Zygmunt Mazur, Hanna Mazur, Teresa Mendyk-Krajewska

Politechnika Wrocławska

Wydział Informatyki i Zarządzania

Katedra Inżynierii Oprogramowania

e-mail: zygmunt.mazur@pwr.edu.pl, hanna.mazur@pwr.edu.pl, teresa.mendyk-krajewska@pwr.edu.pl

Ryzyko w sektorze publicznym w kontekście zintegrowanej informatyzacji

Kody JEL: H83, L86, M15

Słowa kluczowe: normy, zarządzanie ryzykiem, ZUS, sektor publiczny

Streszczenie. Rozwój technologii teleinformatycznych ma duży wpływ na intensyfikację wdrażania systemów informatycznych do podmiotów sektora publicznego. Dotychczasowe rozwiązania są zastępowane nowszymi, które wkrótce, jak pokazuje praktyka, są modernizowane i dostosowywane do aktualnych potrzeb i technologii. Zapewnienie ciągłości i niezawodności działania wymaga wiedzy na temat ryzyka, jego identyfikowania, analizy oraz odpowiedniego nim zarządzania. Celem artykułu jest analiza bieżącego stanu normatywnego dla jednostek sektora publicznego w zakresie zarządzania ryzykiem oraz wskazanie istotnych wyzwań w kontekście wprowadzanej informatyzacji i poszerzania listy usług świadczonych drogą elektroniczną.

Wprowadzenie

Przez ryzyko rozumiemy prawdopodobieństwo wystąpienia zdarzenia, negatywnie wpływającego na realizację zadań i określonych celów. Zdarzenia oddziałujące pozytywnie nie są przedmiotem naszych rozważań. Źródłem ryzyka, jako zdarzenia o negatywnych skutkach, może być otoczenie zewnętrzne (m.in. zmiany gospodarcze czy polityczne) lub czynniki wewnętrzne (np. modernizacja sprzętu, zmiana oprogramowania lub struktury organizacyjnej firmy). Zdarzenia te mogą być przyczyną utrudnień bądź zakłóceń w realizacji procesów biznesowych lub wręcz mogą uniemożliwiać ich przebieg i osiąganie założonych celów. Z tego powodu należy je identyfikować, aby móc właściwie nimi zarządzać.

Ministerstwo Cyfryzacji (MC) oraz Ministerstwo Rozwoju i Finansów realizują obecnie projekt „Od papierowej do cyfrowej Polski”, zgodny z Planem na rzecz odpowiedzialnego rozwoju, zakładający rozwój e-administracji i efektywnego systemu ochrony zdrowia, będących podstawowymi obszarami dla sprawnego funkcjonowania państwa.

Informatyzacja urzędów i szybki rozwój technologii informatycznych narzucają konieczność zmiany i dostosowywania aktów prawnych do nowych rozwiązań. Obecne przepisy w Polsce, dotyczące bezpieczeństwa teleinformatycznego zawarte są w różnych aktach prawnych, ustawach i rozporządzeniach. Żaden z aktów prawnych nie reguluje bezpieczeństwa teleinformatycznego państwa całościowo. Pośrednio dotyczą go m.in. ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawa o ochronie baz danych, prawo telekomunikacyjne, ustawa o finansach publicznych, ustawa o dostępie do informacji publicznej, ustawa o ochronie niektórych usług świadczonych drogą elektroniczną opartych na dostępie warunkowym, ustawa o ochronie informacji niejawnych. Mnogość dokumentów, projektów i inicjatyw w zakresie cyfryzacji państwa utrudnia ich analizę i jednoznaczną interpretację przepisów. Tym bardziej, że nawet na stronach internetowych MC¹ nie ma dat, które umożliwiłyby ocenę aktualności informacji.

27 września 2016 roku rząd przyjął Program Zintegrowanej Informatyzacji Państwa. Nadal jednak nie ma ustawy o krajowym systemie cyberbezpieczeństwa, która miała powstać do końca 2016 roku, ani jednolitego podejścia do interpretacji i stosowania zapisów w różnych aktach prawnych. Jest to poważny problem dla osób odpowiedzialnych za zapewnienie bezpieczeństwa w obszarze IT oraz za wykazanie należytego wykonywania swoich obowiązków w tym zakresie (Pietruszyński, 2016). Za ochronę teleinformatyczną w Polsce odpowiada wiele instytucji, m.in. Ministerstwo Obrony Narodowej, Ministerstwo Cyfryzacji, Ministerstwo Sprawiedliwości, Rada Ministrów, Komenda Główna Policji, Agencja Bezpieczeństwa Wewnętrznego, Rządowe Centrum Bezpieczeństwa oraz Urząd Komunikacji Elektronicznej.

Celem artykułu jest analiza bieżącego stanu normatywnego dla jednostek sektora publicznego w zakresie zarządzania ryzykiem oraz wskazanie istotnych wyzwań w kontekście powszechnej informatyzacji.

