WYBRANE PROBLEMY BADAŃ ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI JEDNOSTKI ORGANIZACYJNEJ O SPECJALNYM PRZEZNACZENIU (JWSP)

Sebastian Malinowski

Akademia Obrony Narodowej

Streszczenie. Intencją autora jest przedstawienie wybranych problemów zarządzania bezpieczeństwem informacji jednostki organizacyjnej o specjalnym przeznaczeniu oraz badań z tym związanych. Poznanie współczesnej rzeczywistości, a w niej ww. problemów i zagadnień, nabiera szczególnego znaczenia ze względów poznawczych i utylitarnych. Artykuł ukazuje wybrane aspekty zagadnienia i jest próbą udzielenia odpowiedzi przynajmniej w przypadku niektórych z nich. Przedstawione informacje i treści są wynikiem procesu poznania, własnych analiz i obserwacji autora przeprowadzonych na potrzeby studiów doktoranckich w Akademii Obrony Narodowej, w wyniku których opracowano rozprawę na temat *Zarządzanie bezpieczeństwem informacji jednostki wojskowej specjalnego przeznaczenia*.

We współczesnym świecie o informacji można mówić właściwie tak jak o każdym innym towarze czy produkcie. Stała się ona czwartym czynnikiem produkcji, nie mniej ważnym niż ludzie, kapitał i przemysł. Ma ona jednocześnie swoją, często trudną do określenia wartość, która w nowych i zmiennych uwarunkowaniach ekonomicznych implikuje, ale też przyczynia się do stosowania przez niektóre podmioty nieetycznych metod pozyskiwania pożądanych informacji. Jednocześnie działalność oraz funkcjonowanie organizacji nieodłącznie związane jest z ciągłym pozyskiwaniem, gromadzeniem, opracowywaniem, przechowywaniem oraz przesyłaniem coraz większej ilości informacji wewnątrz posiadanych systemów informacyjnych oraz na zewnątrz, poza organizację. To coraz bardziej uwidacznia i uświadamia uzależnienie od skomputeryzowanych systemów informacyjnych, które często są powodem problemów wielorakiej natury. Problemy te, zwłaszcza związane z informacją, musimy ciągle rozważać i starać się je zrozumieć, a następnie podjąć działania dążące do ich rozwiązania. Musimy także zacząć doceniać istotę przyjmowanych istniejących już zasad, standardów i procedur, metodyk oraz „dobrych praktyk" mających na celu ochronę informacji i dzielić posiadane zasoby w sposób pozwalający osiągnąć: założony poziom bezpieczeństwa, zmniejszenie ryzyka oraz ewentualnych strat w aktywach informacyjnych – bez uszczerbku i utrudnień dla realizacji podstawowych zadań i procesów w organizacji. Należy zwrócić uwagę, że przy nagromadzeniu różnorodności i wielości propozycji oraz „sposobów na bezpieczeństwo" nieuchronnie pojawia się moment, kiedy musimy poznać podstawowe problemy związane z bezpieczeństwem informacji, a następnie musimy zacząć bezpieczeństwem informacji zarządzać, organizować je oraz poddawać celowym i sprawnym procesom – stosowanym z pełną świadomością do osiągnięcia określonych zamierzonych celów.

Stąd wynika, że problematyka sprawnego i efektywnego, nadążającego za zmianami zarządzania bezpieczeństwem informacji jest bardzo ważna dla takich instytucji jak siły zbrojne[1] nie tylko dlatego, że zawiera systemy potencjalnie niebezpieczne, ale przede wszystkim dlatego, że w naturalny sposób są one w zainteresowaniu grup przestępczych, terrorystów i oczywiście wywiadów innych państw. Ewentualna utrata, ujawnienie lub zafałszowanie informacji może mieć ogromny wpływ na bezpieczeństwo narodowe oraz postrzeganie danego państwa jako pewnego i odpowiedzialnego partnera we współpracy międzynarodowej[2].

Rozwiązywanie aktualnie pojawiających się problemów związanych z bezpieczeństwem informacji ważne jest także między innymi z kilku zasadniczych powodów. Pierwszym takim powodem jest to, że istnieją poważne zobowiązana mające na celu zapewnienie bezpieczeństwa informacjom sojuszniczym[3] i międzynarodowym. Po drugie na bieżąco są realizowane przedsięwzięcia z zakresu bezpieczeństwa państwa, np. kierowanie przygotowaniami i obroną państwa. Po trzecie trwa proces przeobrażenia w strukturach organizacyjnych, wyposażeniu oraz dyslokacji jednostek resortu Obrony Narodowej. Wreszcie po czwarte można stwierdzić, że przewaga potencjału informacyjnego jest współcześnie istotnym czynnikiem decydującym o przewadze potencjału dowodzenia i rażenia w konfrontacji z przeciwnikiem.

Biorąc to pod uwagę, można stwierdzić, że zintegrowany, nowoczesny i sprawny system kierowania państwem i dowodzenia Siłami Zbrojnymi musi być wspomagany bezpiecznym, niezawodnym, zintegrowanym systemem informacyjnym odpornym na oddziaływania zewnętrzne i wewnętrzne. Niestety, wymaga to rozwiązania całego szeregu bardzo istotnych i trudnych koncepcyjnie oraz decyzyjnie problemów szczegółowych, zwłaszcza w kwestii bezpieczeństwa informacji i zarządzania nim.

Oczywiście „nowe systemy broni" zasadniczo zawsze zmieniają przebieg działań bojowych. Jednak w dalszym ciągu to żołnierze pozostają najważniejszym elementem

[1] Należy podkreślić, że rosnąca wartość informacji powoduje wzrost zagrożeń dla ich bezpieczeństwa, zatem ważnym problemem staje się ochrona (obrona) systemów informacyjnych oraz zawartych i przetwarzanych w nich informacji. Wraz z rozwojem systemów rozwija się technologia zabezpieczeń, jednak same zabezpieczenia już nie wystarczą – należy je optymalnie dobierać, odpowiednio stosować i wreszcie właściwie nimi zarządzać.

[2] Sprawa niedoceniana do momentu ujawnienia tzw. afery Wikileaks, która obrazuje skalę mogących się pojawić w tym zakresie utrudnień, komplikacji i kompromitacji na poziomie dyplomacji poszczególnych państw, w sprawach często pozornie błahych. „WikiLeaks (z ang. Leak – przeciek) – witryna internetowa […], umożliwiająca publikowanie w sposób anonimowy dokumentów (często tajnych) […] przez informatorów chcących zasygnalizować działania niezgodne z prawem (tzw. *whistleblowers*). Operatorzy tej witryny twierdzą, że niemożliwe jest wyśledzenie, skąd pochodzą wpisy, w związku z czym ich autorzy nie ponoszą ryzyka związanego z ujawnianiem takich informacji". http://pl.wikipedia.org/wiki/WikiLeaks [stan na dzień 2013-09-06].

[3] M.in. umowa między stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r. Dz.U. 2000.64.740 (Dz.U. z dnia 7 sierpnia 2000 r.), także inne umowy obowiązujące w relacjach międzysojuszniczych.

operacji przy radykalnej zmianie ich możliwości i bezpieczeństwa. Ponadto każdy dowódca obecnie musi umiejętnie łączyć siłę i możliwości oddziaływania z koniecznością unikania nadmiernych zniszczeń oraz jakichkolwiek strat osobowych wśród ludności cywilnej[4]. Te ograniczenia zmuszają dowódców do wprowadzania limitów i do pełniejszej identyfikacji z otrzymanym zadaniem oraz potrzeby izolowania wybranych obszarów zewnętrznych i wewnętrznych. Powoduje to, że walka będzie najczęściej złożona z serii małych, szeroko rozproszonych działań prowadzonych przez jednostki (grupy zadaniowe) specjalizowane – specjalne, które będą miały coraz większe zapotrzebowanie na duże ilości „dobrej" informacji, będą wytwarzały, gromadziły i przetwarzały informacje, którym będzie należało zapewnić odpowiedni poziom bezpieczeństwa.

