dr inż. ANDRZEJ BIAŁAS
Instytut Technik Innowacyjnych EMAG

Zintegrowany system zarządzania ciągłością działania i bezpieczeństwem informacji – podsumowanie wyników prac ukierunkowanych na budowę modeli systemu

Integrated system for business continuity and information security management – summary of the project results orientated towards the construction of system models

Tematyka artykułu jest związana z wspólną implementacją znanych na świecie standardów: BS 25999 dotyczącego ciągłości działania instytucji oraz ISO/IEC 27001 dotyczącego bezpieczeństwa informacji instytucji, w ramach jednego zintegrowanego systemu zarządzania. Ciągłość działania jest rozumiana jako strategiczna i taktyczna zdolność instytucji do reagowania na incydenty i zakłócenia w funkcjonowaniu biznesowym oraz do ograniczania strat w przypadku wystąpienia tych czynników szkodliwych, zaś bezpieczeństwo informacji związane jest z ochroną integralności, dostępności i poufności informacji. Artykuł przedstawia założenia i dotychczasowe rezultaty projektu celowego dotyczącego opracowania komputerowo wspomaganego systemu zarządzania przeznaczonego dla firm i instytucji, dla których aspekt ciągłości procesów biznesowych oraz bezpieczeństwa informacji jest szczególnie istotny. W artykule podsumowano prace nad modelem systemu, w tym studia wykonalności dotyczące różnych aspektów oprogramowania tworzonego na podstawie tych modeli. Zwrócono uwagę na możliwe zastosowania tworzonego systemu, w tym również w dziedzinie górnictwa.

The topic of the article is related to the joint implementation of two widely used standards, BS 25999 concerning business continuity and ISO/IEC 27001 – information security, within one integrated management system. Business continuity is understood as a strategic ability of an organization to react to incidents and disturbances in its business functioning and to mitigate losses in case these harmful factors occur. Information security, in turn, is related to the protection of information integrity, availability and confidentiality. The article presents the assumptions and recently achieved results of a specific-targeted project whose objective is to develop a computer-supported management system for organizations which set a lot of store by the continuity of business processes and information security. The works on the system model were summarized, including a feasibility study concerning different aspects of software which is developed on the basis of these models. Additionally, the application possibilities of the newly developed system were pointed out, including those in the mining industry.

1. WSTĘP

Tematyka artykułu jest związana z wspólną implementacją znanych na świecie rodzin standardów:
- BS 25999 [1], [2] dotyczących zapewnienia ciągłości działania instytucji (ang. *BCMS – Business Continuity Management Systems*),
- ISO/IEC 27001 [3], [4] dotyczących zapewnienia bezpieczeństwa informacji w instytucji (ang. *ISMS – Information Security Management Systems*),
- w ramach jednego zintegrowanego systemu zarządzania.

Ciągłość działania jest rozumiana jako zdolność instytucji do reagowania na incydenty i zakłócenia w realizacji procesów biznesowych oraz do ograniczania strat w przypadku wystąpienia czynników szkodliwych, zaś bezpieczeństwo informacji związane jest z ochroną integralności, dostępności i poufności informacji. Oba zagadnienia mają podobny charakter i wzajemnie się przenikają, co przemawia za integracją obu systemów zarządzania.

Artykuł przedstawia założenia i dotychczasowe rezultaty projektu celowego dotyczącego opracowania komputerowo wspomaganego zintegrowanego systemu zarządzania przeznaczonego dla firm i instytucji, dla których aspekt ciągłości procesów biznesowych oraz bezpieczeństwa informacji jest szczególnie istotny.

W artykule podsumowano prace nad założeniami i modelem systemu, w tym studia wykonalności dotyczące różnych aspektów oprogramowania tworzonego na podstawie tych modeli. Zwrócono uwagę na możliwe zastosowania tworzonego systemu, w tym również w dziedzinie górnictwa.

O ile zagadnienie bezpieczeństwa informacji jest już obecnie dość dobrze znane, to ciągłość działania wymaga dodatkowego wyjaśnienia. Ciągłość działania (ang. *BC – Business Continuity*) jest rozumiana jako strategiczna i taktyczna zdolność instytucji do [1], [2]:
- zaplanowania reagowania i 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.

Zapewnienie ciągłości działania jest szczególnie ważne, a zarazem trudne, dla firm lub instytucji:
- mających rozbudowane więzi kooperacyjne, połączone w tak zwane łańcuchy dostaw,
- których procesy biznesowe są silnie uzależnione od sprawnego funkcjonowania systemów informatycznych,

1. INTRODUCTION

The article features the issues concerning the joint implementation of two basic groups of security standards:
- BS 25999 [1], [2] on business continuity (BCMS – Business Continuity Management Systems), and
- ISO/IEC 27001 [3], [4] on information security (ISMS – Information Security Management Systems),
- within one integrated management system.

Business continuity is understood as a strategic ability of the organization to react to incidents and disturbances in its business functioning and to mitigate losses in case such harmful factors occur, while information security is related to the protection of the information integrity, availability and confidentiality. These issues are of the same character and intermingle, which speaks for the integration of both management systems.

The article features the assumptions and achieved results of the specific-targeted project aimed at the development of a computer-supported integrated management system for organizations who set a lot of store by the continuity of business processes and information security.

The article summarizes the works on the system assumptions and model, including a feasibility study concerning different aspects of software developed on the basis of these models. The application possibilities of the newly developed system were pointed out, including those in the mining industry.

Information security is a commonly known issue these days. However, business continuity needs some explanation. Business continuity is understood as a strategic ability of the organization to [1], [2]:

- plan its reactions and react to incidents and disturbances in its business functioning so that its operations could be continued on an acceptable, previously determined level,
- mitigate losses in case such harmful factors occur.

To secure business continuity is extremely important and, at the same time, difficult for organizations:
- which have expanded co-operation links functioning within the so called supply chains,
- whose business processes depend strongly on efficient operations of IT systems,

- pracujących w trybie *Just in time*,
- w których pracują systemy usług *on-line*, będące jedną z najbardziej rozwiniętych form zastosowań informatyki do wspomagania procesów biznesowych.

Ciągłość procesów biznesowych w instytucjach stanowi podstawę ich konkurencyjności i sukcesu. Ciągłość ta jest uzależniona od prawidłowego funkcjonowania infrastruktury informatycznej (IT) wspomagającej realizację procesów biznesowych, ale nie tylko, gdyż wiele innych czynników może tę ciągłość zakłócić. Należy zwrócić uwagę, że funkcjonowanie rozwiązań IT związane jest z wieloma formami ryzyka (awarie sprzętu i oprogramowania, ataki z sieci, powodzie, ataki terrorystyczne, itp.), których wystąpienie powoduje zakłócenie funkcjonowania systemów teleinformatycznych, a to z kolei powoduje zakłócenie realizacji procesów biznesowych. Reagowanie na zagrożenia i przeciwdziałanie ich skutkom stanowi nowe wyzwanie dla firm i instytucji dążących do zapewnienia ciągłości działania w celu podwyższenia swojej konkurencyjności.

Wdrożenie systemu zarządzania ciągłością działania w instytucji stymuluje utworzenie odpowiedniej struktury organizacyjnej zapewniającej zwiększenie odporności na te zagrożenia i umożliwiającej właściwe reagowanie tak, by negatywne skutki dla ciągłości biznesowej były jak najmniejsze. Wytyczne i wymagania dotyczące zapewnienia ciągłości działania zawarte są w normie BS 25999.

Artykuł ma charakter wprowadzenia do problematyki ciągłości działania. Na tym tle przedstawia założenia projektu celowego OSCAD (Otwartego Szkieletowego Systemu Zarządzania Ciągłością Działania), współfinansowanego ze środków Ministerstwa Nauki i Szkolnictwa Wyższego, który od roku jest realizowany w Instytucie Technik Innowacyjnych EMAG.

2. PODSTAWY MERYTORYCZNE PROJEKTU OSCAD

Prace objęte projektem koncentrują się wokół rozwinięcia oraz implementacji ogólnej koncepcji systemu zarządzania ciągłością działania zawartej w normie BS 25999. Norma składa się z dwóch części:

- *BS 25999-1:2006 Business Continuity Management – Part 1: Code of practice* – zawiera definicję słownictwa używanego w normach oraz stanowi zbiór dobrych praktyk i rekomendacji w zakresie zarządzania ciągłością działania;

- working in the Just-in-time mode,
- which have on-line services systems that are one of the most advanced forms of IT applications supporting business processes.

The continuity of business processes in organizations is the basis to successfully compete on the market. This continuity depends on proper operation of the IT infrastructure which supports the execution of business process, still there are many other factors that may disturb this continuity. It is important to note that the functioning of IT solutions is related to many risks (hardware and software breakdowns, attacks from the network, floods, terrorist attacks, etc.) whose occurrence causes disturbances in the operations of IT systems. This, in turn, causes disturbances in business processes. Reacting to threats and counteracting their results has become a new challenge for organizations which aim at securing their business continuity with a view to increase their competitive position on the market.

The implementation of a business continuity management system in an organization results in the development of a suitable business structure that will have higher resistance to threats and will enable to react to incidents in such a way that negative impact for business continuity will be of the smallest possible degree. The recommendations and requirements concerning business continuity are included in the BS 25999 standard.

The article is an introduction to the issue of business continuity. It presents the assumptions of the specific-targeted project OSCAD (open, frame-type system for business continuity and information security management), co-financed by the Ministry of Science and Higher Education, which has been carried out for a year in the Institute of Innovative Technologies EMAG.

2. BASIC STANDARDS OF THE OSCAD PROJECT

The works within the project are focused on the development and implementation of the concept of a business continuity management system included in the BS 25999 standard. The standard has two parts:

- *BS 25999-1:2006 Business Continuity Management – Part 1: Code of practice* – contains definitions related to business continuity, along with a set of best practices and recommendations in the range of business continuity management;

- *BS 25999-2:2007 Business Continuity Management – Part 2: Specification for Business Continuity Management* – zawiera wymagania, według których będzie prowadzona certyfikacja zgodności systemu.

Systemy zarządzania ciągłością działania, tak jak inne podobne (zarządzania bezpieczeństwem informacji, jakością, usługami informatycznymi, BHP) buduje się na bazie cyklu W.E. Deminga, zwanego również cyklem PDCA (ang. *Plan-Do-Check-Act*) [5], który to cykl składa się z następujących faz grupujących odpowiednie procesy zarządzania:

- Planuj *(*ang. *Plan*): procesy związane z opracowaniem planu przedsięwzięcia dotyczącego zarządzania na bazie wypracowanej metody;
- Wykonaj (ang. *Do*): procesy dotyczące próbnej implementacji planu oraz wdrożenia tej metody;
- Sprawdzaj (ang. *Check*): procesy oceniające, czy nowy sposób działania daje lepsze wyniki;
- Działaj (ang. *Act*): jeśli nowy sposób działania przynosi lepsze rezultaty, należy go uznać za normę (obowiązującą procedurę), zestandaryzować, monitorować jego stosowanie i doskonalić.

