KONCEPCJA KONSOLIDACJI SYSTEMÓW ZARZĄDZANIA JAKO ELEMENTÓW KONTROLI ZARZĄDCZEJ NA PRZYKŁADZIE URZĘDU KONTROLI SKARBOWEJ W OPOLU

Ewa KULIŃSKA, Agnieszka DORNFELD

Streszczenie: W publikacji wskazano na możliwość integracji trzech systemów stosowanych standardowo w Urzędach Kontroli Skarbowej (UKS). Badania dotyczą Systemu Zarządzania Bezpieczeństwem Informacji, Kontroli Zarządczej oraz Zarzadzania Kryzysowego. Wskazano wspólne obszary realizowane we wszystkich wymienionych systemach oraz oszczędności wynikające z ich integracji

Słowa kluczowe: kontrola zarządcza, System Zarządzania Bezpieczeństwem Informacji, zarządzanie ryzykiem, identyfikacja i analiza ryzyka.

1. Wprowadzenie

Celem publikacji jest pokazanie koncepcji dokonania konsolidacji 3 systemów zarządzania, takich jak kontrola zarządcza, system zarządzania bezpieczeństwem informacji oraz zarządzanie kryzysowe. Dokonana konsolidacja zbudowana jest na podwalinach kontroli zarządczej będącej punktem wyjścia omawianych systemów, ponieważ kontrola zarządcza odnosi się do całego procesu organizacji i zarządzania jednostką, w związku z powyższym zawiera w sobie wszystkie elementy tamtych systemów. Kolejne systemy powinny stanowić tylko doprecyzowanie poszczególnych wskazanych celów kontroli zarządczej.

2. Istota integrowanych systemów

W art. 68 ust. 1. określono definicję kontroli zarządczej, przez którą rozumiemy ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Celem kontroli zarządczej jest zapewnienie:

1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi,
2) skuteczności i efektywności działania,
3) wiarygodności sprawozdań,
4) ochrony zasobów,
5) przestrzegania i promowania zasad etycznego postępowania,
6) efektywności i skuteczności przepływu informacji,
7) zarządzania ryzykiem. [1]

Odnosząc się do elementów celów kontroli zarządczej, jako głównego systemu zarządzania w oparciu, o który powinny być zbudowane pozostałe systemy należy wskazać, że cele są bardzo szczegółowo sprecyzowane.

Kontrola zarządcza – stanowi ogół działań (procedur, instrukcji, zasad i mechanizmów), które wspomagają zarządzanie, zmierzając do uzyskania pewności, że cele jednostki, poprzez maksymalizację szans i minimalizację zagrożeń zostaną osiągnięte.

Według E. Nowaka kontrola zarządcza definiowana jest jako proces sprawdzania, czy przebieg działalności jednostki sektora finansów publicznych jest zgodny z ustaleniami zawartymi w planie działalności oraz czy jednostka osiąga założone cele [7]. Kontrola zarządcza jest elementem systemu sterowania działalnością jednostki, który obejmuje

monitorowanie przebiegu działalności oraz stanowi podstawę do podejmowania działań korygujących, które powinny zapobiec pojawieniu się nieprawidłowości w przyszłości. Według B.R. Kuca kontrola w ujęciu kierowniczej funkcji zarządzania określana jest jako zbiór czynności, których istotą jest pozyskiwanie informacji, a celem - wykorzystanie tych informacji do korekty procesów lub zachowań ludzi poddawanych kontroli [5]. Kontrola zarządcza w jednostkach sektora finansów publicznych obejmuje pięć grup zagadnień, tj. środowisko wewnętrzne, cele i zarządzanie ryzykiem, mechanizmy kontroli, informację i komunikację, monitorowanie i ocenę. Katalog celów kontroli zarządczej ma charakter otwarty i wymaga określenia przez kierownika jednostki sektora finansów publicznych celów dodatkowych jednostki, uwzględniających specyfikę, przedmiot działalności i warunki funkcjonowania kierowanej przez niego jednostki [6].

System Zarządzania Bezpieczeństwem Informacji (SZBI) to część systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanowienia, wdrożenia, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji. SZBI zawiera strukturę organizacyjną polityki, zakres odpowiedzialności, zasady, procedury, procesy i zasoby według Polskiej Normy PN-ISO/IEC 27001: 2007 [4].

Etap pierwszy – Ustanowienie SZBI w Urzędzie

W celu ustanowienia SZBI podjęte zostały następujące działania:

1) Zdefiniowano zakres i granice SZBI poprzez dokonanie analizy celów i ich zabezpieczeń, uzasadniając każde wyłączenie – zgodnie z załącznikiem A do Polskiej Normy ISO/IEC 27001:2007.
2) Opracowano i zatwierdzono PBI, która zawiera:
   a) definicję bezpieczeństwa informacji,
   b) ogólne zasady i ramy działania dotyczące bezpieczeństwa informacji, które mają szczególne znaczenie dla Urzędu,
   c) definicję ogólnych i szczegółowych obowiązków nałożonych na struktury zarządzające bezpieczeństwem, dokonano podziału ról i zadań w procesie bezpieczeństwa informacji,
   d) podejście do zarządzania ryzykiem zgodnie z etapami zarządzania ryzykiem.
3) Określenie ryzyka (w ramach rejestru czynników ryzyka na dany rok określanych przez zespół ds. zarządzania ryzykiem w Urzędzie).
4) Zakres realizacji SZBI w Urzędzie.

