ZASTOSOWANIE METODY FMEA DO OCENY POZIOMU BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE

Michał PAŁĘGA, Marcin KNAPIŃSKI, Wiesław KULMA

Streszczenie: W artykule zwrócono uwagę na podstawowe aspekty związane z problematyką zapewnienia bezpieczeństwa i ochrony najważniejszych zasobów współczesnych organizacji gospodarczych – danych i informacji. Przedstawiono w nim istotę oraz znaczenie bezpieczeństwa informacji, dokonano identyfikacji podstawowych zagrożeń, a także wskazano na ocenę ryzyka, jako podstawowy mechanizm przeciwdziałania zagrożeniom informacyjnym. Rozważania teoretyczne w tym zakresie zostały wzbogacone o studium przypadku (case study). W artykule przedstawiono przykład oceny ryzyka bezpieczeństwa informacji przy zastosowaniu metody FMEA dla konkretnego przedsiębiorstwa przemysłowego.

Słowa kluczowe: bezpieczeństwo informacji, ryzyko, ocena ryzyka, innowacyjność, metoda FMEA

1. Wstęp

Dokonująca się w ostatnich kilkunastu latach ewolucja funkcji informacji w procesie zarządzania organizacją podyktowana jest przede wszystkim niepohamowanym rozwojem techniki i technologii informatyczno- komunikacyjnej, a co się z tym wiąże również wirtualizacją działalności gospodarczej. Wzrost wartości informacji do rangi zasobu ekonomicznego oraz czynnika konkurencyjności powoduje, że jednym z podstawowych zadań, a zarazem i wyzwań dzisiejszych organizacji jest właściwe zarządzanie aktywami informacyjnymi [8]. Koniecznością zatem, staje się nie tylko ich pozyskiwanie, przetwarzanie czy transmitowanie, ale także zagwarantowanie należytego poziomu bezpieczeństwa realizowanym procesom informacyjnym. Wiąże się to przede wszystkim z określeniem procedur postępowania dotyczących magazynowania oraz wymiany informacji, kształtowaniem w świadomości personelu poczucia odpowiedzialności za ich bezpieczeństwo oraz implementacją rozwiązań mających na celu weryfikację skuteczności stosowanych zabezpieczeń [3, 8]. Niemniej jednak, kwestią nadrzędną jest identyfikacja i analiza ryzyka ziszczenia się zagrożeń bezpieczeństwa informacji. Pozwala ona zlokalizować oraz zidentyfikować słabe punkty organizacji, a także wskazać miejsca, w których informacje narażone są na największe ryzyko ich utraty, modyfikacji, zniszczenia czy też kradzieży.

Przedmiotem niniejszej publikacji jest przedstawienie przeprowadzonej analizy ryzyka przy zastosowaniu metody FMEA. Wskazana metoda stanowi powszechne narzędzie wykorzystywane w procesie kompleksowego zarządzania jakością. Jednakże, ze względu na jej dużą uniwersalność, może posłużyć również do identyfikacji i oceny wad (zagrożeń) w systemie bezpieczeństwa informacji.

2. Bezpieczeństwo informacyjne

Zgodnie z definicją zawartą w normach PN-ISO/IEC 27001: 2007 oraz PN-ISO/IEC 17799: 2007 przez bezpieczeństwo informacji rozumie się „*zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność*".

Poufność oznacza, że tylko i wyłącznie uprawione osoby mają dostęp do określonego zbioru informacji, danych bądź systemu. Zapewnienie poufności informacji zatem, polega na zagwarantowaniu dostępu tylko uprawnionym użytkownikom oraz zabronieniu dostępu osobom nieuprawnionym. Integralność danych zakłada, że dane nie zostały podmienione, zmodyfikowane lub zniekształcone bez wiedzy ich właścicieli. Idea dostępności danych z kolei, wyraża się w zapewnieniu możliwości ciągłego korzystania zarówno z systemu, jak i danych przez uprawnionych użytkowników [8,9].