Cykl Deminga zapewnia kontrolowane wdrożenie systemu zarządzania, a później jego utrzymywanie i doskonalenie w oparciu o mierzalne wskaźniki. Dla realizowanego projektu OSCAD przyjęto trójwarstwową architekturę:

- warstwa organizacyjna – obejmuje procesy zarządcze, planowanie i utrzymanie systemu, zbudowanie struktury organizacyjnej, opracowanie procedur i planów operacyjnych, procesy szkolenia i uświadamiania, komunikowanie się wewnętrzne i zewnętrzne, opracowanie i analizę danych statystycznych; warstwa organizacyjna jest wspomagana przez oprogramowanie;
- warstwa logiczna – jest realizowana przez oprogramowanie i obejmuje komputerowe wspomaganie decyzji, prowadzenie analiz BIA (ang. *Business Impact Analysis*), zarządzanie ryzykiem, utrzymanie bazy danych, zarządzanie zadaniami, gromadzenie zapisów działania systemu, monitorowanie incydentów i zagrożeń oraz automatyczne generowanie ostrzeżeń, gromadzenie wzorców postępowania, raportowanie;
- warstwa fizyczna – obejmuje realizację kanałów komunikacyjnych, współpracę z systemami komputerowymi w sieci, budowę i utrzymanie punktów zgłaszania zagrożeń oraz powiadamiania o zagrożeniach; warstwa fizyczna wchodzi w zakres tworzonego oprogramowania, jak również jest wspomagana przez jego otoczenie, w tym przez infrastrukturę IT, aplikacje biznesowe oraz infrastrukturę techniczną (fizyczną).

- *BS 25999-2:2007 Business Continuity Management – Part 2: Specification for Business Continuity Management* – contains requirements which are the basis to certify business continuity management systems.

Business continuity management systems, just as similar systems (information security management-, quality management-, IT services-, or health and occupational safety systems), are developed on the basis of the Deming cycle, also known as the PDCA cycle (Plan-Do-Check-Act). The cycle groups management processes of a system in the following four steps:

- Plan – processes related to working out the plan of a project concerning the management on the basis of a previously elaborated method;
- Do – processes concerning a trial implementation of the plan and implementation of the method;
- Check – evaluation processes which check whether the new method gives better results;
- Act – if the new method brings better results, it should be considered as a valid procedure, standardized, its functioning should be monitored and continuously improved.

The Deming cycle ensures controlled implementation of a management system, its unassisted adaptation to new challenges as well as improvement based on measurable indicators. For the OSCAD project a three-layer architecture was adopted:

- organizational layer – includes management processes, system planning and maintenance, development of organizational structure, elaboration of procedures and operational plans, training and awareness raising processes, internal and external communication, preparation and analysis of statistical data; the organizational layer is supported by software;
- logical layer – is executed by software and encompasses computer-based decision support, Business Impact Analyses (BIA), risk management, database maintenance, task management, records of system operations, monitoring incidents and threats and automatic generation of warnings, collecting procedure patterns, reporting;
- technical layer – includes the execution of communication channels, co-operation with computer systems working in a network, development and maintenance of threat reporting- and warning points; the physical layer is part of the developed software and is supported by its environment, including IT infrastructure, business applications and physical infrastructure.

Powyższe zagadnienia zostały przedstawione szerzej w Materiałach EMTECH 2010 [6]. Należy podkreślić, że dodatkowo w projekt systemu zarządzania ciągłością działania wkomponowano elementy systemu zarządzania bezpieczeństwem informacji według [3], [4], który jest również oparty na wspomnianym cyklu Deminga. Na poziomie logicznym oba systemy zarządzania są implementowane w ramach tak zwanej zintegrowanej platformy bezpieczeństwa ISP (ang. *Integrated Security Platform*), której koncepcję przedstawiono w pracy [7]. Platforma funkcjonuje w oparciu o wspólną bazę danych, będącą rozwinięciem koncepcji bazy CMDB (ang. *Configuration Management Database*), stosowanej w [8], [9], [10]. Platforma ISP zapewnia integrację systemów zarządzania od strony informatycznej, natomiast od strony organizacyjno-proceduralnej wykorzystywane są zalecenia BS PAS 99 [11]. Celem integracji systemów zarządzania współistniejących w instytucji jest obniżenie kosztów i poprawa efektywności zarządzania.

3. AKTUALNY STAN REALIZACJI PROJEKTU OSCAD

Podstawowym celem projektu OSCAD jest opracowanie zintegrowanego systemu zarządzania ciągłością działania i bezpieczeństwem informacji zapewniającego:

- płynne, kontrolowane funkcjonowanie instytucji w sytuacjach kryzysowych, kiedy to ciągłość procesów biznesowych jest zakłócana lub bezpieczeństwo informacji zostaje naruszone,
- zdolność ograniczania skutków zakłóceń ciągłości działania lub naruszeń bezpieczeństwa,
- zdolność odtwarzania procesów biznesowych do postaci pierwotnej po różnego typu incydentach.

Sprowadza się to do opracowania pewnych metod i narzędzi, a także dostarczenia wiedzy, jak w praktyce należy się nimi posługiwać. W szczególności w ramach projektu OSCAD opracowane zostaną:

- metodyka budowy otwartego, szkieletowego, zintegrowanego systemu zarządzania ciągłością działania i bezpieczeństwem informacji w postaci zbioru modułów wzorcowych,
- metodyka wdrożenia systemu polegająca na zidentyfikowaniu potrzeb i wymagań instytucji, która planuje wdrożenie oraz na rozwinięciu lub przystosowaniu modułów wzorcowych do postaci modułów docelowych na podstawie tych potrzeb i wymagań,
- oprogramowanie wspomagające proces wdrażania, a później eksploatacji zintegrowanego systemu zarządzania ciągłością działania i bezpieczeństwem informacji,

The above issues were presented in a more elaborate form in the proceedings of the EMTECH 2010 conference [6]. It is important to note that the project of the business continuity management system was supplemented with some elements of an information security management system according to [3], [4], also based on the above mentioned Deming cycle. On the logical level both management systems are implemented within the so called ISP platform (Integrated Security Platform) whose concept was presented in [7]. The platform functions on the basis of a common database which has been developed with the use of the CMDB basis (Configuration Management Database) used in [8], [9], [10]. The platform ensures the integration of management systems from the point of view of information technology, while its organization and procedures are based on BS PAS 99 recommendations [11]. The management systems are integrated in order to lower the costs and improve management efficiency.

3. CURRENT STATE OF THE OSCAD PROJECT EXECUTION

The basic objective of the OSCAD project is to develop an integrated management system for business continuity and information security. The system is to ensure:

- fluent, monitored functioning of an organization in crisis situations when business continuity is disturbed or information security breached,
- ability to mitigate the impact of business continuity disturbances or information security breaches,
- ability to restore business processes to their original form after different types of incidents.

It comes down to the elaboration of certain methods and tools, including knowledge how to use these methods and tools. Within the OSCAD project the following will be elaborated:

- methodology to build an open, frame-type, integrated management system for business continuity and information security in the form of standard modules (patterns),
- methodology to implement the system based on the identification of the needs and requirements of the organization which plans to implement the system and on the adaptation of standard modules (patterns) to the form of final modules on the basis of these needs and requirements,
- software supporting the process of implementation and, later, exploitation of the integrated management system for business continuity and information security,

- oprogramowanie do budowy systemu gromadzenia, analizy i udostępniania informacji statystycznej o zagrożeniach, podatnościach i incydentach zakłócających procesy biznesowe instytucji.

Realizacja projektu nawiązuje do wcześniej prowadzonych badań z zakresu bezpieczeństwa informacji [12], [13], [14], [15], [16], [17], [18], zarządzania ryzykiem [19], [20] oraz ontologii bezpieczeństwa [21].

3.1. Zadania obejmujące analizy wstępne

Na wstępie projektu zrealizowano zadania mające na celu pozyskanie i uporządkowanie wiedzy dotyczącej obecnego stanu badań nad systemami typu BCMS, jak również możliwej ich integracji z systemami typu ISMS oraz z innymi systemami zarządzania.

W ramach zadania 1:

- opracowano profile wdrożeniowe systemu oraz kryteria kwalifikacji danej instytucji do określonego profilu,
- opracowano metodę identyfikacji potrzeb i wymagań instytucji, pozwalającą na wybór profilu wdrożeniowego systemu dla danej instytucji,
- dokonano walidacji metody na przykładzie Instytutu EMAG oraz firm współpracujących z Instytutem w łańcuchu dostaw.

W ramach prac nad zadaniem 2 dokonano obszernego przeglądu istniejących w kraju i na świecie metod oraz narzędzi związanych z tematyką projektu, zidentyfikowano najważniejsze podmioty na rynku, dokonano analizy trendów na tym rynku. Wyniki tych prac pozwoliły doprecyzować założenia projektu. Przedstawiono również wstępne założenia dla statystycznej części systemu OSCAD – systemu OSCAD-STAT, jak również zidentyfikowano punkty zbieżne i rozbieżne systemów zarządzania, opartych na normach: ISO/IEC 27001 i BS 25999.

W ramach prac nad zadaniem 3 dokonano analizy treści materiałów normatywnych, wzorcowych praktyk (wytycznych) i przepisów prawnych, bezpośrednio lub pośrednio związanych z systemami zarządzania ciągłością działania i bezpieczeństwem informacji. Służyło to prawidłowemu ukierunkowaniu dalszych prac poprzez zdefiniowanie szczegółowych wymagań technicznych, organizacyjnych i prawnych. Określono możliwości i ograniczenia związane z budową krajowego systemu informacji statystycznej, w których byłyby gromadzone, przetwarzane oraz udostępnianie informacje pozyskiwane z działających systemów typu OSCAD oraz od instytucji posiadających wdrożone podobne rozwiązania.

- software to build a system that will collect, analyze and provide statistical information about threats, vulnerabilities and incidents disturbing the organization's business processes.

The execution of the project refers to previously conducted research on information security [12], [13], [14], [15], [16], [17], [18], risk management [19], [20] and security ontology [21].

3.1. Initial analyses tasks

At the beginning of the project the project team took up the task aimed at gathering and organizing the current state of the art in the range of BCMS systems research, as well as their possible integration with ISMS systems and other management systems.

The following were performed within task 1:

- implementation profiles of the system were elaborated, along with the criteria for qualifying a given institution to a particular profile,
- a method for the identification of the organization's needs and requirements was elaborated, enabling to select an implementation profile for a given organization,
- the method was validated based on the example of the EMAG Institute and organizations that cooperate with EMAG within a supply chain.

