DĘBICKA Ewa[1]

Zarządzanie ryzykiem, jako warunek konieczny zapewnienia bezpieczeństwa informacji w instytutach badawczych

Zarządzanie ryzykiem, identyfikacja ryzyka, ocena ryzyka, redukcja ryzyka, monitorowanie ryzyka, dokumentowanie ryzyka, bezpieczeństwo informacji w instytutach badawczych

Streszczenie

Instytuty badawcze ze względu na swój znaczny udział w budowaniu nowoczesnej gospodarki opartej na wiedzy powinny przede wszystkim zapewnić bezpieczeństwo informacji, gdyż jest ona ich najcenniejszym aktywem. Podstawowym elementem systemu zarządzania bezpieczeństwem informacji w instytutach badawczych jest zarządzanie ryzykiem. W artykule podjęto próbę przedstawienia działań składających się na kompleksowe zarządzanie ryzykiem w instytutach badawczych. Skutecznie przeprowadzony proces zarządzania ryzykiem ma na celu przede wszystkim jego ograniczenie i zabezpieczenie się przed jego negatywnymi skutkami.

THE RISK MANAGEMENT, AS A NECESSARY CONDITION FOR ENSURING INFORMATION SECURITY AT THE RESEARCH INSTITUTES

Abstract

The research institutes due to their significant contribution to building modern economy relying on the knowledge, should first of all, ensure security of the information, as it is their most valuable asset. The fundamental element of the information security management system at the research institutes is the risk management. The article attempts to present the actions that amount to a comprehensive risk management at the research institutes. Effectively carried out process of the risk management is aimed, first of all, at limiting it and protecting against it is negative consequences.

1. WSTĘP

Pod koniec XX wieku gwałtownie wzrosło znaczenie informacji, którą zaczęto traktować, jako jedno z najważniejszych aktywów każdego przedsiębiorstwa. Informacja stała się towarem, głównym elementem gospodarki opartej na wiedzy i zaczęła podlegać tym samym prawom, co inne towary i usługi. To spowodowało, że znacznie wzrósł popyt na rzetelną i wiarygodną informację, która decydowała o zdobyciu lub utrzymaniu przewagi konkurencyjnej. Gromadzenie, analizowanie oraz przetwarzanie informacji o konkurencie i jego otoczeniu w celu uzyskania przewagi na rynku zaczęło odbywać się w ramach zorganizowanego wywiadu gospodarczego[2]. Zagrożenie związane z wywiadem gospodarczym stało się także realnym zagrożeniem dla instytutów badawczych, które prowadzą badania naukowe i prace rozwojowe mające na celu pozyskanie nowych technologii dla tak newralgicznych obszarów, jak obronność i bezpieczeństwo państwa, medycyna, telekomunikacja, informatyka, transport. Zapewnienie bezpieczeństwa informacji, czyli poufności dostępności i integralności na każdym etapie jej przetwarzania, powinno być priorytetowym działaniem podjętym przez instytuty badawcze[2]. Do podstawowej działalności instytutów badawczych należy:

- prowadzenie badań naukowych i prac rozwojowych,
- przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki,
- wdrażanie wyników badań naukowych i prac rozwojowych[15].

Konieczność zapewnienia bezpieczeństwa informacji w instytutach badawczych jest tym bardziej uzasadniona, że 80% wdrożeń w polskim przemyśle jest wynikiem prac badawczo-rozwojowych prowadzonych właśnie przez te jednostki organizacyjne[13]. Zarządzanie ryzykiem w instytutach badawczych jest podstawowym elementem zapewnienia bezpieczeństwa informacji, gdyż wyniki z jego oceny stanowią podstawę do podjęcia decyzji dotyczących przyjęcia do realizacji bądź odmówienia realizacji specyficznych badań naukowych i prac rozwojowych oraz zasadności stosowania odpowiednich środków zapewnienia bezpieczeństwa informacji w instytucie.

2. ZARZĄDZANIE RYZKIEM, JAKO ELEMENT ZAPEWNIENIA BEZPIECZEŃSTWA INFORMACJI W INSTYTUTACH BADAWCZYCH

2.1 Pojęcie ryzyka

Słowo *ryzyko* jest zapożyczeniem i wywodzi się z języka starowłoskiego, gdzie słowo *risicare* znaczy odważyć się [7]. W języku angielskim *risk* oznacza sytuację powodującą niebezpieczeństwo lub możliwość, że zdarzy się coś złego.

