Zeszyty Naukowe UNIWERSYTETU PRZYRODNICZO-HUMANISTYCZNEGO w SIEDLCACH
Seria: Administracja i Zarządzanie
Nr 105 2015

mgr inż. Michał Klimek
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Bezpieczeństwo teleinformatyczne i bezpieczeństwo informacji w przedsiębiorstwach budownictwa inżynieryjnego

Communication technology security and information security in enterprises of engineering construction

Streszczenie: Celem artykułu jest przybliżenie aspektów związanych z bezpieczeństwem teleinformatycznym i zastosowaniem Systemu Zarządzania Bezpieczeństwem Informacji w przedsiębiorstwach budownictwa inżynieryjnego. System ten wchodzi w skład Zintegrowanego Systemu Zarządzania w tych przedsiębiorstwach. Stanowi jeden z najważniejszych elementów Zintegrowanego Systemu Zarządzania. Pomaga w zdobywaniu pozycji firm budowlanych na rynku krajowym i międzynarodowym oraz wspiera zarządzanie poufną informacją, jak również niezakłóconą i bezpieczną pracą stosowanych technologii przetwarzania i transmisji danych.

Słowa kluczowe: System Zarządzania Bezpieczeństwem Informacji, bezpieczeństwo teleinformatyczne, bezpieczeństwo informacji, bezpieczeństwo usług, bezpieczeństwo decyzji

Abstract: The aim of the article is to present aspects related to the teleinformatic safety and use of the Information Security Management System in engineering construction enterprises. This system is part of the Integrated Management System in these companies. It is one of the most important elements of the Integrated Management System. It helps in building the position of construction companies at the domestic and international level, and supports the management of confidential information, as well as the smooth and secure operation of applied technology and data processing.

Keywords: Information Security Management System (ISMS), Communication Technology Security, Information Security Services Security, Decisions Security

Wstęp

Bezpieczeństwo teleinformatyczne odnosi się w szczególności do niczym niezakłóconej pracy systemów informatycznych, natomiast zastosowanie normatywnego Systemu Zarządzania Bezpieczeństwem Informacji w przedsiębiorstwach budownictwa inżynieryjnego odgrywa istotną rolę w procesie obiegu informacji i w tych organizacjach oraz ochronie danych, zarówno dotyczących pracowników i klientów, jak również danych strategicznych, związanych z podejmowanymi przez kierownictwo decyzjami. System zarządzania związany z bezpieczeństwem, wchodzący w skład zintegrowanego systemu zarządzania w przedsiębiorstwach sektora budownictwa, stanowi jeden z czynników, który przyczynia się do budowania przewagi firm budowlanych na rynku krajowym i międzynarodowym. Troska o skuteczne zarządzanie poufną informacją, jak

również niezakłóconą i bezpieczną pracą stosowanych technologii przetwarzania i transmisji danych należy do celów strategicznych, które pochodzą bezpośrednio ze stosowanej polityki jakości w badanych przedsiębiorstwach z sektora budownictwa inżynieryjnego.

Prezentowana publikacja będzie stanowiła jakby próbę nakreślenia praktycznego funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji stosowanego w sektorze przedsiębiorstw budownictwa inżynieryjnego, w których został wdrożony, zgodnego z normą PN-ISO/IEC 27001. Należy jednak pamiętać, że bezpieczeństwo informacji dotyczy również skutecznie podejmowanych decyzji i powiązane jest z bezpieczeństwem usług. Odpowiednie zarządzanie informacją, wchodzącą w skład aktywów przedsiębiorstwa i posiadającą wysoką wartość i znaczenie dla organizacji, powinno odbywać się poprzez jej pogrupowanie, oznaczenie, przefiltrowanie oraz odpowiednie uporządkowanie. Działania takie zabezpieczają i obniżają poziom ryzyka związanego z utratą cennych danych, które wykorzystane przez innych mogą wręcz zaszkodzić organizacji.

