5

ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA INFORMACJI W ŚWIETLE WYMAGAŃ NORMATYWNYCH

5.1 WPROWADZENIE

Efektywne zarządzanie przedsiębiorstwem uwarunkowane jest właściwym zarządzaniem jego wszystkimi zasobami, tj. rzeczowymi, finansowymi, ludzkimi oraz informacyjnym. To właśnie informacjami obecnie przypisuje się kluczowe znaczenie w działalności gospodarczej, naukowej, politycznej, czy kulturalnej. Najprościej informacje można określić jako niezbędne do podejmowania odpowiednich decyzji. Stanowią one swego rodzaju majątek firmy, który narażony jest na ryzyko związane z utartą, ujawnienie czy niekontrolowaną modyfikacją.

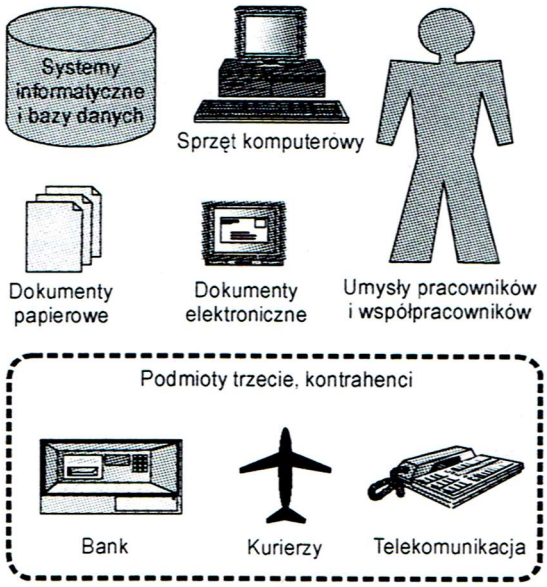
Znaczącą wartość informacji w gospodarce potwierdzają incydenty związane z jej wyciekiem, które obecnie stały się powszechnością. Praktycznie codziennie dochodzi do kolejnych ataków na informacje przez nielojalnych pracowników, nieuczciwą konkurencję czy cyberprzestępców. Zagrożenia te dotyczą nie tylko dużych koncernów, ale także uczelni wyższych, instytucji państwowych, a także pojedynczej jednostki społecznej. W związku z tym problematyka bezpieczeństwa informacji wpisuje się w nowoczesne trendy zarządzania przedsiębiorstwem.

W aspekcie bezpieczeństwa informacji wskazać należy na dwa zasadnicze problemy, do których należy: wielopostaciowość informacji oraz cykl życia informacji.

Informacje w organizacji tak naprawdę mogą występować wszędzie, przybierając rozmaite formy bądź też być utrwalane i udostępniane za pomocą różnego rodzaju środków i narzędzi (rys. 5.1). I tak, mogą one być:

- przechowywane w systemach komputerowych (serwery plików, komputery, urządzenia mobilne, bazy danych, aplikacje);
- pisane i drukowane w formie papierowej (dokumentacja, umowy, projekty, plany);
- przechowywane na różnego rodzaju nośnikach danych (dyski optyczne CD/DVD, dyski przenośne, karty pamięci, PenDrive);
- przesyłane faksem;

- przesyłane pocztą elektroniczną;
- wypowiadane w rozmowie;
- znane pracownikowi (np. wiedza, umiejętności, doświadczenie pracownika).

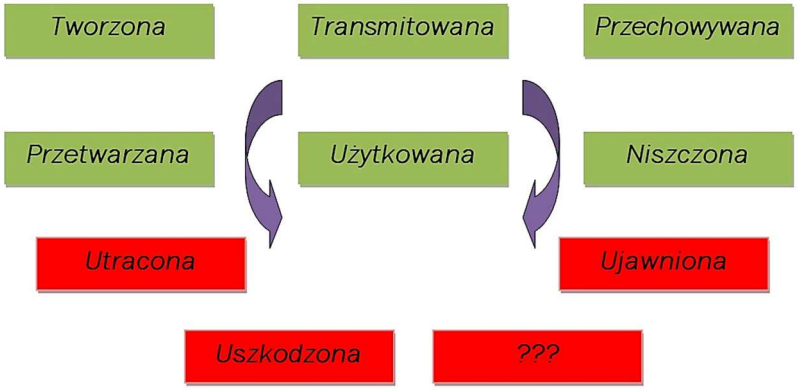


Rys. 5.1 Miejsca przechowywania informacji w organizacji
Źródło: opracowanie na podstawie [5]

Wobec powyższego każdy podmiot gospodarczy zobligowany jest podejmować starania zmierzające do zapewnienia informacjom optymalnego stanu bezpieczeństwa, mając na uwadze fakt, że każdy błąd związany z przetwarzaniem bądź niewłaściwym zabezpieczeniem może generować straty finansowe i operacyjne, a także świadczyć o słabościach przedsiębiorstwa i negatywnie wpływać na jego renomę.

