Akademia Ekonomiczna w Poznaniu
Wydział Informatyki
i Gospodarki Elektronicznej

ROZPRAWA DOKTORSKA

Metoda oceny ryzyka związanego z bezpieczeństwem systemów informatycznych dla potrzeb ubezpieczenia

mgr Aleksander Poniewierski

rozprawa doktorska
przygotowana pod kierunkiem
prof. dr hab. inż. Wojciecha Cellarego

Poznań, 2008

SPIS TREŚCI

1 Wstęp

Na przestrzeni minionych lat rola systemów informatycznych w gospodarce zmieniła się w sposób znaczący. Trzydzieści lat temu systemy informatyczne były jedynie wsparciem dla automatyzacji produkcji, później były traktowane jako czynnik umożliwiający redukcję kosztów produkcji przez zmniejszenie zatrudnienia. Obecnie ich rola jest zupełnie inna – traktuje się je jako główne narzędzie służące do realizacji strategicznych celów organizacji, a realizacja tych celów ma za zadanie uzyskanie konkretnych korzyści ekonomicznych, krótko i długofalowych. Zmianę roli systemów informatycznych w ostatnich dekadach można postrzegać jako wynik przemian, które dokonywały się w otoczeniu biznesu, ale oddziaływały na organizacje, przemysł, procesy biznesowe i metody zarządzania. Można wyróżnić cztery podstawowe kategorie tych przemian:

1. Socjologiczne, wynikające ze zwiększonych oczekiwań konsumentów dotyczących nowych produktów, ich jakości, ceny i z dbałości o ochronę środowiska oraz przemian związanych z wyłanianiem się globalnego społeczeństwa informacyjnego[1];
2. Polityczne, spowodowane zmianami zaistniałymi w Europie, takimi jak powstanie jednolitego rynku europejskiego, powszechna globalizacja czy upadek ZSRR;
3. Ekonomiczne, na które wpływ mają silne gospodarki takich państw jak Stany Zjednoczone, Japonia czy zjednoczone Niemcy oraz nowi gracze gospodarczy, tacy jak Chiny i Indie;
4. Technologiczne, będące efektem gwałtownego rozwoju produktów, procesów i nowych technologii, w szczególności informatyczno-telekomunikacyjnych.

Na skutek rozwoju nowych technologii gwałtownie zwiększyły się możliwości systemów informatycznych – zwiększyła się moc obliczeniowa komputerów i pojemność ich pamięci, poprawiła się komunikacja przez sieci telekomunikacyjne, przewodowe i

[1] Cellary, W., "Globalization from the Information and Communication Perspective", Proc. The 4th International Conference on Distributed Computing and Internet Technology ICDCIT 2007, Bangalore (India), December 17-20, 2007, Tomasz Janowski, Hrushikesha Mohanty (eds.), Lecture Notes in Computer Science No 4882; Springer-Verlag Berlin Heidelberg, pp. 283-292. [15]

bezprzewodowe, przy jednoczesnym ciągłym obniżaniu kosztów zastosowań tych technologii. Równocześnie organizacje zaczęły działać pod silną presją konkurencji, zatem informatyka stała się niezbędnym narzędziem przetrwania organizacji na rynku i jej rozwoju. W wyniku tych przemian zaistniało duże zapotrzebowanie na kompleksowe rozwiązania informatyczne[2], takie jak: zintegrowane systemy zarządzania, centralne systemy informatyczne i hurtownie danych[3]. Ich zadaniem jest utrzymywanie, przetwarzanie i przesyłanie coraz większej ilości informacji. Stymulują one rozwój technik multimedialnych i wzrost ich zastosowań w biznesie, rozwój telekomunikacji oraz powstanie zupełnie nowego sektora działalności gospodarczej jakim jest elektroniczny biznes.

Wraz z rozwojem przedsiębiorstw wzrasta też troska właścicieli o ich majątek, a informacje stały się jednym z istotnych elementów tego majątku. Stale rosnąca ilość i wartość informacji powoduje wzrost zagrożeń, dlatego niezwykle istotnym problemem staje się ochrona systemów informatycznych i przetwarzanych przez nie danych, albowiem zapewnienie bezpieczeństwa systemom informatycznym służy tak naprawdę zabezpieczeniu interesów całej organizacji. Przez ochronę systemów informatycznych rozumie się działania mające na celu zapobieganie wystąpieniom zdarzeń niekorzystnych dla systemów informatycznych lub minimalizację skutków ich wystąpienia[4].

Wprawdzie równolegle z rozwojem systemów, rozwijają się również technologie zabezpieczeń, muszą one jednak być starannie dobierane i odpowiednio zarządzane. Zapewnienie bezpieczeństwa nie jest bowiem aktem jednorazowym, polegającym tylko na wdrożeniu zabezpieczeń, lecz procesem – ciągłym, dynamicznym i bardzo złożonym, wymagającym stałego nadzoru i bieżącego przystosowywania do zmiennych warunków otoczenia[5].

Właściciele majątku zawsze dążą do uniknięcia zdarzeń mogących spowodować szkody w ich własności oraz konsekwencji tych zdarzeń. Samo pojęcie szkody nie zostało

---

[2] Cellary, W., "Zarządzanie informacją zamiast zarządzania dokumentami drogą do unowocześnienia administracji", w: Krajowa Administracja Skarbowa, t. III: Nowoczesna Administracja Skarbowa, Ministerstwo Finansów, Warszawa, Wyd. DELFIN, pp. 173-183, 2007. [16]

[3] Merkury. 2004. IT Governance – Running IT like business. White Paper (www.mercury.com) [za Carr, Nicholas G., Does IT Matter? Information Technology and the Corrosion of Competitive Advantage, Harvard Business School Press, April 2004.] [58]

[4] Wong K., 1977, Risk Analysis and Control. Manchester: National Computer Center Publications. Wood C., 1990, Principles of secure information systems design, Computers & Security 9, 1 (Feb), str. 13 - 24. [126]

[5] Białas A., 2006, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT, str. 167 [5]

jednoznacznie zdefiniowane, jednak w literaturze prawnej *szkodą określa się uszczerbek, jakiego doznał poszkodowany w dobrach i interesach wszelkiego rodzaju chronionych przez prawo, wbrew swojej woli*[6]. Zatem za uszczerbek w majątku można uznać zarówno utratę majątku w sensie fizycznym jak i utratę spodziewanych korzyści, które przedsiębiorstwo mogłoby osiągnąć, gdyby szkoda nie zaistniała. Kodeks cywilny stanowi: „*…naprawienie szkody obejmuje straty, które poszkodowany poniósł, oraz korzyści, które mógłby osiągnąć, gdyby szkody nie wyrządzono*".[7] Szkoda, którą poszkodowany poniósł w terminologii prawniczej jest określana terminem *damnum emergens,* natomiast strata korzyści, które poszkodowany mógłby osiągnąć gdyby strata w majątku nie nastąpiła określana jest terminem *lucrum cessans.*

Zatem jak zauważa M. Kuchlewska *„straty, na jakie naraża przedsiębiorstwo jego otoczenie oraz straty, na jakie naraża się przedsiębiorstwo swoimi decyzjami wyznaczają zakres jego ryzyka"*[8], gdzie ryzyko rozumiane jako zagrożenie, oznacza li tylko możliwość wystąpienia określonych zdarzeń i ich skutków, a nie pewność wystąpienia, przy czym wielkości ryzyka rosną wraz ze wzrostem skali działalności przedsiębiorstwa oraz zakresu jego działania. Do tej definicji można dodać jeszcze trzecią możliwość, a mianowicie straty, na jakie może być narażone otoczenie przez niewłaściwe decyzje przedsiębiorstwa.

Postęp w zakresie nauk o zarządzaniu doprowadził do powstania w połowie lat sześćdziesiątych nowej wyspecjalizowanej dyscypliny zarządzania, jaką jest zarządzanie ryzykiem organizacji[9]. Przez zarządzanie ryzykiem określa się „*proces, obejmujący całokształt działań podejmowanych przez podmiot w celu panowania nad ryzykiem, nastawionych na zapewnienie bezpieczeństwa działalności i osiągania celów przy zachowaniu optymalnego poziomu kosztu ryzyka*"[10]. Głównym celem zarządzania ryzykiem organizacji jest zarówno poprawa wyników finansowych jak też ograniczenie możliwych strat przez kontrolowanie ryzyka.

Jako pierwsze ideę zarządzania ryzykiem jako funkcji organizacji przyjęły instytucje finansowe, choć początkowo zarządzanie ryzykiem dotyczyło tylko zarządzania

---

[6] Duży A., 1993, Dyferencyjne metoda ustalania wysokości szkody. Państwo i Prawo nr 10 [34]
[7] Art. 361 §2 k. c. wymienia obie postacie szkody w przepisach księgi trzeciej Zobowiązania
[8] Kuchlewska M., 2003, Ubezpieczenie jako metoda finansowania ryzyka przedsiębiorstw. Akademia Ekonomiczna w Poznaniu, str. 40 [51]
[9] Różycki, P. Jak ubezpieczają się przedsiębiorstwa, Wiadomości Ubezpieczeniowe, 2005, nr ¾ [103]
[10] Kuchlewska M., op. cit., str. 70 [51]

pakietem ubezpieczeniowym firmy w celu optymalizacji budżetu ubezpieczeń w zależności od zakresu zabezpieczeń i kosztów z nimi związanych. Z czasem ten rodzaj zarządzania ewoluował w kierunku odejścia od tradycyjnych produktów ubezpieczeniowych na rzecz zarządzania systemowego określanego jako *kompleksowe zarządzanie ryzykiem* (ang. total risk management), które swoim zasięgiem obecnie obejmuje[11]:

1. pomoc dla organizacji w zakresie identyfikacji ryzyka,
2. wdrażanie programów zapobiegania stratom i programów kontroli szkodowości,
3. opiniowanie umów i dokumentów wykorzystywanych w zarządzaniu ryzykiem,
4. prowadzenie szkoleń z zakresu bezpieczeństwa (bezpieczeństwo miejsca pracy, prawo do informacji),
5. działania w celu zapewnienia zgodności z zaleceniami instytucji rządowych lub ustawodawczych,
6. projektowanie nieubezpieczeniowych programów finansowania (np. programów samoubezpieczeniowych lub tworzenia filii zależnych towarzystw ubezpieczeniowych),
7. zarządzanie roszczeniami oraz współpracę z radcami prawnymi w procesach sądowych.

Wobec tak szerokiego pojmowania problemu kompleksowego zarządzania ryzykiem, metody zarządzania nim ulegają ewolucji. Jednym z rodzajów aktywności przedsiębiorstw w ramach zarządzania ryzykiem są działania zmierzające do transferu ryzyka na inne podmioty, który można dokonywać na trzy sposoby[12]:

- przez transfer działalności obarczonej ryzykiem, którego podmiot nie chce podejmować, na inne podmioty w ramach umów kooperacyjnych,
- przez transfer odpowiedzialności za straty na kontrahentów, na podstawie kontraktowych klauzul o charakterze wyłączeniowym,

[11] Wiliams C. A., Smith M. L., Young P. C., 2002, Zarządzanie ryzykiem a ubezpieczenia. Wydawnictwo Naukowe PWN, str. 53 [124]
[12] Kuchlewska M., ibidem, str. 71 [51]

- przez transfer odpowiedzialności finansowej za straty na zakłady ubezpieczeń, na podstawie umów ubezpieczenia.

Pierwsze dwa sposoby są już powszechnie wykorzystywane przez organizacje gospodarcze, jako najprostsze i najłatwiejsze do zastosowania, a także najtańsze, natomiast strategia transferu ryzyka na zakłady ubezpieczeniowe jest wciąż jeszcze nie dość efektywnie wykorzystywana, zazwyczaj z powodu braku dobrze przygotowanej oferty rynkowej. Natomiast ryzyko związane z nieprawidłowym przetwarzaniem informacji w systemach informatycznych w ogóle nie jest traktowane jako przedmiot zainteresowania zakładów ubezpieczeniowych. Nawet bardzo pobieżne wywiady z osobami odpowiedzialnymi w polskich przedsiębiorstwach za bezpieczeństwo systemów informatycznych potwierdziły, że istnieje duże zapotrzebowanie na złożone produkty ubezpieczeniowe od ryzyk związanych z bezpieczeństwem systemów informatycznych, przy całkowitym braku podaży ze strony zakładów ubezpieczeń. Oznacza to, że problem tkwi w braku możliwości dostarczenia takiego produktu przez zakład ubezpieczeń, a powodem nieoferowania na rynku europejskim produktów ubezpieczeniowych tego typu jest brak po stronie zakładów ubezpieczeń odpowiedniej metody służącej ocenie ryzyka związanego z bezpieczeństwem systemów informatycznych. Po przeanalizowaniu szeregu metod dedykowanych dla oceny tego ryzyka okazało się, że są one nieprzydatne z punktu widzenia zakładów ubezpieczeń. Dlatego celem tej rozprawy jest przedstawienie oryginalnej metody oceny bezpieczeństwa systemów informatycznych **ORBI** (**O**cena **R**yzyka **B**ezpieczeństwa systemów **I**nformatycznych), za pomocą której zakłady ubezpieczeń mogą precyzyjnie diagnozować stan bezpieczeństwa systemów informatycznych przedsiębiorstw występujących o udzielenie ochrony ubezpieczeniowej oraz wyznaczyć wartość ryzyka związanego z bezpieczeństwem tych systemów.

Teza rozprawy jest następująca:

> *Metoda **ORBI** umożliwia zakładowi ubezpieczeń wykonanie obiektywnej, jednoznacznej i porównywalnej oceny ryzyka związanego z bezpieczeństwem systemów informatycznych przy udzielaniu podmiotom gospodarczym ochrony od skutków materializacji ryzyk wynikających z nieprawidłowego przetwarzania informacji w systemach informatycznych.*

Za jej pomocą zakład ubezpieczeń będzie mógł opracowywać i sprzedawać produkty ubezpieczeniowe adresowane do firm szczególnie zainteresowanych tego typu ofertą oraz wyznaczać indywidualne warunki dla poszczególnych organizacji w zakresie ubezpieczenia jej systemów informatycznych,

Organizacja rozprawy jest następująca:

W **rozdziale drugim** przedstawiono problematykę bezpieczeństwa systemów informatycznych. Sklasyfikowano i przeanalizowano metody oceny i zarządzania ryzykiem związane z bezpieczeństwem systemów informatycznych. Wskazano specyfikę wszystkich tego typu metod oraz cechy różniące je między sobą.

W **rozdziale trzecim** przedstawiono aktualny stan wiedzy w zakresie ubezpieczeń w szczególności z zakresu bezpieczeństwa systemów informatycznych. Dokonano analizy produktów ubezpieczeniowych oraz generalnych warunków umów na nie wskazując ich słabości i ograniczenia. Rozdział zakończono podsumowaniem, które jest zarazem krytyką obecnego stanu wiedzy i postawieniem problemu badawczego.

Rozdział czwarty jest poświęcony metodzie ORBI (**O**ceny **R**yzyka **B**ezpieczeństwa systemów **I**nformatycznych). Najpierw jest przedstawiona ogólna koncepcja metody ORBI, a następnie jest szczegółowo opisana sama metoda.

Rozdział piaty przedstawia przykład zastosowania metody ORBI.

W **rozdziale szóstym** podsumowano całość rozprawy i wskazano kierunki dalszych prac badawczych, w szczególności w zakresie możliwości rozbudowy metody ORBI.

2 Bezpieczeństwo systemów informatycznych i przetwarzanych przez nie danych

Postęp technologiczny końca XX i początku XXI wieku wymusza zmiany strategii biznesowych, określając nowe kierunki rozwoju organizacji gospodarczych[13]. Głównym celem tych zmian jest usprawnienie procesów biznesowych i produkcyjnych, służących zwiększeniu wydajności, efektywności i jakości przez maksymalne wykorzystanie istniejących zasobów materialnych, niematerialnych i ludzkich. Możliwości nowoczesnej technologii dają firmom szansę na osiągnięcie przewagi konkurencyjnej. Organizacje gospodarcze informatyzując się mogą nie tylko przyspieszyć procesy decyzyjne dzięki szybkiej wymianie informacji, skrócić procesy produkcyjne i organizacyjne, ale też zmniejszyć zapasy magazynowe przez zastosowanie nowoczesnych programów logistycznych, zredukować koszty transakcji oraz lepiej poznać potrzeby klientów dzięki np.: kontroli struktury zakupów i ich regionalizacji. Rozwój Internetu zrewolucjonizował techniki sprzedaży oraz spowodował powstanie nowych rodzajów usług. Informatyzacja procesów przepływu informacji pomiędzy organizacją a klientami ułatwia dotarcie do nich z nową ofertą, przyspiesza wymianę handlową upraszczając transakcje finansowe dzięki możliwości dokonywania płatności elektronicznych i umożliwia dostęp klientów do pełnej oferty, niezależnie od lokalizacji firmy. Dzięki niej jest również możliwe rozpoznanie potrzeb klientów i śledzenie ich preferencji, a także generowanie popytu na nowe, nieistniejące wcześniej produkty lub usługi, a następnie ciągłe ich udoskonalanie.

2.1 Zarządzanie organizacją gospodarczą z uwzględnieniem roli systemów informatycznych

Rozwój technologii informatycznych, a zwłaszcza integracja technologii informatycznych z procesami biznesowymi, powoduje konieczność właściwego zabezpieczenia zasobów informatycznych organizacji, od których często są uzależnione jej wyniki ekonomiczne. Właściwe zabezpieczenie zasobów zależy w dużym stopniu od kultury organizacyjnej przedsiębiorstw oraz przyjętego modelu zarządzania.

[13] Cellary, W. (ed.), *Polska w drodze do społeczeństwa informacyjnego. Raport o rozwoju społecznym,* , UNDP, ISBN: 83-917047-5-0, 01/2002. [18]

W latach dziewięćdziesiątych XX wieku bardzo dużą popularność w teorii zarządzania zdobyło podejście procesowe[14] wywodzące się z koncepcji *doskonalenia procesów biznesowych* (ang. business process reengineering). Twórcami tego podejścia byli M. Hammer i J. Champy[15]

Zgodnie z koncepcją *doskonalenia procesów biznesowych* w centrum uwagi osób zarządzających organizacjami gospodarczymi znalazły się procesy. W tej koncepcji przyjęto, że czynnikami przesądzającymi w rozwoju współczesnych organizacji stała się umiejętność wykorzystania potencjału intelektualnego wszystkich uczestników organizacji, wsparta technologią informatyczną i automatyzacją[16].

Ze względu na znaczenie dla organizacji, procesy grupuje się w następujących kategoriach[17]:

1. Strategiczne – związane z definiowaniem wizji, misji, celów i strategii organizacji. Procesy te mają bezpośredni wpływ na dalsze procesy składowe, natomiast nie dotyczą bezpośrednio systemu informatycznego.
2. Główne procesy operacyjne – będące kluczowym elementem działania każdej firmy i instytucji. Nadają one tempo jej działalności.
3. Pomocnicze procesy operacyjne.

Ze względu na miejsce przestrzenno-organizacyjne, wyróżnia się procesy:

- wewnątrzfunkcyjne – procesy zawierają się w ramach jednej funkcji (np.: w zaopatrzeniu), lub komórki organizacyjnej (np.: magazynie zaopatrzenia),
- międzyfunkcyjne – procesy przebiegają przez różne komórki realizujące różne funkcje przedsiębiorstwa (przygotowanie nowego produktu, wykonanie zamówienia klienta).

Procesy biznesowe z natury rzeczy mają tendencję do przechodzenia przez kilka jednostek organizacyjnych firmy, a rosnący stopień ich komplikacji przekłada się na coraz większą złożoność systemów informatycznych. Systemy te, obsługujące różne działy

[14] Według Polskiej Normy podejście procesowe jest definiowane jako „systematyczna identyfikacja procesów stosowanych w organizacji i zarządzanie nimi, a szczególnie wzajemnymi oddziaływaniami między takimi procesami" (zob. Systemy zarządzania jakością. Podstawy i terminologia. PNEN ISO 9000. PKN 2001, s.15.
[15] Hammer M., Champy J.: Reengineering w przedsiębiorstwie, Neumann Management Institute, Warszawa 1996, s. 45-49. [45]
[16] Grajewski P.: Koncepcja struktury organizacji procesowej. Dom Organizatora Toruń 2003 s. 7-8 [44]
[17] Audyt wewnętrzny. Spojrzenie praktyczne. Stowarzyszenie księgowych w Polsce, Warszawa 2003 s. 77 [2]

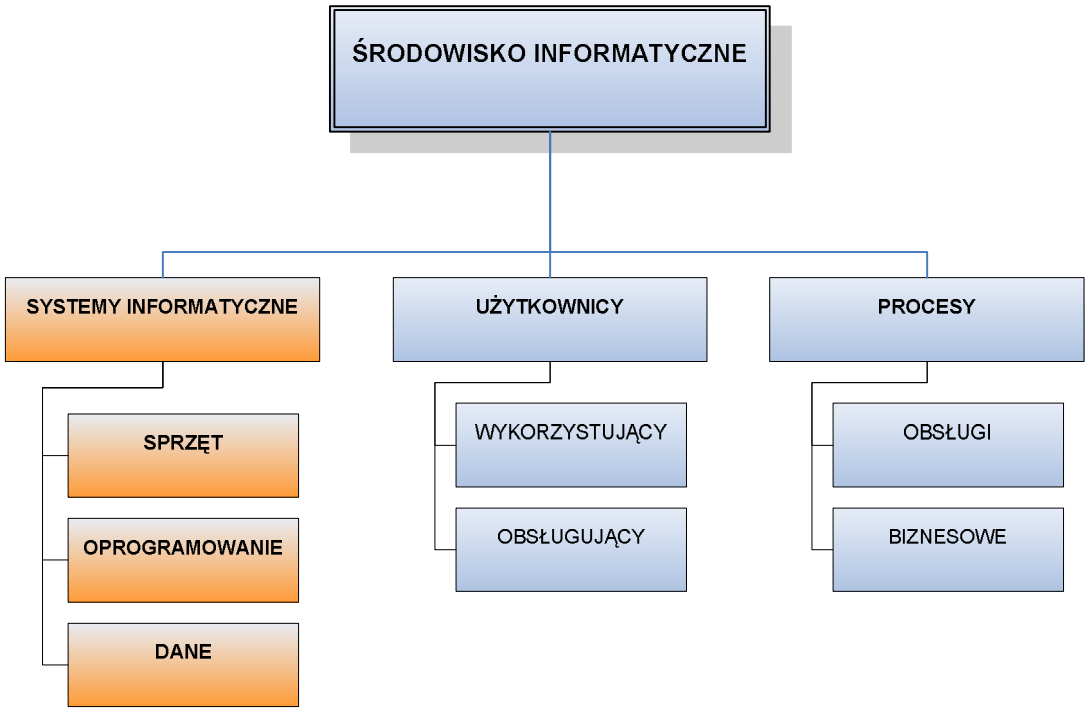
przedsiębiorstwa, muszą być integrowane. Ponadto, systemy informatyczne ulegają ciągłym zmianom, gdyż muszą być na bieżąco dopasowywane do zmiennych wymagań procesów biznesowych.

2.2 Składowe środowiska informatycznego organizacji gospodarczej

W rozwiniętej gospodarce, nie ma już praktycznie organizacji niekorzystających z mniej lub bardziej rozwiniętych systemów informatycznych, których osadzenie w konkretnym środowisku informatycznym służy realizacji procesów biznesowych[18] [19] [20].

Na środowisko informatyczne organizacji gospodarczej składają się zasoby materialne, które stanowią elementy składowe środowiska informatycznego organizacji gospodarczej, zasoby ludzkie, czyli użytkownicy tych systemów, i procesy niezbędne do prawidłowego funkcjonowania przedsiębiorstwa[21] [22] [23].

[18] Carvalho, J.A. 2000. Information System? Which one do you mean? Universidade do Minho, Departamento de Sistemas de Informacao. Portugalia. [13]
[19] Falkenberg, E.D., Hesse, W., Lindgreen, P., Nilssen, B.E., Oei, J.L.H., Rolland, C., Stamper, R.K., Assche, F.J.M.V., Verrijn-Stuart, A.A., Voss, K. 1996. FRISCO: A Framework of Information Systems Concepts, IFIP WEDŁUG 8.1 Task Group FRISCO. [35]
[20] Falkenberg, E.D. Rolland, C. 1992. Information Systems Concepts: Improving the Understanding, North-Holland. [36]
[21] Cellary, W., "People and Software in a Knowledge-Based Economy", *Computer, January 2005, Volume 38, No 1*, IEEE Computer Society, pp. 114-116, 01/2005. [17]
[22] Finkelstein, C. 1989. An Introduction to Information Engineering: From Strategic Planning to Information Systems. Sydney: Addison-Wesley.[38]
[23] Le Moigne, J.-L. 1977. La Théorie du Système Général: Théorie de la Modélisation, Presses Universitaires de France. [53]



Rysunek 2.2.-1Środowisko informatyczne organizacji gospodarczej

[źródło: opracowanie własne]

2.2.1 Systemy informatyczne

Systemy informatyczne składają się z trzech podstawowych elementów[24]:

1. Sprzętu (ang. hardware), czyli urządzeń komputerowych, okablowania telekomunikacyjnego, zasilania oraz urządzeń i pomieszczeń, w których znajduje się sprzęt informatyczny, na który w szczególności składają się:
   - serwery,
   - urządzenia sieciowe,
   - terminale użytkownika,
   - urządzenia składowania danych,
   - specjalizowany sprzęt służący bezpieczeństwu i niezawodności systemu informatycznego.

[24] Gerrard, M. 2003. Creating an effective IT Governance process. Gartner Research (com-21-2931) [41]

2. Oprogramowania (ang. software) zainstalowanego na sprzęcie informatycznym, na które składają się:
    - system operacyjny – jest to oprogramowanie zarządzające podstawowymi działaniami systemu informatycznego;
    - systemy zarządzania bazami danych – jest to oprogramowanie służące do gromadzenia i udostępniania danych;
    - aplikacje – jest to oprogramowanie służące do wprowadzania danych do systemu informatycznego przez jego użytkowników, przetwarzania danych dla potrzeb, dla których system informatyczny został zbudowany i wdrożony, oraz prezentacji danych użytkownikom we właściwej formie.
3. Danych, zarówno o konfiguracji sprzętu jak i reprezentujących informacje biznesowe.

2.2.2 Użytkownicy

Wśród użytkowników środowiska informatycznego organizacji gospodarczej wyróżnia się:

1. Użytkowników korzystających z aplikacji systemów informatycznych, używających zaszytej w nich logiki biznesowej i przetwarzających za ich pomocą dane składowane w bazach danych.
2. Użytkowników uprawnionych do obsługi systemów informatycznych, realizujących funkcje operacyjne, rozwoju i wsparcia.

2.2.3 Procesy zachodzące w systemach informatycznych

Integracja technologii informacyjnej z procesami biznesowymi ma na celu osiągnięcie korzyści dla organizacji, której dotyczy, oraz jej klientów. Procesy informatyczne można podzielić ze względu na funkcję, jaką pełnią w organizacji, na następujące rodzaje:

1. Biznesowe, związane z aplikacjami służącymi określonym celom:
    - planowaniu zasobów przedsiębiorstwa,
    - finansowo-księgowym,
    - zarządzaniu relacjami z klientami,
    - zarządzaniu przepływem prac,

- logistyce,
- produkcji.

2. Obsługi systemu informatycznego:
    - operacyjne – podstawowe, powtarzalne działania, realizowane przez użytkowników uprawnionych do tych działań, związane z wykonywaniem rutynowych czynności, nie wymagające zbyt wysokich kompetencji,
    - eksploatacyjne – bieżące, niezbędne do zapewnienia dostępności rozwiązań informatycznych w tym bieżące wsparcie użytkowników, usuwanie awarii, nadzór itp.,
    - utrzymania – bieżące, niezbędne do zapewnienia dostępności, wydajności i ciągłości w średnim i długim okresie czasu,
    - rozwoju – dotyczące planowania zmian w systemie informatycznym przez wdrażanie nowych rozwiązań i przekazywania ich do eksploatacji lub modyfikacje istniejących systemów informatycznych.

Systemy informatyczne wraz z zachodzącymi w nich procesami są podstawowymi narzędziami wspomagającymi działalność organizacji gospodarczych w XXI wieku. Są one również elementami współpracy i konkurowania organizacji pomiędzy sobą. W zależności od wielkości i charakteru organizacji, społecznego i biznesowego znaczenia realizowanych przez nią zadań, poziomu informatyzacji, a także roli, jaką organizacja przypisze do konkretnego systemu informatycznego, poszczególne systemy pełnią w niej różne funkcje. Dlatego systemy te można sklasyfikować według dwóch powszechnie przyjętych i ważnych z punktu widzenia organizacji kryteriów[25]:

1. Istotności, czyli miary ważności danego systemu informatycznego dla całości organizacji.
2. Bezpieczeństwa, czyli ochrony danych i zasobów przed przypadkowym lub złośliwym działaniem takim jak: zniszczenie, modyfikacja lub ujawnienie, przy wykorzystaniu środków służących poprawnemu przetwarzaniu danych przez

[25] Woodley, B. 2001. The Impact of Transformative Technologies on Governance: Some Lessons from History. Institute on Governance. Ontario. [127]

system informatyczny przy równoczesnym adekwatnym poziomie ochrony poufności danych.

2.3 Pojęcie bezpieczeństwa systemów informatycznych i przetwarzanych przez nie danych

W Polskiej Normie przyjęto następującą definicję bezpieczeństwa systemu informatycznego: „*ochrona danych i zasobów przed przypadkowymi lub złośliwymi czynami, polegająca zwykle na podjęciu właściwych działań*”[26]. Zgodnie z tą definicją należy mówić o systemie bezpieczeństwa jako szeregu powiązanych ze sobą procesów, z których każdy ma swoją wartość dla całego systemu i jednocześnie każdy z nich determinuje wartość całości systemu.

2.4 Zagrożenia dla systemu informatycznego

Zagrożenia, na jakie jest narażony system informatyczny, to takie czynniki, które w sposób przypadkowy lub celowy mogą doprowadzić do ujawnienia przetwarzanej w nim informacji, utraty integralności tych informacji lub ich niezamierzonej modyfikacji a także mogą doprowadzić do sytuacji, gdy system informatyczny będzie niedostępny przez określony czas dla swych użytkowników, przez co nie będą oni mogli realizować swoich zadań przy zakładanych parametrach jakościowych i w określonym czasie. Dlatego zagrożenia związane z nieprawidłowym przetwarzaniem informacji: wytwarzanych, przetwarzanych, przechowywanych i przesyłanych przez system, mogą spowodować znaczne straty dla organizacji, której ten system służy.

Standard Brytyjski BS 7799[27] i jego odpowiednik Polska Norma ISO/IEC 17799 opisuje zagrożenia dokonując równocześnie ich klasyfikacji:

[26] PN-I-02000, marzec 2002, Technika informatyczna, Zabezpieczenia w systemach informatycznych. Terminologia [118]
[27] British Standard, BS 7799, 1995. (Information Security Management), Part 1: Code of practice for information security management. [8]

…" W coraz większym stopniu instytucje i ich systemy i sieci informatyczne stają w obliczu zagrożeń pochodzących z wielu źródeł, takich jak: oszustwa dokonywane za pomocą komputera, szpiegostwo, sabotaż, wandalizm, pożar lub powódź. Źródła uszkodzeń takie jak: wirusy komputerowe, hakerstwo komputerowe i ataki powodujące odmowę usługi stają się coraz powszechniejsze, ambitniejsze i bardziej wyrafinowane." [28]

Według tej klasyfikacji zagrożenia dla systemów informatycznych dzieli się na następujące grupy:

1. Naturalne – tę grupę stanowią wszelkie niekorzystne dla systemów informatycznych aktywności przyrody tj. powodzie, tornada, burze śnieżne i deszczowe, pożary, trzęsienia ziemi itp. Wartości tej klasy zagrożeń są zazwyczaj wyznaczane z danych statystycznych. W szczególności jest określana częstotliwość (średnia arytmetyczna lub mediana) występowania danego zagrożenia w przeciągu określonego czasu (roku kalendarzowego) na danym terytorium.
2. Techniczne – do tej grupy zalicza się wszelkie nieprawidłowości działania sprzętu wchodzącego w skład systemów informatycznych lub elementów, od których nieprzerwanej pracy zależy ich poprawne działanie.
3. Programowe – największa i najbardziej nieokreślona grupa zagrożeń. W jej skład wchodzą zarówno umyślne jak i nieumyślne błędy oprogramowania samego systemu informatycznego, jak i programy, których celem jest zakłócenie poprawnego funkcjonowania systemów informatycznych (np.: wirusy, robaki, konie trojańskie i inne groźne programy komputerowe).
4. Środowiskowe – zbiór wszelkich czynników, bezpośrednio i pośrednio związanych z systemami informatycznymi, które niekorzystnie wpływają na poufność, dostępność lub integralność danych. Większość zagrożeń tej grupy stanowią działania użytkowników systemów informatycznych. W tej grupie można wyodrębnić dwa rodzaje:
    - działania nieumyślne, takie jak np.: błędy operatorskie,

[28] Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, 2003. PN-ISO/IEC 17799. str. 8. [117]

- działania umyślne, takie jak: próby penetracji i włamań, ataki destrukcyjne, podsłuch i przechwytywanie połączeń sieciowych, kradzież danych, nadużycia, niedozwolone działania operatorskie itp.

2.5 Podatność systemów informatycznych na zagrożenia

W literaturze przedmiotu problem podatności systemów informatycznych na zagrożenia jest przedstawiany na dwa sposoby. Po pierwsze, przez podatność rozumie się „*słabość lub lukę w systemie przetwarzania danych* (3.1.074)”[29], co oznacza możliwość dokonywania analizy i wyznaczania stopnia podatności (np. w metodzie CRAMM). Po drugie, przez podatność rozumie się „*wady i luki w strukturze fizycznej, organizacji, procedurach, zarządzaniu, administrowaniu, sprzęcie, oprogramowaniu, a także zamierzone lub niezamierzone działania personelu, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika* (3.1.075)[30]. W tej rozprawie przyjęto to drugie rozumienie podatności systemów informatycznych na zagrożenia, ponieważ jest wieloaspektowe.

Zgodnie z przyjętą definicją, system informatyczny organizacji gospodarczej może znajdować się w jednym z dwóch stanów podatności na dane zagrożenie:

- nie jest podatny na dane zagrożenie – oznacza to, że dane zagrożenie nie jest adekwatne dla systemu informatycznego, czyli pomimo realizacji, zagrożenie to nie ma wpływu na system informatyczny;
- jest podatny na dane zagrożenie – oznacza to, że dane zagrożenie może mieć wpływ na system informatyczny, czyli realizacja zagrożenia będzie miała wpływ na system informatyczny, a w konsekwencji na organizację i jej otoczenie.

[29] PN-I-02000, marzec 2002, Technika informatyczna, Zabezpieczenia w systemach informatycznych. Terminologia. [118]
[30] PN-I-02000, marzec 2002, Technika informatyczna, Zabezpieczenia w systemach informatycznych. Terminologia. [118]

2.6 Ryzyko związane z bezpieczeństwem systemów informatycznych

Jeżeli system informatyczny jest podatny na zagrożenie, to znaczy, że jest narażony na ryzyko związane z jego bezpieczeństwem. Ryzyko związane z bezpieczeństwem systemu informatycznego można zdefiniować jako „*prawdopodobieństwo, że podatność zasobu lub grupy zasobów zostanie wykorzystana przez określone zagrożenie, aby spowodować straty lub zniszczenie zasobów*”[31]. Bezpieczeństwo systemu informatycznego obejmuje trzy podstawowe atrybuty: poufność, dostępność i integralność, które Polska Norma PN-13335-1 definiuje następująco[32]:

1. Poufność – jest to właściwość danych, wskazująca obszar, w którym te dane nie powinny być dostępne lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom.
2. Dostępność – jest to właściwość danych lub zasobów polegająca na tym, że mogą one być dostępne i wykorzystywane na żądanie uprawnionej jednostki.
3. Integralność – jest to właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.

W związku z powyższą klasyfikacją atrybutów, można wyodrębnić trzy główne kategorie ryzyk związanych z opisanymi atrybutami:[33]

1. Ryzyko utraty poufności – system informatyczny jest podatny na zagrożenia mogące doprowadzić do ujawnienia osobom nieuprawnionym danych poufnych.
2. Ryzyko utraty dostępności – system informatyczny jest podatny na zagrożenia mogące doprowadzić do braku dostępu autoryzowanych użytkowników do systemu informatycznego, aplikacji lub danych przez pewien czasie.
3. Ryzyko utraty integralności – system informatyczny jest podatny na zagrożenie mogące doprowadzić do nieautoryzowanej zmiany danych przetwarzanych przez ten system.

---

[31] PN-I-13335-1, styczeń 1999, Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych. [119]

[32] PN-I-02000, marzec 2002, Technika informatyczna, Zabezpieczenia w systemach informatycznych. Terminologia. [118]

[33] Zasady szacowania ryzyka technologicznego (pr. zb.) 1999, Conference Papers. The Third Conference of the Polish-British School of Insurance, Zakopane [129]

Materializacja opisanych ryzyk systemu informatycznego może spowodować duże straty dla organizacji, dlatego te ryzyka muszą być uwzględnione w procesie zarządzania ryzykiem całej organizacji, a nie tylko być elementem zarządzania ryzykiem procesów informatycznych.

2.7 Ekonomiczne skutki materializacji ryzyk utraty poufności, dostępności i integralności dla organizacji gospodarczych

Jednym z największych zagrożeń dla organizacji korzystających z nowoczesnych technologii informatycznych jest materializacja ryzyk wymienionych w rozdziale 2.6. Zagrożeniom tym sprzyja zarówno stale rosnąca liczba użytkowników systemów informatycznych, rosnąca liczba specjalistów mogących spowodować straty w celach przestępczych, jak i wysoka standaryzacja sprzętu komputerowego ułatwiająca osobom nieuprawnionym dostęp do cudzych zasobów informatycznych. Materializacja ryzyk utraty poufności, dostępności i integralności, może skutkować dla organizacji nie tylko stratami materialnymi wymiernymi finansowo, ale też utratą spodziewanych korzyści, utratą reputacji firmy i długotrwałymi procesami sądowymi z innymi podmiotami gospodarczymi powiązanymi z organizacją, którą to zdarzenie dotknęło[34] [35] [36].

Straty materialne organizacji mogą obejmować zarówno uszkodzenia sprzętu, oprogramowania, utratę danych i konieczność ich odtworzenia, a w dalszej konsekwencji niedostępność systemu informatycznego wraz z finalnymi konsekwencjami finansowymi takimi jak: dodatkowe koszty operacyjne przedsiębiorstwa; utraty przychodów; roszczenia z tytułu niewykonania bądź nienależytego wykonania usług pochodzące od partnerów biznesowych; roszczenia cywilno-prawne osób trzecich z tytułu czynów niedozwolonych – ujawnienie danych osobowych; kary nałożone przez organy publiczne; oraz dodatkowe koszty, np.: obrony prawnej[37].

Przykładem, który wyjątkowo dobitnie pokazuje szkody, jakie materializacja ryzyk w organizacji może spowodować zarówno w samej organizacji, jak i innym użytkownikom

[34] CSI/FBI. 2001. Computer Crime & Security Survey. Vol. VII 2001. [28]
[35] CSI/FBI. 2001. Computer Crime & Security Survey. Vol. VIII 2002. [29]
[36] CSI/FBI. 2001. Computer Crime & Security Survey. Vol. IX 2003. [30]
[37] Poniewierski, A. 2003, Ryzyko bezpieczeństwa systemów informatycznych. Rynek Terminowy. ISSN 1508-972x/ Nr 2/03 str. 24-25 [95]

systemów, jest sytuacja z systemem transakcyjnym VISA, która zdarzyła się w połowie stycznia 2008 roku i została szeroko opisana w mediach. Użytkownicy kart płatniczych i kredytowych VISA zostali pozbawieni możliwości dokonywania transakcji przy użyciu własnych kart, a niektórzy z nich także zostali pozbawieni wszelkich zasobów finansowych znajdujących się wcześniej na kontach bankowych na skutek wielokrotnego potrącenia tej samej kwoty w ramach transakcji. Konieczność ponownego sprawdzania wszystkich operacji i ręcznego księgowania spowodowała olbrzymie koszty zarówno dla właściciela uszkodzonego systemu jak i dla użytkowników instytucjonalnych, głównie banków. Pozostałe instytucje, które również korzystają z usług systemu VISA mogły zostać pokrzywdzone jeśli awaria spowodowała opóźnienia w płatnościach zobowiązań należnych Skarbowi Państwa (w połowie miesiąca w Polsce wypadają terminy płatności podatków) a awaria zdarzyła się z niedzieli 14 na poniedziałek 15 stycznia 2008 i dotknęła nie tylko Polskę ale również dużą część Europy wschodniej i środkowej.

2.8 Zarządzanie ryzykiem przez organizację gospodarczą w procesie przetwarzania informacji

Przez zarządzanie ryzykiem w organizacji określa się „proces, obejmujący całokształt działań podejmowanych przez podmiot w celu panowania nad ryzykiem, nastawionych na zapewnienie bezpieczeństwa działalności i osiągania celów przy zachowaniu optymalnego poziomu kosztu ryzyka”[38]. Dlatego zarządzanie ryzykiem w odniesieniu do systemów informatycznych odgrywa ogromną rolę w procesie tworzenia systemów bezpieczeństwa dla całej instytucji[39]. Istotną rolę w procesie wprowadzania tego elementu zarządzania pełni analiza, związana z określeniem obszarów występowania zagrożeń – ich rodzaju i charakteru. Zarządzanie jest w tym przypadku rozumiane jako „permanentne zabezpieczanie się”, a jego celem jest redukcja ryzyka[40]. Zarządzanie ryzykiem jest procesem składającym się z trzech głównych etapów[41]:

[38] Kuchlewska M., op. cit., str. 70 [51]
[39] Poniewierski, A. Ryba, M. 2008, Jak zbudować system bezpieczeństwa informacji w firmie. Harvard Business Review, Maj 2008 r. str. 156 – 161 [89]
[40] Białas A., 2006, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, str. 93 [5]
[41] Poniewierski, A. 1999, Analiza ryzyka w kontekście Polityki Zabezpieczeń Systemów Informatycznych. Biuletyn Bankowy. ISSN 1233-0566 / Nr 21, str. 17 – 27 [94]

1. Oceny ryzyka. Podczas tego etapu jest wyznaczona wartość ryzyka związanego z bezpieczeństwem systemów informatycznych. Na ten etap składają się: identyfikacja zasobów, które w kontekście systemów informatycznych są definiowane jako ”*składniki systemu spełniające żądaną rolę prezentacji, pamiętania, transmisji lub przetwarzania*[42]”, analiza zagrożeń i ocena podatności[43],
2. Strategii postępowania z ryzykiem. Ten etap polega na dokonaniu wyboru i wdrożeniu zabezpieczeń lub podjęciu innych działań (w literaturze ten etap jest zazwyczaj sprowadzany do wyboru jednej strategii postępowania z ryzykiem – zabezpieczenia).
3. Kontroli ryzyka. Jest to etap, podczas którego jest przygotowany plan działań zgodnie z przyjętą strategią, a następnie są wdrożone procedury mające za zadanie stałe monitorowanie ryzyka.

Rysunek 2.8.- 2 - Zarządzanie ryzykiem związanym z bezpieczeństwem systemów informatycznych *[źródło: opracowanie własne na podstawie Boehm, B. 1989. Tutorial: Software Risk Management. IEEE Computer Society]*

[42] PN-I-02000, marzec 2002, Technika informatyczna, Zabezpieczenia w systemach informatycznych. Terminologia. [118]
[43] Boehm B., 1989. Tutorial: Software Risk Management. IEEE Computer Society. [6]

2.9 Metody zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych

Wraz z upowszechnianiem systemów informatycznych zmieniały się metody zarządzania ryzykiem[44]. Można wyróżnić trzy zasadnicze, następujące po sobie podejścia do problemu zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych, które następowały po sobie ze względu na zmiany technologiczne i popularyzację systemów informatycznych[45]:

- podejście techniczne,
- podejście zarządcze,
- podejście instytucjonalne.

W podejściu technicznym skupiano się głównie na rozwiązywaniu problemów związanych z dostępnością systemu informatycznego[46]. Zarządzanie ryzykiem polegało na identyfikacji prawdopodobnych awarii systemu i przygotowaniu określonych scenariuszy działań awaryjnych lub przygotowaniu zapasowych ośrodków przetwarzania danych. Ten etap jest charakterystyczny dla okresu przetwarzania danych w centralnych wojskowych systemach komputerowych i rządowych ośrodków przetwarzania.

