IDENTYFIKACJA I OCENA ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI ZA POMOCĄ WYBRANYCH INSTRUMENTÓW ZARZĄDZANIA JAKOŚCIĄ

Michał PAŁĘGA, Marcin KNAPIŃSKI, Dariusz RYDZ

Streszczenie: W artykule przedstawiono zastosowanie wybranych metod i narzędzi zarządzania jakością do identyfikacji i oceny zagrożeń bezpieczeństwa informacji. W poszczególnych rozdziałach publikacji przedstawiono znaczenie bezpieczeństwa informacji w przedsiębiorstwie, a także dokonano taksonomii zagrożeń związanych z utratą informacji, nieuprawionym ich udostępnianiem, a także nieautoryzowaną modyfikacją. Naukowy charakter niniejszej pracy stanowi zaimplementowanie wybranych metod i narzędzi jakościowych do oceny zagrożeń bezpieczeństwa informacji. Do jej przeprowadzenia zastosowano: analizę FMEA, diagram Pareto-Lorenza, diagram Ishikawy, metodę 5 x dlaczego? oraz analizę drzewa błędów. W efekcie pozwoliło to na określenie potencjału do działań doskonalących, które można zastosować, aby zwiększyć poziom bezpieczeństwa informacji.

Słowa kluczowe: bezpieczeństwo informacji, zarządzanie bezpieczeństwem informacji, zagrożenia, jakość, zarządzania jakością, analiza FMEA, diagram Pareto-Lorenza, diagram Ishikawy, metoda 5 x dlaczego?, analiza drzewa błędów

1. Wstęp

Celem każdej działalności gospodarczej jest osiąganie określonych korzyści oraz kreowanie dobrobytu. Jest to jednak niemożliwe bez przetwarzania odpowiedniego rodzaju informacji. Rewolucja technologiczna, jaka się dokonała na przełomie XX i XXI wieku dostarczyła człowiekowi środki umożliwiające gromadzenie, przetwarzanie oraz transmitowanie informacji. Wówczas aktywa te stały się podstawowym zasobem przedsiębiorstw produkcyjnych, firm handlowych oraz organizacji finansowych, które posiadają określoną wartość i mogą podlegać transakcjom kupna-sprzedaży [7, 8, 16].

Wraz z upływem czasu oraz rozwojem społeczeństwa informacyjnego informacje zaczęły znacząco wpływać na wszystkie strefy egzystencji człowieka. Natłok informacji spowodował, że obecnie dostrzec można pewnego rodzaju chaos informacyjny, w którym paradoksalnie podjęcie właściwej decyzji staje się coraz trudniejsze. Wobec powyższego zarówno podmioty gospodarcze, jak również pojedyncze jednostki społeczne powinny podejmować starania w zakresie właściwej oceny jakości informacji.

Jakość informacji oznacza jej zdolność do zaspokajania określonych potrzeb użytkownika, a określa się ją na podstawie następujących atrybutów [1, 6]:

- relatywność – wiąże się ze zdolnością do zaspokajania potrzeb użytkowników informacji;
- dokładność – mówi o tym, że informacja jest precyzyjna, zgodna ze stanem faktycznym;

- autentyczność – oznacza, że informacja, aby była użyteczna i mogła umożliwić podjęcie trafnej decyzji musi być dostarczona w odpowiednim czasie i do odpowiedniej osoby; wraz z upływem czasu poziom autentyczności obniża się na skutek pojawiania się nowych, aktualnych faktów;
- kompletność – mówi o tym, że informacja zawiera optymalną ilość danych, pozwalającą przekształcić je w konkretną wiedzę;
- spójność – wskazuje, że wszystkie elementy informacji (dane) tworzą całość, a forma prezentacji informacji odpowiednia jest do jej treści;
- dostępność – oznacza, że informacja jest dostępna dla upoważnionych użytkowników w odpowiedniej formie i czasie;
- rzetelność – wiąże się z dokładnym, starannym, obiektywnym i poprawnym sporządzaniem danych oraz sformułowaniem komunikatu, którego treść stanowi informacja;
- jednoznaczność – oznacza takie opracowanie komunikatu (stosowanie języka i pojęć), które nie budzą u odbiorcy wątpliwości i są dla niego w pełni zrozumiałe;
- wystarczalność – oznacza taką informację, która pozwala na podjęcie właściwej decyzji i umożliwia logiczne, efektywne postępowanie;
- przyswajalność – wskazuje, że informacja jest zgodna z innymi informacjami, a także interpretowana jest we właściwym kontekście oraz funkcjonuje w określonym systemie komunikacji.

Wobec przytoczonych powyżej atrybutów można stwierdzić, iż jakość informacji nierozerwalnie związana jest z jej bezpieczeństwem, które należy postrzegać z jednej strony jako możliwość pozyskania dobrej informacji, zaspokajającej potrzeby użytkownika, z drugiej zaś jako ochronę posiadanych zasobów informacyjnych przed ich utratą, niekontrolowanym ujawnieniem, nieautoryzowaną zmianą, czy też kradzieżą.

Nadrzędną kwestią związaną z zapewnieniem właściwej jakości informacji, charakteryzującej się odpowiednim poziomem bezpieczeństwa jest rzetelna i skrupulatna analiza zagrożeń. Zadanie to nie jest proste, a wręcz przeciwnie, gdyż wymaga wiedzy i doświadczenia osób je realizujące. Poza tym dużym utrudnieniem jest brak jednoznacznej metodyki prowadzania tego procesu. Niemniej jednak w literaturze przedmiotu znaleźć można mniej lub bardziej ogólne wytyczne, jak chociażby te zawarte w standardzie ISO/IEC 27001: 2014, czy ISO/IEC 27005: 2014 [14, 15].