[1]Instytut Transportu Samochodowego, email: ewa.debicka@its.waw.pl . Praca naukowa finansowana ze środków budżetowych na naukę w latach 2010-2012 jako projekt badawczy.

[2] Instytutem badawczym w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych jest jednostka organizacyjna, wyodrębniona pod względem prawnym, organizacyjnym i ekonomiczno-finansowym, która prowadzi badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie i zastosowanie w praktyce

Pojęcie ryzyka jest niejednoznaczne i definiowane na wiele różnych sposobów, często ze sobą niespójnych, co potwierdza fakt, że nie wypracowano, jak dotąd jednej definicji ryzyka. W zakresie zapewnienia bezpieczeństwa informacji ryzyko definiowane jest przede wszystkim w dokumentach normatywnych. I tak według normy PN-I-13335-1:1999 ryzyko to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie tych zasobów [9]. Zbliżoną definicję ryzyka podaje norma PN-ISO/IEC 17799:2007, wg której ryzyko to kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji [10]. Na potrzeby niniejszego artykułu przyjęto definicję przedstawioną w normie PN-ISO/IEC 27005:2010, według której ryzyko związane z bezpieczeństwem informacji to potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę dla instytutu badawczego[11]. Definicję ryzyka w ujęciu systemowym dotyczącym zarządzania bezpieczeństwem informacji podaje K. Liderman, według niego termin ryzyko oznacza miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji, wyrażoną jako iloczyn prawdopodobieństwa (lub możliwości) wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków (strat)[8]. Generalnie, ryzyko odnoszące się do zapewnienia bezpieczeństwa informacji opisywane jest przez kombinacje dwóch czynników: prawdopodobieństwa wystąpienia niechcianego incydentu oraz związanych z nim negatywnych następstw.

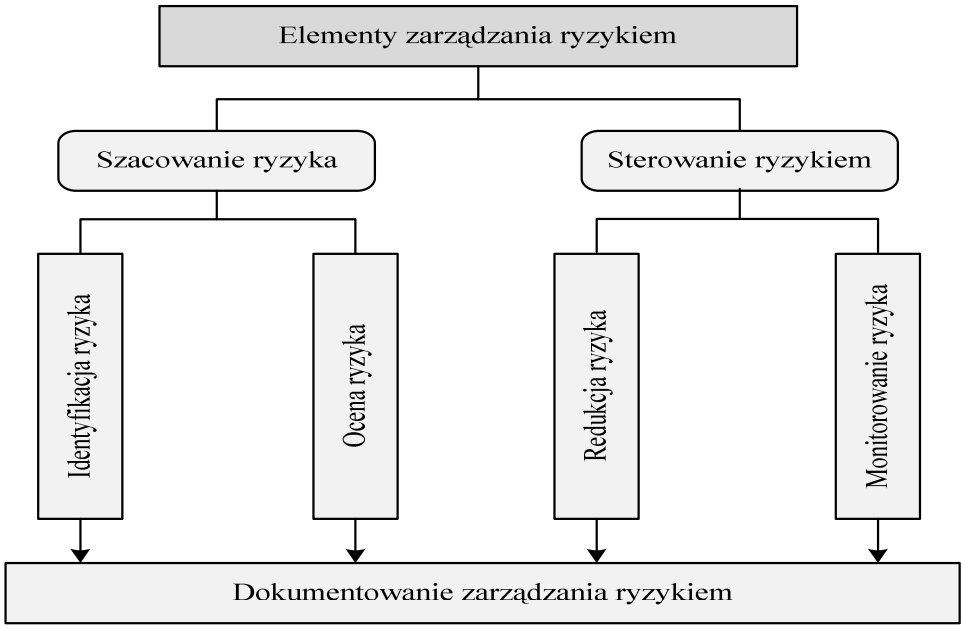
2.2 Zarządzanie ryzykiem w zapewnieniu bezpieczeństwa informacji w instytutach badawczych

