6

MACIERZ RYZYKA JAKO NARZĘDZIE OCENY ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI

6.1 WSTĘP

Od zarania dziejów przesyłanie informacji było jednym z kluczowych warunków prawidłowego zarządzania zarówno państwa jaki i każdej organizacji. W czasach kiedy podstawowym źródłem transferu informacji był list przekazywany przez gońca wystarczyło wpłynąć na osobę przynoszącą informację. Z biegiem czasu zostało opracowane dużo szybsze i bezpieczniejsze metody przesyłania danych, jednak zawsze czynnik był najsłabszym ogniwem całego systemu. Obecnie rozwój systemów teleinformatycznych umożliwia w znacznym stopniu wyeliminowanie tegoż ogniwa. Należy jednak podkreślić że to nadal ludzie są odbiorcami i producentami informacji. Obecnie można wydzielić dwa podstawowe obszary utraty danych. Pierwszym z nich jest celowy atak na system przechowywania informacji poprzez atak na centra danych, drugim jest celowy atak na kadrę pracowniczą wykorzystując do tego celu metodę fishingu. Rozwój teleinformatyki dał więc człowiekowi szereg możliwości celowego działania. Informacja przechowywana w systemach sieciowych należy do jednej z najbardziej narażonych na różnego rodzaju ataki. Dlatego tak ważnym staje się odpowiednie zabezpieczanie informacji w każdym przedsiębiorstwie. Najczęstszymi obecnie metodami wykorzystywanymi przez przestępców są: oszustwa komputerowe, fałszerstwa komputerowe, niszczenie danych lub programów komputerowych, sabotaż komputerowy, włamanie do systemu komputerowego, podsłuch komputerowy. Jeszcze kilkanaście lat temu zapewnienie właściwego poziomu bezpieczeństwa informacji cyfrowej nie było aż tak trudnym zadaniem, jednak w dzisiejszych czasach gdzie większość informacji jest zapisana w formie cyfrowej problem ten nabiera szczególnego znaczenia. Konsekwencje nie należycie prowadzonej polityki bezpieczeństwa mogą być katastrofalne, począwszy od utraty zaufania klientów, pozycji na rynku, płynności finansowej aż po brak konkurencyjności i upadek firmy. W XXI wieku, wieku systemów sieciowych oraz przechowywania danych w chmurach danych hakerzy nie potrzebują dużej ilości sprzętu aby włamać się do systemu informatycznego. Dla dobrego hakera każdy system teleinformatyczny jest tak odporny, podobnie jak łańcuch, jak wytrzymałe jest jego najsłabsze ogniwo.

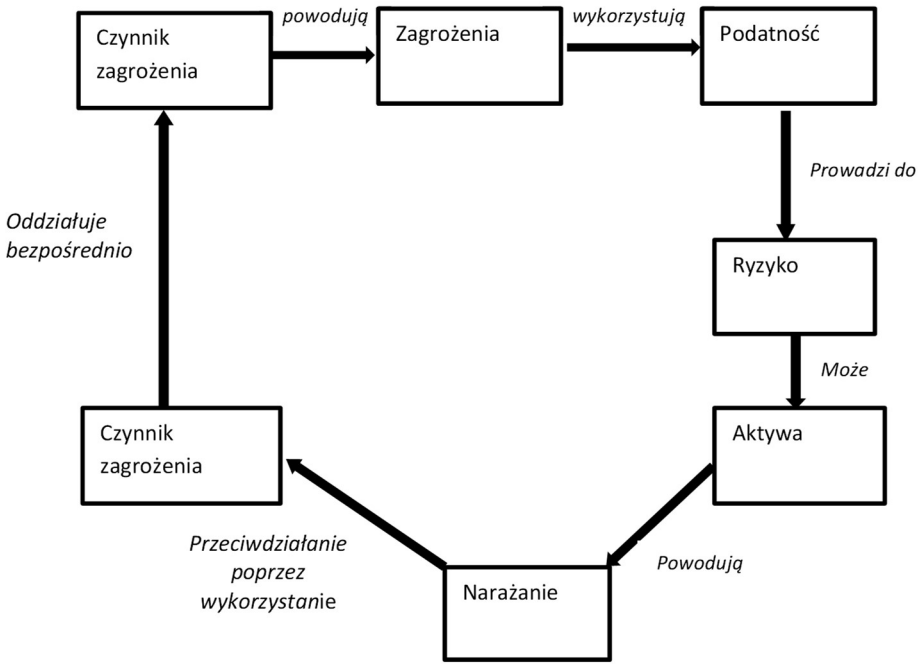
Każdy haker znajdzie taką możliwość prędzej czy później. Nawet coraz bardziej skomplikowane systemy informatyczne, posiadają słabe strony, które pozwalają na dotarcie do informacji osobom postronnym. Widząc więc, jak ogromna jest liczba zagrożeń bezpieczeństwa informacji, winno się odpowiednio oszacować najgroźniejsze obszary ich występowania, stosując odpowiednie procedury, czy też transmisję danych wprowadzając stosowne metody ograniczające zagrożenia zgodne z polityką bezpieczeństwa. Literatura przedmiotu szeroko omawia uregulowania prawne do których należą: akty prawne, normatywne, standardy, reguły i inne metody dotyczące oprogramowania i narządzi elektronicznych.Zatem, wszystkie te czynności powinny przyczynić się do zapewnienia stanu niezagrożenia, spokoju, pewności i poczucia zabezpieczenia, szczególnie co do bezpieczeństwa informacji [7, 10, 15]. Trafny wybór metod ochrony informacji jest również istotny z innego powodu. Od tego zależy efektywność całego systemu bezpieczeństwa. Przy podejmowaniu decyzji w zakresie jego wyboru, warto skorzystać z wiedzy i doświadczenia specjalistów którzy znają możliwości wdrożeniasystemu i są przekonani o sukcesie w zapewnieniu bezpieczeństwa informacji w organizacji.

