Małgorzata Wiśniewska
Państwowa Wyższa Szkoła Zawodowa we Włocławku
Sławomir Tylczyński[1]

Wdrażanie polityki bezpieczeństwa informacji w polskich uczelniach technicznych w świetle badań empirycznych

Streszczenie

Artykuł dotyczy badań przeprowadzonych w polskich uczelniach technicznych w zakresie bezpieczeństwa przetwarzanych informacji. W artykule przedstawione zostały wnioski z badań dotyczących stanu wdrożenia polityki bezpieczeństwa informacji w uczelniach, m.in. podejście uczelni do polityki bezpieczeństwa informacji, organizacji bezpieczeństwa w uczelni i zasad bezpieczeństwa informacji dotyczących współpracy uczelni z podmiotami zewnętrznymi w ramach realizacji badań naukowych, doradztwa, przedsięwzięć związanych z patentami, nowymi rozwiązaniami technicznymi i technologicznymi, pracami dyplomowymi itp. Wyniki badań w tym obszarze wskazują, że w zakresie utrzymania koniecznej współpracy z podmiotami zewnętrznymi, uczelnie w większości przypadków wdrażają podstawowe zasady dotyczące bezpieczeństwa informacji.

Słowa kluczowe: organizacja, bezpieczeństwo informacji, polityka bezpieczeństwa informacji

Implementation of Information Security Policy in the Polish Technical Universities Based on Empirical Research

Abstract

This article applies to research conducted in Polish technical universities in terms of security of the processed information. The article presents the conclusions of research on the state of implementation of information security policies in higher education, including university approach to information security policy, security organization at the university and safety information concerning the coope-

[1] Mgr inż. Sławomir Tylczyński współpracuje z Państwową Wyższą Szkołą Zawodową we Włocławku w zakresie dydaktyki.

ration of universities with external entities as part of the research, consultancy, projects related to patents, new technical solutions and technology, theses, etc. The results of research in this area suggests that in terms of maintaining the necessary liaison with external entities, universities in most cases implement the basic principles of information security.

Keywords: organization, information security, information security policy

1. Wstęp

W każdej organizacji informacja jako kluczowy element jej funkcjonowania zyskuje coraz większe znaczenie. Właściwie cała działalność gospodarcza opiera się na informacjach. Poczynając od danych, które mogą się wydawać prozaiczne, a jednak niezbędne do formalnego zaistnienia każdej organizacji (dokumentacja księgowa, dane personalne pracowników, zezwolenia na działalność, produkcję itd.), po informacje, które determinują ich działalność i sens egzystowania na rynku (dane kontrahentów, dokumentacje technologiczne, strategie rozwoju, patenty itd.). Ponadto, mając na uwadze to, że technologie informatyczne wciąż się rozwijają, a proces ten postępuje często o wiele szybciej niż możliwość implementacji i adaptacji zmian, trzeba mieć świadomość, że wraz z tymi możliwościami pojawiły się równocześnie nieznane dotąd zagrożenia. W związku z tym organizacje są zmuszone zadbać o bezpieczeństwo swoich informacji, decydując się na przykład na opracowanie polityki bezpieczeństwa i wdrożenie systemu ochrony informacji.

Pod pojęciem „polityka bezpieczeństwa" należy rozumieć zbiór zasad i norm, które powinny służyć właściwemu zabezpieczeniu zasobów systemu. Natomiast system ochrony to z kolei odpowiednie środki oraz mechanizmy techniczne, organizacyjne i prawne wykorzystywane w celu ochrony informacji. Właściwie można powiedzieć, że system ochrony informacji jest narzędziem wykonawczym polityki bezpieczeństwa. Istnieje oczywiście wiele możliwości ochrony informacji, jednak najskuteczniejszym okazuje się podejście kompleksowe do tych kwestii. Konieczne zatem jest zarówno wdrażanie odpowiednich rozwiązań technologicznych, tworzenie i wprowadzanie wymaganych procedur, jak i szkolenia oraz budowanie świadomości pracowników w zakresie odpowiedzialności za bezpieczeństwo przetwarzanych informacji.