Rozwój cywilizacyjny sprawia, że niestety zagrożeń informacyjnych wciąż przybywa, co narzuca konieczność opracowywania należytego systemu zabezpieczeń. Efektywna ochrona wymaga zastosowania kombinacji różnorodnych mechanizmów ochronnych, z uwzględnieniem środków technicznych, jak również i rozwiązań organizacyjnych [3]. Minimalne wymagania w tym zakresie prezentuje system zgodny z ISO 27001, który umożliwia zarządzanie bezpieczeństwem informacji w sposób kompleksowy i usystematyzowany, oparty na podejściu wynikającym z ryzyka biznesowego. Wskazana norma ISO/IEC 27001 jest rozpoznawalnym standardem w zakresie zarządzania bezpieczeństwem informacji i z powodzeniem może zostać zastosowana w każdego typu organizacji, niezależnie od wielkości przedsiębiorstwa, formy działalności bądź gałęzi gospodarki.

3. Ryzyko w systemie bezpieczeństwa informacji

Ryzyko jest pojęciem dość powszechnie stosowanym, gdyż towarzyszy niemal każdej działalności człowieka. Wynika bowiem z faktu, iż każde podejmowane przez człowieka przedsięwzięcie dotyczące przyszłości charakteryzuje niepewny rezultat. W kontekście bezpieczeństwa informacji można uznać, że ryzyko oznacza *„(...) miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażoną jako iloczyn prawdopodobieństwa wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków"* [4]. Wobec powyższego ryzyko utraty informacji należy traktować, jako wypadkową prawdopodobieństwa zaistnienia niekorzystnego zdarzenia oraz konsekwencji z tym związanych, wyrażonych pewną stratą.

Niezbędnym w zakresie identyfikacji zagrożeń występujących w przedsiębiorstwie oraz słabych jego punktów jest analiza ryzyka. Systematyczne badanie ryzyka umożliwia przegląd aktualnych zagrożeń oraz wprowadzanie modyfikacji w funkcjonującym systemie ochrony. Niestety, nie istnieje jeden idealny sposób przeprowadzania analizy ryzyka. Wybór podejścia w głównej mierze uzależniony jest od rodzaju prowadzonej działalności, przyjętej przez organizację strategii w zakresie bezpieczeństwa oraz wielu innych czynników [4, 5].

Najogólniej metody oceny ryzyka obejmują metody ilościowe, w których wyniki oszacowanego ryzyka wyrażone zostają w formie procentowej bądź pieniężnej oraz metody jakościowe, polegające na tym, iż do opisu zdarzeń i ich skutków wykorzystywane są różnego rodzaju skale [5]. Jedną z metod jakościowych jest prezentowana w niniejszej publikacji metoda FMEA.

Metoda FMEA (*ang. Failure Mode and Effects Analysis*) służy do identyfikowania wad (niezgodności, błędów) i wywołujących je przyczyn, które mogą wystąpić w procesach konstrukcyjnych i wytwórczych oraz projektowania na ich podstawie działań zapobiegawczych bądź korygujących. Pierwsze zastosowanie FMEA miało miejsce w latach sześćdziesiątych XX wieku w USA, w przemyśle kosmicznym. Wraz z upływem czasu zakres stosowania tej metody systematycznie wzrastał i obejmował kolejne branże przemysłu [7].