6.2 ISTOTA I POJĘCIE RYZYKA

Z uwagi na to że każdego dnia podejmujemy różne decyzje, powinniśmy być świadomi podjęcia bezpiecznych postanowień czyli pozbawionych wystąpienia negatywnych konsekwencji ale i ryzykownych decyzji które mogą determinować wiele ujemnych skutków. Zależy to w dużej mierze od stopnia pewności, w jakim podejmowana jest określona decyzja. Wobec tego za tą bezpieczną można uznać, tą która zakłada że wyznaczone założenie zostanie osiągnięte. Natomiast, gdy osiągnięcie założeń jest prawdopodobne to działanie to można nazywamy ryzykownym. Zdecydowana większość osób wybiera mimo wszystko ryzyko umiarkowane nie związane z dużym ryzykiem. Jest to uzależnione od wielkości strat jakie można ponieść, gdy zamierzony cel spełznie na niczym. Decyduje o tym również w znacznym stopniu czas i wysiłek na to poświęcony.

Mimo że pojęcie ryzyka jest znane już od dawien dawna i ma charakter interdyscyplinarny, występujący w każdej fazie życia społecznego, gospodarczego, to jednak nie jest jednoznacznie określony. W języku angielskim *risk* znaczy, możliwość wydarzenia się czegoś niekorzystnego. W języku hiszpańskim *arrisco* można przetłumaczyć na niebezpieczeństwo lub odwagę. Mimo różnej interpretacji językowej definicje te posiadają wspólny mianownik, dotyczą zdarzeń bezpośrednio związanych z zagrożeniem. Jednakże na gruncie nauki właściwe określenie ryzyka jest niezbędne. Ryzyko nie stanowi zagrożenia, ale oznacza że może ono się pojawić. Ryzykiem można nazwać wykorzystanie zagrożenia, towarzyszy każdej działalności człowieka, i decyzji która w przyszłości może mieć niepewny rezultat. Ustawa z dn. 5 sierpnia 2010 roku o ochronie informacji niejawnych wskazuje na definicję ryzyka jako kombinacji prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji. Zatem ryzyko to zespół czynników i działań w wyniku których

następuje szkoda, strata materialna czy inne straty [13]. Natomiast Norma PN-I_13335-1 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych, definiuje ryzyko jako prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów aby spowodować straty [8, 11]. Przez podatność zasobu lub grupy zasobów należy rozumiećsłabość zasobu która może być wykorzystana przez zagrożenie. Do charakterystycznych czynników ryzyka zaliczamy: niepewność, zagrożenie straty, proces podejmowania decyzji. Natomiast poprzez elementy bezpieczeństwa informacji rozumie się ogół aspektów na których oparty jest system zarządzania bezpieczeństwem informacji. Na rysunku 6.1 przedstawiono zależności dotyczące bezpieczeństwa informacji.



Rys. 6.1 Zależności czynników ryzyka

Źródło: opracowanie własne na podstawie [9]

Warto zaznaczyć że wszystkie elementy są wzajemnie ze sobą powiązane. Podatność zasobu lub grupy informuje nas o słabości zasobu lub grupy zasobów.Ważnym czynnikiem w kształtowaniu systemu zarządzania bezpieczeństwem informacji jest analiza ryzyka. Obejmuje ona zestawienia zidentyfikowanych podatności wraz z potencjalnymi zagrożeniami i ich skutkach. Negatywny wpływ zagrożeń, to tak zwane następstwa związane z utratą lub naruszeniem zasobów.Dlatego badanie ryzyka umożliwi wskazanie luk i błędów w systemie bezpieczeństwa które powinny być zweryfikowane przez kierownika czy menadżera firmy. Otrzymane wyniki z szacowania ryzyka pokazują dlaczego należy angażować dodatkowe środki finansowe i dlaczego należy zabezpieczyć aktywa przed utratą poufności, dostępności i integralności. Bez wątpienia wyniki wskazują

kierunki działań pozwalające na zminimalizowanie poziomu ryzyka. Analiza ryzyka jest więc niezbędna w zakresie precyzyjnego zidentyfikowania zagrożeń i słabych punktów które mogą wystąpić w danej organizacji.