The works within task 2 comprised an extensive review of the existing national and international methods and tools related to the project topic. The main stakeholders on the market were identified and market trends analyzed. The results of these works enabled to define the project assumptions more precisely. Additionally, initial assumptions for the statistical part of the OSCAD system – OSCAD STAT – were presented. Finally, the coincident and divergent issues of the two management systems were identified, based on the ISO/IEC 27001 and BS 25999 standards.

Task 3 comprised the analysis of standards, best practices (recommendations) and laws which are directly or indirectly related to business continuity and information security systems. This aimed at proper orientation of further works by defining detailed technical, organization and legal requirements. The possibilities and limitations were determined which are related to the development of a national statistical information system. The system would store, process and provide access to information derived from the operating OSCAD-type systems and from organizations which have had similar solutions implemented.

3.2. Zadania dotyczące budowy modeli systemu

Wiedza zgromadzona w toku realizacji badań została wyrażona w postaci modeli systemu w ramach kolejnych zadań.

Zadanie 4 obejmowało budowę modeli podstawowych elementów systemu OSCAD w języku UML:

- modelu głównego szkieletowego systemu zarządzania ciągłością działania,
- modeli jego procesów zarządzania uwzględniających specyfikę profili instytucji,
- modelu procesu zarządzania ryzykiem opartego na rachunku ekonomicznym i uwzględniającego zarówno potrzeby systemu typu BCMS, jak i ISMS,
- modelu procesów zarządzania ciągłością działania w ramach łańcucha dostaw,
- modelu centralnej bazy danych i repozytorium dokumentów.

Po przeprowadzeniu analizy funkcjonalności i interoperacyjności elementów OSCAD, model główny systemu zarządzania ciągłością działania rozszerzono o moduł współpracy z współistniejącymi w instytucji systemami zarządzania. Uruchomiono prototypowe podsystemy monitorowania infrastruktury informatycznej i technicznej instytucji. Pozwala to na zbieranie informacji o zdarzeniach w sposób półautomatyczny. Gromadzone dane są wykorzystywane do realizacji sytemu OSCAD-STAT oraz do badań niezawodnościowych prowadzonych w Wyższej Szkole Biznesu w Dąbrowie Górniczej, która to uczelnia współpracuje przy realizacji projektu OSCAD. Opracowano wstępne rozwiązanie do zbierania informacji o zdarzeniach (ankiety), zgromadzono pewną liczbę tych zdarzeń w Instytucie EMAG i firmach współpracujących, które to ankiety również będą wykorzystane w OSCAD-STAT.

W ramach zadania 5, poświęconego modelowaniu systemu gromadzenia, analizy i udostępniania informacji statystycznej o incydentach, zagrożeniach i podatnościach związanych z bezpieczeństwem informacji oraz ciągłością działania, opracowano:

- model ogólny systemu informacji statystycznej – model modułu centralnego i jego procesów zarządzania,
- model centralnej bazy danych statystycznych,
- model podsystemu dwukierunkowej wymiany informacji pomiędzy modułem centralnym a systemami typu BCMS/ISMS działającymi w różnych instytucjach.

Zadanie 6 dotyczyło opracowania modelu współpracy systemu OSCAD z systemem zarządzania bezpieczeństwem informacji według ISO/IEC 27001 z uwzględnieniem możliwości wykorzystania elementów wspólnych obu systemów zarządzania, tzn.

3.2. Tasks related to the development of system models

The knowledge accumulated during the research was expressed in the form of system models within the next tasks.

Task 4 encompassed the development of basic models of the OSCAD system elements in the UML language:

- main model of the frame-type business continuity management system,
- models of its management processes with respect to the specifics of the organization's profiles,
- model of the risk management process based on economic calculation and taking into account the needs of both BCMS and ISMS,
- model of business continuity management processes within a supply chain,
- model of a central database and documents repository.

After conducting an analysis of the OSCAD elements functionality and interoperability, the main model of the business continuity management system was extended by a module for co-operation with other management systems functioning in the organization. The prototype subsystems were activated for monitoring the IT and technical infrastructures of the organization. This allows to collect information about events in a semi-automatic manner. The collected data are used to develop the OSCAD-STAT system and to undertake reliability tests. The tests are carried out by the WSB Business School in Dąbrowa Górnicza which co-operates with EMAG within the OSCAD project. The initial assumptions were formulated about collecting information on events (questionnaires), a certain number of such events were recorded in EMAG and in co-operating organizations. The questionnaires will be used in the OSCAD-STAT system too.

Task 5 focused on modelling a system for collecting, analyzing and giving access to statistical information about incidents, threats and vulnerabilities related to information security and business continuity. The following were elaborated:

- general model of the statistical information system – a model of the central module and its management processes,
- model of the central statistical database,
- model of a subsystem of two-way information exchange between the central module and BCMS/ISMS systems operating in different organizations.

Within task 6 there was a model elaborated for the co-operation of the OSCAD system with information security management systems according to ISO/IEC 27001. Here the project team considered the possibility to use common elements of two management sys-

BCMS i ISMS. Szczególną uwagę poświęcono procesowi zarządzania ryzykiem, który musi odpowiadać potrzebom każdego z systemów zarządzania. W rezultacie proces ten stał się podstawą do integracji obu systemów.

Wyniki trzech ostatnich zadań w postaci zbioru modeli będą służyły do opracowania prototypów oprogramowania, stąd modele powstały na dość wysokim poziomie szczegółowości, pozwalającym komunikować się z zespołem programistów implementujących modele. Opracowano wymagania dotyczące oprogramowania, zdefiniowano bazę danych, przypadki użycia i projekty interfejsów użytkownika. Przeprowadzono analizę wykonalności (ang. *feasibility study*) kluczowych elementów systemu OSCAD. W tym celu dokonano wstępnej implementacji tych elementów w postaci oprogramowania oraz przeprowadzono analizę wyników. W ten sposób uzyskano wartościowy materiał do prac nad prototypem.

3.3. Aktualnie realizowane i planowane zadania

Aktualnie trwają prace nad:

- opracowaniem metodyki przystosowania i wdrażania systemu zarządzania ciągłością działania z uwzględnieniem współpracy z innymi systemami zarządzania w instytucji, która ma wskazać, jak zbadać potrzeby instytucji, dostosować wzorce projektowe OSCAD do tych potrzeb i całość wdrożyć w instytucji,
- pozyskaniem wiedzy niezbędnej dla ustalenia właściwego zakresu i sposobów komputerowego wspomagania procesu zarządzania ciągłością działania w instytucji poprzez badanie modelu systemu i metodyki jego wdrażania.

Prace te umożliwią realizację prototypów oprogramowania.

4. BUDOWA I DZIAŁANIE KOMPUTEROWO WSPOMAGANEGO, ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA OSCAD

4.1. Ogólny schemat funkcjonowania OSCAD w instytucji

Na rysunku 1, na tle elementów zewnętrznych biorących udział w procesie zarządzania ciągłością działania i bezpieczeństwem informacji, przedstawiono podstawowe elementy systemu OSCAD [22]:

- grupę wewnętrznych modułów systemu OSCAD, odpowiedzialnych za realizację podstawowych zadań w zakresie wspomagania zarządzania (w celu

tems – BCMS and ISMS. Special focus was put on the risk management process which has to meet the needs of each management system. This process became the basis to integrate both systems.

The results of the three latter tasks, in the form of a set of models, will serve to develop software prototypes. That is why the models were elaborated on a significantly high level of detail which enables to communicate with the team of programmers who implement the models. The requirements for the software were elaborated. The database and use cases were defined and user interface designed. The feasibility study of key elements of the OSCAD system was conducted. In order to perform it, the initial implementation of these elements in the form of software took place and the results were analyzed. This way valuable material was obtained to work on the prototype.

3.3. Currently performed tasks and planned tasks

The currently performed works focus on:

- elaborating a methodology for customization and implementation of the business continuity management system with regard to co-operation with other management systems of the organization; the methodology is to indicate how to identify the needs of the organization, adapt the OSCAD patterns to these needs, and implement the whole in the organization,
- acquiring knowledge indispensable to define the proper range and methods of computer support of the business continuity management process in the organization by testing the system model and its implementation methodology.

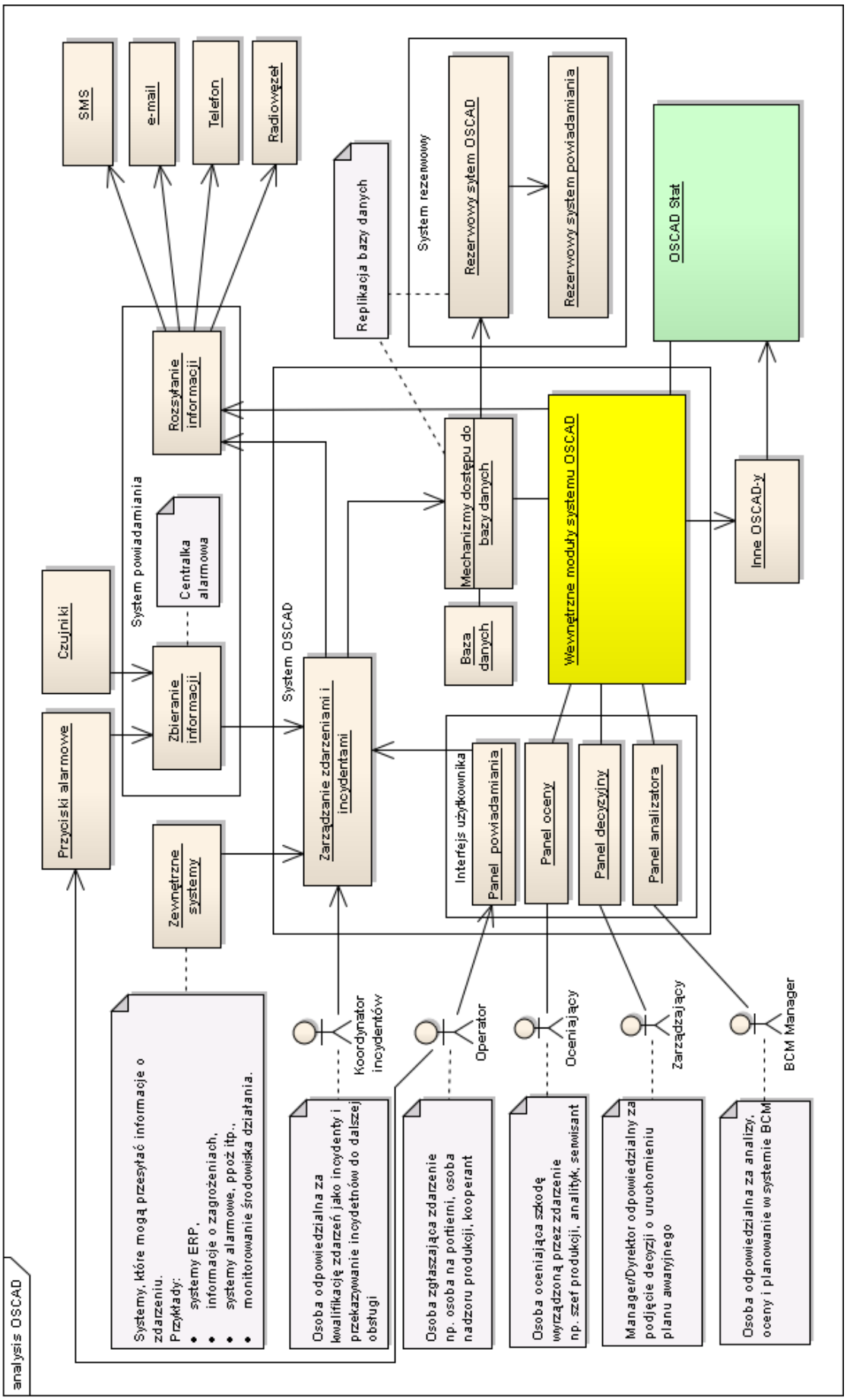
These works will enable to make software prototypes.

