Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 355 · 2018

Informatyka i Ekonometria 13

Elżbieta Andrukiewicz

Instytut Łączności – Państwowy Instytut Badawczy
e.andrukiewicz@itl.waw.pl

Marian Kowalewski

Instytut Łączności – Państwowy Instytut Badawczy
m.kowalewski@itl.waw.pl

PRAKTYCZNE PODEJŚCIE DO WDRAŻANIA SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTWACH

Streszczenie: Zaproponowano praktyczny sposób podejścia do wyboru strategii wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) na podstawie znanej metodyki SWOT. Dla celów analizy dokonano klasyfikacji czynników zewnętrznych (umożliwiających identyfikację szans i zagrożeń dla organizacji) oraz wewnętrznych (umożliwiających identyfikację silnych i słabych stron organizacji). Następnie zastosowano algorytm umożliwiający kwantyfikację czynników i uzyskanie wskaźnika dla wyboru najlepszej strategii dla danej organizacji. Dane zebrane na potrzeby analizy SWOT równolegle wykorzystano do przeprowadzenia wysokopoziomowej analizy ryzyka związanego z bezpieczeństwem informacji. Oszacowane poziomy ryzyka pozwalają określić priorytety działań w organizacji w obszarze zarządzania bezpieczeństwem informacji. W końcowej części artykułu przedstawiono zastosowanie proponowanego podejścia w wybranej organizacji.

Słowa kluczowe: zarządzanie bezpieczeństwem informacji, MŚP, analiza ryzyka.

JEL Classification: C19.

Wprowadzenie

Uwarunkowania prawne, kontraktowe lub rynkowe mogą wykreować potrzebę wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI) w organizacji. Należy wskazać, że SZBI jest przedsięwzięciem długoterminowym, które po zakończeniu projektowej fazy wdrożenia przechodzi w fazę utrzymania, z założonymi rezultatami oraz długookresowym wpływem na organizację i jej otoczenie. Sukces przedsięwzięcia, mierzony osiągnięciem celów

bezpieczeństwa informacji, jest wynikiem wykorzystania wielu czynników, zewnętrznych i wewnętrznych, wśród których można wymienić:
- potencjał i umiejętności ludzi,
- możliwość finansowania przedsięwzięcia w założonej skali i zakresie,
- dojrzałość procesów realizowanych w danej organizacji,
- rozumienie istoty ryzyka, w tym ryzyka związanego z bezpieczeństwem informacji i skuteczne nim zarządzanie.

Norma PN-EN ISO/IEC 27001 [2016] może stanowić podstawę do wdrażania mechanizmów skutecznego, przydatnego i adekwatnego do potrzeb bezpieczeństwa informacji przetwarzanych przez organizację. Norma zawiera jednak ponad 100 wymagań, które wszystkie należy spełnić, aby można było uznać, że System Zarządzania Bezpieczeństwem Informacji (SZBI) wdrożony w danej organizacji jest z nią zgodny. Trudność i wysokie koszty wdrożenia oraz utrzymania SZBI zgodnego ze wskazaną normą są istotnym czynnikiem ograniczającym powszechność jej stosowania, czego przejawem jest liczba organizacji, które uzyskały certyfikaty zgodności z normą sięgającą 33 000 na całym świecie [www 1]. Jednakże normę ISO/IEC 27001 można wykorzystać do wdrożeń bardziej ograniczonych w zakresie wymagań oraz skali lub terminu ich wdrażania, co w dłuższej perspektywie pozwoli organizacji osiągnąć swoje cele bezpieczeństwa informacji.

W artykule przedstawimy metodę wdrażania SZBI, możliwą do zastosowania przez organizację dysponującą ograniczonymi zasobami organizacyjnymi, technicznymi i finansowymi, charakterystycznymi zwłaszcza dla małych i średnich przedsiębiorstw (MŚP).