6.3 PROCES ZARZĄDZANIA RYZYKIEM W PRZEDSIĘBIORSTWIE

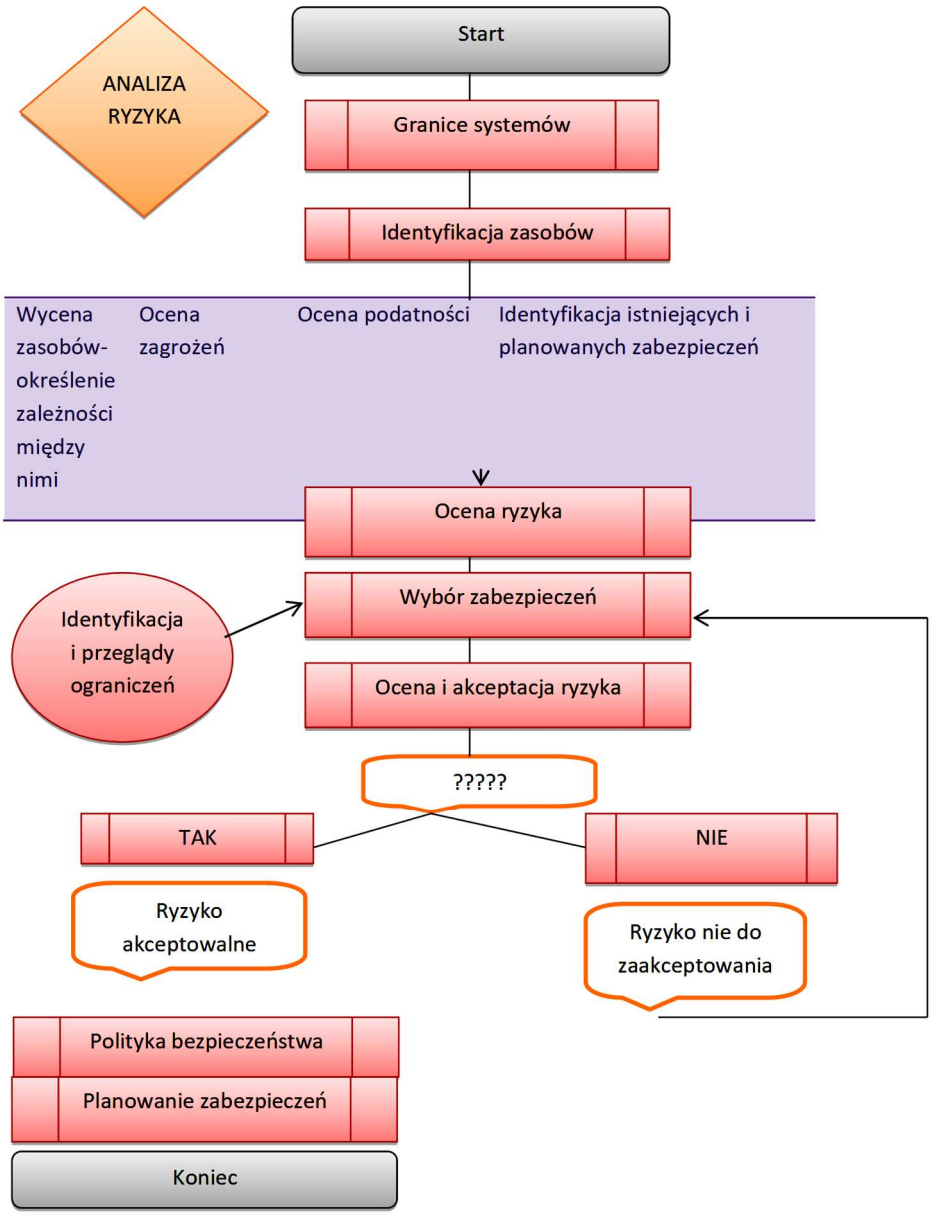
Z uwagi na to że istotne jest rozpoznanie ryzyka oraz jego redukcji, pracodawca zobowiązany jest np: do zapewnienia jak najbezpieczniejszego miejsca pracy, oraz informacji o istniejących zagrożeniach, które mogą zaistnieć podczas wykonywanej pracy. Niezbędne w tym celu jest oszacowanie wielkości ryzyka występującego na danym stanowisku pracy i kolejno wdrożenia zabezpieczeń redukujących ich wielkość do poziomu ryzyka akceptowalnego. Czynność taką określamy mianem zarządzania ryzykiem. Zatem takie podejmowanie działań ma na celu rozpoznanie i ocenę sterowania ryzykiem, jak również kontrolą nad podjętymi działaniami, zmniejszającymi ten stan ryzyka [3]. Według A. Białasa analiza ryzyka systemów teleinformatycznych polega na identyfikacji wszelkich przypadków ryzyka, a następnie określeniu jego wielkości. Można bez wątpienia powiedzieć że sprowadza się to do wykrycia wszelkich potencjalnych zdarzeń, mających negatywny wpływ na funkcjonowanie instytucji, i do określenia możliwości ich wystąpienia. Analizując fakt iż w przedsiębiorstwie występują niekorzystne zdarzenia, to można pokazać następujące czynniki:

- Atrakcyjność zasobu dla potencjalnego intruza.
- Prawdopodobieństwo wystąpienia zagrożenia.
- Łatwość wykorzystania podatności zasobu.

Konstatując, można wyciągnąć wniosek że analiza ryzyka daje pewien uporządkowany obraz zagrożeń, szeregując go wg. szacowanych następstw, oraz możliwości wystąpienia w przedsiębiorstwie, wytyczając kierunki i priorytety wyboru odpowiednich narzędzi.

Interpretując rysunek 6.2 można ustalić, że analiza ryzyka obejmuje identyfikację zasobów czyli aktywów w danej instytucji, ustala wzajemne relacje między nimi, analizuje podatności zasobów, poznaje zagrożenia w którym wyeksponowano podatne zasoby [2].

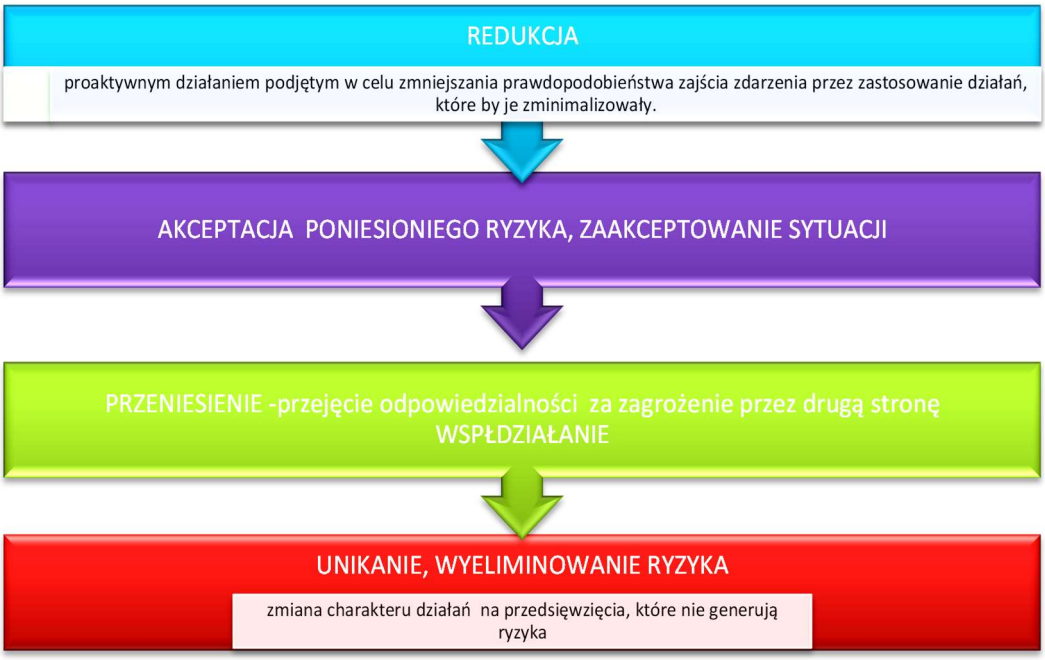
Prowadząc rozważania na temat procesu zarządzania ryzykiem warto zauważyć jest procesem ciągłym, który należałoby wdrożyć już na etapie projektowania i organizacji systemu. Proces ten należy postrzegać jako utrzymanie ryzyka wynikłych z naruszenia bezpieczeństwa i wystąpienia sytuacji kryzysowych na akceptowalnym poziomie, poprzez zapoznanie osób odpowiedzialnych za zapewnienie ochrony, ze sposobami zminimalizowania ryzyka do poziomu akceptowalnego [1].



