Kesra Nermend, Imed El Fray

Rola bezpieczeństwa i ochrony danych w rozwoju regionalnym

Ekonomiczne Problemy Usług nr 71, 289-301

2011

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 655 EKONOMICZNE PROBLEMY USŁUG NR 71 2011

KESRA NERMEND
Uniwersytet Szczeciński
IMED EL FRAY
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

ROLA BEZPIECZEŃSTWA I OCHRONY DANYCH W ROZWOJU REGIONALNYM

Wprowadzenie

Tematyka rozwoju regionalnego nabrała szczególnego znaczenia w kontekście wstąpienia Polski do Unii Europejskiej, głównie ze względu na konieczność osiągnięcia w stosunkowo krótkim czasie standardów zbliżonych do tych, jakie obowiązują w krajach członkowskich. Mimo że uruchomiono wiele programów pomocowych, to istniejące dysproporcje są tak duże, że władze samorządowe muszą w sposób istotny włączać się w proces dostosowawczy. Skuteczne wspieranie tego procesu wymaga przede wszystkim właściwego zdiagnozowania i oceny aktualnego poziomu rozwoju regionalnego, a następnie zaplanowania działań zmierzających do wyeliminowania dysproporcji.

W niniejszym artykule pod pojęciem rozwoju regionalnego rozumie się „trwały wzrost poziomu życia mieszkańców i potencjału gospodarczego w skali określonej jednostki terytorialnej”[1]. Diagnoza i ocena poziomu

[1] T. Kudłacz, *Programowanie rozwoju regionalnego*, Warszawa 1999. Inne definicje patrz w bibliografii pozycje: J. Kudełko; K. Secomski; M. Markowska; M. Pięta; J. Kaj, K. Piech; A. Jewtuchowicz; S. Korenik; K. Gawlikowska-Hueckel; W. Dziemianowicz; J. Chądzyński, A. Nowakowska, Z. Przygodzki; J. Adamiak, W. Kosiedowski, A. Potoczek, B. Słowińska.

rozwoju regionalnego jest zadaniem bardzo trudnym, a stosowane do tego metody powinny pozwalać na jednoczesne uwzględnianie wielu czynników (ekonomicznych, środowiskowych, politycznych, infrastrukturalnych, demograficznych oraz technologicznych) składających się na rozwój regionalny. W artykule autorzy koncentrują się głównie na czynnikach technologicznych, zwłaszcza tych warunkujących rozwój społeczeństwa informacyjnego. Według jednej z definicji społeczeństwo informacyjne to „społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła utrzymania większości społeczeństwa”[2]. Społeczeństwo informacyjne po raz pierwszy zostało zdefiniowane w tzw. raporcie Bangemanna[3]. Tym mianem określa się społeczeństwo nowoczesnego, wysoko rozwiniętego państwa, w którym istnieje rozbudowana infrastruktura teleinformacyjna, umożliwiająca pełny dostęp do usług i informacji. Wraz z rozwojem społeczeństwa informacyjnego powiększają się zasoby danych i informacji, gromadzone w różnych systemach informatycznych. Zagrożeniem dla tych zasobów, niejednokrotnie bardzo istotnych ze względu na bezpieczeństwo państwa, gospodarki i obywateli, mogą być różnego rodzaju ataki. Ich odparcie wymaga zapewnienia ochrony na pożądanym poziomie. Niestety, większość jednostek na szczeblu regionalnym nie dostrzega konieczności wdrożenia odpowiednich zabezpieczeń opartych na wynikach analizy ryzyka (lub nie ma odpowiednich środków i wiedzy). Brak spójnej polityki bezpieczeństwa na tym szczeblu dotyczącej ochrony zgromadzonych danych oraz niepodejmowanie odpowiednich kroków w tym kierunku może mieć nieodwracalne, negatywne skutki.

Biorąc pod uwagę możliwe zagrożenia i podatność systemów informacyjnych jednostek samorządów terytorialnych w obszarze ochrony danych i informacji w różnych jej postaciach, autorzy niniejszego referatu przedstawią ogólny przegląd na temat istniejącego stanu bezpieczeństwa oraz techniki zarządzania bezpieczeństwem systemów informacyjnych i monitorowania ich, w tym budowę i wdrażanie polityki bezpieczeństwa i ochrony danych w tych instytucjach.