W podejściu zarządczym, w związku z upowszechnieniem się systemów informatycznych, rozszerzono zakres zarządzania na nowe ryzyka związane z poufnością i integralnością danych. Głównym elementem służącym zabezpieczeniu systemów informatycznych były zaawansowane technologicznie systemy zabezpieczeń oraz dokumenty opisujące procedury dotyczące polityki bezpieczeństwa.

W podejściu instytucjonalnym, które obecnie dominuje, główny nacisk jest położony na następujące zagadnienia:

---

[44] Domżał, T. 1995. Analiza ryzyka związanego z utratą danych lub naruszeniem ich poufności. Materiały szkoleniowe Instytutu Łączności - Bezpieczeństwo i poufność danych w systemach informatycznych. Warszawa. [33]

[45] Solms B., 2000. Information Security – the third wave? Computers & Security 19, 2000, 615 - 620. Oxford: Elsevier [110]

[46] Poniewierski, A. 2000, Zarządzanie ryzykiem bezpieczeństwa systemów informatycznych, materiały konferencyjne COMNET. Warszawa, Polska. [91]

- Standaryzację bezpieczeństwa systemów informatycznych – rozumianą jako wykorzystywanie najlepszych praktyk w dziedzinie bezpieczeństwa oraz wprowadzanie standardowych mechanizmów ochrony danych.
- Certyfikację rozwiązań bezpieczeństwa – rozumianą jako niezależną ocenę przyjętych rozwiązań (konstrukcja) i metod ich stosowania (efektywność).
- Wprowadzenie jednolitych mechanizmów służących mierzeniu poziomu bezpieczeństwa systemu informatycznego – rozumiane jako wprowadzenie zarówno procedur, jak i mechanizmów technologicznych zabezpieczających system informatyczny, przy równoczesnym stałym mierzeniu efektywności ich działania.

Istnieje bardzo silny związek między metodami oceny ryzyka a metodami zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych. Metody zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych można podzielić na dwie grupy[47]:

1. Formalne – posługiwanie się nimi polega na konsekwentnym korzystaniu z ustalonego algorytmu działania, który ma swój początek i koniec[48]. Metody formalne dzielą się na[49]:

    - ilościowe – wyniki uzyskuje się w konkretnych jednostkach miary np. w kwotach pieniężnych powstałych z pomnożenia wielkości prawdopodobieństwa niekorzystnego zdarzenia i potencjalnych strat;
    - jakościowe – wyniki uzyskuje się w postaci sformułowań takich jak: ryzyko niskie, średnie, większe niż…, podobnie jak…. Proces analizy związków przyczynowo-skutkowych może być bardzo szczegółowy.

2. Nieformalne – posługiwanie się nimi polega na konsekwentnym stosowaniu szeregu wytycznych i dobrych praktyk, do których należą:

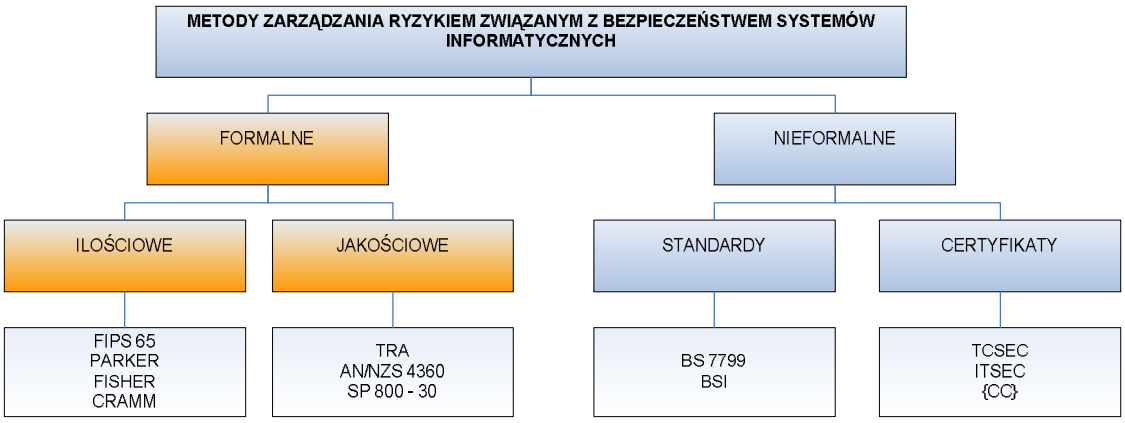
[47] Białas A., 2006, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa, str. 76 [5]
[48] Ozier, W. 1992. Risk Assessment and Management Data Security Management Report 85-01-20. New York: Auerbach. [83]
[49] Poniewierski, A. 1999, Zarządzanie ryzykiem bezpieczeństwa systemów informatycznych, materiały konferencyjne SecurNET. Warszawa, Polska [90]

- Standardy – kryteria ustalone wspólnie przez powołane do tego organizacje (międzynarodowe np. ISO, IEC), regionalne (np. ETSI) lub krajowe, określające najbardziej pożądany zestaw parametrów, zwykle posiadający nazwę (np. BS 7799), który zapewnia odpowiedni poziom bezpieczeństwa, lub zgodności z innymi standardami. Niektóre normy narodowe stają się faktycznym standardem międzynarodowym w danej dziedzinie, np. BSI w Niemczech. W Polsce istnieje zestaw regulacji dotyczących zarządzania bezpieczeństwem systemów informatycznych o nazwie PN – I-13335-1.
- Certyfikaty – dokumenty potwierdzające prawo do wykonywania czynności określonych w nich, stwierdzające zgodność produktu z właściwościami deklarowanymi przez wytwórcę lub określonymi w przepisach lub normach, albo potwierdzenie posiadania kompetencji w zakresie określonym w certyfikacie, np. SAS 70, WebTrust, ISO 27001. Certyfikaty są wydawane przez akredytowane lub cieszące się powszechnym zaufaniem instytucje. Certyfikaty są również zestawami wymagań ustalonych przez instytucje rządowe lub wojskowe (Np. TCSEC lub CC), których wypełnienie jest równoznaczne z osiągnięciem określonego poziomu bezpieczeństwa (np. w przypadku TCSEC - C2).

Tylko w metodach formalnych zarządzania ryzykiem występuje element oceny ryzyka, ponieważ końcowym efektem zastosowania każdej z nich jest dokument zawierający rekomendacje dotyczące zabezpieczeń systemów informatycznych wraz z ich ekonomicznym uzasadnieniem[50].

Podział metod zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych wraz z przykładowymi metodami przedstawia Rysunek 2.9.-3.

[50] Information Systems Audit And Control Association, Control Objectives for Information and related Technology (CobiT) [47]



Rysunek 2.9.-3 - Podział metod zarządzania ryzykiem związanym z bezpieczeństwem systemów *informatycznych* *[źródło: opracowanie własne, skróty: AN/NZS 4360:1999 – Standard Australia – Risk Management* [51], *BS 7799 – British Standard 7799* [52], *BSI - Bundesamt Für Sicherheit in der Informationstechnik* [53], *CC – Common Criteria* [54], *CRAMM - CCTA's Risk Analysis and Management Metodology* [55], *ITSEC - Information Technology Security Evaluation Criteria* [56], *FIPS – Federal Information Processing Standard, SP – Special Publication* [57], *TCSEC - Trusted Computer Systems Evaluation Criteria* [58], *TRA - Threat and Risk Assessment* [59]*]*

[51] Standards Australia AS/NZS 4360:1999, Risk management. [111]
[52] British Standard BS 7799. 1995. (Information Security Management), Part 1: Code of practice for information security management. [8]
[53] Bundesamt Für Sicherheit in der Informationstechnik (BSI) 1997. IT Baseline Protection Manual (Recommended Measures to meet Medium-Level Protection Requirements). [10]
[54] Określenie wytycznych z zakresu bezpieczeństwa w poszczególnych krajach (Common Criteria and Methodology for Information Technology Security Evaluation: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (United Kingdom), NIST (USA) and NSA (USA), 1999.) oraz wytycznych typu RFC (Holbrook, P., Reynolds, J. 1991. Site Security Handbook. Request for Comments (RFC) Nr 1244, Wznowienie, 1997 – RFC 2196 [46]).
[55] CCTA, 1991. SSADM-CRAMM Subject Guide for SSADM Version 3 and CRAMM Version 2. Central Computer and Telecommunications Agency, IT Security and Privacy Group, Her Majesty's Government, London (February). [14]
[56] Commission of European Communities 1990. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria, Version 1.2. Brussels, Belgium: Commission of European Communities, Directorate—General XIII (June). [26]
[57] National Institute of Standards and Technology, 2001. Risk management guide for Information Technology Systems, SP 800 – 30. [68]
[58] U.S. Department of Defense 1985. Trusted Computer Systems Evaluation Criteria. DOD 5200.28 – STD. [123]
[59] Government of Canada, Communications Security Establishment. 1999. Threat and Risk Assessment Working Guide. [43]

2.9.1 Metody ilościowe zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych i przetwarzania informacji

Pierwszą grupą metod formalnych są *metody ilościowe*. Metody te powstały na początku rozwoju tej dyscypliny, tj. w latach siedemdziesiątych i osiemdziesiątych XX wieku. Opierają się one na matematycznych obliczeniach: wpływu zagrożenia na bezpieczeństwo systemu informatycznego oraz prawdopodobieństwa wystąpienia opisywanego zagrożenia. Operują wyłącznie danymi liczbowymi zaczerpniętymi z analizy danych statystycznych i historycznych. Wartości najczęściej stosowane w metodach formalnych analizy ryzyka to: wartość monetarna, procentowa, liczba wystąpień i prawdopodobieństwo. Wyniki w tych metodach uzyskuje się w postaci konkretnych jednostek miary, najczęściej w kwotach pieniężnych, powstałych z pomnożenia wielkości prawdopodobieństwa niekorzystnego zdarzenia i potencjalnych strat. Prawdopodobieństwo w tym przypadku pełni rolę współczynnika wagowego[60]. Można do nich zaliczyć metody Courtneya, Fishera, Parkera[61] oraz metodę CRAMM.

2.9.1.1 Metoda Courtneya (opisana w FIPS 65 jako ALE)

Pierwsze formalne rozpoznanie problematyki oceny ryzyka związanego z bezpieczeństwem systemów informatycznych zostało przedstawione w czerwcu 1974 roku w publikacji FIPS 31 w pracy pod tytułem „Bezpieczeństwo fizyczne i zarządzanie ryzykiem automatycznego przetwarzania danych" (ang. Automated Data Processing Physical Security and Risk Management)[62]. Metoda analizy ryzyka bazująca na pracach Roberta H. Courtney'a, opisanych w FIPS 31 (ang. Federal Information Processing Standards Publication), przedstawiona w publikacji FIPS 65 „Wytyczne dla analizy ryzyka automatycznego przetwarzania danych" (ang. Guideline for Automatic Data Procesing Risk Analysis) z 1979 roku jest jedną z pierwszych, a zarazem najpowszechniej stosowaną i cytowaną w literaturze.[63]

---

[60] Białas A. 2006, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT [5]
[61] Baskerville, R. 1992. The developmental duality of information systems security. The Journal of Management Systems 4, 1, 1-12. [4]
[62] Ozier, W. 1997. Issues in Quantitative versus Qualitative risk analysis. DataPro Report, August. New York: McGraw-Hill. [82]
[63] U.S. Department of Commerce, National Bureau of Standards, 1979. Guideline for Automatic Data Processing Risk Analysis, Federal Information Processing Standards Publication FIPS 65. [122]

W tej metodzie ryzyko utraty bezpieczeństwa systemów informatycznych jest rozpatrywane w kontekście trzech głównych atrybutów: poufności, dostępności i integralności. Jest ono wyrażone wielkością możliwych strat spowodowanych przez wystąpienie danego zagrożenia.

Metoda oceny ryzyka, którą zaproponował Robert Courtney, jest najbardziej znana i jest do dziś uważana za podstawę dla oceny ryzyka związanego z bezpieczeństwem systemów informatycznych[64].

Courtney definiuje dwa główne składniki ryzyka (***R***)[65]:

P – prawdopodobieństwo, że dane zagrożenie wystąpi określoną liczbę razy w ciągu zadanego czasu.

C – wartość potencjalnych strat powstałych w wyniku wystąpienia zagrożenia.

Wartość ryzyka związanego z bezpieczeństwem systemów informatycznych jest iloczynem kartezjańskim wyrażonym wzorem 2.9.-1[66]:

$$R = P \times C \qquad \textit{Wzór 2.9.- 1}$$

W tej samej pracy została też wprowadzona pierwsza formalna metoda oceny ryzyka związanego z bezpieczeństwem systemów informatycznych zawierająca prosty opisowy algorytm ilościowej oceny ryzyka[67] zwany ALE (ang. Annualized Loss Expectancy). Definicję ALE można również odnaleźć w polskiej normie PN – I – 02000:

„Przewidywane straty roczne – wartość przewidywanych strat rocznych w systemie przetwarzania danych lub w wynikach jego działalności, poniesionych skutkiem ataków (3.1.005) na jego aktywa informatyczne (3.1.001)”.[68]

---

[64] Courtney, R. 1977. Security risk assessment in electronic data processing. AFIPS Conference Proceedings National Computer Conference 46, 97-104. [27]
[65] Meritt, W.J. 1998. Risk Management. 21th NISSC (National Information Systems Security Conference). Arlington, Virginia. [59]
[66] National Bureau of Standards, 1974. Guidelines for Automatic Data Processing Physical Security and Risk Management, Federal Information Processing Standards Publication FIPS 31. [67]
[67] Sumner, M. 1992. The impact of Computer Assisted Software Engineering on Systems Development in Kendall, K. Lyytinen, K., DeGross, J. IFIP Transactions A8 The Impact of Computer Supported Technologies on Information Systems Development. Amsterdam: North-Holland, 43-60. [113]
[68] Technika Informatyczna. Zabezpieczenia w systemach informatycznych. 2002. PN – I – 02000. [118]

Algorytm obliczania wartości przewidywanych strat rocznych[69], ALE jest wielkością wyznaczaną ze wzoru 2.9.-2:

$$ALE = SLE \cdot ARO, \qquad \textit{Wzór 2.9.- 2}$$

gdzie:

ARO – *roczny wskaźnik wystąpienia zdarzenia* (ang. Annualized Rate of Occurance) jest szacowaną częstością wystąpienia zdarzenia powodującego daną stratę,

SLE – *spodziewana jednorazowa strata* (ang. Single Loss Expectancy) jest wielkością przewidywanej straty wynikłej z jednokrotnego wystąpienia zdarzenia powodującego daną stratę, wyrażoną w pieniądzu – wielkość ta jest wyznaczana ze wzoru 2.9.- 3:

$$SLE = AV \cdot EF, \qquad \textit{Wzór 2.9.- 3}$$

gdzie:

AV – *wartość zasobu* (ang. Asset Value) jest wyrażoną w pieniądzu wartością zasobu, do którego odnosi się analizowane zdarzenie powodującego daną stratę,

EF – *wskaźnik ekspozycji* (ang. Exposure Factor) określa procent wartości zasobu AV, jaka zostaje utracona w wyniku pojedynczego zdarzenia powodującego daną stratę.

W celu uproszczenia procesu wyliczania wielkość ALE w oparciu o wzory 2.9.-2 i 2.9.-3, stosuje się wzór postaci wzoru 2.9.-4:

$$ALE = \frac{10^{f+i-3}}{3}, \qquad \textit{Wzór 2.9.- 4}$$

gdzie:

f – indeks określający szacowaną częstość wystąpienia zdarzenia powodującego daną stratę, którego wartości ze zbioru $\{1,..,9\}$ są określone w dokumencie FIPS 65,

[69] Security of Federal Automated Information Systems, Office of Management and Budget 1978. OMB Circular A-71. Washington. [108]

i – indeks określający szacowaną wysokość straty spowodowanej wystąpieniem zdarzenia powodującego tę stratę, którego wartości ze zbioru $\{1,..,9\}$ są określone w dokumencie FIPS 65.

Powszechność oceny ryzyka systemów informatycznych za pomocą metody Courtney'a wynika z prostoty zastosowanego podejścia, łatwości i intuicyjności obliczania ALE, oraz z faktu, że była ona jedną z pierwszych sformalizowanych metod analizy zagadnienia oceny ryzyka związanego z bezpieczeństwem systemów informatycznych, które zostało przyjęte jako standard rządowy w USA.

2.9.1.2 Metoda Fishera

Metoda zaproponowana przez Roberta Fishera[70] w pracy „Information Systems Security[71]" jest rozwinięciem metody Courtney'a. Metoda Fishera jest całościową metodą projektowania rozwiązań bezpieczeństwa systemów informatycznych. W tej metodzie proces zarządzanie ryzykiem systemów informatycznych składa się z pięciu faz, z których trzy środkowe odnoszą się do oceny ryzyka związanego z bezpieczeństwem systemów informatycznych. Te fazy to:

1. Inwentaryzacja zasobów.
2. Identyfikacja zagrożeń. Zidentyfikowane zagrożenia są podzielone na jedenaście grup zagrożeń będących rozszerzeniem sześciu grup zagrożeń występujących w metodzie Courteny'a.
3. Ocena ryzyka. Poziom ryzyka dla systemu informatycznego jest wyliczany na podstawie informacji zgromadzonych w fazie pierwszej przy użyciu aparatu Courtney'a opisanego w rozdziale 2.9.1.1 „Metoda Courtneya (opisana w FIPS 65 jako ALE)".
4. Projektowanie mechanizmów kontrolnych. W tej fazie następuje projektowanie mechanizmów kontrolnych w zakresie zapobiegania, detekcji oraz poprawy poziomu zabezpieczeń systemu informatycznego. Dla określonej klasy ryzyka jest dobierana odpowiednia klasa ochrony. Zasadą rządzącą tej fazy jest dobór zabezpieczeń adekwatnych do potrzeb – poziomu ryzyka oraz do wartości zasobów.

[70] Fisher, R. 1984. Information Systems Security. Englewood Cliffs: Prentice-Hall. [39]
[71] Baskerville, R. 1991. Risk analysis as a source of professional knowledge, Computers & Security 10 (8), 749 – 764. Oxford: Elsevier. [3]

5. Analiza kosztów i efektywności zabezpieczeń w porównaniu z korzyściami (ang. Cost – Benefit Analysis, CBA). Zidentyfikowane mechanizmy ograniczające ryzyko podlegają analizie w odniesieniu do ich ekonomicznej opłacalności, gdzie maksymalny koszt zabezpieczeń danego systemu informatycznego nie może być wyższy niż całkowita wartość tego systemu.

Głównym celem przeprowadzenia oceny ryzyka przy użyciu metody Fishera jest opracowanie polityk i planów zabezpieczeń dla ochrony poszczególnych systemów informatycznych. Nowością tej metody było opracowanie efektywnych ekonomicznie mechanizmów ograniczenia ryzyka związanego z systemami informatycznymi.

2.9.1.3 Metoda Parkera

Metoda zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych opracowana przez Davida Parkera[72] w 1981 roku na wniosek Computer Security Institute składa się z pięciu faz, z których najważniejsze w tej metodzie są fazy druga i trzecia.

1. Identyfikacja i wycena zasobów.
2. Identyfikacja zagrożeń. Za pomocą tej metody odbywa się ona zgodnie z przynależnością każdego zagrożenia do określonych kategorii zaproponowanych przez Parkera, np.: źródło zagrożeń, motywy działania stron będących zagrożeniem, lub wielkość spowodowanych przez nie strat.
3. Ocena ryzyka. Odbywa się ona przy wykorzystaniu metody Courtne'ya rozbudowanej o macierz analizy zagrożeń (ang. Exposure Analysis Matrix). Przy konstrukcji tej macierzy przyjęto, że istotność zagrożeń jest funkcją liczby osób mogących spowodować stratę. To założenie prowadzi do analizy ryzyk w podziale na poszczególne grupy zawodowe.
4. Identyfikacja, selekcja i implementacja zabezpieczeń.
5. Zalecenia dla programu ochrony.

Głównym celem przeprowadzenia oceny ryzyka przy użyciu metody Parkera jest opracowanie polityk i planów zabezpieczeń dla ochrony poszczególnych systemów informatycznych. W tej metodzie są również wykorzystane elementy metody Courtne'ya

[72] Parker, D. 1976. Crime by Computer. New York: Chas Scribners Sons. [84]

poszerzone o jakościową ocena ryzyka i wzbogacone o wpływ czynnika ludzkiego na to ryzyko. Istotny jest w niej również proces zarządzania bezpieczeństwem systemów informatycznych, co odróżnia ją od innych metod.

2.9.1.4 Metoda CRAMM (CCTA Risk Analysis Management Methodology)

Brytyjska metoda CRAMM (ang. CCTA Risk Analysis Management Methodology), opracowana przez CCTA (ang. U.K. Government Central Computer and Telecommunications Agency), wzbogacona o dedykowane oprogramowanie, została przyjęta jako rządowy standard oceny ryzyka i zarządzania bezpieczeństwem systemów informatycznych. Jest to metoda, w której cały proces zarządzania ryzykiem systemów informatycznych składa się z trzech, następujących po sobie etapów:

1. Identyfikacji i wyceny zasobów, w ramach których jest określany szczegółowy zakres analizy systemów informatycznych w odniesieniu do sprzętu, oprogramowania i danych. Dla wszystkich zidentyfikowanych i opisanych zasobów fizycznych jest przeprowadzana indywidualna wycena według ich wartości odtworzeniowej. Dla oprogramowania i danych wyceny dokonuje się na podstawie szacowanej straty wynikłej z niedostępności, zniszczenia, ujawnienia lub nieautoryzowanej modyfikacji. Dla wszystkich opisywanych zasobów dokonuje się (w skali od 1 do 10) oceny istotności danego zasobu dla organizacji oraz wpływu nieprawidłowości w funkcjonowaniu danego zasobu na funkcjonowanie całej organizacji.
2. Oceny zagrożeń i podatności dla wyróżnionych zasobów. Ten etap rozpoczyna pogrupowanie (częściowo automatyczne) zidentyfikowanych i opisanych zasobów na cztery możliwe typy: informacje, oprogramowanie, środki teleinformatyczne i otoczenie. Następnie zostają ustalone relacje pomiędzy poszczególnymi grupami i dopiero wtedy można ocenić poziom zagrożeń i podatności. Dla poszczególnych grup zasobów są automatycznie generowane wykazy zagrożeń i jest wyznaczana ocena poziomu zagrożenia dla każdej z tych grup, w pięciostopniowej skali, od bardzo niski, przez niski, średni, wysoki do bardzo wysoki. Dla oceny podatności została przyjęta skala trójstopniowa: niska, średnia i wysoka. Na podstawie wartości zasobów, poziomu zagrożeń i podatności jest wyznaczana wartość ryzyka w siedmiostopniowej skali, gdzie 1 oznacza najniższą wymagana ochronę, a 7 oznacza bardzo wysokie wymagania.

3. Zarządzania ryzykiem, które polega na wyborze rekomendowanych mechanizmów kontrolnych i zabezpieczających z istniejącej bazy danych. Baza ta zawiera ponad 3000 elementarnych wymagań bezpieczeństwa uzgodnionych z agencjami bezpieczeństwa i właściwymi organizacjami standaryzującymi. Wdrożenia tych zabezpieczeń znacząco ogranicza zidentyfikowane wcześniej zagrożenia.

2.9.2 Metody jakościowe zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych

Drugą grupą metod formalnych zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych są metody, w których wartości ryzyka są wyrażane *jakościowo*.[73] Są one dużo bardziej subiektywne niż metody ilościowe, ponieważ bazują na ocenie i wiedzy ekspertów, a wykorzystuje się w nich miary opisowe. Wyniki końcowe uzyskuje się w postaci określeń typu: ryzyko niskie, średnie, większe niż…, podobne jak…, i chociaż mogą one posiadać liczbowe odpowiedniki, a sam proces analizy związków przyczynowo-skutkowych może być szczegółowy[74].

2.9.2.1 Metoda TRA (Threat and Risk Assessment)

Metoda TRA – *Szacowanie Zagrożeń i Ryzyka* (ang. Threat and Risk Assessment)[75] została opracowana dla agencji federalnych i jest oficjalnym zestawem wytycznych z zakresu zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych Rządu Kanadyjskiego. Ze względu na wysoką jakość opracowania oraz możliwość stosowania jej w instytucjach o innym profilu działalności niż rządowy, jest ona szeroko rozpowszechniona i adaptowana dla lokalnych potrzeb. W Polsce zastosowano ją w oficjalnych pracach Rady Bankowości Elektronicznej przy Związku Banków Polskich[76].

Metoda ta jest mocno zintegrowana z *cyklem życia systemu informatycznego* (ang. System Development Life Cycle – SDLC), który jest analogiczny do cyklu życia zabezpieczeń

[73] Management of Federal Information Resources, Office of Management and Budget 1996. OMB Circular A-130. Washington. [56]
[74] Białas A. 2006, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT [5]
[75] Government of Canada, Communications Security Establishment. 1999. Threat and Risk Assessment Working Guide. [43]
[76] Wołowski, F. 2000. Wprowadzenie do problematyki analizy ryzyka dla Wspólnej Sieci Bankowości Elektronicznej. Rada Bankowości Elektronicznej przy Związku Banków Polskich. [125]

systemu informatycznego. Dodatkowo została ona rozbudowana o elementy raportowania o stanie ryzyka.

W metodzie TRA, podobnie jak w poprzednich metodach, wyróżnia się dobrze zdefiniowane fazy (łącznie jest ich trzynaście), z których pierwsze trzy są najistotniejsze z punktu widzenia tej rozprawy, dotyczą oceny ryzyka związanego z bezpieczeństwem systemów informatycznych. Te fazy to:

1. Planowanie działań.
2. Przygotowanie, w czasie którego dokonuje się oceny ważności atrybutów bezpieczeństwa dla danego systemu informatycznego (poufność, dostępność, integralność).
3. Analiza – kluczowa faza w tej metodzie, obejmująca analizę zagrożeń i ocenę ryzyka.
4. Rekomendacje. W metodzie TRA przyjmuje się cztery główne klasy sposobów postępowania z ryzykiem, którym w następnej fazie zarządza się już automatycznie.
5. Decyzja o redukcji, akceptacji, transferze, lub unikaniu ryzyka.
6. Określenie wymagań dotyczących zabezpieczeń.
7. Wybór zabezpieczeń adekwatnych do potrzeb (administracyjnych, technicznych, fizycznych i osobowych);
8. Konstrukcja i wdrożenie zabezpieczeń obniżających ryzyko do poziomu akceptowalnego i weryfikowalnego.
9. Certyfikacja za pomocą testów.
10. Decyzja o akredytacji.
11. Akredytacja.
12. Utrzymanie i eksploatacja.
13. Ewentualne decyzje o zmianach.

Jedynym elementem odróżniającym tę metodę od innych jest wprowadzenie do analizy elementów takich jak: wartość podatności, prawdopodobieństwo wystąpienia zagrożeń, konsekwencje wystąpienia zagrożeń, efektywność zabezpieczeń itp.

2.9.2.2 Metoda AN/NZS 4360:1999

Jedną z podstawowych i powszechnie stosowanych metod zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych jest opisana przez Standard Australijski i Nowozelandzki *„Zarządzanie ryzykiem”* (ang. Risk Management) metoda AN/NZS 4360:1999. Została ona również przyjęta jako obowiązująca metoda w Federacji Europejskich Managerów do spraw Ryzyka FERMA (ang. Federation of European Risk Management Associations).

Najważniejszym dokumentem, na którym opiera się cały proces zarządzania ryzykiem, jest *„Polityka zarządzania ryzykiem”* (ang. Risk Management Policy). Polityka musi nawiązywać do strategii biznesowej organizacji i musi być z nią spójna. Konsekwencją dobrze opracowanego dokumentu polityki jest istnienie w organizacji dobrze funkcjonującego systemu planowania zarówno zadań, jak i zasobów, ale organizacja musi być gotowa do wdrożenia metody zarządzania ryzykiem, a wyniki zarządzania tym ryzykiem muszą być akceptowane i respektowane przez jej zarząd. Wymagania te stanowią podstawę dla prawidłowego przygotowania, wdrożenia i operacyjnego wykorzystania metody zarządzania ryzykiem, a ich niespełnienie w większości przypadków prowadzi do błędnych wniosków, które w rezultacie mogą doprowadzić do nieodpowiedniego zabezpieczenia systemu informatycznego.

W metodzie zarządzania ryzykiem AS/NZS 4360:1999 wyróżnia się siedem faz:

1. Ustalenie zakresu analizy.
2. Identyfikacja ryzyka. Tę fazę rozpoczyna opis organizacji, której dotyczy planowana ocena, pod kątem otoczenia: prawnego, społecznego, politycznego i kulturowego. Następnym działaniem jest opis obszarów działalności organizacji obejmujący zarówno długofalowe cele strategiczne, jak i bieżące procesy operacyjne, finansowe, kadrowe, aż po obszar zarządzania wiedzą i zgodności z przepisami nałożonymi przez organy regulacyjne kraju, w którym dana organizacja funkcjonuje. Po dokonaniu takich opisów można zdefiniować związane z nimi ryzyka, na które organizacja jest narażona.
3. Analiza ryzyka. Celem tej fazy jest opisanie zakresu i charakteru ryzyk oraz przedstawienie ich w przejrzystej formie. W następnej kolejności należy rozważyć prawdopodobieństwo materializacji zidentyfikowanych ryzyk i określić rozmiar

ewentualnych skutków wystąpienia zagrożenia. W tej metodzie można użyć tablic dla miar jakościowych ryzyka.

4. Szacowanie ryzyka. Faza mająca na celu określenie prawdopodobieństwa wystąpienia danego ryzyka i określenie możliwych następstw w sposób ilościowy, półilościowy lub jakościowy. Skutki materializacji ryzyka dzieli się na duże, średnie i małe. Prawdopodobieństwo również opisuje się jako duże, średnie i małe. W oparciu o wyniki analizy można opracować profil ryzyka – każdemu ryzyku jest przypisywana ocena opisująca jego znaczenie, co porządkuje je pod względem istotności i pozwala na ustalenie priorytetów działania W procesie konstruowania profilu ryzyka następuje przypisanie konkretnych ryzyk do określonych dziedzin działalności i przypisanie odpowiedzialności. Oznacza to, że każdemu ryzyku są podporządkowane odpowiednie zasoby menadżerskie.
   Dobór zabezpieczeń.
5. Monitorowanie i przeglądy.
6. Konsultacje.

Z perspektywy tej rozprawy najważniejsze są fazy druga, trzecia i czwarta składające się razem na ocenę ryzyka.

Końcowym elementem oceny ryzyka jest porównanie szacunkowej wartości ryzyka z przyjętymi w organizacji kryteriami: kosztami, korzyściami, wymogami prawnymi, względami społeczno-ekonomicznymi lub ekologicznymi. Stanowi ona podstawę do podjęcia dalszych decyzji biznesowych.

2.9.2.3 Metoda NIST SP 800-30

Wytyczne opracowane przez NIST (ang. National Institute of Standards and Techology) w publikacji „Special Publication 800-30”[77] stanowią rekomendacje dla instytucji publicznych i rządowych Stanów Zjednoczonych Ameryki Północnej w zakresie zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych. Metoda przedstawiona w tej publikacji jest najnowszą ze wszystkich opisywanych w tej rozprawie. Różni się ona od wcześniejszych metod stanowiących standardy NIST. Zmiana polega na tym, że zarządzanie

[77] National Institute of Standards and Technology, 2001. Risk management guide for Information Technology Systems, SP 800 – 30 [68]

ryzykiem jest w niej podporządkowane instytucji i misji realizowanej przez tę instytucję, a nie ochronie samych jej zasobów informatycznych. Podobnie jak w TRA, u podstaw tej metody leży stwierdzenie:„*…efektywne zarządzanie ryzykiem musi być w pełni zintegrowane z cyklem życia i rozwoju systemu*[78]*”*.

Cały proces zarządzania ryzykiem składa się z dwóch etapów:

I. Ocena ryzyka.

II. Ograniczanie ryzyka.

Etap pierwszy – ocena ryzyka – jest podzielony na dziewięć faz. W pierwszych trzech dokonuje się oceny ryzyka związanego z bezpieczeństwem systemów informatycznych. Są to:

1. Wybór systemów podlegających ocenie.
2. Identyfikacja i opracowanie listy zagrożeń wraz z klasyfikacją ich źródeł (ludzkie, naturalne, środowiskowe).
3. Identyfikacja i opracowanie listy podatności.

Pozostałe fazy to:

4. Analiza mechanizmów kontrolnych.
5. Określenie prawdopodobieństw wykorzystania podatności.
6. Analiza skutków przy użyciu modelu analizy wpływu na biznes (ang. Business Impact Analysis).
7. Wyznaczenie wartości ryzyka za pomocą macierzy (wysokie, średnie lub niskie).
8. Rekomendacje mechanizmów zabezpieczających.
9. Dokumentacja – raport stanowiący podstawę dla następnego etapu metody zarządzania ryzykiem, etapu ograniczania ryzyka.

2.10 Wnioski z analizy metod zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych

Wadą metod ilościowych jest konieczność posługiwania się prawdopodobieństwem w warunkach braku długookresowych danych statystycznych, podczas gdy używana w tych

[78] National Institute of Standards and Technology, 2001. Risk management guide for Information Technology Systems, SP 800 - 30 s. 15. [68]

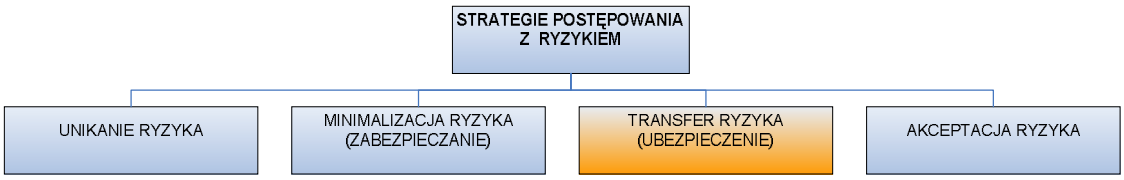
metodach ilościowa miara następstw określana w jednostkach miary – najczęściej w kwotach pieniężnych, powstałych z pomnożenia wielkości prawdopodobieństwa niekorzystnego zdarzenia i potencjalnych strat, zależy od zakresu i dokładności zdefiniowanej skali pomiarowej. Uzyskane wyniki mogą być zatem niepewne lub nawet mylące. Metody ilościowe wymagają także interpretacji lub co najmniej komentarza, przy czym taka interpretacja wymaga dużego doświadczenia i jest droższa niż w przypadku metod jakościowych.

Natomiast wadą metod jakościowych jest to, że nie można wyrażać w nich następstw za pomocą miar liczbowych, a ich wyniki nie są porównywalne, są bowiem subiektywne. Ponadto analiza korzyści w stosunku do kosztów jest trudna. Wszystkie te metody sprowadzają się do odpowiednich scenariuszy, w których aspekt ekonomiczny i biznesowy bezpieczeństwa odgrywa istotną rolę. Jednak główną wadą metod jakościowych z perspektywy niniejszej rozprawy jest fakt, że służą one organizacji do odpowiedniego doboru mechanizmów bezpieczeństwa (strategia minimalizacji lub redukcji ryzyka) przy założeniu, że organizacja powinna dokonać stosownych zabezpieczeń lub świadomej akceptacji ryzyka w miejscu jego powstawania. Nie mogą one jednak być przydatne dla zakładów ubezpieczeń, które na podstawie obliczeń wartości ryzyka za ich pomocą miałyby podjąć decyzję o przejęciu go na siebie, czyli ubezpieczeniu systemów informatycznych przedsiębiorstwa, gdyż metody te nigdy do tego celu nie były konstruowane i nie sposób ich do tego celu zaadaptować[79].

2.11 Strategie postępowania z ryzykiem związanym z bezpieczeństwem systemu informatycznego

Istnieją cztery główne strategie postępowania z ryzykiem związanym z bezpieczeństwem systemów informatycznych przedstawione na rysunku 2.11.- 4:

[79] Saarinen, T., Sääksjävi, M. 1989. The missing concepts of user participation: An empirical assessment of user participation and information system success, in Bødker, Susanne (Ed.) Proceedings of the 12th IRIS—Part II. Computer Science Department, Aarhus University DAIMI PB 296-II (December) 533-551. [105]



Rysunek 2.11.- 4 – Strategie postępowania z ryzykiem związanym z bezpieczeństwem systemów informatycznych *[źródło: opracowanie własne]*

1. Unikanie ryzyka to strategia, zgodnie z którą system informatyczny przedsiębiorstwa nie jest narażony na określone zagrożenia dzięki świadomemu zaniechania działań mogących doprowadzić do powstania ryzyka.
2. Minimalizacja lub redukcja ryzyka to strategia, zgodnie z którą system informatyczny przedsiębiorstwa jest wyposażony w mechanizmy zabezpieczające adekwatne do potrzeb.
3. Transfer ryzyka to strategia, zgodnie z którą określone ryzyka systemu informatycznego przedsiębiorstwa są przeniesione na stronę trzecią przez zawarcie odpowiednich umów cywilno-prawnych.
4. Akceptacja ryzyka to strategia, zgodnie z którą system informatyczny jest narażony na określone ryzyka, jednak organizacja nie realizuje działań zapobiegawczych.

Istnieją cztery podstawowe strategie minimalizacji lub redukcji ryzyka różniące się przede wszystkim sposobem jego analizy[80] [81]:

- zastosowanie zabezpieczeń typowych dla określonych warunków, często nawet skatalogowanych, czyli *ochrona podstawowa* (ang. baseline approach); całość systemów jest traktowana w ten sam sposób, niezależnie od rzeczywistego ryzyka, które nie jest badane, co prowadzi zwykle albo do niedoszacowania ryzyka, albo do przeszacowania nakładów na zabezpieczenia;
- przyjęcie zabezpieczeń po przeprowadzeniu uproszczonej analizy ryzyka zwanej *nieformalną* (ang. informal approach) – analiza koncentruje się na tych obszarach, które wydają się być najbardziej narażone;

[80] Białas A. 2006 Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie WNT [5]
[81] Manunta, G. 2000. Is Security Utilitarian?, Security Jurnal vol thirteen No. 2, 49 - 58. London: Perpetuity Press. [57]

- przyjęcie zabezpieczeń wynikających z formalnej, zwykle *szczegółowej analizy ryzyka* (ang. detailed risk analysis) – całość systemów jest poddana dokładnej analizie ryzyka, często wspomaganej narzędziami programowymi;
- metoda mieszana – w wyniku ogólnej (prowadzonej na wysokim poziomie ogólności) analizy ryzyka (ang. High Level Risk Analysis) wyznacza się obszary systemu szczególnie narażone lub mające fundamentalne znaczenie dla funkcjonowania instytucji, dla których zabezpieczenia dobiera się na podstawie analizy ryzyka, natomiast dla reszty systemów jest stosowana ochrona podstawowa (ang. combined approach).

Niezależnie od przyjętej strategii zarządzania ryzykiem związanym z bezpieczeństwem systemu informatycznego, pozostaje jeszcze kontrola rzeczywistej efektywności i sprawności zastosowanych zabezpieczeń, dokonywana również przez pryzmat ekonomiczny. Wdrożone zabezpieczenia powinny być bowiem adekwatne do chronionych zasobów, a kontrola tych zabezpieczeń musi się odbywać w sposób planowy, według opracowanego wcześniej harmonogramu.

Głównym dokumentem regulującym w sposób systemowy sposoby zapewnienia bezpieczeństwa systemów informatycznych i zarządzanie ryzykiem w organizacjach jest „Polityka bezpieczeństwa systemów informatycznych".

„Polityka bezpieczeństwa systemów informatycznych" jest to dokument zawierający zbiór reguł i zasad oraz praw i obowiązków, które określają, w jaki sposób należy zarządzać, ochraniać i dystrybuować wszelkie dane w organizacji, a w szczególności dane poufne."[82]

Polska norma PN-I-13335-1 w następujący sposób opisuje układ i zawartość dokumentu „Polityki bezpieczeństwa systemów informatycznych"[83]:

„... Dokument polityki powinien zostać zatwierdzony przez kierownictwo, opublikowany i udostępniony w odpowiedni sposób wszystkim pracownikom. Powinien on deklarować

[82] Glossary of Computer Security Terms (NCSC-TG-004 ver. 1). 1998. DataPro Report, July 98. New York: McGraw-Hill [42]
[83] Technika Informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. 1999. PN-I-13335-1, str. 13 [119]

zaangażowanie kierownictwa i wyznaczać podejście instytucji do zarządzania bezpieczeństwem danych. Jako minimum zaleca się, aby dokument zawierał:

1. *definicję bezpieczeństwa danych, jego ogólne cele i zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie danych;*
2. *oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa danych;*
3. *krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności mających szczególne znaczenie dla instytucji, np.:*
    - *zgodność z prawem i wymaganiami wynikającymi z umów;*
    - *wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa;*
    - *zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania;*
    - *zarządzanie ciągłością działania biznesowego;*
    - *konsekwencje naruszenia polityki bezpieczeństwa;*
4. *definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem danych, w tym zgłaszania przypadków naruszenia bezpieczeństwa;*
5. *odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dla poszczególnych systemów informatycznych lub zasad bezpieczeństwa, których użytkownicy powinni przestrzegać.*

Zaleca się udostępnienie tej polityki użytkownikom w całej instytucji w formie właściwej, dostępnej i zrozumiałej dla czytelników, do których jest adresowana."[84]

Na potrzeby zbioru wymagań bezpieczeństwa systemów informatycznych, zostały opracowane szczegółowe mechanizmy kontrolne, które definiuje Standard Brytyjski BS 7799-2[85]. Standard ten jest cytowany w niniejszej rozprawie ze względu na swoją popularność. Stanowi on jednak tylko „szkielet". W zastosowaniu praktycznym, model odniesienia musi być znacznie bardziej uszczegółowiony[86].

[84] Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji. 2003. PN-ISO/IEC 17799. str. 13. [117]
[85] British Standard BS 7799-2: 2002. 2002. Information Security Management System, Part 2: Specification with guidance for use. [9]
[86] Plate, A. 1997. Application of the IT Baseline Protection. 20th NISSC (National Information Systems Security Conference). Baltimore, Maryland. [88]

Zestaw wymagań stanowi skończony zbiór, a same wymagania bezpieczeństwa zgodnie ze standardem BS 7799-2 zostały pogrupowane w następujące kategorie[87]:

1 Polityka Bezpieczeństwa
- **1.1** Dokument
- **1.2** Proces przeglądu i oceny

2 Organizacja bezpieczeństwa
- **2.1** Infrastruktura bezpieczeństwa przedsiębiorstwa
- **2.2** Bezpieczeństwo stron trzecich
- **2.3** Wydzielanie (ang. outsourcing)

3 Klasyfikacja i kontrola aktywów
- **3.1** Rozliczalność aktywów
- **3.2** Klasyfikacja informacji
- **3.3** Oznaczanie informacji i manipulacja

4 Bezpieczeństwo personelu
- **4.1** Bezpieczeństwo ujęte w zakresie obowiązków i opisie zadań
- **4.2** Szkolenie użytkowników systemów informatycznych
- **4.3** Reagowanie na incydenty naruszenia bezpieczeństwa

5 Bezpieczeństwo fizyczne
- **5.1** Strefy bezpieczeństwa
- **5.2** Bezpieczeństwo sprzętu
- **5.3** Higiena i etyka pracy z systemem informatycznym

6 Komunikacja i zarządzanie operacyjne
- **6.1** Procedury operacyjne i odpowiedzialność
- **6.2** Planowanie zmian i akceptacja
- **6.3** Ochrona przed czynnikami destabilizującymi pracę systemu informatycznego
- **6.4** Bezpieczeństwo operacji
- **6.5** Zarządzanie siecią komputerową
- **6.6** Zarządzanie nośnikami danych
- **6.7** Wymiana danych i oprogramowania

7 Kontrola dostępu
- **7.1** Wymagania biznesowe dostępu do systemu informatycznego
- **7.2** Zarządzanie dostępem użytkowników
- **7.3** Odpowiedzialność użytkowników
- **7.4** Kontrola dostępu do sieci komputerowej
- **7.5** Kontrola dostępu do systemu operacyjnego
- **7.6** Kontrola dostępu do aplikacji
- **7.7** Monitorowanie dostępu
- **7.8** Kontrola dostępu zdalnego

8 Rozwój systemu informatycznego
- **8.1** Wymagania bezpieczeństwa dla zmian w systemie informatycznym
- **8.2** Bezpieczeństwo aplikacji
- **8.3** Ochrona kryptograficzna

[87] W tym rozdziale zostaną przedstawione jedynie główne domeny oraz pierwszy poziom szczegółowości wymagań bez ich objaśniania.

