Zeszyty Naukowe Wydziału Informatyki
Wyższej Szkoły Informatyki Stosowanej i Zarządzania
„Informatyka Stosowana”
Nr 1/2014

WYKORZYSTANIE STANDARDU PCI DSS ORAZ NORMY ISO/IEC 27001 W CELU ZAPEWNIENIA BEZPIECZEŃSTWA INFORMACJI

Tomasz Brożek, Jarosław Sikorski, Grzegorz Stanio

Wyższa Szkoła Informatyki Stosowanej i Zarządzania,
01-447 Warszawa, ul. Newelska 6

Streszczenie

W artykule poruszono zagadnienia, związane z zarządzaniem bezpieczeństwem informacji w organizacjach w kontekście wdrożenia i wykorzystywania określonych standardów bezpieczeństwa informacji. Przeprowadzono analizę porównawczą, dotyczącą wymagań, występujących w standardach bezpieczeństwa PCI DSS oraz ISO/IEC 27001. Na podstawie tej analizy sformułowano wnioski, odnoszące się do własności oraz zastosowania obu rozważanych standardów.

Słowa kluczowe: informacja, bezpieczeństwo, standardy, zarządzanie

1. Wstęp

Współczesny wzrost znaczenia i wartości informacji (por. np. Anderson, 2000) wymusza na organizacjach konieczność zapewnienia wyższego poziomu ich ochrony poprzez implementację zróżnicowanych mechanizmów bezpieczeństwa. Jedną z możliwości realizacji tego zadania jest uzyskanie zgodności z przygotowanymi w tym celu standardami, takimi jak np. Payment Card Industry Data Security Standard (PCI DSS), lub ISO/IEC 27001. Kluczowym czynnikiem sukcesu w tym zakresie jest wdrożenie adekwatnych zabezpieczeń, odpowiadających celom biznesowym danej organizacji. Temu właśnie istotnemu zagadnieniu poświęcony jest niniejszy krótki artykuł.

2. Bezpieczeństwo informacji

2.1. Pojęcie bezpieczeństwa informacji

Zachowanie bezpieczeństwa informacji (Polski Komitet Normalizacyjny, 2007) należy rozumieć jako zapewnienie występowania trzech następujących własności w odniesieniu do informacji: poufności, integralności i dostępności, które to własności są rozumiane jako:

Poufność (ang. *confidentiality*) – zapewnienie dostępu do informacji tylko osobom do tego upoważnionym.

Integralność (ang. *integrity*) – zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.

Dostępność (ang. *availability*) – zapewnienie osobom upoważnionym wglądu do informacji wtedy, gdy to jest potrzebne.

Powyższe atrybuty, ze względu na ich angielską pisownię, są często nazywane łącznie triadą CIA, która to triada jest podstawą wszystkich rozważań związanych z bezpieczeństwem informacji. W niektórych sytuacjach (por. Polski Komitet Normalizacyjny, 1999), mogą zostać również uwzględnione określone dodatkowe atrybuty, takie jak, w szczególności: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

W celu zachowania tych własności opracowywane i wdrażane są odpowiednie mechanizmy zabezpieczeń odnoszące się do różnego rodzaju zagrożenia i podatności. Należy zwrócić uwagę na fakt, że należy poddać ochronie nie tylko informacje, ale również całe środowiska, w których one występują. Składniki tych środowisk można w skrócie przedstawić (Clinch, 2009) używając symbolu 4P, który jest rozwijany jako: ludzie (ang. *people*), procesy (ang. *processes*), produkty (ang. *products*) oraz kontrahenci (ang. *partners*). Z każdym z tych składników związane są obszary bezpieczeństwa, które dotyczą ochrony informacji.

2.2. System Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji (SZBI), Łuczak i Tyburski (2010), można określić jako systematyczne podejście do zarządzania kluczowymi informacjami firmy w celu zapewnienia dla nich należytego poziomu ochrony. Jego podstawą jest wykorzystanie analizy ryzyka w celu identyfikacji kluczowych zagrożeń i podatności oraz optymalizacji stosowanych zabezpieczeń. Dzięki temu możliwe jest zróżnicowanie metod realizacji ochrony w zależności od istotności informacji, z którymi mamy do czynienia.

