PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1115 2006
Gospodarka a Środowisko 5

Paweł Skowron

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – KONCEPCJA I ZASTOSOWANIE

1. Wstęp

W związku z ekspansją rozwiązań teleinformatycznych i upowszechnianiem się dostępu do Internetu nasilają się zjawiska włamań do systemów informacyjnych, kradzieży baz danych czy zasobów intelektualnych zgromadzonych w organizacji. Ma to swoje skutki w zapewnieniu ciągłości działania podmiotu. Dla wielu organizacji ochrona aktywów niematerialnych (informacyjnych) nie jest jeszcze ani elementem strategii, ani częścią codziennej pracy, co może wynikać z przekonania o decydującym wpływie aktywów materialnych na wartość podmiotu. Coraz więcej współczesnych organizacji dostrzega jednak ryzyko gospodarowania informacją. Wiele z nich podejmuje działania związane z analizą i ograniczaniem tego ryzyka, a podejmowane działania mają charakter systemowy.

2. Systemy zarządzania bezpieczeństwem informacji

Systemowe zarządzanie bezpieczeństwem informacji (*Information Security Management System – ISMS*) nabiera szczególnego znaczenia w dobie informacji, kiedy jest ona najważniejszym aktywem każdej organizacji [2, s. 13].

Prace związane z ustanowieniem jednolitego systemu zarządzania dotyczącego bezpieczeństwem informacji zostały zapoczątkowane na początku lat 90. ubiegłego stulecia.

W 1995 r. pojawiło się pierwsze wydanie brytyjskiej normy BS 7799-1 – *Code of practice for Information Security Management*. Niniejsza norma była zbiorem doświadczeń wielu firm, a wymagania w niej zawarte w normie odniesiono wyłącznie do anielskiego prawodawstwa, co uniemożliwiało stosowanie jej w innych krajach. W 1999 r. dokonano nowelizacji pierwszego wydania normy brytyjskiej. Znowelizowana norma otrzymała numer ISO/IEC 17799:2000 – *Code of practice for Information Security Management*, a w 2003 r. norma została przetłumaczona na język polski i wydana jako polska norma PN-ISO/IEC 17799:2003 – *Technika informatyczna. Praktyczne zasady zarządzania bezpieczeń-*

stwem informacji. Norma ta jest zbiorem 127 propozycji zabezpieczeń organizacji przed zagrożeniami oraz „drogowskazem" przy projektowaniu systemu zarządzania bezpieczeństwem informacji.

Międzynarodowa norma ISO/IEC 17799 tak oto definiuje pojęcie informacji. *Informacja jest aktywem, który podobnie, jak inne ważne aktywa biznesowe, ma dla instytucji wartość i dlatego należy ją odpowiednio chronić przed wieloma zagrożeniami.*

Bezpieczeństwo informacji polega na zachowaniu trzech podstawowych aspektów informacji:

– **poufność**: zapewnienie dostępu do informacji tylko osobom upoważnionym,

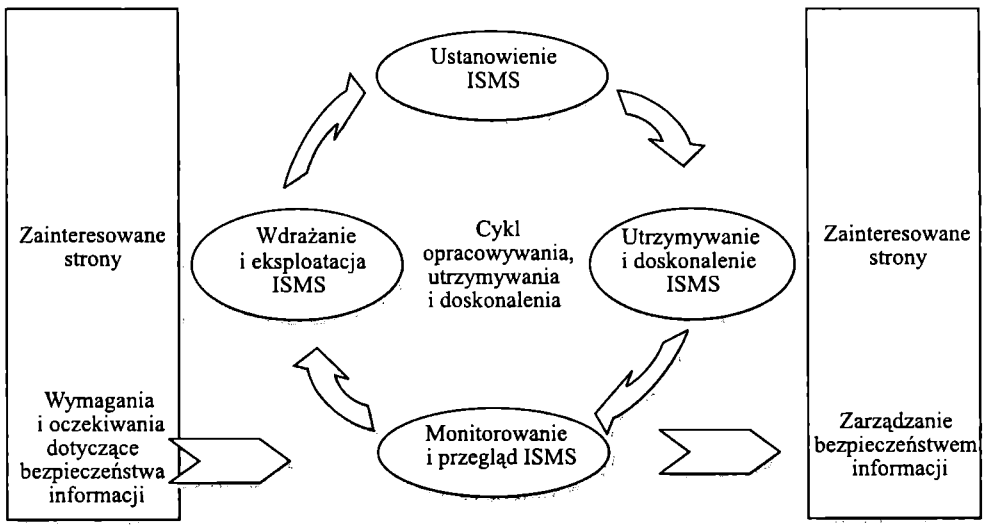
– **integralność**: zapewnienie dokładności i kompletności oraz metod jej przechowywania,

– **dostępność**: zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne [7, s. 7].

