowania ryzyka jest duży możemy ryzyko wrazić jakościowo np. „wysokie", „średnie" „niskie" lub „bardzo niskie". Jako skutek niepewności taka reprezentacja ryzyka może być uznana za jakościową ocenę ryzyka, chociaż taka przybliżona klasyfikacja ma zwykle zgrubną liczbową ocenę np. 10% to „ryzyko bardzo niskie", a 50% to średnie itp.

Jak wynika z przeglądu literatury górniczej w języku polskim, utożsamianie ryzyka z zagrożeniem zintensyfikowało się w ostatnich latach, kiedy to zaczęto częściej posługiwać się terminem ryzyko. W przeszłości, zamienne stosowanie tych terminów można było znaleźć jedynie w mniej rygorystycznych fragmentach tekstów i było spowodowane raczej pewnymi ograniczeniami języka niesformalizowanego w wyrażeniu złożonych i nieostrych sytuacji.

Utożsamianie tych pojęć w języku naukowym jest niedopuszczalne. Fakt, że są jednak często utożsamiane dowodzi, że zarówno pojęcie ryzyka jak i pojęcie zagrożenia są niewystarczająco ostro zdefiniowane. Zachodzi więc pilna potrzeba opracowania precyzyjnych definicji zagrożeń górniczych. Z uwagi na specyfikę poszczególnych zagrożeń górniczych, podejmowane są w praktyce ruchowej różne działania dostosowane do specyficznego zagrożenia, np. inne działania podejmowane są w przypadku zagrożenia pożarowego, a inne w przypadku zagrożenia wodnego. Definicja zagrożenia winna być ostra, aby spełnić rolę operacyjną tj. móc być wykorzystana w procesie tworzenia scenariuszy działań i szacowania ryzyka.

Jeśli spojrzeć na zagrożenie Z jako na obiekt w przestrzeni U zagrożeń, to można przypisać mu skończony niepusty zbiór atrybutów (cech) $C = \{c_1, ... c_{n_C}\}$ tj. przyporządkowań (funkcji) $c : U \rightarrow V_C^c$ dla $c \in C$, gdzie V_C^c jest zbiorem wartości cechy c zwanym dziedziną cechy c.

W przypadku gdy wszystkie cechy ze zbioru C przyjmują wartości rzeczywiste, tj. $c_i : U \rightarrow \Re$ dla $i = \{1, ... n_{n_C}\}$, na zagrożenia (obiekty) ze zbioru U możemy patrzeć jak na punkty $P_u = (c_1(u), c_2(u), ..., c_{n_C}(u))$ w n_C wymiarowej przestrzeni afinicznej $\Re^{n_C}$.

Wobec tego opracowując scenariusze S_i np. prowadzenia wyrobiska górniczego w złożu z p-tu A do p-tu B, w którym występują liczne zagrożenia, aby dokonać analizy ryzyka musimy odwołać się do przestrzeni zagrożeń U. Jeśli nasza wiedza o przestrzeni U jest pełna to mamy do czynienia z przepadkiem pewności i brakiem ryzyka w podejmowaniu decyzji. Z kolei gdy nic nie wiemy o przestrzeni U mamy do czynienia z pełną niewiedzą, a więc z przypadkiem niepewności, w którym nie możemy określić prawdopodobieństwa jakiegokolwiek zdarzenia a tym samym określić ryzyka związanego z dokonanym wyborem działania. Niektórzy autorzy (Ashram, 2003) twierdzą, iż w takim przypadku, tj. pełnej niepewności uzasadnione jest przyjęcie równomiernego rozkładu prawdopodobieństwa zdarzeń. Taka postawa wydaje się być niewłaściwa, gdyż posiadanie wiedzy o rozkładzie prawdopodobieństwa zdarzeń pozwala na wyznaczenia ryzyka z tym zdarzeniem związanego, a tym samym przeczy postulowanej sytuacji pełnej niepewności. Niezależnie od różnych niuansów terminologicznych pewnym jest to, że jeśli zagrożenie nie zostanie zidentyfikowane, nie można ocenić ryzyka, a tym samym nim zarządzać.