Etap drugi – Wdrożenie i eksploatacja SZBI w Urzędzie

W celu wdrożenia i eksploatacji SZBI podjęte zostały następujące działania polegające na:

1) Sformułowaniu i wdrożeniu planu postępowania z czynnikami ryzyka, zgodnie z etapami zarządzania ryzykiem, określonymi w niniejszym dokumencie oraz w „Księdze Kontroli Zarządczej i zarządzania ryzykiem w Urzędzie".
2) Wdrożeniu zabezpieczeń, które pozwolą osiągnąć cele stosowania zabezpieczeń, wdrożeniu programu szkoleń.

Etap trzeci – Monitorowanie i przegląd SZBI w Urzędzie

Monitoring i przegląd SZBI realizowany jest poprzez:

1) Opracowanie procedur monitorowania i przeglądu SZBI,
2) Wykonywanie regularnych przeglądów skuteczności SZBI,
3) Wykonywanie pomiarów skuteczności zabezpieczeń,
4) Wykonywanie przeglądów szacowania ryzyka w zaplanowanych odstępach czasu,
5) Modernizacja systemów teleinformatycznych,
6) Przeprowadzanie wewnętrznych audytów SZBI.

Etap czwarty – Utrzymanie i doskonalenie SZBI w Urzędzie

W celu utrzymania i doskonalenia SZBI należy:

1) Wdrażać zidentyfikowane udoskonalenia, w celu osiągnięcia jak najlepszego poziomu zabezpieczeń podejmować odpowiednie działania korygujące lub zapobiegawcze.
2) Zapewnić, że udoskonalenia w ramach systemu osiągają zamierzone cele.
3) Zapewniać, że wdrożony System Zarządzania Bezpieczeństwem Informacji gwarantuje adekwatne do oszacowanego poziomu ryzyka zabezpieczenia techniczne i organizacyjne w obszarach określonych na podstawie załącznika A do Polskiej Normy PN-ISO/IEC 27001:2007.

W Urzędzie zidentyfikowano następujące obszary stosowania zabezpieczeń wraz z określeniem dla nich celu stosowania zabezpieczeń:

Obszar I– Polityka Bezpieczeństwa Informacji – Cel: zapewnienie funkcjonowania i obowiązywania w Urzędzie dokumentu PBI zgodnego z przepisami prawa oraz regulacjami wewnętrznymi.

Obszar II– Organizacja bezpieczeństwa informacji – Cel: zapewnienie efektywnego zarządzania bezpieczeństwem informacji wewnątrz Urzędu.

Obszar III– Zarządzanie aktywami – Cel: zapewnienie efektywnego zarządzania bezpieczeństwem informacji wewnątrz Urzędu.

Obszar IV– Bezpieczeństwo zasobów ludzkich – Cel: przeciwdziałanie zagrożeniom związanym z bezpieczeństwem informacji ze strony pracowników Urzędu oraz innych osób, w tym wykonawców

Obszar V– Bezpieczeństwo fizyczne i środowiskowe – Cel: zabezpieczenie informacji przetwarzanych w Urzędzie przed nieautoryzowanym dostępem oraz przed ich uszkodzeniem lub zniszczeniem.

Obszar VI –Zarządzanie systemami i sieciami – Cel: zapewnienie prawidłowej i bezpiecznej eksploatacji środków przetwarzania informacji.

Obszar VII – Kontrola dostępu – Cel: ochrona przed nieautoryzowanym dostępem do informacji.

Obszar VIII – Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych – Cel: zapewnienie, że wszystkie systemy spełniają wymagania bezpieczeństwa informacji, a wymagania bezpieczeństwa dla systemów informatycznych są ich istotnym elementem.

Obszar IX – Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji – Cel: Zapewnienie spójnego i jednolitego podejścia do zarządzania incydentami związanymi z bezpieczeństwem informacji.