1. Identyfikacja i analiza ryzyka

Do prawidłowej identyfikacji ryzyka niezbędna jest znajomość obszaru działalności jednostki, jej celów i metod pracy, struktury organizacyjnej, zasobów i infrastruktury teleinformatycznej oraz zasad współpracy z podmiotami zewnętrznymi a także otoczenia zewnętrznego, wpływającego na dany podmiot. Ważne są wszelkie dotychczasowe doświadczenia, czyli zdarzenia z przeszłości, które mogły być lub były przyczyną

¹ Np. mc.gov.pl/projekty/gik-glowny-informatyk-kraju.

problemów bądź zakłóceń w działalności jednostki. Zarówno identyfikacja, jak i analiza ryzyka są procesami, które należy wykonywać systematycznie.

Analiza ryzyka IT jest przeprowadzana w celu ustalenia, w jakim stopniu systemy informatyczne są narażone (podatne) na ryzyko. To pociąga za sobą konieczność identyfikacji i oceny zagrożeń² dla systemów informatycznych z uwzględnianiem częstotliwości, z jaką mogą się pojawiać oraz szacowaniem skutków, w przypadku ich wystąpienia a także niewystąpienia. Podatność systemu na dane zagrożenie jest obliczana na podstawie oceny kosztu wpływu zagrożenia na działalność jednostki i szacunkowej częstości jego występowania.

Analiza ryzyka obejmuje inwentaryzację zasobów (wewnętrznych, zewnętrznych, ocenę ich krytyczności i aktualny stan ochrony), określenie potencjalnych zagrożeń naruszających bezpieczeństwo systemów informatycznych (mogą to być m.in. czynniki ludzkie, techniczne, prawne, organizacyjne, naturalne), zidentyfikowanie podatności potencjalnych luk i słabości systemów (m.in. dzięki testom penetracyjnym, doświadczeniu, wiedzy i intuicji pracowników/ekspertów) oraz określenie ryzyka i wpływu danego zagrożenia na realizację celów (z wykorzystaniem analizy jakościowej³, ilościowej⁴ oraz szacowania strat). Zidentyfikowane ryzyko można zaklasyfikować jako:

- istotne zagrożenie dla działalności firmy, wymagające dlategoszczególnej uwagi i monitorowania,
- istotne i wymagające dodatkowych działań,
- nieistne lub mało istotne zagrożenie, niewymagające szczególnej uwagi.

W zależności od klasyfikacji ryzyka, nadanego mu priorytetu, ważności i stanu akceptowalności – należy podjąć stosowne działania. Niestety, w wielu przypadkach ograniczeniem dla realizowania adekwatnych do zagrożenia działań są wymagane środki finansowe. Trudnością jest odpowiedni dobór mierników umożliwiających ewaluację korzyści i strat wynikających z wprowadzenia zarządzania ryzykiem i zatrudnienia specjalisty ds. zarządzania ryzykiem.

2. Ryzyko IT i zarządzanie nim

Sytuacją idealną i niemożliwą raczej do osiągnięcia jest podjęcie wszelkich działań zmierzających do całkowitego wyeliminowania ryzyka w sferze technologii informacyjnych (IT). Niestety, zmiany zachodzące w jednostkach sektora publicznego i w otoczeniu, zależność od nieprzewidywalnych warunków zewnętrznych (np. ustawowych, klimatycznych czy technologicznych) uniemożliwiają zredukowanie ryzyka

² Zagrożenie rozumiemy jako wszelkie możliwe niepożądane zdarzenie lub działanie, które może wpływać na system informacji, np. awaria sprzętu, pożar, nieuprawniony dostęp.

³ Wyrażoną w skali wartości informacji odnośnie do poufności, dostępności i integralności, np. nieistotna, niska, średnia wysoka, bardzo wysoka.

⁴ Wyrażoną w skali liczbowej lub w jednostkach walutowych.

IT do poziomu zerowego na stałe i wymuszają podejmowanie systematycznych działań w celu utrzymania ryzyka na akceptowalnym poziomie. Rosnąca liczba systemów teleinformatycznych i ich różnych konfiguracji oraz baz i rejestrów danych powoduje, że środowisko informatyczne jest coraz bardziej rozbudowane i skomplikowane. Systemy są ze sobą powiązane nie tylko w obrębie danego podmiotu, ale często komunikują się i są uzależnione od systemów i ludzi z zewnątrz. Rośnie także liczba osób z uprawnieniami dostępu do tych systemów i danych. Złożoność i rozległość infrastruktury (podlegającej często wielu różnym podmiotom) ma znaczący wpływ na zarządzanie ryzykiem w obszarze IT. Wiele danych jednak nie jest archiwizowanych ani odpowiednio chronionych. W Rozporządzeniu Ministra Rozwoju i Finansów z 27 grudnia 2016 roku w sprawie środków i warunków technicznych służących do przekazywania niektórych informacji przez podmioty nadzorowane przez Komisję Nadzoru Finansowego określono, że przekazywanie informacji odbywa się za pomocą Elektronicznego Systemu Przekazywania Informacji (ESPI) przy zachowaniu zasad bezpiecznego przekazu, zgodnie z aktualnymi standardami opracowanymi przez *Internet Engineering Task Force* opublikowanymi w postaci *Request For Comments* (RFC) stosowanymi adekwatnie do potrzeb w zakresie bezpieczeństwa transmisji danych.