Aby jednak polityka w zakresie bezpieczeństwa informacji mogła odnosić pożądany skutek, jej utworzenie powinno zostać poprzedzone dokładnym zidentyfikowaniem i poznaniem zagrożeń, na jakie narażone są informacje zgromadzone i przetwarzane przez organizację.

Polityka bezpieczeństwa informacji stanowi dokument ogólny, który definiuje zasady dostępu do zasobów gromadzonych i przetwarzanych przez system. Określa, w jaki sposób wyegzekwować te zasady, oraz opisuje podstawy architektury zabezpieczeń systemu. Z uwagi na istotność podejmowanych tematów dokument ten ma najczęściej rangę oficjalnego wewnętrznego regulaminu zatwierdzonego przez zarząd organizacji. Przestrzeganie zasad wynikających z polityki bezpieczeństwa jest obowiązkiem wszystkich pracowników zatrudnionych w organizacji. Dodatkowo w celu sprawnego przebiegu działań związanych z wdrożeniem i egzekwowaniem polityki bezpieczeństwa w strukturach organizacji muszą zostać wyznaczone osoby do pełnienia związanych z tym obowiązków.

Uczelnie techniczne funkcjonują w otoczeniu, które determinuje określone postępowanie w zakresie współpracy z podmiotami zewnętrznymi, w tym przedsiębiorstwami. Warunki te skłaniają do nawiązywania formalnej i nieformalnej współpracy w zakresie wymiany *know-how*. To z kolei wymusza przepływy nie tylko strumieni materiałów i pieniądza, ale przede wszystkim informacji, która jest obecnie dobrem najcenniejszym. Zarządzającym uczelniami często brak narzędzi oraz rozwiązań, które w rzetelny sposób zabezpieczałyby ich interesy w otoczeniu gospodarczym. Poza procesami polegającymi na współpracy uczelni z przemysłem istnieje wiele innych związanych z przetwarzaniem informacji, niezbędnym do realizacji działań, takich jak dydaktyka, obsługa dydaktyki, zatrudnianie, obsługa administracyjna i inne. We wszystkich obszarach funkcjonowania uczelni istnieje pilna potrzeba wdrożenia nowoczesnych zasad zarządzania bezpieczeństwem informacji.

Tematyka wdrażania polityki bezpieczeństwa informacji w organizacjach niebiznesowych typu uczelnie wyższe nie była dotąd podejmowana. Powodem zajęcia się tym problemem były wyniki badań wstępnych wśród uczelni technicznych w Polsce, gdzie większość wskazała na brak zarządzania ryzykiem naruszenia bezpieczeństwa informacji (jedna trzecia stosuje nieformalne procedury, inni zaś w ogóle nie zajmują się tą kwestią).

Z obserwacji wynika, że w szkolnictwie wyższym nie ma systemowego rozwiązania kwestii związanych z zarządzaniem bezpieczeństwem informacji, zatem wdrożenie takiego działania powinno być skierowanie jak najszybciej do uczelni, ponieważ utrata lub niepożądana modyfikacja informacji może być źródłem poważnych konsekwencji. Bardzo istotne dla uczelni jest zmniejszenie ryzyka informacji takich zagrożeń w podstawowej działalności.

W artykule przedstawiono wyniki badań w zakresie jednego z podstawowych elementów systemu bezpieczeństwa informacji, jakim jest wdrożenie polityki bezpieczeństwa informacji. Otrzymane rezultaty są częścią szerszego projektu realizowanego we wszystkich uczelniach technicznych w Polsce[2].

2. Metodyka badań

Podmiotem badań były polskie publiczne uczelnie techniczne, dla których utrata lub niepożądana modyfikacja informacji może być źródłem poważnych konsekwencji. Badania były przeprowadzone dla wszystkich wydziałów tych uczelni oraz wśród kanclerzy (dyrektorów administracyjnych) i dotyczyły stosowania zasad bezpieczeństwa informacji[3].