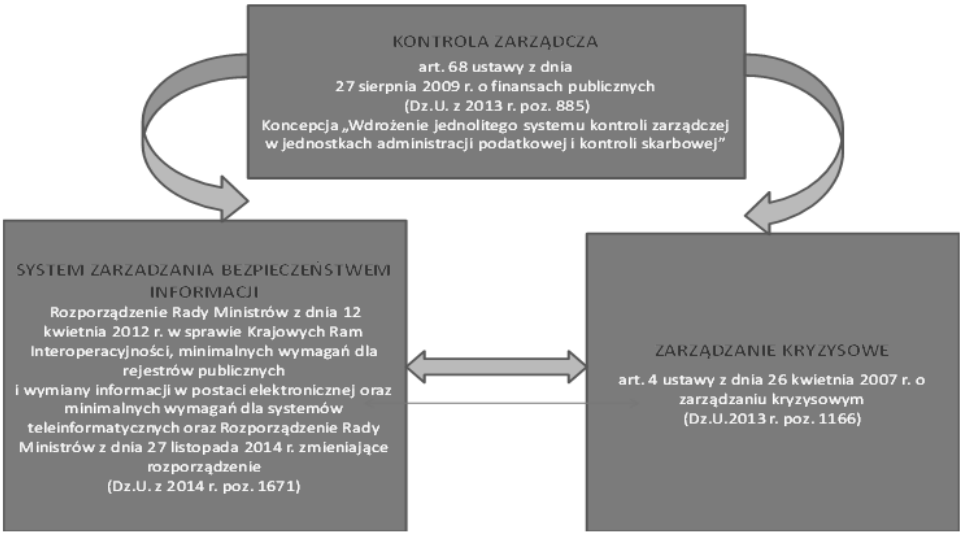
Obszar X – Zarządzanie ciągłością działania – Cel: przeciwdziałanie przerwom w działalności Urzędu oraz ochrona krytycznych procesów przetwarzania informacji.

Obszar XI – Zgodność – Cel: zapewnienie zgodności z przepisami prawa i regulacjami wewnętrznymi.

Obowiązek wdrożenia SZBI wynika z Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoparacyjności oraz minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych [2].

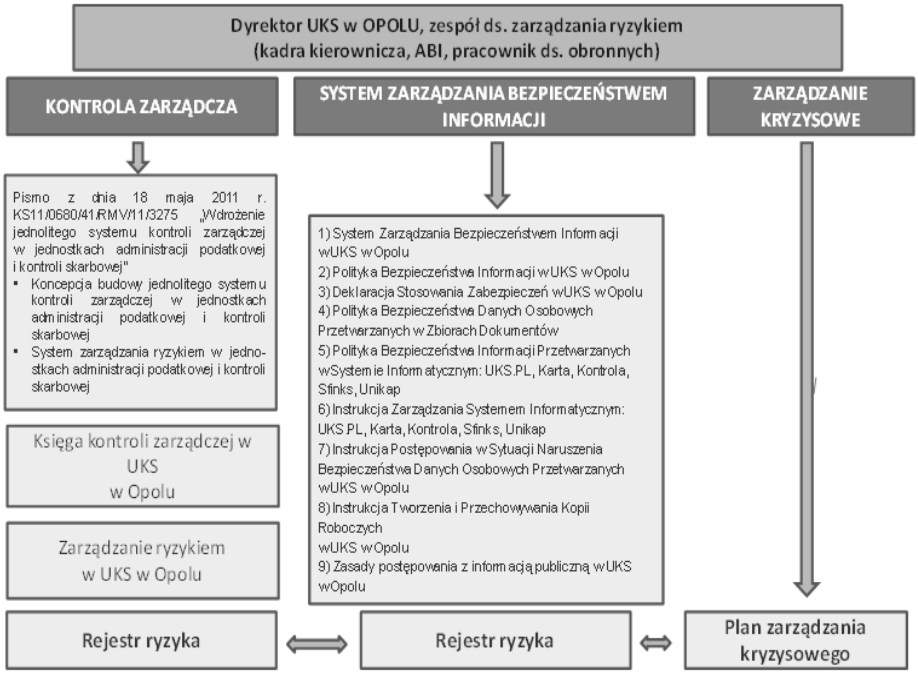
Zarządzanie kryzysowe (ZK) regulują dwie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Jest to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej [3].

Systemy zarządzania w UKS w Opolu i podstawy prawne ich funkcjonowania przedstawiono na rys.1.



Rys.1. Systemy zarządzania w UKS w Opolu i podstawy prawne ich funkcjonowania
Źródło: opracowanie własne

Zestawienie dokumentów regulujących trzy integrowane koncepcje przedstawia rys. 2.