4. STRUCTURE AND OPERATIONS OF THE COMPUTER-SUPPORTED INTEGRATED MANAGEMENT SYSTEM OSCAD

4.1. How OSCAD functions in an organization

Figure 1 presents the basic elements of the OSCAD system against the background of external elements which take part in the business continuity and information security management process [22]:

- a group of internal modules of the OSCAD system which are responsible for the execution of basic tasks in the range of management support (to show-



Rys.1. Schemat poglądowy dotyczący funkcjonowania systemu OSCAD

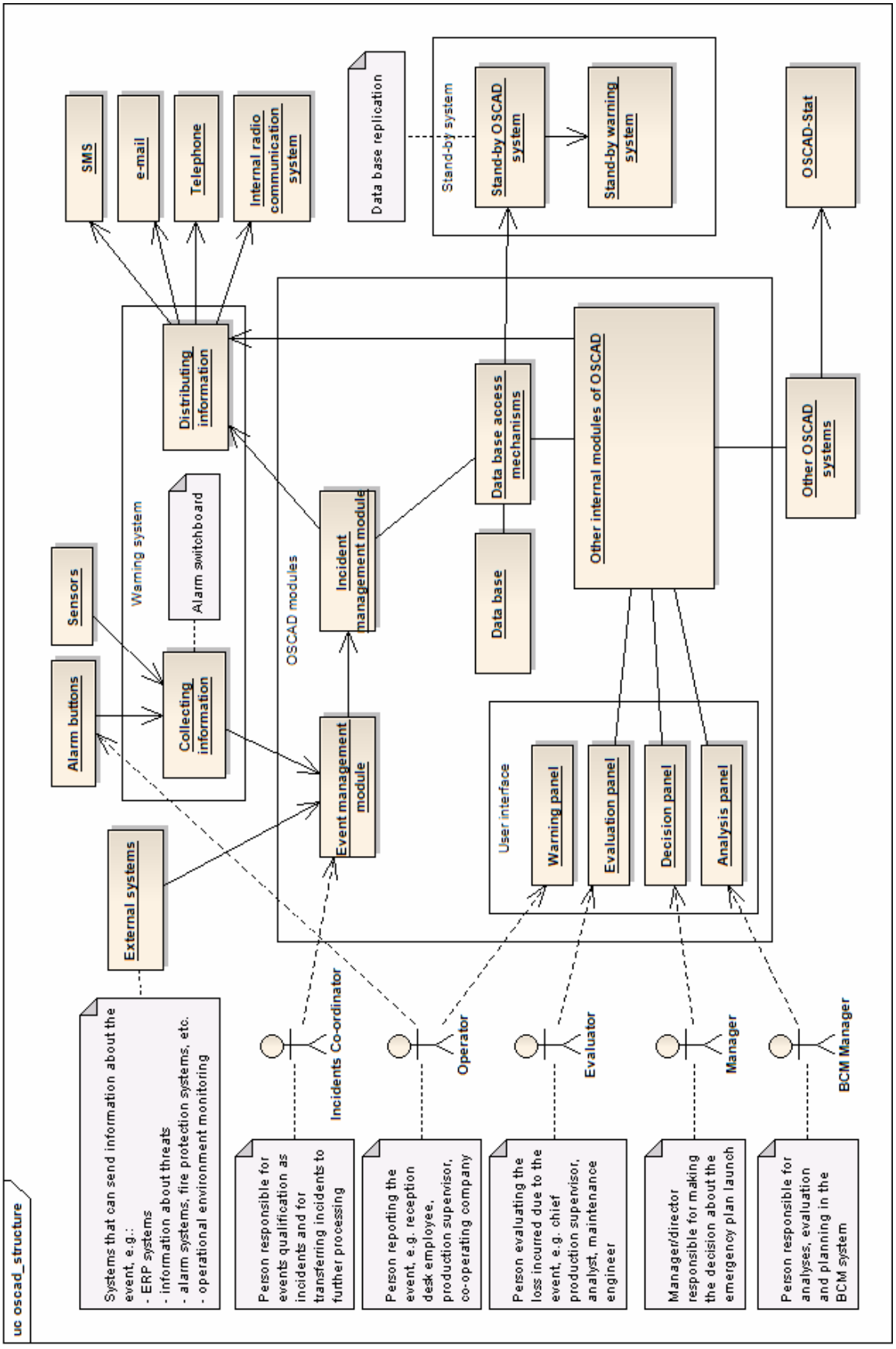


Fig.1. Diagram of the OSCAD system operations

pokazania szczególnych powiązań z grupy tej wyodrębniono moduł zarządzania zdarzeniami i incydentami),
- moduł zarządzania zdarzeniami i incydentami, jako centralny element gromadzący informacje o zdarzeniach w systemie,
- interfejs użytkownika w postaci grupy paneli współpracy z głównymi użytkownikami systemu,
- podsystem powiadamiania,
- podsystem bazodanowy.

Grupa modułów wewnętrznych zostanie scharakteryzowana w dalszej części artykułu (Rys. 2).

Moduł zarządzania zdarzeniami i incydentami pozwala na wymianę informacji z zewnętrznymi systemami zbierającymi informacje o zdarzeniach, takimi jak: systemy zarządzania zasobami przedsiębiorstwa, systemy monitorowania infrastruktury teleinformatycznej i fizycznej, systemy ochrony obiektu, w tym przeciwpożarowe, itp. Przewidziano także bezpośrednie zgłaszanie zdarzeń za pomocą formularzy oraz komunikowanie się z innymi systemami OSCAD, działającymi w innych instytucjach lub oddziałach instytucji. Wyróżniono moduł interfejsu użytkownika, za pomocą którego użytkownicy – aktorzy pełniący różne funkcje zarządzania – komunikują się z systemem OSCAD (zgłaszają zdarzenia, oceniają je, reagują lub prowadzą różne analizy).

System powiadamiania składa się z dwóch podstawowych elementów: zbierającego i rozsyłającego informacje. Pierwszy z nich pozyskuje informacje z własnego systemu powiadamiania (centralka alarmowa z przyciskami alarmowymi np. „Awaria" lub „Wypadek" na linii produkcyjnej). Możliwe jest automatyczne pozyskiwanie danych z różnego typu czujników lub zewnętrznych systemów komputerowych, np. typu ERP (ang. *Enterprise Resource Planning*). Moduł rozsyłania informacji ma za zadanie poinformowanie dostępnymi kanałami (SMS, e-mail, telefon, radiowęzeł) osób, których powiadomienie jest wymagane przez odpowiednie plany działania.

Informacje o konfiguracji systemu, rolach, słownikach, incydentach, procesach biznesowych, wynikach analiz ryzyka, wynikach audytów, podejmowanych działaniach, miernikach i wskaźnikach, itp., przechowywane są w bazie danych systemu OSCAD. Jest ona centralną częścią systemu i pełni rolę integrującą i pomocniczą dla wszystkich modułów wewnętrznych.

Ze względów bezpieczeństwa, zakładane jest uruchomienie rezerwowego systemu OSCAD i replikacja bazy danych w celu ich wykorzystania w sytuacji braku dostępności systemu głównego.

OSCAD-STAT to centralny system statystyczny, z którym systemy OSCAD wymieniają informacje, który zostanie przedstawiony w dalszej części artykułu (Rys. 3).

specific relations, the events and incidents management module was distinguished from the group),
- events and incidents management module as a central element collecting information about events in the system,
- user interface in the form of a group of panels cooperating with main users of the system,
- notification subsystem,
- database subsystem.

The group of internal modules will be described further in the article (Fig. 2).

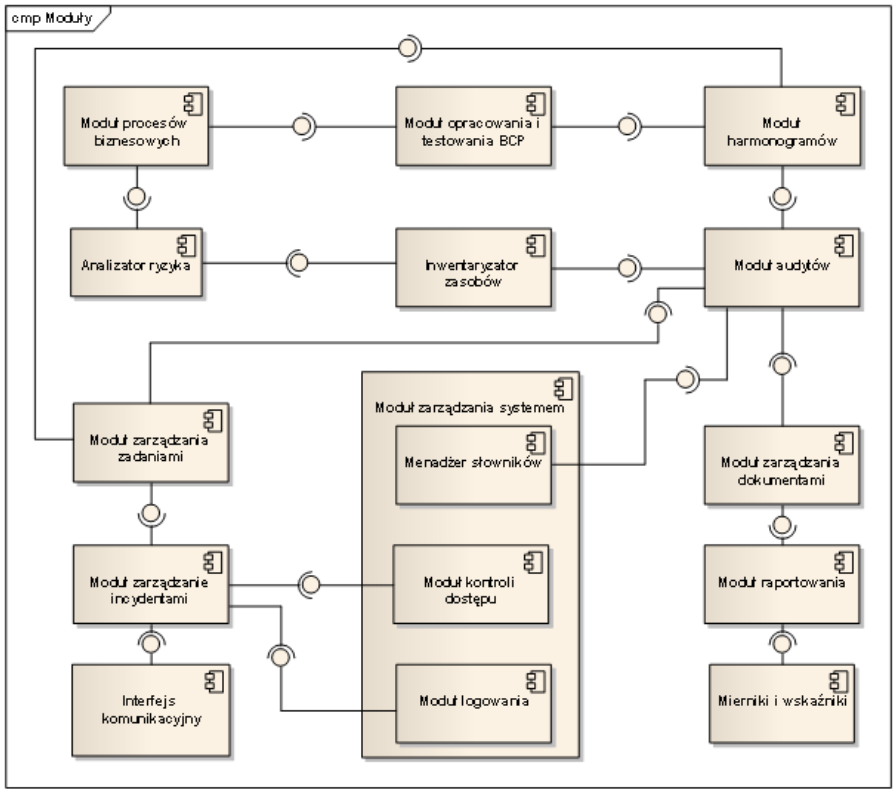
The events and incidents management module enables to exchange information with external systems which collect information about events, such as: organization's assets management systems, systems for monitoring IT and physical infrastructure, facility protection systems, including fire protection systems, etc. Direct notification about events was envisaged too by means of e-forms, along with communication with other OSCAD systems working in other organizations or in the organization's departments. The user interface module was distinguished which allows the users – actors performing different management functions to communicate with the OSCAD system (they report events, assess them, react or conduct different analyses).