W opisywanej metodzie wartość ryzyka wyraża się iloczynem trzech następujących parametrów: znaczenia wady, prawdopodobieństwa jej występowania oraz wykrywalności wady. Powyższą zależność opisuje wzór [1,2,7]:

$$WPR = Z \cdot R \cdot W$$

gdzie:
WPR – wskaźnik priorytetu ryzyka
Z – znaczenie wady ze względu na skutek
R – prawdopodobieństwo wystąpienia wady lub przyczyny wady
W – możliwość wykrycia wady

Wskaźniki *Z, R, W* ocenia się w skali od 1 do 10, mając na uwadze następujące kryterium:

- Z (1 – bardzo małe, 10 – krytyczne);
- R (1 – nieprawdopodobne, 10 – bardzo często)
- W (1 – bardzo wysoka, 10 – niemożliwa)

4. Zastosowanie metody FMEA w ocenie poziomu bezpieczeństwa informacji – studium przypadku

Analiza ryzyka utraty bezpieczeństwa informacji została przeprowadzona za pomocą jakościowej metody FMEA dla konkretnego przedsiębiorstwa przemysłowego. Badana firma działa na rynku usług budowlanych. W swojej bogatej ofercie posiada również takie usługi jak: wykonywanie robót budowlanych, konstrukcji stalowych oraz urządzeń technologicznych. Jednakże, podstawową jej domeną jest budowa oczyszczalni ścieków oraz sieci kanalizacji, realizowana na zlecenie samorządów terytorialnych. Ponadto, przedsiębiorstwo korzysta z własnego zaplecza projektowego oraz laboratorium badawczego [6]. Z tego też względu, problematyka bezpieczeństwa informacji nabiera szczególnego znaczenia.

Kryteria doboru poszczególnych wskaźników ilościowych zaprezentowano w tab. 1 – 3.

Celem dokonania hierarchizacji czynników wpływających na utratę bezpieczeństwa informacji w badanej jednostce gospodarczej przeprowadzono analizę Pareto – Loreza. Pozwoliła ona na wskazanie tych czynników, które mają zasadniczy wpływ na jakość procesu zarządzania bezpieczeństwem informacji i wobec, których należy bezwzględnie zastosować środki ochronne. Zestawienie otrzymanych wyników prezentuje tab. 5.

Tabela 1. Kryteria dla wskaźnika Z

Ocena	Określenie znaczenia
1	Wada jest niezauważalna, nie wpływa na funkcjonowanie procesów biznesowych
2 – 3	Wada wywołuje nieznaczne utrudnienia w systemie bezpieczeństwa oraz nie wpływa na funkcjonowanie procesów biznesowych
4 - 5	Wada wywołuje małe utrudnienia w systemie bezpieczeństwa oraz może mieć wpływ na realizację procesów biznesowych
6 – 7	Wada wywołuje utrudnienia w systemie bezpieczeństwa oraz powoduje zakłócenia w realizacji procesów biznesowych
8 - 9	Wada wywołuje znaczące utrudnienia w systemie bezpieczeństwa informacji oraz powoduje poważne zakłócenia procesów biznesowych
10	Wada powoduje przerwanie procesów biznesowych

Źródło: opracowanie własne na podstawie [6]

Tabela 2. Kryteria dla wskaźnika R

Ocena	Wskaźnik R [%]
1	1 – 10
2	11 – 20
3	21 – 30
4	31 – 40
5	41 – 50
6	51 – 60
7	61 – 70
8	71 – 80
9	81 – 90
10	91 – 100

Źródło: opracowanie własne na podstawie [6]

Tabela 3. Kryteria dla wskaźnika W

Ocena	Wskaźnik W [%]
1	1 – 10
2	11 – 20
3	21 – 30
4	31 – 40
5	41 – 50
6	51 – 60
7	61 – 70
8	71 – 80
9	81 – 90
10	91 – 100

Źródło: opracowanie własne na podstawie [6]

Wyniki z przeprowadzonej analizy ryzyka zawarto w tab. 4.