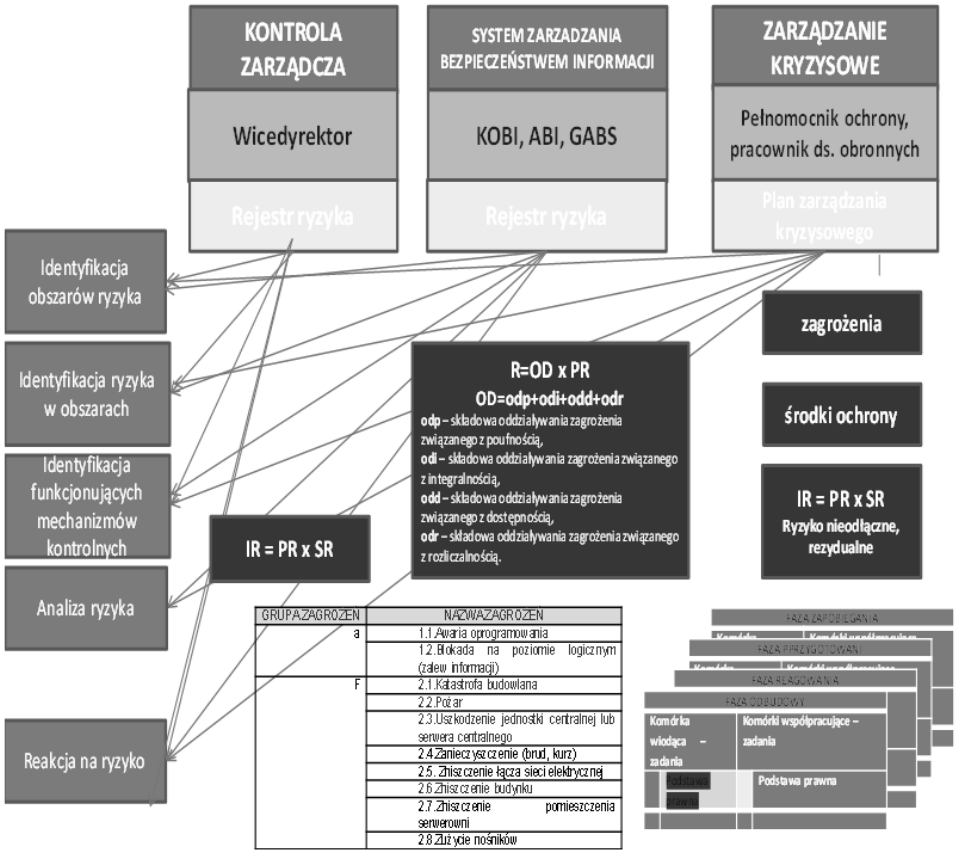


Rys. 2. Systemy zarządzania funkcjonujące w UKS w Opolu i dokumenty je regulujące
Źródło: opracowanie własne

3. Integracja trzech koncepcji

Analizując system SZBI, można na nim wskazać elementy powtarzające się w systemie KZ. A skoro występują one również w zarządzaniu kryzysowym, postawiono tezę, że możliwa jest ich integracja.

Na rysunku 3 przedstawiono elementy wspólne i oddzielne w integrowanych systemach zarządzania. W szczególności dotyczą one identyfikacji i analizy ryzyka.



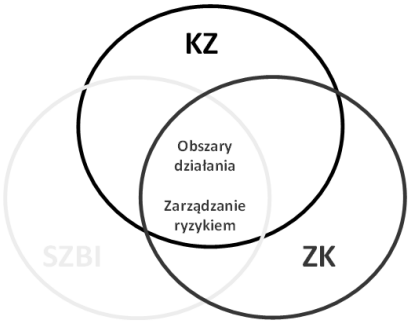
Rys. 3. Elementy wspólne i oddzielne w integrowanych systemach zarządzania
Źródło: opracowanie własne

Podstawowe założenia integracji, to przede wszystkim:

- w wymienionych systemach powtarzają się niektóre obszary działania, funkcjonujące już w rejestrze kontroli zarządczej,
- skoro występuje powtarzalność obszarów działania, to również powtarzają się czynniki ryzyka w ramach tych obszarów (ta sama identyfikacja czynników ryzyka),
- stosujemy jednolite mechanizmy kontrolne we wszystkich trzech systemach zarządzania,

- skoro występują te same obszary ryzyka, taka sama musi być ich analiza do wszystkich czynników ryzyka w systemach (niejednolita metoda przyjęta do analizy spowoduje, że te same czynniki ryzyka mogą otrzymać różną wartość punktową w każdym z systemów, co z kolei może przełożyć się na różny ich zabezpieczenie),
- przy takiej samej metodzie prowadzenia analizy, czynniki ryzyka muszą otrzymać taką samą wartość punktową (we wszystkich 3 systemach zarządzania).

Zarządzanie ryzykiem jest procesem wspólnym dla trzech integrowanych systemów - rys. 4.



Rys. 4. Wspólne obszary w systemie zarzadzania
Źródło: opracowanie własne

W obszarze bezpieczeństwa informacji w Urzędzie zarządzanie ryzykiem odbywa się na zasadach określonych w „Księdze Kontroli Zarządczej i Zarządzania Ryzykiem w Urzędzie Kontroli Skarbowej w Opolu". W obszarze bezpieczeństwa informacji, zarządzanie ryzykiem koncentruje się na zapobieganiu zdarzeniom, które mogą mieć niekorzystne następstwa związane z utratą podstawowych cech informacji tj. poufności, integralności, dostępności i rozliczalności (w przypadku danych osobowych).

Skuteczny system zarządzania ryzykiem daje wymierne korzyści w postaci większej koncentracji kierownictwa na zagadnieniach o kluczowym znaczeniu dla organizacji, obniżeniu czasu reakcji na sytuacje kryzysowe, eliminacji niespodzianek, większą koncentrację wewnętrzną na podejmowaniu prawidłowych działań w prawidłowy sposób, zwiększa prawdopodobieństwo osiągnięcia celów oraz prawdopodobieństwo realizacji inicjatyw na rzecz zmian, redukuje ogólne koszty kontroli, a co najważniejsze podejście do ryzyka i podejmowania decyzji odbywa się w oparciu o większą ilość informacji [6].