Niewątpliwą zaletą SZBI (Białas, 2007) jest możliwość integracji celów biznesowych organizacji z wymaganiami dotyczącymi zapewnienia odpowiedniego poziomu bezpieczeństwa. Jednakże nie zawsze jest to łatwe do pogodzenia. Przykładem są najbardziej zabezpieczone informacje, które znajdują się w tak odizolowanym i chronionym miejscu, że dostęp jest do nich mocno ograniczony, uniemożliwiając tym samym ich stały udział w procesach biznesowych organizacji.

Należy zwrócić uwagę, że przewagą SZBI nad pojedynczymi regulacjami, związanymi z zapewnieniem bezpieczeństwa, jest jego kompleksowy charakter oraz zaangażowanie wszystkich osób w organizacji. W proces zarządzania bezpieczeństwem informacji włączone jest aktywnie zarówno kierownictwo organizacji, dokonujące nadzoru nad całym systemem, jak i zwykli pracownicy, którzy poddawani są regularnym szkoleniom oraz są zobowiązani do podejmowania konkretnych działań mających na celu zapewnienie bezpieczeństwa.

Do korzyści wynikających z wdrożenia SZBI należą w szczególności:

- Niższe koszty utraty lub naruszenia informacji,
- Większa wiarygodność i zaufanie, zarówno pracowników, jak i kontrahentów,
- Zgodność z przepisami prawa,
- Przewidywanie zagrożeń i zapobieganie im odpowiednio wcześnie,
- Zapewnienie ciągłości świadczonych usług,
- Wzrost świadomości personelu w zakresie ochrony informacji i tajemnic organizacji.

2.3. Regulacje i standardy dotyczące bezpieczeństwa informacji

Działania podejmowane przez różnego rodzaju firmy oraz instytucje z różnych sektorów gospodarki przyczyniają się do powstawania zbiorów najlepszych praktyk z zakresu bezpieczeństwa, por. Anderson (2005), a w szczególności bezpieczeństwa informacji. Zazwyczaj tego rodzaju standardy są częścią wewnętrznych zasad ochrony i nie są one udostępniane na zewnątrz. Jednakże występują sytuacje, w których wymagania bezpieczeństwa są upublicznianie lub też są specjalnie w tym celu opracowywane przez organizacje rządowe jako mechanizmy regulacyjne.

W przypadku regulacji dotyczących bezpieczeństwa informacji, które wynikają bezpośrednio z przepisów prawa, należy przede wszystkim wspomnieć o obowiązującej w Polsce, Ustawie o Ochronie Danych Osobowych. Jest to akt prawny, który narzuca zarówno organizacyjne jak i technologiczne mechanizmy ochrony danych osobowych. Podobne regulacje można znaleźć w przypadku innych rodzajów danych, np. medycznych – amerykańska ustawa HIPAA (ang. *Health Insurance Portability and Accountability Act*). Z kolei – komercyjny standard, dotyczący bezpieczeństwa danych kart płatniczych – PCI DSS – został opisany w kolejnym rozdziale artykułu.

Poza standardami, opierającymi się bezpośrednio na podmiocie danych, należy zwrócić uwagę na bardziej wszechstronne regulacje, które mogą być wykorzystane niezależnie od rodzaju informacji. Najpopularniejszym standardem w tym zakresie jest międzynarodowa Norma ISO/IEC 27001, która została przedstawiona w rozdziale trzecim.

3. PCI DSS

Celem standardu PCI DSS (PCI SSC, 2010) jest zapewnienie skutecznej ochrony danych posiadaczy kart kredytowych przed możliwością ich nieautoryzowanego wykorzystania. Jest on odpowiedzią na liczne przypadki materializacji ryzyka poufności danych kartowych. Stanowi on wytyczne do stosowania zabezpieczeń technicznych oraz organizacyjnych, zaprojekowanych w celu ochrony danych posiadacza karty (Calder i Carter, 2008).

