SZACOWANIE RYZYKA UTRATY BEZPIECZEŃSTWA INFORMACJI NA PRZYKŁADZIE WYBRANEJ JEDNOSTKI GOSPODARCZEJ

Estera PIETRAS

Streszczenie: Artykuł dotyczy analizy szacowania ryzyka utraty bezpieczeństwa informacji zgodnego z normą PN-I_13335-1:1999, gdzie zawarte są wytyczne zarządzania bezpieczeństwem systemów informatycznych. Omówiono znaczenie bezpieczeństwa informacji, zarządzania ryzykiem oraz podkreślono znaczenie ryzyka. Przedstawiono przykład oceny ryzyka przy zastosowaniu metody prawdopodobieństwa i skutku określona definicją ryzyka, w konkretnym przedsiębiorstwie. Zaprezentowano także wyniki badań empirycznych przeprowadzonych w oparciu o metodę ankietowania.

Słowa kluczowe: zarządzanie ryzykiem, identyfikacja ryzyka

1. Wstęp

Rewolucja informacyjna naszego pokolenia jest tym, czym dla naszych pradziadków rewolucja przemysłowa. Ciąg zmian, których doświadczamy ma ogromny wpływ na otaczającą nas rzeczywistość. Tworzenie się społeczeństwa informacyjnego obserwuje większość ludzi na Ziemi. Uświadomienie sobie, że decyzje, jakie podejmujemy, są wynikiem posiadanych informacji sprawiło, że trudno sobie wyobrazić przedsiębiorstwo bez sprawnego systemy informatycznego [1]. Szeroko pojmowana niezawodność i bezpieczeństwo systemu informacyjnego mają podstawowe znaczenie w przedsiębiorstwie. Większość informacji posiadanych przez przedsiębiorstwo jest przechowywana w formie elektronicznej, np.: na serwerach. Jednak należy stwierdzić że popularność systemów informatycznych sprawiła, iż nie są one wolne od niebezpieczeństw, przybierających coraz to nowe formy. Konsekwencje dla przedsiębiorstwa mogą być bardzo znaczące - począwszy od utraty dobrego wizerunku czy wiarygodności, po utratę płynności finansowej, generując przy okazji kolosalne straty czy wręcz konsekwencje prawne [17]. W dobie rozwoju technologii komputerowej, gdzie wszyscy powinni czuć się bezpiecznie, codziennością stały się wycieki nieodpowiednio chronionej informacji, wynikające ze szpiegostwa przemysłowego, włamań hakerów do systemów komputerowych, podsłuchu, kradzieży tożsamości lub tym podobne. Koniecznością stało się więc nie tylko pozyskiwanie, przetwarzanie ale przede wszystkim zagwarantowanie należytego poziomu bezpieczeństwa informacji. Wiąże się to z określonymi procedurami postepowania wynikającymi z wymiany informacji, magazynowania jej, oraz implementacji skutecznych rozwiązań zabezpieczeń. W każdym jednak przypadku zostaje ryzyko, którego nie da się całkowicie wyeliminować i które jest na stałe wpisane w działalność organizacji.

