dr hab. inż. ANDRZEJ BIAŁAS
Instytut Technik Innowacyjnych EMAG

Zarządzanie ciągłością działania oraz bezpieczeństwem informacji i innych zasobów w górnictwie

Artykuł poświęcony jest sposobom rozwiązywania wybranych problemów dotyczących ciągłości działania i ochrony zasobów, w tym zasobów informacji, w przedsiębiorstwie branży górniczej z wykorzystaniem zintegrowanego, komputerowo wspomaganego systemu OSCAD. System ten powstał na bazie standardów międzynarodowych: BS 25999/ISO 22301 (ciągłość działania) i ISO/IEC 27001 (bezpieczeństwo informacji). Po zaprezentowaniu budowy i możliwości funkcjonalnych samego narzędzia uwagę skupiono na funkcjach, które zdaniem autora są najbardziej użyteczne w warunkach zakładu górniczego, tj. na: analizowaniu incydentów i spowodowanych przez nie strat, tworzeniu związanych z tym statystyk, analizowaniu parametrów bezpieczeństwa i parametrów produkcji oraz zarządzania ryzykiem. Dane zgromadzone w toku tych analiz mogą służyć kierownictwu do doskonalenia procesów produkcji oraz do poprawy bezpieczeństwa załóg. Rozważania prowadzone są na poziomie zakładu górniczego (proces wydobycia) oraz częściowo na poziomie spółek koordynujących pracę tych zakładów (procesy zarządzania). W podsumowaniu zwrócono uwagę na inne potencjalne możliwości wykorzystania oprogramowania OSCAD w górnictwie.

1. WSTĘP

Zapewnienie ciągłości działania, jak również ochrona zasobów przedsiębiorstwa czy instytucji wpływają pozytywnie na efektywność ich funkcjonowania. Realizacja tego celu sprowadza się do kontrolowania czynników zakłócających prawidłowe funkcjonowanie lub naruszających zasoby firmy czy instytucji. Podczas analizy ryzyka prognozuje się czynniki szkodliwe, a w przypadku ich wystąpienia następuje zaplanowana reakcja zmierzająca do minimalizacji strat i do możliwie szybkiego przywrócenia funkcjonowania na zadanym poziomie.

W każdej dziedzinie w nieco odmienny sposób podchodzi się do rozwiązywania tych problemów. Zależy to od wymagań biznesowych, specyfiki funkcjonowania firmy czy instytucji oraz charakteru czynników szkodliwych. Artykuł prezentuje te zagadnienia na przykładzie przedsiębiorstwa branży górniczej, rozpatrując je na dwóch poziomach:

- na poziomie biznesowym, w odniesieniu do spółki górniczej koordynującej pracę zakładów górniczych; należy zwrócić uwagę, że działalność biznesowa spółki jest podobna do działalności innych przedsiębiorstw,
- na poziomie procesu wydobycia węgla realizowanego w warunkach zakładu górniczego; występują tu problemy charakterystyczne dla działalności zakładu górniczego.

Artykuł przedstawia, w jaki sposób te zagadnienia można rozwiązać, wykorzystując produkty niedawno zakończonego projektu celowego OSCAD (Otwarty Szkieletowy System Zarządzania Ciągłością Działania), który był współfinansowany przez Narodowe Centrum Badań i Rozwoju oraz Instytut Technik Innowacyjnych EMAG [1]. Wynikiem realizacji projektu OSCAD są:

1. Zbiór wzorców projektowych służących do ustanowienia i wdrożenia systemu zarządzania ciągłością działania i bezpieczeństwem informacji w instytucji. Składa się na niego szkielet systemu

(ang. *framework*), w którym są osadzone procesy zarządzania zgodnie z wymaganiami normy. Wzorce dotyczą specyfikacji procesów zarządczych, wymagań bezpieczeństwa i ciągłości działania, instrukcji oraz innych dokumentów.

2. Metodyka wdrażania systemu zarządzania ciągłością działania i bezpieczeństwem informacji w różnego typu instytucjach. Określa ona, jak na podstawie wspomnianych wzorców zbudować system zarządzania dla danej instytucji, i obejmuje: badanie struktury biznesowej instytucji, opracowanie polityki zarządzania bezpieczeństwem informacji, polityki zarządzania ciągłością działania i założeń do dokumentacji systemu, analizę procesów biznesowych, opracowanie planów ciągłości działania, analizę potrzeb biznesowych i ryzyka danej instytucji, dobór zabezpieczeń i ich wdrożenie oraz metody utrzymania i kontroli osiągniętego poziomu bezpieczeństwa i ciągłości działania, w tym prowadzenia audytów i przeglądów.
3. Oprogramowanie OSCAD wspomagające proces wdrażania i utrzymywania systemu zarządzania ciągłością działania i bezpieczeństwem informacji. Narzędzie wyposażono w serwer informacji statystycznych o incydentach OSCAD-STAT.
4. Wiedza niezbędna do wdrożenia systemu zarządzania ciągłością działania i bezpieczeństwem informacji zawarta w podręcznikach użytkowania, administrowania i wdrażania systemu OSCAD.

Podstawowa wersja OSCAD, opracowana w toku projektu celowego, powstała na bazie obowiązujących na świecie standardów:

- BS 25999 [2, 3], dotyczącego systemów zarządzania ciągłością działania (SZCD) instytucji (ang. *BCMS – Business Continuity Management System*); obecnie ten standard został zastąpiony przez ISO 22301 [4] (wersja rozszerzona względem poprzednika i o większym zasięgu międzynarodowym);
- ISO/IEC 27001 [5, 6], dotyczącego systemów zarządzania bezpieczeństwem informacji (SZBI) instytucji (ang. *ISMS – Information Security Management System*).

Ciągłość działania [2, 3] jest określana jako strategiczna i taktyczna zdolność instytucji do:

- zaplanowania reagowania i samego reagowania na incydenty oraz zakłócenia w funkcjonowaniu biznesowym instytucji w celu kontynuowania jej działalności na akceptowalnym, wcześniej ustalonym poziomie,
- ograniczania strat w przypadku wystąpienia incydentów lub innych zakłóceń.

Rozważa się dostępność procesów (lub usług), co jest utożsamiane z ciągłością działania. W warunkach przedsiębiorstwa górniczego zagadnienie ciągłości działania występuje zarówno na poziomie spółki, jak i zakładu górniczego, przy czym inne czynniki zakłócające dotyczą każdego z tych przypadków.

Bezpieczeństwo informacji [5, 6] sprowadza się do ochrony jej trzech podstawowych atrybutów: integralności, dostępności i poufności – niezależnie od postaci informacji i miejsca jej występowania (informacje przetwarzane, przechowywane, przesyłane w systemach, wydruk, głos, obraz). Zapewnienie integralności informacji sprowadza się do tego, by w sposób nieautoryzowany informacja nie mogła być fałszowana, fabrykowana czy też usuwana. Ochrona dostępności informacji (lub procesu, usługi) sprowadza się do zapewnienia, by informacja (proces, usługa) była możliwa do wykorzystania w założonym czasie wyłącznie przez podmiot, który ma do tego prawo (autoryzowany). W przypadku poufności chodzi o zapewnienie, by informacja nie była udostępniana lub ujawniana nieautoryzowanym podmiotom.

W warunkach przedsiębiorstwa górniczego zagadnienie bezpieczeństwa informacji występuje na obu rozważanych w artykule poziomach, jednak jego charakter jest inny na każdym z nich.

Jak już wspomniano, informacja jest zasobem, który może być chroniony według ISO/IEC 27001. W toku realizacji projektu OSCAD zauważono duże podobieństwo zagadnień ochrony informacji i ochrony innych rodzajów zasobów. Ogólnie rzecz biorąc, rozważa się zawsze ochronę zasobu przed zagrożeniami, które mają zdolność wykorzystywania podatności (słabości systemu ochrony), co prowadzi do następstw (strat). Część tego typu zdarzeń może być mało dotkliwa, stąd są one pomijane. Jednak niektóre mogą przynosić znaczące straty i wówczas te zdarzenia są nazywane incydentami. W systemach przeznaczonych do ochrony różnego typu zasobów prognozuje się ryzyko zmaterializowania się zagrożeń, objawiającego się w postaci incydentów [7, 8]. Stosowanie zabezpieczeń pozwala obniżyć ryzyko. Obszerne przedstawienie zagadnień analizy ryzyka i zarządzania ryzykiem zawiera monografia [9]. Przeprowadzono badania sposobów ochrony różnego typu zasobów, w wyniku których powstały wersje systemu OSCAD dedykowane do innych zastosowań – ukierunkowane na ochronę innego typu zasobów, niż informacje.

Jedna z wersji dedykowanych powstała do ochrony zasobów produkcyjnych zakładu górniczego. Zasobami są środki techniczne i personel zaangażowane w proces wydobycia kopalin. Ochronę tego typu zasobów można rozpatrywać z punktu widzenia integralności i dostępności, gdyż poufność nie ma tu zastosowania.

Inne przykłady wersji dedykowanych to wersje: do planowania i wspomagania działań związanych z ryzykiem pożaru [10] oraz do ochrony ludzi, mienia i infrastruktury przed powodzią [10]. Ta druga dedykowana wersja (tzw. OSCAD-Flood) jest wykorzystywana jako komponent oceny ryzyka przed powodzią na terenie kraju związkowego Saksonia-Anhalt w Niemczech w ramach jednego z pięciu przypadków użycia (ang. *use cases*) projektu EC FP7 ValueSec [11].

System OSCAD jest systemem zintegrowanym, co znaczy, że uwzględnia w sobie więcej niż jeden aspekt zarządzania w instytucji (tu: ciągłość działania i bezpieczeństwo informacji) z możliwością rozszerzenia o inne aspekty (jakość, środowisko, BHP itp.). Tego typu systemy zarządzania budowane są w oparciu o popularne normy (ISO 9001, ISO 14000, ISO 18000), bazujące na tzw. cyklu W.E. Deminga: Planuj-Wykonaj-Sprawdzaj-Działaj (ang. *PDCA – Plan-Do-Check-Act*) [12]. Do integracji tych systemów zarządzania w warstwie organizacyjno-proceduralnej wykorzystuje się zalecenia brytyjskie – BS PAS 99 [13].