W niniejszym artykule zaprezentowano przykładową identyfikację i ocenę zagrożeń związanych z bezpieczeństwem informacji, wykorzystując do tego celu wybrane instrumenty zarządzania jakością, które służą nie tylko do określania niezgodności wyrobów (lub poszczególny jego elementów) czy procesów wytwórczych, ale mogą znaleźć bardziej uniwersalne zastosowanie.

2. Bezpieczeństwo informacji

Współczesna działalność gospodarcza nierozerwalnie wiąże się z przetwarzaniem ogromnych ilości informacji. Jedne z nich mogą stanowić strategiczne znaczenie dla realizacji jej celów, z kolei inne są mniej istotne. Niemniej jednak niezaprzeczalnym jest fakt, iż informacje są jednymi z najważniejszych zasobów organizacji, które wymagają odpowiedniego zabezpieczenia przed szeroką gamą zagrożeń. W związku z tym problem bezpieczeństwa informacji dotyczy każdego przedsiębiorstwa, bez względu na jego wielkość, formę zorganizowania, reprezentowaną branżę, czy stopień rozwoju.

Najprościej bezpieczeństwo informacji utożsamiane jest z zapewnieniem poufności, integralności oraz dostępności informacji. Dodatkowo pod uwagę mogą być brane takie atrybuty jak: autentyczność, rozliczalność, niezaprzeczalność czy niezawodność [11]. Zdefiniowane atrybuty prezentuje rysunek 1.

Rys. 1. Atrybuty bezpieczeństwa informacji
Źródło: opracowanie własne na podstawie [11]

Podchodząc kompleksowo do problematyki bezpieczeństwa informacji należy rozumieć ją jako proces zapewniający, że informacje nie są zagrożone utratą, nieautoryzowaną zmianą czy ujawnieniem osobom lub podmiotom nieupoważnionym. Tak więc, pełna ochrona informacji wiąże się z zabezpieczeniem systemów i sieci teleinformatycznych narażonych na awarie sprzętowe czy ataki hakerów, ale także stanowisk pracy oraz pomieszczeń, w których są one przetwarzane. Zapewnienie bezpieczeństwa informacji to ciągły i złożony proces, który wymaga uwzględnienia indywidualnej sytuacji każdego przedsiębiorstwa oraz zmian powstających w środowisku (otoczeniu). Polegać on powinien przede wszystkim na neutralizowaniu zagrożeń oraz ich skutków, co wiąże się z potrzebą identyfikacji i oceny potencjalnych niebezpieczeństw, określaniem zasad polityki bezpieczeństwa informacji, wyborem odpowiednich zabezpieczeń technicznych i organizacyjnych, a także permanentną kontrolą stanu bezpieczeństwa w przedsiębiorstwie. Decyzja o wyborze adekwatnych mechanizmów ochronnych podejmowana powinna być w oparciu o analizę warunków otoczenia zewnętrznego i wewnętrznego organizacji, a także wartości posiadanych informacji oraz ich wpływu na kształtowanie przewagi konkurencyjnej [8, 11]. Ponadto, zaimplementowanie skutecznych zabezpieczeń wymaga interdyscyplinarnej wiedzy z zakresu zarządzania, ekonomii, informatyki, prawa, inżynierii produkcji, a nawet psychologii i socjologii.

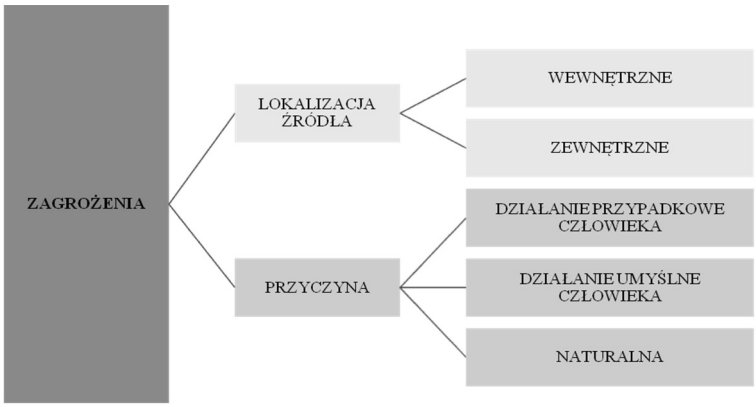
3. Rodzaje zagrożeń bezpieczeństwa informacji

Era społeczeństwa informacyjnego, w której szczególnie wartościowym zasobem są dane powoduje wzrost liczby i różnorodności zagrożeń oraz potencjalnych skutków ich wystąpienia. Zapewnienie odpowiedniego poziomu bezpieczeństwa informacji wymaga zaimplementowania konkretnych działań neutralizujących ich negatywny wpływ na funkcjonowanie organizacji. Nie jest to jednak możliwe bez rzetelnej i skrupulatnej identyfikacji i oceny zagrożeń. Stąd też niezmiernie ważnym problemem jest znajomość podstawowych źródeł niebezpieczeństw.

S. Koziej [9] definiuje zagrożenie jako „*pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot, w podziale na zagrożenie potencjalne lub realne, subiektywne i obiektywne, zewnętrzne i wewnętrzne, militarne i niemilitarne (umiejscawiając zagrożenia informacyjne w grupie zagrożeń niemilitarnych, wraz z zagrożeniami politycznymi, ekonomicznymi, społecznymi, ekologicznymi).* Zgodnie z normą PKN-ISO Guide 73:2012

[13] zagrożenie stanowi źródło potencjalnej szkody. Zagrożenie może być uszczegółowione przez wskazanie jego pochodzenia (np. mechaniczne, elektryczne) bądź charakteru potencjalnej szkody (np. utrata poufności danych).

Literatura przedmiotu, jak również doświadczenia ostatnich lat wskazują na bardzo szeroki podział zagrożeń bezpieczeństwa informacji. W najprostszym ujęciu zagrożenia można podzielić ze względu na lokalizację (umiejscowienie) ich źródła oraz przyczynę ich powstawania, co prezentuje rysunek 2.