2. Techniczne bezpieczeństwo informacji a ryzyko ujawnienia lub zniszczenia wiadomości

W dobie gdzie komunikowanie odbywa się za pomocą środków przekazu w sposób

błyskawiczny, współczesne przedsiębiorstwo jest zobligowane do dbania o swoje informacje, gdyż mogą one w znaczący sposób zaważyć na konkurencyjności wobec innych podmiotów na rynku. Ochrona informacji to nie tylko działanie organizacyjno-techniczne, którego głównym zadaniem jest kontrola dostępu danych ale także zarządzanie informacjami oraz zasobami informatycznymi. Bezpieczeństwo informacji to już nie tylko norma i wymóg czasu ale obowiązek każdej organizacji będącej w posiadaniu informacji. Wymogi prawa nakładają na zarządy organizacji obowiązek podjęcia szeregu działań o charakterze organizacyjno-technicznym z zakresu ochrony przetwarzanych informacji. Dobór zabezpieczeń z uwagi na koszt powinien zostać dobrany stosownie do wartości szkód, które może ponieść firma w sytuacji gdy ich nie zastosuje. Wskazane jest wiec określenie celów bezpieczeństwa w instytucji i jej systemów. Jednym z ważniejszych celów to zidentyfikowanie zasad bezpiecznego przetwarzania informacji, szkolenia, uświadamianie pracowników, monitorowanie aktualnego stanu bezpieczeństwa, doskonalenie systemów bezpieczeństwa. Bezpieczeństwo nie jest więc aktem jednorazowym, lecz bardzo złożonym procesem, wymagającym stałego nadzoru i przystosowania się do zmieniających się warunków otoczenia [11]. Zgodnie z poglądami P. A. Nowickiego bezpieczeństwo procesu informacyjnego jest zapewnione, gdy istnieje możliwość sprawnego i poufnego gromadzenia informacji, ich przetwarzania, przetrzymywania i przesyłania [14]. Zapewnienie opisanego stanu wymaga ciągłego uwzględniania prawdopodobieństwa zajścia niekorzystnych zdarzeń np.: kradzież danych. Rosnąca konkurencja spowodowała, że informacja stała się dla przedsiębiorstw czynnikiem istotniejszym niż zasoby materialne. Przedsiębiorstwa handlowe, które posiadają patenty, tajemnice technologii produkcji, zdają sobie sprawę z nieodwracalnych konsekwencji utraty takich informacji.

Ryzyko towarzyszy każdej działalności prowadzonej przez człowieka i każdej decyzji przez niego podjętej. Norma PN-I-02000:2002 definiuje ryzyko jako „możliwość, że konkretne zagrożenie wykorzysta konkretną podatność w systemie przetwarzania danych”[2]. Ryzyko związane jest z prawdopodobieństwem zaistnienia określonej możliwości, w której podatność zasobu zostanie wykorzystana w celu stworzenia zagrożenia, co może spowodować jego utratę i w rezultacie niekorzystnie wpłynąć na funkcjonowanie przedsiębiorstwa. Ryzyko określane jest jako iloczyn prawdopodobieństwa wystąpienia niepożądanego zdarzenia i wielkości strat, które występują w danym zdarzeniu. Dlatego każda zmiana podatności, może mieć znaczny wpływ na ryzyko. Powyższą zależność opisuje wzór [3].

$$R=P*S \tag{1}$$

gdzie:

R – ryzyko,
P – prawdopodobieństwo zagrożenia,
S – skutek, straty.

Graficzną interpretację ryzyka przedstawia rysunek 1, z którego wynika że, ryzyko jest zbiorowym elementem prawdopodobieństwa i strat. Ryzyko jest tym większe im większy jest jego obszar.

Rys. 1. Interpretacja ryzyka [13]

Można więc wyciągnąć wniosek, że ryzyko może być wyliczone i ma konkretną wartość, która w dobrze funkcjonującej organizacji powinna być uwzględniona. Ryzyko jest wspólnym obszarem strat i prawdopodobieństwa. Podejście takie wymaga od organizacji porównania wartości ryzyka z możliwością pokrycia prawdopodobnych strat wynikających z urzeczywistnienia się tego ryzyka. W zależności od otrzymanego wyniku organizacja powinna określić strategię działania i politykę postępowania w zakresie zarządzania ryzykiem. Profil ryzyka każdej organizacji jest inny i wymaga dostosowania metody łagodzenia go. Zależy to od specyfiki korzystania z systemów informacyjnych oraz woli i zdolności organizacji do przeciwdziałania ryzyku w przyszłości. Oznacza to że nie ma jednego poprawnego podejścia do przeciwdziałania ryzyku. Rysunek 2 pokazuje proces postepowania z ryzykiem.

