OCENA RYZYKA BEZPIECZEŃSTWA INFORMACJI W RELACJACH Z DOSTAWCAMI
RISK EVALUATION OF INFORMATION SECURITY IN RELATIONS WITH SUPPLIERS

Barbara GRUSZKA
bpajak@wip.pcz.pl

Politechnika Częstochowska
Wydział Zarządzania
Instytut Inżynierii Produkcji

Monika GÓRSKA
monika.gorska77@wp.pl

Politechnika Częstochowska
Wydział Inżynierii Produkcji i Technologii Materiałów
Katedra Zarządzania Produkcją i Logistyki

Streszczenie: W artykule przeprowadzona została ocena ryzyk bezpieczeństwa informacji w relacjach z dostawcami wśród przedsiębiorstw zajmujących się produkcją konstrukcji stalowych. Analizie została poddana zarówno dokumentacja, dotycząca bezpośrednio dostawy jak również wszystkie aktywa informacyjne, z którymi dostawcy mogą mieć kontakt podczas współpracy. Przeprowadzona ocena ryzyka umożliwiła ujawnienie tych zagrożeń, które mogą wystąpić podczas współpracy z partnerami logistycznymi.

Abstract: In this paper. risks evaluation of information security in relations with suppliers among companies involved in the production of steel structures was carried out. Documents concerning direct delivery and information assets with which suppliers may come into contact during cooperation have been subjected to analysis. The risk assessment allowed the disclosure of the risks that can occur during working with logistics partners.

Słowa kluczowe: bezpieczeństwo informacji, ryzyko, relacje, dostawcy
Key words: information security, risk, relations, suppliers

WSTĘP

Rola informacji w różnego typu przedsiębiorstwach nie od dziś jest przedmiotem dociekań badaczy nauk ekonomicznych i nauk o zarządzaniu (Materska, 2003). W gospodarce opartej na wiedzy, to właśnie informacja jest zasobem, który zyskuje coraz większe znaczenie (Liderman, 2009). Odpowiednio wykorzystana we właściwym miejscu i czasie istotnie wpływa na proces tworzenia przewagi konkurencyjnej przedsiębiorstw na rynku kapitałowym. Również w przypadku współpracy logistycznej, oprócz wywiązania się z wcześniej określonych warunków umowy, bardzo ważny jest przepływ informacji (Bielecki

i Szymonik, 2014). Informacyjne relacje pomiędzy klientami a ich dostawcami mają za zadanie przede wszystkim przynosić korzyści dla obu stron. Podczas współpracy klient uzyskuje dostęp do informacji, które świadczą między innymi o jakości towaru i usług z nim związanych, o jego cechach charakterystycznych oraz tych odróżniających go od oferty konkurencji. W proces wymiany informacji zaangażowane są w równym stopniu obie strony – dostawca i odbiorca.

.

1. BEZPIECZEŃSTWO INFORMACJI JAKO ELEMENT KSZTAŁTOWANIA RELACJI POMIĘDZY DOSTAWCĄ A ODBIORCĄ

Wzrost znaczenia informacji w przedsiębiorstwie sprawia, że jednym z podstawowych wyzwań dzisiejszych firm jest odpowiednie zarządzanie aktywami informacyjnymi (Czekaj, 2012). Zasób, który może stać się źródłem przewagi konkurencyjnej dla organizacji musi być poddany ochronie. Dotyczy to zarówno ochrony przed zagrożeniami zewnętrznymi, jak i wewnętrznymi, pasywnymi i aktywnymi (Żebrowski, 2004). Można zatem stwierdzić, że niezbędnym elementem zarządzania zasobami informacyjnymi jest wymóg ochrony własności intelektualnych, które tworzą aktywa niematerialne takie jak patenty, wzory, licencje itp. (Romanowska, 2001). Pojęcie bezpieczeństwa informacji jest złożonym i wielowymiarowym zagadnieniem będącym przedmiotem zainteresowania wielu badaczy. W opinii K. Liderman termin bezpieczeństwo informacyjne określa jako uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej i wykorzystywanej informacji (Liderman, 2012). Oznacza to, że pojęcie te dotyczy człowieka, lub ogólnie organizacji, która może być zagrożona utratą zasobów informacyjnych albo otrzymaniem informacji o nieodpowiedniej jakości. Warto również zaznaczyć, że pojęcie bezpieczeństwa informacji zostało szczegółowo wyjaśnione w międzynarodowej normie standaryzującej system zarządzania bezpieczeństwem informacji ISO 27001:2007, która określa wymagania związane z ustanowieniem, wdrażaniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem oraz doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji - PN-ISO/IEC 27001:2007.