Zapewnienie właściwego bezpieczeństwa informacji wymaga także zwrócenia uwagi na cykl życia informacji (ILM). Zgodnie z poglądami F. Bienia [2007] stanowi on zbiór procedur, praktyk i narzędzi, które wykorzystywane są w procesie zarządzania informacją, od chwili jej utworzenia, do momentu jej dezaktualizacji i zniszczenia. Ponadto, cykl życia informacji wskazuje na zagrożenia związane z ich utratą, niekontrolowaną modyfikacją, uszkodzeniem czy nieuprawnionym ujawnieniem, co prezentuje rysunek 5.2.

Bezpieczeństwo informacji można także definiować jako systematyczne podejście do zarządzania kluczowymi informacji instytucji bądź podmiotów gospodarczych w celu zagwarantowania racjonalnego poziomu ich bezpieczeństwa. Obejmuje ono ludzi, procesy oraz technologię – obecnie nie można bowiem ograniczać się do bezpieczeństwa danych gromadzonych i przetwarzanych w systemach informatycznych [3, 10].



Rys. 5.2 Etapy życia informacji
Źródło: opracowanie własne na podstawie [6]

5.2 PODSTAWOWE WYMAGANIA W ZAKRESIE ZARZĄDZANIA RYZYKIEM BEZPIECZEŃSTWA INFORMACJI

Zarządzanie ryzykiem stanowi integralną część całościowego procesu zarządzania bezpieczeństwem informacji. Kluczowe znaczenie zarządzania ryzykiem w bezpieczeństwie informacji podkreśla norma PN-ISO/IEC 27001:2014. Zawiera ona szereg wytycznych do stosowania przez różnego rodzaju podmioty gospodarcze oraz instytucje. Podstawowe wymagania w zakresie zarządzania ryzykiem w bezpieczeństwie informacji opisane w przytoczonej normie zawiera tabela 5.1.

Na podstawie informacji zamieszczonych w tabeli 5.1 można wnioskować, iż aktualne podejście do kwestii zarządzania bezpieczeństwem informacji oparte jest na ryzyku. Zgodnie z ideą normy PN-ISO/IEC 27001 może ono występować we wszystkich realizowanych w organizacji procesach oraz systemach, a także dotyczyć ich różnorodnych zasobów (aktywów). Oprócz tego standard ten nie wskazuje konkretnej metodyki identyfikacji i oceny ryzyka, a wręcz przeciwnie. Podkreśla on, że organizacja powinna wybrać takie podejście do zarządzania ryzykiem, które będzie odpowiednie dla jej otoczenia oraz dostosowane do strategicznych wyzwań organizacji.

Tabela 5.1 Wymagania normy PN-ISO/IEC 27001:2014 w zakresie zarządzania ryzykiem

Punkt normy	Treść wymagania
6.1.1	Planując system zarządzania bezpieczeństwem informacji, organizacja powinna rozważyć czynniki wymienione w 4.1 oraz wymagania podane w 4.2, a także określić ryzyka i szanse, do których należy się odnieść, w celu: a) zapewnienia, że system zarządzania bezpieczeństwem informacji może osiągnąć zamierzony (-e) wynik (-i); b) zapobieżenia wystąpieniu niepożądanych skutków lub ich zredukowania; oraz c) ciągłego doskonalenia. Organizacja powinna zaplanować: d) działania odnoszące się do ryzyk i szans; e) sposób: 1) ich zintegrowania i wdrożenia w procesach składających się na system zarządzania bezpieczeństwa informacji; 2)oceny ich skuteczności