W 2015 roku, z polskich firm i urzędów administracji publicznej, odnotowano 200 mln zgłoszeń o atakach, z czego 1,5 tys. wymagało działań specjalnych (Gadomska, 2016). Z badań firmy Intel przeprowadzonych w 2016 roku w Polsce, Czechach, Rumunii i na Węgrzech wynika, że 60% dużych przedsiębiorstw w Polsce (a także na Węgrzech) nie ma przygotowanego scenariusza działań na wypadek cyberataku. Przygotowanie w zakresie bezpieczeństwa IT w Polsce jest na znacznie niższym poziomie niż w Czechach (84% firm dysponuje odpowiednim planem) czy w Rumunii (72%) (Intel, 2016). Aż 68% pracowników urzędów samorządowych w Polsce uważa pocztę elektroniczną za najbardziej narażony na atak element sieci (Czubkowska, Sikora, Józwiak, 2016).

Najważniejsze ogniwa procesu zarządzania ryzykiem wymieniane w standardach to: identyfikacja zagrożeń, analiza ryzyka, ocena ryzyka, reakcja na ryzyko i działania zaradcze. Podejście do zarządzania ryzykiem może być różne ze względu na przyjęte kryterium, np. czas (ryzyko krótko- lub długoterminowe) czy zmiany otoczenia (ryzyko statyczne – niezwiązane z rozwojem technologicznym, lub dynamiczne – zależne od zmian).

Wobec zidentyfikowanego ryzyka mogą być podejmowane różne działania, m.in. wyeliminowanie jego źródła, akceptacja (tolerowanie) ryzyka lub unikanie go, zmiana jego skutków działania, zaniechanie działalności (przy zbyt dużym ryzyku) lub dzieleńie się nim z innym podmiotem (transfer ryzyka), np. przez ubezpieczenie zasobów. Przeprowadzając analizę ryzyka systemów IT pod kątem bezpieczeństwa (rozumianego jako zapewnienie poufności, dostępności i integralności danych) należy mieć na uwadze główny cel organizacji związany najczęściej z maksymalizacją korzyści i minimalizacją strat.

Dla nowo wdrażanego systemu informatycznego zarządzanie ryzykiem wiąże się z kontrolą jakości systemu (w tym także w zakresie bezpieczeństwa) i poświadczeniem

prawidłowości jego wdrożenia, z integracją z innymi systemami oraz z prawidłową migracją danych z poprzedniego systemu, jeśli takowy istniał.

W odniesieniu do systemów informatycznych, ryzyko dotyczy także konfiguracji zabezpieczeń, rozdziału ról i obowiązków personelu, ograniczeń w dostępie, automatyzacji i optymalizacji kontroli, zarządzania danymi, ich analizy i raportowania. Strategia zarządzania ryzykiem powinna wspierać proces podejmowania decyzji w zakresie sposobu postępowania z ryzykiem (jego unikania lub przeniesienia oraz wyboru narzędzi do jego redukcji lub całkowitej wyeliminowania).

3. Krajowe i międzynarodowe standardy w zakresie zarządzania ryzykiem

Istniejące standardy (wytyczne, kryteria) i normy (dokumenty opisujące standardy) dotyczące zarządzania ryzykiem mogą być punktem wyjścia do opracowania SZR – Systemu Zarządzania Ryzykiem lub ZZR – Zintegrowanego Zarządzania Ryzykiem (*Enterprise Risk Management* – ERM). Wśród dokumentów o istotnym znaczeniu dla intensywnie informatyzowanego sektora publicznego znajduje się wiele norm, zaleceń i dobrych praktyk dotyczących zarządzania, kontroli finansów, wytwarzania oprogramowania, świadczenia usług drogą elektroniczną, ładu korporacyjnego.

Wśród międzynarodowych standardów dotyczących zarządzania ryzykiem wysoko oceniane przez ekspertów są: europejski standard FERMA, amerykański COSO II oraz międzynarodowy standard ISO 31000 (EnergSys, 2016).

FERMA to europejski standard *Federation of European Risk Management Associations* opracowany w 2003 roku przez trzy brytyjskie organizacje: *The Institute of Risk Management* (Instytut Zarządzania Ryzykiem), *The Association of Insurance and Risk Managers* (Stowarzyszenie Menedżerów Ubezpieczeniowych i Zarządzających Ryzykiem) i *ALARM The National Forum for Risk Management in the Public Sector* (Krajowe Forum na rzecz Zarządzania Ryzykiem w Sektorze Publicznym). W dokumencie dotyczącym standardu opisano proces zarządzania ryzykiem wraz z przykładowymi narzędziami i scenariuszami działania w celu ustalenia jednolitego ogólnoeuropejskiego podejścia do procedur zarządzania ryzykiem, począwszy od sformułowania ogólnych celów organizacji aż do identyfikacji, oceny i ograniczania ryzyka, a nawet przeniesienia ryzyka na ubezpieczyciela.