OSCAD jest systemem komputerowo wspomaganym, gdyż obejmuje zarówno warstwę proceduralno-organizacyjną, jak i oprogramowanie wspomagające procesy zarządzania. Od strony informatycznej integracji dokonano na poziomie wspólnej bazy danych [14]. Najbardziej złożone, powtarzalne lub żmudne czynności operatorskie są realizowane za pomocą tego specjalistycznego oprogramowania. Uzyskuje się przy tym korzyści podobne do korzyści z systemów komputerowego wspomagania projektowania czy wytwarzania (CAD/CAM).

OSCAD jest systemem otwartym, możliwym do zastosowania w instytucjach lub firmach o różnej wielkości i o różnym profilu funkcjonowania, jednak – jak już wcześniej wspomniano – każdorazowo wymaga on pewnego przystosowania do potrzeb danej dziedziny. W zastosowaniach typowych, pokrywających się z zastosowaniem standardów ISO 22301 i ISO/IEC 27001, zakres przystosowania jest mniejszy. Sprowadza się do opracowania słowników, ról, dokumentów, wykorzystania standardowych list zasobów, zagrożeń i podatności w toku analizy ryzyka itp. W przypadku tzw. wersji dedykowanych, na przykład górniczej, zakres przystosowania jest szerszy. Może dodatkowo obejmować przygotowanie danych do opisania dziedziny, specyficznych interfejsów zewnętrznych, a nawet zmodyfikowania napisów menu oprogramowania i komunikatów.

W artykule zwięźle opisano funkcjonalność systemu OSCAD, zidentyfikowano zagadnienie ciągłości działania oraz ochrony zasobów na poziomie spółki i zakładu górniczego, a następnie zaproponowano rozwiązania najważniejszych w tym obszarze problemów. Wskazano przykłady kilku możliwych zadań, które mogą być tam realizowane przy pomocy systemu OSCAD. W podsumowaniu zwrócono uwagę na inne potencjalne możliwości wykorzystania oprogramowania OSCAD w górnictwie.

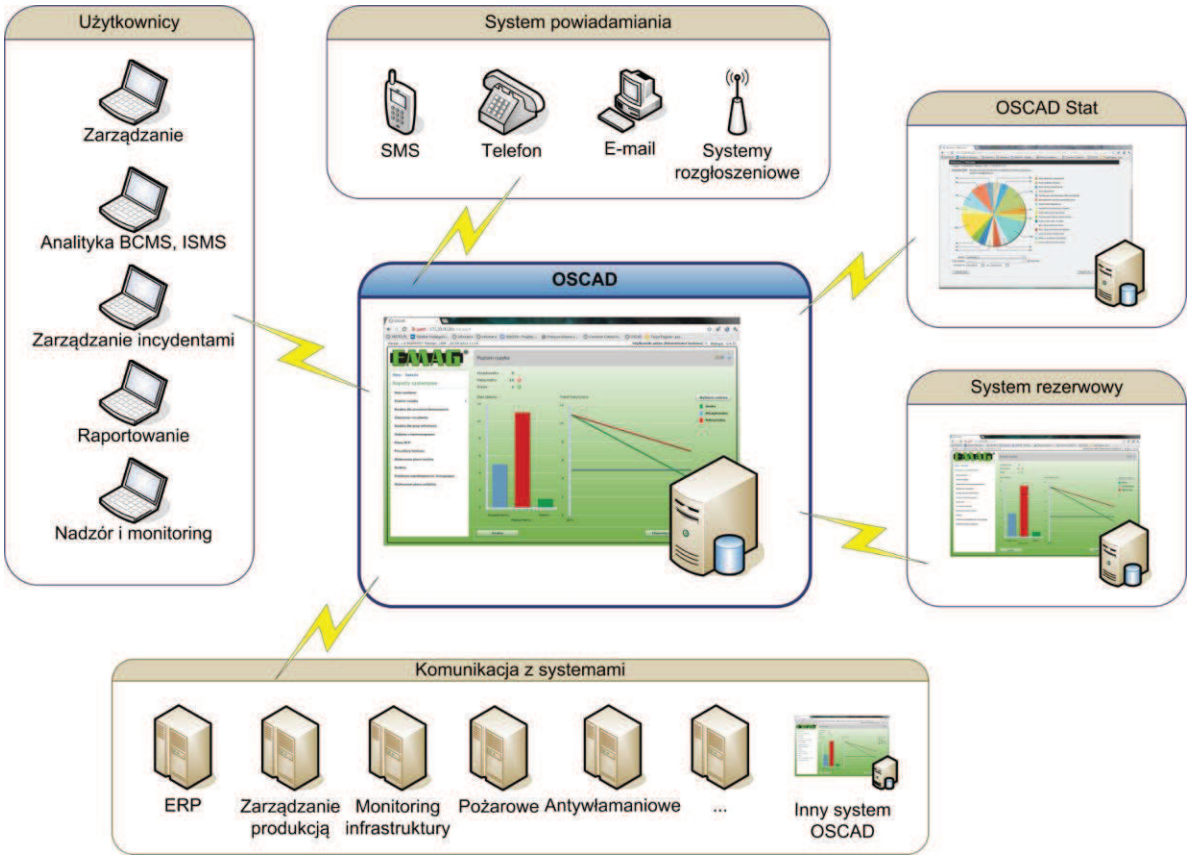
2. ARCHITEKTURA OPROGRAMOWANIA OSCAD I REALIZOWANE PRZEZ NIE FUNKCJE

Schemat oprogramowania systemu OSCAD, zrealizowanego na zasadzie serwer-klient, przedstawiono na rys. 1. Użytkownicy kontaktują się z serwerem za pomocą przeglądarek internetowych. Schemat jest na tyle ogólny, że odnosi się zarówno do wersji podstawowej, jak i dedykowanych. W centralnej części zaznaczono komponent główny OSCAD, który oferuje interfejsy dla różnych użytkowników według pełnionych przez nich ról: dla administratorów, dla osób zarządzających, dla prowadzących analizy, zwłaszcza analizę ryzyka, dla zarządzających incydentami, dla osób przygotowujących raporty oraz personelu utrzymania. Dla wersji dedykowanych definiowane są specyficzne role związane z pełnionymi stanowiskami – na przykład dla wersji górniczej mogą to być role: dyspozytor, nadsztygar, inspektor BHP.

System OSCAD wyposażono w szereg interfejsów do komunikowania się z otoczeniem. Służą one m.in. do pobierania informacji, w tym komunikatów ostrzegawczych z systemów otoczenia, w szczególności z systemów:

- typu ERP (ang. *Enterprise Resource Planning*), np. o kończących się zapasach komponentów do produkcji,
- typu SCADA (ang. *Supervisory Control and Data Acquisition*) nadzorujących zautomatyzowany proces produkcji, np. o zdarzeniach zachodzących w procesie wytwarzania,
- monitorujących funkcjonowanie infrastruktury teleinformatycznej i innych infrastruktur technicznych, np. o awariach i innych incydentach o podłożu teleinformatycznym,
- antywłamaniowych, np. o naruszeniach stref dostępu,
- przeciwpożarowych, np. o symptomach pożaru.

Dany komponent OSCAD komunikuje się (np. przekazując ostrzeżenia o zagrożeniach lub podatnościach) z innymi komponentami OSCAD pracującymi w firmach danego łańcucha dostaw. Możliwość ta może być wykorzystana do komunikowania się komponentu OSCAD spółki z komponentami OSCAD zakładów górniczych.



Rys. 1. Schemat ogólny systemu OSCAD (źródło: Instytut EMAG)

W przypadku wersji dedykowanej dla zakładu górniczego poprzez dostępne interfejsy można podłączyć systemy funkcjonujące w tym zakładzie. Obecnie istnieje połączenie z systemem dyspozytorskim SD 2000, monitorującym parametry produkcji i bezpieczeństwa. Istnieje możliwość integracji z innymi tego typu systemami, na przykład z systemem THOR firmy SEVITEL.

Każdy komponent OSCAD wyposażono w podsystem łączności (e-mail, urządzenia mobilne, telefon itp.), służący do przyjmowania i wysyłania komunikatów ostrzegawczych oraz powiadomień o zadaniach przydzielonych do wykonania dla personelu zarządzającego. W tym przypadku możliwe jest połączenie ze stosowanymi w zakładach górniczych systemami łączności i powiadamiania.

W przypadku zagrożenia komponentu OSCAD następuje przełączenie na równolegle działający komponent rezerwowy OSCAD. Jest to możliwe, gdyż podczas normalnej pracy OSCAD rezerwowy replikuje bazy danych i wymienia się sygnałem czuwania.

Istotnym elementem systemu jest moduł OSCAD-STAT, który przyjmuje informacje o zakończonych incydentach pochodzących z jednego lub kilku komponentów OSCAD, tworzy dla nich różnorodne statystyki, które następnie są udostępniane kadrze zarządzającej. Dane statystyczne są podstawą do realizacji działań korygujących i doskonalących systemy zarządzania, jak również mogą być pomocne podczas analizy ryzyka (do periodycznej weryfikacji prognoz ryzyka). Działania te ułatwiają bardzo rozbudowane funkcje raportowania. W przypadku wersji dedykowanej dla zakładu górniczego mogą to być dowolnie zdefiniowane statystyki dotyczące bezpieczeństwa, przestojów, awarii itp. Wystarczy uruchomić jeden komponent OSCAD-STAT dla całego przedsiębiorstwa. Zebranie obszernych informacji na temat incydentów i ich przyczyn pozwala na doskonalenie systemów zabezpieczeń, procesów zarządzania i utrzymania.