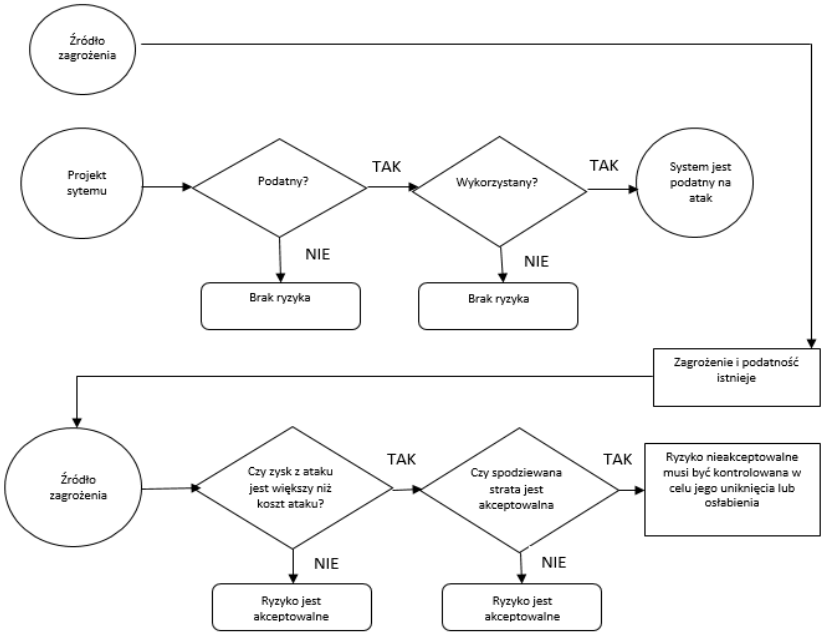
Niezbędne są rozwiązania systemowe dotyczące kontroli ryzyka w celu jego uniknięcia lub osłabienia. Aby organizacja uzyskała stabilną pozycję biznesową na rynku, zobowiązana jest redukować ryzyko nieuprawnionego ujawnienia informacji. Powinien być to główny cel projektu, do którego zamierza przedsiębiorstwo. Utrata istotnych informacji lub niepoprawne zarządzanie nimi może być powodem utraty stabilności ekonomiczno-finansowej przedsiębiorstwa.

Ponieważ ryzyko jest funkcją konsekwencji, która następuje w wyniku niepożądanego zdarzenia i prawdopodobieństwem zajścia określonego zdarzenia, to szacowanie ryzyka polega na:

a) Analizie ryzyka obejmującej:
- identyfikację ryzyka,
- wycenę ryzyka,

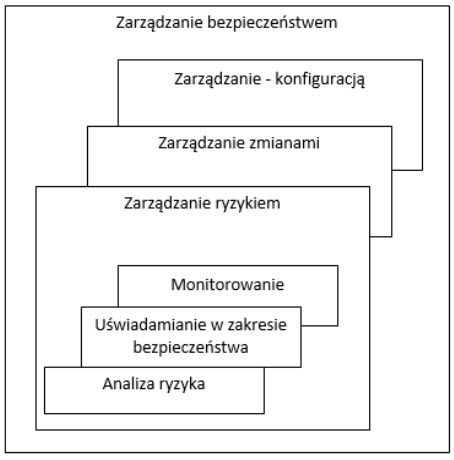
b) Ocenie ryzyka.

Szacowanie ryzyka określa wartość zasobów informacyjnych, rozpoznaje zagrożenia i występujące podatności, wskazuje istniejące środki kierowania bezpieczeństwem i ich wpływ na zidentyfikowanie ryzyka. W przyszłości aby szacowanie ryzyka było skuteczne, powinno mieć się jasno zdefiniowany zakres w odniesieniu do ustalenia poziomu ryzyka w innych obszarach [3]. Wybór zastosowania zabezpieczeń powinien ściśle odpowiadać wynikom szacowania i postępowania z ryzykiem, wymaganiach prawnych, wymaganiach nadzoru. Stąd podstawą do budowania systemu zarządzania bezpieczeństwa informacji jest szacowanie ryzyka [10]. M.E. Whitman zwraca uwagę na wzajemną relację między