Rys. 2. Podział zagrożeń bezpieczeństwa informacji
Źródło: opracowanie własne na podstwie [15]

Zgodnie z przedstawioną klasyfikacją rozróżnia się zagrożenia wewnętrzne (np. działanie pracownika, awaria systemu komputerowego) oraz zagrożenia zewnętrzne (np. atak DDoS). Z kolei biorąc pod uwagę przyczynę powstawania, zagrożenia mogą być następstwem działania człowiaka bądź środowiska naturalnego. Zagrożenia związane z czynnikiem ludzkim można podzialić na te przypadkowe, wynikające z błędu, pomyłki, braku świadomości (np. przypadkowe skasowanie pliku, uszkodzenie nośnika danych) oraz celowe, umyślne podyktowane checią zemsty na procodawcy czy osiągnięcia zysku (np. kradzież danych, szpiegostwo przemysłowe). Natomiast do zagrożeń środowiskowych zaliczyć można powódź, poażar, wyładowania atmosferyczne, trzesienie ziemii i inne.

Nieco inną taksonomię zagrożeń przedstawia na swoich stronach interentowych Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. (tab.1).

Jak wynika z tabeli 1 podział zagrożeń zaproponowany przez CERT.GOV.PL koncentruje się przede wszystkim na zagrożeniach systemów i sieci komputerowych. Rozwój teleinformatyki oprócz wielu korzyści sprzyja także powstawaniu różnych form niebezpieczeństw. Systemy informatyczne z racji swojego przeznaczenia (tj. gromadzenie, przetwarzanie oraz przesyłanie danych) narażone są na liczne ataki, których celem jest przejęcie nad nimi kontroli oraz nieuprawniony dostęp do danych.

Reasumując, zaprezentowane typy zagrożeń stanowią jedynie niewielki wycinek, tego co rzeczywiście może stanowić przyczynę utraty bezpieczeństwa informacji w przedsiębiorstwie. Stąd też zagrożenia powinny być określane indywidualnie przez każdy podmiot, z uwzględnieniem m.in. kontekstu, celu oraz zakresu przetwarzanych informacji. Wyłącznie takie podejście do kwestii identyfikacji i oceny zagrożeń może przyczynić się do podejmowania właściwych decyzji i wyboru skutecznych narzędzi zabezpieczających aktywa informacyjne.

Tab. 1. Katalog zagrożeń stosowany przez CERT.GOV.PL

ZAGROŻENIA		PODATNOŚCI				
DZIAŁANIA CELOWE	1.1. ZŁOŚLIWE OPROGRAMOWANIE	1.1.1. wirus	1.1.2. robak sieciowy	1.1.3. koń trojański	1.1.4. dialer	1.1.5. klient botnetu
	1.2. PRZEŁAMYWANIE ZABEZPIECZEŃ	1.2.1. nieuprawnione logowanie	1.2.2. włamanie na konta/ ataki siłowe	1.2.3. włamanie do aplikacji		
	1.3. PUBLIKACJE W SIECI INTERNET	1.3.1. treści obraźliwe	1.3.2. pomawianie (zniesławienie)	1.3.3. naruszenie praw autorskich	1.3.4. dezinformacja	
	1.4. GROMADZENIE INFORMACJI	1.4.1. skanowanie	1.4.2. posłuch	1.4.3. inżynieria społeczna	1.4.4. szpiegostwo	1.4.5. SPAM
	1.5. SABOTAŻ KOMPUTEROWY	1.5.1. nieuprawniona zmiana informacji	1.5.2. nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji			
		1.5.3. atak odmowy dostępu (DDoS, DoS)	1.5.4. skasowanie danych			
		1.5.5. wykorzystanie podatności w urządzeniach	1.5.6. wykorzystanie podatności aplikacji			
	1.6. CZYNNIK LUDZKI	1.6.1. naruszenie procedur bezpieczeństwa	1.6.2. naruszenie obowiązujących przepisów prawnych			
	1.7. CYBERTERRORYZM	1.7.1. Przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni				
DZIAŁANIA NIECELOWE	2.1. WYPADKI I ZDARZENIA LOSOWE	2.1.1. awarie sprzętowe	2.1.2. awarie łącza	2.1.3. awarie (błędy) oprogramowania		
	2.2. CZYNNIK LUDZKI	2.2.1. naruszenie procedur	2.2.2. zaniedbanie	2.2.3. błędna konfiguracja urządzenia	2.2.4. brak wiedzy	2.2.5. naruszenia praw autorskich

Źródło: [5]

4. Zastosowanie wybranych instrumentów zarządzania jakością do identyfikacji i oceny zagrożeń bezpieczeństwa informacji

W literaturze przedmiotu z zakresu zarządzania jakością bądź zapewnienia jakości prezentowany jest szeroki katalog metod, narzędzi i technik, którymi można się posługiwać w zależności od tego, jaki problem dotyczący kształtowania jakości i doskonalenia procesów bądź wyrobów należy rozwiązać. W niniejszej pracy do przeprowadzenia analizy zagrożeń związanych z utratą bezpieczeństwa informacji zastosowano następujące metody i narzędzia zarządzania jakością:

- Analiza FMEA;
- Diagram Pareto – Lorenza;
- Diagram Ishikawy;
- Metoda 5 x dlaczego?
- Analiza drzewa błędów.

4.1. Analiza FMEA

Analiza FMEA (ang. Failure Mode and Effects Analysis) jest uznaną oraz powszechnie stosowaną metodą, która służy do identyfikacji błędów oraz pomaga w ich ograniczaniu. Analiza FMEA pozwala na rozpoznawanie i ocenę ryzyka występowania potencjalnych błędów, które mogą wystąpić w poszczególnych elementach wyrobu bądź etapach procesu jego wytwarzania. Uwzględnia ona także skutki występowania wspomnianych niezgodności. Celem stosowania tej metody jest zidentyfikowanie tych elementów wyrobu bądź procesu względem, których niezbędne jest zaimplementowanie działań eliminujących bądź redukujących ryzyko potencjalnych błędów.