1. Tło i związane prace

Koszt bezpieczeństwa informacji był zawsze kwestią kontrowersyjną. Większość praktycznych metodyk wykorzystuje paradygmat możliwych zysków i strat w odniesieniu do kosztów ochrony aktywów informacyjnych organizacji. W innych szacuje się straty poniesione w wyniku ataku w odniesieniu do kosztów zabezpieczenia przed atakiem. Jednakże dokładność takich szacunków zależy od metody pomiaru ryzyka związanego z bezpieczeństwem informacji (możliwy zysk vs strata), co jest trudne i wysoce nieprecyzyjne z uwagi na dynamiczne zmiany w środowisku ryzyka [Gordon, Loeb, 2002, s. 438-457]. Z powyższego względu wielu autorów koncentruje się na ograniczeniu rozważań dotyczących kosztów inwestycji w bezpieczeństwo informacji, stosując typowe modele ekonomiczne. Szeroki przegląd różnych możliwych do zastosowania

metod znajduje się w pracy [Schatz, Bashroush, 2017]. Z przeglądu tego wynika, że w zastosowaniach dominują trzy metody: zwrotu z inwestycji w bezpieczeństwo (RO[S]I – Return on [Security] Investment), teorii możliwych wariantów (ROT – Real Options Theory) oraz maksymalizacji wykorzystania (UM – Utility Maximization).

Metoda RO(S)I wykazuje silną zależność między czynnikami kosztów i korzyści oraz od początku dominowała w praktycznych zastosowaniach. Stopniowo badania nad ROI zostały rozszerzone, po czym uwzględniały nowe ekonomiczne kwestie dotyczące zależności przychodów, oszczędności, efektywności kosztowej, zmiennej wartości ryzyka od nakładów inwestycyjnych, co skutkowało zastosowaniem metod dyskontowych, takich jak wartość bieżąca netto (NPV – Net Present Value) i wewnętrzny zwrot z inwestycji (IRR – Internal Rate of Return) [Purser, 2004, s. 542-546].

ROT jest metodą ilościową służącą do oceny elastyczności związanej z procesem podejmowania decyzji. W ostatnich pięciu latach takie podejście zyskało popularność z uwagi na zastosowanie w systemach wymiany informacji dotyczącej cyberbezpieczeństwa między organizacjami, przyczyniając się do rozwiązania takich zagadnień, jak przewidywane czas urzeczywistnienia się zagrożeń w oparciu o modele predykcyjne wykorzystujące dane historyczne [Gordon i in., 2015, s. 509-515].

UM odnosi się do koncepcji, w której podmiot próbuje wykazać największą możliwą wartość inwestycji. Analiza literatury wykazuje stale zmniejszające się zainteresowanie tymi metodami [Schatz, Bashroush, 2017]. Szersze podejście do ekonomii bezpieczeństwa informacji zostało zaproponowane w [Tsiakis, Stephanides, 2005, s 105-108]. Autorzy rekomendują określenie ścisłego związku między kosztami a bezpieczeństwem i zakładają dynamiczne, mocne włączenie bezpieczeństwa do wszystkich procesów biznesowych organizacji. Na tej podstawie można określić długoterminową efektywność oraz skuteczność w krótszej perspektywie, mierzone kluczowymi wskaźnikami (KPI – Key Performance Indicators), wprowadzonymi przez SZBI [Boehmer, 2009].

Należy wskazać, że wszystkie przedstawione metody muszą uwzględniać dodatkowe czynniki, jeśli próbować je stosować w realiach małych i średnich przedsiębiorstw, które stanowią istotną część globalnej gospodarki, zwłaszcza w Unii Europejskiej. Zgodnie z ostatnimi badaniami [European Commission, 2016] w całej gospodarce EU (z pominięciem sektora bankowego) MŚP stanowią 99,8% wszystkich przedsiębiorstw, wytwarzają 57,4% produktu narodowego brutto oraz zapewniają 66,8% zatrudnienia. W wypadku MŚP możliwości przeznaczenia części budżetu na bezpieczeństwo informacji są często ograni-

czone. W porównaniu do dużych organizacji MŚP nie mogą sobie pozwolić na wdrożenie wielu środków zabezpieczeń i długoterminowe oszacowania efektywności inwestycji. Zastosowania modeli ekonomicznych w MSE zostało przedstawione w [Mayadunne, Park, 2016, s. 519-530], gdzie analizowano skłonność MŚP do podejmowania inwestycji na podstawie stosunku do ryzyka związanego z bezpieczeństwem informacji.

Celem pracy jest poddanie dalszej analizie specyfiki organizacji typu MŚP pod względem zakresu wdrożenia systemu zarządzania bezpieczeństwem informacji, priorytetów działań oraz tempa, z jaką te organizacje mogą wdrażać SZBI, tak aby osiągnąć cele bezpieczeństwa informacji przy uwzględnieniu typowych dla MŚP ograniczeń.