Tabela 4. Arkusz FMEA analizy ryzyka bezpieczeństwa informacji

Nr wady	Potencjalna wada	Potencjalne skutki wady	Potencjalne przyczyny wady	Z	R	W	WPR	Nowe działania zapobiegawcze	Z	R	W	WPR
1.	Nieświadomość pracownika	- Nieznajomość zagrożeń; - Nieświadomość wartości informacji; - Ujawnianie firmowych danych; - Niszczenie informacji.	Brak planowania szkoleń	9	8	5	360	Plan szkoleń	9	3	2	54
			Nieobecność personelu na szkoleniach	9	8	6	432	Dokumentowanie obecności na szkoleniach	9	4	2	72
			Niewłaściwie prowadzone szkolenia, niejasne i niezrozumiałe treści	8	7	5	280	Przegląd i aktualizacja programu szkoleń	8	3	2	48
2.	Niestosowanie się do obowiązujących regulaminów i procedur	- Narażenie firmowych danych na ich niekontrolowany wyciek, utratę, zniszczenie bądź zmodyfikowanie.	Nadmiernie skomplikowane przepisy -„Droga na skróty”	8	6	4	192	Przegląd i aktualizacja instrukcji postępowania w zakresie BI	8	3	2	42
			Nieznajomość i niezrozumiałość przepisów	7	7	5	245	Kontrola wiedzy w zakresie przepisów	7	4	2	56
			Nieegzekwowanie przestrzegania regulaminów	9	8	6	432	Wprowadzenie instrukcji dyscyplinowania pracowników	9	3	3	81
3.	Brak zasilania, awaria łączności	- Zakłócenie ciągłości działania; - Brak możliwości realizacji procesów; - Problemy z wymianą informacji i właściwą komunikacją; - Ogólny chaos i dezorganizacja.	Uszkodzenie sieci energetycznej na zewnątrz budynku	7	5	3	105	Przegląd i konserwacja awaryjnych źródeł zasilania (UPS-y)	7	3	1	21
			Awaria urządzeń wchodzących w skład sieci energetycznej	8	6	2	96	Dziennik przeglądu i konserwacji urządzeń sieci energetycznych	8	2	1	16
			Uszkodzenie podzespołów	7	5	4	140	Przegląd i konserwacja podzespołów systemu	7	2	1	14
4.	Awaria łączy internetowych	- Problemy operacyjne; - Problemy z właściwą wymianą informacji; - Problemy z komunikacją z klientami i dostawcami - Nadszarpnięty wizerunek firmy.	Błąd człowieka	7	4	3	84	Opracowanie instrukcji i zasad postępowania dot. korzystania z Internetu	7	2	2	28
			Uszkodzenie podzespołów serwera (np. płyty głównej)	8	7	3	168	Przegląd i konserwacja podzespołów	8	2	1	16
			Atak hackerski	8	8	4	256	Wdrożenie zabezpieczeń systemu (ogólne, firewall, skaner zmian w plikach) oraz wprowadzenie systemu uświadamiania personelu	8	3	2	48
5.	Nieprawidłowe działanie oprogramowania	- Obniżenie wartości użytkowej oprogramowania; - Błędny rezultat działania oprogramowania; - Ograniczony dostęp do danych - Problemy z poprawnym zapisywaniem informacji	Niewłaściwe i nieumiejętne korzystanie	8	7	4	224	Opracowanie instrukcji korzystania z oprogramowania	8	2	2	32
			Brak właściwego nadzoru nad oprogramowaniem	8	7	3	168	Ustanowienie stałego nadzoru nad oprogramowaniem	8	3	1	24
			Zakup wadliwego oprogramowania	7	6	5	210	Testowanie oprogramowania przed jego eksploatacją	7	2	1	14
6.	Awaria serwera	- Brak możliwości realizacji procesów; - Brak dostępu do bazy danych; - Brak możliwości przesyłania danych; - Zakłócenia w realizacji procesów; - Straty finansowe.	Awaria podzespołów serwera	8	7	4	224	Przegląd i konserwacja	8	3	1	24
			Manipulacja nieuprawnionych użytkowników przy podzespołach serwera	9	8	6	432	Zabezpieczenie dostępu do serwera przed nieuprawnionym dostępem	9	3	2	54
			Pożar w serwerowni	9	8	5	360	Przegląd systemu p.poż. w serwerowni	9	3	2	54

