Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/EPU.2018.131/1-33 | strony: 331–346

Jerzy Stanik, Maciej Kiedrowicz
Wojskowa Akademia Techniczna,
Wydział Cybernetyki
jerzy.stanik@wat.edu.pl, maciej.kiedrowicz@wat.edu.pl

Model systemu zarządzania bezpieczeństwem organizacji jako podstawa kształtowania polityki bezpieczeństwa informacjnego

Kody JEL: D81, D82, D83
Słowa kluczowe: bezpieczeństwo informacyjne, system zarządzania bezpieczeństwem, ryzyko, system zarzadzania ryzykiem
Streszczenie. Autorzy przedstawiają model systemu zarzadzania bezpieczeństwem organizacji (SZBO) na potrzeby kształtowania polityki bezpieczeństwa informacyjnego. Zaproponowany model ma charakter rozwiązania kompleksowego. Daje się łatwo zaimplementować i wdrożyć w dowolnej organizacji. Kluczowym jego elementem jest podsystem sterowania bieżącymi właściwościami zarówno samego SZBO, jak i systemów stanowiących jego bliższe otoczenie. Artykuł stanowi również próbę naszkicowania najistotniejszych zagrożeń w sferze bezpieczeństwa informacyjnego współczesnej organizacji.

Wprowadzenie

Na progu XXI wieku jesteśmy świadkami gwałtownego, niezwykle przyspieszonego rozwoju potencjału informacyjnego. Jedną z wybijających się na pierwszy plan cech rozwojowych współczesnej cywilizacji jest nieustanny wzrost roli informacji. Jest to wynik rewolucji informacyjnej, która wprowadziła świat w erę społeczeństwa informacyjnego, czyli społeczeństwa, w którym informacja stanowi kluczowy produkt, a wiedza niezbędne bogactwo. Istotną konsekwencją takiego stanu rzeczy jest systema-

tyczne podnoszenie rangi bezpieczeństwa informacyjnego[1] i bezpieczeństwa informacji[2] w organizacji. Dokonując konceptualizacji oraz konstruując i wcielając w życie politykę bezpieczeństwa informacyjnego (PBI) lub system zarzadzania bezpieczeństwem organizacji (SZBO) należy pamiętać, iż mimo zwiększającej się systematycznie dominacji systemów elektronicznych, nadal informacja jest gromadzona i użytkowana w tradycyjnych formach – nie można zatem pomijać ani lekceważyć tego faktu. Podkreślenia wymaga także to, że zapewnienie bezpieczeństwa informacyjnego stanowi jeden z kluczowych celów, który musi być obecny w strategiach każdej chcącej działać efektywnie organizacji. Skuteczność i rozwój są zależne od posiadania i stosowania zasobów informacyjnych o odpowiedniej wielkości i jakości.

Zarówno SZBO, jak i polityka bezpieczeństwa informacyjnego oraz wypływająca z niej polityka bezpieczeństwa informacji muszą być systematycznie aktualizowane w oparciu o:

- bieżące wyniki analizy kontekstu organizacji[3],
- wyniki analizy ryzyka lub wyniki audytów uwzględniających nie tylko funkcjonowanie organizacji czy systemu bezpieczeństwa informacyjnego danego pomiotu, ale także zmiany w ich otoczeniu (prawnym, organizacyjnym, technicznym, kulturowym itp. – patrz rys. 1.

Zagadnienie bezpieczeństwa organizacji, jak i bezpieczeństwa informacyjnego we współczesnym świecie ulega dynamicznym przeobrażeniom. Zarówno krajowi, jak i zagraniczni badacze tego obszaru dowodzą, że przez ostatnie 15 lat zmieniło się postrzeganie i podmiotu, i przedmiotu bezpieczeństwa informacyjnego.

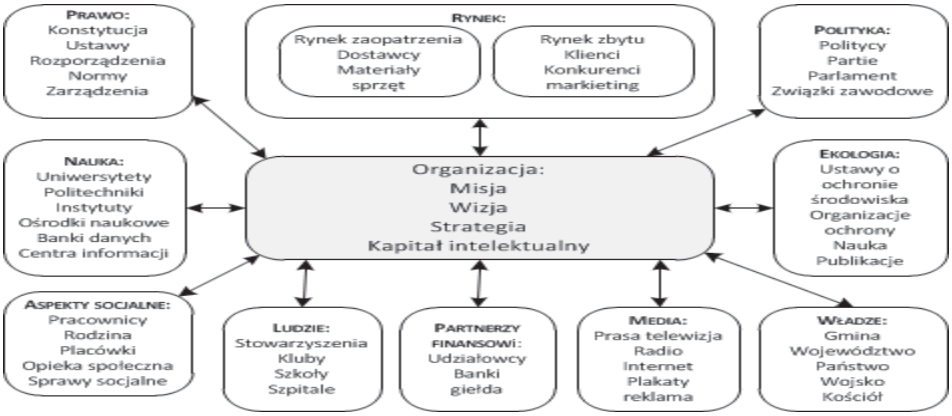
Analiza bezpieczeństwa informacyjnego jest szczególnie istotna z uwagi na dynamikę jego istoty i zakresu, wyznaczaną przez intensywny rozwój technologiczny, zwłaszcza w zakresie technik gromadzenia, przechowywania, przetwarzania i przesyłania informacji. W wymiarze informacyjnym bezpieczeństwo wiąże się z zabezpieczeniem interesów organizacji przed wszelkimi, tak zamierzonymi, jak i niezamierzonymi działaniami skierowanymi przeciw zasobom informacyjnym. Zapewnianie bezpieczeństwa informacyjnego rozumieć należy zatem jako działania mające na celu zabezpieczenie organizacji przed wszelkimi negatywnymi wpływami w sferze informacyjnej.