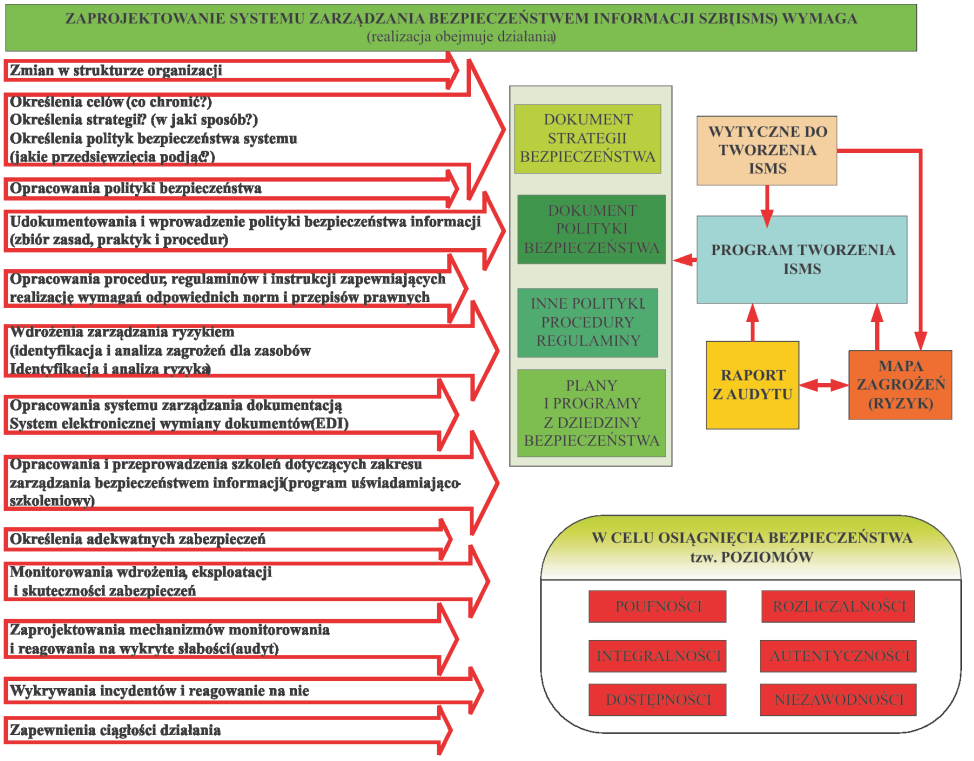
Należy jednocześnie podkreślić, że współcześnie oprócz zasobów kadrowych[5], wyszkolenia i sprzętu, uzbrojenia oraz wyposażenia technicznego najważniejszymi aktywami jednostek organizacyjnych o specjalnym przeznaczeniu są właśnie ich zasoby i powiązania informacyjne (wewnętrzne i zewnętrzne) nabierające szczególnego znaczenia przy działaniach wymagających precyzji, dokładności i idealnego czasowego umiejscowienia oraz natychmiastowej reakcji na zmiany w sytuacji taktyczno-operacyjnej. Zatem zapewnianie bezpieczeństwa informacji dla tego typu organizacji powinno stać się priorytetem. Tylko dzięki właściwej ochronie informacji (a w konsekwencji odpowiednim zarządzaniu bezpieczeństwem informacji), jej użytkownicy mogą być pewni, że zachowane są najważniejsze właściwości (atrybuty bezpieczeństwa informacji), stanowiące o ich przydatności dla jednostek specjalnego przeznaczenia, a więc poufność, autentyczność, dostępność, integralność (danych, systemu), rozliczalność, niezawodność itd. Jednak aby były one spełnione, konieczne staje się zastosowanie szeregu działań i mechanizmów z zakresu infrastruktury technicznej, organizacyjnej oraz personalnej[6]. Na rysunku 1 przedstawiono wybrane działania, których celem jest zaprojektowanie systemu zarządzania bezpieczeń-

[4] W tym kontekście szczególnie należy przywołać zdarzenia dotyczące np. oskarżonych polskich żołnierzy w sprawie Nangar Khel.

[5] Realizowanie procesu identyfikacji zagrożeń dla JWSP nie jest proste i dlatego w każdym przypadku należy zastosować metodyczne podejście do określenia kategorii chronionych zasobów. Chronione zasoby dzielimy na kategorie, którym następnie przyporządkowujemy zależne i odpowiednie od potrzeb priorytety: ludzie (funkcjonariusze, żołnierze służby stałej i kontraktowi, pracownicy cywilni, goście itp.); mienie (budynki, zabudowania, fortyfikacje, miejsca dyslokacji itd.); uzbrojenie, środki pola walki, maszyny i urządzenia, sprzęt informatyczny i łączności, pojazdy; informacje; procesy (kierowanie i dowodzenie, gotowość bojowa, uzupełnianie środków pola walki oraz inne krytyczne dla JWSP). **Szczególnie wnikliwie oraz z najwyższym priorytetem należy traktować ochronę ludzi. Tworzą oni organizację, jej „know-how", straty w przypadku narażenia życia oraz zdrowia personelu dla organizacji o specjalnym przeznaczeniu będą najbardziej dotkliwe i trudne do odtworzenia.**

[6] W opinii autora ogromnym błędem jest utożsamianie bezpieczeństwa informacji wyłącznie z bezpieczeństwem informatycznym oraz fizycznym, co w praktyce ma negatywny wpływ na całokształt zagadnień związanych z bezpieczeństwem informacji w organizacji dowolnego typu.

stwem informacji, dla porównania na kolejnych rysunkach przedstawiono obszary: kluczowych zagadnień bezpieczeństwa (rys. 2), zarządzania bezpieczeństwem informacji (rys. 3) oraz wariantu przebiegu procesu wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (rys. 4).



Rys. 1. Wymagania dla projektowania Systemu Zarządzania Bezpieczeństwem Informacji (wariant)
Źródło: opracowanie własne

Coraz powszechniejsze są informacje, że organizacje różnego typu ponoszą straty spowodowane utratą informacji lub brakiem ciągłości działania systemów informacyjnych. Niektóre z nich, chcące mieć świadomy wpływ oraz skutecznie przeciwdziałać temu zjawisku, wprowadzają najczęściej w organizacji *System Zarządzania Bezpieczeństwem Informacji (SZBI)* i starają się go w pełni zintegrować z innymi systemami[7]. Poprawne wdrożenie SZBI[8] gwarantuje, że bezpieczeństwo

[7] Szczególną uwagę należy zwrócić na wypracowany standard zarządzania bezpieczeństwem informacji w postaci ISO/IEC 27001. Głównym uzasadnieniem dla takiego wyboru jest to, że to właśnie wykorzystanie i wdrożenie tego standardu umożliwia przygotowanie oraz przeprowadzenie organizacji i jej systemu informacyjnego (wdrożonego SZBI) przez certyfikację.

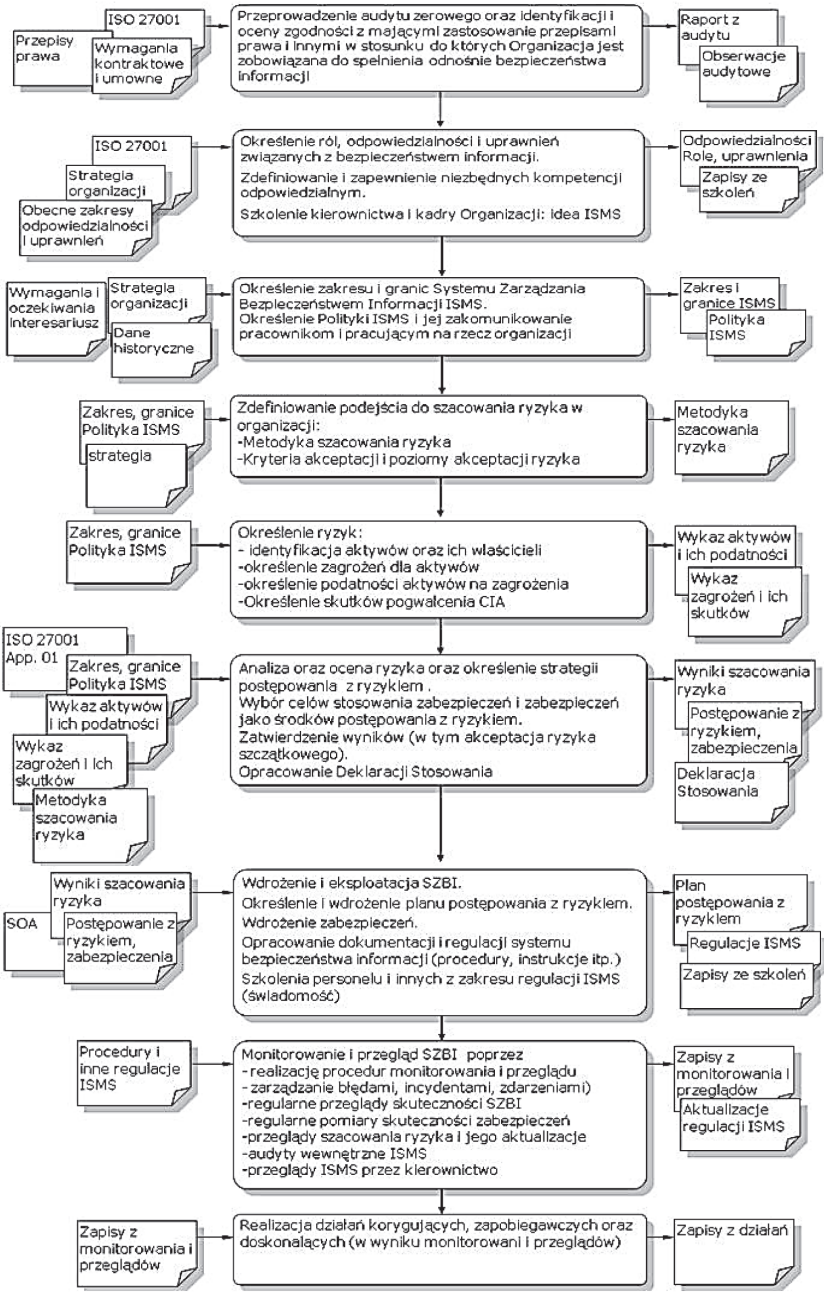
[8] Ideę przedstawia rys. nr 1.

