OCENA RYZYKA BEZPIECZEŃSTWA INFORMACJI W PROCESIE ZAOPATRZENIA

THE INFORMATION SECURITY RISK ASSESSMENT IN THE SUPPLY PROCESS

Kamila KOKOSZCZYK
kadamus@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 zaprezentowano wybrane zagadnienia teoretyczne związane z bezpieczeństwem informacji w przedsiębiorstwie. Następnie dokonano analizy i oceny ryzyka bezpieczeństwa informacji w procesie zaopatrzenia zachodzącym w wybranym przedsiębiorstwie branży metalowej. Oszacowanie ryzyka bazowało na podejściu zgodnym z normą ISO 27001. Wyniki prowadzonych badań poddano omówieniu, co w efekcie pozwoliło na sformułowanie wniosków końcowych.

Abstract: In this paper were presented selected theoretical issues associated with security information in an enterprise. Then were made the analysis and assessment of information security in the supply process taking place in the selected enterprise from the metal industry. The risk assessment was based on an approach with accordance to ISO 27001 standard. The results of studies were discussed, which allowed to formulate final conclusions.

Słowa kluczowe: proces zaopatrzenia, bezpieczeństwo informacji, ocena ryzyka

Key words: supply process, information security, risk assessment

WSTĘP

W dobie ciągłych przemian, globalizacji i nasilonej konkurencji wzrosło znaczenie informacji we współczesnym świecie. Dziś traktuje się je, jako jeden z najcenniejszych zasobów o strategicznym znaczeniu dla przedsiębiorstwa. Jak pokazują badania już 77% organizacji zdaje sobie sprawę, jak dużą wartość mają informacje, a zadbanie o ich bezpieczeństwo uważa się za jedno z priorytetowych działań. Zatem świadomość ważności informacji znacząco wzrosła, gdy jeszcze kilka lat temu był to temat, do którego przedsiębiorstwa nie przywiązywały znaczącej uwagi (Góra, 2013). Niemały wpływ na taki przebieg wydarzeń miał rozwój nowoczesnych technologii informatycznych, które sprawiły, że dostęp do wszelkiego rodzaju informacji i dzielenie się nimi stały się o wiele prostsze niż

było to kiedyś. Z tego powodu również i ich ochrona oraz bezpieczeństwo nabrały zupełnie innego wymiaru, bowiem ryzyko utraty cennych danych także znacząco wzrosło.

W związku powyższym głównym celem artykułu jest ocena ryzyka bezpieczeństwa informacji w procesie zaopatrzenia zachodzącym w wybranym przedsiębiorstwie branży metalowej. Do jej przeprowadzenia zostały wykorzystane dane źródłowe pochodzące z badanego podmiotu oraz procedura szacowania ryzyka zaprezentowana w normie ISO serii 27001, odpowiednio zaadoptowana do potrzeb przedsiębiorstwa. Efektem badań jest określenie stanu bezpieczeństwa zidentyfikowanych w procesie zaopatrzenia aktywów informacyjnych.

1. ROLA BEZPIECZEŃSTWA INFORMACJI W LOGISTYCE

Informacje nabierają szczególnego znaczenia w kontekście logistyki. Ich efektywny przepływ w procesach logistycznych sprawia, że przedsiębiorstwo może odpowiednio reagować na potrzeby rynku, obniżać poziom niepewności w procesach związanych z logistyką, identyfikować obszary wymagające podjęcia działań naprawczych, czy też skutecznie rozwiązywać aktualne problemy logistyczne (Gąsowska, 2014). Zatem rzetelna informacja zespaja ze sobą wszystkie ogniwa logistyki i przyczynia się do właściwego funkcjonowania procesów w całym łańcuchu.

Wiedząc, jak istotną i poważną kwestią jest bezpieczeństwo informacji zarówno w procesach logistycznych, jak i w całym przedsiębiorstwie powstaje pytanie, co można zrobić, aby należycie je chronić? Jednym z rozwiązań, które wspomaga kompleksową ochronę informacji jest norma ISO/IEC 27001. Jak piszą autorzy (Brożek, Sikorski, Stanio, 2014) głównym motywem dla jej opracowania było zebranie i ujednolicenie najlepszych praktyk i doświadczeń dotyczących zarządzania bezpieczeństwem informacji. Jest to bowiem norma, która pozwala przedsiębiorstwu zapewnić ochronę wszystkich informacji, także tych finansowych i ściśle poufnych w sposób kompleksowy i usystematyzowany. Ponadto jej wdrożenie znacząco minimalizuje prawdopodobieństwo, że ktoś uzyska dostęp do danych w sposób nielegalny lub bez zezwolenia.