Reasumując, zarządzanie ryzykiem powinno mieć charakter planowy i celowy, tzn. działania w tym kierunku nie powinny być podejmowane bardziej lub mniej sporadycznie, lecz systematycznie i długofalowo. Konieczna jest także integracja tych przedsięwzięć w ramach kompleksowego systemu zarządzania organizacją [7].

Proces zarządzania ryzykiem jest procesem identyfikacji, oceny i przeciwdziałania występowaniu czynników ryzyka. Celem procesu zarządzania ryzykiem jest ograniczenie ryzyka do akceptowalnego poziomu poprzez podnoszenie świadomości istnienia czynników ryzyka, usprawnienie procesu planowania, zwiększenie prawdopodobieństwa realizacji zadań i osiągania celów oraz zapewnienie odpowiednich mechanizmów KZ.

Zarządzanie ryzykiem jest procesem permanentnym, który przeprowadzany jest według następujących etapów:

1) etap pierwszy – kategoryzacja czynników ryzyka (identyfikacja czynników ryzyka),
2) etap drugi – analiza czynników ryzyka,
3) etap trzeci – postępowanie z ryzykiem (reakcja na ryzyko).

Etap pierwszy – Kategoryzacja czynników ryzyka

Należy przeprowadzić identyfikację posiadanych informacji, bez względu na formę ich przetwarzania i przypisać je do jednej z trzech grup informacji, a następnie określić zagrożenia mające wpływ na bezpieczeństwo informacji.

W tab. 1. zamieszczono dane dotyczące bazy zagrożeń, natomiast w tab. 2 przedstawiono bazy podatności na czynniki ryzyka, wykorzystywane do kategoryzacji czynników ryzyka celem ujęcia ich w rejestrze ryzyka Urzędu na dany rok.

Tab. 1. Zestawienie zidentyfikowanych zagrożeń

GRUPA ZAGROŻEŃ	NAZWA ZAGROŻEŃ
1. Awaria techniczna	1.1. Awaria oprogramowania
	1.2. Blokada na poziomie logicznym (zalew informacji)
2. Fizyczne zniszczenie	2.1. Katastrofa budowlana
	2.2. Pożar
	2.3. Uszkodzenie jednostki centralnej lub serwera centralnego
	2.4. Zanieczyszczenie (brud, kurz)
	2.5. Zniszczenie łącza sieci elektrycznej
	2.6. Zniszczenie budynku
	2.7. Zniszczenie pomieszczenia serwerowni
	2.8. Zużycie nośników
3. Naruszenie bezpieczeństwa informacji	3.1. Kradzież
	3.2. Nieuprawnione odzyskanie skasowanych danych
	3.3. Podglądanie
	3.4. Podsłuch
	3.5. Szpiegostwo
4. Naruszenie funkcjonalności	4.1. Błąd administratora
	4.2. Błąd programisty
	4.3. Błąd projektanta lub instalatora systemu teleinformatycznego
	4.4. Błąd użytkownika systemu
	4.5. Brak rozliczalności działań administratora
	4.6. Włamanie
	4.7. Skasowanie zawartości logów
5. Zdarzenie losowe	5.1. Huragan
	5.2. Ładunki elektrostatyczne
	5.3. Nieodpowiednia temperatura
	5.4. Trzęsienie ziemi
	5.5. Nieodpowiednia wilgotność
	5.6. Woda (powódź, zalanie)
	5.7. Wyładowanie atmosferyczne
6. Nieuprawnione działanie	6.1. Socjotechnika „social engineering”
	6.2. Manipulacje danymi
	6.3. Maskarada tożsamości
	6.4. Naruszenie bezpieczeństwa
	6.5. Nieautoryzowany dostęp – fizyczny

	6.6. Nieautoryzowany dostęp – logiczny
	6.7. Nieuprawnione użycie nośników
	6.8. Atak terrorystyczny
	6.9. „Zero-day exploit”
	6.10. Złośliwe oprogramowanie
7. Utrata podstawowych usług	7.1. Awaria klimatyzacji
	7.2. Awarie sieci zasilającej lub/oraz systemów zasilających
	7.3. Uszkodzenie sieci komputerowej
	7.4. Personelu
8. Zakłócenia spowodowane promieniowaniem	8.1. Promieniowanie elektromagnetyczne
	8.2. Promieniowanie termiczne