System OSCAD realizuje kilka grup funkcji. **Grupa funkcji ogólnego przeznaczenia** obejmuje funkcje:

- administracji i gromadzenia danych, służące do: zarządzania rolami i kontami użytkowników, zarządzania danymi opisującymi instytucję, jej strukturę organizacyjną, procesy biznesowe, słownictwo, normy, wzorce itp.,
- zarządzania dokumentacją; wszelkie dokumenty wytworzone lub zarejestrowane w systemie posiadają swoje metryki, przez co można nimi zarządzać; dokumenty mogą występować jako formularze elektroniczne lub pliki dołączone do systemu,

- komunikacji zewnętrznej, grupujące różnego rodzaju interfejsy komunikacyjne służące do dwustronnej wymiany informacji,
- zarządzania zadaniami; koordynują one proces realizacji zadań przydzielonych do osób pełniących w systemie wyznaczone role; wszystkie działania zarządcze w systemie traktowane są jako zadania do wykonania; zadania mogą być grupowane w czasie w postaci harmonogramów,
- raportowania, pozwalające na generowanie różnego typu raportów, w tym porównawczych.

Grupa funkcji do zarządzania ryzykiem realizuje następujące zadania:

- identyfikację i specyfikację procesów biznesowych instytucji, z uwzględnieniem grup informacji (i innych zasobów) związanych z realizacją poszczególnych procesów,
- przeprowadzenie analizy typu BIA (ang. *Business Impact Analysis*); w kilku definiowanych horyzontach czasowych bada się skutki utraty atrybutu dostępności wybranego procesu oraz skutki utraty atrybutów integralności, dostępności i poufności zasobów informacji (integralności i dostępności dla innych zasobów); skutki określają szkodliwy wpływ na funkcjonowanie instytucji lub firmy; tego typu analiza nazywana jest też ogólną albo wysokopoziomową analizą ryzyka (ang. *HLRA – High Level Risk Analysis*); identyfikowane są procesy o krytycznym znaczeniu dla instytucji i wyznaczane są maksymalne, tolerowane czasy niedostępności procesów; analiza ta skupia się więc na negatywnych skutkach dla realizacji zadań biznesowych wynikających z prognozowanych incydentów,
- zgromadzenie szczegółowych informacji o zasobach instytucji wymagających ochrony, a związanych z realizacją jej procesów biznesowych; są to funkcje realizowane przez inwentaryzator zasobów; w wersji podstawowej rozważa się zasoby informacyjne, zaś w wersjach dedykowanych – inne zasoby wymagające ochrony, np. życie i zdrowie człowieka;
- przeprowadzenie szczegółowej (niskopoziomowej) analizy ryzyka (ang. *LLRA – Low Level Risk Analysis*), która pozwala określić wartość ryzyka dla każdej trójki zasób-zagrożenie-podatność (scenariusza ryzyka); uwzględniane są przy tym istniejące zabezpieczenia, ich stopień zaawansowania technicznego (zautomatyzowane, proceduralne) i stopień wdrożenia (planowane, implementowane, funkcjonujące); analiza ta skupia się na przyczynach prognozowanych incydentów,
- dobór zabezpieczeń redukujących wielkość ryzyka (zarządzanie ryzykiem); dla każdego scenariusza ryzyka można rozważyć do pięciu wariantów zabezpieczeń różniących się zdolnością do obniżenia ryzyka i kosztami implementacji (amortyzacji i utrzymania); do wdrożenia przyjmuje się wariant najkorzystniejszy.

Funkcje do zarządzania incydentami rejestrują zdarzenia nadchodzące z różnych źródeł (proste formularze wypełniane przez użytkowników, SMS, e-mail, ERP, systemy monitorowania działające w otoczeniu, inne systemy OSCAD itp.). Dla każdego zdarzenia prowadzi się wstępną ocenę jego skutków. Zdarzenia o znaczących skutkach negatywnych zaliczane są do incydentów i w zależności od rodzaju oraz wagi incydentu inicjowane są dla nich adekwatne działania – do uruchomienia planu ciągłości działania włącznie. Po zakończeniu incydentu następuje jego tzw. zamknięcie. *Ex post* oceniane są wówczas jego przyczyny i skutki, sporządzany jest krótki raport podsumowujący, którego uproszczona (zanonimizowana) wersja jest kierowana do systemu OSCAD-STAT. Z incydentów zawsze wyciągane są wnioski (ang. *lessons learnt*), by w przyszłości móc ich uniknąć.

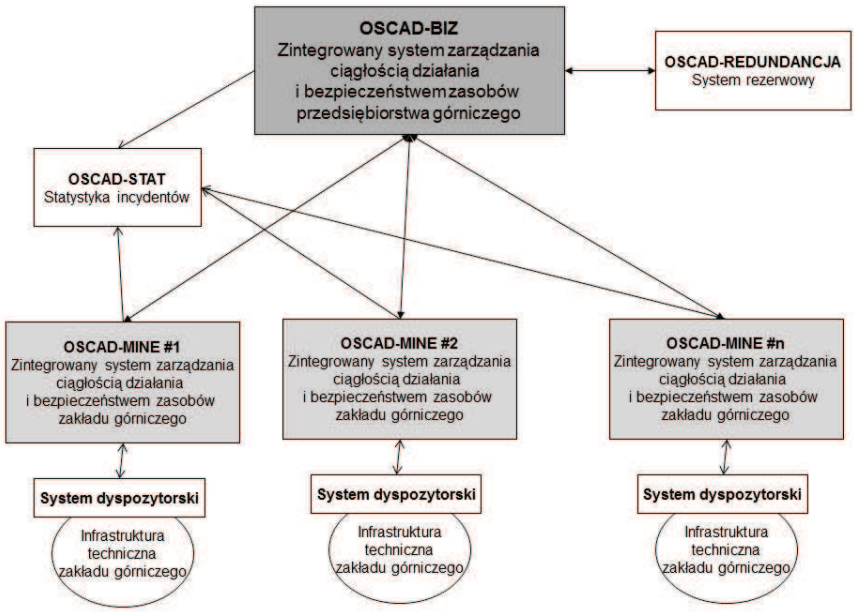
Funkcje związane z audytem i przeglądami zarządzają informacjami o wykonanych audytach zgodności lub przeglądach, w tym generują raporty i wspomagają proces ich zatwierdzania. System OSCAD dysponuje szeregiem list audytowych na zgodność z podstawowymi normami i przepisami prawa. Listy te znacząco ułatwiają prowadzenie audytu oraz półautomatyczne generowanie raportów. Samo planowanie audytu lub przeglądu odbywa się za pomocą funkcji związanych z harmonogramowaniem. Plan audytu uwzględnia daty rozpoczęcia i zakończenia całego audytu, osoby prowadzące oraz szczegółowe zadania audytowe (godzina rozpoczęcia i zakończenia zadania, sprawdzany punkt normy/wymagań technicznych lub prawnych, komórki organizacyjne/osoby poddawane audytowi). Na podstawie planów generowane są zadania dla osób odpowiedzialnych.

Funkcje zarządzania planami ciągłości działania (ang. *BCP – Business Continuity Plan*) wspomagają użytkownika systemu w opracowywaniu, utrzymywaniu i testowaniu planów ciągłości działania. Plany takie są opracowywane dla procesów biznesowych uznanych za krytyczne dla funkcjonowania instytucji. Wskazują zasoby potrzebne do realizacji konkretnego procesu, środowisko realizacji, listę kontaktową osób zaangażowanych oraz operacje, które należy wykonać. Plany muszą być okresowo testowane w praktyce przez pracowników instytucji. Planowanie testów odbywa się również w oparciu o funkcje harmonogramowania.

Funkcje obsługi mierników i wskaźników pozwalają je definiować i nimi zarządzać; miernikiem jest mechanizm cyklicznego pomiaru wartości wybranej zmiennej, dokonywany automatycznie lub ręcznie, zawierający zdefiniowane wartości progowe, których przekroczenie skutkuje wygenerowaniem zadania dla osoby odpowiedzialnej za miernik; ogólnie mierniki wykorzystuje się do poprawy efektywności realizowanych zadań (doskonalenia procesów).

3. BEZPIECZEŃSTWO ZASOBÓW I CIĄGŁOŚĆ DZIAŁANIA PRZEDSIĘBIORSTWA GÓRNICZEGO

Schemat ogólny systemu zarządzania ciągłością działania oraz bezpieczeństwem informacji i innych zasobów w przedsiębiorstwie górniczym przedstawiono na rys. 2. Uwzględnia on obecną strukturę organizacyjną przedsiębiorstw górniczych.



Rys. 2. Schemat ogólny systemu zarządzania ciągłością działania oraz bezpieczeństwem informacji i innych zasobów w przedsiębiorstwie górniczym (źródło: Instytut EMAG)

W pewnym uproszczeniu struktura organizacyjna przedsiębiorstwa górniczego obejmuje dwa poziomy:

- jednostkę nadrzędną (kompanię, holding, spółkę), zarządzającą kilkoma/kilkunastoma kopalniami,
- kopalnie prowadzące wydobycie kopalin.

Jednostki nadrzędne koordynujące działalność zakładów górniczych są typowymi przedsiębiorstwami ukierunkowanymi na biznes. Tu są prowadzone rozliczenia finansowe, realizowane zadania wspólne, odbywa się planowanie. Dla tego typu jednostek można zastosować wersję podstawową systemu OSCAD (oznaczoną na rys. 2. jako OSCAD-BIZ) ze wskazaniem dwóch głównych celów ochrony:

- zapewnienie ciągłości procesów biznesowych jednostki nadrzędnej według BS 25999 (ISO 22301),
- ochrona zasobów informacji jednostki w rozumieniu ISO/IEC 27001.

Opcjonalnie do zintegrowanego systemu OSCAD można dołączyć inne systemy zarządzania: jakością, środowiskiem czy BHP – o ile występują w danej jednostce. OSCAD może wówczas służyć do analizy ryzyka zawodowego czy też aspektów środowiskowych. OSCAD-BIZ może być zasilany z ERP podstawowymi informacjami zwiastującymi możliwość wystąpienia incydentów (np. zapasy materiałów, części zamiennych).

Zakres prac przystosowawczych dla OSCAD-BIZ jest typowy, podobny do wdrożeń w innych dziedzinach – sprowadza się do opracowania słownictwa przedsiębiorstwa, miar ryzyka, wskaźników, procedur oraz innych dokumentów itp.

