PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2014, t. II, s. 223–238

http://dx.doi.org/10.16926/tiib.2014.02.19

Michał Pałęga, Marcin Knapiński, Wiesław Kulma
Politechnika Częstochowska
al. Armii Krajowej 19, 42-200 Częstochowa,
e-mail: mpalega@wip.pcz.pl, knap@wip.pcz.pl, wkulma@onet.pl

ZARZĄDZANIE RYZYKIEM W SYSTEMIE BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE

Streszczenie. Zasoby informacyjne jako jedne z podstawowych aktywów biznesowych przedsiębiorstwa warunkują sukces rynkowy organizacji oraz utrzymanie jej konkurencyjności. Wobec powyższego istnieje potrzeba zbudowania w organizacji odpowiedniego systemu gwarantującego ochronę informacji przed zagrożeniami. Podstawowym elementem w systemie bezpieczeństwa informacji w przedsiębiorstwie jest zarządzanie ryzykiem. W artykule zaprezentowano wyniki analizy ryzyka bezpieczeństwa informacji w wybranym przedsiębiorstwie przemysłowym.
Słowa kluczowe: bezpieczeństwo informacji, zagrożenia, szacowanie ryzyka, zarządzanie ryzykiem.

RISK MANAGEMENT IN THE INFORMATION SECURITY SYSTEM IN THE ENTERPRISE

Abstract. Information resources, as one of the basic assets of enterprises determine a market success of organization and keeping its competitiveness. Therefore, it's necessary to construct appropriate system in organization, which guarantee information security before threats. The fundamental element of the information security system in the enterprise is the risk management. In the article the results of risk analysis of information security in the chosen industrial enterprise was presented.
Keywords: information security, threats, risk assessment, risk management.

Wprowadzenie

Doświadczenia ostatnich lat dowodzą wysokiego znaczenia informacji we współczesnym świecie oraz wskazują na narastanie zjawisk powodujących stany zakłócenia jej bezpieczeństwa, takie jak: zniszczenie, nieautoryzowana modyfikacja, udostępnianie osobom nieupoważnionym, niekontrolowany wyciek, kradzież itp. Wobec powyższego kierownictwo organizacji zmuszone jest do bacznego przyglądania się problematyce zapewnienia racjonalnego poziomu bezpieczeństwa w swojej jednostce oraz wdrażania skutecznych mechanizmów zabezpieczających i profilaktycznych. Funkcje te coraz częściej w przedsiębiorstwie pełni kompleksowy system zarządzania bezpieczeństwem informacji, którego kluczowy element stanowią procesy związane z zarządzaniem ryzykiem bezpieczeństwa informacji.

Ryzyko, zgodnie z normą PN-I-13335-1:1999, (…) *jest prawdopodobieństwem określającym możliwość wykorzystania określonej podatności przez dane zagrożenie w celu spowodowania strat lub zniszczenia zasobu lub grupy zasobów, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na instytucję* [7]. Zatem ryzyko jest kombinacją dwóch czynników: prawdopodobieństwa wystąpienia negatywnego zdarzenia (incydentu) i związanych z nim następstw. W kontekście bezpieczeństwa informacji należy rozumieć je jako potencjalne szkody spowodowane utratą poufności, integralności, dostępności, rozliczalności, autentyczności oraz niezawodności informacji [3].

Artykuł podejmuje problematykę zarządzania ryzykiem bezpieczeństwa informacji w przedsiębiorstwie. Omówiono w nim poszczególne etapy zarządzania ryzykiem, a także przedstawiono charakterystykę wybranych metod oceny ryzyka. Zasadniczym punktem niniejszego opracowania jest zaprezentowanie wyników przeprowadzonej analizy ryzyka utraty bezpieczeństwa informacji w wybranym przedsiębiorstwie przemysłowym.

Istota zarządzania ryzkiem bezpieczeństwa informacji i jego etapy

Zarządzanie ryzykiem jest procesem ciągłym ukierunkowanym na identyfikację, ocenę oraz przeciwdziałanie ryzyka. Uwzględniając problematykę bezpieczeństwa informacji, będzie on obejmował swoim zakresem przede wszystkim [11]:

- identyfikację ryzyka związanego z utratą bezpieczeństwa informacji w organizacji;
- ocenę stopnia wpływu ryzyka bezpieczeństwa informacji na wyznaczone przez jednostkę cele oraz kierunki działania;

- wdrożenie odpowiednich środków profilaktycznych, redukujących poziom ryzyka.