Wdrożenie certyfikowanego systemu bezpieczeństwa informacji zgodnego z PN-ISO/IEC 27001 niesie ze sobą wiele korzyści na różnych obszarach działalności firmy. Wśród nadrzędnych Polski Komitet Normalizacyjny wymienia (Polski Komitet Normalizacyjny, 2016):

- Świadomość - podniesienie poziomu świadomości pracowników, co do znaczenia bezpieczeństwa informacji i strat, wynikających z naruszenia bezpieczeństwa informacji.

- Wiarygodność, pewność, zaufanie - klient jest pewny, że informacje (w tym jego dane osobowe), które powierzył firmie są odpowiednio zabezpieczone. System potwierdzony dodatkowo certyfikatem PN na zgodność z normą PN-ISO/IEC 27001:2007, wydanym przez PKN, jest dla klienta obiektywnym dowodem na wiarygodność przedsiębiorstwa.
- Zgodność - ustanowiony SZBI (System Zarządzania Bezpieczeństwem Informacji) daje pewność, że przedsiębiorstwo zidentyfikowało i spełniło wymagania prawne oraz inne obowiązujące go przepisy.
- Zapewnienie ciągłości funkcjonowania firmy - identyfikacja możliwych zagrożeń oraz redukcja poziomu ryzyka związanego z utratą kontroli nad bezpieczeństwem informacji.
- Zaangażowanie - skuteczny system to wysiłek i zaangażowanie każdego pracownika, niezależnie od zajmowanego stanowiska.
- Marketing - wdrożony system jest elementem zwiększającym konkurencyjność firmy na rynku.

Reasumując należy zaznaczyć, że w dzisiejszym globalnym świecie biznesu świadomość wartości informacji wzrosła, a nawet stała się jedną z głównych kart przetargowych na rynku. Informacja to wiedza, która odpowiednio chroniona jest kluczem do osiągnięcia przewagi konkurencyjnej. W jej zdobyciu niezwykle pomocne i wskazane może okazać się wdrożenie całościowego Systemu Zarządzania Bezpieczeństwem Informacji, który zapewni niezakłócony przepływ informacji zachodzącym procesom i zminimalizuje ryzyko wystąpienia zagrożeń związanych z utratą informacji.