[2] K. Nermend, *Vector Calculus in Regional Development Analysis*, Berlin–Heidelberg 2009.

[3] M. Bangemann i in., *Europe and the Global Information Society*, <http://www.cyber-rights.org/documents/bangemann.htm> [data dostępu: 13.04.2010].

Przegląd istniejącego stanu bezpieczeństwa w organizacji na przykładzie jednostek samorządu terytorialnego

Jak wynika z raportów z analiz[4], do najczęściej spotykanych przyczyn szkód należą nadal błędy ludzkie, które stanowią prawie 50%, najczęściej powodowane przez pracowników – ok. 70%. Pomimo utrzymywania się wciąż wysokiego odsetka błędów ludzkich jako przyczyn szkód i pracowników jako ich sprawców, zaobserwowano jednak w latach 2005–2009 tendencję spadkową o około 5–10%. Większość szkód organizacji nadal powodują ludzie, jednak często zupełnie nieświadomie. Jak wynika z opublikowanych, cytowanych wyżej, raportów, stwierdzono również wzmożoną aktywność kierownictwa organizacji w rozwiązywaniu problemów związanych z bezpieczeństwa danych i informacji. Dane wskazują, że około 75% kadry kierowniczej ma świadomość potrzeby wdrażania polityki bezpieczeństwa i czynnego udziału w jej realizacji (z analiz z 2005 roku wynika, że około 40% kierowników nie widziało potrzeby czynnego udziału w spotkaniach poświęconych bezpieczeństwu informacji). Pomimo dużego zaangażowania kierownictwa w rozwiązywanie problemów bezpieczeństwa w obrębie własnych organizacji, co skutkowało wyraźnie mniejszymi stratami, nadal duże zaniepokojenie budzi rosnąca liczba prób ataków na systemy organizacji, a przede wszystkim zaobserwowany ostatnio wysoki stopień znajomości świata biznesu wśród przestępców, a także ich zdolności techniczne wykorzystywane do zwiększenia skali działania oraz unikania wykrycia. Główne powody ataków to nadal chęć wzbogacenia się i zdobywania ważnych danych i informacji, w tym również biznesowych. Proporcje te, w porównaniu do analiz z 2005 roku[5], są prawie na tym samym poziomie (około połowy wszystkich przestępstw komputerowych to kradzież pieniędzy, około 15–20% to kradzież danych, 10% dotyczy modyfikacji danych itp.). Niektóre jednostki samorządowe wprowadziły już politykę bezpieczeństwa, jednak samo wdrożenie nie rozwiązuje problemu. Potrzebne jest przede wszystkim egzekwowanie zasad i procedur

[4] <http://www.ey.com/PL/pl/Newsroom/News-releases/PR10_GISS-2009> [data dostępu: 02.04.2010]; <http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2009.pdf > [data dostępu: 02.04.2010]; < http://www.symantec.com/about/news/release/article.jsp? prid=20070205_01> [data dostępu: 02.04.2010].

[5] <http://www.ey.com/PL/pl/Newsroom/News-releases/PR10_GISS-2005> [data dostępu: 02.05.2006].

bezpieczeństwa zawartych w tej polityce. Do czynników najbardziej sprzyjających niestosowaniu się do procedur i zasad bezpieczeństwa, a w konsekwencji utracie danych i informacji, należą: użycie bez kontroli m.in. urządzeń przenośnych, wymiennych nośników, sieci bezprzewodowych itd. Zasady polityki bezpieczeństwa, rozumiane przez większość jednostek samorządowych, nie kończą się tylko na ochronie informacji w formie elektronicznej, ale również ochronie informacji w formie papierowej[6]. Utrata dokumentów dotyczących np. strategii inwestycyjnych, planów finansowych czy zbiorów danych osobowych mieszkańców jest przestępstwem surowo karanym prawem, a jednocześnie są to informacje niezwykle pożądane przez różne firmy itp.

