ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2017
Seria: ORGANIZACJA I ZARZĄDZANIE z. 107 Nr kol. 1982

Ewa KULIŃSKA
Politechnika Opolska
e.kulinska@po.opole.pl

Monika ODLANICKA-POCZOBUTT
Politechnika Śląska
monika.odlanicka-poczobutt@polsl.pl

Paweł DORNFELD
Politechnika Opolska
pdornfeld@po.opole.pl

# CZYNNIKI RYZYKA W OBSZARZE PROCESÓW PRZEPŁYWU INFORMACJI W JEDNOSTKACH SAMORZĄDOWYCH – WYNIKI BADAŃ

**Streszczenie.** Celem artykułu była identyfikacja czynników ryzyka oraz pomiar stopnia ich występowania w procesach przepływu informacji w jednostkach samorządowych, na przykładzie wybranych gmin województwa opolskiego. Dokonano analizy występujących czynników ryzyka w odniesieniu do ośmiu wyodrębnionych procesów realizowanych w wybranych podmiotach badawczych.

**Słowa kluczowe:** ryzyko, bezpieczeństwo przepływu informacji, instytucja, jednostki samorządowe, mechanizmy kontrolne

# RISK FACTORS IN THE AREA OF FLOW INFORMATION PROCESSES IN LOCAL GOVERNMENT UNITS – RESULTS OF RESEARCH

**Abstract.** The aim of the article was to identify risks and measure the level of risk factors present in the processes of information flow in self-government units, on the example of selected communes in the Opolskie voivodship. An analysis of the existing risk factors for eight isolated processes carried out in selected research entities.

**Keywords:** risk, information security, institution, local government, control mechanisms

# 1. Wprowadzenie

Informacja coraz powszechniej jest traktowana jako towar masowy podlegający regułom handlowym, ponieważ stanowi podstawę funkcjonowania organizacji. Bezpieczeństwo informacji umieszczonej zarówno w systemie informatycznym, jak i w postaci papierowej jest priorytetem dla każdej instytucji. Organizacje, ich systemy informacyjne i sieci są narażone na zagrożenia bezpieczeństwa pochodzące z wielu różnych źródeł, włączając w to przestępstwa przy użyciu komputera, szpiegostwo, sabotaż, wandalizm, pożar czy powódź. Powodujące szkody złośliwe kody, włamania komputerowe, ataki typu „odmowa usługi" stają się bardziej powszechne, bardziej ambitne i coraz bardziej wyrafinowane.

Bezpieczeństwo przepływu informacji rozumiemy jako pewne pożądane i wartościowane pozytywnie relacje zachodzące w procesie przeniesienia przez źródło wiedzy nowej zdolności do rozwiązania problemu praktycznego, zapewniający rozwój i ukształtowany przez podmioty transferu zespół wartości organizacyjnych, technicznych, technologicznych, majątkowych i innych, mających znaczenie gospodarcze. Umiejętność przeciwdziałania zagrożeniom i ich złożonej naturze możliwa jest tylko w warunkach skutecznego zarządzania bezpieczeństwem przepływu informacji.

Międzynarodowa norma ISO 27001 określa wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji. Wskazując elementy bezpieczeństwa fizycznego, osobowego, teleinformatycznego oraz prawnego, jednocześnie nie określa szczegółowych technicznych wymagań, lecz wskazuje na obszary, które należy uregulować. Sposób zabezpieczenia tych obszarów powinien być oparty na przeprowadzonej uprzednio analizie ryzyka. Norma może być podstawą budowy Systemu Zarządzania Bezpieczeństwem Informacji w różnych sektorach branżowych[1].

Bezpieczeństwo informacji jest ważne zarówno dla sektora publicznego, jak prywatnego, służąc ochronie infrastruktury krytycznej. W obu sektorach bezpieczeństwo informacji może funkcjonować jako dźwignia biznesu, np. umożliwiając wprowadzenie e-rządu lub e-gospodarki oraz unikanie lub redukowanie odpowiednich ryzyk. Wzajemne przenikanie się sieci publicznych i prywatnych oraz współużytkowanie zasobów informacyjnych utrudnia utrzymanie kontroli dostępu. Tendencja wprowadzania rozproszonego przetwarzania także osłabia efektywność centralnych, specjalizowanych mechanizmów zarządzania[2].

Bezpieczeństwo przepływu informacji powinno być kształtowane na podstawie jego dualistycznej formy postrzegania, rozumianego jako:

- Bezpieczeństwo jako odporność na powstanie sytuacji zagrożeń, przy czym uwaga głównie koncentruje się na zawodności skojarzenia wiedzy (rozwiązanie naukowo-

[1] http://www.centrum.bezpieczenstwa.pl/index.php/standardy-othermenu-16/55-iso-27001, 04.02.2017.
[2] Kulińska E., Dornfeld A.: Kontrola zarządcza w jednostkach sektora finansów publicznych. Difin, Warszawa 2015.

badawcze) i jej użytkownika (przedsiębiorcy), stanowiącego podmiot przenoszący zdolność do rozwiązania problemu praktycznego oraz jego innej podatności na powstanie sytuacji niebezpiecznych.