Zakłady górnicze (kopalnie) stanowią wyodrębnione technologicznie i organizacyjnie zespoły środków służących bezpośrednio do wydobywania kopalin ze złoża. Do tych środków zalicza się na przykład: wyrobiska górnicze, obiekty budowlane i technologiczne czy urządzenia przeróbcze. Dla zakładów górniczych można zastosować wersje dedykowane systemu OSCAD (oznaczone na rys. 2. jako OSCAD-MINE #i). Wersje te są zasilane informacjami z systemów dyspozytorskich i innych systemów zarządzania (np. ERP, BHP).

Można wówczas wskazać trzy główne cele ochrony:
- zapewnienie ciągłości procesów zakładu według BS 25999 (ISO 22301), w tym zwłaszcza ciągłości procesu wydobycia,
- ochrona integralności i dostępności zasobów ludzkich i materialnych zaangażowanych w proces wydobycia; rozpatruje się tu takie czynniki naruszające zasoby, jak: powodujące zniszczenie maszyn i urządzeń, utratę życia lub zdrowia górników, awarie, przestoje, braki w zaopatrzeniu itp.,
- ochrona integralności, dostępności i poufności informacji związanych z realizacją procesów biznesowych zakładu w rozumieniu ISO/IEC 27001.

Zakres przystosowania systemu OSCAD-MINE do pracy w warunkach zakładu górniczego jest znacznie szerszy w porównaniu z OSCAD-BIZ i obejmuje następujące działania:
- opracowanie słownictwa systemu, obejmującego dodatkowe zasoby i role związane z procesami zakładu górniczego, specyficzne zagrożenia, podatności i zabezpieczenia,
- predefiniowanie struktury organizacyjnej i ról – jako wzorców do uszczegółowienia podczas wdrożenia,
- predefiniowanie wzorców typowych procesów zakładu górniczego – do uszczegółowienia podczas wdrożenia,
- identyfikacja zasobów i procesów zakładu górniczego,
- skonfigurowanie narzędzia analizy ryzyka (matryca oceny strat biznesowych i inne miary),
- opracowanie taksonomii zagrożeń i incydentów odzwierciedlających realia zakładu górniczego, przystosowanie OSCAD-STAT do działania w oparciu o tę taksonomię,
- zintegrowanie OSCAD z systemem SD 2000 (lub innym podobnym), monitorującym parametry produkcji i bezpieczeństwa, opracowanie zintegrowanego systemu monitorowania incydentów (OSCAD/SD 2000) i połączenie go z systemem OSCAD-STAT.

Wskazane jest wyposażenie systemu OSCAD-BIZ w system rezerwowy, a system OSCAD-MINE należy podłączyć do istniejących w zakładach systemów dyspozytorskich. W Instytucie EMAG zrealizowano przykład takiego połączenia – z systemem SD 2000. Szczegóły dotyczące współpracy OSCAD z systemem SD 2000 przedstawiono w pracy [15]. Więcej informacji o rozwiązaniach OSCAD przedstawiono w pracach [16, 17].

Niezwykle istotną kwestią jest gromadzenie informacji statystycznych o incydentach, gdyż pozwala to doskonalić funkcjonujące w firmach systemy. Nawet z pozoru błahe, umykające uwadze incydenty, gdy ich liczba jest znacząca, w sumie mogą powodować duże straty. OSCAD-STAT może być niezwykle pomocnym narzędziem w rozwiązywaniu tego typu problemów. Proponuje się zainstalowanie jednego serwera danych statystycznych na przedsiębiorstwo.

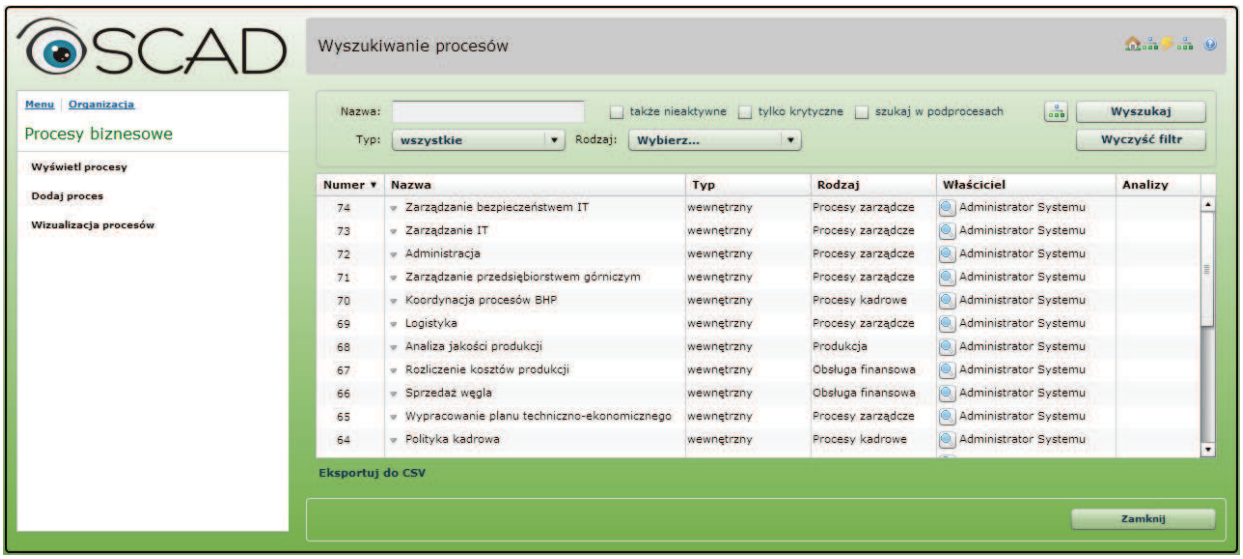
4. WYBRANE ASPEKTY ZASTOSOWANIA SYSTEMU OSCAD W PRZEDSIĘBIORSTWIE GÓRNICZYM I JEGO ZAKŁADACH

Zaproponowana dla przedsiębiorstwa górniczego struktura systemu OSCAD jest dwupoziomowa, co uwzględnia strukturę przedsiębiorstwa i powiązania kooperacyjne. Poziom wyższy dotyczy jednostki nadrzędnej, która jest typowym przedsiębiorstwem ukierunkowanym na osiąganie zysku. Standardy BS 25999 (ISO 22301) i ISO/IEC 27001 powstały dla tego typu przedsiębiorstw. W ich opracowaniu uczestniczyli przedstawiciele największych firm międzynarodowych, głównie brytyjskich.

Rysunek 3. pokazuje jedno z okienek aplikacji OSCAD, gdzie przedstawiono przykłady procesów biznesowych przedsiębiorstwa górniczego. Modelowanie procesów pozwala określić relacje między procesami, a także zdekomponować proces na podprocesy. Rozważa się wejścia i wyjścia procesów, identyfikuje się procesy krytyczne, zasilające i konsumujące, a także parametry procesów związane z ciągłością działania (np. maksymalny, tolerowany przez firmę czas nieaktywności procesu). Model procesowy firmy jest podstawą analizy ryzyka typu BIA (ukierunkowanej procesowo). Podczas tej analizy bada się wpływ utraty atrybutów ciągłości i integralności poszczególnych procesów na funkcjonowanie firmy. W toku analizy BIA (ukierunkowanej na zasoby) można rozpatrywać wszelkie zasoby informacji związane z realizacją danego procesu i rozważać wpływ utraty atrybutów integralności, dostępności i poufności tych informacji na funkcjonowanie firmy.

Wdrożenie pełnej funkcjonalności OSCAD w przedsiębiorstwie działającym na rynku uznaje się za działania rutynowe. Tego typu prace oferuje na rynku wiele firm konsultingowych, jednak nie dysponują one tak zaawansowanymi narzędziami, jak OSCAD.

W dalszej części artykułu uwaga zostanie skoncentrowana na rozwiązaniach nietypowych i innowatorskich, dotyczących przystosowania systemu OSCAD do potrzeb zakładu górniczego. Zostanie to zilustrowane przykładami rozwiązania wybranych problemów.



Rys. 3. Procesy biznesowe przedsiębiorstwa górniczego w OSCAD-BIZ (źródło: Instytut EMAG)

4.1. Zarządzanie ryzykiem

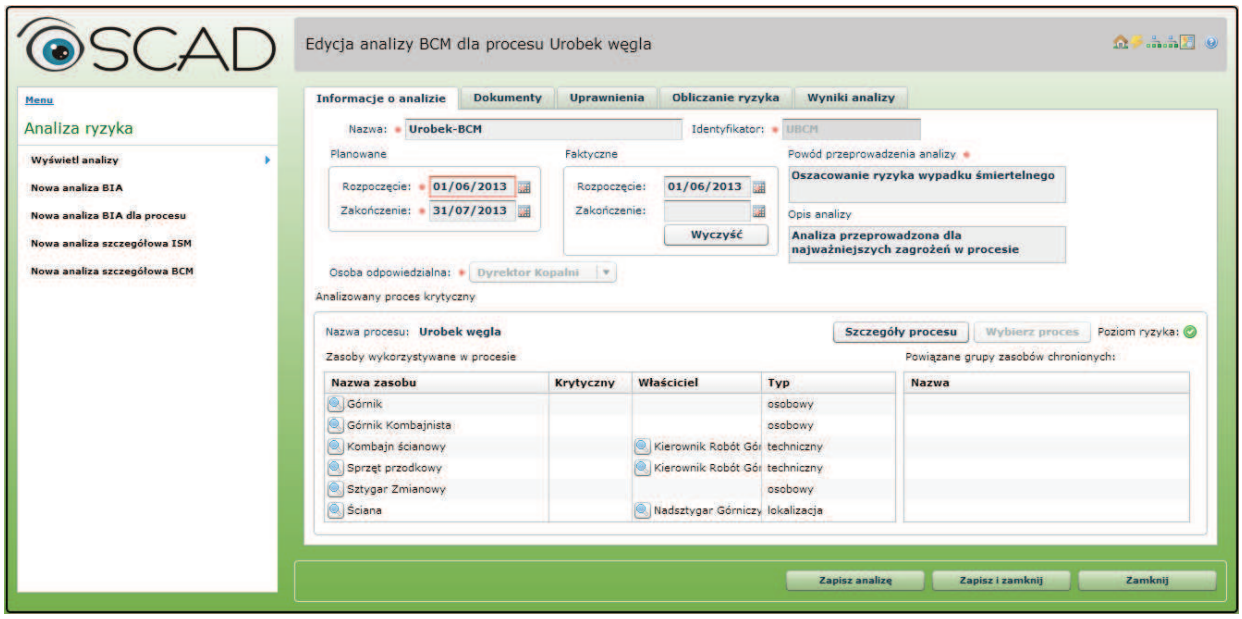
Zakład górniczy jest środowiskiem, w którym realizowany jest proces wydobycia węgla i inne wspomagające go procesy. Istotne jest zapewnienie ciągłości tego procesu, co ma bezpośredni związek z jego efektywnością w sensie ekonomicznym. W tym środowisku występuje wiele czynników zakłócających proces wydobycia.