Standard PCI DSS zobowiązuje podmioty, występujące w procesie rozliczenia transakcji zawieranych kartami płatniczymi, które przesyłają, przetwarzają lub przechowują dane z kart płatniczych, do podjęcia i skutecznego przestrzegania odpowiednich środków bezpieczeństwa. Wśród tych podmiotów można wyróżnić m.in. kontrahentów, obsługujących punkty handlowo-usługowe, banki, agentów rozliczeniowych, czy też dostawców usług. Wymaganie przestrzegania standardu jest elementem zobowiązań kontraktowych pomiędzy tymi podmiotami. Każdy podmiot, który dąży do zgodności z PCI DSS musi egzekwować tę zgodność od swoich partnerów biznesowych. Warto jednak przy tym podkreślić, że w obecnej chwili zgodność z PCI DSS nie jest nigdzie na świecie wymagana prawnie, tak jak ma to miejsce np. w przypadku standardów dotyczących bezpieczeństwa danych osobowych.

PCI DSS został opracowany i jest utrzymywany przez organizacje płatnicze, które razem założyły PCI Security Standards Council (PCI SSC). Tymi organizacjami są: American Express, Discover Financial Services, JCB International, MasterCard Worldwide i Visa. Do zakresu obowiązków PCI SSC należy przede wszystkim definiowanie kolejnych wersji standardu PCI DSS, certyfikacja firm i audytorów przeprowadzających badanie zgodności ze standardem.

Do prekursorów PCI DSS należy zaliczyć indywidualne programy organizacji płatniczych mające na celu zapewnienie bezpieczeństwa danych posiadacza karty:

- Visa Cardholder Information Security Program (CISP)
- MasterCard Site Data Protection (SDP)
- American Express Data Security Operating Policy
- Discover Information Security and Compliance (DISC)
- JCB Data Security Program.

Cele tych inicjatyw były ze sobą zbieżne. Miały one na celu określenie minimalnego poziomu ochrony przetwarzanych, przechowywanych i transmitowanych danych posiadacza kart. W związku z tym, organizacje płatnicze utworzyły 15 grudnia 2004 r. PCI SSC, którego głównym zadaniem było ujednolicenie indywidualnych inicjatyw organizacji płatniczych dotyczących bezpieczeństwa klientów. Produktem tych działań było wydanie pierwszej wersji (1.0) standardu PCI DSS w 2005 roku, przy czym wersja ta jest regularnie aktualizowana.

4. ISO/IEC 27001

Międzynarodowa norma ISO/IEC 27001 określa wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Motywem dla jej opracowania było zebranie i ujednolicenie najlepszych praktyk i doświadczeń dotyczących zarządzania bezpieczeństwem informacji.

System Zarządzania Bezpieczeństwem Informacji może być ustanowiony niezależnie od branży, wielkości, rodzaju działalności, czy statusu prawnego organizacji.

Szczególnymi adresatami SZBI są organizacje z branży informatycznej, finansowej, ubezpieczeniowej, medycznej, oświatowej i sektora administracji publicznej. Wynika to z potrzeb tych podmiotów do utrzymania należytego poziomu przetwarzanych przez nich danych.

Genezą normy było rozpoczęcie w roku 1992 przez Departament Handlu i Przemysłu w rządzie Wielkiej Brytanii prac nad zebraniem i opracowaniem najlepszych praktyk z zakresu zarządzania bezpieczeństwem informacji. Wynikiem tych działań było opracowanie dokumentu BS PD0003:1993, który był dalej rozwijany przez *British Standards Institute* (BSI) dwutorowo. Równolegle opracowywane były wymagania bezpieczeństwa informacji oraz wytyczne do ich prawidłowego wdrożenia. Tym samym, na przestrzeni lat opracowane zostały dwie powiązane ze sobą normy: ISO/IEC 27001 i ISO/IEC 27002.

Obecnie za rozwój standardu odpowiedzialna jest jednostka organizacyjna będąca częścią Międzynarodowej Organizacji Normalizacyjnej (ang. *International Organization for Standardization*). Jest nią podkomitet SC27, obejmujący swoim zakresem techniki bezpieczeństwa informatycznego, który wchodzi w skład komitetu JTC1 (ang. *Joint Technical Commitee on Information Technology*) istniejącego od 1987 roku.