Pozostała część artykułu jest zorganizowana następująco. W rozdziale drugim przedstawiono metodykę SWOT z punktu widzenia zastosowania do wypracowania strategii wdrażania SZBI. W rozdziale trzecim scharakteryzowano dane wejściowe do analizy SWOT, w rozdziale czwartym przedstawiono model obliczeniowy SWOT, a w rozdziale piątym – podejście do wysokopoziomowej analizy ryzyka przy wykorzystaniu danych wejściowych do analizy SWOT. W rozdziale szóstym omówiono praktyczne zastosowanie wypracowanego podejścia w wybranej organizacji.

2. Zastosowanie metody SWOT do wyboru strategii wdrażania SZBI

2.1. Wymagania normy

Wskazówki w zakresie wyboru strategii wdrażania SZBI można znaleźć w normie PN-ISO/IEC 27001 [2016], w rozdziale 4.1, w którym sformułowano wymagania dotyczące zrozumienia organizacji i jej kontekstu, tak: „aby określić czynniki zewnętrzne i wewnętrzne istotne dla celu jej działania i takie, które wpływają na zdolność organizacji do osiągnięcia zamierzonych wyników działania systemu zarządzania bezpieczeństwem informacji”.

Zidentyfikowanie tych czynników oraz zastosowanie metody analizy zebranych informacji pozwalają na określenie celów bezpieczeństwa informacji w danej organizacji oraz długofalowego planu działania zorientowanego na realizację tych celów, czyli strategii wdrażania SZBI.

2.2. Metodyka SWOT

Analiza wysokopoziomowa SWOT uwarunkowań zewnętrznych i wewnętrznych, przeprowadzona zgodnie z metodyką opisaną np. w [Obłój, 2007], jest odpowiednia do wyboru wdrażania SZBI. Do analizy należy przyjąć dane wejściowe, sklasyfikowane w poszczególnych kategoriach:
– czynniki zewnętrzne – szanse (O), zagrożenia (T),
– czynniki wewnętrzne – mocne strony (S), słabe strony (W).

Zebrane dane należy oszacować pod względem wpływu i znaczenia (wagi) oraz na podstawie uzyskanego wyniku można wyznaczyć optymalną strategię.

2.3. Zbieranie i analiza danych dotyczących uwarunkowań zewnętrznych i wewnętrznych

2.3.1. Uwarunkowania zewnętrzne

Analiza uwarunkowań zewnętrznych organizacji obejmuje:
– uwarunkowania prawne,
– specyfikę działalności,
– opis relacji ze światem zewnętrznym,
– kluczowe trendy.

W ramach **uwarunkowań prawnych** analizie należy poddać zarówno przepisy ogólne mające zastosowanie do każdej organizacji (np. ochrona danych osobowych czy przepisy o ochronie przed nieuczciwą konkurencją), jak i przepisy szczegółowe, mające zastosowanie do konkretnej organizacji, z uwagi na jej status lub charakter działalności, jaką prowadzi. Z uwarunkowań prawnych mogą wynikać przede wszystkim zagrożenia dla organizacji, wynikające z ryzyka związanego z naruszeniem obowiązujących przepisów prawa.

Specyfika działalności umożliwia zidentyfikowanie ryzyka z punktu widzenia bezpieczeństwa informacji, w tym także ryzyka niematerialne, np. wizerunkowe. Niektóre rodzaje działalności mogą mieć immanentne ryzyka, których inne są pozbawione. Specyfika działalności może wpływać zarówno na szanse, jak i na zagrożenia.

Opis relacji ze światem zewnętrznym dotyczy głownie wielkości struktury przychodów organizacji oraz zainteresowanych stron. Wielkość i struktura przychodów charakteryzują działalność biznesową organizacji oraz pozwalają zidentyfikować szanse oraz zagrożenia. Należy podkreślić, że struktura przy-

chodów determinuje priorytety organizacji dla działań zorientowanych na minimalizowanie ryzyka z punktu widzenia:
- strat finansowych (utrata przychodów, kary finansowe) na skutek braku możliwości świadczenia usług,
- utraty reputacji lub strat finansowych związanych z naruszeniem bezpieczeństwa informacji (utraty poufności informacji lub dostępności systemów teleinformatycznych)

dla zasadniczych kierunków działalności organizacji.