- Bezpieczeństwo rozumiane jako jego zdolność do ochrony wartości, jaką niesie gospodarcze skojarzenie wiedzy i jej użytkownika w działaniach logistycznych przed zewnętrznymi i wewnętrznymi zagrożeniami (zorganizowany potencjał odporności na bariery i zagrożenia)[3].

Celem artykułu była identyfikacja czynników ryzyka oraz pomiar stopnia występujących w procesach przepływu informacji w jednostkach samorządowych, na przykładzie wybranych gmin województwa opolskiego.

## 2. Zagrożenia dla bezpieczeństwa przepływu informacji

Analizę zagrożeń dla bezpieczeństwa przepływu informacji często opiera się na określeniu prawdopodobieństwa wystąpienia przewidywalnych zagrożeń wynikających z doświadczenia, standardowej podatności i oszacowania ich wpływu na działalność instytucji w zakresie:

1. Źródła zagrożeń wynikających z istoty przepływu informacji:
   - Nieskuteczność zaplanowanego przepływu informacji spowodowana błędnym:
     a. rozpoznaniem możliwości i potrzeb docelowego odbiorcy wiedzy (zdolność innowacyjna);
     b. zdefiniowaniem i sklasyfikowaniem rodzaju wiedzy, jaka ma być przekazywana.
   - Błędne rozumienie bezpieczeństwa przepływu informacji, polegające na złej ocenie posiadanej odporności na powstanie sytuacji zagrożeń i zdolności do ochrony wartości, jaką niesie gospodarcze skojarzenie wiedzy i jej użytkownika.
   - Niedostrzeganie różnicy pomiędzy pracą zgodną z posiadanymi w firmie procedurami a pracą wymagającą wdrożenia wiedzy, która implikuje zmianę dotychczasowych standardów obowiązujących w instytucji.
   - Brak możliwości zastosowania w praktyce rozwiązań innowacyjnych z powodu:
     a. współzawodnictwa wewnątrz organizacji, które blokuje pełne korzystanie z posiadanych zasobów wiedzy;
     b. przywiązania do standardowych rozwiązań, które często są szkodliwe i również działa hamująco na proces pozyskiwania wiedzy;
     c. strachu i tak zwanej złej atmosfery w pracy, która powoduje poważne trudności w przekładaniu wiedzy na działania.

[3] Por. Sienkiewicz P.: Teoria bezpieczeństwa systemów. AON, Warszawa 2005.

- Występowanie barier organizacyjnych i przyczyn psychologicznych w transferze wiedzy, wynikających z faktu, iż:
  a) pracownicy naukowi nie chcą się dzielić wiedzą, ponieważ identyfikują program z ujawnianiem własnych porażek i nie chcą siebie stawiać w złym świetle;
  b) istnieje obawa, że wyniki doświadczeń nie będą uważane za wyjątkowe;
  c) obawa przed nowym, powodująca brak akceptacji;
  d) różnice i bariery kulturowe i religijne utrudniające komunikację;
  e) kult ekspertów i obrona terytoriów;
  f) postrzeganie wdrażającego wiedzę jako eksperta w wąskim i teoretycznym obszarze działań przedsiębiorstwa.
- Zastosowanie modelu transferu ekspertów jako przepływu informacji spowodowało zmianę podmiotu zatrudniającego i odpływ z ośrodków naukowo-badawczych potencjału intelektualnego.

2. Źródła zagrożeń ekonomicznych:
   - Przeszacowanie kosztów organizacji przepływu informacji (koszty organizacji spotkań, wideokonferencji, briefingów).
   - Błędnie zaprojektowane finansowanie przepływu informacji w instytucji, który nie uwzględniał:
     a) kosztów uzyskania przychodów (zużycie materiałów i energii, usług obcych, wynagrodzeń, kosztów wytworzenia, kosztów sprzedaży, kosztów handlowych);
     b) przewidywanej wartości sprzedanych towarów;
     c) kosztów operacji finansowych obejmujących odsetki od kredytów i pożyczek;
     d) strat nadzwyczajnych;
     e) przychodów ze sprzedaży produktów transferu, praw autorskich, wyniki na pozostałej sprzedaży;
   - Zagrożenia finansowe dla przepływu informacji wynikające:
     a) ze zmiany struktury kapitału początkowego związanego z prawem własności i posiadaniem udziałów, które upoważniają do uczestniczenia (w odpowiedniej proporcji) w wypracowanym zysku oraz możliwością oddziaływania na obsadę personalną kierownictwa i na politykę spółki przez udział w radzie nadzorczej;
     b) z zobowiązań długoterminowych, którymi firmy finansują swój rozwój, ale też te zobowiązania mogą prowadzić do przejmowania własności organizacji przez wierzycieli w całości lub w części.
   - Błędnego zarządzania kosztami, które prowadzą do utraty kapitału obrotowego i zahamowania przepływów pieniężnych.

