The International Journal of
TRANSPORT & LOGISTICS
Medzinárodný časopis
DOPRAVA A LOGISTIKA

ISSN 1451-107X

PROPOSAL OF THE METHOD FOR SAFETY ASSESSMENT (WMOB) AS REGARDS COST CALCULATION OF RISK AND RISK ASSESSMENT[1]

Jozef Koczwara[1], Adam Zygmunt[2]

Key words: safety assessment, cost calculation of risk, risk assessment

Abstract:
A proposal of the method for safety assessment (WMOB) as regards cost calculation of risk and risk assessment in mining industry was presented in the paper. The method for safety assessment (WMOB) in relation to changes introduced to technical objects of mining plants, especially those "life" of which (time of operation) exceeds expected time of legal force of regulations, was suggested. It should be emphasized that a proposal of the method for safety assessment (WMOB) as regards cost calculation of risk and risk assessment in the mining industry is a direct transfer of regulations of Decree of Commission (EC) No. 352/2009 dated 24th April 2009.

1. Wstęp

Regulacje prawne obowiązujące w państwach członkowskich EU powinny być spójne i wzajemnie przystające. Sprawy wymagań technicznych dla bezpieczeństwa wyrobów wprowadzanych do obrotu w obszarze EU, regulują postanowienia aktów prawnych państw członkowskich implementujących do prawa krajowego odpowiednie dyrektywy EU lub wydane rozporządzenia. Problemem pozostaje jednak fakt przepisów technicznych prawa krajowego poszczególnych państw członkowskich w przypadkach zamiaru wprowadzenia zmian w obiektach technicznych np. zakładów górniczych, a szczególnie takich obiektów których czas „życia" (funkcjonowania) przekracza granice przewidywalnej przyszłości obowiązywania regulacji prawnych, np.: stacji elektroenergetycznych wysokiego i średniego napięcia, górniczych wyciągów szybowych, stacji wentylatorów głównego przewietrzania kopalń itd. Dostrzegając ten problem zaproponowano poniżej wspólną metodę oceny bezpieczeństwa (WMOB) w zakresie wyceny i oceny ryzyka w odniesieniu do zmian:

- nie uznanych za znaczące (istotne) dla bezpieczeństwa,
- uznanych za znaczące (istotne) bez udziału (interwencji) organów nadzoru górniczego,
- uznanych za znaczące z udziałem (interwencją) organu nadzoru górniczego.

Podkreślić należy, że propozycja wspólnej metody oceny bezpieczeństwa (WMOB) w zakresie wyceny i oceny ryzyka w dziedzinie górnictwa jest bezpośrednim przeniesieniem postanowień ROZPORZĄDZENIA KOMISJI (WE) NR 352/2009 z dnia 24 kwietnia 2009r. w sprawie przyjęcia wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka, o której mowa w art. 6 ust. 3 lit. a) dyrektywy 2004/49/WE Parlamentu Europejskiego i Rady.

2. Wprowadzenie

Wspólną metodę oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka (WMOB) należy stosować, aby zapewnić zachowanie równego poziomu bezpieczeństwa oraz jego poprawę, gdy jest to konieczne i praktycznie możliwe.

[1] **Jozef Koczwara, M.Sc. Eng.**, State Mining Authority, Poniatowskiego 31, 40-055 Katowice, Poland, phone: +48 32 7361724, +48 32 7361728, fax: +48 32 2514228, +48 32 2514884, e-mail: gem@wug.gov.pl
[2] **Adam Zygmunt, Ph.D. Eng.**, Mining Authority for Control Tests of Energomechanical Equipment, Obroki 87, 40-929 Katowice, Poland, phone: +48 32 7889800, fax: +48 32 7889888, e-mail: adazyg@op.pl

Aby ułatwić wzajemną akceptację sądów, należy zharmonizować metody stosowane przez podmioty uczestniczące w rozwoju i eksploatacji obiektów technicznych zakładów górniczych do identyfikacji ryzyka i zarządzania nim oraz metody wykazywania zgodności z wymogami bezpieczeństwa.
Pierwszy konieczny krok to zharmonizowanie procedur i metod przeprowadzania ocen ryzyka oraz stosowania środków nadzoru ryzyka w sytuacjach, gdy zmiana warunków prowadzenia ruchu lub wprowadzenie „nowości" (nowego rozwiązania technicznego) stwarza nowe zagrożenia (dla infrastruktury lub prowadzenia ruchu).
Jeżeli nie istnieją przepisy, na podstawie których określa się, czy zmiana jest znacząca, czy też nie, wprowadzający zmianę jest odpowiedzialny za wprowadzenie danej zmiany i dokonuje wstępnej oceny potencjalnego wpływu danej zmiany na bezpieczeństwo.
W przypadku, gdy proponowana zmiana ma wpływ na bezpieczeństwo, wprowadzający zmianę powinien ocenić znaczenie zmiany, kierując się fachowym osądem i na podstawie określonych w WMOB kryteriów.
Ocena wprowadzającego zmianę powinna prowadzić do jednego z trzech następujących wniosków:
- zmiana nie zostaje uznana za znaczącą i wprowadzający zmianę wprowadza ją stosując własną metodę oceny bezpieczeństwa,
- zmiana zostaje uznana za znaczącą i wprowadzający zmianę wprowadza, stosując zasady WMOB i wtedy nie zachodzi potrzeba interwencji ze strony organu nadzoru górniczego,
- zmiana zostaje uznana za znaczącą, ale istnieją przepisy, które nakazują podjęcie określonej interwencji przez organ nadzoru górniczego, np. wydania nowego zezwolenia na oddanie do ruchu, dopuszczenia do stosowania, aktualizacji certyfikatu bezpieczeństwa itp.