Ryzyko oblicza się na podstawie trzech parametrów: znaczenia wady (błędów), prawdopodobieństwa ich wystąpienia, a także możliwości wykrycia błędów [4, 10, 12, 18]. Powyższą zależność wyraża wzór:

$$LPR = Z \times R \times W$$

gdzie:

LPR – liczba priorytetowa ryzyka;
Z – znaczenia dla klienta;
R – prawdopodobieństwo;
W – wykrywalność.

Zastosowanie analizy FMEA w obszarze bezpieczeństwa informacji pozwoliło na analizę zagrożeń pod względem przyczyn (źródeł) ich powstawia, a także potencjalnych skutków, jakie mogą one powodować dla funkcjonowania przedsiębiorstwa. W tabeli 2 zaprezentowano wybrane wyniki z przeprowadzonej analizy FMEA.

Tab. 2. Przykładowa ocena zagrożeń bezpieczeństwa informacji za pomocą analizy FMEA

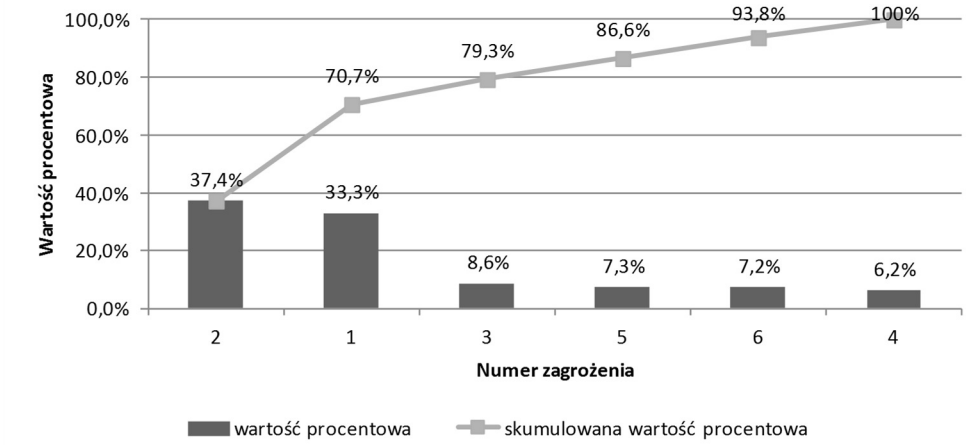
Lp.	Nazwa zagrożenia	Potencjalne skutki zagrożenia	Potencjalne przyczyny zagrożenia	Z	R	W	LPR
1.	Nieświadomość personelu	Nieświadomość zagrożeń oraz wartości informacji. Ujawnienie informacji. Utrata danych.	Brak planowania bądź organizacji szkoleń	9	8	9	648
2.	Nieuprawiony udostępnienie danych	Rozpowszechnianie danych. Ujawnienie danych konkurencji. Straty finansowe. Utrata przewagi konkurencyjnej	Nieprzestrzeganie zasad czystego biurka i ekranu. Łatwy dostęp do informacji. Niewłaściwe zarządzanie personelem. Nieświadomość pracowników.	9	9	9	729
3.	Awaria sprzętu komputerowego	Brak lub ograniczony dostęp do danych. Zakłócenie realizacji procesów. Możliwe straty finansowe.	Awaria podzespołów. Nieumiejętne użytkowanie sprzętu. Celowa ingerencja człowieka.	7	6	4	168
4.	Awaria systemu łączności	Zakłócenie ciągłości działania. Problemy z wymianą informacji i komunikacją.	Uszkodzenie sieci energetycznej. Awaria urządzeń.	8	5	3	120
5.	Nieprawidłowe działanie oprogramowania	Obniżenie wartości użytkowej oprogramowania. Błędny rezultat działania. Ograniczony dostęp do zbiorów danych.	Niewłaściwe lub nieumiejętne korzystanie z oprogramowania. Brak właściwej konserwacji i serwisu. Zakup wadliwego oprogramowania.	7	7	3	143
6.	Zdarzenia losowe (pożar, powódź)	Zniszczenie zbiorów danych. Brak lub utrudniony dostęp do danych. Zakłócenie funkcjonowania przedsiębiorstwa. Straty finansowe. Utrata renomy	Warunki atmosferyczne. Celowe lub przypadkowe działania człowieka. Awaria podzespołów.	7	5	4	140

Źródło: opracowanie własne

Na podstawie danych zestawionych w tabeli 2 można wnioskować, że największym poziomem ryzyka charakteryzują się następujące zagrożenia: nieuprawnione udostępnianie danych oraz nieświadomość personelu. Z kolei najmniejszy wpływ na system bezpieczeństwa informacji mają: zdarzenia losowe oraz awaria systemu łączności. Na podstawie zabranych danych można wnioskować, że wdrożone zabezpieczenia techniczne sprawiają, że prawdopodobieństwo wystąpienia zagrożeń związanych z infrastrukturą informatyczną jest na średnim poziomie. Oprócz tego, rozpatrując wartości LPR poszczególnych zagrożeń stwierdzić można, iż potencjał do doskonalenia powinny stanowić działania związane z czynnikiem ludzkim. Zaleca się skupienie większej uwagi na podnoszeniu poziomu wiedzy pracowników w zakresie należytego postępowania ze zbiorami danych oraz świadomości występowania różnych form zagrożeń bezpieczeństwa informacji. Uzasadnionym zatem byłoby m.in. wprowadzenie systematycznych szkoleń dla całego personelu, a także ciągłe jego edukowanie poprzez np. rozpowszechnianie ulotek i folderów promujących przestrzeganie zasad bezpiecznej pracy z informacjami.