Zarządzanie ryzykiem obejmuje kompleksowe działania związane z identyfikacją, kontrolą, eliminacją bądź minimalizacją prawdopodobieństwa wystąpienia negatywnych zdarzeń, które mogą mieć wpływ na zasoby systemu informacyjnego i informatycznego przedsiębiorstwa.

Celem procesu zarządzania ryzykiem jest przede wszystkim ograniczenie ryzyka do poziomu akceptowalnego, co wymaga opracowania właściwego planu postępowania z ryzykiem, który może wiązać się z [6]:

- zastosowaniem właściwych zabezpieczeń, adekwatnych do zagrożeń i poziomu ryzyka;
- zaakceptowaniem ryzyk, w sposób świadomy i obiektywny, przy założeniu, że jasno spełniają warunki określone w polityce bezpieczeństwa oraz kryteria akceptowania ryzyk;
- unikaniem ryzyka;
- transferem ryzyka na inne podmioty, np. ubezpieczycieli, dostawców itp.

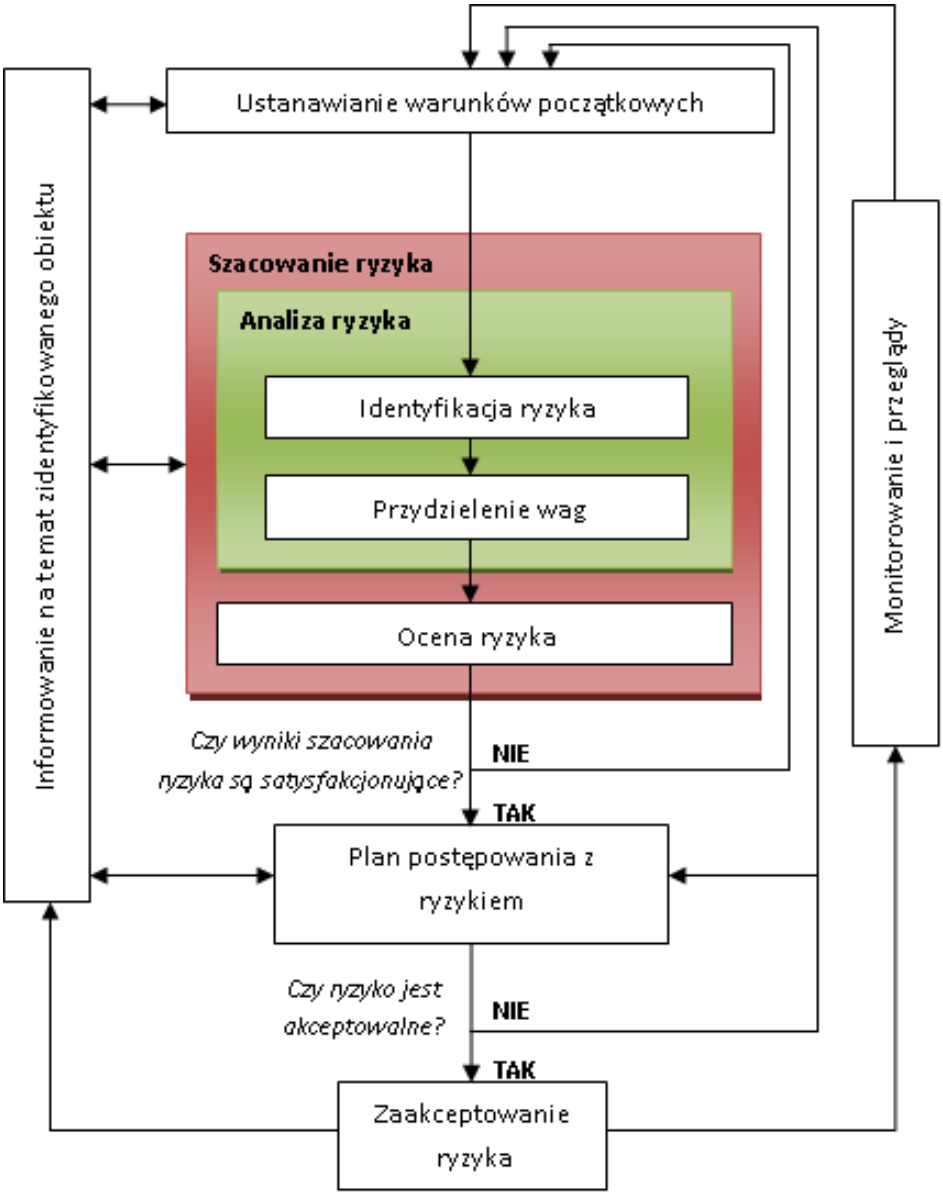
Model zarządzania ryzykiem został przedstawiony w formie graficznej na rys. 1.