3. Zagrożenia prawne:
   - Działania stanowiące czyn nieuczciwej konkurencji, rozumiane jako działanie sprzeczne z prawem lub dobrymi obyczajami, które zagrażają lub naruszają interes instytucji.
   - Naruszenie zasad ochrony praw autorskich oraz własności przemysłowej (patenty, wynalazki, modele przemysłowe).
   - Błędy w zapisie istotnych warunków w umowach.
   - Nowelizacja ustaw i aktów podstawowych.
   - Zagrożenia karno-skarbowe.
   - Naruszenie przepisów materialno-karnych, a w tym:
     a) ujawnienie informacji prawnie chronionych;
     b) ujawnienie nielegalności oprogramowania.
4. Zagrożenia komunikacji:
   - Niewłaściwe oddziaływanie kierownictwa, powodujące:
     a) brak stymulujących postaw akceptujących innowacyjność;
     b) negatywną ocenę kierownictwa firmy przez personel, co powoduje reaktywność pracowników.
   - Niewypełnienie podstawowych funkcji komunikacji sprowadzających się do:
     a) budowania wizerunku wewnętrznego organizacji;
     b) budowy kanałów kontaktu (kanały informacyjne) między poszczególnymi szczeblami organizacji.
   - W obszarze komunikacji podmiotowej nie stosowano elementów kultury zarządzania obejmującej:
     a) udział wszystkich pracowników firmy,
     b) system motywacji i raportowania,
     c) udział podmiotów powiązanych (doradcy, eksperci).
   - Nakładany na zarządzanie przedmiotowe przepływu informacji podmiotowy wyznacznik nie uwzględniał tego, że brak związanego z transferem wiedzy specjalistycznego szkolenia, którego niedostosowana do potrzeb i wyników audytu wstępnego tematyka może być przyczyną braku świadomości i lojalności pracowniczej, indukującej akceptację i motywację do działań innowacyjnych.
   - Następstwa związkowego konfliktu przemysłowego.
5. Zagrożenia informacji:
   - Utrata niejawności informacji zawartych w transferze wiedzy, powodująca obniżenie jej wartości gospodarczej, co prowadzi do powstania szkody z tytułu utraconych korzyści (utrata przewagi konkurencyjnej).
   - Brak sprecyzowanego i zdefiniowanego systemu i warunków bezpieczeństwa informatycznego przeznaczonego do obsługi przepływu informacji, obejmującego:

a) utrzymanie założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności;
b) błędnie szacowane ryzyka, co doprowadziło do błędów w analizie zagrożeń dla bezpieczeństwa przepływu informacji.

- Informacja jako źródło prognoz i analiz nie stanowiła elementu rozpoznania zagrożeń, a zarządzanie bezpieczeństwem przepływu informacji odbywało się w zakresie podejmowania decyzji w oparciu o zbiór nieuporządkowanych i nieprzeanalizowanych informacji.

Zarządzanie bezpieczeństwem informacji w systemach informatycznych obejmuje zespół procesów zmierzających do osiągnięcia i utrzymania ustalonego poziomu bezpieczeństwa[4].

## 3. Istotne aspekty przetwarzania informacji w instytucjach

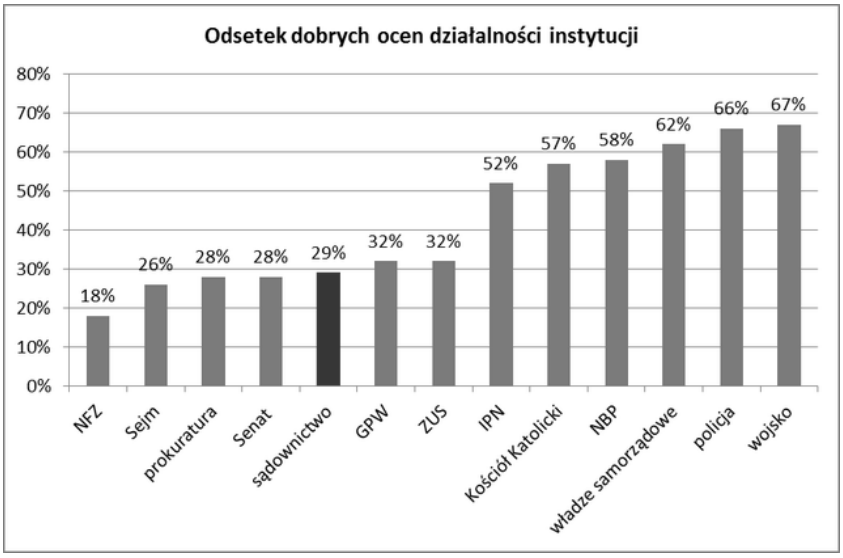
Istotne zmiany systemowe mają wpływ zarówno na przedsiębiorstwa, jak i instytucje, mające istotne znaczenie dla rozwoju gospodarczego. Zainteresowanie pojęciem instytucji w literaturze traktowane jest jako powrót do klasyków teorii ekonomii, takich jak A. Smith czy D. Ricardo, gdzie analizy systemu ekonomicznego były prowadzone w kontekście instytucjonalnym i historyczno-ewolucyjnym[5]. Instytucje mogą zarówno hamować rozwój, jak i mu sprzyjać, co funkcjonuje w literaturze jako *endogeniczna zmiana instytucjonalna*[6]. Ograniczona racjonalność instytucji i dominujące zwyczaje mają decydujący wpływ na podejmowane wybory i reguły współpracy, stanowiące przejaw efektywności adaptacyjnej systemu instytucjonalnego[7]. Efektywność adaptacyjna to zdolność systemu instytucji do rozwiązywania problemów społeczno-gospodarczych. D. North do tych problemów zalicza: zdolność społeczeństwa do akumulacji wiedzy, zdolność do generowania innowacji, wyzwalanie skłonności do ryzyka, wyzwalanie przedsiębiorczych zachowań czy eliminację wąskich gardeł w systemie społecznym[8]. Wszystko to ma służyć wzrostowi gospodarczemu. Podstawowym wyznacznikiem efektywności adaptacyjnej jest wdrażanie instytucji zmniejszających koszty transakcyjne przy spełnieniu szeregu warunków ograniczających, jak

