Rozdział VIII

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI (ISO/IEC 27001)[434]

Wprowadzanie technologii informatycznych i komputerowych oraz coraz powszechniejsze ich wykorzystanie doprowadziło do sytuacji, w której istnieje nieskrępowana wymiana informacji pomiędzy oddalonymi od siebie podmiotami i nie mają znaczenia logistyczne uwarunkowania. Technika umożliwia równocześnie szybkie i poprawne gromadzenie, przechowywanie, przetwarzanie i przekazywanie informacji w wielu dotychczas nieosiągalnych płaszczyznach i aspektach[435]. Burzliwy i bardzo dynamiczny rozwój technik informatycznych, jak również rosnąca ilość przetwarzanych danych wymusiły poszukiwanie rozwiązań pozwalających skutecznie zarządzać informacją z uwzględnieniem ryzyka, jakie jest z tym związane.

Bez wątpienia najbardziej poszukiwanym zasobem w dzisiejszych czasach jest informacja. **Informacja** etymologicznie wywodzi się z łacińskiego słowa **informatio**, co oznacza – wyobrażenie, wizerunek, zarys, pojęcie[436]. Pojęcie to jest jednak wieloznaczne, bowiem funkcjonuje w języku potocznym i w wielu dziedzinach nauk, co stwarza wiele problemów definicyjnych. W zależności od kontekstu i obszarów nauki można wyodrębnić różne jej znaczenie, uwarunkowane określonym punktem postrzegania rzeczywistości. Trudno wskazać definicję, która odpowiadałaby potrzebom przynajmniej kilku obszarom dziedzin życia społecznego[437].

---

[434] Por. także J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji*, op.cit.

[435] I. Krysowaty, P. Niedziejko, *Bezpieczeństwo IT jako usługa kształtująca wartość i jakość informacji*, w: J. Żuchowski (red.), *Innowacyjność w kształtowaniu jakości wyrobów i usług*, Wydawnictwo Instytutu Technologii Eksploatacyjnej, Radom 2006, s. 278.

[436] K. Kumaniecki, *Słownik łacińsko-polski*, PWN, Warszawa 1996.

[437] B. Stefanowicz wyróżnia kilka teorii podejmujących próbę wyjaśnienia pojęcia informacja: ilościową teorię informacji C.E. Shannona, nieprobabilistyczną teorię A.N. Kołmogorowa, teorię R.W.L. Hartleya oraz polskich autorów: jakościową teorię informacji M. Mazura, teorię pragmatyczną K. Szaniawskiego oraz semantyczną wykładnię J. Oleńskiego. Wskazuje również trzy podejścia do pojęcia informacji: jako pojęcia pierwotnego; terminu definiowanego na podstawie pewnych zasad dostosowanych do potrzeb danej dziedziny badawczej oraz terminu, który jest opisywany przez swoje

Warto też zwrócić uwagę na inną uniwersalną definicję przyjętą w ramach OAIS (Open Archival Information System) i wykorzystywaną między innymi przez NASA. Według niej informacja to wiedza dowolnego rodzaju, którą można się dzielić, niezależnie do formy (fizykalnej, cyfrowej) użytej dla jej wyrażenia (reprezentacji). Z kolei dane (data) stanowią zgodnie z tym ujęciem formy reprezentacji konkretnej informacji. Dostęp do informacji jest więc możliwy dla odbiorcy, który dysponując danymi, interpretuje je zgodnie z zasadami dotyczącymi konkretnej formy reprezentacji[438].

Według normy ISO/IEC 27002 informacja określona jest jako aktyw, który ma dla instytucji wartość i dlatego należy go odpowiednio chronić[439]. Dodatkowo opisywane są rożne formy występowania informacji, na przykład:

- wydrukowana,
- pisemna,
- elektroniczna,
- audio i wideo,
- ustna.

Bezpieczeństwo informacji jest pojęciem z pogranicza techniki, organizacji i prawa. **Przewodnik dotyczący systemowego zarządzania bezpieczeństwem informacji ISO/IEC 27002 definiuje je jako zachowanie trzech cech informacji: poufności (confidentiality), spójności (*integrity*) oraz dostępności (*availability*).** W odróżnieniu od poprzedniej edycji normy z 2000 r., obecnie standard zwraca uwagę również na zachowanie takich cech, jak: rozliczalność (*accountability*), autentyczność (*authenticity*), niezaprzeczalność (*non-repundation*) i niezawodność (*reliability*); mogą to być także czytelność (*legibility*), zdolność przetwarzania (*survivability*), funkcjonalność (*functionality*), przedstawienie (*performance*), zrozumiałość (*comprehensibility*). Niemniej pierwsze trzy cechy[440] bezpieczeństwa informacji stanowią trzon dla budowy systemu bezpieczeństwa informacji (SZBI) i zrozumienia istoty bezpieczeństwa informacji. To, które z cech w danym momencie są kluczowe, zależy od okoliczności, na przykład dane składowane na taśmach przede wszystkim powinny mieć zdolność przetrwania, wykład – prowadzony w języku obcym musi być zrozumiały itd.

Wzrasta zainteresowanie certyfikowaniem ZSBI; w grudniu 2008 r. zarejestrowano na świecie w 82 państwach (w 2007 r. było to 70 państw) 9246[441] certyfikowane systemy zarządzania bezpieczeństwem informacji.

---

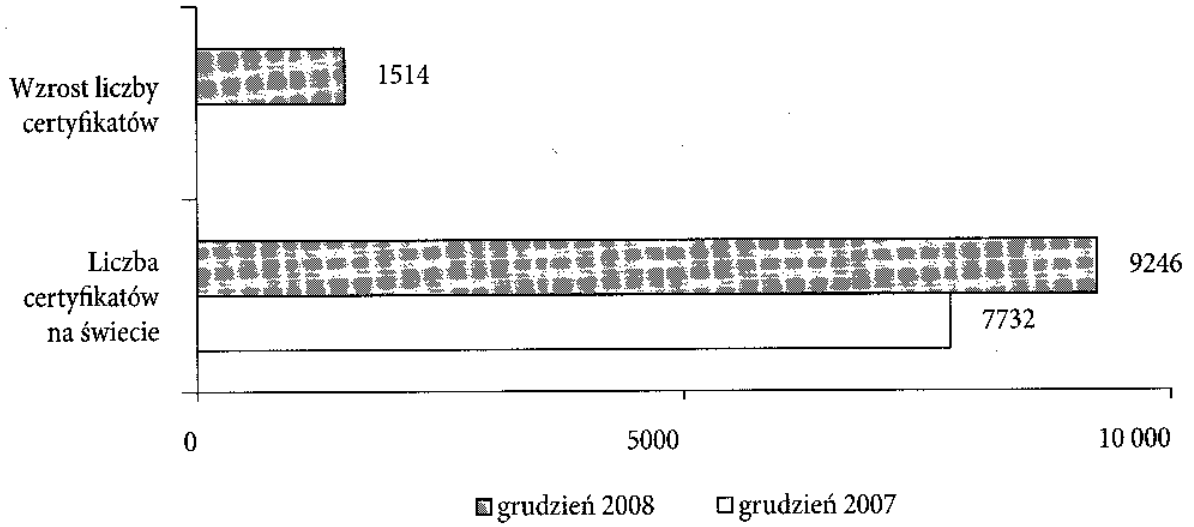
cechy, własności i funkcje (B. Stefanowicz, *Informacja*, Wydawnictwo SGH, 2004, s. 9–14). Por. także Z. Gomółka, *Cybernetyka w zarządzaniu*, Placet, 2000, s. 51–52; N. Wiener, *Cybernetyka społeczna*, KiW, 1961, s. 18.

[438] L. Reich, D. Sawyer, *Archiving Referencing Model*, White Book, Issue 5, CCSDS 1999.

[439] ISO/IEC 27002 (wcześniej 17799) Information technology – Security techniques – Code of practice for information security management, ISO, Genewa 2005, s. 9.

[440] J. Stokłosa, T. Bilski, T. Pankowski rozróżniają integralność oraz spójność (patrz J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa – Poznań 2001, s. 17).

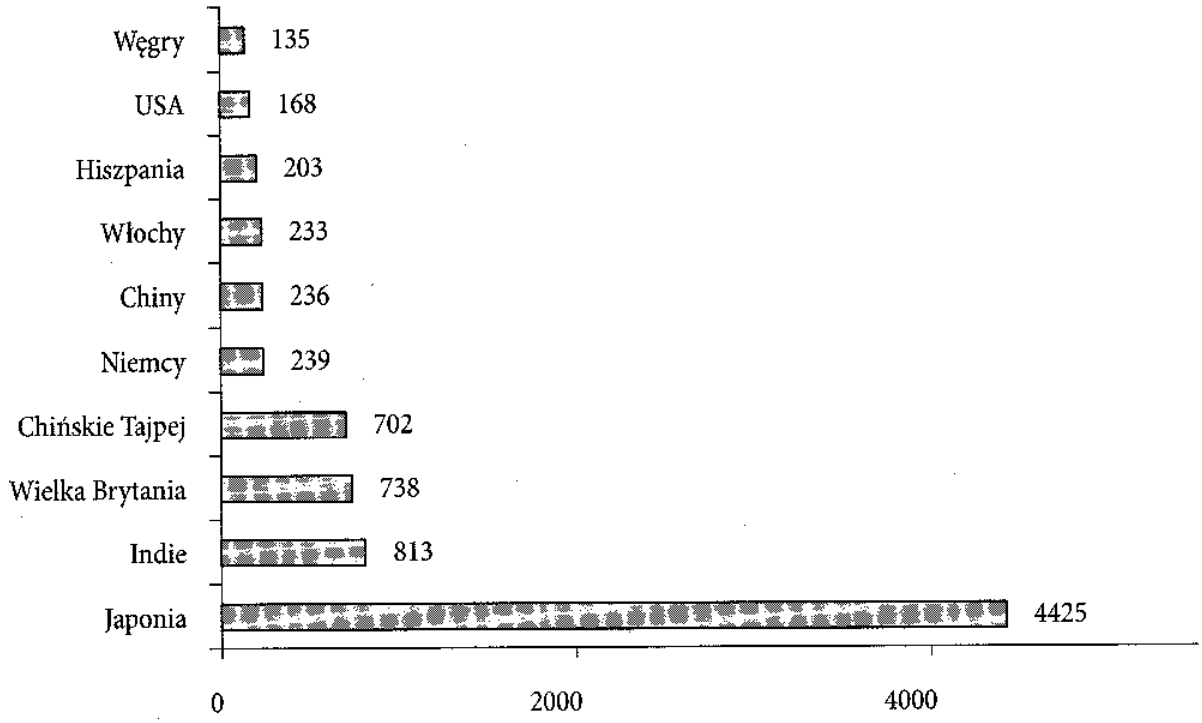
[441] *The ISO Survey of certifications 2008*, ISO, 2009, s. 15.



Rys. 30. Liczba certyfikatów ISO/IEC 27001 na świecie w 2008 i 2007 r.

Źródło: The ISO Survey of certifications 2008, ISO, 2009, s. 15

Dominującymi krajami w zakresie stosowania normy ISO/IEC 27001 są: Japonia, Indie, Wielka Brytania, Chińskie Tajpej (rysunek 31). Popularność standardu w Japonii tłumaczy fakt, że tamtejsze prawodawstwo wskazuje normę ISO/IEC 27001 (dawniej BS 7799-2) jako punkt odniesienia dla prowadzenia niektórych obszarów biznesu.



Rys. 31. Dziesięć państw z największą liczbą certyfikatów ISO/IEC 27001 (2008 r.)

Źródło: The ISO Survey of certifications 2008, ISO, 2009, s. 15

Zdecydowanie największy wzrost liczby certyfikowanych systemów bezpieczeństwa informacji miał miejsce w Chińskim Tajpej oraz Indiach, które są w chwili obecnej zagłębiem informatyków, call-centers i wielu usług informatycznych; ale także w Wielkiej Brytanii, Hiszpanii, Niemczech, Korei Północnej, Chinach, we Włoszech, w USA i na Węgrzech.

Do końca 2008 r. w Polsce zarejestrowano 75 certyfikatów[442]. Liczba przeprowadzonych dotychczas w Polsce akredytowanych certyfikacji SZBI nie jest duża, jednakże można zaobserwować wzrost liczby wydanych certyfikatów na świecie, a w naszym kraju – rosnące zainteresowanie szkoleniami z zakresu SZBI oraz wzrost liczby zapytań o możliwość certyfikacji.

1. Kluczowe czyniki bezpieczeństwa informacji

Mając na myśli elementy bezpieczeństwa, należy rozumieć wszystko to, na czym opiera się system zarządzania bezpieczeństwem informacji. Głównym celem SZBI jest zarządzanie ryzykiem w taki sposób, aby minimalizować ryzyko wystąpienia zagrożeń i implementować skutecznie zabezpieczenia[443].

W tym miejscu konieczne jest wyjaśnienie kluczowych terminów związanych z zarządzaniem ryzykiem. PN-I-13335-1 wyjaśnia je w następujący sposób:

- **zagrożenie** – potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji[444],
- **zasoby** – to wszystko, co ma wartość dla instytucji[445],
- **zabezpieczenie** – praktyka, procedura lub mechanizm redukujący ryzyko[446],
- **podatność** – słabość zasobu, lub grupy zasobów, która może być wykorzystana przez zagrożenie[447].

M. Osborne wskazuje na większy zakres terminów związanych z ryzykiem bezpieczeństwa informacji[448].

---

[442] Według innych źródeł: www.iso27000.pl (z 12.09.2009) – rejestr certyfikatów ISO/IEC 27001 w Polsce wskazuje liczbę 93 certyfikatów.

[443] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji*, op.cit., s. 135.

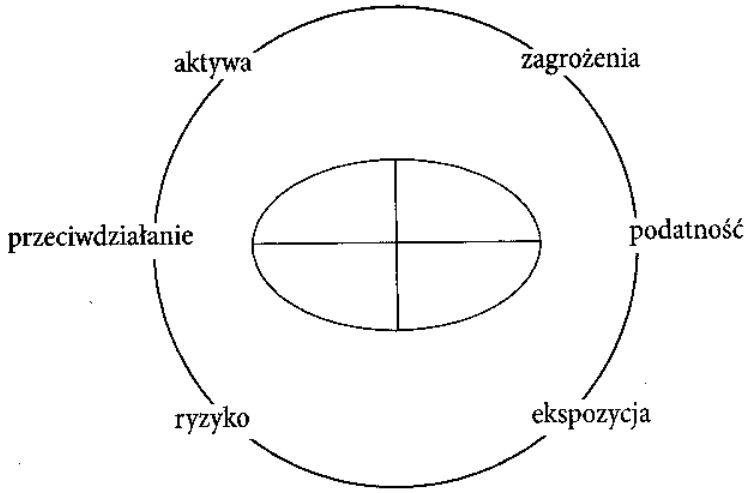
[444] PN-I-13335-1 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych, PKN, 1999, s. 9.

[445] PN-I-13335-1, s. 8.

[446] PN-I-13335-1, s. 8.

[447] PN-I-13335-1, s. 9.

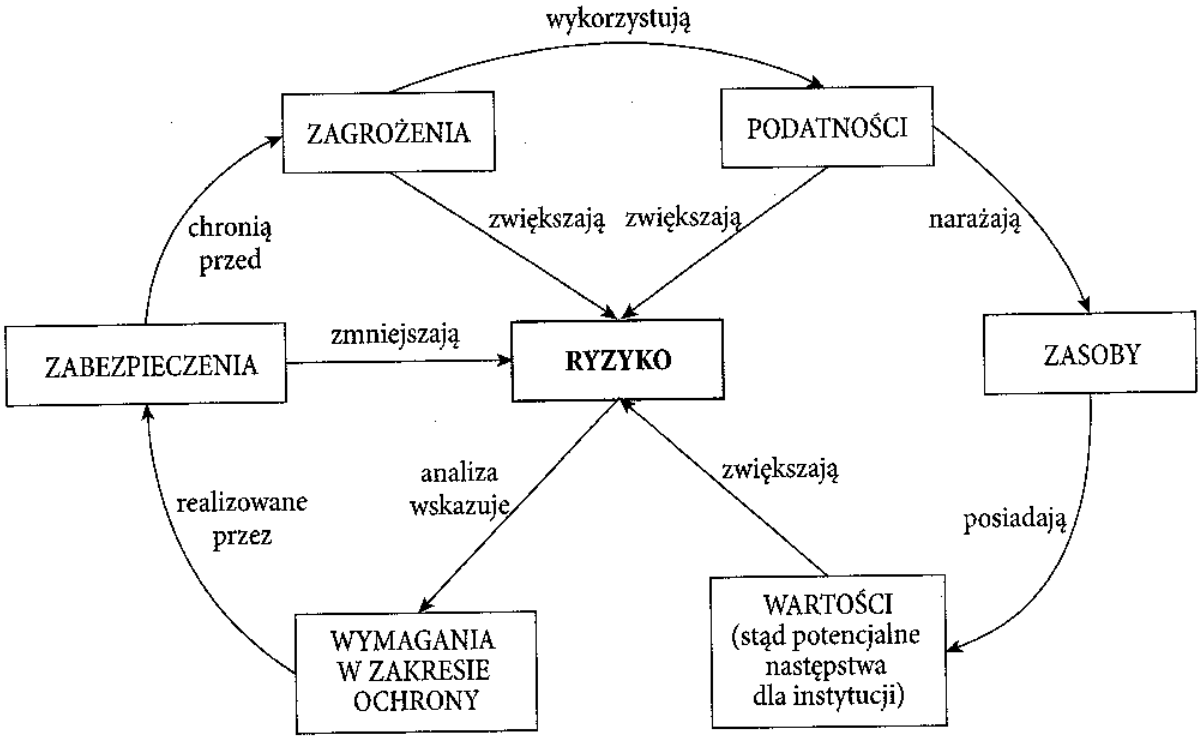
[448] M. Osborne, *How to Cheat at Managing Information Security*, Syngress Publishing Inc., Rockland 2006, s. 54.