Bezpieczeństwo informacji ma na celu ochronę wartościowych informacji przed nieautoryzowanym dostępem lub zmianą. Systemowe podejście odnosi się do zabezpieczenia informacji w zakresie:

- Poufności - zapewnienia, że informacja jest dostępna jedynie osobom upoważnionym;
- Integralności - zapewnienia dokładności i kompletności informacji oraz metod jej przetwarzania;

- Dostępności - zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów zawsze wtedy, gdy jest to potrzebne.

Norma ISO 27001:2007 zakłada, że w każdym systemie zarządzania bezpieczeństwem informacji należy przeprowadzić szacowanie ryzyka w odniesieniu do najważniejszych aktywów informacyjnych znajdujących się w posiadaniu przedsiębiorstwa. Na tej podstawie określa się postępowanie z ryzykiem oraz wybiera odpowiednie zabezpieczenia.

2. OKREŚLANIE RYZYKA BEZPIECZEŃSTWA INFORMACJI W RELACJACH Z DOSTAWCAMI DLA WYBRANEJ GRUPY PRZEDSIĘBIORSTW SEKTORA METALOWEGO.

Sektor metalowy na świecie dostarcza komponentów oraz wyrobów gotowych praktycznie dla wszystkich pozostałych sektorów produkcji, w tym przede wszystkim dla przemysłu motoryzacyjnego, lotniczego, transportowego i maszynowego (Górska i Pająk, 2015). Badaniami objęto 10 przedsiębiorstw metalowych zajmujących się produkcją metalowych elementów konstrukcyjnych.

Celem przygotowanych i przeprowadzonych badań empirycznych była ocena ryzyka bezpieczeństwa informacji w relacjach z dostawami, która umożliwiła poznanie realnych zagrożeń pojawiających się podczas współpracy. Na podstawie uzyskanych wyników ze wszystkich przedsiębiorstw stworzone zostały wartości średnie przedstawiające skale zjawiska w konkretnej branży. Pierwszym etapem oceny ryzyka jest klasyfikacja aktywów informacyjnych, podczas której konieczne jest zidentyfikowanie przetwarzanych w przedsiębiorstwach informacji, powiązanie ich w logiczny sposób w grupy oraz określenie wrażliwości grup poprzez przydzielenie im stosownych wartości współczynników poufności, integralności i dostępności (Białas, 2006). Wrażliwość grupy określono korzystając ze wzoru

$$WG = 2 \times P + I + D \quad (1)$$

gdzie:

WG = wrażliwość grupy informacji,
P = współczynnik poufności danej grupy informacji,
I = współczynnik integralności danej grupy informacji,
D = współczynnik dostępności danej grupy informacji.

Wartości poszczególnych współczynników ustala się na podstawie skal stosowanych podczas analizy ryzyka bezpieczeństwa przedstawionych w tabeli 1, 2, 3.

Tabela 1. Skala poziomu poufności

Skala	Poziom poufności (P)
0	Informacje ogólnodostępne wewnątrz i na zewnątrz przedsiębiorstwa.
1	Informacje ogólnodostępne wewnątrz przedsiębiorstwa oraz stron zewnętrznych związanych umowami lub nadrzędnymi przepisami prawa.
2	Informacje dostępne dla wybranych komórek/uprawnionych pracowników w przedsiębiorstwie oraz stron zewnętrznych związanych umowami lub nadrzędnymi przepisami prawa.
3	Informacje dostępne dla: 1) wybranych komórek organizacyjnych/pracowników przedsiębiorstwa uprawnionych do przetwarzania informacji prawnie chronionych. 2) pracowników stron zewnętrznych uprawnionych do przetwarzania informacji prawnie chronionych, związanych umowami lub nadrzędnymi przepisami prawa.

Źródło: opracowanie własne na podstawie

Tabela 2. Skala poziomu integralności

Skala	Poziom Integralności (I)
1	Nieautoryzowana zmiana informacji na nie wpływu na realizację zadań/procesów.
2	Nieautoryzowana zmiana informacji ma wpływ na realizację zadań/procesów.