[4] Nowak A., Schefes W.: Zarządzanie bezpieczeństwem informacyjnym. AON, Warszawa 2010, s. 34.
[5] Nelson R.R., Sampat B.N.: Making Sense of Institutions as a Factor Shaping Economic Performance. „Journal of Economic Behaviour and Organization", January, Vol. 44, 2001.
[6] Odlanicka-Poczobutt M., Knop L.: Rozwój i funkcjonowanie sieci w świetle podejścia endogenicznego. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 89, 2016, s. 367-377.
[7] Staniek Z.: Uwarunkowania i wyznaczniki efektywności systemu instytucjonalnego [w:] Pacho W. (red.): Szkice ze współczesnej teorii ekonomii. SGH, Warszawa 2005, s. 125-180.
[8] North D.: Institutions, Institutional Change and Economic Performance. Cambridge University Press, Cambridge 1994, p. 80.

np. potrzeba niezbędnych informacji, poziom kapitału społecznego czy tworzenie instytucji dla koordynacji działań gospodarczych. Zachodzi tu jednak zjawisko inercji instytucjonalnej[9].

Istotne znaczenie w zarządzaniu instytucją ma przetwarzanie informacji. Informacje właściwe to dane przetworzone w ramach działalności organizacji, posiadające pewną wartość poznawczą. Zazwyczaj mają postać zagregowanych i strukturalizowanych zbiorów, którymi łatwo można zarządzać. Gromadzi się je na bieżąco. Odtworzenie utraconych informacji przy braku środków zabezpieczających jest bardzo kosztowne, a czasem wręcz niemożliwe[10].

Działalność instytucji jest różnie oceniana przez społeczeństwo. Wyniki badań dotyczących opinii Polaków na temat działalności samorządów wskazują na wysokie notowania, bo aż 62% wysoko ocenia ich pracę. Wysokie wyniki osiągają takie instytucje, jak wojsko (67% dobrych ocen), policja (66%), Narodowy Bank Polski (58%), Kościół katolicki (57%) czy Instytut Pamięci Narodowej (52%). Odsetek dobrych ocen działalności instytucji przedstawiono na rys. 1.




Rys. 1. Odsetek dobrych ocen działalności instytucji
Źródło: Opracowanie na podstawie CBOS, wrzesień 2014.

Ze względu na swoją rolę w społeczeństwie informacyjnym instytucje powinny szczególnie dbać o bezpieczeństwo przechowywanych i przetwarzanych informacji. Nigdy nie ma pewności, że tajemnice instytucji są odpowiednio chronione. Zawsze należy podejmować działania zmniejszające ryzyko utraty informacji. Każda instytucja, niezależnie od wielkości i przedmiotu działalności, gromadzi ogromne ilości informacji, które traktuje jako swój dorobek, i które posiadają określoną wartość. Istnieje również niebezpieczeństwo

[9] Odlanicka-Poczobutt M.: Inercja instytucjonalna a innowacyjne rozwiązania w sądach powszechnych w sprawach cywilnych. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 89, 2016, s. 351-365.

[10] http://www.egospodarka.pl/25690,Bezpieczenstwo-systemow-informatycznych-rodzaje-zagrozen,1,20,2.html, 14.05.2017.

zatrzymywania informacji. Rozważania teoretyczne w zakresie trendów i tendencji w dziedzinie udostępniania informacji – udostępnianie w Internecie, standaryzacja formatów dokumentów, prawo w sieci semantycznej, wykonalność przepisów, analiza zagadnień związanych z integracją teorii prawa i informatyki prawniczej – są obecne w badaniach literaturowych[11].

## 4. Czynniki ryzyka w zakresie bezpieczeństwa informacji w jednostkach samorządowych – metodyka badań

Badania w zakresie wskazania czynników ryzyka przeprowadzono w 8 gminach województwa opolskiego. Na potrzeby realizacji badania wyodrębniono osiem procesów realizowanych w podmiotach badawczych i były to procesy takie jak:

- Proces 1. Tworzenie uchwał Rady Gminy;
- Proces 2. Udzielenie odpowiedzi w ramach informacji publicznej;
- Proces 3. Biuletyn Informacji Publicznej;
- Proces 4. Wydawanie decyzji;
- Proces 5. Wydawanie zezwoleń;
- Proces 6. Wydawanie zaświadczeń;
- Proces 7. Obieg korespondencji przychodzącej;
- 8. Sprawozdania.