Norma ta, ze względu na swoją formę, nie stanowi podstawy do ubiegania się o certyfikat systemu zarządzania bezpieczeństwem informacji.

Taką możliwość stwarzał dotychczas standard BS 7799 – 2 wydany w 2002 r. Norma ta nie była standardem międzynarodowym, niemniej jednak stanowiła podstawę do opracowania i wydania w październiku 2005 r. normy ISO/IEC 27001:2005 – *Specyfikacja systemów zarządzania bezpieczeństwem informacji*, która jest podstawą do audytowania organizacji.

Brytyjski standard ma swój odpowiednik w polskiej wersji językowej wydany przez PKN pod numerem PN-I-07799-2:2005 – *Systemy zarządzania bezpieczeństwem informacji. Specyfikacja i wytyczne stosowania.*



Rys. 1. Model PDCA stosowany w procesach SZBI

Źródło: [6, s. 8].

Tabela 1. Charakterystyka wymagań normy PN-I-07799-2:2005

Faza cyklu PDCA	Wymaganie	Charakterystyka
1	2	2
Planowanie	Określenie zakresu i polityki SZBI	Organizacja powinna: – podjąć działania zmierzające do opracowania, wdrożenia, doskonalenia i dokumentowania SZBI, w kontekście całościowych działań biznesowych i ryzyka z tym związanego, – ustalić, czy SZBI będzie obejmował część lub całość organizacji, w zależności od rodzaju prowadzonej działalności, lokalizacji organizacji, posiadanych aktywów informacyjnych i stosowanych technologii, – prowadzić politykę, która powinna zawierać ramy ustalania celów, wyznaczać ogólny kierunek i zasady działania w odniesieniu do ochrony informacji, uwzględniać wymagania biznesowe i prawne, wyznaczać strategiczne działania w zarządzaniu bezpieczeństwem informacji oraz jasno precyzować kryteria oceny ryzyka, – zidentyfikować procesy SZBI
	Identyfikacja i szacowanie ryzyka	Do zadań organizacji należą: – wskazanie na metodę systematycznego szacowania ryzyka oraz określenie bezpieczeństwa informacji organizacji pod względem biznesowym, prawnym oraz wynikającym z zakresu prowadzonej działalności, – określenie ryzyka, tj. wskazanie na aktywa objęte SZBI oraz ich właścicieli, a także zagrożenia dla zidentyfikowanych aktywów oraz skutki utraty przez te aktywa poufności, integralności i dostępności, – oszacowanie ryzyka pod względem strat biznesowych, które mogą wyniknąć z naruszenia bezpieczeństwa informacji, prawdopodbieństwa takiego naruszenia oraz poziomu akceptowalności ryzyka i ryzyka szczątkowego
	Plan postępowania z ryzykiem	Organizacja powinna: – wskazać i ocenić warianty postępowania z ryzykiem, obejmujące: zastosowanie odpowiednich zabezpieczeń, zaakceptowanie ryzyka, w sposób świadomy i obiektywny, unikanie ryzyka, czy przeniesienia ryzyka na ubezpieczycieli lub dostawców – wybrać cele stosowania zabezpieczeń udokumentować je w deklaracji stosowania
Wdrażanie i funkcjonowanie	Wprowadzenie	Działania związane z tą fazą cyklu PDCA są zaprojektowane w celu wdrożenia wybranych zabezpieczeń oraz promowania działań koniecznych do zarządzania ryzykiem związanymi z bezpieczeństwem informacji zgodnie z decyzjami podjętymi w fazie planowania
	Zasoby, szkolenia i kompetencje	Działania dla organizacji, wynikające z tej fazy: – zapewnienie odpowiednich zasobów (ludzi, czasu, środków finansowych) w celu zapewnienia należytego funkcjonowania SZBI, – zbudowanie podstaw „dobrych kultur" postępowania z ryzykiem i bezpieczeństwem informacji poprzez skuteczne programy szkoleniowe, – określenie koniecznych kompetencji personelu, którego praca objęta jest SZBI
	Postępowanie z ryzykiem	Organizacja powinna ustanowić procedury i inne działania zdolne do zapewnienia natychmiastowego wykrycia i reakcji na incydenty związane z naruszeniem bezpieczeństwa informacji. Uwaga: ryzyko zakwalifikowane jako akceptowalne nie wymaga dodatkowych działań