w organizacji koncentruje się na bieżącej analizie ryzyk i z jej rezultatów wynika uzasadnienie wdrożenia odpowiednich zabezpieczeń i rozwiązań organizacyjnych[9].

Rys. 2. Obszar kluczowych zagadnień bezpieczeństwa
Źródło: opracowanie własne

Rys. 3. Praktyczne zasady zarządzania bezpieczeństwem informacji – obszary zarządzania
Źródło: opracowanie własne na podstawie PN-ISO/IEC 17799:2007

[9] Wdrożenie SZBI obejmuje sobą szeroki zakres działań i mechanizmów, między innymi takich jak: szkolenia wewnętrzne, budowanie świadomości bezpieczeństwa oraz wyrabianie właściwych nawyków i umiejętności, wdrażanie odpowiednich technologii informacyjno-informatycznych.



Rys. 4. Prezentacja graficzna dla wariantu przebiegu procesu wdrażania Systemu Zarządzania Bezpieczeństwem Informacji
Źródło: http://www.iso.org.pl/proces-wdrazania-iso-27001

W tym kontekście kluczowym elementem stanowiącym filar bezpieczeństwa informacji jest dobrze opracowana i wdrożona Polityka Bezpieczeństwa Informacji (PBI), odpowiednia dla danego typu organizacji, gdzie podstawowym mechanizmem służącym dla wdrożenia PBI jest stworzenie kompleksowego zestawu Procedur Bezpieczeństwa Informacji. Określa ona podejście instytucji do zarządzania bezpieczeństwem informacji i dzięki zaangażowaniu czynników decyzyjnych pozwala na jej wdrożenie w odniesieniu do wszystkich elementów organizacyjnych poprzez jasne określenie obowiązujących celów oraz zasad bezpieczeństwa informacji.

Należy jednocześnie pamiętać, że bezpieczeństwo informacji musi być kompleksowe i obejmować informacje we wszelkiej możliwej postaci, nie tylko informacje przechowywane w plikach na dysku, lecz także w dokumentach papierowych, przekazywanych podczas rozmów telefonicznych oraz spotkań służbowych i towarzyskich.

W celu efektywnego wprowadzenia ZBI w jednostce organizacyjnej specjalnego przeznaczenia należy odpowiedzieć na kilka zasadniczych pytań jej dotyczących, m.in.:

1) czym jest bezpieczeństwo informacji dla samej organizacji i jej kierownictwa?
2) dlaczego jest ono dla JWSP ważne i potrzebne?
3) jak określimy wymagania bezpieczeństwa informacji?
4) w jaki sposób podejdziemy do kwestii ryzyka w organizacji i jak je oszacujemy?
5) w jaki sposób dokonamy wyboru zabezpieczeń?
6) jak ocenimy efektywność i skuteczność przyjętych rozwiązań? Co będzie stanowić o krytycznych czynnikach sukcesu dla organizacji (KCS)?

Aby móc odpowiedzieć na tak postawione pytania, organizacja musi przeanalizować i określić jedenaście obszarów dotyczących bezpieczeństwa jej informacji. Rysunek nr 3 przedstawia prezentowaną ideę. Kolejność przedstawionych obszarów nie stanowi o ich ważności dla problematyki, której dotyczy. W opinii autora (pomimo istniejącej ewidentnej fakultatywności poszczególnych zagadnień dla dowolnej jednostki organizacyjnej) w przypadku stosowania **dla jednostek organizacyjnych o szczególnym stopniu wrażliwości pod względem ochrony informacji należy bezwzględnie i każdorazowo rozważać wszystkie zagadnienia, ocenić ich ważność i odnieść je do procesów w analizowanej organizacji**.

Prowadząc rozważania i badania nad bezpieczeństwem informacji, można przyjąć, że istniejący stan wiedzy i możliwości oraz ograniczenia w procesie poznania powodują, że jest to poznawczo bardzo trudny obszar[10], a w przypadku dotyczącym jednostek organizacyjnych o specjalnym przeznaczeniu dodatkowo „niedostępny instytucjonalnie" z przyczyn obiektywnych (głównie wynika to z samego charakteru

[10] Praktyczne działania najczęściej ograniczone są do bieżących potrzeb na zasadzie – zajmiemy się tym, jeśli ktoś będzie od nas tego wymagał (wiedza sprowadza się do zapoznania z poszczególnymi zapisami prawnymi i dostosowania się do nich tylko w niezbędnym zakresie).

organizacji). W opinii autora spowodowane jest to najprawdopodobniej między innymi:

1) interdyscyplinarnością i rozległością zagadnień dotyczących samego bezpieczeństwa informacji;
2) istniejącą różnorodnością stanowisk, poglądów, opinii oraz różnego rodzaju uogólnień prezentowanych w literaturze przedmiotu[11];
3) stanem wiedzy ogólnej i szczegółowej, który jest niezwykle obszerny[12], ale jednocześnie rozdrobniony i rozproszony (charakteryzujący się różnorodnością i wielością opracowań szczegółowych oraz wąskotematycznych) – zwłaszcza w aspekcie pojawiających się nowych zagrożeń;
4) stanem wiedzy ogólnej i szczegółowej dla analizowanego przedmiotu bezpieczeństwa informacji, który uwzględniałby specyfikę oraz działalność poszczególnych organizacji;
5) brakiem w literaturze pozycji dotyczących i przekładających się na zagadnienia związane z zarządzaniem bezpieczeństwem informacji w formacjach wojskowych – tym bardziej Sił Zbrojnych RP, które są odmiennym środowiskiem od gospodarczego (w gospodarczym chronimy pieniądze i zasoby, a w militarnym dodatkowo realne bezpieczeństwo narodowe);
6) warunkami, w jakich jest najczęściej podejmowana realizowana problematyka stanu bezpieczeństwa informacji, które są tak dynamiczne, że nie można przyjąć wszystkich zagadnień za rozwiązane.

Dodatkowo sytuację najprawdopodobniej komplikują w większości organizacji zagadnienia związane z m.in.:

1) ograniczonymi środkami finansowymi;
2) brakiem wystarczających zasobów osobowych własnej kadry (wykształconej i posiadającej potrzebne w tym zakresie: wiedzę, uprawnienia i kompetencję);
3) brakiem jasno określonego modelu przebiegu służby (pracy) osób odpowiedzialnych bezpośrednio za bezpieczeństwo informacji;
4) niepełnym wyobrażeniem o potrzebie wdrożenia i użytkowania systemu zarządzania bezpieczeństwem informacji[13];

[11] Jednym z podstawowych zagadnień (na jakie autor zwrócił uwagę w toku prowadzonych własnych badań) jest definiowanie – jest to problem funkcjonowania odmiennej terminologii (także problemy z terminologią w związku z przekładem np. na język polski) w poszczególnych dziedzinach dotyczących i powiązanych z bezpieczeństwem. Różni specjaliści w swoich opracowaniach używają odmiennych definicji dla wydawałoby się tych samych treści pojęciowych.