COSO II – wprowadzony w 1992 roku amerykański standard COSO I (*The Committee of Sponsoring Organizations of the Treadway Commission*) dotyczył kontroli wewnętrznej w przedsiębiorstwie, a COSO II to jego modyfikacja z 2004 roku, uwzględniająca całościowe zarządzanie ryzykiem i łącząca cele strategiczne, operacyjne, sprawozdawczości oraz zgodności z prawem z wszelkimi elementami i jednostkami organizacyjnymi. Standard ten znany jako **COSO ERM**, to zintegrowana struktura ramowa dla zarządzania ryzykiem korporacyjnym, którą można zastosować do zbudowania dowolnego SZR lub ZZR.

ISO 31000 Risk Management: Guidelines for principles and implementation of risk management – zasady i wytyczne dotyczące zarządzania ryzykiem, to rodzina międzynarodowych norm, która obejmuje:

- ISO 31000:2009 *Risk management – Principles and guidelines* (Zarządzanie ryzykiem – Zasady i wytyczne),
- ISO/IEC 31010:2009 *Risk management – Risk assessment techniques* (Zarządzanie ryzykiem – Metody szacowania ryzyka),
- ISO Guide 73:2009 *Risk management: Vocabulary – Guidelines for use in standards* (Zarządzanie ryzykiem: Słownictwo – Wytyczne dla standardów).

AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines (Zarządzanie ryzykiem – Zasady i wytyczne) to australijski i nowozelandzki zaadaptowany standard zarządzania ryzykiem ISO 31000:2009, który zastąpił normę AS/NZS 4360:2004.

BS 6079-1:2010 Project management. Principles and guidelines for the management of projects. Part 3: Guide to the management of business related project risk – trzecia część (z czterech) normy opracowanej przez British Standard Institution, dotycząca opisu procesu zarządzania ryzykiem. Prace standaryzacyjne BSI dotyczące zarządzania projektami są prowadzone od 1968 roku.

COBIT (Control Objectives for Information and related Technology) to zestaw wskazówek z zakresu IT Governance dotyczących dostosowywania technologii informatycznych do przyjętej strategii i celów zgodnie z obowiązującymi standardami (regulacjami). Opracowany przez ISACA dokument (obecnie wersja 5) jest zbiorem dobrych praktyk dla audytorów systemów informatycznych i zawiera opisy procesów dotyczących zarządzania ryzykiem. Metodologia COBIT zalecana jest do stosowania w jednostkach wykorzystujących technologie informatyczne m.in. do zarządzania ryzykiem w bankowych systemach informatycznych i telekomunikacyjnych.

NIST – opracowane przez amerykański National Institute of Standards and Technology wytyczne do zarządzania ryzykiem w systemach teleinformatycznych.

Bazylea III – opracowany przez Bazylejski Komitet Nadzoru Bankowego zbiór standardów i zasad dotyczących zarządzania ryzykiem banków i panowania nad nim, m.in. w zakresie ochrony kapitału przez określenie minimalnych wymogów kapitałowych na ryzyko kredytowe, rynkowe, operacyjne i systemów.

Risk IT – ramy obejmujące kompleksowo wszelkie źródła ryzyka wynikające ze stosowania technologii informatycznych oraz kompleksowe zarządzanie ryzykiem (ZR), jego akceptację (*risk appetite*) i tolerancję. Standard Risk IT został wydany w 2009 roku przez międzynarodowe stowarzyszenie ISACA. Podstawowe zasady Risk IT to: dostosowywanie zarządzania ryzykiem do celów biznesowych a zarządzania ryzykiem IT do całościowego procesu ZR; bilansowanie kosztów i korzyści zarządzania ryzykiem IT; promowanie otwartej komunikacji w sprawie ryzyka IT; rzetelne definiowanie i przydzielanie odpowiedzialności. Ocena ryzyka IT musi być procesem ciągłym i powinna być częścią codziennych działań. Informacje w ZR powinny być zwarte, użyteczne, jedno-

znaczne, przekazywane w odpowiednim czasie i do właściwego odbiorcy oraz udostępniane tylko w uzasadnionych wypadkach osobom uprawnionym, czyli osobom, którym są one niezbędne do wykonywania swoich obowiązków (zasada *need to know*).

ITIL (*Information Technology Infrastructure Library*) to zbiór zaleceń dla działów informatyki, wykorzystywanych do efektywnego i skutecznego oferowania usług informatycznych (*IT service management* – ITSM). Model ITIL jest bardzo często stosowany także w sektorze publicznym ze względu na jego kompleksowe podejście i opis działania profesjonalnego dostawcy usług IT. Wersja trzecia (ITIL v3) z 2007 roku obejmuje pięć części (faz w cyklu życia usługi): *Service Strategy* (Strategia usługi), *Service Design* (Projektowanie usługi), *Service Transition* (Przekazanie usługi), *Service Operation* (Eksploatacja usługi), *Continual Service Improvement* (Ciągła poprawa usługi).