Rys. 32. Terminologia związana z ryzykiem bezpieczeństwa informacji

Źródło: M. Osborne, *How to Cheat*, op.cit, s. 54

Wszelkie związki pomiędzy tymi elementami zostały opisane i przedstawione poprzez prosty model ujęty w normie ISO/IEC 13335 poświęconej technice informatycznej. W dalszej części rozdziału zostaną omówione elementy, jak również relacje zachodzące między nimi. Najprościej można to zaprezentować poprzez schematyczny rysunek 33.



Rys. 33. Związki w zarządzaniu ryzykiem

Źródło: PN-I-13335-1, s. 19

Przedstawione związki w zarządzaniu ryzykiem nie pozostawiają żadnych wątpliwości, że niezależnie od założeń dla SZBI zdecydowanie koniecznym elementem, absolutnie niezbędnym, jest zarządzanie ryzykiem. Pominięcie któregokolwiek z jego składowych naraża bezpieczeństwo informacji, bowiem intuicyjny system zarządzania bezpieczeństwem informacji może być nieskuteczny.

1.1. Zasoby w SZBI

Typowe podejście do klasyfikacji zasobów przy ich analizie pod kątem SZBI wynika z PN-I-13335-1.

Należy mieć na uwadze sześć postaci, w jakich występują w organizacjach[449] zasoby:
- zasoby fizyczne (wszelkiego rodzaju sprzęt informatyczny, urządzenia komunikacyjne, budynki, infrastruktura techniczna i informatyczna),
- informacje (dokumenty, bazy danych),
- oprogramowanie (wszelkie systemy operacyjne, aplikacje),
- zdolność produkowania lub świadczenia usług,
- personel,
- dobra niematerialne (reputacja, wizerunek).

Każdy z wymienionych powyżej zasobów posiada określoną wartość, co wskazuje na konieczność zagwarantowania pewnego minimalnego stopnia ochrony. **W systemie zarządzania bezpieczeństwem informacji należy wszystkie zasoby zidentyfikować.** Pozwoli to na przegląd całej organizacji pod kątem jej wyposażenia. W praktyce nie jest to sprawa łatwa, z uwagi na czasochłonność i koszt. Księgowe zestawienie środków trwałych jest zaledwie fragmentem bazy, jaką trzeba zbudować. Identyfikacja może być oparta na zastosowaniu różnych technik – ogólnej, szczegółowej, grupowaniu zasobów itp. To, co należy wziąć pod uwagę przy identyfikowaniu, to atrybuty zasobów, tj.: gestorów, ich wartość, wrażliwość oraz związane z nimi zabezpieczenia. Na wymagania w zakresie ochrony zasobów wpływa także ich podatność na konkretne zagrożenia.

1.2. Zagrożenia związane z bezpieczeństwem informacji

Zagrożenie może być potencjalną przyczyną niepożądanego incydentu, który może spowodować szkodę dla systemu lub instytucji i jej zasobów. Szkoda ta może powstać jako skutek bezpośredniego lub pośredniego ataku na informację

[449] PN-I-13335-1, s. 13.

przetwarzaną przez system lub usługę informatyczną, na przykład uszkodzenie, ujawnienie, modyfikację, utratę informacji lub jej dostępności. Zagrożeniem jest wykorzystanie istniejącej podatności tych zasobów. Zagrożenia mogą mieć pochodzenie środowiskowe lub ludzkie, mogą być przypadkowe lub rozmyślne. **Należy zidentyfikować zarówno zagrożenia przypadkowe, jak i rozmyślne oraz określić ich poziom i prawdopodobieństwo**[450]. Dla zilustrowania powyższych rozważań można posłużyć się zestawieniem zaprezentowanym w tabeli 29.

Tab. 29. Podział zagrożeń ze względu na źródło pochodzenia

Ludzkie		Środowiskowe
Rozmyślne	Przypadkowe	
podsłuch	pomyłki i pominięcia	trzęsienie ziemi
modyfikacja informacji	skasowanie pliku	piorun
włamania do systemu	nieprawidłowe skierowanie	powódź
kradzież, złośliwy kod	wypadki fizyczne	pożar

Źródło: PN-I-13335-1, s. 11.

W literaturze przedmiotu, raportach i opracowaniach można znaleźć bardzo wiele zestawień zagrożeń. M. Whitman podaje kategorie zagrożeń oraz ich przykłady (tabela 30)[451].

Tab. 30. Rodzaje zagrożeń bezpieczeństwa informacji

Kategoria zagrożenia	Przykłady
Błędy i pomyłki ludzkie	wypadki, błędy pracowników
Naruszenie własności intelektualnej	piractwo, naruszenie praw autorskich
Zamierzone działania o charakterze szpiegowskim lub wtargniecie	nieautoryzowany dostęp lub/i gromadzenie danych
Zamierzone działania w zakresie wyłudzenia informacji	szantaż lub ujawnienie informacji
Zamierzone działania o charakterze sabotażu lub wandalizmu	zniszczenie systemów lub informacji
Kradzież	nielegalne skonfiskowanie sprzętu lub informacji
Zamierzone ataki na oprogramowanie	wirusy, robaki, makra, odmowa wykonania usługi
Siły natury	pożar, powódź, błyskawice, trzęsienie ziemi
Odchylenie w jakości usług	ISP, zasilanie, lub usługi WAN od dostawców usług
Techniczne błędy i awarie sprzętu	awarie sprzętu
Techniczne błędy i awarie oprogramowania	pluskwy, problemy kodowania, nieznane luki
Technologiczne starzenie	przestarzałe technologie

Źródło: M. Whitman, *Enemy at the gates*, op.cit., s. 91–96.

[450] PN-I-13335-1, s. 13.

[451] M. Whitman, *Enemy at the gates: threats to information security*, Communications of the ACM, 48 (8), 2003, s. 91–96.

Próbując usystematyzować identyfikację zagrożeń, można je opisać i rozróżnić w nich takie cechy, jak:
- źródło występowania (zewnętrzne, wewnętrzne),
- motywacja (zyski finansowe, wyprzedzenie konkurencji),
- częstotliwość pojawiania się,
- dotkliwość określona poprzez zakres szkodliwości lub określona poprzez różnego rodzaju skale, na przykład skala Richtera, Beauforta,
- rodzaj szkody (czasowa – na przykład przerwa w dostępie, stała – zniszczenie zasobu).

Dla wielu rodzajów zagrożeń środowiskowych dostępne są dane statystyczne, które powinny zostać uwzględnione podczas określania zagrożeń w instytucji. Środowisko oraz uwarunkowania kulturowe, w których działa instytucja, mogą mieć znaczący wpływ na sposób postępowania w odniesieniu do zagrożeń w instytucji. W przypadkach wyjątkowych, ze względu na specyficzne uwarunkowania kulturowe, pewne zagrożenia mogą w ogóle nie być uznane za szkodliwe[452].

1.3. Podatności informacji

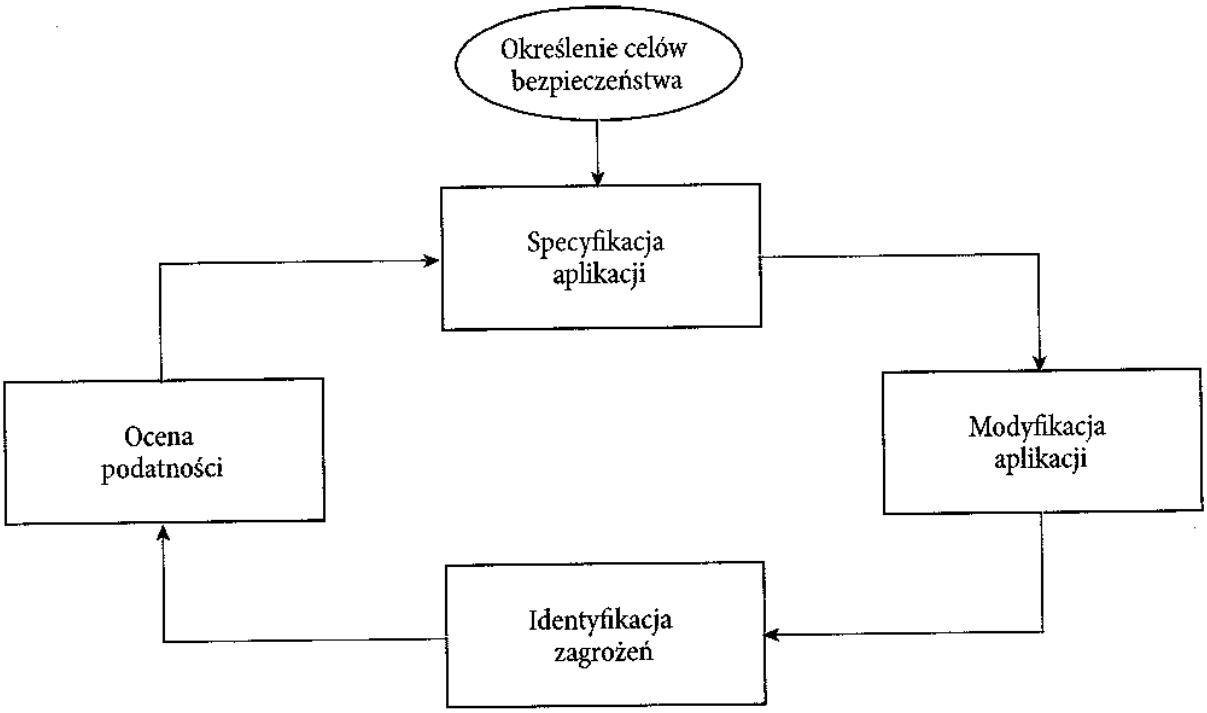
Kolejnym elementem ważnym dla budowy systemu bezpieczeństwa są podatności. Są to pewne słabości fizyczne, organizacyjne, systemowe, proceduralne, osobowe, infrastrukturalne, oprogramowania czy informacji. Zasoby nierozerwalnie związane a są podatnościami, które to z kolei mogą być wykorzystane przez zagrożenia. To z kolei prowadzić może do wystąpienia pewnej szkody lub straty.

Podatność sama w sobie nie generuje szkody, lecz jest warunkiem lub zbiorem warunków, które mogą umożliwić zagrożeniu wpłynąć na zasoby. Podatność obejmuje słabości w systemie bezpieczeństwa, które mogą być wykorzystane i w konsekwencji doprowadzać do niepożądanych efektów. Na przykład brak mechanizmu kontroli dostępu jest podatnością, która może pozwolić zaistnieć zagrożeniu w postaci włamania i utraty zasobów informacyjnych.

Na przykład w stosowaniu the threat risk modeling process, dla zapewnienia bezpieczeństwa tworzonego i rozwijanego oprogramowania, istotą jest identyfikacja zagrożeń oraz ocena podatności.

Przeprowadzając analizę podatności należy określić wszelkie słabości, które mogą być wykorzystywane przez zidentyfikowane wcześniej zagrożenia. Należy rozważyć podatności pochodzące z różnych źródeł, na przykład wewnętrzne względem zasobu. Podatność może istnieć dopóty, dopóki same zasoby nie zmienią się tak, że podatność nie będzie się do nich odnosić. Dodatkowo należy przy tym wziąć pod

[452] PN-I-13335-1, s. 14.



Rys. 34. Microsoft Threat Modeling Process

Źródło: Threat Analysis & Modeling v2.1.2, © Microsoft Corporation, 2007; J.D. Meier, A. Mackman, B. Wastell, Threat *Modeling Web Applications,* © Microsoft Corporation, May 2005; *Improving Web Application Security: Threats and Countermeasures,* J.D.; F. Swiderski, W. Snyder, *Threat Modeling, Microsoft Press,* June 2004

uwagę środowisko i istniejące zabezpieczenia. W pewnym uproszczeniu podatność konkretnego systemu lub zasobu jest określeniem łatwości, z jaką temu systemowi lub zasobowi może być wyrządzona szkoda. Możliwe jest, że w danym systemie lub instytucji nie wszystkie podatności będą podlegały zagrożeniom. Natomiast konieczne jest natychmiastowe zainteresowanie się tymi podatnościami, z którymi związane są zagrożenia. Otoczenie zewnętrzne i wewnętrzne może zmieniać się dynamicznie, dlatego jest potrzeba monitorowania podatności, aby zidentyfikować te, które zostały narażone na stare lub nowe zagrożenia.

1.4. Incydenty

Incydenty związane z bezpieczeństwem informacji to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji[453]. Zarządzanie in-

[453] ISO/IEC TR 18044 Information technology – Security techniques – Information security incident management, ISO, Genewa 2004.

cydentami jest obowiązkowym elementem SZBI (ISO/IEC 27001)[454], a rejestracja kluczem do analiz i wnioskowania.

W 2008 r. odnotowanych zostało 1796 incydentów[455] w Polsce. Według typów najwięcej dotyczy oszustw komputerowych, obraźliwych i nielegalnych treści oraz złośliwego oprogramowania.

Tab. 31. Charakterystyka typów incydentów

Typ/podtyp incydentu	Liczba
Obraźliwe i nielegalne treści	**0**
Spam	466
Dyskredytacja, obrażanie	8
Pornografia dziecięca, przemoc	8
Złośliwe oprogramowanie	**143**
Wirus	3
Robak sieciowy	24
Koń trojański	104
Oprogramowanie szpiegowskie	2
Dialer	0
Gromadzenie informacji	**0**
Skanowanie	84
Podsłuch	0
Inżynieria społeczna	2
Próby włamań	**11**
Wykorzystanie znanych luk systemowych	24
Próby nieuprawnionego logowania	62
Wykorzystanie nieznanych luk systemowych	0
Włamania	**2**
Włamanie na konto uprzywilejowane	6
Włamanie na konto zwykłe	16
Włamanie do aplikacji	57
Atak na dostępność zasobów	**0**
Atak blokujący serwis (DoS)	4

[454] Patrz wymagania dotyczące zarządzania incydentami (ISO/IEC 27001); ISO/IEC TR 18044; PN ISO/IEC TR 15947 Technika informatyczna – Techniki zabezpieczeń – Struktura wykrywania włamań w systemach teleinformatycznych; ISO/IEC TR 19791 (WD) Information technology Security techniques – Security assessment of operational systems.

[455] Na podstawie: Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłoszonych do zespołu CERT Polska w roku 2008, Raport, Cert Polska, 2008. CERT (Computer Emergency Response Team) Polska (www.cert.pl) działa od 1996 r., a od 1997 r. jest członkiem FIRST (*Forum of Incidents Response and Security Team* – www.fist.org) – największej na świecie organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od 2000 r. jest także członkiem TERENA TF – CRIST (www.terena.org) oraz TRUSTED INTRODUCER (www.trusted-introducer.org).

cd. tab. 31

Typ/podtyp incydentu	Liczba
Rozproszony atak blokujący serwis (DDoS)	22
Sabotaż komputerowy	0
Atak na bezpieczeństwo informacji	1
Nieuprawniony dostęp do informacji	5
Nieuprawniona zmiana informacji	1
Oszustwa komputerowe	10
Nieuprawnione wykorzystanie zasobów	5
Naruszenie praw autorskich	316
Kradzież tożsamości, podszycie się (w tym *phishing*)	400
Inne	10
Suma	1796

Źródło: Analiza incydentów, op.cit., s. 6.

Niechlubnym liderem incydentów są oszustwa komputerowe (ponad 40%), a pośród nich *phishing* (kradzież tożsamości i podszywanie się). Odnotowano wiele przypadków narzuszenia praw autorskich (17,59%) i podobnie jak w 2007 r. – drugim najsilniej reprezentowanym typem incydentów były obraźliwe i nielegalne treści. To prawie wyłącznie przypadki spamu, najliczniejszy podtyp incydentów.

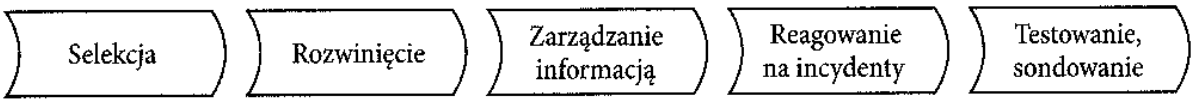
Kolejną kategorią jest złośliwe oprogramowanie (15,37%). Były to strony automatycznie infekujące komputer (*drive by download*) oraz konie trojańskie. Autorzy raportu zwracają uwagę na mniejszą liczbę incydentów dotyczących gromadzenia informacji (głównie przez skanowanie) (poniżej 5%).

Kiedy dojdzie do niepożądanego incydentu spowodowanego rozmyślnie bądź zaistniałego przypadkowo, należy zdiagnozować konsekwencje. Może to być zniszczenie zasobów, awaria sprzętu, strata finansowa, utrata jednej z cech bezpieczeństwa informacji – są one określane jako następstwa. Ich pomiar i analiza umożliwia z kolei utrzymanie równowagi pomiędzy następstwami incydentu a kosztami wprowadzonych zabezpieczeń użytych w celu zapobieżenia jego wystąpieniu. Takie zestawienie następstw i kosztów jest elementem określenia ryzyka i wyboru zabezpieczeń. Można je określić ilościowo, jakościowo, uwzględniając między innymi:

- koszt finansowy,
- skale szkodliwości,
- częstotliwość (wielkość szkody spowodowanej przez incydent może być niska, lecz łączny efekt wystąpienia wielu incydentów w dłuższym okresie może być wysoki).

M. Osborne prezentuje fazy zarządzania incydentami: selekcja, rozwinięcie, zarządzanie informacją, reagowanie, testowanie i sondowanie (rysunek 35)[456].

[456] M. Osborne, *How to Cheat*, op.cit., s. 216.



Rys. 35. Fazy zarządzania incydentami

Źródło: M. Osborne, *How to Cheat*, op.cit., s. 216

Identyfikacja i rejestracja incydentów poprzedza selekcję – przede wszystkim pod kątem szkodliwości. W dalszych krokach konieczne jest rozwinięcie incydentu, charakterystyka, analiza przyczyn. Niezbędne jest podjęcie działań dla zabezpieczenia informacji, która być może jest w niebezpieczeństwie lub w odniesieniu do której zasady bezpieczeństwa zostały złamane. Konieczne jest zaplanowanie działań krótkookresowych i dalekosiężnych – w tym przede wszystkim działań korygujących. Zamknięciem procesu jest analiza skuteczności podjętych działań oraz utrwalenie skutecznych rozwiązań w ramach SZBI.