W przypadku każdej zmiany już eksploatowanego obiektu technicznego ocena znaczenia tej zmiany powinna uwzględniać wszystkie zmiany związane z bezpieczeństwem, które dokonano wcześniej. Ocena ta ma na celu sprawdzenie, czy zmiany wprowadzone wcześniej nie składają się w sumie na znaczącą zmianę, wymagającą pełnego zastosowania WMOB w zakresie wyceny i oceny ryzyka.
Dopuszczalność ryzyka związanego ze znaczącą zmianą należy badać za pomocą co najmniej jednej z następujących zasad akceptacji ryzyka:
- zastosowanie kodeksu postępowania,
- porównanie z podobnymi rozwiązaniami technicznymi,
- szacowanie jawnego ryzyka.

Wszystkie te zasady są wykorzystywane z powodzeniem w szeregu zastosowań wielu branż.
Zasada „szacowania jawnego ryzyka" jest często stosowana w przypadku zmian o charakterze kompleksowym lub nowatorskim. Odpowiedzialność za wybór zastosowanej zasady ponosi wprowadzający zmianę.
Zgodnie z powszechną zasadą proporcjonalności nie powinno się wykraczać poza to, co jest niezbędne do osiągnięcia celu w zakresie wyceny i oceny ryzyka.
W przypadku korzystania z powszechnie uznanego kodeksu postępowania należy pozwalać na ograniczony zakres stosowania WMOB.
W przypadku istnienia przepisów, które nakazują podjęcie określonej interwencji przez organ nadzoru górniczego, organ działa zgodnie z tymi przepisami.

3. Zakres

WMOB w zakresie wyceny i oceny ryzyka ma zastosowanie do wszelkich zmian, które są uznawane za znaczące. Zmiany takie mogą mieć charakter techniczny, eksploatacyjny lub organizacyjny. W przypadku zmian organizacyjnych, brane są pod uwagę pod uwagę wyłącznie zmiany, które mogą mieć wpływ na warunki eksploatacji.

4. Definicje

Stosuje się następujące definicje:
- „ryzyko" oznacza częstotliwość wypadków i incydentów prowadzących do szkody (spowodowanej zagrożeniem) oraz stopień powagi tej szkody;
- „analiza ryzyka" oznacza systematyczne wykorzystywanie wszystkich dostępnych informacji do identyfikowania zagrożeń i szacowania ryzyka;
- „wycena ryzyka" oznacza procedurę opierającą się na analizie ryzyka, która ma na celu ustalenie, czy osiągnięto poziom dopuszczalnego ryzyka;
- „ocena ryzyka" oznacza całościowy proces obejmujący analizę ryzyka i wycenę ryzyka;
- „bezpieczeństwo" oznacza brak niedopuszczalnego ryzyka szkody;
- „zarządzanie ryzykiem" oznacza planowe stosowanie polityki, procedur i praktyk zarządczych w ramach zadań dotyczących analizy, wyceny i nadzoru ryzyka;
- „interfejsy" oznacza wszystkie punkty interakcji podczas cyklu życia obiektu technicznego, w tym utrzymanie i eksploatację, w których ramach różne podmioty współpracują ze sobą, aby zarządzać ryzykiem;

- „podmioty” oznacza wszystkie strony, które są zaangażowane, bezpośrednio lub na mocy porozumień umownych,
- „wymogi bezpieczeństwa” oznacza właściwości bezpieczeństwa (jakościowe lub ilościowe) odnoszące się do obiektu technicznego i jego eksploatacji (w tym zasady eksploatacji), które są konieczne do spełnienia prawnych lub wewnętrznych celów w zakresie bezpieczeństwa;
- „środki bezpieczeństwa” oznacza pakiet działań zmniejszających częstotliwość zagrożeń albo łagodzących ich skutki, który ma na celu osiągnięcie lub utrzymanie dopuszczalnego poziomu ryzyka;
- „wnioskodawca” oznacza jednostkę organizacyjną wprowadzającą zmianę, podmioty zamawiające lub producentów, lub podmioty składające wnioski o zezwolenie, dopuszczenie itp.;
- „zagrożenie” oznacza stan, który może prowadzić do wypadku;
- „jednostka oceniająca” oznacza niezależną kompetentną osobę, organizację lub podmiot, które przeprowadzają badanie w celu ocenienia, na podstawie dowodów, o spełnieniu przez obiekt techniczny wymogów bezpieczeństwa, które się do niego stosują;
- „kryteria akceptacji ryzyka” oznacza kryteria, na podstawie których oceniana jest dopuszczalność danego ryzyka; kryteria te stosuje się, aby ustalić, czy poziom ryzyka jest na tyle niski, że nie jest konieczne podejmowanie natychmiastowych działań w celu jego zredukowania;
- „rejestr zagrożeń” oznacza dokument, w którym rejestruje się i opatruje odniesieniami zidentyfikowane zagrożenia, związane z nimi środki i źródło zagrożeń oraz wskazuje organizację, która ma nimi zarządzać;
- „identyfikacja zagrożeń” oznacza proces wykrywania zagrożeń oraz sporządzanie ich wykazu i opisu;
- „zasada akceptacji ryzyka” oznacza zasady, które są stosowane w celu wyciągnięcia wniosku o dopuszczalności lub niedopuszczalności ryzyka związanego z określonym zagrożeniem lub określonymi zagrożeniami;
- „kodeks postępowania” oznacza spisany zbiór zasad, które mogą być wykorzystywane do nadzorowania określonego zagrożenia lub określonych zagrożeń, pod warunkiem ich prawidłowego stosowania;
- „system odniesienia” oznacza system, który sprawdził się w praktyce jako system o dopuszczalnym poziomie bezpieczeństwa i z którym można porównywać system oceniany pod kątem dopuszczalności ryzyka;
- „szacowanie ryzyka” oznacza proces prowadzący do uzyskania pomiaru poziomu analizowanego ryzyka, na który składają się następujące etapy: analiza częstotliwości, analiza skutków i połączenie tych dwóch typów analiz;
- „system techniczny” oznacza obiekt techniczny, w tym projekt oraz dokumentację wykonawczą i pomocniczą; proces opracowywania systemu technicznego rozpoczyna się od opracowania specyfikacji wymogów, a kończy odbiorem technicznym obiektu technicznego; system techniczny nie obejmuje użytkowników ani ich działań, chociaż uwzględnia się projekt odpowiednich interfejsów z zachowaniami ludzi. Proces utrzymania jest opisany w instrukcjach utrzymania, ale sam nie stanowi części systemu technicznego;
- „katastroficzne konsekwencje” oznacza ofiary śmiertelne lub osoby poważnie ranne lub poważne szkody wyrządzone w wyniku wypadku;