1	2	3
Monitorowanie i przegląd	Wprowadzanie	Działania monitorujące powinny być tak zaplanowane, aby zapewnić, że ustanowione zabezpieczenia funkcjonują w sposób zamierzony (skuteczny), a wdrożony SZBI jest efektywny
	Rutynowe sprawdzanie	Organizacja powinna: – wykonywać regularne przeglądy skuteczności SZBI, biorąc pod uwagę wynik audytów wewnętrznych, incydentów, sugestii oraz informacji zwrotnych uzyskanych od wszystkich zainteresowanych stron, – dokonywać przeglądów ryzyka szczątkowego nie akceptowanego, biorąc pod uwagę zmiany: w organizacji, stosowanej technologii, celów biznesowych, procesów, zagrożeń utraty informacji, uregulowań prawnych oraz stosowanych regulacji
	Audyty wewnętrzne	W zaplanowanych odstępach czasu organizacja powinna przeprowadzać audyty wewnętrzne w celu uzyskania obiektywnego dowodu, że wdrożony system funkcjonuje w sposób zamierzony i efektywny
	Przegląd kierownictwa	W regularnych odstępach czasu należy podejmować przeglądy SZBI dokonywane przez kierownictwo, by zapewnić, że SZBI jest poprawny, odpowiedni i skuteczny. Efektem przeglądu kierownictwa powinno być wszelkie decyzje i działania doskonalące SZBI, a jeśli to konieczne – modyfikujące stosowane procedury – w celu skuteczniejszej reakcji na wewnętrzne i zewnętrzne zagrożenia.
	Zapisy	Należy dokumentować działania i zdarzenia, które mogą mieć wpływ na skuteczność i jakość w utrzymaniu SZBI
Doskonalenie	Wprowadzenie	W celu utrzymania skuteczności SZBI organizacja powinna podjąć działania związane z jego doskonaleniem na podstawie informacji zebranych w fazie monitorowania i przeglądu
	Działania korygujące i zapobiegawcze	Organizacja powinna podjąć działania w celu: – wyeliminowania przyczyn niezgodności związanych z wdrożeniem i utrzymaniem SZBI, tak by przeciwdziałać powtórnemu ich wystąpieniu, – określenia niezbędnych działań wyeliminowania przyczyn potencjalnych niezgodności lub innych potencjalnych, niepożądanych sytuacji tak, by przeciwdziałać ich wystąpieniu

Źródło: opracowanie własne na podstawie [6] oraz [7].

Norma składa się z siedmiu rozdziałów, a szczegółowe wymagania zostały zawarte w rozdziałach od czwartego do siódmego. Szczególne znaczenie dla tworzenia systemu zarządzania bezpieczeństwem informacji, oprócz określenia zakresu SZBI i systematycznego podejścia do szacowania ryzyka, ustanowienia polityki bezpieczeństwa informacji oraz określenia i oszacowania ryzyka ma także wskazanie na cele stosowania zabezpieczeń, jako środków do postępowania z ryzykiem. W załączniku A do niniejszej normy BS 7799-2 zamieszczono zestawienie zabezpieczeń, które mają swoje odniesienie do normy ISO 17799. Wybór celów zabezpieczeń organizacja powinna dostosować do własnych potrzeb i warunków funkcjonowania.

Struktura rozdziałów wskazuje na zastosowanie w normie podejścia procesowego, opartego na idei ciągłego doskonalenia E. Deminga, podczas ustanawiania, wrażania, eksploatacji, monitorowania, utrzymywania i poprawy skuteczności SZBI. Podejście to zostało zaprezentowane na rys. 1.