2.2. Ryzyko a niezawodność

Rozróżnienie pomiędzy niezawodnością a ryzykiem nie ma wyłącznie znaczenia semantycznego; raczej stanowi ono główny element procesu alokacji zasobów w okresie życia produktu (czy to projektu, działań operacyjnych, utrzymania lub wymiany).

Zawodność, jako miara prawdopodobieństwa tego, ze system nie spełni oczekiwanych funkcji, nie zawiera efektów takiego zdarzenia. Z drugiej strony, ryzyko jako miara prawdopodobieństwa (tj. zawodności) i srogości (konsekwencji) niepożądanego zdarzenia włącznie jest bardziej reprezentatywne.

Bez wątpienia, nie wszystkim wadom można zapobiec za każdą cenę. Tak więc niezawodność nie może stanowić metryki zmiennej dla alokacji zasobów dopóki nie zostanie określony poziom niezawodności a priori. To prowadzi nas do dychotomii pomiędzy ryzykiem a niezawodnością z jednej strony i do optymalizacji wielokryterialnej i jednokryterialnej z drugiej. W modelu optymalizacji wielokryterialnej, poziom akceptowalnej niezawodności jest związany z odpowiednimi konsekwencjami (tj. stanowiąc miarę ryzyka) i jest zatem porównywany z towarzyszącym kosztem, który jest wymagany do redukcji ryzyka (poprzez poprawę niezawodności). W modelu z jedną funkcją celu, poziom akceptowalnej niezawodności nie jest jawnie związany z odpowiednimi konsekwencjami; raczej jest on wcześniej określany (lub parametrycznie oceniany) i tym samym jest traktowany jako ograniczenie w modelu.

Istnieją oczywiście, zarówno historyczne/ewolucyjne powody dla tego, że powszechniej stosowana jest w inżynierii analiza niezawodności niż analiza ryzyka jak również powody natury zasadniczej i funkcjonalnej. Historycznie, inżynierowie zawsze koncentrowali się na wytrzymałości materiałów, trwałości produktu, bezpieczeństwie, pewności i funkcjonalności różnych systemów. Pojęcie ryzyka jako ilościowa miara zarówno prawdopodobieństwa jak i konsekwencji (zdarzenia niekorzystnego) zniszczenia rozwinęła się stosunkowo niedawno. Z punktu widzenia zasadniczo-funkcjonalnego jednakże wielu inżynierów lub decydentów nie może robić użytku z mieszaniny dwu różnych pojęć o różnych jednostkach, prawdopodobieństwa i konsekwencji, w postaci jednego pojęcia zwanego ryzykiem jak również nie mogą zaakceptować metryki w jakiej zazwyczaj ryzyko jest mierzone. Powszechna miara ryzyka jaką jest wartość oczekiwana straty spowodowanej zajściem niekorzystnego zdarzenia – zasadniczo utożsamia zdarzenia o małym prawdopodobieństwie wystąpienia i wysokich konsekwencjach z tymi o wysokim prawdopodobieństwie zajścia i niskich konsekwencjach. W tym sensie można znaleźć podstawowe filozoficzne uzasadnienia dla inżynierów na unikanie stosowania miary ryzyka i korzystania z niezawodności. Ponadto, i to najważniejsze, korzystanie z niezawodności nie wymaga od inżyniera konieczności dokonywania wymiany między kosztami a zdarzeniem wynikającym ze zniszczenia produktu. Tak więc, inżynierowie projektanci izolują się od społecznych konsekwencji, które są produktami ubocznymi wymiany pomiędzy niezawodnością i kosztami.

3. Model zagrożeń

Zagrożeniem dla bezpieczeństwa systemu określać będziemy każde zjawisko (proces, zdarzenie) niepożądane z punktu widzenia niezakłóconego działania systemu. Takie zjawiska lub ich kumulacja w określonym miejscu i czasie, oddziałując destrukcyjnie na system, tworzą sytuację niebezpieczną dla egzystencji (rozwoju) systemu. Należy także zwrócić uwagę na możliwość powstawania sytuacji niebezpiecznych dla systemu, będących skutkiem zagrożeń wewnętrznych wynikających np. z zawodności systemu.

