KWARTALNY BIULETYN
MINISTERSTWA FINANSÓW
Nr 2 (19)/2016
PR 19353

KONTROLA ZARZĄDCZA W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO

SPIS TREŚCI:

tel.: 22 694 42 42

fax: 22 694 47 41

e-mail:

RedakcjaBKZ@mf.gov.pl

www.mf.gov.pl

Ministerstwo Finansów/Działalność/Finanse publiczne/Kontrola zarządcza i audyt wewnętrzny

DEPARTAMENT POLITYKI WYDATKOWEJ

WARSZAWA CZERWIEC 2016 R.

SŁOWO WSTĘPNE

Szanowni Państwo,

główne tematy tego numeru *Biuletynu* to ponowne wykorzystanie informacji sektora publicznego oraz nowoczesne technologie cyfrowe i bezpieczeństwo teleinformatyczne w sektorze publicznym.

Informacja stanowi jeden z najcenniejszych, ale również najbardziej wrażliwych zasobów znajdujących się w posiadaniu administracji publicznej. Coraz powszechniejsze stosowanie informatycznych systemów gromadzących i przetwarzających informacje oraz sieci i urządzeń umożliwiających ich przesyłanie, z jednej strony stanowi przejaw innowacyjności zarządzania w administracji publicznej oraz odpowiedzi na potrzeby jej klientów, z drugiej zaś generuje szereg zagrożeń, którym należy przeciwdziałać. Na łamach naszego Biuletynu pisaliśmy już o bezpieczeństwie informacji[1] oraz wykorzystaniu nowoczesnych narzędzi komunikacji z klientem urzędu[2].

W tym wydaniu w pierwszym artykule zwracamy Państwa uwagę na kluczowe zmiany przepisów w zakresie ponownego wykorzystania informacji sektora publicznego.

W drugim przedstawiamy wybrane wnioski z trzech kontroli przeprowadzonych w latach 2014 – 2016, w których Najwyższa Izba Kontroli oceniła wykorzystanie rozwiązań informatycznych umożliwiających świadczenie e-usług przez administrację publiczną oraz cyberbezpieczeństwo w sektorze publicznym.

Prezentujemy również informacje na temat dwóch opracowań na temat funkcji audytu wewnętrznego w sektorze publicznym, przygotowanych przez Departament Polityki Wydatkowej, oraz innych publikacji na stronie Ministerstwa Finansów.

Katarzyna Szarkowska

Redaktor Naczelny

---

[1] Biuletyn Nr 2 (11)/2014 *„Istotność analizy ryzyka dla dobrego zarządzania bezpieczeństwem informacji na przykładzie Urzędu Miasta Krakowa”*, Biuletyn Nr 4 (9)/2013 *„Zapewnienie okresowego audytu wewnętrznego w zakresie systemu bezpieczeństwa informacji w JST”*, Biuletyn Nr 2 (7)/2013 *„Audyt bezpieczeństwa informacji”.*

[2] Biuletyn Nr 1 (14)/2015 *„Aplikacje mobilne – sposób na wzmocnienie komunikacji i informacji zwrotnej”* w Gminie Dobrcz, Biuletyn Nr 3 (8)/2013 *„Efektywność prowadzenia stron Biuletynu Informacji Publicznej w JST*”.

PONOWNE WYKORZYSTANIE INFORMACJI SEKTORA PUBLICZNEGO

NOWA USTAWA W ZAKRESIE PONOWNEGO WYKORZYSTANIA INFORMACJI

Jak podkreśla Ministerstwo Cyfryzacji: *Informacja sektora publicznego jest dziś ważnym materiałem wyjściowym dla produktów i usług związanych z zasobami cyfrowymi o dotychczas niewykorzystanym potencjale. Podmioty publiczne wytwarzają, gromadzą lub przechowują ogromną ilość informacji i treści (...). Wraz z rewolucją cyfrową istotnie wzrosła wartość tego źródła dla innowacyjnych produktów lub usług wykorzystujących takie zasoby.*[3]

Dotychczasowe przepisy o ponownym wykorzystywaniu informacji publicznej znajdowały się w rozdziale 2a ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[4]. Zostały one wprowadzone do uoddip w związku z wdrożeniem w 2011 r. dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady w sprawie ponownego wykorzystywania informacji sektora publicznego (tzw. pierwszej dyrektywy re-use).

