Ekspertyzy i opracowania

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Nr 115, 2020

www.nist.gov.pl

Zarządzanie bezpieczeństwem informacji w jst

dr hab. Małgorzata Ganczar,
Katolicki Uniwersytet Lubelski Jana Pawła II,
Wydział Prawa, Prawa Kanonicznego i Administracji

W ostatnich latach skala zbierania i wymiany informacji w jednostkach samorządu terytorialnego diametralnie wzrosła, a dzięki technologii ICT[1] na niespotykaną dotąd skalę przetwarzają dane w ramach realizacji nałożonych na nie zadań. Dodatkowo wzrosły oczekiwania społeczne dotyczące z jednej strony usprawnień w zakresie funkcjonowania usług elektronicznych administracji publicznej, z drugiej strony odpowiedniego zabezpieczenia danych przed dostępem osób nieupoważnionych. Ponadto sama administracja publiczna w coraz większym stopniu komunikują się wzajemnie za pośrednictwem środków komunikacji elektronicznej w celu załatwienia spraw. Dlatego zapewnienie bezpieczeństwa przetwarzania informacji w jednostkach samorządu terytorialnego staje się jednym z najistotniejszych wyzwań. Niewłaściwe zarządzanie bezpieczeństwem informacji może doprowadzić do wycieku, utraty lub sfałszowania informacji będących w dyspozycji j.s.t., a niewykluczony jest także paraliż pracy urzędu. Postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie bezpieczeństwa informacji, a to wymaga wprowadzenia stabilnych, spójniejszych ram ochrony oraz zdecydowanego ich egzekwowania tak aby prawo w zakresie wdrażania systemów zarządzania bezpieczeństwem informacji nie było ignorowane.

Obecne uwarunkowania prawne wskazują na potrzebę wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI) w jednostkach samorządu terytorialnego. Należy podkreślić, że SZBI jest przedsięwzięciem długoterminowym, które po zakończeniu projektowej fazy wdrożenia przechodzi w fazę utrzymania, z założonymi rezultatami oraz długookresowym wpływem na wdrażający podmiot i jego otoczenie. Wyniki kontroli przeprowadzanych przez Najwyższą Izbę Kontroli wskazują na liczne uchybienia w tym zakresie. W wyniku przeprowadzonej w 2014 r. kontroli wdrażania wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności nieprawidłowości w obszarze zapewnienie bezpieczeństwa systemów informatycznych stwierdzono w 87% skontrolowanych urzędów miast. Kontrola NIK z 2016 r. dotycząca *Systemu Rejestrów Państwowych* wykazała, że kierownicy kontrolowanych urzędów na ogół nie przywiązywali dostatecznej wagi do zapewnienia bezpieczeństwa przetwarzania informacji z wykorzystaniem tego systemu, w którym przetwarzane są bardzo istotne dane o obywatelach (m.in.: imię, nazwisko, nr PESEL, adres). W szczególności, w 62% skontrolowanych urzędów miast nie opracowano i nie wdrożono polityk bezpieczeństwa informacji, w 38% badanych urzędów miast wystąpiły nieprawidłowości w zakresie blokowania lub odbierania dostępu do systemu byłym pracownikom, a w 23% badanych urzędów nie przeprowadzano obowiązkowego corocznego audytu bezpieczeństwa informacji[2]. Kontrola przeprowadzona w latach 2017-2018 wykazała w 61% skontrolowanych urzędów brak systemowego podejścia do zapewnienia bezpieczeństwa informacji. W 74% badanych urzędów brak było pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych, co w przypadku wystąpienia poważnej awarii lub innego zdarzenia losowego (zalanie, pożar, kradzież), może znacząco utrudnić szybkie odtworzenie infrastruktury i zapewnienie ciągłości świadczenia usług dla obywateli. W wielu skontrolowanych urzędach j.s.t. nie dostrzegano występujących zagrożeń. W 48% jednostek nie dokonywano analiz ryzyka, a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji. Kontrola wykazała, że w części urzędów j.s.t. zasady mające na celu zwiększenie