1.5. Ryzyko

Ryzyko jest prawdopodobieństwem określającym możliwość wykorzystania określonej podatności przez dane zagrożenie w celu spowodowania straty lub zniszczenia zasobu lub grupy zasobów, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na działanie organizacji.

Tab. 32. Kategorie ryzyka

Ryzyko	Opis
Główne ryzyka biznesowe	fuzje, przejęcia, wprowadzenie nowej strony internetowej, uregulowania prawne
Główne ryzyka IT	wprowadzenie nowych technologii wspierających procesy wewnętrzne oraz zewnętrzne
Ryzyka projektowe	zagrożenie dla ciągłości biznesu spowodowane realizacją projektu, ryzyko w zakresie osiągnięcia założonych korzyści z projektu, ryzyko braku osiągnięcia oczekiwanego sukcesu
Indywidualne ryzyka i incydenty	nieodłączne w pracy oraz działaniach związanych z wykorzystaniem IT

Źródło: M.E. Whitman, H.J. Mattord, *Readings and Cases in the Management of Information Security*, Thomson Course Technology, Boston 2006, s. 52

Scenariusz ryzyka opisuje, w jaki sposób dane zagrożenie lub grupa zagrożeń może wykorzystać konkretną podatność lub grupę podatności, narażając zasoby na szkodę. **Ryzyko jest opisywane poprzez kombinację dwu czynników: prawdopodobieństwa wystąpienia incydentu oraz związanych z nim następstw.** Dowolna zmiana

w zasobach, zagrożeniach, podatnościach i zabezpieczeniach może mieć znaczący wpływ na ryzyko. Wczesne wykrywanie i świadomość zmian w środowisku i systemie, zwiększa możliwości podjęcia odpowiednich działań w celu redukcji ryzyka[457].

Pojęcie ryzyka, definiowanie, szacowanie, ocena i postępowanie z nim jest przedmiotem kolejnego rozdziału, w którym jest to opisane bardziej szczegółowo. Niemniej jest to konieczne, aby w tym miejscu przybliżyć to zagadnienie.

1.6. Zabezpieczenia w SZBI

Zabezpieczenia to praktyki, procedury lub mechanizmy, które mogą chronić przed zagrożeniem, redukować podatność, ograniczać następstwa, wykrywać niepożądane incydenty i ułatwiać odtwarzanie. Efektywna ochrona wymaga zwykle kombinacji różnych zabezpieczeń w celu zapewnienia ochrony zasobów. Na przykład mechanizmy kontroli dostępu stosowane dla komputerów powinny być wspomagane przez narzędzia audytu, procedury postępowania dla personelu, szkolenia i zabezpieczenia fizyczne. Pewne zabezpieczenia mogą już istnieć jako element środowiska lub jako cecha własna zasobów, mogą też być już zaimplementowane w organizacji. Zabezpieczenia realizują jedną lub więcej następujących funkcji:

- wykrywanie,
- odstraszanie,
- zapobieganie,
- ograniczanie,
- poprawianie,
- odtwarzanie,
- monitorowanie,
- uświadamianie.

Odpowiedni dobór zabezpieczeń jest kluczowy dla prawidłowego wdrożenia polityki bezpieczeństwa. Wiele zabezpieczeń może służyć różnym funkcjom. Korzystny może być wybór zabezpieczeń, które będą jednocześnie spełniały wiele funkcji. Niektóre zabezpieczenia wyraźnie i jasno informują użytkowników o nastawieniu instytucji do bezpieczeństwa. W związku z tym ważne jest, aby wybór zabezpieczeń nie był kontrowersyjny dla kultury lub społeczeństwa, w którym działa instytucja.

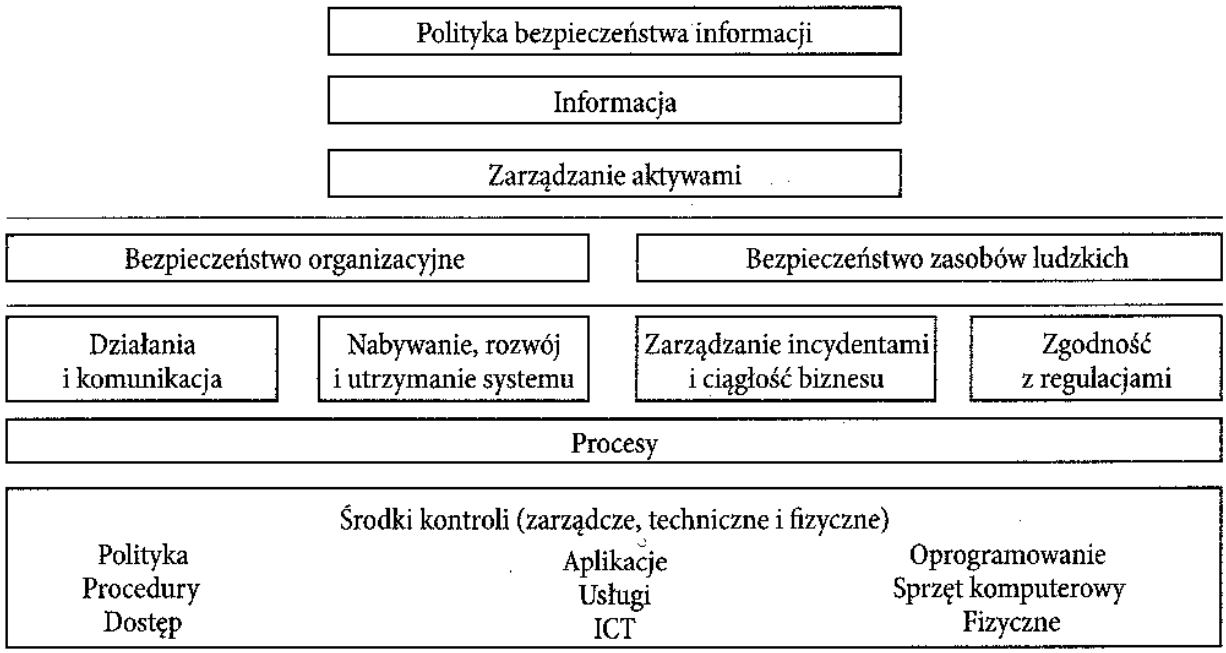
Zabezpieczenie jako jedyne ze wszystkich omawianych elementów ma właściwość redukowania ryzyka. Należy podkreślić jednoznacznie, że wprowadzenie zabezpieczeń nie wyeliminuje ryzyka; pozwoli tylko na jego zmniejszenie. Istnieje również zależność kosztowa – skuteczne zabezpieczenia są kosztowne. Wtedy trzeba już rozpatrywać wprowadzanie zabezpieczeń z punktu widzenia kryterium efektywnościowego. Przy tym rozwiązania w SZBI powinny być skalowane, a za-

[457] PN-I-13335-1, s. 15.

tem adekwatne dla zdefiniowanego ryzyka (proste sytuacje wymagają prostych rozwiązań). Elementem podejmowania decyzji o adekwatności zabezpieczeń do potrzeb instytucji jest akceptacja ryzyka szczątkowego[458]. Proces ten znany jest jako akceptacja ryzyka.

Kierownictwo organizacji powinno być uświadomione o istnieniu ryzyka szczątkowego w kontekście następstw oraz prawdopodobieństwa zajścia określonego zdarzenia. Decyzja o zaakceptowaniu ryzyka powinna być podejmowana przez te osoby, które są uprawnione do akceptacji konsekwencji ewentualnych skutków incydentu oraz autoryzacji wdrożenia dodatkowych zabezpieczeń, jeśli poziom pozostałego ryzyka szczątkowego jest nie do przyjęcia[459].

W przypadku budowy SZBI, zgodnie z ISO/IEC 27001, struktura zabezpieczeń opisana w SoA[460] (deklaracji stosowania) najczęściej odzwierciedla strukturę załącznika A do normy (rysunek 36)[461].



Rys. 36. Struktura zabezpieczeń w SZBI

Źródło: E. Humphreys, *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, Boston 2007, s. 104

[458] Ryzyko szczątkowe (*residual risk*) – ryzyko pozostające po procesie postępowania z ryzykiem [ISO/IEC Guide 73]. Ryzyko, które pozostaje po podjęciu wszystkich możliwych bądź opłacalnych kroków zmierzających do unikania ryzyka, jego kontrolowania lub przeniesienia (transferu). Praktycznie żadnego rodzaju ryzyka nie można zmniejszyć do wartości zerowej i zawsze pozostaje choćby marginalny poziom ryzyka szczątkowego. Termin występuje również pod nazwami: „ryzyko rezydualne" lub „ryzyko resztkowe" (http://www.polrisk.pl).

[459] PN-I-13335-1, s. 15.

[460] SoA (*Statement of Applicability*) – deklaracja stosowania.

[461] Załącznik nr 3 Deklaracja stosowania (na przykładzie przedsiębiorstwa z branży energetycznej); warto zwrócić uwagę na fakt, że deklaracja stosowania może mieć dowolną strukturę (niekoniecznie odzwierciedlającą strukturę załącznika A do ISO/IEC 27001).

Analiza ryzyka oraz skuteczności zagrożeń wskazuje, że w dużej mierze zabezpieczenia powinny być ukierunkowane na wiedzę i świadomość pracowników.

2. Podstawy normatywne w zarządzaniu bezpieczeństwem informacji

Pierwszą normą o wymiarze międzynarodowym w zakresie ochrony informacji została w 2000 r. ISO/IEC 27002 Information Technology – Code of Practice for Information Security Management. Norma brytyjska BS 7799-1 została znowelizowana i zaakceptowana przez ISO/IEC, tym samym uzyskując status normy międzynarodowej. Norma ta zawiera opisy i zalecenia dla stosowania najlepszych praktyk z zakresu bezpieczeństwa informacji oraz szeroki zestaw proponowanych zabezpieczeń. Nie może być podstawą do certyfikowania systemu zarządzania bezpieczeństwem informacji. Wytyczne do certyfikacji przedstawia druga część[462] omawianej normy BS 7799-2 Information security management systems – Specification with guidance for use.

Kolejna aktualizacja norm nastąpiła 5 września 2002 r., kiedy to BS 7799-2 została oficjalnie opublikowana na konferencji „BS 7799 Goes Global" w Londynie. Nowa wersja standardu została opracowana, aby zharmonizować ją z innymi standardami zarządzania, takimi jak ISO 9001 i ISO 14001. Najistotniejszą zmianą jest to, że nakłada na organizację obowiązek starannej oceny ryzyka dla działalności firmy ze strony wskazanych czynników, takich jak: utrata danych, dostęp osób nieuprawnionych, zaatakowanie przez wirusy, powiązania z elementami elektronicznymi, włamania do systemu oraz odzyskiwanie utraconych danych. Zwraca się uwagę na potrzebę wskazania obszarów, w których zachodzi konieczność poprawy. Nowa wersja standardu wprowadza również model PDCA[463], jako cześć podejścia do tworzenia, implementacji i zwiększenia efektywności działania SZBI w organizacji.

Najnowsze wydanie ISO/IEC 17799 opublikowano 15 czerwca 2005 r. Najbardziej dostrzegalną różnicą w stosunku do poprzednich edycji jest zmiana układu zabezpieczeń. Zmiany, zgodnie z założeniami, zostały omówione w sposób bardziej przejrzysty, wychodząc naprzeciw uwagom kontrowersyjnym i krytycznym. Pojawiły się także nowe działania kontrolne; wyodrębniono jedną nową sekcję główną – zabezpieczenie kontrolne dotyczące zarządzania incydentami bezpieczeństwa.

[462] Dokładnie rzecz ujmując, chodzi o drugi arkusz normy. Numer po myślniku normy w oznaczeniach standardów ISO wskazuje na numer arkusza.

[463] Patrz więcej: J. Łuczak, A. Matuszak-Flejszman, *Metody i techniki zarządzania jakością. Kompendium wiedzy*, Quality Progress, Poznań 2007.

14 października 2005 r. brytyjska wersja normy bezpieczeństwa po raz pierwszy została opublikowana przez międzynarodową organizację normalizacyjną ISO, przyjmując nową numerację ISO/IEC 27001. Nowy standard, który jest specyfikacją systemów zarządzania bezpieczeństwem informacji, na zgodność z którą będą wydawane certyfikaty, opiera się na wcześniejszej normie brytyjskiej z roku 2002 BS 7799-2. Poprzedni standard był krytykowany głównie za trudności interpretacyjne i niejasności dotyczące katalogu zabezpieczeń. Małe i średnie organizacje miały problemy z odpowiednim uwzględnieniem niektórych wymagań – na przykład zawartych w rozdziale A.10 (Rozwój i utrzymanie systemu)[464]. Nowy standard, będący modelowym ujęciem systemu zarządzania bezpieczeństwem informacji, zwraca uwagę na konieczność udokumentowania metody szacowania ryzyka bezpieczeństwa informacji i monitorowanie skuteczności stosowania zabezpieczeń.

Tab. 33. Historia standardów dotycząca zarządzania bezpieczeństwem informacji

Departament of Trade and Industry – **DTI**	1993	DTI Code of Practice	
British Standards Institution – **BSI**	1995	BS 7799-1:1995	
	1998		BS 7799-2:1998
	1999	BS 7799-1:1999	BS 7799-2:1999
International Standards Organization – **ISO**	2000	ISO 17799:2000	
	2002		BS 7799-2:2002
	2005	ISO/IEC 17799:2005	ISO/IEC 27001:2005
International Standards Organization – **ISO**	2007	ISO/IEC 27002:2005	

W rodzinie norm ISO/IEC 27000 są także standardy:
- ISO 27000 Information technology: Information security management systems, Overview and vocabulary,
- ISO 27007 Guidelines for Information Security Management Systems Audyting,
- ISO 27008 Guidelines for ISM audyting with respect to security controls (approved April 2008),
- ISO 27011 Information technology: Information security management guidelines for telecommunications,
- ISO 27799 Health Informatics: Information security management in health using ISO/IEC 17799.

W przygotowaniu natomiast są:
- ISO 27010 ISM Guidelines for Sector–Sector Working and Communications,
- ISO 27031 ICT Readiness for Business Continuity,
- ISO 27032 Cyber Security,

[464] M. Zastawa, *Nowe trendy w bezpieczeństwie informacji*, Magazyn Klientów TUV Nord Polska, 2006 (12), nr 3, s. 11.

- ISO 27033 Network Security / Intrusion Detection (to replace ISO 18028),
- ISO 27034 Guidelines for application security,
- ISO 27051 Telecommunications (ITU–T).

Prawdopodobne jest także wydanie w przyszłości branżowych standardów dotyczących SZBI:

- ISO 27012 Finance (ref ISO TC 68),
- ISO 27013 Manufacturing,
- ISO 27012 Automotive Industry,
- ISO 27013 Lotteries.

Pojawienie się na rynku nowego standardu jest konsekwencją prowadzonych prac nad rozwojem systemu oraz chęcią popularyzacji na całym świecie systemu zarządzania bezpieczeństwem jako międzynarodowej normy. Nowe oznaczenie, niebędące konsekwencją poprzednich wersji, wynika z planu stworzenia rodziny standardów bezpieczeństwa ISO serii 27000. Takie działanie ma na celu zgromadzenie wszystkich dotychczasowych standardów dotyczących bezpieczeństwa w jednej serii norm.

Normy (wydawane przez PKN, co odpowiada także koncepcji norm ISO) w zakresie zarządzania, w tym także zarządzania bezpieczeństwem informacji, można zaklasyfikować do trzech typów:

- typ A – normy zawierające wymagania dotyczące systemu zarządzania,
- typ B – normy zawierające wytyczne dotyczące systemu zarządzania,
- typ C – normy związane z systemami zarządzania.

Należy zwrócić uwagę na Polskie Normy i Raporty Techniczne dotyczące całościowego zarządzania bezpieczeństwem informacji w organizacjach oraz dotyczące wycinka tego problemu – zarządzania bezpieczeństwem informacji przechowywanej i przetwarzanej w systemach informatycznych.

Normą pierwszego typu (typu A) jest PN-ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – system zarządzania bezpieczeństwem informacji. Norma ta została opracowana na podstawie ISO/IEC 27001 i zastąpiła PN-I-07799-2. Mówi ona o tym, jak należy zaprojektować system zarządzania bezpieczeństwem informacji i jak go utrzymywać i rozwijać adekwatnie do zmieniających się warunków otoczenia. W niniejszej normie określono wymagania dotyczące ustanawiania, wdrażania, eksploatacji, śledzenia (monitorowania) i przeglądów oraz utrzymywania i doskonalenia udokumentowanego SZBI. Duży nacisk położono na spójność SZBI z innymi funkcjonującymi w organizacji znormalizowanymi systemami zarządzania, a szczególnie z systemem zarządzania jakością (PN-EN ISO 9001) i systemem zarządzania środowiskowego (PN-EN ISO 14001). Każda organizacja, bez względu na wielkość, profil itd., może certyfikować system zarządzania bezpieczeństwem informacji – na zgodność z niniejszym standardem.

Normą typu B jest PN-ISO/IEC 17799 Technika informatyczna – Technika bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji; zastąpiła ona PN-ISO/IEC 17799, a jej podstawą jest ISO/IEC 17799 (ISO/IEC 27002).

Zamieszczono w niej praktyczne zasady mogące być punktem wyjścia do tworzenia przez organizację własnych wytycznych polityki bezpieczeństwa informacji spójnej z polityką bezpieczeństwa firmy i uwzględniającej specyfikę i wielkość organizacji. Intencją twórców tej normy było dostarczenie wspólnej, możliwie jednolitej podstawy do rozwijania przez organizację własnych standardów bezpieczeństwa informacji i efektywnego sposobu zarządzania nim. Celem normy jest także budowanie zaufania w kontaktach pomiędzy instytucjami, które powierzają sobie swoje zasoby informacyjne lub je współdzielą.