W wyniku przeprowadzonych analiz uznano, że spełnienie niezbędnych warunków doboru losowego jest zbyt pracochłonne i zbędne, bo w przypadku próby badania cech będących sednem przedmiotowego opracowania dotarcie do wszystkich podmiotów i wyegzekwowanie rzetelnego udziału w badaniu okazało się całkowicie realne. Dobór taki (uniwersum) nie odpowiada zasadom doboru losowego. Nie zmienia to faktu, że na podstawie tych wyników można formułować uprawnione twierdzenia, ponieważ są one weryfikowalne[4].

Ustalono liczność próby na poziomie 221 podmiotów. W przypadku tych badań wybrano 26 publicznych (wszystkie) uczelni technicznych (195 wydziałów + 26 kanclerzy). Poza tym ustalono, posiłkując się opra-

[2] Badania są wynikiem realizacji projektu badawczego, finansowanego przez Ministerstwo Nauki i Szkolnictwa Wyższego nr N115 062 32/2940.
[3] Badania zrealizowano jednokrotnie, nie mają charakteru ciągłego ani okresowego.
[4] A. Zeliaś, *Metody statystyczne*, Warszawa 2000, s. 13.

cowaniami literaturowymi, że taki poziom liczności próby jest optymalny do tego rodzaju i rozmachu badań, nawet gdy byłaby to liczność mająca zapewnić reprezentatywność przy doborze losowym, a nawet kwotowym (w przypadku badań, w których byłaby konieczność przebadania jedynie części populacji).

Do badań wykorzystano metodę ankiety elektronicznej (stworzono portal internetowy dedykowany na potrzeby badania). Narzędziem badawczym był ustrukturyzowany i wystandaryzowany kwestionariusz wypełniany elektronicznie przez respondentów. Respondentami byli dziekani, kanclerze badanych uczelni. Kwestionariusz był zbudowany według normy PN-ISO/IEC 17799:2007 oraz wytycznych wynikających w wymogów prawa w powiązaniu z zasadami związanymi ze specyfiką działania uczelni wyższych. Kwestionariusz zawierał pytania dotyczące obszarów związanych z wdrażaniem polityki bezpieczeństwa informacji, klasyfikacją przetwarzanych informacji, organizacją bezpieczeństwa w organizacji, bezpieczeństwem fizycznym i osobowym, przetwarzaniem informacji w systemach informatycznych, dostępem do informacji, bezpieczeństwem systemów i sieci, zgodnością zastosowanych rozwiązań w zarządzaniu informacją w organizacji z przepisami prawa. Ankieta zawierała 788 pytań pogrupowanych w odpowiednie kategorie tematyczne. Cały materiał podzielony został na 74 rozdziały, zagregowane w 16 sekcji. W każdym z rozdziałów było od kilku do kilkudziesięciu pytań zamkniętych. Każdy z rozdziałów (obszarów) stanowi pewien aspekt badanej rzeczywistości. Odpowiada on pewnej kategorii wymogów określonych prawem, normami i innymi standardami dobrych praktyk. Opracowane rozdziały są efektem analizy zasobów informacyjnych badanych jednostek oraz analizy zagrożeń i ryzyka.

Na ankietę odpowiedziało 135 jednostek (61% badanych), co – biorąc pod uwagę fakt dość niskiej świadomości w tym zakresie na uczelniach wyższych – wskazuje na ogromny postęp w kwestii zainteresowania badanych przedmiotowym zagadnieniem.