Źródło: opracowanie własne na podstawie

Tabela 3. Skala poziomu integralności

Skala	Poziom dostępności (D)
1	Informacje mogą być niedostępne powyżej dwóch dni roboczych, maksymalnie, o ile to możliwe , do 14 dni roboczych.
2	Informacje mogą być niedostępne maksymalnie do dwóch dni roboczych.
3	Informacje mogą być niedostępne maksymalnie do 8 godzin w czasie dnia roboczego.

Źródło: opracowanie własne na podstawie

Kolejnym etapem badawczym była analiza ryzyka bezpieczeństwa informacji, którą przeprowadza się w kontekście możliwych zagrożeń i podatności dotyczących konkretnego aktywa. Wartość ryzyka (R) wylicza się w oparciu o wzór:

$$R = WA \times ŁW \times Pr \times S \quad (2)$$

gdzie:

R - wartość ryzyka bezpieczeństwa informacji,
WA - wartość aktywa,
ŁW - łatwość wykorzystania podatności przez zagrożenie,
Pr - prawdopodobieństwo wystąpienia zagrożenia,
S - straty biznesowe.

Przyjmuje się, że wartość konkretnego (WA) równa jest maksymalnej wartości wrażliwości grupy informacji przetwarzanej przez to aktywo, zgodnie z zależnością $WA = WG_{max}$. Prawdopodobieństwo wystąpienia zagrożenia (Pr) zostało określone zgodnie z wytycznymi przedstawionymi w tabelach 4.

Tabela 4. Skala poziomu prawdopodobieństwa wystąpienia zagrożenia

Skala	Prawdopodobieństwo wystąpienia zagrożenia (Pr)
1	Zagrożenie jest mało realne.
2	Zagrożenie jest bardzo realne i może wystąpić w każdej chwili

Źródło: opracowanie własne na podstawie

Łatwość wykorzystania podatności przez zagrożenie obliczona została w oparciu o wzór:

$$ŁW = Pd \times Z \quad (3)$$

gdzie:

Pd - znaczenie podatności w kontekście zidentyfikowanego zagrożenia,
Z - poziom zabezpieczeń.

Parametry Pd i Z określone zostały zgodnie ze skalami z tabel 5 i 6.

Tabela 5. Skala znaczenia podatności w kontekście zidentyfikowanego zagrożenia

Skala	Znaczenie podatności (Pd) w kontekście zidentyfikowanego zagrożenia
1	Niska, gdy stwierdzono niski poziom znaczenia podatności w kontekście danego zagrożenia.
2	Średnia, gdy stwierdzono średni poziom znaczenia podatności w kontekście danego zagrożenia.
3	Wysoka, gdy stwierdzono wysoki poziom znaczenia podatności w kontekście danego zagrożenia.

Źródło: opracowanie własne na podstawie

Tabela 6. Skala poziomu zabezpieczenia

Skala	Poziom zabezpieczenia (Z)
1	Zabezpieczenia są stosowane i formalizowane.
2	Zabezpieczenia są stosowane, ale są niesformalizowane.
3	Zabezpieczenia nie są stosowane, ale są sformalizowane.
4	Zabezpieczenia nie są stosowane i nie są sformalizowane.

Źródło: opracowanie własne na podstawie

Straty biznesowe zostały określone na podstawie wzoru 4 i zgodnie ze skalami z tabel 7, 8, 9.

$$S = Sf + Sp + Sw \quad (4)$$

gdzie:

S - straty biznesowe,
Sf - skutek finansowe,
Sp - skutek prawny,
Sw - skutek wizerunkowy.

Tabela 7. Skala skutku finansowego

Skala	Skutek finansowy (Sf)
1	Materializacja zagrożenia nie spowoduje strat finansowych, lub spowoduje straty finansowe: $Sf \leq 100$ tys. zł.
2	Materializacja zagrożenia spowoduje straty finansowe: $Sf > 100$ tys. zł.

Źródło: opracowanie własne na podstawie

Tabela 8. Skala skutku prawnego

Skala	Skutek prawny (Sp)
1	Materializacja zagrożenia nie prowadzi do naruszenia przepisów prawa lub regulacji wewnętrznych.
2	Materializacja zagrożenia prowadzi do naruszenia przepisów prawa lub regulacji wewnętrznych.