Po zapoznaniu się z tymi analizami i mając świadomość, że tylko niespełna 15% organizacji z Europy brało udział w tych badaniach oraz wiedząc, że liczba ataków, także coraz bardziej wyrafinowanych, z roku na rok podwaja się, bez względu na to, czy celem ataku jest prywatna firma, instytucja finansowa, rządowa, czy nawet militarna, powstaje przekonanie, że wdrażanie polityki bezpieczeństwa w instytucjach samorządowych, towarzyszących jej procedur, szkoleń, audytów itp. jest niezbędne i nieuniknione.

Polityka bezpieczeństwa informacji w jednostkach samorządu terytorialnego

Polityka bezpieczeństwa jest zbiorem dokumentów o znaczeniu strategicznym zawierającym cele, strategie oraz zakres działań zgodnych z obowiązującym prawem, przepisami i procedurami, będących konsekwencją działania i nadzoru, warunkujących możliwość efektywnego i całościowego zarządzania bezpieczeństwem informacji w przedsiębiorstwie[7]. Istotne znaczenie dla wdrażania polityki bezpieczeństwa ma zrozumienie przez pracowników, do czego służą procedury bezpieczeństwa i kiedy należy je stosować. Dlatego też konieczne są okresowe szkolenia z zakresu bezpieczeństwa i ochrony danych. Pracownicy muszą być informowani o przyjętych przez pracodawcę procedurach i zasadach ochrony danych, ponieważ pozwoli to na uświadomienie, jakie zagrożenia i ryzyka są związane z ich codziennymi obowiązkami

[6] <www.pbsg.pl> [data dostępu: 14.04.2010].

[7] Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management ISO/IEC 13335–1:2004.

i wykonywanymi czynnościami, a tym samym na zwiększenie efektywności wykorzystywania istniejących systemów zabezpieczeń.

Aby opracować dokument polityki bezpieczeństwa, należy przeprowadzić analizę ryzyka w zakresie prowadzonej przez instytucję działalności, wykorzystywanej technologii informatycznej, obiegu informacji oraz zdefiniować cele strategiczne, standardy i normy, a także strategie realizacji zadań ochrony informacji. Jak już wspomniano, niektóre jednostki samorządowe wdrażały wcześniej politykę bezpieczeństwa, jednak nie była ona oparta na wynikach przeprowadzonej analizy ryzyka, a jedynie na punktach kontrolnych zawartych w normie ISO/IEC 27001[8]. Działania takie nie są wiarygodne, ponieważ nie odzwierciedlają rzeczywistego stanu zagrożeń, ryzyka, panującego w jednostce itp.

Prawidłowo wdrożona polityka bezpieczeństwa powinna być zbudowana według następujących wytycznych[9]:

- identyfikacja i klasyfikacja zasobów jednostki;
- identyfikacja zagrożeń, na jakie podatny jest system informacyjny jednostki;
- analiza i ocena ryzyka związanego z bezpieczeństwem systemu informacyjnego jednostki (powinny być oparte na odpowiednio dobranej metodzie analizy ryzyka);
- dobranie zabezpieczeń adekwatnych do wyników oceny ryzyka;
- wyznaczenie osoby odpowiedzialnej związanej z bezpieczeństwem systemu informacyjnego jednostki;
- opracowanie dokumentu polityki bezpieczeństwa informacji;
- edukacja i szkolenia personelu w dziedzinie bezpieczeństwa informacji;
- zgłaszanie przypadków naruszenia bezpieczeństwa;
- zarządzanie ciągłością działania jednostki;
- monitorowanie poziomu ryzyka, wykorzystania zabezpieczeń i ich efektywności.

[8] Information technology – Security techniques – information security management systems, ISO/IEC 27001:2005.

[9] Tamże.

Analiza ryzyka

Zalecenie ISO/IEC nr 73 definiuje ocenę ryzyka jako proces złożony z analizy ryzyka oraz jego ewaluacji[10]. Analiza ryzyka jest procesem identyfikacji opisu i pomiaru ryzyka. Identyfikacja wymaga szczegółowej wiedzy na temat jednostki, dogłębnego zrozumienia jej celów strategicznych i operacyjnych, w tym czynników kluczowych do osiągnięcia powodzenia oraz zagrożeń i szans związanych z realizacją tych celów. Opis zidentyfikowanych źródeł ryzyka powinien być przedstawiony w czytelnej formie, np. w postaci tabeli ułatwiającej przejrzystą prezentację i ewaluację poszczególnych źródeł ryzyka[11].