Ponadto należy zwrócić uwagę na PN-ISO/IEC 27006 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji; została ona opracowana na podstawie ISO/IEC 27006. Ciekawą normą jest także PN-EN ISO 27799 Informatyka w ochronie zdrowia – zarządzanie bezpieczeństwem informacji w ochronie zdrowia przy użyciu ISO/IEC 27002.

3. Koncepcja systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001)

Ukoronowaniem działań ISO w zakresie unifikacji wymagań dotyczących systemowego zarządzania bezpieczeństwem informacji jest standard ISO/IEC 27001, w najnowszej w wersji z 2005 r. Wcześniejsze normy, przede wszystkim BS 7799 oraz ISO/IEC 27001 z 2000 r., były zapowiedzią dostrzeżenia bezpieczeństwa informacji jako kategorii biznesowej, stanowiącej o przewadze konkurencyjnej, a często być albo nie być – z uwagi na odpowiedzialność prawną czy utratę żywotnych interesów organizacji. Niniejszy standard został opracowany przez Wspólny Komitet Techniczny JTC 1 – Technika informatyczna i z założenia pozwala na integrację z innymi modułami znormalizowanych systemów zarządzania, na przykład ISO 9001, ISO 14001[465]. A zatem jeden właściwie zaprojektowany system może spełniać wymagania wielu standardów.

Wymagania ISO/IEC 27001 pogrupowane zostały w rozdziałach:
- System zarządzania bezpieczeństwem informacji,
- Odpowiedzialność kierownictwa,
- Wewnętrzne audyty jakości,
- Przeglądy SZBI realizowane przez kierownictwo,
- Doskonalenie systemu zarządzania bezpieczeństwem informacji.

[465] Parz tablica C1. w ISO/IEC 27001 ilustruje powiązania pomiędzy niniejszym standardem a ISO 9001 oraz ISO 14001.

Norma ISO/IEC 27001 stanowi model SZBI, który może być zastosowany przez każdą organizację, niezależnie od specyfiki jej działalności, wielkości, realizowanych procesów, statusu prawnego czy struktury organizacyjnej; pozwala na ustanowienie, wdrożenie, eksploatowanie, monitorowanie, przegląd i doskonalenie systemu. Wdrożenie SZBI powinno być postrzegane jako decyzja strategiczna i wypływać z potrzeb biznesowych organizacji. Rozwiązania stosowane w ramach SZBI powinny być adekwatne dla potrzeb organizacji.

Decyzja o wdrażaniu systemu według ISO/IEC 27001 nie pozwala na dokonanie wyłączeń jakiegokolwiek wymagania z niniejszej normy[466]. Możliwe jest natomiast wyłączenie wybranych zabezpieczeń, jednak pod warunkiem spełnienia kryteriów akceptacji ryzyka – co powinno być uzasadnione, udokumentowane i zatwierdzone. Taka sytuacja nie może wpłynąć na obniżenie poziomu bezpieczeństwa organizacji oraz spełnienie wymagań wynikających z szacowania ryzyka, wymagań prawnych oraz niniejszego standardu.

Źródłem modelowego ujęcia systemowego zarządzania bezpieczeństwem informacji jest już wcześniej wspominana norma ISO/IEC 27001. Standard przedstawia wymagania dotyczące zarządzania bezpieczeństwem informacji w organizacjach. Jej uzupełnieniem jest opublikowany w 2005 r. zbiór najnowszych praktycznych wymagań (Information Technology – Code of practice for Information Security Management).

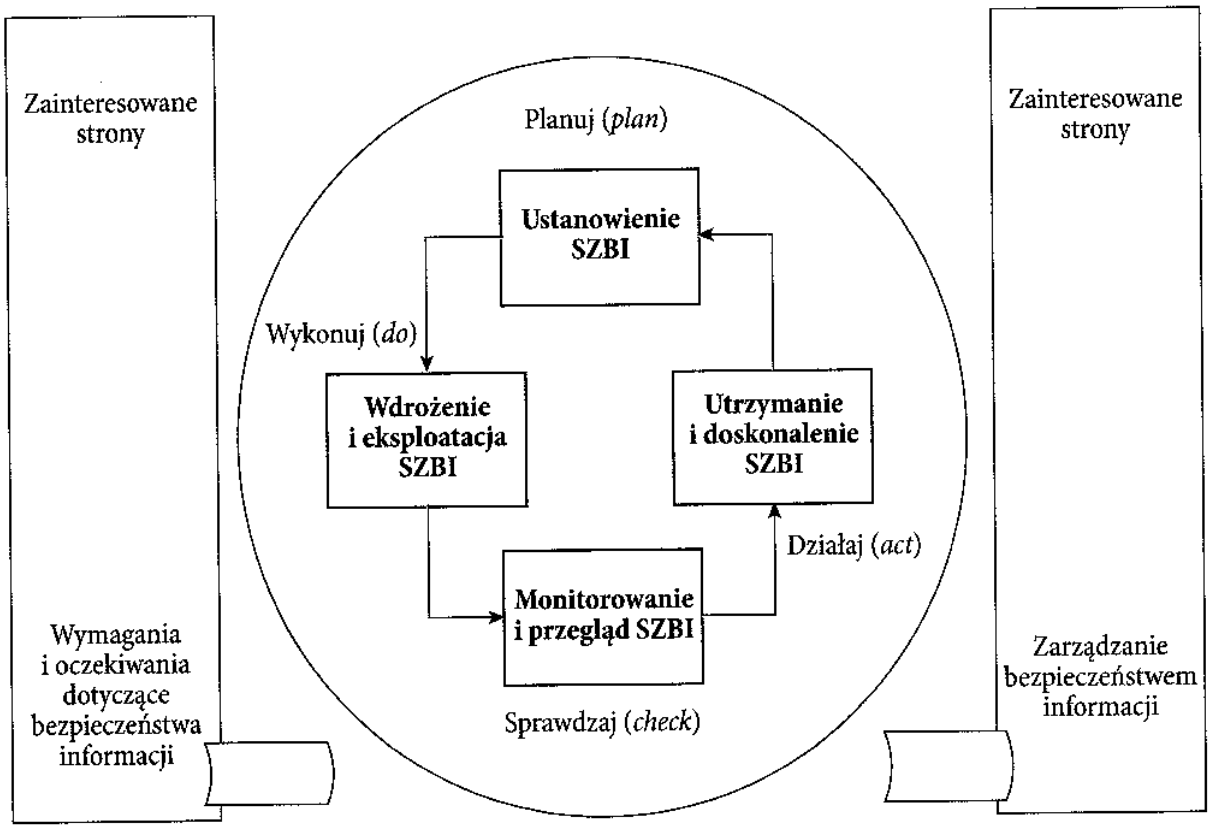
Norma definiuje poszczególne elementy kontroli i sterowania bezpieczeństwem informacji, podporządkowanych dziesięciu grupom wymagań, co pozwala organizacji na zidentyfikowanie najwłaściwszych zabezpieczeń w kontekście specyfiki działalności, jaką prowadzą, oraz otoczenia rynkowego i potrzeb w powyższym zakresie. Szczególny nacisk położony jest na zarządzanie ryzykiem. Norma dotyczy wszystkich form informacji, w tym także ustnych i graficznych, powstających z wykorzystaniem telefonów komórkowych i faksów. Standard uwzględnia najnowsze formy działalności gospodarczej, na przykład: *e-commerce*, Internet, *outsourcing*, *teleworking*, *mobile computing*. Poniżej przedstawiono krótką charakterystykę poszczególnych rozdziałów.

- **Polityka bezpieczeństwa.** Polityka jest najważniejszym dokumentem w systemie zarządzania bezpieczeństwem informacji. Tworzy wytyczne i ramy dla pozostałych zasad. Punkt opisuje wskazówki właściwe dla organizacji, które należy wziąć pod uwagę podczas tworzenia polityki bezpieczeństwa informacji.
- **Organizacja bezpieczeństwa.** Stworzenie zasad zabezpieczania informacji nie gwarantuje jeszcze stworzenia systemu. Konieczne jest powołanie odpowiednich struktur zarządzania wewnątrz organizacji. Ważne jest również zidentyfikowanie firm zewnętrznych mających dostęp do informacji i wyznaczenie odpowiednich metod nadzoru nad takimi stronami trzecimi.

[466] ISO/IEC 27001, wymagania określone w rozdziałach 4–8.

- **Zarządzanie aktywami.** Konieczna jest weryfikacja informacji przetwarzanych i składowanych w organizacji. Efektem klasyfikacji informacji jest stworzenie grup informacji o różnych stopniach poufności oraz opisanie zasad postępowania ze zidentyfikowanymi grupami.
- **Bezpieczeństwo zasobów ludzkich.** Najsłabszym elementem każdego systemu są ludzie. Norma wymaga, aby sprawować nadzór nad poszczególnymi grupami pracowników: potencjalnych kandydatów, praktykantów, nowych pracowników, pracowników przewidzianych do awansu. Konieczne jest stworzenie systemu szkoleń i uświadamiania pracowników odnośnie do zagrożeń.
- **Bezpieczeństwo fizyczne i środowiskowe.** Punkt opisuje wymagania dotyczące fizycznego zabezpieczania budynków, pomieszczeń użytkowych, serwerowni. Niezbędne jest również opisanie zasad związanych z konserwacją urządzeń, w tym komputerów oraz ustalenia wymaganej kultury pracy, na przykład Zasada czystych biurek.
- **Zarządzanie systemami i sieciami.** Wiele błędów związanych z bezpieczeństwem informacji dotyczy niewłaściwego użytkowania urządzeń. Dlatego konieczne jest opracowanie zasad korzystania z funkcjonujących urządzeń, w tym również będących własnością firm zewnętrznych. Dużym zagrożeniem są wirusy i inne niebezpieczne oprogramowanie. Aby uniknąć utraty cennych danych elektronicznych, konieczne jest opracowanie zasad tworzenia i zarządzania kopiami zapasowymi. Bardzo ważnym elementem jest bezpieczne postępowanie z mobilnymi nośnikami danych oraz ustalenie zasad wymiany informacji ze stronami trzecimi.
- **Kontrola dostępu do systemów.** Systemy informatyczne zawierają ogromne ilości danych. Niezbędne jest kontrolowanie dostępu do danych poprzez jasne ustalenie grup użytkowników oraz zdefiniowanie uprawnień do edycji i odczytu. Dotyczy to informacji dostępnych zarówno w sieciach wewnętrznych, jak i sieciach zewnętrznych. Kontrola dostępu powinna rozpoczynać się już na poziomie systemów operacyjnych.
- **Nabycie systemu informacyjnego, rozwój i utrzymanie.** Podczas rozbudowy systemów informatycznych należy również pamiętać o zabezpieczeniach. Każda zmiana musi być autoryzowana przez odpowiednie osoby oraz przed zastosowaniem przetestowana w wydzielonym środowisku testowym. Punkt ten opisuje również, w jaki sposób bezpiecznie stosować metody kryptograficzne.
- **Zarządzanie incydentami bezpieczeństwa informacji.** Zgłaszanie, rejestrowanie i reagowanie na wszelkie incydenty związane z bezpieczeństwem informacji jest kluczowym elementem systemu zarządzania bezpieczeństwem informacji. Systemowe rozwiązania komunikacyjne wewnątrz firmy, wskazanie osób odpowiedzialnych za reagowanie na incydenty, określenie ścieżek komunikacyjnych i określenie maksymalnych czasów reakcji na incydenty gwarantuje skuteczność SZBI i jest podstawą do precyzyjnego określenia poziomów ryzyka.

- **Zarządzanie ciągłością działania**. Każda organizacja powinna poczynić odpowiednie kroki w celu zapewnienia ciągłości najważniejszych działań biznesowych. Obejmuje to analizę najbardziej prawdopodobnych i najdotkliwszych w skutkach awarii oraz opracowanie planów mających na celu jak najszybsze przywrócenie organizacji do poprawnego funkcjonowania. Dodatkowo wszystkie stworzone plany muszą być okresowo testowane pod kątem przydatności w momencie materializacji zagrożeń.
- **Zgodność z prawem i własnymi wymaganiami**. Podstawowym warunkiem certyfikowania systemu bezpieczeństwa informacji jest pełna zgodność z obowiązującymi przepisami prawnymi. Aby spełnić przedstawiane w normie wymagania, należy przeanalizować akty normatywne w zakresie bezpieczeństwa informacji i wprowadzić rozwiązania gwarantujące spełnienie wymagań prawnych. Dodatkowo konieczne jest wprowadzenie pewnych instrumentów, takich jak audyty wewnętrzne, przeglądy kierownictwa, zapewniające doskonalenie systemu bezpieczeństwa informacji.



Rys. 37. Model PDCA stosowany w procesach SZBI

Źródło: ISO/IEC 27001, figure 1 – PDCA model applied to SZBI processes, s. vi

Istotną cechą standardu jest powiązanie potencjalnych zagrożeń zewnętrznych, powszechnie uznawanych za najbardziej niebezpieczne, z analizą zagrożeń wewnętrznych. Oznacza to, że w rozumieniu normy nie tylko partnerzy rynkowi,

dostawcy i odbiorcy mogą stanowić potencjalne zagrożenie dla informacji gospodarczych, równie istotne są zagrożenia wewnętrzne, związane z pracownikami.

Model systemu powinien zostać podporządkowany podejściu procesowemu. W praktyce zachodzi konieczność wykorzystania filozofii zawartej w spirali Deminga (PDCA), a w przypadku systemów zintegrowanych z SZJ – niezbędne jest uwzględnienie zarządzania bezpieczeństwem informacji w strukturze procesów wynikających chociażby z SZJ (ISO 9001).

Podejście procesowe ma szczególne znaczenie wobec:
- zrozumienia wymagań bezpieczeństwa informacji w organizacji oraz ustanowienia zasad i celów bezpieczeństwa organizacji,
- wdrożenia i eksploatacji zabezpieczeń w celu zarządzania ryzykiem bezpieczeństwa informacji w kontekście całkowitego ryzyka biznesowego organizacji,
- monitorowania i przeglądu wydajności oraz skuteczności SZBI,
- ciągłego doskonalenia zgodnie z obiektywnym pomiarem.

Norma ISO/IEC 27001, oprócz wymagań związanych stricte z budową, funkcjonowaniem i utrzymaniem systemu zarządzania bezpieczeństwem informacji, określa także cele i zabezpieczenia. Cała lista konkretnych wymagań w tym zakresie opisanych jest w załączniku A. Składa się on z 11 rozdziałów ponumerowanych od A.5 do A.15. Numeracja ta wynika ze struktury ISO/IEC 27002, będącej zbiorem dobrych praktyk w zakresie bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.

Dla zapewnienia lepszej czytelności niniejszej części podręcznika zastosowana została numeracja z normy ISO/IEC 27002 (Załącznik A).

A.5. Polityka bezpieczeństwa,
A.6. Organizacja bezpieczeństwa informacji,
A.7. Zarządzanie aktywami,
A.8. Bezpieczeństwo zasobów ludzkich,
A.9. Bezpieczeństwo fizyczne i środowiskowe,
A.10. Zarządzanie systemami i sieciami,
A.11. Kontrola dostępu,
A.12. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
A.13. Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
A.14. Zarządzanie ciągłością działania,
A.15. Zgodność.

Obszary bezpieczeństwa wymienione przez standard w tej kolejności nie określają w żaden sposób ich znaczenia dla systemu zarządzania bezpieczeństwem informacji. Wszystkie obszary są równoważne.

Poszczególne obszary składają się łącznie z 39 celów zabezpieczeń (*objectives*), w których to wskazano zabezpieczenia (*controls*) wraz ze wskazówkami realizacji, innymi informacjami o charakterze technicznym lub prawnym.

Każdy obszar bezpieczeństwa (A.5, A6...) składa się z poszczególnych celów zabezpieczeń (A.5.1, A.6.1...). Cele zabezpieczenia mają pokazywać, co powinno zostać osiągnięte. Każdy cel zabezpieczeń musi natomiast zawierać co najmniej jedno zabezpieczenie (A.5.1.1, A.5.1.2...), czyli konkretny środek do osiągnięcia danego celu.

Cele stosowania zabezpieczeń i zawarte w nich zabezpieczenia wymienione w załączniku A nie wyczerpują tematu bezpieczeństwa informacji. Załącznik należy traktować jako absolutne minimum w zakresie zarządzania bezpieczeństwem informacji. W związku z tym organizacja może zadecydować o wprowadzeniu dodatkowych zabezpieczeń i celów zabezpieczeń.

Tab. 34. Struktura załącznika A

Zagadanie bezpieczeństwa	Liczba celów zabezpieczeń	Liczba zabezpieczeń
A.5. Polityka bezpieczeństwa	1	2
A.6. Organizacja bezpieczeństwa informacji	2	11
A.7. Zarządzanie aktywami	2	5
A.8. Bezpieczeństwo zasobów ludzkich	3	9
A.9. Bezpieczeństwo fizyczne i środowiskowe	2	13
A.10. Zarządzanie systemami i sieciami	10	32
A.11. Kontrola dostępu	7	25
A.12. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych	6	16
A.13. Zarządzanie incydentami związanymi z bezpieczeństwem informacji	2	5
A.14. Zarządzanie ciągłością działania	1	5
A.15. Zgodność	3	10
SUMA	**3**	**133**

3.1. Ustanowienie i zarządzanie SZBI

Stosowanie standardu nie jest obowiązkowe, jednak w przypadku podjęcia decyzji o wdrażaniu SZBI oraz ubieganiu się o certyfikat konieczne jest ustanowienie, wdrożenie, eksploatowanie, monitorowanie, przeglądanie, utrzymywanie i doskonalenie udokumentowanego systemu w odniesieniu do prowadzonej działalności i ryzyka występującego w organizacji[467]. Wszystkie zatem wymagania muszą zostać wnikliwie przeanalizowane; nie wystarczy że przybiorą postać deklaracji, bowiem konieczne jest zapewnienie dowodów ich stosowania. Jeżeli jest to wymagane, konieczne jest udokumentowanie rozwiązań, a w każdym przypadku niezbędna jest ich weryfikacja

[467] ISO/IEC 27001, p. 4.1.

pod kątem adekwatności, wystarczalności i skuteczności. Kluczem do zaprojektowania wdrożenia optymalnego SZBI jest oparcie się na wyniku szacowania ryzyka.