Pojęcie bezpieczeństwa teleinformatycznego

Bezpieczeństwo teleinformatyczne odnosi się do bezpieczeństwa systemów komputerowych, danych elektronicznych oraz transmisji danych w sieciach teleinformatycznych. Zagrożenie dla bezpieczeństwa teleinformatycznego stanowią osoby naruszające zasady bezpieczeństwa danego systemu, złośliwe oprogramowanie, błędy w programach, przerwy w łączach sieci teleinformatycznych oraz zjawiska losowe np. pożar, powódź itp. Zagadnienia związane z bezpieczeństwem teleinformatycznym, dotyczą ochrony systemów teleinformatycznych przed włamaniami, ochrony przed kradzieżą danych i oprogramowania, zniszczeniem danych i programów, ochroną poufności i zapewnieniem integralności danych oraz ochroną systemów teleinformatycznych przed złośliwym oprogramowaniem. Bezpieczeństwo teleinformatyczne realizowane jest poprzez określenie zasad autoryzacji i kontroli dostępu do systemów, zasobów i usług, zdefiniowania zasad poufności i integralności danych w systemach komputerowych oraz zdefiniowania mechanizmów podnoszenia stopnia dostępu do informacji, w tym odpowiednich uprawnień personelu[1].

Zarządzanie bezpieczeństwem teleinformatycznym będzie polegało na tworzeniu polityki bezpieczeństwa dla wdrożonych systemów komputerowych, określenia w jakiej klasie bezpieczeństwa znajduje się stosowany system, monitorowanie i nadzorowanie zabezpieczeń oraz tworzenie zasad dostępu do zasobów, w tym również proces uwierzytelniania użytkowników, tworzenia procedur związanych z analizą ryzyka oraz procedur reagowania na incydenty naruszenia bezpieczeństwa teleinformatycznego systemów operacyjnych i aplikacji[2].

Termin bezpieczeństwo teleinformatyczne określa przede wszystkim systemy stosowane przez jednostki i organizacje rządowe, wojskowe oraz publiczne w kraju oraz przedsiębiorstwa i organizacje w znaczeniu strategicznym. Specyfi-

[1] Lipiński Z., *Bezpieczeństwo teleinformatyczne - Wstęp.* Wykład 1' Instytut Matematyki i Informatyki Uniwersytetu Opolskiego, s. 1-2.
[2] Tamże.

kacje i dokumenty dotyczące bezpieczeństwa teleinformatycznego regulowane są przez ustawy i rozporządzenia Rady Ministrów.

W organizacjach i przedsiębiorstwach przemysłowych, należących do sektora budownictwa inżynieryjnego, w celu zapewnienia poufności, dostępności i integralności danych, czyli ochrony informacji oraz jej przetwarzania w systemach i sieciach teleinformatycznych, stosowany jest normatywny system zarządzania bezpieczeństwem informacji, zgodne z PN-ISO/IEC 27001.

System Zarządzania Bezpieczeństwem Informacji zgodny z PN-ISO/IEC 27001 stosowany w przedsiębiorstwach budownictwa inżynieryjnego