The notification system consists of two basic elements: one that collects information and the other that distributes it. The first one gets information from its own notification system (burglar-, fire-, and safety alarm systems optionally equipped with alarm buttons "Damage" or "Accident" on a production line). It is possible to collect data automatically from different types of sensors or external computer systems, e.g. Enterprise Resource Planning (ERP) systems. The module that distributes information has to inform, by means of all available channels (SMS, e-mail, telephone, internal radio communication system), the people who have to be informed about the event according to proper operation procedures.

Information about the system configuration, roles, dictionaries, incidents, business processes, risk analysis results, audit results, undertaken actions, measures and indicators, etc. are stored in the OSCAD system database. This database is the central part of the system that plays an integrating and supporting role for all internal modules.

Due to security reasons, it is assumed to run a stand-by OSCAD system and to replicate the database in order to use them both in situations when the main system is not available.

OSCAD-STAT is a central statistical system that exchanges information with the OSCAD systems. OSCAD-STAT will be described further in the article (Fig. 3).



Rys. 2. Podstawowe komponenty systemu OSCAD

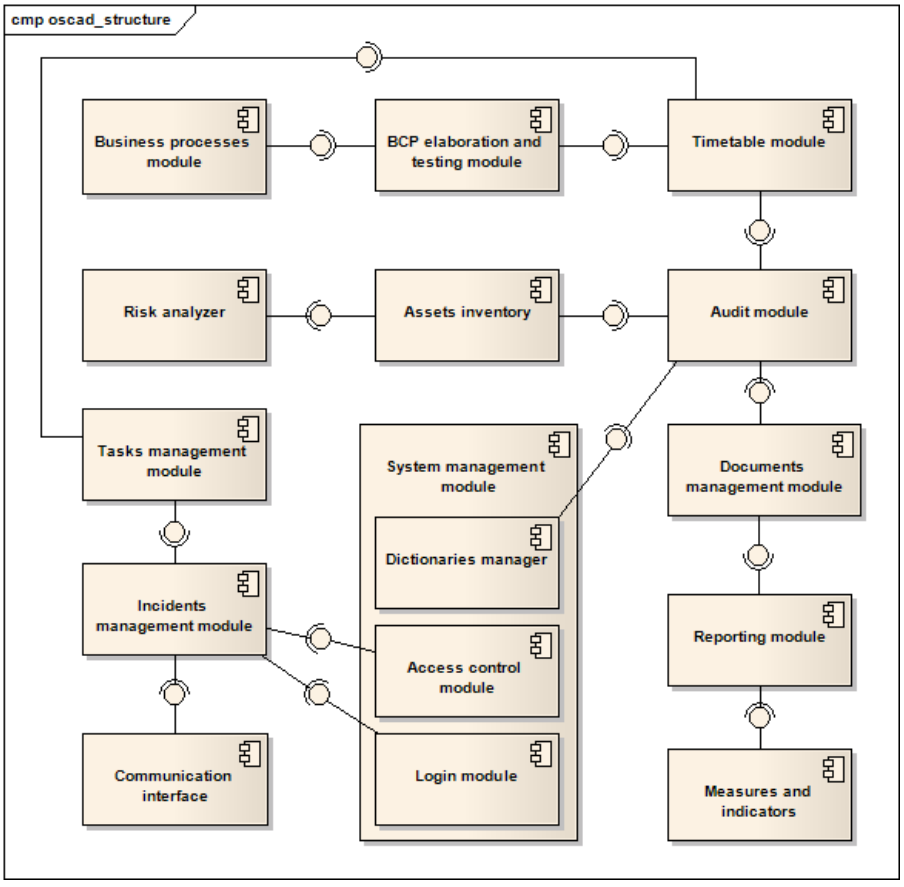


Fig. 2. Basic components of the OSCAD system

4.2. Przegląd podstawowych modułów systemu OSCAD

Diagram komponentów zamieszczony na rysunku 2 przedstawia moduły wewnętrzne systemu OSCAD oraz ich wzajemne powiązania (jako interfejsy w języku UML). Dla zachowania czytelności diagramu pokazane zostały tylko najważniejsze powiązania z modułami.

Moduł zarządzania systemem wspomaga realizacje zadań przez inne moduły i dotyczy odpowiedniego skonfigurowania systemu OSCAD, przygotowania danych predefiniowanych, w tym słowników, informacji podstawowych na temat instytucji, parametrów analizy ryzyk (macierz strat biznesowych, akceptowalny poziom ryzyka) oraz ról osób uczestniczących w procesach zarządzania ciągłością działania i bezpieczeństwem informacji. Przewiduje się możliwość ładowania do systemu predefiniowanych profili wdrożeniowych.

Działanie systemu zarządzania ciągłością działania opiera się na identyfikacji krytycznych dla instytucji procesów biznesowych i usług, a następnie na podjęciu działań zmierzających z jednej strony do minimalizacji ryzyka wystąpienia incydentu powodującego zagrożenie dla ciągłości działania, a z drugiej strony do wypracowania metod postępowania, które po wystąpieniu incydentu zmierzają do jak najszybszego przywrócenia dostępności krytycznych procesów i usług w instytucji.

Zaplanowanie systemu BCMS wymaga więc wcześniejszego dokładnego poznania sposobu działania instytucji, jej procesów biznesowych oraz wzajemnych zależności wewnętrznych (w procesach biznesowych i pomiędzy procesami) oraz zewnętrznych (relacje z dostawcami i kontrahentami, uwarunkowania środowiskowe). System OSCAD umożliwia gromadzenie informacji o instytucji i jej procesach biznesowych, które następnie są wykorzystane w kolejnych procesach zarządzania (np. w analizie ryzyka). Wokół procesów biznesowych koncentrują się wszelkie zabiegi zapewniające ciągłość działania w instytucji.

Moduł inwentaryzatora zasobów jest odpowiedzialny za zgromadzenie informacji o zasobach, grupach zasobów związanych zarówno z systemem zarządzania ciągłością działania, jak i bezpieczeństwem informacji. Wyróżniono trzy podzbiory danych odnoszące się do danego zasobu:

- dane wspólne – wykorzystywane w każdym z systemów, obejmujące m.in. nazwę zasobu, rodzaj zasobu, określenie właściciela zasobu, przypisanie zasobu do procesów,

4.2. Review of basic modules of the OSCAD system

The UML component diagram in Figure 2 presents internal modules of the OSCAD system and their mutual relations (as interfaces in UML). To make the diagram easy to read, only the most important relations with modules were shown.

The system management module supports the execution of tasks by other modules and concerns proper configuration of the OSCAD system, preparation of pre-defined data, including dictionaries, basic information about the organization, risk analysis parameters (business loss matrix, acceptable risk level), and the roles of people who take part in business continuity and information security management processes. It is assumed that pre-defined implementation profiles can be uploaded.

The operation of the business continuity management system is based on the identification of business processes and services which are critical for the organization. Then, certain actions are undertaken to minimize the risk of an incident which threatens the business continuity and to work out methods which, after the incident occurs, enable to restore access to the organization's critical processes and services as quickly as possible.

Therefore, before a BCMS system is planned, it is first necessary to get familiar with the way the organization functions, with its business processes and mutual internal dependencies (within particular business processes and between processes) and external dependencies (relations with suppliers and contractors, environmental conditions). The OSCAD system enables to store information about the organization and its business processes which are then used in successive management processes (e.g. risk analysis). All actions undertaken to provide business continuity in the organization are focused around business processes.

The assets inventory module is responsible for storing information about assets and asset groups related both to the business continuity- and information security management system. Three subsets of data related to the given asset were distinguished:

- common data – used in each system and comprising, among others: asset name, asset kind, asset owner, asset assignment to certain processes,

- dane wymagane przez system BCMS, czyli związane z ciągłością działania, takie jak: określenie krytyczności zasobu pod względem dostępności, czas i nakłady związane z odtworzeniem zasobu,
- dane wymagane przez system ISMS, czyli związane z bezpieczeństwem informacji, takie jak: przypisanie zasobu do grupy informacji i określenie w ten sposób wagi zasobu (ważności).

Zgodnie z założeniami, moduł ma umożliwiać zbieranie, modyfikowanie i usuwanie informacji o wprowadzonych do bazy zasobach.

Moduł analizatora ryzyka jest jednym z kluczowych modułów systemu OSCAD. Pozwala on ukierunkować wdrożenie tego systemu w środowisku operacyjnym instytucji. Moduł wspomaga realizację działań związanych z zarządzaniem ryzykiem, takich jak:

- konfigurowanie parametrów analizy ryzyka – ustawienie akceptowalnego poziomu ryzyka, określenie matrycy poziomów strat biznesowych, metody obliczania ważności (wagi) procesu,
- analiza wpływu na biznes (BIA) utraty takich parametrów jak dostępność, integralność procesu, usługi, informacji oraz poufności informacji (istotne w przypadku systemu zarządzania bezpieczeństwem informacji),
- określenie krytyczności procesów na podstawie wyników analizy BIA,
- określenie wartości parametrów maksymalnego dopuszczalnego czasu niedostępności (ang. *MTPD – Maximum Tolerable Period of Disruption*) i wymaganego czasu odtworzenia (ang. *RTO – Recovery Time Objective*),
- zbieranie informacji o zagrożeniach i podatnościach dla procesów, grup informacji (możliwość wyboru zdefiniowanych w bazie/słownikach zagrożeń i podatności, bądź wprowadzenia nowych),
- wycenę poziomu ryzyka z uwzględnieniem funkcjonujących zabezpieczeń,
- raportowanie wyników analizy,
- tworzenie planu postępowania z ryzykiem: akceptacja ryzyka, bądź dobór zabezpieczeń z uwzględnieniem kosztów implementacji (uwzględnienie tzw. rachunku ekonomicznego).

Analiza BIA jest wymagana przez różne systemy zarządzania, również przez system zarządzania ciągłością działania opisany normą BS 25999. Może być również częścią procesu analizy ryzyka systemów zarządzania bezpieczeństwem informacji opisanych normami z rodziny ISO 2700x.

Moduł zarządzania zdarzeniami i incydentami, którego powiązania pokazano na rysunku 1, jest odpowiedzialny za realizację następujących czynności w systemie BCMS:

- data required by the BCMS system, i.e. related to business continuity, such as: determining the asset criticality with respect to its availability, time and expenditure needed to restore the asset,
- data required by the ISMS system, i.e. related to information security, such as: the asset assignment to a certain information group and this way determining the importance of the asset.