---

[1] Bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem.

[2] Bezpieczeństwo informacji to zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

[3] Pojęcie kontekstu organizacji znajduje się już w jednolitej strukturze, która od 2012 r. jest określona dla wszystkich systemów zarządzania w „High Level Structure" – Anneks SL.



Rysunek 1. Kontekst organizacji – przykładowe powiązania

Źródło: opracowanie własne.

W niniejszej pracy problem badawczy sprowadza się do odpowiedzi na pytanie: jakie zagrożenia bezpieczeństwa informacyjnego występują we współczesnej organizacji i jakie działania można zaproponować w systemach zarządzania organizacją, np. w SZBO, aby kadra zarządzająca mogła łatwo kształtować politykę bezpieczeństwa informacyjnego w rytm zmieniającego się kontekstu organizacji?

Ze względu na złożoność problemu głównego, pomocne staje się sformułowanie celów szczegółowych, prowadzących do odpowiedzi na pytania:

Jak rozumieć bezpieczeństwo informacyjne?

- Na czym polega specyfika zagrożeń bezpieczeństwa informacyjnego?
- Jaki powinien być model systemu zarzadzania bezpieczeństwem organizacji?
- Czy polityka bezpieczeństwa informacyjnego jest częścią SZBO czy samodzielnym dokumentem opracowywanym jedynie na potrzeby spełnienia wymogów prawa?

1. Bezpieczeństwo informacyjne i jego zagrożenia

Analiza literatury przedmiotu pozwala zauważyć, że nie istnieje jedna definicja bezpieczeństwa informacyjnego. W literaturze przedmiotu napotkać można wiele definicji bezpieczeństwa informacyjnego. Potocznie rozumiane jest ono jako ochrona informacji stanowiących tajemnicę państwową lub służbową. W przypadku bezpieczeństwa informacyjnego i związanych z nim zagrożeń mamy spore zamieszanie. Jego istotę ukazują funkcjonujące w literaturze przedmiotu definicje bezpieczeństwa informacyjnego, koncentrujące się wokół kwestii ochrony informacji niejawnych czy też bezpieczeństwa systemów teleinformatycznych. Przykładowo Potejko (2009) uważa, że: „bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmie-

rzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, przez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem". Istnienie takiego podejścia potwierdza Liedl (2008) pisząc: „Bezpieczeństwo informacyjne bardzo często rozumiane jest przez praktyków jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwianiem jej przetwarzania". Nieco szersze w stosunku do tych stanowisk ujęcie proponuje Korzeniowski (2012) według którego „przez bezpieczeństwo informacyjne podmiotu (człowieka lub organizacji), należy rozumieć możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą".

Spoglądając na powyższe przykłady, należy uznać za Fehlerem (2012), iż nie jest to poprawny, odpowiadający współczesnej roli informacji opis istoty bezpieczeństwa informacyjnego. W adekwatnym ujęciu bezpieczeństwo informacyjne należy widzieć jako „stan, w którym zapewniona jest swoboda dostępu i przepływu informacji połączona z racjonalnym i prawnym wyodrębnieniem takich ich kategorii, które podlegają ochronie ze względu na bezpieczeństwo podmiotów których dotyczą". Podejmując problem określenia istoty bezpieczeństwa informacyjnego warto mieć na uwadze fakt, że dopóki nie ma uniwersalnej, szeroko akceptowanej ogólnej definicji bezpieczeństwa – tak prawdopodobne jest, że problem ten będzie trwał, jeśli nie powstanie uniwersalne określenie bezpieczeństwa informacyjnego i pojęć z nim pokrewnych.

Spośród wielu definicji w teorii bezpieczeństwa informacyjnego następująca zmodyfikowana definicja z Korzeniowskiego (2012, s. 147) najbardziej odpowiada wymogom niniejszej pracy: „przez bezpieczeństwo informacyjne organizacji należy rozumieć możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą podstawowych atrybutów bezpieczeństwa". Jest to określenie bardziej uniwersalne, ujmujące wielowymiarowy i interdyscyplinarny charakter bezpieczeństwa informacyjnego.

Obserwując codzienną praktykę rzeczywistości gospodarczej, śledząc doniesienia medialne, stajemy się świadkami, a często uczestnikami, zdarzeń świadczących o tym, że zagrożenie bezpieczeństwa informacyjnego jest zagrożeniem realnym, a utrata informacji może naruszyć żywotne interesy organizacji.

Współcześni przedsiębiorcy, aktywnie działając na płaszczyźnie biznesowej w otoczeniu rynkowym opartym na nowoczesnych technikach przetwarzania informacji, widzą i identyfikują zagrożenia z tym związane umiejscawiając je w obszarach, które zobrazowano na rysunku 2.

Rysunek 2. Zagrożenia dla współczesnej organizacji

Źródło: opracowanie na podstawie https://www.pwc.pl/pl/publikacje_2011.pdf (12.01.2018).

W odpowiedzi na zagrożenia bezpieczeństwa informacyjnego organizacje podjęły wysiłki, aby wdrożyć i udoskonalić swoje środki zapewnienia bezpieczeństwa informacyjnego, opracowując:

- systemy zarzadzania bezpieczeństwem organizacji,
- strategie zarzadzania bezpieczeństwem organizacji,
- polityki bezpieczeństwa informacyjnego,
- systemy zarzadzanie bezpieczeństwem informacji,
- polityki bezpieczeństwa informacji,
- ogromne ilości zaleceń, norm, technologii powiązanych z bezpieczeństwem informacyjnym.