[12] Przede wszystkim dla sfery gospodarczej i prywatnej.

[13] W tym przypadku autor zauważa pozytywną zmianę, niestety wymuszoną nową ustawą z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228) oraz związane z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. Nr 0, poz. 526).

5) obawą przed poznaniem faktycznego stanu przygotowania organizacji do ochrony posiadanych przez nią informacji.
6) brakiem wypracowanych zoptymalizowanych rozwiązań systemowych dotyczących zarządzania bezpieczeństwem informacji w kwestii współczesnych zagrożeń.

Jednocześnie można założyć, że taki stan prawdopodobnie może być spowodowany w niektórych organizacjach następującymi przyczynami:

1) niepełną lub nieumiejętnie sprecyzowaną polityką bezpieczeństwa informacji (PBI);
2) w niektórych przypadkach niedopracowanymi lub niewystarczającymi przyjętymi rozwiązaniami[14];
3) ewolucją zagrożeń, także poprzez permanentną ewolucję technologii informatycznych, systemy same niosą pewne zagrożenia wynikające z ich awaryjności i przestarzałości;
4) błędnym rozpoznaniem zagrożeń, ryzyka oraz problemów przetwarzania informacji;
5) niewłaściwym rozpoznaniem rodzajów przetwarzanych w organizacji informacji;
6) stanem lub brakiem wiedzy na temat bezpieczeństwa informacji i współczesnych zagrożeń;
7) brakiem przygotowania do niwelowania i identyfikacji nowo powstających zagrożeń;
8) często nieaktualnością obowiązujących dotychczas ustaleń, przepisów, regulaminów oraz poglądów w zmieniających się warunkach;
9) istnieniem zjawisk, które trudno klasyfikować jednoznacznie jako zagrożenia;
10) powolnym tempem zmian ustawowych czy nowelizacją dotychczas obowiązujących, powstawaniem nowych dokumentów normatywnych (różnego rodzaju dyrektywy, wytyczne, regulaminy, instrukcje często nie nadążają za aktualnymi potrzebami)[15].

Wydaje się, że w polskich warunkach zainteresowanie problematyką bezpieczeństwa informacji najczęściej spowodowane jest wymuszeniem przez regulacje prawne[16] (i niestety nie dotyczy to tylko sektora prywatnego, administracji,

[14] Sprawa trudna i specyficzna ze względu na istniejące ograniczenia w zasobach finansowych i sposób ich podziału w organizacji, a nawet wewnątrz „pionu bezpieczeństwa" odpowiedzialnego za bezpieczeństwo.

[15] Patrz ustawa o ochronie informacji niejawnych (z 2010 r.), gdzie przepisy wykonawcze pojawiły się dopiero w drugiej połowie 2011 roku.

[16] Ustawy, np. o ochronie informacji niejawnych; o ochronie danych osobowych; o zwalczaniu nieuczciwej konkurencji; o dostępie do informacji publicznej; o prawie autorskim i prawach pokrewnych oraz rozporządzenia związane z ww. ustawami.

lecz także prawdopodobnie resortu Obrony Narodowej), w wyniku których są powoływani np.:

1) administratorzy systemów;
2) inni w zależności od bieżących potrzeb, np.: Główny Administrator Informacji (GAI), Główny Administrator Bezpieczeństwa Informacji (GABI), Administrator Grupy Informacji (AI), Administrator Bezpieczeństwa Grupy Informacji (ABI), Administrator Systemu (AS), Administrator Bezpieczeństwa Systemu (ABS) i inne.

W wyniku tak realizowanego podejścia można zauważyć następujące możliwe słabości:

1) powyższe funkcje niestety często są pełnione jako dodatkowe zadanie do niezwiązanych z tym obowiązków służbowych, najczęściej bardzo pracochłonne, często też bez dodatkowego wynagrodzenia;
2) mianowanie oraz ewentualne wyznaczanie (z tzw. „łapanki", jako wynik chwilowego braku obciążenia zadaniami) jest często przypadkowe bez uwzględniania rzeczywistych kwalifikacji danej osoby[17];
3) niejednoznaczność zapisów ustaw i rozporządzeń, często nieprecyzyjna nowa terminologia oraz brak jednoznacznego rozdziału zakresów kompetencji i odpowiedzialności za realizowane przedsięwzięcia;
4) brak określenia zasobu wiedzy, jaki jest potrzebny np. administratorowi bezpieczeństwa informacji, a jaki administratorowi systemu itd.

Można przedstawić następujące wnioski: po pierwsze zawsze niezbędne jest całościowe spojrzenie na systemy informacyjne w aspekcie zarządzania bezpieczeństwem informacji (nawet wtedy gdy analizujemy z pozoru identyczne jednostki organizacyjne) oraz możliwych korzyści uzyskanych z podejścia systemowego, a po drugie konieczne jest podejmowanie prób przedstawienia modelu systemu bezpieczeństwa informacji i zarządzania nią dla poszczególnych typów jednostek organizacyjnych, uwzględniając przede wszystkim obszary:

1) obowiązku dostosowania się do wymogów prawnych – mnogość przepisów obowiązujących w zakresie bezpieczeństwa informacji oraz konsekwencje wynikające z ich nieprzestrzegania (w wielu przypadkach może to być główny argument uzasadniający ponoszenie określonych nakładów finansowych – co może uczynić bezpieczeństwo informacji integralnym elementem prowadzonej działalności);
2) rosnącej globalnej współzależności informacyjnej – musimy mieć zaufanie do poziomu bezpieczeństwa zapewnianego przez podmiot, z którym mamy współpracować;

[17] To powinno uzmysłowić nam, że może występować u takich osób brak podstawowej wiedzy z zakresu metod formalnych (analiza ryzyka, audytowania itp.), informatyki oraz zarządzania – wiedza sprowadza się do zapoznania z poszczególnymi zapisami prawnymi lub odbycia krótkich kursów lub szkoleń.

3) wymogów współczesnego (oraz prognozowanego i przyszłego) pola walki wymuszających wprowadzanie nowych rozwiązań technicznych – które w nieodpowiedni sposób (lub w nieodpowiednim czasie) rozważone niosą ze sobą poważne zagrożenia;
4) zapewnienia spójności z celami organizacji oraz właściwej ich realizacji – poprzez właściwą realizację bezpieczeństwo informacji może stanowić istotny element szans stojących przed organizacją w zakresie realizacji ich strategicznych działań.

Biorąc pod uwagę powyżej przedstawione argumenty, autor wyraża przekonanie, że problemy związane z bezpieczeństwem informacji będą niestety w dalszym ciągu niewystarczająco rozważone i uporządkowane, zwłaszcza w kwestii współczesnych zagrożeń dla systemów informacyjnych i możliwości ich eliminacji[18]. Dlatego też rozwiązując problemy związane z bezpieczeństwem informacji w organizacji, wydaje się słuszne przyjęcie określonego sposobu postępowania na drodze do uzyskania odpowiedzi na nurtujące nas pytania w postaci: opisu sytuacji (jak jest), wyjaśnienia sytuacji (dlaczego tak jest), przewidywania „przyszłości" w interesującym nas zakresie (co należy zrobić, żeby uzyskać poprawę), jak sprawdzić, czy wypracowane rozwiązania są efektywne. A już bardziej szczegółowo można prowadzić rozważania np. w postaci określonych funkcji, jakie mają spełniać w stosunku do podejmowanych działań (oczywiście przytoczono poniżej wybrane przykłady):

– opis FAKTOGRAFICZNY (funkcja deskryptywna – opis sytuacji):
  1) jakie jest znaczenie informacji dla analizowanej organizacji i uświadomienie w tym zakresie?
  2) czym charakteryzują się zasoby informacyjne i systemy informacyjne danej organizacji?
  3) jakie są specyficzne wymagania (kryteria) i wynikające z nich przedsięwzięcia warunkujące zarządzanie bezpieczeństwem informacji?
  4) jakie jest aktualnie „rozpoznane" zagrożenia dla informacji i systemów im dedykowanych?
– opis DIAGNOSTYCZNY (funkcja eksplikacyjna – wyjaśnienie sytuacji):

[18] Należy zauważyć, że główną cechą systemu informacyjnego dowolnej z jednostek organizacyjnych o specjalnym przeznaczeniu (determinującym działalność i funkcjonowanie tego typu organizacji) związanych z wytwarzaniem, opracowywaniem, przechowywaniem i przesyłaniem oraz dystrybucją informacji przy użyciu najczęściej dedykowanych środków telekomunikacyjnych i informatycznych oraz biorącego w tym udział personelu **jest swoista odmienność i niepowtarzalność rozwiązań organizacyjnych każdej z nich**. Dlatego należy zawsze przeanalizować, opracować i przedstawić model systemu informacyjnego danej JWSP, który pozwoli na identyfikację głównych problemów w zakresie charakteryzującego je obiegu, zarządzania oraz wykorzystywania informacji, co umożliwia, w późniejszym etapie, określenie sposobów, możliwości, celowości oraz ekonomiczności doboru adekwatnych zabezpieczeń oraz prawidłowe zarządzanie bezpieczeństwem informacji.