Fundamentalne znaczenie w procesie zarządzania ryzykiem ma jego analiza. Pozwala ona na zidentyfikowanie nowych bądź zweryfikowanie istniejących zagrożeń oraz obszarów wymagających wprowadzania działań profilaktycznych i zabezpieczających. Przeprowadzona w sposób rzetelny umożliwia wyznaczyć warunki, jakim musi odpowiadać organizowany i funkcjonujący w przedsiębiorstwie system bezpieczeństwa informacji. Istota analizy ryzyka sprowadza się do określenia prawdopodobieństwa wystąpienia zdarzenia oraz oszacowania wielkości jego skutków (strat).

Metody szacowania ryzyka

Obecnie w literaturze opisywanych jest kilkadziesiąt metod szacowania i oceny ryzyka, z których duża część stała się powszechnie obowiązującym standardem, znajdującym zastosowanie w praktyce. Najogólniej można wyróżnić trzy podstawowe grupy:

- metody ilościowe;
- metody jakościowe;
- metody mieszane.



Rys. 1. Model zarządzania ryzykiem
Źródło: [8]

Metody ilościowe (kwantyfikatywne) – polegają na zastosowaniu matematycznych obliczeń w celu wyznaczenia wpływu zagrożeń (skutków) na bezpieczeństwo systemu oraz określenia prawdopodobieństwa ich wystąpienia. Skutki te mogą być wyznaczane w oparciu o ocenę wyników zdarzeń bądź przez ekstrapolację, biorąc pod uwagę dane z przeszłości (statystyczne, archiwalne). Wyniki oszacowanego ryzyka mogą być wyrażone w formie procentowej bądź pieniężnej. Wśród zalet opisywanej metodyki szacowania ryzyka można wyróżnić [4]:

- szacowanie oraz wyniki są obiektywne i mogą być ze sobą porównywane;
- wartość informacji wyrażona jest w postaci konkretnej kwoty pieniężnej;
- wyniki oszacowanego ryzyka mają określoną strukturę (postać) finansową bądź procentową.

Do wad metod ilościowych można natomiast zaliczyć [4]:

- wyliczenia dokonywane są kompleksowo, dlatego też wymagają odpowiedniego zrozumienia oraz wytłumaczenia, w przeciwnym przypadku kierownictwo organizacji może nie ufać wynikom oszacowanego ryzyka, uznając je za efekt „czarnej skrzynki”;
- praktyczne oraz skuteczne stosowanie metod ilościowych narzuca konieczność wykorzystywania zautomatyzowanych narzędzi oraz aplikacji informatycznych;
- konieczność gromadzenia informacji odnośnie do środowiska IT, zabezpieczeń oraz zasobów.

Metody jakościowe (kwalifikatywne) – charakteryzują się dość dużym subiektywizmem z uwagi na fakt, iż w procesie szacowania ryzyka wykorzystuje się wiedzę i doświadczenie specjalistów oraz tzw. dobre praktyki [2]. W analizie jakościowej ryzyko oraz potencjalne jego skutki mogą zostać przedstawione w sposób opisowy, przy użyciu różnych wariantów scenariuszy zdarzeń. W praktyce często zawierają one bardzo dużo detali determinujących trafność podejmowanych decyzji w kwestii konkretnych działań oraz wyboru mechanizmów ochronnych (zabezpieczeń). Do opisu zdarzeń i sytuacji używa się różne skale (np. ryzyko małe – 1; ryzyko maksymalne 4).

Zaletami metod jakościowych są [4]:

- brak kalkulacji i obliczeń, a jeżeli one występują, to są zrozumiałe i bardzo proste;
- w większości przypadków nie istnieje konieczność wyceny informacji (jej dostępności, poufności oraz integralności);
- brak jest konieczności ilościowej oceny skutków negatywnych zdarzeń oraz częstotliwości ich występowania;
- nie istnieje potrzeba szacowania kosztów zalecanych zabezpieczeń oraz ewentualnych strat;

– ogólne wskazanie sfer związanych z występowaniem ryzyka, na które należy położyć szczególny nacisk.

Ponadto wśród korzyści z użycia metod jakościowych można wskazać możliwość uwzględniania w procesie szacowania ryzyka takich sfer, jak np. kultura organizacyjna czy wizerunek przedsiębiorstwa. Należy także podkreślić, iż zastosowanie tego rodzaju metod nie wymaga zbierania konkretnych informacji i danych ilościowych, jak w przypadku metod ilościowych [4].