1 Information and Communication Technologies.

2 *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego,* Najwyższa Izba Kontroli, Warszawa 2019, s. 6.

bezpieczeństwa przetwarzania danych nie były przestrzegane. W ponad 80% skontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych. W zakresie uzyskiwania dostępu do systemów informatycznych, w ponad połowie kontrolowanych urzędów (57%) ustanowione zasady nie były przestrzegane, np. użytkownicy używali haseł do systemów informatycznych krótszych niż wymagane. W 56% jednostek wykorzystywano komputery z zainstalowanym systemem operacyjnym bez wsparcia producenta, a w 48% urzędów stwierdzono nieprawidłowości w zakresie tworzenia, przechowywania oraz weryfikacji kopii zapasowych danych[3].

Administracja publiczna stoi obecnie przed wyzwaniem integrowania baz danych zamiast tworzenia odrębnych systemów teleinformatycznych do obsługi zasobu informacyjnego jednej kategorii. Jest to zgodne także z kierunkiem jaki wskazuje się z projekcie nowego Program Zintegrowanej Informatyzacji Państwa – Program rozwoju na lata 2019-2022 (maj 2019 r.), w ramach którego nacisk kładzie się na zapewnienie interoperacyjności, która umożliwi sprawną współpracę instytucji w realizacji złożonych procesów administracyjnych i wymianę informacji. W PZIP wskazuje się na problem w postaci powielania danych na poziomie centralnym, regionalnym i lokalnym, brak ich ponownego wykorzystywania w wystarczającym stopniu, co skutkuje zwielokrotnionymi nakładami na gromadzenie danych i niespójnością informacyjną. Rozproszone i nieskoordynowane zarządzanie zasobami informacyjnymi powoduje ponoszenie wysokich kosztów budowy i utrzymania systemów i rejestrów publicznych.

W tym miejscu warto wskazać na konieczność właściwego rozumienia pojęć: systemu informacyjnego i systemu teleinformatycznego. W doktrynie[4] system informacyjny określany jest jako wielopoziomowa struktura, pozwalająca użytkownikowi na transformowanie informacji wejściowych w wyjściowe za pomocą określonego modelu i przy zastosowaniu określonych procedur. Jest centralnym ogniwem koordynującym procesy wewnątrz organizacji i integrującym go z otoczeniem zewnętrznym. System informacyjny powinien umożliwiać: pozyskiwanie informacji; przesyłanie informacji pomiędzy co najmniej dwoma użytkownikami; przechowywanie – magazynowanie informacji; przetwarzanie informacji; udostępnianie informacji w określonym miejscu i czasie[5]. System informacyjny powinien: dostarczać kompleksowych i aktualnych informacji, zapewniać selektywne i skuteczne wykorzystanie informacji oraz właściwą wymianę informacji między komórkami organizacyjnymi, przełożonymi i podwładnymi w obydwu kierunkach; zapewniać prostotę w użytkowaniu i zapewnieniu stałej, automatycznej metody pozyskiwania informacji z ustalonych źródeł; umożliwiać natychmiastowe pozyskanie danych, nawet z najniższego poziomu zarządzania, wyszukiwanie i kojarzenie informacji z różnych źródeł, przedstawienie danych i wyników ich analiz w różnych układach sprawozdawczych; zapewnić przepływ informacji oparty na sprzężeniach zwrotnych[6].

Pojęcie systemu informacyjnego należy odróżniać od pojęcia systemu informatycznego[7]. System informacyjny rozumiany będzie jako wydzielona część systemu społecznego, gospodarczego lub technicznego, składająca się z takich elementów, jak ludzie, procesy informacyjne, zasoby danych, realizująca swoje funkcje i cele. Do głównych zadań systemu informacyjnego należy zaspokajanie potrzeb informacyjnych organizacji, tak aby możliwe było podejmowanie trafnych decyzji. Skomputeryzowanie wyodrębnionej części systemu informacyjnego staje się systemem informatycznym[8] i jako część systemu informacyjnego wspomaga organizację w realizacji jej zadań. System informacyjny wymaga wsparcia systemów informatycznych, które określane są mianem formalnych systemów komputerowych umożliwiających zbieranie, przetwarzanie, udostępnianie i integrację danych pochodzących z różnych źródeł, by w odpowiednim czasie dostarczyć niezbędnych informacji i wspomóc proces podejmowania decyzji[9]. Zgodnie z art. 3 pkt 3 ustawy o informatyzacji system teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz.U. z 2018 r. poz. 1954, 2245 i 2354).