ISO/IEC 27005:2011 *Information technology – Security techniques – Information security risk management* oraz polska norma **PN-ISO/IEC 27005:2014-01** *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji* – zawierają wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji oraz rozwinięcie ogólnych koncepcji zawartych w normie ISO/IEC 27001. Normę ISO/IEC 27005 opracowano w celu wspomagania organizacji w zadawalającej realizacji polityki bezpieczeństwa informacji opartej na zarządzaniu ryzykiem. Pozostałe normy z rodziny ISO/IEC 27000 to:

- ISO/IEC 27002:2013 *Information technology – Security techniques – Code of practice for information security controls (second edition)* – wytyczne dotyczące Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- ISO/IEC 27003:2010 *Information security management system implementation guidance* – porady i wskazówki pomocne przy wdrażaniu SZBI,
- ISO/IEC 27004:2016 *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation* – wytyczne przydatne do monitorowania, pomiaru i analizy wskaźników w zarządzaniu bezpieczeństwem informacji.

Podejście do zarządzania ryzykiem może być bardzo różne, stąd standardy dotyczące tego procesu różnią się między sobą (Machowiak, Staniec, 2007).

W 2013 roku na XXI Kongresie INTOSAI (*International Organization of Supreme Audit Institutions* – Międzynarodowa Organizacja Najwyższych Organów Kontroli) opracowano trzeci poziom Międzynarodowych Standardów Najwyższych Organów Kontroli (**ISSAI**) dotyczący podstawowych zasad kontroli. Celem opracowania standardu było określenie jednolitych ram, umożliwiających profesjonalne przeprowadzanie kontroli w sektorze publicznym, dla wszystkich naczelnich organów kontroli. Kontrola powinna być realizowana w sposób oszczędny, wydajny, skuteczny i zgodny z przyjętym harmonogramem. Zadaniem INTOSAI jest wspieranie swoich członków w realizacji kontroli sektora publicznego poprzez opracowywanie standardów i wytycznych, umożliwienie wymiany informacji i doświadczeń, organizowanie konferencji tematycznych, i co trzy lata kongresów. Standardy trzeciego poziomu dla Najwyższych

Organów Kontroli (NOK) definiują Podstawowe zasady kontroli w sektorze publicznym – ISSAI 100, Podstawowe zasady kontroli finansowej – ISSAI 200, Podstawowe zasady kontroli wykonania zadań – ISSAI 300, oraz Podstawowe zasady kontroli zgodności (standardy sprawozdawcze kontroli państwowej – ISSAI 400).

NOK odgrywają istotną rolę we wzmacnianiu administracji sektora publicznego, kładąc nacisk na przestrzeganie zasad przejrzystości, rozliczalności, nadzoru nad jednostką i wykonywaniem zadań. Odpowiednie wskazówki w tym zakresie zawiera standard **ISSAI 20** – Zasady przejrzystości i rozliczalności. Kontrole przeprowadzane przez NOK muszą być niezależne, obiektywne i wiarygodne w zakresie weryfikacji i oceny, czy wszelkie publiczne przedsięwzięcia, systemy i instytucje funkcjonują zgodnie z zasadami oszczędności, wydajności i skuteczności, oraz czy istnieje obszar wymagający poprawy. W grudniu 2008 roku, na podstawie Międzynarodowego Standardu Kontroli Jakości 1, powstał dokument **ISSAI 40** – Kontrola jakości w NOK, określający ramy pełnej kontroli NOK (m.in. finansowej, zgodności, wykonywania zadań).

Zasady zawarte w **ISSAI 200** dotyczą kontroli finansowej, w tym także wykorzystywania technologii informatycznych, znaczących dla sprawozdań finansowych operacji w systemie informacyjnym niebędących transakcjami oraz sposobu przeprowadzania korekt w zapisach księgowych (INTOSAI, 2016, s 51).

Obecnie trwają prace nad standardem **ISSAI 5300**, dotyczącym kontroli informatycznej – w pierwszej kolejności uwzględniającym tylko kwestie podstawowe, a docelowo także ryzyko informatyczne, kontrolę inwestycji IT oraz kontrolę informatyczną (w ramach kontroli finansowej i innych kontroli). Jest to jeden z ważniejszych projektów INTOSAI, w którym uczestniczy także Polska. Wynikami prac jest zainteresowana także europejska Grupa robocza ds. IT. W grudniu 2016 roku, podczas XXII Kongresu INTOSAI w Abu Dhabi, przedstawiono zaktualizowany Kodeks Etyki INTOSAI (ISSAI 30 *Code of Ethics*) oraz standard ISSAI 5300.

Dokument **ISSAI 5310** *Information System Security Review Methodology – A Guide for Reviewing Information System Security in Government Organisations* jest przewodnikiem umożliwiającym przegląd systemu bezpieczeństwa informacji (*Information System Security – ISS*) w jednostkach rządowych.

Istotnym problemem w zarządzaniu ryzykiem jest oparcie wielu działań na subiektywnym odczuciu, wiedzy i doświadczeniu pracowników. Wyniki przeprowadzanych audytów i kontroli mogą być nierzetelne, wybiórcze, zbyt pesymistyczne lub zbyt optymistyczne, eksponujące zalety a pomijające wady (lub odwrotnie). Szybko zmieniające się nowe technologie powodują, że opracowane wcześniej standardy ich nie uwzględniają, przez co mogą być pominięte w zarządzaniu ryzykiem lub niedostatecznie zarządzane.