5. Znaczące (istotne) zmiany

1. Jeżeli nie istnieją przepisy, na podstawie których określa się, czy zmiana jest znacząca, czy też nie, wnioskodawca dokonuje oceny potencjalnego wpływu danej zmiany na bezpieczeństwo.
2. W przypadku, gdy proponowana zmiana nie ma wpływu na bezpieczeństwo, nie istnieje konieczność stosowania procesu zarządzania ryzykiem.
3. W przypadku gdy proponowana zmiana ma wpływ na bezpieczeństwo, wnioskodawca, kierując się fachowym osądem, decyduje o znaczeniu zmiany na podstawie następujących kryteriów:
   a) skutki awarii systemu: wiarygodny najgorszy scenariusz w przypadku awarii ocenianego systemu, uwzględniający istnienie barier zabezpieczających poza tym systemem;
   b) innowacja wykorzystana przy wprowadzaniu zmiany; kryterium to obejmuje również innowacje wnioskodawcy;
   c) złożoność zmiany;
   d) monitoring: niezdolność monitorowania wprowadzonej zmiany podczas całego cyklu życia systemu i dokonywania odpowiednich interwencji;
   e) odwracalność zmiany: niezdolność powrotu do systemu sprzed zmiany;
   f) dodatkowość: ocena znaczenia zmiany z uwzględnieniem wszystkich przeprowadzonych niedawno zmian ocenianego systemu, które były związane z bezpieczeństwem i nie zostały

ocenione jako znaczące. Wnioskodawca przechowuje odpowiednią dokumentację, która uzasadnia jego decyzję.

6. Proces zarządzania ryzykiem

1.Opisany w załączniku I proces zarządzania ryzykiem stosuje się w przypadku znaczącej zmiany,
2.Proces zarządzania ryzykiem opisany w załączniku I jest stosowany przez wnioskodawcę.
3.Wnioskodawca gwarantuje zarządzanie ryzykiem powodowanym przez dostawców i usługodawców, w tym ich podwykonawców. W tym celu wnioskodawca może poprosić dostawców i usługodawców, w tym ich podwykonawców, o uczestniczenie w procesie zarządzania ryzykiem opisanym w załączniku I.

7. Niezależna ocena

1.Niezależnej oceny prawidłowości stosowania procesu zarządzania ryzykiem, który jest opisany w załączniku I, oraz jego wyników dokonuje jednostka spełniająca kryteria wymienione w załączniku II.
2.Wnioskodawca ustala swoją własną jednostkę oceniającą, którą może być inna jednostka organizacyjna lub dział wewnętrzny.
3.Należy unikać dublowania prac pomiędzy oceną zgodności systemu zarządzania bezpieczeństwem i/lub oceną zgodności z wymaganiami zasadniczymi.

8. Raporty w sprawie oceny ryzyka

1.Jednostka oceniająca przedstawia wnioskodawcy raport w sprawie oceny bezpieczeństwa.
2.Raport w sprawie oceny bezpieczeństwa jest brany pod uwagę przez organ nadzoru górniczego przy podejmowaniu decyzji.
3.Jeżeli dokonano już odbioru systemu lub jego części po przeprowadzeniu procesu zarządzania ryzykiem określonego WMOC, raport w sprawie oceny bezpieczeństwa dotyczący takiego wcześniejszego procesu nie powinien być kwestionowany przez inną jednostkę oceniającą, która dokonuje nowej oceny tego samego systemu.

Warunkiem uznania jest wykazanie, że system będzie użytkowany w takich samych warunkach funkcjonalnych, eksploatacyjnych i środowiskowych jak już zaakceptowany system oraz że zastosowano równoważne kryteria akceptacji ryzyka.

Literatura:

[1] opracowano w oparciu o rozporządzenie komisji (WE) NR 352/2009 z dnia 24 kwietnia 2009r. w sprawie przyjęcia wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka o której mowa w art. 6 ust. 3 lit. a) dyrektywy 2004/49/WE Parlamentu Europejskiego i Rady

Załącznik I

1. Główne zasady stosujące się do procesu zarządzania ryzykiem

1.1. Główne zasady i obowiązki

1.1.1. Proces zarządzania ryzykiem, rozpoczyna się od zdefiniowania systemu podlegającego ocenie i obejmuje następujące działania:

a) proces oceny ryzyka, w ramach którego identyfikuje się zagrożenia, ryzyko, związane z nimi środki bezpieczeństwa oraz wymogi bezpieczeństwa, które powinien spełniać oceniany system;

b) wykazanie zgodności systemu ze zidentyfikowanymi wymogami bezpieczeństwa;

c) zarządzenie wszystkimi zidentyfikowanymi zagrożeniami oraz związanymi z nimi środkami bezpieczeństwa. Proces zarządzania ryzykiem ma charakter wieloetapowy. Jego przebieg przedstawiono na schemacie w załączniku III. Proces ten kończy się z chwilą wykazania zgodności systemu ze wszystkimi wymogami bezpieczeństwa koniecznymi do zaakceptowania ryzyka związanego ze zidentyfikowanymi zagrożeniami.