Pełna nazwa omawianej normy to ISO/IEC 27001:2005 *Information technology - Security techniques - Information security management systems – Requirements*. Jest ona dostępna jedynie odpłatnie, niezależnie od celu jej stosowania. Norma ta została przetłumaczona oficjalnie na wiele języków. W szczególności, Polski Komitet Normalizacyjny opublikował jej polską wersję pod nazwą PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania.

5. Analiza porównawcza

5.1. Metodyka przeprowadzonych prac

Punktem wyjścia do wykonania analizy porównawczej standardu PCI DSS oraz normy ISO/IEC 27001 było ustalenie kontekstu oraz przyjęcie założeń, mających na celu wyznaczenie podobnego poziomu szczegółowości.

Przyjęte zostało założenie, że PCI DSS jest stosowany i obowiązuje dla całej organizacji. Domyślnie ten standard jest stosowany jedynie w ograniczonym środowisku, co jest niezgodne z podejściem ISO/IEC 27001, w ramach którego cała organizacja jest obejmowana Systemem Zarządzania Bezpieczeństwem Informacji.

Na potrzeby analizy pominięte zostały szczegółowe wymagania dokumentacyjne, specyficzne dla każdego ze standardów. Forma ustanowienia zabezpieczeń lub ich formalizacja nie mają bezpośredniego wpływu na poziom bezpieczeństwa, który jest zapewniany przez dany zestaw wymagań.

Wymagania związane z uzyskaniem i utrzymaniem certyfikacji oraz zgodności z danym standardem zostały wyłączone z zakresu analizy. Wynika to z ich niezależności od zapisów zawartych bezpośrednio w standardach.

W celu jak najdokładniejszego przeprowadzenia porównania obu rozważanych standardów uwzględnione zostały dodatkowe materiały uzupełniające, które umożliwiły lepszą interpretację wymagań oraz celów ich stosowania. Należą do nich, w szczególności, materiały oraz informacji publikowane przez organizacje odpowiedzialne za rozwój tych standardów, a także doświadczenia zawodowe autorów, związane z ich wdrażaniem.

Prezentowana tutaj analiza została wykonana w dwóch etapach. Pierwszym z nich było wskazanie związków pomiędzy poszczególnymi wymaganiami obu standardów na podstawie ich treści i jej interpretacji. Drugi etap dotyczył porównania kluczowych obszarów bezpieczeństwa zawartych w obu standardach poprzez wskazanie różnic i podobieństw, a także praktyczne odniesienie się do możliwości realizacji danych wymagań.

5.2. Wysokopoziomowe mapowanie wymagań

Na podstawie wymagań zawartych w PCI DSS oraz ISO/IEC 27001 wykonane zostało mapowanie pomiędzy nimi, którego wynik przedstawia Tablica 1.

		Wymagania ISO/IEC 27001										
		A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15
Wymagania PCI DSS	1						X	X				
	2						X	X	X			
	3						X		X			
	4						X					
	5						X					
	6						X		X			
	7							X				
	8				X			X				
	9					X	X					
	10						X					
	11						X		X			
	12	X	X	X	X		X	X		X	X	X

Tablica 1. Wysokopoziomowe mapowanie wybranych wymagań PCI DSS i ISO/IEC 27001. (Opracowanie własne)

Zaznaczono w ramach tego mapowania relacje wynikające z istotnych związków tematycznych pomiędzy parami poszczególnych wymagań. Jak widać, wymagania z jednego standardu nie mogą być wzajemnie jednoznacznie przypisane do wymagań z drugiego. Wskazuje na to występowanie więcej niż jednego związku (występowanie takich związków oznaczono w tabeli znakiem „X") zarówno w niektórych

kolumnach jak i wierszach tablicy. Obrazuje to różnice w opisie obszarów bezpieczeństwa pomiędzy jednym i drugim standardem. Widać natomiast, że w każdym wierszu i w każdej kolumnie Tablicy 1. jest przynajmniej jeden związek tematyczny, ale trzeba pamiętać, że przedstawia ona tylko wybrane wymagania z obu standardów.