Do **stron zainteresowanych** zalicza się – w zależności od specyfiki działalności organizacji – klientów, partnerów biznesowych, konkurentów, regulatorów, sponsorów, administrację państwową, organizacje pozarządowe, samorządy branżowe i inne grupy zainteresowania. Strony zainteresowane mogą być dla organizacji źródłem możliwości, a także zagrożeń.

Kluczowe trendy warto analizować co najmniej w obszarze polityczno-prawnym, ekonomicznym, społeczno-kulturowym oraz technologicznym[1]. Nowe trendy powodują powstanie nowych ryzyk dla bezpieczeństwa, ponieważ ich źródła mogą być wirtualne, ale konsekwencje jak najbardziej rzeczywiste, takie jak chociażby utrata lub nieuprawnione wykorzystanie tożsamości osoby fizycznej czy strata finansowa na skutek działań przestępczych w cyberprzestrzeni. W ramach tej części analizy warto wykonać przegląd dających się przewidzieć regulacji prawnych, które będą obowiązywać w przyszłości. Wyniki analizy trendów pozwalają zidentyfikować zagrożenia (chociażby takie, jak sygnalizowane przez nowe ryzyka wynikające z rozwoju technologicznego), ale też mogą wskazywać na nowe możliwości stojące przed organizacją.

2.3.2. Uwarunkowania wewnętrzne

Analiza uwarunkowań wewnętrznych organizacji obejmuje:
- cele, strategie i misje,
- dojrzałość i kulturę,
- ład organizacyjny,
- wymagania bezpieczeństwa wynikające z potrzeb organizacji,
- potencjał organizacji.

Cele, strategie, misję – jako elementy działalności organizacji – służą identyfikacji możliwości integracji celów bezpieczeństwa informacji z długookreso-

[1] Omówienie metodyki analizy trendów (np. PEST) znajduje się poza zakresem tematycznym tego artykułu.

wymi kierunkami i celami wyznaczonymi w organizacji, co wpływać będzie bezpośrednio na szybkość i intensywność wdrażania strategii SZBI.

Dojrzałość i kultura organizacji decydują o możliwościach integracji procesów bezpieczeństwa z istniejącymi procesami biznesowymi, a także determinują zakres wdrożenia mechanizmów pomiaru i oceny skuteczności SZBI. Poziom dojrzałości organizacji, jak również tradycje i przyzwyczajenia wynikające z historii oraz specyfiki działalności organizacji, mogą stanowić czynnik ograniczający skuteczność wdrożenia.

Ład organizacyjny, którego elementy, takie jak regulacje wewnętrzne, struktura organizacyjna, podział ról i zakresy odpowiedzialności oraz ścieżki raportowania, wyznaczają możliwości organizacji w zakresie wdrażania mechanizmów bezpieczeństwa informacji w realizowanych procesach biznesowych. Analiza stanu wyjściowego może wskazywać na niedostatek istniejących mechanizmów i potrzeby istotnych zmian.

Na **wymagania bezpieczeństwa wynikające z potrzeb organizacji** wpływa specyfika prowadzonej działalności. Dla przykładu, analiza potrzeb w zakresie zachowania poufności może wskazywać na przeciwstawne kierunki mechanizmów, które trzeba wdrażać w jednej organizacji (przetwarzanie informacji publicznych, wymuszająca jawność i otwartość vs działalność na rynku konkurencyjnym, wymuszająca ochronę tajemnic przedsiębiorstwa).

Potencjał organizacji jest mierzony szeregiem parametrów, w których skład wchodzą:

1. Ludzie – należy poddać analizie strukturę wiekową, wykształcenie, doświadczenie w obszarze bezpieczeństwa informacji mierzone realizacją projektów lub doświadczeniem zawodowym. Ten parametr pozwoli zidentyfikować szybkość wdrażania mechanizmów bezpieczeństwa oraz sprofilować programy uświadamiania i szkolenia, identyfikując zakres i charakter słabości lub mocnych stron organizacji.
2. Teren, budynki i pomieszczenia – ten parametr pozwoli na ocenę możliwości zarówno zachowania, jak i rozszerzenia zakresu przetwarzania. W wyniku analizy można otrzymać charakterystyki zagrożeń oraz siły istniejących zabezpieczeń fizycznych lub technicznych.
3. Systemy teleinformatyczne – analiza infrastruktury teleinformatycznej, sposobów jej utrzymania, w tym zakresu i jakości usług outsourcingu, a także aplikacji i baz danych, w których wprowadza się mechanizmy bezpośredniego dostępu do przetwarzanych danych, pozwala na formułowanie wniosków dotyczących słabości tego przetwarzania oraz zidentyfikowanie ryzyk dla

bezpieczeństwa informacji (w szczególności związanych z poufnością lub integralnością informacji).