Zadaniem OSCAD jest wsparcie w identyfikacji tych czynników i trzymanie ich pod kontrolą. Do tego celu można wykorzystać funkcje dotyczące analizy i zarządzania ryzykiem wbudowane do systemu. Można prowadzić trzy warianty analizy ryzyka:

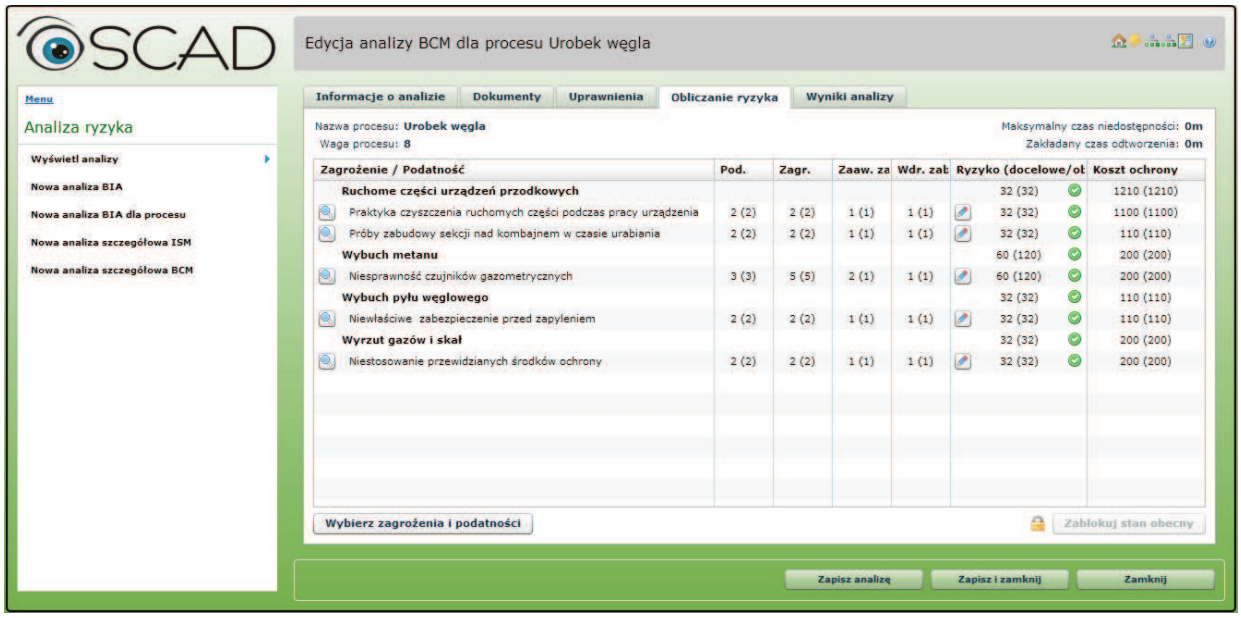
- analizę skutków biznesowych (wspomnianą wyżej analizę BIA); w jej wyniku uzyskuje się informacje na temat, jakie skutki biznesowe dla zakładu górniczego przyniesie utrata atrybutu ciągłości działania rozpatrywana w określonych przedziałach czasu; wyznacza się przy tym tzw. procesy krytyczne (w przypadku zakładu procesem takim jest proces wydobycia),
- szczegółową analizę ryzyka typu BCM (zorientowaną na procesy); służy ona do badania przyczyn zjawisk niekorzystnych dla procesu; dla każdego procesu krytycznego rozważa się zagrożenia i wykorzystywane przez nie podatności wpływające negatywnie na proces, zaś zasoby są tu traktowane w sposób ogólny, jako całość; tego typu szczegółowość analizy jest wystarczająca dla oceny czynników zakłócających ciągłość działania;
- szczegółową analizę ryzyka typu ISM (bazującą na mechanizmach analizy systemu ISMS, stąd nazwa, ukierunkowana na zasoby); w tym przypadku zasoby są podzielone na kategorie (definiuje to jeden ze słowników systemu), zaś analizę zagrożeń i podatności prowadzi się dla każdego zasobu oddzielnie (w oprogramowaniu używa się pojęcia „grupa zasobów chronionych"); w ten sposób dla każdego scenariusza ryzyka („jak zagrożenie, wykorzystując podatność, wpływa negatywnie na zasób") wyznacza się wielkość ryzyka, w tym wielkość strat i możliwość ich wystąpienia.

Rysunek 4. przedstawia okienko OSCAD (zakładka „Informacje o analizie") pozwalające na określenie kontekstu rozpoczynanej analizy ryzyka typu BCM dla procesu urobku węgla. Każda analiza ma swoje parametry opisowe, jak również ogół zasobów zaangażowanych w realizację tego procesu. Analiza BCM nie rozważa zagrożeń dla każdego z zasobów osobno, lecz skupia uwagę na zagrożeniach naruszających ciągłość realizacji procesu jako całości. Zasobem jest tu więc ciągłość procesu. Bardziej szczegółowe wyniki może dać analiza typu ISM, rozważająca z punktu widzenia zagrożeń i podatności grupy zasobów chronionych związane z danym procesem.

Analizator ryzyka posiada wiele zakładek. Zakładka „Dokumenty" służy do zarządzania dokumentami dołączanymi do systemu, zaś zakładka „Uprawnienia" – do zarządzania dodatkowymi uprawnieniami związanymi z daną analizą. Rysunek 5. pokazuje zakładkę „Obliczanie ryzyka" z przykładowymi wynikami analizy. Dla każdej pary zagrożenie-podatność oszacowano powagę podatności (możliwość wystąpienia), powagę zagrożeń (wielkość powodowanych strat), stopień zaawansowania technicznego istniejących zabezpieczeń (automatyczne - 3, półautomatyczne - 2, organizacyjno-proceduralne - 1), stopień zaawansowania wdrożenia zabezpieczeń (wdrożone - 3, wdrażane - 2, planowane - 1).



Rys. 4. Rozpoczęcie analizy ryzyka typu BCM dla procesu urobku węgla (OSCAD-MINE) (źródło: Instytut EMAG)



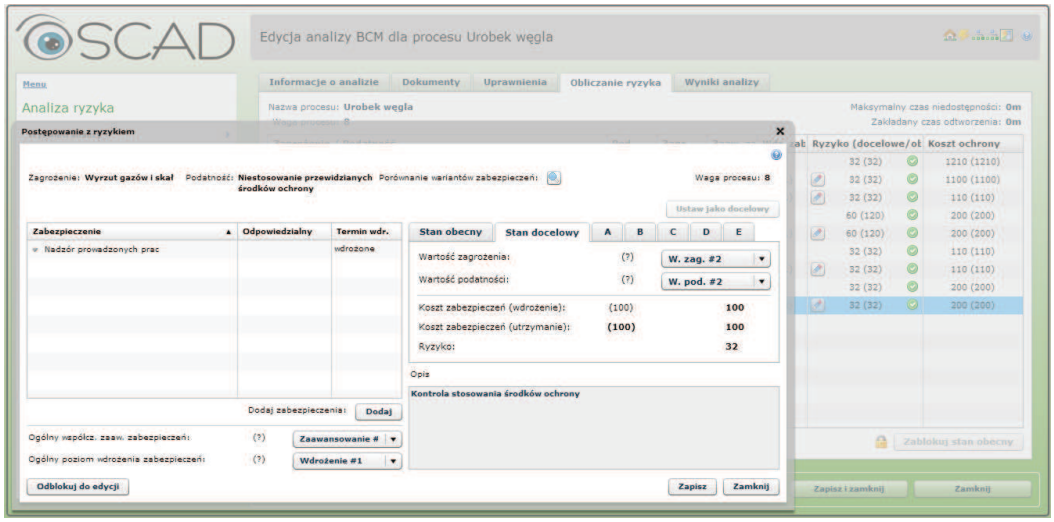
Rys. 5. Wyniki analizy ryzyka BCM dla procesu urobku węgla (OSCAD-MINE) (źródło: Instytut EMAG)

Na podstawie odpowiednich formuł matematycznych [17] wielkość ryzyka wyznaczana jest w punktach stosowanej skali pomiarowej. Liczby w nawiasach oznaczają ryzyko pierwotne („zastane", szacowane po raz pierwszy) lub oszacowane podczas poprzedniej analizy. Przy analizie rozważane są istniejące zabezpieczenia – samoistne lub wdrożone na podstawie wyników poprzedniej analizy. Dla zabezpieczeń rejestruje się ich koszt, obejmujący dwa składniki: koszt nabycia/amortyzacji oraz koszt utrzymania. Podczas analizy BCM rozważa się ponadto zachowanie relacji między dwoma podstawowymi parametrami ciągłości działania:

zakładany czas odtworzenia <= maksymalny czas niedostępności.

Wynikiem analizy jest lista rankingowa przypadków ryzyka uporządkowana według wielkości ryzyka. Dla przypadków przekraczających poziom akceptowalności ustalony dla firmy (zakładu) należy zastosować zabezpieczenia redukujące ryzyko.