Rozważając skutki i prawdopodobieństwo realizacji poszczególnych niebezpieczeństw, można zdefiniować priorytety, to jest wybrać najważniejsze źródła ryzyka, które należy poddać bardziej szczegółowej analizie i dokonać pomiaru ich wag. Pomiar ryzyka można przedstawić w postaci ilościowej lub jakościowej. Rysunek 1 przedstawia znaną metodę CRAMM stosowaną do analizy ryzyka.

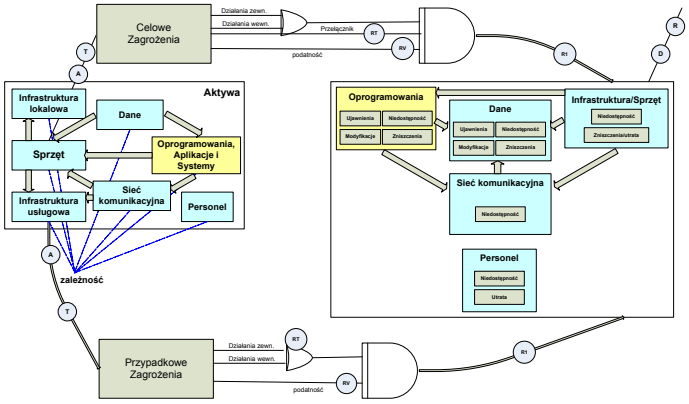
Pomiar ten wymaga tworzenia schematów klasyfikowania zagrożeń i podatności na nie systemu informacyjnego jednostki. Uwzględniając te wartości w macierzach, tworzymy macierz ryzyka (rys. 2).

Ostatnim etapem procesu analizy ryzyka jest opracowanie profilu, w którym każdemu źródłu ryzyka jest przypisana ocena opisująca jego znaczenie. Profil ryzyka porządkuje zatem zidentyfikowane pod względem istotności oraz stanowi narzędzie do określenia priorytetów działania względem ryzyka. W procesie konstruowania profilu następuje przypisanie źródeł ryzyka do poszczególnych dziedzin działalności, a także wskazanie podstawowych mechanizmów kontrolnych oraz obszarów, w jakich należy zwiększyć, zmniejszyć lub zreorganizować wydatki związane z kontrolowaniem ryzyka. Ewaluacja ryzyka zatem stanowi podstawę do podjęcia decyzji co do tego, na ile dane ryzyko jest dla organizacji istotne, a także czy należy je przyjąć i jakie działania względem niego podjąć. Postępowanie takie wymaga porównania szacunkowej wielkości ryzyka z przyjętymi przez organizację kryteriami. Kryteria te

[10] Risk Management – Vocabulary – Guidelines for use in standards, ISO/IEC Guide 73:2002.

[11] *Risk Management Standard*, Federation of European Risk Management in Dynamic Open Systems, London 2003.

mogą dotyczyć kosztów i korzyści, wymogów prawnych itp. Zakończeniem procesu oceny ryzyka jest ponowna analiza, tzw. analiza ryzyka szczątkowego. Jest przeprowadzana po podjęciu decyzji przez jednostkę o doborze i implementacji podstawowych mechanizmów zabezpieczających, tam gdzie obliczona waga ryzyka dla danego scenariusza jest nieakceptowana.



Rys. 1. Metoda analizy ryzyka CRAMM

Źródło: *CCTA Risk Analysis and Management Method CRAMM*, Central Computing and Telecommunications Agency, United Kingdom Government, UK 1987.