Metody mieszane – stanowią kombinację dwóch wyżej prezentowanych metod (ilościowej i jakościowej). Na etapie identyfikowania wszystkich obszarów ryzyka oraz jego skutków wykorzystuje się metody jakościowe, najczęściej z użyciem narzędzia, jakim jest scenariusz zdarzeń. Analiza ilościowa natomiast służy do oszacowania kosztów skutków wystąpienia ryzyka. Zastosowanie takiego podejścia znacznie zwiększa wiedzę użytkową kierownictwa organizacji w kwestii zachodzących procesów oraz uświadamiania potencjalnego ryzyka [5].

Ocena ryzyka bezpieczeństwa informacji za pomocą metody CRAMM – studium przypadku

1. Ogólne informacje o przedsiębiorstwie

Badane przedsiębiorstwo działa na krajowym i zagranicznym rynku usług budowlanych od wielu lat. W szczególności specjalizuje się w realizacji dużych projektów inwestycyjnych dla samorządów terytorialnych w zakresie budowy oczyszczalni ścieków oraz sieci kanalizacji. Firma swoją pozycję konkurencyjną zawdzięcza przede wszystkim wysoko wykwalifikowanej kadrze technicznej, administracyjnej i wykonawczej oraz profesjonalizmowi, dokładności i terminowości wykonywanych robót. Ponadto przedsiębiorstwo korzysta z własnego zaplecza projektowego oraz laboratorium badawczego, posiadającego akredytację PCA w zakresie normy PN-EN ISO/IEC 17025:2005.

2. Metodologia badań

Do przeprowadzenia analizy ryzyka związanego z bezpieczeństwem informacji dla wybranego przedsiębiorstwo przemysłowego zastosowano metodę CRAMM (Crisis Risk Analysis and Management Method). Prezentowana metoda należy do grupy metod jakościowych i opiera się na dwóch wskaźnikach: prawdopodobieństwie wystąpienia danego zagrożenia oraz wielkości strat spowodowanych zaistnieniem danego zdarzenia. Zależność tę przedstawia następująca formuła:

$$\boldsymbol{R = S \; x \; P} \qquad (1)$$

gdzie:
R – wielkość oczekiwane straty związanej z danym ryzykiem;
S – wielkość straty, w przypadku wystąpienia danego zdarzania;
P – prawdopodobieństwo wystąpienia danego zdarzenia.

W tab. 1. zaprezentowano cztery przyjęte poziomy wielkości ryzyka.

Tab. 1. Kategorie ryzyka

Przedział wielkości ryzyka	Kategoria ryzyka
1 – 20	Niskie
21 – 60	Średnie
61 – 80	Wysokie
81 – 100	Maksymalne

Źródło: opracowanie własne na podstawie: [1]

Wskazana metoda zakłada także, iż ryzyko po przekroczeniu wartości 20 wymaga szczegółowej analizy, z kolei po przekroczeniu wartości 60 – bezwzględnej redukcji podatności.

3. Wyniki z przeprowadzonych badań własnych

Zgodnie z założeniami przyjętej metodologii analizy ryzyka, pierwszy jej etap polega na identyfikacji możliwych do wystąpienia w przedsiębiorstwie zagrożeń związanych z bezpieczeństwem informacji oraz zdefiniowaniu, co organizacja rozumie przez dane zagrożenie. Jest to niezbędne działanie, mające na celu zapewnienie poprawnej weryfikacji i oceny niebezpieczeństw (tab. 2).

Tab. 2. Identyfikacja zagrożeń bezpieczeństwa informacji w badanym przedsiębiorstwie

Numer zagrożenia	Nazwa zagrożenia	Opis zagrożenia
ZG-1	Pożar	Niekontrolowane rozprzestrzenianie się ognia
ZG-2	Zalanie	Wydostanie się wody, pary lub innej cieczy w wyniku niedrożnej bądź uszkodzonej instalacji
ZG-3	Klęska żywiołowa	Klęska żywiołowa: sztorm, wichura, trzęsienie ziemi, tornado, tsunami, ekstremalne temperatury
ZG-4	Katastrofa budowlana	Niezamierzone, nagłe zniszczenie obiektu budowlanego, bądź jego części