Na etapie wdrażania, utrzymania i rozwoju systemu konieczne jest[468]:

- zdefiniowanie zakresu i granic SZBI,
- określenie polityki bezpieczeństwa informacji,
- określenie metody szacowania ryzyka oraz jej zastosowanie, analiza i ocena ryzyka,
- zdefiniowanie i ocena wariantów postępowania z ryzykiem,
- określenie celów stosowania zabezpieczeń oraz zabezpieczenia – jako środki postępowania z ryzykiem,
- uzyskanie akceptacji dla ryzyka szczątkowego,
- uzyskanie zatwierdzenia przez kierownictwo dla wdrażania i utrzymania SZBI,
- przygotowanie deklaracji stosowania,
- praktyczna realizacja wszystkich elementów SZBI wynikających z wymagań oraz ustanowionych w odpowiedzi na nie przez daną organizację.

Każda organizacja może zaprojektować własny, indywidualny SZBI, może on być oparty na dowolnym modelu. Jednak w przypadku wybrania ISO/IEC 27001 oraz zamiaru ubiegania się o certyfikat – konieczne jest spełnienie wszystkich wymagań. Dopuszczalne są wyłączenia odnoszące się wyłącznie do zabezpieczeń, jednak pod pewnymi warunkami, o jakich była mowa wcześniej. Konieczne jednak jest ustanowienie granic SZBI, a zatem tego, czy objęte nim będą wszystkie procesy, wszystkie struktury organizacji, oddziały itd.

Wiodącym dokumentem w SZBI jest polityka bezpieczeństwa i przy jej definiowaniu należy zapewnić charakterystykę prowadzonej działalności, specyfikę organizacji, lokalizację, aktywa i technologię. Przykład podano poniżej.

Polityka bezpieczeństwa firmy informatycznej w ramach SZBI

Informacja jest bardzo ważnym aktywem przedsiębiorstwa ABC i dlatego należy ją odpowiednio chronić.

Jakość naszej pracy zależy w dużej mierze od jakości informacji.

Chroniąc informacje, zachowujemy prywatność i godność każdego pracownika oraz dbamy o interesy partnerów i klientów.

Bezpieczeństwo informacji w przedsiębiorstwie ABC ma podstawowe znaczenie dla utrzymania naszej konkurencyjności, płynności finansowej, zysku, zgodności z przepisami prawa i wizerunku firmy.

Spełnienie wymagań prawnych jest celem podstawowym i stanowi podstawę ustanowionego i rozwijanego SZBI ISO/IEC 27001:2005.

[468] ISO/IEC 27001, p. 4.2.1.

Niniejszy dokument jest nadrzędny wobec pozostałych polityk (haseł, dostępu, sieciowej, eksploatacji komputerów) i przywołuje najważniejsze zasady postępowania z informacją w przedsiębiorstwie ABC.

Obowiązkiem pracowników jest przestrzeganie postanowień niniejszej polityki bezpieczeństwa przedsiębiorstwa ABC, a w szczególności zasad: co nie jest wyraźnie dozwolone, jest zabronione, czystego biurka i czystego ekranu.

Źródło: dokumentacja SZBI firmy informatycznej.

Treść polityki bezpieczeństwa informacji, niezależnie od tego, jak będzie oryginalna, musi[469]:

- zawierać ramy dla ustalania celów oraz wyznaczać ogólny kierunek oraz zasady działania dotyczące bezpieczeństwa informacji,
- brać pod uwagę wymagania biznesowe oraz prawne lub o charakterze regulacyjnym, a także wynikające z umów zobowiązania związane z bezpieczeństwem,
- ustanawiać w organizacji kontekst strategiczny zarządzania ryzykiem dający obszar ustanowienia i utrzymania SZBI,
- określać kryteria, według których ma być oceniane ryzyko.

Treść polityki bezpieczeństwa musi być zatwierdzona przez kierownictwo.

Kolejnym istotnym wymaganiem stawianym przez ISO/IEC 27001 jest konieczność zdefiniowania podejścia do szacowania ryzyka w organizacji[470]. W tym zakresie konieczne jest:

- wskazanie metody szacowania ryzyka, odpowiedniej dla SZBI, określenie bezpieczeństwa informacji w kontekście prowadzonej działalności, wymagań prawnych i wymagań nadzoru,
- opracowanie kryteriów akceptacji ryzyka i określenie akceptowalnego poziomu ryzyka,
- wybranie metody szacowania ryzyka, która powinna zapewnić, że szacowanie to daje porównywalne i powtarzalne rezultaty[471].

Następnie wymagane jest określenie ryzyka poprzez[472]:

- określenie aktywów znajdujących się w zakresie SZBI oraz właścicieli[473] tych aktywów,

[469] ISO/IEC 27001, p. 4.2.1.

[470] ISO/IEC 27001, p. 4.2.1.

[471] Autorzy zwrócili uwagę, że można dokonać wyboru metody szacowania ryzyka spośród wielu dostępnych, jak też opracować własną – indywidualną, przy tym konieczne jest udowodnienie jej skuteczności i porównywalności wyników. ISO/IEC 27001 wskazuje, że istnieją różne metody szacowania ryzyka. Przykłady metod szacowania ryzyka są omówione w ISO/IEC TR 13335–3, Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security.

[472] ISO/IEC 27001, p. 4.2.1d.

[473] Patrz przypis nr 2 w ISO/IEC 27001, s. 11. Termin „właściciel" określa osobę lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność za nadzorowanie produkcji, rozwój, utrzyma-

- zdefiniowanie zagrożeń dla tych aktywów,
- określenie podatności, które mogą być wykorzystane przez zagrożenia,
- określenie skutków utraty poufności, integralności i dostępności w odniesieniu do wskazanych aktywów.

Kolejny krok wymagany przez normę związany jest z koniecznością dokonania analizy i oceny ryzyka. W niniejszym zakresie konieczne jest[474]:

- oszacowanie szkód i strat biznesowych w organizacji, które mogą wyniknąć z naruszenia bezpieczeństwa, biorąc pod uwagę potencjalne konsekwencje utraty poufności, integralności i dostępności aktywów,
- oszacowanie realnego prawdopodobieństwa zdarzenia się takiego naruszenia bezpieczeństwa w świetle istotnych zagrożeń i podatności oraz konsekwencji związanych z tymi aktywami oraz aktualnie wdrożonymi zabezpieczeniami,
- wyznaczenie poziomu ryzyka,
- stwierdzenie w kontekście przyjętych kryteriów, czy ryzyko jest akceptowalne, czy też wymaga postępowania.

Kolejna konieczność związana ze spełnieniem wymagań to identyfikacja i ocena wariantów postępowania z ryzykiem. Możliwości w tym względzie obejmują[475]:

- zastosowanie odpowiednich zabezpieczeń,
- poznanie i zaakceptowanie ryzyka, w sposób świadomy i obiektywny, przy założeniu, że jasno spełnia warunki wyznaczone w polityce organizacji oraz kryteria akceptowania ryzyka,
- unikanie ryzyka,
- przeniesienie związanego ryzyka biznesowego na innych uczestników, na przykład ubezpieczycieli, dostawców.

Należy pamiętać, że minimalny zestaw zabezpieczeń został przedstawiony w załączniku A do normy[476] i wszystkie powinny być stosowane. Przy tym jednak ważniejsze jest kluczowe osiąganie celów dotyczących bezpieczeństwa informacji. A zatem możliwe jest wyłączenie niektórych z nich, ale warunek konieczny w tym zakresie to zapewnienie zaplanowanego poziomu bezpieczeństwa (osiąganie celów – zapewnienie skuteczności systemu). Zestawienie wybranych i stosowanych zabezpieczeń musi zostać określone w specyficznym dla SZBI dokumencie – deklaracji stosowania.

Ponadto postępując z ryzykiem, można je wykluczyć z organizacji, z realizowanych w niej procesów. Rozwiązaniem w tym zakresie są procesy realizowane outsourcingowo, na przykład utrzymanie ruchu, zarządzanie kadrami, archiwizacja dokumentów czy procesy technologiczne. Realizacja procesów, czy tylko wybranych

---

nie, korzystanie i bezpieczeństwo aktywów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do aktywów.

[474] ISO/IEC 27001, p. 4.2.1e.

[475] ISO/IEC 27001, p. 4.2.1f.

[476] Zabezpieczenia (Załącznik A do ISO/IEC 27001) omówione zostały w dalszej części podręcznika.

działań na zewnątrz organizacji, jest możliwa tylko w ograniczonym zakresie i należy pamiętać, że taka koncepcja tworzy nowe ryzyko, jakie niesie ze sobą zewnętrzny wykonawca, komunikacja zewnętrzna, transport itd. Stąd konieczność przeniesienia ryzyka na innych uczestników.

Radykalnym działaniem jest taka reorganizacja procesów, która wyeliminuje dane ryzyko. Na przykład rezygnacja z danego procesu, działania czy nawet technologii dla wykluczenia wystąpienia konkretnego ryzyka. Brzmi to niewiarygodnie, ale staje się realne, kiedy zestawimy cele, zagrożenia, podatności i okaże się, że ryzyko stanowi zagrożenie dla żywotnych interesów organizacji.

Kolejnym wymaganiem stawianym przez normę ISO/IEC 27001 jest konieczność dokonania wyboru celów stosowania zabezpieczeń i zabezpieczenia jako środki postępowania z ryzykiem. Odzwierciedleniem spełnienia niniejszego wymagania jest także deklaracja stosowania, przy tym należy ją opracowywać w relacji z treścią polityki bezpieczeństwa.

Cele stosowania zabezpieczeń i zabezpieczenia powinny być wybrane i wdrożone w taki sposób, aby spełniały wymagania zidentyfikowane w procesach szacowania ryzyka i postępowania z ryzykiem. W wyborze powinno się brać pod uwagę kryteria akceptacji ryzyka, jak również wymagania prawne, wymagania nadzoru oraz zobowiązania wynikające z umów[477].

Zgodnie z obowiązującą zasadą, tak cele, jak zabezpieczenia określone w załączniku A do normy ISO/IEC 27001 nie stanowią wyłącznego ich źródła, ale zaledwie minimum, które powinno być wybrane jako część tego procesu, by w odpowiedni sposób spełnić zidentyfikowane wymagania.

Zależnie od specyfiki prowadzonej działalności mogą więc być wybrane dodatkowe cele stosowania zabezpieczeń i zabezpieczenia. Wskutek zaplanowanych i realizowanych działań związanych z postępowaniem z ryzykiem (bowiem są to działania realizowane zgodnie ze spiralą Deminga) pozostaje ryzyko szczątkowe, dlatego konieczne jest uzyskanie akceptacji kierownictwa dla jego poziomu[478]. Następne niezbędne kroki (wymagania) stawiane przez normę to uzyskanie autoryzacji kierownictwa do wdrażania i stosowania rozważań systemowych oraz przygotowanie deklaracji stosowania[479]. Deklaracja stosowania jest najbardziej specyficznym dla SZBI dokumentem, jednocześnie musi zawierać:

- cele stosowania zabezpieczeń i wybrane zabezpieczenia oraz uzasadnienie ich wyboru,
- cele stosowania zabezpieczeń i zabezpieczenia już wdrożone,
- informację o wykluczeniu jakiegokolwiek celu stosowania zabezpieczeń i zabezpieczenia wymienionego w załączniku A wraz z uzasadnieniem wykluczenia.

[477] ISO/IEC 27001, p. 4.2.1g.
[478] ISO/IEC 27001, p. 4.2.1h.
[479] ISO/IEC 27001, p. 4.2.1i–j.

Jest oczywiste, że treść deklaracji stosowania stanowi zwieńczenie działań dotyczących postępowania z ryzykiem, a uzasadnienie wyłączeń umożliwia powtórne sprawdzenie, czy żadne zabezpieczenie nie zostało nieumyślnie pominięte.

3.2. Wdrożenie i stosowanie SZBI

W ramach działań określonych w normie jako wdrożenie i stosowanie rozwiązań w ramach SZBI konieczne jest[480]:

- sformułowanie planu postępowania z ryzykiem, w którym są określone odpowiednie działania kierownictwa, zakresy odpowiedzialności oraz priorytety dla zarządzania ryzykiem związanym z bezpieczeństwem informacji,
- wdrożenie planu postępowania z ryzykiem w celu osiągnięcia zidentyfikowanych celów stosowania zabezpieczeń, które obejmują rozważenie przydzielania ról i zakresów odpowiedzialności,
- wdrożenie zabezpieczeń określonych w SoA tak, aby osiągnąć cele ich stosowania,
- określenie metod mierzenia skuteczności i efektywność wybranych zabezpieczeń (i grup zabezpieczeń) oraz wskazanie, jak te mierniki powinny być stosowane w ocenie efektywności zabezpieczeń[481],
- wdrożenie programów uświadamiania i szkolenia,
- zarządzanie rozwiązaniami ustanowionymi w ramach SZBI oraz zasobami SZBI,
- wdrożenie procedur i innych skutecznych zabezpieczeń dla zapewnienia natychmiastowego wykrycia i reakcji na incydenty związane z naruszeniem bezpieczeństwa.

To ogólne wymagania, jednak definiujące strategiczne kierunki działań w systemie. Nawiązują bezpośrednio do wymagań związanych z ustanowieniem i wdrożeniem systemu, wskazują także konkretne opracowania – ponownie SoA, ale także opracowanie i wdrożenie planu postępowania z ryzykiem, określenie w tym względzie odpowiedzialności.

Typowe dla międzynarodowych standardów jest ogólne definiowanie wymagań. Także w tym przypadku konieczne jest zaplanowanie i wykonanie działań związanych z postępowanie z ryzykiem, przy czym może to być konkretny dokument oparty na raporcie szacowania ryzyka, czy też różne opracowania wyczerpujące niniejszy temat. Zwykle są to zakresy obowiązków i uprawnień pracowników związane z bezpieczeństwem informacji, procedury opracowane w ramach SZBI, plany ciągłości działania itd.

Ważne wymaganie dotyczy tak wdrożenia zabezpieczeń określonych w deklaracji stosowania, jak konieczności monitorowania ich skuteczności. To jest element

[480] ISO/IEC 27001, p. 4.2.2a–h.

[481] Aby otrzymać porównywalne i powtarzalne rezultaty.

„nowy", który w praktyce sprawia bardzo wiele problemów. Działania w tym względzie najczęściej są wielorakie, sprowadzają się do typowych narzędzi SZBI, przede wszystkim zarządzania incydentami, audytów, działań kontrolnych, zabezpieczeń, oceny skuteczności szkoleń, ale także specyficznych – wskaźników dotyczących konkretnych zabezpieczeń. Trzeba pamiętać, że za właściwie zdefiniowane działania w ramach postępowania z ryzykiem należy uznać działania adekwatne. O ile w odniesieniu do ryzyka niewiele przekraczającego poziom ryzyka marginalnego mogą to być standardowe zabezpieczenia, o tyle w przypadku ryzyka określonego jako kluczowe działania muszą być szczególnie dobrze dobrane. Dlatego też konieczne jest określenie priorytetów dla zarządzania ryzykiem, związanych z bezpieczeństwem informacji. Plan postępowania z ryzykiem powinien obejmować zróżnicowane działanie, co zwiększa prawdopodobieństwo skuteczności.

3.3. Monitorowanie i przegląd SZBI

W ramach systemu zarządzania bezpieczeństwem informacji wymagane jest tak monitorowanie, jak i przegląd systemu. Organizacja musi w tym względzie realizować procedury monitorowania i przeglądu oraz inne zabezpieczenia w celu[482]:

- natychmiastowego wykrywania błędów w wynikach przetwarzania,
- natychmiastowego identyfikowania naruszeń bezpieczeństwa i incydentów, zakończonych niepowodzeniem lub sukcesem,
- umożliwienia kierownictwu stwierdzenia, czy działania związane z bezpieczeństwem delegowane są na poszczególne osoby lub wdrożone za pomocą środków informatycznych są wykonywane zgodnie z oczekiwaniami,
- pomocy w wykrywaniu naruszeń bezpieczeństwa, tym samym niedopuszczenia do incydentów bezpieczeństwa przez użycie wskaźników,
- określenia, czy działania podjęte w celu rozwiązania naruszeń bezpieczeństwa były efektywne.

Ponadto konieczne jest:

- wykonywanie regularnych przeglądów efektywności SZBI (w tym zgodności z polityką i celami SZBI oraz przegląd zabezpieczeń), biorąc pod uwagę wyniki audytów bezpieczeństwa, incydenty, rezultaty pomiarów efektywności, sugestie oraz informacje zwrotne od wszystkich zainteresowanych stron,
- mierzenie efektywności zabezpieczeń w celu weryfikacji ich zgodności z wymaganiami bezpieczeństwa,
- dokonywanie przeglądu szacowania ryzyka w zaplanowanych odstępach czasu, przeglądu ryzyka szczątkowego oraz przeglądu poziomów ryzyka akceptowalnego, przy uwzględnieniu zmian w organizacji, technologii, celów biznesowych

[482] ISO/IEC 27001, p. 4.2.3a 1–5.

i procesowych, zidentyfikowanych zagrożeń, efektywności wdrożonych zabezpieczeń, zewnętrznych zdarzeń, takich jak zmiany prawa lub stosownych regulacji, zmian wynikających z umów oraz zmiany o charakterze społecznym),
- przeprowadzanie wewnętrznych audytów SZBI w zaplanowanych odstępach czasu.

Ponadto niezbędne jest zaplanowanie i wykonywanie, w regularnych odstępach czasu, przeglądów SZBI realizowanych przez kierownictwo; celem przeglądów zarządzania jest weryfikacja adekwatności zakresu systemu oraz określenie ewentualnych zmian. Należy także aktualizować plany bezpieczeństwa, opierając modyfikacje na rezultacie monitorowania oraz weryfikacji zakresu i skuteczności rozwiązań systemowych.

Obowiązkowe jest także rejestrowanie działań i zdarzeń, które mogą mieć wpływ na efektywność lub wydajność realizacji SZBI.