Ryzyko obejmujące obszar działania instytutów badawczych, ze względu na zmienność, powinno być stale i odpowiednio monitorowane. Wymaga to przeznaczenia na ten cel wystarczających zasobów, infrastruktury, zapewnienia kompetentnego personelu, postepowania według określonych i zatwierdzonych procedur innymi słowy ryzykiem należy skutecznie zarządzać. Rzeczywisty stan zarządzania ryzykiem w organizacji wskazuje na to, że do zagadnienia tego podchodzi się w sposób intuicyjny bez ustalonych i sprawdzonych metod oceny ryzyka. Z opublikowanych wyników badań [4] wynika, że ponad 20% organizacji w ogóle nie ocenia najważniejszych form ryzyka, ponad 30% organizacji nie stosuje żadnej formalnej metodyki oceny ryzyka, 50% organizacji jest częściowo przekonana o skuteczności zarządzania ryzykiem, w tym tylko 10% wprowadziło działania związane z zarządzaniem ryzykiem. Głównym celem zarządzania ryzykiem w zapewnieniu bezpieczeństwa informacji jest maksymalne jego ograniczenie i możliwie najlepsze zabezpieczenie się przed jego negatywnymi skutkami. Jest to możliwe poprzez wcześniejsze rozpoznanie ryzyk, na które narażona jest organizacja, a następnie ich pomiar, kontrole, redukcje oraz monitorowanie.

Opinie wielu autorów prac dotyczących ryzyka takich, jak np.: J. Jasińska i J. Śmiałkowska [5], K. Polkowski [12] są na ogół zgodne, co do tego, że zarządzanie ryzykiem powinno obejmować działania:

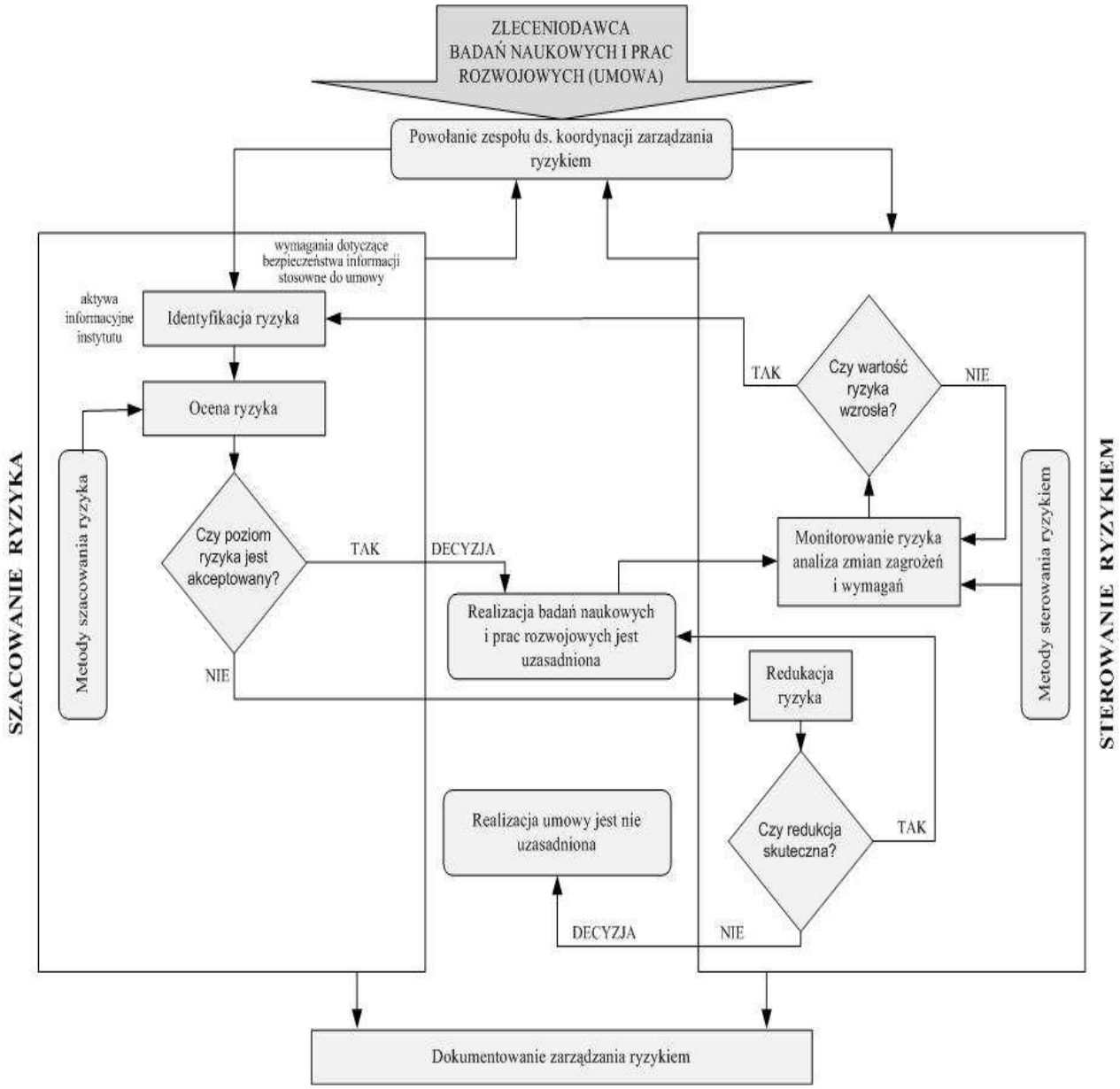
- **szacowania ryzyka** w tym:
  - identyfikację ryzyka,
  - ocenę ryzyka,
- **sterowania ryzykiem**, w tym:
  - redukcję ryzyka,
  - monitorowanie ryzyka
- oraz **dokumentowania zarządzania ryzykiem**.