Wielorakość i niesymetryczność tych rozwiązań przyczyniła się do tego, iż organizacje zaczęły poszukiwać:

- innych modeli lub metodyk kształtowania polityki bezpieczeństwa informacyjnego lub
- jednorodnego systemu ochrony informacji.

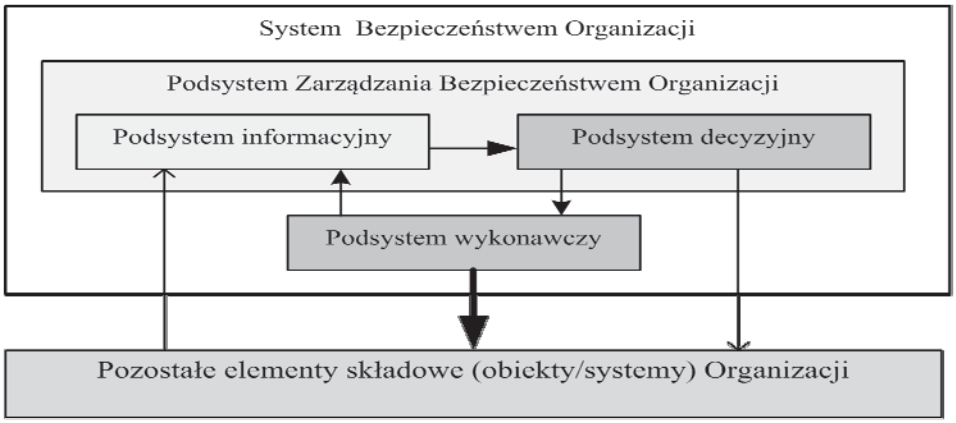
Zważywszy na to, że zagrożenia informacyjne mogą powstawać na gruncie różnie skonfigurowanych sytuacji, w których występuje: brak informacji, ograniczenie dostępu do informacji, nadmiar informacji, informacja zmanipulowana, informacja sfałszowana, informacja nieczytelna, informacja pozyskana nielegalnie, informacja zdezaktualizowana itp. można przyjąć, że zagrożenie informacyjne to (Stanik, Kiedrowicz, 2016) „sytuacja, w której mamy do czynienia z uświadomionymi lub nie, ograniczeniami lub nadużyciami w zakresie zgodnego z prawem dostępu oraz swobodnego posługiwania się aktualną, rzetelną, integralną i właściwie ochranianą pod kątem poufności informacją".

Podsumowując można stwierdzić, że do zapewnienia bezpieczeństwa informacyjnego na odpowiednim poziomie organizacja powinna możliwie najwięcej zadań z tym

związanych wykonywać we własnym zakresie, bazując na dobrych modelach SZBO i dobrych praktykach kształtowania polityki bezpieczeństwa informacyjnego, lub powierzyć te zadania zaufanym ekspertom z dziedziny bezpieczeństwa informacyjnego.

2. Model systemu bezpieczeństwem organizacji

Potocznie system bezpieczeństwa organizacji rozumiany jest jako zespół sił i środków oraz powiązań pomiędzy nimi, zapewniających pożądany poziom bezpieczeństwa organizacji (rys. 3).



Rysunek 3. Model systemu bezpieczeństwa organizacji

Źródło: opracowanie własne.

Podstawowym/kluczowym elementem systemu bezpieczeństwa organizacji jest system zarzadzania bezpieczeństwem organizacji (SZBO). Jako model systemu bezpieczeństwa organizacji (SBO) przyjmujemy uporządkowaną czwórkę:

$$SBO = \langle PZBO, PWY, OSBO, MET, DB \rangle,$$

gdzie:

- $PZBO$ – podsystem zarzadzania bezpieczeństwem organizacji zawierający podsystem informacyjno-decyzyjny, w skład którego wchodzi podsystem informacyjny i podsystem decyzyjny,
- PWY – podsystem wykonawczy rozumiany jako zbiór zespołów i relacji/powiązań pomiędzy nimi, zapewniających określone ich działanie,
- MET– Metodyka zarządzania bezpieczeństwa organizacji,
- $OSBO$ – otoczenie systemu bezpieczeństwa organizacji,
- DB – Dokumentacja bezpieczeństwa, w tym dokument Polityki Bezpieczeństwa Informacji.

Zarządzanie bezpieczeństwem organizacji musi uwzględniać bardzo różne aspekty bezpieczeństwa, nie tylko teleinformatycznego, ale również fizycznego, osobowego, organizacyjnego, prawnego, społecznego, psychologicznego, a nawet kulturowego (Stanik, Kiedrowicz, Hoffmann, 2017). Kompleksowo zagadnienie bezpieczeństwa informacji można przedstawić jako wielopoziomowy model odniesienia oparty o cele, strategie i polityki organizacji. Bezpieczeństwo w organizacji należy traktować jako proces ciągły, o charakterze organizacyjno-technicznym.