Na podstawie analizy dokumentacji oraz przeprowadzonych wywiadów bezpośrednich standaryzowanych z pracownikami gmin na szczeblach kierowniczych oraz wśród personelu średniego szczebla – w ramach każdego procesu zidentyfikowano czynniki ryzyka występujące w tym obszarze. Przy analizie ryzyka uwzględniono funkcjonujące mechanizmy kontrolne.

Istotne czynniki ryzyka w gminie w zakresie zarządzania bezpieczeństwem informacji określono i wytypowano wstępnie w każdym ze wskazanych procesów, których zestawienie zawiera tabela 1.

[11] Por. Odlanicka-Poczobutt M., Kulińska E.: Kierunki rozwoju informacji prawnej w ramach gospodarki elektronicznej. Zeszyty Naukowe Uniwersytetu Szczecińskiego, s. Ekonomiczne Problemy Usług, nr 113, 2014, s. 103-111.

Tabela 1

Zestawienie procesów realizowanych w gminie oraz wstępne wyodrębnienie występujących czynników ryzyka

| Procesy | Czynniki ryzyka |
|---|---|
| **1. Tworzenie uchwał Rady Gminy** | Brak szkoleń na określonych stanowiskach pracy |
| | Nieprzesyłanie dokumentów w wyznaczonych terminach |
| | Przesyłanie dokumentów zawierających błędy |
| **2. Udzielanie odpowiedzi w ramach informacji publicznej** | Odpowiedzi na zapytania bez zachowania terminu wynikającego z ustaw o dostępie do informacji publicznej |
| | Brak odpowiedzi lub odpowiedzi niepełne i niewłaściwe |
| **3. Biuletyn Informacji Publicznej** | Nieterminowe umieszczenie informacji w BIP |
| | Prowadzenie BIP-u niezgodnie z wymaganiami ustawy |
| | Umieszczenie w BIP niewłaściwych informacji lub informacji niepełnych |
| | Nieumieszczanie wymaganych informacji w BIP |
| **4. Wydawanie decyzji** | Wydawanie decyzji wbrew obowiązującym przepisom prawa |
| | Wydawanie decyzji zawierających błędne dane |
| **5. Wydawanie zezwoleń** | Wydawanie zezwolenia z błędnymi danymi |
| | Nieterminowe wydawanie zezwolenia |
| | Wydawanie zezwolenia niezgodnie z obowiązującą procedurą lub regulacjami prawnymi |
| **6. Wydawanie zaświadczeń przez Urząd Gminy** | Nieterminowe wydawanie zaświadczenia |
| | Wydawanie zaświadczenia z niewłaściwymi danymi |
| | Wydawanie zaświadczeń wadliwych |
| **7. Obieg korespondencji przychodzącej** | Korespondencja skierowana do niewłaściwej komórki lub osoby |
| **8. Sprawozdania** | Niesporządzenie lub nieprzesłanie sprawozdań |
| | Przesłanie sprawozdań po terminie |
| | Przesłanie niepełnych lub źle wypełnionych sprawozdań |
| | Przesłanie sprawozdań na niewłaściwych drukach lub w niewłaściwy sposób lub niewłaściwej formie |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Jako najważniejsze mechanizmy kontrolne, w największym stopniu niwelujące ryzyka, wskazano: nadzór administratora danych osobowych, zakres obowiązków pracowników, nadzór kierownika oraz nadzór wójta gminy. Ustalono trzy poziomy ryzyka – wysoki (W), średni (S) oraz niski (N).

Pogłębione wywiady oraz ustalenie wartości prawdopodobieństwa wystąpienia czynnika oddziaływania na proces na podstawie zastosowanych metod[12] pozwoliły na ustalenie końcowej wartości ryzyka. W tabelach 2-9 przedstawiono szczegółowe wyniki badania.

[12] Metody zostały przedstawione i szczegółowo omówione w: Kulińska E., Dornfeld A.: Zarządzanie ryzykiem procesów: identyfikacja-modelowanie-zastosowanie. Oficyna Wydawnicza Politechniki Opolskiej, Opole 2009, s. 135-140.

Tabela 2

Identyfikacja czynników ryzyka w PROCESIE 1 – Tworzenie uchwał rady gminy

| | **Wartość prawdopodobieństwa** | **Wartość oddziaływania** | **Końcowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko ujawnienia informacji i danych osobowych | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko ujawnienia informacji prawnie chronionych | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko nieudostępnienia wszystkich informacji | **4** | **5** | **20** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko niewłaściwego udostępnienia danych | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko braku osoby odpowiedzialnej za BIP | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Tabela 3

Identyfikacja czynników ryzyka w PROCESIE 2 – Udzielenie odpowiedzi w ramach informacji publicznej

| | **Wartość prawdopodobieństwa** | **Wartość oddziaływania** | **Końcowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko ujawnienia danych osobowych | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko ujawnienia informacji prawnie chronionych | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |

cd. tabeli 3

| | | | | | |
|---|---|---|---|---|---|
| Ryzyko nierozpatrzenia wniosku o udostępnienie informacji w wymaganych terminach | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko nieprzekazania danych | **4** | **5** | **20** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko braku odpowiedzi osobie składającej wniosek | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko przekazania informacji niewłaściwej osobie | **4** | **5** | **20** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Tabela 4