Rys. 2. Proces postepowania z ryzykiem [10]

szacowaniem ryzyka, a jego osłabieniem. Proces ten nazywamy jest zarządzaniem ryzykiem [6]. Ustawa o finansach publicznych z dnia 27 sierpnia 2009 określa zarządzanie ryzykiem, jako jeden z elementów kontroli zarządczej, definiowanej jako ogół działań zapewniających realizację celów i zadań w sposób zgodny z prawem , efektywny i terminowy [12]. Zarządzanie ryzykiem uwzględnia poszczególne elementy całościowego procesu, a nie pojedynczego etapu. W działalności gospodarczej zarządzanie ryzykiem stanowi identyfikację zagrożeń mogących spowodować realne zagrożenie dla zysku finansowego przedsiębiorstwa, a także zaplanowanie zabezpieczeń charakterystycznych dla zaistniałego ryzyka [16].



Rys. 3. Zarzadzanie bezpieczeństwem [10]

O skutecznym zarządzaniu ryzykiem można mówić wtedy gdy podejmowane są zdecydowane działania związane z ciągłym monitorowaniem i analizą ryzyk coraz to nowszych zagrożeń i podatności. Będzie miało to na celu zmniejszenie prawdopodobieństwa zaistnienia zagrożenia w przedsiębiorstwie oraz ograniczenie jej skutków. Istotnym czynnikiem podejmując decyzję będzie zarówno zminimalizowanie strat jak również wyprzedzenie przyszłych zdarzeń. Aby nie dopuścić do sytuacji utraty wiarygodności przedsiębiorstwa należy prawidłowo opracować i wdrożyć system zarządzania bezpieczeństwem informacji z uwzględnieniem wpływających na nie czynników zagrożenia [17]. Pierwszą grupą zagrożeń występujących w procesie przetwarzania informacji i jej przesyłania to, zagrożenia wynikające z braku stosowania odpowiedniej polityki bezpieczeństwa, braku odpowiednio zastosowanego systemu zarzadzania bezpieczeństwem informacji wszystkich posiadanych aktywów w przedsiębiorstwie. Sposobem na ograniczenie tych zagrożeń jest wdrożenie systemu przedstawionego w normie PN-ISO/IEC 27001. Drugą grupą zagrożeń można określić zagrożenia techniczne, wynikające ze źle skonfigurowanego i wyposażonego systemu informatycznego. Taki system nie będzie funkcjonował prawidłowo w wyniku czego może spowodować awarie systemu komputerowego. Ten rodzaj zagrożeń można zminimalizować poprzez prawidłowe wdrożenie normy IEC 61508 oraz jej pochodnych; IEC 61511 oraz IEC 61515 w zależności od przedsiębiorstwa [17].

Nie istnieje jeden idealny sposób na przeprowadzenie analizy ryzyka. To rodzaj działalności dyktuje wybór strategii bezpieczeństwa informacji. Aby móc zapewnić przedsiębiorstwu odpowiedni poziom bezpieczeństwa, konieczna jest więc szczegółowa analiza wszystkich narażonych na niebezpieczeństwo zasobów w funkcjonującym przedsiębiorstwie, uwzględniając zagrożenia [17]. Analiza ryzyka jest więc niezbędna w zakresie precyzyjnego zidentyfikowania zagrożenia dla bezpieczeństwa informacji i jego słabego punktu, który może wystąpić w danej organizacji.