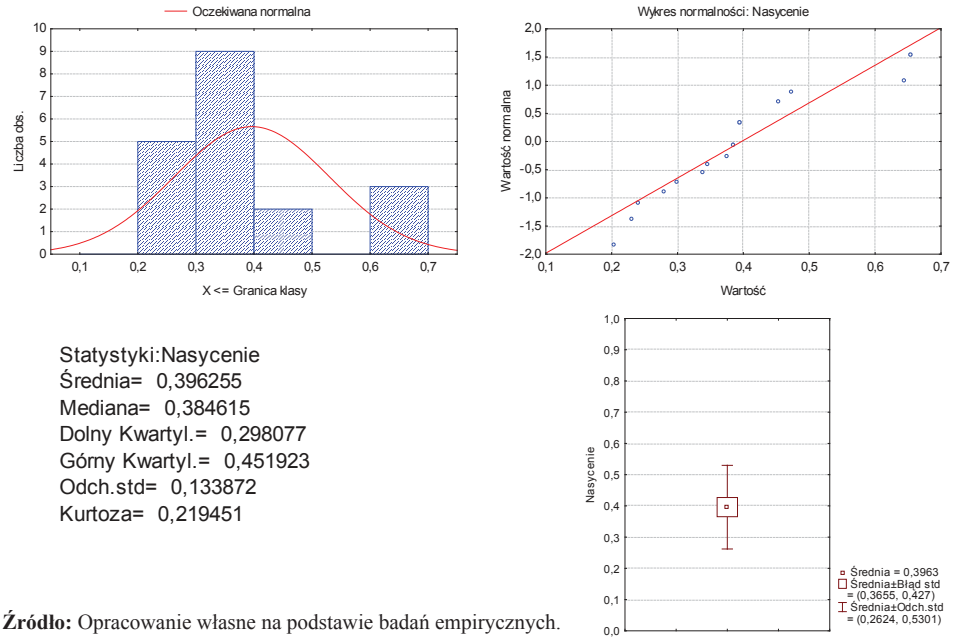
W opracowaniu zostały przedstawione cząstkowe wyniki badań odnoszące się do zagadnień związanych z kwestiami dotyczącymi wdrożenia polityki bezpieczeństwa informacji w technicznych uczelniach w Polsce.

3. Wyniki badań – ocena poziomu spełnienia wymogów w zakresie wdrożenia polityki bezpieczeństwa w uczelniach technicznych

Posługując się wynikami z przeprowadzonego badania, uzyskano wiedzę na temat przetwarzanych informacji oraz środków, jakie zostały podjęte w celu minimalizacji utraty atrybutów bezpieczeństwa informacji. Wynikiem realizacji tego etapu badań był raport obrazujący stan bezpieczeństwa systemów informacyjnych w badanych wyższych uczelniach technicznych. Raport ten zawiera informacje i obserwacje dotyczące faktycznego stanu bezpieczeństwa w badanych jednostkach, a ponadto uwzględnia wskazania dotyczące działań koniecznych do podjęcia w celu usystematyzowania i uporządkowania kwestii związanych z bezpieczeństwem informacji na wyższych uczelniach technicznych.

W kwestiach związanych z polityką bezpieczeństwa badane jednostki wykazały, że poziom spełnienia wymogów wynosi 39,6%. Szczegóły zostały przedstawione na rysunku 1.

Rysunek 1. Statystyki opisowe dla badanej sekcji (sekcja 3 – polityka bezpieczeństwa)



Źródło: Opracowanie własne na podstawie badań empirycznych.

Podano najważniejsze kwestie, w których respondenci udzielali najczęściej odpowiedzi świadczących o spełnieniu odpowiednich wymogów. 37,5% badanych stwierdziło, że istnieje w organizacji dokument polityki bezpieczeństwa informacji. Spośród nich 45,2% podało, że jest on zatwierdzony przez kierownictwo, opublikowany i udostępniony w odpowiedni sposób wszystkim pracownikom. Poniższe wnioski dotyczące odsetków populacji odnoszą się do tej jej części, która posiada dokument polityki bezpieczeństwa (owych 37,5%).

Ci, którzy posiadają dokument polityki, uznają, że zawiera:

1) definicje bezpieczeństwa informacji (ogólne cele, zakres, znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji – 47,1%),
2) oświadczenie o intencjach kierownictwa (potwierdzające cele i zasady bezpieczeństwa informacji – 39,4%),
3) krótkie wyjaśnienie polityki bezpieczeństwa (39,4%)
4) definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji (39,4%),
5) odsyłacze do dokumentacji mogącej uzupełniać politykę (38,5%).