W dniu 16 czerwca 2016 r. weszła w życie ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego[5], określająca:

- zasady i tryb udostępniania lub przekazywania informacji sektora publicznego w celu ponownego wykorzystywania,
- podmioty, które udostępniają lub przekazują te informacje,
- warunki oraz opłaty za ponowne wykorzystywanie.

Wprowadzenie ustawy stanowi implementację dyrektywy Parlamentu Europejskiego i Rady 2013/37/UE z dnia 26 czerwca 2013 r. zmieniającej pierwszą dyrektywę re-use.

Wyłączenie przepisów o ponownym wykorzystaniu informacji z uoddip było również odpowiedzią na trudności interpretacyjne dotyczące stosowania przepisów. Zgodnie z nimi przed udostępnieniem informacji należało ustalić, czy stanowi ona informację publiczną w rozumieniu uoddip. Pojawiały się również trudności z odróżnianiem „dostępu do informacji" od jej „ponownego wykorzystania".

---

[3] https://mc.gov.pl/aktualnosci/sejm-uchwalil-ustawe-o-ponownym-wykorzystywaniu-informacji-sektora-publicznego-0 .

[4] Dalej jako: uoddip (Dz. U. z 2015 r. poz. 2058, z późn. zm.).

[5] Dalej jako: ustawa lub uopwisp (Dz. U. z 2016 r. poz. 352).

ZAKRES PODMIOTOWY USTAWY

Uopwisp rozszerza zakres podmiotów zobowiązanych do jej stosowania, dodając do jednostek i osób prawnych ujętych w art. 3 ustawy również biblioteki naukowe[6], Instytut Meteorologii i Gospodarki Wodnej oraz Państwowy Instytut Geologiczny, do zasobów których dostęp był dotychczas ograniczony.

Na mocy ustawy zasoby tych instytucji, nie objęte ochroną praw autorskich, mogą być ponownie wykorzystywane na zasadach określonych w uopwisp.

Dotyczy to także informacji sektora publicznego będących w posiadaniu Instytutu Meteorologii i Gospodarki Wodnej oraz Państwowego Instytutu Geologicznego, które w myśl nowej ustawy będą przekazywane nieodpłatnie do ponownego wykorzystywania (np. dane meteorologiczne).

INFORMACJA SEKTORA PUBLICZNEGO I JEJ PONOWNE WYKORZYSTANIE - DEFINICJE

Zgodnie z art. 2 ust. 1 uopwisp przez informację sektora publicznego należy rozumieć każdą treść lub jej część, niezależnie od sposobu utrwalenia (w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej), będącą w posiadaniu podmiotów zobowiązanych do udostępnienia na mocy ustawy.

Obecnie w praktyce funkcjonują dwa typy informacji w sferze publicznej, tj. informacja publiczna oraz informacja sektora publicznego. Przy czym pojęcie informacji sektora publicznego jest szersze i zawiera wszystkie informacje, w tym również będące informacją publiczną. Takie rozwiązanie pozwala uniknąć dotychczasowych wątpliwości interpretacyjnych.

Z ponownym wykorzystywaniem informacji sektora publicznego mamy do czynienia wówczas, gdy osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej wykorzystują tę informację w celu innym niż ten, dla którego informacja została wytworzona. Dotyczy to każdego twórczego wykorzystania informacji (np. łączenia danych z różnych źródeł w celu tworzenia aplikacji lub innych innowacyjnych produktów).

Jednocześnie ponownym wykorzystywaniem **nie jest** udostępnianie lub przekazanie informacji sektora publicznego przez podmiot wykonujący zadania publiczne innemu podmiotowi wykonującemu zadania publiczne, w celu realizacji tych zadań.