4. Badania własne

Przedstawione odejście pozwala zarówno zidentyfikować rodzaje ryzyka na podstawie potencjalnych zagrożeń, jak i poznać techniki ich łagodzenia. Właściwe zrozumienie wymagań przez kierownictwo wpłynie na podjęcie właściwych decyzji w ramach zarządzania ryzykiem. Na konkretnym przedsiębiorstwie została przeprowadzona analiza ryzyka utraty bezpieczeństwa informacji. Przedsiębiorstwo to zajmuje się wyrobem taśm transporterowych, do wszystkich branż przemysłowych oraz sit i siatek z drutu. Te ostatnie znajdują zastosowanie w przemyśle wydobywczym, spożywczym, gastronomicznym, elektronicznym, chemicznym, motoryzacyjnym. Ponieważ firma współpracuje od lat ze znanymi producentami w wielu gałęziach gospodarki, szczególnie zależy jej na zachowaniu odpowiedniego poziomu bezpieczeństwa informacji. Badana firma istnieje na rynku od roku 1957 z pełnym sukcesem biznesowym. Przeprowadzenie badań obejmowało dostarczenie osobiście 60 kwestionariuszy ankiet. Kwestionariusz ankiety składał się z 15 pytań dla badanej grupy respondentów. Był on anonimowy co zwiększyło prawdopodobieństwo udzielenia trafnych odpowiedzi. Po upływie terminu 9dni, nastąpiło zbieranie kwestionariuszy ankiet. Otrzymane wyniki badań pozwoliły sformułować wnioski na temat tego, jaka jest wiedza respondentów w zakresie analizy ryzyka bezpieczeństwa informacji. W artykule zamieszczono tylko wybrane wyniki badań. Parametry doboru poszczególnych wskaźników ilościowych zaprezentowano w tabeli od 1 do 5. W organizacji przeprowadzono analizę ryzyka polegającą na przeanalizowaniu

prawdopodobieństwa i skutku, opisującą definicję ryzyka. Analiza pozwoliła na określenie czynników które mają znaczny wpływ na jakość procesów zarządzania bezpieczeństwem informacji. Badania pokazały że należy zastosować środki ochronne. Tabela 4 reprezentuje otrzymane wyniki.

Tab. 1. Parametry dla wskaźnika koszt- skutek

Ocena	**Charakterystyka znaczenia**	
1	Bardzo mały	Wada nie wpływa na funkcjonowanie firmy
2	Mały	Wada wywołuje nieznaczne utrudnienia w funkcjonowaniu przedsiębiorstwa
3	Średni	Wada jest zauważalna i powoduje utrudnienia w systemie bezpieczeństwa informacji
4	Duży	Wada powoduje znaczne utrudnienia w systemie bezpieczeństwa informacji czego wynikiem są zakłócenia w przedsiębiorstwie
5	Bardzo duży	Wada wywołuje ogromne straty finansowe w przedsiębiorstwie

Tab. 2. Parametry dla wskaźnika prawdopodobieństwo

Ocena	Poziom prawdopodobieństwa	Charakterystyka
1	Bardzo rzadko	Zdarzenie wykrycia 1x na 5lat
2	Rzadko	Zdarzenie wykrycia 1x na 3lata
3	Umiarkowanie	Zdarzenie wykrycia 1x1 w roku
4	Często	Zdarzenie wykrycia 1x w miesiącu
5	Bardzo często	Zdarzenie wykrycia 1x na tydzień

Identyfikację zagrożeń wskazał sam autor artykułu na podstawie [14].

Tab. 3. Identyfikacja zagrożeń w badanej jednostce.

Zagrożenia			
Nazwa zagrożenia		Przyczyna	Skutek
1	Kradzież danych	Brak zabezpieczeń	Wydostanie się danych do konkurencji. Utrata konkurencyjności
2	Włamania do systemu komputerowego	Ignorowanie zasady korzystania z poczty elektronicznej. Instalowanie nielegalnego oprogramowania.	Brak zaufania kontrahentów. Kradzież danych.
3	Nieprzestrzeganie regulaminu obowiązującego w firmie	Brak zrozumienia przepisów. Nieprzestrzeganie regulaminów.	Narażenie danych na utratę, zmodyfikowanie.
4	Przekroczenie uprawnień	Pochopne wydawanie uprawnień w systemach informatycznych. Brak wyciągania konsekwencji za przekroczenie uprawnień	Nieuprawniony dostęp do informacji w wyniku tego straty finansowe firmy.
5	Awaria sprzętu	Kupno uszkodzonego sprzętu. Nieumiejętne użytkowanie.	Ograniczony dostęp do danych organizacji. Zakłócenia w procesie realizacji procesów
6	Złamanie haseł	Nieprzestrzeganie zasad czystego biurka i pulpitu. Niewłaściwe tworzenie zasad.	Upowszechnianie haseł. Kradzież danych.