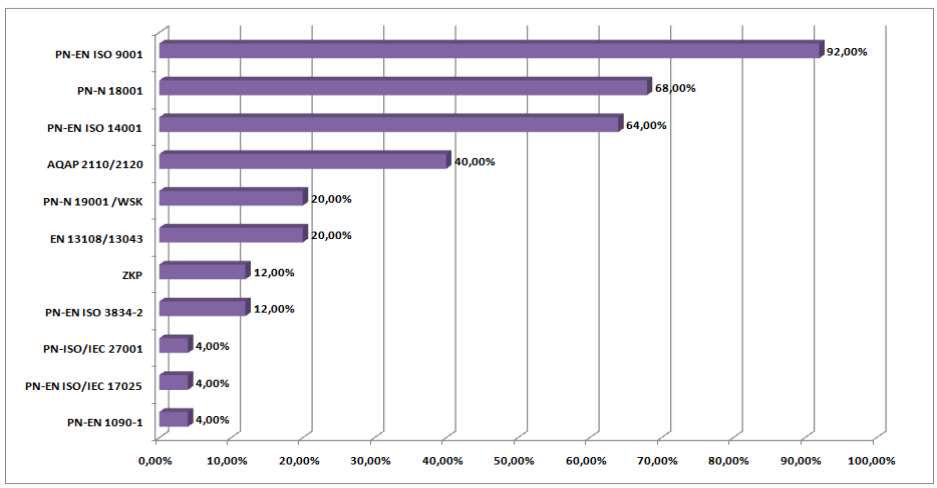
Prowadząc badania wśród przedsiębiorstw z grupy budownictwa inżynieryjnego, można zauważyć, że tylko nieznaczna część tych organizacji posiada wdrożony normatywny System Zarządzania Bezpieczeństwem Informacji, zgodny z normą PN-ISO/IEC 27001. Zgodnie z normą, system ten odnosi się do Techniki Informatycznej, Technik Bezpieczeństwa, Systemu Zarządzania Bezpieczeństwem Informacji i Wymagań, związanych z tym aspektem. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) było dla przedsiębiorstw budownictwa inżynieryjnego decyzją strategiczną, płynącą z polityki bezpieczeństwa i ochrony danych. System SZBI stanowi część zintegrowanego systemu zarządzania. Oparty jest na podejściu wynikającym z ryzyka biznesowego i odnosi się głównie do eliminacji incydentów i niespodziewanych zdarzeń, związanych z bezpieczeństwem informacji. Na projektowanie i wdrażanie SZBI w powyższych organizacjach mają wpływ zarówno potrzeby i cele biznesowe, ale również wymagania bezpieczeństwa, realizowane procesy oraz wielkości i struktura przedsiębiorstw budownictwa inżynieryjnego. Aby system SZBI mógł efektywnie funkcjonować, należy stosować podejście procesowe w celu ustanawiania, wdrożenia, eksploatacji, monitorowania, przeglądu i utrzymania, doskonalenia systemów zarządzania oraz bezpieczeństwa informacji. Termin bezpieczeństwo informacji, zgodnie z normą PN-ISO/IEC 27001 oznacza zachowanie poufności, integralności i dostępu informacji. Dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozłączalność, niezaprzeczalność oraz niezawodność informacji[3].

W wyniku przeprowadzonych badań pilotażowych, wśród 25 największych przedsiębiorstw w Polsce, należących do sektora budownictwa inżynieryjnego, autor stwierdza, że tylko nieznaczna część z nich posiada wdrożony System Zarządzania Bezpieczeństwem Informacji, zgodny z normą PN-ISO/IEC 27001, co obrazuje wykres 1.

W przedsiębiorstwach budownictwa inżynieryjnego, które zdecydowały się wdrożyć System Zarządzania Bezpieczeństwem Informacji, została wprowadzona polityka bezpieczeństwa informacji, której celem jest zapewnienie faktu, że kierownictwo wspiera i kieruje bezpieczeństwem informacji zgodnie z wymaganiami biznesowymi i właściwymi przepisami prawa oraz regulacjami wewnętrznymi. Wprowadzona została wewnętrzna organizacja bezpieczeństwa,

[3] M. Klimek, H. Wyrębek, *Bezpieczeństwo i źródła sukcesu w przedsiębiorstwach budownictwa inżynieryjnego,* [w:] *Efektywność organizacji,* red. M. Cisek, A. Marciniuk-Kluska, Wydawnictwo Studio EMKA, Warszawa 2013, s. 329-330.

służąca wewnętrznemu zarządzaniu bezpieczeństwem informacji. Zasadniczy udział w organizacji wewnętrznej posiada zaangażowane kierownictwo, które aktywnie wspiera bezpieczeństwo informacji w całej organizacji, poprzez wskazanie wyraźnego kierunku działania, demonstrowanie własnego zaangażowania, jednoznaczne przypisanie i przyjmowanie odpowiedzialności w zakresie bezpieczeństwa informacji i oceny występującego ryzyka. Koordynacja bezpieczeństwa informacji oraz działania w tym zakresie koordynowane są przez reprezentantów różnych części organizacji, pracowników pełniących odpowiednie role i funkcje[4].