Rys. 6.2 Zarządzanie ryzykiem wspierane analizą ryzyka
Źródło: opracowanie własne na podstawie [2]

6.4 SPOSOB POSTĘPOWANIA Z RYZYKIEM W PRZEDSIĘBIORSTWIE

Akceptacja ryzyka jest ostatnim etapem zarządzania ryzykiem. Analizy wyników pozwalają zorientować się, które z zagrożeń są najpoważniejsze. Na ich podstawie podejmowane są odpowiedzialne decyzje, które mają na celu ewentualne działania zmniejszające wystąpienie określonych zdarzeń. Następnym krokiem jest podjęcie działań powodujących, iż w efekcie końcowym będzie możliwe zaakceptowanie wielkości ryzyka. Może jednak zdarzyć się, że zostaną wyczerpane wszystkie możliwości działania i nie będzie szans na osiągnięcie jego satysfakcjonującego poziomu. Konieczna będzie wtedy inna metoda reagowania na ryzyko. Strategie oddziaływania w takiej sytuacji przedstawia rysunek 6.3.



Rys. 6.3 Strategie postępowania z ryzykiem
Źródło: opracowanie własne na podstawie [5]

Zakończenie procesu zarządzania ryzykiem wiąże się z wdrożeniem planu redukcji ryzyka. Po zakończeniu tego procesu można określić hierarchię zagrożeń, ich charakter oraz środki planowane, które mają je zredukować [5].

6.5 ANALIZA I OCENA RYZYKA ZA POMOCĄ METODY MACIERZY W WYBRANYM PRZEDSIĘBIORSTWIE

Na przykładzie badanego przedsiębiorstwie produkcyjnego została przeprowadzona analiza ryzyka utraty bezpieczeństwa informacji. Omawiane przedsiębiorstwo znajduje się w województwie Śląskim i 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. Przedsiębiorstwo istnieje na rynku od roku 1957 z pełnym sukcesem biznesowym i systematycznie poszerza swój asortyment. W związku z tym wprowadza modernizację obecnej linii technologicznej. Dział produkcji siatek jest na bieżąco unowocześniany, ponieważ przedsiębiorstwo skutecznie pozyskuje środki z dofinansowania Unii Europejskiej. W celu zebrania opinii na temat funkcjonowania w przedsiębiorstwie systemu bezpieczeństwa informacji został sporządzony kwestionariusz ankiet w którym zidentyfikowano najczęstsze zagrożenia. Na osiemnaście zagrożeń wskazał sam autor artykułu na podstawie katalogu najczęściej występujących w przedsiębiorstwach. Respondenci dokonali wyboru pięciu, które wg. nich najczęściej występują w ich organizacji. Ankieta była

anonimową metodą uzyskania odpowiedzi polegającą na wypełnieniu przez respondenta wytypowanych pytań. Kwestionariusz którym się posłużono zawierał 15 pytań. Badaniem objęto 60 pracowników przedsiębiorstwa. W artykule zostały zamieszczone tylko wybrane wyniki z otrzymanych badań. Parametry doboru poszczególnych wskaźników ilościowych zaprezentowano w tabeli od 6.1 do 6.6. Wybrane zagrożenia, zaprezentowano w tabeli 6.1.

Tabela 6.1 Identyfikacja zagrożeń występujących w danym przedsiębiorstwie

Rodzaje zagrożeń występujących w przedsiębiorstwie			
Rodzaj zagrożenia	**Charakterystyka**	**Przyczyna zagrożenia**	**Skutki**
Podszywanie się pod inną osobę	Mogą występować na terenie całego przedsiębiorstwa	Nieuwaga personelu Brak odpowiedniej weryfikacji tożsamości	Przejęcie danych o umowach związanych z klientami Utrata reputacji przedsiębiorstwa
Włamanie do systemu komputerowego	Występują na terenie całego przedsiębiorstwa, ponieważ w każdym pomieszczeniu biurowym znajduje się komputer	Łamanie zasad korzystania z poczty służbowej Brak oprogramowania służbowego	W wyniku braku poufności przedsiębiorstwo traci zaufanie odbiorców towaru Nieautoryzowana modyfikacja systemu
Podejrzenie informacji	Występuje głównie w holu głównym gdzie jest bardzo dużo stanowisk z komputerami	Nieprzestrzeganie zasad czystego biurka Pod złym kątem ustawione komputery	Konkurencja jest w posiadaniu ważnych informacji badanego przedsiębiorstwa Brak konkurencyjności
Awaria zasilania	Mogą występować na terenie całego przedsiębiorstwa ponieważ w każdym pomieszczeniu znajdują się urządzenia elektryczne	Awaria w zewnętrznej sieci elektrycznej Awaria w wewnętrznej sieci elektrycznej	W wyniku braku prądu, przestoje a w następnej kolejności straty finansowe Brak wymiany informacji
Podsłuch komputerowy	Może to zjawisko wystąpić w każdym komputerze	Nieostrożność pracowników Brak odpowiednio rozpowszechnionej wśród pracowników polityki bezpieczeństwa informacji	Naruszenie poufności danych Wyciek newralgicznych informacji do konkurencji

Źródło: opracowanie własne

Tabela 6.2 przedstawia pięciostopniową skale prawdopodobieństwa (częstotliwości) występowania zagrożeń. Prawdopodobieństwo w ujęciu jakościowym, opisuje skala: bardzo rzadkie, rzadkie, średnie, duże, bardzo prawdopodobne. Ustalone kryteria opierają się na analizie danych statystycznych, pochodzących z badanego przedsiębiorstwa.