Rysunek 6. przedstawia dobór zabezpieczeń dla konkretnego przypadku ryzyka, czyli pary zagrożenie („Wyrzut gazów i skał") – podatność („Niestosowanie przewidzianych środków ochrony"). Dla takiej pary dobiera się stosowne zabezpieczenie (tu „Nadzór prowadzonych prac"), pamiętając, że każde zabezpieczenie ma swoją zdolność do obniżenia ryzyka i swój koszt. Dla danego przypadku ryzyka można przeanalizować do pięciu wariantów zabezpieczeń (A-E) i jako docelowy wybrać wariant najkorzystniejszy, to znaczy taki, który obniża ryzyko poniżej progu akceptowalności, a jego koszty nie są większe niż zakładane. Zabezpieczenia są umieszczane w planach zabezpieczeń, które wskazują czas, miejsce i koszt wdrożenia oraz osoby za to odpowiedzialne.



Rys. 6. Zarządzanie ryzykiem – dobór zabezpieczeń (OSCAD-MINE) (źródło: Instytut EMAG)

Należy zauważyć, że wyniki analizy ryzyka mają charakter prognozy niekorzystnych zdarzeń. Zawsze pojawia się kwestia, na ile realne były te prognozy, stąd należy je skonfrontować z rzeczywistą liczbą zaistniałych incydentów i wynikających z nich strat w porównywalnym czasie. Jest to jeden z powodów konieczności monitorowania i analizy incydentów, by uzyskać tego typu dane.

4.2. Zarządzanie incydentem i centralne monitorowanie incydentów

System OSCAD ma rozbudowaną funkcjonalność do zarządzania incydentami, w tym do automatycznej akwizycji informacji o incydentach. Dość szczegółowo to zagadnienie opisano w artykule [15].

Zarządzanie incydentami w systemie OSCAD zaczyna się od zgłoszenia i klasyfikacji zdarzenia, wprowadzonego do systemu:

- ręcznie przez uprawnioną do tego osobę za pomocą prostego formularza elektronicznego,
- automatycznie przez interfejs z zewnętrznymi systemami monitorującymi lub zarządzającymi, takimi jak np. SD 2000.

Kolejna uprawniona osoba ocenia wstępnie i klasyfikuje zdarzenia według ich powagi. Poważniejsze zdarzenia są zaliczane do incydentów, zaś mniej groźne nadal pozostają zdarzeniami. Incydenty są poddawane dalszej szczegółowej obsłudze, zaś zdarzenia są tylko odnotowywane w bazie danych.

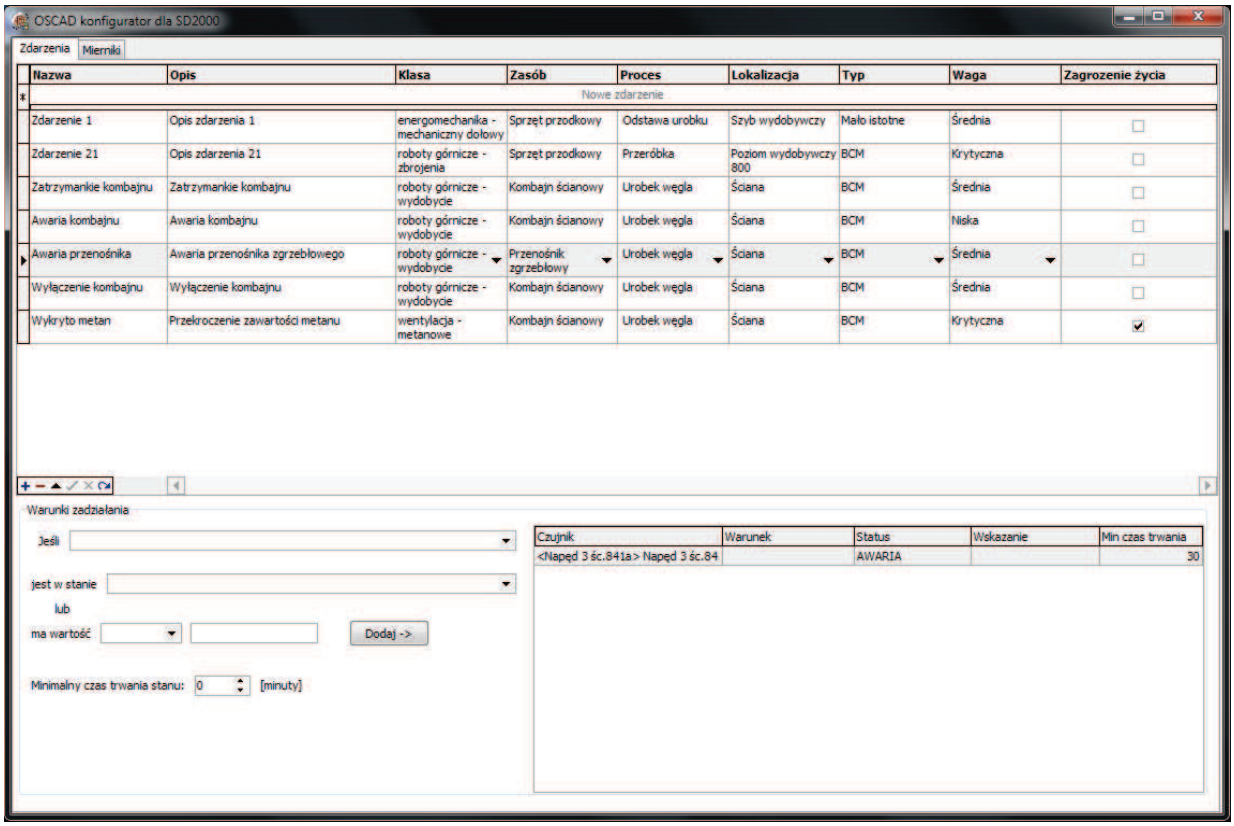
System SD 2000 jest przykładem systemu, który z zewnątrz i w sposób automatyczny zasila zdarzeniami nadrzędny wobec niego OSCAD.

Nie każde zdarzenie rejestrowane w systemie SD 2000 można uznać za zdarzenie w rozumieniu procesu zarządzania incydentem, stąd system ten wyposażono w specjalny filtr (rys. 7), pozwalający na ustawienie warunków brzegowych.

Rysunek 8. przedstawia okienko ze zgłoszonymi zdarzeniami zakwalifikowanymi już jako incydenty, gdyż straty z nimi związane uznano za poważniejsze.

Każdy z incydentów, niezależnie od sposobu zgłoszenia, jest przedmiotem procesu zarządzania incydentem zaimplementowanego w OSCAD, który obejmuje następujące działania:

1. Analiza incydentu; polega ona na określeniu między innymi:
   - typu incydentu,
   - występującego zagrożenia, które go spowodowało,
   - zidentyfikowanych podatności wykorzystywanych przez zagrożenie,
   - rzeczywistej straty poniesionej w wyniku incydentu.



Rys. 7. Filtrowanie zdarzeń w SD 2000 przed ich zgłoszeniem do OSCAD (źródło: Instytut EMAG)

Rys. 8. Przegląd zgłoszonych zdarzeń (OSCAD-MINE) (źródło: Instytut EMAG)

2. Wskazanie osób odpowiedzialnych za realizację obsługi incydentu (zlecenie im podzadań).
3. Przeprowadzenie akcji powiadamiania za pomocą dostępnych w OSCAD kanałów łączności.
4. Uruchomienie wcześniej przygotowanego planu BCP (tylko dla poważniejszych incydentów, następuje uruchomienie zadań przewidzianych w sytuacji kryzysowej).
5. Przekierowanie zadania do innej osoby odpowiedzialnej (w razie potrzeby).
6. Zamknięcie incydentu (incydent uzyskuje status „obsłużony" i można do niego dodać zadanie na-

prawcze wynikające z wniosków płynących z incydentu; jest to określane popularnym terminem angielskim *lessons learnt*, rozumianym potocznie jako „uczenie się na błędach").

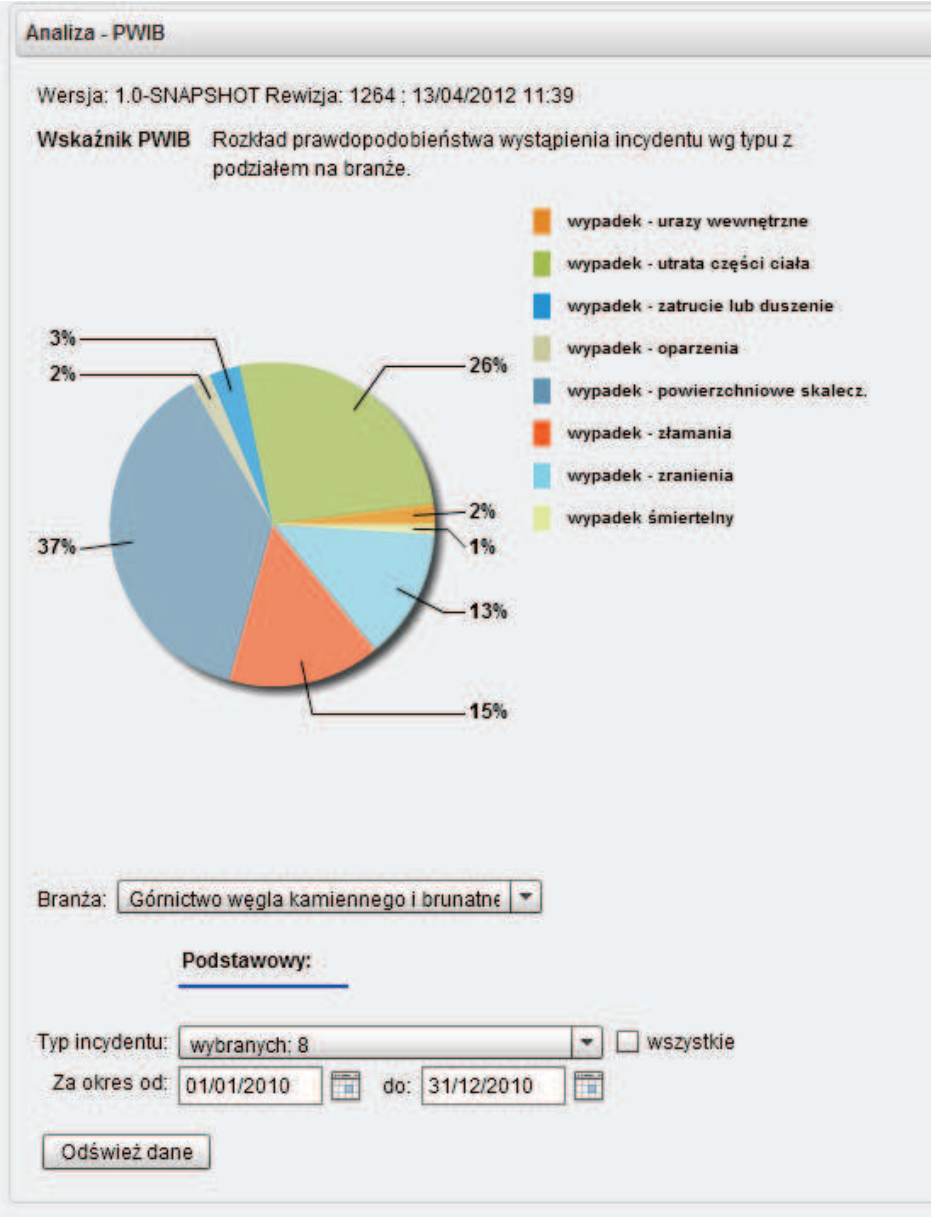
7. Przesłanie informacji o incydencie do systemu informacji statystycznej OSCAD-STAT.