Wykres 1. Systemy zarządzania stosowane w badanych przedsiębiorstwach budownictwa inżynieryjnego w 2013 roku
Źródło: Opracowanie własne na podstawie danych z przedsiębiorstw budownictwa inżynieryjnego 2013.

Przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji zostało wyraźnie zdefiniowane i przydzielone pracownikom. W badanych przedsiębiorstwach budownictwa inżynieryjnego, posiadających wdrożony SZBI, zostały określone wymagania, dotyczące umów o zachowaniu poufności i nieujawnianiu informacji. Potrzeby w zakresie ochrony informacji są regularnie przeglądane i uaktualniane, a podtrzymywane kontakty z właściwymi organami władzy oraz grupami zaangażowanym w zapewnieniu bezpieczeństwa występują w sposób naturalny. System Zarządzania Bezpieczeństwem Informacji wprowadza określanie ryzyka związanego ze stronami zewnętrznymi, czyli formy określania ryzyka informacji należących do organizacji, jak również środków przetwarzania tych informacji, związanych ze stronami zewnętrznymi, które należy zidentyfikować przed przyznaniem dostępu tym stronom[5].

Bezpieczeństwo w kontaktach z klientem polega na tym, że wymagania bezpieczeństwa powinny być określone i wprowadzone przed przyznaniem klientom dostępu do informacji lub aktywów należących do organizacji. Bezpieczeństwo w umowach zawieranych ze stroną trzecią, które dotyczy dostępu, przetwa-

[4] Tamże, s. 329-331.
[5] Tamże, s. 330-331.

rzania, przekazywania lub zarządzania informacjami przedsiębiorstwa oraz środkami przetwarzania informacji lub dodawania produktów i usług do środków przetwarzania informacji, obejmuje wszystkie stosowane wymagania bezpieczeństwa w badanych przedsiębiorstwach budownictwa inżynieryjnego.

System Zarządzania Bezpieczeństwem Informacji wprowadza odpowiedzialność za osiągnięcie i utrzymywanie odpowiedniego poziomu ochrony aktyw, ich inwentaryzację, badania własności, czyli określenie właściciela aktyw, oraz akceptowanie ich użycia w celu dopuszczenia do korzystania z informacji o aktywach. Klasyfikacja informacji, czyli zapewnienie, że informacje uzyskują ochronę na odpowiednim poziomie, zawiera zalecenia do klasyfikacji pod względem wartości informacji i wymagań prawnych oraz wrażliwości informacji i danych. Odpowiedni zbiór procedur do oznaczenia informacji i postępowania z nimi, został opracowany i wdrożony według schematów klasyfikacji informacji, przyjętych w przedsiębiorstwach[6].

Bezpieczeństwo zasobów ludzkich zapewnia, że pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecią, rozumieją swoje obowiązki, są w odpowiedni sposób przydzieleni do swoich ról. Taki przydział redukuje ryzyko kradzieży, naruszenia i niewłaściwego korzystania z narzędzi, urządzeń do przetwarzania informacji. Role i zakresy odpowiedzialności pracowników zostały udokumentowane zgodnie z polityką bezpieczeństwa informacji w organizacji. Podczas zatrudnienia pracowników, aż do ich odejścia z przedsiębiorstwa, kierownictwo ponosi odpowiedzialność, za uświadamianie, kształtowanie i szkolenia z zakresu bezpieczeństwa informacji, jak również czuwa nad ewentualnym odebraniem praw dostępu lub zwrotu aktywów[7].