Identyfikacja czynników ryzyka w PROCESIE 3 – Biuletyn Informacji Publicznej

| | **Wartość prawdo-podo-bieństwa** | **War-tość oddzia-ływania** | **Koń-cowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko ujawnienia informacji i danych osobowych | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko ujawnienia informacji prawnie chronionych | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko nieudostępnie-nia wszystkich informacji | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko niewłaściwego udostępnienia danych | **4** | **5** | **20** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |
| Ryzyko braku osoby odpowie-dzialnej za BIP | **5** | **5** | **25** | **W** | • Nadzór administratora danych osobowych<br>• Zakres obowiązków pracowników<br>• Nadzór kierownika<br>• Nadzór wójta gminy |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Tabela 5

Identyfikacja czynników ryzyka w PROCESIE 4 – Wydawanie decyzji

| | **Wartość prawdo-podo-bieństwa** | **War-tość oddzia-ływania** | **Koń-cowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko niewłaściwej analizy sprawy | **4** | **4** | **16** | **W** | • Weryfikacja decyzji na wszystkich szczeblach<br>• Nadzór merytoryczny kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków pracownika<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór wójta |
| Ryzyko braku nadzoru kierownika | **1** | **3** | **3** | **N** | • Weryfikacja decyzji na wszystkich szczeblach<br>• Nadzór merytoryczny kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków pracownika<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór wójta |
| Ryzyko braku podpisu wójta – decyzja nieważna | **1** | **3** | **3** | **N** | • Weryfikacja decyzji na wszystkich szczeblach<br>• Nadzór merytoryczny kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków pracownika<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór wójta |
| Ryzyko niezachowania wymaganego terminu | **2** | **3** | **6** | **S** | • Weryfikacja decyzji na wszystkich szczeblach<br>• Nadzór merytoryczny kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków pracownika<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór wójta |
| Ryzyko wydania decyzji mimo braków formalnych | **3** | **4** | **12** | **Ś** | • Weryfikacja decyzji na wszystkich szczeblach<br>• Nadzór merytoryczny kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków pracownika<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór wójta |

cd. tabeli 5

| | | | | | |
|---|---|---|---|---|---|
| Ryzyko wysłanie decyzji do niewłaściwej osoby | **1** | **3** | **3** | **N** | • Weryfikacja decyzji na wszystkich szczeblach<br>• Nadzór merytoryczny kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków pracownika<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór wójta |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Tabela 6

Identyfikacja czynników ryzyka w PROCESIE 5 – Wydawanie zezwoleń

| | **Wartość prawdo-podo-bieństwa** | **War-tość oddzia-ływania** | **Koń-cowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko niewłaściwej analizy sprawy | **4** | **4** | **16** | **W** | • Weryfikacja zezwolenia na wszystkich szczeblach<br>• Nadzór kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Uregulowanie wewnętrzne dotyczące wydawania zezwoleń<br>• Nadzór wójta |
| Ryzyko braku nadzoru kierownika | **1** | **3** | **3** | **N** | • Weryfikacja zezwolenia na wszystkich szczeblach<br>• Nadzór kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Uregulowanie wewnętrzne dotyczące wydawania zezwoleń<br>• Nadzór wójta |
| Ryzyko braku podpisu wójta – zezwolenie nieważne | **1** | **3** | **3** | **N** | • Weryfikacja zezwolenia na wszystkich szczeblach<br>• Nadzór kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Uregulowanie wewnętrzne dotyczące wydawania zezwoleń<br>• Nadzór wójta |
| Ryzyko niezachowania wymaganego terminu | **2** | **3** | **6** | **N** | • Weryfikacja zezwolenia na wszystkich szczeblach<br>• Nadzór kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Uregulowanie wewnętrzne dotyczące wydawania zezwoleń<br>• Nadzór wójta |

cd. tabeli 6

| | | | | | |
|---|---|---|---|---|---|
| Ryzyko wydania zezwolenia mimo braków formalnych | **3** | **4** | **12** | **Ś** | • Weryfikacja zezwolenia na wszystkich szczeblach<br>• Nadzór kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór Wójta |
| Ryzyko wysłania zezwolenia do niewłaściwej osoby | **1** | **3** | **3** | **N** | • Weryfikacja zezwolenia na wszystkich szczeblach<br>• Nadzór kierownika<br>• Opiniowanie dokumentacji<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Uregulowanie wewnętrzne dotyczące wydawania decyzji<br>• Nadzór Wójta |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Tabela 7