Szczegółową charakterystykę wymagań normy PN-I-07799-2:2005, w odniesieniu do poszczególnych faz cyklu PDCA, zaprezentowano w tab. 1.

Konieczność ochrony zasobów informacyjnych organizacji jest bezdyskusyjne. Zaproponowany standard BS 7799 może przyczynić się, w sposób systemowy, do ograniczenia ryzyka utraty aktywów informacyjnych.

3. Integracja systemu zarządzania bezpieczeństwa informacji

Analizując istotę standardu BS 7799, można powiedzieć, że zawarte w nim regulacje powinno się traktować jako uniwersalne dla każdego typu organizacji i każdego systemu informacyjnego [2, s. 17]

Brytyjska norma BS 7799-2 została tak zaprojektowana, by ułatwić organizacji dopasowanie lub integrację własnego systemu zarządzania bezpieczeństwa informacji z wymaganiami innych systemów zarządzania.

W załączniku C normy BS 7799-2 umieszczone zostały powiązania pomiędzy normą a normą ISO 9001:2000 oraz ISO 14001:1996. Raczej nie będzie możliwe zbudowanie zintegrowanego systemu przez specjalistów ds. jakości nie posiadających dodatkowej wiedzy na temat bezpieczeństwa informacji i informatyki [3, s. 30].

Niektóre podmioty rozwijają politykę bezpieczeństwa informacji w ramach systemu zarządzania jakością. Organizacja jest prawnie zobowiązana do ochrony powierzonej jej własności klienta, obejmującej produkty i półprodukty, materiały, w tym również informację o klientach i ich dane osobowe. A zatem rozwiązanie to jest zasadne, gdyż oprócz zagwarantowania satysfakcji klientowi obejmuje również bezpieczeństwo informacji wynikające ze wzajemnej współpracy czy bezpieczeństwo procedur zarządzania. Nie powinno się jednak traktować systemu zarządzania bezpieczeństwem informacji jako jednego z wielu procesów w systemie jakości, gdyż ochrona informacji dotyczy wszystkich elementów działalności organizacji, których system zarządzania jakością może nie obejmować.

Wysiłek zintegrowania SZBI z systemem zarządzania jakością może przynieść wymierne efekty w postaci:

- stworzenia jednolitej dokumentacji,
- niższych kosztów opracowania, wdrożenia i utrzymania systemu,
- podobnych zasad przeprowadzania audytów,
- objęcia systemem całej organizacji (pracowników, dokumentów, sprzętu),
- zwrócenia szczególnej uwagi na szacowanie ryzyka i zarządzania nim.

Faktem jest, że zakres SZBI zależy od wrażliwości organizacji na ochronę aktywów informacyjnych. Organizacja, w której świadomość utraty cennych zasobów, dających niejednokrotnie przewagę konkurencyjną, jest wysoka, powinna ukierunkować swoje działania na tworzenie systemu, dającego wyraźne efekty synergii w postaci systemów zarządzania, wzajemnie ze sobą zsynchronizowanych.

4. Funkcjonowanie systemu zarządzania bezpieczeństwem informacji

Szczególne zainteresowanie systemami bezpieczeństwa wykazują instytucje finansowe (banki, firmy ubezpieczeniowe), organizacje państwowe, samorządowe i wojskowe, dostawcy usług internetowych oraz przedsiębiorstwa świadczące usługi telekomunikacyjne. Organizacje te przetwarzają i gromadzą informacje, najczęściej niejawne, wymagające ścisłego nadzoru a także dysponują nimi [5]. Dlatego, w sposób szczególny, są one narażone na zamierzone i niezamierzone naruszenie bezpieczeństwa informacji.

Istnieją dwa zasadnicze źródła zagrożeń: wewnętrzne i zewnętrzne. Na zagrożenia wewnętrzne składają się m.in.:

- pracownicy,
- stosowana technologia (systemy informacyjne i informatyczne, służące do przetwarzania informacji),
- struktura organizacyjna (a w szczególności zakres odpowiedzialności za bezpieczeństwo informacji),
- procesy, którymi zarządza organizacja (klienci, kanały dystrybucji, zakres dostępu do informacji, zmiana haseł, zarządzanie incydentami i in.) [1, s. 84].