Bezpieczeństwo fizyczne i środowiskowe zapewnia ochronę przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w siedzibie organizacji oraz w odniesieniu do informacji. Następuje określenie granic obszaru bezpieczeństwa, oraz barier w celu ochrony obszarów zawierających dane i środki przetwarzania informacji. System Zarządzania Bezpieczeństwem Informacji czuwa nad bezpieczeństwem sprzętu, zapobiega jego utracie, kradzieży lub naruszeniu aktywów oraz przerwaniu ciągłości działalności organizacji. Zarządzanie systemami informatycznymi i sieciami transmisji danych zapewnia prawidłową i bezpieczną eksploatację urządzeń i środków przetwarzających informację. Zarządzanie usługami informatycznymi przedsiębiorstwa budownictwa inżynieryjnego zawiera planowanie i odbiór systemów podczas awarii, tworzenie kopii zapasowych posiadanych danych, ochronę przed złośliwym kodem i oprogramowaniem, bezpieczną wymianę informacji i usług elektronicznych, monitorowanie nieautoryzowanych działań, związanych z przetwarzaniem informacji. Kontrola dostępu użytkowników i pracowników, zawarta została w polityce kontroli dostępu. Zarządzanie dostępem poprzez rejestrację użytkowników i pracowników, zapobiega nieautoryzowanemu dostępowi nieuprawnionym osobom[8].

[6] PN-ISO/IEC 27001*, Technika Informatyczna, Techniki Bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania,* styczeń 2007, s. 20-23.
[7] Tamże, s. 21-23.
[8] M. Klimek, H. Wyrębek, *Bezpieczeństwo i źródła sukcesu w przedsiębiorstwach budownictwa inżynieryjnego,* [w:] *Efektywność organizacji,* red. M. Cisek, A. Marciniuk-Kluska, Wydawnictwo Studio EMKA, Warszawa 2013, s. 330-331.

Bezpieczeństwo usług i bezpieczeństwo podejmowanych decyzji i wpływ na efektywność przedsiębiorstwa, w tym budownictwa inżynieryjnego

Powiązanie z ochroną informacji oraz bezpieczeństwem teleinformatycznym występuje również w bezpieczeństwie usług i podejmowanych przez kierownictwo strategicznych decyzjach.

Bezpieczeństwo usług, rozumiane jako niczym niezakłócone funkcjonowanie systemów podczas realizacji wyznaczonych dla nich zadań, wykonywane jest dla dobra organizacji. Bezpieczeństwo usług dotyczy również usług elektronicznych świadczonych w instytucjach za pomocą systemów informatycznych, stąd też często bezpieczeństwo usług odnosi się do bezpieczeństwa teleinformatycznego, związanego ze stosowaniem środków łączności. Termin bezpieczeństwo teleinformatyczne (ang. Information and Communication Technology Security) rozumiane jest jako zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności, czyli atrybutów bezpieczeństwa w systemach teleinformatycznych[9].

Bezpieczeństwo podejmowanych decyzji odnosi się przede wszystkim do skutecznego zarządzania, zdefiniowanego między innymi jako decydowanie na podstawie informacji. Skuteczność takiego zarządzania, czyli osiąganie zaplanowanego, a nie przypadkowego rezultatu, wynika z podjętych przez kierownictwo decyzji. Bezpieczeństwo decyzji ma na celu uświadamianie menedżerom problemów osobistej odpowiedzialności, wynikającej z prowadzenia przedsiębiorstwa. Decydowanie, to między innymi odpowiedzialność za skutki podejmowanych decyzji. Kierownictwo oraz zarząd ponosi odpowiedzialność prawną za podejmowane decyzje. W spółkach kapitałowych, odpowiedzialność menedżerska i zarządu obejmuje odpowiedzialność cywilnoprawną, podatkową oraz karną[10].