Źródło: opracowanie własne na podstawie

Tabela 9. Skala skutku wizerunkowego

Skala	Skutek wizerunkowy (Sw)
1	Materializacja zagrożenia nie ma negatywnego wpływu na wizerunek przedsiębiorstwa.
2	Materializacja zagrożenia ma negatywny wpływ na wizerunek przedsiębiorstwa.

Źródło: opracowanie własne na podstawie

W celu oddzielenia ryzyka akceptowalnego od ryzyka nieakceptowanego należy określić próg akceptowalności ryzyka bezpieczeństwa informacji. Do wskazania ryzyka nieakceptowanego wykorzystana została reguła Pareto, która przyjmuje, że 20% rodzajów ryzyka o największej wartości jest przyczyną 80% pojawiających się zdarzeń.

$$R_{AKC} = (R_{MAX} - R_{MIN}) \times 0,8 + R_{MIN} \quad (5)$$

gdzie:

R_{AKC} - wartość progu akceptowalności ryzyka,
R_{MAX} - ryzyko o największej wartości,
R_{MIN} - ryzyko o najmniejszej wartości.

Każde ryzyko bezpieczeństwa informacji, którego wartość przekracza próg akceptowalności, zaliczane jest do grupy ryzyka nieakceptowanego, tj. do ryzyka, które wymaga podjęcia odpowiednich działań.

3.1 OCENA RYZYKA BEZPIECZEŃSTWA INFORMACJI W RELACJACH Z DOSTAWCAMI DLA WYBRANYCH PRZEDSIĘBIORSTW SEKTORA METALOWEGO

Bezpieczeństwo informacji jest niezwykle ważnym elementem tworzenia i utrzymywania relacji logistycznych pomiędzy dostawcą a odbiorcą. Podstawowym jego celem we współpracy logistycznej jest zapewnienie ochrony aktywów organizacji udostępnianych dostawcom. Jest to możliwe dzięki zastosowaniu odpowiedniej polityki bezpieczeństwa, która polega na uzgodnieniu i udokumentowaniu z dostawcą odpowiednich wymagań zmniejszających ryzyko nieprawidłowego wykorzystania aktywów informacyjnych. Przedsiębiorstwa produkcyjne powinny określić wszystkie istotne

wymagania dotyczące bezpieczeństwa informacji, a następnie uzgodnić je z każdym dostawcą, który może zyskać dostęp, przetwarzać lub dostarczać elementy infrastruktury teleinformatycznej dla przedsiębiorstwa. Wszystkie porozumienia z dostawcami powinny również uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów. Warto również dodać, że ochrony wymagają nie tylko aktywa informacyjne związane z relacjami logistycznymi, ale również inne dokumenty, których niezabezpieczenie może stanowić zagrożenie dla przedsiębiorstwa. Dokumentacja przedsiębiorstw zajmujących się produkcją metalowych elementów konstrukcyjnych została odpowiednio zaszeregowana w grupy informacyjne, dla których została wyliczona wrażliwość (tab.10).

Tabela 10. Wyliczanie wrażliwości grup informacji

Oznaczenie	Grupa informacji	P	D	I	WG
I1	Dokumentacja zawierające informacje chronione firmy	3	3	2	11
I2	Dokumentacja zarządcza i prawno-organizacyjna	2	3	2	9
I3	Dokumentacja finansowa	2	3	2	9
I4	Dokumentacja strategiczna	2	3	2	9
I5	Dokumentacja informatyczna	2	3	2	9
I6	Dokumentacja technologiczno-produkcyjna	1	3	2	9
I7	Dokumentacja ogólnie dostępna wewnątrz i na zewnątrz przedsiębiorstwa	0	1	2	3