System informatyczny w znaczący sposób porządkuje przepływ informacji wewnątrz organizacji. Ogólnie rzecz ujmując systemy informatyczne to technologie, które pozwalają na

3 Tamże, s.7.

4 Ficoń K., *Logistyczne systemy informacyjne podstawą budowy informatycznych systemów zarządzania*. [w:] Systemy logistyczne Wojsk. Warszawa 1998; Kisielnicki J., H. Sroka. *Systemy informacyjne biznesu*, Warszawa 2001; Walasek J., Projektowanie systemu informacyjnego organizacji, Zeszyty Naukowe Politechniki Śląskiej, 2015, seria: Transport, z. 87.

5 Kucyk J., *Nowoczesne technologie w logistyce*, Warszawa 2013.

6 Janczak J., *Systemy informatyczne wspomagania zarządzania i dowodzenia*, Warszawa 2011.

7 Rozróżnianie tych pojęć i ich wykorzystywania w sposób poprawny omawia: Kuraś M., *System informacyjny a system informatyczny – co oprócz nazwy różni te dwa obiekty?*, Zeszyty Naukowe UEK 2009, nr 770.

8 Fajfer P., *Wdrożenie systemu informatycznego – korzyści płynące z użytkowania systemu ERP*, Organizacja i zarządzanie 2011, nr 2.

9 Chmielarz W., *Systemy informatyczne wspomagające zarządzanie. Aspekt modelowy w budowie systemów*, Warszawa 1996.

zarządzanie określonymi organizacjami i procesami dochodzącymi w ich ramach, przy czym ich funkcjonowanie opiera się na wykorzystywaniu narzędzi informatycznych, m. in. takich, za pomocą których przetwarza się w sposób cyfrowy i gromadzi określone dane[10]. Skupiając się na wyraźnym rozróżnieniu cech systemu informacyjnego od cech systemu informatycznego należy podkreślić ich wzajemne, ścisłe powiązanie, wręcz współzależne istnienie. Proces zbierania i utrzymywania informacji o zasobach własnych wymaga długofalowego działania dla zorganizowania hierarchicznego, wielopoziomowego lub sieciowego (macierzowego) systemu informowania z wykorzystaniem doświadczeń obcych i własnych. Różnorodność systemów informacyjnych implikuje różnorodność systemów informatycznych. Stąd też wdrażanie nowej strategii informacyjnej wymaga oceny funkcjonujących dotychczas rozwiązań informatycznych oraz opracowania koncepcji budowy całościowego systemu informatycznego dla obsługi systemu informacyjnego[11].

Interoperacyjność rozumiana jest jako opracowanie technologii, które są uniezależnione od sprzętu i oprogramowania, a co za tym idzie tworzą warunki sprzyjające uproszczeniu i maksymalnemu wykorzystaniu stworzonych już zasobów informacyjnych oraz tworzenie nowych zasobów kompatybilnych i opartych na już istniejących. Podstawowa definicja interoperacyjności, na którą należy się powoływać, zawarta jest w dokumencie *European Interoperability Framework for European Public Services Version 2.0*[12]. Według tego dokumentu interoperacyjność oznacza możliwość współdziałania różnych odrębnych organizacji na rzecz osiągnięcia uzgodnionych i korzystnych dla wszystkich stron celów, przy jednoczesnym dzieleniu się informacjami i wiedzą pomiędzy tymi organizacjami poprzez wspierane przez nie procesy biznesowe, za pomocą wymiany danych za pośrednictwem odpowiednich systemów. W myśl EIF, interoperacyjność ze swej natury jest wielostronna i najlepiej jest ją rozumieć jako wspólną wartość danej społeczności. Tworzone w ramach państw członkowskich krajowe ramy interoperacyjności mają być zgodne z EIF i powinny wzajemnie się uzupełniać. Zgodnie z zaleceniami Komisji Europejskiej administracje publiczne państw członkowskich powinny ujednolicić swoje ramy interoperacyjności z europejskimi ramami interoperacyjności w celu uwzględnienia europejskiego wymiaru świadczenia usług użyteczności publicznej.