4. Sytuacja finansowa – analiza struktury kosztów daje podstawy do formułowania wniosków o elastyczności kosztowej mającej bezpośredni wpływ na tzw. apetyt organizacji na ryzyko (mierzony gotowością do zaakceptowania strat w wypadku zmaterializowania się danego ryzyka); analogicznie, analiza rentowności organizacji wskaże możliwości formułowania inwestycyjnych planów poprawy bezpieczeństwa. Te parametry mają zasadnicze znaczenie dla strategii wdrażania SZBI.

2.4. Model obliczeniowy SWOT

Zakłada się, że w toku analizy zidentyfikowano wszystkie czynniki zewnętrzne oraz wewnętrzne (*S*, *W*, *O*, *T*) dla oceny potencjału organizacji przy wdrożeniu SZBI oraz przypisano im wagi *G* sumujące się do wartości 1 we wszystkich kategoriach.

Słabości: $Wj\,, j \in \{1, \dots, x\}$ oraz $\sum_1^x G\_W_j = 1$

Mocne strony: $Sj\,, j \in \{1, \dots, y\}$ oraz $\sum_1^y G\_S_j = 1$

Szanse: $Oj\,, j \in \{1, \dots, v\}$ oraz $\sum_1^v G\_O_j = 1$

Zagrożenia: $Tj\,, j \in \{1, \dots, z\}$ oraz $\sum_1^z G\_T_j = 1$

W kolejnym kroku analizuje się powiązania SWOT, badając relacje zachodzące między silnymi i słabymi stronami a szansami i zagrożeniami za pomocą następujących pytań:

- Czy zidentyfikowane silne strony pozwolą wykorzystać szanse, które mogą wystąpić?
- Czy zidentyfikowane silne strony zawierają mechanizmy zmniejszające prawdopodobieństwo lub ograniczające skutki mogących wystąpić zagrożeń?
- Czy zidentyfikowane słabe strony ograniczą wykorzystanie mogących się pojawić szans?
- Czy zidentyfikowane słabe strony zwiększają prawdopodobieństwo wystąpienia zagrożenia?

Oszacowanie siły powiązań następuje przez zbudowanie zero-jedynkowej macierzy relacji między czterema kategoriami SWOT, a następnie zsumowanie wszystkich interakcji oraz iloczynów liczby i interakcji wag. Na przykład jedna

z czterech macierzy relacji między zbiorem szans (O) a zbiorem zidentyfikowanych słabościami (W) jest wyliczana w następujący sposób:

- $a_{i,j} = 1$, w wypadku zaistnienia relacji między daną szansą O_i a daną słabością W_j,
- $a_{i,j} = 0$, jeśli taka relacja nie występuje.

Liczba interakcji N jest sumą relacji $a_{i,j}$:

$$N = \sum_{i,j} a_{i,j} \tag{1}$$

Natomiast ważona liczba interakcji WN wyraża się następującym wzorem:

$$WN = \sum_{j}(\sum_{i} a_{i,j}) * G\_W_j + \sum_{i}(\sum_{j} a_{i,j}) * G\_O_i \tag{2}$$

Do interpretacji wyników wykorzystano macierz strategii normatywnych, na którą składają się:

- strategia agresywna – polegająca na maksymalnym wykorzystaniu efektu synergii występującej między silnymi stronami organizacji i szansami generowanymi przez otoczenie,
- strategia konserwatywna – polegająca na minimalizowaniu negatywnego wpływu otoczenia przez maksymalne i zarazem aktywne wykorzystanie potencjału tkwiącego w organizacji,
- strategia konkurencyjna – polegająca na eliminowaniu słabych stron funkcjonowania organizacji oraz budowaniu jej konkurencyjnej siły przez maksymalne wykorzystanie istniejących szans sprzyjających rozwojowi,
- strategia defensywna – polegająca na zapewnieniu przetrwania przez minimalizowanie wpływu zarówno występujących wewnątrz organizacji słabości, jak i zagrożeń ze strony otoczenia.