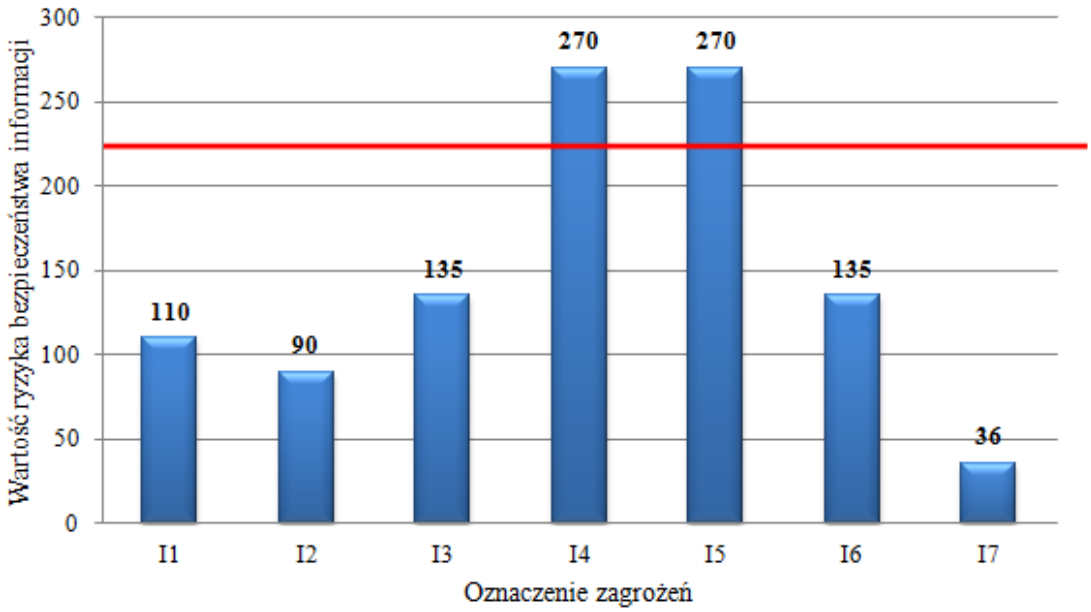
Źródło: opracowanie własne

Aby oddzielić ryzyko akceptowalne od ryzyka nieakceptowanego określony został próg akceptowalności ryzyka bezpieczeństwa informacji, który wyniósł 223. Oznacza to, że ryzyka znajdujące się powyżej tego poziomu stanowią największe zagrożenie dla analizowanych przedsiębiorstw i w stosunku do nich należy określić odpowiednie postępowanie, mające na celu obniżenie ryzyk aktywów informacyjnych poniżej ustalonej wartości ryzyka akceptowalnego. Uzyskane wyniki oceny ryzyka bezpieczeństwa informacji w relacjach z dostawcami przedsiębiorstw branży metalowej wraz z wartością ryzyka akceptowalnego zostały graficznie zaprezentowane na rys. 1.

Tabela 11. Szacowanie ryzyka bezpieczeństwa informacji w kontekście możliwych zagrożeń

	Zagrożenie	WA	Pd	Z	ŁW	PR	Sf	Sp	Sw	S	R
I1	Zagrożenia związane z bezpieczeństwem danych osobowych	11	2	1	2	1	1	2	2	5	110
I2	Zagrożenia dotyczące zgodności z obowiązującymi regulacjami prawnymi	9	2	1	2	1	1	2	2	5	90
I3	Zagrożenia dotyczące ujawnienia działań finansowych	9	3	1	3	1	2	2	1	5	135
I4	Zagrożenia związane z bezpieczeństwem informacji strategicznych dla firm	9	3	2	6	1	2	2	1	5	270
I5	Zagrożenia związane z bezpieczeństwem haseł dostępu do systemów informatycznych	9	3	2	6	1	1	2	2	5	270
I6	Zagrożenia związane z ujawnieniem wykorzystywanej technologii	9	3	1	3	1	2	2	1	5	135
I7	Zagrożenia związane z niewłaściwym wykorzystaniem dokumentacji	3	1	4	4	1	1	1	1	3	36

Źródło: opracowanie własne na podstawie



Rys. 1. Ocena ryzyka bezpieczeństwa informacji w relacjach z dostawcami przedsiębiorstw branży metalowej.