1.1.2. Wieloetapowy proces zarządzania ryzykiem:

a) obejmuje odpowiednie działania w zakresie zapewnienia jakości i przeprowadza go kompetentny personel;

b) jest niezależnie oceniany przez jednostkę oceniającą lub jednostki oceniające.

1.1.3. Wnioskodawca odpowiedzialny za proces zarządzania ryzykiem, prowadzi rejestr zagrożeń zgodnie z pkt. 4.

1.1.4. Podmioty, które stosują już metody lub narzędzia oceny ryzyka, mogą je dalej stosować, o ile są one zgodne z niniejszymi WMOB i spełniają następujące warunki:

a) metody lub narzędzia oceny ryzyka są opisane w systemie zarządzania bezpieczeństwem,

b) metody lub narzędzia oceny ryzyka są zgodne z Polskimi Normami

1.1.5. Bez uszczerbku dla odpowiedzialności cywilnej zgodnej z prawnymi wymogami, za proces oceny ryzyka jest odpowiedzialny wnioskodawca. Wnioskodawca, za zgodą zainteresowanych podmiotów, decyduje w szczególności o tym, kto będzie odpowiadał za spełnienie wymogów bezpieczeństwa wynikających z oceny ryzyka. Decyzja ta jest uzależniona od charakteru środków bezpieczeństwa, które zostały wybrane, aby nadzorować ryzyko, utrzymując je na dopuszczalnym poziomie. Zgodność z wymogami bezpieczeństwa wykazuje się zgodnie z pkt. 3.

1.1.6. Pierwszy etap procesu zarządzania ryzykiem polega na określeniu przez wnioskodawcę w specjalnym dokumencie zadań poszczególnych podmiotów oraz ich działań z zakresu zarządzania ryzykiem. Wnioskodawca koordynuje bliską współpracę pomiędzy poszczególnymi zaangażowanymi podmiotami, stosownie do zadań tych podmiotów, w celu zarządzania zagrożeniami i związanymi z nimi środkami bezpieczeństwa.

1.1.7. Za ocenę prawidłowości stosowania procesu zarządzania ryzykiem opisanego w WMOB odpowiada jednostka oceny.

1.2. Zarządzanie interfejsami

1.2.1. Zainteresowane podmioty współpracują ze sobą w odniesieniu do wszystkich interfejsów mających znaczenie dla ocenianego systemu, aby identyfikować zagrożenia dotyczące tych interfejsów i środki bezpieczeństwa związane z tymi zagrożeniami oraz wspólnie nimi zarządzać. Zarządzanie wspólnym ryzykiem na interfejsach jest koordynowane przez wnioskodawcę.

1.2.2. Jeżeli podmiot stwierdzi, że istnieje potrzeba zastosowania środka bezpieczeństwa, którego nie jest w stanie wdrożyć samodzielnie, podmiot ten, działając w porozumieniu z innym podmiotem, przenosi na niego zarządzanie danym zagrożeniem zgodnie z procedurą opisaną w pkt. 4.

1.2.3. Każdy podmiot, który stwierdzi, że środek bezpieczeństwa dotyczący ocenianego systemu jest niezgodny lub nieodpowiedni, ma obowiązek zgłosić to wnioskodawcy, który z kolei poinformuje podmiot wprowadzający ten środek bezpieczeństwa.

1.2.4. Podmiot wprowadzający środek bezpieczeństwa poinformuje następnie wszystkie podmioty, których dotyczy problem w ramach ocenianego systemu lub (zgodnie z wiedzą podmiotu) w ramach innych istniejących systemów, w których stosowany jest ten sam środek bezpieczeństwa.

1.2.5. W przypadku niemożności osiągnięcia porozumienia pomiędzy dwoma podmiotami lub większą ich liczbą, za znalezienie odpowiedniego rozwiązania odpowiada wnioskodawca.

1.2.6. Jeżeli podmiot nie jest w stanie spełnić wymogu zawartego w przepisach, wnioskodawca zwraca się o radę do właściwego organu.

1.2.7. Niezależnie od definicji ocenianego systemu wnioskodawca jest zobowiązany zagwarantować, że zakres zarządzania ryzykiem obejmuje sam system oraz jego integrację w inne.

2. Opis procesu ryzyka

2.1. Opis ogólny

2.1.1. Proces oceny ryzyka jest całościowym, wieloetapowym procesem obejmującym:

a) zdefiniowanie systemu;

b) analizę ryzyka, w tym identyfikację zagrożeń;

c) wycenę ryzyka. Proces oceny ryzyka jest powiązany z zarządzaniem zagrożeniami zgodnie z pkt. 4.1.

2.1.2. Definicja systemu powinna uwzględniać co najmniej:

a) cel systemu, np. zamierzone przeznaczenie;

b) funkcje i elementy systemu, jeżeli ma to zastosowanie (w tym np. element ludzki, techniczny i operacyjny);

c) granicę systemu, z uwzględnieniem innych systemów, z którymi system ten współpracuje;

d) interfejsy fizyczne (tj. systemy, z którymi system współpracuje) i funkcjonalne (tj. nakłady i efekty dotyczące działania);

e) otoczenie systemu (np. przepływy energii i przepływy termiczne, wstrząsy, wibracje, zakłócenia elektromagnetyczne, przeznaczenie eksploatacyjne);

f) istniejące środki bezpieczeństwa oraz definicje wymogów bezpieczeństwa określonych po procesu oceny ryzyka (na kolejnych etapach);

g) założenia określające progi mające zastosowanie do oceny ryzyka.