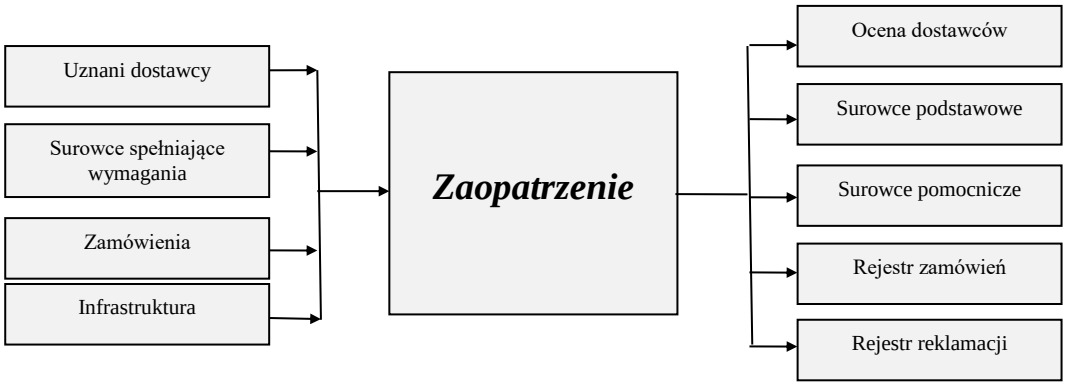
2. ANALIZA I OCENA RYZYKA BEZPIECZEŃSTWA INFORMACJI W PROCESIE ZAOPATRZENIA

2.1 Prezentacja podmiotu badań i charakterystyka procesu zaopatrzenia

Przedsiębiorstwo poddane badaniu działa w branży metalowej (produkcja drutu i wyrobów z drutu) i posiada ugruntowaną pozycję na rynku. Należy do grupy dużych podmiotów i dysponuje wysoko wykwalifikowaną kadrą pracowników. Swoją pozycję podmiot zbudował bazując na takich wartościach jak: tradycja, rzetelność, jakość. Z kolei nadrzędny cel działalności firmy stanowi dbanie o potrzeby i preferencje klientów oraz dostarczenie im produktu i rozwiązań najwyższej jakości. W kontekście prowadzonych badań należy dodać, że przedsiębiorstwo jest na etapie wdrażania całościowego Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z omawianą normą ISO 27001 i jego

integracji z obowiązującym już w firmie Systemem Zarządzania Jakością zgodnym z wymaganiami normy ISO 9001.

Przedmiotem rozważań w niniejszym artykule jest bezpieczeństwo informacji w procesie zaopatrzenia (elementy wejściowe i wyjściowe zaprezentowano na rys. 1). Głównym celem realizacji zaopatrzenia w badanym przedsiębiorstwie jest zakup surowców o wymaganej jakości i ilości oraz dostarczenie ich w ustalonym czasie w taki sposób, aby było zapewnione terminowe wykonanie zadań produkcyjnych. Proces ten odgrywa istotną rolę, ponieważ od tego, jaki będzie jego wynik zależy realizacja dalszych etapów produkcyjnych. Dlatego płynny przepływ sprawdzonych informacji i ich bezpieczeństwo są tu niezwykle istotne.



Rys. 1. Elementy wejścia i wyjścia składające się na proces zaopatrzenia w badanym przedsiębiorstwie

Źródło: Księga Jakości badanego przedsiębiorstwa

Analizując proces zaopatrzenia w analizowanym podmiocie warto również dodać, że przedsiębiorstwo posiada grupę sprawdzonych dostawców, z którymi kooperuje na zasadach partnerstwa. Przed podjęciem decyzji o współpracy są oni poddawani procesowi kwalifikacji, a w jej trakcie okresowo oceniani i weryfikowani. Ocenie poddawane są takie parametry jak: jakość dostarczanych surowców, terminowość, współpraca z danym dostawcą oraz kształtowanie cen.

2.2. Analiza i ocena ryzyka w procesie zaopatrzenia

Procedura oceny ryzyka przebiegła zgodnie z wdrażaną w podmiocie normą ISO 27001, odpowiednio zaadoptowaną do potrzeb przedsiębiorstwa. Pierwszym krokiem była identyfikacja głównych aktywów informacyjnych w procesie zaopatrzenia, rozumianych jako przetwarzane informacje. Zostały one podzielone na osiem grup (oznaczonych symbolicznie od A1 do A8), a każda z nich była ściśle związana z danym etapem procesu zaopatrzenia. Następnie wyznaczono właścicieli aktywów informacyjnych oraz tzw. aktywa wspierające,

czyli określone środki wspomagające. Zgodnie z przyjętą procedurą badawczą każda z grup aktywów informacyjnych posiada pewną wartość dla przedsiębiorstwa, zwaną *wrażliwością grupy (WG)*. Określono ją poprzez przyporządkowanie danej grupie aktywów informacyjnych odpowiednich wartości poziomów *poufności (P)*, *dostępności (D)* oraz *integralności (I)*, zgodnie z formułą:

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

Wartości poszczególnych parametrów ustalono na podstawie przyjętych w przedsiębiorstwie wzorów oraz skal stosowanych podczas analizy ryzyka bezpieczeństwa informacji (tabela 1).

Tabela 1. Skala poziomu poufności, integralności, dostępności

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

Na podstawie uzyskanych wartości *wrażliwości grupy (WG)* poszczególne grupy aktyw informacyjnych przyporządkowano do ustalonych w przedsiębiorstwie poziomów ochrony. W badanym podmiocie wyróżniono cztery poziomy, a mianowicie:

- poziom I – informacje ogólnodostępne (wartość *wrażliwości grupy (WG)* w zakresie 2 – 4),

- poziom II – informacje ogólnodostępne wewnątrz przedsiębiorstwa (wartość *wrażliwości grupy (WG)* w zakresie 5 – 7),
- poziom III – informacje chronione, nadzorowane i kontrolowane w przedsiębiorstwie (wartość *wrażliwości grupy (WG)* w zakresie 8 – 9),
- poziom IV – informacje szczególnie chronione, nadzorowane i kontrolowane w przedsiębiorstwie (wartość *wrażliwości grupy (WG)* w zakresie 10 – 11).