Zagrożenie		B.M	B.M	B.M	M	M	M	S	S	S	W	W	W	B.W.	B.W	B.W
Podatność		M	S	W	M	S	W	M	S	W	M	S	W	M	S	W
Aktywa / Wartość	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
	2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
	3	1	2	2	2	2	2	2	3	3	3	3	4	3	4	4
	4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
	5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
	6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
	7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
	8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
	9	4	5	5	5	5	6	5	6	6	6	6	7	6	7	7
	10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

B.M - Bardzo mała, **M** - Mała, **S** - Średnia, **W** - Wysoka, **B.W** - Bardzo wysoka,

Rys. 2. Macierz ryzyka według CRAMM

Źródło: *CCTA Risk Analysis and Management Method CRAMM*, dz. cyt.

Budowa polityki bezpieczeństwa w jednostce samorządu terytorialnego

Warunkiem budowy polityki bezpieczeństwa w jednostkach samorządu terytorialnego jest zaangażowanie wszystkich stron – od starosty, prezydenta, wójta aż po portiera[12]. Bez ich akceptacji i pomocy nie da się ustanowić skutecznej polityki bezpieczeństwa. Ważnym argumentem dla aktywizacji działań starosty, prezydenta, wójta w tym kierunku jest fakt, że to właśnie oni ponoszą odpowiedzialność za bezpieczeństwo teleinformatyczne w jednostce. Drugim ważnym krokiem jest spełnienie wymogów:

– Ustawy o ochronie danych osobowych z dnia 27 sierpnia 1997 r. (Dz. U., 2002 r., Nr 101, poz. 925 z późn. zm.);
– Rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. (Dz. U., 2004, Nr 100, poz. 1024), zawartych w części „Polityka bezpieczeństwa", w tym „Polityka bezpieczeństwa informacji" i „Polityka bezpieczeństwa systemu teleinformatycznego".

Budowa polityki bezpieczeństwa informacji w jednostkach samorządu terytorialnego polega na stopniowym opracowywaniu sposobów zabezpieczenia zasobów informacyjnych przez nie zgromadzonych, kierując się zasadą od ogólności do szczegółowości. Dokument polityki bezpieczeństwa informacji powinien dotyczyć wszystkich funkcjonujących procesów przetwarzania informacji w jednostce. Pomocne przy budowie polityki są wyniki analizy ryzyka przeprowadzone wcześniej.

Prace nad polityką bezpieczeństwa należy rozpocząć od zdefiniowania, tak jak w normach ISO, pojęć, skrótów itd., które będą użyte w dokumencie. Kolejnym krokiem jest określenie wszystkich zachodzących w jednostce procesów, w tym:

– przetwarzania informacji;
– składowania i archiwizacji informacji, w tym metod stosowanych do ich archiwizacji;
– obiegu informacji;
– pozyskiwania i udostępniania informacji, w tym zasad związanych z bieżącym wewnętrznym dostępem i dostępem do archiwum informacji;

[12] K. Nermend, I. El Fray, *Znaczenie bezpieczeństwa informacji dla prawidłowego funkcjonowania jednostek samorządu terytorialnego*, Zeszyty Naukowe PWSZ w Kaliszu (w druku).

– wymiany informacji z podmiotami zewnętrznymi;
– kontroli dostępu do informacji i stosowanych zabezpieczeń.

Realizacja zadań statutowych wymaga zagwarantowania odpowiedniego poziomu bezpieczeństwa dla procesów przedstawianych wyżej. Tak więc oprócz ich oczywistej ochrony i powiązanych z nimi zasobów teleinformatycznych ważna jest także ochrona jednostki na takim poziomie, aby mogła ona nieprzerwanie działać. Ochrona jednostki powinna być budowana na trzech, w zasadzie niezmiennych, poziomach[13]:
– bezpieczeństwie jednostki;
– bezpieczeństwie teleinformatycznym jednostki;
– bezpieczeństwie systemów jednostki.