Strategię optymalną dla danej organizacji wyznacza najwyższa wartość N oraz WN.

3. Wysokopoziomowa analiza ryzyka związanego z bezpieczeństwem informacji

Dane zebrane podczas przygotowania do analizy SWOT mogą być podstawą do analizy ryzyka związanego z bezpieczeństwem informacji. O ile wybór strategii wdrażania SZBI wskazuje kierunek i intensywność działań w perspektywie długookresowej, to wysokopoziomowa analiza ryzyka pozwala na ustalenie priorytetów działań w ramach wybranej strategii. Wysokopoziomową analizę ryzyka warto przeprowadzić z wykorzystaniem modelu opisanego w normie

PN-ISO 31000 [PN-ISO/31000, 2010], odnoszącego się do scenariuszy zdarzeń przez zidentyfikowanie źródeł ryzyka w postaci słabych stron i zagrożeń.

Metodę szacowania ryzyka wykonuje się przez oszacowanie prawdopodobieństwa zmaterializowania się danego scenariusza zdarzenia oraz powagi konsekwencji, jakie może spowodować, i na tej podstawie wskazanie poziomu ryzyka w zdefiniowanej skali jakościowej, zgodnie z załącznikiem E normy PN-ISO/IEC 27005 [2013].

4. Praktyczne zastosowanie modelu SWOT oraz wysokopoziomowej analizy ryzyka

W wybranej organizacji należącej do kategorii MŚP przeprowadzono analizy zgodnie z metodyką opisaną w podrozdziale 3, tj. określono niezbędne czynniki analizy SWOT i nadano im wagi. Dane wynikowe zebrano w tabeli 1.

Tabela 1. Zestawienie danych wejściowych do analizy SWOT dla wybranej organizacji

Waga	Czynniki wewnętrzne		Waga	Czynniki zewnętrzne	
1,00	**Mocne strony**	**Id**	**1,00**	**Szanse**	**Id**
0,20	Doświadczone zespoły projektowe	[S1]	0,40	Duże potrzeby organów rządowych w obszarze organizacji cyberbezpieczeństwa	[O1]
0,20	Specjalny status organizacji realizującej zadania zlecane przez rząd	[S2]	0,15	Postrzeganie organizacji jako niezależnego ośrodka kompetencyjnego	[O2]
0,15	Nowoczesna infrastruktura informatyczna	[S3]	0,20	Dostępność różnorodnych funduszy finansowania projektów	[O3]
0,25	Strategiczne położenie (15 km od centrum stolicy, z łatwym dojazdem)	[S4]	0,10	Duży potrzeby standaryzacyjne (*best practices*) w obszarze cyberbezpieczeństwa	[O4]
0,20	Własne zespoły informatyczne	[S5]	0,15	Wieloletnie powiązania z innymi organizacjami o podobnym profilu działania	[O5]
1,00	**Słabe strony**	**Id**	**1,00**	**Zagrożenia**	**Id**
0,30	Zaawansowanie wiekowe pracowników	[W1]	0,20	Silna konkurencja ze strony innych organizacji o podobnym profilu działania	[T1]
0,30	Wyniki finansowe na niskim poziomie rentowności	[W2]	0,30	Szybki postęp technologiczny kreujący nowe zagrożenia w obszarze cyberbezpieczeństwa	[T2]
0,20	Niedostatek zabezpieczeń technicznych (w tym dla infrastruktury informatycznej)	[W3]	0,25	Duża liczba podmiotów współużytkujących siedzibę główną	[T3]
0,20	Niski poziom dojrzałości procesów, w tym związanych z bezpieczeństwem	[W4]	0,25	Niepewność co do przyszłych uregulowań prawnych dot. sektora modelowej organizacji	[T4]

Źródło: Opracowanie własne.

Dane wejściowe posłużyły do stworzenia macierzy interakcji. W tabeli 2 zamieszczono jedną z czterech macierzy dla wybranej organizacji.