Interoperacyjność jest zarówno warunkiem wstępnym, jak i czynnikiem ułatwiającym efektywne świadczenie usług użyteczności publicznej. Interoperacyjność jest odpowiedzią na potrzebę:

- *współpracy* między administracjami publicznymi mającej na celu ustanowienie usług użyteczności publicznej;
- *wymiany informacji* między administracjami publicznymi w celu wypełnienia wymogów prawnych lub zobowiązań politycznych;
- *dzielenia się informacjami i ich ponownego wykorzystywania* przez administracje publiczne w celu zwiększenia wydajności administracyjnej i ograniczenia biurokracji z korzyścią dla obywateli i przedsiębiorstw[13].

Legalna definicja interoperacyjności została ujęta w art. 3 pkt. 18 ustawy z dnia 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[14]. Zgodnie z tym przepisem interoperacyjność to zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych. Dodatkowo ustawodawca upoważnił Radę Ministrów do wydania rozporządzeń określających minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, uwzględniając konieczność zachowania spójności prowadzenia rejestrów publicznych i wymiany informacji w formie elektronicznej z podmiotami publicznymi, a także Krajowe Ramy Interoperacyjności obejmujące zagadnienia interoperacyjności semantycznej, organizacyjnej oraz technologicznej, z uwzględnieniem zasady równego traktowania różnych rozwiązań informatycznych, Polskich Norm oraz innych dokumentów normalizacyjnych zatwierdzonych przez krajową jednostkę normalizacyjną.

Dnia 12 kwietnia 2012 r. Rada Ministrów wydała rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (dalej rozporządzenie KRI)[15]. Zgodnie z legalną definicją zawartą

10 D. Przybył, *Informatyczne systemy zarządzania*, Zeszyty Naukowe Politechniki Poznańskiej. Budowa Maszyn i Zarządzanie Produkcją, numer 3/2006, s. 61.

11 Por. P. Zaskórski, *Systemy informacji menadżerskiej*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, 2006, nr 1.

12 Europejskie Ramy Interoperacyjności dla europejskich usług użyteczności publicznej, 16/12/2010, jako załącznik 2 do komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „W kierunku interoperacyjności europejskich usług użyteczności publicznej".

13 M. Ganczar, *Interoperacyjność usług administracji publicznej świadczonych drogą elektroniczną,* w: M. Rudnicki, M. Jabłoński, K. Sobieraj, *Nowoczesna administracja publiczna. Zadania i działalność – uwarunkowania prawne,* Lublin 2013, s. 112.

14 T.j., Dz. U., 2013, poz. 235.

15 T.j. Dz. U. 2017 r., poz. 2247.

w ustawie o informatyzacji Krajowe Ramy Interoperacyjności to zestaw wymagań semantycznych, organizacyjnych oraz technologicznych dotyczących interoperacyjności systemów teleinformatycznych i rejestrów publicznych, gdzie określone są m.in. sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz sposoby postępowania podmiotu realizującego zadania publiczne w zakresie przejrzystego wyboru norm, standardów i rekomendacji w zakresie interoperacyjności semantycznej, organizacyjnej oraz technologicznej, z zapewnieniem zasady neutralności technologicznej.

Zgodnie z § 3 ust. 1 Krajowe Ramy Interoperacyjności (KRI) określają sposoby postępowań podmiotów realizujących zadania publiczne w zakresie doboru środków, metod i standardów, które są wykorzystywane do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego, który jest wykorzystywany do realizacji zadań tego podmiotu oraz procedur organizacyjnych. Mają one zapewnić w szczególności obywatelom i przedsiębiorcom dostęp do usług świadczonych przez te podmioty w wersji elektronicznej, zwiększyć efektywność świadczonych usług, zapewnić podmiotom publicznym redukcję kosztów związanych z ich funkcjonowaniem, gwarantować racjonalne gospodarowanie funduszami publicznymi czy też wreszcie zapewnić swobodę gospodarczą i równy dostęp do rynku informatycznego w zakresie usług i dostaw podczas udzielania zamówień publicznych dla wszystkich jego uczestników.