3.4. Utrzymanie i doskonalenie SZBI

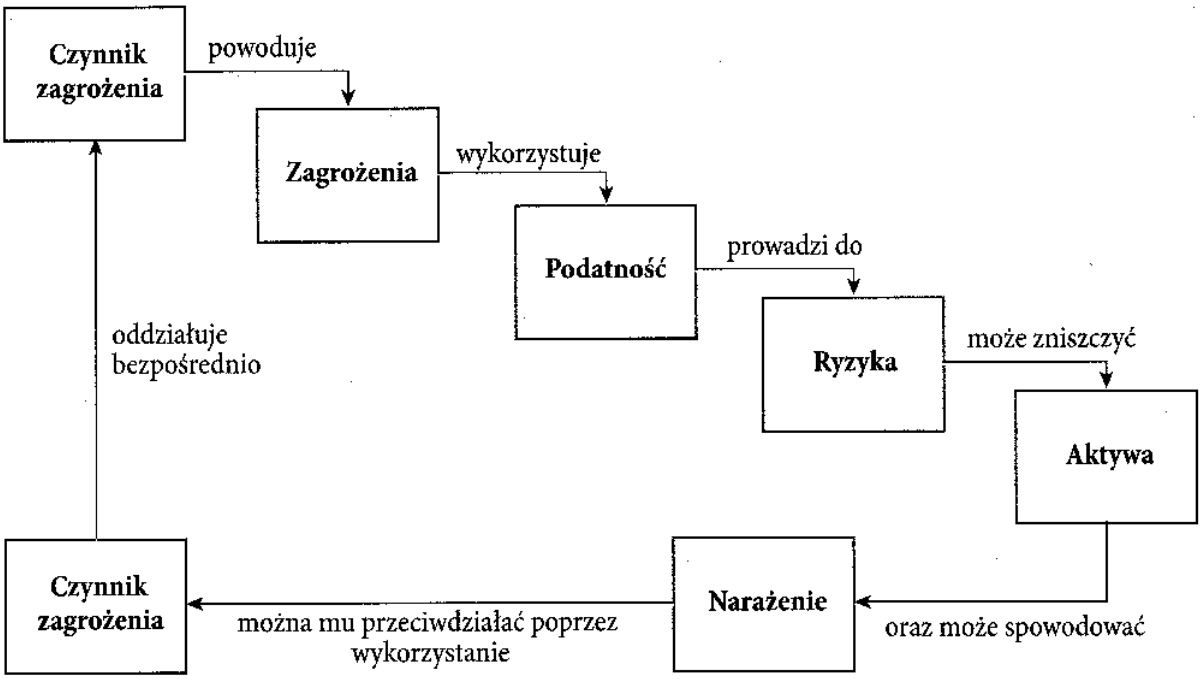
Organizacja, która posiada lub ubiega się o certyfikowany system zarządzania bezpieczeństwem informacji, musi podejmować następujące działania[483]:
- wdrażać w SZBI zidentyfikowane udoskonalenia,
- podejmować odpowiednie działania korygujące lub zapobiegawcze,
- wyciągać wnioski z doświadczeń w dziedzinie bezpieczeństwa zarówno innych organizacji, jak i własnych,
- informować wszystkie zainteresowane strony o działaniach i udoskonaleniach na odpowiednim do okoliczności poziomie szczegółowości oraz, jeśli konieczne, uzgodnić sposób dalszego postępowania,
- zapewnić, że udoskonalenia osiągają zamierzone cele.

4. Zadządzanie ryzykiem bezpieczeństwa informacji

Na systemy informacyjne składają się zasoby, które powinny być chronione (mogą one pochodzić z zewnątrz i wewnątrz). **Wszystkie zasoby posiadają pewne podatności, które mogą zostać wykorzystane przez zagrożenia. Ryzykiem w tym przypadku można nazwać prawdopodobieństwo takiego niepożądanego wykorzystania podatności**. W celu zminimalizowania ryzyka stosuje się zabezpieczenia (procedury, dobre praktyki, ochrona fizyczna, softwareowa, mechanizmy redukujące

[483] ISO/IEC 27001, p. 4.2.4a–d.

ryzyko itp.). Jednak zastosowanie żadnego z nich czy też ich kombinacji nie daje pewności bezpieczeństwa informacji; w każdym przypadku pozostaje ryzyko szczątkowe. Może również okazać się, że podatności nie mają żadnych zagrożeń, które by je wykorzystywały, co z kolei skutkuje tym, że nie muszą (aczkolwiek mogłyby) być chronione odpowiednimi zabezpieczeniami. Na rysunku 38 przedstawiono czynniki ryzyka, które wyodrębnili M.E. Whitman oraz H.J. Mattord[484].



Rys. 38. Zależności w zakresie czynników ryzyka

Źródło: Por. M.E. Whitman, H.J. Mattord, *Readings and Cases*, op.cit., s. 53

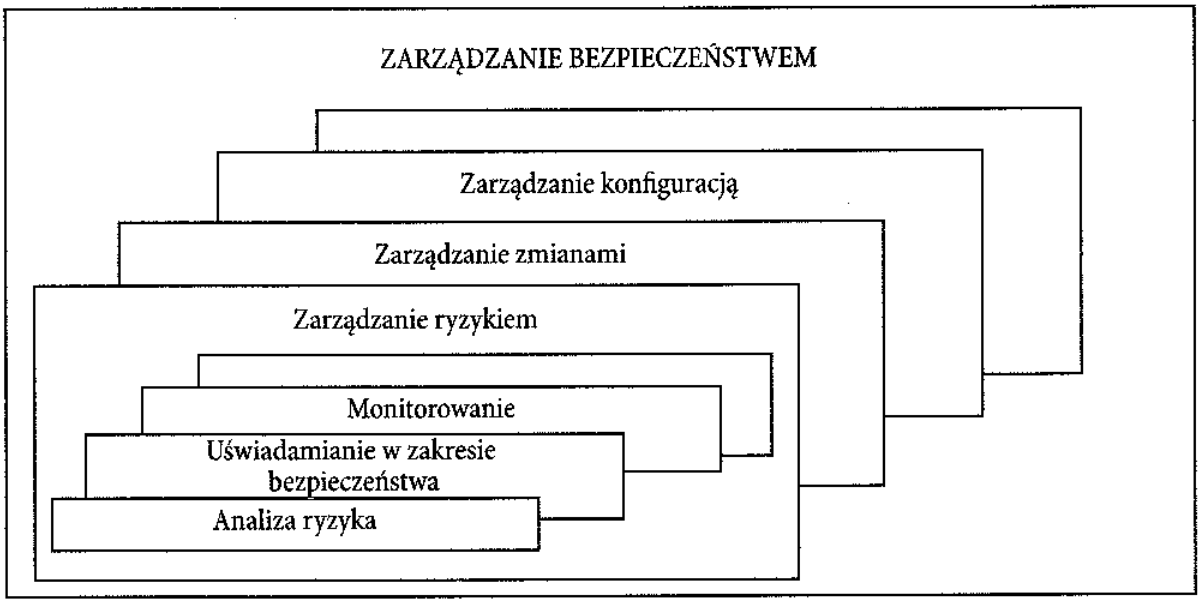
Całościowy i ciągły proces prowadzący do stworzenia i utrzymania bezpieczeństwa w instytucji jest nazywany zarządzaniem bezpieczeństwem. Składa się on z wielu podprocesów, wśród których jest zarządzane ryzykiem. Kluczowym elementem tego ostatniego jest natomiast analiza ryzyka. Podział ten przedstawiono na rysunku 40[485].

Norma PN-I-13335-1 definiuje ryzyko jako prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów[486]. Przez podatność zasobu lub grupy zasobów należy rozumieć słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie[487].

Rozumiejąc w ten sposób ryzyko, można je określić najprościej jako iloczyn prawdopodobieństwa (częstości) zdarzenia i miary strat spowodowanych tym

[484] M.E. Whitman, H.J. Mattord, *Readings and Cases*, op.cit., s. 53.
[485] http://kni.kul.lublin.pl/~andy/ref/other/risk.pdf, s.3.
[486] PN-I-13335-1.
[487] PN-I-13335-1.

zdarzeniem lub wartości aktywu. Takie podejście traktuje, że ryzyko jest takie samo, kiedy prawdopodobieństwo wystąpienia niekorzystnego zdarzenia jest małe, a miara strat duża, jak również w sytuacji, kiedy prawdopodobieństwo zajścia zdarzenia jest duże, lecz potencjalne straty są nieznaczne z punktu widzenia prowadzenia działalności.



Rys. 39. Zarządzanie bezpieczeństwem

Źródło: http://kni.kul.lublin.pl/~andy/ref/other/risk.pdf, s.3

Zarządzanie bezpieczeństwem (informacji) jest zatem zbiorem złożonych zależności, obejmującym na pewno, choć nie tylko: analizę ryzyka, świadomość, monitorowanie skuteczności zabezpieczeń, zarządzanie ryzykiem, zmianami i konfiguracją.

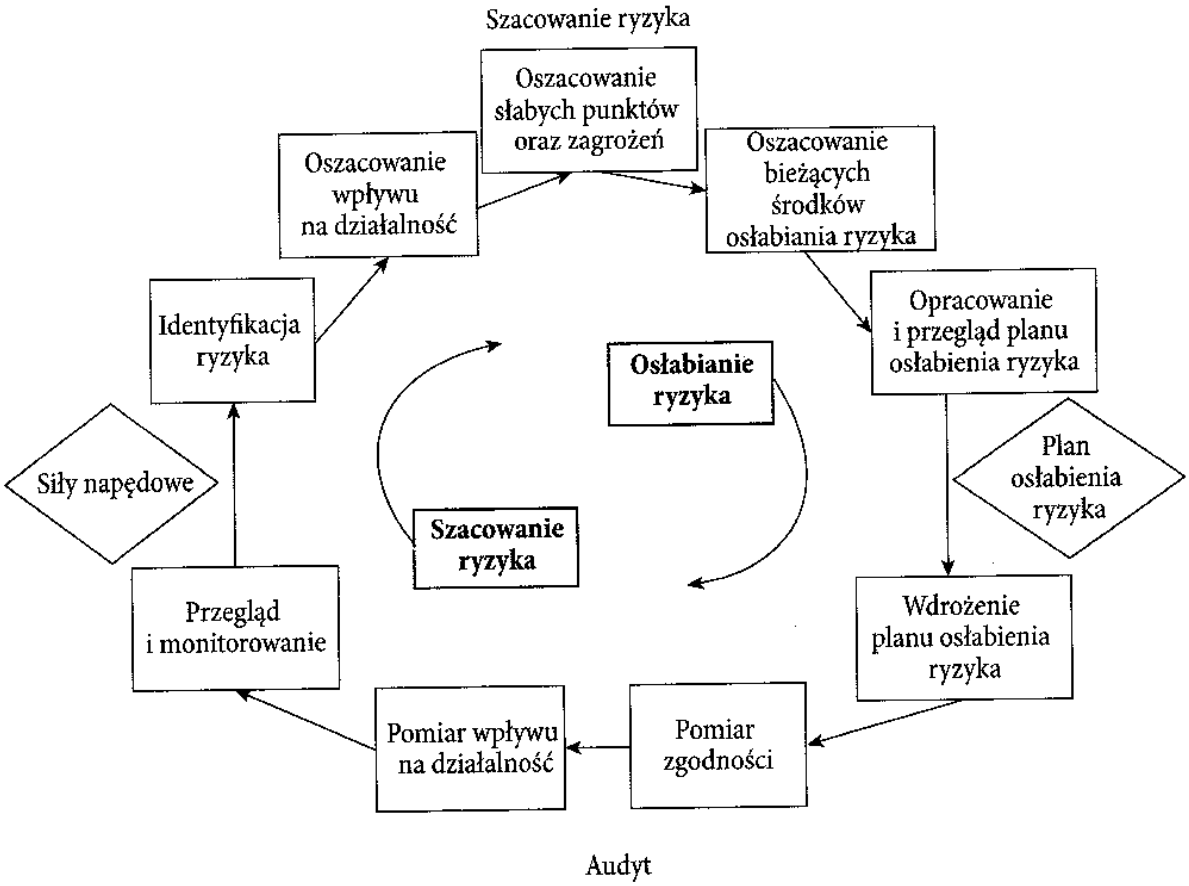
Zarządzanie ryzykiem to proces szacowania ryzyka mający na celu ograniczenie go do akceptowalnego poziomu. Powinien składać się z następujących faz: planowanie, nabywanie, rozwój, testowanie oraz odpowiednie rozmieszczenie systemów informatycznych[488].

Według A. Zoła[489] zarządzanie ryzykiem (*risk management*) to całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego. Natomiast analiza ryzyka (*risk analysis*) to proces identyfikacji ryzyka, określania jego wielkości i identyfikowania obszarów wymagających zabezpieczeń.

[488] M. Molski, M. Łachota, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007, s. 90.

[489] http://kni.kul.lublin.pl/~andy/ref/other/risk.pdf, s. 3.

M.E. Whitman zwraca uwagę na wzajemną relację pomiędzy szacowaniem ryzyka a jego osłabieniem – co stanowi istotę zarządzania ryzykiem[490].



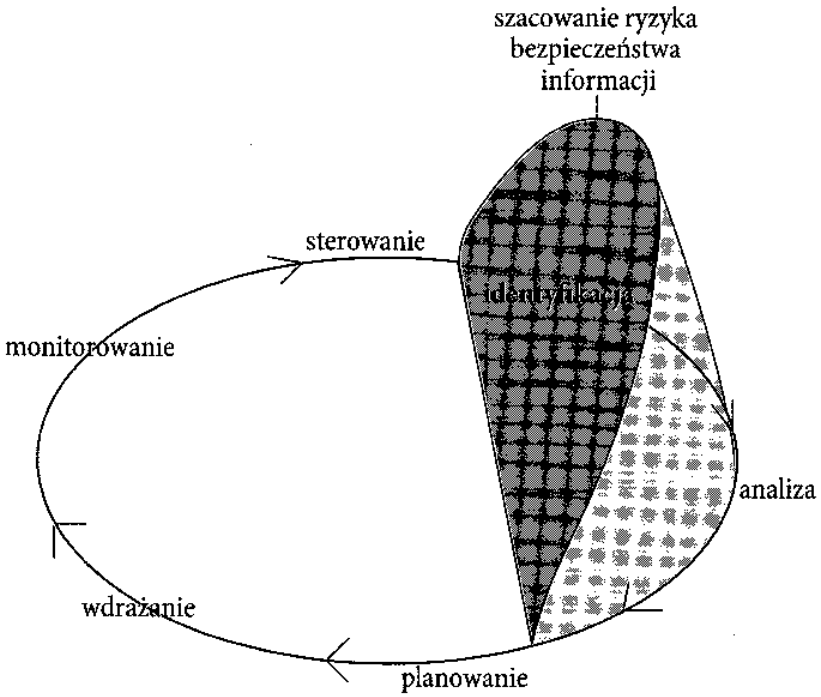
Rys. 40. Ogólna struktura zarządzania ryzykiem w SZBI

Źródło: między innymi M.E. Whitman, H.J. Mattord, *Readings and Cases*, op.cit., s. 50

M.E. Whitman[491] wskazuje na następujące etapy zarządzania ryzykiem:
- identyfikacja ryzyka,
- oszacowanie wpływu na działalność,
- oszacowanie słabych punktów i zagrożeń,
- oszacowanie bieżących środków osłabienia ryzyka,
- opracowanie i przegląd planu osłabienia ryzyka,
- wdrożenie planu osłabienia ryzyka,
- pomiar zgodności,
- pomiar wpływu na działalność,
- przegląd i monitorowanie.

[490] M.E. Whitman, H.J. Mattord, *Readings and Cases*, op.cit., s. 50.
[491] Ibidem, s. 53.

Zgodnie z PN-I-13335-1[492] zarządzanie ryzykiem jest rozumiane jako całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego[493]. Takie podejście ilustrują także Ch. Alberts oraz A. Dorofee, wykorzystujący zmodyfikowaną spiralę jakości (PDCA) (rys. 41).



Rys. 41. Ocena ryzyka w procesie zarządzania ryzykiem bezpieczeństwa informacji

Źródło: Ch. Alberts, A. Dorofee, *Managing Information Security Risks. The OCTAVE Approach*, Addison-Wesley, Boston 2003, s. 11

W ujęciu modelowym celem procesu zarządzania ryzykiem jest ograniczenie ryzyka do akceptowalnego poziomu przez opracowanie odpowiedniego planu postępowania z ryzykiem. Założeniem wpisanym w ten model jest to, że działania realizowane za jego pomocą są skuteczne i są wykonywane w sposób ciągły i systematyczny (monitoring, przeglądy).

M.E. Whitman oraz H.J. Mattord określają proces zarządzania ryzykiem w koniecznym układzie: kategoryzacja – szacowanie – komunikowanie (rysunek 42)[494].

[492] PN-I-13335-1 jest polskim tłumaczeniem standardu wydanego przez Międzynarodową Organizację Normalizacyjną (International Standard Organization) oraz Międzynarodową Komisję Elektrotechniczną (International Electrotechnical Commission) pod nazwą ISO/IEC TR 13335-1.

[493] PN-I-13335-1, s. 9.

[494] M.E. Whitman, H.J. Mattord, *Readings and Cases*, op.cit., s. 56.

Rys. 42. Proces zarządzania ryzykiem

Źródło: M.E. Whitman, H.J. Mattord, *Readings and Cases*, op.cit., s. 56

Zwracają jednocześnie uwagę, że brak odpowiedniego zdefiniowania i zakomunikowania przebiegu procesu zarządzania ryzykiem staje się hazardem.

Działania zmierzające do ochrony informacji muszą mieć charakter wynikowy, w żadnym razie początkiem (i końcem) działań w tym zakresie nie może być wybór zabezpieczeń. Niezależnie od zamiaru wdrażania SZBI według ISO/IEC 27001 (i jego certyfikacji) czy też budowy systemu opartego na innych (własnych) podstawach – jego istotą musi być zarządzanie ryzykiem.