Polityka bezpieczeństwa jest udostępniona użytkownikom w całej organizacji w formie właściwej, dostępnej i zrozumiałej dla czytelników, do których jest adresowana (39,4%). Ma ona właściciela, który jest odpowiedzialny za jej stosowanie i dokonywanie przeglądu według określonego procesu (38,5%). W organizacji występuje planowanie i wykonywanie okresowych przeglądów efektywności polityki (34,6%)

Poza tym za ważne uznano kwestie związane z tym, że są procedury dotyczące zabezpieczeń fizycznych pomieszczeń i obszarów przetwarzania informacji (65,4%), procedury dotyczące systemów informatycznych przetwarzających dane osobowe (65,4%) oraz procedury dotyczące zarządzania dostępem do poszczególnych informacji przetwarzanych przez organizację (64,4%), co potwierdza wcześniejsze wnioski uzyskane po analizie wyników z poprzednich sekcji.

4. Analiza sekcji zależnych

Zagadnienia prezentowane w badaniu funkcjonują w praktyce zarządczej nie autonomicznie, lecz komplementarnie z innymi. Zostało to ujęte przez połączenie poszczególnych kwestii w określone rozdziały, opisujące podobne znaczeniowo zagadnienia. Nie można jednak i tych rozdziałów traktować w oderwaniu od pozostałych. Wiele kwestii dotyczących bezpieczeństwa informacji opisywanych w poszczególnych rozdziałach jest uzależnionych od innych rozdziałów. Oznacza to, że konsekwencją celowych działań w pewnych obszarach winno być osiąganie wysokiego poziomu nasycenia w innych. Dla stworzonego zestawu zagadnień można wyróżnić istotne związki przyczynowo-skutkowe. Na potrzeby niniejszego opracowania w tabeli 1 przedstawiono przykładowo jedno z nich, odnoszące się do przedmiotowego obszaru dotyczącego polityki bezpieczeństwa informacji oraz powiązanych z nim znaczeniowo obszarów. Wskazując sekcje do analizy, spodziewano się uzyskać ciekawe związki i relacje zachodzące między przedmiotowymi zagadnieniami – nierozerwalnie ze sobą łączącymi się chociażby kwestiami wynikającymi ze standardów, dobrych praktyk oraz przepisów prawa.

Tabela 1. Przykład implikacji sekcji uwzględniający obszar dotyczący polityki bezpieczeństwa informacji

Poprzednik	**Poprzednik**	**Następnik**
Polityka bezpieczeństwa (sekcja 3)	Organizacja bezpieczeństwa (sekcja 4)	Zasady bezpieczeństwa informacji dotyczące współpracy uczelni z podmiotami zewnętrznymi w ramach realizacji badań naukowych, doradztwa, przedsięwzięć związanych z patentami, nowymi rozwiązaniami technicznymi i technologicznymi, pracami dyplomowymi itp. (sekcja 16)

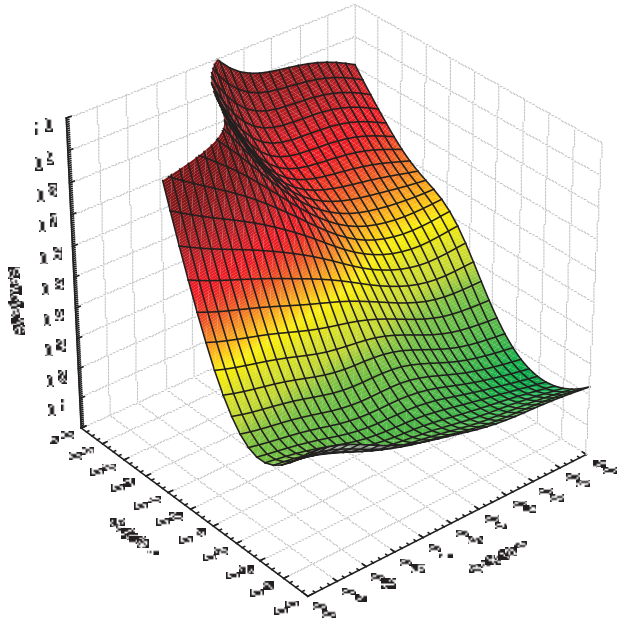
Źródło: Opracowanie własne.