Źródło: Dane uzyskane podczas badań prowadzonych w UKS w Opolu

Tab. 2. Zestawienie podatności na czynniki ryzyka

GRUPA PODATNOŚCI	NAZWA PODATNOŚCI
1. Dokumenty	1.1. Brak aktualizacji planów zachowania ciągłości działania
	1.2. Brak dokumentacji systemów
	1.3. Brak dokumentacji wymaganej prawem
	1.4. Brak dokumentów polityki bezpieczeństwa informacji
	1.5. Brak dzienników operatorów
	1.6. Brak kontroli zmian
	1.7. Brak listy osób upoważnionych do dostępu do określonej informacji
	1.8. Brak opracowanych planów ciągłości działania
	1.9. Brak Administratora Bezpieczeństwa informacji / Administratora Bezpieczeństwa
	1.10. Brak stosowania zasad czystego biurka i ekranu
	1.11. Brak wylogowania się przy opuszczaniu miejsca pracy
2. Sieć	2.1. Brak alternatywnych dróg połączenia
	2.2. Brak szyfrowania łączności radiowej
3. Sprzęt	3.1. Brak kopii zapasowych / archiwalnych
	3.2. Niewłaściwe wycofywanie nośników z użycia
	3.3. Niewłaściwe zabezpieczenie okablowania
	3.4. Pojedynczy punkt uszkodzenia (brak rezerwy)
4. Środowisko i infrastruktura	4.1. Brak elektronicznej kontroli dostępu
	4.2. Brak fizycznej ochrony budynków, drzwi, okien
	4.3. Brak gwarantowanego zasilania
	4.4. Brak mechanicznych i budowlanych systemów zabezpieczeń
	4.5. Brak monitorowania przez wyspecjalizowane jednostki
	4.6. Brak planów wymiany infrastruktury
	4.7. Brak systemów sygnalizacji napadu i włamania
	4.8. Lokalizacja na terenie zagrożonym powodzią
	4.9. Stan techniczny budynku
	4.10. Stan techniczny instalacji grzewczych
	4.11. Stan techniczny instalacji odgromowych
	4.12. Stan techniczny instalacji zasilania
	4.13. Usytuowanie budynku
	4.14. Wrażliwość na promieniowanie elektromagnetyczne
	4.15. Wrażliwość na wilgotność

	4.16. Wrażliwość na zanieczyszczenie (kurz)
	4.17. Wrażliwość na zmiany napięcia
	4.18. Wrażliwość na zmiany temperatury

Źródło: Dane uzyskane podczas badań prowadzonych w UKS w Opolu

Na podstawie danych przedstawionych tab. 1 oraz w tab. 2 istnieje możliwość dokonania kategoryzacji czynników ryzyka.

Etap drugi – analiza czynników ryzyka, polega na tym, że właściciel ryzyka dokonuje oceny oddziaływania zagrożenia na kryteria bezpieczeństwa informacji, tj. poufność, integralność, dostępność, rozłączalność. Przyjmuje się skalę punktową i ujmuje w rejestrze ryzyka na dany rok – przykład przedstawiono w tab. 3.

Tab. 3. Skala punktowa dla rejestru ryzyka

STOPIEŃ ODDZIAŁYWANIA WYSTĄPIENIA RYZYKA	OPIS SZCZEGÓŁOWY	WARTOŚĆ PUNKTOWA SKUTKU
nieznaczny	• znikomy wpływ na realizację celów i zadań, • brak skutków prawnych, • nieznaczny skutek finansowy, • brak wpływu na bezpieczeństwo pracowników, • brak wpływu na wizerunek Urzędu,	1
mały	• mały wpływ na realizację celów i zadań, • brak skutków prawnych, • mały skutek finansowy, • brak wpływu na bezpieczeństwo pracowników, • niewielki wpływ na wizerunek Urzędu,	2
średni	• średni wpływ na realizację celów i zadań, • umiarkowane konsekwencje prawne, • średni skutek finansowy, • brak wpływu na bezpieczeństwo pracowników, • średni wpływ na wizerunek Urzędu,	3
poważny	• poważny wpływ na realizację zadania, w tym poważne zagrożenie terminu jego realizacji, jak i osiągnięcia celu; • poważne konsekwencje prawne; • zagrożenie bezpieczeństwa pracowników; • poważne straty finansowe; • poważny wpływ na wizerunek Urzędu;	4
katastrofalny	• brak realizacji zadania i brak realizacji celu; • bardzo poważne i rozległe konsekwencje prawne; • naruszenie bezpieczeństwa pracowników	5

	(ujemne konsekwencje dla ich życia i zdrowia); • wysokie straty finansowe; • utrata dobrego wizerunku Urzędu w środowisku oraz w opinii publicznej	

Etap trzeci – postępowanie z ryzykiem oznacza, że „właściciel ryzyka" określa punktowe prawdopodobieństwo wystąpienia zagrożenia, przyjmując skalę, którą przedstawiono w tab. 4.