8.4 Bezpieczeństwo danych
8.5 Proces bezpieczeństwa rozwoju systemu informatycznego i wspomagania zmiany

9 Zapewnienie ciągłości działalności
9.1 Zarządzanie ciągłością działalności

10 Zgodność
10.1 Zgodność przetwarzania danych z prawem
10.2 Przegląd polityki bezpieczeństwa i zgodność ze standardami technicznymi
10.3 Audyt systemu informatycznego

Każda z kategorii jest rozwinięta na określone grupy zagadnień, a te następnie na grupy wymagań. Dla przykładu:

7. Kontrola dostępu

7.2. Zarządzanie dostępem użytkowników
7.2.1. Identyfikacja użytkownika i rejestracja (logowanie)
7.2.2. Zarządzanie uprawnieniami
7.2.3. Zarządzanie hasłami dostępu
7.2.4. Przegląd uprawnień

Dla poszczególnych grup wymagań powinny być opracowane szczegółowe wymagania bezpieczeństwa. Przykładowe szczegółowe wymagania wyglądają następująco[88]:

7. Kontrola dostępu

7.2. Zarządzanie dostępem użytkowników
7.2.3. Zarządzanie hasłami dostępu
a) standardowe hasła systemu operacyjnego klasy Unix,
b) hasło dialogowe o minimalnej długości 6 znaków, z alfabetu 56 znaków, zmieniane co 30 dni, tezaurus haseł trywialnych, minimalny odstęp zmiany hasła 1 dzień, 3 próby dostępu po których następuje blokada konta na okres 60 minut,
c) hasło jednorazowe 64 bitowe, generowane przez system oraz „tan" karty po stronie klienckiej,
d) „token" sprzętowy 128 bitowy z interwałem synchronizacji zegara do 60 sekund,
e) procedura zmiany haseł dostępowych,
f) procedura przechowywania haseł do kont specjalnych,

[88] Przykładowe wymagania szczegółowe przedstawione w niniejszym rozdziale są podstawą dla zbioru wymagań metody ORBI. Przy zastosowaniu metody ORBI do rzeczywistego procesu oceny ryzyka związanego z bezpieczeństwem systemów informatycznych pełen zbiór wymagań powinien być określony i zaakceptowany przez zakład ubezpieczeń.

g) hasła dostępowe zaszyfrowane w miejscu składowania oraz w kanałach wymiany informacji algorytmem symetrycznym o długości klucza min. 64 bitów,
h) …

Zestaw rzeczywistych zabezpieczeń w zależności od organizacji i używanych systemów informatycznych będzie się różnił, bo zastosowane mechanizmy będą zależne od wielkości organizacji, zadań biznesowych, kultury organizacyjnej, możliwości finansowych, a także świadomości kadry zarządzającej.

2.12 Instytucje powołane do reagowania na incydenty związane z bezpieczeństwem systemów informatycznych oraz monitorowania bezpieczeństwa systemów informatycznych

Zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet jest CERT, który działa w Polsce w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej). CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (ang. Forum of Incidents Response and Security Teams). W ramach tej organizacji współpracuje z podobnymi zespołami na całym świecie[89].

Do głównych zadań tego zespołu należy:

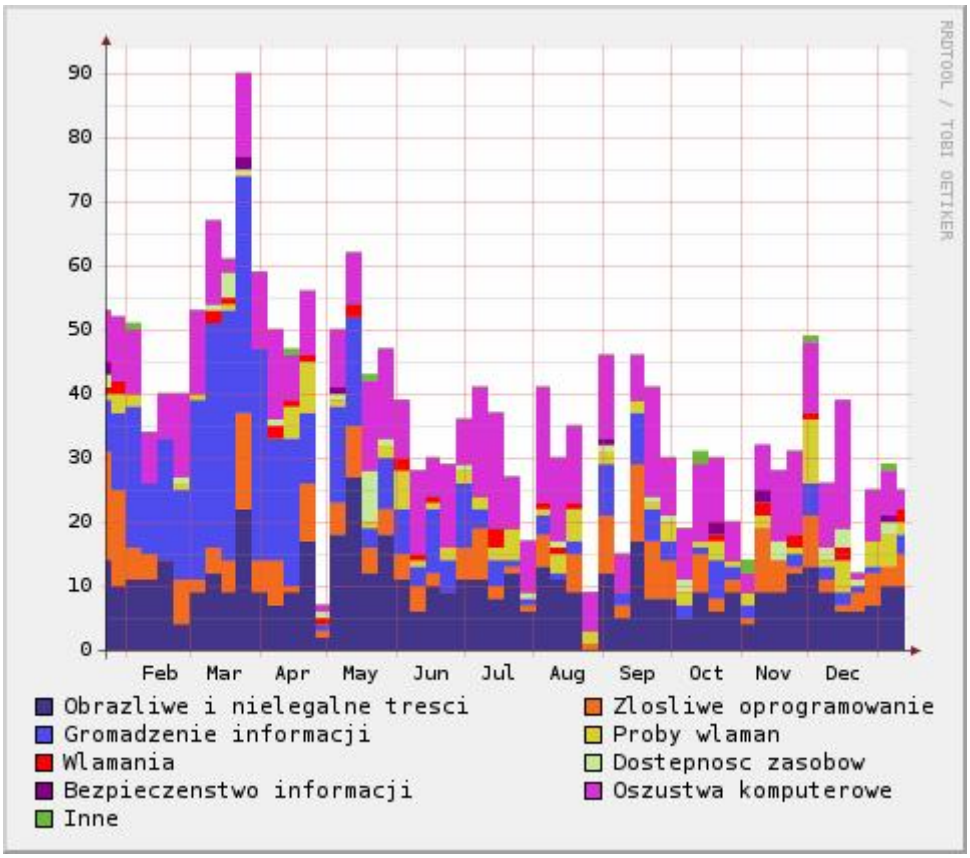
- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń,
- współpraca z innymi zespołami IRT (ang. Incidents Response Team) działającymi w ramach FIRST,
- prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego,
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu,

[89] Poniewierski, A. 2001, Strategia i Polityka zabezpieczenia elektronicznego dowodu przestępstwa pochodzącego z systemów IDS, materiały konferencyjne, IV Seminarium Naukowe Wyższej Szkoły Policyjnej w Szczytnie - Techniczne aspekty przestępczości komputerowej. Szczytno, Polska [93]

- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego,
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk.

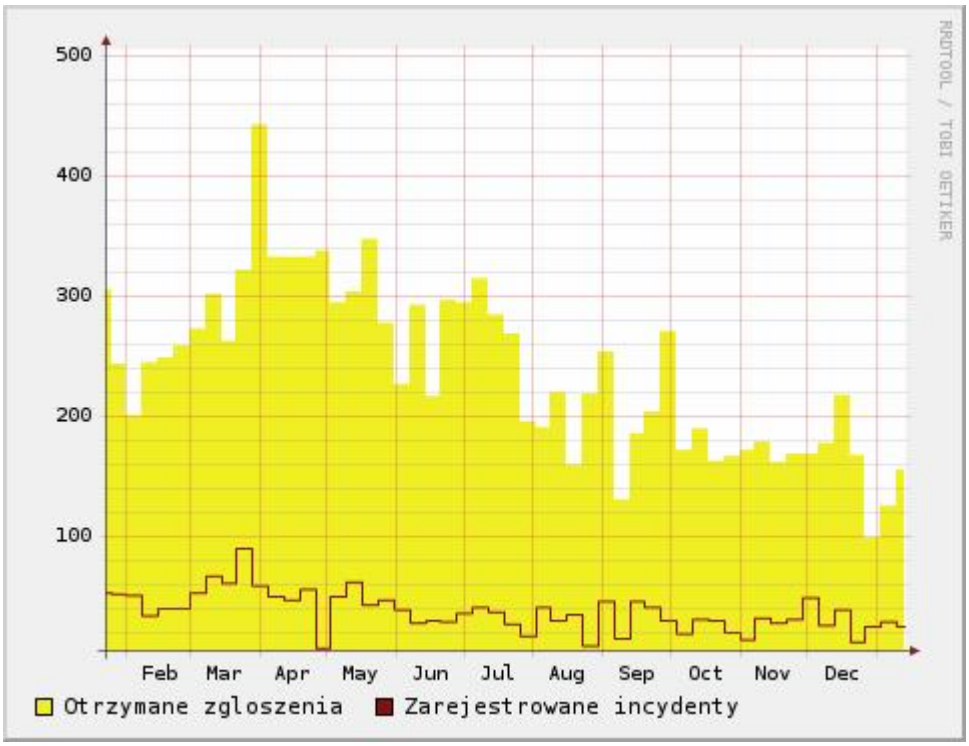
Jednym z efektów prac tego zespołu są raporty roczne „Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska" publikowane na stronach internetowych CERT [90] [91] [92] [93]. Z raportów, opublikowanych w ciągu ostatnich trzech lat wynika, że zdarzenia – incydenty (wg terminologii CERT) naruszające bezpieczeństwo informacji, dostępność zasobów oraz próby włamań i gromadzenie informacji, które mogą w rezultacie prowadzić do naruszenia bezpieczeństwa, stanowią znaczny odsetek wszystkich incydentów zgłoszonych do CERT. Strukturę i statystykę incydentów przedstawia rysunek 2.12.- 5.

[90] CERT Polska, Raport 2000, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2000 [19]
[91] CERT Polska, Raport 2001, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2001 [20]
[92] CERT Polska, Raport 2002, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2002 [21]
[93] CERT Polska, Raport 2003, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2003 [22]



Rysunek 2.12.- 5 - Liczba incydentów tygodniowo z podziałem na główne kategorie
[źródło: CERT Polska]

O ile zdarzenia dotyczące spamu czy złośliwego oprogramowania (wirusy, robaki komputerowe, konie trojańskie i inne) są zgłaszane przez wszystkich użytkowników Internetu (CERT, inne instytucje zajmujące się bezpieczeństwem, instytucje niekomercyjne, jednostki rządowe i osoby prywatne) w jednakowym stopniu, o tyle zdarzenia dotyczące bezpieczeństwa systemów, zwłaszcza w przypadku organizacji komercyjnych są zgłaszane niechętnie, najczęściej anonimowo. Jest to zrozumiałe, ponieważ organizacje te z obawy przed utratą zaufania klientów i wizerunku firmy wolą nie nagłaśniać problemu.



Rysunek 2.12.- 6 - Liczba zgłoszeń a liczba incydentów
[źródło: CERT Polska]

Z najnowszego raportu CERT[94] wynika, że firmy komercyjne stanowią tylko około 15% podmiotów zgłaszających incydenty dotyczące naruszenia bezpieczeństwa (w roku 2005 było to 4,5%[95] a w roku 2004 9,5%[96]), i prawdopodobnie jest to tylko „wierzchołek góry lodowej". Organizacje te bowiem nie mają obowiązku zgłaszania przypadków naruszeń bezpieczeństwa. W przypadku organizacji komercyjnych, przestępstwa komputerowe są ścigane na wniosek pokrzywdzonego na podstawie artykułów 267, 268 i 269 kodeksu karnego.

Inaczej sprawa naruszenia bezpieczeństwa wygląda w instytucjach publicznych. Instytucje te mają obowiązek zgłaszania przypadków naruszeń bezpieczeństwa, ponieważ w ich zasobach informatycznych mogą znajdować się informacje należące do kategorii informacji niejawnych, których ochronę reguluje Ustawa o ochronie informacji niejawnych z dnia 22

[94] CERT Polska, Raport 2006, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2006. [25]
[95] CERT Polska, Raport 2005, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2005. [24]
[96] CERT Polska, Raport 2004, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2004 [23]

stycznia 1999 r.[97] oraz dane osobowe, których ochronę reguluje ustawa o ochronie danych osobowych[98]. Ta ostatnia ustawa w sposób restrykcyjny nakłada obowiązek zabezpieczenia systemu informatycznego, w którym są gromadzone i przetwarzane dane[99] oraz zgłaszania wszelkich naruszeń bezpieczeństwa. Niestety w kulturze organizacyjnej większości tych instytucji nie ma jeszcze „zakodowanego" na trwałe myślenia o naruszeniu bezpieczeństwa w kategorii przestępstwa. Ponadto bardzo często instytucje te nie mają jasno opisanych kryteriów określających granicę pomiędzy nadużyciem a naruszeniem bezpieczeństwa oraz przygotowanych na taką ewentualność procedur zgłaszania tego typu incydentów[100], stąd prawdopodobnie nie wszystkie takie przypadki są przez nie zgłaszane do CERT.

Z danych zawartych w raportach CERT wynika również, że naruszenia, o których mowa, stanowią 11,5% wszystkich incydentów w roku 2004, 6,6% w roku 2005 i 6,2% w roku 2006. Mimo, że jest widoczna tendencja spadkowa, z całą pewnością zagrożeń tego typu nie uda się nigdy całkowicie wyeliminować.

[97] Dziennik Ustaw nr 11 poz. 95.
[98] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) [121]
[99] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych (Dz. U. Nr 100, poz. 1024). [102]
[100] Z raportu NIK „Informacja o wynikach kontroli prawidłowości przestrzegania w urzędach wojewódzkich i urzędach marszałkowskich przepisów dotyczących ochrony informacji niejawnych, stanowiących tajemnice służbową" opublikowanego w 2006 r., którego jednym z zagadnień było „Wytwarzanie i przetwarzanie dokumentów niejawnych opatrzonych klauzulą poufne i zastrzeżone" wynika, że instytucje te bardzo często nie posiadają zarówno ram organizacyjno-prawnych w postaci dokumentów – szczególnych wymagań bezpieczeństwa, procedur bezpiecznej eksploatacji oraz uzyskanych od służb ochrony państwa stosownych certyfikatów.

3 Ubezpieczenia organizacji gospodarczych i ich systemów informatycznych

Wszystkie organizacje gospodarcze funkcjonują w warunkach niepewności związanej z możliwością wystąpienia różnych zdarzeń losowych, będących skutkiem obiektywnie istniejących ryzyk, których nie można uniknąć. Dotyczy to zarówno całych organizacji, jak i ich pojedynczych zasobów. Jednym z takich zasobów, szczególnie narażonym na różnego rodzaju ryzyka, są systemy informatyczne. Ich poprawne funkcjonowanie jest niezwykle istotne w kontekście działalności całej organizacji. Przed negatywnymi finansowymi skutkami realizacji określonych ryzyk można się jednak zabezpieczyć na dwa sposoby: przez indywidualne zgromadzenie środków finansowych służących pokryciu strat spowodowanych realizacją ryzyk lub przez przeniesienie tego ryzyka na inny podmiot gospodarczy[101].

Z ekonomicznego i zarazem racjonalnego punktu widzenia zazwyczaj bardziej uzasadnione jest skorzystanie z tej drugiej możliwości, przez powołaną do tego celu instytucję – zakład ubezpieczeń.[102]

3.1 Definicja ubezpieczeń

Istnieje wiele definicji ubezpieczenia. Jedną z popularniejszych w polskiej literaturze przedmiotu, przytaczaną przez wielu autorów prac dotyczących tego tematu, jest definicja podkreślająca aspekt ekonomiczny: ubezpieczenie jest to „*urządzenie gospodarcze, zapewniające pokrycie przyszłych potrzeb majątkowych, wywołanych u poszczególnych jednostek przez odznaczające się pewną prawidłowością zdarzenia losowe, w drodze rozłożenia ciężaru tego pokrycia na wiele jednostek, którym te same zdarzenia losowe zagrażają*”[103]. W aspekcie organizacyjnym ubezpieczenie „*jest operacją, przez którą jedna ze stron, ubezpieczony, w zamian za zapłaconą przez niego składkę ubezpieczeniową, zapewnia sobie lub osobie trzeciej, (na którą dane ubezpieczenie zostało zawarte), świadczenie strony drugiej, czyli ubezpieczyciela, w przypadku zaistnienia zdarzenia określonego w umowie*

[101] Sangowski T. (red.), 2001, Ubezpieczenia gospodarcze, Poltext, Warszawa, str. 59 [107]
[102] Zdanowski, M. 1995, Wstęp do ubezpieczeń podmiotów gospodarczych. Warunki i rozwiązania krajowe. Przedsiębiorstwo Wydawnicze LAM, Warszawa [128]
[103] Łazowski J. 1948, Wstęp do nauki o ubezpieczeniach, PZU [54]

ubezpieczeniowej"[104]. Z kolei Kodeks cywilny przedstawia jeszcze inną definicję „*Ubezpieczenie – umowa między zakładem ubezpieczeń (ubezpieczycielem) a ubezpieczającym, w której ten pierwszy zobowiązuje się do spełnienia określonego świadczenia w postaci umówionej sumy pieniędzy, renty lub innego świadczenia, w razie zajścia przewidzianego w umowie wypadku, a ubezpieczający zobowiązuje się do zapłacenia składki*"[105].

Istotnym elementem pierwszej z tych definicji jest podkreślenie faktu repartycji strat na wiele podmiotów w razie zaistnienia niekorzystnych zdarzeń losowych. Najważniejszym elementem trzeciej z nich jest wyraźne określenie stron umowy ubezpieczenia, tzn.: ubezpieczającego (podmiot, który zawiera umowę ubezpieczenia i zobowiązuje się zapłacić składkę), ubezpieczonego (podmiot, którego dobra są objęte ochroną ubezpieczeniową) oraz ubezpieczyciela (osoba prawna uprawniona do świadczenia usług ubezpieczeniowych)[106].

3.2 Funkcje ubezpieczeń

Najważniejszymi funkcjami ubezpieczeń są:

1. Funkcje ochrony ubezpieczeniowej.
2. Funkcje prewencyjne.
3. Funkcje finansowe.

Nadrzędną z nich jest funkcja ochrony ubezpieczeniowej, pozostałe dwie są natomiast skutkiem pierwszej.

3.2.1 Funkcja ochrony ubezpieczeniowej

Istotą usługi ubezpieczeniowej jest sprzedaż ochrony ubezpieczeniowej podmiotowi ubezpieczającemu. Oznacza to gotowość przejęcia przez ubezpieczyciela na siebie materialnych skutków realizacji ryzyk objętych umową, zawartą pomiędzy ubezpieczającym a zakładem ubezpieczeń w zamian za składkę ubezpieczeniową. Ochrona ubezpieczeniowa

[104] Michalski T. (red.), 2004, Ubezpieczenia gospodarcze. Ryzyko i metodologia oceny, Wydawnictwo C. H. Beck. Warszawa, str. X [60]
[105] Art. 805 Kodeks cywilny, Księga trzecia XXVII Umowa ubezpieczenia
[106] Sangowski, T. 1994. Gospodarka finansowa kapitałami i rezerwami ubezpieczyciela, w : Ubezpieczenia w gospodarce rynkowej, Wosiewicz A. red. t.1. Oficyna Wydawnicza Branta . Bydgoszcz. [106]

jest świadczona przez cały czas trwania stosunku ubezpieczenia i polega na stałej gotowości do pokrycia ewentualnej straty.

3.2.2 Funkcja prewencyjna

Istotą prewencji jest działalność zmierzająca zarówno do zmniejszenia ewentualnych szkód losowych, jak również ich ograniczenia lub zmniejszenia prawdopodobieństwa ich wystąpienia. Często zakłady ubezpieczeń są bardziej od ubezpieczających zainteresowane, by do wypadku ubezpieczeniowego nie doszło.

3.2.3 Funkcja finansowa

Funkcje finansowe ubezpieczeń polegają na gromadzeniu środków niezbędnych do wypłaty ewentualnych odszkodowań w postaci funduszy i rezerw. Do tych funkcji zalicza się funkcję:

- redystrybucyjną, polegającą na kumulowaniu i odpowiednim rozdzielaniu środków finansowych,
- fiskalną, polegająca na odprowadzaniu podatków do właściwych podmiotów publicznych,
- lokacyjną, polegającą na lokowaniu wolnych środków w inne instrumenty finansowe, które generują dodatkowe dochody,
- interwencyjną lub stymulacyjną, polegającą na kreowaniu bodźców służących zmniejszeniu ryzyka, stymulując rozwój nowych dziedzin gospodarki wykorzystujących postęp technologiczny,
- kontrolną, polegającą na monitorowaniu postępowania ubezpieczającego z przedmiotem ubezpieczenia.

3.3 Ryzyko ubezpieczeniowe

Uzasadnieniem wszelkiej działalności ubezpieczeniowej jest istnienie ryzyka, dlatego „idea ubezpieczeń powstała w wyniku dążenia ludzi do ograniczenia lub wyłączenia zdarzeń losowych występujących w postaci niszczącego oddziaływania sił przyrody lub będących skutkiem działalności człowieka[107]. Jednak zdefiniowanie ryzyka, choć jest bardzo istotne z punktu widzenia ubezpieczeń, jest trudne z uwagi na to, że ryzyko jest uzależnione od wielu różnych czynników.

W obszarze ubezpieczeń istnieje wiele definicji ryzyka, które można spotkać w polskiej literaturze ubezpieczeniowej[108]. Większość z nich powstawała na początku kształtowania się teorii ubezpieczeniowych i z biegiem lat zostały one porzucone jako nieprzydatne, a dziś mają wartość wyłącznie historyczną, pokazują bowiem ewolucję podejścia do problematyki ryzyka. Na potrzeby tej rozprawy należy przyjąć (w odróżnieniu od definicji ryzyka związanego z bezpieczeństwem systemów informatycznych opisanych w rozdziale 2 tej rozprawy), że „*ryzyko jest prawdopodobieństwem wystąpienia straty*", przy czym za definicję strat przyjmuje się: „*…straty, które poszkodowany poniósł, oraz korzyści, które mógłby osiągnąć, gdyby szkody nie wyrządzono*". [109] Zatem stratą może być nie tylko fizyczne uszkodzenie sprzętu służącego działalności biznesowej, ale też utrata danych, których ręczne odtworzenie jest dodatkowym kosztem jaki musi ponieść organizacja by powrócić do swojej działalności (przypadek Visa por. rozdział 2.7). Kolejną stratą dla organizacji mogą być dodatkowe koszty obrony procesowej, jeśli strata organizacji spowodowała również straty innych podmiotów gospodarczych powiązanych z nią biznesowo. Natomiast stratą w sferze niematerialnej jest utrata zaufania klientów do firmy, a także zła opinia o organizacji kreowana przez media na skutek nagłośnienia zdarzenia będącego materializacją ryzyka (ponownie przypadek Visy ze stycznia 2008 roku por. rozdział 2.7 tej rozprawy).

---

[107] Śliwiński A., 2002, Ryzyko ubezpieczeniowe taryfy – budowa i optymalizacja, Wydawnictwo Poltext, Warszawa, str. 35 [116]

[108] Definicje te są cytowane przez autorów popularnych na rynku polskim podręczników: Śliwiński A., 2002, Ryzyko ubezpieczeniowe taryfy – budowa i optymalizacja, Wydawnictwo Poltext, Warszawa [116] i przez Michalski T., (red.), 2004, Ubezpieczenia gospodarcze. Ryzyko i metodologia oceny, Wydawnictwo C.H. Beck [60]

[109] Art. 361 §2 k. c. księga trzecia Zobowiązania

3.3.1 Identyfikacja ryzyka ubezpieczeniowego

Identyfikacja ryzyka jest procesem systematycznego i nieustannego rozpoznawania typów ryzyka i niepewności, z którymi można się spotkać w organizacji. Celem tych działań jest gromadzenie informacji na temat źródeł ryzyka, zagrożeń, czynników ryzyka, niebezpieczeństw i podatności na straty[110].

Metody identyfikacji ryzyk można podzielić na prewencyjne i kontrolne. Podstawową metodą identyfikacji ryzyk w ubezpieczeniach jest technika polegająca na analizie szkód historycznych z danej grupy ryzyk dotyczących podmiotu lub przedmiotu ubezpieczenia. Metoda ta wykorzystuje przede wszystkim dane statystyczne, rachunek prawdopodobieństwa oraz teorię procesów stochastycznych[111]. Zgodnie z tą metodą w celu identyfikacji grup potencjalnych ryzyk związanych z określonym podmiotem gospodarczym należy:

- opracować listę kontrolną wszystkich możliwych ryzyk oraz związanych z nimi strat mogących potencjalnie wystąpić w danej organizacji,
- określić możliwą wielkość strat dla poszczególnych ryzyk lub ich grup,
- stale uaktualniać listę ryzyk przez identyfikowanie nowych.

Metoda ta nadaje się jedynie dla ryzyk powszechnie znanych. Istnieją gotowe scenariusze ułatwiające zastosowanie tej metody w praktyce. Zostały one zbudowane dzięki współpracy i wymianie doświadczeń eksperckich przez organizacje specjalizujące się w problematyce identyfikacji ryzyk oraz metod ich oceny. Obecnie najbardziej rozpowszechnione i najczęściej stosowane są metody opracowane przez Amerykańskie Stowarzyszenie na rzecz Zarządzania – AMA (ang. American Management Association), Towarzystwo na rzecz Zarządzania Ryzykiem i Ubezpieczeniami – RIMS oraz Międzynarodowy Instytut Zarządzania Ryzykiem – IRMI (ang. International Risk Management Institute).

Kolejną metodą identyfikacji ryzyk ubezpieczeniowych jest tzw. metoda analizy warunków środowiskowych[112]. Wywodzi się ona z metod zarządzania strategicznego Freemana[113].

---

[110] Williams, C. A., Smith M.L., Young P.C., 2002. op. cit. str. 69. [124]
[111] Ronka – Chmielowiec W. (red.), 2000. Zarządzanie ryzykiem w ubezpieczeniach. Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu. Wrocław. str. 144. [100]
[112] Ronka – Chmielowiec W. (red.), 2000. ibidem str. 77 – 79. [100]
[113] Szczegóły tej metody zostały opisane w 1984 roku w publikacji Strategic Management: A Stakeholder Approach, (za Williams, C.A, Smith, M.L., Young, P. C., 2002. Zarządzanie ryzykiem a ubezpieczenia), Wydawnictwo Naukowe PWN. Warszawa, str. 77 [112]

Podstawą tej metody identyfikacji ryzyka jest budowanie scenariuszy jego występowania na podstawie modeli zadań organizacji i strategicznych kierunków jej rozwoju. Budowa scenariuszy opiera się na określeniu zagrożeń i czynników ryzyka, niebezpieczeństw i źródeł potencjalnego ryzyka.

Metody identyfikacji ryzyk zastosowane w scenariuszach mogą być oparte na:

- metodach rachunku finansowego,
- metodach wykresu chronologicznego,
- inspekcjach w miejscu pracy,
- planowym współdziałaniu z innymi jednostkami organizacyjnymi,
- wewnątrz organizacji,
- współdziałaniu z innymi organizacjami w środowisku zewnętrznym,
- analizie umów,
- statystycznej analizie poniesionych strat.

W tej metodzie również mają zastosowanie techniki oparte na obserwacji szkód historycznych.

3.3.2 Klasyfikacja ryzyka ubezpieczeniowego

Najczęściej dokonywaną klasyfikacją ryzyka ze względu na jego charakter jest podział na ryzyko obiektywne i subiektywne[114].

Ryzyko obiektywne ma charakter obiektywnej oceny możliwości wystąpienia danych skutków i jest określane jako „*względne odchylenie straty rzeczywistej w stosunku do wielkości prawdopodobnej lub inaczej oczekiwanej*[115]". Odnosi się do niego prawo wielkich liczb, dlatego w praktyce ubezpieczeniowej oznacza to wielkość nadającą się do pomiaru tzw. zagrożeń masowych. Dla zakładu ubezpieczeń jest to możliwy margines błędu w stosunku do wielkości oczekiwanych.

[114] Sangowski T., 2001, Ubezpieczenia gospodarcze. Poltext. Warszawa. str. 32 – 34 [107]
[115] Ibidem, str. 33 [107]

Ryzyko subiektywne jest związane z indywidualną oceną prawdopodobieństwa wystąpienia określonego rezultatu i jest definiowane jako niepewność oparta na osobistych uwarunkowaniach. „*Pomimo, że jest to ryzyko niemierzalne, jego ocena jest niezwykle ważna z punktu widzenia zakładu ubezpieczeń*[116]".

C. Kulp w 1928 roku zaproponował podział ryzyka na systematyczne i specyficzne[117].

Ryzykiem systematycznym jest ryzyko wynikające z działania sił przyrody i oddziałujące na dużą część populacji. Przez analogię do ryzyka wynikającego z sił przyrody, ryzyko systematyczne można też odnosić do ekonomii i polityki. Cechą charakterystyczną ryzyka systematycznego jest fakt, że zawsze istnieje i nie można go wyeliminować.

Ryzykiem specyficznym jest natomiast ryzyko, które daje się kontrolować, a nawet minimalizować. Jest ono różne dla poszczególnych branż. W dużych organizacjach narażonych na ryzyko specyficzne związane z daną branżą można je minimalizować dzięki uelastycznieniu i dywersyfikacji produkcji.

Ryzyko spekulatywne i czyste. Ten podział został wprowadzony w roku 1961 przez A. H. Mowbraya[118] i jest uznany za najbardziej użyteczny w procesie oceny ryzyka ubezpieczeniowego ze względu na klasyfikację według konsekwencji powstania strat wynikających z materializacji określonego ryzyka. Ryzyko spekulatywne dotyczy takich sytuacji, gdzie w przypadku jego materializacji mogą zajść trzy sytuacje: strata, zysk lub brak straty i zysku. W przypadku ryzyka czystego mamy do czynienia wyłącznie ze stratą majątkową, a brak materializacji ryzyka nie daje żadnych korzyści.

Kolejny podział ryzyk zaproponował E. J. Vaughan[119] na statyczne i dynamiczne w zależności od czasu ich wystąpienia. Ryzyko statyczne jest niezależne od czasu i dotyczy ryzyk wynikających z działania sił przyrody. Ryzyko dynamiczne natomiast zmienia się w czasie wraz z postępem cywilizacyjnym i przemianami gospodarczymi.

---

[116] Śliwiński A., Ryzyko ubezpieczeniowe, taryfy – budowa i optymalizacja, s. 23 [116]
[117] Michalski T. (red.), 2004. Ubezpieczenia gospodarcze. Ryzyko i metodologia oceny. Wydawnictwo C. H. Beck. Warszawa. str. 60, [za Kulp C. A. 1928. Casualy Insurance. Roland Press. New York. str. 2 - 7] [60]
[118] Michalski T. (red.), 2004. Ubezpieczenia gospodarcze. Ryzyko i metodologia oceny. Wydawnictwo C. H. Beck. Warszawa. str. 61. [za Mowbray A.H., Blanchard R.H..1961. Insurance. It's theory and practice in the United States. New York.] [60]
[119] Michalski T. (red), 2004. ibidem. str. 62 [60]

Ryzyka można również klasyfikować ze względu na charakter strat powstałych na skutek ich realizacji. Są to ryzyka finansowe i niefinansowe [120]. Zgodnie z tą klasyfikacją, ryzyka finansowe powodują stratę finansową dla podmiotów a ryzyka niefinansowe powodują negatywne skutki, niewywołujące bezpośredniej straty finansowej, wywołują natomiast potrzebę finansową w określonej perspektywie czasu.

Podział ryzyka na probabilistyczne i estymacyjne zaproponowany w 1957 roku przez F. H. Knighta[121] [122] jest istotny dla metod oceny ryzyka. Zgodnie z tym podziałem, ryzykiem probabilistycznym nazywamy ryzyko możliwe do kwantyfikacji przy użyciu metod matematycznych (ryzyko aprioryczne) lub danych statystycznych (ryzyko statystyczne). Ryzyko estymacyjne występuje w sytuacji, gdy kwantyfikacja jest wprawdzie możliwa, ale jest obarczona dużym błędem, co zbliża je do niepewności, która powoduje, że ryzyko to jest według Knighta nieubezpieczalne.

Jedną z podstawowych klasyfikacji budzącą wiele sporów, jest podział ryzyka ze względu na charakter niepewności[123]. W tej klasyfikacji wyróżnia się cztery podstawowe grupy ryzyka:

- ryzyko niepewności faktu realizacji – niepewność wystąpienia określonego zdarzenia, czyli realizacji ryzyka,
- ryzyko niepewności czasu – pewność wystąpienia realizacji ryzyka bez znajomości czasu tej realizacji,
- ryzyko niepewności skutku – pewność czasu i realizacji ryzyka bez posiadania wiedzy na temat skutków jego wystąpienia,
- ryzyko niepewności miejsca – niepewność miejsca realizacji danego ryzyka.

W teorii ubezpieczeń występują jeszcze inne klasyfikacje. Są między innymi klasyfikacje ryzyka na: fundamentalne i partykularne[124] oraz przyrodnicze i społeczne[125].

---

[120] Śliwiński A., 2002. Ryzyko ubezpieczeniowe taryfy – budowa i optymalizacja. Wydawnictwo Poltext. Warszawa. str. 27 – 28 [116]
[121] Michalski T. (red), 2004. Ubezpieczenia gospodarcze. Ryzyko i metodologia oceny. Wydawnictwo C. H. Beck. Warszawa. str. 63 [za Knight, F.H. 1957. Risk, Uncertainty and Profit. New York.] [60]
[122] Knight, F.H. 1957. Risk, Uncertainty and Profit. New York [49]
[123] Śliwiński A., 2002. Ryzyko ubezpieczeniowe taryfy – budowa i optymalizacja. Wydawnictwo Poltext. Warszawa. str. 29. [116]
[124] Michalski T. (red.), 2004, op. cit. str. 63 [60]
[125] Śliwiński A., 2002, ibidem, str. 30 [116]

Ryzyko fundamentalne ma charakter bezosobowy, a konsekwencją jego realizacji są straty odczuwalne przez całe społeczeństwa. Źródłem tego ryzyka mogą być np. klęski żywiołowe. Ryzyko partykularne natomiast ma charakter osobowy i jego realizacja może wynikać z działań jednostki (kradzież lub podpalenie) lub może spowodować straty jednostki, choć jest od działań jednostki niezależna.

Ryzyko przyrodnicze to podobnie jak wyżej klęski żywiołowe, natomiast ryzyko społeczne jest związane z działalnością człowieka.

3.3.3 Ocena i pomiar ryzyka ubezpieczeniowego

Ubezpieczenie jest narzędziem chroniącym ubezpieczonego przed niepomyślnymi skutkami zdarzeń losowych, powodujących szkody. Przewidywanie szkód losowych wiąże się natomiast z oceną i pomiarem ryzyka[126].

W teorii ubezpieczeń przyjmuje się, że pomiarem ryzyka jest nazywany proces, w którym zidentyfikowane ryzyko otrzymuje pewna konkretną wartość. Ta wartość jest mierzona dla każdego ryzyka osobno lub dla pewnych grup ryzyk łącznie.

Do oceny i pomiarów ryzyka służy statystyka ubezpieczeniowa, za pomocą której bada się dwie następujące zbiorowości statystyczne[127]:

- zbiór ubezpieczonych obiektów lub osób,
- zbiór wypadków ubezpieczeniowych powodujących powstanie roszczeń względem ubezpieczyciela.

Zarówno zbiór ubezpieczonych obiektów jak i zbiór wypadków ubezpieczeniowcy są zbiorami o określonej liczbie jednostek statystycznych – przedmiotów ubezpieczenia. Jednostki statystyczne natomiast mają cechy ilościowe takie jak: liczba wypadków ubezpieczeniowych i wielkość szkód oraz cechy jakościowe: czasowe, rzeczowe lub przestrzenne. Najistotniejsze z punktu widzenia zakładu ubezpieczeń jest posiadanie odpowiednio dużej liczby udokumentowanych danych historycznych dotyczących zarówno zdarzeń, jak i wypłaconych odszkodowań.

---

[126] Miscellaneous Errors and Omissions liability Insurance Application, ACE USA, 09. 1998 r. [61]
[127] Ronka-Chmielowiec W., 2002, op. cit. str. 174 [101]

„*Trzeba jednak pamiętać, że w działalności ubezpieczeniowej występuje również takie ryzyko, do oceny którego statystyka nie jest nauką przydatną . Czasami metody statystyczne można stosować, co najwyżej w ograniczonym zakresie. Sytuacja taka może się pojawić, gdy towarzystwo ubezpieczeniowe decyduje się na wprowadzenie na rynek ubezpieczeniowy nowych produktów ubezpieczeniowych lub gdy poprzednio sprzedawany produkt zyskał niewielką liczbę nabywców. W takich przypadkach ocenę ryzyka opiera się na opinii ekspertów lub na ocenie ryzyka podobnego*"[128].

3.3.4 Ryzyko ubezpieczeniowe i ryzyko ubezpieczyciela

Zakład ubezpieczeń jest instytucją finansową funkcjonującą na określonym rynku i w konkretnym środowisku gospodarczym, dla której ryzyko jest z jednej strony celem, a z drugiej przedmiotem działalności, która również generuje ryzyko. Ryzyko bowiem ma dla zakładu ubezpieczeń szczególne znaczenie, dlatego wyróżnia się[129]:

1. Ryzyko ubezpieczyciela związane z funkcjonowaniem zakładu ubezpieczeń.
2. Ryzyko ubezpieczeniowe związane z przedmiotem działalności.

Ponadto ryzyka towarzyszące kompleksowej działalności zakładu ubezpieczeń można podzielić na:

- zewnętrzne,
- wewnętrzne.

Do ryzyk zewnętrznych, zwanych też systematycznymi, niepodlegających kontroli podmiotu, na który oddziałują, należą: ryzyka związane z siłami przyrody, ryzyka stopy procentowej, walutowe, rynku, polityczne i inne.

Do ryzyk wewnętrznych, zwanych niesystematycznymi, związanych z działalnością podmiotu – zakładu ubezpieczeń, które mogą być kontrolowane i zarządzane, należą: ryzyko niedotrzymania warunków, ryzyko zarządzania, biznesu, finansowe, upadłości i inne.

Czynnikami wewnętrznymi wpływającymi bezpośrednio na ryzyko funkcjonowania zakładu ubezpieczeń są ryzyka: działalności techniczno-ubezpieczeniowej, ryzyka prowadzenia gospodarki finansowej i zarządzania lokatami, ryzyka związane ze strukturą własnościową

[128] Ronka-Chmielowiec W., 2002, ibidem str. 176. [101]
[129] Ronka-Chmielowiec W., 2002, ibidem str. 139 [101]

firmy i zachowaniem akcjonariuszy, ryzyka związane z funkcjonowaniem systemu informatycznego i inne.

Źródłami ryzyka związanego z prowadzeniem działalności ubezpieczeniowej są[130]:

- identyfikacja i ocena ryzyka ubezpieczeniowego,
- pomiar ryzyka ubezpieczeniowego,
- podział ryzyka ubezpieczeniowego na portfele – homogeniczne grupy o podobnych parametrach – i ocena równowagi finansowej w portfelach,
- decyzje o ubezpieczeniu ryzyka i zastosowanie właściwej techniki ubezpieczeniowej,
- kalkulacja składki ubezpieczeniowej netto i brutto,
- decyzje reasekuracyjne i ustalenie udziału własnego w reasekuracji,
- proces likwidacji szkód i ustalanie wielkości wypłaconych odszkodowań i świadczeń.

W tym kontekście największym ryzykiem dla zakładu ubezpieczeń jest „możliwość niekorzystnego odchylenia rzeczywistej wielkości roszczeń (odszkodowań) od ich wartości kalkulacyjnej"[131]. Dlatego z obawy przed nadmiernym ryzykiem zakładu ubezpieczeń, które w skrajnych przypadkach może prowadzić do jego upadłości, może on odmówić ubezpieczenia takiego ryzyka, które nie ma cech ubezpieczalności i którego przyjęcie wiąże się ze zbyt wielkim ryzykiem dla samego zakładu ubezpieczeń.

3.3.5 Zarządzanie ryzykiem w zakładach ubezpieczeniowych

Z uwagi na specyfikę prowadzonej działalności przez zakłady ubezpieczeniowe, proces zarządzania w nich ryzykiem, przybiera inną formę niż we wszelkich innych organizacjach gospodarczych[132]. Zakład ubezpieczeń z jednej strony musi prowadzić proces zarządzania własnym ryzykiem tak samo jak każda inna organizacja, a więc dokonywać: identyfikacji, analizy, oceny i pomiaru ryzyk grożących mu tak samo jak innym firmom, a z

[130] Kuchlewska M. (red.), 2006, Szkice o ubezpieczeniach, Zeszyt 75, Ronka-Chmielowiec W., Ryzyko zakładu ubezpieczeń a ryzyko ubezpieczeniowe. Wydawnictwa Akademii Ekonomicznej w Poznaniu, str. 166 – 168 [52]
[131] Monkiewicz J. (red.), 2004, Podstawy ubezpieczeń. Tom III – przedsiębiorstwo, Poltext, Warszawa [64]
[132] Capik, M. i M., Zarządzanie ryzykiem ubezpieczeniowym dużych podmiotów gospodarczych, Prawo, Ubezpieczenia, Reasekuracja, 1997 r. nr 2. [12]

drugiej strony musi prowadzić dokładną analizę cudzych ryzyk przejmowanych od ubezpieczanych podmiotów. W zakładach ubezpieczeniowych proces zarządzania ryzykiem skupia się na czterech głównych etapach, które nie odpowiadają poszczególnym etapom zarządzania ryzykiem w innych organizacjach:

1. Analiza ryzyka.
2. Kontrola ryzyka.
3. Finansowanie ryzyka.
4. Administrowanie procesem bezpiecznego kierowania zakładem ubezpieczeń.

3.3.5.1 Analiza ryzyka

Zarządzanie ryzykiem w zakładach ubezpieczeniowych obejmuje zarówno analizę ryzyk wewnętrznych opisanych w rozdziale 3.3.4 jak i analizę wszystkich ryzyk związanych z prowadzoną działalnością ubezpieczeniową, za które odpowiada Dział Akceptacji (ang. underwriting). Są to ryzyka zidentyfikowane wcześniej przez menedżerów do spraw ryzyka klienta, które pracownicy Działu Akceptacji zakładu ubezpieczeń muszą ponownie przeanalizować.

3.3.5.2 Kontrola ryzyka

Podczas całego okresu trwania umowy ubezpieczenia ryzyka przyjęte do ubezpieczenia powinny być monitorowane przez zakład ubezpieczeń w celu ewentualnego korygowania zawartych umów lub podejmowania działań prewencyjnych. Na podstawie wyników kontroli firma ubezpieczeniowa może podjąć decyzję o weryfikacji warunków ogólnych tak, by przyjmowanie do ubezpieczenia następnych klientów odbywało się na lepszych warunkach.

Likwidacja szkód w poszczególnych grupach powinna być również dokonywana na podstawie określonych procedur, które muszą być elementem kompleksowego procesu zarządzania ryzykiem zakładu ubezpieczeń.

3.3.5.3 Finansowanie ryzyka

Przez finansowanie ryzyka z poziomu zarządzania ryzykiem zakładu ubezpieczeń należy rozumieć decyzje strategiczne dotyczące wyboru sposobu finansowania lub połączenia sposobów finansowania poszczególnych ryzyk polegające między innymi na przyjęciu grupy

ryzyk w całości lub w części. Jeśli tylko w części, wtedy jest to tzw. franszyza. Franszyza „*jest to postanowienie umowy ubezpieczenia, zwane klauzulą umowną, uzgodnione i zapisane w polisie, przerzucające na ubezpieczającego część poniesionej szkody na określonych warunkach*”[133].

3.3.5.4 Administrowanie procesem bezpiecznego kierowania zakładem ubezpieczeń

Administrowanie procesem bezpiecznego kierowania zakładem ubezpieczeń polega na opracowaniu bezpiecznego programu działania zakładu ubezpieczeń, ocenie jego przebiegu i dostosowywaniu go do polityki związanej z kompleksową działalnością finansową. Obejmuje w szczególności tworzenie rezerw i lokaty wolnych środków, za które odpowiada aktuariusz z racji obowiązków nałożonych przez ustawę o działalności ubezpieczeniowej[134], pełniący także rolę nadzoru wewnętrznego zakładu ubezpieczeń[135].

Na tym etapie jest również istotna analiza konkurencyjności i opłacalności oferowanych produktów oraz dostosowywanie ich do ciągle zmieniających się warunków otoczenia[136].

Kompleksowe zarządzanie ryzykiem zakładu ubezpieczeniowego to również konieczność współpracy z niezależnymi ekspertami z poszczególnych dziedzin oraz firmami świadczącymi usługi doradztwa dla tych zakładów, niezbędna zwłaszcza w procesie tworzenia nowych produktów, gdzie tylko obiektywizm podmiotów zewnętrznych może zagwarantować właściwą klasyfikację i ocenę możliwych zagrożeń.