---

[6] W rozumieniu przepisów ustawy z dnia 27 czerwca 1997 r. o bibliotekach (Dz.U. z 2012 r. poz. 642, z późn. zm.).

W ustawie podkreślono, że ponowne wykorzystywanie ma odbywać się z pełnym poszanowaniem praw własności. Przepisów ustawy nie stosuje się do informacji sektora publicznego, których udostępnianie lub przekazanie zostało uzależnione od wykazania przez użytkowników interesu prawnego lub faktycznego na podstawie odrębnych przepisów.

UDOSTĘPNIANIE I PRZEKAZYWANIE INFORMACJI SEKTORA PUBLICZNEGO W CELU PONOWNEGO WYKORZYSTYWANIA

Uopwisp formułuje następujące zasady udostępniania i przekazywania informacji:

- niedyskryminacji – podmiot zobowiązany w porównywalnych sytuacjach udostępnia lub przekazuje informacje sektora publicznego w celu ponownego wykorzystywania na takich samych zasadach,
- niewyłączności – podmiot zobowiązany, który udostępnia lub przekazuje informacje sektora publicznego w celu ponownego wykorzystywania, nie może wprowadzać ograniczenia korzystania z tych informacji przez innych użytkowników,
- udostępniania danych elektronicznych w formatach umożliwiających odczyt maszynowy,
- określenia przez podmiot zobowiązany warunków ponownego wykorzystywania informacji sektora publicznego (tzw. oferta),
- informowania o warunkach ponownego wykorzystywania informacji sektora publicznego.

Ponadto ustawa określa:

- tryby udostępnienia (bezwnioskowy lub na wniosek),
- termin rozpatrzenia wniosku (14 dni),
- tryb odwołania od odmowy (odwołanie do organu wyższego stopnia, a następnie skarga do sądu administracyjnego),
- wyjątki od zasad przekazywania (określone przez podmiot zobowiązany w *warunkach ponownego wykorzystywania* dla informacji podlegającej innym ustawom),
- ograniczenia korzystania z prawa do ponownego wykorzystywania informacji sektora publicznego (np. ze względu na: tajemnice ustawowo chronione, prywatność osób fizycznych lub tajemnicę przedsiębiorcy, przepisy innych ustaw, prawa autorskie lub prawa pokrewne).

Jak wskazuje ustawa informacje sektora publicznego udostępnia się bezpłatnie, jednak podmiot zobowiązany może nałożyć opłatę za ponowne wykorzystywanie, w zależności od poniesionych dodatkowych kosztów oraz sposobu korzystania z informacji.

ZADANIA PODMIOTU ZOBOWIĄZANEGO

W związku z wejściem w życie uopwisp podmiot zobowiązany:

1. Ustala, które z informacji z posiadanego zasobu mogą podlegać ponownemu wykorzystywaniu bezwarunkowo, a które wymagają określenia warunków ponownego wykorzystywania.
2. Zamieszcza na stronie BIP informacje dotyczące:
   - warunków ponownego wykorzystywania, jeżeli zostały określone,
   - wysokości opłat za ponowne wykorzystywanie,
   - środków prawnych przysługujących w przypadku odmowy wyrażenia zgody na ponowne wykorzystywanie,
   - umowy o udzielenie wyłącznego prawa do korzystania z informacji sektora publicznego, powodów jej zawarcia oraz wyników oceny tej umowy, o ile taka umowa została zawarta.
3. W przypadku udostępniania informacji sektora publicznego w celu ponownego wykorzystywania w sposób inny niż w BIP lub w centralnym repozytorium, wraz z ich udostępnieniem informuje o dostępności tych informacji oraz:
   - określa warunki lub wysokość opłat za ponowne wykorzystywanie albo
   - informuje o braku warunków lub opłat za ponowne wykorzystywanie.

Podmioty zobowiązane **nie są obowiązane** do tworzenia informacji sektora publicznego, ich przetwarzania w sposób lub w formie wskazanych we wniosku o ponowne wykorzystywanie oraz sporządzania z nich wyciągów, jeżeli spowoduje to konieczność podjęcia nieproporcjonalnych działań przekraczających proste czynności.