Powyższe działania zostały przedstawione w sposób graficzny na rysunku 1.



Rys.1. Działania w zarządzaniu ryzykiem
opracowanie własne

Zatem zarządzanie ryzykiem w zapewnieniu bezpieczeństwa informacji w instytutach badawczych polega na skoordynowaniu działań dotyczących identyfikacji, oceny, redukcji, monitorowania oraz dokumentowania ryzyka. Cykl zarządzania ryzykiem w instytucie badawczym przedstawiono na rysunku 2.



Rys.2. Cykl zarzadzania ryzykiem bezpieczeństwa informacji w instytucie badawczym
opracowanie własne

Na identyfikację ryzyka w zapewnieniu bezpieczeństwa informacji składa się:

- sporządzenie listy aktywów informacyjnych,
- klasyfikacja i oznaczenie informacji,
- określenie potencjalnych zagrożeń bezpieczeństwa informacji,
- analiza podatności informacyjnej aktywów.

Podstawą identyfikacji ryzyka jest sporządzenie listy aktywów objętych systemem zarządzania bezpieczeństwem informacji oraz klasyfikacja i oznaczenie informacji. Aktywem informacyjnym jest wszystko to, co stanowi źródło informacji w instytucie badawczym. Aktywa mogą mieć naturę materialną, jak i nie materialną. Przykładowy katalog aktywów przedstawia się następująco:

- dokumentacja prowadzonej działalności w tym dokumentacja kadrowa, księgowa, prawna,
- oprogramowanie komputerowe,
- aktywa fizyczne, np.: sprzęt komputerowy, nośniki informacji,
- usługi, w tym: usługi informatyczne, remontowe, konserwacyjne,
- pracownicy, ich kwalifikacje, umiejętności i doświadczenie,
- wartości niematerialne takie, jak reputacja, wizerunek.

Oczywiście nie jest to katalog zamknięty, a stanowi jedynie ogólny podział na grupy aktywów informacyjnych i może być dowolnie modyfikowany przez instytuty badawcze pod kątem indywidualnych potrzeb. Po dokonaniu inwentaryzacji należy wyznaczyć do każdego aktywa właściciela, który będzie za nie odpowiedzialny. Jednakże największym problemem praktycznym jest klasyfikacja informacji i jej prawidłowe oznaczanie. Od właściwie przeprowadzonej klasyfikacji informacji zależy sposób projektowania całego systemu zarządzania bezpieczeństwem informacji, ponieważ jest ona jedną z danych wejściowych w ocenie ryzyka. Klasyfikacja informacji jest czynnością grupowania wzajemnie powiązanych informacji, określenia znaczenia tych grup dla instytutu oraz przypisywania ujednoliconych etykiet ułatwiających gromadzenie, odszukiwanie i analizę informacji [1], zaś jej celem zapewnienie, że wskazana informacja uzyskuje skuteczną ochronę na odpowiednim poziomie [14]. Generalizując, klasyfikacja informacji ma określić, które informacje są ważne i należy je chronić, a które nie mają dla instytutu istotnej wartości i nie wymagają ochrony. Oznaczenie informacji odbywa się najczęściej na dwa sposoby: opisowy (np. informacja bardzo ważna, ważna, nieistotna) i cyfrowy (np. skala od 1 do 10). Przy klasyfikacji należy uwzględnić także wymagania prawne. I tak, np.; ustawa o ochronie informacji niejawnych czy ustawa o ochronie danych osobowych wręcz narzuca sposób klasyfikacji pewnych informacji, sposób ich oznaczania, przetwarzania, przechowywania. Kolejną czynnością w identyfikacji ryzyka jest identyfikacja zagrożeń, czyli potencjalnych przyczyn niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji. Zagrożeniami mogą być wszystkie działania dotyczące informacji powodujące zakłócenia związane z poufnością, integralnością i dostępnością. Informacje podlegają różnym zagrożeniom, które generalnie możemy podzielić na dwie grupy główne:

- zagrożenia środowiskowe (zjawiska klimatyczne, sejsmiczne, epidemie, katastrofy),
- zagrożenia ludzkie (szpiegostwo, podsłuch, kradzież, pomyłki i pominięcia).

Zagrożenia wynikają z podatności, czyli słabości aktywu lub grupy aktywów do ochrony informacji. Słabość aktywu może być fizyczna, organizacyjna, proceduralna, osobowa, zarządcza, administracyjna, informatyczna lub informacyjna. Warto zaznaczyć, że podatność sama w sobie nie powoduje negatywnych skutków. Podatność jest jedynie warunkiem umożliwiającym zagrożeniu wpłynąć na zasoby. Podatnością może być:

- brak fizycznej ochrony pomieszczeń,
- brak procedur postępowania,
- brak szkoleń dla personelu,
- brak właściwych zabezpieczeń.

Kolejnym etapem w szacowaniu ryzyka jest ocena ryzyka, która polega na:

- przyjęciu określonych metod oceny ryzyka,
- określeniu wartości prawdopodobieństwa wystąpienia zagrożeń bezpieczeństwa informacji,
- określeniu wartości skutków zagrożeń bezpieczeństwa informacji,
- ustaleniu kryterium akceptowalności ryzyka,
- ocenie poziomu ryzyka.

Ocena ryzyka polega na porównywaniu oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka. Kryteria akceptacji ryzyka i akceptowalny poziom ryzyk powinny zostać określone i zaakceptowane przez najwyższe kierownictwo instytutu badawczego na etapie definiowania podejścia do szacowania. Wyznaczanie poziomu akceptacji ryzyka powinno być szczegółowo rozpatrywane w celu ustalenia optymalnej równowagi między występującym zagrożeniem a kosztami i efektywnością kosztową jego ograniczenia. Powodzenie szacowania ryzyka determinuje wybór odpowiedniej metody jego szacowania, czyli sposobu postępowania przy realizacji zadań związanych z szacowaniem ryzyka. Metoda powinna być dobrana do indywidualnego charakteru jednostki organizacyjnej, uwzględniając specyfikę prowadzonej działalności, wymagania prawne oraz regulacje wewnętrzne jednostki. Dobór metody szacowania ryzyka powinien być także adekwatny do posiadanych zasobów, w tym zasobów ludzkich, posiadanej wiedzy, potrzeb, kultury organizacyjnej. Wybór właściwej metody jest dużym wyzwaniem. Szczególnie istotne jest zapewnienie, że wybrana metoda szacowania ryzyka będzie zapewniała metodyczne podejście umożliwiające uzyskanie porównywalnych i powtarzalnych rezultatów. Wybór metody szacowania ryzyka powinien być udokumentowany. Niewłaściwie dobrana metoda może prowadzić do błędnej diagnozy ryzyka. W literaturze spotyka się z liczne metody szacowania ryzyka, tak ilościowe jak i jakościowe. Do najpopularniejszych metod szacowania ryzyka należą następujące metody:

- drzewa zdarzeń,
- drzewa błędów,
- delficka,
- "burza mózgów",
- diagram Ishikawy,
- analiza Pareto-Lorenza,
- FMEA *(Failure Mode and Effect Analysis).*

Jeżeli po przeprowadzeniu całościowego procesu identyfikacji i oceny ryzyka otrzymano nieakceptowalny poziom ryzyka, należy dokonać jego redukcji. **Redukcja nieakceptowalnego ryzyka polega na:**

- określeniu stosownych środków redukcji ryzyka,
- wdrożeniu środków redukcji ryzyka,
- ocenie skuteczności redukcji ryzyka.