Interoperacyjność osiągana jest przez ujednolicenie, wymienność i zgodność. Ujednolicenie to stosowanie kompatybilnych norm, standardów i procedur przez różne podmioty realizujące zadania publiczne. Wymienność jest rozumiana jako możliwość zastąpienia produktu, procesu lub usługi bez jednoczesnego zakłócenia wymiany informacji pomiędzy podmiotami realizującymi zadania publiczne lub pomiędzy tymi podmiotami a ich klientami, przy spełnieniu wszystkich wymagań funkcjonalnych i pozafunkcjonalnych współpracujących systemów. Natomiast zgodność to przydatność produktów, procesów lub usług które są przeznaczone do wspólnego użytkowania (§ 4 ust. 1 rozporządzenia KRI).

Omawiane rozporządzenie wskazuje na trzy poziomy interoperacyjności: organizacyjny, semantyczny i technologiczny (§5 rozporządzenia KRI). Interoperacyjność organizacyjna umożliwia współdziałanie podmiotów publicznych, przedsiębiorców i obywateli. Osiągana jest poprzez informowanie o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez podmioty a także standaryzację i ujednolicenie procedur z uwzględnieniem konieczności zapewnienia poprawnej współpracy podmiotów realizujących zadania publiczne, oraz poprzez publikowanie w BIP podmiotów opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną. Interoperacyjność semantyczna to zdolność dwóch lub więcej systemów teleinformatycznych do wymiany informacji oraz do precyzyjnego określania znaczenia tych informacji zarówno przez nadawcę jak i odbiorcę, zapewnia usunięcie konfliktów zarówno na poziomie danych (różnice w interpretacji) jak i struktury danych (niespójności). Umożliwia ona systemom łączenie otrzymywanych informacji z innymi zasobami informacji i ich rozumienie, które umożliwia przetwarzanie. Interoperacyjność na poziomie technologicznym zapewnia wspólne funkcjonowanie systemów informatycznych współpracujących podmiotów pod względem technicznym. Osiągana jest poprzez stosowanie minimalnych wymagań dla systemów teleinformatycznych, które są określone w rozdziale IV omawianego rozporządzenia oraz stosowanie regulacji zawartych w przepisach odrębnych, a gdy jest ich brak uwzględnienia postanowień odpowiednich Polskich Norm[16], norm międzynarodowych lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe.

Każdy system teleinformatyczny, w którym przetwarzane są informacje m.in. przez j.s.t., powinien spełniać minimalne wymagania określone w rozdziale IV wskazanego rozporządzenia. Kluczowe znaczenie ma w tym zakresie §20 rozporządzenia KRI zobowiązujący podmiot realizujący zadania publiczne do opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji, który zapewnia poufność[17], dostępność[18] i integralność[19] informacji z uwzględnieniem takich atrybutów, jak autentyczność[20], rozliczalność[21], niezaprzeczalność[22] i niezawodność.

16 Zob. szerzej J. Stanik, *Wybrane aspekty standaryzacji w ochronie publicznych baz danych*, [w:] G. Szpor, Internet. Publiczne bazy danych i big data, Warszawa 2014, SIP Legalis.

17 poufność - właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym.

18 dostępność - właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym.

19 integralność - właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.

20 autentyczność - właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane.

21 rozliczalność - właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.

22 niezaprzeczalność - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

W § 20 ust. 2 wskazano warunki jakie powinno zapewnić kierownictwo podmiotu publicznego w zakresie realizacji systemu zarządzania bezpieczeństwem informacji. Konieczne jest zatem zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. W przypadku jednostek samorządu terytorialnego konieczne jest zweryfikowania dotychczas przyjętych polityk bezpieczeństwa informacji[23] pod kątem ich dostosowania do obecnie obowiązujących przepisów prawa lub obecnej struktury organizacyjnej, która na przykład uległa zmianie na skutek zmiany siedziby czy też restrukturyzacji.