4.2. Diagram Pareto-Lorenza

Diagram Pareto-Lorenza ma na celu w sposób graficzny zaprezentować najważniejsze czynniki, które wpływają na badane zjawisko. Opiera się on na zasadzie 80/20, która głosi, że 80% wszystkich wad (niezgodności) wynika z 20% przyczyn. Diagram Pareto-Lorenza stanowi prosty histogram, który przedstawia dane w porządku malejącym. Na wykres słupkowy nanoszony jest wykres liniowy, który przedstawia wartości skumulowane [17]. Metoda Pareto-Lorenza charakteryzuje się bardzo dużą uniwersalnością i może być wykorzystywana przy rozwiązywaniu bardzo wielu problemów. W niniejszej pracy została ona użyta, aby wskazać dominujące wady (zagrożenia) w systemie bezpieczeństwa informacji, które wymagać będą priorytetowego traktowania. Na rysunku 3 przedstawiono diagram Pareto-Lorenza na podstawie wyników otrzymanych z analizy FMEA (tab. 2).



Rys. 3. Diagram Pareto-Lorenza dla zagrożeń bezpieczeństwa informacji
Źródło: opracowanie własne

Na podstawie przeprowadzonej analizy można zaobserwować, że 79,3% ogółu zagrożeń stanowią:

- nieuprawnione udostępnienie danych;
- nieświadomość personelu;
- oraz awaria sprzętu komputerowego.

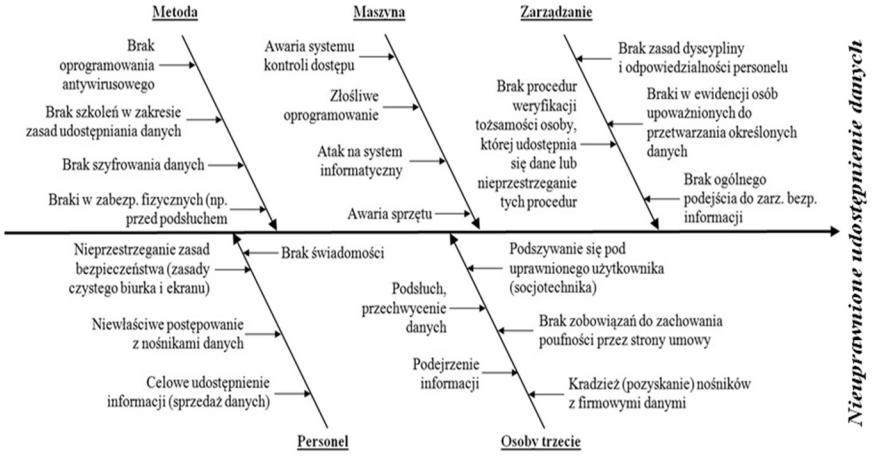
To właśnie na tych zagrożeniach przedsiębiorstwo powinno skupić największą uwagę.

Podjęcie określonych działań doskonalących wymaga zidentyfikowania potencjalnych przyczyn wskazanych zagrożeń. Stąd też do przeprowadzenia dalszych analiz (diagram Ishikawy, metoda 5 x dlaczego?, analiza drzewa błędów) wybrano zagrożenie polegające na nieuprawnionym udostępnieniu danych.

4.3. Diagram przyczynowo-skutkowy Ishikawy

Diagram przyczynowo-skutkowy służy do graficznej prezentacji analizy wzajemnych powiązań przyczyn powodujących określone problemy. Jest on powszechnie stosowanym narzędziem zarządzania jakością, pozwalającym dokonać identyfikacji oraz hierarchizacji czynników składających się na dane zjawisko. Do jego najważniejszych zalet zaliczyć można: uporządkowany przekaz informacji, trafność prowadzonej analizy (od ogółu do szczegółu), staranność oraz nacisk na lokalizację i eliminację przyczyn problemu [3, 10, 17].

Zastosowanie diagramu przyczynowo-skutkowego w obszarze bezpieczeństwa informacji pozwala na określenie wszelkiego rodzaju podatności, które mogą prowadzić do zmaterializowania się określonego zagrożenia. Właściwe rozpoznanie słabości aktywów bądź grupy aktywów informacyjnych umożliwia ich zabezpieczenie przed zagrożeniami. Do przeprowadzania analizy przyczynowo-skutkowej wyróżniono pięć grup przyczyn, tj.: metoda, maszyna, zarządzanie, personel oraz osoby trzecie (rys. 4).



Rys. 4. Diagram przyczynowo-skutkowy Ishikawy dla zagrożenia związanego z nieuprawnionym udostępnieniu danych
Źródło: opracowanie własne

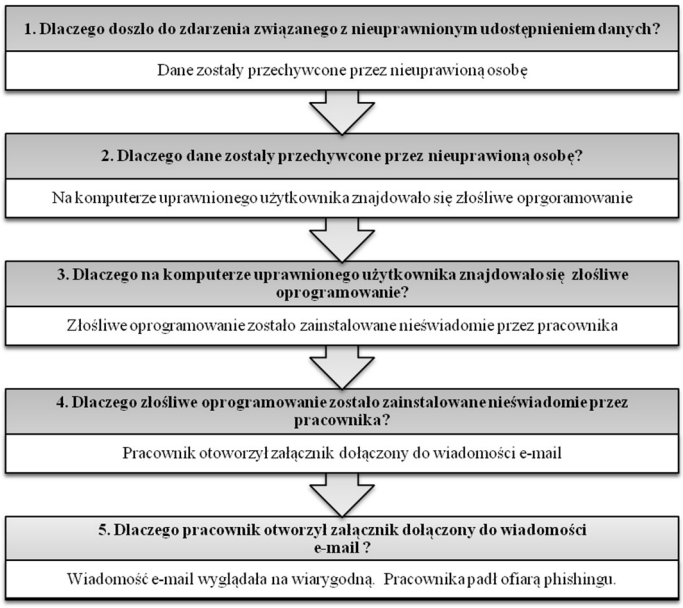
Diagram Ishikawy pozwolił na zidentyfikowanie wielu przyczyn nieuprawnionego udostępniania danych, które sklasyfikowane zostały w pięciu następujących obszarach:

- w obszarze metoda wskazano m.in. na brak oprogramowania antywirusowego, co pozwala na zainfekowanie komputerowa złośliwym oprogramowaniem przeznaczonym do wyłudzania danych (np. keyllogery). Poza tym istotną nieprawidłowością jest brak szkoleń w zakresie udostępniania danych czy też nieszyfrowanie szczególnie wrażliwych informacji. Oprócz tego zwrócić uwagę należy na dostateczne zabezpieczenia fizyczne, uniemożliwiające dostęp do pomieszczeń osobom nieuprawnionym. Ponadto, szczególne strefy przedsiębiorstwa powinny być chronione np. przed podsłuchem czy promieniowaniem elektromagnetycznym;
- w obszarze maszyna wskazać należy przede wszystkim na podatności związane z awaryjnością sprzętu komputerowego bądź systemu kontroli dostępu. Analiza wykazała także, że do nieuprawnionego udostępnienia danych może dojść na skutek ataku na system informatyczny przedsiębiorstwa bądź zainfekowania komputera szkodliwym oprogramowaniem;
- obszar zarządzania wymaga zwrócenia uwagi na kwestie związane z tym, komu powierza się dostęp do danych. W tym względzie wskazać można na dwa zasadnicze błędy. Po pierwsze, brak ewidencji osób upoważnionych do przetwarzania określonych kategorii danych może spowodować, że pracownicy będą mieć dostęp do wszystkich informacji, niezależnie czy potrzeba taka wynika z realizacji ich obowiązków służbowych, cz też nie. Po drugie, brak procedur udostępniania danych osobom trzecim bądź ich nieprzestrzeganie sprzyjać mogą zmaterializowaniu się zagrożenia związanego z podszywaniem się pod inną osobę bądź instytucję w celu wyłudzenia danych. W ten sposób bardzo łatwo może dojść do przekazania strategicznych informacji podmiotom konkurencyjnym. Istotne znaczenie w kształtowaniu bezpieczeństwa informacji ma również podejście kierownictwa organizacji do rażących naruszeń przepisów i regulaminów przez pracowników. Brak należytej reakcji na takie sytuacje może wzmacniać tego typu zachowania oraz wzbudzać w pracownikach poczucie bezkarności;
- kolejne dwa obszary dotyczą najsłabszego ogniwa w systemie bezpieczeństwa, a mianowicie czynnika ludzkiego. Biorąc pod uwagę źródło jego umiejscowienia wyróżnić można personel (zagrożenia wewnętrzne) oraz osoby trzecie (zagrożenia zewnętrzne). Wśród potencjalnych przyczyn nieuprawnionego udostępnienia informacji po stronie pracowników wskazać można m.in.: nieświadomość pracowników, nieprzestrzeganie zasad bezpieczeństwa oraz celowe działanie na szkodę przedsiębiorstwa. Z kolei osoby trzecie mogą zapoznać się przypadkowo z informacjami, do których nie są upoważnieni (np. poprzez podejrzenie informacji), a także dopuścić się celowego wyłudzenia danych. Poza tym zadbać także należy o zobowiązanie stron umowy do zachowania poufności przekazanych im informacji, aby ustrzec się przed wykorzystaniem przez nich danych udostępnionych w ofercie.

4.4. Metoda 5 x dlaczego?

Metoda 5 x dlaczego? (nazywana także 5 x Why) jest typową metodą, która pozwala na zidentyfikowanie przyczyn określonego problemu. W odróżnieniu od innych metod, jak np. diagramu Ishikawy, metoda 5 x dlaczego? pozwala nie tylko na wskazanie bezpośrednich przyczyn problemu, ale pełną jego diagnozę. Kilkukrotne zadawanie pytania *dlaczego?* umożliwia wskazanie pierwotnych źródeł powstawania zakłóceń [2].

Na rysunku 5 przedstawiono przykładowe zastosowanie metody 5 x dlaczego? do wskazania potencjalnych źródeł zagrożeń związanych z nieuprawnionym udostępnieniem informacji.



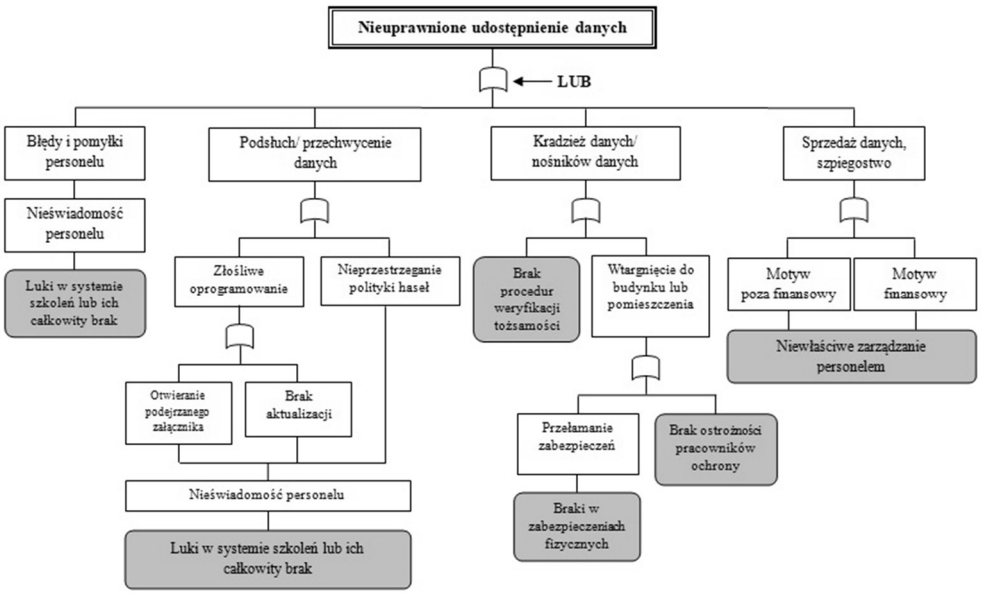
Rys. 5. Metoda 5 x dlaczego? przeprowadzona dla zagrożenia związanego z nieuprawnionym udostępnieniem informacji
Źródło: opracowanie własne