W praktyce zastosowanie mają następujące środki redukcji ryzyka:

- odpowiednio dobrane zabezpieczenia,
- unikanie ryzyk,

- świadoma akceptacja ryzyk,
- przeniesienie ryzyk na inne podmioty.

Wybór optymalnych zabezpieczeń jest konsekwencją przeprowadzonej wcześniej oceny ryzyka. Termin „zabezpieczenia" oznacza elementy techniczne, osobowe, programowe lub organizacyjne wykorzystywane w działaniach ochronnych, których nadrzędnym celem jest zapewnienie odpowiedniego poziomu ochrony logicznej i fizycznej informacji. Ich zadaniem jest ochrona przed zagrożeniami, redukcja podatności, ograniczanie następstw niepożądanych czynności, wykrywanie incydentów oraz ułatwianie odtwarzania sytuacji sprzed krytycznego zdarzenia. Drugim wariantem postępowania z ryzykiem jest jego unikanie. Unikanie ryzyka należy do negatywnych metod radzenia sobie z ryzykiem i w praktyce oznacza to, że instytut badawczy świadomie rezygnuje z realizacji pewnych badań naukowych i prac rozwojowych, które są obciążone zbyt dużym ryzykiem. Wpływa to na hamowanie pewnych przedsięwzięć i może być oznaką niedoskonałości zarządzania bezpieczeństwem informacji. Trzecią metodą redukcji ryzyka jest świadoma akceptacja ryzyk, czyli świadome podejmowanie przez kierownictwo instytutu decyzji na podstawie wyników otrzymanych z szacowania ryzyka. Kierownictwo jest świadome istniejących ryzyk, ale je akceptuje. Akceptacja ryzyka wymaga wcześniejszego ustalenia kryteriów akceptowania ryzyka. Powodem tego może być na przykład wynik analizy wskazujący, że koszt zakupu nowych zabezpieczeń będzie wyższy od potencjalnych skutków utraty poufności, integralności czy dostępności informacji. Przenoszenie ryzyka, czwarty wariant – to świadoma decyzja polegająca na przesunięciu problemów związanych z ryzykiem i kosztami ryzyka na inny podmiot. Takie działanie pozwala w pełni realizować wszystkie działania zgodnie z celem organizacji. Najpopularniejszą formą przenoszenia ryzyka jest ubezpieczenie ryzyka, czyli przeniesienie go na towarzystwo ubezpieczeniowe. Zawarcie umowy ubezpieczenia skutkuje rozłożeniem ciężaru ekonomicznego potencjalnych strat pomiędzy podmiotami o podobnym stopniu zagrożenia identycznym ryzykiem dzięki wniesieniu specjalnych składek, z których tworzy się fundusz. Jest to korzystna forma zabezpieczania się przed ryzykiem, gdyż instytut nie musi tworzyć własnego funduszu przeznaczonego na ten cel. Nawet po dokonaniu wyboru środka redukcji ryzyka oraz implementacji określonych wymagań nie osiągnie się sytuacji, w której ryzyko zostanie definitywnie wyeliminowane. Ryzyko, które pozostaje po wykonaniu działań redukujących nazywane jest ryzykiem szczątkowym. Podobnie, jak ryzyko akceptowalne i nieakceptowane tak, też ryzyko szczątkowe powinno uzyskać aprobatę najwyższego kierownictwa.

Kolejnym elementem procesu zarządzania ryzykiem jest monitorowanie ryzyka i polega ono na:

- stałej kontroli zmian zagrożeń i ich wpływu na poziom ryzyka,
- stałej analizie zmian wymagań dotyczących bezpieczeństwa informacji,
- podjęciu decyzji o ponowieniu cyklu zarządzania ryzykiem, jeśli zmiany zagrożeń skutkują nieakceptowalnym poziomem ryzyka.

Monitorowanie ryzyka w znacznej mierze uzależnione jest od tego czy:

- działania redukujące ryzyko są rzeczywiście realizowane,
- każdy nowy przypadek zmiany ryzyka jest szybko identyfikowany i oceniany,
- podejmowane działania dotyczące ryzyka odnoszą oczekiwany skutek,
- będą podejmowane nowe działania dotyczące ryzyka, jeżeli aktualnie podjęte nie były skuteczne.