2.1.3. Identyfikacja zagrożenia dotyczy zdefiniowanego systemu, zgodnie z pkt. 2.2.

2.1.4. Dopuszczalność ryzyka dotyczącego ocenianego systemu jest badana za pomocą jednej lub kilku z poniższych zasad akceptacji ryzyka:

a) stosowanie kodeksów postępowania (pkt 2.3);

b) porównanie z podobnymi systemami (pkt 2.4);

c) szacowanie jawnego ryzyka (pkt 2.5).

Zgodnie z ogólną zasadą, o której mowa w sekcji 1.1.5, jednostka oceniająca nie narzuca wnioskodawcy zasady akceptacji ryzyka, którą powinien stosować.

2.1.5. Wnioskodawca wykazuje w wycenie ryzyka, że wybrana zasada akceptacji ryzyka została odpowiednio zastosowana. Wnioskodawca sprawdza ponadto, czy wybrane zasady akceptacji ryzyka są stosowane konsekwentnie.

2.1.6. Zastosowanie tych zasad akceptacji ryzyka pozwoli zidentyfikować możliwe środki bezpieczeństwa, które sprawią, że ryzyko dotyczące ocenianego systemu stanie się dopuszczalne. Spośród zidentyfikowanych w ten sposób środków bezpieczeństwa zostaną wybrane środki służące do nadzoru ryzyka, które staną się wymogami bezpieczeństwa, które powinien spełniać system. Zgodność z tymi wymogami bezpieczeństwa jest wykazywana zgodnie z sekcją 3.

2.1.7. Wieloetapowy proces oceny ryzyka można uznać za zakończony, gdy wykazane zostanie, że wszystkie wymogi bezpieczeństwa zostały spełnione i nie istnieje potrzeba uwzględnienia jakichkolwiek dodatkowych, racjonalnie przewidywalnych zagrożeń.

2.2. Identyfikacja zagrożeń

2.2.1. Wnioskodawca, korzystając z szerokiej wiedzy specjalistycznej kompetentnego zespołu, identyfikuje regularnie wszystkie racjonalnie przewidywalne zagrożenia dotyczące całego ocenianego systemu, jego funkcji (jeżeli ma to zastosowanie) i interfejsów. Wszystkie zidentyfikowane zagrożenia są umieszczane w rejestrze zagrożeń zgodnie z pkt. 4.

2.2.2. Aby w ocenie móc skupić się na najważniejszym ryzyku, zagrożenia należy klasyfikować według wynikającego z nich szacowanego ryzyka. Jeżeli tak wskazuje fachowy osąd, zagrożenia związane z zasadniczo dopuszczalnym ryzykiem nie muszą być głębiej analizowane, należy je jednak umieścić w rejestrze zagrożeń. Klasyfikacja zagrożeń powinna być opatrywana uzasadnieniem, aby umożliwić jednostce oceniającej jej niezależną ocenę.

2.2.3. Ryzyka wynikające z zagrożeń mogą zostać zaklasyfikowane jako zasadniczo dopuszczalne, gdy spełnione jest kryterium, zgodnie z którym ryzyko powinno być na tyle małe, że wprowadzanie jakichkolwiek dodatkowych środków bezpieczeństwa jest nieracjonalne. Podczas fachowego osądu należy zwrócić uwagę, czy suma zasadniczo dopuszczalnego ryzyka nie przekracza określonego udziału w ryzyku całkowitym.

2.2.4. Podczas identyfikacji zagrożeń mogą zostać określone środki bezpieczeństwa. Należy je umieścić w rejestrze zagrożeń zgodnie z pkt. 4.

2.2.5. Identyfikacja zagrożeń powinna być dokonywana na poziomie szczegółowości, który jest konieczny, aby określić przypadki, w których środki bezpieczeństwa powinny utrzymywać ryzyko pod kontrolą zgodnie z jedną z zasad akceptacji ryzyka, o których mowa w pkt 2.1.4. W związku z tym konieczne może być powtarzanie etapów analizy ryzyka i wyceny ryzyka do czasu osiągnięcia dostatecznego poziomu szczegółowości, aby możliwa była identyfikacja zagrożenia.

2.2.6. W każdym przypadku gdy ryzyko jest kontrolowane za pomocą kodeksu postępowania lub systemu odniesienia, identyfikację zagrożeń można ograniczyć do:
a) sprawdzenia, czy kodeks postępowania lub system odniesienia są właściwe w danym przypadku;
b) wskazania niezgodności z kodeksem postępowania lub systemem odniesienia.

2.3. Korzystanie z kodeksów postępowania przy wycenie ryzyka

2.3.1. Wnioskodawca bada, z pomocą innych zaangażowanych podmiotów i kierując się wymogami wymienionymi w pkt 2.3.2, czy zagrożenie lub zagrożenia są objęte zakresem odpowiednich kodeksów postępowania.

2.3.2. Kodeksy postępowania spełniają przynajmniej następujące wymagania:
a) są powszechnie uznane w branży górniczej; w przeciwnym wypadku kodeks postępowania należy uzasadnić i powinien on być akceptowalny dla jednostki oceniającej;
b) są relewantne z punktu widzenia nadzoru nad rozważanymi zagrożeniami występującymi w ocenianym systemie;
c) są publicznie dostępne dla wszystkich podmiotów, które chcą z nich korzystać.

2.3.3. Wymagania przepisów ustalające proces zarządzania ryzykiem w odniesieniu do określonych systemów mogą być stosowane jako kodeksy postępowania do celów nadzoru nad zagrożeniami dla potrzeb WMOB, pod warunkiem, że spełniony jest wymóg, o którym mowa w pkt 2.3.2 lit. c).

2.3.4. W odniesieniu do systemów dla których nie ma obowiązku stosowania procesu zarządzania ryzykiem, do celów nadzoru nad zagrożeniami dla potrzeb WMOB mogą być stosowanie kodeksy postępowania, o których mowa w pkt 2.3.3.