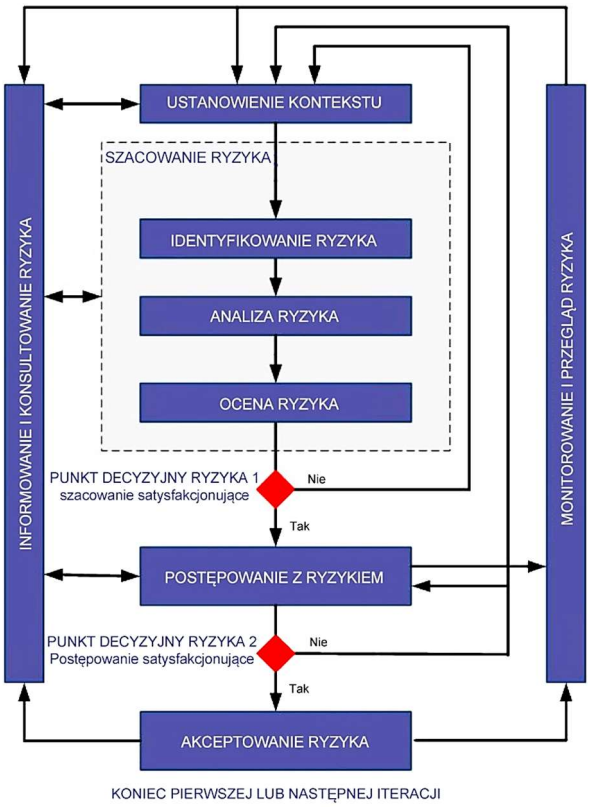
Punkt normy	Treść wymagania
6.1.2	Organizacja powinna opracować i wdrożyć proces szacowania ryzyka w bezpieczeństwie informacji, który: a) ustanawia i utrzymuje kryteria ryzyka bezpieczeństwa informacji obejmujące: 1) kryteria akceptacji ryzyka; oraz 2) kryteria szacowania ryzyka w bezpieczeństwie informacji; b) zapewnia spójne, poprawne i porównywalne wyniki w kolejnych szacowaniach ryzyka; c) identyfikuje ryzyka w bezpieczeństwie informacji: 1) stosuje proces szacowania ryzyka w bezpieczeństwie informacji do zidentyfikowania ryzyk związanych z utratą poufności, integralności i dostępności informacji będących w zakresie systemu zarządzania bezpieczeństwem informacji; oraz 2) identyfikuje właścicieli ryzyka; d) analizuje poszczególne ryzyka w bezpieczeństwie informacji 1) szacuje potencjalne następstwa zmaterializowania się ryzyk zidentyfikowanych w 6.1.2 c) 1); 2) realistycznie szacuje prawdopodobieństwo wystąpienia ryzyk zidentyfikowanych 6.1.2 c) 1); oraz 3) określa poziomy ryzyka; e) ocenia ryzyka w bezpieczeństwie informacji: 1) porównuje wyniki analizy ryzyka z kryteriami określonymi w 6.1.2 a); oraz 2) nadaje analizowanym ryzykom priorytety dla celów postępowania z ryzykiem. Organizacja powinna zachować udokumentowane informacje o procesie szacowania ryzyka w bezpieczeństwie informacji.
6.1.3	Organizacja powinna opracować i wdrożyć proces postępowania z ryzykiem w bezpieczeństwie informacji w celu a) wyboru odpowiednich opcji postępowania z ryzykiem w bezpieczeństwie informacji z uwzględnieniem wyników szacowania ryzyka; b) określeniu wszystkich zabezpieczeń niezbędnych do wdrożenia wybranej(-ych) opcji postępowania z ryzykiem w bezpieczeństwie informacji; UWAGA: Organizacje mogą zaprojektować zabezpieczenia odpowiednie do swoich potrzeb lub wybrać je z dowolnego źródła. c) porównania zabezpieczeń … d) opracowania Deklaracji Stosowania …. e) sformułowaniu planu postępowania z ryzykiem w bezpieczeństwie informacji; oraz f) uzyskania zgodny właścicieli ryzyka na plan postępowania z ryzykiem w bezpieczeństwie informacji i ich akceptacji dla rezydualnych ryzyk w bezpieczeństwie informacji. Organizacja powinna zachować udokumentowane informacje o procesie postępowania z ryzykiem w bezpieczeństwie informacji. UWAGA Proces szacowania ryzyka oraz postępowania z ryzykiem w bezpieczeństwie informacji w Niniejszej Normie Międzynarodowej odpowiada zasadom i wytycznym wprowadzonym przez ISO 31000.
6.2 c)	Organizacja powinna ustanowić cele bezpieczeństwa informacji dla odpowiednich funkcji i szczebli. Cele bezpieczeństwa informacji powinny:… c) uwzględniać mające zastosowanie wymagania bezpieczeństwa informacji, wyniki szacowania ryzyka i postępowania z ryzykiem;
8.2	Organizacja powinna szacować ryzyko w bezpieczeństwie informacji w zaplanowanych odstępach czasu lub wtedy, gdy proponowane jest wprowadzenie istotnych zmian, a także wtedy, gdy występują istotne zmiany z uwzględnieniem kryteriów określonych w 6.1.2 a).
8.3	Organizacja powinna wdrożyć plan postępowania z ryzykiem w bezpieczeństwie informacji.
9.3 e)	Przegląd zarządzania powinien uwzględniać:… e) wyniki szacowania ryzyka i stanów planów postępowania z ryzykiem;

Źródło: opracowanie własne na podstawie [14]

5.2 PROCES ZARZĄDZANIA RYZYKIEM W OBSZARZE BEZPIECZEŃSTWA INFORMACJI

Każda jednostka gospodarcza bądź działalność biznesowa narażone są na występowanie ryzyka, które stwarzają niebezpieczeństwa związane z realizacją jej celów. Najogólniej pod pojęciem ryzyka rozumie się prawdopodobieństwo wystąpienia zdarzenia, które w negatywny sposób wpływa na urzeczywistnienie założonych celów. Źródeł ryzyka należy poszukiwać zarówno we wewnątrz jednostki, jak również w otoczeniu działania organizacji. Biorąc pod uwagę, iż ryzyko charakteryzuje pewnego rodzaju nieograniczoność należy skutecznie nim zarządzać. Celem zarządzania ryzykiem jest identyfikacja potencjalnych zdarzeń, które mogą oddziaływać na jednostkę i realizację jej celów oraz utrzymanie ryzyka na ustalonym (racjonalnym) poziomie. Wobec powyższego, zarządzanie ryzykiem jest: procesem, który [2]:

- zachodzi w obrębie całego przedsiębiorstwa;
- realizowany przez ludzi na każdym szczeblu organizacji;
- umożliwia identyfikację potencjalnych zagrożeń oraz utrzymywanie ryzyka w określonych granicach;
- pozwala zapewnić rozsądny poziom pewności kierownictwu i zarządowi przedsiębiorstwa;
- skierowany jest na osiąganie celów w jednej lub kilku nakładających się na siebie kategoriach.



Rys. 5.3 Etapy zarządzania ryzykiem

Źródło: [15]

Proces zarządzania ryzykiem składa się z ośmiu zasadniczych etapów, które tworzą zamkniętą pętlę (rys. 5.3) [19]

Jak przedstawiono na rysunku 5.3 dla działań szacowania ryzyka oraz postępowania z ryzykiem, proces zarządzania ryzykiem w bezpieczeństwie informacji może być iteracyjny. Podejście iteracyjne może polegać na zwiększaniu szczegółów w każdej iteracji. Iteracyjne podejście pozwala na zapewnienie równowagi pomiędzy minimalizowaniem nakładu czasu i wysiłku na identyfikowanie zabezpieczeń, a pewnością odpowiedniego oszacowania dużego ryzyka.

Zarządzanie ryzykiem rozpoczyna się od ustanowienia kontekstu, a następnie szacowane jest ryzyko. w sytuacji, gdy w jego wyniku uzyska się niezbędne informacje do wskazania właściwych zabezpieczeń (redukujących ryzyko do poziomu akceptowalnego)zadanie jest zakończone i przechodzi się do postępowania z ryzykiem. Jeżeli zaś informacje okażą się niewystarczające należy przeprowadzić kolejną iteracje szacowania ryzyka w zmienionym kontekście (np. kryteriów oceny ryzyka, kryteriów akceptacji ryzyka lub kryteriów skutków) – punkt decyzyjny 1.

Podkreślić należy także, że postępowanie z ryzykiem może nie doprowadzić do obniżenia ryzyka do poziomu akceptowalnego. Wówczas, należy przeprowadzić następna iteracje szacowania ryzyka przy zmienionych parametrach kontekstu ryzyka i dopiero po tej iteracji następuje kolejne postępowanie z ryzykiem – punkt decyzyjny 2 [15].

Zgodnie z normą ISO 27001, w ramach systemu zarządzania bezpieczeństwem informacji (SZBI) ustalanie oczekiwań wobec zarządzania ryzykiem, ocena ryzyka, planowanie, łagodzenie bądź akceptacja ryzyka stanowią elementy fazy „*Planuj*" cyklu PDCA. Faza „*Wykonuj*" tego cyklu koncentruje się na wdrażaniu działań i środków sterowania bezpieczeństwem informacji, prowadzących do redukcji ryzyka do akceptowalnego poziomu, zgodnie z przyjętym planem. W fazie „*Sprawdzaj*" kierownictwo określa wymagania w kwestii przeglądów postępowania z ryzykiem, uwzględniając incydenty związane z naruszaniem bezpieczeństwa informacji oraz zmian w otoczeniu. Faza „*Działaj*" obejmuje realizację wszystkich niezbędnych działań związanych z procesem zarządzania ryzykiem w bezpieczeństwie informacji [15, 20]. W tabeli 5.2 usystematyzowano działania w zakresie zarządzanie bezpieczeństwem informacji odnoszące się do procesu SZBI

Tabela 5.2 Zastosowanie modelu PDCA w procesie zarządzania ryzykiem w bezpieczeństwie informacji

Proces SZBI	Proces zarządzania ryzykiem w bezpieczeństwie informacji
Planuj	Ustanawianie kontekstu Szacowanie ryzyka Opracowanie planu postępowania z ryzykiem Akceptowanie ryzyka
Wykonuj	Wdrożenie planu postępowania z ryzykiem
Sprawdzaj	Ciągłe monitorowanie i przegląd ryzyka
Działań	Utrzymanie i doskonalenie procesu zarządzania ryzykiem w bezpieczeństwie informacji

Źródło: opracowanie własne [15]

W kolejnych podrozdziałach omówiono wszystkie osiem etapów zarządzania ryzykiem w bezpieczeństwie informacji.