Identyfikacja czynników ryzyka w PROCESIE 6 – Wydawanie zaświadczeń

| | **Wartość prawdopodobieństwa** | **Wartość oddziaływania** | **Końcowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko ujęcia nieprawidłowych danych w zaświadczeniu | **4** | **4** | **16** | **W** | • Nadzór kierownika<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Nadzór wójta |
| Ryzyko brak zweryfikowania danych | **3** | **4** | **12** | **Ś** | • Nadzór kierownika<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Nadzór wójta |
| Ryzyko niewłaściwej analizy sprawy | **3** | **4** | **12** | **Ś** | • Nadzór kierownika<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Nadzór wójta |
| Ryzyko braku nadzoru kierownika | **1** | **3** | **3** | **N** | • Nadzór kierownika<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Nadzór wójta |
| Ryzyko wydania zaświadczenia niewłaściwej osobie | **1** | **3** | **3** | **N** | • Nadzór kierownika<br>• Szczegółowa analiza danych<br>• Zakres obowiązków<br>• Nadzór wójta |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Tabela 8

Identyfikacja czynników ryzyka w PROCESIE 7 – Obieg korespondencji przychodzącej

| | **Wartość prawdo-podo-bieństwa** | **War-tość oddzia-ływania** | **Koń-cowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko ujawnienia informacji i danych osobowych | **5** | **5** | **25** | **W** | • Instrukcja kancelaryjna<br>• Nadzór administratora danych osobowych<br>• Zakres obowiązków<br>• Nadzór kierownika<br>• Nadzór wójta |
| Ryzyko niezabezpiecza nia lub niewłaściwe zabezpieczenie danych i informacji | **5** | **5** | **25** | **W** | • Instrukcja kancelaryjna<br>• Nadzór administratora danych osobowych<br>• Zakres obowiązków<br>• Nadzór kierownika<br>• Nadzór wójta |
| Ryzyko dekretacji niewłaściwej osobie | **2** | **5** | **10** | **Ś** | • Instrukcja kancelaryjna<br>• Nadzór administratora danych osobowych<br>• Zakres obowiązków<br>• Nadzór kierownika<br>• Nadzór wójta |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Tabela 9

Identyfikacja czynników ryzyka w PROCESIE 8 – Sprawozdania

| | **Wartość prawdo-podo-bieństwa** | **War-tość oddzia-ływania** | **Koń-cowa wartość ryzyka** | **Stopień ryzyka (niskie/ średnie/ wysokie)** | **Mechanizmy kontrolne** |
|---|---|---|---|---|---|
| Ryzyko braku właściwej analizy | **3** | **3** | **9** | **Ś** | • Zakres obowiązków<br>• Regulamin organizacyjny<br>• Nadzór osób odpowiedzialnych (kierownika)<br>• Właściwy podział zadań<br>• Rozliczanie pracowników<br>• Nadzór wójta |
| Ryzyko braku właściwej weryfikacji danych do sprawozdań | **3** | **3** | **9** | **Ś** | • Zakres obowiązków<br>• Regulamin organizacyjny<br>• Nadzór osób odpowiedzialnych (kierownika)<br>• Właściwy podział zadań<br>• Rozliczanie pracowników<br>• Nadzór wójta |
| Ryzyko braku wszystkich danych | **4** | **4** | **16** | **W** | • Zakres obowiązków<br>• Regulamin organizacyjny<br>• Nadzór osób odpowiedzialnych (kierownika)<br>• Właściwy podział zadań<br>• Rozliczanie pracowników<br>• Nadzór wójta |

cd. tabeli 9

| | | | | | |
|---|---|---|---|---|---|
| Ryzyko braku weryfikacji samych sprawozdań | **2** | **4** | **8** | **N** | • Zakres obowiązków<br>• Regulamin organizacyjny<br>• Nadzór osób odpowiedzialnych (kierownika)<br>• Właściwy podział zadań<br>• Rozliczanie pracowników<br>• Nadzór wójta |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

## 5. Podsumowanie

Przeprowadzone badania w zakresie wskazania czynników ryzyka przeprowadzone w gminach województwa opolskiego odnosiły się do wyodrębnionych ośmiu procesów realizowanych w podmiotach badawczych:

- Proces 1. Tworzenie uchwał Rady Gminy;
- Proces 2. Udzielenie odpowiedzi w ramach informacji publicznej;
- Proces 3. Biuletyn Informacji Publicznej;
- Proces 4. Wydawanie decyzji;
- Proces 5. Wydawanie zezwoleń;
- Proces 6. Wydawanie zaświadczeń;
- Proces 7. Obieg korespondencji przychodzącej;
- Proces 8. Sprawozdania.

Na podstawie przeprowadzonych badań zidentyfikowano czynniki ryzyka na poziomie wysokim, przedstawione w tabeli 10.