Tabela 2. Macierz interakcji słabych stron i szans

Szanse / Słabe strony	[O1]	[O2]	[O3]	[O4]	[O5]	Waga	Liczba interakcji	Iloczyn wag i interakcji
[W1]	1	0	1	1	1	0,30	4	1,20
[W2]	0	1	1	1	0	0,30	3	0,90
[W3]	1	1	0	1	0	0,20	3	0,60
[W4]	1	1	1	0	1	0,20	4	0,80
Waga [*Wt*]	0,40	0,15	0,20	0,10	0,15			
Liczba interakcji	3	3	3	3	2			
Iloczyn wag i interakcji	1,20	0,45	0,60	0,30	0,30			
Suma interakcji							28	
Suma iloczynów								6,35

Źródło: Opracowanie własne.

Optymalną strategię dla wybranej organizacji określono na podstawie wyliczeń liczb interakcji *N* (wzór [1]) i ważonych liczb interakcji *WN* (wzór [2]), które zaprezentowano w tabeli 3.

Tabela 3. Wartości *N* i *WN* dla wybranej organizacji w odniesieniu do strategii normatywnych

	Szanse	Zagrożenia
Mocne strony	**Strategia agresywna**	**Strategia konserwatywna**
	Liczba interakcji	Liczba interakcji
	28	16
	Ważona liczba interakcji	Ważona liczba interakcji
	6,10	3,55
Słabe strony	**Strategia konkurencyjna**	**Strategia defensywna**
	Liczba interakcji	Liczba interakcji
	28	20
	Ważona liczba interakcji	Ważona liczba interakcji
	6,35	5,15

Źródło: Opracowanie własne.

Zgodnie z metodyką opisaną w rozdziale 5 zebrane dla wybranej organizacji dane wykorzystano do wysokopoziomowej, jakościowej analizy ryzyka. Dla tej organizacji określono scenariusze zdarzeń oraz zestawienie zagrożeń (T) i słabości (W), które z oszacowanym prawdopodobieństwem mogą spowodować wskazane następstwa, scharakteryzowane rodzajem i powagą strat. Na tej podstawie oszacowano ryzyka dla zdefiniowanych scenariuszy. Wyniki wysokopoziomowej analizy ryzyka związanego z bezpieczeństwem informacji dla wybranej organizacji przedstawiono w tabeli 4.

Tabela 4. Zidentyfikowane i oszacowane wysokopoziomowe ryzyka dla wybranej organizacji

	Scenariusz zdarzenia	Prawdopodobieństwo zdarzenia		Następstwa		Poziom ryzyka
		interakcja słabych stron (W) i zagrożeń (T)	oszacowana waga	charakterystyka	oszacowana waga	
1.	Przypadkowe ujawnienie informacji na masową skalę	W[4]-T[3]	wysokie	straty wizerunkowe	znaczne	krytyczne
2.	Cyberatak	W[4]-T[1] W[1]-T[2]	wysokie	straty wizerunkowe	znaczne	krytyczne
3.	Nielegalne lub nieupoważnione przetwarzanie danych osobowych	T[4]-W[4]	wysokie	konsekwencje prawne; straty wizerunkowe; ew. kary administracyjne (RODO)	znaczne	krytyczne
4.	Długotrwała niedostępność budynku głównego	W[3]-T[3]	niskie	straty materialne	znaczne	umiarkowane
5.	Długotrwała niedostępność zasilania elektroenergetycznego	W[3]-T[3]	niskie	straty materialne	znaczne	umiarkowane
6.	Przypadkowa utrata integralności bazy danych	W[3]-T[2] W[4]-T[2]	niskie	straty wizerunkowe; straty materialne	znaczne	umiarkowane

Źródło: Opracowanie własne.

Działania wynikające z konieczności zmniejszenia ryzyk zidentyfikowanych jako krytyczne mogą zniwelować część słabych stron. W konkretnej sytuacji wybranej organizacji określono możliwości działań w kategorii bezinwestycyjnych lub niskoinwestycyjnych, jak uzyskanie wyższej dojrzałości realizowanych procesów oraz uświadamianiu i szkoleniu pracowników. Intensywne działania organizacyjne zrealizowano w odniesieniu do ochrony danych osobowych. Działania o charakterze inwestycyjnym, kierowane na niwelowanie wpływu zagrożeń, zostały podjęte w powiązaniu z wykorzystywaniem szans w postaci nowych projektów. W ten sposób osiągnięto wyspowy rozwój systemu zarządzania bezpieczeństwem informacji, w którym zabezpieczenia o większej skuteczności i odporności na przełamanie, ale przez to kosztowniejsze, a także bardziej dojrzałe mechanizmy zarządzania bezpieczeństwem informacji, dotyczyły niektórych systemów teleinformatycznych.