7	Kradzież nośników danych, dokumentów	Wynoszenie danych, nośników poza siedzibę firmy. Kontrahenci pozostawieni bez opieki .	Wyciek informacji do firm konkurencyjnych, w wyniku tego straty finansowe.
8	Awaria łączności systemu komputerowego	Nieodpowiednie użytkowanie systemu. Brak legalnego oprogramowania. Uszkodzenie podzespołów.	Zakłócenia związane z komunikacją. Brak możliwości poprawnej realizacji procesów
9	Nieprawidłowe działania oprogramowania	Brak odpowiedniego nadzoru nad oprogramowaniem. Nieumiejętne korzystanie z oprogramowania.	Przekłamanie w działaniu, zapisywaniu, i przetwarzaniu informacji.
10	Odtworzenie danych z odnalezionych nośników danych	Zagubienie, zniszczenie, nośników informacji.	Modyfikacja, nie kontrolowane rozpowszechnienie danych.
11	Nieodpowiednie przygotowanie umowy z personelem i kontrahentami firmy i dostawcami	Brak świadomości zarządu	Wykorzystanie informacji w wyniku tego utrata pozycji na rynku.
12	Brak zapewnienia bezpieczeństwa informacji w przedsiębiorstwie	Niedobór informacji w świadomości opracowania planu bezpieczeństwa informacji	Wyciek i kradzież informacji .Narażenie aktywów informatycznych na ich utratę.
13	Brak szkoleń dla kadry pracowników z zakresu bezpieczeństwa informacji	Brak świadomości kierownictwa. Brak finansów	Nieświadome narażenie danych na ich utratę.
14	Wykorzystanie informacji udostępnionych w firmie	Brak świadomości kierownictwa. Brak finansów	Utrata pozycji na rynku, w wyniku czego utrata części klientów

Źródło Opracowanie własne na podstawie wyników badań ankietowych

Tab. 4. Wyniki obliczeń szacowania ryzyka w badanej jednostce organizacyjnej.

Szacowanie ryzyka				
Numer	Nazwa zagrożenia	Skutek	Prawdopodobieństwo	Miara ryzyka
1	Kradzież danych	3.88	1.95	7.57
2	Włamania do systemu komputerowego	3.91	2.55	9.98
3	Nieprzestrzeganie regulaminu obowiązującego w firmie	2.12	1.39	2.95
4	Przekroczenie uprawnień	3.91	4.16	16.26
5	Awaria sprzętu, awaria podzespołów	1.65	0.89	1.47
6	Złamanie haseł	4.37	4.58	20.01
7	Kradzież nośników danych, dokumentów	3.96	3.58	14.18
8	Awaria łączności(systemu komputerowego)	1.56	1.17	1.83
9	Niewłaściwe działania oprogramowania	0.97	0.45	0.44

10	Odtworzenie danych z odnalezionych nośników danych	4.07	4.9	19.94
11	Nieodpowiednie przygotowanie umowy z personelem i kontrahentami firmy i dostawcami	1.71	3.42	5.85
12	Brak zapewnienia bezpieczeństwa informacji w przedsiębiorstwie	4.28	3.79	16.22
13	Brak szkoleń dla kadry pracowników z zakresu bezpieczeństwa informacji	3.54	1.78	6.30
14	Wykorzystanie informacji udostępnionych w firmie	2.54	2.96	7.52