Numer zagrożenia	Nazwa zagrożenia	Opis zagrożenia
ZG-5	Oddziaływanie elektromagnetyczne	Interferencja fal radiowych, pola magnetyczne, ultrafiolet
ZG-6	Awaria sprzętu	Awaria sprzętu, która może wynikać z wady sprzętu lub pojawić się w trakcie jego użytkowania i narastać do momentu całkowitego zniszczenia
ZG-7	Awaria oprogramowania	Awaria oprogramowania, która może wynikać z wady oprogramowania lub pojawić się w trakcie jego użytkowania i narastać do momentu całkowitego zniszczenia
ZG-8	Przerwy w zasilaniu	Przerwy w zasilaniu
ZG-9	Awaria łączności	Brak lub zaniki transmisji danych pomiędzy lokalizacjami, komputerami. Najczęściej wynika ze zniszczenia, awarii okablowania, lub przeciążeń, zniszczenia urządzeń sieciowych
ZG-10	Uszkodzenie nośników	Uszkodzenie elektronicznych nośników danych, uniemożliwiających odczytywanie, zapisywanie i przetwarzanie danych
ZG-11	Braki organizacyjne	Brak jasno zdefiniowanego zakresu odpowiedzialności (kto za co odpowiada), brak raportowania do kierownictwa, brak działań koordynacyjnych
ZG-12	Przypadkowe działania,błędy użytkowników	Przypadkowy wyciek, zmiana, uszkodzenie, ujawnienie informacji. Przypadkowe wprowadzenie błędnych informacji
ZG-13	Błędy oprogramowania	Błędy występujące w oprogramowaniu, niewynikające z działania użytkownika
ZG-14	Złośliwy kod	Program lub kod zdolny do przenikania do systemów, dysków lub indywidualnych plików, najczęściej bez zgodny i wiedzy użytkownika
ZG-15	Podsłuch	Przechwycenie danych i informacji przekazywanych za pomocą różnych kanałów komunikacyjnych bądź bezpośrednio pomiędzy stronami upoważnionymi do informacji stanowiącymi własność firmy

Numer zagrożenia	Nazwa zagrożenia	Opis zagrożenia
ZG-16	Złamanie hasła	Nieuprawnione wejście w posiadanie haseł dostępu do systemów, wskutek ich odgadnięcia, odszyfrowania
ZG-17	Braki personelu	Nieobecność personelu np. z powodu choroby, zdarzeń losowych, problemów komunikacyjnych
ZG-18	Nieświadomość pracownika	Brak znajomości procedur i regulaminów firmy przez personel
ZG-19	Przekroczenie kompetencji	Działanie pracownika (współpracownika) niezgodne z udzielonym zakresem uprawnień
ZG-20	Niestosowanie się do regulaminów	Postępowanie niezgodne z regulaminami firmy (oraz klientów) – w przypadku, gdy pracownicy zostali z nimi zapoznani i zobligowani do ich przestrzegania
ZG-21	Uchybienia proceduralne	Działanie uprawnionego pracownika firmy, które narusza obowiązujące w organizacji regulaminy i procedury oraz przepisy prawa
ZG-22	Sabotaż	Umyślne niewypełnianie lub wadliwe wypełnianie obowiązków przez personel w celu spowodowania dezorganizacji, szkód i strat
ZG-23	Kradzież	Przywłaszczenie sprzętu, danych, nośników, wyposażenia będących własnością bądź w posiadaniu firmy; w wyniku kradzieży może nastąpić brak dostępu do danych
ZG-24	Wtargnięcie	Wtargniecie nieuprawnionej osoby na teren, do budynku bądź pomieszczenia
ZG-25	Socjotechnika	Oddziaływanie na personel w celu spowodowania określonego działania

Źródło: opracowanie własne na podstawie [5]

W ramach dalszych badań dla każdego zidentyfikowanego zagrożenia określono prawdopodobieństwo jego wystąpienia oraz wielkość strat, jakie organizacja poniesie w związku z jego wystąpieniem. W tym celu posłużono się dziesięciostopniową skalą w zakresie od 1 do 10, gdzie 1 oznacza niski poziom prawdopodobieństwa bądź kosztów, natomiast 10 – bardzo wysoki poziom. Wyniki szacowania ryzyka dla badanego obiektu zostały zawarte w tab. 3.