Wyniki przeprowadzonych na tym etapie działań przedstawia tablica 2.

Tabela 2. Określenie głównych aktywów informacyjnych i szacowanie wskaźnika wrażliwości grupy informacji

Symbol aktywów informa-cyjnych	**Główne aktywa informacyjne/ Główne etapy procesu zaopatrzenia**	**Właściciel aktywów informacyjnych**	**Aktywa wspierające**	**P**	**D**	**I**	**WG**	**Poziom ochrony**
A1	Informacje dotyczące rozeznania cen i dostawców / Analiza rynku, dostawców	- Kierownik działu zaopatrzenia. - Kierownicy odpowiednich komórek organizacyjnych.	- Personel zaangażowany w proces zaopatrzenia. - Sprzęt komputerowy. - Bazy i zbiory danych, rejestry. - Oprogramowanie informatyczne. - Nośniki danych (papier, dysk komputerowy, magnetyczny, elektroniczny). - Wzory umów, dokumentów. - Urządzenia sieciowe i telefoniczne. - Urządzenia transportowe.	2	2	2	**8**	III
A2	Informacje na temat wymagań surowców / Określenie wymagań surowców			1	2	2	**6**	II
A3	Informacje na temat zapotrzebowania na materiały i surowce / Sformułowanie zamówienia			2	3	2	**9**	III
A4	Informacje na temat umów z dostawcami / Wybór dostawcy			2	3	2	**9**	III
A5	Informacje zawarte w rejestrach zamówień / Zakup materiałów			2	3	2	**9**	III
A6	Informacje na temat procedury kontroli dostawy / Kontrola dostawy			1	3	2	**7**	II
A7	Informacje na temat dostawy i jej akceptacji / Dostawa materiałów, przyjęcie na magazyn			1	3	2	**7**	II
A8	Informacje na temat reklamacji dostawy / Zwrot dostawy			1	3	2	**7**	II

Źródło: opracowanie własne

Poddając dyskusji dane na temat wskaźnika *wrażliwości grupy informacji (WG)* można zauważyć, że najwyższy jego poziom uzyskały aktywa informacyjne oznaczone symbolami *A1, A3, A4, A5*, które zostały przyporządkowane do III poziomu ochrony informacji w przedsiębiorstwie. Analizując dalej można wnioskować, że żadna grupa aktywów informacyjnych nie posiada najniższego (I) i najwyższego (IV) poziomu ochrony informacji. Jest to zapewne spowodowane tym, że w badanym procesie zaopatrzenia nie występują informacje o takim poziomie poufności, który wymagałby szczególnego nadzoru i kontroli. Zatem utrata ich atrybutów bezpieczeństwa nie miałaby kluczowego wpływu na biznesowe i strategiczne działanie badanego podmiotu.

W kolejnym etapie badań dokonano analizy ryzyka bezpieczeństwa informacji w procesie zaopatrzenia. Przeprowadzono ją w kontekście możliwych zagrożeń i podatności, które mogą dotyczyć danego aktywa informacyjnego. W tym celu w pierwszej kolejności dla każdej grupy informacji określono możliwe zagrożenia (skupiono się na najważniejszych zagrożeniach). Następnie oszacowano wartość *ryzyka (R)*, które zostało obliczone na podstawie wzoru:

$$\boldsymbol{R = WA \; x \; ŁW \; x \; Pr \; x \; S} \tag{2}$$

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

Poszczególne czynniki ryzyka zostały oszacowane zgodnie z wytycznymi ustalonymi przez przedsiębiorstwo. W pierwszym etapie przyjęto założenie, że *wartość danego aktywa informacyjnego (WA)* jest równa wrażliwości danej grupy informacji (czyli *WA = WG*). Następnie dokonano obliczeń dla współczynnika *łatwość wykorzystania podatności przez zagrożenie (ŁW)* w oparciu o formułę:

$$\boldsymbol{ŁW = Pd \; x \; Z} \tag{3}$$

Parametr *znaczenie podatności w kontekście zidentyfikowanego zagrożenia (Pd)* został oszacowany zgodnie ze skalą:

- 1 – niski poziom podatności na zagrożenie,
- 2 – średni poziom podatności na zagrożenie,
- 3 – wysoki poziom podatności na zagrożenie.