5.2.1 Ustanawianie kontekstu

Pierwszy etap zarządzania ryzyka wiąże się ustanowieniem kontekstu strategicznego, organizacyjnego oraz związanego z ryzykiem. Przez kontekst działalności należy rozumieć zestaw czynników zewnętrznych i wewnętrznych wpływających na funkcjonowanie przedsiębiorstwa, jego cele oraz sposoby ich realizacji. Kontekst zewnętrzny tworzą m.in. czynniki: kulturowe, społeczne, polityczne, prawne, finansowe, technologiczne, a także ekonomiczne i środowiskowe. Poza tym przedsiębiorstwa powinny uwzględniać również relacje oraz oczekiwania wszystkich interesariuszy. Z kolei kontekst wewnętrzny obejmuje m.in.: strukturę organizacyjną, podział zadań, strategie i cele przedsiębiorstwa, potencjał organizacji (techniczny, ludzie, zasoby, wiedza, itp.), system informacyjny, relacje z wewnętrznymi interesariuszami, kulturę organizacyjną, stosowane normy i standardy oraz kontrakty biznesowe [12]. Kontekst działalności stanowi podstawę do ustalenia kryteriów szkód, oceny wpływu zagrożeń (ryzyka), a także kryteriów akceptowania ryzyka. Podkreślić należy, iż przyjęte założenia dotyczące całego procesu zarządzania ryzykiem powinny gwarantować powtarzalność oraz porównywalność wyników, uwzględniać stopień wrażliwości informacji oraz prawdopodobieństwo wystąpienia zdarzeń kryzysowych (zagrożeń) i konsekwencji ich zmaterializowania się (skutków) [19].

5.2.2 Identyfikacja ryzyka

Identyfikacja ryzyk polega na określeniu przyczyn i sposobu materializacji niepożądanych incydentów. Obejmuje ustalenie zasobów (aktywów) informacyjnych, zagrożeń i źródeł ich powstawania, podatności oraz potencjalnych skutków i strat zidentyfikowanych incydentów.

Dokonując inwentaryzacji aktywów informacyjnych należy pamiętać, że na zasoby składa się to wszystko, co posiada dla instytucji określoną wartość. Wyróżnić można następujące kategorie aktywów: informacyjne (dokumenty, bazy danych), fizyczne (sprzęt komputerowy, budynki, urządzenia komunikacyjne), oprogramowanie (systemy operacyjne, aplikacje); personel (wiedza, doświadczenie, umiejętności). Poza tym aktywa stanowią również dobra niematerialne takie jak: reputacja, czy wizerunek organizacji [13]. Podczas klasyfikacji zasobów istotne jest wskazanie, kto jest właścicielem (gestorem) danego aktywu informacyjnego. Jest to osoba odpowiedzialna za sterowanie wytwarzaniem, rozwój, utrzymanie, korzystanie oraz bezpieczeństwo zasobów.

Następnie, dla każdego zidentyfikowanego zasobu należy określić potencjalne zagrożenia. Zgodnie z normą PN-ISO/IEC 27005:2014 zagrożenia można podzielić na pochodzenia środowiskowego (np. trzęsienie ziemi, piorun, powódź, pożar) oraz ludzkiego (umyślne i przypadkowe).

W dalszej kolejności zagrożeniom tym przypisuje się podatności. Są to wszelkiego rodzaju słabości bądź luki w systemie przetwarzania danych, które umożliwiają jego uszkodzenie lub zakłócenie działalności użytkownika. Podatności dotyczyć mogą: organizacji, procesów i procedur, zarządzania, personelu, środowiska naturalnego, informacji o konfiguracji systemu, a także sprzętu, oprogramowania oraz rozwiązań łączności [20].

5.2.3 Analiza (estymacja) ryzyka

Istota analizy ryzyka sprowadza się do oszacowania wielkości prawdopodobieństwa oraz skutków (strat) zaistnienia uprzednio zidentyfikowanych ryzyk.

Podczas oceny prawdopodobieństwa urzeczywistnienia się określonych zagrożeń należy rozważyć m.in. [19, 20]:

- motywację źródła zagrożenia;
- możliwości dostępne dla ewentualnych atakujących;
- akcyjność i wrażliwość zasobów;
- lokalizację prowadzenia działalności gospodarczej (np. bliskie sąsiedztwo zakładów chemicznych, naftowych);
- możliwość występowania ekstremalnych warunków atmosferycznych;
- czynniki determinujące powstawanie błędów i pomyłek.