1) jaki jest aktualny stan bezpieczeństwa informacji w danej jednostce organizacyjnej oraz jakie są w tym obszarze najistotniejsze zależności?
    1) Jaka jest struktura i funkcjonowanie istniejącego systemu?
    2) Jakie są przyczyny ukształtowania się określonego stanu systemu i czy jest on zadowalający?
    3) Jaki jest stan niedomagań i czy przyczyny tego stanu mogą być usunięte?
   – jakie czynniki (zagrożenia, źródła, przyczyny i skutki nieprawidłowości) wpływają na konieczność zastosowania ochrony informacji i w jakim zakresie?
   – jakie są metody i sposoby eliminacji nieprawidłowości występujących w systemie informacyjnym?
   – jakie przyjąć kryteria oceny efektywności zaproponowanych rozwiązań?
   – jakie zaproponować narzędzia modelowania (testowania) przeznaczone do oceny rozwiązań, mające na celu określenie, czy przyjęte warianty są efektywne?

– opis PROGNOSTYCZNY (przewidywanie sytuacji):
   – czy system informacyjny i w jakim stopniu wymagać będzie dalszego (ciągłego) udoskonalenia bądź modyfikacji?
   – jakie mogą pojawić się w przyszłości nowe problemy lub nabrać nowego znaczenia dotychczas nieuwzględniane?
   – jaka będzie prognoza problemu w bliższej i dalszej perspektywie czasowej?
– podejście PRAKTYCZNE:
   – w jaki sposób przejść od istniejącego do pożądanego stanu systemu bezpieczeństwa informacji organizacji, by można go było uznać za efektywny przy uwzględnieniu racjonalnych kosztów jego funkcjonowania;
   – co należy zmienić lub poprawić, aby informacja w systemie informacyjnym JWSP uznana była za bezpieczną?
   – jak wypracować właściwą koncepcję Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w danej organizacji?
– podejście INNOWACYJNE (stymulowanie sytuacji):
   – jakie przedsięwziąć działania, aby SZBI był ewolucyjny i nadążał za zmianami?
– podejście KONTROLNE (monitorowanie efektywności):
   – jak kontrolować istniejący stan systemu?
   – jak zaprojektować mechanizmy monitorowania i reagowania na wykryte słabości?

Wracając do analizy i opracowywania systemu zarządzania bezpieczeństwem informacji dla wydzielonych jednostek organizacyjnych, w tym także jednostki organizacyjnej specjalnego przeznaczenia (JWSP/JOSP) – zwłaszcza działających w określonych realiach i uwarunkowaniach, należy pamiętać, że nie jest możliwa bez aktywnego udziału innych osób (w realizowanym procesie badań – odpowiednimi do potrzeb metodami). Udział ten jest niezbędny przede wszystkim w fazie analizy, służącej zidentyfikowaniu najważniejszych potrzeb, barier, uwarunkowań,

priorytetów oraz występujących nieprawidłowości i możliwości ich eliminacji. Wyniki takiej analizy umożliwiają opracowanie modelu systemu zarządzania bezpieczeństwem informacji, identyfikację problemów oraz wskazanie zagadnień, zjawisk oraz perspektyw mogących się pojawić w najbliższej przyszłości.

Do osiągnięcia założonego przez badacza celu, jakim jest opracowanie modelu, najbardziej odpowiednią metodą badawczą jest analiza systemowa (warunki analizy systemowej problemu zarządzania bezpieczeństwem informacji przedstawia rys. 5), „która ma na celu określenie pożądanego działania lub linii postępowania przez rozpoznanie i rozważenie dostępnych wariantów oraz porównanie przewidywanych ich bliższych i dalszych następstw”[19].

W ramach takiej analizy można przeprowadzić m.in.: analizę diagnostyczną, prognostyczną, efektywności[20], krytyczną. Przedmiotem analizy diagnostycznej są: struktura i funkcjonowanie systemu istniejącego (jak jest?), przyczyny ukształtowania się określonego stanu systemu (dlaczego tak jest?), określenie, czy stan systemu jest zadowalający, sprecyzowanie stanu niedomagań i czy przyczyny tego stanu mogą być usunięte, sposoby przejścia od stanu istniejącego do pożądanego (jak zmienić?). Analizę prognostyczną możemy oprzeć na dwóch podejściach[21]:

- rozpoznawczym, które pozwoli określić przyszłość możliwych stanów, zdarzeń i sytuacji oraz oceny czasu i prawdopodobieństwa zaistnienia tych stanów;
- normatywnym, które umożliwi sformułowanie alternatywnych działań mających doprowadzić do osiągnięcia celu.

Następnie na podstawie przeprowadzonych analiz możemy przeprowadzić syntezę wniosków wynikających z aktualnego systemu bezpieczeństwa informacji i postarać się odnieść do doświadczeń z zakresu tej problematyki.

Przeprowadzone analiza systemowa i synteza pozwolą na zgromadzenie wiedzy o zasadach i możliwościach zarządzania bezpieczeństwem informacji w jednostkach organizacyjnych o specjalnym przeznaczeniu, a także polityce bezpieczeństwa informacji, ocenie ryzyka, analizie kosztów i zysków, zarządzaniu bezpieczeństwem informacji.

Jednocześnie należy pamiętać, że w ramach badań empirycznych, oprócz podstawowej metody analizy systemowej, niezbędne jest zastosowanie metod uzupełniających, tj. obserwacji uczestniczącej oraz sondażu diagnostycznego[22], w ramach których z powodzeniem zastosujemy technikę ankiety i wywiadu.

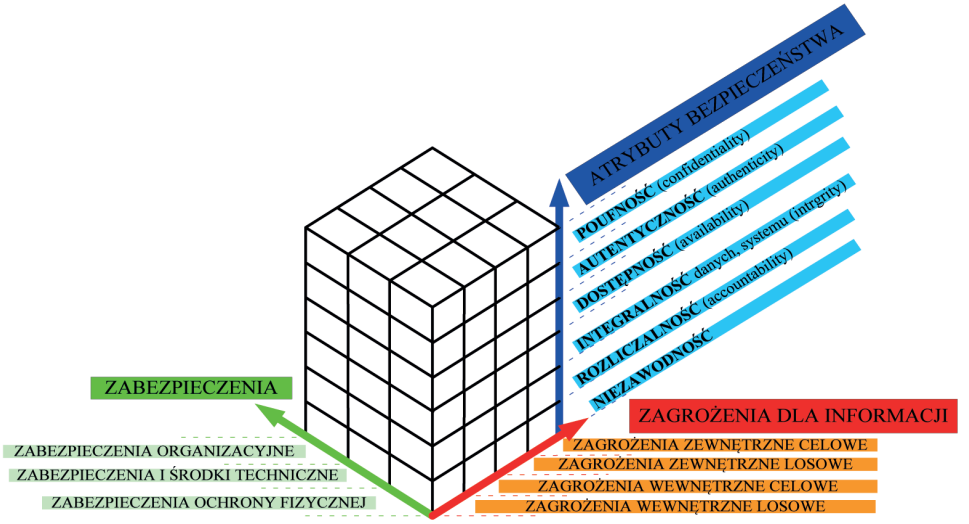
---

19 P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Wyd. Bellona, Warszawa 1994.

20 Analiza (ocena) efektywności systemów jest centralnym zagadnieniem analizy systemowej. Ważne etapy tej analizy to wybór kryteriów oceny systemu, wariantów jego organizacji, funkcjonowania i rozwoju, które przesądzają o trafności następnych wyborów.

21 Łącznie występuje ok. 72 obiektów cząstkowych analizy.