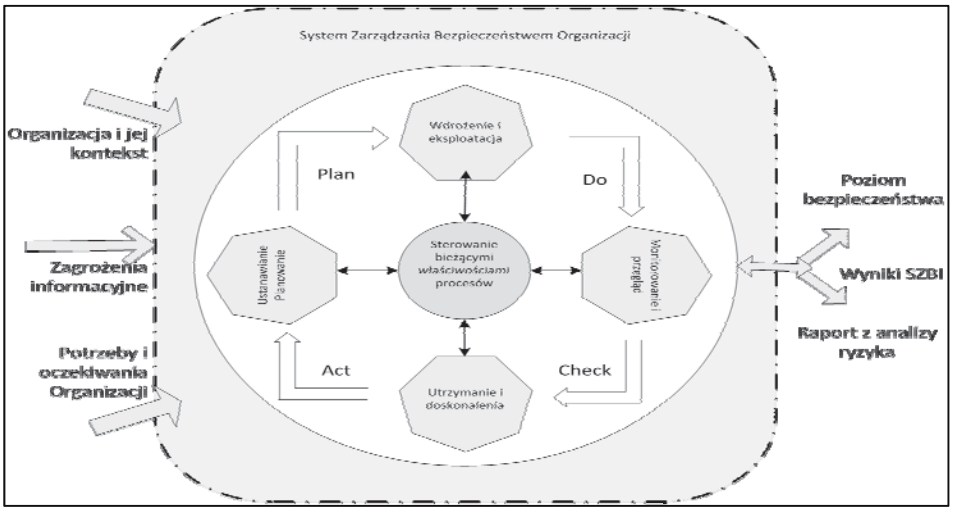
Zdaniem autora, polityka bezpieczeństwa organizacji powinna być konstruowana i realizowana w oparciu o pewien skonstruowany model (np. zestaw spójnych, precyzyjnych reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia aktywa organizacji lub procesy, systemy, podsystemy oraz powiązania między nimi, które zapewniają, aby informacja, którą posługuje się dany podmiot była bezpieczna w każdej fazie cyklu życia. Model systemu zarządzania zarzadzania bezpieczeństwem organizacji w ujęciu procesowym – model PDCA[4] zaprezentowano na rysunku 4. Na rysunku tym wyróżniono klasyczny cyklu PDCA oraz element dodatkowy, zarządzający interakcjami między procesami opartymi o cykl PDCA oraz sterujący bieżącymi właściwościami poszczególnych procesów. Korzyści z zastosowania takiego podejścia są dość łatwe do zidentyfikowania i wynikające wprost. To m.in. zwiększone prawdopodobieństwo osiągnięcia planowanego wyniku danego procesu (osiągnięcie celu procesu). A ponadto m.in.:

- wzrost wydajności procesów poprzez ukierunkowane działania doskonalące,
- zwiększenie przejrzystości działań w łańcuchu procesów,
- zwiększona wiedza na temat powiązań i relacji procesów,
- usprawnienie komunikacji pomiędzy procesami,
- identyfikacja możliwości optymalizacji,
- identyfikacja potencjału zakłóceń i ograniczeń (wąskie gardła) w przebiegu procesu,
- podstawa do inwestowania w doskonalenie.

3. Model systemu zarzadzania bezpieczeństwem organizacji na potrzeby kształtowania polityki bezpieczeństwa informacyjnego

Ponieważ okoliczności poszczególnych procesów i całego łańcucha procesu ulegają ciągłym zmianom (ze względu na zmienność kontekstu organizacji), ważne jest – w sensie ciągłego kształtowania bezpieczeństwa informacyjnego – aby weryfikować interakcje i związane z nimi procesy, podsystemy/systemy organizacji oraz plany ich działania.

[4] Cykl Deminga (model PDCA, cykl PDCA, koło Deminga, pętla Deminga, model PDSA, cykl PDSA) – schemat ilustrujący podstawową zasadę ciągłego ulepszania (ciągłego doskonalenia, Kaizen), stworzoną przez Williama Edwardsa Deminga.



Rysunek 4. Model systemu zarządzania zarzadzania w ujęciu procesowym

Źródło: opracowanie własne.

Zatem, mając powyższe na uwadze, jako model systemu zarzadzania bezpieczeństwem organizacji (SZBO) przyjęto uporządkowaną piątkę:

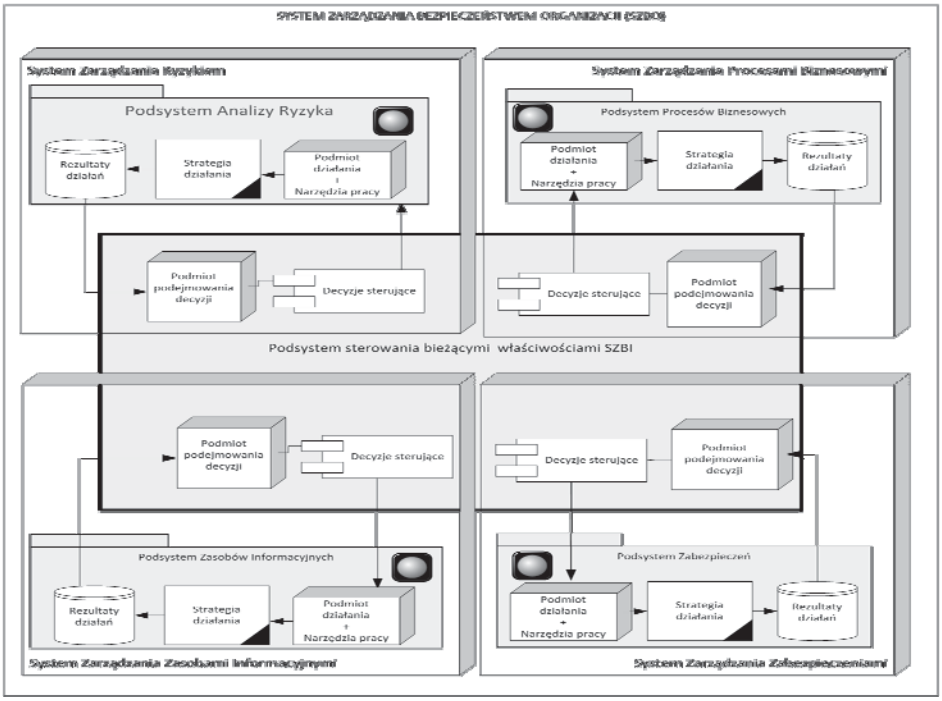
$$SZBO = \langle SZZI, SZAR, SZPB, SZZ, PSWPB \rangle$$

gdzie:

- *SZZI* – system zarządzania zasobami informacyjnymi,
- *SZAR* – system zarządzania ryzykiem,
- *SZPB* – system zarządzania procesami biznesowymi organizacji,
- *SZZ* – system zarządzania mechanizmami bezpieczeństwa – zabezpieczeniami,
- *PSWPB* – podsystem sterowania właściwościami użytkowymi wyżej wymienionych systemów, łączący je w zintegrowany system zarzadzania bezpieczeństwem informacji w organizacji.

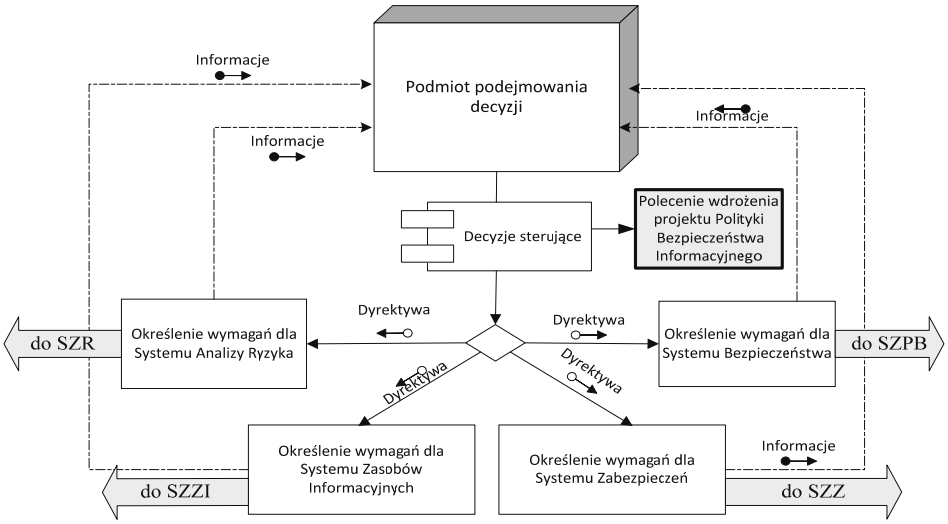
Schematyczną ilustrację SZBO z punktu widzenia kształtowania polityki bezpieczeństwa informacyjnego przedstawiono na rysunku 5.

Podstawowym elementem tego modelu jest podsystem sterowania właściwościami użytkowymi SZBI. Zakłada się, że celem działania podsystemu sterowania właściwościami użytkowymi poszczególnych podsystemów lub systemów tworzących SZBO jest utrzymywanie wymaganego poziomu bezpieczeństwa organizacji nakreślonego w dokumencie Polityki Bezpieczeństwa Organizacji. Cel ten można osiągnąć poprzez bieżące sterowanie konfiguracjami funkcjonalnymi systemów wchodzących w skład SZBO oraz jakością dokumentacji bezpieczeństwa, a w szczególności jakością polityki bezpieczeństwa informacyjnego. Graficzną ilustrację podsystemu sterowania właściwościami użytkowymi (PSWU) przedstawiono na rysunku 6.



Rysunek 5. Ilustracja modelu SZB z punktu widzenia kształtowania polityki bezpieczeństwa informacyjnego

Źródło: opracowanie własne.



Rysunek 6. Ilustracja podstawowych elementów podsystemu sterowania właściwościami użytkowymi SZBO

Źródło: opracowanie własne.

4. Modele podstawowych składników systemu zarzadzania bezpieczeństwem organizacji

4.1. Podsystem sterowania właściwościami użytkowymi SZBI

Jako model podsystemu sterowania właściwościami użytkowymi SZBI przyjmujemy uporządkowaną czwórkę:

$$PSWU =< SP, D >$$

Podstawowymi elementami PSWU są:

1. Podmiot decydowania, którym jest zbiór stanowisk (SP) uczestniczących w procesie wypracowania decyzji sterujących, np. stanowiska pracy tzw. Forum Bezpieczeństwa Organizacji.
2. Zbiór decyzji sterujących (D – dyrektyw), przy pomocy których osoby funkcyjne wyróżnionych stanowisk pracy mogą ustalać bieżące właściwości:
   – obiektów stanowiących części składowe SZBO (systemy: SZPB, SZZ, SZR, SZZI),
   – strategii lub projektu polityki bezpieczeństwa organizacji, w tym polityki bezpieczeństwa informacyjnego.