Za spełnienie wymagań rozporządzenia KRI uznaje się opracowanie systemu zarządzania bezpieczeństwem informacji na podstawie Polskiej Normy PN-ISO/IEC 27001, przy jednoczesnym ustanawianiu zabezpieczeń, zarządzaniu ryzykiem oraz audytowaniu systemu na podstawie:

1. PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń,
2. PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem,
3. PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Osiągnięcie bezpieczeństwa informacji, jest wynikiem wykorzystania wielu czynników, zewnętrznych i wewnętrznych, wśród których można wymienić: potencjał i umiejętności ludzi, możliwość finansowania przedsięwzięcia w założonej skali i zakresie, dojrzałość procesów realizowanych w danej organizacji, a także rozumienie istoty ryzyka, w tym ryzyka związanego z bezpieczeństwem informacji i skuteczne nim zarządzanie[24].

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

- utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfiguracja;
- przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
- podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji; bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których tu mowa;
- zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
  - a) zagrożenia bezpieczeństwa informacji,
  - b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
  - c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
- zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
  a) monitorowanie dostępu do informacji,
  b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
  c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
- ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
- zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
- ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
- zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
  a) dbałości o aktualizację oprogramowania,
  b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
  c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
  d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
  e) zapewnieniu bezpieczeństwa plików systemowych,
  f) redukcji ryzyk wynikających z wykorzystania opubli-

23 polityka bezpieczeństwa informacji - zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania.

24 E. Andrukiewicz, M. Kowalewski, praktyczne podejście do wdrażania systemów zarządzania bezpieczeństwem informacji w małych i średnich przedsiębiorstwach, Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach, nr 355/2018, s. 8.

kowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

- bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
- zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Posiłkując się normą ISO/IEC 9126 (oraz jej kolejnymi wersjami) można wskazać, że system teleinformatyczny cechuje:

- funkcjonalność – cechy definiujące funkcje i właściwości oprogramowania. Funkcje te mają spełniać wyrażone wprost lub niewyrażone potrzeby użytkownika. Obejmuje: odpowiedniość, dokładność, interoperacyjność, zgodność, bezpieczeństwo.
- niezawodność – cechy opisujące zdolność systemu do wykonywania i utrzymywania wymagań dotyczących jego stabilności działania: dojrzałość systemu, odporność na błędy, zdolność do odtworzenia.
- użyteczność – składa się z cech informujących o nakładzie pracy niezbędnej do łatwości poruszania się po oprogramowaniu: transparentność, intuicyjność, łatwość w obsłudze, operatywność.
- wydajność – atrybuty wydajności opisują powiązanie między wydajnością systemu a wykorzystywanymi zasobami: czas, rzetelność zasobów, ich ilość i jakość, kompletność.
- utrzymywalność – zbiór cech określa nakład pracy potrzebny do wprowadzenia modyfikacji do oprogramowania: stabilność, elastyczność jeżeli chodzi o dostosowanie do zmian, łatwość analizy w przypadku wystąpienia konieczności wprowadzenia zmian.
- przenośność – w jej skład wchodzą cechy dotyczące zdolności oprogramowania do przenoszenia się między środowiskami: adaptacja, zgodność, łatwość instalacji, zastąpienia nowymi rozwiązaniami, aktualizacje.

System Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 rozporządzenia KRI opiera się na zabezpieczeniach proceduralno-prawnych, fizycznych i informatycznych, świadomości pracowników oraz posiadanych aktywach: informacje, sprzęt, zasoby ludzkie, infrastruktura, itd. Wspomniana norma PN-ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji z uwzględnieniem uwarunkowań, w których działa organizacja. Podano również dostosowane do potrzeb organizacji wymagania, dotyczące szacowania i postępowania z ryzykami w bezpieczeństwie informacji. Wymagania mają charakter ogólny i są przeznaczone do stosowania w organizacji każdego rodzaju, wielkości czy charakteru.