22 Na podstawie A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy BELLONA, Warszawa 2003.



Rys. 5. Warunki analizy systemowej problemu Zarządzania Bezpieczeństwem Informacji[23]
Źródło: opracowanie własne[24]

W opinii autora każde podejmowane próby[25] (bardziej lub mniej udane) wyjaśnienia wybranych złożonych problemów, a zwłaszcza tych dla jednostek organizacyjnych przeznaczonych do realizowania trudnych, specjalnych (specjalistycznych) zadań są na tyle ważne, że mogą w istotny sposób przyczynić się (poprzez analogię) do rozwiązywania przyszłych problemów mogących wystąpić w danym typie organizacji lub innych organizacjach i ich systemach, w których informacje wrażliwe mają kluczowe znaczenie dla istnienia danej organizacji oraz ogólnie rozumianego bezpieczeństwa.

[23] Pierwsze podejście ma udzielić odpowiedzi na pytania „Jak będzie" oraz „Jak może być". Zatem chodzi o przewidywanie przyszłości. Drugie podejście ma zastosowanie zwłaszcza przy zaistnieniu stanów niekorzystnych i niepożądanych z punktu widzenia założonego celu. Wówczas konieczne jest określenie alternatywnych działań.

[24] Jedną z technik zbierania materiału badawczego omówiono w publikacji – S. Malinowski, *CAWI jako metoda badawcza w naukach o obronności – wybrane zagadnienia*, „Studia Bezpieczeństwa Narodowego (National Security Studies)" Nr 3, Wojskowa Akademia Techniczna, Instytut Organizacji i Zarządzania WCY, Warszawa 2012.

[25] Także w postaci tylko badań wstępnych. Szczególną definicję **badań wstępnych** w postaci przedstawionej jako „Proces wykorzystywania prototypów w celu wsparcia rozwoju możliwości systemu. *Uwagi:* 1. Eksploracyjne badania wstępne stosuje się w celu wyjaśnienia i zrozumienia wymagań użytkownika oraz pożądanych właściwości systemu lub jego elementu. 2. Eksperymentalne badanie wstępne stosuje się w celu oceny wykonalności i ryzyka proponowanego projektu oraz do potwierdzania specyfikacji technicznych systemu lub jego elementu. 3. Ewolucyjne badanie wstępne stosuje się w celu dostosowania prototypu do eksploatacji użytkowej", można znaleźć w AAP-6(2010), s. 18.

Przeprowadzone badania[26] potwierdziły, że współcześnie wszystkie organizacje, zarówno gospodarcze, jak i pozostałe, dążą do osiągania dużej efektywności i bezpieczeństwa w dziedzinach swojego funkcjonowania. W związku z tym oczywisty wydaje się fakt szukania rozwiązań, które w sposób obiektywny określą np. poziom bezpieczeństwa informacji w organizacji. Bezsprzecznie takie cechy posiada potwierdzenie tego faktu przez niezależne podmioty w toku uzyskiwania przez daną organizację certyfikatów zgodności np. z wymaganiami normy (PN-) ISO/IEC 27001 oraz w późniejszym etapie uzyskania akredytacji.

Należy ciągle podkreślać role czynnika ludzkiego w bezpieczeństwie informacji, bowiem tylko odpowiedzialność, uświadomienie pracowników może podnieść poziom bezpieczeństwa informacji w organizacji. Nie należy przy tym jednak w żaden sposób rezygnować z egzekwowania bezpieczeństwa z wykorzystaniem dostępnych środków technicznych. Ponadto same narzędzia bezpieczeństwa mogą być (w związku z wielością i szybkością zachodzących zmian) nieakceptowane w pełni przez pracowników. Jeśli istnieje sytuacja, że pracownicy mogą nie wiedzieć, jakie są mechanizmy zabezpieczeń i jaki jest cel ich stosowania, to najprawdopodobniej odsuną bezpieczeństwo na dalszy plan, jako jeszcze jedno dodatkowe obciążenie niebędące dla nich istotne lub wręcz utrudniające podstawowe obowiązki lub zadania. To może powodować tendencje do nieświadomego lub świadomego obchodzenia zabezpieczeń w celu ułatwienia sobie pracy lub nawet innowacyjnego wykorzystania.

Musimy pamiętać, że nie ma prostych i całościowych rozwiązań dotyczących bezpieczeństwa informacji (zwłaszcza dla szczegółowych problemów specyficznych dla danej organizacji) oraz pełnej wyczerpującej jego oceny. Nie należy ulegać przeświadczeniu, że gdy zabezpieczymy się na akceptowalnym poziomie, to zapewni nam bezpieczeństwo do końca istnienia organizacji. Zapewnienie bezpieczeństwa informacji jest procesem ciągłym, w którym zawsze jest możliwość podniesienia skuteczności jej ochrony. Problemy związane z informacją w organizacji musimy każdorazowo zrozumieć i zarządzać nią tak samo jak innymi zasobami. Decydującą rolę ma kadra kierownicza, która poprzez zrozumienie przyjętych zasad, procedur i standardów w ochronie informacji we właściwy sposób przydziela zasoby, żeby można było to bezpieczeństwo osiągnąć. Musi ona także zrozumieć problemy dotyczące wartości aktywów informacyjnych, kosztów, jakie może ponieść organizacja w razie ich utraty lub ujawnienia.

Należy także pamiętać o wykorzystaniu norm i standardów zawierających wytyczne do zarządzania bezpieczeństwem informacji, dzięki którym nasze działania nie będą oderwane od rzeczywistości i unikniemy uczenia się przez organizację bezpieczeństwa na jej własnych błędach.

Nie można mówić o zarządzaniu bezpieczeństwem bez próby określenia, czym jest samo pojęcie bezpieczeństwa. Zarówno praktycy, jak i teoretycy problemu bezpieczeństwo

[26] S. Malinowski, *Zarządzanie bezpieczeństwem informacji...*, op. cit.

informacyjne określają jako wszelkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności. Drugie kluczowe pojęcie, które w tym miejscu należy przytoczyć, to polityka bezpieczeństwa instytucji w zakresie systemów informacyjnych. Obejmuje ona zasady, zarządzenia i procedury, które określają, jak zasoby – włącznie z informacjami wrażliwymi – są zarządzane, chronione i dystrybuowane w instytucji i jej systemach.

Musimy zawsze pamiętać, że jeśli zarządzanie bezpieczeństwem informacji (systemów informacyjnych) obejmuje zespół procesów zmierzających do osiągnięcia i utrzymywania ustalonego poziomu bezpieczeństwa, tzn. poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności, to jego realizacja musi obejmować co najmniej takie działania jak:

1) określenie celów (co należy chronić), strategii (w jaki sposób) i polityk bezpieczeństwa systemów informatycznych w instytucji (jakie konkretne przedsięwzięcia należy podjąć);
2) identyfikowanie i analizowanie zagrożeń dla zasobów;
3) identyfikowanie i analizowanie ryzyka;
4) określenie adekwatnych zabezpieczeń;
5) monitorowanie wdrożenia, eksploatacji (skuteczności) zabezpieczeń;
6) opracowanie i wdrożenie programu szkoleniowo-uświadamiającego;
7) wykrywanie incydentów i reakcja na nie.

Ponadto osoby odpowiedzialne za bezpieczeństwo muszą uzmysławiać pracownikom i szkolić ich, że kluczowym elementem, stanowiącym główny filar bezpieczeństwa informacyjnego JWSP, jest właściwie opracowana i wdrożona **Polityka Bezpieczeństwa Informacyjnego**[27] **(PBI)**, odpowiednia i dopracowana dla tego typu organizacji. Poprzez określenie przez nią podejścia instytucji do zarządzania bezpieczeństwem informacji i dzięki zaangażowaniu czynników decyzyjnych, pozwala na jej wdrożenie w odniesieniu do wszystkich żołnierzy i pracowników wojska przez jasne określenie obowiązujących celów oraz zasad bezpieczeństwa informacji. Podczas wdrażania SZBI nie należy zapominać, że obejmuje ono sobą szeroki zakres działań i mechanizmów, co najmniej takich jak:

1) szkolenia wewnętrzne;
2) budowanie świadomości bezpieczeństwa[28] oraz
3) wyrabianie odpowiednich nawyków;
3) wdrażanie odpowiednich technologii informacyjno-informatycznych;
4) oraz wiele innych (ideę przedstawia rysunek nr 1).