Tabela 10

Zidentyfikowane w analizowanych procesach czynniki ryzyka na poziomie wysokim

| |
|---|
| W **PROCESIE 1** |
| Ryzyko ujawnienia informacji i danych osobowych |
| Ryzyko ujawnienia informacji prawnie chronionych |
| Ryzyko nieudostępnienia wszystkich informacji |
| Ryzyko niewłaściwego udostępnienia danych |
| Ryzyko braku osoby odpowiedzialnej za BIP |
| W **PROCESIE 2** |
| Ryzyko ujawnienia danych osobowych |
| Ryzyko ujawnienia informacji prawnie chronionych |
| Ryzyko nierozpatrzenia wniosku o udostępnienie informacji w wymaganych terminach |
| Ryzyko nieprzekazania danych |
| Ryzyko braku odpowiedzi do osoby składającej wniosek |
| Ryzyko przekazania informacji niewłaściwej osobie |

cd. tabeli 10

| W **PROCESIE 3** |
|---|
| Ryzyko ujawnienia informacji i danych osobowych |
| Ryzyko ujawnienia informacji prawnie chronionych |
| Ryzyko nieudostępnienia wszystkich informacji |
| Ryzyko niewłaściwego udostępnienia danych |
| Ryzyko braku osoby odpowiedzialnej za BIP |
| W **PROCESIE 4** |
| Ryzyko niewłaściwej analizy sprawy |
| W **PROCESIE 5** |
| Ryzyko niewłaściwej analizy sprawy |
| W **PROCESIE 6** |
| Ryzyko ujęcia nieprawidłowych danych w zaświadczeniu |
| W **PROCESIE 7** |
| Ryzyko ujawnienia informacji i danych osobowych |
| Ryzyko niezabezpieczania lub niewłaściwe zabezpieczenie danych i informacji |
| W **PROCESIE 8** |
| Ryzyko braku wszystkich danych |

Źródło: Opracowanie na podstawie przeprowadzonych badań.

Mnogość metod i podejść do procesu zarządzania ryzykiem wskazuje na fakt, że ważnym punktem działalności jednostek samorządowych powinno być dbanie o optymalne rozwiązania w zakresie istniejących zagrożeń. Decyzje odnośnie do bezpieczeństwa informacji podejmowane winny być w efekcie przeprowadzenia procesu zarządzania ryzykiem, w którym bardzo ważnym punktem wyjścia staje się zlokalizowanie i uświadomienie sobie wagi ryzyka zagrażającego jednostce. Identyfikacja i pomiar czynników ryzyka są tu o tyle istotne, że determinują wybór metody kontroli ryzyka, a to oznacza określone decyzje oraz nakłady. Znając wagę ryzyka, można świadomie zadecydować, jakie działania podejmować. Odpowiednia ocena ryzyk jest tu niezmiernie ważna dla podjęcia przyszłych decyzji odnośnie do sposobów manipulacji zidentyfikowanymi zagrożeniami, a co za tym idzie – odnośnie do alokacji zasobów na wyznaczone przez proces zarządzania ryzykiem cele. Wskazanym jest zatem przeanalizowanie tego problemu bardziej szczegółowo, korzystając z osiągnięć rozwiniętych matematyczno-statystycznych metod.

Ryzyko w jednostkach samorządowym wynika w znacznej mierze z funkcjonowania dużej liczby złożonych i zmiennych podmiotów, zachodzących między nimi zależności, zmian w ich otoczeniu, ograniczonej możliwości kontrolowania oraz ich wyników. Głównym kierunkiem działań powinno być dążenie do ograniczenia, redukowania ryzyka.

## Bibliografia

1. http://www.centrum.bezpieczenstwa.pl/index.php/standardy-othermenu-16/55-iso-27001, 4.02.2017.
2. http://www.egospodarka.pl/25690,Bezpieczenstwo-systemow-informatycznych-rodzaje-zagrozen,1,20,2.html, 14.05.2017.
3. Kulińska E., Dornfeld A.: Kontrola zarządcza w jednostkach sektora finansów publicznych. Difin, Warszawa 2015.
4. Kulińska E., Dornfeld A.: Zarządzanie ryzykiem procesów: identyfikacja-modelowanie-zastosowanie. Oficyna Wydawnicza Politechniki Opolskiej, Opole 2009.
5. Nelson R.R., Sampat B.N.: Making Sense of Institutions as a Factor Shaping Economic Performance. „Journal of Economic Behaviour and Organization", January, Vol. 44, 2001.
6. North D.: Institutions, Institutional Change and Economic Performance. Cambridge University Press, Cambridge 1994.
7. Nowak A., Schefes W.: Zarządzanie bezpieczeństwem informacyjnym. AON, Warszawa 2010.
8. Odlanicka-Poczobutt M., Knop L.: Rozwój i funkcjonowanie sieci w świetle podejścia endogenicznego. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 89, Gliwice 2016.
9. Odlanicka-Poczobutt M., Kulińska E.: Kierunki rozwoju informacji prawnej w ramach gospodarki elektronicznej. Zeszyty Naukowe Uniwersytetu Szczecińskiego, s. Ekonomiczne Problemy Usług, nr 113, 2014.
10. Odlanicka-Poczobutt M.: Inercja instytucjonalna a innowacyjne rozwiązania w sądach powszechnych w sprawach cywilnych. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 89, Gliwice 2016.
11. Sienkiewicz P.: Teoria bezpieczeństwa systemów. AON, Warszawa 2005.
12. Staniek Z.: Uwarunkowania i wyznaczniki efektywności systemu instytucjonalnego, [w:] Pacho W. (red.): Szkice ze współczesnej teorii ekonomii. SGH, Warszawa 2005.