Źródłem ryzyka IT może być oprogramowanie, które obecnie bywa bardzo złożone, wielomodułowe, wytwarzane przez różne zespoły programistyczne. Wskaźniki *defect density* (stosunek liczby błędów do liczby linii kodu) wynoszą ok. 15–50 błędów na 1 tys. linii dostarczonego kodu. Minimalizacja ryzyka w sektorze publicznym jest

związana z jak najlepszym wytwarzaniem oprogramowania na jego potrzeby. Normą wspomagającą wytwarzanie bezpiecznego oprogramowania jest ISO/IEC 15504-5:2012, dotycząca oceny najważniejszych procesów związanych z zarządzaniem wytwarzania oprogramowania poprzez zdefiniowanie pięciu poziomów dojrzałości firmy:

1. *Performed* – procesy tworzenia oprogramowania realizowane są bez formalnego podejścia.
2. *Managed* – procesy są zarządzane biernie i zorientowane na rozwiązywanie problemów.
3. *Established* – systematyczne podejście oparte o zdefiniowane procesy.
4. *Predictable* – doskonalenie i dokonywanie pomiarów umożliwiających ocenę osiągania celów.
5. *Optimising* – bardzo wysoki poziom organizacyjny i innowacyjność.

Norma ISO/IEC 15504, znana jako SPICE (*Software Process Improvement and Capability dEtermination*), pozwala na doskonalenie procesów związanych z wytwarzaniem oprogramowania o wysokiej jakości i niezawodności dla systemów o krytycznym znaczeniu, np. finansowych, medycznych czy transportowych.

W dokumentach dotyczących cyberbezpieczeństwa Polski (strategia, Doktryna cyberbezpieczeństwa, Polityka Bezpieczeństwa Cyberprzestrzeni RP), dostępnych na stronach internetowych MC i CERT, zarządzanie ryzykiem traktowane jest priorytetowo. W celu osiągnięcia akceptowalnego poziomu bezpieczeństwa, zakłada się, że odpowiednie jednostki administracji rządowej do 31 stycznia każdego roku będą przekazywały do ministra ds. informatyzacji sprawozdanie podsumowujące wyniki szacowania ryzyka według wzorca opracowanego przez ministra. Sprawozdanie powinno zawierać ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów zdiagnozowanych w każdym z sektorów, w których poszczególne instytucje działają, i za które odpowiada. W wielu jednostkach zagadnienie to jest marginalizowane i traktowane jako zbędny obowiązek. Często osoby odpowiedzialne za bezpieczeństwo bagatelizują rzetelną analizę ryzyka. Ważną rolę w standaryzacji działań administracji publicznej przez odpowiednie przygotowanie systemów IT odrywają Krajowe Ramy Interoperacyjności, minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych (KRI, 2012).

Od 16 czerwca 2016 roku obowiązuje Ustawa z 25 lutego 2016 roku o ponownym wykorzystywaniu informacji sektora publicznego, w której wprowadzono duże zmiany w zakresie informacji wytwarzanych i posiadanych przez organy władzy publicznej, jednostki organizacyjne samorządu terytorialnego i inne podmioty sektora finansów publicznych oraz spółki państwowe i samorządowe. Zmiany te dotyczą m.in. dostępu do informacji publicznej oraz ochrony danych osobowych. W tym kontekście istotne jest rozróżnianie pojęć informacja publiczna i informacja sektora publicznego, dostęp do informacji publicznej, a jej ponowne wykorzystanie.

Zasadnicze zmiany związane z analizą ryzyka w sektorze publicznym (i nie tylko) wynikają z:

- unijnego rozporządzenia o ochronie danych osobowych GDPR (*General Data Protection Regulation*) z 27 kwietnia 2016 roku (Sobczak, 2016),
- eIDAS – rozporządzenia Parlamentu Europejskiego (PE) i Rady, w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, zatwierdzonego 1 lipca 2016 roku,
- Dyrektywy NIS (*Network and Information Security*) przyjętej przez PE 6 lipca 2016 roku.

Rozporządzenia te wymuszają konieczność zmian w wielu aktach prawnych, procedurach i przepisach w jednostkach administracyjnych. Zasadniczym elementem tych zmian było uchwalenie w Polsce 5 września 2016 roku Ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw.

4. Case study – zarządzanie ryzykiem w ZUS

Do podmiotów sektora publicznego należą m.in. organy administracji rządowej, samorządu terytorialnego i kontroli państwa, publiczne uczelnie wyższe, Narodowy Fundusz Zdrowia, Zakład Ubezpieczeń Społecznych (ZUS), jednostki budżetowe i ochrony zdrowia, sądy i trybunały. Zestawiając ich pełną listę z zakończonymi, trwającymi lub planowanymi projektami informatycznymi otrzymujemy obraz długoterminowego, kosztownego i szeroko zakrojonego przedsięwzięcia dotyczącego informatyzacji państwa i wprowadzania e-usług. Zarządzanie ryzykiem w pewnych obszarach, jak np. w ochronie informacji niejawnych, ma charakter obligatoryjny i ściśle wiąże się z wypełnianiem wymagań dotyczących bezpieczeństwa teleinformatycznego.

ZUS, jako jednostka sektora publicznego, podlega pod ustawę o finansach publicznych, pod standardy kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF, nr 15, poz. 84) oraz pod wytyczne dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (Dz. Urz. MF z 2012 r., poz. 56).