W przypadku pierwszego poziomu w skład polityki wchodzą takie elementy, jak: polityka działania instytucji wynikająca z jej celów i strategii istnienia, polityka finansowa, polityka zastosowania zasobów teleinformatycznych w jednostce, jak również inne wynikające ze specyfiki jednostki, takie jak normy prawne, zwłaszcza przepisy bądź umowy. Na drugim poziomie polityka rozumiana jest jako prawa, zasady postępowania i ochrony dotyczące systemów i zasobów teleinformatycznych w całej instytucji, w tym informacji niejawnych i wrażliwych, wszelkich usług ze szczególnym uwzględnieniem usług krytycznych dla istnienia i działania jednostki. Trzeci z kolei poziom polityki bezpieczeństwa dotyczy bezpieczeństwa dla systemów w jednostce. Powstający dokument lub dokumenty polityki bezpieczeństwa dla konkretnego systemu lub systemów powinny wynikać z polityk poziomu pierwszego i drugiego. Przykładowymi rodzajami tworzonych dokumentów są m.in. procedury:
– korzystania z komputerów, internetu czy poczty, w tym zasady tworzenia haseł i częstotliwość ich zmiany, nadawania uprawnień, uwierzytelniania użytkowników w sieciach itp.;
– reakcji na incydenty i odzyskiwanie systemów po awarii na podstawie tworzonych kopii zapasowych i awaryjnych.

Jak można zauważyć, tworzenie polityki bezpieczeństwa informacji polega z jednej strony na ewolucyjnym postępie w budowie i zabezpieczaniu dostępu do informacji zgromadzonych przez organizację, a z drugiej

[13] J. Papińska-Kacperek, *Społeczeństwo informacyjne*, Warszawa 2008.

na zwiększeniu świadomości pracowników w odniesieniu do wartości danych osobowych itp. Często zdarza się, że działania podwyższające bezpieczeństwo powodują obniżenie wygody użytkowników. Np. wprowadzenie obowiązku częstszego używania haseł w danym roku lub kilku haseł w razie korzystania z różnych systemów może spowodować łamanie zaleceń przez personel, np. poprzez zapisywanie hasła na kartkach. Dlatego równie ważne jak działania jest tworzenie klimatu do szkolenia użytkowników i uświadamianie ich odnośnie do bezpieczeństwa teleinformatycznego. Świadomy użytkownik jest w stanie zaakceptować dodatkowe utrudnienia, jeśli zrozumie, w jakim celu zostały wprowadzone. Będzie również mniej podatny na wszelkie działania inżynierii społecznej, a także będzie szybciej identyfikował i reagował na incydenty. Poziom szkoleń z zakresu bezpieczeństwa powinien być zróżnicowany dla różnych grup personelu. Inny poziom i zakres szkoleń będzie potrzebny pracownikom zajmującym się wdrażaniem zasad bezpieczeństwa, inny szeregowym pracownikom czy też kadrze kierowniczej.

Osiągnięcie założonego poziomu bezpieczeństwa nie kończy realizacji przyjętej polityki bezpieczeństwa. Proces taki ma charakter ciągły i wymaga systematycznej kontroli, analizy i weryfikacji. W przypadku zabezpieczeń, które w dużej mierze opierają się na nowoczesnej technologii, rodzi się pytanie, jak długo zastosowane rozwiązania będą jeszcze skuteczne. Dlatego co jakiś czas powinna zostać przeprowadzona weryfikacja polityki bezpieczeństwa oraz wszystkich mechanizmów zabezpieczeń.

Podsumowanie

W społeczeństwie informacyjnym wraz z rozwojem systemów informatycznych i internetu wyraźnie widać stały wzrost zagrożeń dla bezpieczeństwa informacji. Przedsiębiorstwa, prywatne firmy oraz organizacje rządowe, w tym jednostki samorządu terytorialnego, za jedno z najważniejszych aktywów biznesowych uważają informacje, które przetwarzają i przechowują. Polityka bezpieczeństwa informacji stanowi swoisty zbiór metod i zasad ochrony oraz zapewnienia bezpieczeństwa informacji. Umożliwia zorganizowanie i bezpieczne gromadzenie, przetwarzanie, przesyłanie i przechowywanie informacji. Powinna być ciągle aktualizowana i stanowić dokument czytelny

i zrozumiały dla wszystkich pracowników jednostki. Każda jednostka winna budować zasoby informacyjne, zarządzać nimi i udostępniać je na podstawie zbioru procedur wskazujących elementy, które powinny zostać nią objęte[14]. Polityka bezpieczeństwa w instytucji powinna spełniać oczekiwania właściciela i pozwalać na szybkie wskazywanie możliwości naruszenia bezpieczeństwa informacji w przyszłości, a także na przygotowanie odpowiednich działań i procedur o charakterze organizacyjnym i technicznym, które pozwolą uniknąć powtórzenia się danego zdarzenia.