PODSUMOWANIE

Ponowne wykorzystywanie zasobu, jakim jest informacja sektora publicznego, ma wpływać na rozwój innowacyjności i stymulować rozwój gospodarczy oraz pozwalać na wykorzystywanie zasobów, które powstały bądź które uzyskano na skutek zaangażowania środków publicznych. Nowe przepisy mają zapewnić przejrzyste i równe dla wszystkich zasady korzystania z informacji sektora publicznego.

ŹRÓDŁA:

- Ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego.
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej.
- Publikacja pod nazwą: *Sejm uchwalił ustawę o ponownym wykorzystywaniu informacji sektora publicznego* na stronie internetowej Ministerstwa Cyfryzacji:

https://mc.gov.pl/aktualnosci/sejm-uchwalil-ustawe-o-ponownym-wykorzystywaniu-informacji-sektora-publicznego-0.

- Artykuł „Nowa ustawa o ponownym wykorzystywaniu informacji sektora publicznego" autor: Marlena Sakowska – Bryła, Kurier Prawny Stały dodatek do Pisma Samorządu Terytorialnego WSPÓLNOTA nr 11/2016 (1999) z dnia 21 maja 2016 r.

Opracowanie: Departament Polityki Wydatkowej Ministerstwa Finansów.

INFORMATYZACJA I CYBERBEZPIECZEŃSTWO SEKTORA PUBLICZNEGO W OCENIE NAJWYŻSZEJ IZBY KONTROLI

Stosowanie nowoczesnych technologii cyfrowych ma wspierać tworzenie i funkcjonowanie nowoczesnej administracji. Stanowi również jeden z priorytetów Strategii „Sprawne Państwo 2020"[7]. Wśród głównych celów Strategii wskazano „Zwiększenie skuteczności i efektywności państwa otwartego na współpracę z obywatelami", które ma być realizowane poprzez cele szczegółowe, w tym: wprowadzenie **zasad otwartego rządu**, zwiększenie **sprawności instytucjonalnej państwa** oraz poprawę relacji między wynikami i nakładami w zakresie **świadczenia usług publicznych**.

Wśród działań określonych w Strategii w ramach realizacji tych celów wskazano m.in.:

- stworzenie nowoczesnej i bezpiecznej infrastruktury informatycznej, zbudowanej w oparciu o niezawodne zintegrowane systemy teleinformatyczne, stanowiącej podstawę funkcjonowania urzędu oraz wymiany informacji pomiędzy urzędami i obywatelem, a także samymi urzędami i innymi podmiotami publicznymi,
- usprawnienie procesów wewnętrznych realizacji zadań, podniesienie jakości i dostępności świadczonych usług przez urzędy administracji publicznej i udostępnienia zasobów informacyjnych przy wykorzystaniu nowoczesnych systemów informacyjno-komunikacyjnych,
- podniesienie efektywności i dostępności świadczenia usług publicznych, w tym rejestrów centralnych, oraz wprowadzenie standaryzacji i nowoczesnego zarządzania usługami publicznymi, utworzenie zintegrowanej platformy informatycznej o usługach publicznych, zapewnienie kompletności dostępnych usług publicznych, promowanie wykorzystania danych publicznych na rzecz tworzenia innowacyjnych usług elektronicznych we współpracy ze środowiskiem pozarządowym, promowanie standardów interoperacyjności oraz zasad

---

[7] Uchwała Nr 17 Rady Ministrów z dnia 12 lutego 2013 r. w sprawie przyjęcia *Strategii Sprawne Państwo 2020* (M. P. z 2013 r. poz. 136).

otwartości i transparentności, wsparcie usług elektronicznej administracji o zasięgu paneuropejskim oraz działań o charakterze edukacyjno-promocyjnym.