2.3.5. Jeżeli zagrożenie lub zagrożenia są kontrolowane za pomocą kodeksów postępowania spełniających wymogi, o których mowa w pkt 2.3.2, ryzyko związane z tymi zagrożeniami uważa się za dopuszczalne. Oznacza to, że:
a) nie istnieje potrzeba głębszego analizowania tego ryzyka;
b) stosowanie kodeksów postępowania zostaje odnotowane w rejestrze zagrożeń jako wymóg bezpieczeństwa w odniesieniu do odpowiednich zagrożeń.

2.3.6. W przypadku gdy podejście alternatywne nie jest w pełni zgodne z kodeksem postępowania, wnioskodawca musi wykazać, że zastosowanie alternatywnego podejścia zapewnia co najmniej taki sam poziom bezpieczeństwa.

2.3.7. Jeżeli ryzyko dotyczące określonego zagrożenia nie może zostać zredukowane do dopuszczalnego poziomu przez zastosowanie kodeksu postępowania, należy określić dodatkowe środki bezpieczeństwa za pomocą jednej z dwóch pozostałych zasad akceptacji ryzyka.

2.3.8. Jeżeli wszystkie zagrożenia są kontrolowane za pomocą kodeksów postępowania, proces zarządzania ryzykiem można ograniczyć do:
a) identyfikacji zagrożeń zgodnie z sekcją 2.2.6;
b) odnotowania faktu stosowania kodeksu postępowania w rejestrze zagrożeń zgodnie z pkt.2.3.5;
c) udokumentowania stosowania procesu zarządzania ryzykiem zgodnie z pkt.5;
d) niezależnej oceny zgodnie z art. 6.

2.4. Korzystanie z systemu odniesienia przy wycenie ryzyka

2.4.1. Wnioskodawca bada, z pomocą innych zaangażowanych podmiotów, czy zagrożenie lub zagrożenia są uwzględnione w podobnym systemie, który można wykorzystać jako system odniesienia.

2.4.2. System odniesienia spełnia przynajmniej następujące wymagania:
a) sprawdził się już w praktyce jako system o dopuszczalnym poziomie bezpieczeństwa i również obecnie spełniłby warunki wymagane do jego zatwierdzenia;
b) ma podobne funkcje i interfejsy jak oceniany system;
c) jest eksploatowany w podobnych warunkach eksploatacji jak oceniany system;
d) jest eksploatowany w podobnych warunkach środowiskowych jak oceniany system.

2.4.3. Jeżeli system odniesienia spełnia wymogi wymienione w pkt 2.4.2, oznacza to, że w przypadku ocenianego systemu:
a) ryzyko związane z zagrożeniami uwzględnionymi w systemie odniesienia uważa się za dopuszczalne;
b) wymogi bezpieczeństwa dotyczące zagrożeń uwzględnionych w systemie odniesienia można przenieść z analiz dotyczących bezpieczeństwa lub z oceny zapisów dotyczących bezpieczeństwa systemu odniesienia;
c) określone w ten sposób wymogi bezpieczeństwa odnotowuje się w rejestrze zagrożeń jako wymogi bezpieczeństwa dotyczące odpowiednich zagrożeń.

2.4.4. Jeżeli występują różnice pomiędzy ocenianym systemem a systemem odniesienia, wycena ryzyka powinna wykazać, że oceniany system cechuje co najmniej taki sam poziom bezpieczeństwa jak system odniesienia. W takim przypadku ryzyko związane z zagrożeniami uwzględnionymi w systemie odniesienia uważa się za dopuszczalne.

2.4.5. Jeżeli niemożliwie jest wykazanie takiego samego poziomu bezpieczeństwa jak w przypadku systemu odniesienia, należy określić, za pomocą jednej z dwóch pozostałych zasad akceptacji ryzyka, dodatkowe środki bezpieczeństwa w odniesieniu do różnic między systemami.

2.5. Szacowanie i wycena jawnego ryzyka

2.5.1. W przypadku gdy zagrożenia nie są objęte jedną z dwóch zasad akceptacji ryzyka opisanych w pkt. 2.3 i 2.4, dopuszczalność ryzyka jest udowadniana za pomocą szacowania i wyceny jawnego ryzyka. Ryzyka wynikające z tych zagrożeń powinny być szacowane jakościowo lub ilościowo, z uwzględnieniem istniejących środków bezpieczeństwa.

2.5.2. Dopuszczalność szacowanego ryzyka jest badana za pomocą kryteriów akceptacji ryzyka, które wynikają z wymogów prawnych albo bazują na tych wymogach. W zależności od kryteriów akceptacji ryzyka dopuszczalność ryzyka może być badana pojedynczo, w odniesieniu do każdego powiązanego zagrożenia, lub zbiorczo, w odniesieniu do kombi-nacji wszystkich zagrożeń rozważanych w wycenie jawnego ryzyka. Jeżeli szacowane ryzyko nie jest dopuszczalne, należy określić i wdrożyć dodatkowe środki bezpieczeństwa, aby zredukować ryzyko do dopuszczalnego poziomu.

2.5.3. Jeżeli ryzyko związane z zagrożeniem lub kombinacją kilku zagrożeń jest uważane za dopuszczalne, zidentyfikowane środki bezpieczeństwa zostają odnotowane w rejestrze zagrożeń.

2.5.4. Jeżeli zagrożenia wynikają z awarii systemów technicznych, które nie są objęte kodeksami postępowania ani nie można wykorzystać w ich przypadku systemu odniesienia, wówczas w odniesieniu do projektu systemu technicznego ma zastosowanie poniższe kryterium akceptacji ryzyka. Ryzyko związane z systemami technicznymi, w przypadku których zachodzi wiarygodne prawdopodobieństwo katastroficznych konsekwencji w bezpośrednim wyniku awarii działania, nie musi być dalej redukowane, jeżeli częstotliwość takich awarii jest równa lub mniejsza niż 10^{-9} na godzinę pracy systemu.