Literatura

Adamiak J., Kosiedowski W., Potoczek A., Słowińska B., *Zarządzanie rozwojem regionalnym i lokalnym, problemy teorii i praktyki*, Toruń 2001.

Bangemann M. i in., *Europe and the Global Information Society*, <http://www.cyber--rights.org/documents/bangemann.htm>.

CCTA Risk Analysis and Management Method CRAMM, Central Computing and Telecommunications Agency, United Kingdom Government, UK 1987.

Chądzyński J., Nowakowska A., Przygodzki Z., *Region i jego rozwój w warunkach globalizacji*, Warszawa 2007.

Dziemianowicz W., *Kapitał zagraniczny a rozwój regionalny i lokalny w Polsce*, Warszawa 1997.

Gawlikowska-Hueckel K., *Procesy rozwoju regionalnego w Unii Europejskiej*, Gdańsk 2003.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999.

Information technology – Security techniques – information security management systems, ISO/IEC 27001:2005.

Jewtuchowicz A., *Terytorium i współczesne dylematy jego rozwoju*, Łódź 2005.

Kaj J., Piech K. (red.), *Rozwój oraz polityka regionalna i lokalna w Polsce*, Warszawa 2005.

Korenik S., *Dysproporcje w rozwoju regionów Polski – wybrane aspekty*, Wrocław 2003.

Kowalewski M., Ołtarzewska A., *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego*, „Telekomunikacja i Techniki Informacyjne" 3–4/2007.

[14] M. Kowalewski, A. Ołtarzewska, *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego*, „Telekomunikacja i Techniki Informacyjne" 3–4/2007.

Kudełko J., *Poziom rozwoju społeczno-gospodarczego województw Polski*, Zeszyty Naukowe Akademii Ekonomicznej w Krakowie, nr 651, Kraków 2004.

Kudłacz T., *Programowanie rozwoju regionalnego*, Warszawa 1999.

Markowska M., *Czynniki rozwoju regionalnego*, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, nr 939, Wrocław 2002.

Nermend K., *Vector Calculus in Regional Development Analysis*, Berlin–Heidelberg 2009.

Pięta M., *Czynniki i uwarunkowania kształtujące rozwój regionu ekonomicznego*, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, nr 938, Wrocław 2002.

Nermend K., El Fray I., *Znaczenie bezpieczeństwa informacji dla prawidłowego funkcjonowania jednostek samorządu terytorialnego*, Zeszyty Naukowe PWSZ w Kaliszu (w druku).

Papińska-Kacperek J., *Społeczeństwo informacyjne*, Warszawa 2008.

Raport Bezpieczeństwa, Cisco 2009, <http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2009.pdf>.

Risk Management Standard, Federation of European Risk Management in Dynamic Open Systems, London 2003, <http://www.theirm.org/publications/documents/ARMS_2002_IRM.pdf >.

Risk Management – Vocabulary – Guidelines for use in standards, ISO/IEC Guide 73:2002.

Secomski K., *Teoria regionalnego rozwoju i planowania*, Warszawa 1987.

Symantec IT Risk Management Report, Symantec 2007, <http://www.symantec.com/about/news/release/article.jsp? prid=20070205_01>.

Światowe badanie bezpieczeństwa informacji, Raport 2009, Ernst & Young, <http://www.ey.com/PL/pl/Newsroom/News-releases/PR10_GISS-2009>

THE ROLE OF SECURITY AND DATA PROTECTION IN REGIONAL DEVELOPMENT

Summary

This article contains a brief survey of the different methods and approaches for the risk evaluation and analysis. Proposed idea should be particularly useful in local governmental unit systems. Such systems can consist of many separated subsystems with completely different security mechanisms. In this article, was proposed to verify the quality and integration of these mechanisms on the basis of the initial risk analysis. The purpose of the article is to present the concept of a construction of a coherent security policy for these units based on the results of the risk analysis.

Translated by Imed El Fray