Korzystanie z nowoczesnych narzędzi i przenoszenie coraz większej gamy usług publicznych do cyberprzestrzeni[8] z jednej strony przyczynia się do poprawy skuteczności i efektywności administracji publicznej. Jednak z drugiej strony stosowanie tych narzędzi jest związane z powstawaniem zagrożeń, z których ich użytkownicy nie zawsze zdają sobie sprawę. Dlatego rozwojowi e-usług musi towarzyszyć zapewnienie odpowiednich standardów bezpieczeństwa systemów teleinformatycznych administracji publicznej oraz ochrony danych osobowych użytkowników publicznych. Niezbędne są również szkolenia dla pracowników urzędów administracji publicznej nt. zapewnienia bezpieczeństwa sieci teleinformatycznych, rodzajów zagrożeń i możliwości ich występowania oraz sposobów szybkiego na nie reagowania.

Najwyższa Izba Kontroli[9] przeprowadziła w latach 2014 – 2016 ocenę stopnia wykorzystywania rozwiązań informatycznych umożliwiających świadczenie e-usług przez administrację publiczną oraz stanu bezpieczeństwa cyberprzestrzeni RP.

ZAKRES KONTROLI

NIK przeprowadziła następujące kontrole w obszarach związanych z:

1. „Świadczeniem usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego”[10].
2. „Realizacją przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP”[11].
3. „Zapewnieniem bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych”[12].

---

[8] Przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114, z późn. zm.), wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

[9] Dalej jako: NIK.

[10] https://www.nik.gov.pl/plik/id,10420,vp,12749.pdf.

[11] https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf .

[12] https://www.nik.gov.pl/plik/id,10771,v,artykul_12904.pdf.

W artykule pragniemy zwróć Państwa uwagę na powyższe kontrole NIK, a przede wszystkim na wybrane wnioski z nich wynikające, które mogą mieć znacznie dla funkcjonowania jednostek samorządu terytorialnego. W celu zapoznania się ze wszystkimi wnioskami i zaleceniami pokontrolnymi zachęcamy do zapoznania się z raportami opublikowanymi na stronie NIK.

„ŚWIADCZENIE USŁUG PUBLICZNYCH W FORMIE ELEKTRONICZNEJ NA PRZYKŁADZIE WYBRANYCH JEDNOSTEK SAMORZĄDU TERYTORIALNEGO"

Stosowanie usług publicznych w formie elektronicznej ma na celu ułatwienie komunikacji pomiędzy urzędami oraz, przede wszystkim, pomiędzy urzędem i obywatelami. Dzięki temu łatwiejszy staje się dostęp do wzorów dokumentów oraz możliwe jest załatwienia spraw urzędowych bez konieczności wizyty w urzędzie. Zastosowanie e-usług, dzięki wykorzystywaniu gotowych szablonów, pozwala również na standaryzację usług publicznych na oczekiwanym poziomie, a także lepsze wykorzystanie zasobów oraz poprawę efektywności urzędu.

Stosowanie usług publicznych w formie elektronicznej wymaga znacznych inwestycji przygotowujących w urzędzie odpowiednią infrastrukturę oraz jej pracowników. Niezbędne są również szkolenia dla pracowników urzędów administracji publicznej dotyczące zapewnienia bezpieczeństwa sieci teleinformatycznych, rodzajów zagrożeń i możliwości ich występowania oraz sposobów szybkiego reagowania.

Obecnie w Polsce wdrażanych jest szereg rozwiązań informatycznych umożliwiających świadczenie e-usług przez administrację publiczną. Od 14 kwietnia 2008 r. do 12 sierpnia 2015 r. korzystanie z e-usług w urzędach umożliwiała przede wszystkim platforma ePUAP1, zarządzana przez Centrum Projektów Informatycznych (od 3 listopada 2015 r. Centrum Cyfrowej Administracji), podlegające Ministerstwu Administracji i Cyfryzacji (obecnie Ministerstwu Cyfryzacji). 17 sierpnia 2015 r. Centrum uruchomiło platformę ePUAP2, która stanowi zmodernizowaną wersję platformy ePUAP1. E-usługi mogą być również udostępniane za pomocą regionalnych platform samorządowych.

OCENA NIK

> Poziom wykorzystania usług elektronicznych w urzędach jest zbyt niski w stosunku do dużych sum wydanych na tego typu inwestycje.