Pierwszym krokiem do wdrożenia systemu zarządzania bezpieczeństwem informacji jest zidentyfikowanie: informacji, zagrożeń występujących w organizacji i aktywów, które są bezpośrednio lub pośrednio związane z obiegiem informacji. Kolejnym etapem szacowania ryzyka jest wartościowanie informacji i przypisanie im właścicieli. Kolejnym etapem jest identyfikacja i analiza zagrożeń. Ostatecznym efektem jest ocena ryzyka, na podstawie której można określić odpowiednie plany zarządzania ryzykiem w celu zminimalizowania istniejącego ryzyka do akceptowalnego poziomu. W ramach analizy ryzyka należy ocenić jakie informacje ma w swoich zasobach podmiot, np. j.s.t., jakim ryzykiem obarczone jest przetwarzanie informacji w tych zbiorach, by następnie wdrożyć mechanizmy zapobiegające wystąpieniu tych ryzyk.

Biorąc pod uwagę element oceny ryzyka dotyczący identyfikacji zagrożeń, konieczne jest oszacowanie prawdopodobieństwa wystąpienia danego zagrożenia, jak również ewentualnych strat, które ze sobą niesie. Prawdopodobieństwo definiujemy jako możliwość, szansę wystąpienia zdarzenia[25]. Prawdopodobieństwo wystąpienia danego zagrożenia można szacować na podstawie następujących czynników:

1. ekspozycja na zagrożenie (np. rzadka, występuje czasami, występuje często);
2. występowanie konkretnego zagrożenia w przeszłości (np. nigdy się nie wydarzyło, wydarzyło się tylko raz, wydarzyło się kilkakrotnie).

Przykładowo można wskazać następujące szacowanie prawdopodobieństwa wystąpienia zagrożenia/ryzyka:

- Znikomo małe, ale prawdopodobne – np.: sposoby wykorzystania zagrożenia nie są znane lub bardzo mało prawdopodobne jest ich wykorzystanie w eksploatowanym środowisku; dużo standardowych zabezpieczeń, które obniżają prawdopodobieństwo wystąpienia zagrożenia; zagrożenie zmaterializowało się w ciągu ostatnich 24 miesięcy.
- Małe prawdopodobieństwo – np.: sposoby wykorzystania zagrożenia nie są publicznie dostępne lub są mało prawdopodobne w eksploatowanym środowisku; dostępne są standardowe zabezpieczenia, które obniżają prawdopodobieństwo wystąpienia zagrożenia; zagrożenia zmaterializowało się w ciągu ostatnich 12 miesięcy.

25 Źródło: ISO Guide 73:2009 *Risk Management – Vocabulary*, definicja 3.6.1.1. Za: D. Wróblewski (red.), *Zarządzanie ryzykiem – przegląd wybranych metodyk*, Józefów 2015, s. 46.

- Duże prawdopodobieństwo – np.: sposoby wykorzystania zagrożenia są znane, ale wymagają umiarkowanego stopnia umiejętności do wykorzystania zagrożenia; ograniczona liczba standardowych zabezpieczeń, która tylko częściowo obniża prawdopodobieństwo wystąpienia zagrożenia; zagrożenie zmaterializowało się w ciągu ostatnich 6 miesięcy.
- Bardzo prawdopodobne – np.: łatwo wykorzystać zagrożenie , a narzędzia do tego konieczne są łatwo dostępne; brak standardowych zabezpieczeń w celu obniżenia prawdopodobieństwa wystąpienia zagrożeni; zagrożenie zmaterializowało się w ciągu ostatnich 3 miesięcy[26].