Źródło: opracowanie własne

Przeprowadzona ocena ryzyka bezpieczeństwa informacji wykazała, że najwyższy poziom, przekraczający próg akceptacji uzyskały dwie grupy zagrożeń: związane z bezpieczeństwem haseł dostępu do systemów informatycznych oraz wyciekiem informacji strategicznych. Są to zagrożenia, które wraz z rozwojem nowoczesnych technologii coraz częściej stanowią bardzo groźne źródło potencjalnych niebezpieczeństw. Przedsiębiorstwa uwzględniając uzyskaną ocenę ryzyka powinny określić odpowiednie postępowanie. Najpowszechniejszą strategią reagowania na ryzyko jest próba jego obniżenia poprzez wybór odpowiednich zabezpieczeń. Jednak takie rozwiązanie związane jest nakładami finansowymi oraz zmianami organizacyjnymi. Drugim rozwiązaniem jest przeniesienie przez przedsiębiorstwo skutków zdarzeń niepożądanych na inny podmiot. Najczęściej, podmiotami tymi są bezpośredni kontrahenci lub zakłady ubezpieczeniowe. Przedsiębiorstwa mogą się również zdecydować na akceptacje ryzyka, co jest związane z przyjęciem wszystkich konsekwencji wynikających z wystąpienia zjawiska.

3. PODSUMOWANIE

Informacje stanowią charakterystyczny rodzaj aktywów każdego przedsiębiorstwa, chociaż bardzo często są niedostatecznie chronione. Są one związane, że wszystkimi aspektami działalności przedsiębiorstwa, dlatego również w przypadku relacji z dostawcami bezpieczeństwo informacji posiada określoną wartość i powinno być właściwie chronione. Pojęcie bezpieczeństwa informacji współpracy logistycznej, można zatem określić jako zbiór działań, który podejmują jego uczestnicy w celu zabezpieczenia informacji przed nieuprawnionym dostępem, zniszczeniem, lub też nieodpowiednim modyfikacjom. W artykule przeprowadzona została ocena ryzyk bezpieczeństwa informacji w relacjach z dostawcami wśród przedsiębiorstw zajmujących się produkcją konstrukcji stalowych. Analizie została poddana nie tylko dokumentacja, która tylko bezpośrednio dotyczy dostawy, ale również wszystkie aktywa informacyjne, z którymi dostawcy mogą mieć kontakt podczas współpracy. Przeprowadzona ocena ryzyka pozwoliła wyszczególnić dwie grupy zagrożeń, których poziom ryzyka wyniósł 270, co oznacza, że przekroczyły one poziom akceptacji. Są to zagrożenia związane z bezpieczeństwem haseł dostępu do systemów informatycznych oraz wyciekiem informacji strategicznych. Reasumując, przeprowadzony proces szacowania ryzyk aktywów umożliwił wskazanie aktywów najbardziej zagrożonych, dzięki czemu przedsiębiorstwa uzyskują wiedzę, którymi aktywami należy się zająć w pierwszej kolejności i wdrożyć dla nich zabezpieczenia.

LITERATURA

1. Materska, K. (2003). O wartości informacji w systemach zarządzania informacją i wiedzą. W: L. Drelichowskiego, A. Januszewskiego, G. Dzieży (red.) *Zastosowanie technik informacyjnych w gospodarce i zarządzanie wiedzą*, Bydgoszcz.
2. Czekaj, R. (red.). (2012). *Podstawy zarządzania informacją*. Kraków: Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.
3. Bielecki, M. Szymonik, A. 2014. Bezpieczeństwo systemów logistycznych w wymogach i normach międzynarodowych. *Systemy Logistyczne Wojsk* (41). 21-40.
4. Żebrowski, A. (2004). Bezpieczeństwo wiedzy – nowy atrybut działalności przedsiębiorstwa. W R. Borowiecki (red.) *Informacja i wiedza w zintegrowanym systemie zarządzania*. Kraków.
5. Romanowska, M. (2001). Kształtowanie wartości firmy w oparciu o kapitał intelektualny. W: R. Borowiecki, M. Romanowska (red.) *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa.* Warszawa: Wydawnictwo Difin.
6. Liderman, K. (2012). *Bezpieczeństwo informacyjne*. Warszawa: Wydawnictwo Naukowe PWN.
7. Liderman, K. (2009). *Analiza ryzyka i ochrona informacji w systemach komputerowych.* Warszawa: Wydawnictwo Naukowe PWN Mikom.
8. Górska, M. Pająk, B. (2015). Wybrane zagadnienia zarządzania relacjami w sferze Zaopatrzenia przedsiębiorstw przemysłu metalowego. *Systemy Logistyczne Wojsk (42).* 81-90.
9. Białas, A. (2006). *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie.* Warszawa: Wydawnictwo Naukowo-Techniczne.
10. PN-ISO/IEC 27001:20