[27] Podstawowym mechanizmem służącym do wdrożenia Polityki Bezpieczeństwa Informacyjnego jest stworzenie kompleksowego zestawu Procedur Bezpieczeństwa Informacji. Prawidłowo stworzony zestaw procedur jest nieodzownym i podstawowym środkiem wdrażania Polityki Bezpieczeństwa Informacyjnego w JWSP.

[28] Konieczności edukowania w tym zakresie szczególnie kadry zarządzającej.

Gdy rodzą się wątpliwości co do wprowadzania w organizacji kolejnego systemu, należy pamiętać o głównych właściwościach Systemu Zarządzania Bezpieczeństwem Informacji:

1) SZBI może być wdrożony w organizacji dowolnej wielkości niezależnie od specjalizacji (branży), w jakiej działa;
2) podstawą systemu nie jest wdrożenie konkretnej listy zabezpieczeń, ale odpowiednie zarządzanie bezpieczeństwem. Szczególnie ważne jest posiadane SZBI przez wszystkie jednostki organizacyjne posiadające szereg ważnych i poufnych informacji;
3) jest on odpowiedzią na ciągle rosnące zagrożenia związane z utratą bądź niewłaściwym użyciem posiadanych informacji. Informacja stanowi bowiem wymierną wartość, dlatego należy ją odpowiednio chronić i dbać o jej bezpieczeństwo (chronimy swoje tajemnice, plany oraz inne zasoby istotnych dla nas informacji);
4) pomoc w skutecznej i kompleksowej ochronie zasobów informacyjnych przed rozmaitymi zagrożeniami, do których najczęściej należą:
    1) utrata, zagubienie, kradzież ważnych danych;
    2) „przecieki" poufnych informacji, np. do prasy, do konkurencji (przeciwnika) itp.;
    3) włamania do systemów informatycznych, szpiegostwo, wirusy komputerowe;
    4) zniszczenie fizyczne informacji oraz jej nośników (z powodu pożaru, zalania, sabotażu, wandalizmu);
    5) złamanie prawa z powodu niedozwolonego wykorzystania informacji;
    6) straty zdolności działania, finansowe, prestiżowe oraz utrata wiarygodności, wynikłe z niedbałości o bezpieczeństwo oraz rzetelność przetwarzanych i posiadanych informacji.

Z przeprowadzonych analiz i badań wynika, że podstawowymi korzyściami wynikającymi dla organizacji z wdrożenia SZBI są:

1) zmniejszenie ryzyka i problemów związanych z utratą lub „wyciekiem" informacji;
2) skuteczniejsza ochrona przed przechwyceniem ważnych tajemnic i informacji przez przeciwnika[29];
3) zmiana wizerunku organizacji na bezpieczną i wiarygodną;
4) spełnienie wymagań przepisów dotyczących bezpieczeństwa informacji;
5) podwyższenie świadomości i umiejętności w tym zakresie pracowników;

[29] Szczególne znaczenie będzie tu miało poznanie technicznych możliwości i ograniczeń potencjalnego przeciwnika oraz umożliwienie „obrońcy" postawienie się w sytuacji atakującego. J. McNamara, *Arkana szpiegostwa komputerowego*, Helion, Gliwice 2004, s. 18.

6) zwiększenie bezpieczeństwa informacji powierzonej przez partnerów (sojuszników) dla organizacji.

Badania wskazują, że na stan bezpieczeństwa informacji można skutecznie wpływać przez odpowiednią optymalizację systemu zarządzania bezpieczeństwem, co można osiągnąć przez[30]:

1) optymalizację metod osiągania bezpieczeństwa informacyjnego w całym procesie korzystania z informacji (niezależnie od sposobu jej wytwarzania, gromadzenia, przetwarzania i dystrybucji);
2) maksymalizację możliwości identyfikacji zagrożeń (niektóre z zagrożeń, jeśli nie są odkryte, mogą rozwijać się utajone w bardzo długim okresie) poprzez poznanie form, metod oraz sposobów i trendów zmian związanych z ewolucją zagrożeń – ze szczególnym zwróceniem uwagi na zagrożenia wewnętrzne;
3) pełną analizę współzależności czynników w wytypowanych aspektach bezpieczeństwa informacji (podmiotów bezpieczeństwa, ich charakterystyk oraz związków między nimi w kwestii zagrożeń);
4) zweryfikowanie aktualnych ustaleń w dziedzinie zarządzania bezpieczeństwem informacji oraz sprecyzowanie dalszych wskazań w rozwoju i optymalizacji systemów informacyjnych (określenie miejsc występowania sprzeczności między stanem faktycznym a docelowym w ochronie informacji);
5) zdefiniowanie wymagań w zakresie bezpieczeństwa informacji, które pozwoli uniknąć niejednoznaczności co do stwierdzenia faktu naruszenia bezpieczeństwa;
6) propagację i intensyfikację szkoleń specjalistycznych (na odpowiednim poziomie wiedzy) w dziedzinie bezpieczeństwa informacji;
7) rozważenie stworzenia nowej, dodatkowej oraz samodzielnej specjalności w dziedzinie bezpieczeństwa informacji w strukturach organizacyjnych, która mogłaby uzupełniać i wspomóc pełnomocnika ds. ochrony informacji oraz administratorów systemów teleinformatycznych.

Podsumowując, należy podkreślić, że jednym z podstawowych wyzwań współczesnego pola walki jest zapewnienie bezpieczeństwa zarówno w skali całej jednostki organizacyjnej, żołnierzy, pracowników, jak i jej zasobów informacyjnych oraz danych. Zlekceważenie (także nieprawidłowa ocena) potencjalnych zagrożeń skutkuje najczęściej nieodwracalnymi następstwami. Najważniejsza jest równowaga, znalezienie „złotego środka", bo przesada może doprowadzić finalnie do takich samych skutków jak brak ochrony zasobów informacyjnych.

[30] Oczywiście wymaga to potwierdzenia odpowiednimi badaniami.

Podejmowanie decyzji we współczesnym otoczeniu wymusza na nas posiadanie wiarygodnej i kompletnej informacji. Kluczem do sukcesu jednostek organizacyjnych o specjalnym przeznaczeniu jest profesjonalne zarządzanie zwłaszcza bezpieczeństwem informacji. Ma to szczególne znaczenie w sytuacji, gdzie coraz więcej obszarów działalności jednostek organizacyjnych (nie tylko o specjalnym przeznaczeniu) ma dla nich znaczenie krytyczne.

Należy jeszcze raz podkreślić, że bezpieczeństwo informacji ma charakter złożony i dotyczy:

- po pierwsze **samej informacji** w jej specyficznej postaci, często nieuchwytnej dla wielu osób (można zostać okradzionym z informacji, nie będąc tego świadomym);
- po drugie **systemów**, w których jest ona wytwarzana, przetwarzana, przechowywana i przekazywana;
- po trzecie **środowiska**, w którym te systemy działają – każdy szczegół dotyczący pomieszczenia, okablowania czy zasilania może okazać się decydujący w skutkach;
- po czwarte **personelu**, który korzysta z tych systemów i który często bywa „niedouczony", nieobliczalny w swoich działaniach i trudny do skontrolowania;
- i wreszcie po piąte, **otoczenia prawnego**[31], które jest ciągle kształtowane i próbuje nadążyć za rozwojem technologii.

Dodając do tego, że wszystko wokół jest zmienne i słabo określone, a pomylić się można tylko raz, zapewnienie bezpieczeństwa złożonego systemu nie jest sprawą prostą i oczywistą, wymaga wzorowej organizacji, dyscypliny, wiedzy i sprawnego zarządzania.

Jeżeli przyjmiemy, że zarządzanie bezpieczeństwem informacji zajmuje się definiowaniem, osiąganiem i utrzymaniem bezpieczeństwa rozumianego jako zapewnienie dla systemów poufności, integralności, dostępności, autentyczności, rozliczności oraz

[31] Uwaga na podstawie http://www.iso27000.pl/sites/view/news=123 [stan na dzień 2013.09.06]. Należy podkreślić ważność przepisów prawnych często najskuteczniej wymuszających określone działania. Nabiera to szczególnego znaczenia po wejściu takich przepisów – **Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych** (31 maja 2012 roku przywołany przepis wszedł w życie). Samo zarządzenie zdefiniowało wymogi odnośnie do trzech aspektów w postaci: Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, minimalnych wymagań dla systemów teleinformatycznych. Dla minimalnych wymagań dla systemów informatycznych na uwagę zasługuje określenie sposobów zapewnienia bezpieczeństwa przy wymianie informacji. Rozporządzenie ma istotny wpływ na poziom bezpieczeństwa informacji. Należy podkreślić, że posiadanie certyfikacji na zgodność z PN-ISO/IEC 27001 oznacza automatyczne spełnienie wymagań prawnych wskazanych w rozporządzeniu, co powinno być koronnym argumentem (w aspekcie dostosowania i zgodności z polskimi przepisami prawa) do wdrażania w organizacjach norm ISO z zakresu bezpieczeństwa informacji.

niezawodności, to kluczowymi pojęciami dla tego obszaru zagadnień będą: zasoby (aktywa), zagrożenia, podatności, następstwa oraz ryzyko. Ich zrozumienie pozwala przejść do przedstawienia kolejnych: analizy ryzyka, ochrony podstawowej, zarządzania ryzykiem i samego zarządzania bezpieczeństwem informacji jako zbioru procesów.