Tabela 6.2 Jakościowy opis skali prawdopodobieństwa

Skala	Prawdopodobieństwo	Opis
1	Bardzo rzadkie	Występuje raz na siedem lat.
2	Rzadkie	Występuje raz na pięć lat.
3	Średnie	Występuje raz na trzy lata.
4	Duże	Występuje raz na dwa lata.
5	Bardzo prawdopodobne	Występuje w ciągu roku.

Źródło: opracowanie własne

Tabela 6.3 Szacowanie strat generowanych, związanych z zagrożeniami bezpieczeństwa informacji i ich opis

Skala	Skutki	Kategoria	Opis najbliższy rzeczywistości
1	Nieważne	UP-utrata pozycji	Brak wpływu na całą organizację. Przedsiębiorstwo nie traci odbiorców
		P-przestoje	Przerwa w pracy [do 1 h]
		Prze-przedsiębiorczość	Utrata finansów w organizacji rzędu < 500zł-1000zł
		D-dobra reputacja	Brak wpływu na wyobrażenie o organizacji
2	Mały	UP-utrata pozycji	Przedsiębiorstwo traci jednego średniego odbiorcę
		P-przestoje	Zauważalne przerwy w pracy [do 2h]
		Prze-przedsiębiorczość	Utrata finansów rzędu < 1000zł-5000zł
		D-dobra reputacja	Zauważalny wpływ na wyobrażenie o organizacji
3	Średni	UP-utrata pozycji	Zauważalny wpływ na opinię firmy. Przedsiębiorstwo traci kilku średnich odbiorców swego towaru
		P-przestoje	Przestoje w produkcji na poszczególnych działach [do 5h]
		Prze-przedsiębiorczość	Utrata finansów rzędu < 5000zł-10000zł
		D-dobra reputacja	Przeciętny wpływ na wyobrażenie organizacji
4	Duży	UP-utrata pozycji	Środowisko biznesowe zmienia wyobrażenie na negatywne o firmie. Przedsiębiorstwo straciło jednego kluczowego odbiorcę
		P-przestoje	Przestoje w produkcji na jednym wydziale [do 8h]
		Prze-przedsiębiorczość	Utrata zamówienia w wysokości < 10000zł-50000zł
		D-dobra reputacja	Decydujący wpływ na wyobrażenie o organizacji
5	Katastrofalny	UP-utrata pozycji	Przedsiębiorstwo utraciło dobrą opinię i straciło kluczowych odbiorców swojego towaru
		P-przestoje	Przerwa w pracy na więcej niż 1 wydziale [do 8h]
		Prze-przedsiębiorczość	Utrata finansowa z rzedu < 50000zł-100000zł
		D-dobra reputacja	Utrata pozytywnego wizerunku organizacji

Źródło: opracowanie własne

Tabela 6.3 przedstawia pięciostopniową skale skutków wystąpienia zagrożeń. Skutek w ujęciu jakościowym, opisuje skala: nieważne, mały, średni, duży, katastrofalny. Ustalone kryteria opierają się na analizie danych statystycznych, pochodzących z badanego przedsiębiorstwa, dodatkowo badając ich wpływ o utratę pozycji (UP), przestoje (P), przedsiębiorczość (Prze), dobrą reputację (D).

Analiza finansowa przedsiębiorstwa wykazała wartość strat wynoszących od 500zł do 100000zł.

Analiza studium literaturowego, wskazuje iż ryzyko jest iloczynem prawdopodobieństwa wystąpienia niepożądanego zdarzenia i wielkości strat, które występują w danym zdarzeniu. Dlatego każda zmiana podatności, może mieć znaczny wpływ na ryzyko. Powyższe założenie opisane jest następującym wzorem :

$$R = P \cdot S$$

gdzie:
R – ryzyko,
P – prawdopodobieństwo zagrożenia,
S – skutek, straty [15].

Niezbędnym więc jest zestawienie otrzymanych wyników (tabela 6.4).