Ewaluacja ryzyka ma istotny wpływ na proces podejmowania decyzji. Wyniki analizy ryzyka stanowią podstawę do podjęcia decyzji, które ryzyka i w jakim stopniu wymagają wdrożenia przez organizację właściwego algorytmu postępowania z nimi oraz ustalenia priorytetu ich uruchamiania. Następnie ustalone poziomy ryzyka powinny zostać porównane z ich kryteriami, z uwzględnieniem ustanowionego na wejściu kontekstu. Ewaluacja umożliwi w tym wypadku określenie, w jaki sposób postąpić z danymi ryzykiem[27]. Idea podejścia opartego na ryzyku polega na tym, że ryzykiem najlepiej zarządza ten kto je zna. Ważne aby skład zespołu ds. szacowania ryzyka bezpieczeństwa informacji obejmował przedstawicieli wszystkich obszarów organizacji (m.in. pełnomocnik ds. systemu zarządzani jakością, dyrektorzy, kierownicy działów, pracownik kadr, kierownik biura zarządu, administrator sieci, itp.). Praca w tak zbudowanym zespole umożliwiła objęcie wszystkich procesów realizowanych w organizacji związanych z tematem bezpieczeństwa informacji.

Efektem przeprowadzonej analizy ryzyka jest stworzenie odpowiedniej polityki bezpieczeństwa informacji, która stanowi zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania (§ 2 pkt 15 rozporządzenia KRI). Polityka bezpieczeństwa, zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych informacji[28]. Konieczne jest następnie wdrożenie ujętych w niej zasad i procedur poprzez ich zakomunikowanie pracownikom i wreszcie monitorowanie ich stosowania w praktyce.

Podsumowując powyższe rozważania, zapewnienie interoperacyjności systemów informacyjnych spowoduje, że zawarte tam dane będą odzwierciedlały stan rzeczywisty, będą niepodważalne, budzące zaufanie, umożliwiające tworzenie na ich podstawie kolejnych informacji, potrzebnych do podejmowania decyzji. W założeniu projektu PZIP realizacja zasady interoperacyjności może wpływać na obniżenie kosztów funkcjonowania całej administracji publicznej jak i racjonalne gospodarowanie funduszami publicznymi. Systemy teleinformatyczne wspierające funkcjonowanie administracji państwa funkcjonują w ramach złożonego ekosystemu prawno-organizacyjno-technicznego, który musi być zarządzany jednolicie, w sposób spójny i racjonalny, przy zachowaniu autonomii decyzyjnej urzędów j.s.t. i organów państwa na szczeblu centralnym w zakresie ich właściwości. Pozwoli to na zwiększenie zaufania obywateli do usług cyfrowych świadczonych przez administrację publiczną. Analiza przepisów dotyczących osiągania interoperacyjności wskazuje na obowiązek aktualizowania systemu zarządzania bezpieczeństwem informacji. Sposób osiągnięcia bezpieczeństwa informacji zależny jest od okoliczności wynikających z szacowania ryzyka oraz z właściwości projektowanego systemu teleinformatycznego, w którym prowadzone są zasoby informacyjne, jego zasięgu oraz dostępnych rozwiązań na rynku. Zapewnienie bezpieczeństwa informacji, a także funkcjonalności systemu teleinformatycznego, powinno być gwarantowane wdrożonymi i stale aktualizowanymi procedurami wewnętrznymi, a także dostosowaniem infrastruktury do pojawiających się nowych zagrożeń albo rozwiązań technologicznych, które należy wdrożyć (np. technologia 5G).

26 M. Ganczar, *Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych*, [w:] G. Szpor, K Czaplicki (red.) Internet, Przetwarzanie danych osobowych, Warszawa 2019, s. 42-43.

27 D. Wróblewski, B. Połeć, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, [w:] D. Majchrzak (red.), Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje, Warszawa 2014, s. 206.

28 Polityka bezpieczeństwa może określać w szczególności: obowiązki pracowników/użytkowników, bezpieczeństwo zasobów ludzkich, szacowanie ryzyka dla informacji chronionych, struktury zbiorów informacji, strefy przetwarzania informacji, kontrolę dostępu, zarządzanie systemami i sieciami, rozwój i utrzymywanie systemów informatycznych, zarządzanie incydentami, i in.

Narodowy Instytut Samorządu Terytorialnego powstał w 2015 r.
Jest państwową jednostką budżetową podległą MSWiA.
Działa na rzecz dalszej profesjonalizacji samorządu terytorialnego i administracj publicznej.

EKSPERTYZY NIST, ul. Zielona 18, Łódź 90-601
Sekretariat tel. +48 42 633 10 70
e-mail: sekretariat@nist.gov.pl