Zakładamy, że w ramach zbioru D istnieją również specjalne dyrektywy/decyzje sterujące o charakterze:

1. Ogólnej funkcji rekonfiguracji FR, którą opisać można za pomocą następującego odwzorowania (Stanik, 2013):

$$FR : 2^{SZBO} \rightarrow 2^{SZBO},$$

określonego następująco:

$$FR(SZBO^n) = SZBO^s, n, s \in \mathbb{N}, \mathrm{n} \neq \mathrm{s},$$

gdzie:
   – 2^{SZBO} – rodzina systemów zarzadzania bezpieczeństwem organizacji,
   – $SZBO^w$ – zbiór nieskutecznych systemów zarządzania bezpieczeństwem organizacji,
   – $SZBO^v$ – zbiór skutecznych systemów zarzadzania bezpieczeństwem organizacji.
2. Szczegółowej funkcji rekonfiguracji Q, którą opisać można za pomocą następującego odwzorowania:

$$Q : 2^{PBI} \rightarrow 2^{PBI},$$

określonego następująco:

$$FR(PBI_{t-1}^n) = PBI_t^{n+1}, n \in \mathbb{N}, t \in \mathrm{T},$$

gdzie:
– 2^{PBI} – rodzina dopuszczalnych polityk bezpieczeństwa informacyjnego $2^{PBI} = \{PBI_{dop}^n, n = \overline{1, \vec{N}}\}$
– (PBI_t^n) – n-ta wersja polityki bezpieczeństwa opracowana w chwili $t - 1 \in \mathrm{T}$ i obowiązująca do chwili $t \in \mathrm{T}$,
– PBI_{t+1}^{n+1} – kolejna (n + 1) wersja dokumentu polityki bezpieczeństwa (udoskonalona), obowiązująca od chwili $t \in \mathrm{T}$.

Podmiot decydowania podejmując decyzję, np. dotyczącą rekonfiguracji (FR) SZBO lub zmiany zapisów w strategii/dokumencie Polityki Bezpieczeństwa Informacyjnego, korzysta z podsystemu informacyjnego systemu SZBO w zakresie następujących danych:

- informacji na temat bieżącego ryzyka (raportu z analizy i oceny ryzyka),
- informacji o aktualnie zastosowanych mechanizmach bezpieczeństwa (zabezpieczenia techniczne, logiczne, organizacyjne),
- informacji o charakterystykach procesów biznesowych,
- informacji o stanie zasobów informacyjnych SI,
- rekomendacji kierownika zespołu analizy zagrożeń i oceny ryzyka w zakresie strategii postępowania z ryzykiem.

4.2. System zasobów informacyjnych

Jako model systemu zarządzania zasobami informacyjnymi (SZZI) przyjmujemy uporządkowaną czwórkę:

$$SZZI = \langle ZIK, WZI, ZI, R, O, ABI, MET \rangle,$$

gdzie:

- *ZIK* – zespół do spraw inwentaryzacji i klasyfikacji zasobów informacyjnych,
- ZI – zbiór/katalog potencjalnych zasobów informacyjnych przetwarzanych w ramach SI, $ZI = \{z_i, i = 1, I\}$,
- WZI – zbiór właścicieli zasobów informacyjnych,
- $R = ZI \times ZI$ – zbiór relacji/powiązań pomiędzy zasobami informacyjnymi,
- O – zbiór dopuszczalnych operacji przetwarzania zasobów informacyjnych,
- *ABI* – zbiór nazw potencjalnych atrybutów bezpieczeństwa dla zasobów informacyjnych,
- MET – metodyka wyceny istotności zasobów informacyjnych.

4.3. System zarządzania procesami biznesowymi

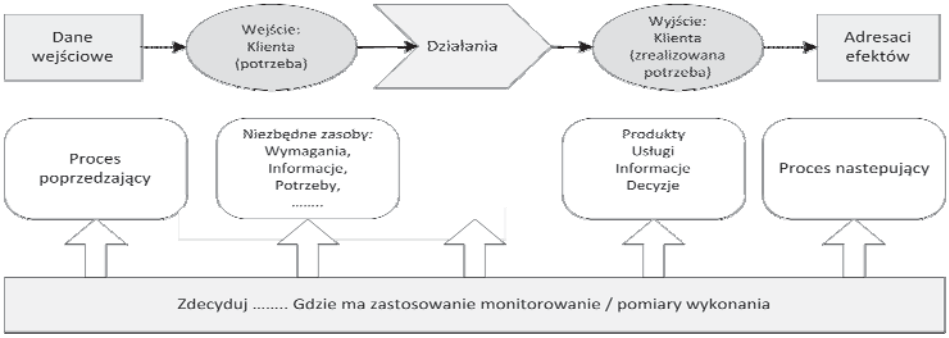
Jako model systemu zarzadzania procesami biznesowymi (SZPB) przyjmujemy uporządkowaną czwórkę:

$$SZPI = \langle ZWP, ZP, RP, KCHP, ABP, ZMPPB \rangle,$$

gdzie:

- ZWP – zbiór właścicieli procesów biznesowych,
- ZP – zbiór/katalog procesów biznesowych organizacji, $ZP = \{p_j, j = 1,J\}$,
- $RP = ZP \times ZP$ – zbiór relacji/interakcji pomiędzy procesami,
- $KCHP$ – zbiór istotnych charakterystyk procesów, np. w postaci tzw. kart charakterystyk procesu,

- $ZMPPB$ – modele pojedynczych procesów biznesowych (rys. 7),
- ABP – zbiór nazw potencjalnych atrybutów bezpieczeństwa dla zasobów informacyjnych.



Rysunek 7. Model pojedynczego procesu

Źródło: opracowanie na podstawie ISO 9001:2015.

4.3. System zarządzania ryzykiem

Jako model systemu zarzadzania ryzykiem (SZR) przyjmujemy uporządkowaną piątkę:

$$SZR = \langle ZAR, KR, MOR, ME, RAR \rangle,$$

gdzie:

- ZAR – zbiór rodzajów zespołów analizy ryzyka, $ZAR = \{zar_r, r = \overline{1,R}\}$,
- KR – zbiór dopuszczalnych konfiguracji zespołu zarządzania ryzykiem (wariant Zespołu Zarządzania Ryzykiem); pod pojęciem konfiguracji zespołu ryzyka rozumie się odpowiednio dobrany zbiór zespołów dziedzinowych lub pojedynczych zasobów osobowych o ściśle określonym doświadczeniu i kompetencjach z zakresu zarządzania ryzykiem w bezpieczeństwie informacji,
- MOR – model zarzadzania ryzykiem,
- RAR – wyniki z analizy ryzyka (Raport),
- ME – zbiór mechanizmów/środków zarządzania ryzykiem.