Zakres implikowany (następnik)

Sekcja 16: Zasady bezpieczeństwa informacji dotyczące współpracy uczelni z podmiotami zewnętrznymi w ramach realizacji badań naukowych, doradztwa, przedsięwzięć związanych z patentami, nowymi rozwiązaniami technicznymi i technologicznymi, pracami dyplomowymi itp.

Poprzednik
Sekcja 3: Polityka bezpieczeństwa
Sekcja 4: Organizacja bezpieczeństwa

Rysunek 2. Zależność nasycenia w sekcji 16 od poziomów nasyceń w sekcjach 3 i 4



Źródło: Opracowanie własne.

W tym przypadku widać zależność silnej korelacji między poziomem nasycenia w zakresie organizacji bezpieczeństwa a sekcją 16, przy zupełnym braku zależności nasycenia w sekcji 16 od polityki bezpieczeństwa.

Fakt, że zostały stworzone jasno sprecyzowane procedury dotyczące współpracy uczelni z przemysłem, opracowano sposób postępowania z informacjami, które zostały pozyskane w ramach tworzenia nowych rozwiązań technicznych, technologicznych przez pracowników uczelni, dyplomantów, doktorantów itp., stworzono procedury postępowania z przemysłem, w sytuacji gdy uczelnia pełni funkcję doradcy naukowego, współpracuje z przemysłem na poziomie rozwiązań szczególnych, *know -how* itp. oraz że zostały stworzone procedury postępowania z informacjami pozyskanymi z przemysłu w ramach prowadzenia badań, projektów naukowych, doradztwa naukowego, wynika m.in. z tego, że:

1) w organizacjach powołane jest forum kierownicze, które wskazuje wyraźny kierunek działań i udziela wsparcia dla inicjatyw w dziedzinie bezpieczeństwa;
2) forum propaguje bezpieczeństwo wewnątrz organizacji przez odpowiednie zaangażowanie i przydzielanie zasobów;
3) w organizacjach za koordynowanie wszystkich działań związanych z bezpieczeństwem odpowiedzialny jest jeden z członków kierownictwa;
4) występuje koordynacja wdrażania zabezpieczeń informacji przez zespół złożony z przedstawicieli kadry kierowniczej poszczególnych działów organizacji;
5) zespół uzgadnia określone funkcje i zakres odpowiedzialności związany z bezpieczeństwem informacji w organizacji, metodyki i procesy związane z bezpieczeństwem informacji;
6) zespół przyjmuje i wspiera inicjatywy dotyczące zabezpieczeń informacji w całej organizacji, zapewnia włączenie bezpieczeństwa do procesu planowania informatycznego, ocenia adekwatność i koordynuje wdrażanie określonych środków zabezpieczania informacji w nowych systemach lub usługach;
7) zespół dokonuje przeglądu naruszeń bezpieczeństwa informacji oraz promuje w wyraźny sposób wsparcie dla bezpieczeństwa informacji w całej organizacji.

Poza tym zostały stworzone jasno sprecyzowane zasady dla stron ww. przedsięwzięć dotyczące zachowania poufności informacji: dyplomanci, doktoranci, promotorzy wiedzą, w jaki sposób postępować z informacjami pozyskanymi w ramach prac naukowych, tak aby zachować poufność danych. Zostały stworzone procedury dotyczące prac naukowych, projektów naukowych, patentów w zakresie przechowywania informacji, dostępu do informacji itp.