W podsumowaniu z 2013 roku dotyczącym ZUS stwierdzono brak narzędzi informatycznych wspierających proces zarządzania ryzykiem oraz brak wiedzy w zakresie efektywnego zastosowania procedur podnoszących poziom bezpieczeństwa, brak systematycznej i kompleksowej analizy ryzyka, brak lub znikomą wiedzę na temat znaczenia zarządzania ryzykiem, niski poziom percepcji ryzyka, brak świadomości na temat częstotliwości, rozmiarów i skutków potencjalnego ryzyka, brak świadomości pracowników, że wszyscy zarządzają ryzykiem, brak wiedzy i umiejętności w zakresie zarządzania ryzykiem przez kierownictwo wyższego i średniego szczebla (Jedynak, 2013). Zasady postępowania w zakresie zarządzania ryzykiem na rok 2015 określono w *Planie działalności Zakładu Ubezpieczeń Społecznych na rok 2015*, przy czym jako główny aspekt określono zapewnienie odpowiedniego poziomu ochrony zasobów i ich efektywnego wykorzystania, zgodnie z zasadą gospodarności środkami publicznymi. W 2015 roku działania podejmowane w ramach zarządzania ryzykiem koncentrowały się na utrzymywaniu ryzyka na akceptowalnym poziomie, poprzez zapewnianie kom-

pleksowej identyfikacji ryzyka, jego prawidłowego zdefiniowania oraz wymiernej oceny, w celu skutecznego zarządzania nim i monitorowania go. Proces zarządzania ryzykiem realizowany był w kilku dokumentowanych etapach: identyfikacja ryzyka, pomiar i ocena ryzyka, reakcja na ryzyko, monitorowanie i przegląd ryzyka, komunikowanie ryzyka. W grudniu 2015 roku ZUS opublikował dokument *Strategia Zakładu Ubezpieczeń Społecznych na lata 2016–2020*, w którym określono, że będą podejmowane inicjatywy związane z wdrażaniem efektywnych systemów bezpieczeństwa sieci teleinformatycznych, z monitorowaniem bezpieczeństwa teleinformatycznego oraz będzie prowadzona stała analiza ryzyka. Wybrane cele i ich mierniki przedstawiono w tabeli 1.

Tabela 1. Wybrane cele ZUS i ich mierniki na lata 2016–2020

Cel		Miernik	Poziom bazowy na koniec 2014 r.	Poziom docelowy na koniec 2020 r.
Kod	Opis			
P1.3	doskonalenie systemu zarządzania bezpieczeństwem informacji	procent pozytywnie zakończonych testów ciągłości działania	0%	100%
		stopień wdrożenia Systemu Monitorowania Bezpieczeństwa Środowiska Teleinformatycznego	0%	100%
R1.2	integracja i konsolidacja aplikacji systemów IT	liczba zintegrowanych aplikacji angażowanych w obsługę całości procesu biznesowego	zostanie ustalony w I kw. 2017 r.	zostanie ustalony w I kw. 2017 r.
R1.3	wdrażanie interoperacyjnych rozwiązań IT w celu poprawy dostępu i poziomu świadczonych usług	liczba wykorzystywanych przez aplikacje usług w architekturze SOA (<i>Service-Oriented Architecture</i>)	zostanie ustalony w I kw. 2017 r.	zostanie ustalony w I kw. 2017 r.
R1.4	zbudowanie i wdrożenie narzędzi i rozwiązań wspierających potencjał analityczny ZUS	stopień dojrzałości środowiska Business Intelligence	2	3
		stopień wdrożenia Hurtowni Danych	0%	nie mniej niż 80%
R1.5	optymalizacja rozwiązań organizacyjnych służących realizacji usług i procesów	liczba odstępstw od standardu w strukturach organizacyjnych	205	spadek

Zródło: opracowanie własne na podst. *Strategia Zakładu Ubezpieczeń Społecznych na lata 2016–2020*.

Ze względu na specyfikę ZUS, w którego gestii leży kontrola środków publicznych (płatności składek ubezpieczeniowych), planowane jest wdrożenie analizy ryzyka (identyfikowanie zagrożeń, nadawanie im priorytetów, szacowanie potencjalnych strat,

proponowanie postępowania z ryzykiem) oraz podniesienie efektywności działań kontrolnych prowadzonych przez pracowników ZUS.

W celu poprawy komunikacji wewnętrznej i z klientami planowane są dalsze prace nad elektronicznym systemem obiegu dokumentów. Aby sprostać wysokim oczekiwaniom klientów i świadczyć usługi wysokiej jakości, konieczne jest wdrażanie nowych rozwiązań technologicznych i systemów teleinformatycznych. Ponadto, konieczna jest integracja systemów, zapewnienie interoperacyjności rejestrom i systemom, w celu umożliwienia współdziałania oraz dalszego wykorzystywania otrzymywanych danych w różnych postaciach (w ramach ZUS, a także w kontaktach ZUS-u z podmiotami zew.). W celu umożliwienia otwartego dostępu do danych publicznych rozwijany będzie Portal Statystyczny ZUS.