W różnych jednostkach organizacyjnych są różne zasoby, podatności i zagrożenia, zaś ją samą można uznawać za mniej lub bardziej uzależnioną od środków teleinformatycznych – **stąd wydaje się logiczne przyjęcie założenia, że poszczególne jednostki organizacyjne (nawet o podobnym charakterze działalności) będą musiały różnić się także w zakresie optymalnego doboru zabezpieczeń.**

Jednocześnie należy zwrócić uwagę na to, że bezpieczeństwo systemów informacyjnych w organizacji jest takie, jakie jest bezpieczeństwo każdego z eksploatowanych w niej systemów, a ściślej – najsłabszego spośród nich.

Ponadto współcześnie w celu identyfikacji i określenia zagrożeń (zwłaszcza dla jednostek organizacyjnych o specjalnym przeznaczeniu) należy uwzględnić w szczególności:

1) zmiany co do charakteru działań potencjalnych napastników;
2) zmiany motywacji – w przeszłości główną motywacją było zyskanie sławy i/lub uznania po dokonaniu udanych włamań do sieci wojskowych, rządowych oraz korporacyjnych – współcześnie działania podejmowane są najczęściej z chęci zysku;
3) zmiany charakteru działań napastników na wrażliwe i poufne dane w postaci ataków dyskretnych, bez zbędnego rozgłosu.

Biorąc pod uwagę powyższe, można stwierdzić, że dane o charakterze wrażliwym są i będą atrakcyjne ze względu na cenę, jaką mogą za nie zaoferować rządy lub służby specjalne obcych państw, a także organizacje o charakterze terrorystycznym. Należy jednocześnie założyć, że posiadają one nielimitowane środki i dysponują nimi na ten cel w dowolny sposób.

Trzeba jednocześnie podkreślić, że **współcześnie nie istnieją systemy bezpieczeństwa informacji, które uwzględniałyby wszystkie potencjalne zagrożenia oraz potrafiłyby zapobiec ich realizacji. Ponadto podejmowane działania w zakresie bezpieczeństwa informacji nie nadążają za zmianami i rosnącą liczbą zagrożeń.**

Zarządzanie bezpieczeństwem to ciągły i złożony proces zachodzący w stale zmieniającym się środowisku, przy występowaniu coraz nowszych form zagrożeń i wyzwań dla organizacji, a także przy niebywałym postępie technologicznym.

Bezpieczeństwo to nie tylko stosowanie zabezpieczeń. Zabezpieczenia są kosztowne, więc muszą być dobrane stosownie do zagrożeń oraz do wartości szkód, które by można ponieść w sytuacji, gdy ich nie zastosujemy. Dobór zabezpieczeń powinien zostać poprzedzony starannym określeniem celów bezpieczeństwa dla organizacji i jej systemów, uwzględniających realizację misji w sytuacji występowania zagrożeń. Wdrożenie zabezpieczeń nie oznacza jeszcze osiągnięcia zaplanowanego poziomu bezpieczeństwa. Równie ważnymi zadaniami są: zdefiniowanie zasad bezpiecznego przetwarzania informacji,

szkolenie i uświadamianie pracowników, monitorowanie aktualnego stanu bezpieczeństwa, jak i stałe doskonalenie i adaptacja systemów oraz organizacji do zmieniającego się otoczenia. Samo **zminimalizowanie dysproporcji pomiędzy stanem bezpieczeństwa informacji a zagrożeniami można osiągnąć poprzez wykorzystanie efektywnego systemu zarządzania bezpieczeństwem informacji (SZBI)**.

Bezpieczeństwo nie jest więc aktem jednorazowym, polegającym na wdrożeniu zabezpieczeń, lecz ciągłym, dynamicznym, a przy tym bardzo złożonym procesem, wymagającym stałego nadzoru i przystosowywania się do zmiennych warunków otoczenia. **Poprawnie zbudowany system zarządzania bezpieczeństwem informacji (SZBI) pozwoli na osiągnięcie założonego (uwarunkowanego dopuszczalnym poziomem ryzyka) i optymalnego poziomu bezpieczeństwa informacji dla danego typu organizacji.** Szczególnie nabiera to znaczenia dla jednostek organizacyjnych o specjalnym przeznaczeniu.

Z tego wynika, że zarządzanie bezpieczeństwem z wykorzystaniem SZBI jest gwarancją bezpieczeństwa informacji, racjonalności w ponoszonych na nią i jej ochronę kosztach oraz daje możliwość pełnego jej wykorzystania do realizacji celów organizacji.

LITERATURA:

1. AAP-6(2010). *Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO*, Agencja Standaryzująca NATO.
2. A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych*, Wydawnictwo Akademii Podlaskiej, Siedlce 2002.
3. A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy BELLONA, Warszawa 2003.
4. P. Beynon-Davies, *Inżynieria systemów informacyjnych, Wprowadzenie,* wydanie drugie, Wydawnictwa Naukowo-Techniczne, Warszawa 2004.
5. A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2007.
6. L. Ciborowski, *Pojęciowa interpretacja terminu „informacja" i jej pochodnych,* „Zeszyty Naukowe AON", nr 4(81) 2010, s. 58-108.
7. D.E. Denning, *Wojna informacyjna i bezpieczenstwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
8. S. Malinowski, *CAWI jako metoda badawcza w naukach o obronności – wybrane zagadnienia*, „Studia Bezpieczeństwa Narodowego (National Security Studies)" Nr 3, Wojskowa Akademia Techniczna, Instytut Organizacji i Zarządzania WCY, Warszawa 2012.
9. S. Malinowski, *Zarządzanie bezpieczeństwem informacji jednostki wojskowej specjalnego przeznaczenia*, rozprawa doktorska pod kier. naukowym prof. dr. hab. inż. A.A. Barczaka, Akademia Obrony Narodowej, Warszawa 2012.
10. M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

11. M. Molski, S. Opala, *Elementarz bezpieczeństwa systemów informatycznych*, MIKOM, Warszawa 2002.
12. A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Wydawnictwo AON, Warszawa 2010.
13. D.L. Pipkin, *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
14. PN-ISO/IEC 27001:2007, *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem. Wymagania*, „Information Security Management Systems. Requirements", Polski Komitet Normalizacyjny, polska norma wprowadzająca ISO/IEC 27001:2005, zastępująca PN-l-07799-2:2005.
15. T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, HELION, Gliwice 2006.
16. P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Wyd. Bellona, Warszawa 1994.
17. R.J. Sutton, *Bezpieczenstwo telekomunikacji. Praktyka i zarządzanie*, Wydawnictwa Komunikacji i Łączności, Warszawa 2004.
18. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. Nr 0, poz. 526.
19. Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. Nr 182, poz. 1228.
20. www.iso.org.pl
21. www.iso27000.pl

SELECTED RESEARCH ISSUES OF INFORMATION SECURITY MANAGEMENT OF ORGANIZATIONAL UNIT FOR SPECIAL PURPOSES (JWSP)

Abstract. The intention of the author was to present various problems of information security management of an organizational special purpose units within armed forces or similar. The article is based on detailed information and research on a subject. The recognition of contemporary legitimacy in the research area, with its new problems and questions included, presents actual significance, not only in cognitive, but also utilitarian sense. The paper shows different aspects of a substance discussed and its purpose is to present types of questions and answers on it, at least in some of the cases. Presented information and contents are result of cognition process, analyses and observations of author, pursued as required for the postgraduate studies at National Defense University. It's consequence was Ph.D. thesis on the subject, titled *Information security management of organizational unit of special purpose*. This article presents some of its main ideas compiled.