7.	Złamanie haseł	- Rozpowszechnienie haseł; - Nieuprawniony dostęp do kluczowych informacji (w tym prawnie chronionych); - Kradzież danych; - Restrykcje prawne i finansowe; - Utrata konkurencyjności.	Nieprzestrzeganie zasad czystego biurka i pulpitu	8	8	5	320	Rozpowszechnienie zasad czystego biurka i pulpitu	8	3	2	48
			Niewłaściwe generowanie haseł	9	9	5	405	Wdrożenie oprogramowania ograniczającego stosowanie pospolitych haseł	9	3	2	54
			Atak socjotechniczny – phishing	9	9	6	486	Przestrzeganie pracowników przed phishingiem za pomocą okien pop-up	9	4	3	108
8.	Włamanie do systemu komputerowego	- Nieuprawniony dostęp do danych; - Kradzież danych; - Modyfikacja bądź zniszczenie danych; - Wyciek kluczowych informacji do konkurencji; - Brak zaufania klientów; - Straty finansowe.	Luki w systemach operacyjnych	9	7	4	252	Raportowanie zmian i nieprawidłowości działania systemu	9	4	1	36
			Nieprawidłowo zainstalowane oprogramowanie antywirusowe	8	6	4	192	Instrukcje dot. instalowania oprogramowania antywirusowego	8	3	2	48
			Złośliwe oprogramowanie	9	8	5	360	Zastosowanie skanerów wykrywających i usuwających złośliwe oprogramowanie	9	3	2	54
9.	Kradzież danych	- Utrata tajemnicy przedsiębiorstwa; - Przedostanie się unikatowych cech produktu bądź usługi do konkurencji; - Utrata pozycji na rynku; - Utrata klientów; - Straty finansowe.	Zbyt łatwy dostęp do pomieszczeń	9	8	5	360	Wprowadzenie systemu weryfikacji tożsamości i uwierzytelniania pracowników	9	4	2	72
			Nieuwaga i nieostrożność pracowników pionu ochrony	8	7	4	224	Wprowadzenie specjalnych identyfikatorów i przepustek dla gości	8	3	2	48
			Nieświadome udostępnianie informacji i dokumentów	8	7	5	280	Plan szkoleń dla pracowników	8	3	3	72
			Pozostawianie osób postronnych bez nadzoru i opieki	8	7	3	168	Zasady przyjmowania i eskortowania gości	8	2	1	16
10.	Brak odpowiednich przepisów i regulaminów	- Niewłaściwe postępowanie pracowników; - Uchybienia proceduralne; - Dezorganizacja.	Brak świadomości kierownictwa	8	6	4	192	Szkolenia dla kierownictwa w zakresie wymagań prawnych i normy ISO 27001	8	3	3	72
11.	Brak polityki bezpieczeństwa informacji	- Wyciek informacji; - Kradzież informacji i dóbr materialnych; - Koszty finansowe; - Utrata wiarygodności w oczach klientów; - Utrata pozycji na rynku.	Brak świadomości potrzeby opracowania polityki BI	8	8	5	320	Planowanie szkoleń w zakresie podstawowych dokumentów BI	8	4	2	64
12.	Brak monitorowania poziomu bezpieczeństwa informacji w organizacji	- Brak identyfikacji zagrożeń; - Ograniczenie możliwości przeciwdziałania niebezpieczeństwom; -Narażanie zasobów na ich utratę, uszkodzenie, itp.; - Brak reakcji na incydenty naruszania BI.	Brak świadomości w zakresie potrzeby monitorowania poziomu BI oraz jego nieumiejętność	7	8	4	224	Opracowanie wytycznych w zakresie monitorowania i analizowania poziomu BI	7	3	2	42