Z przedstawionej analizy wynika ekonomicznie uzasadnione podejście do rozwoju bezpieczeństwa informacji – znane jako *baseline security*, przeznaczone dla całości wybranej organizacji, z dźwignią w postaci większej dojrzałości procesów, wyższej świadomości użytkowników, a w szczególności kadry kierowni-

czej średniego szczebla – oraz poziomu umiejętności administratorów systemów. W wybranych obszarach działalności tej organizacji (związanych z częścią prowadzonych projektów lub efektami tych projektów) są wprowadzane silniejsze mechanizmy zarządzania bezpieczeństwem, w tym system zgodny z normą PN-EN ISO/IEC 27001 [2016].

Podsumowanie

Wynikowa strategia bezpieczeństwa informacji oraz wysokopoziomowa analiza ryzyka określają, odpowiednio, kierunki działań oraz priorytety działań w obszarze bezpieczeństwa informacji. Do korzyści płynących z zastosowania analizy SWOT jako podstawy do wyboru strategii wdrażania systemów zarządzania bezpieczeństwem informacji można zaliczyć ekonomiczne uzasadnienie dla zmian wynikających z wymagań bezpieczeństwa informacji, możliwość dostosowania szybkości zmian do uwarunkowań organizacji, optymalizację działań o charakterze analitycznym (analiza SWOT i analiza ryzyka związanego z bezpieczeństwem informacji przeprowadzone z wykorzystaniem tych samych danych).

Literatura

Boehmer W. (2009), *Cost-benefit Trade-off Analysis of an ISMS Based on ISO 27001*, "Availability, Reliability and Security", 2009, ARES '09, International Conference on Fukuoka, Japan, March.

European Commission (2016), *Annual Report on European SMEs 2015/2016. SME Recovery Continues*, https://ec.europa.eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf (dostęp: 20.11.2017).

Gordon L.A., Loeb M.P. (2002), *The Economics of Information Security Investment*, "ACM Transactions of Information and System Security", Vol. 5(4), s. 438-457.

Gordon L.A., Loeb M.P., Lucyshyn W., Zhou L. (2015), *The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective*, "Journal of Accounting and Public Policy", Vol. 34(5), s. 509-519.

Mayadunne S., Park S. (2016), *Economic Valuation for Information Security Investment: A Systematic Literature Review*, "International Journal of Production Economics", Vol. 182, s. 519-530.

Obłój K. (2007), *Strategia organizacji*, Państwowe Wydawnictwa Ekonomiczne, Warszawa.

PN-ISO 31000 (2010), *Zarządzanie ryzykiem – Zasady i wytyczne*.

PN-ISO/IEC 27005 (2013), *Zarządzanie ryzykiem w bezpieczeństwie informacji*.

PN-EN ISO/IEC 27001 (2016), *Systemy zarządzania bezpieczeństwem informacji – Wymagania*.

Purser S.A. (2004), *Improving the ROI of the Security Management Process*, "Computers & Security", Vol. 23(7), s. 542-546.

Schatz D., Bashroush R. (2017), *Economic Valuation for Information Security Investment: A Systematic Literature Review*, "Information Systems Frontiers" October, Vol. 19, Iss. 5, s. 1205-1228.

Tsiakis T., Stephanides G. (2005), *The Economic Approach of Information Security*, "Computers & Security", Vol. 24(2), s. 105-108.

[www 1] https://www.iso.org/the-iso-survey.html (dostęp: 20.11.2017).

ECONOMY ASPECTS OF THE ISMS STRATEGY IMPLEMENTATIONS IN SMES

Summary: A practical approach to the Information Security Management System (ISMS) strategy implementation based on SWOT methodology is proposed in this paper. A classification of external factors (allowing identification of opportunities and threats), and internal ones (allowing identification of strengths and weaknesses) for an organization, is presented. Next, a quantifying algorithm for these factors allows to determine the choice of optimal strategy for a given organization. Simultaneously, high-level information security risk analysis approach based on gathered data is performed. Estimated risk levels allow to indicate priorities for the organization activities determined at the strategy level. An example of application of the method proposed is presented in the final part.

Keywords: information security management, SME, risk analysis.