Tab. 4. Punktowe prawdopodobieństwo wystąpienia czynników ryzyka dla rejestru ryzyka

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA RYZYKA	OPIS SZCZEGÓŁOWY	WARTOŚĆ PUNKTOWA SKUTKU
bardzo rzadkie lub prawie niemożliwe	• zdarzenie może zaistnieć jedynie w wyjątkowych okolicznościach, • wystąpi sporadycznie raz na 5 lat, a najprawdopodobniej w ogóle nie zaistnieje, • nie wystąpiło dotychczas, • dotyczy jednostkowych spraw, • prawdopodobieństwo wystąpienia określa się na 1-20%,	1
małe	• istnieje małe prawdopodobieństwo, że wystąpi kilka razy w ciągu 3 lat, • dotyczy nielicznych spraw, • prawdopodobieństwo wystąpienia określa się na 21-40%,	2
średnie	• zaistnienie zdarzenia jest średnio możliwe, może wystąpić częściej niż kilka razy w ciągu 3 lat, • dotyczy niektórych spraw, • prawdopodobieństwo wystąpienia określa się na 41-60%,	3
wysokie	• zaistnienie zdarzenia jest bardzo prawdopodobne, • wystąpi regularnie przynajmniej raz w roku, • dotyczy większości spraw, • prawdopodobieństwo wystąpienia określa się na 61-80%,	4
prawie pewne	• oczekuje się, że zdarzenie takie nastąpi na pewno, • wystąpi regularnie co miesiąc lub częściej, • dotyczy wszystkich lub prawie wszystkich spraw, • prawdopodobieństwo wystąpienia określa się na 81-100%.	5

Po przeprowadzeniu trzech etapów analizy należy obliczyć współczynnik istotności ryzyka na podstawie wzoru (1).

$$IR = PR \times SR \quad (1)$$

gdzie:

- IR – to współczynnik istotności ryzyka,
- PR – to prawdopodobieństwo wystąpienia ryzyka,
- SR – to potencjalne oddziaływanie wystąpienia ryzyka.

Punktowej oceny ryzyka, dokonuje się obliczając wartość **ryzyko (R)**, która stanowi iloczyn **oddziaływania (od)** i **prawdopodobieństwa (pr)**, ze wzoru (2).

$$R = od \times pr \quad (2)$$

gdzie:

- od = odp + odi + odd + odr
- odp – składowa oddziaływania zagrożenia związanego z poufnością, Poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym / nieupoważnionym osobom, podmiotom lub procesom,
- odi – składowa oddziaływania zagrożenia związanego z integralnością, Integralność - zapewnienie, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- odd – składowa oddziaływania zagrożenia związanego z dostępnością, Dostępność - właściwość polegająca na zapewnieniu, że osoby upoważnione mają dostęp do informacji wtedy, gdy jest to potrzebne,
- odr – składowa oddziaływania zagrożenia związanego z rozliczalnością. Rozliczalność - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

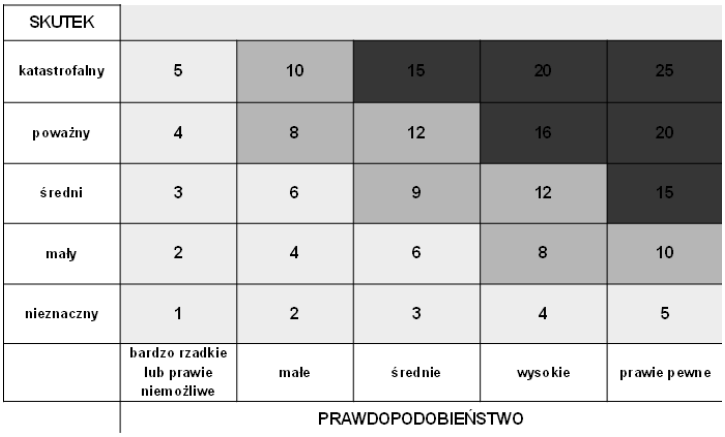
Po przeprowadzonej analizie wyniki można umieścić na mapie ryzyka zaprezentowanej na rys. 5.

Wyniki uzyskane w UKS w Opolu podczas prowadzonych badań dla czynnika ryzyka „zagrożenia wewnętrzne, bezpieczeństwo informacji i dokumentów" przedstawiono w tab. 5 oraz w tab. 6.

4. Wnioski

Połączone systemy KZ, SZBI i ZK dają wiele korzyści w zakresie procesu zarządzania ryzykiem:

- jednolite podejście do procesu identyfikacji obszarów ryzyka,
- wspólny we wszystkich systemach proces identyfikacji obszarów ryzyka i czynników ryzyka w tych obszarach (jedna struktura, jeden rejestr),
- wspólne mechanizmy kontrolne (te same działania),
- jednolita metodologa analizy ryzyka,
- jednakowa wartość ryzyka w obszarze wskazuje na poziom ryzyka – jeden obszar ryzyka = ta sama wartość końcowa ryzyka w systemach,
- uniknięcie wielokrotnej analizy ryzyka tych samach obszarów,



Rys. 5. Mapa ryzyka „5x5" analiza ryzyka dla KZ, ZK, SZBI – UKS w Opolu

Tab. 5. Fragment rejestru do analizy KZ, SZBI oraz ZK

Obszar działalności	System	Symbol z bazy podatności	Symbol z bazy zagrożeń	OCENA RYZYKA			Ocena poziomu istotności (niski/średni/wysoki)	Istniejące mechanizmy kontroli
				PR	SR składowa oddziaływania	IR poziom istotności		
Zagrożenia wewnętrzne: bezpieczeństwo informacji i dokumentów	KZ			4	5	20	wysoki	1. Bieżący nadzór kierownika komórki 2. Nadzór Dyrekcji Urzędu 3. Nadzór sprawowany przez POIN, ABI 4. Szkolenia
	SZBI	1.1, 1.2, 2.1 – 2.5, 3.1	1.2 – 1.4, 1.6, 2.3, 2.6	4	5 1 (poufność) + 2 (integralność) + 1 (dostępność) + 1 (rozliczalność)	20	wysoki	
	ZK			5	5	25 nieodłączne (pierwotne)	wysoki	
				4	5	20 rezydualne (końcowe, po zastosowaniu mechanizmów)		

Źródło: opracowanie własne.