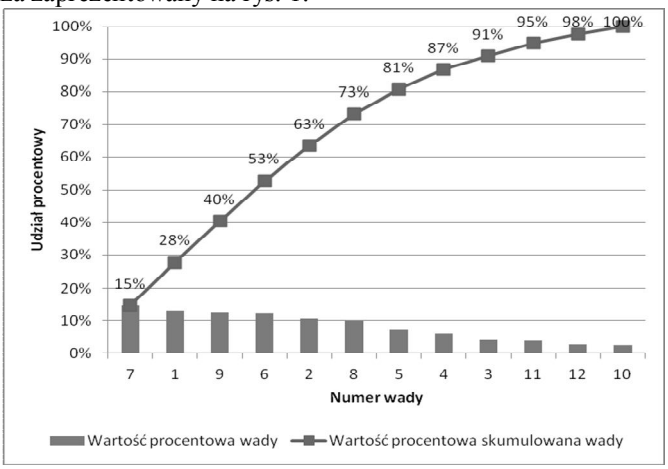
Źródło: opracowanie własne na podstawie [6]

Tabela 5. Analiza Pareto – Lorenza systemu bezpieczeństwa informacji

Numer wady	Nazwa wady	Wartość wskaźnika WPR	Wartość procentowa wskaźnika WPR	Wartość skumulowana
7	Złamanie hasła	1211	15%	15%
1	Nieświadomość pracownika	1072	13%	28%
9	Kradzież danych	1032	13%	40%
6	Awaria serwera	1016	12%	53%
2	Niestosowanie się do obowiązujących regulaminów i procedur	869	11%	63%
8	Włamanie do systemu komputerowego	804	10%	73%
5	Nieprawidłowe działanie oprogramowanie	602	7%	81%
4	Awaria łączy internetowych	508	6%	87%
3	Brak zasilania, awaria łączności	341	4%	91%
11	Brak polityki bezpieczeństwa informacji	320	4%	95%
12	Brak monitorowania poziomu bezpieczeństwa informacji	224	3%	98%
10	Brak odpowiednich przepisów i regulaminów	192	2%	100%
Suma		**8191**	**100%**	

Źródło: opracowanie własne

Na podstawie odpowiednio zhierarchizowanych wad (tab.5) sporządzono diagram Pareto – Lorenza zaprezentowany na rys. 1.



Rys. 1. Diagram Pareto – Lorenza dla niezgodności występujących w procesie zarządzania bezpieczeństwem informacji. Źródło: opracowanie własne

Analiza danych zawartych na rys. 1 wskazuje, że 81% zagrożeń związanych z bezpieczeństwem informacji generowanych jest przez 7 następujących zjawisk, do których należą:

- Złamanie hasła.
- Nieświadomość pracownika.
- Kradzież danych.
- Awaria serwera.
- Niestosowanie się do obowiązujących regulaminów i procedur.
- Włamanie do systemu komputerowego.
- Nieprawidłowe działanie oprogramowania.

Wyżej wymienione niebezpieczeństwa wymagają priorytetowego zastosowania działań korygujących oraz prewencyjnych.

5. Podsumowanie

Zmiany zachodzące w otoczeniu zmuszają kierowników jednostek organizacyjnych do systematycznej weryfikacji istniejących zagrożeń (również w sferze informacyjnej) oraz obszarów wymagających zabezpieczeń. Niezbędnym w tym zakresie jest badanie ryzyka, które pozwala wskazać wszystkie newralgiczne miejsca w systemie bezpieczeństwa informacji oraz wspomaga podejmowanie decyzji w zakresie przedsięwzięć, mających na celu przeciwdziałanie zaistnieniu niepożądanych dla organizacji zjawisk.