W wielu przypadkach, z zasady często menedżerowie nie zdają sobie sprawy z odpowiedzialności, jaka na nich ciąży. Uznają, że ponoszenie ryzyka nie będzie ich dotyczyło po zaprzestaniu pełnienia funkcji zarządzającej. Z przeprowadzonych badań w przedsiębiorstwach budownictwa inżynieryjnego wynika, że w większości tych organizacji bezpieczeństwo podejmowanych decyzji jest niestety zaniedbywane. Osoby zajmujące stanowiska kierownicze nie czują się odpowiedzialne za podejmowane, bardzo często nieskuteczne decyzje. Efekty takich decyzji i związane z nimi problemy przekierowywane są na pracowników niższych szczebli, którzy są niesłusznie obwiniani za powstałe sytuacje. Problemy w przedsiębiorstwach budownictwa inżynieryjnego pojawiają się również w samej komunikacji kierownictwa z personelem. W badanych instytucjach pracownicy twierdzili, że decyzje narzucane są z góry przez dyrekcję i kierownictwo, nawet jeśli są niesłuszne lub nieprzeanalizowane w sposób skuteczny, oparty na standardach zarządzania i skutecznego podejmowania decyzji. Postępowanie takie w wielu przypadkach zostało zweryfikowane przez rynek, gdyż obecnie większość przed-

[9] Białas A.*., Bezpieczeństwo informacji i usług,* Wydawnictwo Naukowo-Techniczne, Warszawa 2006, s. 27-34.
[10] Kamińska I.*, Bezpieczeństwo decyzji,* Biblioteka Szkoły Transformacji, Wrocław 2009, s. 13-18.

siębiorstw branży budowlanej, w szczególności budownictwa inżynieryjnego w kraju przeżywa kryzys[11].

Wzrost efektywności organizacji, w tym również przedsiębiorstw budownictwa inżynieryjnego, zależy w głównej mierze od zaplanowanych etapów rozwoju danego przedsiębiorstwa. Efektywnie zarządzana organizacja powinna mieć na celu przynoszenie zysku, nie tylko pokrywającego jej aktualną działalność, ale również z uwzględnieniem przyszłej modernizacji i wprowadzenia zmian, które wynikają z wpływu turbulentnego otoczenia. Istotną rolę odgrywa również zarządzanie wiedzą i posiadanymi przez firmę informacjami. Idąc za E. Skrzypek, jednym z warunków poprawy efektywności i skuteczności zarządzania organizacją w zmiennym otoczeniu jest stała poprawa jakości zasobów niematerialnych, w tym wiedzy, kapitału intelektualnego i informacji. Jakość zarządzania przekłada się na jakość efektów ludzkiej pracy. Jakość zarządzania zdeterminowana jest przez metody, narzędzia i techniki zarządzania, a te zależą w dużej mierze od jakości wiedzy i umiejętności ludzkich[12].

Problematyka zarządzania i opracowanie systemu zarządzania wiedzą w przedsiębiorstwach daje szanse na wzrost efektywności i wartości organizacji. Wskazanie tendencji światowych w pomiarze efektywności, przedstawiono poprzez system LEAD jako czynnik sukcesu organizacji. Istotną rolę odgrywają zasoby niematerialne w firmie, nakierowanej na innowacje[13].

Jednym z rozwiązań jest wprowadzanie w przedsiębiorstwach, w tym z sektora budownictwa inżynieryjnego, rozwiązań, do których należy integracja systemów zarządzania, stanowiąca istotny element budowania przewagi konkurencyjnej tych organizacji. Planowanie sukcesu przedsiębiorstwa w przyszłości, powinno opierać się o sprawdzone techniki i mechanizmy zarządzania.

Na wzrost efektywności przedsiębiorstw istotny wpływ wywiera również podejście procesowe w zarządzaniu. Buduje ono trwałą jakość świadczonych usług i daje podłoże dla innowacyjności.