Źródło Opracowanie własne na podstawie wyników badań ankietowych

Tab. 5. Propozycja działań ustalających postępowanie z ryzykiem

Działania korygujące		
	Nazwa zagrożenia	Prawdopodobne działania korygująco- naprawcze
1	Kradzież danych	Monitoring. Nie pozostawianie osób postronnych samych, bez nadzoru i opieki. Należyte niszczenie niepotrzebnych dokumentów.
2	Włamania do systemu komputerowego poprzez nieuprawnione instalowanie aplikacji i oprogramowania	Używanie służbowej poczty tylko do celów firmowych.
3	Nieprzestrzeganie regulaminu obowiązującego w firmie	Zapoznanie całego personelu z obowiązującym regulaminem oraz klientów. Zwolnienia dyscyplinarne na naruszenie zasad bezpiecznej informacji.
4	Przekroczenie uprawnień	Wprowadzenie aktualnie obowiązującego rejestru osób uprawnionych do bazy informacji. Egzekwowanie w razie potrzeby przekroczeń uprawnień.
5	Awaria sprzętu, awaria podzespołów	Wytyczne w zakresie odpowiedzialności pracowników za powierzone im mienie firmy tym samym ograniczając celowe uszkodzenia sprzętu.
6	Złamanie haseł	Dbanie o czystość na biurku, w komputerze na pulpicie. Zakaz pożyczania kart dostępu, identyfikatorów oraz innych dokumentów uwierzytelniających. Właściwe generowanie haseł-trudne dla innych do odgadnięcia.
7	Kradzież nośników danych, dokumentów	Monitoring. Utrudnienie dostępu do pomieszczeń osobom postronnym, lub podejrzanie się zachowujących. Administrator jeszcze większą wagę przykłada do właściwej ochrony danych nośników.
8	Awaria łączności systemu komputerowego	Umiejętne użytkowanie aplikacji, legalne oprogramowanie, zainstalowanie systemów antywirusowych. Dbanie o stan komputera i jego podzespoły.
9	Niewłaściwe korzystanie z oprogramowania	Rozpowszechnienie instrukcji korzystania z danego oprogramowania i ustanowienie stałego nadzoru nad oprogramowaniem.
10	Odtworzenie danych z odnalezionych nośników danych	Nośniki danych należy niszczyć mechanicznie.

11	Nieodpowiednie przygotowanie umowy z personelem i kontrahentami firmy i dostawcami	Przygotować umowę pracownika co do zachowania poufności informacji. Dotyczy to również klientów i dostawców.
12	Brak zapewnienia bezpieczeństwa informacji w przedsiębiorstwie	Uświadomienie kierownictwo i pracowników o monitorowaniu poziomu bezpieczeństwa.
13	Brak szkoleń dla kadry pracowników z zakresu bezpieczeństwa informacji	Inwestowanie w szkolenia kadry pracowniczej.
14	Wykorzystanie informacji udostępnionych w firmie	Uświadamianie zarówno właściciela organizacji jak i klientów o zagrożeniach wynikających z przetwarzania informacji. Wprowadzenie klauzul o zachowanie poufności.

Literatura podaje wiele działań korygująco-naprawczych. Tabela 5 podane propozycje które mogą posłużyć przy wyborze zabezpieczeń przez kierownika jednostki organizacyjnej. Analizując tabelę można stwierdzić, że wybrane przez respondentów zagrożenie jakim jest łamanie haseł, można naprawić dokonując zmian w zakresie dbania o czystość biurka, czystość w komputerze na pulpicie. Jednocześnie kluczową rolę w bezpieczeństwie informacji odegrał zakaz pożyczania kart dostępu, identyfikatorów oraz innych dokumentów uwierzytelniających tożsamość. Istotnym czynnikiem naprawczym jest też właściwe generowanie haseł-trudnych dla innych do odgadnięcia.