Zagrożenia można klasyfikować na podstawie różnych kryteriów, na przykład ze względu na:

a) własności fizykalne,
b) czas trwania,
b) zasięg.

Rozpatrzmy sytuację systemową:

$$\sum = \langle S, O, R \rangle$$

gdzie:

S – system będący obiektem zagrożeń;
O – otoczenie, które tworzą obiekty będące źródłem zagrożeń;
$R \subset S \times O$ – zbiór relacji.

System jako obiekt zagrożeń charakteryzuje się potencjałem obronnym (odpornością) P_o:

$$P_o(s) \geq 0,\ s \in S.$$

Źródło zagrożeń, z kolei, charakteryzuje się potencjałem destrukcyjnym P_d:

$$P_d(o) \geq 0,\ o \in O.$$

Na zbiorze R określono relację zagrożenia $Rz = Rz\ (o,s)$, taką że:

$$\underset{o,s}{\forall} Rz \Leftrightarrow P_d(o) \geq P_o(s)$$

czyli obiekt $s \in S$ jest zagrożony przez $o \in O$.

Relacją zagrożenia może być funkcja $Rz(t)$ czasu rzeczywistego $t \in T$. Stan zagrożenia można natomiast interpretować jako punkt na płaszczyźnie zespolonej Gaussa opisanej współrzędnymi

$$P_d(o), P_o(s), \text{ czyli } z = z(o,s) \overset{df}{=} \langle P_d(o), P_o(s) \rangle$$

Analiza systemowa sytuacji zagrożenia może być „skalowana" według dwóch kryteriów oceny:

a) prawdopodobieństwa zaistnienia stanu zagrożenia (lub innej miary charakteryzującej możliwość wystąpienia zagrożenia, np. miary rozmytej);
b) powagi stanu zagrożenia (np. ryzyko oraz wartość zabezpieczanego systemu lub wartość dysponowanych przez niego zasobów).

Poszukując analogii, należy zwrócić uwagę na techniki oceny bezpieczeństwa konstrukcji o określonej nośności i podlegające określonym obciążeniom (Haimes, 1998).

4. Model bezpieczeństwa

Jeżeli dokonano identyfikacji zagrożeń, to warunkiem bezpieczeństwa systemu jest wyposażenie go w określony potencjał obronny (odporność). W szczególności może wyrażać go określony, najczęściej warstwowy, system zabezpieczenia przed zagrożeniami.

Rozpatrzmy, jak poprzednio, pewną sytuację systemową $\sum$ oraz załóżmy, że dane są wielkości:

– zagrożenia zewnętrzne $Z(t)$ pochodzące z otoczenia (O) systemu (S), którym odpowiada funkcja potencjału destrukcyjnego;
– odporność $B(t)$ systemu (S) na zagrożenia zewnętrzne, która odpowiada funkcji potencjału obronnego.

Powyższe charakterystyki sytuacji są funkcjami losowymi o znanych rozkładach prawdopodobieństwa:

$$F(a,t) = \Pr\{Z(t) < a\},\ a \geq 0,$$
$$G(b,t) = \Pr\{B(t) < b\},\ b \geq 0,$$
$$t \in T$$

Uogólnionym wskaźnikiem bezpieczeństwa systemu może być prawdopodobieństwo, że zagrożenia nie przekroczą pewnego krytycznego (dopuszczalnego) poziomu $a_0 \geq 0$, i odporność systemu będzie większa od pewnej wartości granicznej b_o, czyli

$$\beta(t) \equiv \beta(a_o, b_o) = \Pr\{Z(t) \leq a_o,\ B(t) > b_o\}$$

co przy założeniu statystycznej niezależności rozpatrywanych wielkości prowadzi do wskaźnika oceny bezpieczeństwa systemu:

$$\beta(t) = F(a_o, t)\,[1 - G(b_o, t)]$$

Przyjmując pożądany poziom bezpieczeństwa systemu jako $\beta_o > 0$, powiemy, że w czasie T system jest bezpieczny, jeżeli w każdej chwili $t \in T$ spełniony jest warunek:

$$\beta(t) \geq \beta_o$$

W analizach bezpieczeństwa obiektów technicznych stosowane są pewne uproszczone procedury, które sprowadzają się do wyznaczenia prawdopodobieństwa „zniszczenia":

$$P = P(P_o \leq P_d),\ P_d \equiv Z(t),\ P_o \equiv B(t)$$

czyli prawdopodobieństwo zdarzenia, że uogólniona odporność (nośność) P_o nie jest większa od uogólnionego zagrożenia (obciążenia) P_d.