Przeprowadzone badania w zakresie oceny poziomu bezpieczeństwa informacji za pomocą metody FMEA oraz analizy Pareto – Lorenza wskazały na kilkanaście znaczących niebezpieczeństw. Zaproponowane działania zapobiegawcze pozwoliły na zredukowanie poziomu ryzyk oraz biorąc pod uwagę przyjęte kryteria ustanowione w polityce bezpieczeństwa na ich zaakceptowanie przez kierownictwo jednostki gospodarczej. Dla zobrazowania zaistniałej sytuacji przedstawiono wartości współczynnika WPR przed i po wprowadzeniu zmian, które zostały zastawione w tab. 6.

Tabela 6. Wartości wskaźnika WPR

Numer wady	**Nazwa wady**	**Wartość wskaźnika WPR przed zmianami**	**Wartość wskaźnika WPR po zmianach**	**Współczynnik redukcji wyrażony procentowo**
7	Złamanie hasła	1211	210	577%
1	Nieświadomość pracownika	1072	172	**623%**
9	Kradzież danych	1032	208	496%
6	Awaria serwera	1016	132	**770%**
2	Niestosowanie się do obowiązujących regulaminów i procedur	869	179	485%
8	Włamanie do systemu komputerowego	804	138	583%
5	Nieprawidłowe działanie oprogramowanie	602	70	**860%**
4	Awaria łączy internetowych	508	92	552%

3	Brak zasilania, awaria łączności	341	51	**669%**
11	Brak polityki bezpieczeństwa informacji	320	64	500%
12	Brak monitorowania poziomu bezpieczeństwa informacji	224	42	533%
10	Brak odpowiednich przepisów i regulaminów	192	72	267%

Źródło: opracowanie własne

Dane zamieszczone w tabeli 6 wskazują, że największy współczynnik redukcji poziomu ryzyka odnotowano dla czterech zagrożeń: nieprawidłowe działanie oprogramowania, awaria serwera, brak zasilania, awaria łączności oraz nieświadomość pracownika. Skuteczność wdrożonych zabezpieczeń wynika przede wszystkim z uprzednio rzetelnie przeprowadzonej analizy zagrożeń oraz zastosowania kombinacji rozwiązań technicznych i organizacyjnych. Tylko takie podejście organizacji do problematyki bezpieczeństwa informacji gwarantuje oczekiwany rezultat.

Literatura

1. Gołębiowski M., Janasz W., Prozorowicz M., „Zarządzanie jakością w przedsiębiorstwie", Wyd. Uniwersytetu Szczecińskiego, Szczecin 1999.
2. Hamrol A., „Zarządzanie jakością z przykładami", Wyd. PWN, Warszawa 2005.
3. Janczak J, Nowak A., „Bezpieczeństwo informacyjne. Wybrane problemy", Wyd. AON, Warszawa 2013.
4. Liderman K., „Bezpieczeństwo teleinformatyczne", Wyd. WSISiZ, Warszawa 2002.
5. Łuczak J., Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001, Zeszyty Naukowe, Wyd. Akademia Morska w Szczecinie, Nr 19(91) 2009.
6. Materiał źródłowy przedsiębiorstwa
7. „Podstawy kompleksowego zarządzania jakością TQM", red. Łańcucki J., Wyd. Akademii Ekonomicznej w Poznaniu, Poznań 2001.
8. „Podstawy zarządzania informacją", red. Czekaj R., Wyd. Uniwersytetu Ekonomicznego w Krakowie, Kraków 2012.
9. Wrzosek M., Nowak A., „Identyfikacja zagrożeń determinujących zmiany w systemie bezpieczeństwa społeczeństwa informacyjnego", Wyd. AON, Warszawa 2009.

Mgr inż. Michał PAŁĘGA
Dr hab. inż. Marcin KNAPIŃSKI, prof. PCz.
Dr Wiesław KULMA
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Politechnika Częstochowska
42 – 201 Częstochowa, Dąbrowskiego 69
tel./fax: (0-34) 325 07 90
e-mail: mpalega@wip.pcz.pl
knap@wip.pcz.pl
wkulma@wip.pcz.pl