Na rynku są dostępne narzędzia do zarządzania ryzykiem, np. e-risk, z którego korzysta administracja rządowa i samorządowa. Wśród branż wykorzystujących to narzędzie dominują: administracja publiczna, publiczna ochrona zdrowia, finanse i bankowość, sektor energetyczny, przemysł spożywczy oraz uczelnie wyższe. Najczęściej system e-risk jest wykorzystywany w odniesieniu do norm ISO 31000, ISO 27005, COSO II, Kontroli Zarządczej oraz Systemu Przeciwdziałania Zagrożeniom Korupcyjnym/BS 10500.

Podsumowanie

Strategie zarządzania ryzykiem dotyczą zazwyczaj czterech kluczowych obszarów: zarządzania strategicznego i procesowego ludzi, zmian organizacyjnych oraz technologii teleinformatycznych. Istotą dobrego zarządzania ryzykiem jest zachowanie staranności, systematyczności, czujności i elastyczności w ochronie zasobów. Należy eksponować zasadę zachowania czujności przez uświadamianie zagrożeń zarówno pracownikom sektora publicznego, jak i obywatelom korzystającym z jego usług oraz rozwijanie umiejętności wykrywania pozytywnych i negatywnych wzorców zachowań w celu ochrony ważnych zasobów.

W kontekście zarządzania ryzykiem w sektorze publicznym należy także uwzględnić dwa obserwowane trendy – wykorzystywanie firmowych urządzeń teleinformatycznych do celów prywatnych oraz wykorzystywanie urządzeń prywatnych do realizacji zadań służbowych (BOYD – *Bring Your Own Device*), które generują dodatkowe ryzyko dla bezpieczeństwa systemów.

W celu prawidłowego zarządzania ryzykiem w sektorze publicznym konieczne są ciągłe działania w edukacji pracowników w tym zakresie, promowanie dobrych praktyk i przykładów korzyści osiągniętych dzięki wdrożeniu rozwiązań kontroli zarządczej, definiowanie przez osoby decyzyjne mierzalnych celów, mierników ich realizacji oraz osób odpowiedzialnych za ich realizację. Konieczna jest ocena działań i rozliczanie osób zarówno podejmujących decyzje, jak i odpowiedzialnych za wyniki i zarządzanie ryzykiem w danym obszarze.

Bibliografia

- Czubkowska, S., Sikora, P., Jóźwiak, Z. (2016). *Adminstracja przygotowana na cyberatak? Dziś nie, ale ma być lepiej*. Pobrano z: serwisy.gazetaprawna.pl (20.05.2016).
- EnergSys (2016). *Międzynarodowe standardy w zakresie zarządzania ryzykiem*. Pobrano z: ryzykoprojektowe.pl/poznaj-risky-project/ryzyko-w-projekcie-baza-wiedzy/miedzynarodowe-standardy-w-zakresie-zarzadzania-ryzykiem (20.12.2016).
- Gadomska, M. (2016). *NIK ostrzega: Systemy państwowe są zagrożone. Ministerstwo Cyfryzacji szykuje rewolucję*. Pobrano z: serwisy.gazetaprawna.pl (20.05.2016).
- Intel (2016). Pobrano z: intel.pl/content/www/pl/pl/it-managers/it-security-large-companies-report-2016.html (20.12.2016).
- INTOSAI (2016). Standardy ISSAI 100, ISSAI 200, ISSAI 300, ISSAI 400, NIK.
- Jedynak, M. (2013). *Wdrażanie zarządzania ryzykiem w Zakładzie Ubezpieczeń Społecznych*. Warszawa. Pobrano z: zus.pl/warsztaty/pliki/Warsztaty_4_Prezentacja_2.ppt.
- KRI (2012). Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 31 maja 2012.
- Machowiak, W., Staniec, I. (2007). *Nie ma jednego sposobu zarządzania ryzykiem*. Pobrano z: www.cxo.pl/news (20.12.2016).
- Pietruszyński, P. (2016). *Kto i na ile odpowiada za cyberbezpieczeństwo w firmie*. Pobrano z: computerworld.pl (16.12.2016).
- Sobczak, K. (2016). *800 przepisów trzeba przejrzeć przed wdrożeniem unijnych zasad ochrony danych*. Pobrano z: www.lex.pl (8.08.2016).

PUBLIC SECTOR RISK IN THE CONTEXT OF INTEGRATED COMPUTERIZATION

Keywords: standards, risk management, ZUS, public sector

Summary. Progress in ICT development intensifies the deployment of information systems in public sector entities. Existing solutions are replaced with newer, which again will soon be modernized and adapted to new needs and technology solutions. Ensuring continuity and reliability requires knowledge and ability to identify risks, their analysis and appropriate management. This article aims to analyze the current state of the art and identify major challenges for public sector entities in the field of risk management in the context of computerization roll-out and expansion of the number of services provided electronically.

Translated by Zygmunt Mazur

Cytowanie

Mazur, Z., Mazur, H., Mendyk-Krajewska, T. (2017). Ryzyko w sektorze publicznym w kontekście zintegrowanej informatyzacji. *Ekonomiczne Problemy Usług*, 1 (126/2), 371–384. DOI: 10.18276/epu.2017.126/2-37.