Tab. 3. Szacowanie ryzyka bezpieczeństwa informacji w badanym przedsiębiorstwie

Numer zagrożenia	Nazwa zagrożenia	Strata	Prawdo-podobieństwo	Miara ryzyka	Kategoria ryzyka
ZG-1	Pożar	8	3	24	Średnie
ZG-2	Zalanie	9	3	27	Średnie
ZG-3	Klęska żywiołowa	5	2	10	Niskie
ZG-4	Katastrofa budowlana	9	1	9	Niskie
ZG-5	Oddziaływanie elektromagnetyczne	8	4	32	Średnie
ZG-6	Awaria sprzętu	7	5	35	Średnie
ZG-7	Awaria oprogramowania	6	5	30	Średnie
ZG-8	Przerwy w zasilaniu	7	7	49	Średnie
ZG-9	Awaria łączności	7	3	21	Średnie
ZG-10	Uszkodzenie nośników	9	7	63	Wysokie
ZG-11	Braki organizacyjne	7	6	42	Średnie
ZG-12	Przypadkowe działania	6	5	30	Średnie
ZG-13	Błędy oprogramowania	7	6	42	Średnie
ZG-14	Złośliwy kod	8	7	56	Średnie
ZG-15	Podsłuch	8	7	56	Średnie
ZG-16	Złamanie hasła	9	5	45	Średnie
ZG-17	Braki personelu	7	7	49	Średnie
ZG-18	Nieświadomość pracownika	9	8	72	Wysokie
ZG-19	Przekroczenie kompetencji	9	5	45	Średnie
ZG-20	Niestosowanie się do regulaminów	8	8	64	Wysokie
ZG-21	Uchybienia proceduralne	7	7	49	Średnie
ZG-22	Sabotaż	9	4	36	Średnie
ZG-23	Kradzież	9	9	81	Maksymalne
ZG-24	Wtargnięcie	9	9	81	Maksymalne
ZG-25	Socjotechnika	8	5	40	Średnie

Źródło: opracowanie własne na podstawie danych źródłowych przedsiębiorstwa

Przeprowadzona analiza ryzyka wskazuje na podstawowe wymagania w zakresie ochrony informacji przedsiębiorstwa. W oparciu o zaprezentowane w tab. 3 wyniki można stwierdzić, iż największe zagrożenie utraty bezpieczeństwa informacji wiąże się z wtargnięciem oraz kradzieżą dokumentów, sprzętu czy też nośników danych. Wysoki poziom ryzyka oszacowany został dla takich zagrożeń, jak: uszkodzenie nośników, nieświadomość pracowników, niestosowanie się do regulaminów. Z przeprowadzonych badań wynika zatem, że najsłabszym ogniwem w systemie bezpieczeństwa informacji w badanym przedsiębiorstwie jest czynnik ludzki, i to właśnie ten obszar bezpieczeństwa wymaga szczegółowej analizy oraz zaimplementowania działań profilaktycznych i kontrolnych. Dlatego też budowanie skutecznego systemu ochrony informacji wymaga obok wdrażania nowych zabezpieczeń także podnoszenia ogólnej świadomości pracowników w zakresie bezpieczeństwa informacji, np. za pośrednictwem cyklicznie organizowanych szkoleń.

W tabeli 4 zaprezentowano przykładowe rozwiązania techniczne i organizacyjne mające na celu obniżenie wszystkich oszacowanych dla badanego przedsiębiorstwa ryzyk do poziomu akceptowalnego.

Tab. 4. Środki i zabezpieczenia wdrożone w badanym przedsiębiorstwie

Numer zagrożenia	**Nazwa zagrożenia**	**Wdrożone środki i zabezpieczenia**
ZG-1	Pożar	Sprzęt i jego otoczenie powinny zostać należycie zabezpieczone przed rozprzestrzenianiem się ognia; należy wdrożyć środki utrudniające zaprószenie ognia oraz zabezpieczenia przeciwpożarowe (czujki ognia i dymu, alarmy, środki gaszące)
ZG-2	Zalanie	Najważniejsze urządzenia i nośniki danych powinny być zlokalizowane w miejscach, które nie są szczególnie narażone na wyciek wody bądź innych płynów
ZG-3	Klęska żywiołowa	Należy wykonywać kopie zapasowe, które powinny być przechowywane poza terenem przedsiębiorstwa
ZG-4	Katastrofa budowlana	Należy wykonywać kopie zapasowe, które powinny być przechowywane poza terenem przedsiębiorstwa
ZG-5	Oddziaływanie elektromagnetyczne	Należy zastosować właściwe uziemienie, separację urządzeń, ekranowanie okablowania