Z kolei drugi parametr przedstawionej formuły, czyli *poziom wdrożonych zabezpieczeń (Z)* zostały oszacowane na podstawie skali:

- 1 – zabezpieczenia są stosowane oraz sformalizowane,
- 2 – zabezpieczenia są stosowane ale nie są sformalizowane,
- 3 – zabezpieczenia są stosowane i nie są sformalizowane.

Po dokonaniu wyliczeń współczynnika *ŁW* należało przejść do oszacowania *prawdopodobieństwa wystąpienia zagrożenia (Pr)*, które zostało określone zgodnie z wytycznymi:

- 1 – zagrożenie jest mało realne,
- 2 – zagrożenie jest bardzo realne i może wystąpić w każdej chwili.

Po określeniu jego wartości oszacowano *straty biznesowe (S)*, jakie mogą wyniknąć na skutek naruszenia bezpieczeństwa informacji w zakresie poufności, dostępności i integralności. Straty są sumą skutków: *finansowego (Sf), prawnego (Sp)* oraz *wizerunkowego (Sw)*. Do oszacowania *skutków finansowych (Sf)* przyjęto skalę:

- 1 - materializacja zagrożenia nie spowoduje strat finansowych, lub spowoduje małe straty finansowe (do 50 tys. zł),
- 2 - materializacja zagrożenia spowoduje straty finansowe (większe niż 50 tys. zł).

Skutki prawne (Sp) oszacowano zgodnie z wytycznymi:

- 1 - materializacja zagrożenia nie prowadzi do naruszenia przepisów prawa lub regulacji wewnętrznych,
- 2 - materializacja zagrożenia prowadzi do naruszenia przepisów prawa lub regulacji wewnętrznych.

Skutki wizerunkowe (Sw) określono zgodnie z następującym podziałem:

- 1 - materializacja zagrożenia nie ma negatywnego wpływu na wizerunek przedsiębiorstwa,
- 2 - materializacja zagrożenia ma negatywny wpływ na wizerunek przedsiębiorstwa.

Po oszacowaniu wszystkich parametrów była możliwa ocena *ryzyka (R)*. Wyniki zaprezentowano w tabeli 3.

Tabela 3. Szacowanie *ryzyka bezpieczeństwa informacji (R)* w kontekście możliwych zagrożeń

Symbol grupy informacji	**Główne aktywa informacyjne/ Główne etapy procesu zaopatrzenia**	**Główne kategorie możliwych zagrożeń**	**WA**	**Pd**	**Z**	**ŁW**	**Pr**	**Sf**	**Sp**	**Sw**	**S**	**R**
A1	Informacje dotyczące rozeznania cen i dostawców / Analiza rynku, dostawców	Zagrożenia związane z ujawnieniem poufnych analiz rynkowych, dostęp osób nieuprawnionych do danych.	**8**	3	3	**9**	**1**	2	1	2	**5**	**360**
A2	Informacje na temat wymagań surowców / Określenie wymagań surowców	Awaria systemu komputerowego, awaria łączności, brak zasilania, dostęp osób nieuprawnionych do danych, nieprawidłowe działanie oprogramowania, błąd ludzki.	**6**	2	2	**4**	**2**	1	1	1	**3**	**144**
A3	Informacje na temat zapotrzebowania na materiały i surowce / Sformułowanie zamówienia	Błąd ludzki, niedostosowanie się do procedur, awaria systemu, awaria zasilania, nieprawidłowe działanie oprogramowania, awaria łączności.	**9**	2	2	**4**	**2**	1	2	1	**4**	**288**
A4	Informacje na temat umów z dostawcami / Wybór dostawcy	Wyciek informacji na temat dostawców, dostęp osób nieuprawnionych do umów, szpiegostwo gospodarcze.	**9**	2	4	**8**	**1**	2	2	2	**6**	**432**
A5	Informacje zawarte w rejestrach zamówień / Zakup materiałów	Awaria sprzętu komputerowego, wady oprogramowania, błąd ludzki, złamanie hasła, dostęp osób niepowołanych.	**9**	2	2	**4**	**2**	2	1	2	**5**	**360**
A6	Informacje na temat procedury kontroli dostawy / Kontrola dostawy	Zagrożenia związane z niewłaściwą kontrolą, przyjęcie zamówienia niezgodnego z	**7**	1	4	**4**	**1**	2	2	1	**5**	**140**