Komunikat ostrzegawczy o incydencie może być wysłany do innych systemów OSCAD instytucji współpracujących (na przykład w ramach łańcucha dostaw).

Należy zauważyć, że OSCAD dostarcza jednolity, centralny system zarządzania incydentami dla zakładu górniczego, wspomagany serwerem danych statystycznych OSCAD-STAT. Gromadzone w czasie informacje dotyczące natury incydentów stanowią wartość dodaną, jaką wnosi OSCAD dla klienta. Informacje można wykorzystywać do korygowania procesów zarządzania w firmie, w działaniach doskonalących, jak również jako informacje wejściowe do analizy ryzyka. Przykład statystyki oferowanej przez OSCAD-STAT pokazano na rysunku 9. (dane fikcyjne). Przedstawia ona rozkład wypadków dla wybranej branży (tu górnictwa). OSCAD-STAT umożliwia tworzenie statystyk do własnych potrzeb.

Istnieje możliwość rejestrowania incydentów pozornie mało znaczących, na co dzień umykających uwadze. Często ich liczba jest duża, przez co w sumie powodują znaczące straty dla firmy. Również i z takich przypadków należy wyciągać wnioski.

System zarządzania incydentem może służyć do rejestracji wypadków przez służby BHP. Generowane na ten temat raporty dają diagnozę dotyczącą poprawy sytuacji w tym obszarze. Istnieje możliwość włączenia do systemu OSCAD innych elementów systemu zarządzania bezpieczeństwem i higieną pracy.



Rys. 9. Przykład statystyki incydentów utworzonej w aplikacji OSCAD-STAT (źródło: Instytut EMAG)

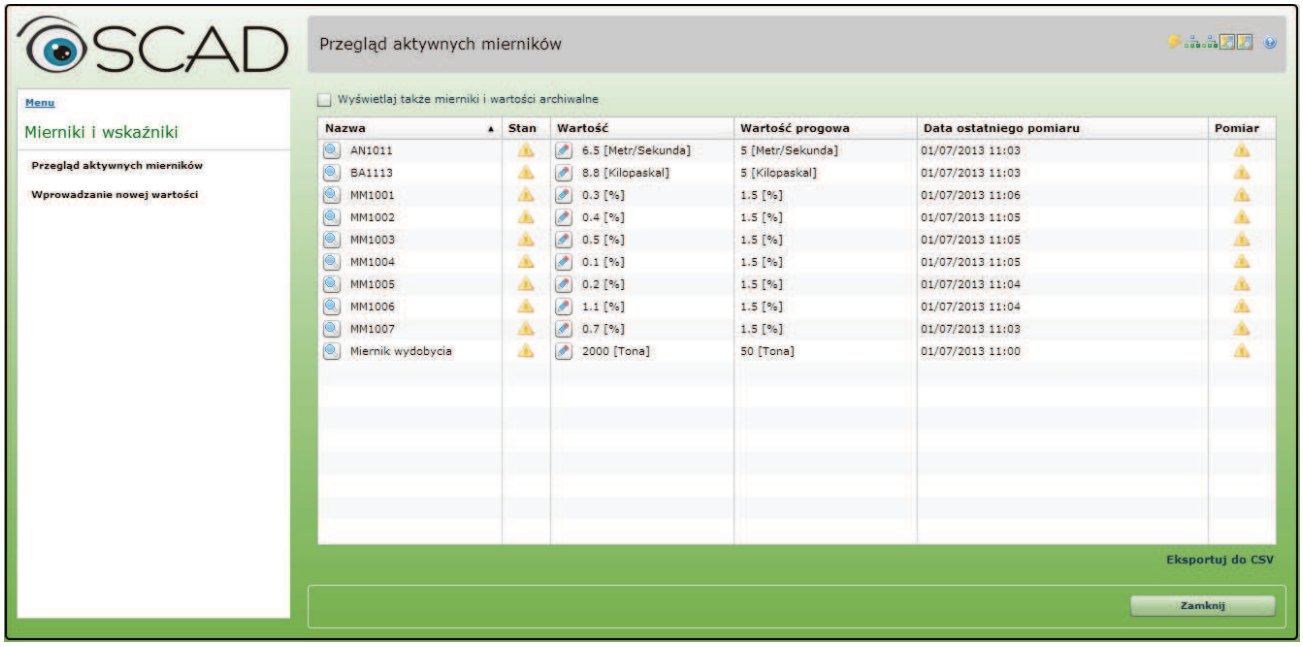
4.3. Mierniki i wskaźniki

System OSCAD, jako system wspomagający procesy zarządzania, ma wbudowany mechanizm mierników i wskaźników. Służą one do gromadzenia informacji wykorzystywanych do doskonalenia procesów biznesowych, jak i samego systemu zarządzania nimi. Mierniki pozwalają na cykliczne próbkowanie zmiennych fizykalnych (np. ciśnienie, stężenie metanu) lub zmiennych procesowych (np. aktualna wielkość wydobycia, liczba awarii maszyny X, sumaryczny czas przestoju spowodowanego przez Y itp.). Pomiar dokonywany jest automatycznie lub ręcznie. Mierniki posiadają zdefiniowane wartości progowe, których przekroczenie skutkuje wygenerowaniem zadania dla osoby odpowiedzialnej za zachowanie poprawnej wartości zmiennej.

Poza miernikami definiowanymi ręcznie w wersji OSCAD-MINE zdefiniowano mierniki pobierające automatycznie wyselekcjonowane dane z systemu SD 2000. Jako mierniki systemu OSCAD-MINE są traktowane wszystkie pojedyncze czujniki, które zostały zdefiniowane w systemie SD 2000. Informacje z nich nadchodzące są na bieżąco aktualizowane w bazie danych OSCAD-MINE. Są to np. czujnik analogowy stężenia metanu, czujnik dwustanowy pracy kombajnu lub licznik skipów wydobytego na powierzchnię węgla.

W ramach integracji obu systemów po stronie SD 2000 zostały opracowane mechanizmy, które pozwalają na dowolne definiowanie sytuacji w zakładzie górniczym, odzwierciedlanych przez mierniki, jak również przez przedstawione już wcześniej zdarzenia i incydenty.

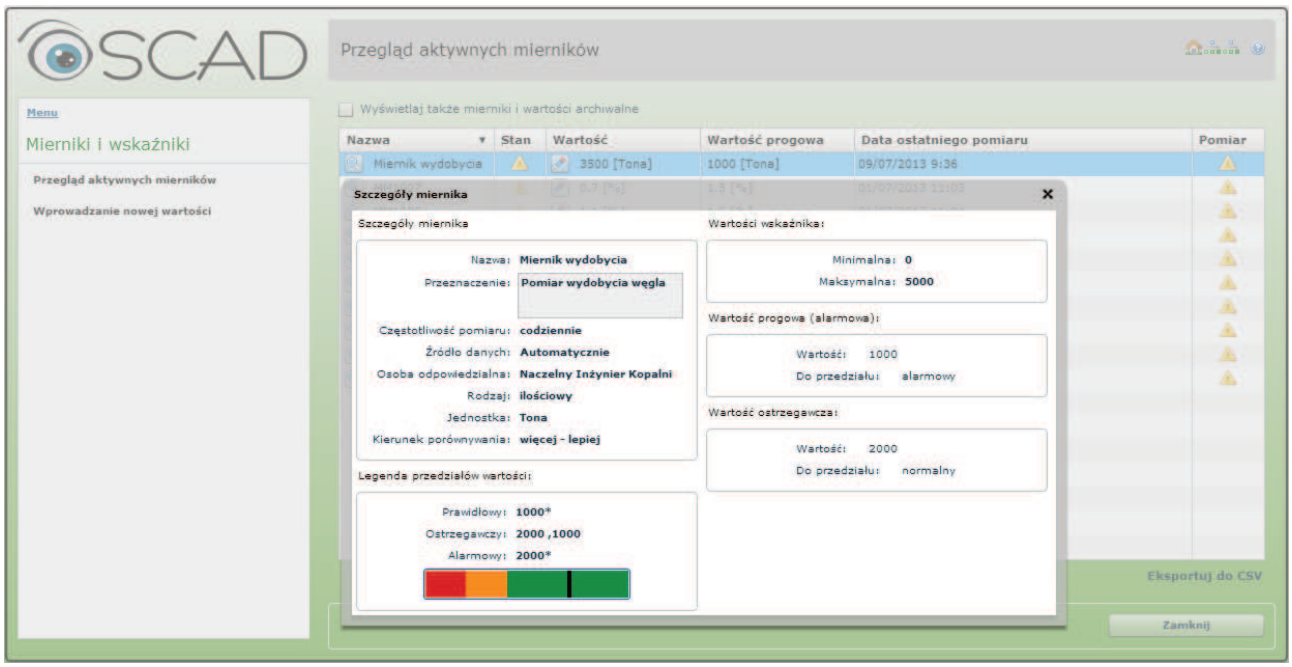
Na rysunku 10. pokazano okienko z listą aktywnych mierników w systemie OSCAD. Dotyczą one parametrów bezpieczeństwa (pomiary atmosfery w środowisku produkcyjnym – anemometr, barometr i metanomierze) oraz parametrów wydobycia (miernik wydobycia zliczający skipy). Przekroczenie określonych progów/zakresów skutkuje wygenerowaniem zadania dla wyznaczonej osoby odpowiedzialnej za zapewnienie odpowiedniej reakcji.