5. Etapy wdrażania SZBI

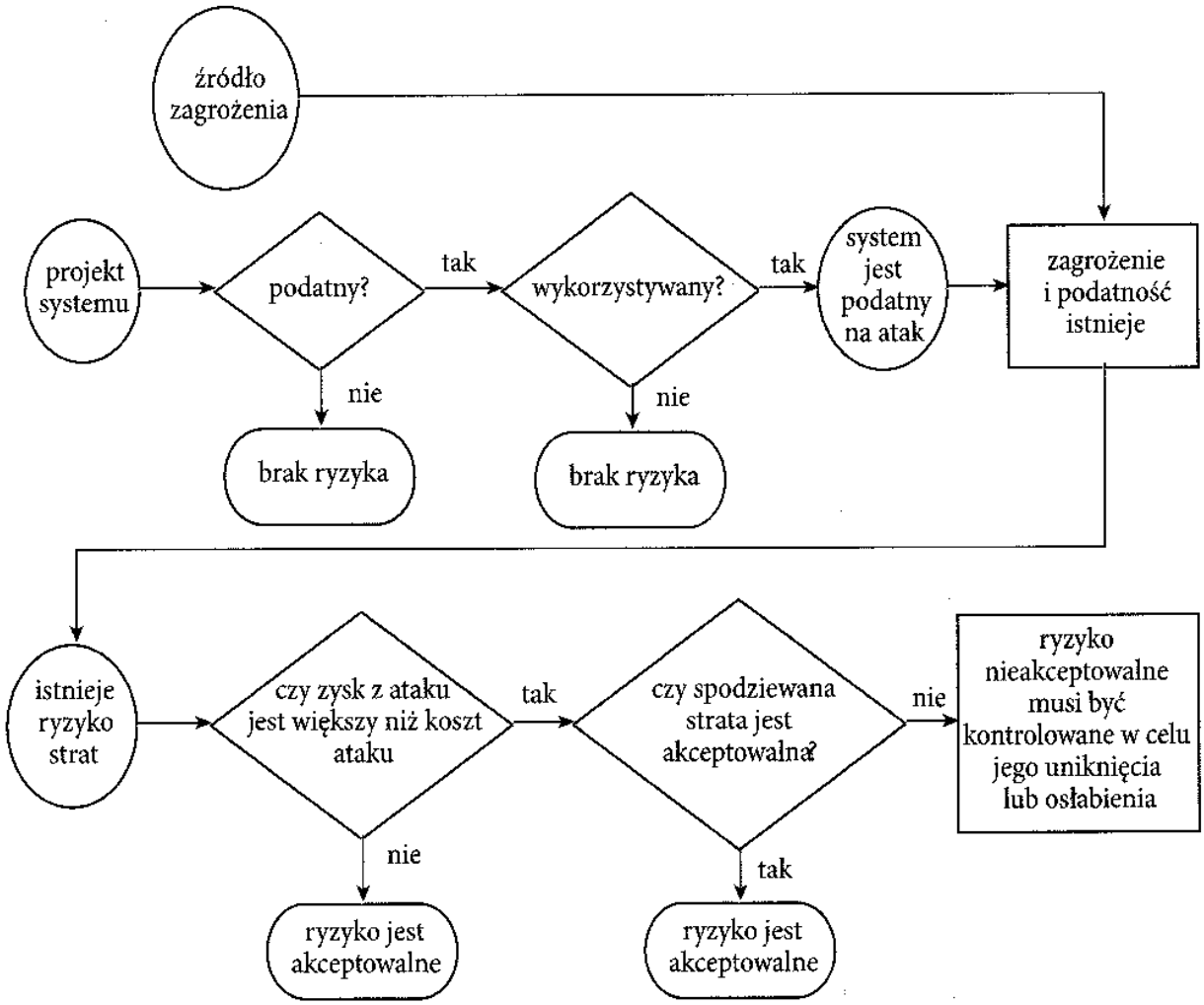
Wdrażanie SZBI bezwzględnie powinno opierać się na procesie szacowania ryzyka i – w szerszym ujęciu – na zarządzaniu ryzykiem bezpieczeństwa informacji. Zdaniem M.E. Whitmana oraz H.J. Mattorda, postępowanie z ryzykiem powinno przebiegać według schematu przedstawionego na rysunku 43[495].

Ostatecznie niezbędne są rozwiązania systemowe dotyczące kontroli ryzyka nieakceptowalnego, dla jego uniknięcia lub osłabienia.

Standard ISO/IEC 27001 określa w swojej treści wymagania, które dotyczą ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalenia udokumentowanego SZBI w całościowym kontekście ryzyka biznesowego. Zostały w niej określone także wymagania dotyczące wdrożenia zabezpieczeń dostosowanych do potrzeb pojedynczych organizacji lub ich części. Koncepcja stworzenia

[495] M.E. Whitman, H.J. Mattord, *Management of Information Security*, op.cit., s. 304.

systemu zarządzania bezpieczeństwem informacji jest taka, aby zagwarantować adekwatne i proporcjonalne zabezpieczenia, które w odpowiedni sposób chronią aktywa informacyjne, oraz aby możliwe było uzyskanie zaufania zainteresowanych stron. Nawiązania do biznesowej strony w niniejszej normie powinny być tłumaczone szeroko, z uwzględnieniem działań, które są głównym celem istnienia organizacji.



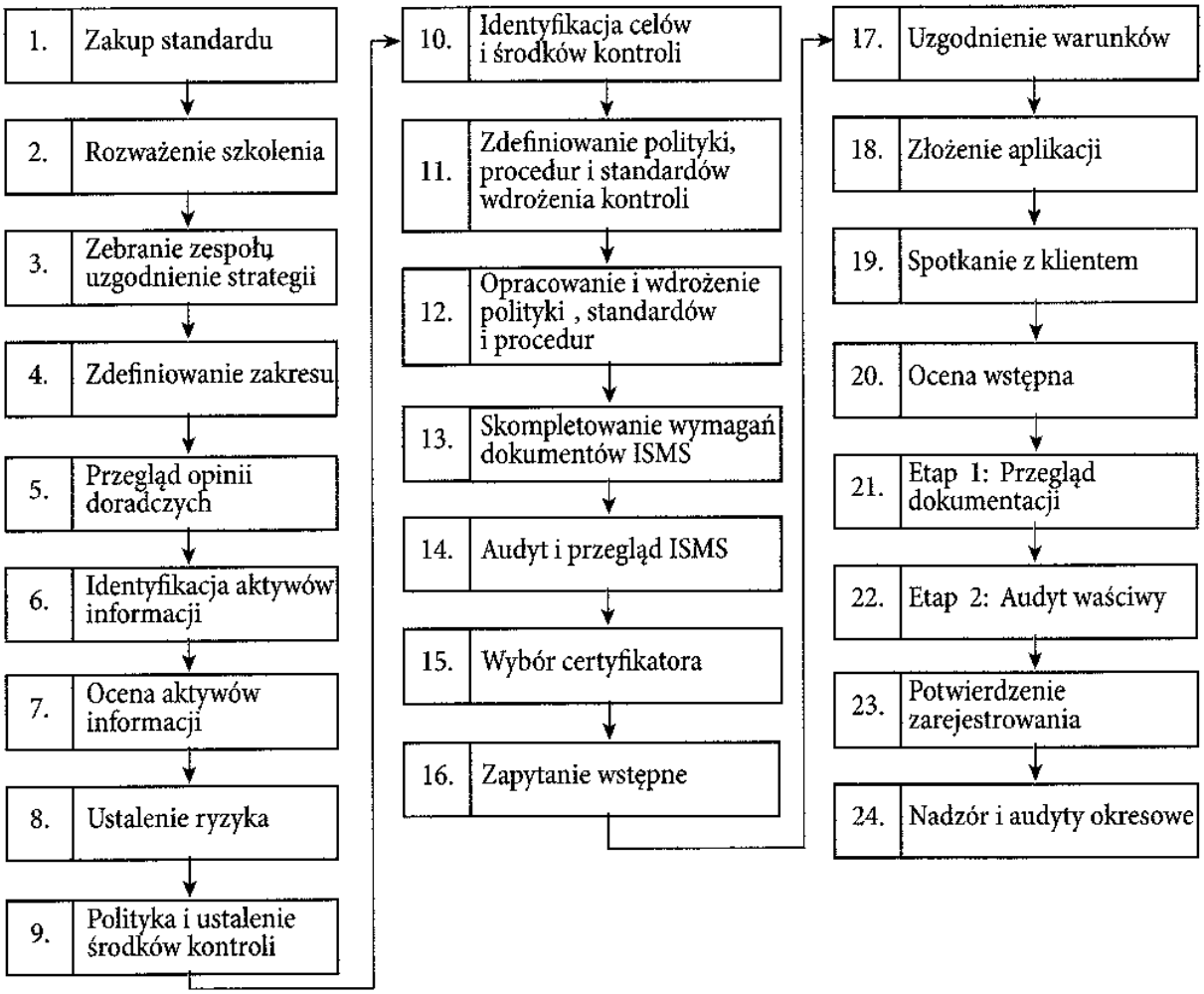
Rys. 43. Postępowanie z ryzykiem

Źródło: Por. M.E. Whitman, H.J. Mattord, *Management of Information Security*, op.cit., s. 304

Wymagania zawarte w powyższym standardzie są ogólne i przeznaczone do zastosowania we wszystkich organizacjach, niezależnie od typu, rozmiaru, rodzaju prowadzonej działalności gospodarczej. Jeżeli organizacja oczekuje zgodności ze standardem bezpieczeństwa, nie jest akceptowalne wyłączenie jakiegokolwiek wymagania opisanego w rozdziałach 4, 5, 6, 7 i 8 standardu. Jakiekolwiek wykluczenie zabezpieczenia, niezbędne do spełnienia kryteriów akceptacji ryzyka, powinno być uzasadnione i udokumentowane, a związane z tym ryzyko powinno być zaakceptowane przez upoważnione do tego osoby. W przypadku wykluczenia zabezpieczenia

nie można stwierdzić zgodności z normą ISO/IEC 27001, chyba że wykluczenia te nie mają wpływu na możliwości organizacji co do zapewnienia poziomu bezpieczeństwa informacji, spełniającego wymagania bezpieczeństwa określonego przez szacowanie ryzyka i odpowiednie wymagania prawne lub ustawowe[496]. Wynika z tego zatem, że **najważniejsze jest osiągnięcie celów związanych z bezpieczeństwem informacji. Są one kształtowane zgodnie z wymaganiami ustawowymi, wymaganiami klienta oraz czy wewnętrznymi organizacji. Dla ich realizacji konieczne jest zastosowanie wszystkich zabezpieczeń, przy czym wyłączenia są możliwe tylko wtedy, kiedy kombinacja zabezpieczeń lub inne zabezpieczenia pozwolą na osiągnięcie celów dotyczących bezpieczeństwa.**

Literatura i praktyka związana z SZBI podpowiada konieczne etapy wdrażania systemu (rysunek 44).

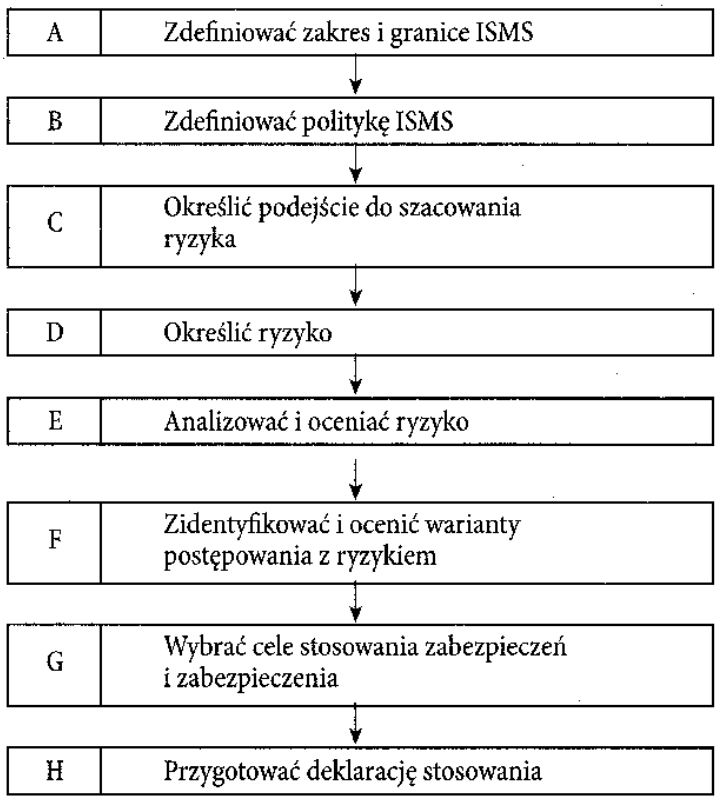


Rys. 44. Etapy wdrażania SZBI (ISO/IEC 27001)

Źródło: między innymi M.E. Whitman, H.J. Mattord, *Management of Information Security*, op.cit., s. 217

[496] PN ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN, Warszawa, 2007, s. 8.

Cały proces ustanowienia systemu zarządzania bezpieczeństwem informacji, jaki przedstawia model zaprezentowany w normie ISO/IEC 27001:2005, składa się z ośmiu etapów. Został on ujęty w punkcie 4.2. Ustanowienie SZBI wyżej wymienionego standardu. Schematycznie przedstawia to rysunek 45.



Rys. 45. Etapy ustanawiania SZBI

Źródło: opracowanie własne na podstawie normy ISO/IEC 27001

A. Zdefiniowanie zakresu i granic SZBI

Punktem początkowym do ustanowienia systemu zarządzania bezpieczeństwem informacji jest określenie i zdefiniowanie zakresu i granic systemu zarządzania. Powinno to być oparte na charakterystyce i specyfice prowadzonej działalności organizacji, włączając w to lokalizację, aktywa, technologię. W przypadku jakichkolwiek wyłączeń, czy to w postaci komórek organizacyjnych, części, wydziałów, działów organizacji, czy wykonywanych procesów, taki stan rzeczy powinien być szczegółowo opisany i uzasadniony.

B. Zdefiniowanie polityki SZBI

Kolejnym krokiem jest zdefiniowanie polityki systemu zarządzania bezpieczeństwem informacji. Dokładnie określona polityka bezpieczeństwa informacji w firmie jest podstawą dla strategii bezpieczeństwa informacji. W każdej firmie powinien się znajdować oficjalny dokument polityka bezpieczeństwa informacji, zawierający jasną i precyzyjną definicję bezpieczeństwa informacji i związaną z nią politykę

ochrony. Najwyższe kierownictwo organizacji jest zobowiązane do jasnego i precyzyjnego prezentowania swojego poparcia dla założeń polityki oraz ich wdrożenia.

Dokument deklaracji polityki bezpieczeństwa informacji powinien być dostępny dla wszystkich osób bezpośrednio odpowiedzialnych za realizowanie koncepcji ochrony danych i systemu. Najwyższe kierownictwo powinno formalnie poinformować i zobowiązać wszystkich pracowników do respektowania założeń polityki. Norma ISO/IEC 27001 określa pięć elementów, które polityka powinna spełniać[497]:

- musi wyznaczać ogólny kierunek i definiować zasady działania w odniesieniu do bezpieczeństwa informacji, dodatkowo polityka powinna zawierać ramy dla ustalania celów niniejszej polityki,
- powinna brać pod uwagę cele biznesowe (m.in. wynikające z umów zobowiązania dotyczące bezpieczeństwa, wymagania klienta), wymagania prawne lub o charakterze regulacyjnym,
- powinna ustalić zakres i kontekst strategiczny zarządzania ryzykiem, co spowoduje tym samym, że zostanie ustanowiony konkretny obszar do ustanowienia SZBI,
- powinna określić kryteria, według których ryzyko będzie szacowane, analizowane i oceniane,
- polityka bezpieczeństwa musi być zaakceptowana przez najwyższe kierownictwo.

Polityka bezpieczeństwa informacji jest elementem planowania, a zatem niezbędne jest także opracowanie koncepcji stawiania celów w tym zakresie, w relacji z celami działania organizacji.

C. Określenie podejścia do szacowania ryzyka

Następnym działaniem prowadzącym do ustanowienia SZBI jest zdefiniowanie podejścia do szacowania ryzyka w organizacji. Norma nakazuje zastosowanie konkretnej metody szacowania ryzyka. Ma to przede wszystkim zagwarantować, że metodyczne podejście do szacowania ryzyka pozwoli na porównywanie wyników w czasie, jak również na powtarzalność rezultatów. Konieczne jest, aby dodatkowo opracować kryteria akceptacji ryzyka i określić akceptowalne poziomy ryzyka. Norma ISO/IEC 27001 nie określa, z jakiej metody skorzystać, choć przykładowo podaje w uwadze metody szacowania ryzyka omówione w ISO/IEC TR 13335-3 Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security. Do wyboru jest wiele metod szacowania ryzyka[498], które zostały opublikowane i są powszechnie wykorzystywane przez organizacje. Niektóre

[497] Por. A. Calder, *Implementing Information Security based on ISO 27001/ ISO 17799*, Van Haren Publishing, Amersfoort 2007, s. 41.

[498] J. Łuczak zwraca uwagę na metody ilościowe, jakościowe, mieszane i autorskie szacowania ryzyka, przywołuje m.in. metody OCTAVE, FMEA, CRAMM, COBRA, MARION, MEHARI, ISACA oraz metody z otwartych źródeł internetowych (por. J. Łuczak, *Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/ IEC 27001*, Zeszyty Naukowe Akademii Morskiej w Szczecinie 19 (91), Szczecin 2009, s. 63–70.

z nich zostały pozytywnie zweryfikowane przez jednostki certyfikujące, które w trakcie audytu certyfikacyjnego badają między innymi skuteczność szacowania ryzyka bezpieczeństwa informacji. Oczywiście możliwe jest stosowanie przez organizacje metod opracowanych na postawie własnych doświadczeń. Takie podejście jest właściwe dla dużych organizacji, które posiadają odpowiednie struktury organizacyjne do tego, aby taką metodę opracować i zwalidować. Niewątpliwą korzyścią tego podejścia jest świadomość metody, jak i całego procesu szacowania ryzyka u wszystkich uczestników biorących udział przy szacowaniu ryzyka bezpieczeństwa informacji. Oczywiście istnieje zagrożenie, że wypracowana metoda okaże się nieskuteczna, a organizacja nie dostanie rekomendacji przy audycie certyfikacyjnym, co tym samym może skutkować nieprzyznaniem certyfikatu. Dlatego też małe organizacje, ze względu na brak przede wszystkim zasobów personalnych, nie decydują się na opracowywanie własnych metod i częściej wybierają jedną z wielu już dostępnych, pozytywnie zaaprobowanych przez audytorów podczas audytów certyfikacyjnych.