		wymaganiami.										
A7	Informacje na temat dostawy i jej akceptacji / Dostawa materiałów, przyjęcie na magazyn	Błąd ludzki, niestosowanie się do obowiązujących regulaminów i procedur.	**7**	1	2	**2**	**1**	2	2	1	**5**	**70**
A8	Informacje na temat reklamacji dostawy / Zwrot dostawy	Błąd ludzki, niestosowanie się do obowiązujących regulaminów i procedur.	**7**	1	2	**2**	**1**	2	2	1	**5**	**70**

Źródło: opracowanie własne

Można zauważyć, że najwyższy poziom *ryzyka (R*) został zaobserwowany na etapie wyboru dostawcy w procesie zaopatrzenia (*A4 - informacje na temat umów z dostawcami*). Z kolei najniższe ryzyko pojawiło się przy grupach aktywów informacyjnych oznaczonych symbolami *A7 - informacje na temat dostawy i jej akceptacji* oraz *A8 - informacje na temat reklamacji dostawy.*

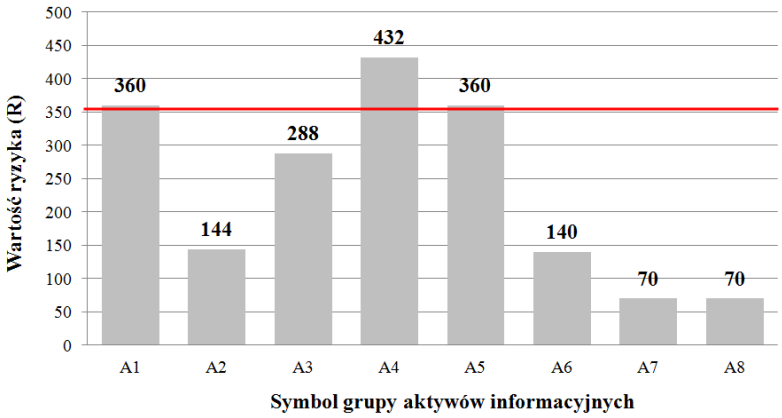
W końcowym etapie szacowania należało wydzielić ryzyko akceptowalne od ryzyka nieakceptowanego. W tym celu wyliczono próg akceptowalności ryzyka bezpieczeństwa informacji zgodnie z formułą:

$$R_{akc} = (R_{max} - R_{min}) \times 0{,}8 + R_{min} \quad (4)$$

gdzie: R_{akc} – *wartość progu akceptowalności ryzyka,*
R_{max} – *ryzyko o największej wartości,*
R_{min} – *ryzyko o najmniejszej wartości.*

Ryzyko akceptowalne (R_{akc}) obliczone według wzoru wyniosło 359,6. Oznacza to, że zgodnie z obowiązującą w przedsiębiorstwie procedurą każde ryzyko bezpieczeństwa informacji, którego wartość przekracza obliczony próg akceptowalności, zaliczane jest do grupy ryzyka nieakceptowanego, czyli do takiego, które wymaga podjęcia odpowiednich działań zapobiegawczych w celu obniżenia jego wartości.

Aby wskazać, które z grup aktywów informacyjnych znalazły się powyżej progu akceptowalności ryzyka dane dotyczące wartości *ryzyka (R)* przedstawiono graficznie (rys. 1).