Mechanizmy zarządzania ryzykiem można zdefiniować jako zbiór sześciu niezbędnych elementów:

- strategie i polityki – generalne zasady zarządzania ryzykiem, odpowiednie dla danego obszaru,
- procesy operacyjne i procesy zarządzania ryzykiem – szczegółowe procedury zarządzania ryzykiem wbudowane w bieżące procesy operacyjne,
- ludzie – pracownicy operacyjni, realizujący procesy operacyjne, zaznajomieni z systemem zarządzania ryzykiem, tworzący szczegółowe procedury zarządzania ryzykiem,

- raporty zarządcze – raporty dla kierownictwa organizacji wskazujące na stopień „otwarcia" organizacji na ryzyko, trendy zmian wskaźników ryzyka, działania podejmowane w ramach realizacji strategii zarządzania ryzykiem,
- metodologie – dostępne dla pracowników operacyjnych rozwiązania, wspomagające ich działalność w procesach operacyjnych i w procesie zarządzania ryzykiem (analizy, systemy oceny),
- systemy – rozwiązania informatyczne wspomagające pracę pracowników operacyjnych.

Opracowanie i wdrożenie mechanizmów kontroli ryzyka odbywa się w sposób ciągły. Poszczególne elementy powinny podlegać stałemu usprawnianiu.

4.4. System zarzadzania zabezpieczeniami

System zarzadzania zabezpieczeniami (SZZ) stanowi jedno z kluczowych ogniw systemów bezpieczeństwa organizacji. Właściwy dobór procesów ochronnych, odpowiednia konfiguracja zabezpieczeń oraz efektywne wykorzystanie mechanizmów bezpieczeństwa pozwalają na znaczną redukcję kosztów bezpieczeństwa informacji organizacji, zapewniając jednocześnie wysoki poziom jej ochrony. Wszelkie zabezpieczenia należy postrzegać jako kompleksowy, spójny i niesprzeczny system zabezpieczeń, ukierunkowany na obniżenie prawdopodobieństwa realizacji zagrożenia w wyniku wykorzystania podatności aktywów organizacji lub systemu informacyjnego organizacji.
Utrzymanie wysokiego/wymaganego poziomu bezpieczeństwa zasobów informacyjnych organizacji wymaga skutecznej ochrony przed zagrożeniami napływającymi zarówno z zewnątrz, jak i wewnątrz organizacji. Właściwa obrona/ochrona opiera się na opracowaniu skutecznego systemu zabezpieczeń. Skuteczny system zabezpieczeń powinien wyeliminować lub zredukować zagrożenia do poziomu akceptowalnego. Jako model systemu zarządzania zabezpieczeniami (SZZ) przyjmujemy uporządkowaną piątkę:

$$SZ = \langle STRZ, ZZPW, PRZ, KB, MB \rangle,$$

gdzie:

- $STRZ$ – strategia zabezpieczeń,
- $ZZPW$ – zbiór potencjalnych rodzajów zespołów projektowo-wdrożeniowych, $ZZ = \{zz_r, r = 1, R\}$,
- PRZ – program zabezpieczeń, czyli całokształt działań ochrony zasobów informacyjnych organizacji,
- KB – zbiór dopuszczalnych konfiguracji bezpieczeństwa; pod pojęciem konfiguracji bezpieczeństwa rozumie się odpowiednio zaprojektowany i zaimplementowany zbiór mechanizmów bezpieczeństwa [3] o ściśle określonych funkcjach bezpieczeństwa.

- MB – zbiór mechanizmów bezpieczeństwa, na podstawie których generowana jest bieżąca konfiguracja bezpieczeństwa.

Zbiór mechanizmów bezpieczeństwa (zabezpieczeń) można zdekomponować na następujące podzbiory, odzwierciedlające poszczególne kategorie:

$$MB = MB^{ZF} \cup MB^{ZS} \cup MB^{ZO} \cup MB^{RNP} \cup MB^{ZU},$$

gdzie:

- MB^{ZF}– zabezpieczenia fizyczne, których stosowanie ma na celu zabezpieczenie podstawowej infrastruktury organizacji oraz niedopuszczenie do fizycznego dostępu przez nieuprawnione podmioty, oraz zabezpieczenie przed skutkami pożarów, zalania czy awarii/ katastrofy budowlanej,
- MB^{ZS}– zabezpieczenia systemowe i programowe wiążą się zwykle z systemami logicznej kontroli dostępu (zastosowanie uwierzytelniania i weryfikacji autoryzacji), z zabezpieczeniami kryptograficznymi, monitorowaniem ruchu w sieciach, systemami antywirusowymi i ścianami ogniowymi, tworzeniem kopii zapasowych, zapewnieniem właściwej eksploatacji i konserwacji wykorzystywanych systemów informatycznych oraz elementów infrastruktury technicznej,
- MB^{ZO} – zabezpieczenia organizacyjne – polegające na przeprowadzeniu zmian organizacyjnych mających na celu zwiększenie poziomu bezpieczeństwa systemu (zaprojektowanie regulaminów i polityk bezpieczeństwa, opracowanie procedur bezpiecznej eksploatacji, procedur lub planów[5] postępowania awaryjnego, odpowiedzialność pracowników itp).
- MB^{RNP} – rozwiązania natury prawnej – zorientowane przede wszystkim na działania w kierunku zapewnienia legalności, czyli zgodności z prawem oraz działania z ogólnie obowiązującymi standardami,
- MB^{ZU} – zabezpieczenia użytkowników – identyfikacja, uwierzytelnianie, kontrola dostępu do zasobów informacyjnych.