D. Określenie ryzyka

Celem tego etapu jest zidentyfikowanie wszystkich aktywów znajdujących się w zakresie SZBI oraz wskazanie właścicieli tych aktywów.

Zaplanuj i zorganizuj proces
Stwórz system zawierający kategorie
Dokonaj inwentaryzacji aktywów
Zidentyfikuj zagrożenia
Określ podatność aktywów
Przypisz wartość lub współczynnik wpływu dla aktywów
Oszacuj prawdopodobieństwo dla podatności
Oblicz współczynnik ryzyka dla aktywów
Dokonaj wstępnego przeglądu środków kontroli
Skompletuj dokumentację

Rys. 46. Proces identyfikacji ryzyka

Źródło: M.E. Whitman, H.J. Mattord, *Management of Information Security*, op.cit., s. 261

W tym miejscu należy wyjaśnić dwa pojęcia, ponieważ norma bardzo szeroko traktuje powyższe terminy. Aktywa mogą być rozumiane w trzech znaczeniach:

- aktywa informacyjne: zbiory danych, pliki z danymi, dokumentacja systemu, instrukcje użytkownika, materiały szkoleniowe, procedury eksploatacyjne, plany ciągłości działania, *backupy*,
- aktywa oprogramowania: oprogramowanie aplikacyjne, oprogramowanie systemowe, programy narzędziowe i użytkowe,
- aktywa fizyczne: sprzęt komputerowy, sprzęt komunikacyjny, nośniki magnetyczne, inny sprzęt techniczny, meble, pomieszczenia.

Określenie „właściciel" natomiast oznacza osobę lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność za nadzorowanie, rozwój, utrzymanie, korzystanie i bezpieczeństwo aktywów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do aktywów[499].

Na tym etapie należy również zidentyfikować zagrożenia i podatności. Przy identyfikacji można się posłużyć różnymi kluczami i przewodnikami, które metodycznie nie pozwolą na pominięcie żadnego z obszarów działalności organizacji. Dodatkowo należy przeanalizować skutki utraty trzech cech bezpieczeństwa: poufności, integralności i dostępności w odniesieniu do aktywów.

E. Analiza i ocena ryzyka

Po identyfikacji ryzyka należy skoncentrować się na jego analizie i ocenie. Konieczne jest w tym miejscu oszacowanie potencjalnych szkód i strat biznesowych w organizacji, które mogą powstać z naruszenia bezpieczeństwa. Naruszenie bezpieczeństwa należy rozpatrywać jako utratę poufności, integralności i dostępności aktywów. Kolejnym krokiem jest oszacowanie realnego prawdopodobieństwa zdarzenia się incydentu bezpieczeństwa (naruszenia bezpieczeństwa) w świetle istotnych zagrożeń, podatności, konsekwencji związanych z tymi aktywami oraz aktualnie wdrożonymi zabezpieczeniami. Na podstawie wybranej metody szacowania ryzyka należy określić poziom ryzyka. O tym, czy dane ryzyko jest dla nas istotne, czy nie, decydować będzie kryterium akceptacji, czyli z góry ustalony poziom ryzyka. Ryzyko znajdujące się powyżej progu akceptowalności jest ryzykiem nieakceptowanym dla organizacji. Dla takiego ryzyka wymaga się zaplanowania i wykonania konkretnych działań.

F. Identyfikacja i ocena wariantów postępowania z ryzykiem

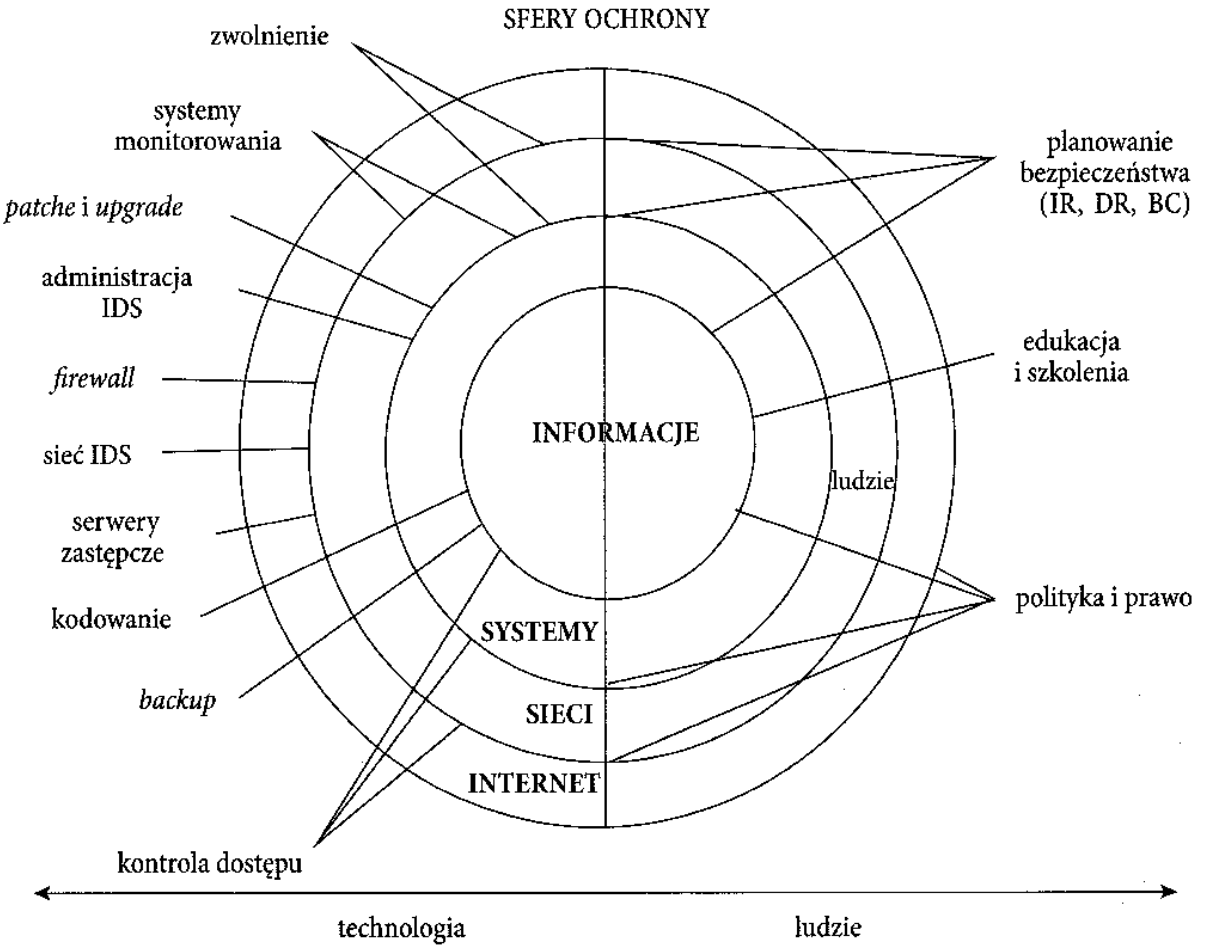
Dla ryzyka nieakceptowanego przez organizację (ryzyko, które przekracza próg akceptowalności) norma ISO/IEC 27001 zaleca podjęcie działań. Możliwe działania obejmują:

- zastosowanie odpowiednich zabezpieczeń,
- poznanie i zaakceptowanie ryzyka, w sposób świadomy i obiektywny, przy założeniu, że jasno spełnia warunki wyznaczone w polityce organizacji, oraz kryteria akceptowania ryzyka,
- unikanie ryzyka,

[499] PN ISO/IEC 27001, s. 11.

– przeniesienie ryzyka biznesowego na innych uczestników, na przykład ubezpieczycieli, dostawców[500].

M.E. Whitman oraz H.J. Mattord zwracają uwagę na definiowanie stref zabezpieczeń w odniesieniu do: ludzi, systemów, sieci i Internetu[501].



Rys. 47. Sfery bezpieczeństwa (zabezpieczeń)

Źródło: M.E. Whitman, H.J. Mattord, *Management of Information Security*, op.cit., s. 342

Uogólniając niniejszy podział, chodzi o klasyfikację w odniesieniu do: ludzi oraz technologii. Przytaczają jako konieczne zabezpieczenia, między innymi: planowanie, edukację i szkolenie, politykę, kontrole dostępu, backupy, kodowanie, serwery zastępcze.

G. Wybór celów stosowania zabezpieczeń i zabezpieczenia

System zarządzania bezpieczeństwem informacji opisany w standardzie zakłada z góry, że wszystkie postulaty i wymogi określone w jego treści zostaną całkowicie spełnione przez organizacje. W ten sposób jest możliwa porównywalność budowanych systemów bezpieczeństwa. W normie ISO/IEC 27001 w załączniku A zo-

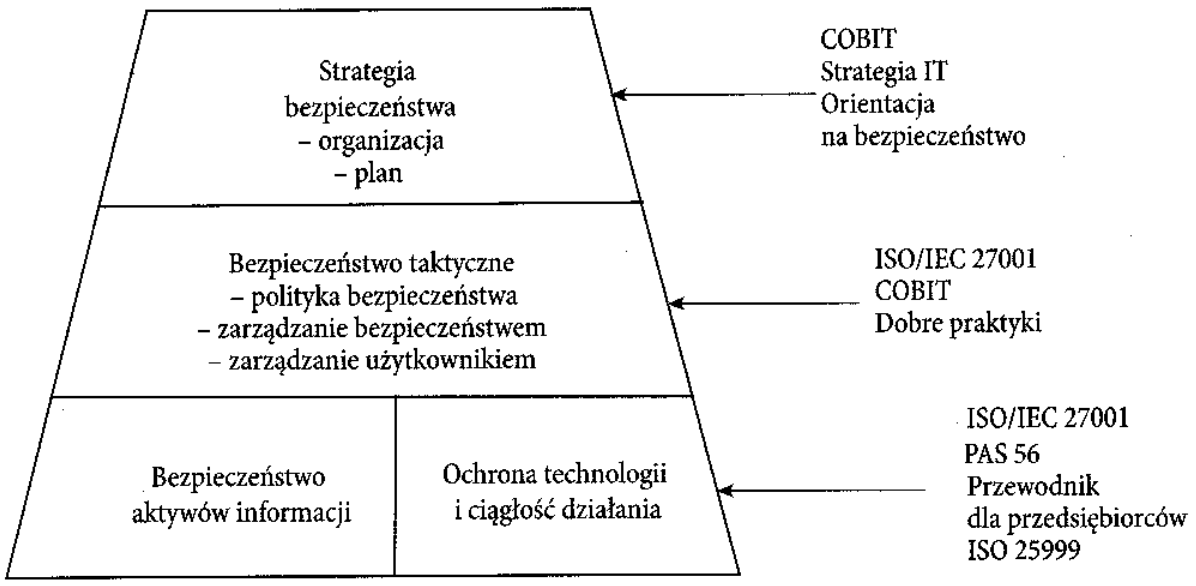
[500] PN ISO/IEC 27001, s. 12.

[501] M.E. Whitman, H.J. Mattord, *Management of Information Security*, op.cit., s. 342.

stało sformułowanych 39 celów zabezpieczeń i 133 zabezpieczeń uszeregowanych kolejno w 10 rozdziałach. Zabezpieczenie stanowi bezwzględne minimum, które organizacja musi uwzględnić. Oczywiście istnieje możliwość rozszerzenia systemu zarządzania bezpieczeństwem informacji i wprowadzenia dodatkowych zabezpieczeń niewymienionych w załączniku A, ale pod warunkiem, że do wszystkich 133 organizacja się odniosła. Lista celów i zabezpieczeń sformułowana w załączniku A nie jest wyczerpująca, jednakże zawiera obszerny opis zabezpieczeń znajdujących powszechne zastosowanie w organizacjach. Organizacje powinny więc traktować niniejszą listę jako punkt wyjścia do wyboru zabezpieczeń, aby upewnić się, że żadna istotna opcja zabezpieczeń nie zostanie przeoczona.

Cele stosowania zabezpieczeń i zabezpieczenia powinny być wybrane i wdrożone zgodnie z wynikami powstałymi w procesie szacowania ryzyka. Na decyzje o wyborze i stosowaniu zabezpieczeń powinny mieć wpływ również kryteria akceptacji ryzyka, wymagania prawne, wymagania nadzoru, a także zobowiązania wynikające z umów.

Konieczne jest ostatecznie zapewnienie skuteczności i efektywności rozwiązań, dlatego niezbędne jest korzystanie nie tylko z ISO/IEC 27001, ale także z przewodników i dobrych praktyk zabezpieczeń.



Rys. 48. Osiąganie bieżącej efektywności zabezpieczeń

Źródło: opracowanie własne na podstawie M. Osborne, *How to Cheat*, op.cit., s. 47

H. Przygotowanie deklaracji stosowania

Ostatnim ogniwem procesu szacowania ryzyka bezpieczeństwa informacji jest przygotowanie deklaracji stosowania (SoA – *statement of applicability*), określanej czasami w polskiej literaturze przedmiotu jako oświadczenie o stosowalności. Deklaracja stosowania jest dokumentem, który jest zbiorem wszystkich zabezpieczeń

stosowanych w organizacji. Przybiera on najczęściej strukturę załącznika A normy ISO/IEC 27001:2005. W dokumencie przywołuje się wszystkie 39 celów zabezpieczeń i 133 zabezpieczenia, do których organizacja określa stopień, rodzaj, formę i zakres stosowania wymienionych zabezpieczeń. Należy tutaj zwrócić uwagę na to, że cele stosowania i zabezpieczenia opisywane w deklaracji stosowania zostały już wcześniej wdrożone. Oczywiście jeżeli organizacja zdecyduje się na stosowanie innych, dodatkowych zabezpieczeń niewymienionych w załączniku A, to dokument deklaracja stosowania również będzie się odnosił do tychże zabezpieczeń.

Możliwe jest natomiast wykluczenie celu stosowania zabezpieczeń i zabezpieczenia wymienionego w załączniku A, przy czym taka informacja wraz z uzasadnieniem wykluczenia powinna być udokumentowana.

Deklaracja stosowania jest podsumowaniem dotyczącym postępowania z ryzykiem, a uzasadnienie jakichkolwiek wyłączeń umożliwia powtórne sprawdzenie, czy żadne zabezpieczenie nie zostało nieumyślnie pominięte.

Literatura

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłoszonych do zespołu CERT Polska w roku 2008, Raport, Cert Polska, 2008.

Calder, A., *Implementing Information Security based on ISO 27001/ ISO 17799*, Van Haren Publishing, Amersfoort 2007.

Gomółka, Z., *Cybernetyka w zarządzaniu*, Placet, 2000.

Krysowaty, J. Niedziejko, P., *Bezpieczeństwo IT jako usługa kształtująca wartość i jakość informacji*, w: J. Żuchowski (red.), *Innowacyjność w kształtowaniu jakości wyrobów i usług*, Wydawnictwo Instytutu Technologii Eksploatacyjnej, Radom 2006, s. 278.

Kumaniecki, K., *Słownik łacińsko-polski*, PWN, Warszawa 1996.

Łuczak, J., *Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpiczęństwem informacji ISO/ IEC 27001*, Zeszyty Naukowe Akademii Morskiej w Szczecinie 19 (91), Szczecin 2009.

Łuczak, J., Matuszak-Flejszman, A., *Metody i techniki zarządzania jakością. Kompendium wiedzy*, Quality Progress, 2007.

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

Molski, M., Łachota, M., *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

Osborne, M., *How to Cheat at Managing Information Security*, Syngress Publishing Inc., Rockland 2006.

Reich, L., Sawyer, D., *Archiving Referencing Model*, White Book, Issue 5, CCSDS 1999.

Stefanowicz, B., *Informacja*, Wydawnictwo SGH, 2004.

Stokłosa, J., Bilski, T., Pankowski, T., *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa–Poznań 2001.
The ISO Survey of certifications 2008, ISO, 2009, s. 15.
Whitman, M., *Enemy at the gates: threats to infomration security*, Comunications of the ACM, 48 (8), 2003.
Whitman, M.E., Mattord, H.J., *Management of Information Security, second edition*, Thomson Course Technology, Boston 2008.
Whitman, M.E., Mattord, H.J., *Readings and Cases in the Management of Information Security*, Thomson Course Technology, Boston 2006.
Wiener, N., *Cybernetyka społeczna*, KiW, 1961.
Zastawa, M., *Nowe trendy w bezpieczeństwie informacji*, Magazyn Klientów TUV Nord Polska, 2006, No. 3.

Normy

Information technology Security techniques – Security assessment of operational systems
ISO 9001 System zarządzania jakością.
ISO 14001 System zarządzania środowiskowego.
ISO/IEC 27001 Specyfikacja systemów zarządzania bezpieczeństwem.
ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, ISO 2005.
ISO/IEC 27002 (wcześniej 17799:2005) Information technology – Security techniques – Code of practice for information security management, ISO, 2005.
ISO/IEC TR 18044 Information technology – Security techniques – Information security incident management, ISO, 2004.
ISO/IEC TR 13335-3 Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security.
PN-I-13335-1 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych, PKN, 1999.
PN ISO/IEC TR 15947 Technika informatyczna – Techniki zabezpieczeń – Struktura wykrywania włamań w systemach teleinformatycznych, ISO/IEC TR 19791 (WD), PKN, Warszawa 2002.
PN ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN, Warszawa 2007.

Strony internetowe

http://kni.kul.lublin.pl/~andy/ref/other/risk.pdf.
http://www.polrisk.pl.
www.iso27000.pl (z dnia 12.09.2009) – rejestr certyfikatów ISO/IEC 27001 w Polsce.