Na potrzeby lepszego oddania relacji pomiędzy wymaganiami zostało także wykonane bardziej szczegółowe mapowanie uwzględniające najniższy poziom wymagań zawartych w obu standardach. Wynika z niego, że powiązane ze sobą lub odpowiadające sobie wymagania szczegółowe są porozmieszczane w ramach różnych wymagań wysokopoziomowych w obu rozważanych standardach i nie pokrywają się one w całości.

5.3. Porównanie tematyczne

Na potrzeby przeprowadzenia analizy porównawczej obu standardów wyróżnionych zostało 15 obszarów bezpieczeństwa, umożliwiających określenie kontekstu, względem którego możliwe jest porównanie wymagań wchodzących w zakres każdego ze standardów. Dzięki takiemu podejściu możliwe było analizowanie wymagań występujących na przestrzeni całych standardów bez ograniczania się do pojedynczych zagadnień.

Zarówno standard PCI DSS jak i norma ISO/IEC 27001, pomimo zróżnicowanego podejścia do kwestii zapewnienia bezpieczeństwa (Wright, 2008), realizują założone cele. Można uznać, że dane wchodzące w zakres ochrony obu tych standardów są faktycznie należycie chronione w przypadku ich stosowania. Większość analizowanych obszarów jest w analogiczny sposób zaadresowana przez oba standardy. Elementy różnicujące te standardy mają zazwyczaj charakter uzupełniający bądź też optymalizujący – czyli wywierają one mniejszy wpływ na poziom stosowanych zabezpieczeń.

Rekomendacje dotyczące wyboru standardu do zastosowania w danym obszarze przedstawia Tablica 2. Zidentyfikowane zostały trzy obszary, w których zdecydowanie powinny zostać zastosowane wymagania znajdujące się w obu standardach. Są to obszary: klasyfikacji informacji, rozwoju i utrzymania infrastruktury, a także obszar dokumentacji i zapewnienia zgodności z prawem.

Uniwersalność wykorzystania jest zdecydowanie zaletą ISO/IEC 27001, co jest, zarazem, zgodne z celem powstania tej normy. Wynika to w dużej mierze z większej elastyczności tej normy, która umożliwia pominięcie niektórych jej wymagań, a także z powodu bardziej ogólnego poziomu wymagań. Jednakże wadą tego rozwiązania jest brak porównywalności poziomu ochrony pomiędzy większą liczbą organizacji. Każda z nich bowiem mogła uwzględnić i zaimplementować inny zestaw zabezpieczeń. Kluczową przewagą nad PCI DSS jest bardzo rozbudowany model zarządzania ryzykiem, który umożliwia analizowanie zagrożeń i podatności na poziomie aktywów firmy.

Standard PCI DSS jest znaczniej mniej elastyczny i wymaga wdrożenia wszystkich jego wymagań, które są bardziej szczegółowe i konkretne niż te zawarte w normie ISO. Dzięki temu zapewniany jest zbliżony poziom ochrony we wszystkich

organizacjach, posiadających tę certyfikację. Największą zaletą PCI DSS jest dążenie do maksymalnej izolacji środowisk, zawierających dane kartowe od reszty organizacji. Wadą tego standardu jest skupianie się w swoich podstawowych założeniach jedynie na danych kartowych pomijając szereg innych istotnych rodzajów danych.

Nazwa obszaru	PCI DSS	ISO/IEC 27001
Koncept bezpieczeństwa informacji		X
Analiza ryzyka		X
Klasyfikacja informacji	X	X
Kontrola dostępu		X
Bezpieczeństwo fizyczne i środowiskowe		X
Rozwój i utrzymanie infrastruktury	X	X
Zarządzanie podatnościami	X	
Zarządzanie danymi	X	
Zabezpieczenia kryptograficzne	X	
Zarządzanie incydentami bezpieczeństwa		X
Rejestrowanie zdarzeń i działań	X	
Zarządzanie ciągłością działania		X
Pracownicy i partnerzy biznesowi		X
Dokumentacja i zapewnienie zgodności z prawem	X	X
Rozwiązania informatyczne	X	

Tablica 2. Rekomendacje do zastosowania standardów.
(Opracowanie własne)

Trudno jest określić, który z analizowanych standardów można uznać za lepszy. W każdym z nich zidentyfikowane zostały pewne luki oraz obszary do usprawnień. Ponadto, pomimo stosowania tych standardów w organizacjach występują sytuacje naruszenia bezpieczeństwa oraz wycieku istotnych danych. Warto mieć na uwadze, że stosowanie szerszego zakresu zabezpieczeń podnosi poziom ochrony. W związku z tym, dobrym rozwiązaniem jest jednoczesne wdrażanie kilku standardów omawianego typu.