Właściwe zaprojektowanie i wdrożenie profesjonalnego systemu zabezpieczeń wymaga: zrozumienia organizacji i jej kontekstu oraz przeprowadzenia indywidualnej analizy zagrożeń wynikających z charakteru prowadzonej działalności, topografii terenu, rozmiaru i kształtu infrastruktury oraz z opracowaniem odpowiednich założeń projektowych.

[5] Planów zapewnienia ciągłości działania (BCP), Planów reagowania na incydenty cybernetyczne (CIRP), Planów odtwarzania funkcji systemów po katastrofie (DRP), Planów zapewnienia ciągłości działania systemów IT (ISCP) itp.

Podsumowanie

Gwałtowny postęp cywilizacyjny, powstanie zbiorów olbrzymich zasobów informacji oraz rozwój środków komunikowania, jako zjawiska charakterystyczne dla czasów nam współczesnych, niosą szczególne zagrożenia dla bezpieczeństwa informacyjnego, a katalog tych zagrożeń jest katalogiem otwartym, gdyż wraz z rozwojem społeczeństwa informacyjnego pojawiają się nowe możliwości i wyzwania.

W publikacjach dotyczących bezpieczeństwa informacyjnego zwraca się głównie uwagę na aspekty techniczne i formalne. Tymczasem badania empiryczne wykazują, że w systemie bezpieczeństwa najsłabszym ogniwem jest człowiek, jego kultura bezpieczeństwa oraz niska jakość lub brak podsystemu sterowania właściwościami użytkowymi systemów wchodzących w skład SZBO. Dlatego też, w niniejszym artykule zagadnieniu sterowania bieżącymi właściwościami SZBO poświęcono najwięcej miejsca.

Zagrożenia bezpieczeństwa informacyjnego są zagrożeniami realnymi, obecnymi w codziennej rzeczywistości życia podmiotu, zatem rozpoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego i SZBO staje się nieodzowne do zapewnienia przewagi konkurencyjnej organizacji, płynności finansowej, rentowności czy pozostawania w zgodzie z literą prawa. Trzeba zaznaczyć również, iż każda polityka bezpieczeństwa informacyjnego zawiera w sobie dwa podstawowe aspekty: aspekt obiektywny, obejmujący istnienie realnych i potencjalnych zagrożeń i wyzwań, oraz aspekt subiektywny, związany ze sposobami ich percepcji oraz wyborem koncepcji przezwyciężania i oddalania.

Polityka bezpieczeństwa informacyjnego oraz wypływająca z niej polityka bezpieczeństwa informacji i właściwości SZBO muszą być systematycznie aktualizowane w oparciu m.in. o analizy ryzyka i audyty uwzględniające nie tylko funkcjonowanie systemu bezpieczeństwa lub systemu zarządzania informacją danego pomiotu, ale także zmiany w ich otoczeniu.

Znaczenie bezpieczeństwa informacyjnego będzie wzrastać wraz z rozwojem cywilizacji informacyjnej i cywilizacji wiedzy. Bez dbałości o bezpieczeństwo informacyjne i utrzymywanie systemu bezpieczeństwa organizacji trudno wyobrazić sobie zapewnianie wymaganego poziomu bezpieczeństwa w kluczowych obszarach funkcjonowania organizacji.

Literatura

Korzeniowski, L.F. (2012). *Podstawy nauk o bezpieczeństwie*. Warszawa.

Fehler, W. (2012). *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne.* Warszawa.

https://www.pwc.pl/pl/publikacje_2011.pdf (12.01.2018).

Liedl, K. (2008). *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*. Toruń.

Potejko, P. (2009). Bezpieczeństwo informacyjne. W: K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*. Warszawa.

Stanik, J. (2013). *Metoda utrzymywania wymaganego poziomu bezpieczeństwa w elektronicznych platformach integracyjnych*. 80th Anniversary of Breaking the Enigma Code – Return to the Roots.

Stanik, J., Kiedrowicz, M. (2017). Model ryzyka procesów biznesowych. *Ekonomiczne Problemy Usług*, *1* (126, t. 1), 325–338.

Stanik, J., Kiedrowicz, M., Hoffmann, R. (2017). Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych. *Ekonomiczne Problemy Usług*, *1* (126, t. 1), 339–354.

MODEL OF THE ORGANIZATION SAFETY MANAGEMENT SYSTEM AS A BASIS FOR SHAPING INFORMATION SECURITY POLICIES

Keywords: information security, security management system, risk, risk management system.

Summary. The authors present the model of the organization's safety management system (OSMS) for the purposes of shaping the information security policy. The proposed model is a comprehensive solution. It can be easily implemented and implemented in any organization. The key element of this model is the subsystem controlling the current properties of both the itself OSMS and the systems constituting its immediate environment. The article is also an attempt to outline the most important threats in the area of information security of the contemporary organization.

Translated by Jerzy Stanik and Maciej Kiedrowicz

Cytowanie

Stanik, J., Kiedrowicz, M. (2018). Model systemu zarządzania bezpieczeństwem organizacji jako podstawa kształtowania polityki bezpieczeństwa informacyjnego. *Ekonomiczne Problemy Usług*, *2* (131/1), 331–346. DOI: 10.18276/epu.2018.131/1-33.