Procedury uczelni zapewniają zachowanie pełnej poufności informacji firmom zewnętrznym, z którymi lub dla których uczelnia prowadziła badania. Uczelnia każdorazowo dopełnia obowiązku poinformowania firm zewnętrznych, z którymi prowadzi współpracę w ramach ww. prac, o tym, w jaki sposób będą przechowywane informacje pozyskane w trakcie trwania prac oraz po ich ustaniu, a także w odniesieniu do produktów uzy-

skanych na każdym etapie tych prac. Na uczelniach zostały opracowane jasno sprecyzowane, ogłoszone do wiadomości wszystkich pracowników, studentów, dyplomantów, doktorantów, promotorów, zasady udostępniania wyników badań wykonywanych w ramach prac naukowych.

Wyniki analizy świadczą, że może to być efektem tego, że w organizacji została wyznaczona osoba odpowiedzialna za wdrażanie zabezpieczeń informacji, która:

1) uzgadnia określone funkcje i zakres odpowiedzialności związany z bezpieczeństwem informacji,
2) uzgadnia określone metodyki i procesy związane z bezpieczeństwem informacji,
3) przyjmuje i wspiera inicjatywy dotyczące zabezpieczeń informacji w całej organizacji,
4) zapewnia włączenie bezpieczeństwa do procesu planowania informatycznego,
5) ocenia adekwatność i koordynuje wdrażanie określonych środków zabezpieczania informacji w nowych systemach lub usługach,
6) dokonuje przeglądu naruszeń bezpieczeństwa informacji,
7) promuje w wyraźny sposób wsparcie dla bezpieczeństwa informacji w całej organizacji.

Przedstawione zależności (korelacje) niekoniecznie zachodzą wprost. To przykład powiązania pomiędzy poszczególnymi obszarami dotyczącymi bezpieczeństwa informacji, które muszą zostać w organizacji uwzględnione podczas procesu definiowania i wdrażania zasad bezpieczeństwa informacji. Często są to związki przechodnie polegające na tym, że podobieństwo trendów w konkretnych sekcjach może być spowodowane czynnikiem innym niż rzeczywista wzajemna zależność. Przy analizie wpływu (implikacji) zawsze istnieje ryzyko takiej interpretacji. W przypadku poruszanych w tym opracowaniu problemów nie ma większego znaczenia, czy zależność między pewnymi cechami jest zależnością wprost, czy przechodnią. Wynika to z tego, że zagadnienia ze wszystkich badanych sekcji w istotny sposób oddziałują na siebie. Ważne jest natomiast, czy w najistotniejszych kwestiach zachodzą zależności wzajemnego wpływu. Do zidentyfikowania tego wystarczą analizy takie jak przedstawiona powyżej.

Wybrane kombinacje sekcji zostały tak dobrane, aby w jak najlepszy sposób zidentyfikować, czy pozytywne rezultaty w jakiejś dziedzinie są efektem celowych działań w innej zależnej dziedzinie (wtedy istnieje duże prawdopodobieństwo, że organizacje poprawnie interpretują zasady bezpieczeństwa informacji), czy też zbieżność jest efektem przypadkowym.

Bibliografia

Babbie E., *Badania społeczne w praktyce*, Warszawa 2003.

Czerwiński K., Grocholski H., *Podstawy audytu wewnętrznego*, Szczecin 2003.

Ćwiklicki M., *Koncepcja zarządzania elektronicznymi zasobami informacyjnymi w przedsiębiorstwie*, Zeszyty Naukowe – Akademia Ekonomiczna w Krakowie 2003, nr 616.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

Lacheta M., Molski M., *Przewodnik audytora systemów informatycznych*, Gliwice 2006.

Nawojczyk M., *Przewodnik po statystyce dla socjologów*, Kraków 2002.

Papkin D.L., *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, Warszawa 2002.

Polaczek T., *Audyt bezpieczeństwa informacji w praktyce*, Gliwie 2006.

Tinnefeld M., *Państwo, bezpieczeństwo, informacja i ochrona danych*, Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji 2004, t. 59.

Zarządzanie organizacjami. Kulturowe uwarunkowania zarządzania zasobami ludzkimi, K. Konecki, P. Chomczyński (red.), Łódź 2007.

Zeliaś A., *Metody statystyczne*, Warszawa 2000.