2.5.5. Bez uszczerbku dla procedur określonych w przepisach można przewidzieć bardziej rygorystyczne kryterium w celu utrzymania poziomu bezpieczeństwa.

2.5.6. W przypadku systemu technicznego, który został opracowany przy użyciu określonego w pkt 2.5.4 kryterium 10^{-9}, stosuje się zasadę wzajemnej akceptacji.

2.5.7. Szacowanie i wycena jawnego ryzyka spełniają co najmniej następujące wymogi:

a) metody stosowane do celów szacowania jawnego ryzyka są prawidłowo dobrane do ocenianego systemu i jego parametrów (w tym wszystkich trybów pracy);

b) wyniki są dostatecznie dokładne, aby mogły służyć jako wiarygodne uzasadnienie decyzji, tzn. niewielkie zmiany w założeniach wejściowych lub warunkach wstępnych nie powodują znacząco odmiennych wyników dotyczących wymogów.

3. Wykazywanie niezgodności z wymogami bezpieczeństwa

3.1. Przed odbiorem zmiany w zakresie bezpieczeństwa należy wykazać pod nadzorem wnioskodawcy, że spełnia ona wymogi bezpieczeństwa określone na etapie oceny ryzyka.

3.2. Do wykazania zgodności zobowiązany jest każdy podmiot odpowiedzialny za spełnienie wymogów bezpieczeństwa, stosownie do pkt 1.1.5.

3.3. Jednostka oceniająca dokonuje niezależnej oceny podejścia przyjętego do celów wykazania zgodności z wymogami bezpieczeństwa oraz samego wykazania.

3.4. Gdy środki bezpieczeństwa, dzięki którym powinny zostać spełnione wymogi bezpieczeństwa, okażą się nieodpowiednie lub gdy podczas wykazywania zgodności z wymogami bezpieczeństwa odkryte zostaną nowe zagrożenia, wnioskodawca dokonuje ponownej oceny i wyceny powiązanego ryzyka zgodnie z pkt. 2. Nowe zagrożenia są umieszczane w rejestrze zagrożeń zgodnie z pk. 4.

4. Zarządzanie zagrożeniami

4.1. Proces zarządzania zagrożeniami

4.1.1. Podczas etapu planowania i wdrażania oraz przed odbiorem zmiany albo przedłożeniem raportu w sprawie oceny bezpieczeństwa wnioskodawca tworzy rejestr lub rejestry zagrożeń, a jeżeli taki rejestr lub rejestry już istnieją, aktualizuje je. W rejestrze zagrożeń rejestruje się monitoring ryzyka związanego ze zidentyfikowanymi zagrożeniami. Po odbiorze systemu i rozpoczęciu jego eksploatacji rejestr zagrożeń jest dalej prowadzony przez zarządcę infrastruktury odpowiedzialnego za eksploatację ocenianego systemu, jako integralny element systemu zarządzania bezpieczeństwem tego zarządcy.

4.1.2. Rejestr zagrożeń obejmuje wszystkie zagrożenia oraz wszystkie związane z nimi środki bezpieczeństwa i założenia dotyczące systemu, które zostały określone podczas procesu oceny ryzyka. Rejestr ten powinien w szczególności wskazywać wyraźnie źródło zagrożenia i wybrane zasady akceptacji ryzyka oraz podmiot lub podmioty odpowiedzialne za nadzór nad każdym zagrożeniem.

4.2. Wymiana informacji

Wszystkie zagrożenia i związane z nimi wymogi bezpieczeństwa, których nie jest w stanie samodzielnie nadzorować jeden podmiot, są zgłaszane innemu właściwemu podmiotowi w celu wspólnego opracowania odpowiedniego rozwiązania. Zagrożenia figurujące w rejestrze zagrożeń prowadzonym przez podmiot, który dokonuje przeniesienia zagrożeń, są „nadzorowane" tylko wówczas, gdy wycena ryzyka związanego z tymi zagrożeniami została dokonana przez inny podmiot, a rozwiązanie zostało uzgodnione przez wszystkie zainteresowane strony.

5. Dowody wynikajace ze stosowania procesu zarządzania ryzykiem

5.1. Proces zarządzania ryzykiem stosowany do celów oceny poziomów bezpieczeństwa i zgodności z wymogami bezpieczeństwa jest dokumentowany przez wnioskodawcę w taki sposób, że wszystkie niezbędne dowody świadczące o prawidłowym stosowaniu procesu zarządzania ryzykiem są dostępne dla jednostki oceniającej. Jednostka oceniająca przedstawia swoje wnioski w raporcie w sprawie oceny bezpieczeństwa.

5.2. Dokument przedstawiony przez wnioskodawcę zgodnie z pkt 5.1 obejmuje co najmniej:

a) opis organizacji i specjalistów wyznaczonych do przeprowadzenia procesu oceny ryzyka;