Numer zagrożenia	Nazwa zagrożenia	Wdrożone środki i zabezpieczenia
ZG-6	Awaria sprzętu	Należy wdrożyć procedury dokonywania okresowych przeglądów i konserwacji sprzętu IT oraz wprowadzić procedury reagowania na incydenty
ZG-7	Awaria oprogramowania	Oprogramowanie przed jego wdrożeniem do eksploatacji powinno zostać poddane dokładnym testom. Należy systematycznie monitorować zmiany oprogramowania oraz raportować osobie odpowiedzialnej wszystkie nieprawidłowe działania oprogramowania
ZG-8	Przerwy w zasilaniu	Należy dokonywać systematycznej konserwacji i przeglądów awaryjnych źródeł zasilania (UPS-ów), mechanizmów zwalniania zwór elektromagnetycznych itp.
ZG-9	Awaria łączności	Należy starannie rozmieścić i rozłożyć okablowanie oraz zastosować zabezpieczenia fizyczne chroniące przed przypadkowym bądź umyślnym uszkodzeniem. W uzasadnionych przypadkach należy zastosować zabezpieczenia przed podsłuchem. Ponadto należy prawidłowo eksploatować i utrzymywać sprzęt sieciowy, aby uniknąć błędów transmisji
ZG-10	Uszkodzenie nośników	Należy przechowywać nośniki pamięci tak, aby uniknąć wpływu szkodliwych czynników środowiskowych oraz czynników zewnętrznych, które mogą spowodować ich uszkodzenie. Należy wprowadzić procedury bezpiecznego przekazywania i zbywania nośników pamięci
ZG-11	Braki organizacyjne	Polityka bezpieczeństwa informacji firmy oraz pozostałe dokumenty związane z bezpieczeństwem powinny być systematycznie monitorowane oraz aktualizowane
ZG-12	Przypadkowe działania, błędy użytkowników	Należy wprowadzić cykliczne szkolenia użytkowników, z zakresu prawidłowego korzystania ze środków teleinformatycznych i unikania błędów z tym związanych. Personel powinien systematycznie otrzymywać instrukcje i inne materiały podnoszące jego świadomość bezpieczeństwa

Numer zagrożenia	Nazwa zagrożenia	Wdrożone środki i zabezpieczenia
ZG-13	Błędy oprogramowania	Oprogramowanie przed jego wdrożeniem do eksploatacji powinno zostać poddane dokładnym testom. Należy systematycznie monitorować zmiany oprogramowania oraz raportować osobie odpowiedzialnej wszystkie nieprawidłowe działania oprogramowania
ZG-14	Złośliwy kod	Należy stosować skanery celem wykrycia i usunięcia szkodliwego oprogramowania – najlepszym rozwiązaniem są skanery pracujące on-line, które gwarantują wykrycie i ewentualne usunięcie szkodliwego oprogramowania zanim zostanie zainfekowany i uszkodzony system. Skanery powinny być stale aktualizowane. Należy opracować wytyczne ograniczające ryzyko wprowadzenia szkodliwego oprogramowania (np. zakaz uruchamiania gier i innych programów, sprawdzanie plików nieznanych typów) oraz organizować systematyczne szkolenia z zakresu procedur i wskazówek związanych z ochroną przed szkodliwym oprogramowaniem.
ZG-15	Podsłuch	Należy zastosować taką konstrukcję pokoi, ścian pomieszczeń, budynku, która znacznie utrudni bądź uniemożliwi podsłuch. Należy zastosować właściwe uziemienie, separację urządzeń, ekranowanie okablowania
ZG-16	Złamanie hasła	Należy kontrolować przydzielanie haseł oraz ich regularną zmianę. Użytkownicy powinni zostać zaznajomieni z zasadami tworzenia bezpiecznego hasła. Postuluje się wdrożenie oprogramowania ograniczającego stosowanie pospolitych haseł. Kopie haseł powinny zostać zdeponowane w bezpieczny sposób.
ZG-17	Braki personelu	Należy wdrożyć właściwą politykę kadrowo-finansową, przeszkolić dodatkowe osoby funkcyjne celem zastąpienia etatowego personelu
ZG-18	Nieświadomość pracownika	Każdy pracownik powinien być świadomy swojej odpowiedzialności i roli w utrzymaniu bezpieczeństwa. Należy systematycznie organizować szkolenia dla personelu podnoszące świadomość bezpieczeństwa informacji w firmie. Szkolenia takie muszą być obowiązkowe, a obecność na nich pracowników dokumentowana.