Tabela 6.4 Wyniki obliczeń szacowania ryzyka w przedsiębiorstwie

Nr. wady	Potencjalna wada	Prawdopodobieństwo	Skutek	Ryzyko
Zag. 1	Podszywanie się pod inną osobę	2	3	6
Zag. 2	Włamanie do systemu komputerowego	4	4	16
Zag. 3	Podejrzenie informacji	3	4	12
Zag. 4	Awaria zasilania	5	4	20
Zag. 5	Podsłuch komputerowy	1	3	3

Źródło: opracowanie własne

Jednym z najbardziej uciążliwych zagrożeń występujących na terenie zakładu produkcyjnego jest awarii zasilania.Brak zasilania może wydarzyć się właściwie w każdej części zakładu. Może to wskazywać na niedostateczną ochronę przed przepięciami energii elektrycznej. Zakupione w przedsiębiorstwie agregaty prądotwórcze są zbyt słabe.

Szacując parametry ryzyka (prawdopodobieństwa wystąpienia danego zagrożenia, oraz skutków zagrożenia) określa się wartość ryzyka, i następnie umieszcza się ją w wyznaczonym miejscu macierzy (rys. 6.4).

skutek	5	5	10	15	20	25 (Zag.4)
	4	4	8	12 (Zag.3)	16 (Zag.2)	20
	3	3 (Zag.5)	6 (Zag.1)	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
		Prawdopodobieństwo				

Rys. 6.4 Macierz poziomu ryzyka w badanym przedsiębiorstwie

Źródło: opracowanie własne

W dalszej kolejności analizy, określono granicę szacującą poziom ryzyka, klasyfikując je jako: małe, średnie czy wysokie ryzyko (tabela 6.5).

Tabela 6.5 Ocena wielkości oszacowanego ryzyka

Ocena	Wielkość ryzyka
	Minimalne ryzyko
	Małe ryzyko
	Średnie ryzyko
	Duże ryzyko
	Bardzo duże ryzyko

Źródło: opracowanie własne

W przypadku przekroczenia powyższych wskaźników niezbędne jest podjęcie wyznaczonych kroków w celu przeprowadzenia planu zapobiegawczego postępowania z ryzykiem. W planie takim winny być jasno zdefiniowany czas i wartość ryzyka.

Z przeprowadzonej analizy wynika że podsłuch komputerowy, znajduje się na minimalnym poziomie ryzyka, w związku z tym nie wymaga podejmowania dodatkowych środków zapobiegawczych. Natomiast, włamanie się do systemu komputerowego i podejrzenie informacji, oraz podszywanie się pod inną osobę znajdują się na poziomie średnim. Należałoby zatem, zredukować poziom oszacowanego ryzyka poprzez wprowadzenie dodatkowych zabezpieczeń i unowocześnień. Opracowany macierz pokazuje że największym zagrożeniem dla przedsiębiorstwa okazała się awaria zasilania. W związku z otrzymanym wynikiem oscylującym na poziomie ryzyka 20, można oszacować że jest to ryzyko bardzo duże, nieakceptowalne. Trzeba zatem wdrożyć działania zapobiegawcze. Dlatego aktualna sytuacja w przedsiębiorstwie wymaga bezwzględnej reakcji na to zjawisko używając środków zapobiegawczych, wprowadzając dodatkowe lub zupełnie nowe rozwiązania.

PODSUMOWANIE

W wyniku ciągle postępującego rozwoju teleinformatyki, dużym wyzwaniem dla kadry kierowniczej, menadżerów, i właścicieli organizacji stało się zapewnienie spójności, tajności i niezawodności w działaniu skierowanym na gromadzenie, udostępnianie danych czy też przetwarzanie informacji [15]. Zasadniczym jest stwierdzenie że, znacząca wartość informacji spowodowała, iż bezpieczeństwo stało się strategicznym punktem w działalności jednostek gospodarczych w każdym fragmencie gospodarki. Informacja to w dzisiejszych czasach majątek firmy, decydujący o rozwoju i sukcesie na rynku lub porażce w dążeniu do określonego celu, determinując pozycję ekonomiczną organizacji. Organizacje gromadzą, przechowują, wytwarzają i dystrybuują ogromne ilości informacji, które determinują jej istnienie i potencjał. Dlatego też od kierownictwa firmy wymaga się właściwego zarządzania informacją, ponieważ jej utrata przyczynia się do obniżenia pozycji i konkurencyjności na rynku pracy. Dzięki takiej polityce przedsiębiorstwa

stają się liderami w swojej branży i bardzo szybko pną się po szczeblach awansu, osiągając szybki i dynamiczny progres [12]. Celem niniejszego artykułu było zlokalizowanie i dokonanie identyfikacji słabych punktów w przedsiębiorstwie, w których zasoby informacyjne narażone są na utratę bezpieczeństwa informacji. Prawidłowa analiza szacowania ryzyka pozwoliła zidentyfikować zagrożenia możliwe do wystąpienia, określając rozmiar strat. Ograniczenie ryzyka jest możliwe dzięki, odpowiedniemu zarządzaniu ryzykiem w przedsiębiorstwie na co się składa jego identyfikacja, planowanie, podejmowanie decyzji i kontrolowanie ryzyka na akceptowalnym poziomie. Zatem, najważniejszym etapem ograniczenia ryzyka jest jego dokładny pomiar, co umożliwia metoda macierzy ryzyka. Zgodnie z opiniami ekspertów proces szacowania ryzyka winien być przeprowadzony raz na rok. Pozwoliło by to na zidentyfikowanie coraz to nowych zagrożeń form zagrożeń i utrzymanie w przedsiębiorstwie akceptowalnego poziomu ryzyka.