According to the assumptions, the module will enable to collect, modify and delete information about assets placed in the database.

The risk analyzer module is one of the key modules of the OSCAD system. It allows to orientate the implementation of the system in the organization's operational environment. The module supports the execution of activities related to risk management, such as:

- configuration of risk analysis parameters – determining the acceptable risk level, determining the business loss matrix, the method to calculate the importance of the process,
- Business Impact Analysis (BIA) of the loss of such parameters as availability, integrity of a process, service or information as well as information confidentiality (important in the case of an information security management system),
- determining criticality of processes based on the BIA analysis results,
- determining parameter value of Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO),
- collecting information about threats and vulnerabilities for processes, information groups (possibility to select threats and vulnerabilities defined in bases/dictionaries or to enter new ones),
- risk level assessment with respect to existing security measures,
- analysis results reporting,
- preparing a risk treatment plan: risk acceptance or selection of security measures with respect to implementation costs (the so called economic calculation).

The BIA analysis is required by different management systems, also by a business continuity management system described in BS 25999. Additionally, BIA can be part of the risk analysis process of information security management systems described by the standards of the ISO/IEC 2700x family of standards.

The events and incidents management module, whose connections are presented in Figure 1, is responsible for the execution of the following tasks in the BCMS system:

- rejestracja zdarzenia, klasyfikacja i rejestracja incydentu,
- wstępna ocena i wybór ścieżki postępowania,
- zainicjowanie działań ratowniczych zmierzających do zabezpieczenia życia i zdrowia pracowników i klientów,
- analiza problemu i uruchomienie właściwego planu ciągłości działania (ang. *BCP – Business Continuity Plan*),
- powiadamianie zainteresowanych stron i współpraca z kooperantami,
- zapewnienie dostępności podstawowej i zapasowej lokalizacji zarządzania incydentem,
- udostępnienie wszelkich wymaganych dokumentów,
- zamknięcie incydentu,
- raportowanie,
- nauka z incydentów (ang. *lessons learnt*).

Istotnym zadaniem realizowanym w fazie D w cyklu Deminga jest opracowanie i utrzymanie planów ciągłości działania BCP, które określają:

- w jaki sposób instytucja dąży do zapewniania ciągłości działania,
- w jaki sposób przeprowadzone zostanie przywrócenie funkcjonowania procesów biznesowych do stanu normalnego.

Moduł opracowania i utrzymania planów zachowania ciągłości działania wspomaga trzy podstawowe grupy działań: opracowanie, uruchomienie i testowanie planu BCP. Przyjęto, że plany są tworzone dla procesów, które w wyniku analizy ryzyka mają przypisany atrybut „krytyczny". Plan BCP wskazuje:

- zasoby konieczne do jego uruchomienia i wykonania,
- środowisko realizacji planu – lokalizacje podstawowe i zapasowe w instytucji,
- listę kontaktową osób zaangażowanych w jego wykonanie,
- czynności planowane do wykonania podczas realizacji.

Testy mogą mieć różny charakter, zależny od rodzaju działań podejmowanych w ramach planu, zaś planowanie testów jest wspomagane przez moduł harmonogramów.

Moduł zarządzania zadaniami ma dość uniwersalny charakter. Umożliwia definiowanie zadań do realizacji przez poszczególnych użytkowników systemu oraz kontrolę ich wykonania. Zadania mogą być generowane bezpośrednio z tego modułu, bądź tworzone z poziomu innych modułów w wyniku prowadzonych w nich działań. Jako przykłady można wymienić:

- działania implikowane przez analizę ryzyka,
- działania związane z obsługą incydentu zarejestrowane w module zarządzania incydentami,

- event registration, incident classification and registration,
- preliminary evaluation and selection of proper proceedings,
- initiation of rescue operations to protect lives and health of employees and clients,
- problem analysis and start-up of a proper Business Continuity Plan (BCP),
- communication with interested parties and co-operation with contractors,
- providing accessibility of the basic and stand-by locations of incident management,
- providing all required documents,
- closing the incident,
- reporting,
- lessons learnt.

An important task within the D phase of the Deming cycle is the elaboration and maintenance of business continuity plans (BCP) which determine:

- how the organizations aims to ensure business continuity,
- how business processes will be restored to their normal condition.

The BCP elaboration and maintenance module supports three basic activity groups: elaboration, start-up and testing of the BCP plan. It was assumed that plans are created for processes which, as a result of the conducted risk analysis, have the "critical" attribute assigned. The BCP plan points at:

- assets necessary to start-up and perform the plan,
- plan execution environment – basic and stand-by locations in the organization,
- contact list of people involved in the plan execution,
- operations to be carried out.

Tests can be of different character, depending on the kinds of operations undertaken within the plan. Tests planning is supported by the timetable module.

The task management module has a universal character. It enables to define tasks to be performed by particular users of the systems and to control the performance. The tasks can be generated directly from this module or created from the level of other modules as a result of operations carried out in the module. The sample operations can be the following:

- operations implied by the risk analysis,
- incident-handling operations registered in the incident management module,

- działania wynikające z działań zaplanowanych w module harmonogramów,
- działania wynikające z opracowanych planów BCP, w przypadku konieczności uruchomienia danego planu.

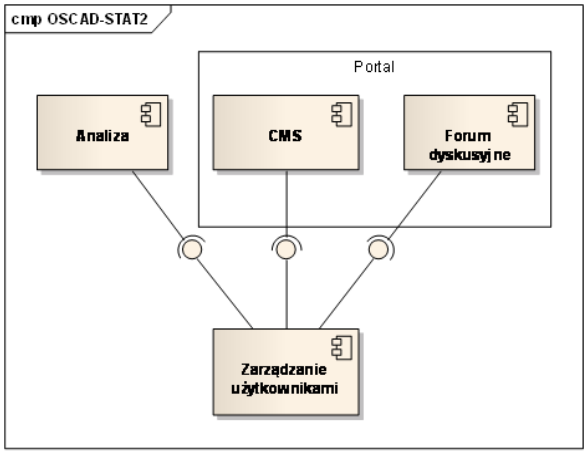
Podstawowymi funkcjami modułu są planowanie, zlecenie, nadzorowanie wykonania i przeglądanie zadań. Poza zarządzaniem ciągłością działania i bezpieczeństwem informacji w instytucji, zadania mogą dotyczyć dowolnego innego aspektu jej działalności. Warunkiem jest jedynie to, aby użytkownik, któremu zlecamy zadanie do wykonania miał konto w systemie OSCAD. Moduł zawiera funkcje powiadamiania użytkowników o zdarzeniach związanych z przepływem zadań w systemie (zlecenie, wykonanie, przeterminowanie) oraz umożliwia planowanie zadań. Funkcjonalność modułu stanowi bazę dla funkcjonalności modułu zarządzania incydentami oraz uzupełnienie funkcjonalności wielu innych modułów systemu.

Moduł audytów wspomaga zarządzanie audytami w systemie OSCAD, czyli gromadzi informacje na temat realizacji każdego audytu, wspomaga przygotowanie raportów z audytu, pomaga w zatwierdzaniu audytu przez osoby nadzorujące audyt. Samo planowanie audytów jest obsługiwane w module harmonogramów.

- operations resulting from actions planned in the timetable module,
- operations resulting from the elaborated BCP plans, in case a particular plan has to be launched.

The basic functions of the module are planning, ordering, supervising the performance and reviewing tasks. Apart from the management of business continuity and information security in the organization, the tasks can refer to any other aspect of the organization's operations. The only condition is that the user to whom the task performance is assigned should have an account in the OSCAD system. The module contains functions notifying the users about events related to the tasks flow in the system (ordered, performed, overdue) and allows to plan the tasks. The module functionality is the basis for the functionality of the incidents management module and supplements the functionalities of many other modules of the system.

The audit module supports audit management in the OSCAD system, i.e. it collects information about the execution of each audit, supports audit reports preparation, helps in audit approval by people who supervise it. Audit planning as such is handled in the timetable module.



Rys. 3. Podstawowe komponenty systemu OSCAD-STAT

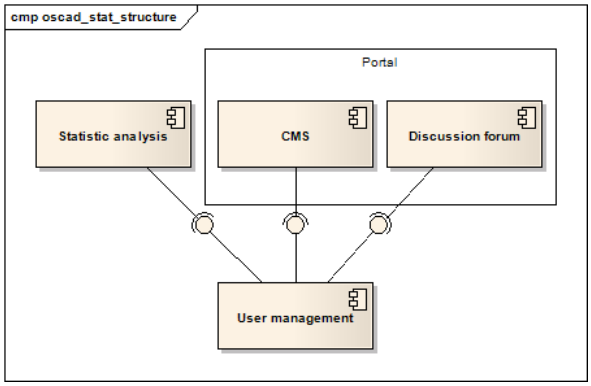


Fig. 3. Basic components of the OSCAD-STAT system

Moduł harmonogramów wspomaga planowanie działań zarządczych podejmowanych w pewnym horyzoncie czasowym w ramach różnych modułów.

Informacje o systemie BCMS/ISMS zebrane w toku jego wdrażania i utrzymywane podczas eksploatacji mogą być prezentowane w formie tekstowej, graficznej lub eksportowane na zewnątrz z wykorzystaniem popularnych formatów. Jest za to odpowiedzialny moduł raportów. Przewidywane są co najmniej następujące raporty zawierające:

- informacje o instytucji i jej procesach biznesowych,
- informacje o zasobach instytucji zaangażowanych w realizację procesów i systemu OSCAD,
- podsumowanie przebiegu analizy ryzyka,
- podsumowanie planowanych zadań wchodzących w skład harmonogramów,
- informacje o planach BCP,
- podsumowanie wyników przeprowadzonych audytów,
- podsumowanie działań korygujących i naprawczych,
- wartości mierników i wskaźników służących do doskonalenia systemu BCMS/ISMS,
- podsumowanie realizacji różnych zadań,
- statystyki związane z incydentami.

Moduł zarządzania dokumentami jest odpowiedzialny za rejestrowanie, wersjonowanie, obieg, zatwierdzanie, wyszukiwanie, itp., dokumentów systemów zarządzania BCMS oraz ISMS według wymagań standardów. Dokumenty i ich szablony dołączane do systemu są przechowywane w repozytorium danych. Jako przykłady dokumentów można wymienić: „Politykę systemu zarządzania ciągłością działania", „Opis metodyki szacowania ryzyka oraz kryteriów jego akceptacji", czy też „Procedurę nadzoru nad zapisami".

Zadaniem modułu komunikacji jest wymiana informacji z systemami zewnętrznymi i osobami funkcyjnymi. Interfejs komunikacyjny realizuje w trybie automatycznym fazy wykrycia i zgłoszenia zdarzenia dla modułu zarządzania incydentem. Rejestracja zdarzeń może przebiegać w sposób „ręczny" (wprowadzenie przez osobę zgłaszającą informacji o zdarzeniu), bądź automatyczny, poprzez szablon w języku XML generowany i wysyłany przez system lub urządzenia zewnętrzne, w tym również inne systemy typu OSCAD.