Numer zagrożenia	Nazwa zagrożenia	Wdrożone środki i zabezpieczenia
ZG-19	Przekroczenie kompetencji	Pracownicy powinny być świadomi konsekwencji naruszenia postanowień polityki bezpieczeństwa informacji, polityki bezpieczeństwa teleinformatycznego oraz innych związanych z bezpieczeństwem dokumentów. Należy regularnie weryfikować i uaktualniać przyznawane prawa dostępu. Trzeba dokonywać kontroli uprawnień personelu, aby upewnić się, że nie są one nadużywane. Ponadto prawa dostępu powinny być wycofywane, gdy nie są już potrzebne
ZG-20	Niestosowanie się do regulaminów	Należy wprowadzić restrykcje za nieprzestrzeganie zasad obowiązujących w firmie regulaminów i procedur, zapoznać z nimi personel oraz bezwarunkowo stosować je wobec pracowników
ZG-21	Uchybienia proceduralne	Należy wprowadzić restrykcje za nieprzestrzeganie zasad obowiązujących w firmie regulaminów i procedur, zapoznać z nimi personel oraz bezwarunkowo stosować je wobec pracowników
ZG-22	Sabotaż	Należy wprowadzić restrykcje za nieprzestrzeganie zasad obowiązujących w firmie regulaminów i procedur, zapoznać z nimi personel oraz bezwarunkowo stosować je wobec pracowników
ZG-23	Kradzież	Należy oznakować posiadany sprzęt, umożliwiając w ten sposób jego lokalizację. Wprowadzić procedury przechowywania i udostępniania dokumentów zawierających wrażliwe informacje oraz procedury dotyczące kontroli dostępu do określonych pomieszczeń i stref ochronnych
ZG-24	Wtargnięcie	Należy wdrożyć stosowne środki ochrony fizycznej – w szczególności środki kontroli dostępu. Należy zobligować pracowników pionu ochrony do przeprowadzania systematycznych kontroli
ZG-25	Socjotechnika	Każdy pracownik powinien być świadomy swojej odpowiedzialności i roli w utrzymaniu bezpieczeństwa. Należy systematycznie organizować szkolenia dla personelu podnoszące świadomość bezpieczeństwa informacji w firmie

Źródło: opracowanie własne na podstawie danych źródłowych przedsiębiorstwa

Podsumowanie

Zarządzanie ryzkiem pełni szczególną rolę w procesie kształtowania systemu bezpieczeństwa informacji w organizacji. Umożliwia ono identyfikację różnego rodzaju zagrożeń determinujących utratę poufności, integralności i dostępności informacji, oszacowanie wielkości strat oraz prawdopodobieństwa ich wystąpienia w konkretnej jednostce gospodarczej. Ponadto nieodzownym elementem zarządzania ryzkiem jest jego akceptacja oraz wybór odpowiedniej strategii postępowania z ryzkiem.

Literatura przedmiotu wskazuje na trzy podstawowe strategie: ignorowanie występowania ryzyka, transferowanie ryzyka bądź jego redukcja do poziomu akceptowanego (ryzyko rezydualne).

W przypadku omawianego przedsiębiorstwa, w reakcji na oszacowane ryzyko kierownictwo podjęło decyzję o redukcji wartości poszczególnych podatności poprzez zastosowanie właściwych zabezpieczeń, adekwatnych do bieżących i przyszłych zagrożeń, zgodnych z przyjętymi wymogami bezpieczeństwa.

Literatura

[1] Anzel M., Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dn. 5 sierpnia 2010 r. o ochronie informacji niejawnych, PHU One, Poznań 2011.
[2] http://www.computerworld.pl/artykuly/318160/Zarzadzanie.ryzykiem.bezpieczenstwa.informacji.w.systemach.TI.html
[3] Janczak J., Nowak A., Bezpieczeństwo informacyjne. Wybrane problemy, Akademia Obrony Narodowej, Warszawa 2013.
[4] Łuczak J., Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001, Zeszyty Naukowe, Akademia Morska w Szczecinie, Nr 19(91) 2009.
[5] Łuczak J., Tyburski M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Uniwersytet Ekonomiczny w Poznaniu, Poznań 2010.
[6] Nowak A., Scheffs W., Zarządzanie bezpieczeństwem informacyjnym, Wyd. AON, Warszawa 2010.
[7] PN-I-13335-1: 1999, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – pojęcia i modele bezpieczeństwa systemów informatycznych, PKN, Warszawa 1999.
[8] PN-ISO/IEC 27005:2010 Technika informatyczna – techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

[9] Prauzner T., Prawo a bezprawie w Internecie [w:] Prace Naukowe Akademii im. Jana Długosza w Częstochowie, Tom IV, AJD, red. A. Gil, Częstochowa 2009.
[10] Prauzner T., Technologia informacyjna – wybrane problemy społeczne, [w] Edukacja-Technika-Informatyka nt: „Wybrane problemy edukacji informatycznej i informacyjnej", Rocznik Naukowy Nr 3/2012 cz.2, red. dr hab. prof. UR Walat W., FOSZE, Rzeszów 2012.
[11] Sasor T., Ryzyko i polityka bezpieczeństwa w przedsiębiorstwie wirtualnym [w:] Kisielnicki J., Grabara J.K., Nowak J.S., Informatyka i współczesne zarządzanie, Polskie Towarzystwo Informatyczne, Katowice 2005.