Rys. 10. Przegląd aktywnych mierników (OSCAD-MINE) (źródło: Instytut EMAG)

Na rysunku 11. przedstawiono szczegóły dotyczące przykładowego miernika (wydobycie węgla), dla którego dane pomiarowe są pobierane z systemu SD 2000. Należy zwrócić uwagę na trzy zakresy: alarmowy, ostrzegawczy i wyrażający stan prawidłowy. W przykładzie założono, że wydobycie mieści się w zakresie 0-5000 t. Aktualna wartość wynosi 3500 t i mieści się w zakresie normalnym. Spadek wydobycia poniżej 2000 t generuje sygnał ostrzeżenia, zaś poniżej 1000 t – sygnał alarmu. Mierniki mogą być definiowane również jako „wartość z przedziału od x do y".

Zestaw mierników pozwala uchwycić najważniejsze zmienne opisujące efektywność procesów biznesowych oraz procesów wchodzących w skład systemów zarządzania tymi procesami.



Rys. 11. Przykład miernika-wskaźnika (OSCAD-MINE)
(źródło: Instytut EMAG)

5. PODSUMOWANIE

OSCAD jest systemem wspomagania działań kierownictwa przedsiębiorstwa górniczego na różnych szczeblach zarządzania. Obejmuje zarówno warstwę proceduralno-organizacyjną, jak i oprogramowanie wspomagające procesy zarządzania. Został opracowany według obowiązujących na świecie standardów, m.in. BS 25999 (ISO 22301), dotyczącego ciągłości działania instytucji, oraz ISO/IEC 27001, dotyczącego bezpieczeństwa informacji instytucji. Jest systemem otwartym, możliwym do zastosowania w instytucjach lub firmach o różnej wielkości i o różnym profilu funkcjonowania, jednak każdorazowo wymaga pewnego przystosowania do potrzeb danej dziedziny.

W artykule przedstawiono ogólnie funkcjonalność systemu OSCAD, a następnie bardziej szczegółowo pokazano jego możliwości w zakresie wspomagania zarządzania ciągłością działania i ochrony zasobów na poziomie przedsiębiorstwa górniczego i jego zakładów. Przedsiębiorstwo górnicze, jako ukierunkowane na zysk, należy do typowych zastosowań standardów BS 2599 (ISO 22301) / ISO/IEC 27001 i opracowanego na ich podstawie systemu OSCAD.

Artykuł skupia uwagę na trzech podstawowych zastosowaniach systemu OSCAD w zakładzie górniczym:

- na analizie ryzyka, która pozwala kierownictwu zidentyfikować potencjalne czynniki mogące zakłócać proces wydobycia i naruszać zaangażowane w niego zasoby ludzkie oraz materialne, wybierać stosowne środki zaradcze w postaci zabezpieczeń, kontrolując ich koszt względem zdolności do obniżania ryzyka; prognozy dotyczące ryzyka pozwalają zdefiniować działania zapobiegawcze i właściwe reakcje na incydenty; zarządzanie oparte na analizie ryzyka podnosi efektywność funkcjonowania firm i jest źródłem przewagi konkurencyjnej;
- na systemie zarządzania incydentami, który dostarcza kierownictwu syntetycznych informacji na temat rzeczywistych zdarzeń i incydentów, ich przyczyn i skutków, co pozwala na bieżąco wyciągać wnioski na temat poprawy warunków bezpieczeństwa załóg i efektywności funkcjonowania zakładu górniczego;
- na miernikach / wskaźnikach efektywności i bezpieczeństwa, które dostarczają kierownictwu aktualnych, syntetycznych informacji o stanie procesów i bezpieczeństwa zakładu, w tym o stanie reagowania na sytuacje potencjalnie kryzysowe.

Wszystkie te działania zmierzają do poprawy efektywności funkcjonowania przedsiębiorstw górniczych oraz do poprawy bezpieczeństwa załóg. Gromadzone informacje są przeznaczone dla kierownictwa różnych szczebli, pomagają mu podejmować decyzje na podstawie aktualnych informacji o stanie firmy.

Poza wyżej wymienionymi trzema podstawowymi obszarami zastosowań w artykule zaprezentowano pozostałe funkcje systemu OSCAD, na przykład: zarządzanie ochroną informacji w przedsiębiorstwie, zarządzanie audytami, planowanie przeglądów i szkoleń, planowanie zabezpieczeń, zarządzanie planami awaryjnymi i procedurami testowymi,

zarządzanie obiegiem zadań, zarządzanie normami i dokumentami, w tym wynikającymi z przepisów prawa.

W ramach OSCAD istnieje możliwość integracji z systemami zarządzania jakością, środowiskiem i BHP.

Literatura

1. OSCAD, http://www.oscad.eu.
2. BS 25999-1:2006. *Business Continuity Management – Code of Practice*.
3. BS 25999-2:2007. *Business Continuity Management – Specification for Business Continuity Management*.
4. ISO 22301:2012. *Societal security – Business continuity management systems – Requirements*.
5. PN-ISO/IEC 27001. *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania* (ISO/IEC 27001:2005. *Information technology – Security techniques – Information security management systems – Requirements*).
6. ISO/IEC 27002. *Information security – Security techniques – Information security management systems – Code of practice*.
7. ISO 31000:2009. *Principles and Guidelines on Implementation*.
8. ISO/IEC 27005:2008. *Information technology – Security techniques – Information security risk management*.
9. Białas A.: *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006, 2007.
10. Białas A.: *Some aspects of information security and business continuity in public administration*. In: P. Pikiewicz, M. Rostański: *Internet in the information Society – Computer Systems Architecture and Security*, Academy of Business in Dabrowa Gornicza, 2013, pp. 125-140.
11. FP7 ValueSec: http://valuesec.eu.
12. http://pl.wikipedia.org/wiki/Cykl_Deminga.
13. BS PAS 99:2006. *Specification of common management system requirements as a framework for integration*.
14. Białas A.: *Development of an Integrated, Risk-based Platform for Information and E-services Security*. In: J. Górski: *Computer Safety, Reliability and Security*, 25th International Conference SAFECOMP 2006, Springer Lecture Notes in Computer Science (LNCS4166), Springer Verlag, Berlin – Heidelberg – New York 2006, ISBN 3-540-45762-3, pp. 316-329.
15. Białas A., Cała D., Napierała J.: *Wspomaganie zarządzania ciągłością działania zakładu górniczego za pomocą systemu OSCAD*, Konferencja EMTECH'2012 „Zasilanie, informatyka techniczna i automatyka w przemyśle wydobywczym – Innowacyjność i bezpieczeństwo", Szczyrk, 16-18 maja 2012.
16. Białas A.: *Computer support in business continuity and information security management*. In: A. Kapczyński, E. Tkacz, M. Rostański (Eds.): *Internet – Technical Developments and Applications 2*. *Advances in Intelligent and Soft Computing*, vol. 118, 2011, Springer Verlag, Berlin – Heidelberg, ISBN 978-3-642-25354-6, pp. 129-144.
17. Bagiński J., Rostański M.: *Modeling of Business Impact Analysis for the Loss of Business Processes and Data Integrity, Confidentiality and Availability*. In: *Theoretical and Applied Informatics*, Instytut Informatyki Teoretycznej i Stosowanej PAN, vol.23 (2011), no. 1, pp. 73-82.
18. Raporty projektu OSCAD, Instytut Technik Innowacyjnych EMAG, 2013.

Z kart historii polskiego górnictwa

Z okazji 25. rocznicy górniczych strajków z 1988 roku powstał film dokumentalny „Skok ku wolności", upamiętniający ówczesne wydarzenia. Autorem dokumentu jest katowickie 8bit Studio.

Głównym wątkiem filmu jest strajk z 15 sierpnia 1988 r. w KWK „Manifest Lipcowy".

Film jest dokumentem, lecz dokumentem opowiadanym z perspektywy ludzi, którzy przewodniczyli strajkowi z 15 sierpnia 1988 r. lub odgrywali w nim ważną rolę. Nacisk położony został nie na daty i suche fakty, lecz na emocje osób, które tworzą swoje własne opowieści z uwzględnieniem anegdot i innych ciekawych historii.

Bohaterami filmu są: Marek Bartosiak, ks. prałat Bernard Czernecki, Jan Golec, Edward Jarek, Tadeusz Jedynak, Alojzy Pietrzyk oraz Jan Piłat.

Narratorem oraz konsultantem historycznym jest Przemysław Miśkiewicz, prezes Stowarzyszenia „Pokolenie" oraz współtwórca „Encyklopedii Solidarności".

Ciekawym i ważnym elementem dokumentu są animacje obiektów 2D w przestrzeni trójwymiarowej, które połączone z materiałami archiwalnymi oraz zrealizowanymi na potrzeby filmu tworzą unikalną całość.

Mecenasem filmu jest SKOK Ubezpieczenia. Film powstał również dzięki wsparciu Komisji Krajowej NSZZ „Solidarność".

Premiera filmu: 3 września w kopalni „Zofiówka" w Jastrzębiu Zdroju podczas obchodów 25-lecia strajków w kopalni „Manifest Lipcowy" z 1988 r. Film będzie dostępny również na kanale YouTube 8bit Studio (http://www.youtube.com/8bitStudioTV).