Obecnie rozpatrywane systemy zewnętrzne można podzielić ze względu na realizowane funkcje:

- systemy planowania zasobów przedsiębiorstwa (ERP),
- systemy zarządzania usługami informatycznymi,
- systemy automatyki budynków,
- systemy sygnalizacji włamania i napadu.

The timetable module supports to plan management operations undertaken at a certain time horizon within different modules.

Information about the BCMS/ISMS system collected during its implementation and kept during exploitation can be presented as text, graphics or exported with the use of popular formats. This job is done by the reports module. The following reports are expected as minimum:

- information about the organization and its business processes,
- information about the organization's assets involved in the execution of the OSCAD system,
- summary of the risk analysis process,
- summary of planned tasks which are part of timetables,
- information about BCP plans,
- summary of audit results,
- summary of preventive and corrective actions,
- values of measures and indicators used for continual improvement of the BCMS/ISMS system,
- summary of different tasks execution,
- statistics related to incidents.

The documents management module is responsible for registration, version control, circulation, confirmation, search, etc. of BCMS and ISMS systems documents according to the requirements of standards. Documents and their templates are attached to the system and stored in the data repository. Sample documents are: "Business continuity management system policy", "Description of risk assessment methodology and risk acceptance criteria", or "Records supervision procedure".

The communication module is responsible for information exchange between external systems and appointed persons. The communication interface automatically performs the phases of event detection and notification for the incident management module. Events registration can be done "manually" (entered by a person who gives information about the event) or automatically by means of an XML template generated and sent by the system or by external devices, including other OSCAD-type systems.

The external systems that are currently taken into account can be divided with respect to the functions they perform:

- Enterprise Resource Planning (ERP) systems,
- IT services management systems,
- building automation systems,
- burglary or fire alarm systems.

Interfejs komunikacyjny będzie realizował połączenie z zewnętrznymi systemami poprzez moduł Stacja monitorująca, który będzie zawierał implementację wszystkich rozpoznanych protokołów komunikacyjnych.

Moduł mierników i wskaźników przechowuje parametry systemu zarządzania dotyczące jego efektywności. Pozwala to na ich okresową analizę i podejmowanie działań doskonalących system.

Moduł słowników wynika z potrzeby stosowania dla danej instytucji różnego typu list predefiniowanych wykorzystywanych przez oprogramowanie. Słowniki pozwalają na łatwe dostosowanie systemu OSCAD do profilu instytucji, w której będzie on wdrażany. Słowniki zawierają także elementy specyficzne, jak wymagania podlegające audytom. Mogą to być wymagania norm, aktów prawnych, czy wewnętrznych regulacji instytucji. W słownikach zostaną zapisane również zagrożenia, podatności oraz zabezpieczenia specyficzne dla konkretnej instytucji.

4.3. System zbierania danych statystycznych i inne wspomagające

Na rysunku 3 przedstawiono podstawowe elementy systemu OSCAD-STAT.

Założono, że system OSCAD-STAT powinien składać się z dwóch niezależnych modułów funkcjonalnych. Pierwszy z nich, OSCAD-STAT ANALIZA jest odpowiedzialny za:

- wymianę danych z systemami OSCAD działającymi w różnych instytucjach,
- przygotowanie danych statystycznych,
- udostępnianie poprawek i nowych wersji systemu OSCAD (opcja).

Moduł OSCAD-STAT PORTAL jest odpowiedzialny za:

- prezentację danych statystycznych zebranych przez system OSCAD i inne systemy wspomagające,
- upowszechnianie wiedzy dotyczącej zarządzania ciągłością działania i wiedzy zdobytej w ramach prowadzonego projektu,
- udostępnienie platformy wymiany doświadczeń z tematyki bezpieczeństwa informacji i ciągłości działania pomiędzy wszystkimi zainteresowanymi stronami.

Dodatkowo prowadzone są prace nad modułem OSCAD-REDUNDANCJA, który będzie odpowiedzialny za udostępnienie kompleksowej platformy informatyczno-komunikacyjnej umożliwiającej instalację zapasowych instancji systemu OSCAD, uruchamianych w przypadku sytuacji kryzysowej powodującej niedostępność dla instytucji podstawowej instancji systemu OSCAD.

The communication interface will provide connection with external systems through the monitoring station module which will also contain the implementation of all recognized communication protocols.

The measures and indicators module stores the efficiency parameters of the management system. This allows to conduct periodical analyses and make decisions about actions to improve the system.

The dictionaries module results from the need to apply different types of pre-defined lists used by the software. Dictionaries allow to easily adapt the OSCAD system to the organization's profile. They also contain specific elements, such as requirements that are subject to audits. These can be the requirements of standards, laws or internal regulations of the organization. The dictionaries also encompass threats, vulnerabilities and security measures specific for the given organization.

4.3. Statistical data collection system and other auxiliary modules

Figure 3 features basic elements of the OSCAD-STAT system.

It was assumed that OSCAD-STAT should consist of two independent functional modules. The first one, OSCAD-STAT ANALIZA is responsible for:

- data exchange with OSCAD systems working in different organizations,
- preparation of statistical data,
- giving access to corrections and new versions of the OSCAD system (option).

The OSCAD-STAT PORTAL module is responsible for:

- presentation of statistical data collected by the OSCAD system and other supporting systems,
- dissemination of knowledge concerning business continuity and knowledge accumulated within the conducted project,
- giving access to a platform where there is exchange of experiences on information security and business continuity between all interested parties.

Additionally, there are works conducted on the OSCAD-REDUNDANCJA module which will be responsible for providing access to a complex information and communication platform. The platform will enable to start up the redundant OSCAD system which will be run only in crisis situations when the basic system is not accessible by the organization.

5. PODSUMOWANIE

Artykuł dotyczy założeń i pierwszych rezultatów projektu celowego pn. „Otwarty Szkieletowy System Zarządzania Ciągłością Działania" (OSCAD), który od około roku jest realizowany w Instytucie Technik Innowacyjnych EMAG.

Projekt dotyczy zagadnień techniczno-organizacyjnych związanych z budową w instytucjach systemów zarządzania ciągłością działania. Elementami innowacyjnymi w projekcie OSCAD są:

- otwartość systemu uzyskana przez odstąpienie od rozwiązania dedykowanego i opracowanie zbioru modułów wzorcowych oraz metodyki ich przystosowania i wdrażania zgodnie z potrzebami danej instytucji;
- opracowanie zaawansowanego narzędzia wspomagającego procesy wdrożenia i utrzymania systemu typu BCMS;
- integracja z systemem zarządzania bezpieczeństwem informacji ISMS (ISO/IEC 27001);
- możliwość analizy statystycznej zdarzeń i analizy niezawodnościowej funkcjonowania systemów informatycznych;
- możliwość wymiany informacji między różnymi instytucjami;
- łatwa integracja z innymi systemami zarządzania współistniejącymi w instytucji;
- wspomaganie funkcjonowania instytucji w łańcuchu dostaw.

Dzięki modułom wzorcowym i sparametryzowanym zapewniona zostanie konfigurowalność i skalowalność systemu. System można budować wybierając określone moduły ze zbioru predefiniowanych wzorców, a następnie je przystosowując (ang. *customization*) do indywidualnych potrzeb instytucji. Potrzeby te są identyfikowane w pierwszym etapie metodyki przystosowania i wdrażania.

Zagadnienie zarządzania ciągłością działania ma duże znaczenie dla współczesnego biznesu i administracji publicznej, jednak rozwiązania należy wdrażać i eksploatować z uwzględnieniem analizy potrzeb oraz kosztów. Dzięki zastosowanej metodzie zarządzania ryzykiem, relacje między osiąganymi wskaźnikami ciągłości działania a kosztami ich osiągania będą mogły być kontrolowane, co pozytywnie wpłynie na efektywność procesu zarządzania ciągłością działania w instytucji.

Wyniki projektu są dedykowane głównie dla:

- firm będących elementem krytycznej infrastruktury państwa (energetyka, produkcja i dystrybucja paliw, telekomunikacja, itp.),

5. CONCLUSIONS

The article concerns assumptions and first results of the specific-targeted project "OSCAD – open, frame-type, integrated management system for business continuity and information security" which has been carried out for a year at the Institute of Innovative Technologies EMAG.

The project concerns technical and organizational issues related to the construction of business continuity management systems in organizations. The OSCAD project has the following innovative elements:

- open character of the system achieved due to withdrawal from a dedicated solution and the development of a set of standard modules (patterns), along with the methodology of their adaptation and implementation according to the organization's needs;
- development of an advanced tool supporting the implementation and maintenance processes of a BCMS system;
- integration with an information security management system ISMS (ISO/IEC 27001);
- possibility to conduct a statistical analysis of events and reliability analysis of IT systems functioning;
- possibility to exchange information between different organizations;
- easy integration with other management systems co-existing in the organization;
- support for organizations working within supply chains.

The system configurability and scalability are achieved thanks to standard and parameterized modules. The system can be constructed by means of selecting particular modules from the set of predefined patterns and then customizing them to the needs of the organization. These needs are identified in the first phase of the customization and implementation methodology.

Business continuity issues are of key importance for modern businesses and public administration. However, the solutions have to be implemented and exploited with respect to the needs and costs analysis. Thanks to the applied risk management method, it is possible to control the relations between the achieved business continuity indicators and the costs to achieve them. This has a positive impact on the efficiency of the business continuity management process in the organization.

The project results are chiefly dedicated to:

- organizations which are elements of the critical infrastructure of the country (power engineering, production and distribution of fuels, telecommunications, etc.),

- instytucji finansowych (np. w sektorze ubezpieczeń czy bankowości),
- firm świadczących usługi w formie elektronicznej,
- instytucji administracji publicznej (rządowej, samorządowej),
- instytucji reprezentujących służbę zdrowia,
- instytucji zajmujących się bezpieczeństwem grup osób,
- innych firm handlowych i przemysłowych.

Zainicjowany projekt jest ukierunkowany głównie na różne formy biznesu i potrzeby administracji, a także, po pewnych modyfikacjach, może zostać użyty np. w systemach wspomagających zarządzanie kryzysowe.

W toku realizacji prototypów szczególna uwaga zostanie poświęcona wersjom dedykowanym do specjalistycznych zastosowań. W obszarze górnictwa realizatorzy projektu dostrzegają możliwość realizacji wersji dedykowanych systemu OSCAD do wspomagania zarządzania:

- ciągłością działania zakładu górniczego, jako wartość dodana do systemu monitorowania parametrów produkcji i bezpieczeństwa oferowanego przez Instytut EMAG,
- działaniem służb ratunkowych w górnictwie,
- ciągłością pracy maszyn i urządzeń.