5. Zarządzanie bezpieczeństwem

W analizie systemowej bezpieczeństwa założono, że na efektywność systemu mają wpływ:

a) niezawodność systemu jako jego zdolność do sprawnego (bez uszkodzeń, awarii, błędów itp.) funkcjonowania w określonym czasie;
b) bezpieczeństwo systemu jako jego zdolność do skutecznego zabezpieczenia przed skutkami zagrożeń zewnętrznych

Zarządzanie bezpieczeństwem systemu stanowi integralną część zarządzania systemowego i związane jest z racjonalizacją wyboru środków (metod, technologii) zapewniających bezpieczne (zgodne z przeznaczeniem) funkcjonowanie systemu w niebezpiecznym środowisku (otoczeniu).

Jeżeli nie istnieją zagrożenia zewnętrzne, to zarządzanie bezpieczeństwem systemu można sprowadzić do problemu zarządzania niezawodnością systemu: należy dokonać wyboru takiej strategii niezawodności, dla której wartość kryterium oceny niezawodności (funkcja niezawodności systemu) przyjmuje wartość maksymalną przy spełnieniu warunku, że koszty wzrostu niezawodności (lub utrzymania niezawodności na pożądanym poziomie) nie przekroczą wartości granicznej (dopuszczalnej) – rysunek 2.

Jeżeli jednak mamy do czynienia z sytuacją zagrożenia dla bezpieczeństwa systemu, to wtedy problem zarządzania bezpieczeństwem systemu można sprowadzić do wyboru takiej strategii bezpieczeństwa (środków zabezpieczenia systemu przed zagrożeniami) ze zbioru strategii dopuszczalnych, dla której np. wartość oczekiwana skutków (strat) zagrożeń przyjmuje wartość minimalną pod warunkiem że koszty zastosowania strategii (wdrożenia środków zabezpieczenia) nie przekroczą wartości granicznej (dopuszczalnej).

Należy zauważyć, że zarówno problem zarządzania niezawodności, jak i problem zarządzania bezpieczeństwem systemu, można sprowadzić do problemu: (1) minimalizacji funkcji ryzyka pod warunkiem, że wartość efektów (użyteczności) uzyskiwanych dzięki funkcjonowaniu systemu będą nie mniejsze od wartości granicznej (pożądanej) albo (2) maksymalizacji funkcji efektywności systemu pod warunkiem, że funkcja ryzyka nie przekroczy wartości dopuszczalnej („bezpiecznej").

NIEZAWODNOŚĆ / ZAGROŻENIA	Niska	Wysoka
Brak	„zarządzanie niezawodnością": minimalizacja kosztów dla pożądanego poziomu niezawodności (ryzyka, efektywności)	„zarządzanie niezawodnością": utrzymanie stanu niezawodności dla dopuszczalnego poziomu nakładów na zabezpieczecnie przed awariami
Występują	„zarządzanie bezpieczeństwem": minimalizacja kosztów dla pożądanego poziomu niezawodności i bezpieczeństwa (ryzyka)	„zarządzanie bezpieczeństwem": minimalizacja kosztów dla pożądanego poziomu ryzyka i zachowania poziomu niezawodności

Rys. 2. Zarządzanie bezpieczeństwem

Załóżmy, że dany jest system jako obiekt zagrożenia, który charakteryzuje uogólniona funkcja bezpieczeństwa:

$$\beta = f(P_d, P_o, v)$$

gdzie: v – wartość systemu, $0 \le P_d \le P_{d\max}$, $0 \le P_o \le P_{o\max}$, $v > 0$

oraz funkcja kosztu zabezpieczenia przed zagrożeniami:

$$K = \varphi(P_o, v) > 0$$

Zakłada się, że koszty są wprost proporcjonalne zarówno do wartości sytemu, jak i wielkości dysponowanego potencjału bezpieczeństwa.