Regularne i zaplanowane obserwacje ryzyka można prowadzić metodami badań auditowych poprzez ocenę osiągnięcia zaplanowanych zamierzeń oraz w ramach przeglądu zarządzania bezpieczeństwem informacji, którego celem jest ocena przydatności, adekwatności i skuteczności przyjętych rozwiązań [6]. Badania auditowe są oceną odbywającą się systematycznie i w zaplanowanych odstępach czasu, mającą na celu obiektywne poszukiwanie dowodów potwierdzających prawidłowość realizacji procesów i działań wcześniej określonych [3]. Badania auditowe mogą potwierdzić, bądź nie, prawidłowość przyjętych przez instytuty badawcze rozwiązań oraz realizację założonych wymagań odnośnie zarządzania ryzykiem. Ich najważniejszą zaletą jest możliwość krytycznego spojrzenia na realizowane działania oraz określenie czy obecna dokumentacja, zasoby, personel są wystarczające. Dodatkowym atutem jest fakt, że są one punktem wyjścia do podejmowania działań korygujących i zapobiegawczych, które w konsekwencji implikują doskonalenie bezpieczeństwa informacji. Wykorzystanie metody badań auditowych do monitorowania ryzyka daje szerokie możliwości:

- określenia zmian zagrożeń i ich wpływu na poziom ryzyka,
- zweryfikowania czy określone elementy procesu zarządzania ryzykiem są zgodne z wymaganiami normatywnymi oraz wewnętrznymi instytutu badawczego,
- oceny skuteczności podejmowanych działań dotyczących ryzyka,
- wsparcia kierownictwa w podejmowaniu decyzji odnośnie ryzyka.

Drugą metodą służąca do regularnego i planowanego monitorowania ryzyka, jest przegląd zarządzania bezpieczeństwem informacji, czyli popularne narzędzie wykorzystywane w systemach zarządzania. Przegląd bezpieczeństwa informacji należy do obowiązków najwyższego kierownictwa. Jest przeprowadzany w celu zapewnienia poprawności i skuteczności funkcjonowania systemu, a także oceny możliwość jego doskonalenia i wskazania potrzebnych zmian [16]. Zaleca się, aby przeglądy zarządzania stanowiły platformę do wymiany nowych idei, otwartych dyskusji i oceny danych wejściowych. Koncentrując się na monitorowaniu ryzyka szczególnie ważne dane wejściowe będą stanowiły:

- wyniki auditów,
- informacje zwrotne,
- informacje na temat statusu działań korygujących i zapobiegawczych,
- wyniki pomiarów skuteczności stosowanych zabezpieczeń,

- informacje o zmianach, które mogłyby wpłynąć na zapewnienie bezpieczeństwa informacji w instytucie badawczym,
- istotne zalecenia dotyczące doskonalenia.

Przegląd bezpieczeństwa informacji jest podsumowaniem wszystkich ważkich wydarzeń na przestrzeni roku, a w jego wyniku planowane są działania na kolejny rok w zakresie uaktualnienia planów szacowania ryzyka i postępowania z ryzykiem, uaktualnienia wymagań w odniesieniu do zapewnienia bezpieczeństwa informacji, a także w zakresie zmian wyznaczonych poziomów ryzyka i kryteriów jego akceptacji. Podsumowując, właściwie przeprowadzony przegląd dostarcza kierownictwu instytutu badawczego kompleksowych i rzetelnych informacji o działaniach podejmowanych w ramach zarządzania ryzykiem.

Ważnym elementem procesu zarządzania ryzykiem jest dokumentowanie wszelkich działań i podjętych decyzji w tym obszarze. Zasadniczym celem dokumentowania jest formalne zakomunikowanie przez najwyższe kierownictwo pracownikom instytutu badawczego podejścia do zarządzaniem ryzykiem. Ponadto dokumentowanie podjętych czynności umożliwia przypisanie pracownikom odpowiedzialności za konkretne zadania, a następnie daje możliwość rozliczenia ich z wykonanej pracy. Dokumentowanie stanowią zapisy będące dowodem przeprowadzonych działań i ich wyników po dokonaniu identyfikacji, oceny, redukcji i monitorowania ryzyka. Na dokumentację zarządzania ryzykiem składają się:

- lista zidentyfikowanych aktywów,
- powtarzalna metoda oceny ryzyka,
- opis wybranych i wdrożonych zabezpieczeń,
- plan postępowania z ryzykiem, który określa zaplanowane działania do wykonania, ich kolejność oraz wskazuje osoby odpowiedzialne,
- zapisy z pomiaru skuteczności zabezpieczeń,
- zapisy z przeprowadzonych szkoleń,
- wyniki auditów,
- raport z przeglądu zarządzania.