5. Podsumowanie

Nie ulega dziś wątpliwości, że w każdym przedsiębiorstwie istnieją zasoby, które należy chronić, niezależnie od tego czy są to zasoby materialne, czy niematerialne. Dużo prostsze jest ustanowienie zabezpieczeń dla zasobów materialnych. Można ustanowić dozór, monitoring służb ochronnych, zastosować urządzenia alarmujące. Trudniejszym jest zabezpieczenie przed niepowołanym dostępem, kradzieżą, zniszczeniem. A jeszcze trudniej zarządzać bezpieczeństwem, zasobami informatycznymi w których strategiczną wartość stanowią aktywa informacyjne. Jednak przedsiębiorstwa które korzystają z odpowiednich metod zabezpieczeń informacji osiągają sukces biznesowy. Organizacje te podeszły priorytetowo do bezpieczeństwa przechowywania, przetwarzania i przesyłania informacji. Ponadto, uwzględniając dynamikę zmian identyfikują zagrożenia informacyjne, używając do tego narzędzia jakim jest analiza ryzyka, która pozwala zlokalizować słabe punkty w systemie bezpieczeństwa informacji. Taka poprawna analiza ryzyka wskaże warunki, jakimi powinien kierować się zorganizowany przedsiębiorca. Przeprowadzona analiza ryzyka utraty bezpieczeństwa informacji na konkretnym przedsiębiorstwie wykazała niedostateczną ochronne. Zlokalizowanie i zidentyfikowanie słabych punktów organizacji pokazało, że narażone jest ono na większe ryzyko utraty poufności, dostępności i integralności informacji. Szacowanie ryzyka pozwoliło na zidentyfikowanie zagrożenia możliwego do wystąpienia, określając rozmiar strat i powstałych szkód. Wyniki badania nasuwają wniosek, że większość osób w badanej grupie ocenę ryzyka traktuje jako charakterystykę zagrożeń. Za największe zagrożenie respondenci uznali, łamanie haseł. A od razu po nim klasyfikuje się odtworzenie danych z odnalezionych nośników danych, a po nim brak zapewnienia bezpieczeństwa informacji w przedsiębiorstwie i kradzież nośników danych, dokumentów. Niewątpliwie te zagrożenia respondenci uznali za realne i

prawdopodobne. Wyniki badania nasuwają wniosek, iż respondenci zdają sobie sprawę z istniejących zagrożeń i realnego prawdopodobieństwa ich wystąpienia. Działania korygująco naprawcze mogą pozwolić na zredukowanie poziomu ryzyka oraz biorąc pod uwagę politykę bezpieczeństwa w organizacji - na ich zaakceptowanie.

Literatura

1. Liedel K., Serafin T.: Otwarte źródła informacji w działalności wywiadowczej. Zarządzanie Bezpieczeństwem Dyfin, Warszawa, 2011.
2. Ludwiszewski B., Redlarski K., Gardzioła T. :Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie w świetle norm PN-ISO/IEC 27001 oraz 61508.Zeszyty naukowe politechniki poznańskiej 2009
3. Jańczak J., Nowak A. : Bezpieczeństwo informacyjne Wybrane problemy. Akademia Obrony Narodowej, Warszawa 2012.
4. Nowicki A., Sitarska M., (red.): Procesy informacyjne w zarządzaniu. UE, Wrocław 2010.
5. PN-I-02000:2002
6. Wołowski F., Zawiła-Niedzwiecki J.: Bezpieczeństwo systemów informacyjnych Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, Wydawnictwo edu-Libri s.c. Kraków 2012
7. Grocki R., :Zarzadzanie kryzysowe. Dobre praktyki. Wydawnictwo Dyfin, Warszawa 2012.
8. Łuczak J., Trybulski M.: Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC27001
9. Whitman M.E., Mattord H.J.:Readings and Cases in the Management of Information Security.Thomas Course Technology.Boston 2006.
10. Ustawa z dnia 27 sierpnia 2009 o finansach publicznych. Przepisy wprowadzające ustawę o finansach publicznych.
11. Wójcik-Mazur A.: Zarządzanie ryzykiem płynności w bankach. Wydawnictwo Politechniki Częstochowskiej 2012
12. Borowiecki R., Romanowska M.: System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa Dyfin Warszawa 2001.
13. Kifner T.: Polityka bezpieczeństwa i ochrony informacji Wydawnictwo Helion 1999.
14. Pałęga M.: Rola czynnika ludzkiego w systemie bezpieczeństwa informacji w przedsiębiorstwie. Praca doktorska Częstochowa 2015.

Mgr inż. Estera PIETRAS
Politechnika Częstochowska
Wydział Inżynierii Produkcji i Technologii Materiałów
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa.
al. Armii Krajowej 19, 42-200 Częstochowa
e-mail estera.pietras@wp.pl