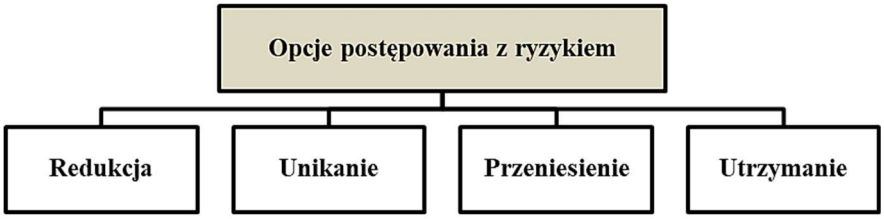
Dokonując natomiast oceny wielkości skutków uwzględnić należy zarówno te bezpośrednie, jak i pośrednie. Do skutków bezpośrednich zaliczyć można m.in.: koszty odtworzenia utraconych aktywów bądź nabycia, konfiguracji i instalacji nowego zasobu, a także wszelkie straty poniesione w wyniku naruszenia bezpieczeństwa, w tym ponoszone w wyniku zawieszenia świadczenia usług. Natomiast skutki pośrednie mogą mieć wymiar pieniężny (np. koszty wymiany lub naprawy aktywów) bądź niepieniężny (np. naruszenie obowiązków ustawowych i wykonawczych lub kodeksu postępowania) [20].

5.2.4 Ocena ryzyka

Ocena ryzyka pozwala odpowiedzieć na pytanie: czy dane ryzyko jest akceptowalne ? Etap ten polega na porównaniu wartości oszacowanego ryzyka z przyjętymi kryteriami oceny, co umożliwia uszeregowanie ryzyk oraz określenie priorytetów postępowania z nim.

5.2.5 Postępowanie z ryzykiem

Kolejnym etapem zarządzania ryzykiem, po jego oszacowaniu i ocenie poprzez kryteria akceptowalności jest postępowanie z ryzykiem. Do powszechnie stosowanych strategii reagowania na ryzyka zalicza się: redukcję ryzyka, jego unikanie, przeniesienie bądź utrzymanie (rys. 5.4) [19].



Rys. 5.4 Działania postępowania z ryzykiem
Źródło: opracowanie na podstawie [15]

Redukcja. Strategia ta oznacza obniżenie ryzyka do poziomu akceptowalnego (tzw. ryzyko szczątkowe) poprzez wybór oraz zastosowanie odpowiednich zabezpieczeń. Najogólniej zabezpieczenia te można podzielić na fizyczne, organizacyjne, osobowe, prawne oraz teleinformatyczne. W sytuacji, gdy przedsiębiorstwo zdecyduje się na wdrożenie u siebie systemu zarządzania bezpieczeństwem informacji w oparciu o normę PN-ISO/IEC 27001:2014, może skorzystać z propozycji zabezpieczeń zawartych w załączniku A ww. normy. Istotną kwestią w zakresie wdrażania zabezpieczeń jest uwzględnienie ograniczeń finansowych, czasowych, organizacyjnych oraz technicznych.
Unikanie. Unikanie ryzyka zakłada konieczność podjęcia działań mających na celu zmodyfikowanie bądź zaprzestanie aktywności powodującej powstawanie określonych zagrożeń.
Przeniesienie. W praktyce transfer ryzyka polega na ubezpieczeniu się od jakiegoś zagrożenia bądź przekazaniu odpowiedzialności za określone działania na podmioty zewnętrzne.
Utrzymanie. Utrzymanie czyli akceptacja ryzyka jest formą postępowania z ryzykiem, która wiąże się z podjęciem świadomej decyzji osób związanych z zarządzeniem ryzykiem w zakresie odmowy zastosowania zabezpieczeń minimalizujących ryzyko oraz przyjęcia konsekwencji wynikających z ewentualnych sytuacji kryzysowych. Zgodnie z normą PN-ISO/IEC 27001:2014 akceptacja ryzyk musi odbywać się w sposób świadomy i obiektywny, a ryzyka spełniać warunki wyznaczone w polityce organizacji oraz kryteria akceptowalności ryzyka.
Reasumując należy dodać, iż sposób postępowania z ryzykiem powinien zostać jasno i wyraźnie wyartykułowany, a także właściwie opisany w dokumencie zwanym *planem postępowania z ryzykiem* [4].

5.2.6 Akceptacja ryzyka

Kolejnym krokiem zarządzania ryzykiem jest akceptacja ryzyka pozostającego po wdrożeniu mechanizmów ochronnych zwanego ryzykiem szczątkowym (rezydualnym). Jest to ryzyko, którego nie można całkowicie wyeliminować. Istotną kwestią w tym zakresie jest ustalenie przez kierownictwo kryteriów akceptacji ryzyka oraz jego poziomu.

5.2.7 Informowanie o ryzyku

Podstawowym etapem procesu zarządzania ryzykiem jest także informowanie uczestników tego procesu o bieżącym statusie ryzyka. Organizacja, budując system zarządzania ryzykiem zobligowana jest do określenia mechanizmów informacyjnych, które zapewnią dostępność informacji właściwym osobom, w określonym czasie oraz pozwolą na wymianę informacji oraz konsultacje z poszczególnymi uczestnikami procesu zarządzania ryzykiem. Istotą informowania ryzyku jest zapewnienie, że każdy właściciel ryzyka świadomy jest swojej roli oraz zakresu obowiązków i odpowiedzialności [19].