W zaprezentowanym przykładzie główną przyczyną nieuprawnionego udostępnienia informacji okazał się phishing. Jest to dość popularna metoda polegająca na podszywaniu się pod inną osobę bądź instytucję w celu wyłudzenia poufnych informacji lub nakłonienia ofiary do podjęcia określonych działań. Metoda phishingu bazuje na niewiedzy i nieświadomości użytkowników sieci internet. Poza tym dostępność technologii komputerowych sprawia, że bardzo prosto można spreparować wybraną stronę internetową, tak aby wyglądała ona na autentyczną.

4.5. Analiza drzewa błędów

Analiza drzewa błędów jest zaawansowaną dedukcyjną techniką wykorzystywaną do identyfikacji i analizy czynników wywołujących niepożądane zdarzenia. Konstrukcję drzewa błędów należy rozpocząć od zidentyfikowania zdarzenia (zagrożenia) nadrzędnego, stanowiącego górę diagramu. Następnie określa się i porządkuje w sposób logiczny zdarzenia pośrednie, wpływające na zdarzenie główne. Zdarzenia między sobą powiązane są dwoma rodzajami tzw. bramek logicznych: „I" bądź „LUB".
Bramka I – wskazuje, ze warunkiem wystąpienia kolejnego zdarzenia jest zaistnienie wszystkich zdarzeń poprzednich („wychodzących");
Bramka LUB – wskazuje, ze warunkiem wystąpienia kolejnego zdarzenia jest zaistnienie jednego ze zdarzeń poprzednich („wychodzących").

Przykładową analizę drzewa błędów związaną z nieuprawionym udostępnieniem danych, w sposób graficzny przedstawiono na rysunku 6.



Rys. 6. Analiza drzewa błędów przeprowadzona dla zagrożenia związanego z nieuprawnionym udostępnieniem danych
Źródło: opracowanie własne

Na podstawie przeprowadzonej analizy drzewa błędów można stwierdzić, iż do zdarzeń inicjujących (początkowych) nieuprawnione udostępnienie danych zaliczyć można:

- luki w systemie szkolenia lub ich całkowity brak, co przekłada się na nieświadomość personelu. Niedostateczna wiedza pracowników w zakresie bezpieczeństwa informacji sprzyjać może błędnemu przekazywaniu danych bądź też niewłaściwym zachowaniom, chociażby w zakresie polityki haseł czy postępowania z podejrzanie wyglądającymi załącznikami wiadomości e-mail. W konsekwencji prowadzić to może do zainstalowania przez użytkownika złośliwego oprogramowania i przechwycenia danych przez nieuprawnionych użytkowników;
- brak procedur weryfikacji tożsamości – prowadzić może do wyłudzenia danych przez nieuprawnioną osobą;
- braki w zabezpieczeniach fizycznych oraz brak ostrożności pracowników ochrony – mogą one powodować wtargnięcia do pomieszczeń, w których przetwarzane są dane w celu ich kradzieży;
- niewłaściwe zarządzanie personelem – wzbudzać może w pracownikach finansowe bądź poza finansowe motywy sprzedaży danych. Motywy finansowe wiązać się mogą z chęcią szybkiego zysku i wynikać mogą one z niskiego wynagrodzenia, niewłaściwego systemu premiowania itp. Z kolei do motywów poza finansowych zaliczyć można te związane ze światopoglądem, niską motywacją, chęcią zemsty i odwetu na pracodawcy, np. za odmowę przyznania podwyżki czy awansu.

5. Podsumowanie

Spoglądając na przedsiębiorstwo z punktu widzenia zachodzących w nim procesów można stwierdzić, że jednym z najważniejszych są te związane z gromadzeniem, przetwarzaniem oraz przesyłaniem informacji. Bowiem stanowią one podstawowy element wszystkich podejmowanych przez kierownictwo decyzji w zakresie produkcji (świadczeniu usług), finansów, logistyki, dystrybucji, marketingu czy zarządzania personelem. Dodatkowo rozwój teleinformatyki i sieci internet spotęgował znaczenie informacji w działalności każdej jednostki gospodarczej oraz budowaniu przewagi konkurencyjnej na rynku. Stąd też aktywa informacyjne stanowią jedne z najważniejszych zasobów przedsiębiorstwa, a ich udział w strukturze wartości wszystkich zasobów może osiągać nawet 80%. Wynika z tego, że aktywa informacyjne uznać należy za najważniejszy czynnik w osiąganiu celów każdego podmiotu gospodarczego.

Strategiczna wartość informacji powoduje, że liczba oraz skala incydentów związanych z ich zniszczeniem, kradzieżą, brakiem dostępności ciągle wzrasta. Wobec tego rozpoznawanie i ocena zagrożeń staje się podstawowym zadaniem, a jednocześnie wyzwaniem nie tylko dla przedsiębiorców, ale także pojedynczego człowieka. Mimo tego, że doświadczenia dnia codziennego wskazują na różnorodność zagrożeń bezpieczeństwa informacji, a w piśmiennictwie prezentowane są różne kategorie podziału niebezpieczeństw, katalog zagrożeń nadal pozostaje otwarty. Brakuje również jednego, ustandaryzowanego instrumentu, który mógłby być pomocy w procesie identyfikacji i oceny zagrożeń. Dlatego też wybór odpowiednich metod i narzędzi pod tym względem jest bardzo szeroki, a każdy sposób, który pozwoli na kompleksowe podejście do tego problemu można uznać za odpowiedni.