Podsumowanie

Podsumowując pracę można byłoby postawić hipotezę, czy System Zarządzania Bezpieczeństwem Informacji (SZBI) daje możliwość utrzymania bezpieczeństwa systemów informatycznych i informacyjnych w przedsiębiorstwach budownictwa inżynieryjnego oraz czy jest w stanie zapewnić ciągłość działania, i zgodność z przepisami prawa, oraz stosowaną polityką bezpieczeństwa? Odpowiedź wymaga jednak bardziej szerszego spojrzenia i przeprowadzenia szczegółowych badań z funkcjonowania SZBI wdrożonego w przedsiębiorstwach grupy budownictwa inżynieryjnego. Zapoczątkowany w 2010 roku kryzys rynku budownictwa, który trwa do dziś, nie jest spowodowany nieprawidłowym funkcjonowaniem wdrożonych, normatywnych systemów, lecz związany jest z proce-

[11] M. Klimek, H. Wyrębek, *Bezpieczeństwo i źródła sukcesu w przedsiębiorstwach budownictwa inżynieryjnego,* [w:] *Efektywność organizacji,* red. M. Cisek, A. Marciniuk-Kluska, Wydawnictwo Studio EMKA, Warszawa 2013, s. 332-333.

[12] Skrzypek E. (red)., *Jakość zasobów niematerialnych a doskonalenie organizacji w warunkach turbulentnego otoczenia,* Katedra Zarządzania Jakością i Wiedzą, Wydział Ekonomiczny Uniwersytetu Marii Curie-Skłodowskiej w Lublinie, Lublin 2011, s. 7.

[13] Tamże, s. 7.

sem podejmowania decyzji, oceną ryzyka z tym związanego oraz bezpieczeństwem decyzji i usług, na które przedsiębiorstwa z badanego sektora nie brały stanowczo pod uwagę.

Podsumowując artykuł można stwierdzić, że System Zarządzania Bezpieczeństwem Informacji należy do źródeł sukcesu organizacji, w których został wdrożony. Zwiększa przez to szansę pozyskiwania lepszej pozycji tych przedsiębiorstw na rynkach krajowym i europejskim, dzięki racjonalnemu zarządzaniu procedurami bezpieczeństwa informacji, podejmowanych decyzji i świadczonych usług.

Skuteczność podejmowanych decyzji zależy w szczególności od trafnej oceny ryzyka poprzez stosowanie, w niektórych trudnych przypadkach powtórnej analizy ryzyka, co wiąże się jednak ze skuteczną umiejętnością zarządzania czasem. Jak widać w przedsiębiorstwach, w tym sektora budownictwa inżynieryjnego, kierownictwo nie radzi sobie z tym aspektem, co ma bezpośredni wpływ na podejmowane przez nie decyzje.

Bibliografia

Białas A.*, Bezpieczeństwo informacji i usług,* Wydawnictwo Naukowo-Techniczne, Warszawa 2006.

Kamińska I.*, Bezpieczeństwo decyzji,* Biblioteka Szkoły Transformacji, Wrocław 2009.

Klimek M., Wyrębek H., *Bezpieczeństwo i źródła sukcesu w przedsiębiorstwach budownictwa inżynieryjnego,* [w:] *Efektywność organizacji,* red. M. Cisek, A. Marciniuk-Kluska, Wydawnictwo Studio EMKA, Warszawa 2013.

Lipiński Z., *Bezpieczeństwo teleinformatyczne - Wstęp. Wykład 1'* Instytut Matematyki i Informatyki Uniwersytetu Opolskiego, Opole 2013.

PN-ISO/IEC 27001*,Technika Informatyczna, Techniki Bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania,* styczeń 2007.

Skrzypek E. (red.)*, Jakość zasobów niematerialnych a doskonalenie organizacji w warunkach turbulentnego otoczenia,* Katedra Zarządzania Jakością i Wiedzą, Wydział Ekonomiczny Uniwersytetu Marii Curie-Skłodowskiej w Lublinie, Lublin 2011.