3.3.6 Rola i zadania aktuariusza w zakładzie ubezpieczeń

Zgodnie z obowiązującą ustawą o działalności ubezpieczeniowej[137], każdy zakład ubezpieczeniowych jest zobowiązany do zatrudniania aktuariusza, czyli osoby fizycznej,

---

[133] Słownik terminów finansowo-ekonomicznych.
[134] Ustawa o działalności ubezpieczeniowej z dn. 22 maja 2003 roku (Dz. U. z dn. 16 lipca 2003, poz. 1151), rozdz. 9 [120]
[135] Królikowska-Bocheńczyk, J. Wyłączenia odpowiedzialności, cz. 1 (04. 04. 2006 r.), cz. 2 (18. 04. 2006 r.), cz., 3 (02. 05. 2006 r.) i cz. 4 (13. 06. 2006 r.) Gazeta Ubezpieczeniowa [50]
[136] Nagle, W. Ubezpieczenia w transformacji ubezpieczeniowej, Prawo, Ubezpieczenia, Reasekuracja, 2006 nr 12 [66]
[137] Ustawa o działalności ubezpieczeniowej z dn. 22 maja 2003 roku (Dz. U. z dn. 16 lipca 2003, poz. 1151) [120]

spełniającej wymogi określone ustawą, wykonującej czynności w zakresie matematyki ubezpieczeniowej, finansowej i statystyki, wpisanej do rejestru aktuariuszy[138].

Do głównych zadań aktuariusza należy:

1. Ustalanie wartości rezerw techniczno-ubezpieczeniowych.
2. Kontrolowanie zgodności aktywów stanowiących pokrycie rezerw techniczno-ubezpieczeniowych na warunkach określonych w art. 167 ww. Ustawy.
3. Wyliczanie marginesu wypłacalności.
4. Sporządzanie rocznego raportu o stanie portfela ubezpieczeń.
5. Ustalanie wartości składników zaliczanych do środków własnych.

Ponadto aktuariusz powinien kontrolować wszystkie aspekty działania zakładu ubezpieczeń, które mogłyby mieć wpływ na jego sytuację finansową, stąd musi mieć on stały dostęp do wszelkich informacji, w szczególności do informacji dotyczących[139]:

- stanu portfela ubezpieczeń oraz informacji o jego zmianach w ciągu roku rozliczeniowego,
- składek brutto płaconych przez klientów w już istniejących portfelach oraz składek, według których towarzystwo zamierza sprzedać nowe polisy,
- charakteru zawartych umów, w odniesieniu do różnego rodzaju gwarancji w nich zawartych, umów reasekuracyjnych oraz umów planowanych,
- aktualnego portfela aktywów oraz zasad polityki inwestycyjnej dotyczących poszczególnych funduszy,
- aktualnego poziomu kosztów zakładu oraz oczekiwanego poziomu przyszłych kosztów wraz z podziałem na ich rodzaje,
- aktualnej i przewidywanej sytuacji podatkowej zakładu ubezpieczeń,
- wyceny jednostek, które są umarzane w celu wypłaty świadczeń ubezpieczeniowych.

[138] Ustawa o działalności ubezpieczeniowej z dn. 22 maja 2003 roku (Dz. U. z dn. 16 lipca 2003, poz. 1151), rozdz. 9 art. 158 – 159 [120]
[139] Pietrzykowska A., Rola aktuariusza i nadzór wewnętrzny, Prawo Asekuracyjne, 2002 nr 4 [87]

Wiedza na temat szczegółowej działalności finansowej jest niezbędna aktuariuszowi w procesie kompleksowego monitorowania i nadzoru nad gospodarką finansową całego zakładu ubezpieczeń. Ze względu na nadzór wewnętrzny do czynności wykonywanych przez aktuariusza należą:

1. Ustalanie założeń do wyliczenia składek brutto dla ubezpieczeń tradycyjnych oraz poziomu opłat pobieranych w przypadku umów z funduszem inwestycyjnym, przy czym założenia przyjęte do kalkulacji składek podlegają ciągłemu monitorowaniu i weryfikacji.
2. Monitorowaniu źródeł zysku zakładu ubezpieczeń.
3. Kalkulacja wartości portfeli oraz zrealizowanego poziomu zyskowności na nowo sprzedanych umowach w danym okresie sprawozdawczym, która jest związana z monitorowaniem bieżącego portfela oraz założeń przyjętych do wyliczeń.
4. Określenie poziomu wymagań kapitałowych niezbędnych do funkcjonowania zakładu. Przez kalkulacje marginesu wypłacalności wymaganego dla danego portfela określane zostają wymagania kapitałowe w takiej wysokości, aby zapewnić środki własne towarzystwa na jego pokrycie.
5. Określenie scenariuszy niebezpiecznych dla danego portfela ubezpieczeń.
6. Analiza umów reasekuracyjnych.
7. Weryfikacja przyznanej stopy udziału w zyskach inwestycyjnych w danej umowie ubezpieczenia.
8. Tworzenie zasad funkcjonowania nowych produktów ubezpieczeniowych.

Jednym z podstawowych zadań aktuariusza w stosunku do rady nadzorczej zakładu ubezpieczeniowego jest sporządzanie rocznego raportu o „Sytuacji Finansowej Zakładu Ubezpieczeń", zawierającego analizy, wyniki badań i opinię dotyczącą bieżącej i przyszłej sytuacji finansowej. Raport ten jest przedstawiany zarządowi i radzie nadzorczej. Analizy zawarte w tym raporcie pomagają władzom w podejmowaniu krótko i długookresowych decyzji strategicznych. Aktuariusz, będąc często członkiem zarządu, lub będąc powoływany przez zarząd, pełni nadrzędną rolę w stosunku do innych departamentów zakładu ubezpieczeń w tym także Działu Akceptacji, który jest odpowiedzialny wyłącznie za decyzje związane z konkretnym ryzykiem ubezpieczeniowym.

3.3.7 Rola i znaczenie działu akceptacji w działalności ubezpieczeniowej

Angielskie słowo *underwriting* w dosłownym tłumaczeniu oznacza podpisywanie. Nazwa ta początkowo była utożsamiana z najstarszym towarzystwem ubezpieczeniowym, brytyjskim Lloydem, który w XVII wieku rozpoczął działalność w jednej z portowych kawiarni w Londynie, a słowo *underwriter* oznaczało osobę, która składała podpis pod umową ubezpieczeniową, tym samym potwierdzając jej ważność i wiarygodność.

3.3.7.1 Pojęcie akceptacji ubezpieczeniowej

Obecnie *akceptacja* (ang. underwriting) to znacznie szersze pojęcie i nie oznacza jedynie podpisywania umów, albowiem przedmiotem zainteresowanie działu akceptacji jest przede wszystkim ryzyko ubezpieczeniowe, a w szczególności proces oceny tego ryzyka. Najczęściej definiuje się, że: „*akceptacja ubezpieczeniowa jest procesem, w którym dokonuje się selekcji ryzyk ubezpieczeniowych, a następnie na jej podstawie akceptuje się ubezpieczenia na odpowiednich warunkach lub całkowicie się je odrzuca* [140]*”* lub też, że jest to: „*proces selekcji i klasyfikacji zagrożeń deklarowanych do ubezpieczenia* [141]*”*. Niezależnie od przyjętej definicji, na akceptacje ryzyka ubezpieczeniowego składają się trzy podstawowe działania:

- ukierunkowana analiza ryzyka,
- selekcja ryzyka ubezpieczeniowego,
- klasyfikacja ryzyka ubezpieczeniowego, podział na różne typy podzbiorów w zależności od przyjętych zasad.

Te trzy elementy składają się na system przyjmowania ryzyka do ubezpieczenia oraz jego monitorowanie.

3.3.7.2 Cele akceptacji ryzyka ubezpieczeniowego

Akceptacja ryzyka jest ważną funkcją firmy ubezpieczeniowej ponieważ stanowi istotny element całościowego zarządzania firmą ubezpieczeniową. Często jest on niesłusznie utożsamiany z zarządzaniem ryzykiem tej firmy, ponieważ stanowi zbiór metod działania,

[140] Rogala I., Rola i znaczenie underwritingu w kształtowaniu i realizacji strategii firmy ubezpieczeniowej. „Prawo Asekuracyjne" 1997, nr 3 [99]
[141] Jedynak P., 2003, Ubezpieczenia gospodarcze. Wybrane elementy teorii i praktyki, Księgarnia Akademicka, Kraków, str. 61 [48]

form organizacyjnych oraz instrumentów zarządzania mających istotny wpływ na bezpieczeństwo ekonomiczne firmy ubezpieczeniowej. Są to jednak dwa różne obszary działalności, z których jeden jest elementem drugiego.

Głównymi przesłankami, które zadecydowały o obecnej pozycji działu akceptacji ryzyka w firmach ubezpieczeniowych, były[142]:

- doświadczenia związane z zagrożeniami ekonomicznymi towarzystw ubezpieczeniowych, wywołanymi zbyt dużą kumulacją strat powstałych na skutek niedostatecznego rozpoznania ryzyka na skutek źle przeprowadzonej analizy,
- ograniczenia identyfikacyjne i diagnostyczne przy zastosowaniu statystycznych metod oceny ryzyka,
- wymagania towarzystw reasekuracyjnych i poszczególnych technik reasekuracji.

Podstawowym celem działu akceptacji, niezależnie od rodzaju ryzyka, jest ograniczenie *selekcji negatywnej* (ang. adverse selection), która może powstać w sytuacji, *„kiedy sprzedaż polis ubezpieczeniowych wyzwala popyt podmiotów o zwiększonym stopniu ryzyka[143]”*. Oczywiście celem nie jest też taki dobór ryzyk, które na pewno nie zakończą się szkodami ubezpieczeniowymi, bo prowadziłoby to do sytuacji absurdalnych, a zbiór „pewnych klientów” mógłby zostać szybko wyczerpany. Jeżeli za nadrzędny cel akceptacji ryzyka przyjmuje się ograniczenie zjawiska selekcji negatywnej, to celami cząstkowymi są[144]:

1. Uzyskanie adekwatności warunków ochrony ubezpieczeniowej w stosunku do faktycznych rozmiarów ryzyka zgłoszonego do ubezpieczenia.
2. Tworzenie wśród podmiotów ubezpieczanych świadomości związku pomiędzy rozmiarami ryzyka a warunkami ochrony ubezpieczeniowej.
3. Stymulowanie ubezpieczających się podmiotów do „zmniejszania ryzyka”.
4. Obniżenie kosztów odszkodowań wypłacanych przez zakłady ubezpieczeniowe.
5. Obniżanie kosztów ochrony ubezpieczeniowej w skali całego portfela ubezpieczonych i pojedynczych członków tego portfela.
6. Eliminowanie z portfeli ubezpieczeniowych nielosowych elementów ryzyka.

[142] Jedynak P. 2003, op. cit., str. 62 [48]
[143] Jedynak P. 2003, ibidem., str. 62 [48]
[144] Jedynak P. 2003, ibidem., str. 63 [48]

7. Tworzenie podstaw do rozwoju ubezpieczeń przez coraz lepszą identyfikację ryzyka, np. pod kątem nowych produktów ubezpieczeniowych.

3.3.7.3 Przebieg procesu akceptacji ryzyka

Proces akceptacji ryzyka przebiega w kilku fazach połączonych związkami przyczynowo-skutkowymi przy uwzględnieniu tożsamości stosunku i umowy ubezpieczenia[145]. W każdej z tych faz korzysta się z innych narzędzi i metod. Przykładowe narzędzia zastosowane w kolejnych fazach procesu akceptacji ryzyka przez towarzystwa ubezpieczeniowe przedstawiają się następująco[146]:

1. Analiza ryzyka. Wniosek ubezpieczeniowy, techniki pozyskiwania informacji, techniki badań (wywiad, ankieta), audyt, inspekcja, analiza dokumentacji, informacje od agentów, brokerów i firm specjalistycznych, techniki oceny ryzyka, analiza scenariuszowa, techniki statystyczne, analiza profilowa, drzewo błędów, drzewo zdarzeń.
2. Selekcja ryzyka. Techniki wspomagania podejmowania decyzji, analiza scenariuszowa, testy zgodności, analiza drzew decyzyjnych, tabele decyzyjne, metody punktowe, analiza odchyleń, analiza wartości granicznych, analiza wariantów, techniki portfelowe.
3. Klasyfikacja ryzyka. Listy kontrolne, techniki porządkowania, analiza komputerowa przy użyciu odpowiednich narzędzi, analiza porównawcza, technika przedziałów, metody punktowe, technika wartości progowych.
4. Kontrola ryzyka (ang. postselection underwriting). Techniki pozyskiwania informacji, środki organizacyjno-techniczne rejestracji informacji, techniki oceny ryzyka, techniki wspomagania podejmowania decyzji, techniki i środki klasyfikacji ryzyka.

Ostatnia faza zachodzi tylko wówczas, gdy nie nastąpiła odmowa ubezpieczenia, a jej celem jest obserwowanie i reagowanie na ewentualne zmiany w ubezpieczonym ryzyku.

Naturalnie zakres zadań w ramach funkcji akceptacji ryzyka może być bardzo zróżnicowany w zależności od typu usługi ubezpieczeniowej, ale największą rolę może odegrać w

[145] Maleszka, L. 2000, Zarządzanie ryzykiem a underwriting w ubezpieczeniach na życie, artykuł na podstawie pracy magisterskiej, A E Poznań, Katedra Ubezpieczeń Gospodarczych, www.ryzyko.pl [55]
[146] Jedynak P., 2003, ibidem., str. 66 [48]

ubezpieczeniach dużych i nietypowych przedsięwzięć oraz konstrukcji zupełnie nowych produktów ubezpieczeniowych adresowanych do nowych ryzyk.

3.3.8 Ubezpieczalność ryzyka

Ponieważ „*ubezpieczalność polega na możliwości przekazywania ryzyka*” [147], dla ubezpieczonego oznacza ona limit ochrony ubezpieczeniowej.

Zatem zgodnie z definicją przyjętą przez autorów pracy pt. „Zarządzanie ryzykiem a ubezpieczenia” „*ryzyko można uznać za doskonale ubezpieczalne, jeśli spełnia cztery przedstawione dalej warunki*” [148]:

1. Duża liczba jednostek jest niezależnie i identycznie narażona na ryzyko na tyle istotne, aby zainteresować ubezpieczeniem osoby odpowiedzialne za te jednostki. Duża liczba jednostek oznacza, że dotyczą je prawa wielkich liczb.
2. Szkoda powinna być określona, czyli mieć określony czas zajścia, miejsce, przyczynę i wartość.
3. Oczekiwana szkoda powinna być możliwa do obliczenia w pewnym rozsądnym okresie.
4. Strata powinna być niezamierzona i przypadkowa z punktu widzenia ubezpieczonego.

„Warunek drugi i trzeci są niezbędne. Jeśli zdarzenie powodujące powstanie konieczności wypłaty odszkodowania oraz wynikająca z tego wartość szkody nie są w wyraźny sposób określone, to mogą powstać spory wokół definicji ubezpieczonego zdarzenia oraz ustalenia sumy odszkodowania.[149]”

W polskiej literaturze przedmiotu istnieje również kilka klasyfikacji warunków ubezpieczalności ryzyka. Autor jednego z podręczników do warunków ubezpieczalności zalicza[150]:

[147] Fedor M., 2004, Gazeta Ubezpieczeniowa, 31/2004 [37]
[148] Williams C. A., Smith M. L., Young P. C., 2002, op. cit. str. 354 [124]
[149] Williams C. A., Smith M. L., Young P. C., 2002 ibidem., str. 355 [124]
[150] Perenc J. (red.), 2004, Rynek usług ubezpieczeniowych, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin [86]

- losowość występowania szkód. Dotyczy to zarówno powstania, wielkości, jak i czasu zajścia wypadku ubezpieczeniowego,
- oszacowanie rozkładu prawdopodobieństwa szkód. Oznacza to przyporządkowanie pewnym wielkościom szkód określonego prawdopodobieństwa,
- jednoznaczności rozkładu prawdopodobieństwa szkód, uwarunkowanego cechami wypadku ubezpieczeniowego, na kanwie którego rozgraniczono branże ubezpieczeniowe,
- niezależność ubezpieczeniowych rozkładów szkód od siebie. Nie powinny bowiem istnieć żadne systematyczne związki tego rodzaju, że przy zajściu pewnego zdarzenia zostanie uwolniona reakcja łańcuchowa szkód u innych podmiotów,
- podstawowe wielkości rozkładu szkód muszą być możliwe do oszacowania, aby uchronić towarzystwo przed ruiną, w razie możliwości zajścia dużych szkód.

Z kolei w podręczniku „Podstawy ubezpieczeń. Tom I – mechanizmy i funkcje” [151] J. Monkiewicz za warunek ubezpieczalności ryzyka przyjmuje, że:

- istnieje odpowiednio duża liczba narażonych jednostek – warunek racjonalnego przewidywania strat (ekonomiczne następstwa ryzyka),
- zdarzenie będące następstwem materializacji ryzyka musi mieć charakter nadzwyczajny albo przypadkowy,
- strata spowodowana przez zdarzenie będące następstwem materializacji ryzyka musi być definitywna i mierzalna,
- strata powstała w wyniku materializacji ryzyka nie może mieć charakteru katastrofalnego.

Ujmując problem syntetycznie, podstawowe atrybuty, które bezwzględnie charakteryzują ubezpieczalność ryzyka to[152]:

1. Losowość. Zdarzenia muszą być losowe, aby były ubezpieczalne. Występowanie szkód musi być wynikiem tylko takich zdarzeń, które mogą zajść, ale nie muszą[153].

[151] Monkiewicz, J. (red.) 2000, Podstawy ubezpieczeń. Tom I – mechanizmy i funkcje, Poltext, Warszawa, str. 51 [62]
[152] Fedor. M. 2004, Gazeta Ubezpieczeniowa, 32/2004 [37]
[153] Dotyczy ubezpieczeń majątkowych.

2. Przyszłość. Moment wystąpienia wypadku szkodowego jest nieznany. Ryzyko nie może być zrealizowane w momencie zawarcia umowy ubezpieczenia.
3. Niezależność od woli ubezpieczonego (egzogeniczność). Ponieważ w praktyce istnieją przypadki, kiedy można przewidzieć możliwość zrealizowania ryzyka, zakłady ubezpieczeń wprowadzają franszyzy, których zadaniem jest zmotywowanie ubezpieczonego do większej ostrożności, transferując na niego część ryzyka finansowego.
4. Łączność. Ryzyka łączy się w portfele. Im większa grupa podmiotów należy do jednego portfela, tym mniejsze prawdopodobieństwo błędu statystycznego.
5. Szacowalność. Ryzyko musi podlegać statystycznej prawidłowości, aby było możliwe prognozowanie z dużą dokładnością wartości ekonomicznej skutków wywołanych przez jego materializację. Jeżeli bowiem zakład ubezpieczeń nie może oszacować ryzyka, to nie jest w stanie przewidzieć ewentualnych strat, aczkolwiek *„…niektóre towarzystwa ubezpieczeniowe są skłonne wystawiać ochronę ubezpieczeniową od zagrożeń niezwykłych lub wyjątkowych, których nie dotyczy prawo wielkich liczb* [154]”, oceniają wówczas ryzyko bazując na wiedzy i doświadczeniu swoich pracowników, korzystają z analiz naukowych, lub opinii niezależnych ekspertów.

[154] Wiliams C. A., Smith M. L., Young P. C., 2002 ibidem., str. 355 [124]

3.4 Produkty ubezpieczeniowe adresowane do nowych ryzyk

Przemiany gospodarcze w Polsce po 1990 roku sprawiły, że sektor ubezpieczeniowy stał się jednym z najszybciej rozwijających się obszarów usług finansowych. Szybkie tempo zmian oraz wejście do kraju nowych, zagranicznych podmiotów wpłynęło na wzrost konkurencyjności w całej branży. Wejście kapitału obcego spowodowało rozszerzenie oferty towarzystw ubezpieczeniowych o produkty lepiej odpowiadające potrzebom klientów, a wcześniej nie oferowane na polskim rynku, jak np. ubezpieczenia inżynieryjno-techniczne.

Pierwszym ubezpieczeniem technicznym wprowadzonym prawie 150 lat temu przez brytyjską firmę Steam Boiler Assurance Company było ubezpieczenie kotłów parowych. Obecnie oferta ubezpieczeń tego typu obejmuje kilkanaście różnych produktów. Do tej kategorii nowych produktów ubezpieczeniowych, które źródło mają w tradycji anglosaskiej (stąd angielskie nazwy tych produktów), należą[155]:

1. Ubezpieczenie ryzyk budowlanych (ang. Contractors' All Risks).
2. Ubezpieczenie maszyn i urządzeń budowlanych (ang. Contractor' Plant and Machinery).
3. Ubezpieczenie ryzyk montażowych (ang. Erection All Risks).
4. Ubezpieczenie ryzyk budowlano-montażowych (ang. CAR/EAR – Open Cover); są to ubezpieczenia niepowtarzalne w czasie, zawierane na okresy jednorazowe.
5. Ubezpieczenie maszyn od awarii (ang. Machinery Breakdown).
6. Ubezpieczenie sprzętu elektronicznego (ang. Electronic Equipment Insurance).
7. Ubezpieczenie utraty zysku w wyniku awarii maszyn (ang. Loss of Profits following Mechinery Breakdown).
8. Ubezpieczenie utraty zysku inwestora w wyniku szkody objętej ubezpieczeniem robót budowlanych (ang. Principal's Advanced Loss of profits – AloP/CAR).
9. Ubezpieczenie utraty zysku inwestora w wyniku szkody objętej ubezpieczeniem robót montażowych (ang. Principal's Advanced Los sof profits – AloP/EAR).
10. Ubezpieczenie konstrukcji budowlanych oddanych do eksploatacji (ang. Civil Engeneering Completed Risks – CECR).
11. Ubezpieczenie kotłów i zbiorników ciśnieniowych (ang. Boiler and Pressure Vessel).

[155] Butryn E., Piskozub W., 2003, Ubezpieczenia inżynieryjno-techniczne, Poltext, Warszawa, str. 5 [11]

12. Ubezpieczenie zepsucia się towaru w magazynach i chłodniach (ang. Deterioration of Stock – DOS).
13. Ubezpieczenie maszyn i urządzeń leasingowych (ang. Leasing All Risk).
14. Ubezpieczenie silników lotniczych (ang. Aero – Engine Breakdown).
15. Ubezpieczenie kompleksowe mechanizacji rolniczej (ang. Comprehensive Agricultural Engineering Risk).
16. Ubezpieczenie ryzyk umiejscowionych w środowisku morskim (ang. Working Offschore Risks).

Jest to bardzo specyficzna grupa produktów wymagająca od ubezpieczyciela specjalistycznej wiedzy, albowiem szacowanie ryzyka, kalkulacja składki, a także działania prewencyjne opierają się często na innych kryteriach, o których decyduje głównie specyfika ubezpieczonych ryzyk.

W tej grupie można wydzielić dwa rodzaje ubezpieczeń technicznych:

- ubezpieczenia niepowtarzalne w czasie, zawierane na okresy jednorazowe (pkt. od 1. do 4.),
- ubezpieczenia zawierane na okresy powtarzalne, nieograniczone w czasie.

W pierwszej grupie znajdują się ubezpieczenia wszystkich ryzyk budowlanych oraz montażu, a także ubezpieczenie gwarancji dla maszyn i urządzeń. Ubezpieczeniem tym mogą być objęte kontrakty na uzgodnionych warunkach, po wcześniejszym zgłoszeniu. Ochrona ubezpieczeniowa trwa od chwili rozpoczęcia robót lub momentu rozładowania ubezpieczonych pozycji na placu budowy/montażu i wygasa z chwilą przekazania obiektu inwestorowi, lub do użytku. Okres ubezpieczenia jest związany z czasem trwania budowy lub montażu. W skomplikowanych projektach może trwać nawet 7 do 10 lat. Istnieje także możliwość zawarcia umowy rocznej.

Druga grupa obejmuje wszystkie pozostałe ubezpieczenia.

Jak widać z powyższej klasyfikacji zakres ryzyk objętych ubezpieczeniami inżynieryjno-technicznymi jest bardzo szeroki, co świadczy o rozwijającej się świadomości ubezpieczeniowej właścicieli przedsiębiorstw. Z uwagi na tematykę tej rozprawy najbardziej

interesującymi rodzajami ubezpieczeń są ubezpieczenia dedykowane systemom informatycznym.

3.5 Rozwój produktów ubezpieczeniowych dedykowanych systemom informatycznym

Pierwszą polisą na świecie jaka powstała w celu ochrony sprzętu komputerowego była polisa **Ubezpieczenie komputerów od wszelkich ryzyk**[156]. Służyła ona ochronie sprzętu komputerowego i wyposażenia komputerowego, traktowanego jako nierozłączna jednostka operacyjna, umiejscowiona w konkretnej lokalizacji. Produkt ten obejmował również ryzyka takie jak: dokonanie niewłaściwej operacji, świadome lub złośliwe działanie, natomiast nie obejmował jeszcze komputerów osobistych i przenośnych. Przedmiotem ubezpieczenia były: sprzęt komputerowy, zawartość pamięci komputerów (informacje i programy operacyjne) i koszty dodatkowe związane z odtworzeniem przechowywanych danych.

Zakres ubezpieczenia obejmował trzy sekcje i w dalszym ciągu obejmuje je mimo ewolucji tego produktu :

1. Ubezpieczyciel odpowiada za wszelkie nagłe i nieprzewidziane straty lub szkody materialne w sprzęcie komputerowym, który wymagał naprawy lub wymiany, których przyczyny nie były wymienione na liście wyłączeń od odpowiedzialności.
2. Ubezpieczyciel odpowiada za dane utracone z pamięci komputerów, za nośniki do ich przechowywania oraz ich odtworzenie, jeśli strata była spowodowana przez wydarzenie, za które odpowiada ubezpieczyciel, zgodnie z warunkami sekcji 1.
3. Ubezpieczyciel zwraca również dodatkowe koszty poniesione z powodu konieczności prowadzenia działalności na sprzęcie wynajętym, w wynajętej lokalizacji, lub przeprowadzki a także inne koszty zapewnienia działalności operacyjnej.

W każdej z sekcji były przewidziane wyłączenia, do których należały m.in.: normalne zużycie i eksploatacja; szkody powstałe po uszkodzeniu sprzętu a przed jego naprawą; szkody wynikłe z aktywności sejsmicznej; konsekwencje szkód materialnych dla osób trzecich;

[156] Monkiewicz, J. (red.), 2001, Podstawy ubezpieczeń. Tom II – produkty, Poltext, Warszawa, str. 219 i 220. [63]

utracone korzyści; błędy w oprogramowaniu; perforacji[157]; załadunku danych lub drukowaniu; usunięcie danych, które nie jest spowodowane szkoda materialną chronioną w sekcji 1 i itp.

Jako ubezpieczenie dodatkowe do poprzedniego powstał produkt **Ubezpieczenie sprzętu elektronicznego**. Jego rola z racji coraz szerszego zastosowania wszelkich urządzeń komputerowych służących produkcji i świadczeniu usług, jest coraz większa. Produkt ten „*w chwili obecnej wykazuje największą dynamikę rozwoju z uwagi na tempo wzrostu składki i na ciągle zmieniające się zasady jego działania* [158]”.[159]

Przedmiotem ubezpieczenia jest w tym przypadku wszelki sprzęt elektroniczny, stacjonarny, używany zgodnie z przeznaczeniem, przy czym pojęcie „sprzęt elektroniczny” jest rozumiane bardzo szeroko. Mogą to być zarówno systemy informatyczne, systemy alarmowe, sprzęt medyczny, systemy telefoniczne, sprzęt komputerowy, a także zewnętrzne nośniki danych. Może to być zarówno sprzęt własny jak też wypożyczony lub wzięty w leasing.

Z tak szerokiego pojmowania przedmiotu ubezpieczenia wynika, że adresatem tego produktu może być bardzo duża liczba podmiotów, bowiem obecnie większość organizacji gospodarczych wykorzystuje w bieżącej działalności różne urządzenia elektroniczne i tylko od decyzji zakładu ubezpieczeń zależy, które sprzęty zaliczy on do tej kategorii.

Zakres ubezpieczenia (oprócz tego zawartego w poprzedniej polisie) obejmuje dodatkowo: awarie klimatyzacji, kradzież z włamaniem, krótkie spięcia i zwarcia instalacji elektrycznej, błędy konstrukcyjne, błędy w obsłudze, niedbalstwo pracowników, pracę w godzinach nadliczbowych, transport pracowników.

Największymi problemami związanymi z tym produktem ubezpieczeniowym są[160]:

- problemy z samym zdefiniowaniem sprzętu elektronicznego. Pojęcie to jest bowiem bardzo szerokie i obejmuje zarówno wszelkie produkty elektroniczne,

[157] Wiele z wyłączeń traci zupełnie sens przy dzisiejszym stanie technologicznym. Należy zwrócić uwagę że w obecnych produktach, o których będzie mowa w dalszej części pracy występują wciąż „przestarzałe” technologie natomiast nie występują obecnie używane lub „nowinki” technologiczne.
[158] Monkiewicz J. (red.), ibidem, str. 221. [63]
[159] Sztachelska, J. Ubezpieczenia sprzętu elektronicznego. Coraz bogatsza oferta, Gazeta Ubezpieczeniowa, 2004, 14 grudnia [115]
[160] Monkiewicz J. (red.), ibidem, str. 222 [63]

produkty zawierające komponenty elektroniczne oraz wszelkie precyzyjne urządzenie inżynieryjne,

- wielka koncentracja wartości ubezpieczonych przedmiotów,
- łatwość uszkodzenia a także kradzieży i zniszczenia, dotyczy to zwłaszcza sprzętu przenośnego,
- trudność we właściwym zdefiniowaniu zagrożeń.

Punkt drugi i trzeci łączą się ze sobą. Wielka koncentracja wartości ubezpieczonych przedmiotów, jak też sprzęt przenośny, są już obecnie przeszkodą w zawarciu takiego ubezpieczenia, albowiem przedsiębiorstwa, dla których systemy informatyczne (nazywane w przypadku tego produktu ubezpieczeniowego sprzętem elektronicznym) są istotnym narzędziem służącym prowadzeniu działalności gospodarczej, same zazwyczaj dbają o fizyczne zabezpieczenie posiadanego majątku. Ponadto zakłady ubezpieczeniowe w przypadku ubezpieczeń majątkowych wymuszają na podmiotach ubiegających się o udzielenie ochrony ubezpieczeniowej zastosowanie sprawdzonych i skutecznych zabezpieczeń, a niektóre z nich wręcz bardzo szczegółowo określają rodzaje i typy zabezpieczeń wymaganych do poszczególnych składników majątku.

Natomiast niewątpliwie problemem dla zakładów ubezpieczeń jest zdefiniowanie specyficznych ryzyk ubezpieczeniowych w odniesieniu do systemów informatycznych i przetwarzania informacji.

W chwili obecnej wszystkie duże zakłady ubezpieczeniowe działające w obszarze ubezpieczeń majątkowych w Polsce mają w ofercie ten rodzaj ubezpieczenia technicznego. Należą do nich zarówno polskie towarzystwa ubezpieczeniowe jak i zagraniczne: PZU SA, Warta SA[161], Commercial Union Polska SA, STU Ergo Hestia SA, TU Compensa SA, HDI - Gerling[162], TU Allianz Polska SA, Uniqa, Cigna STU,Generali SA[163] i AIG Europe SA. Jednak choć nazywa się on identycznie, nie jest to dokładnie ten sam produkt.

Już porównanie ogólnych warunków ubezpieczenia sprzętu elektronicznego kilku towarzystw ubezpieczeniowych działających na polskim rynku i oferujących taki produkt (TU Allianz

[161] Ogólne warunki ubezpieczenie sprzętu elektronicznego – Warta SA z dn. 01. 01. 2004 r. [81]
[162] Ogólne warunki ubezpieczenie sprzętu elektronicznego – HDI-Gerling TU SA z dn. 01. 01. 2004 r. [80]
[163] Ogólne warunki ubezpieczenie sprzętu elektronicznego – Generali TU SA z dn. 01. 01. 2004 r. [79]

Polska SA, PZU SA, Commercial Union, Ergo Hestia[164], Compensa SA czy Generali SA i AIG) unaocznia, że cechą wspólną wszystkich tych dokumentów są następujące elementy:

- składka ubezpieczeniowa jest ustalana każdorazowo na podstawie indywidualnej oceny ryzyka,
- ubezpieczyciel zastrzega sobie pisemnie możliwość dodatkowej oceny tego ryzyka podczas trwania umowy w następujący sposób:

Obowiązki ubezpieczającego:

- TU Allianz Polska SA: przedstawiciele ubezpieczyciela mają prawo do lustracji i zbadania ryzyka w każdym stosownym czasie, a ubezpieczający ma obowiązek dostarczenia wszystkich danych i informacji niezbędnych do oceny ryzyka[165], a także niezwłocznego powiadomienia ubezpieczyciela o każdej zmianie w ryzyku i podjęcia na własny koszt wszelkich środków ostrożności, jakich będą wymagać okoliczności;
- Commercial Union Polska SA: Ubezpieczający jest zobowiązany do niezwłocznego powiadomienia ubezpieczyciela o wszelkich zmianach okoliczności mogących mieć wpływ na ocenę dokonaną przez ubezpieczyciela przyjętego do ubezpieczenia ryzyka i na zwiększenie prawdopodobieństwa wystąpienia szkody; towarzystwo zastrzega sobie prawo do inspekcji miejsca i przedmiotu ubezpieczenia w celu oceny ryzyka powstania szkód oraz sformułowania ewentualnych rekomendacji i zaleceń dotyczących kontroli tego ryzyka[166].

Warunki te wynikają również bezpośrednio z reguły najwyższego zaufania (łac. *uberrimae fides*)[167], której cechą charakterystyczną jest szczególne zaufanie łączące strony umowy, a z niej wynika wprost obowiązek ujawnienia przez ubezpieczającego wszelkich faktów i

[164] Ogólne warunki ubezpieczenia sprzętu elektronicznego – Ergo Hestia SA z dn. 01. 01. 2004 r. [77]
[165] Ogólne warunki ubezpieczenia sprzętu elektronicznego, TU Allianz Polska SA, art. 6, Obowiązki Ubezpieczającego, pkt. 3 i 4 [73]
[166] Ogólne warunki ubezpieczenia sprzętu elektronicznego, Commercial Union Polska SA, §29. Obowiązki Ubezpieczającego, pkt. 1. 5) i 2. [72]
[167] Kodeks cywilny, Księga III, Zobowiązania, Art. 815. §1 i 2

informacji mogących mieć znaczenie dla ubezpieczyciela, by był on przekonany, że okoliczności i informacje podane w dokumentach ubezpieczeniowych są rzetelne[168].

O ile w powyższych punktach wszystkie zakłady ubezpieczeń są zgodne, to już wyłączenia odpowiedzialności za szkody wynikłe z nieprawidłowego przetwarzania danych są bardzo różnie definiowane i mogą być wymieniane zarówno w sekcji I (szkody materialne) jak i sekcji II (ubezpieczenie wymiennych nośników danych), a więc wśród ubezpieczycieli nie ma zgodności jak takie ryzyko traktować.

Na przykład Ergo Hestia wymienia je w sekcji I „Ubezpieczenie sprzętu elektronicznego od szkód materialnych", nie odpowiada za: §23, pkt.14) *szkody wynikłe z niedziałania, nieprawidłowego działania lub nieprawidłowego zastosowania sprzętu, oprogramowania lub nośników informacji używanych w dowolnym elektronicznym urządzeniu, systemie (np. komputerze, sterowniku mikroprocesorowym, układzie scalonym) lub sieci, a także niedostępności, utraty lub zniekształcenia informacji przechowywanej lub przetwarzanej przez sprzęt, oprogramowanie lub nośnik informacji, używane w dowolnym elektronicznym urządzeniu, systemie lub sieci, chyba że w następstwie wystąpiło inne zdarzenie niewyłączone z zakresu ubezpieczenia; wówczas Ubezpieczyciel ponosi odpowiedzialność wyłącznie za skutki takiego zdarzenia.*

Również Uniqa[169] wymienia tego rodzaju wyłączenia w sekcji I, §4. *Ochroną ubezpieczeniową nie są objęte szkody: pkt. 7) będące konsekwencją działania wirusów komputerowych, pkt. 8) spowodowane atakami hakerów komputerowych.*

Allianz Polska[170] natomiast w sekcji II „Ubezpieczenie danych, oprogramowania" o.w.u., w Art. 17 w pkt. 2: Wyłączenia odpowiedzialności szczególne wymienia w pkt. 15), 16) i 17) wyłączenia: *w postaci kosztów sprawdzania, weryfikacji lub modyfikacji oprogramowania lub danych; szkód w programach użytkowanych w sposób bezprawny, z naruszeniem praw autorskich lub bez upoważnienia ze strony ich właścicieli lub autorów; w postaci jakichkolwiek kosztów odtworzenia utraconych lub zdeformowanych danych w razie braku, zniszczenia lub utracenia danych bazowych* (ang. Database). Jak widać te wyłączenia realizowane przez Zakład Ubezpieczeń jednoznacznie wykluczają ubezpieczenie aktu

[168] Fuchs D., Wybrane cechy umowy ubezpieczenia majątkowego, Prawo Asekuracyjne 1999 nr 4 [40]
[169] Ogólne warunki ubezpieczenie sprzętu elektronicznego – Uniqa z dn. 13. 10. 2004 r. [78]
[170] Ogólne warunki ubezpieczenie sprzętu elektronicznego – Allianz z dn. 19. 12. 2003 r. [73]

nadużycia, jakim jest włamanie do systemu informatycznego lub utrata integralności danych powstała na skutek błędnego działania systemu informatycznego. Takie wyłączenie czyni ten produkt bezużytecznym z perspektywy problemu bezpieczeństwa systemów informatycznych.

Podobnie PZU SA[171] wymienia je w §10: Wyłączenia odpowiedzialności, opisując jednocześnie jako: *szkody spowodowane błędnym oprogramowaniem, działaniem „wirusów komputerowych" lub spowodowane działaniem pola magnetycznego.*

Compensa SA[172] traktuje te przypadki jako wyłączenia szczególne: §19, pkt. 2. 3) oraz pkt. 3. 2): „*Compensa nie ponosi odpowiedzialności za szkody spowodowane zdarzeniami (...) spowodowanymi przez wirus komputerowy, utratę danych wskutek działania pola elektromagnetycznego lub nieumyślne bądź przypadkowe ich usuniecie*" oraz zakres ochrony ubezpieczeniowej nie obejmuje także poniesionych kosztów „*związanych z utratą bądź niewłaściwym działaniem zabezpieczeń ubezpieczonych danych (tzw. kluczy sprzętowych*). To z kolei wyłączenie pokazuje jak nieaktualny jest produkt ubezpieczeniowy w tym wypadku oraz jak szczegółowe i „przestarzałe" mechanizmy bezpieczeństwa obejmuje w swym zakresie.

AIG[173] w § 20. Wyłączenia, pkt. 2: Zdarzenia wyłączone z zakresu Ubezpieczenia. „*Ubezpieczyciel nie ponosi odpowiedzialności za straty lub szkody na nośnikach danych w tym zniekształcenie, przekręcenie, sfałszowanie, skasowanie bądź utratę danych spowodowane bezpośrednio lub pośrednio przez, lub wynikłe z następujących zdarzeń: f) wszelkiego rodzaju straty następcze jak utrata przychodu/zysku, użyteczność"* i; pkt. 3. Koszty wyłączone z zakresu ubezpieczenia. „*Ubezpieczyciel nie wypłaci odszkodowania za: b) dodatkowe koszty poniesione (np. koszty zakupu nowych licencji) ze względu na zabezpieczenie ubezpieczonych danych lub programów przed kopiowaniem i/lub programami kontroli dostępu lub podobnymi procedurami*".

Commercial Union Polska[174] natomiast umieszcza tego rodzaju wyłączenia w rozdziale „Klauzule i postanowienia generalne dla rozdziałów I, II i III", §25. Wyłączenia ogólne, pkt. 7) *uszkodzenia, zmiany lub zniszczenia, a także ograniczenia zakresu funkcjonalności,*

[171] Ogólne warunki ubezpieczenie sprzętu elektronicznego – PZU z dn. 07. 10. 2003 r. [74]
[172] Ogólne warunki ubezpieczenie sprzętu elektronicznego - TU Compensa SA z dn. 02.11. 2004 r. [75]
[173] Ogólne warunki ubezpieczenie sprzętu elektronicznego – AIG z dn. 20. 11. 2006 r. [76]
[174] Ogólne warunki ubezpieczenie sprzętu elektronicznego – Commercial Union z dn. 08. 12. 2003 r. [72]

dostępności lub działania jakiegokolwiek systemu komputerowego, sprzętu komputerowego (hardware), oprogramowania (software), programów, danych, nośników danych lub mediów służących do przechowywania danych informatycznych, mikroprocesorów, układów scalonych lub podobnych urządzeń lub komponentów stanowiących część sprzętu komputerowego, jeśli zdarzenia opisane powyżej nastąpiły jako rezultat umyślnego (tj. z zamiarem wyrządzenia szkody) lub też przypadkowego przesłania lub przekazania (elektronicznie lub w inny sposób) programu zawierającego jakiekolwiek instrukcje lub kody logiczne działające w niszczący sposób, w szczególności obejmujące wirusy, „robaki" komputerowe lub też programy określane mianem „koni trojańskich", „bomb logicznych" lub analogicznie działające; jeżeli tego rodzaju programy mogą być zidentyfikowane jako przyczyna zaistniałej szkody, ich działanie będzie traktowane jako zdarzenie wyłączone z zakresu ubezpieczenia.

Dodatkowo niektóre towarzystwa (PZU, Ergo Hestia, CU) oferują jeszcze dodatkowe klauzule indywidualne, zawierające albo ubezpieczenie sprzętu przenośnego; ubezpieczenie sprzętu zainstalowanego na stałe w pojazdach samochodowych; statkach powietrznych, lub jednostkach pływających; telefonów komórkowych, albo rozszerzają obszar terytorialny lub zawierają wyłączenia niektórych ryzyk, ale i te, nie opisują całego spektrum możliwych ryzyk, które mogą być przedmiotem dodatkowych umów.

Nie jest celem tego rozdziału szczegółowe porównanie wszystkich produktów oferowanych na polskim rynku ubezpieczeniowym pod jedną nazwą „Ubezpieczenie sprzętu elektronicznego", lecz raczej wykazanie jak wiele trudności mają zakłady ubezpieczeniowe nie tylko ze zdefiniowaniem ryzyk związanych z szeroko rozumianym sprzętem elektronicznym, którego częścią są systemy informatyczne, jak też precyzyjnym opisaniem samego przedmiotu ubezpieczenia oraz wyłączeń odpowiedzialności w poszczególnych sekcjach. W definiowaniu wyłączeń odpowiedzialności panuje największy chaos terminologiczny, związany nie tylko z wyłączeniami nieistniejących już narzędzi informatycznych, ale również z nieprecyzyjnym tłumaczeniem niektórych terminów z języka angielskiego. Wprawdzie niektóre towarzystwa ubezpieczeniowe poprzedzają ogólne warunki ubezpieczeń definicjami, ale większość tych definicji dotyczy elementów umowy ubezpieczeniowej, lub zdarzeń „wyjątkowo często" występujących na obszarze Polski typu: tornado, tajfun czy tsunami. Natomiast systemów komputerowych dotyczą tylko trzy

definicje, powtórzone za „Podręcznym słownikiem terminów informatycznych[175]". Są to definicje: danych, nośników danych i jednostki centralnej komputera. I choć pojęcie to pojawia się prawie we wszystkich omawianych ogólnych warunkach ubezpieczeń, w częściach dotyczących wyłączeń jedynie Compensa SA do tego zestawu dołączyła definicję wirusa komputerowego. Dodatkowo zastanawiający jest fakt, że prawie wszystkie ogólne warunki ubezpieczeń zostały zatwierdzone przed trzema lub czterema laty – koniec 2003 lub 2004 rok (wyjątkiem jest tylko AIG, którego ogólne warunki ubezpieczeń są datowane na listopad 2006 roku).

Biorąc pod uwagę ogromny postęp technologiczny w tej dziedzinie oraz duże zapotrzebowanie na ten produkt, dziwne wydaje się, że zakłady ubezpieczeniowe zdają się nie zauważać potrzeby unowocześnienia i rozwijania go, choć w zgodnej opinii większości badaczy ma on ogromny potencjał rynkowy i bardzo dużą dynamikę rozwoju. Sektor produktów i usług informatycznych jest obecnie najszybciej rozwijającym się sektorem działalności biznesowej.

3.6 Perspektywy dalszego rozwoju produktów ubezpieczeniowych związanych z systemami informatycznymi

Choć ubezpieczenie sprzętu komputerowego ma w nazwie rozszerzenie „od wszelkich ryzyk" jest to tak naprawdę produkt ułomny, ponieważ nie obejmuje ryzyk związanych z bezpieczeństwem systemu informatycznego, w szczególności z nieprawidłowym przetwarzaniem informacji, czyli od ryzyk utraty: poufności, dostępności i integralności[176].