Przykładami zagrożeń zewnętrznych mogą być:

- partnerzy handlowi (dostawcy, odbiorcy),
- osoby trzecie, mające dostęp do aktywów informacyjnych organizacji,
- wrogie działania techniczne (hakerzy, wirusy),
- szpiegostwo gospodarcze i finansowe,
- warunki pogodowe, awarie systemu zasilania, kataklizmy.

Wydawać by się mogło, że gorszymi zagrożeniami są te pochodzące z zewnętrz. Okazuje się jednak, że największe zagrożenie dla aktywów informacyjnych stanowią ludzie. Ludzie kompetentni, a jednocześnie lekkomyślni mają wiele sposobności wykonywania swych zadań z naruszeniem zasad zabezpieczeń, np. pozostawiają hasło zapisane na widocznym miejscu, używają łatwego do złamania hasła, współpracują z prasą, pozostawiają dokumenty biznesowe bez nadzoru na drukarce itp. Drugą dominującą klasę zagrożeń stanowią nieuczciwi pracownicy. Zagrożenie to może się pojawić w różnych formach: czerpania korzyści z wad w oprogramowaniu, błędów w procedurach manualnych, przyjęcia korzyści dostępu do tajnej informacji, wprowadzenie wirusów do systemu informacyjnego itp. [4, s. 431-432].

Jednym z elementów naruszenia bezpieczeństwa jest ryzyko utraty zasobów informacji. Zagrożenie to rośnie w tempie wykładniczym, wraz ze wzrostem liczby użytkowników mających dostęp do danego systemu informatycznego organizacji.

Potwierdzają to wyniki badań opublikowanych przez firmę Ernst & Young [8]. W *Globalnym raporcie bezpieczeństwa informatycznego*, w części dotyczącej Polski, respondenci do największych zagrożeń bezpieczeństwa informacji zaliczyli:

1) działania pracowników,

2) szkodliwe programy,
3) utratę poufnych danych o klientach,
4) rozproszony atak DoS (*Denial of Service*),
5) fizyczne uszkodzenie systemu.

Ankietowani wskazali również na najistotniejsze inicjatywy w obszarze bezpieczeństwa informacji, podjęte w 2004 r. Za najważniejsze uznano: dostosowanie strategii bezpieczeństwa do podstawowych celów przedsiębiorstwa, dostosowanie się do obowiązujących przepisów prawnych związanych z ochroną informacji, wdrożenie polityki bezpieczeństwa informacji, zainicjowanie działań korygujących po wystąpieniu awarii. Działania te mają na celu zapewnienie ciągłości działania. Istnieje jednak wiele przeszkód w osiągnięciu odpowiedniego poziomu bezpieczeństwa aktywów informacyjnych. Można tu wskazać takie, jak:

– brak świadomości oraz trudność uświadomienia zagrożeń wśród użytkowników – problem bezpieczeństwa traktowany jest jako domena działu informatycznego, a pracownicy wykonujący rutynowe działania nie mają nawet nawyku brania pod uwagę kwestii związanych z bezpieczeństwem informacji,

– ograniczenia budżetowe – wynikające ze struktury wydatków na działania związane z bezpieczeństwem informacji. Znamienny jest fakt rosnących nakładów na zabezpieczenia przed utratą informacji. Jednak uwaga firm skupiona jest w dalszym ciągu na zagrożeniach zewnętrznych, w mniejszym stopniu zaś na zagrożeniach wewnętrznych. Zasoby finansowe oraz wszelkie inne działania powinny zmierzać w kierunku budowania kultury bezpieczeństwa informacji, ze szczególnym uwzględnieniem roli kierownictwa,

– brak wykwalifikowanego personelu. W większości polskich przedsiębiorstw nie ma wyznaczonych kierowniczych stanowisk odpowiedzialnych za bezpieczeństwo informacji. Za te kwestie najczęściej odpowiedzialni są dyrektorzy zarządzający lub finansowi. Tylko w 14% badanych przedsiębiorstw za sprawę bezpieczeństwa informacji odpowiedzialny jest dyrektor ds. bezpieczeństwa informacji.