Większość wymagań zawartych w jednym z omawianych standardów można przełożyć na wymagania z drugiego standardu. W związku z tym, możliwe jest zachowanie zgodności z obydwoma standardami. Kolejność ich wdrożenia w organizacji nie ma tutaj znaczenia. Należy w każdym przypadku zapewnić zgodność z bardziej restrykcyjnymi i dokładnymi wymaganiami.

Biorąc pod uwagę szczegółowe mapowanie wymagań jednego standardu na drugi można uznać, że standard PCI DSS może zostać pokryty w około 87% przez normę ISO/IEC 27001. Natomiast norma ISO może być przez niego pokryta tylko w około 41%. Różnice wynikają z liczby wymagań ISO wykraczających w całości poza zakres drugiego standardu.

Pomimo szeregu wymagań zawartych w obu standardach możliwe jest ich dalsze rozszerzanie i uzupełnianie o dodatkowe elementy. W szczególności rekomendowane jest wykorzystywanie bardziej technicznych standardów określających konkretne parametry konfiguracyjne różnego rodzaju rozwiązań informatycznych, a także standardów mających na celu optymalizację procesów zarządzania bezpieczeństwem.

6. Podsumowanie

W pracy zostały przedstawione dwa standardy dotyczące bezpieczeństwa informacji i przeprowadzono analizę porównawczą standardu PCI DSS oraz normy ISO/IEC 27001. W przypadku obu standardów wzięto pod uwagę cele ich powstania oraz główne wymagania w nich zawarte.

W ramach wykonanej analizy porównawczej zostały uwzględnione podobieństwa oraz różnice w obu standardach wraz z rekomendacjami do zastoso-wania jednego z nich. Ponadto, określona została możliwość odniesienia się do jednego standardu w ramach wdrażania drugiego.

Z perspektywy bezpieczeństwa informacji najlepszym rozwiązaniem jest wdrożenie obu analizowanych standardów jednocześnie. Wynika to z faktu, że norma ISO/IEC 27001 adresuje kwestie bezpieczeństwa w szerszym zakresie, natomiast standard PCI DSS jest bardziej szczegółowy i konkretny.

Bibliografia

Anderson R (2005) *Inżynieria zabezpieczeń*. Warszawa, WNT.

Białas A. (2007) *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Warszawa, WNT.

Calder A., Carter N. (2008) PCI DSS: *A Pocket Guide. Chicago*: IT Governance Limited.

Clinch J. (2009) *ITIL V3 and Information Security*. Londyn, OGC.

Łuczak J., Tyburski M. (2010) *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*. Poznań, Wydawnictwo Uniwersytetu Ekonomicznego.

Mitnick K., Simon W. (2003) *Sztuka podstępu*. Gliwice, Helion.

PCI Security Standards Council. *Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures - Version 2.0. PCI SSC*,PCI SSC, 2010.

Polski Komitet Normalizacyjny PN-I-13335-1: *Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*. Warszawa, PKN, 1999.

Polski Komitet Normalizacyjny. PN-ISO/IEC 27001:2007 *Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania*. Warszawa, PKN, 2007.

Pomykalski A. (2001) *Zarządzanie Innowacjami*. Warszawa, PWN, str. 169.

Wright S. (2008) *Using ISO 27001 for PCI DSS Compliance*. Boston,Siemens.

APPLYING PCI DSS AND ISO/IEC 27001 STANDARDIZATION TO ENSURE INFORMATION SECURITY

Abstract: The paper considers the issues associated with the information safety management in organisations, in the context of implementation and use of the information safety standards. Comparative analysis has been performed of the requirements and application aspects of the safety standards PCI DSS and ISO/IEC 27001. On the basis of results from this analysis conclusions and recommendations are formulated, related to the properties and the application of the two standards considered.

Keywords: information, safety, standards, management