W dobie globalizacji, kiedy większość informacji jest przesyłanych drogą elektroniczną za pośrednictwem rozbudowanych sieci komputerowych, zapewnienie bezpieczeństwa tym informacjom staje się sprawą nadrzędną.

Odpowiedzią na zapotrzebowanie na tego typu ubezpieczenie są produkty o nazwie **Ubezpieczenie ryzyka sieciowego – NRI** (ang. Network Risk Insurance[177] [178]) oraz **Program**

[175] Podręczny słownik terminów informatycznych,
[176] Mowbray, A.H., Blanchard, R.H. 1961. Insurance. It's theory and practice in the United States. New York [65]
[177] Network Risk Insurance Program Application – ACE USA, 05. 2005 r. [69]
[178] Network Risk Insurance Program Policy – ACE USA, 02. 2006 r. [70]

ubezpieczeniowy technologii cyfrowej i odpowiedzialności zawodowej – DigiTech (ang. Digital Technology & Professional Liability Insurance Program[179] [180]**)**, oferowane przez towarzystwa ubezpieczeniowe w USA, ale niestety niedostępne jeszcze w Polsce.

NRI i DigiTech są produktami adresowanymi do organizacji gospodarczych, dla których elektroniczne procesy przetwarzania informacji stanowią ważną część działalności biznesowej i których bezpieczeństwo informacyjne może w istotny sposób wpływać na wynik finansowy.

NRI jest produktem składającym się z kilku części, w przypadku AIG zawiera w sobie część DigiTech, natomiast ACE oferuje to samo pokrycie jako dwa odrębne produkty komplementarne względem siebie.

1. Ubezpieczenie działalności podmiotu (ang. First Party). Część produktu, której beneficjentem jest sam ubezpieczający. Zapewnia ona pokrycie strat wynikających z przerw w działalności biznesowej związanych z niedostępnością lub degradacją (zniszczeniem) sieci komputerowej organizacji, włączając w to przychód, ekstra koszty oraz nieplanowaną, nadzwyczajną przerwę w działalności biznesowej. Wartość zasobów cyfrowych organizacji może być ubezpieczona wraz z danymi klientów, danymi wrażliwymi itp. Ponadto dzięki odpowiednim klauzulom dodatkowym, mogą być również objęte ubezpieczeniem straty związane z cyberwymuszeniami, ceberterroryzmem, kosztami dochodzeniowymi i komunikacją kryzysową. W przypadku AIG jest to jedna z części produktu, a w przypadku ACE jest to właściwy produkt NRI.
2. Ubezpieczenie odpowiedzialności cywilnej podmiotu wobec osób trzecich (ang. Third Party). Ta część polisy (AIG) zapewnia pokrycie strat na wypadek kosztów obrony prawnej i jest związana ze szkodami poniesionymi przez inne osoby, w wyniku błędów w sieci komputerowej ubezpieczonego, a także w systemach i aplikacjach biznesowych. Włącza się w nią odpowiedzialność za skutki: działania hakerów, wirusów komputerowych, robaków, nieautoryzowanego dostępu, utratę poufności i kradzież tożsamości. Ta część polisy może także pokrywać koszty związane ze stratami, jakich doznali klienci związani ze zniesławieniem lub oszczerstwem. W przypadku ACE jest to DigiTech**.**

[179] Digital Technology & Professional Liability Insurance Program, Application, ACE USA, 06. 2006 r. [31]
[180] Digital Technology & Professional Liability Insurance Policy, Declarations, ACE USA, 02. 2007 r. [32]

Ponieważ jednak niezależnie od tego, czy są to dwa odrębne produkty, czy jeden obejmujący kilka sekcji, sposoby oceny ryzyka w obu przypadkach są bardzo podobne i dlatego zostaną omówione wspólnie.

3.7 Sposób oceny ryzyka dla Ubezpieczenia ryzyka sieciowego – NRI oraz Programu ubezpieczenia technologii cyfrowej i odpowiedzialności zawodowej – DigiTech przez akceptujących ryzyko

W przypadku NRI i DigiTech, inaczej niż w przypadku innych produktów ubezpieczeniowych, nie ma ustalonego standardu oceny ryzyka, aczkolwiek są pewne stale rosnące wymagania dotyczące dostarczania coraz dokładniejszych informacji o organizacji ubiegającej się o objęcie ochroną ubezpieczeniową. Pracownicy akceptujący ryzyko domagają się dostarczania danych z różnych departamentów, poczynając od osób zarządzających ryzykiem w organizacji, po departament prawny, finansowy, technologiczno-produkcyjny, marketingowy i personalny. Jeśli „Dokumentacja oceny ryzyka" jest kompletna i dobrze napisana, to jej ocena dokonana przez pracownika akceptującego ryzyko może skutkować niższą składką, wyższymi limitami ochrony lub niższym udziałem własnym.

3.7.1 Elementy podlegające szczegółowej ocenie działu akceptacji ryzyka

1. Stabilność finansowa organizacji i brak strat, w tym szczególnie przebiegi szkodowe z ostatnich 5 lat i historie roszczeń. Istotnym elementem oceny jest rodzaj prowadzonej działalności oraz wpływ systemów informatycznych na generowanie przychodów organizacji wyrażony procentowo.
2. Praktyki sprzedażowe i procedury kontraktowe, w tym szczególnie procedury weryfikacji kontrahentów, klientów oraz ograniczenie odpowiedzialności organizacji w ramach gwarancji.
3. Procedury rozwiązywania sporów. Istotniejsze w tym przypadku jest czy można uniknąć procesu, niż to czy organizacja wygra spór.
4. Formalna odpowiedzialność kadry zarządzającej i standardy postępowania wewnątrz firmy, w tym szczególnie odpowiedzialność za utrzymanie bezpiecznego środowiska informatycznego. To jest najobszerniejsza i najbardziej szczegółowa część kwestionariusza aplikacyjnego. W organizacji musi być wyznaczona osoba, umocowana wysoko w hierarchii, która jest odpowiedzialna za bezpieczeństwo. Stosunek zarządu organizacji do spraw bezpieczeństwa też podlega ocenie, stąd ma znaczenie stanowisko osoby, której są przypisane sprawy związane z bezpieczeństwem. Może nią być CFO (ang. Chief Financial Officer),

CSO (ang. Chief Security Officer) lub CIO (ang. Chief Information Officer), lub w przypadku mniejszych organizacji administrator systemów. Musi ona jednak posiadać budżet umożliwiający realizację celów polityki bezpieczeństwa. Akceptujący ryzyko oceniają również systemy informatyczne pod kątem istotności dla prowadzonego przez organizację biznesu oraz adekwatności zastosowanych zabezpieczeń w kontekście istotności systemów. Ostateczna ocena i weryfikacja stanu bezpieczeństwa powinna być dokonywana co najmniej dwa razy w roku. Kluczowymi dokumentami podlegającymi ocenie jest polityka bezpieczeństwa i wdrożone procedury.

5. Fizyczne środki ochrony sieci. Organizacja powinna osiągnąć bezpieczeństwo fizyczne przez karty dostępu dla pracowników, TV przemysłową oraz autoryzowany dostęp do serwerowni, a pracownicy powinni wiedzieć, z kim mają się kontaktować w przypadku zagrożenia lub awarii. Ten element jest równie istotny jak środki logiczne i oba te elementy powinny być stosowane łącznie i spójnie.
6. Środki ochrony logicznej, w szczególności diagramy architektury sieciowej, model informacyjny, informacja o dostawcy programu antywirusowego, kopie „Polityki bezpieczeństwa", procedur operacyjnych i administracyjnych.
7. Kontrola zarządzania zmianą, w szczególności procedury unieważniania dostępu byłych pracowników, współpracowników i dostawców do zasobów organizacji.
8. Kontrola zawartości Internetu, zwłaszcza zasady i procedury umieszczania treści na stronach internetowych organizacji.
9. Przywracanie systemu po awarii (ang. Disaster Recovery) i Planowanie Ciągłości Działania BCP (ang. Business Continuity Planning). Pytania dotyczą w szczególności planów awaryjnych, testowania tych planów, zapisanych procedur itd. W zależności od zadeklarowanej przez ubezpieczonego dopuszczalnej przerwy w prowadzeniu działalności biznesowej – niedostępności systemów (8, 12 lub 24 godziny) – różna jest podstawa do obliczenia wysokości tej części składki.

Tak niedoskonały sposób oceny ryzyka skutkuje tym, że to samo ryzyko wycenione przez różne zakłady ubezpieczeń może się bardzo różnić, co oczywiście zawsze skutkuje wysokością składki ubezpieczeniowej i udziału własnego[181].

3.7.2 Opis produktu – typy pokrycia

Produkty NRI i DigiTech składają się z trzech głównych sekcji:

1. Błędy i Niedopatrzenia (ang. Error and Omissions). Są to roszczenia wynikające z zaniedbania lub błędów w świadczeniu usług przez ubezpieczonego i obejmują ochroną roszczenia za straty finansowe.
2. Technologiczne Błędy i Niedopatrzenia (ang. Technology Error and Omissions). W tej sekcji ubezpieczyciel oferuje pokrycie roszczeń wynikających z błędów w produkcie technologicznym. Sekcja ta może być uzupełniona o pokrycie roszczeń wynikających z naruszenia własności intelektualnej, zaniedbaniem w świadczeniu usług internetowych i odpowiedzialności za środki masowego przekazu.
3. Ryzyko Sieciowe (ang. Network Risk). Jest to pokrycie strat związanych z przerwami w prowadzeniu działalności biznesowej i dodatkowymi kosztami wynikającymi z pewnych niefizycznych zagrożeń, włączając w to nadzwyczajne przerwy w prowadzeniu działalności (ang. Business Interruption).

    - Polityka przestępstw komputerowych (ang. Computer Crime Policy) – obejmuje bezpośrednie szkody samego ubezpieczonego.
    - Strona pierwsza (ang. First Party) – ta część obejmuje szkody poniesione przez samego ubezpieczonego w związku z nieprawidłowym działaniem własnej sieci.
    - Kradzież tożsamości/prywatności pokrywa bezpośrednie szkody samego ubezpieczonego wyłączając z tego szkody, które są rezultatem działań pracowników, a także pośrednie szkody klientów.
    - Strona trzecia (ang. Third Party) jako część NRI dla AIG lub DigiTech dla ACE. Podstawą roszczeń w przypadku tego typu szkód są pozwy wniesione przez osoby trzecie w związku z obniżeniem jakości wykonywanych usług,

[181] Reid, R. C., Floyd, S. A. 2001. Extending the risk analysis model to include market - insurance, Computers & Security 20, 4, 331 - 339. Oxford: Elsevier [97]

opóźnieniami, naruszeniem bezpieczeństwa danych, naruszeniem lub przerwami w transmisji danych lub usług głosowych, niekorzystnymi skutkami działania wirusów komputerowych, koni trojańskich, robaków oraz naruszenia prywatności w relacjach publicznych. Ta część pokrywa szkody, bez względu na rodzaj i przyczynę zaniedbania, w odróżnieniu od sekcji Błędy i Niedopatrzenia, które pokrywa tylko szkody wynikające z samego zaniedbania.

Maksymalny limit ochrony w USA w przypadku DigiTech wynosi 20 mln. USD, a minimalna składka ubezpieczeniowa to 15 000 USD (dane ACE USA), natomiast dla NRI maksymalny limit ochrony wynosi 15 mln USD, a minimalna składka ubezpieczeniowa to 5 000 USD. To oznacza, że wartość pokrycia dla obu tych produktów łącznie wynosi 35 mln USD. Ponieważ jednak w przypadku tych produktów franszyza jest bardzo wysoka, bo wynosi 30%, można wnioskować, że z jednej strony, zakłady ubezpieczeń mają świadomość niedoskonałości wyceny tego ryzyka, stąd zabezpieczają się wysokim udziałem własnym, a z drugiej strony działa tu silnie mechanizm prewencyjnej funkcji ubezpieczeń. Organizacja mając w przypadku zaistnienia szkody ubezpieczeniowej perspektywę poniesienia tak dużej części odpowiedzialności finansowej sama będzie zainteresowana kontrolowaniem stanu bezpieczeństwa własnych zasobów informatycznych.

3.8 Podsumowanie analiz dotyczących oceny ryzyka związanego z bezpieczeństwem systemów informatycznych przez przedsiębiorstwa oraz przez zakłady ubezpieczeń

Jak widać z przedstawionych w rozdziałach 3.4. i 3.5. opisów produktów ubezpieczeniowych dedykowanych nowym technologiom informatycznym oferowanych na rynku polskim i w USA, istnieje zasadnicza różnica zarówno pomiędzy ofertami zakładów ubezpieczeń, jak i stopniem zaawansowania produktów oferowanych na tych rynkach. Różnica ta wynika jednak nie tylko z podaży i wielkości rynku, który w USA jest wielokrotnie większy niż w którymkolwiek z krajów europejskich, lecz także z uregulowań prawnych, wpływających na popyt na nowe produkty ubezpieczeniowe..

Programy ubezpieczeniowe takie jak DigiTech i NRI zostały w dużym stopniu „wymuszone" przez uchwaloną w 2002 roku Ustawę Sarbanes–Oxley. Wprawdzie bezpośrednim powodem wprowadzenia Ustawy Sarbanes–Oxley (Sarbanes-Oxley Act of 2002 – „SOX") były skandale finansowe na wielką skalę i związany z nimi spadek zaufania inwestorów do rynków finansowych oraz kluczowych podmiotów na nich operujących tj. doradców inwestycyjnych, audytorów, notowanych spółek (a dokładniej ich zarządów), ale jej wprowadzenie skutkowało również zaostrzeniem wymagań dotyczących bezpieczeństwa informatycznego. Zgodnie z paragrafem 404 SOX, organizacje gospodarcze muszą każdego roku dokonywać oceny efektywności swoich systemów kontroli wewnętrznej, które wpływają na raportowanie finansowe. Natomiast zgodnie z paragrafem 302, organizacje te co kwartał muszą potwierdzać, że opracowały, udokumentowały i przetestowały systemy kontroli wewnętrznej. Ustawa ta narzuca w ten sposób kontrolę tych procesów, które mają bezpośredni wpływ na raportowanie, a do nich należą również procesy przetwarzania danych finansowych w systemach informatycznych. W większości firm wiarygodność raportów finansowych zależy wprost od kompletności, wiarygodności i aktualności danych przetwarzanych przez systemy informatyczne. Bezpośrednie odniesienie do systemów informatycznych pojawiło się w dokumencie *„Standard audytu nr 2"*, wydanym przez Komisję Nadzoru nad Księgowością Spółek Publicznych (PCAOB), organizację powołaną z mocy ustawy SOX, w celu wprowadzenia jej w życie i ustanowienia odpowiednich przepisów wykonawczych: standardów księgowych i audytorskich. Standard nr 2 jest dziś najważniejszym punktem odniesienia dla dostosowujących się do nowego prawa spółek.

Takie podejście do bezpieczeństwa systemów informatycznych zaowocowało w USA powstaniem popytu na nowe produkty ubezpieczeniowe, które uzupełniają spektrum możliwych do zastosowania strategii postępowania z ryzykiem związanym z bezpieczeństwem systemów informatycznych. Jednak z uwagi na bardzo krótki okres istnienia samych systemów informatycznych w dzisiejszym kształcie, a tym samym brak danych historycznych i statystycznych, produkty te nie mogły bazować na powszechnie przyjętych metodach aktuarialnych, stąd szacowanie tych ryzyk przez towarzystwa ubezpieczeniowe jest oparte na przesłankach niezwiązanych bezpośrednio z bezpieczeństwem systemów informatycznych.

W przypadku bezpieczeństwa systemów informatycznych, o którym mowa w rozdziale 2, brak jest wiarygodnych i kompleksowych danych, a te, które są dostępne (jak w przypadku danych CERT), nie są kompletne a wręcz wyrywkowe. Metody oceny ryzyka związanego z bezpieczeństwem systemów informatycznych przedstawione w rozdziale 2.9, zarówno ilościowe jak i jakościowe, były historycznie konstruowane dla organizacji rządowych i militarnych, a z biegiem czasu ewoluowały i dostosowano je dla organizacji gospodarczych. Nie były one jednak tworzone dla potrzeb zakładów ubezpieczeń. Ich zadaniem jest ocena ryzyka związanego z bezpieczeństwem systemów informatycznych w celu identyfikacji obszarów zagrożonych i doboru odpowiednich zabezpieczeń, a nie wyznaczenie wartości ryzyka związanego z bezpieczeństwem systemów informatycznych na określony moment. Wszystkie opisane w rozdziale 2.9 metody oceny ryzyka związanego z bezpieczeństwem systemów informatycznych mają następujące elementy dyskwalifikujące je z punktu widzenia Zakładu Ubezpieczeń[182]:

1. Metody te były tworzone dla organizacji w celu doboru odpowiednich mechanizmów zabezpieczeń. Wyznaczona wartość ryzyka związanego z bezpieczeństwem systemów informatycznych wskazuje, w które obszary należy inwestować. Nie można przy użyciu tych metod ustalić poziomu ryzyka związanego z bezpieczeństwem systemów informatycznych po zastosowaniu określonych zabezpieczeń.
2. Metody te bazują na prawdopodobieństwie wystąpienia określonych zagrożeń oraz wycenie wartości materialnej poszczególnych komponentów systemów

[182] Przedstawione cechy mają zastosowanie do wszystkich prezentowanych w pracy metod oceny ryzyka związanego z bezpieczeństwem systemów informatycznych.

informatycznych. Wycena ta służy określeniu potrzeb inwestycyjnych organizacji, ale nie ma zastosowania dla potrzeb decyzyjnych zakładu ubezpieczeń.

3. Wyniki oceny ryzyka związanego z bezpieczeństwem systemów informatycznych realizowane za pomocą tych metod nie są obiektywne i w zależności od wiedzy i doświadczenia osoby dokonującej oceny mogą się zasadniczo różnić. Tym trudniejsze staje się porównanie wyników kilku lub kilkunastu przedsiębiorstw. Wynika to z faktu bardzo dużego subiektywizmu w nadawaniu poszczególnych wartości zmiennym używanym w metodach oceny.
4. Metody te są bardzo skomplikowane i zazwyczaj wielofazowe, przez co w praktyce nie są realizowane w całości. Poszczególne fazy są realizowane wybiórczo lub pewne fragmenty metod są pomijane.
5. Celem tych metod jest wskazanie sposobu realizacji określonych działań (procesu), a nie osiągnięcie określonego wyniku (wartość ryzyka).

Towarzystwa ubezpieczeniowe muszą zatem znaleźć porównywalną metodę oceny ryzyka ubezpieczeniowego po to, by rozwijać dalej ten rodzaj produktów zgodnie z postępem w tej dziedzinie oraz by było możliwe skalkulowanie minimalnej składki w takiej wysokości, jaka pozwoli na korzystanie z tych produktów również mniejszym firmom. Obecna minimalna wysokość składki jest bowiem dla wielu z nich „zaporowa" a wysoka franszyza może dodatkowo zniechęcać te organizacje do korzystania z tego typu ubezpieczeń. Z drugiej jednak strony zachowawczość zakładów ubezpieczeń i ograniczenie maksymalnej kwoty pokrycia do ok. 35 mln USD zawęża liczbę zainteresowanych nimi potencjalnych klientów. Dla porównania projekt wdrożenia średniej wielkości systemu informatycznego w średniej wielkości przedsiębiorstwie przewyższa tę kwotę. Największe wdrożenia w Polsce sięgają kwot 500 do 800 mln USD.

Ten rodzaj produktów ubezpieczeniowych będzie z pewnością już wkrótce oferowany również w Europie. Wbrew pozorom Sarbanes-Oxley Act (SOX) dotyczy także bardzo wielu podmiotów działających na europejskim rynku, w tym także w Polsce. Podmioty te należą do dwóch grup. Pierwsza z nich, to spółki zależne podmiotów amerykańskich notowanych na giełdach amerykańskich i kluczowe są tutaj powiązania właścicielskie. Druga grupa, to podmioty zarejestrowane i działające poza Stanami Zjednoczonymi, ale notowane na giełdach amerykańskich. Warto zauważyć, że w chwili obecnej inne kraje poza USA wprowadziły lub wprowadzają odpowiednik SOX, dotyczy to np. Japonii czy Francji. Już teraz polisy NRI oraz DigiTech stają się w Ameryce coraz częściej wymaganiem kontraktowym, wpływającym na

wiarygodność partnera, a bywają również silnym atutem marketingowym i ta tendencja będzie się zapewne utrwalać. Stąd wniosek, że programy ubezpieczeniowe, takie jak NRI oraz DigiTech powinny być uzupełnione o wiarygodną i obiektywną metodę oceny ryzyka systemów informatycznych, stanowiącą jedną z ważniejszych sekcji tego produktu i zintegrowaną z pozostałymi sekcjami składowymi, bo dopiero wtedy będą one posiadały wszystkie cechy prawidłowo skonstruowanego produktu ubezpieczeniowego.

4 Metoda ORBI oceny ryzyka związanego z bezpieczeństwem systemów informatycznych

4.1 Postulaty dotyczące metody oceny ryzyka związanego z bezpieczeństwem systemów informatycznych dla potrzeb ubezpieczenia

Wychodząc od krytyki metod oceny ryzyka związanego z bezpieczeństwem systemów informatycznych oraz metod oceny ryzyka ubezpieczeniowego przedstawionej w rozdziale 3.8. zostały opracowane następujące postulaty dotyczące metody oceny ryzyka związanego z bezpieczeństwem systemów informatycznych dla potrzeb zakładów ubezpieczeń, na podstawie wyników której zakład ubezpieczeń podejmie decyzję o ubezpieczalności danego ryzyka oraz warunkach takiego ubezpieczenia. Metoda taka musi charakteryzować się następującymi cechami:

1. Wyznaczać wartość ryzyka związanego z bezpieczeństwem systemów informatycznych w sposób ilościowy na dany moment oceny, przy zastosowanych przez przedsiębiorstwo zabezpieczeniach.
2. Wyznaczać obiektywną wartość ryzyka związanego z bezpieczeństwem systemów informatycznych, nie uzależniając jej od prawdopodobieństwa wystąpienia zagrożeń lub danych historycznych.
3. Wyznaczać porównywalne wartości ryzyka związanego z bezpieczeństwem systemów informatycznych w skali przedsiębiorstwa oraz przedsiębiorstw co najmniej z tej samej branży.
4. Wyznaczać wartość ryzyka związanego z bezpieczeństwem systemów informatycznych na dany moment oceny w możliwie najprostszy sposób.
5. Wyznaczać wartość ryzyka związanego z bezpieczeństwem systemów informatycznych zrozumiałą dla zakładu ubezpieczeń jak i dla przedsiębiorstwa.

4.2 Koncepcja metody ORBI

W tym punkcie przedstawiono koncepcję oryginalnej metody ORBI (**O**cena **R**yzyka **B**ezpieczeństwa systemów **I**nformatycznych), która spełnia wszystkie postulaty metody oceny ryzyka związanego z bezpieczeństwem systemów informatycznych dla potrzeb ubezpieczenia wskazane w punkcie 4.1.[183]

Metoda ORBI polega na sklasyfikowaniu systemów informatycznych przedsiębiorstwa oraz wyznaczeniu wartości ryzyka związanego z bezpieczeństwem systemów informatycznych. Składa się ona z dwóch części, gdzie część pierwsza jest przygotowaniem do oceny ryzyka, a w ramach drugiej części jest wyznaczana wartość ryzyka i odpowiednio prezentowana dla potrzeb zakładu ubezpieczeń.

Metoda ORBI została skonstruowana w taki sposób, aby jednoznacznie sklasyfikować systemy informatyczne przedsiębiorstwa z perspektywy:

1. Istotności systemów informatycznych dla przedsiębiorstwa.
2. Stopnia dostępności systemów informatycznych wymaganego przez przedsiębiorstwo.
3. Stopnia poufności danych przetwarzanych przez systemy informatyczne przedsiębiorstwa.

Metoda ORBI nie ujmuje stopnia integralności jako osobnej cechy klasyfikacji systemów informatycznych. Ten atrybut bezpieczeństwa jest wymagany w całości, ponieważ nie można określić żadnej gradacji dopuszczalnego braku integralności danych[184].

Do zebrania niezbędnych informacji w metodzie ORBI służą techniki:

1. Kwestionariuszy.
2. Wywiadów z personelem.
3. Przeglądu dokumentacji.

---

[183] Autor niniejszej rozprawy w latach 1997 – 2003 opracował metodę oceny ryzyka związanego z bezpieczeństwem systemów informatycznych, którą wykorzystywał w swojej praktyce zawodowej (*Poniewierski A., 2001, Role of Vulnerability Assessment Technology in IT Risk Management, materiały konferencyjne International Security Summit. Atlanta GA, USA* [92]). Metoda ta została dostosowana w latach 2003 – 2007 dla potrzeb oceny ryzyka ubezpieczeniowego.

[184] Poniewierski, A., Ryba M., Economical aspects of IT Security Risk Management in Industry, materiały konferencyjne IFIP I3E'2005, Poznań, 26-28 października 2005 [96]

Metoda ORBI jest tak skonstruowana, że w wyniku jej realizacji można jednoznacznie określić:

1. Wartość ryzyka w chwili dokonywania oceny, związanego z bezpieczeństwem pojedynczego systemu informatycznego przedsiębiorstwa.
2. Wartość ryzyka w chwili dokonywania oceny, związanego z bezpieczeństwem grupy systemów informatycznych przedsiębiorstwa (z uwzględnieniem ich istotności oraz przynależności do określonej klasy poufności i dostępności).
3. Wartość ryzyka w chwili dokonywania oceny, związanego z bezpieczeństwem wszystkich systemów informatycznych przedsiębiorstwa.

Wyznaczone w metodzie ORBI wartości ryzyka mają następujące cechy:

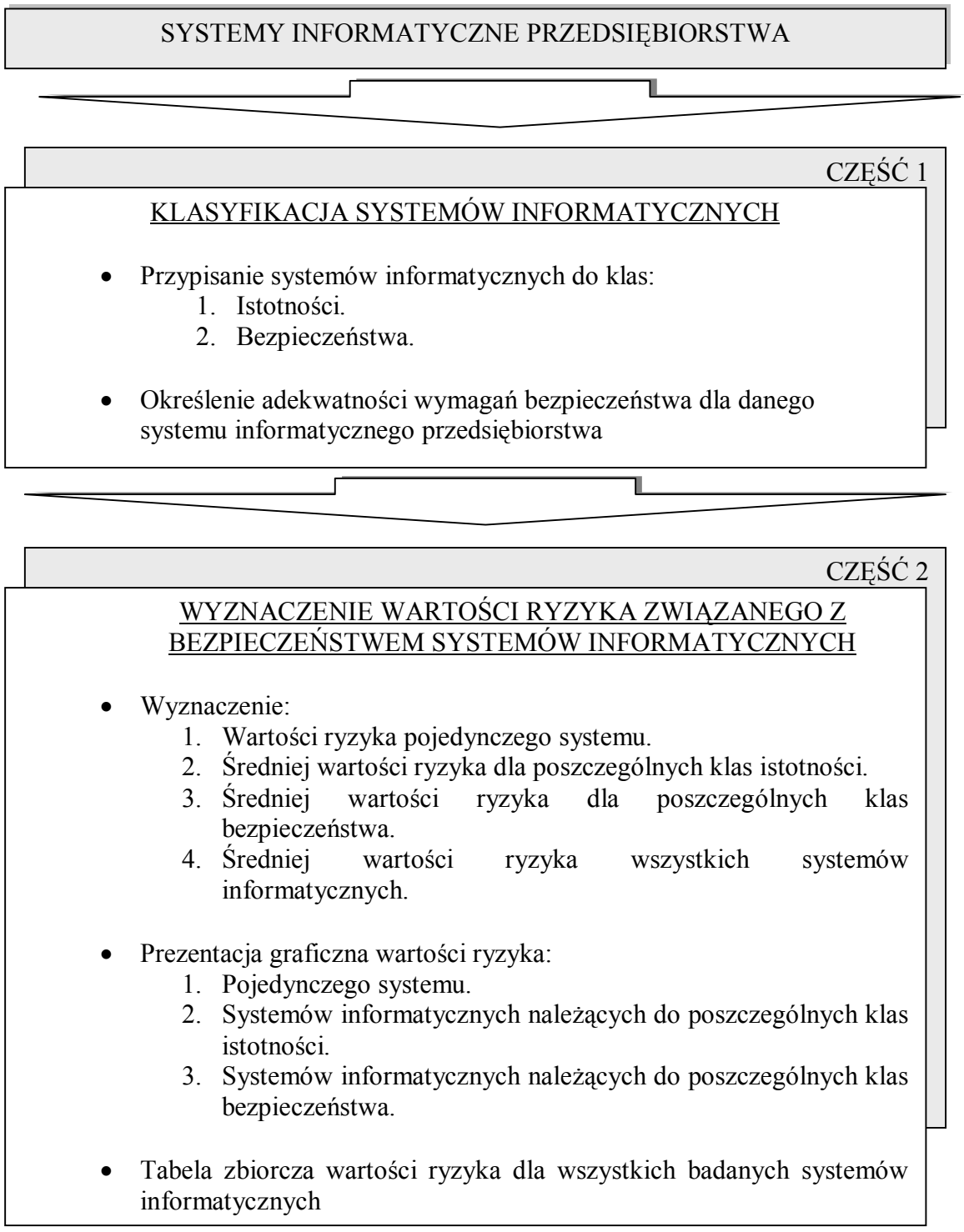
1. Wartości ryzyka związanego z bezpieczeństwem systemów informatycznych są ilościowe.
2. Wartości ryzyka związanego z bezpieczeństwem systemów informatycznych są porównywalne pomiędzy systemami informatycznymi ze względu na przyjętą stałą skalę.
3. Wartość ryzyka związanego z bezpieczeństwem systemów informatycznych nie jest związana z prawdopodobieństwem wystąpienia zagrożeń. Jest zależna od spełnienia wymagań bezpieczeństwa stałych dla metody.

Metoda ORBI prezentuje wyniki oceny pojedynczego systemu informatycznego, grup systemów i wszystkich systemów informatycznych przedsiębiorstwa łącznie, zarówno w formie graficznej, jak i tabelarycznej (zestawienie wyników oceny).

W metodzie ORBI do wyznaczenia wartości spełnienia wymagań bezpieczeństwa jest używany standard BS – 7799 -2. Standard ten jest powszechnie przyjęty, przez co ocena spełnienia wymagań bezpieczeństwa przez przedsiębiorstwo jest obiektywna i porównywalna z innymi przedsiębiorstwami.

Metoda ORBI jest łatwa w użyciu przez specjalistów z zakresu bezpieczeństwa systemów informatycznych oraz audytorów bezpieczeństwa systemów informatycznych.

Rysunek 4.2.- 7 przedstawia ogólną koncepcje metody ORBI w formie graficznej. Na rysunku są przedstawione główne części metody, główne działania i ich wyniki w ramach danej części.



Rysunek 4.2.- 7. Koncepcja metody ORBI

4.3 Opis metody ORBI

Metoda ORBI składa się z dwóch części:

1. Klasyfikacji systemów informatycznych.
2. Oceny wartości ryzyka związanego z bezpieczeństwem systemów informatycznych organizacji.

4.3.1 Część pierwsza metody ORBI – Klasyfikacja systemów informatycznych

W tej części metody ORBI podejmuje się działania, których wynikiem jest:

1. Opis systemów informatycznych organizacji w postaci macierzy klasyfikacji systemów informatycznych, uwzględniający:
    - klasy bezpieczeństwa systemów informatycznych organizacji gospodarczej dla metody ORBI,
    - klasy istotności systemów informatycznych organizacji gospodarczej dla metody ORBI.
2. Określenie za pomocą „macierzy adekwatności wymagań" wartości priorytetów i wartości adekwatności wymagań, względem danego systemu informatycznego, które zostaną wykorzystane dla tego systemu informatycznego w celu określenia stanu spełnienia wymagań bezpieczeństwa.
3. Ocena poziomu realizacji wymagań bezpieczeństwa przez systemy informatyczne organizacji gospodarczej.

Efektem realizacji pierwszej części metody jest wyznaczenie wartości α_{S_i} tj. oceny realizacji wymagań bezpieczeństwa przez system informatyczny S_i. Wyznaczenie wartości α_{S_i} dla wszystkich systemów informatycznych organizacji kończy część pierwszą metody ORBI.

4.3.1.1 Opis systemów informatycznych organizacji gospodarczej w metodzie ORBI

W dalszej części rozdziału zostaną wprowadzone definicje pojęć wykorzystywanych w metodzie ORBI[185].

Definicja 1

Zbiorem systemów informatycznych organizacji gospodarczej O nazywamy skończony i przeliczalny zbiór $S(O)=\{S_1,S_2,..,S_N\}$, gdzie:

- system informatyczny S_i, *i=1,2,...,N*, jest zbiorem celowo powiązanych ze sobą elementów sprzętu komputerowego, oprogramowania i danych;
- $N=\overline{S(O)}$ – jest liczbą systemów informatycznych organizacji gospodarczej O.

Definicja 2

Zbiór $M=\{A,B,C,D\}$ jest zbiorem klas dostępności systemów informatycznych organizacji gospodarczej, gdzie[186][187]:

A – jest klasą dostępności systemów informatycznych, dla których oczekiwana dostępność w skali roku wynosi 99,9%, a maksymalna jednorazowa niedostępność systemu nie przekracza 1 godziny;

B – jest klasą dostępności systemów informatycznych, dla których oczekiwana dostępność w skali roku wynosi 99,5%, a maksymalna jednorazowa niedostępność systemu nie przekracza 1 godziny;

C – jest klasą dostępności systemów informatycznych, dla których oczekiwana dostępność w skali roku wynosi 95%, a maksymalna jednorazowa niedostępność systemu nie przekracza 1 dnia;

---

[185] Definicje i oznaczenia wzorowano na pracy "Ryba M., 2006, Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M. Rozprawa doktorska. Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie" [104]

[186] Na podstawie opisu klas dostępności systemów informatycznych IT Security Cookbook *(Boran S., The IT Security Cookbook, Boran Consulting, październik 2000* [7])

[187] Arnell, A. 1990. Handbook of effective disaster recovery planning. New York: McGraw-Hill. [1]

D – jest klasą dostępności systemów informatycznych, dla których oczekiwana dostępność w skali roku wynosi poniżej 95%, a maksymalna jednorazowa niedostępność systemu może przekroczyć 1 dzień.

Definicja 3

Dostępność systemu informatycznego $S_i \in S(O)$ jest wyrażana przez jego przynależność do klasy dostępności $m \in M$ i oznaczana m_{S_i}. Każdy system informatyczny $S_i \in S(O)$, należy do jednej i tylko jednej klasy dostępności systemu informatycznego $m \in M$.

Definicja 4

Zbiór $F = \{1,2,3,4\}$ jest zbiorem klas poufności danych przetwarzanych przez systemy informatyczne organizacji gospodarczej, gdzie:

1 – oznacza system informatyczny przetwarzający dane o najwyższej klauzuli poufności,

2 – oznacza system informatyczny przetwarzający dane poufne stanowiące tajemnicę przedsiębiorstwa,

3 – oznacza system informatyczny przetwarzający dane wrażliwe nie stanowiące tajemnicy przedsiębiorstwa, ale nie będące danymi publicznymi,

4 – oznacza system informatyczny przetwarzający dane publicznie dostępne.

Definicja 5

Poufność danych przetwarzanych przez system informatyczny $S_i \in S(O)$ jest wyrażana przez jego przynależność do klasy poufności danych $f \in F$ i oznaczana jako f_{S_i}. Każdy system informatyczny $S_i \in S(O)$, należy do jednej i tylko jednej klasy poufności danych $f \in F$.

Definicja 6

Zbiór K będący produktem kartezjańskim $M \times F$ jest zbiorem klas bezpieczeństwa systemów informatycznych organizacji gospodarczej[188].

Definicja 7

Klasa bezpieczeństwa systemu informatycznego $S_i \in S(O)$ jest wyrażana przez jego przynależność do klasy bezpieczeństwa $k \in K$ i oznaczana jako k_{S_i}. Każdy system informatyczny $S_i \in S(O)$, należy do jednej i tylko jednej klasy bezpieczeństwa $k \in K$.

Definicja 8

Zbiór $W = \{w_1, w_2, .., w_z\}$ jest zbiorem wymagań bezpieczeństwa opracowanych na bazie BS 7799-2.

Dla każdego wymagania $w_j \in W$, *j=1,2,...,z*, jest definiowana wielkość priorytetu wymagania bezpieczeństwa względem klas bezpieczeństwa systemu informatycznego.

Definicja 9

Priorytetem wymagania $w_j \in W$ względem klasy bezpieczeństwa systemu informatycznego $k \in K$ nazywamy liczbę $p_k^j \in \{0,..,5\}$, gdzie:

- 0 – oznacza, że wymaganie jest pomijane dla danej klasy bezpieczeństwa systemu informatycznego,
- 5 – oznacza, że wymaganie jest maksymalnie istotne dla danej klasy bezpieczeństwa systemu informatycznego.

Dla każdej klasy bezpieczeństwa k istnieje przynajmniej jedno wymaganie bezpieczeństwa $w_j \in W$ takie, że $p_k^j \neq 0$.

[188] Dla czytelności zapisu element zbioru klas bezpieczeństwa systemów informatycznych oznaczane są: *A1*, *A2*, *A3*, *A4*, *B1*, *B2*, *B3*, *B4*, *C1*, *C2*, *C3*, *C4*, *D1*, *D2*, *D3* i *D4*, gdzie element zbioru klas bezpieczeństwa systemów informatycznych, dla którego klasa dostępności systemu wynosi *A*, a klasa poufności danych przetwarzanych przez system wynosi *1* oznaczany jest *A1*, itd.

Wartości od 1 do 5 są liczbowym wyrażeniem odpowiednio: minimalnego, niskiego, średniego, wysokiego i maksymalnego poziomu istotności wymagania w stosunku do danej klasy bezpieczeństwa systemu informatycznego.

Definicja 10

Zbiór $U = \{I, II, III, IV, V\}$ jest zbiorem klas istotności systemów informatycznych organizacji gospodarczej, gdzie:

I – określa system informatyczny organizacji gospodarczej służący realizacji głównych i najistotniejszych procesów biznesowych. Wartość systemu informatycznego jest porównywalna z wartością rynkową organizacji gospodarczej;

II – określa system informatyczny organizacji gospodarczej służący realizacji głównych procesów biznesowych. Wartość systemu informatycznego jest porównywalna z wartością przychodów osiąganych przez daną organizację gospodarczą w związku z realizacją działalności za pomocą tych procesów biznesowych;

III – określa system informatyczny organizacji gospodarczej służący realizacji głównych procesów biznesowych. Wartość systemu jest porównywalna z wartością komponentów sprzętowych i programowych systemu informatycznego oraz nakładów niezbędnych na wprowadzenie do niego danych;

IV – określa system informatyczny organizacji gospodarczej służący wspieraniu działalności administracyjnej organizacji. Wartość systemu informatycznego jest porównywalna z wartością usługi świadczonej na zlecenie organizacji przez stronę trzecią;

V – określa system informatyczny organizacji gospodarczej nie wspierający istotnych procesów biznesowych organizacji. Wartość systemu jest porównywalna z wartością komponentów sprzętowych i programowych systemu informatycznego według wartości księgowej.

Definicja 11

Istotność systemu informatycznego $S_i \in S(O)$ jest wyrażana przez jego przynależność do klasy istotności $u \in U$ i oznaczana u_{S_i}. Każdy system informatyczny $S_i \in S(O)$ należy do jednej i tylko jednej klasy istotności $u \in U$.

4.3.1.2 Określenie priorytetów wymagań bezpieczeństwa

Na podstawie przyjętej listy wymagań bezpieczeństwa opracowanej na bazie BS 7799-2 tworzy się zbiór wymagań bezpieczeństwa W. Na podstawie tego zbioru oraz poszczególnych klas bezpieczeństwa systemów informatycznych $k \in K$ powstaje macierz priorytetów wymagań bezpieczeństwa względem poszczególnych klas bezpieczeństwa systemów informatycznych. Macierz tę przedstawia Tabeli 4.3.- 1.

		Klasa bezpieczeństwa systemów informatycznych															
		A1	*A2*	*A3*	*A4*	*B1*	*B2*	*B3*	*B4*	*C1*	*C2*	*C3*	*C4*	*D1*	*D2*	*D3*	*D4*
Wymagania bezpieczeństwa ze zbioru W	w_1	p_k^j															
	w_2																
	.																
	.																
	.																
	w_{z-1}																
	w_z																

Tabela 4.3.- 1.Macierz priorytetów wymagań bezpieczeństwa.

Kolumny macierzy odwzorowują poszczególne klasy bezpieczeństwa systemów informatycznych. Wiersze macierzy odwzorowują poszczególne wymagania bezpieczeństwa. Wartości będące na przecięciu wierszy i kolumn macierzy tworzą priorytety wymagań bezpieczeństwa dla poszczególnych klas bezpieczeństwa systemów informatycznych.

W metodzie ORBI macierz priorytetów wymagań bezpieczeństwa jest stała.

4.3.1.3 Macierz klasyfikacji systemów informatycznych

W wyniku dokonania odpowiedniego przydziału systemów informatycznych organizacji gospodarczej do poszczególnych klas, zgodnie z przyjętymi oznaczeniami, powstaje macierz klasyfikacji systemów informatycznych metody ORBI dla danej organizacji. Macierz klasyfikacji systemów informatycznych organizacji gospodarczej jest przedstawiona w Tabeli 4.3.- 2.

	System informatyczny S_i					
	S_1	S_2	.	.	S_{N-1}	S_N
Klasa bezpieczeństwa systemu informatycznego	k_{S_1}	k_{S_2}			$k_{S_{N-1}}$	k_{S_N}
Klasa istotności systemu informatycznego	u_{S_1}	u_{S_2}			$u_{S_{N-1}}$	u_{S_N}

Tabela 4.3.- 2. Macierz klasyfikacji systemów informatycznych

Kolumny macierzy odwzorowują poszczególne systemy informatyczne organizacji gospodarczej. Wiersze macierzy odwzorowują odpowiednio klasę bezpieczeństwa systemu informatycznego oraz klasę istotności systemu informatycznego. Wartości będące na przecięciu wierszy i kolumn macierzy tworzą odpowiednie elementy zbiorów.

W metodzie ORBI macierz klasyfikacji systemów informatycznych jest każdorazowo opracowywana dla organizacji gospodarczej i jest różna dla różnych organizacji.

4.3.1.4 Adekwatność wymagań bezpieczeństwa dla systemu informatycznego S_i

Dla poszczególnych systemów informatycznych organizacji, zaklasyfikowanych do odpowiednich klas bezpieczeństwa systemów informatycznych, określone wymagania bezpieczeństwa mogą być nieadekwatne. Nieadekwatność danego wymagania jest następstwem specyficznych uwarunkowań związanych z przyjętą technologią, organizacją lub sposobem obsługi systemu informatycznego.

Definicja 12

Adekwatnością wymagania $w_j \in W$ względem systemu informatycznego S_i nazywamy liczbę $a_{S_i}^j \in \{0,1\}$, gdzie:

- 0 – oznacza, że wymaganie jest nieadekwatne do systemu S_i,
- 1 – oznacza, że wymaganie jest adekwatne do systemu S_i.

Dla każdego wymagania $w_j \in W$ względem systemu informatycznego $S_i \in S(O)$ (klasy k_{S_i}) jeżeli $p_{k_{S_i}}^j = 0$ to $a_{S_i}^j = 0$.

Dla każdego systemu informatycznego $S_i \in S(O)$ (klasy k_{S_i}) istnieje co najmniej jedno wymaganie $w_j \in W$ takie, że $p_{k_{S_i}}^j \neq 0$ i $a_{S_i}^j \neq 0$.

Na podstawie określenia adekwatności wymagań bezpieczeństwa dla każdego systemu informatycznego S_i powstaje macierz adekwatności wymagań dla systemu informatycznego S_i. Macierz tę przedstawia Tabela 4.3.- 3.

Wymaganie bezpieczeństwa	**Priorytet wymagania p_k^j (dla klasy bezpieczeństwa k_{S_i})**	**Adekwatność wymagania (dla systemu S_i)**
w_1	$p_{k_{S_i}}^1$	$a_{S_i}^1$
w_2	$p_{k_{S_i}}^2$	$a_{S_i}^2$
…	…	…
w_{z-1}	$p_{k_{S_i}}^{z-1}$	$a_{S_i}^{z-1}$
w_z	$p_{k_{S_i}}^z$	$a_{S_i}^z$

Tabela 4.3.- 3.Macierz adekwatności wymagań dla systemu informatycznego S_i

W metodzie ORBI macierz adekwatności wymagań dla systemu informatycznego S_i jest każdorazowo opracowywana dla poszczególnych systemów informatycznych organizacji gospodarczej.