5.2.8 Monitorowanie oraz przegląd ryzyka

Istotne znaczenie w procesie zarządzania ryzkiem przypisuje się monitorowaniu oraz przeglądowi ryzyk. Etap ten ma za zadanie odpowiedzieć na pytanie czy system zarządzania ryzykiem spełnia założone cele, czy polityki i procedury ustanowione w jego ramach są nadal aktualne, odpowiednie i wydajne. Ponadto, monitorowanie ryzyk ma na celu zapewnienie, że wszystkie nowe ryzyka zostaną w odpowiednim czasie zidentyfikowane oraz ustanowione wobec nich priorytety działania. Monitorowanie oraz przegląd ryzyk powinien być prowadzony w kontekście nowych aktywów, zagrożeń i podatności, a także incydentów związanych z naruszeniem bezpieczeństwa informacji. W sytuacji odnotowania jakichkolwiek zmian czynników wpływających na ryzyko, należy dokonać ponownego przeglądu ryzyk oraz zaktualizowania ich wartości, jeżeli jest to uzasadnione [8, 9].

PODSUMOWANIE

Informacje zaliczane są obecnie do jednych z najważniejszych aktywów współczesnych organizacji. Niezbędne są one do zachowania konkurencyjnej pozycji na rynku, płynności finansowej, zyskowności oraz pozytywnego wizerunku na rynku. Informacje mogą być wyrażane i przekazywane za pomocą mowy, znaków, obrazu, dźwięku lub w jakikolwiek inny sposób. Ponadto, mogą one zostać także utrwalone i przechowywane w postaci dokumentów papierowych bądź elektronicznych. Zatem, należy podzielić przekonanie, że informacje pozwalają przejąć kontrolę na rynkiem oraz osiągnąć przewagę konkurencyjną. Mając na uwadze różnorodność informacji, jak i ich znaczenie w działalności gospodarczej istotną kwestią jest wdrażanie systemów oraz procedur mających za zadanie zapobiegać utracie bądź niepożądanemu ujawnieniu informacji. Należy jednak pokreślić, iż podstawą w zakresie racjonalnego podejmowania decyzji związanych z praktycznym zabezpieczeniem informacji odgrywa zarządzanie ryzykiem.

Zarządzanie ryzykiem należy rozumieć jako ciągły proces dopasowany do wyzwań organizacji, który swoim zakresem obejmuje: identyfikowanie ryzyka, postępowanie z ryzkiem oraz plan łagodzenia ryzyka. W szczególności proces zarządzania ryzykiem ukierunkowany jest na: [20]

- identyfikację aktualnych zagrożeń;
- kwantyfikowanie tych zagrożeń pod względem możliwych strat (skutków) oraz prawdopodobieństwa ich wystąpienia;
- zdefiniowanie działań zapobiegawczych, redukujących zidentyfikowane ryzyko do poziomu akceptowalnego;
- implementację zaproponowanych rozwiązań naprawczych;
- edukację kierownictwa oraz pozostałego personelu firmy w zakresie ryzyka, a także działań profilaktycznych;
- nadzorowanie oraz kontrolę wyników procesu zarządzania ryzykiem;
- dostosowywanie działań związanych z redukcją ryzyka do bieżących potrzeb organizacji i jej otoczenia (reakcja na zachodzące wydarzenia);
- doskonalenie procesu zarządzania ryzykiem;
- ewidencjonowanie incydentów związanych z bezpieczeństwem informacji, w celu poprawy procesu zarządzania ryzykiem.

Zarządzanie ryzykiem w bezpieczeństwie informacji wymaga odpowiedniego zaplanowania, organizacji kierowania oraz kontrolowania zasobów. Jest to także proces, który wymaga zaangażowania oraz współpracy wszystkich stron przetwarzających informacje w celu osiągnięcia konsensusu w zakresie określenia wymagań oraz wyboru opcji postępowania z ryzykiem. Oprócz tego, istotną rolę w obszarze zarządzania ryzykiem przypisuje się kierownictwu organizacji, które odpowiedzialne jest za kształtowanie oraz wzmacnianie wśród pracowników poczucia świadomości występowania zagrożeń oraz potrzeby przeciwdziałania sytuacjom kryzysowym.

LITERATURA

[1] F. Bień. *Zarządzanie cyklem życia informacji*. Boston: IT Security Review nr 3, 2017.
[2] COSO ERM – *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa.*
[3] J. Janczak, A. Nowak. *Bezpieczeństwo informacyjne Wybrane problemy*. Warszawa: AON, 2013.
[4] T. Kaczmarek. *Ryzyko i zarządzanie ryzykiem Ujęcie interdyscyplinarne*. Warszawa: Difin, 2008.
[5] T. Kifner. *Polityka bezpieczeństwa i ochrony informacji*. Gliwice: Helion, 1999.
[6] J. Łuczak, M. Tyburski. *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*. Poznań: WUE, 2010.
[7] P. Mazurek. *Realizacja szacowania ryzyka w wybranym przedsiębiorstwie*. J. Brdulak, R. Sobczak (red.) Wybrane problemy zarządzania bezpieczeństwem informacji. Warszawa: SGH, 2014.
[8] Ministerstwo Finansów, Zarządzanie ryzykiem. Pobrano z: http://www.mf.gov.pl/c/document_library/get_file?uuid=55094b15-39ee-4364-aa0d-6fc6c8d99a26&groupId=764034 [01.05.2017].
[9] Ministerstwo Finansów, Zarządzanie ryzykiem w sektorze publicznym. Pobrano z:

http://www.mf.gov.pl/c/document_library/get_file?uuid=69a26897-1c59-45a7-9e84-110a92414587&groupId=764034 [01.05.2017].
[10] A. Nowak, W. Scheffs. *Zarządzanie bezpieczeństwem informacyjnym*. Warszawa: AON, 2009.
[11] M. Pałęga. Ocena poziomu zagrożeń bezpieczeństwa informacji za pomocą macierzy ryzyka*. Wybrane zagadnienia dotyczące usprawniania procesów w przedsiębiorstwie.* Pod red. M. Ogórek, T. Bajor Częstochowa: Wydawnictwo WiPiTM Politechniki Częstochowskiej, 2016.
[12] *PN-EN ISO 9001:2015 Systemy zarządzania jakością – Wymagania.* Warszawa: PKN, 2015.
[13] *PN-I-13335-1:1999 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych*. Warszawa: PKN, 1999.
[14] *PN-ISO/IEC 27001:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*. Warszawa: PKN, 2013.
[15] *PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*. Warszawa: PKN, 2013.
[16] T. Polaczek: *Audyt bezpieczeństwa informacji w praktyce*. Gliwice: Helion, 2006.
[17] Rządowe Centrum Bezpieczeństwa. *Ocena ryzyka na potrzeby zarządzania kryzysowego*. *Raport o zagrożeniach bezpieczeństwa narodowego*, Pobrano z: http://rcb.gov.pl/wp-content/uploads/ocenaryzyka.pdf [01.05.2017]
[18] T. Sasor. Ryzyko i polityka bezpieczeństwa w przedsiębiorstwie wirtualnym. *Informatyka i współczesne zarządzanie*. pod red. J. Kisielnicki, J. Grabara, J. Nowak, Katowice: PTI, 2015.
[19] Stróżyk, *Zarządzanie ryzykiem w bezpieczeństwie informacji*, Pobrano z: http://iso27000.pl/app/webroot/uploads/Zarzadzanie_ryzykiem_w_bezpieczenstwie_informacji.pdf [01.05.2017].
[20] F. Wołowski, J. Zawiła-Niedźwiecki. *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny normami polskimi i międzynarodowymi*. Kraków-Warszawa: Edu-Libri, 2012.

Data przesłania artykułu do Redakcji: 10.2017
Data akceptacji artykułu przez Redakcję: 11.2017

ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA INFORMACJI W ŚWIETLE WYMAGAŃ NORMATYWNYCH

Streszczenie: *Zasoby informacyjne, jako jedne z podstawowych aktywów biznesowych przedsiębiorstwa warunkują sukces rynkowy organizacji oraz utrzymanie jej konkurencyjności. Wobec powyższego istnieje potrzeba zbudowania w organizacji odpowiedniego systemu gwarantującego ochronę informacji przed zagrożeniami. Podstawowym elementem w systemie bezpieczeństwa informacji w przedsiębiorstwie jest zarządzanie ryzykiem. W niniejszym artykule opisano podejście do zarządzania ryzykiem bezpieczeństwa informacji z wykorzystaniem norm PN-ISO/IEC 27001:2014 oraz PN-ISO/IEC 27005:2014.*

Słowa kluczowe: *bezpieczeństwo informacji, ryzyko, zarządzanie ryzykiem, norma PN-ISO/IEC 27001:2014, norma PN-ISO/IEC 27005:2014*

INFORMATION SECURITY RISK MANAGEMENT IN LIGHT OF REGULATORY REQUIREMENTS

Abstract: *Information resources, as one of the basic assets of enterprises determine a market success of organization and keeping its competitiveness. Therefore, it's necessary to construct appropriate system in organization, which guarantee information security before threats. The fundamental element of the information security system in the enterprise is the risk management. In this article describes the way of approach to management risk of information security in accordance with PN-ISO/IEC 27001:2014 and PN-ISO/IEC 27005:2014 norms.*

Key words*: information security, risk, risk management, PN-ISO/IEC 27001:2014 norm, PN-ISO/IEC 27005:2014*

dr inż. Michał Pałęga
Politechnika Częstochowska
Wydział Inżynierii Produkcji
i Technologii Materiałów
Instytut Przeróbki Plastycznej
i Inżynierii Bezpieczeństwa
Al. Armii Krajowej 19
42-201 Częstochowa, Polska
e-mail: palega.michal@wip.pcz.pl