Jak podkreśla NIK, zarówno ePUAP, jak i regionalne platformy samorządowe służyły w niewielkim stopniu do świadczenia usług dla obywateli. ePUAP najczęściej był wykorzystywany jako kanał komunikacyjny pomiędzy organami administracji publicznej. Liczba usług udostępnianych przez kontrolowane urzędy była zróżnicowana. Jednak nawet w przypadkach dużej liczby udostępnionych usług ich wykorzystanie było niewielkie. NIK jako kluczowe przyczyny takiego stanu rzeczy wskazuje:

- dużą liczbą czynności wymagających osobistego kontaktu z urzędem,
- słabą promocję e-usług,

- niski poziom zaufania Polaków do komunikowania się w sprawach urzędowych drogą elektroniczną,
- mały procent dorosłych Polaków posiadających profil zaufany umożliwiający korzystanie z e-usług.

Przyczyną niewielkiego wykorzystania systemu ePUAP1 mogły być również problemy z jego dostępnością i częste awarie. NIK podkreśla jednocześnie, że uruchomienie platformy ePUAP2 ma poprawić operacyjność systemu oraz umożliwić centralne udostępnianie kolejnych e-usług, z wykorzystaniem gotowych szablonów.

WNIOSKI KIEROWANE DO KONTROLOWANYCH URZĘDÓW

Wnioski NIK skierowane do marszałków województw oraz burmistrzów/prezydentów miast dotyczyły m.in.:

- podjęcia działań w zakresie pełnego informowania o usługach elektronicznych oraz ich promowania, w celu szerszego i efektywnego wykorzystania udostępnianych e-usług,
- umieszczenia na stronach BIP urzędu informacji o uruchomieniu elektronicznej skrzynki podawczej (ESP) oraz metodach dostarczania i wymaganiach dla dokumentów elektronicznych,
- doręczania pism za pomocą środków komunikacji elektronicznej w przypadkach złożenia przez stronę podania w formie dokumentu elektronicznego przez ESP urzędu,
- przekazania do centralnego repozytorium danych (CRD) brakujących wzorów dokumentów elektronicznych,
- terminowej obsługi spraw kierowanych do urzędu za pośrednictwem środków komunikacji elektronicznej,
- bezzwłocznego odbierania uprawnień do systemów informatycznych pracownikom kończącym zatrudnienie w urzędzie,
- przechowywania kopii zapasowych systemów informatycznych i danych w nich zawartych w lokalizacji innej niż miejsce przetwarzania danych,
- testowania wykonanych kopii zapasowych systemów i danych w nich zawartych,
- wzmocnienia nadzoru nad procesem świadczenia e-usług,
- przeprowadzania corocznych audytów z zakresu bezpieczeństwa informacji.

WNIOSKI SYSTEMOWE

Promocja e-usług

NIK zwraca uwagę na potrzebę podjęcia przez organy jednostek samorządu terytorialnego szerszych działań w zakresie informowania o e-usługach i ich promowania, co mogłoby wpłynąć na większe zainteresowanie mieszkańców możliwością załatwiania spraw w urzędzie drogą elektroniczną. Aby zwiększyć poziom

wykorzystania e-usług i aby przekonać obywateli do zalet płynących z tej drogi kontaktu z urzędem, usługi elektroniczne powinny być bezpieczne, intuicyjne i stale dostępne dla obywateli w dogodnym dla nich czasie, tj. 24 godziny, siedem dni w tygodniu, przez cały rok. Równie istotne jest też przystępne wyjaśnienie zasad postępowania przy załatwianiu spraw drogą elektroniczną (m.in. dbałość o czytelność zamieszczanych instrukcji).

Działania promocyjne powinny być podejmowane również w wymiarze ogólnokrajowym poprzez uświadamianie obywatelom jakie konkretne sprawy mogą być załatwiane przez Internet.