4.3.1.5 Ocena realizacji wymagań bezpieczeństwa przez system informatyczny $S_i - \alpha_{S_i}$

Definicja 13

Realizacją wymagania $w_j \in W$ względem systemu informatycznego S_i klasy k_{S_i} nazywamy liczbę $\omega_{S_i}^j \in \{1,0.5,1\}$, gdzie:

- 0 – oznacza, że wymaganie nie jest wcale zrealizowane w odniesieniu do systemu S_i,
- 0.5 – oznacza, że wymaganie jest zrealizowane częściowo w odniesieniu do systemu S_i za sprawą poprawnej konstrukcji mechanizmu bezpieczeństwa, lecz nie jest odpowiednio wdrożone,
- 1 – oznacza, że wymaganie jest w pełni zrealizowane w odniesieniu do systemu S_i.

Definicja 14

Oceną realizacji wymagań bezpieczeństwa dla systemu informatycznego S_i nazywamy stosunek procentowy wartości iloczynu Π_{S_i} do iloczynu Φ_{S_i}:

$$\alpha_{S_i} = \frac{\Pi_{S_i}}{\Phi_{S_i}} * 100\% \qquad \textit{Wzór 4.3. - 5}$$

gdzie:

Π_{S_i} – jest sumą iloczynów wartości priorytetów wymagań $p_{k_{S_i}}^j$, wartości adekwatności wymagania $a_{S_i}^j$ i wartości realizacji wymagania $\omega_{S_i}^j$

$$\Pi_{S_i} = \sum_{j=1}^{\overline{W}} p_{k_{S_i}}^j * a_{S_i}^j * \omega_{S_i}^j , \qquad \textit{Wzór4.3. - 6}$$

Φ_{S_i} – jest sumą iloczynów wartości priorytetów wymagań dla danej klasy bezpieczeństwa systemu $p^j_{k_{S_i}}$ oraz wartości adekwatności wymagania $a^j_{S_i}$

$$\Phi_{S_i} = \sum_{j=1}^{\overline{W}} p^j_{k_{S_i}} * a^j_{S_i} \; . \qquad \textit{Wzór4.3. - 7}$$

4.3.2 Część druga metody ORBI – Ocena wartości ryzyka związanego z bezpieczeństwem systemów informatycznych organizacji

Druga część metody ORBI jest zasadniczym etapem oceny ryzyka związanego z bezpieczeństwem systemów informatycznych organizacji. W tej części są realizowane następujące operacje:

1. Wyznaczenie wartości ryzyka związanego z bezpieczeństwem systemów informatycznych organizacji.
2. Grupowanie wyznaczonych wartości z perspektyw poszczególnych klas istotności i klas bezpieczeństwa.
3. Opracowanie reprezentacji graficznej ryzyka.
4. Opracowanie tabeli zbiorczej ryzyk dla systemów informatycznych organizacji.

Efektem realizacji drugiej części metody jest wyznaczenia wartości ryzyka r_{S_i} związanego z bezpieczeństwem systemu informatycznego S_i, wartości ryzyka względnego R_{S_i} związanego z bezpieczeństwem systemu informatycznego S_i oraz wartości ryzyk średnich dla poszczególnych klas istotności i klas bezpieczeństwa. Drugą część metody ORBI kończy wyznaczenie wartości średniej ryzyka $\Re_{S(O)}$ dla wszystkich systemów informatycznych organizacji.

4.3.2.1 Wyznaczenie wartości ryzyk związanych z bezpieczeństwem systemów informatycznych

Definicja 15

Ryzyko r_{S_i} związane z bezpieczeństwem systemu informatycznego S_i jest równe objętości ostrosłupa mającego początek w punkcie (0,0,0) kartezjańskiego układu współrzędnych i jest obliczane ze wzoru:

$$r_{S_i} = \frac{f_k(k_{S_i}) * f_u(u_{S_i}) * f_\alpha(\alpha_{S_i})}{6} \qquad \textit{Wzór 4.3.-8}$$

gdzie:

$f_k(k_{S_i})$ – jest to wartość wyznaczona na osi klasy bezpieczeństwa systemu informatycznego (odpowiednio dla *A1* – wartość 16 na osi *K*, *A2* – wartość 15 na osi *K,* aż do *D4* – wartość 1 na osi *K*),

$f_u(u_{S_i})$ – jest to wartość wyznaczona na osi istotności U systemu informatycznego (odpowiednio dla *I* – wartość 5 na osi *U*, *II* – wartość 4 na osi *U,* aż do *V* – wartość 1 na osi *U*),

$f_\alpha(\alpha_{S_i})$ – jest to wartość wyznaczona na osi realizacji wymagań bezpieczeństwa α (odpowiednio dla α_{S_i}=100% – wartość 0 na osi α, α_{S_i}=99% – wartość 0.1 na osi α, aż do α_{S_i}=0% – wartość 10 na osi α)[189].

Definicja 16

Ryzykiem maksymalnym $r_{\max}$ dla systemów informatycznych należących do zbioru $S(O)$, jest najwyższa możliwa wartość ryzyka związanego z bezpieczeństwem systemów informatycznych $S(O)$, wyliczana ze wzoru:

$$r_{\max} = \frac{\max\left(f_k(k_{S_i})\right) * \max\left(f_u(u_{S_i})\right) * f_\alpha(0\%)}{6}. \qquad \textit{Wzór 4.3. - 9}$$

[189] Wartość spełnienia wymagania bezpieczeństwa α_{S_i} jest odwrotnie proporcjonalna do wartości ryzyka. Zgodnie z tym założeniem wraz ze wzrostem wartości α_{S_i} maleje wartość na osi realizacji wymagań bezpieczeństwa.

Definicja 17

Wartość względna ryzyka R_{S_i} związanego z bezpieczeństwem systemu informatycznego S_i jest ilorazem wartości ryzyka r_{S_i} związanego z bezpieczeństwem systemu S_i i wartości ryzyka maksymalnego związanego z bezpieczeństwem systemów informatycznych $r_{\max}$ należących do zbioru $S(O)$:

$$R_{S_i} = \frac{r_{S_i}}{r_{\max}} * 100\% \qquad \textit{Wzór 4.3. - 10}$$

Definicja 18

Ryzykiem średnim klasy bezpieczeństwa k nazywamy średnią arytmetyczną wartości ryzyk względnych systemów informatycznych należących do klasy bezpieczeństwa k. Ryzyko średnie systemów informatycznych należących do klasy bezpieczeństwa k oznaczamy symbolem $R_{sr(k)}$.

Definicja 19

Ryzykiem średnim klasy istotności u nazywamy średnią arytmetyczną wartości względnych ryzyk systemów informatycznych należących do klasy istotności u. Ryzyko średnie systemów informatycznych należących do klasy istotności u oznaczamy symbolem $R_{sr(u)}$.

Definicja 20

Ryzykiem średnim klasy istotności u i klasy bezpieczeństwa k nazywamy średnią arytmetyczną wartości względnych ryzyk systemów informatycznych należących do klasy istotności u i klasy bezpieczeństwa k. Ryzyko średnie systemów informatycznych należących do klasy istotności u i klasy bezpieczeństwa k oznaczamy symbolem $R_{sr(u)(k)}$.

Definicja 21

Ryzykiem średnim $\Re_{S(O)}$ związanym z bezpieczeństwem systemów informatycznych należących do $S(O)$ nazywamy średnią arytmetyczną ryzyk względnych R_{S_i} dla $S_i \in S(O)$.

Wartość ryzyka r_{S_i} jest obliczana dla pojedynczego systemu informatycznego organizacji. W metodzie ORBI należy posługiwać się pojęciem ryzyka względnego R_{S_i} związanego z bezpieczeństwem systemu informatycznego, ze względu na istnienie wielu systemów informatycznych. Wynika to z konieczności odniesienia miary ryzyka pojedynczego systemu informatycznego S_i do pozostałych systemów informatycznych. Konieczność takiego odniesienia wynika z przyjętej definicji systemu informatycznego organizacji. Zgodnie z tą definicją częścią wspólną wielu systemów informatycznych są dane, których bezpieczeństwo jest zależne od stopnia zabezpieczenia wszystkich przetwarzających je systemów informatycznych. W celu traktowania systemów informatycznych przedsiębiorstwa łącznie, należy dokonać odniesienia wartości ryzyka każdego z systemów do maksymalnej możliwej wartość ryzyka dla systemów informatycznych organizacji.

4.3.2.2 Reprezentacja graficzna wartości ryzyka r_{S_i} oraz ryzyka względnego R_{S_i}

Definicja 22

W celu jakościowego i graficznego przedstawienia poziomu ryzyka r_{S_i} oraz ryzyka względnego R_{S_i} wyznaczonego za pomocą przedstawionej powyżej metody ilościowej, przyjęto następujące przedziały ryzyka względnego:

$R_{S_i} \geq 80\%$ – ryzyko maksymalne, oznaczane kolorem czarnym,

$R_{S_i} \in [60\%,...,80\%)$ – ryzyko bardzo wysokie, oznaczane kolorem czerwonym,

$R_{S_i} \in [40\%,...,60\%)$ – ryzyko średnie, oznaczane kolorem żółtym,

$R_{S_i} \in [1\%,...,40\%)$ – ryzyko niskie, oznaczane kolorem zielonym,

$R_{S_i} < 1\%$ – ryzyko śladowe, oznaczane kolorem niebieskim.

Ostrosłup o wierzchołku w punkcie (0,0,0) jest reprezentacją graficzną poziomu ryzyka r_{S_i}, którego podstawę stanowi trójkąt wyznaczony na kartezjańskim układzie współrzędnych, o osiach przedstawiających odpowiednio wartości:

1. Klasy bezpieczeństwa systemu.
2. Klasy istotności systemu.
3. Oceny realizacji wymagań bezpieczeństwa.

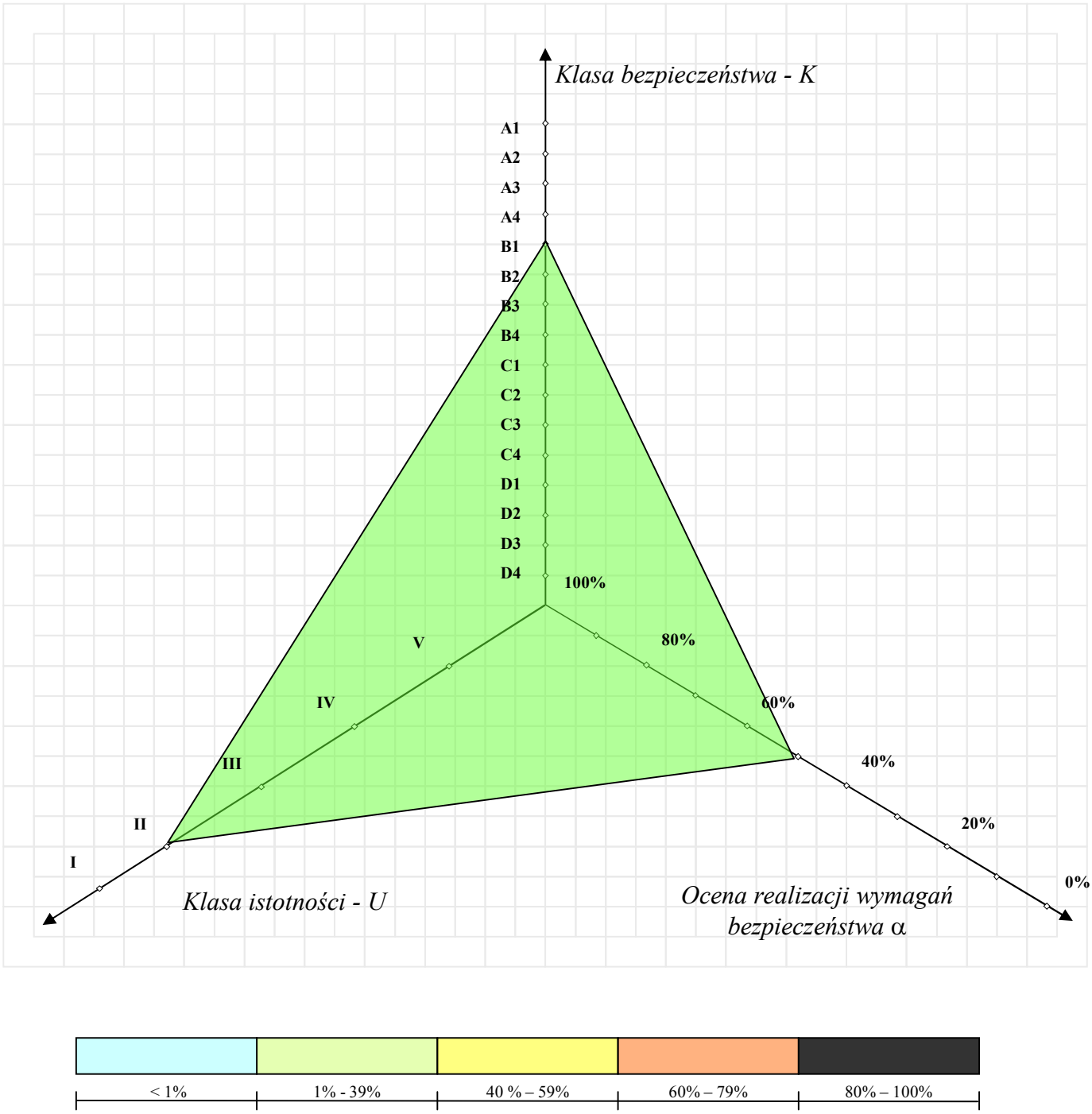
Pole ostrosłupa oznaczone jest kolorem odpowiednim dla poziomu ryzyka względnego R_{S_i} danego systemu informatycznego S_i zgodnie z *Definicją 22*.

Przykład reprezentacji graficznej metody ORBI przedstawia rysunek 4.3.- 8[190].

Dla wizualizacji analiz porównawczych ryzyka względnego w metodzie ORBI są używane wykresy inspirowane pracami J. Nosworthya[191] oraz J. Sherwooda[192].

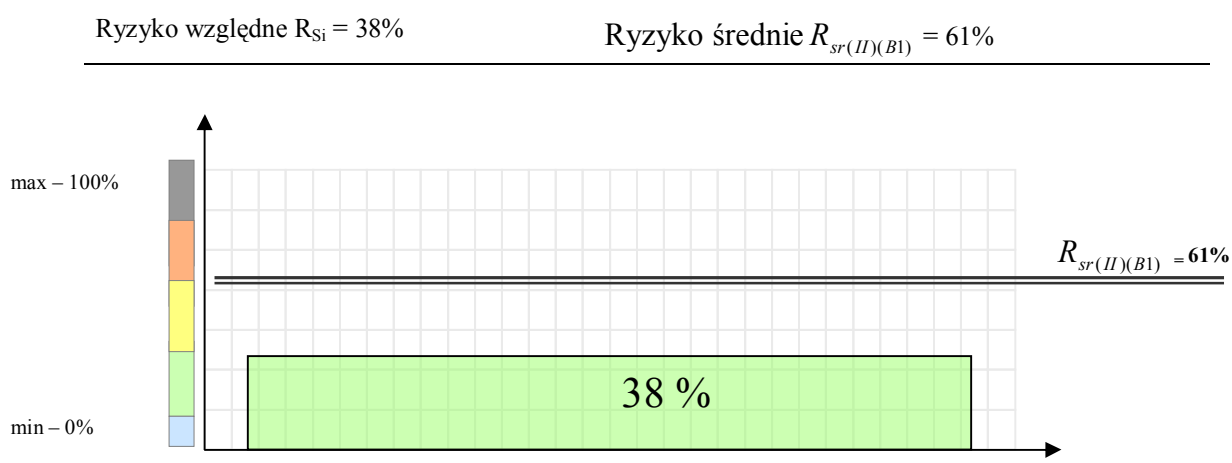
[190] Rolą rysunku jest przedstawienie możliwej prezentacji graficznej. Wartości wykorzystane do rysunków 4.3.-8 oraz 4.3.-9 mają charakter ilustracyjny i nie pochodzą z przykładów ani wyliczeń.
[191] Nosworthy, J. 2000. A Practical Risk Analysis Approach: Managing BCM Risk, Computers & Security 19, 7, 596 - 614. Oxford: Elsevier [71]
[192] Sherwood, J. 1999. Operational Risk Management in Business Information Systems. London: Sherwood Ltd. [109]

Nazwa systemu – S_i	Klasa bezpieczeństwa systemu – B1	Klasa Istotności – II
Wartość spełnienia wymagań bezpieczeństwa - α_j = 50%		Ryzyko systemu S_i = 40
Ryzyko względne R_{Si} = 38%		



Rysunek 4.3.- 8. Graficzna reprezentacja wartości ryzyka r_{S_i} oznaczona jest kolorem odpowiednim dla poziomu ryzyka względnego R_{S_i}

Inną reprezentację graficzną wartości ryzyka względnego R_{S_i} zgodnie z *Definicją 20* przedstawia rysunek 4.3. - 9.



Rysunek 4.3. - 9. Graficzna reprezentacja wartości ryzyka względnego R_{S_i} związanego z bezpieczeństwem systemu informatycznego S_i w stosunku do ryzyka średniego $R_{sr(II)(B1)}$ klasy istotności *II* oraz klasy bezpieczeństwa *B1* systemów informatycznych $S(O)$

4.3.2.3 Tabela zbiorcza ryzyk systemów informatycznych $S(O)$ organizacji.

W metodzie ORBI w celu zebrania i uporządkowania w jednym miejscu wyników oceny ryzyka oraz zestawień z perspektywy systemów informatycznych oraz klas istotności i bezpieczeństwa, należy sporządzić tabelę ryzyk systemów informatycznych $S(O)$. Wyniki te przedstawia Tabela 4.3. - 4.

		System informatyczny S_i					
		S_1	S_2	…	…	…	S_N
Ryzyko r_{S_i} związane z bezpieczeństwem systemu informatycznego S_i							
Ryzyko maksymalne $r_{\max}$ dla systemów informatycznych należących do zbioru $S(O)$							
Ryzyko względne R_{S_i} związane z bezpieczeństwem systemu informatycznego S_i							
Ryzyko średnie $\Re_{S(O)}$ związane z bezpieczeństwem systemów informatycznych należących do zbioru $S(O)$							
Klasa bezpieczeństwa	$R_{sr(k)}$ – ryzyko średnie dla klasy bezpieczeństwa	S_1	S_2	…	…	…	S_N
k	$R_{sr(k)}$						
Klasa istotności	$R_{sr(u)}$ – ryzyko średnie dla klasy istotności	S_1	S_2	…	…	…	S_N
u	$R_{sr(u)}$						

Tabela 4.3. - 4. Tabela zbiorcza ryzyk dla systemów informatycznych $S(O)$ organizacji.

5 Przykład zastosowania metody ORBI

5.1 Założenia przyjęte dla przykładu

Dla potrzeb przykładu przyjęto, że organizacją, której systemy informatyczne będą analizowane, jest przedsiębiorstwo telekomunikacyjne świadczące usługi głosowe telefonii stacjonarnej oraz transmisji danych. Przedsiębiorstwo to ma milion abonentów o rozkładzie 90% klientów indywidualnych i 10% klientów biznesowych. Firma ta świadczy usługi na terenie kraju. Dotyczą one połączeń krajowych (lokalnych i międzystrefowych) w ramach własnej sieci, połączeń międzyoperatorskich (do sieci stacjonarnej i komórkowej) oraz połączeń międzynarodowych. Przedsiębiorstwo ma własną sieć korporacyjną (WAN, LAN) oraz odseparowaną sieć służącą do świadczenia usług. Przedsiębiorstwo ma następujące systemy informatyczne:

1. SYSTEM S_1 – System Bilingowy typu B&CC (ang. Billing and Customer Care) – główny system przetwarzający dane o połączeniach, w skład którego wchodzi system mediacji danych z central, system taryfikacji połączeń oraz system przygotowywania elektronicznych obrazów faktur.
2. SYSTEM S_2 – System Obsługi Klienta typu CRM (ang. Customer Relationship Management) – system przeznaczony do obsługi aktualnych i potencjalnych klientów firmy. System ten posiada centralną bazę danych z dostępem terminalowym (dla konsultantów biura obsługi klienta pracującego w trybie 7/24/365) oraz dostępem bezpośrednim dla klientów za pośrednictwem Internetu.
3. SYSTEM S_3 – System Obsługi Sieci typu C&FMS (ang. Configuration and Fault Management System) – system zarządzania siecią usługową oraz siecią korporacyjną służący do jej konfiguracji i nadzoru.
4. SYSTEM S_4 – System Zarządzania Zasobami typu ERP (ang. Enterprise Resource Planning) – system finansowy (księga główna), zarządzania magazynami i środkami trwałymi oraz kadrami i płacami.
5. SYSTEM S_5 – System poczty korporacyjnej – system służący do komunikacji pomiędzy pracownikami i współpracownikami przedsiębiorstwa.
6. SYSTEM S_6 – System sprawozdawczości giełdowej – służący do generowania raportów finansowych i sprawozdań zgodnych z wymaganiami Komisji Papierów Wartościowych i Giełd.

5.2 Część pierwsza metody ORBI – przykład użycia

W tym punkcie jest przedstawione praktyczne zastosowanie pierwszej części metody ORBI (służącej klasyfikacji systemów informatycznych) na przykładzie systemów informatycznych przedsiębiorstwa telekomunikacyjnego.

5.2.1 Klasyfikacja systemów informatycznych przedsiębiorstwa telekomunikacyjnego

Zgodnie z zasadami opisanymi w rozdziale 4.3 dotyczącymi metody ORBI systemy informatyczne przedsiębiorstwa telekomunikacyjnego zostały zaklasyfikowane odpowiednio do klas bezpieczeństwa i klas istotności. Wyniki klasyfikacji przedstawiają odpowiednio Tabela 5.2. - 5 i Tabela 5.2. - 6.

System	Klasa bezpieczeństwa	Opis
S_1	*A2*	System przetwarza dane poufne stanowiące tajemnicę przedsiębiorstwa dla którego oczekiwana dostępność w skali roku wynosi 99,9% a maksymalna jednorazowa niedostępność systemu nie przekracza 1 godziny. Dane przetwarzane przez systemy bilingowe zawierają informacje o klientach operatora telekomunikacyjnego. Z tego powodu stanowią tajemnicę przedsiębiorstwa (dodatkowo podlegają wymaganiom ochrony przewidzianymi stosownymi aktami prawa np.: Ustawy o ochronie danych osobowych). Ponieważ systemy bilingowe muszą pracować w sposób ciągły (świadcząc usługi np.: sieci inteligentnych) ich dostępność musi być najwyższego, uzasadnionego biznesowo, poziomu.
S_2	*A2*	System przetwarza dane poufne stanowiące tajemnicę przedsiębiorstwa dla którego oczekiwana dostępność w skali roku wynosi 99,9%, a maksymalna jednorazowa niedostępność systemu nie przekracza 1 godziny. Analogicznie jak w systemach bilingowych dane przetwarzane przez te systemy stanowią tajemnicę przedsiębiorstwa (dane o klientach). Z powodu konieczności ciągłej obsługi klientów wymagany jest najwyższy, uzasadniony biznesowo, poziom dostępności.
S_3	*A3*	System przetwarza dane wrażliwe nie stanowiące tajemnicy przedsiębiorstwa ale nie będące danymi publicznymi, dla którego oczekiwana dostępność w skali roku wynosi 99,9%, a maksymalna jednorazowa niedostępność systemu nie przekracza 1 godziny. Systemy tego typu nie przetwarzają danych stanowiących tajemnicę przedsiębiorstwa (bez dodatkowych wymagań prawnych). Informacja o błędach sieci oraz awariach nie jest jednak informacją powszechnie dostępną i powinna być odpowiednio chroniona. Ze względu jednak na konieczność ciągłego monitorowania pracy sieci telekomunikacyjnej, systemy tego typu wymagają wysokiego stopnia dostępności.
S_4	*C2*	System przetwarza dane poufne stanowiące tajemnicę przedsiębiorstwa dla którego oczekiwana dostępność w skali

		roku wynosi 95% a maksymalna jednorazowa niedostępność systemu nie przekracza 1 dnia. Systemy tego typu przetwarzają między innymi informacje finansowe stanowiące tajemnicę przedsiębiorstwa. Ich nieuprawnione ujawnienie miałoby negatywne konsekwencje biznesowe i wizerunkowe dla firmy. Dostępność systemu nie jest krytyczna lecz kilkudziesięciogodzinna przerwa mogłaby spowodować wymierne straty dla firmy spowodowane na przykład zatrzymaniem określonych procesów logistycznych (magazynowych).
S_5	*B4*	System przetwarza dane publiczne dla którego oczekiwana dostępność w skali roku wynosi 99,5%, a maksymalna jednorazowa niedostępność systemu nie przekracza 1 godziny. System służący do komunikacji o realizacji określonych zadań w ramach wykonywanych przez pracowników obowiązków. Utrzymanie poufności danych nie jest konieczne (przy założeniu, że obieg informacji poufnych jest w innym wydzielonym systemie). System ze względu na specyfikę wymiany informacji służącej do obsługi procesów operacyjnych firmy jest jednak bardzo istotny, Jego zatrzymanie (niedostępność) zatrzymuje pracę na stanowiskach. Tym samym jego dostępność odgrywa istotną rolę.
S_6	*D1*	System przetwarza dane o najwyższej klauzuli poufności dla którego oczekiwana dostępność w skali roku wynosi poniżej 95% a maksymalna jednorazowa niedostępność systemu może przekroczyć 1 dzień. System „księga akcjonariuszy" przetwarza dane bardzo istotne dla przedsiębiorstwa. Dane te stanowią tajemnicę przedsiębiorstwa i podlegają stosownym wymaganiom dotyczącym ich poufności. Ciągła dostępność systemu nie jest istotna z powodu cykli raportowych odbywających się raz na miesiąc lub kwartał.

Tabela 5.2. - 5. Systemy informatyczne przedsiębiorstwa telekomunikacyjnego wraz z przyporządkowanymi im klasami bezpieczeństwa. W tabeli wprowadzono uwagi dotyczące opisu klasy bezpieczeństwa

System	Klasa Istotności	Opis
S_1	*I*	System informatyczny służący realizacji głównych i najistotniejszych procesów biznesowych. Wartość systemu informatycznego jest porównywalna z wartością rynkową organizacji gospodarczej. System bilingowy stanowi główny element biznesowy przedsiębiorstwa telekomunikacyjnego. Poza siecią telekomunikacyjną, dzięki której jest świadczona usługa, system bilingowy jest najistotniejszym zasobem firmy telekomunikacyjnej.
S_2	*I*	System informatyczny służący realizacji głównych i najistotniejszych procesów biznesowych. Wartość systemu informatycznego jest porównywalna z wartością rynkową organizacji gospodarczej. Za sprawą danych o transakcjach klientów oraz historii ich aktywności, system tego typu jest jednym z najcenniejszych a zarazem kluczowych zasobów firmy telekomunikacyjnej.

S_3	*II*	System informatyczny służący realizacji głównych procesów biznesowych. Wartość systemu informatycznego jest porównywalna z wartością przychodów osiąganych przez daną organizację gospodarczą w związku z realizacją działalności za pomocą tych procesów biznesowych. System C&FM odpowiada w głównej mierze za poprawną i odpowiednią jakościowo usługę świadczoną przez firmę telekomunikacyjną. Wartość tego typu systemu nie jest związana bezpośrednio z możliwością świadczenia usługi przez firmę, lecz ma bardzo istotny wpływ na przychody firmy za sprawą poprawności naliczania opłat za wyświadczoną usługę oraz liczbę reklamacji i zadowolenie klientów.
S_4	*III*	System informatyczny służący realizacji głównych procesów wspomagających główne procesy biznesowe. Wartość systemu jest porównywalna z wartością komponentów sprzętowych i programowych systemu informatycznego oraz nakładów niezbędnych na wprowadzenie do niego danych. System wspomagający działalność firmy, dzięki któremu wiele operacji wsparcia (ang. back office) jest realizowanych w sposób efektywny, szybki i kontrolowany.
S_5	*III*	System informatyczny służący realizacji głównych procesów wspomagających główne procesy biznesowe. Wartość systemu jest porównywalna z wartością komponentów sprzętowych i programowych systemu informatycznego oraz nakładów niezbędnych na wprowadzenie do niego danych. System ułatwiający i w znaczący sposób przyspieszający realizację zadań przez pracowników firmy. Za sprawą tego typu systemów jest możliwezwiększenie efektywności pracy.
S_6	*IV*	System informatyczny służący wspieraniu działalności administracyjnej organizacji. Wartość systemu informatycznego jest porównywalna z wartością usługi świadczonej na zlecenie organizacji świadczoną przez stronę trzecią. System zastępujący konwencjonalną metodę zbierania, przetwarzania i udostępniania danych.

Tabela 5.2. - 6. Systemy informatyczne przedsiębiorstwa telekomunikacyjnego wraz z przyporządkowanymi im klasami istotności.

Podsumowanie przypisania poszczególnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego do klas bezpieczeństwa i klas istotności tworzy macierz klasyfikacji systemów informatycznych przedsiębiorstwa telekomunikacyjnego. Jest ona przedstawiona w Tabeli 5.2. - 7.

	System informatyczny S_i					
	S_1	S_2	S_3	S_4	S_5	S_6
Klasa bezpieczeństwa systemu informatycznego	*A2*	*A2*	*A3*	*C2*	*B4*	*D1*
Klasa istotności systemu informatycznego	*I*	*I*	*II*	*III*	*III*	*IV*

Tabela 5.2. - 7. Macierz klasyfikacji systemów informatycznych przedsiębiorstwa telekomunikacyjnego

5.2.2 Określenie priorytetów wymagań – przykład użycia

Tabela 5.2. - 8 przedstawia wymagania bezpieczeństwa metody ORBI ograniczone do ośmiu. Ograniczenie wynika z konieczności zachowania przejrzystości przykładu.

Wymaganie	Opis
Wymaganie 1	Wymaganie wysokiej dostępności serwera bazy danych i aplikacji.
Wymaganie 2	Wymaganie wysokiej dostępności i niezawodności sieci komputerowej.
Wymaganie 3	Wymaganie średniej dostępności serwera bazy danych i aplikacji.
Wymaganie 4	Wymaganie średniej dostępności i niezawodności sieci komputerowej.
Wymaganie 5	Wymaganie opracowania procedur operacyjnych dostępu do systemu.
Wymaganie 6	Wymaganie wysokiej poufności – tajne.
Wymaganie 7	Wymaganie poufności danych stanowiących tajemnice przedsiębiorstwa.
Wymaganie 8	Wymaganie przetwarzania zgodnie z ustawą o rachunkowości.

Tabela 5.2. - 8. Wymagania bezpieczeństwa zastosowane dla przykładowego przedsiębiorstwa telekomunikacyjnego

Poszczególnym wymaganiom klas bezpieczeństwa zostały przypisane priorytety wymagań, które przedstawia Tabela 5.2. - 9, będąca macierzą priorytetów wymagań (zgodnie z rozdziałem 4.3.1.2). Priorytety wymagań zostały ograniczone do priorytetów dla klas bezpieczeństwa wykorzystywanych w prezentowanym przykładzie.

		Klasa bezpieczeństwa systemów informatycznych				
		A2	*A3*	*B4*	*C2*	*D1*
Wymaganie bezpieczeństwa	Wymaganie 1	5	5	0	0	0
	Wymaganie 2	4	4	0	0	0
	Wymaganie 3	0	0	5	0	0
	Wymaganie 4	0	0	4	0	0
	Wymaganie 5	3	3	3	3	4
	Wymaganie 6	0	0	0	0	5
	Wymaganie 7	5	0	0	5	0
	Wymaganie 8	2	2	2	5	5

Tabela 5.2. - 9. Macierz priorytetów wymagań bezpieczeństwa dla klas *A2*, *A3*, *B4*, *C2* i *D1* (klas bezpieczeństwa wykorzystywanych w prezentowanym przykładzie)

5.2.3 Ocena adekwatności wymagań bezpieczeństwa systemów informatycznych przedsiębiorstwa telekomunikacyjnego

Poszczególnym systemom informatycznym przedsiębiorstwa telekomunikacyjnego zostały przypisane adekwatności wymagań przedstawione w tabelach: Tabela 5.2. - 10, Tabela 5.2. - 11, Tabela 5.2. - 12, Tabela 5.2. - 13, Tabela 5.2. - 14, Tabela 5.2. - 15 [193].

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_1 należącego klasy *A2*	Adekwatność wymagania dla systemu S_1
Wymaganie 1	5	1
Wymaganie 2	4	0[194]
Wymaganie 3	0	0
Wymaganie 4	0	0
Wymaganie 5	3	1
Wymaganie 6	0	0
Wymaganie 7	5	1
Wymaganie 8	2	1

Tabela 5.2. - 10. Adekwatność wymagań bezpieczeństwa dla systemu informatycznego S_1

[193] Dla przejrzystości przykładu przyjęto, że jedno z wymagań nie będzie adekwatne dla każdego systemu opisywanego przedsiębiorstwa. Dla poszczególnych wymagań, określonych jako nieadekwatne, zostaną podane przykładowe wytłumaczenia. Dla wymagań dla których priorytet wymagań bezpieczeństwa dla systemu, przyjęty w *Definicji 9* wynosi 0, adekwatność takiego wymagania względem danego systemu informatycznego wynosi również 0. Dla przejrzystości wymagania te zaznaczono kolorem szarym.

[194] System nie jest podłączony do sieci komputerowej.

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_2 należącego klasy *A2*	Adekwatność wymagania dla systemu S_2
Wymaganie 1	5	1
Wymaganie 2	4	1
Wymaganie 3	0	0
Wymaganie 4	0	0
Wymaganie 5	3	1
Wymaganie 6	0	0
Wymaganie 7	5	1
Wymaganie 8	2	0[195]

Tabela 5.2. - 11. Adekwatność wymagań bezpieczeństwa dla systemu informatycznego S_2

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_3 należącego klasy *A3*	Adekwatność wymagania dla systemu S_3
Wymaganie 1	5	1
Wymaganie 2	4	1
Wymaganie 3	0	0
Wymaganie 4	0	0
Wymaganie 5	3	1
Wymaganie 6	0	0
Wymaganie 7	0	0
Wymaganie 8	2	0[196]

Tabela 5.2. - 12. Adekwatność wymagań bezpieczeństwa dla systemu informatycznego S_3

[195] Nie ma specyficznych wymagań prawnych dla tego systemu.
[196] Nie ma specyficznych wymagań prawnych dla tego systemu.

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_4 należącego klasy *C2*	Adekwatność wymagania dla systemu S_4
Wymaganie 1	0	0
Wymaganie 2	0	0
Wymaganie 3	0	0
Wymaganie 4	0	0
Wymaganie 5	3	1
Wymaganie 6	0	0
Wymaganie 7	5	0[197]
Wymaganie 8	5	1

Tabela 5.2. - 13. Adekwatność wymagań bezpieczeństwa dla systemu informatycznego S_4

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_5 należącego klasy *B4*	Adekwatność wymagania dla systemu S_5
Wymaganie 1	0	0
Wymaganie 2	0	0
Wymaganie 3	5	1
Wymaganie 4	4	1
Wymaganie 5	3	1
Wymaganie 6	0	0
Wymaganie 7	0	0
Wymaganie 8	2	0[198]

Tabela 5.2. - 14. Adekwatność wymagań bezpieczeństwa dla systemu informatycznego S_5

[197] Dla tego systemu nie muszą być opracowane specyficzne procedury, gdyż wynikają one z przepisów prawa.
[198] Nie ma specyficznych wymagań prawnych dla tego systemu.

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_6 należącego klasy *D1*	Adekwatność wymagania dla systemu S_6
Wymaganie 1	0	0
Wymaganie 2	0	0
Wymaganie 3	0	0
Wymaganie 4	0	0
Wymaganie 5	4	1
Wymaganie 6	5	1
Wymaganie 7	0	0
Wymaganie 8	5	0[199]

Tabela 5.2. - 15. Adekwatność wymagań bezpieczeństwa dla systemu informatycznego S_6

[199] Dla tego systemu nie muszą być opracowane specyficzne procedury, gdyż wynikają one z przepisów prawa.

5.2.4 Ocena realizacji wymagań bezpieczeństwa przez systemy informatyczne przedsiębiorstwa telekomunikacyjnego

Dla poszczególnych systemów informatycznych omawianego przedsiębiorstwa zostały wyznaczone poziomy realizacji adekwatnych wymagań bezpieczeństwa. Są one przedstawione w tabelach: Tabela 5.2. - 16, Tabela 5.2. - 17, Tabela 5.2. - 18, Tabela 5.2. - 19, Tabela 5.2. - 20, Tabela 5.2. - 21.

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_1 należącego klasy *A2*	Adekwatność wymagania dla systemu S_1	Realizacja wymagania dla systemu S_1
Wymaganie 1	5	1	0
Wymaganie 2	4	0	0
Wymaganie 3	0	0	0
Wymaganie 4	0	0	0
Wymaganie 5	3	1	0,5
Wymaganie 6	0	0	0
Wymaganie 7	5	1	0,5
Wymaganie 8	2	1	1

Tabela 5.2. - 16. Realizacja wymagań bezpieczeństwa przez system informatyczny S_1

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_2 należącego klasy A2	Adekwatność wymagania dla systemu S_2	Realizacja wymagania dla systemu S_2
Wymaganie 1	5	1	0,5
Wymaganie 2	4	1	0
Wymaganie 3	0	0	0
Wymaganie 4	0	0	0
Wymaganie 5	3	1	0
Wymaganie 6	0	0	0
Wymaganie 7	5	1	1
Wymaganie 8	2	0	0

Tabela 5.2. - 17. Realizacja wymagań bezpieczeństwa przez system informatyczny S_2

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_3 należącego klasy *A3*	Adekwatność wymagania dla systemu S_3	Realizacja wymagania dla systemu S_3
Wymaganie 1	5	1	0,5
Wymaganie 2	4	1	0
Wymaganie 3	0	0	0
Wymaganie 4	0	0	0
Wymaganie 5	3	1	0
Wymaganie 6	0	0	0
Wymaganie 7	0	0	0
Wymaganie 8	2	0	0

Tabela 5.2. - 18. Realizacja wymagań bezpieczeństwa przez system informatyczny S_3

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_4 należącego klasy *C2*	Adekwatność wymagania dla systemu S_4	Realizacja wymagania dla systemu S_4
Wymaganie 1	0	0	0
Wymaganie 2	0	0	0
Wymaganie 3	0	0	0
Wymaganie 4	0	0	0
Wymaganie 5	3	1	0,5
Wymaganie 6	0	0	0
Wymaganie 7	5	0	0
Wymaganie 8	5	1	1

Tabela 5.2. - 19. Realizacja wymagań bezpieczeństwa przez system informatyczny S_4

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_5 należącego klasy *B4*	Adekwatność wymagania dla systemu S_5	Realizacja wymagania dla systemu S_5
Wymaganie 1	0	0	0
Wymaganie 2	0	0	0
Wymaganie 3	5	1	0
Wymaganie 4	4	1	0,5
Wymaganie 5	3	1	0,5
Wymaganie 6	0	0	0
Wymaganie 7	0	0	0
Wymaganie 8	2	0	0

Tabela 5.2. - 20. Realizacja wymagań bezpieczeństwa przez system informatyczny S_5

Wymaganie	Priorytet wymagań bezpieczeństwa dla systemu S_6 należącego klasy *D1*	Adekwatność wymagania dla systemu S_6	Realizacja wymagania dla systemu S_6
Wymaganie 1	0	0	0
Wymaganie 2	0	0	0
Wymaganie 3	0	0	0
Wymaganie 4	0	0	0
Wymaganie 5	4	1	1
Wymaganie 6	5	1	0,5
Wymaganie 7	0	0	0
Wymaganie 8	5	0	0

Tabela 5.2. - 21. Realizacja wymagań bezpieczeństwa przez system informatyczny S_6

Wartość spełnienia wymagań α_{S_i} dla poszczególnych systemów informatycznych powstaje przez wyznaczenie wartości Π_{S_i} oraz Φ_{S_i} zgodnie z *Definicją 14*.

Realizacja wymagań bezpieczeństwa dla systemu $S_1 - \alpha_{S_1}$:

Wartość Π_{S_1} wynosi:

$$\Pi_{S_1} = \sum_{j=1}^{8} p_{k_{S_1}}^{j} * a_{S_1}^{j} * \omega_{S_1}^{j} = 5 * 1 * 0 + 4 * 0 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + \\ + 3 * 1 * 0{,}5 + 0 * 0 * 0 + 5 * 1 * 0{,}5 + 2 * 1 * 1 = \mathbf{6}$$

Wartość Φ_{S_1} wynosi:

$$\Phi_{S_1} = \sum_{j=1}^{8} p_{k_{S_1}}^{j} * a_{S_1}^{j} = 5 * 1 + 4 * 0 + 0 * 0 + 0 * 0 + 3 * 1 + 0 * 0 + 5 * 1 + 2 * 1 = \mathbf{15}$$

Zatem wartość α_{S_1} wynosi:

$$\alpha_{S_1} = \frac{\Pi_{S_1}}{\Phi_{S_1}} * 100\% = \frac{6}{15} * 100\% = 40\% .$$

Wartość realizacji wymagań bezpieczeństwa przez system S_1 wynosi 40%.

Realizacja wymagań bezpieczeństwa dla systemu $S_2 - \alpha_{S_2}$:

Wartość Π_{S_2} wynosi:

$$\Pi_{S_2} = \sum_{j=1}^{8} p_{k_{S_2}}^{j} * a_{S_2}^{j} * \omega_{S_2}^{j} = 5 * 1 * 0{,}5 + 4 * 1 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + \\ + 3 * 1 * 0 + 0 * 0 * 0 + 5 * 1 * 1 + 2 * 0 * 0 = \mathbf{7{,}5}$$

Wartość Φ_{S_2} wynosi:

$$\Phi_{S_2} = \sum_{j=1}^{8} p_{k_{S_2}}^{j} * a_{S_2}^{j} = 5 * 1 + 4 * 1 + 0 * 0 + 0 * 0 + 3 * 1 + 0 * 0 + 5 * 1 + 2 * 0 = \mathbf{17}$$

Zatem wartość α_{S_2} wynosi:

$$\alpha_{S_2} = \frac{\Pi_{S_2}}{\Phi_{S_2}} * 100\% = \frac{7,5}{17} * 100\% = 44,12\%.$$

Wartość realizacji wymagań bezpieczeństwa przez system S_2 wynosi 44,12%.

Realizacja wymagań bezpieczeństwa dla systemu S_3 – α_{S_3}:

Wartość Π_{S_3} wynosi:

$$\Pi_{S_3} = \sum_{j=1}^{8} p_{k_{S_3}}^{j} * a_{S_3}^{j} * \omega_{S_3}^{j} = 5 * 1 * 0,5 + 4 * 1 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + \\ + 3 * 1 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + 2 * 0 * 0 = \mathbf{2,5}$$

Wartość Φ_{S_3} wynosi:

$$\Phi_{S_3} = \sum_{j=1}^{8} p_{k_{S_3}}^{j} * a_{S_3}^{j} = 5 * 1 + 4 * 1 + 0 * 0 + 0 * 0 + 3 * 1 + 0 * 0 + 0 * 0 + 2 * 0 = \mathbf{12}$$

Zatem wartość α_{S_3} wynosi:

$$\alpha_{S_3} = \frac{\Pi_{S_3}}{\Phi_{S_3}} * 100\% = \frac{2,5}{12} * 100\% = 20,83\%.$$

Wartość realizacji wymagań bezpieczeństwa przez system S_3 wynosi 20,83%.

Realizacja wymagań bezpieczeństwa dla systemu $S_4 - \alpha_{S_4}$:

Wartość Π_{S_4} wynosi:

$$\Pi_{S_4} = \sum_{j=1}^{8} p_{k_{S_4}}^{j} * a_{S_4}^{j} * \omega_{S_4}^{j} = 0 * 0 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + \\ + 3 * 1 * 0{,}5 + 0 * 0 * 0 + 5 * 0 * 0 + 5 * 1 * 1 = \mathbf{6{,}5}$$

Wartość Φ_{S_4} wynosi:

$$\Phi_{S_4} = \sum_{j=1}^{8} p_{k_{S_4}}^{j} * a_{S_4}^{j} = 0 * 0 + 0 * 0 + 0 * 0 + 0 * 0 + 3 * 1 + 0 * 0 + 5 * 0 + 5 * 1 = \mathbf{8}$$

Zatem wartość α_{S_4} wynosi:

$$\alpha_{S_4} = \frac{\Pi_{S_4}}{\Phi_{S_4}} * 100\% = \frac{6{,}5}{8} * 100\% = 81{,}25\% .$$

Wartość realizacji wymagań bezpieczeństwa przez system S_4 wynosi 81,25%.