LITERATURA

[1] M. Anzel, Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych. Poznań: Przedsiębiorstwo Handlowo-Usługowe ONE, 2011.
[2] A. Białas., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Warszawa, Wydawnictwo Naukowo-Techniczne, 2006.
[3] M Biegański i A. Janiec, Por. *Hedging i nowoczesne usługi finansowe*. Poznań, Wydawnictwo Akademii Ekonomiczej w Poznaniu, 2001.
[4] R. Borowiecki, M. Romanowska, *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*. Warszawa: Difin, 2001.
[5] R. Grocki, *Zarządzanie Kryzysowe*. Warszawa: Difin, 2012.
[6] J. Jańczak, A. Nowak, *Bezpieczeństwo informacyjne Wybrane problemy*. Warszawa: Akademia Obrony Narodowej, 2012.
[7] T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Gliwice: Helion, 1999.
[8] B. Ludwiszewski, K. Redlarski, T. Gardzioła, Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie w świetle norm PN-ISO/IEC 27001 oraz 61508. Poznań: *Zeszyty Naukowe Politechniki Poznańskiej* 2009.
[9] J. Łuczak, M. Trybulski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC27001*. Poznań: Wyd. Uniwersytetu Ekonomicznego w Poznaniu, 2010.
[10] A. Nowak, W. Scheffs,: *Zarządzanie bezpieczeństwem informacji*. Warszawa: Wydawnictwo AON, 2010.
[11] *PN-I_13335-1:1999 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych*, PKN, Warszawa 2012.
[12] D. Rydz, M. Krakowiak, T. Bajor, Zapewnienie bezpieczeństwa informacji w przedsiębiorstwach. Prace Naukowe Akademii im. Jana Długosza w Częstochowie. *Technika, Informatyka, Inżynieria Bezpieczeństwa*, Częstochowa, T. 1, 2013, str. 281-288.
[13] Ustawa z dnia 5 Sierpnia 2010 roku o ochronie informacji niejawnych.
[14] A. Wójcik-Mazur, *Zarządzanie ryzykiem płynności w bankach*. Częstochowa: Wydawnictwo Politechniki Częstochowskiej, 2012.

[15] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*. Kraków: Oficyna Wydawnicza Abrys, 2000.

Data przesłania artykułu do Redakcji: 10.2017
Data akceptacji artykułu przez Redakcję: 11.2017

MACIERZ RYZYKA JAKO NARZĘDZIE OCENY ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI

Streszczenie: *Aby zarządzać ryzykiem w danym przedsiębiorstwie należy precyzyjnie określić jego źródła powstawania, które możemy znaleźć w jego otoczeniu jak i samej organizacji. Wnikliwe i dokładne określenie źródła powstawania zagrożeń pomoże ustrzec przedsiębiorstwo od destabilizacji i nadmiernych strat. Artykuł podejmuje temat utraty bezpieczeństwa informacji zgodnego z normą PN-I_13335-1:1999, która określa wytyczne dotyczące zarządzania bezpieczeństwem systemów informatycznych. Celem artykułu jest zidentyfikowanie zagrożeń występujących w przedsiębiorstwie, znaleźć miejsca ich występowania oraz przeprowadzeniu analizy ryzyka za pomocą narzędzia jakim jest macierz ryzyka.*

Słowa kluczowe*: szacowanie ryzyka, macierz ryzyka*

RISK MISCELLANEOUS AS A TOOL FOR EVIDENCE OF INFORMATION HAZARDOUS RISKS

Abstract: *In order to manage the risk in a given enterprise, it is necessary to precisely define its origins, which we can find in its environment as well as the organization itself. Thorough and accurate identification of the source of the hazards will help prevent the company from destabilizing and over-losses. This article deals with information security loophole in accordance with PN-I_13335-1:1999, which defines guidelines for the management of information systems security. The purpose of this article is to identify the threats that occur in an enterprise, find out where they are, and perform risk analysis with a risk matrix tool.*

Key words: *Risk assessment, risk matrix*

mgr inż. Estera Pietras
Politechnika Częstochowska
Wydział Inżynierii Produkcji
i Technologii Materiałów
Instytut Przeróbki Plastycznej
i Inżynierii Bezpieczeństwa
Al. Armii Krajowej 19
42-201 Częstochowa, Polska
e-mail: pietras.estera@wip.pcz.pl