- oszczędność czasu pracy oraz mniejsze obciążenie pracowników (właścicieli ryzyka),
- jeden harmonogram posiedzeń zespołu, na którym analizowane są wszystkie czynniki ryzyka wysokie i średnie,
- możliwość podejmowania jednolitych działań zaradczych,
- każdy z obszarów ryzyka posiada jednego właściciela (a nie np. 3),
- w przypadku zidentyfikowania nowego ryzyka mamy gwarancję ujęcia go w rejestrze wspólnym dla wszystkich systemów oraz poddania go szczegółowej i terminowej analizie.

Tab. 6. Zmodyfikowany rejestr do analizy ryzyka dla wszystkich trzech systemów

Rejestr ryzyk Urzędu Kontroli Skarbowej w Opolu na 2015 r. (przy uwzględnieniu 3 systemów zarządzania)											
Obszar działalności	Identyfikacja ryzyka		Ocena ryzyka				Odpowiedź na ryzyko				Odniesienie do dokumentu SZBI, planu ZK
	Zidentyfikowane ryzyko - opis	Symbol ryzyka	PR	SR	IR	Ocena poziomu istotności	Istniejące mechanizmy kontroli	Reakcja na ryzyko	Planowane mechanizmy kontroli i terminy ich wdrożenia	Właściciel ryzyka	
Zagrożenia wewnętrzne: bezpieczeństwo informacji i dokumentów	1. Ujawnienie prawnie chronionych informacji. 2. Udostępnianie akt kontroli niezgodnie z ustawą o kontroli skarbowej. 3. Nieprawidłowe obchodzenie się z dokumentami. 4. Przechowywanie dokumentów na ogólnodostępnych dyskach, na prywatnych komputerach lub niezabezpieczonych fizycznie lub kryptograficznie nośnikach.	20	4	5	20	wysokie	1. Bieżący nadzór kierownika komórki. 2. Nadzór Dyrekcji Urzędu. 3. Nadzór sprawowany przez Pełnomocnika Ochrony, Administratora Bezpieczeństwa Informacji. 4. Szkolenia w przedmiotowym zakresie. 5. Zakaz tworzenia i przechowywania dokumentów i materiałów niejawnych oraz objętych tajemnicą skarbową w urządzeniach zewnętrznych (W1Y) 6. Uregulowania i procedury wewnętrzne	kontrolowanie i ograniczanie	Analiza obszaru ryzyka w ramach ścieżki procesu według rocznego harmonogramu	ABI	SZBI poz. nr 3 Plan Zarządzania Kryzysowego poz. nr 4

Źródło: opracowanie własne

Literatura

1. Dziennik Ustaw z 2013 r, poz. 885.
2. Dziennik Ustaw z 2012 r. poz. 526.
3. Dziennik Ustaw z.2013 r. poz. 1166.
4. http://www.pkn.pl/sites/default/files/broszura_pkn_szbi.pdf dostęp dnia 5.01.2015 r.
5. Kuc BR., Kontroling narzędzie wczesnego ostrzegania, Wydawnictwo Menedżerskie PTM, Warszawa 2006, s. 145.
6. Kulińska E., Dornfeld A., Zarzadzanie ryzykiem procesów. Identyfikacja – modelowanie – zastosowanie, Wyd. Politechniki Opolskiej, Opole 2009, s.9-15.
7. Kulińska E., Aksjologiczny wymair zarzadzania ryzykiem. Modele i eksperymenty ekonomiczne. Oficyna Wydawnicza Politechniki Opolskiej, opole 2012.
8. Lipiec-Warzecha L, Ustawa o finansach publicznych. Komentarz, Wolters Kluwers Polska, Warszawa 2011.
9. Nowak E., Zawansowana rachunkowość zarządcza, PWE Warszawa 2003, s. 266.

Dr hab. inż. Ewa KULIŃSKA, prof. PO
Katedra Logistyki
Instytut Organizacji Procesów Wytwórczych
Wydział Inżynierii Produkcji i Logistyki
Politechnika Opolska
45-370 Opole, ul. Ozimska 75,
tel./fax: (0-77) 449 8851
e-mail: e.kulinska@po.opole.pl

Dr Agnieszka DORNFELD
Urząd Kontroli Skarbowej
46-020 Opole, ul. Wojciecha Drzymały 22,
tel./fax: 77 401 78 00
e-mail: agdo@onet.eu

Badana finansowane przez NCN projekt nr 2012/05/B/HS4/04139