Realizacja wymagań bezpieczeństwa dla systemu $S_5 - \alpha_{S_5}$:

Wartość Π_{S_5} wynosi:

$$\Pi_{S_5} = \sum_{j=1}^{8} p_{k_{S_5}}^{j} * a_{S_5}^{j} * \omega_{S_5}^{j} = 0 * 0 * 0 + 0 * 0 * 0 + 5 * 1 * 0 + 4 * 1 * 0{,}5 + \\ + 3 * 1 * 0{,}5 + 0 * 0 * 0 + 0 * 0 * 0 + 2 * 0 * 0 = \mathbf{3{,}5}$$

Wartość Φ_{S_5} wynosi:

$$\Phi_{S_5} = \sum_{j=1}^{8} p_{k_{S_5}}^{j} * a_{S_5}^{j} = 0 * 0 + 0 * 0 + 5 * 1 + 4 * 1 + 3 * 1 + 0 * 0 + 0 * 0 + 2 * 0 = \mathbf{12}$$

Zatem wartość α_{S_5} wynosi:

$$\alpha_{S_5} = \frac{\Pi_{S_5}}{\Phi_{S_5}} * 100\% = \frac{3{,}5}{12} * 100\% = 29{,}17\% .$$

Wartość realizacji wymagań bezpieczeństwa przez system S_5 wynosi 29,17%.

Realizacja wymagań bezpieczeństwa dla systemu $S_6 - \alpha_{S_6}$:

Wartość Π_{S_6} wynosi:

$$\Pi_{S_6} = \sum_{j=1}^{8} p_{k_{S_6}}^{j} * a_{S_6}^{j} * \omega_{S_6}^{j} = 0 * 0 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + 0 * 0 * 0 + 0 * 0 * 0 +$$
$$+ 4 * 1 * 1 + 5 * 1 * 0{,}5 + 0 * 0 * 0 + 5 * 0 * 0 = \mathbf{6{,}5}$$

Wartość Φ_{S_6} wynosi:

$$\Phi_{S_6} = \sum_{j=1}^{8} p_{k_{S_6}}^{j} * a_{S_6}^{j} = 0 * 0 + 0 * 0 + 0 * 0 + 0 * 0 + 4 * 1 + 5 * 1 + 0 * 0 + 5 * 0 = \mathbf{9}$$

Zatem wartość α_{S_6} wynosi:

$$\alpha_{S_6} = \frac{\Pi_{S_6}}{\Phi_{S_6}} * 100\% = \frac{6{,}5}{9} * 100\% = 72{,}22\% .$$

Wartość realizacji wymagań bezpieczeństwa przez system S_6 wynosi 72,22%.

5.3 Część druga metody ORBI – przykład użycia

W tym punkcie przedstawiono praktyczne zastosowanie drugiej części metody ORBI (służącej ocenie wartości ryzyka związanego z bezpieczeństwem systemów informatycznych organizacji), na przykładzie systemów informatycznych przedsiębiorstwa telekomunikacyjnego.

5.3.1 Wyznaczenie wartości ryzyka r dla systemów informatycznych przedsiębiorstwa telekomunikacyjnego

Wartość ryzyka r_{S_1}:

System S_1 należy do klasy bezpieczeństwa *A2* i do klasy istotności *I*. Wartość realizacji wymagań bezpieczeństwa α_{S_1} wynosi 40%.

Na podstawie dokonanej klasyfikacji systemu informatycznego S_1 oraz przyjętych dla metody ORBI założeń wiadomo, że:

- wartość $f_k(k_{S_1})$ jest równa odpowiednikowi klasy bezpieczeństwa systemu, który dla klasy *A2* wynosi 15,
- wartość $f_u(u_{S_1})$ jest równa odpowiednikowi klasy istotności, który dla grupy *I* wynosi 5,
- wartość $f_\alpha(\alpha_{S_1})$ jest równa odpowiednikowi 40% realizacji wymagań bezpieczeństwa czyli wynosi 6.

Ostatecznie wartość ryzyka r_{S_1} wynosi:

$$r_{S_1} = \frac{f_k(k_{S_1}) * f_u(u_{S_1}) * f_\alpha(\alpha_{S_1})}{6} = \frac{15 * 5 * 6}{6} = 75,0$$

Wartość ryzyka r_{S_2}:

System S_2 należy do klasy bezpieczeństwa *A2* i do klasy istotności *I*. Wartość realizacji wymagań bezpieczeństwa α_{S_2} wynosi 44,12 %, zatem:

$$r_{S_2} = \frac{f_k(k_{S_2}) * f_u(u_{S_2}) * f_\alpha(\alpha_{S_2})}{6} = \frac{15 * 5 * 5{,}59}{6} = 69{,}9$$

Wartość ryzyka r_{S_3}:

System S_3 należy do klasy bezpieczeństwa *A3* i do klasy istotności *II*. Wartość realizacji wymagań bezpieczeństwa α_{S_3} wynosi 20,83%, zatem:

$$r_{S_3} = \frac{f_k(k_{S_3}) * f_u(u_{S_3}) * f_\alpha(\alpha_{S_3})}{6} = \frac{14 * 4 * 7{,}9}{6} = 73{,}9$$

Wartość ryzyka r_{S_4}:

System S_4 należy do klasy bezpieczeństwa *C2* i do klasy istotności *III*. Wartość realizacji wymagań bezpieczeństwa α_{S_4} wynosi 81,25%, zatem:

$$r_{S_4} = \frac{f_k(k_{S_4}) * f_u(u_{S_4}) * f_\alpha(\alpha_{S_4})}{6} = \frac{7 * 3 * 1{,}9}{6} = 6{,}6$$

Wartość ryzyka r_{S_5}:

System S_5 należy do klasy bezpieczeństwa *B4* i do klasy istotności *III*. Wartość realizacji wymagań bezpieczeństwa α_{S_5} wynosi 29,17%, zatem:

$$r_{S_5} = \frac{f_k(k_{S_5}) * f_u(u_{S_5}) * f_\alpha(\alpha_{S_5})}{6} = \frac{9 * 3 * 7{,}1}{6} = 31{,}9$$

Wartość ryzyka r_{S_6} :

System S_6 należy do klasy bezpieczeństwa *D1* i do klasy istotności *IV*. Wartość realizacji wymagań bezpieczeństwa α_{S_6} wynosi 77,22%, zatem:

$$r_{S_6} = \frac{f_k(k_{S_6}) * f_u(u_{S_6}) * f_\alpha(\alpha_{S_6})}{6} = \frac{4 * 2 * 2{,}8}{6} = 3{,}7$$

5.3.2 Wartość ryzyka $r_{\max}$ dla systemów informatycznych przedsiębiorstwa telekomunikacyjnego

Wartość ryzyka maksymalnego $r_{\max}$ jest najwyższą możliwą wartością ryzyka związanego z bezpieczeństwem systemów informatycznych przedsiębiorstwa telekomunikacyjnego.

Na podstawie dokonanej klasyfikacji systemów informatycznych przedsiębiorstwa telekomunikacyjnego wiadomo, że:

- wartość $\max\left(f_k(k_{S_i})\right)$ jest równa odpowiednikowi klasy bezpieczeństwa systemu, który dla klasy *A2* wynosi 15,
- wartość $\max\left(f_u(u_{S_i})\right)$ jest równa odpowiednikowi klasy istotności, który dla grupy *I* wynosi 5,
- wartość $f_\alpha(0\%)$ jest równa odpowiednikowi 0% realizacji wymagań bezpieczeństwa czyli wynosi 10^{200}.

Ostatecznie wartość ryzyka $r_{\max}$ dla systemów informatycznych przedsiębiorstwa telekomunikacyjnego wynosi:

$$r_{\max} = \frac{\max\left(f_k(k_{S_i})\right) * \max\left(f_u(u_{S_i})\right) * f_\alpha(0\%)}{6} = \frac{15 * 5 * 10}{6} = 125$$

[200] Jest to równoznaczne z niespełnieniem ani jednego wymagania bezpieczeństwa.

5.3.3 Wartość ryzyka względnego R_{S_i} dla systemów informatycznych przedsiębiorstwa telekomunikacyjnego

Podstawiając wartości ryzyka r_{S_i} dla poszczególnych systemów oraz wartość $r_{\max}$ do wzoru *Wzór - 10,* otrzymujemy wartość względną ryzyka R_{S_i} związanego z bezpieczeństwem systemu informatycznego dla poszczególnych systemów. Wartości te wynoszą:

- dla systemu S_1:

$$R_{S_1} = \frac{r_{S_1}}{r_{\max}} * 100\% = \frac{75}{125} * 100\% = 60\%,$$

- dla systemu S_2:

$$R_{S_2} = \frac{r_{S_2}}{r_{\max}} * 100\% = \frac{69,9}{125} * 100\% = 56\%,$$

- dla systemu S_3:

$$R_{S_3} = \frac{r_{S_3}}{r_{\max}} * 100\% = \frac{73,9}{125} * 100\% = 59\%,$$

- dla systemu S_4:

$$R_{S_4} = \frac{r_{S_4}}{r_{\max}} * 100\% = \frac{6,6}{125} * 100\% = 5\%,$$

- dla systemu S_5:

$$R_{S_5} = \frac{r_{S_5}}{r_{\max}} * 100\% = \frac{31,9}{125} * 100\% = 26\%,$$

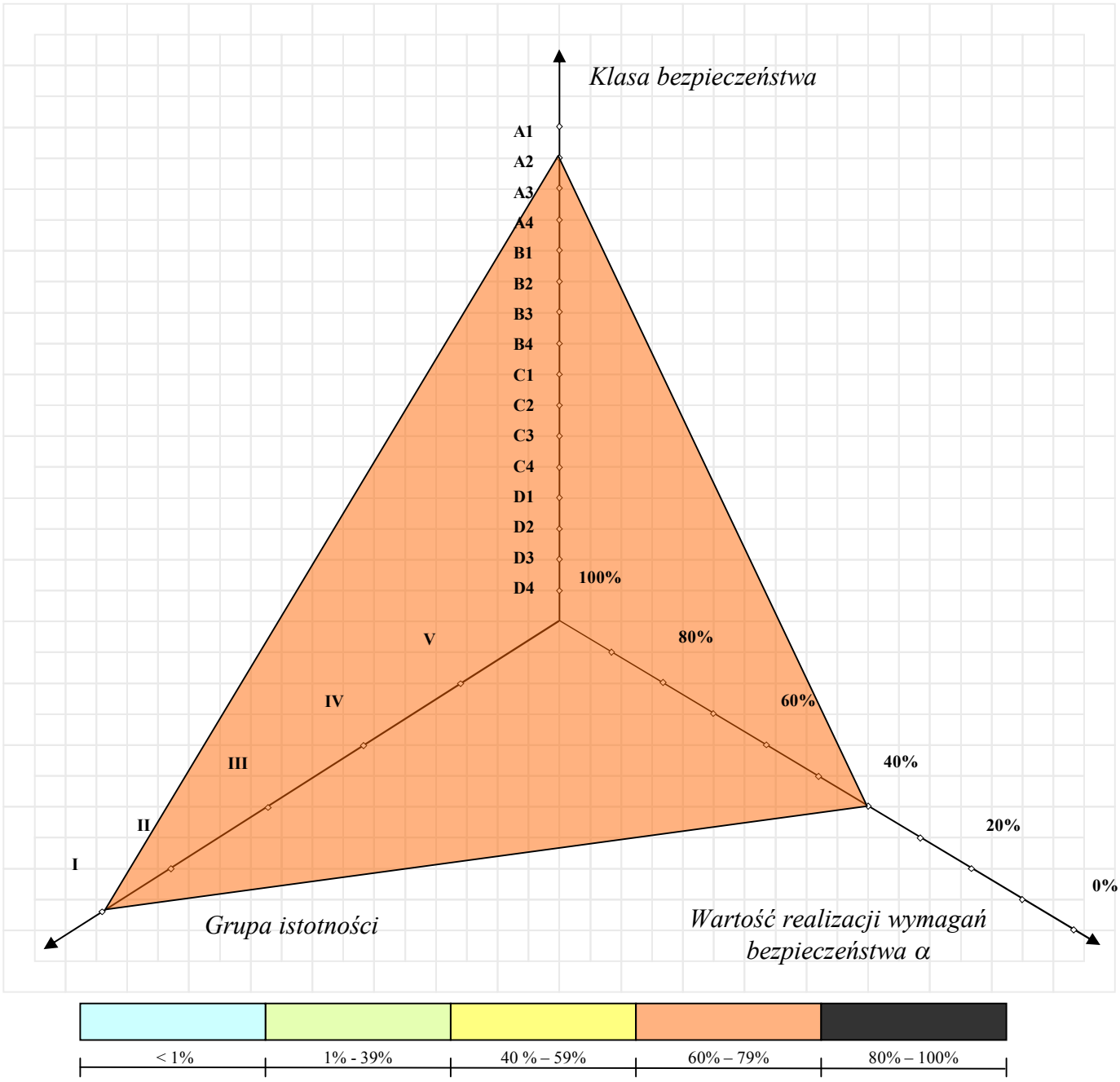
- dla systemu S_6:

$$R_{S_6} = \frac{r_{S_6}}{r_{\max}} * 100\% = \frac{3,7}{125} * 100\% = 3\% .$$

5.3.4 Reprezentacja graficzna poziomów ryzyka oraz ryzyka względnego systemów informatycznych przedsiębiorstwa telekomunikacyjnego

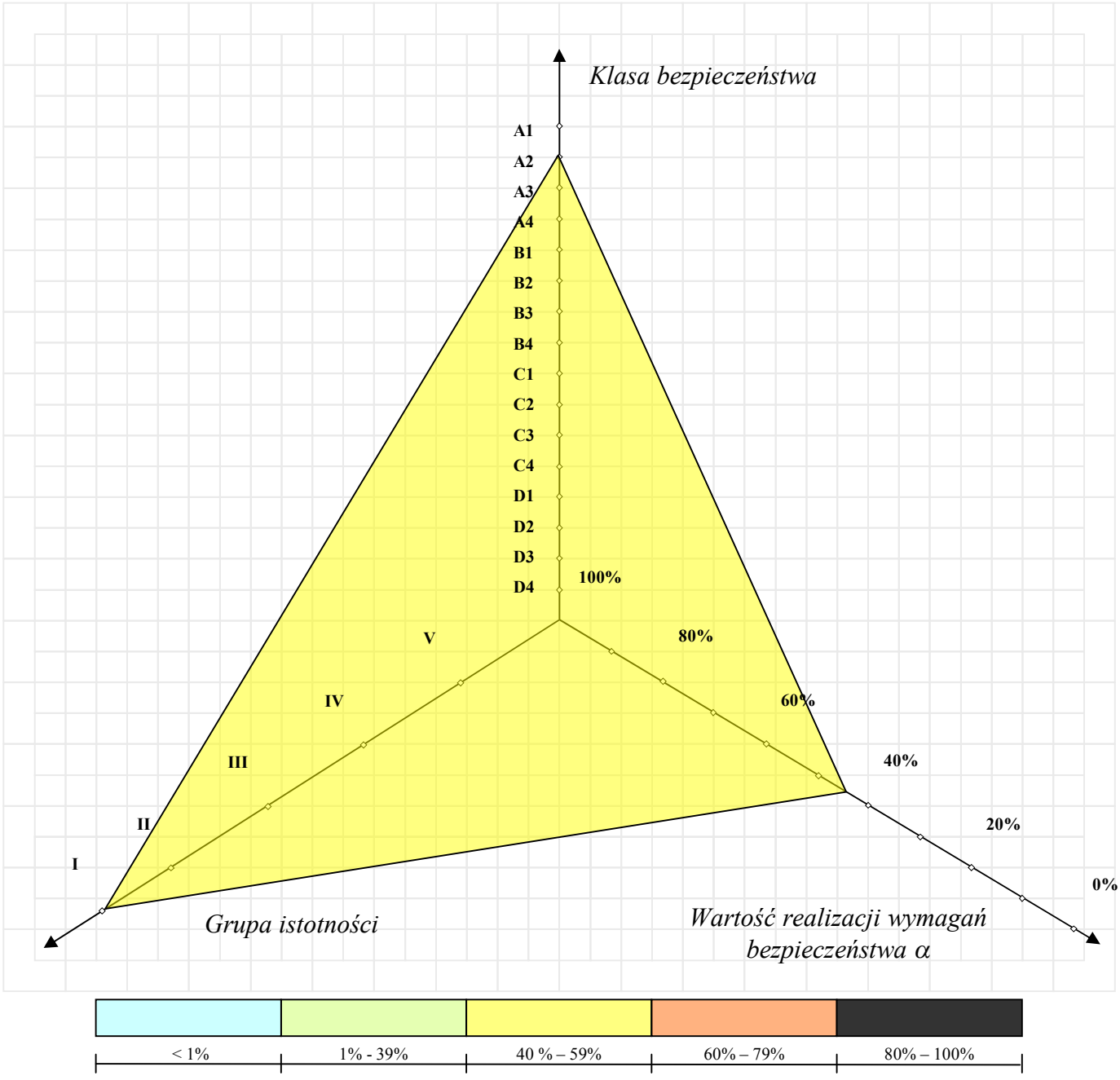
Rysunki: Rysunek 5.3. - 10, Rysunek 5.3. - 11, Rysunek 5.3. - 12, Rysunek 5.3. - 13, Rysunek 5.3. - 14, Rysunek 5.3. - 15 przedstawiają graficzną reprezentację wartości ryzyka oraz ryzyka względnego systemów informatycznych przedsiębiorstwa telekomunikacyjnego.

Nazwa systemu - S_1	Klasa bezpieczeństwa systemu – A2	Grupa Istotności - I
Wartość realizacji wymagań bezpieczeństwa - $\alpha_1 = 40\%$		Wartość ryzyka - $r_1 = 75$
Wartość względna ryzyka $R_1 = 60\%$		



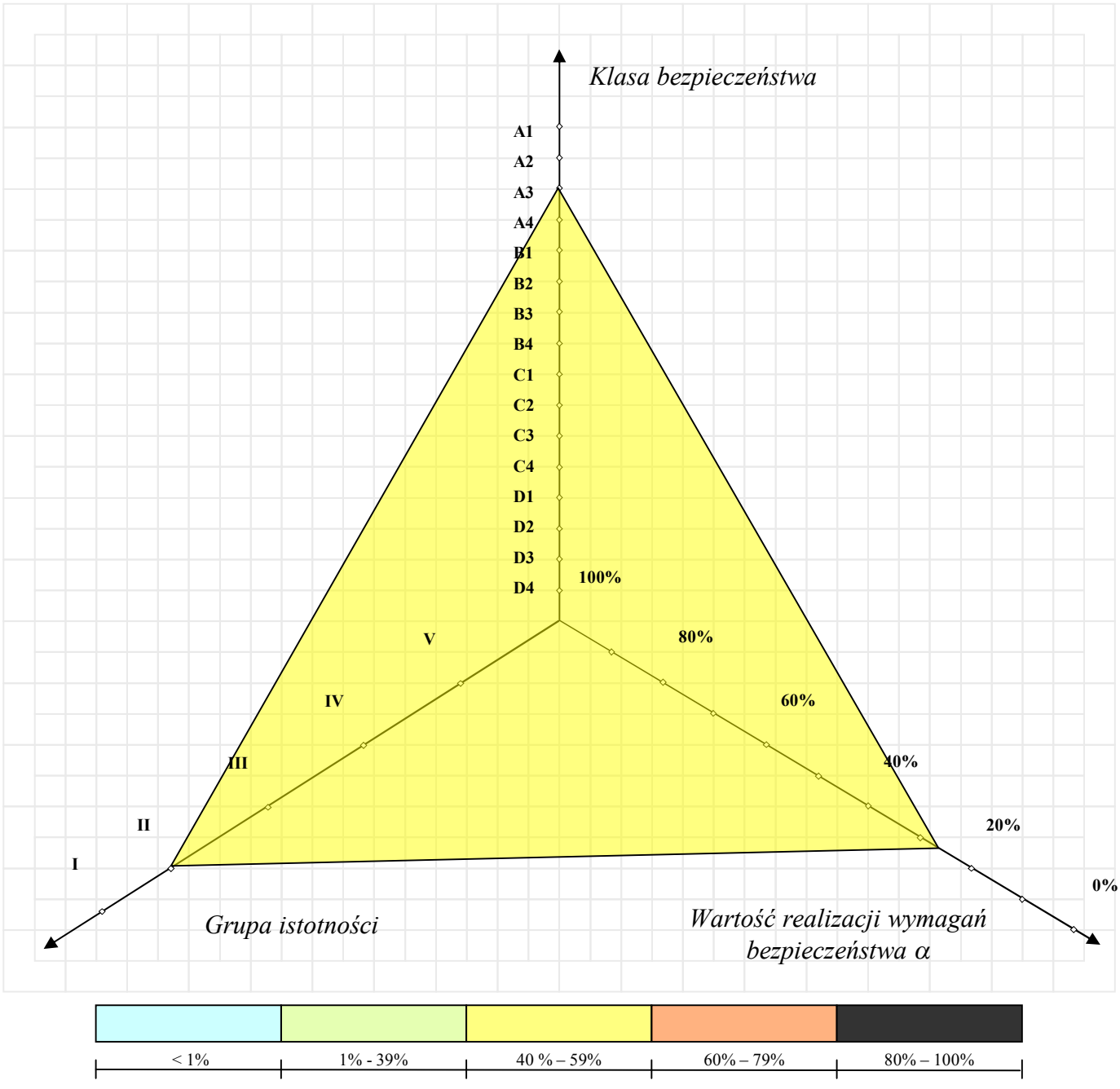
Rysunek 5.3. - 10. Graficzna reprezentacja wartości ryzyka r_{S_1} wraz z kolorem odpowiednim dla poziomu ryzyka względnego R_{S_1}

Nazwa systemu – S_2	Klasa bezpieczeństwa systemu – A2	Grupa Istotności - I
Wartość realizacji wymagań bezpieczeństwa - $\alpha_2 = 44{,}12\%$		Wartość ryzyka - $r_2 = 69{,}9$
Wartość względna ryzyka $R_2 = 56\%$		



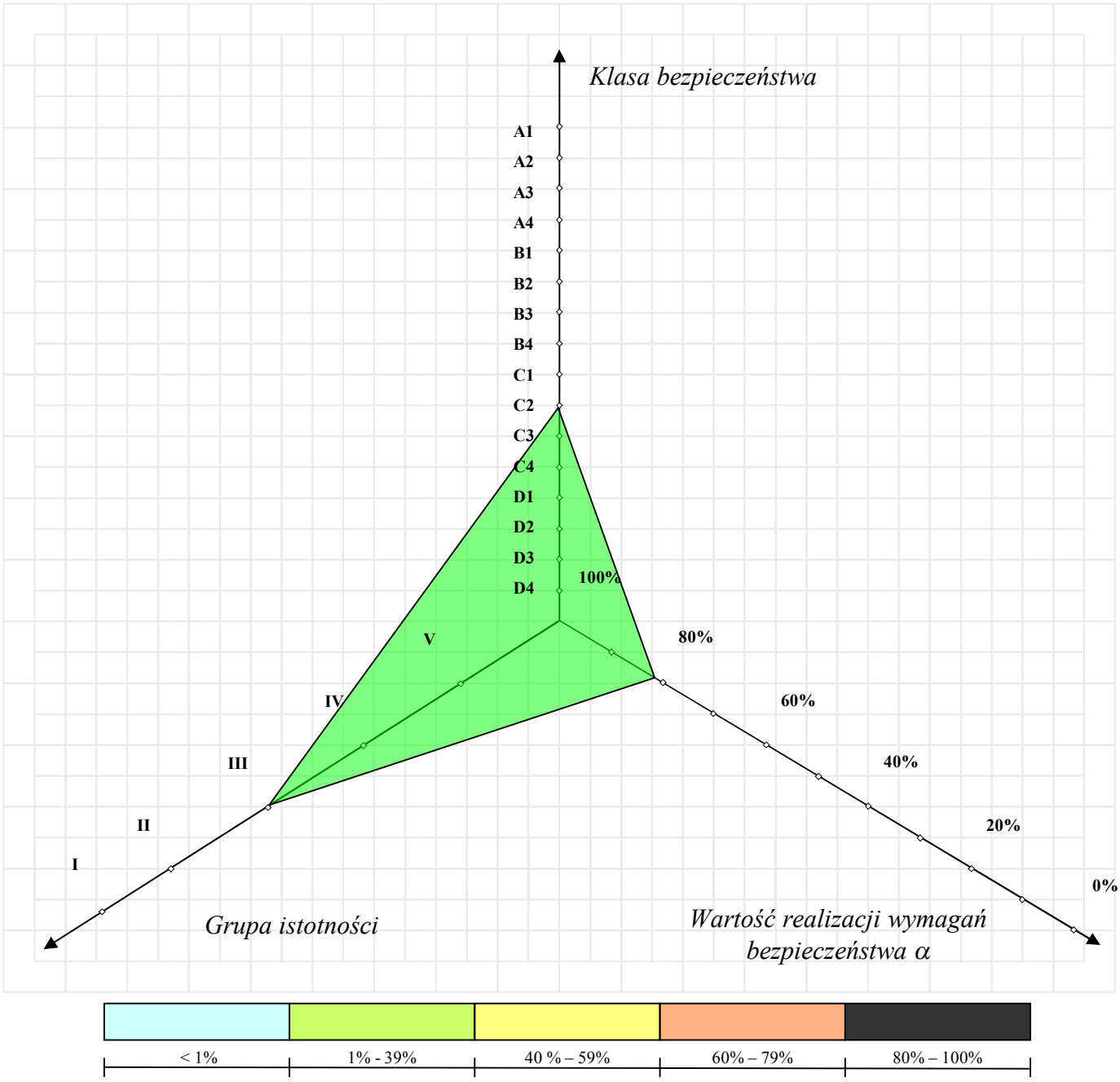
Rysunek 5.3. - 11. Graficzna reprezentacja wartości ryzyka r_{S_2} wraz z kolorem odpowiednim dla poziomu ryzyka względnego R_{S_2}

Nazwa systemu – S_3	Klasa bezpieczeństwa systemu – A3	Grupa Istotności - II
Wartość realizacji wymagań bezpieczeństwa - α_3 = 20,83%		Wartość ryzyka - r_3 = 73,9
Wartość względna ryzyka R_3 = 59%		



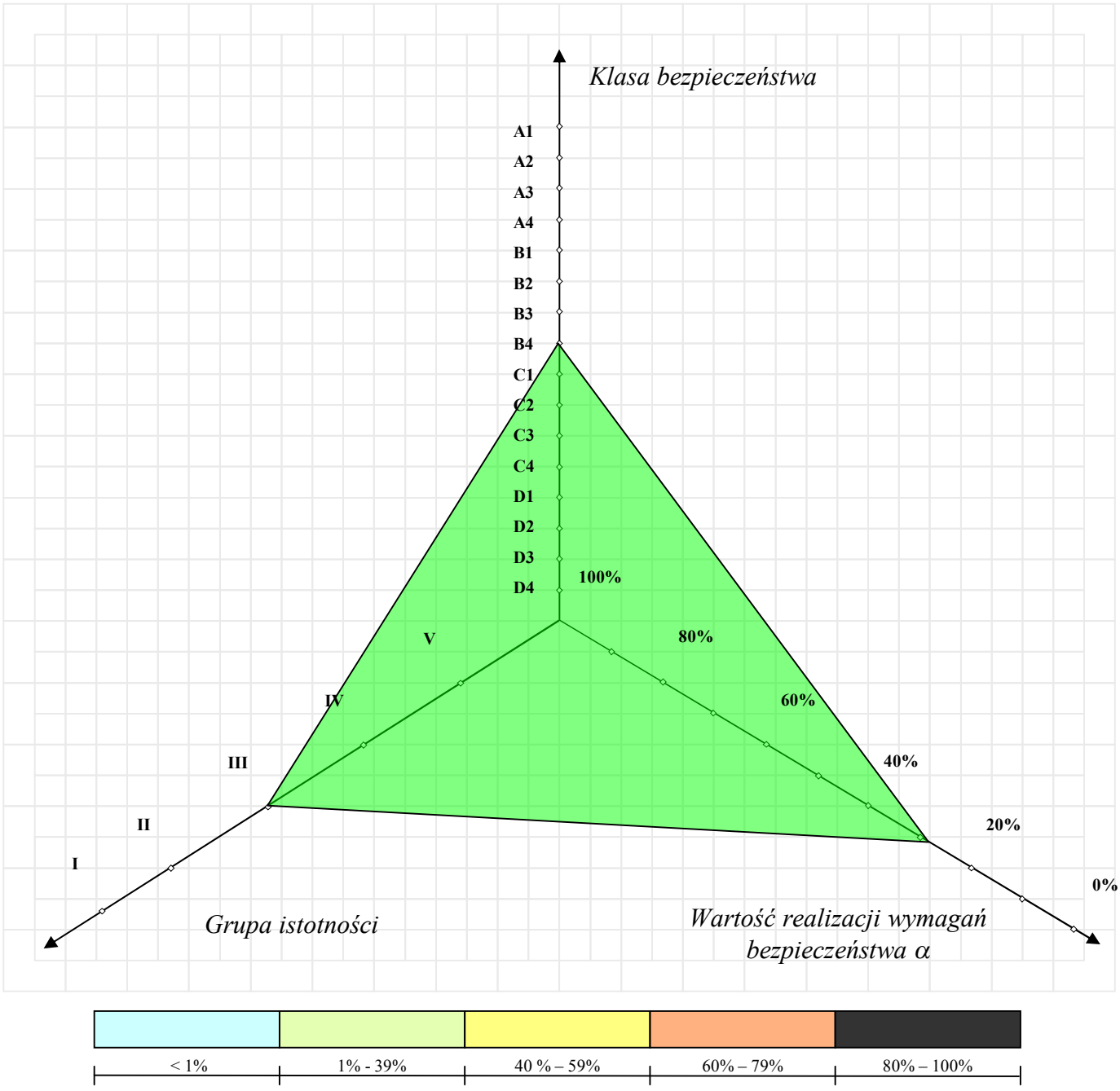
Rysunek 5.3. - 12. Graficzna reprezentacja wartości ryzyka r_{S_3} wraz z kolorem odpowiednim dla poziomu ryzyka względnego R_{S_3}

Nazwa systemu – S_4	Klasa bezpieczeństwa systemu - C2	Grupa Istotności - III
Wartość realizacji wymagań bezpieczeństwa - $\alpha_4 = 81{,}25\%$		Wartość ryzyka - $r_4 = 6{,}6$
Wartość względna ryzyka $R_4 = 5\%$		



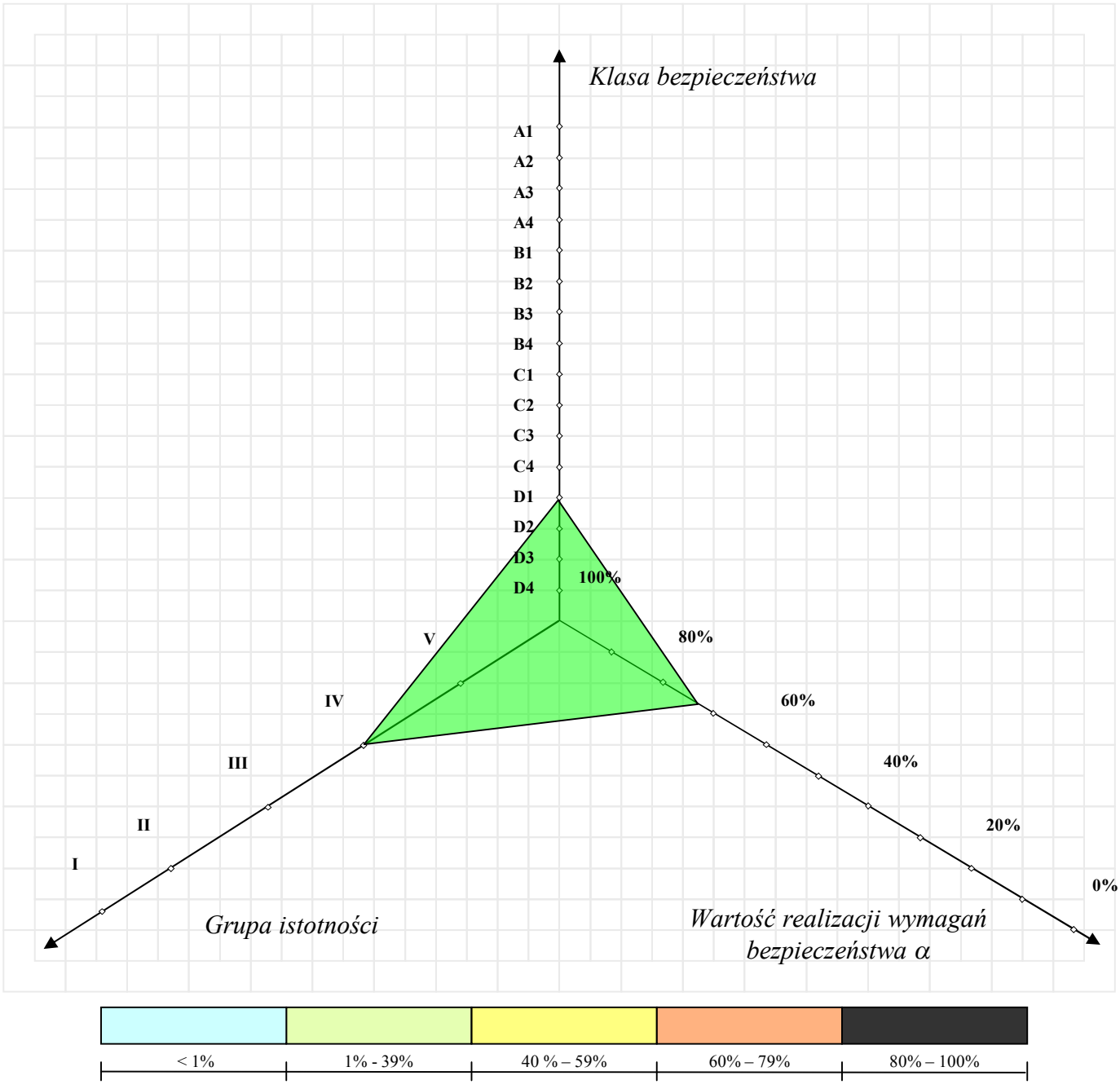
Rysunek 5.3. - 13. Graficzna reprezentacja wartości ryzyka r_{S_4} wraz z kolorem odpowiednim dla poziomu ryzyka względnego R_{S_4}

Nazwa systemu – S_5	Klasa bezpieczeństwa systemu – B4	Grupa Istotności - III
Wartość realizacji wymagań bezpieczeństwa - α_5 = 29,17%		Wartość ryzyka - r_5 = 31,9
Wartość względna ryzyka R_5 = 26%		



Rysunek 5.3. - 14. Graficzna reprezentacja wartości ryzyka r_{S_5} wraz z kolorem odpowiednim dla poziomu ryzyka względnego R_{S_5}

Nazwa systemu – S_6	Klasa bezpieczeństwa systemu – D1	Grupa Istotności - IV
Wartość realizacji wymagań bezpieczeństwa - $\alpha_6 = 72{,}22\%$		Wartość ryzyka - $r_6 = 3{,}7$
Wartość względna ryzyka $R_6 = 3\%$		



Rysunek 5.3. - 15. Graficzna reprezentacja wartości ryzyka r_{S_6} wraz z kolorem odpowiednim dla poziomu ryzyka względnego R_{S_6}

5.3.5 Analiza graficzna poziomów ryzyka względnego systemów informatycznych przedsiębiorstwa telekomunikacyjnego dla poszczególnych klas bezpieczeństwa oraz istotności

Dla poszczególnych klas bezpieczeństwa oraz klas istotności można obecnie dokonać analizy graficznej ryzyk systemów informatycznych przedsiębiorstwa telekomunikacyjnego.

Tabela 5.2. - 22 przedstawia przynależność poszczególnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego do klas istotności i klas bezpieczeństwa.

	System informatyczny S_i					
	S_1	S_2	S_3	S_4	S_5	S_6
Klasa bezpieczeństwa systemu informatycznego	*A2*	*A2*	*A3*	*C2*	*B4*	*D1*
Klasa istotności systemu informatycznego	*I*	*I*	*II*	*III*	*III*	*IV*

Tabela 5.2. - 22. Przynależność systemów informatycznych przedsiębiorstwa telekomunikacyjnego do klas istotności i klas bezpieczeństwa (macierz klasyfikacji systemów informatycznych)

Tabela 5.2. - 23. przedstawia wartości pory obliczone wcześniej dla poszczególnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego.

System	Realizacja wymagań bezpieczeństwa α_{S_i}	Wartość ryzyka r_{S_i}	Wartości ryzyka względnego R_{S_i}
S_1	40,00%	75,0	60%
S_2	44,12%	69,9	56%
S_3	20,83%	73,9	59%
S_4	81,25%	6,6	5%
S_5	29,17%	31,9	26%
S_6	72,22%	3,7	3%

Tabela 5.2. - 23. Wartości realizacji wymagań bezpieczeństwa α_{S_i}, ryzyka r_{S_i} oraz ryzyka względnego R_{S_i} dla systemów informatycznych przedsiębiorstwa telekomunikacyjnego

Aby odnieść się do poszczególnych wartości ryzyk, należy obliczyć średnie wartości względne ryzyka klas bezpieczeństwa i grup istotności ($R_{sr(k)}$ i $R_{sr(u)}$). W tym celu należy dokonać pogrupowania systemów według atrybutów klasy bezpieczeństwa oraz klasy istotności, które są przedstawione w tabelach: Tabela 5.2. - 24 oraz Tabela 5.2. - 25.

Klasa bezpieczeństwa	System	Wartości ryzyk względnych R_{S_i} [%]	Wartość średnia ryzyka $R_{sr(k)}$ dla klasy [%]
A2	S_1 ; S_2	60 ; 56	**58**
A3	S_3	59	**59**
C2	S_4	5	**5**
B4	S_5	26	**26**
D1	S_6	3	**3**

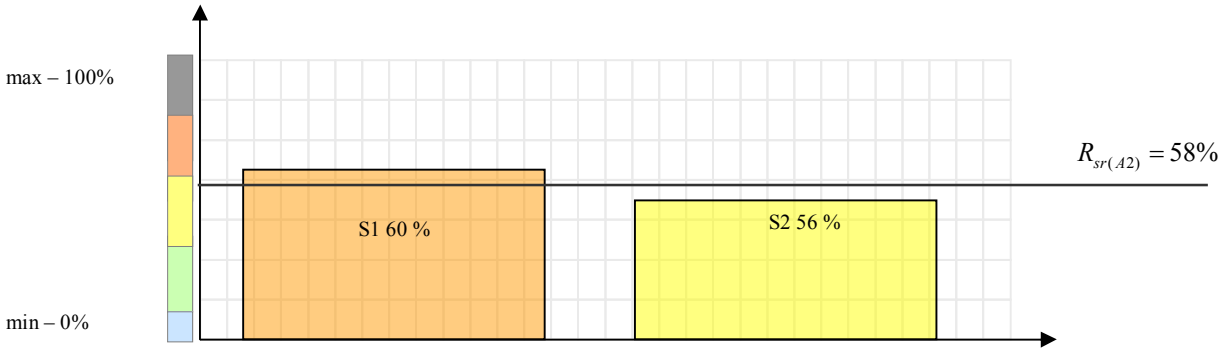
Tabela 5.2. - 24. Wartości ryzyk względnych R_{S_i} oraz wartości średnie ryzyka $R_{sr(k)}$ dla klas bezpieczeństwa i systemów informatycznych przedsiębiorstwa telekomunikacyjnego

Klasa istotności	System	Wartości ryzyk względnych R_{S_i} [%]	Wartość średnia $R_{sr(u)}$ dla klasy [%]
I	S_1 ; S_2	60 ; 56	**58**
II	S_3	59	**59**
III	S_4 ; S_5	5 ; 26	**15,5**
IV	S_6	3	**3**

Tabela 5.2. - 25. Wartości ryzyk względnych R_{S_i} oraz wartości średnie ryzyka $R_{sr(u)}$ dla klas istotności i systemów informatycznych przedsiębiorstwa telekomunikacyjnego

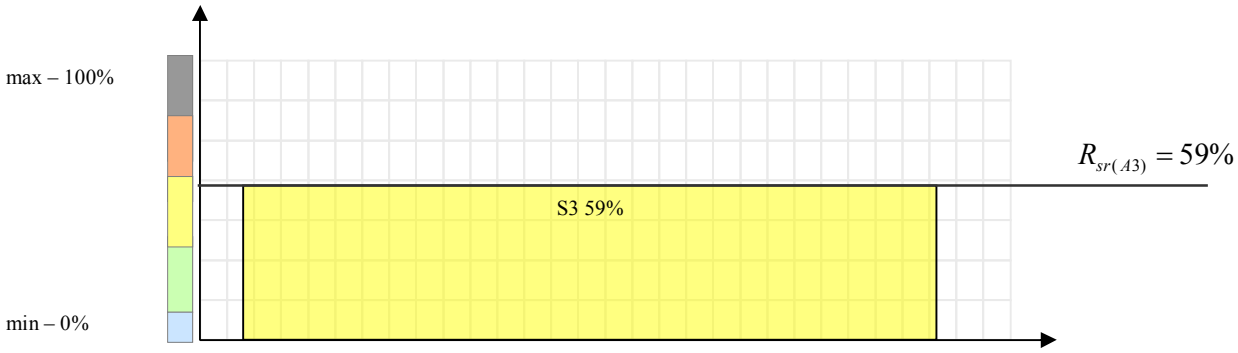
Rysunki: Rysunek 5.3. - 16, Rysunek 5.3. - 17, Rysunek 5.3. - 18, Rysunek 5.3. - 19, Rysunek 5.3. - 20, przedstawiają graficzne reprezentacje ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego, należących do poszczególnych klas bezpieczeństwa.