Z przeprowadzonych analiz wynika, że największym poziomem ryzyka charakteryzuje się zagrożenie polegające na nieuprawionym udostępnieniu danych. Jest to zagrożenie, które może powodować wiele negatywnych konsekwencji, do których zaliczyć można m.in.: rozpowszechnianie poufnych danych, w tym ujawnienie ich podmiotom konkurencyjnym, co powodować może straty finansowe oraz niefinansowe (np. utratę reputacji).

Nieuprawione udostępnienie danych może być przyczyną wielu różnych niedociągnięć przedsiębiorstwa oraz jego personelu. Jako przykład wskazać można brak właściwego podejścia firmy do zarządzania bezpieczeństwem informacji, co wiązać się może np. z brakiem odpowiednich procedur związanych z udostępnianiem informacji osobom trzecim, nieprowadzeniem ewidencji osób upoważnionych do przetwarzania określonego zakresu danych, nieświadomością pracowników, a w skrajnych sytuacjach tolerowaniem przez kierownictwo firmy niewłaściwych zachowań związanych z przetwarzaniem danych co sprzyjać może ich eskalacji. Tego rodzaju uchybienia prowadzić mogą nie tylko do przypadkowych zdarzeń związanych z ujawnieniem informacji, ale także celowego działania na szkodę przedsiębiorstwa. Poza tym pracownicy posiadający niewystarczającą wiedzę w zakresie ochrony informacji bardzo łatwo mogą stać się ofiarami ataków hackerskich oraz innych osób zainteresowanych wyłudzeniem danych. Istotną kwestią jest również należyte zadbanie o właściwy stan infrastruktury informatycznej (i jej właściwe zabezpieczenie), a także systemów chroniących przed przypadkowymi zdarzeniami (np. pożar) czy fizyczną penetracją (np. system alarmowy, system kontroli dostępu).

Reasumując, całość rozważań zawartych niniejszej pracy stwierdzić należy, że powszechnie stosowane w zarządzaniu jakością instrumenty pozwalają na kompleksową identyfikację zagrożeń dla bezpieczeństwa informacji, a także wnikliwą i rzetelną ich ocenę

pod względem źródeł ich powstawania i strat, jakie mogą one powodować dla przedsiębiorstwa, umożliwiając jednocześnie określenie potencjału doskonalenia procesów związanych z przetwarzaniem danych.

Literatura

1. Bączek P., „Zagrożenia informacyjne a bezpieczeństwo państwa polskiego", Wyd. Adam Marszałek, Warszawa 2009.
2. Borkowski S., Ulewicz R., „Zarządzanie produkcją. Systemy produkcyjne", Wyd. Humanitas, Sosnowiec 2009.
3. Frąś J., Gołębiewski M., Bielawa A., „Podstawy zarządzania jakością w przedsiębiorstwie", Wyd. Uniwersytetu Szczecińskiego, Szczecin 2006.
4. Hamrol A., „Zarządzanie jakością z przykładami", Wyd. PWN, Warszawa 2005.
5. https://www.cert.gov.pl/cer/publikacje/katalog-zagrozen-stosow/731,Katalog-zagrozen-stosowany-przez-CERTGOVPL.html [data dostępu: 03.01.2017].
6. https://www.governica.com/Jako%C5%9B%C4%87_informacji [data dostępu: 03.01.2013].
7. Janczak J., Nowak A., „Bezpieczeństwo informacyjne. Wybrane problemy", Wyd. AON, Warszawa 2013.
8. Korzeniowski L.F., „Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych" Wyd. EAS, Kraków 2008.
9. Koziej S., „Teoria sztuki wojennej", Wyd. Bellona, Warszawa 2011.
10. Łuczak J., Matuszak-Flejszman A., „Metody i techniki zarządzania jakością. Kompendium wiedzy", Wyd. Quality Progress, Poznań 2007.
11. Łuczak J., Tyburski M., „Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001", Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010.
12. Pałęga M., Knapiński M., Kulma W., „Zastosowanie metody FMEA do oceny poziomu bezpieczeństwa informacji w przedsiębiorstwie" [w] Innowacje w zarządzaniu i inżynierii produkcji, t.2, pod red. R. Knosali, Wyd., PTZP, Opole 2015.
13. PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia, Wyd. PKN, Warszawa 2012.
14. PN-ISO/IEC 27001:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. Wymagania, Wyd. PKN, Warszawa 2013.
15. PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki Bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, Wyd. PKN, Warszawa 2013.
16. Wołowski F., Zawiła-Niedźwiecki J., „Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi", Wyd. Edu-Libri, Kraków–Warszawa 2012.
17. Zintegrowane zarządzanie jakością", pod red. J. Więcka, Wyd. Uniwersytetu Łódzkiego, Łódź 2007.
18. Zymonik Z., Hamrol A., Grudowski P., „Zarządzanie jakością i bezpieczeństwem", Wyd. PWE, Warszawa 2013.

Dr inż. Michał PAŁĘGA
Dr hab. inż. Marcin KNAPIŃSKI, prof. PCz.
Dr hab. inż. Dariusz RYDZ, prof. PCz.
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Wydział Inżynierii Produkcji i Technologii Materiałów
Politechnika Częstochowska
42 – 201 Częstochowa, Dąbrowskiego 69

tel./fax: (034) 325 07 82
e-mail: mpalega@wip.pcz.pl
knap@wip.pcz.pl
rydz@wip.pcz.pl