Wyniki uzyskanych badań wskazują na wiele uchybień w obszarze bezpieczeństwa informacji. Opieranie bezpieczeństwa informacji na zaufaniu i przekonaniu o posiadaniu wystarczających zabezpieczeń jest niewystarczające wobec współczesnych zagrożeń.

5. Podsumowanie

Liczba wydanych certyfikatów na zgodność z wymaganiami normy BS 7799-2 świadczy o tym, że jest coraz więcej organizacji, które patrzą na ochronę informacji w sposób całościowy – od informacji gromadzonych i przetwarzanych wewnątrz samego podmiotu po wzajemne powiązania biznesowe z innymi podmiotami. Choć takich certyfikatów wydano w Polsce niewiele, to jednak

zainteresowanie problematyką bezpieczeństwa aktywów informacyjnych jest znaczne.

Opracowanie polityki bezpieczeństwa informacji i jej bezwzględne przestrzeganie przyczyni się do właściwej ochrony tworzonej wartości w każdej organizacji, gdzie świadomość naruszenia aktywów informacyjnych jest wysoka.

Dostrzeganie zagrożeń płynących zarówno z wnętrza organizacji, jak i z otoczenia, w jakim dana organizacja funkcjonuje, sprowadza się do tworzenia skutecznych mechanizmów ochronnych. Polegają one na stosowaniu nowoczesnych rozwiązań technicznych oraz ciągłym budowaniu świadomości zarówno wśród partnerów biznesowych, jak i, a może przede wszystkim, wśród własnych pracowników. Największe szkody mogą spowodować właśnie pracownicy korzystający z systemu informatycznego, administratorzy i inni uprawnieni, mający dostęp do zasobów informacyjnych organizacji. Z drugiej jednak strony pracownicy mający odpowiednie wsparcie ze strony kierownictwa, mogą stać się największym „buforem bezpieczeństwa" organizacji. A zatem systemowa ochrona informacji powinna polegać na współdziałaniu zarządzającego organizacją i podległego personelu.

Literatura

[1] Łuczak J., *Systemowe zarządzanie bezpieczeństwem informacji – doskonalenie systemu jakości*, [w:] *Wyzwania zarządzania jakością*, red. M. Salerno-Kochan, Materiały konferencyjne II Ogólnopolskiej Sesji Naukowej Zarządzanie Jakością, wyd. Centrum Rozwoju i Promocji AE w Krakowie, Kraków 2005.

[2] Łuczak J., *Systemy zarządzania bezpieczeństwem informacji (ISMS)*, „Problemy Jakości" 2000 nr 11.

[3] Szomański B., *Systemy zarządzania bezpieczeństwem informacji – założenia i projektowanie*, „Problemy Jakości" 2004 nr 4.

[4] Żebrowski A., *Bezpieczeństwo wiedzy – nowy atrybut działalności przedsiębiorstwa*, [w:] *Informacja i wiedza w zintegrowanym systemie zarządzania*, red. R. Borowiecki, M. Kwieciński, Zakamycze 2004.

[5] Ustawa z dnia 22 stycznia 1999 o ochronie informacji niejawnych (DzU 1999 nr 11, poz. 95 z późn. zm.).

[6] PN-I-07799-2:2005 – *Systemy zarządzania bezpieczeństwem informacji. Specyfikacja i wytyczne stosowania.*

[7] PN-ISO/IEC 17799:2003 – *Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.*

[8] http://www.ey.com/GLOBAL/content.nsf/Poland/TSRS_-_Library_-_GISS_2004, strona dostępna w dniu 1.07.2005 r.

INFORMATION SECURITY MANAGEMENT – CONCEPTION AND USE

Summary

The synthetic expression of concept and structure of requirements of Information Security Management System (ISMS) consistent on BS 7799-2:2002 has been presented on the basis of constant improvement. The article also contains recommendations about the possibilities of implementing ISMS in organizations and its integration with quality management system based on ISO 9001:2000.

In order to visualize the state of Information Security in Poland, a report prepared by a major advisory company has been used. The conclusion that can be drawn from the report is that Polish managers' actions as far as ISMS is concerned are still non-systematic and temporary.

Mgr Pawel Skowron jest pracownikiem Katedry Zarządzania Jakością i Środowiskiem Akademii Ekonomicznej we Wrocławiu – Wydział w Jeleniej Górze.