KLASA BEZPIECZEŃSTWA – **A2**	System S_1 , S_2
Względna wartość ryzyka R_{S1} = 60% Względna wartość ryzyka R_{S2} = 56%	Średnia wartość względna ryzyka dla systemów należących do klasy bezpieczeństwa A2 wynosi $R_{sr(A2)} = 58\%$



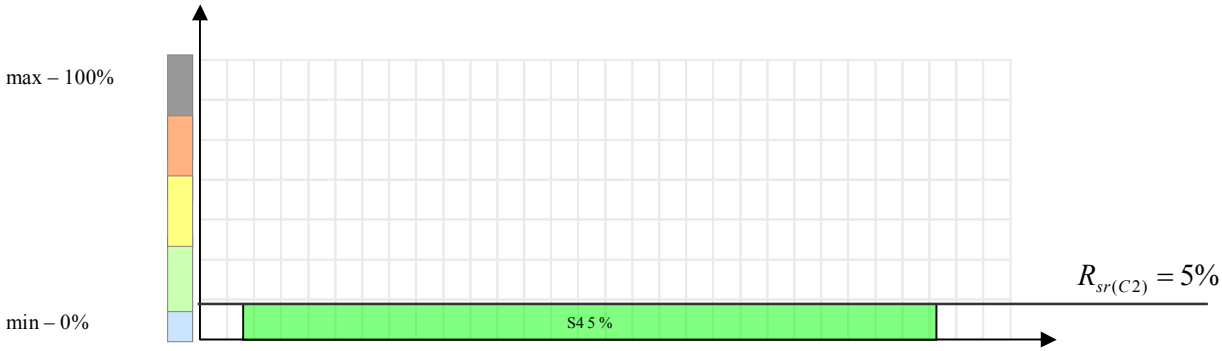
Rysunek 5.3. - 16. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego, należących do klasy bezpieczeństwa *A2*

KLASA BEZPIECZEŃSTWA – **A3**	System S_3
Względna wartość ryzyka R_{S3} = 59%	Średnia wartość względna ryzyka dla systemów należących do klasy bezpieczeństwa A3 wynosi $R_{sr(A3)} = 59\%$



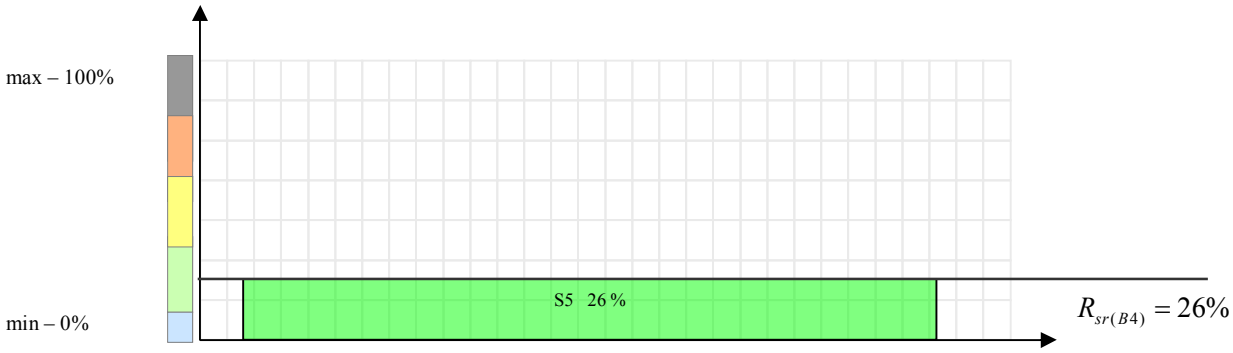
Rysunek 5.3. - 17. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego, należących do klasy bezpieczeństwa *A3*

KLASA BEZPIECZEŃSTWA – **C2**	System S_4
Względna wartość ryzyka R_{S4} = 5%	Średnia wartość względna ryzyka dla systemów należących do klasy bezpieczeństwa C2 wynosi $R_{sr(C2)} = 5\%$



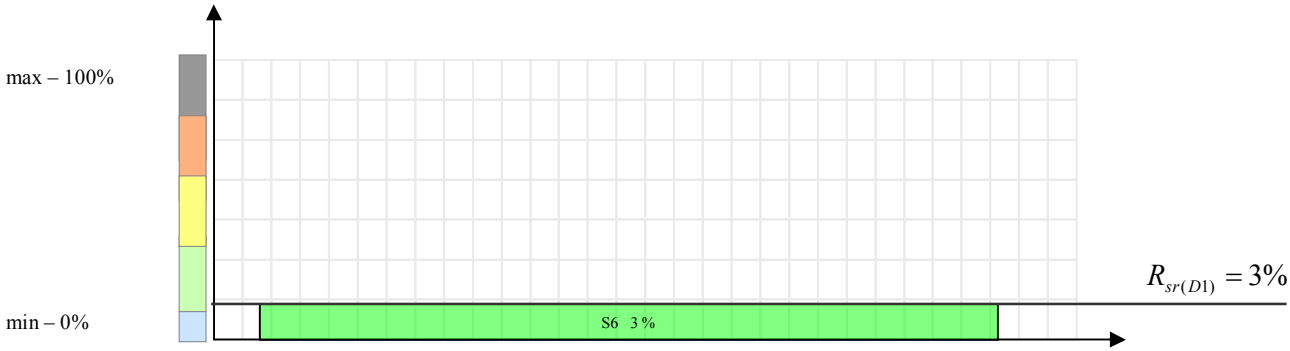
Rysunek 5.3. - 18. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego należących do klasy bezpieczeństwa *C2*

KLASA BEZPIECZEŃSTWA – **B4**	System S_5
Względna wartość ryzyka R_{S5} = 26%	Średnia wartość względna ryzyka dla systemów należących do klasy bezpieczeństwa B4 wynosi $R_{sr(B4)} = 26\%$



Rysunek 5.3. - 19. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego, należących do klasy bezpieczeństwa *B4*

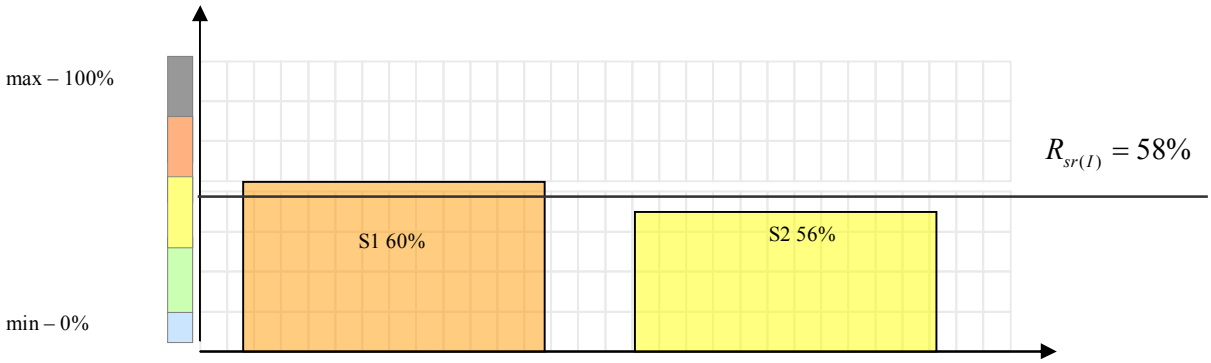
KLASA BEZPIECZEŃSTWA – **D1**	System S_6
Względna wartość ryzyka R_{S6} = 3%	Średnia wartość względna ryzyka dla systemów należących do klasy bezpieczeństwa D1 wynosi $R_{sr(D1)} = 3\%$



Rysunek 5.3. - 20. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego, należących do klasy bezpieczeństwa *D1*

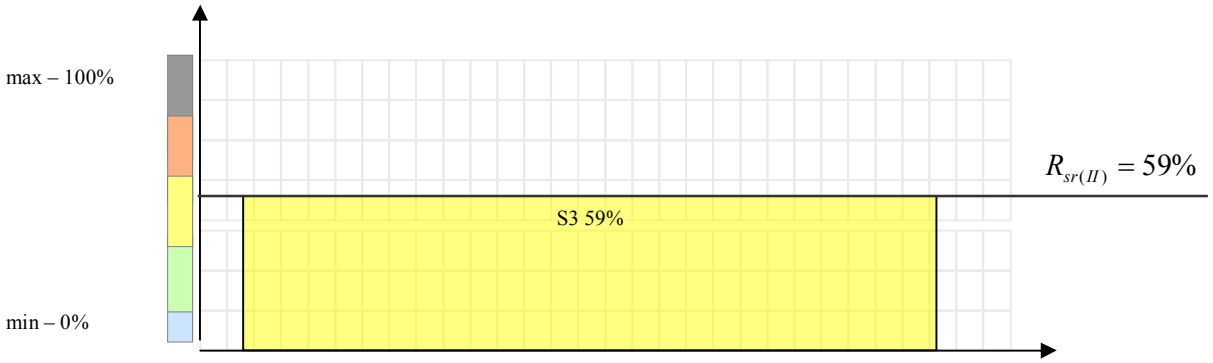
Rysunki: Rysunek 5.3. - 21, Rysunek 5.3. - 22, Rysunek 5.3. - 23, Rysunek 5.3. - 24 przedstawiają graficzne reprezentacje ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego należących do poszczególnych klas istotności.

GRUPA ISTOTNOŚCI – **I**	System S_1 , S_2
Wartość ryzyka (względna) R_{S1} = 60% Wartość ryzyka (względna) R_{S2} = 56%	Średnia wartość ryzyka (względnego) dla systemów należących do grupy istotności I - $R_{sr(I)} = 58\%$



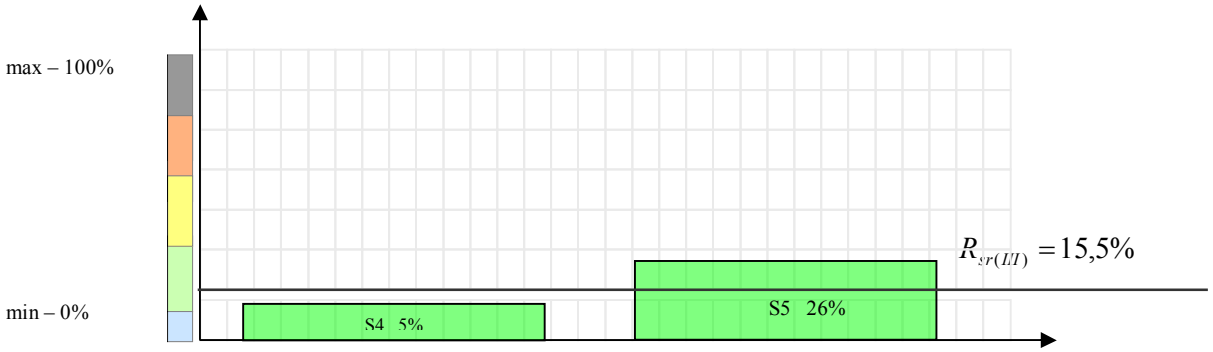
Rysunek 5.3. - 21. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego należących do klasy istotności *I*

GRUPA ISTOTNOŚCI – **II**	System S_3
Wartość ryzyka (względna) $R_{S3} = 59\%$	Średnia wartość ryzyka (względnego) dla systemów należących do grupy istotności II - $R_{sr(II)} = 59\%$



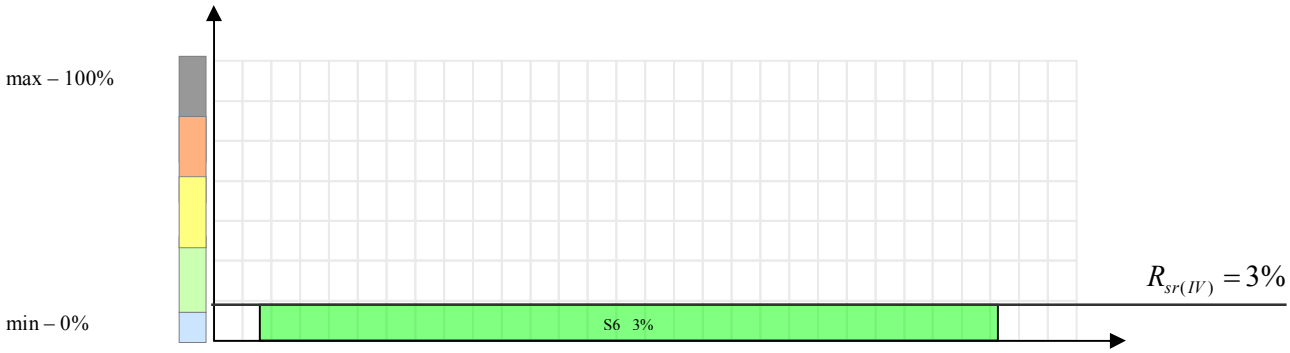
Rysunek 5.3. - 22. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego należących do klasy istotności *II*

GRUPA ISTOTNOŚCI – **III**	System S_4 , S_5
Wartość ryzyka (względna) $R_{S4} = 5\%$ Wartość ryzyka (względna) $R_{S5} = 26\%$	Średnia wartość ryzyka (względnego) dla systemów należących do grupy istotności III - $R_{sr(III)} = 15{,}5\%$



Rysunek 5.3. - 23. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego należących do klasy istotności *III*

GRUPA ISTOTNOŚCI – **IV**	System S_6
Wartość ryzyka (względna) $R_{S6} = 3\%$	Średnia wartość ryzyka (względnego) dla systemów należących do grupy istotności IV - $R_{sr(IV)} = 3\%$



Rysunek 5.3. - 24. Graficzna reprezentacja ryzyk względnych systemów informatycznych przedsiębiorstwa telekomunikacyjnego należących do klasy istotności *IV*

Na koniec części drugiej metody ORBI, należy obliczyć wartość ryzyka średniego $\Re_{S(O)}$ dla wszystkich systemów informatycznych przedsiębiorstwa.

$$\Re_{S(O)} = \frac{60 + 56 + 59 + 5 + 26 + 3}{6} = 34{,}83\%$$

Ostatecznie wyniki oceny ryzyka dla przedsiębiorstwa telekomunikacyjnego zostały zebrane w Tabeli 5.2. - 26.

		System informatyczny S_i					
		S_1	S_2	S_3	S_4	S_5	S_6
Ryzyko r_{S_i} związane z bezpieczeństwem systemu informatycznego S_i		75	69,9	73,9	6,6	31,9	3,7
Ryzyko maksymalne $r_{\max}$ dla systemów informatycznych należących do zbioru $S(O)$		125					
Ryzyko względne R_{S_i} związane z bezpieczeństwem systemu informatycznego S_i		60%	56%	59%	5%	26%	3%
Ryzyko średnie $\Re_{S(O)}$ związane z bezpieczeństwem systemów informatycznych należących do zbioru $S(O)$		34,83%					
Klasa bezpieczeństwa	$R_{sr(k)}$ – ryzyko średnie dla klasy bezpieczeństwa	S_1	S_2	S_3	S_4	S_5	S_6
A2	58						
A3	59						
C2	5						
B4	26						
D1	3						
Klasa istotności	$R_{sr(u)}$ – ryzyko średnie dla klasy istotności	S_1	S_2	S_3	S_4	S_5	S_6
I	58						
II	59						
III	15,5						
IV	3						

Tabela 5.2. - 26. Tabela ryzyk systemów informatycznych przedsiębiorstwa telekomunikacyjnego

5.4 Podsumowanie przykładu użycia metody ORBI.

Przedstawiony w tym rozdziale przykład przedsiębiorstwa telekomunikacyjnego zobrazował sposób użycia metody ORBI do wyznaczenia wartości ryzyka związanego z bezpieczeństwem eksploatowanych w nim systemów informatycznych. Na tym przykładzie pokazano, że zgodnie z postulatami przedstawionymi w rozdziale 4.1, metoda ORBI:

1. Wyznacza wartość ryzyka związanego z bezpieczeństwem systemów informatycznych w sposób ilościowy na dany moment oceny, przy zastosowanych przez przedsiębiorstwo zabezpieczeniach dla poszczególnych systemów informatycznych. W przedstawionym w pracy przykładzie obrazuje to Tabela 5.2. - 26. Z przykładu wynika że zastosowane zabezpieczenia są odpowiednie dla systemów S_4, S_5 i S_6 oraz niewystarczające dla systemów S_2 i S_3. W przypadku systemu S_1 zastosowane zabezpieczenia są nieodpowiednie.
2. Wyznacza obiektywną wartość ryzyka związanego z bezpieczeństwem systemów informatycznych, nie uzależniając jej od prawdopodobieństwa wystąpienia zagrożeń lub danych historycznych. W przedstawionym przykładzie wskazano w sposób jawny wszystkie składowe mające wpływ na wartość ryzyka związanego z bezpieczeństwem systemów informatycznych przedsiębiorstwa.
3. Wyznacza porównywalne wartości ryzyka związanego z bezpieczeństwem systemów informatycznych w skali przedsiębiorstwa oraz przedsiębiorstw co najmniej z tej samej branży. Z przedstawionego przykładu widać, że wartości ryzyka związanego z bezpieczeństwem poszczególnych systemów informatycznych przedsiębiorstwa są porównywalne między sobą. Ta sama zależność dotyczy całej branży telekomunikacyjnej.
4. Wyznacza wartość ryzyka związanego z bezpieczeństwem systemów informatycznych na dany moment oceny w możliwie najprostszy sposób. W zależności od zmian zabezpieczeń systemów informatycznych przykładowego przedsiębiorstwa wartości ryzyka wyznaczonych w przykładzie byłyby różne.

Ostatnim postulatem, o którym mowa w rozdziale 4.1, jest zrozumiałość wyników oceny ryzyka związanego z bezpieczeństwem systemów informatycznych zarówno dla zakładu ubezpieczeń, jak i dla przedsiębiorstwa. Innymi słowy zrozumiałość tę można określić możliwością wykorzystania wyników działania metody ORBI przez te dwa podmioty.

W przypadku przedsiębiorstwa sama znajomość stanu bezpieczeństwa systemów informatycznych stanowi wartość. Dodatkowa szczegółowa wiedza na temat wartości ryzyk związanych z bezpieczeństwem poszczególnych systemów informatycznych przedsiębiorstwa daje podstawę do zarządzania tymi ryzykami. Znając wartość ryzyk związanych z bezpieczeństwem systemów informatycznych można, po pierwsze, zastosować odpowiednią strategię postępowania z ryzykiem. Zakładając, że interesuje nas w przypadku tego przedsiębiorstwa telekomunikacyjnego strategia minimalizacji ryzyka, wówczas bazując na wynikach zastosowanie metody ORBI należy zastanowić się, które z wymagań bezpieczeństwa są niespełnione przez systemy. W szczególności należy przeanalizować przypadek systemu S_1, gdyż wartość ryzyka w przypadku tego systemu jest największa. Z perspektywy przedsiębiorstwa może okazać się, że spełnienie określonego lub określonych wymagań w znaczny sposób obniży wartość ryzyka średniego dla wszystkich systemów informatycznych przedsiębiorstwa. Po drugie, na podstawie wyników porównania poszczególnych klas istotności i klas bezpieczeństwa widać wyraźnie, że problem z wysoką wartością ryzyka dotyczy określonych klas systemów, tych dla których dostępność ma istotne znaczenie. Na podstawie analizy wyników zastosowania metody ORBI można dojść do wniosku, że w przykładowym przedsiębiorstwie telekomunikacyjnym albo istnieje konieczność inwestycji w rozwiązania zapewniające dostępność systemów informatycznych, albo pomimo ich istnienia są one nieefektywnie wykorzystywane.

W przypadku zakładu ubezpieczeń wyniki pochodzące z działania metody ORBI pozwalają na podjęcie decyzji o ubezpieczalności danego systemu informatycznego przedsiębiorstwa (lub systemów informatycznych) oraz warunkach takiego ubezpieczenia. Oczywiście decyzja ta musi być poprzedzona opracowaniem produktu ubezpieczeniowego, który będzie określał:

- parametry ryzyka związanego z bezpieczeństwem systemów informatycznych, po spełnieniu których zakład ubezpieczeń zaoferuje ubezpieczenie np.: maksymalna wartość ryzyka dla danego systemu informatycznego lub maksymalna wartość ryzyka średniego systemów informatycznych przedsiębiorstwa,
- parametry biznesowe takiego produktu jak składka i stopa ubezpieczeniowa oraz jej odniesienie do wartości systemów informatycznych przedsiębiorstwa, wysokość udziału własnego lub typ i wysokość franszyzy oferowanych klientom w relacji do wartości ryzyka średniego związanego z bezpieczeństwem systemów informatycznych przedsiębiorstwa oraz system zniżek i zwyżek składki w relacji

do wartości ryzyka wyznaczanego za pomocą metody ORBI. Ważnym elementem są też parametry produktu związane z wyłączeniem odpowiedzialności.

Analizując opisywane w rozdziale 3 tej rozprawy produkty ubezpieczeniowe DigiTech i NRI z perspektywy przedstawionej w przykładzie oceny ryzyka za pomocą metody ORBI można powiedzieć, że przy tak dokładnej znajomości wartości ryzyka związanego z bezpieczeństwem poszczególnych systemów informatycznych jest możliwe lepsze i dokładniejsze zdiagnozowanie przez zakłady ubezpieczeń ich ryzyka zawarcia umowy ubezpieczeniowej. Tym samym powiększeniu mogła by ulec suma pokrycia lub warunki ubezpieczenia (w tym wyłączenia odpowiedzialności).

Bez względu jednak na kształt i komplikację produktu ubezpieczeniowego, metoda ORBI oferuje zakładowi ubezpieczeń jednoznaczną i porównywalna wartość ryzyka związanego z bezpieczeństwem systemów informatycznych, co zostało przedstawione w przykładzie.

6 Wnioski

Metoda ORBI (**O**cena **R**yzyka **B**ezpieczeństwa systemów **I**nformatycznych), przedstawiona w tej rozprawie, umożliwia dokonanie oceny ryzyka związanego z bezpieczeństwem systemów informatycznych dowolnego przedsiębiorstwa. Za sprawą spełnienia postulatów przedstawionych w rozdziale 4.1 i zweryfikowanych przykładem zastosowania przedstawionym w rozdziale 5, można stwierdzić, że jest odpowiedzią na potrzeby zakładów ubezpieczeń.

Najważniejsze szczegółowe osiągnięcia tej rozprawy to:

1. Przegląd i ocena istniejących metod oceny ryzyka związanego z bezpieczeństwem systemów informatycznych
2. Przegląd i ocena z perspektywy problemu badawczego oferty rynkowej zarówno krajowej, jak i międzynarodowej w zakresie ubezpieczeń systemów informatycznych.
3. Analiza problemu braku oferty ubezpieczeń systemów informatycznych oraz identyfikacja postulatów odpowiedniej dla potrzeb ubezpieczenia metody oceny ryzyka związanego z bezpieczeństwem systemów informatycznych.
4. Opracowanie metody ORBI
    - części pierwszej dokonującej w szczególności klasyfikacji systemów informatycznych przedsiębiorstwa,
    - części drugiej wyznaczającej wartość ryzyka związanego z bezpieczeństwem poszczególnych systemów informatycznych jak również wartości względnych i średnich.
5. Przykład użycia metody ORBI wraz z przedstawieniem wybranych analiz wyników oceny ryzyka związanego z bezpieczeństwem systemów informatycznych.

Zastosowanie metody ORBI dla potrzeb oceny ryzyka związanego z bezpieczeństwem systemów informatycznych otwiera nowe możliwości przed zakładami ubezpieczeń tworzenia nowych, oczekiwanych przez rynek produktów ubezpieczeniowych. Dotyczy to zarówno przygotowania oferty dla branż jak i specyficznych klas bezpieczeństwa systemów informatycznych. Zakład ubezpieczeń posiadając narzędzie jakim jest ORBI, może w sposób

selektywny oferować swoje produkty uznając, że określone systemy lub klasy bezpieczeństwa systemów informatycznych nie będą mogły być objęte ubezpieczeniem (ocena ryzyka przez zakład ubezpieczeń)[201]. Dodatkowo dzięki możliwością analizy wyników przedstawionych w podsumowaniu przykładu, w rozdziale 5.4 tej rozprawy, zakład ubezpieczeń może tworzyć indywidualne oferty dla poszczególnych przedsiębiorstw rekomendując bardzo konkretne działania jakie powinno podjąć przedsiębiorstwo w celu podniesienia poziomu bezpieczeństwa swoich systemów informatycznych. Te możliwości dają zakładowi ubezpieczeń dodatkowo argument i rolę „partnera biznesowego".

Metoda ORBI może być również z powodzeniem wykorzystywana przez przedsiębiorstwa w celu systematycznego zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych lub szerzej z ryzykiem operacyjnym. Jest możliwe rozwinięcie metody ORBI o kolejną część. Częścią tą może być metoda analizy ryzyka polegająca na dokonaniu symulacji zmian wartości wymagań bezpieczeństwa i wpływu tych zmian na wartości ryzyka związanego z bezpieczeństwem pojedynczego systemu informatycznego, jak również wszystkich systemów informatycznych przedsiębiorstwa. Dzięki tej części przedsiębiorstwo mogłoby w sposób optymalny ekonomicznie dobierać kolejne zabezpieczenia dla swych systemów informatycznych posiadając wiedzę o ich wpływie na ogólny poziom przedmiotowego ryzyka.

Cechy, jakie posiada metoda ORBI, oraz konstrukcja, jaka posłużyła do jej opracowania, daje duże możliwości jej rozbudowy. Zakład ubezpieczeń chcąc wykorzystać metodę ORBI może dokonać zmian wartości poszczególnych klas istotności i bezpieczeństwa dostosowując je do indywidualnych potrzeb biznesowych lub szczególnych wymagań prawnych, gdyby takie pojawiły się w przyszłości. Dzięki przyjętemu standardowi definiującemu wymagania bezpieczeństwa, metoda ORBI jest powszechnie zrozumiała zarówno po stronie ocenianych przedsiębiorstw, jak i zakładów ubezpieczeń. Niemniej jednak i tu istnieją możliwości rozwoju. W zależności od preferencji zakładu ubezpieczeń jest możliwe zmienienie standardu odniesienia w zakresie wymagań bezpieczeństwa na inny. Należy jednak pamiętać o zachowaniu pewnych cech jaki posiada standard BS 7799 -2 przyjęty w metodzie.

[201] Reps, S. Zawieranie umów ubezpieczenia odbiegających od treści ogólnych warunków ubezpieczeń, Prawo Asekuracyjne, 1998 nr 2 [98]

Przedstawione w rozprawie zastosowanie metody ORBI dotyczy funkcjonujących w przedsiębiorstwie systemów informatycznych. W drodze dalszych badań naukowych można dokonać analizy potrzeb i możliwości rozbudowy – modyfikacji metody ORBI tak, aby stało się możliwe używanie jej dla opracowywanych i wdrażanych systemów informatycznych. Cechy, jakie mają systemy informatyczne w fazie projektowej, oraz odmienne zagrożenia, na jakie mogą być takie systemy podatne, czyni ten obszar badań niezwykle interesującym. Idąc dalej w rozważaniach możliwych kierunków badań nad poruszanym w tej rozprawie problemem należy wspomnieć o wyzwaniu jakim jest ocena ryzyka związanego z bezpieczeństwem systemów informatycznych nie jednego lecz wielu przedsiębiorstw wzajemnie ze sobą kooperujących. W tym przypadku dane przedsiębiorstwo, mające „pełną kontrolę" nad ryzykiem związanym z bezpieczeństwem własnych systemów informatycznych, jest uzależnione w dużym stopniu od poziomu ryzyka związanego z bezpieczeństwem systemów informatycznych przedsiębiorstw, z którymi współpracuje. Zakład ubezpieczeń oferując produkt ubezpieczeniowy musiałby dokonać oceny ryzyka związanego z bezpieczeństwem całego środowiska informatycznego wszystkich przedsiębiorstw zaangażowanych we współpracę. W tym przypadku należałoby rozwinąć klasyfikację systemów oraz wprowadzić dodatkowe wymiary relacji pomiędzy podmiotami i ich wpływu na wartości ryzyk związanych z bezpieczeństwem systemów informatycznych. W dobie globalizacji przedsiębiorstw oraz ich odmiejscowienia taka potrzeba rozwoju metody ORBI wydaje się być niezwykle interesująca.

Ciekawym, praktycznym zastosowaniem wyników przedstawionych w rozprawie byłoby opracowanie systemu komputerowego, którego celem byłoby zbieranie danych, obliczanie wartości poszczególnych ryzyk związanych z bezpieczeństwem systemów informatycznych oraz analizowanie i symulowanie zmian wartości ryzyk wraz ze zmianami wartości spełnienia wymagań bezpieczeństwa przez poszczególne systemy informatyczne. System taki byłby znakomitym narzędziem zarówno dla zakładu ubezpieczeń, jak i przedsiębiorstw.

7 Bibliografia

1. Arnell, A. 1990. Handbook of effective disaster recovery planning. New York: McGraw-Hill.
2. Audyt wewnętrzny. Spojrzenie praktyczne. Stowarzyszenie księgowych w Polsce, Warszawa 2003
3. Baskerville, R. 1991. Risk analysis as a source of professional knowledge, Computers & Security 10 (8), 749 – 764. Oxford: Elsevier.
4. Baskerville, R. 1992. The developmental duality of information systems security. The Journal of Management Systems 4, 1, 1-12.
5. Białas A., 2006, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT.
6. Boehm, B. 1989. Tutorial: Software Risk Management. IEEE Computer Society.
7. Boran, S. The IT Security Cookbook, Boran Consulting, październik 2000
8. British Standard BS 7799. 1995. (Information Security Management), Part 1: Code of practice for information security management.
9. British Standard BS 7799-2:2002. 2002. Information Security Management System, Part 2: Specification with guidance for use.
10. Bundesamt für Sicherheit in der Informationstechnik (BSI) 1997. IT Baseline Protection Manual (Recommended Measures to meet Medium-Level Protection Requirements).
11. Butryn E., Piskozub W., 2003 Ubezpieczenia inżynieryjno-techniczne, Poltext, Warszawa.
12. Capik, M. i M., Zarządzanie ryzykiem ubezpieczeniowym dużych podmiotów gospodarczych, Prawo, Ubezpieczenia, Reasekuracja, 1997 r. nr 2.
13. Carvalho, J.A. 2000. Information System? Which one do you mean? Universidade do Minho, Departamento de Sistemas de Informacao. Portugalia.
14. CCTA, 1991. SSADM-CRAMM Subject Guide for SSADM Version 3 and CRAMM Version 2. Central Computer and Telecommunications Agency, IT Security and Privacy Group, Her Majesty's Government, London (February).
15. Cellary, W., "Globalization from the Information and Communication Perspective", Proc. The 4th International Conference on Distributed Computing and Internet Technology ICDCIT 2007, Bangalore (India), December 17-20,

2007, Tomasz Janowski, Hrushikesha Mohanty (eds.), Lecture Notes in Computer Science No 4882; Springer-Verlag Berlin Heidelberg, pp. 283-292.

16. Cellary, W., "Zarządzanie informacją zamiast zarządzania dokumentami drogą do unowocześnienia administracji", w: Krajowa Administracja Skarbowa, t. III: Nowoczesna Administracja Skarbowa, Ministerstwo Finansów, Warszawa, Wyd. DELFIN, pp. 173-183, 2007.
17. Cellary, W., "People and Software in a Knowledge-Based Economy", *Computer, January 2005, Volume 38, No 1*, IEEE Computer Society, pp. 114-116, 01/2005.
18. Cellary, W. (ed.), *Polska w drodze do społeczeństwa informacyjnego. Raport o rozwoju społecznym,* , UNDP, ISBN: 83-917047-5-0, 01/2002.
19. CERT Polska 2000. Raport – Przypadki naruszające bezpieczeństwo teleinformatyczne 2000.
20. CERT Polska 2001. Raport – Przypadki naruszające bezpieczeństwo teleinformatyczne 2001.
21. CERT Polska 2002. Raport – Przypadki naruszające bezpieczeństwo teleinformatyczne 2002.
22. CERT Polska 2003. Raport – Przypadki naruszające bezpieczeństwo teleinformatyczne 2003.
23. CERT Polska 2004. Raport – Przypadki naruszające bezpieczeństwo teleinformatyczne 2004.
24. CERT Polska 2005. Raport – Przypadki naruszające bezpieczeństwo teleinformatyczne 2005.
25. CERT Polska 2006. Raport – Przypadki naruszające bezpieczeństwo teleinformatyczne 2006.
26. Commission of European Communities 1990. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria, Version 1.2. Brussels, Belgium: Commission of European Communities, Directorate—General XIII (June).
27. Courtney, R. 1977. Security risk assessment in electronic data processing. AFIPS Conference Proceedings National Computer Conference 46, 97-104.
28. CSI/FBI. 2001. Computer Crime & Security Survey. Vol. VII 2001.
29. CSI/FBI. 2002. Computer Crime & Security Survey. Vol. VIII 2002.
30. CSI/FBI. 2003. Computer Crime & Security Survey. Vol. IX 2003.

31. Digital Technology & Professional Liability Insurance Program, Application, ACE USA, 06. 2006 r.
32. Digital Technology & Professional Liability Insurance Policy, Declarations, ACE USA, 02. 2007 r.
33. Domżał, T. 1995. Analiza ryzyka związanego z utratą danych lub naruszeniem ich poufności. Materiały szkoleniowe Instytutu Łączności - Bezpieczeństwo i poufność danych w systemach informatycznych. Warszawa.
34. Duży, A. 1993, Dyferencyjne metoda ustalania wysokości szkody. Państwo i Prawo nr 10
35. Falkenberg, E.D., Hesse, W., Lindgreen, P., Nilssen, B.E., Oei, J.L.H., Rolland, C., Stamper, R.K., Assche, F.J.M.V., Verrijn-Stuart, A.A., Voss, K. 1996. FRISCO: A Framework of Information Systems Concepts, IFIP WEDŁUG 8.1 Task Group FRISCO.
36. Falkenberg, E.D. Rolland, C. 1992. Information Systems Concepts: Improving the Understanding, North-Holland.
37. Fedor, M. 2004, Gazeta Ubezpieczeniowa, 32/2004
38. Finkelstein, C. 1989. An Introduction to Information Engineering: From Strategic Planning to Information Systems. Sydney: Addison-Wesley.
39. Fisher, R. 1984. Information Systems Security. Englewood Cliffs: Prentice-Hall.
40. Fuchs, D. Wybrane cechy umowy ubezpieczenia majątkowego, Prawo Asekuracyjne, 1999 r. nr 4
41. Gerrard, M. 2003. Creating an effective IT Governance process. Gartner Research (com-21-2931)
42. Glossary of Computer Security Terms (NCSC-TG-004 ver. 1). 1998. DataPro Report, July 98. New York: McGraw-Hill
43. Government of Canada, Communications Security Establishment. 1996. Risk management framework for Information Technology (IT).
44. Grajewski, P.: Koncepcja struktury organizacji procesowej. Dom Organizatora Toruń 2003
45. Hammer, M., Champy, J.: Reengineering w przedsiębiorstwie, Neumann Management Institute, Warszawa 1996
46. Holbrook, P., Reynolds, J. 1991. Site Security Handbook. Request for Comments (RFC) Nr 1244, wznowienie 1997 – RFC 2196

47. Information Systems Audit And Control Association, Control Objectives for Information and related Technology (CobiT)
48. Jedynak, P. 2003, Ubezpieczenia gospodarcze. Wybrane elementy teorii i praktyki, Księgarnia Akademicka, Kraków
49. Knight, F.H. 1957. Risk, Uncertainty and Profit. New York
50. Królikowska-Bocheńczyk, J. Wyłączenia odpowiedzialności, cz. 1 (04. 04. 2006 r.), cz. 2 (18. 04. 2006 r.), cz., 3 (02. 05. 2006 r.) i cz. 4 (13. 06. 2006 r.) Gazeta Ubezpieczeniowa.
51. Kuchlewska, M. 2003. Ubezpieczenie jako metoda finansowania ryzyka przedsiębiorstw. Wydawnictwo Akademii Ekonomicznej w Poznaniu. Poznań.
52. Kuchlewska, M. (red.), 2006, Szkice o ubezpieczeniach, Zeszyt 75, Ronka-Chmielowiec W., Ryzyko zakładu ubezpieczeń a ryzyko ubezpieczeniowe. Wydawnictwa Akademii Ekonomicznej w Poznaniu
53. Le Moigne, J.-L. 1977. La Théorie du Système Général: Théorie de la Modélisation, Presses Universitaires de France.
54. Łazowski, J. 1948, Wstęp do nauki o ubezpieczeniach, PZU
55. Maleszka, L. 2000, Zarządzanie ryzykiem a underwriting w ubezpieczeniach na życie, artykuł na podstawie pracy magisterskiej, A E Poznań, Katedra Ubezpieczeń Gospodarczych, www.ryzyko.pl
56. Management of Federal Information Resources, Office of Management and Budget 1996. OMB Circular A-130. Washington.
57. Manunta, G. 2000. Is Security Utilitarian?, Security Jurnal vol thirteen No. 2, 49 - 58. London: Perpetuity Press.
58. Merkury. 2004. IT Governance – Running IT like business. White Paper (www.mercury.com) [za Carr, Nicholas G., Does IT Matter? Information Technology and the Corrosion of Competitive Advantage, Harvard Business School Press, April 2004.]
59. Meritt, W.J. 1998. Risk Management. 21th NISSC (National Information Systems Security Conference). Arlington, Virginia.
60. Michalski, T. (red) 2004. Ubezpieczenia gospodarcze. Ryzyko i metodologia oceny. Wydawnictwo C. H. Beck. Warszawa.
61. Miscellaneous Errors and Omissions liability Insurance Application, ACE USA, 09. 1998 r.

62. Monkiewicz J. (red.), 2000, Podstawy ubezpieczeń. Tom I – Mechanizmy i funkcje, Poltext, Warszawa
63. Monkiewicz, J. (red.), 2001, Podstawy ubezpieczeń. Tom II – Produkty, Poltext, Warszawa
64. Monkiewicz, J. (red.), 2004, Podstawy ubezpieczeń. Tom III – Przedsiębiorstwo, Poltext, Warszawa
65. Mowbray, A.H., Blanchard, R.H. 1961. Insurance. It's theory and practice in the United States. New York
66. Nagle, W. Ubezpieczenia w transformacji ubezpieczeniowej, Prawo, Ubezpieczenia, Reasekuracja, 2006 nr 12
67. National Bureau of Standards, 1974. Guidelines for Automatic Data Processing Physical Security and Risk Management, Federal Information Processing Standards Publication FIPS 31.
68. National Institute of Standards and Technology, 2001. Risk management guide for Information Technology Systems, SP 800 – 30.
69. Network Risk Insurance Program Application – ACE USA, 05. 2005 r.
70. Network Risk Insurance Program Policy – ACE USA, 02. 2006 r.
71. Nosworthy, J. 2000. A Practical Risk Analysis Approach: Managing BCM Risk, Computers & Security 19, 7, 596 - 614. Oxford: Elsevier
72. Ogólne warunki ubezpieczenie sprzętu elektronicznego – Commercial Union Polska z dn. 08. 12. 2003 r.
73. Ogólne warunki ubezpieczenie sprzętu elektronicznego – Allianz Polska z dn. 19. 12. 2003 r.
74. Ogólne warunki ubezpieczenie sprzętu elektronicznego – PZU SA z dn. 07. 10. 2003 r.
75. Ogólne warunki ubezpieczenie sprzętu elektronicznego – TU Compensa SA z dn. 02.11. 2004 r.
76. Ogólne warunki ubezpieczenie sprzętu elektronicznego – AIG Polska TU SA z dn. 20. 11. 2006 r.
77. Ogólne warunki ubezpieczenia sprzętu elektronicznego – Ergo Hestia SA z dn. 01. 01. 2004 r.
78. Ogólne warunki ubezpieczenie sprzętu elektronicznego – Uniqa TU SA z dn. 13. 10. 2004 r.

79. Ogólne warunki ubezpieczenie sprzętu elektronicznego – Generali TU SA z dn. 01. 01. 2004 r.
80. Ogólne warunki ubezpieczenie sprzętu elektronicznego – HDI-Gerling TU SA z dn. 01. 01. 2004 r.
81. Ogólne warunki ubezpieczenie sprzętu elektronicznego – Warta SA z dn. 01. 01. 2004 r.
82. Ozier, W. 1997. Issues in Quantitative versus Qualitative risk analysis. DataPro Report, August. New York: McGraw-Hill.
83. Ozier, W. 1992. Risk Assessment and Management Data Security Management Report 85-01-20. New York: Auerbach.
84. Parker, D. 1976. Crime by Computer. New York: Chas Scribners Sons.
85. Pawłowski, K. Poszatkowana oferta, CFO, 2006 nr 2
86. Perenc, J. (red.), 2004, Rynek usług ubezpieczeniowych, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin
87. Pietrzykowska, A. Rola aktuariusza i nadzór wewnętrzny, Prawo Asekuracyjne, 2002, nr 4
88. Plate, A. 1997. Application of the IT Baseline Protection. 20th NISSC (National Information Systems Security Conference). Baltimore, Maryland.
89. Poniewierski, A. Ryba, M. 2008, Jak zbudować system bezpieczeństwa informacji w firmie. Harvard Business Review, Maj 2008 r. str. 156 - 161
90. Poniewierski, A. 1999, Zarządzanie ryzykiem bezpieczeństwa systemów informatycznych, materiały konferencyjne SecurNET. Warszawa, Polska
91. Poniewierski, A. 2000, Zarządzanie ryzykiem bezpieczeństwa systemów informatycznych, materiały konferencyjne COMNET. Warszawa, Polska.
92. Poniewierski, A. 2001, Role of Vulnerability Assessment Technology in IT Risk Management, materiały konferencyjne International Security Summit. Atlanta GA, USA
93. Poniewierski, A. 2001, Strategia i Polityka zabezpieczenia elektronicznego dowodu przestępstwa pochodzącego z systemów IDS, materiały konferencyjne, IV Seminarium Naukowe Wyższej Szkoły Policyjnej w Szczytnie - Techniczne aspekty przestępczości komputerowej. Szczytno, Polska
94. Poniewierski, A. 1999, Analiza ryzyka w kontekście Polityki Zabezpieczeń Systemów Informatycznych. Biuletyn Bankowy. ISSN 1233-0566 / Nr 21, str. 17 - 27

95. Poniewierski, A. 2003, Ryzyko bezpieczeństwa systemów informatycznych. Rynek Terminowy. ISSN 1508-972x/ Nr 2/03 str. 24-25
96. Poniewierski, A., Ryba M., Economical aspects of IT Security Risk Management in Industry, materiały konferencyjne IFIP I3E'2005, Poznań, 26-28 października 2005
97. Reid, R. C., Floyd, S. A. 2001. Extending the risk analysis model to include market - insurance, Computers & Security 20, 4, 331 - 339. Oxford: Elsevier
98. Reps, S. Zawieranie umów ubezpieczenia odbiegających od treści ogólnych warunków ubezpieczeń, Prawo Asekuracyjne, 1998 nr 2
99. Rogala, I. Rola i znaczenie underwritingu w kształtowaniu i realizacji strategii firmy ubezpieczeniowej, Prawo asekuracyjne, 1997 r. nr 3
100. Ronka – Chmielowiec, W. (red.) 2000. Zarządzanie ryzykiem w ubezpieczeniach. Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu. Wrocław.
101. Ronka – Chmielowiec, W. (red.) 2002. Ubezpieczenia. Rynek i ryzyko. Polskie Wydawnictwo Ekonomiczne. Warszawa.
102. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych (Dz. U. Nr 100, poz. 1024)
103. Różycki, P. Jak ubezpieczają się przedsiębiorstwa, Wiadomości Ubezpieczeniowe, 2005, nr 3/4
104. Ryba, M. 2006, Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M. Rozprawa doktorska. Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
105. Saarinen, T., Sääksjävi, M. 1989. The missing concepts of user participation: An empirical assessment of user participation and information system success, in Bødker, Susanne (Ed.) Proceedings of the 12th IRIS—Part II. Computer Science Department, Aarhus University DAIMI PB 296-II (December) 533-551.
106. Sangowski, T. 1994. Gospodarka finansowa kapitałami i rezerwami ubezpieczyciela, w : Ubezpieczenia w gospodarce rynkowej, Wosiewicz A. red. t.1. Oficyna Wydawnicza Branta . Bydgoszcz.
107. Sangowski, T. 2001. Ubezpieczenia gospodarcze. Poltext. Warszawa.

108. Security of Federal Automated Information Systems, Office of Management and Budget 1978. OMB Circular A-71. Washington.
109. Sherwood, J. 1999. Operational Risk Management in Business Information Systems. London: Sherwood Ltd.
110. Solms, B. 2000. Information Security – the third wave? Computers & Security 19, 2000, 615 - 620. Oxford: Elsevier
111. Standards Australia AS/NZS 4360:1999, Risk management.
112. Strategic Management: A Stakeholder Approach, (za Williams, C.A, Smith, M.L., Young, P. C., 2002. Zarządzanie ryzykiem a ubezpieczenia), Wydawnictwo Naukowe PWN. Warszawa.
113. Sumner, M. 1992. The impact of Computer Assisted Software Engineering on Systems Development in Kendall, K. Lyytinen, K., DeGross, J. IFIP Transactions A8 The Impact of Computer Supported Technologies on Information Systems Development. Amsterdam: North-Holland, 43-60.
114. Systemy zarządzania jakością. Podstawy i terminologia. PNEN ISO 9000. PKN 2001
115. Sztachelska, J. Ubezpieczenia sprzętu elektronicznego. Coraz bogatsza oferta, Gazeta Ubezpieczeniowa, 2004, 14 grudnia
116. Śliwiński, A. 2002. Ryzyko ubezpieczeniowe taryfy – budowa i optymalizacja. Wydawnictwo Poltext. Warszawa.
117. Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji. 2003. PN-ISO/IEC 17799.
118. Technika informatyczna, Zabezpieczenia w systemach informatycznych. Terminologia. Marzec 2002. PN-I-02000,
119. Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych. Styczeń 1999. PN-I-13335-1.
120. Ustawa o działalności ubezpieczeniowej z dn. 22 maja 2003 roku (Dz. U. z dn. 16 lipca 2003 r.)
121. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
122. U.S. Department of Commerce, National Bureau of Standards, 1979. Guideline for Automatic Data Processing Risk Analysis, Federal Information Processing Standards Publication FIPS 65.

123. U.S. Department of Defense 1985. Trusted Computer Systems Evaluation Criteria. DOD 5200.28 – STD.
124. Williams, C.A, Smith, M.L., Young, P.C. 2002. Zarządzanie ryzykiem a ubezpieczenia. Wydawnictwo Naukowe PWN. Warszawa.
125. Wołowski, F. 2000. Wprowadzenie do problematyki analizy ryzyka dla Wspólnej Sieci Bankowości Elektronicznej. Rada bankowości elektronicznej przy Związku Banków Polskich.
126. Wong, K. 1977. Risk Analysis and Control. Manchester: National Computer Center Publications. Wood, C. 1990. Principles of secure information systems design, Computers & Security 9, 1 (Feb): 13 - 24.
127. Woodley, B. 2001. The Impact of Transformative Technologies on Governance: Some Lessons from History. Institute on Governance. Ontario.
128. Zdanowski, M. 1995, Wstęp do ubezpieczeń podmiotów gospodarczych. Warunki i rozwiązania krajowe. Przedsiębiorstwo Wydawnicze LAM, Warszawa
129. Zasady szacowania ryzyka technologicznego (pr. zb.) 1999, Conference Papers. The Third Conference of the Polish-British School of Insurance, Zakopane

8 Spis rysunków

9 Spis tabel