Problem optymalizacji zarządzania bezpieczeństwem systemu można sformułować jako wyznaczanie takiej wartości P_o, która maksymalizuje poziom bezpieczeństwa, czyli $\beta \rightarrow \max$, przy spełnieniu warunku: $K \leq K_0$, *gdzie* K_0 oznacza wartość dopuszczalnych nakładów na zabezpieczenia systemu przed możliwymi zagrożeniami P_d.

Załóżmy, że danych jest N względnie niezależnie funkcjonujących systemów, zaś każdy charakteryzują wielkości:

$$P_d^i, P_o^i, v^i, \beta_i, K_i, \ i = 1,2,..., N$$

Ponadto określono nadrzędny system zarządzania, który dysponuje „centralnymi" środkami (zasobami) bezpieczeństwa W. W zależności od sytuacji zagrożenia bezpieczeństwa na szczeblu lokalnym, nadrzędny ośrodek decyzyjny może przydzielić i-temu systemowi określoną wielkość potencjału W_i w celu „wzmocnienia" jego bezpieczeństwa.

Wtedy zarządzanie bezpieczeństwem można sformułować jako problem dwupoziomowej optymalizacji, a mianowicie:

a) problem nadrzędny:

$$\beta = F(\beta_1, ..., \beta_n) \rightarrow \max$$

gdzie

$$\beta_i \equiv \beta_i(P_o^i, W_i) \qquad W_i \geq 0, \qquad \sum_{i=1}^{N} W_i = W$$

pod warunkiem, że:

$$K = \sum_{i=1}^{N} K_i(P_o^i, W_i) \leq K_o ;$$

b) problem lokalny:

$$\beta_i = f_i(P_o^i, W_i) \rightarrow \max$$

$$K_i(P_o^i, W_i) \leq K_o^i, \qquad i = 1,2,..., N$$

Zakłada się przy tym, że nadrzędny system zarządzania – dzięki procesom monitorowania i diagnozowania sytuacji bezpieczeństwa – dysponuje informacjami o zagrożeniach, czyli $\{P_d^i, i = 1,2,...,N\}$ dla chwili t (lub okresu T). Stanowią one podstawę optymalizacji przydziału zasobów W_t dla poszczególnych systemów.

6. Zakończenie

Bezpieczeństwo systemów technicznych może być rozpatrywane w dwóch podstawowych aspektach, a mianowicie:

1) jako bezpieczeństwo techniki (technologii) ze względu na jej negatywne skutki (zagrożenia) dla otoczenia (środowiska społecznego, środowiska naturalnego);
2) jako bezpieczeństwo systemu technicznego wynikające z jego stanów funkcjonalnych (zawodności – niezawodności, gotowości, żywotności itp.).

Obecnie można wyróżnić dwa podstawowe nurty badań w zakresie bezpieczeństwa systemów:

1) tworzenie teoretycznych podstaw bezpieczeństwa systemów (technicznych i społecznych),
2) projektowanie systemów bezpieczeństwa, w tym zarządzania bezpieczeństwem, a więc również metod zarządzania ryzykiem (ze szczególnym uwzględnieniem sytuacji kryzysowych).

Można zatem mówić o nauce o bezpieczeństwie, obejmującej teorię i inżynierię bezpieczeństwa systemów (Tarczyński i Mojsiewicz, 2001).

Do podstawowych wniosków metodologicznych płynących z szeroko rozumianych badań systemowych nad bezpieczeństwem obiektów technicznych i społecznych można zaliczyć następujące:

1) bezpieczeństwo jest kategorią systemową, gdyż dotyczy cechy obiektów złożonych (technicznych, socjotechnicznych, społecznych) rozpatrywanych jako strukturalizowane *całości,* aktywne i w aktywnym otoczeniu funkcjonujące;
2) bezpieczeństwo systemu oznacza stan i proces, w którym system może rozwijać się (realizować swe cele rozwojowe);
3) bezpieczeństwo systemu jest pojęciem względnym, zawsze relatywizowanym do ogólnej sytuacji zewnętrznej) a ponadto może oznaczać zarówno brak zagrożenia (stan obiektywny), jak i brak poczucia zagrożenia (stan subiektywny);
4) każda sytuacja konfliktowa, w której uczestniczy dany system, zawiera w sobie potencjalne i realne zagrożenia dla bezpieczeństwa systemu;
5) bezpieczeństwo systemu zależy zarówno od wielkości zagrożeń (intensywności i efektywności oddziaływań zewnętrznych), jak i efektywności systemu zabezpieczenia (ochrony);
6) do podstawowych zadań analizy systemowej należy zaliczyć identyfikację systemowych sytuacji niebezpiecznych (krytycznych), a w tym identyfikację i ocenę źródeł zagrożeń, ich intensywności, form oraz ocenę ryzyka ich potencjalnych skutków;
7) do podstawowych zadań inżynierii bezpieczeństwa systemów należy zaliczyć opracowanie metod projektowania efektywnych systemów zabezpieczenia (ochrony) zapewniających pożądany stopień bezpieczeństwa systemów;
8) problematyka bezpieczeństwa systemów jest problematyką *stricte* interdyscyplinarną, której ranga ze względu na tworzenie się nowego ładu światowego (globalizacja, społeczeństwo informacyjne) będzie z pewnością wzrastać; przy czym na czoło wysuwać się będą problemy bezpieczeństwa systemów, transportu i komunikacji, bezpieczeństwa systemów energetycznych, bezpieczeństwa informacyjnego i ekologicznego itp.;
9) metody badania bezpieczeństwa systemów powinny w większym stopniu opierać się na nowoczesnych metodach i koncepcjach systemowych, jak np. synergetyka, termodynamika nieliniowa, teoria katastrof, teoria zbiorów rozmytych, metody probabilistyczne i posybilistyczne, teoria systemów rozwijających się, teorie konfliktów, zarządzanie kryzysowe itp.;

Praca została wykonana w roku 2008 w ramach prac statutowych realizowanych w IMG PAN w Krakowie, finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego.

Literatura

Ashram H., (2003): *Tools for Decision Analysis*. http://home.ubalt.edu/ntsbarsh/ Business-stat/opre/partIX.htm

Brachinger H.W., Weber M. (1997): *Risk as a primitive: A survey of measures of perceived risk*, OR Spectrum, vol. 19, no 4.

Cyrul T., (2004): *Identyfikacja zagrożeń jako źródeł ryzyka w działalności górniczej*. Prace Instytutu Mechaniki Górotworu PAN, Tom 6, nr 3/4, str. 315-336.

Haimes Y.Y., (1998): *Risk Analysis of fracture and failure*. J. Mat. Res. Innov., vol. 2, no 1, Springer Verlag .

Kerzner H., (2005):, *Zarządzanie projektami. Studium przypadków*, Helion, Warszawa 2005.

Kortas G., (1982), *Model stanu zagrożenia wodnego kopalń soli.* Archiwum Górnictwa, T. 27, z.1-2.

Krzemień S., (1992): Teoretyczne podstawy określania miar stanu zagrożenia bezpieczeństwa w wyrobiskach górniczych. Zeszyty Naukowe Pol. Śl., Seria Górnictwo, Z. 204, Gliwice.

Ryncarz T., (1983): *O systematycznej klasyfikacji zagrożeń występujących w górnictwie podziemnym*. Górnictwo, Kwartalnik AGH, z.3, Kraków.

Sienkiewicz P., (2003): *Geneza i rozwój koncepcji holistycznych i systemowych we współczesnej nauce.* Zeszyty Naukowe AON nr 1(50).

Sienkiewicz P., (2007): *Teoria i inżynieria bezpieczeństwa systemów.* Zeszyty Naukowe AON nr 1(66).

Sobala J., Rosmus P., (1997): System zarządzania bezpieczeństwem pracy w zakładach górniczych. GIG, Katowice

Tarczyński W., Mojsiewicz M., (2001): *Zarządzanie ryzykiem*, PWE, Warszawa 2001.

Recenzent: Dr hab. inż. *Grzegorz Kortas*, Instytut Mechaniki Górotworu PAN