Dokumentowanie jest istotnym elementem zarządzania ryzkiem w zapewnieniu bezpieczeństwa informacji, gdyż gwarantuje odtwarzalność i powtarzalność na etapie szacowania i sterowania ryzykiem, a tym samym umożliwia porównanie otrzymanych wyników z planowanymi.

3. WNIOSKI

Zarządzanie ryzykiem jest procesem determinującym zapewnienie bezpieczeństwa informacji w instytutach badawczych. Niewątpliwie od rzetelności, skrupulatności i dokładności przeprowadzenia procesu szacowania ryzyka zależy czy wszystkie istotne aktywa informacyjne zostały zidentyfikowane i czy informacje, które wymagają szczególnej ochrony będą zabezpieczone na właściwym poziome. Dla instytutów badawczych szczególne znaczenie mają informacje związane z metodami badawczymi oraz wyniki badań przed ich oficjalnym opublikowaniem. Niewłaściwa ochrona tych informacji może w konsekwencji spowodować znaczne straty finansowe, utratę reputacji czy też skutki prawne. Wyniki otrzymane z szacowania ryzyka powinny stanowić podstawę przy podejmowaniu decyzji w kwestiach realizacji lub odmowy realizacji badań naukowych i prac rozwojowych a także wyboru właściwego środka redukcji ryzyka. Podsumowując, zarządzanie ryzykiem w instytutach badawczych powinno być oparte na szacowaniu ryzyka obejmującym identyfikację i ocenę ryzyka oraz na sterowaniu ryzykiem obejmującym redukcję i monitorowanie ryzyka oraz jego dokumentowaniu.

4. BIBLIOGRAFIA

[1] Borucki M.: *Klasyfikacja informacji*, Biuletyn tematyczny Bezpieczeństwo informacji, Nr 1/2006.
[2] Ciecierski M.: *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka*, Toruń, Wydawnictwo Adam Marszałek 2009.
[3] Gruca-Wójtowicz P.*: Determinanty skuteczności auditów wewnętrznych*, Zarządzanie Jakością nr 1/2010.
[4] Jasińska J., *Ocena ryzyka w procesach realizacji wyrobów obronnych*, Warszawa, Instytut Techniczny Wojsk Lotniczych 2008.
[5] Jasińska J., Śmiałkowska J.: *Problematyka zarządzania ryzykiem w procesie realizacji umowy, Problematyka normalizacji, jakości i kodyfikacji w aspekcie integracji z NATO i UE*, Warszawa, ZSJZ 2008.
[6] Jedynak P.: *Orientacja na redukcję ryzyka w wybranych znormalizowanych systemach zarządzania*, Problemy Jakości Nr 11/2011.
[7] Kaczmarek T. T., *Ryzyko i zarządzanie ryzykiem, ujęcie interdyscyplinarne*. Warszawa, Wydawnictwo Difin, 2005.
[8] Liderman K.: *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa, PWN 2008.
[9] Norma PN-I-13335-1:1999 Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.
[10] Norma PN-ISO/IEC 17799:2007 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.
[11] Norma PN-ISO/IEC 27005:2010 Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.

[12] Polkowski K.: *Zasadnicze zmiany w bezpieczeństwie teleinformatycznym – szacowanie i zarządzanie ryzykiem, ogólne uwarunkowania, Ochrona informacji niejawnych, biznesowych i danych osobowych*, Katowice, KSOIN oraz Uniwersytet Śląski 2010.
[13] Sosnowska M.: *Podsumowanie dyskusji, Master of Business Administration 1/2010 (102)*, Warszawa, Wydawnictwo Akademickie i Profesjonalne 2010.
[14] Ślawska J.: Sikora T.: *Kategorie i atrybuty informacji oraz jej ochrona*, Problemy Jakości Nr 12/2011.
[15] Ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. Nr 96, poz. 618 z 2010 r.).
[16] Wojciechowski W., Ślęzak M., Włodarczyk E.: *Przegląd zarządzania w świetle wymagań normy PN-EN ISO 9001:2008 - wybrane zagadnienia*, Warszawa, ZSJiZ 2009.