Podjęcie prac nad wersjami dedykowanymi wymaga nawiązania ścisłej współpracy ze specjalistami z poszczególnych dziedzin zastosowań.

System OSCAD może być stosowany w dowolnej instytucji, która planuje wdrożyć system BCMS lub ISMS zgodny z normami. Wdrożenie to niekoniecznie musi się kończyć formalnym procesem certyfikacji, jednak wykorzystanie systemu OSCAD ułatwi przygotowanie się instytucji do takiej certyfikacji.

- financial institutions (e.g. in the sectors of insurance or banking),
- organizations offering e-services,
- public administration (government- or local government level),
- organizations representing the sector of health services,
- organizations involved in the protection of groups of people,
- other commercial and industrial companies.

The initiated project is directed mainly to different forms of business and the needs of the administration. Additionally, after certain modifications, it can be used, for example, in systems which support crisis management.

In the course of the prototypes development special focus will be on versions dedicated to specific applications. In the mining industry, the project team see the possibility to apply dedicated versions of the OSCAD system in the management support of the following:

- business continuity of a mine as a value added to a system for monitoring production parameters and security – such systems are manufactured by EMAG,
- operations of mining rescue services,
- operating continuity of machines and devices.

In order to start working on dedicated versions it is necessary to take up close co-operation with specialists from particular application domains.

The OSCAD system can be used in any organization which plans to implement a BCMS or ISMS system according to valid standards. This implementation does not have to be completed with a formal certification process, yet the use of the OSCAD system will make it easier for the organization to get prepared for such certification.

Bibliografia

1. BS 25999-1:2006 Business Continuity Management – Code of Practice.
2. BS 25999-2:2007 Business Continuity Management – Specification for Business Continuity Management.
3. PN-ISO/IEC 27001 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
4. PN-ISO/IEC 17799:2007 – Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.
5. http://pl.wikipedia.org/wiki/Cykl_Deminga
6. *Białas A*.: Komputerowo wspomagany system zarządzania ciągłością działania – założenia projektu, Materiały konferencyjne EMTECH'2010 – Zasilanie, informatyka techniczna i automatyka w przemyśle wydobywczym – Innowacyjność i bezpieczeństwo. Ustroń, 19-21 maja 2010, pp. 29-37.
7. *Białas A*.: Development of an Integrated, Risk-based Platform for Information and E-services Security, In: Górski J.: Computer Safety, Reliability, and Security, 25th International Conference SAFECOMP2006, Springer Lecture Notes in Computer Science (LNCS4166), Springer Verlag Berlin Heidelberg New York 2006, ISBN 3-540-45762-3, pp. 316-329.
8. IT Infrastructure Library, www.itil.co.uk

References

1. BS 25999-1:2006 Business Continuity Management – Code of Practice.
2. BS 25999-2:2007 Business Continuity Management – Specification for Business Continuity Management.
3. PN-ISO/IEC 27001 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
4. PN-ISO/IEC 17799:2007 – Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.
5. http://pl.wikipedia.org/wiki/Cykl_Deminga
6. *Białas A*.: Komputerowo wspomagany system zarządzania ciągłością działania – założenia projektu, Materiały konferencyjne EMTECH'2010 – Zasilanie, informatyka techniczna i automatyka w przemyśle wydobywczym – Innowacyjność i bezpieczeństwo. Ustroń, 19-21 May 2010, pp. 29-37.
7. *Białas A*.: Development of an Integrated, Risk-based Platform for Information and E-services Security, In: Górski J.: Computer Safety, Reliability, and Security, 25th International Conference SAFECOMP2006, Springer Lecture Notes in Computer Science (LNCS4166), Springer Verlag Berlin Heidelberg New York 2006, ISBN 3-540-45762-3, pp. 316-329.
8. IT Infrastructure Library, www.itil.co.uk

9. ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification.
10. ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of practice.
11. BS PAS 99:2006, Specification of common management system requirements as a framework for integration.
12. *Białas A.*: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwa Naukowo-Techniczne, Warszawa 2006, 2007.
13. *Białas A.*: Using ISMS concept for critical information infrastructure protection. In: Balducelli A., Bologna S. (eds), Proceedings of the International Workshop on "Complex Network and Infrastructure Protection – CNIP'06", ENEA – Italian National Agency for New Technologies, Energy and the Environment, Rome, March 28-29, 2006, pp. 415-426.
14. *Białas A.*: The ISMS Business Environment Elaboration Using a UML Approach, In: Zieliński K., Szmuc T. (editors): Software Engineering: Evolution and Emerging Technologies, IOS Press, Amsterdam, 2005, ISBN: 1 58603-559-2, pp. 99-110.
15. *Białas A.*: A UML approach in the ISMS implementation, In: Dowland P., Furnell S., Thuraisingham B., Wang X.S. (eds): Security management, integrity, and internal control in information systems, IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference, Springer Science + Business Media, New York 2005, ISBN-10:0-387-29826-6, pp. 285-297.
16. *Białas A.*: Development of the Information Security Management System for the Polish Mining Sector, Mechanizacja i Automatyzacja Górnictwa 2007, nr 8(439), Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 34-41.
17. *Wartak A., Lisek K.*: Walidacja systemu zarządzania bezpieczeństwem informacji dla sektora węgla kamiennego, Mechanizacja i Automatyzacja Górnictwa 2007, nr 10(441), Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 39-46.
18. *Styczeń I., Bagiński J.*: Oprogramowanie wspomagające system zarządzania bezpieczeństwem informacji. Mechanizacja i Automatyzacja Górnictwa 2007, nr 11(442), Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 22-29.
19. *Białas A., Lisek K.*: Integrated, business-oriented, two-stage risk analysis. Journal of Information Assurance and Security, vol. 2, issue 3, Atlanta, September 2007, w.dynamicpublishers.com/JIAS
20. *Bialas A.*: Security Trade-off – Ontological Approach, In: Akbar Hussain D. M. (Ed.), Advances in Computer Science and IT, ISBN 978-953-7619-51-0, In-Tech, Vienna-Austria, Vukovar-Croatia, 2009, pp. 39-64.
21. *Bialas A.*: Ontological Approach to the Business Continuity Management System Development. In: Arabnia H., Daimi K., Grimaila M.R., Markowsky G (Eds.), Proceedings of the 2010 International Conference on Security and Management (The World Congress In Applied Computing – SAM'10: July 12-15, Las Vegas, USA), Vol. II, ISBN: 1-60132-159-7, 1-60132-162-7 (1-60132-163-5), 2010, Publisher: CSREA Press, pp. 386-392.
22. Praca zbiorowa. Raporty projektu celowego pn. „Komputerowo wspomagany system zarządzania ciągłością działania – OSCAD", Instytut EMAG, 2010-2011.

Recenzent: dr inż. Włodzimierz Boroń

9. ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification.
10. ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of practice.
11. BS PAS 99:2006, Specification of common management system requirements as a framework for integration.
12. *Białas A.*: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwa Naukowo-Techniczne, Warszawa 2006, 2007.
13. *Białas A.*: Using ISMS concept for critical information infrastructure protection. In: Balducelli A., Bologna S. (eds), Proceedings of the International Workshop on "Complex Network and Infrastructure Protection – CNIP'06", ENEA – Italian National Agency for New Technologies, Energy and the Environment, Rome, March 28-29, 2006, pp. 415-426.
14. *Białas A.*: The ISMS Business Environment Elaboration Using a UML Approach, In: Zieliński K., Szmuc T. (editors): Software Engineering: Evolution and Emerging Technologies, IOS Press, Amsterdam, 2005, ISBN: 1 58603-559-2, pp. 99-110.
15. *Białas A.*: A UML approach in the ISMS implementation, In: Dowland P., Furnell S., Thuraisingham B., Wang X.S. (eds): Security management, integrity, and internal control in information systems, IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference, Springer Science + Business Media, New York 2005, ISBN-10:0-387-29826-6, pp. 285-297.
16. *Białas A.*: Development of the Information Security Management System for the Polish Mining Sector, Mechanizacja i Automatyzacja Górnictwa 2007, nr 8(439), Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 34-41.
17. *Wartak A., Lisek K.*: Walidacja systemu zarządzania bezpieczeństwem informacji dla sektora węgla kamiennego, Mechanizacja i Automatyzacja Górnictwa 2007, nr 10(441), Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 39-46.
18. *Styczeń I., Bagiński J.*: Oprogramowanie wspomagające system zarządzania bezpieczeństwem informacji. Mechanizacja i Automatyzacja Górnictwa 2007, nr 11(442), Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 22-29.
19. *Białas A., Lisek K.*: Integrated, business-oriented, two-stage risk analysis. Journal of Information Assurance and Security, vol. 2, issue 3, Atlanta, September 2007, www.dynamicpublishers.com/JIAS
20. *Bialas A.*: Security Trade-off – Ontological Approach, In: Akbar Hussain D. M. (Ed.), Advances in Computer Science and IT, ISBN 978-953-7619-51-0, In-Tech, Vienna-Austria, Vukovar-Croatia, 2009, pp. 39-64.
21. *Bialas A.*: Ontological Approach to the Business Continuity Management System Development. In: Arabnia H., Daimi K., Grimaila M.R., Markowsky G (Eds.), Proceedings of the 2010 International Conference on Security and Management (The World Congress In Applied Computing – SAM'10: July 12-15, Las Vegas, USA), Vol. II, ISBN: 1-60132-159-7, 1-60132-162-7 (1-60132-163-5), 2010, Publisher: CSREA Press, pp. 386-392.
22. Team work: Reports of the specific-targeted project "Computer-supported business continuity management system – OSCAD", Instytut EMAG, 2010-2011.

ИНТЕГРИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ РАБОТЫ И БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ – ПОДВЕДЕНИЕ ИТОГОВ РЕЗУЛЬТАТОВ РАБОТ, НАПРАВЛЕННЫХ НА ПОСТРОЙКУ МОДЕЛЕЙ СИСТЕМЫ

Тематика реферата связана с совместным внедрением известных на свете стандартов: BS 25999, касающегося непрерывности работы института, и ISO/IEC 27001, касающегося безопасности информации института, в рамках одной интегрированной системы управления. Непрерывность работы понимается как стратегическая и тактическая способность института реагировать на инциденты и нарушения в деловом функционировании, а также способность ограничивать убытки в случае появления данных вредных факторов, с другой стороны безопасность информации связана с защитой целостности, доступности и тайности информации. Реферат представляет основные положения и существующие результаты целевого проекта, касающегося разработки системы управления, предназначенной для фирм и институтов, для которых вопрос непрерывности деловых процессов и безопасности информации является особенно важным. В реферате подведены итоги работ над моделью системы, в том числе изучений выполнимости, касающихся разных вопросов программного обеспечения, создаваемого на основании данных моделей. Обращено внимание на возможности использования создаваемой системы, в том числе также в горнопромышленной отрасли.