Rys. 2. Zestawienie wyników analizy ryzyka bezpieczeństwa informacji w procesie zaopatrzenia

Źródło: opracowanie własne

Przeprowadzone badania wykazały, że spośród ośmiu grup aktywów informacyjnych tylko trzy są obarczone największym podatnością na wystąpienie zagrożeń. Są nimi: *A4 - informacje na temat umów z dostawcami*, *A5 - informacje zawarte w rejestrach zamówień* oraz *A1 - informacje dotyczące rozeznania cen i dostawców*, z czego dwie (*A1* i *A5*) są na granicy progu akceptowalności. Wobec wskazanych grup aktywów należałoby zastosować właściwe działania zapobiegawcze celem uniknięcia zagrożeń związanych z utratą danych. Należy zwrócić uwagę, że w przypadku wskazanych grup głównym źródłem wycieku informacji z przedsiębiorstwa może być człowiek. Czynnik ludzki, jako jedno z najsłabszych elementów w całym systemie zabezpieczeń powinien stać się jednym z głównych obiektów zainteresowań budowanego w przedsiębiorstwie Systemu Zarządzania Bezpieczeństwem Informacji. A starania badanego podmiotu powinny być ukierunkowane na zwiększenie świadomości pracowników, budowaniu w nich poczucia odpowiedzialności i solidaryzacji z firmą. Ponadto należy stwierdzić, że wdrażany system zabezpieczeń informacji już przynosi pozytywne efekty, bowiem poziomy ryzyka dla pozostałych grup aktywów informacyjnych w procesie zaopatrzenia są relatywnie niskie.

3. PODSUMOWANIE

Brak bezpieczeństwa aktywów informacyjnych to poważny problem przedsiębiorstwa. Analiza i ocena ich ryzyka pozwala na wskazanie tych, które są najbardziej zagrożone. Dzięki temu podmiot wie, w którym miejscu w pierwszej kolejności wdrożyć odpowiednie działania. Najlepszym rozwiązaniem na uniknięcie, czy też zminimalizowanie podatności na zagrożenia jest wdrożenie całościowego Systemu Zarządzania Bezpieczeństwem Informacji, który pozwoli na zaaplikowanie stosownej polityki ochronnej. Wiąże się to z podjęciem wielu

działań, a także kosztów, jednak przynosi mierzalne korzyści, co udowodniły przeprowadzone badania. Przedsiębiorstwo poddane dyskusji jest w trakcie wdrażania systemu zgodnego z ISO 27001 i jego integracji z ISO 9001, a analiza i ocena ryzyka bezpieczeństwa informacji w procesie zaopatrzenia pozwala stwierdzić, że system ten już przynosi korzyści (tylko trzy grupy aktywów znalazły się powyżej akceptowalnego progu ryzyka, z czego dwie znalazły się na jego granicy). Z przeprowadzonych badań wynikło, że zagrożenia, jakie mogą wystąpić mają swoje źródło głównie w personelu i działania zapobiegawcze należałoby skupić na tym czynniku. Ten główny wniosek, jak i pozostałe wyniki prowadzonych badań zostały przekazane kierownikowi działu zaopatrzenia (właścicielowi aktywów informacyjnych w procesie zaopatrzenia), który wspólnie z osobami odpowiedzialnymi za budowę SZBI w przedsiębiorstwie podejmie odpowiednie działania prewencyjne.

LITERATURA

1. Brożek, T., Sikorski, J. i Stanio, G. (2014). *Wykorzystanie standardu PCI DSS oraz normy ISO/IEC 27001 w celu zapewnienia bezpieczeństwa informacji*. Zeszyty Naukowe Wydziału Informatyki Wyższej Szkoły Informatyki Stosowanej i Zarządzania „Informatyka Stosowana" Nr 1.
2. Dane źródłowe badanego przedsiębiorstwa.
3. Gąsowska, M.K. (2014). *System informacji jako narzędzie wspomagające zarządzanie logistyką w przedsiębiorstwie i łańcuchach dostaw*. Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie Z. 68 Nr Kol. 1905.
4. Góra, J. (2013). *Efektywne zarządzanie bezpieczeństwem informacji*. Raport 2013. SZiP i Media Recovery. Na: https://www.us.edu.pl/sites/all/files/www/wiadomosci/pliki /RAPORT2013.pdf (10.05.2016 r.).
5. Księga Jakości badanego przedsiębiorstwa.
6. Polski Komitet Normalizacyjny. *PN-ISO/IEC 27001:2007. Bezpieczeństwo informacji*. Broszura informacyjna. Na: http://www.pkn.pl/sites/default/files/broszura_pkn_szbi.pdf (10.05.2016 r.)