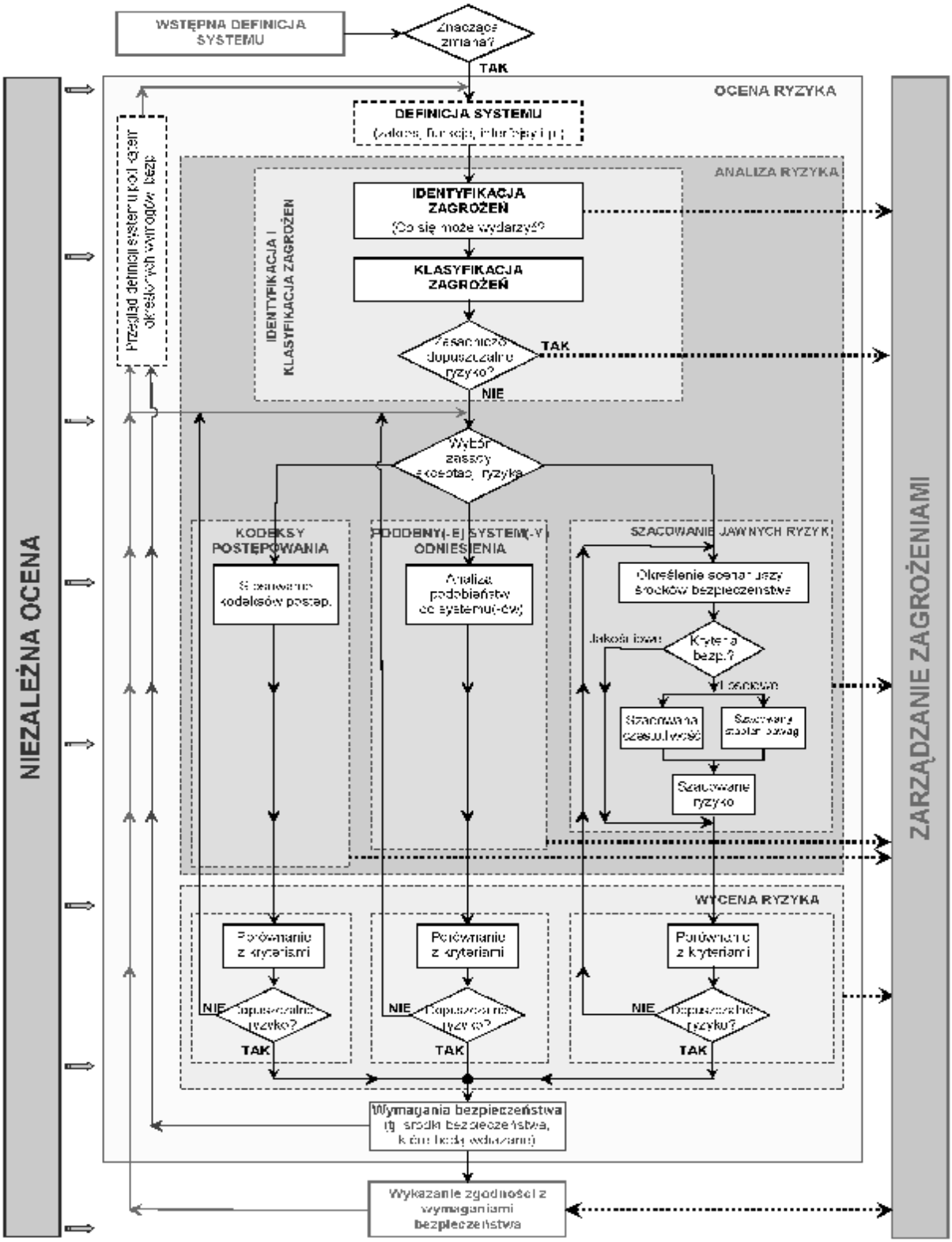
b) wyniki poszczególnych etapów oceny ryzyka oraz wykaz wszystkich wymogów bezpieczeństwa, których dopełnienie jest konieczne, aby nadzorować ryzyko, utrzymując je na dopuszczalnym poziomie.

Załącznik II

KRYTERIA, KTÓRE MUSZĄ SPEŁNIAĆ JEDNOSTKI OCENIAJĄCE

1. Jednostka oceniająca nie może być zaangażowana, bezpośrednio ani jako upoważniony przedstawiciel, w projektowanie, wytwarzanie, budowę, wprowadzanie do obrotu, eksploatację lub utrzymanie ocenianego systemu. Powyższe kryterium nie wyklucza możliwości wymiany informacji technicznych między tą jednostką a wszystkimi zaangażowanymi podmiotami.
2. Jednostka oceniająca ma obowiązek przeprowadzić ocenę z zachowaniem najwyższego stopnia uczciwości zawodowej i kompetencji technicznych oraz nie może podlegać żadnym naciskom ani wpływom, zwłaszcza natury finansowej, które mogłyby mieć wpływ na jej osąd lub wyniki ocen, w szczególności ze strony osób lub grup osób, których dotyczą te oceny.
3. Jednostka oceniająca musi posiadać środki niezbędne do rzetelnej realizacji zadań technicznych i administracyjnych związanych z ocenami. Jednostka powinna mieć także dostęp do sprzętu potrzebnego do dokonywania ocen nadzwyczajnych.
4. Personel odpowiedzialny za oceny:
   - musi być odpowiednio przeszkolony technicznie i zawodowo,
   - musi posiadać wystarczającą znajomość wymogów dotyczących przeprowadzanych przez niego ocen oraz wystarczające doświadczenie praktyczne w ich przeprowadzaniu,
   - musi posiadać umiejętność sporządzania raportów w sprawie oceny bezpieczeństwa, które stanowią formalne wnioski z przeprowadzonych ocen.
5. Niezbędne jest zagwarantowanie niezależności pracowników odpowiedzialnych za przeprowadzanie niezależnych ocen. Urzędnik nie może być wynagradzany w oparciu o liczbę przeprowadzonych ocen ani o ich wyniki.
6. Jeżeli jednostka oceniająca nie należy do struktury organizacyjnej wnioskodawcy, jednostka ta ma obowiązek posiadać ubezpieczenie od odpowiedzialności cywilnej, chyba że zgodnie z prawem odpowiedzialność cywilna spoczywa na państwie
7. Jeżeli jednostka oceniająca nie należy do struktury organizacyjnej wnioskodawcy, personel tej jednostki jest zobowiązany do przestrzegania tajemnicy zawodowej w odniesieniu do wszystkich informacji pozyskanych podczas wykonywania obowiązków (z wyjątkiem właściwych organów administracyjnych w państwa).

Załącznik III



Recenzia/Review: *Ing. Nikoleta Husáková, PhD.*