Uproszczenie dostępu do e-usług

W ocenie NIK wskazany jest przegląd obowiązujących przepisów pod kątem ograniczenia obowiązku składania przez obywateli i przedsiębiorców dokumentów papierowych w urzędach. Korzystne byłoby również wprowadzenie w przyszłości bezpłatnego i prostego rozwiązania technicznego umożliwiającego potwierdzanie tożsamości w elektronicznych kontaktach z administracją (np. poprzez zastosowanie podpisu elektronicznego w dowodzie osobistym).

Rozważenie zasadności uruchomiania nowych platform regionalnych i miejscowych

Mając na uwadze dotychczasowe niewielkie wykorzystanie e-usług i możliwości platform regionalnych i miejscowych, należy rozważyć tworzenie kolejnych platform e-usług finansowanych z budżetu państwa i środków unijnych. Tym bardziej, że objęte kontrolą platformy regionalne i miejscowe oferowały m.in. e-usługi, które równolegle były udostępniane na ogólnopolskiej platformie ePUAP.

Udostępnianie kolejnych usług z użyciem gotowych szablonów

Wskazany jest dalszy rozwój koncepcji centralnego świadczenia e-usług, m.in. poprzez udostępnianie kolejnych szablonów e-usług z wykorzystaniem platformy ePUAP2. Ważne jest przy tym, aby w pierwszej kolejności udostępniać formularze tych e-usług, które dotyczą spraw najczęściej załatwianych przez obywateli w urzędach.

AUDYT BEZPIECZEŃSTWA INFORMACJI

NIK kontrolując świadczenie e-usług, sprawdziła również wypełnienie w urzędach objętych kontrolą obowiązku przeprowadzenia okresowego **audytu w zakresie bezpieczeństwa** informacji w systemach informatycznych[13]. Audytu takiego nie przeprowadzono w 1/3 skontrolowanych urzędów. Nieprawidłowość tę tłumaczono najczęściej brakiem wykwalifikowanych pracowników. W 16 jednostkach, w których przeprowadzono coroczny audyt bezpieczeństwa informacji, sformułowane zalecenia

[13] Więcej na temat obowiązku audytu bezpieczeństwa informacji znajdą Państwo w dalszej części artykułu.

dotyczyły wzmocnienia bezpieczeństwa przetwarzania informacji w systemach informatycznych urzędów.

„REALIZACJA PRZEZ PODMIOTY PAŃSTWOWE ZADAŃ W ZAKRESIE OCHRONY CYBERPRZESTRZENI RP"

Przenoszenie coraz większej aktywności do cyberprzestrzeni (m.in. Internet, e-usługi, przechowywanie danych w chmurze) powoduje dynamiczny rozwój zagrożeń i incydentów mogących naruszyć bezpieczeństwo systemów i sieci komputerowych oraz użytkowników korzystających z usług świadczonych za pomocą nowoczesnych technologii informatycznych. Dlatego zachowanie bezpieczeństwa cyberprzestrzeni jest obecnie jednym z istotnych problemów na poziomie krajowym i międzynarodowym. Wiąże się ono bowiem z zapewnieniem niezakłóconego funkcjonowania państwa, gospodarki i życia społecznego.

Zagrożenia technologiczne bezpieczeństwa (np. infekowanie szkodliwym oprogramowaniem) są coraz bardziej zaawansowane. Wzrasta także problem nielegalnych i szkodliwych treści w Internecie oraz przestępczości w cyberprzestrzeni (np. ransomware[14]).

Zapewnienie bezpieczeństwa cyberprzestrzeni[15] RP jest jednym z ważnych zadań rządu. Działania w tym zakresie wymagają systemowych rozwiązań, za pomocą których państwo jest gotowe ochraniać swoje kluczowe zasoby oraz swoich obywateli przed występującymi zagrożeniami.

NIK w tej kontroli nie badała bezpieczeństwa teleinformatycznego poszczególnych podmiotów, ani wykorzystywanych przez nie systemów informatycznych, lecz zweryfikowała istnienie systemowych rozwiązań w zakresie cyberprzestrzeni RP.

OCENA NIK

> W ocenie NIK bezpieczeństwo w cyberprzestrzeni nie jest w Polsce właściwie zapewnione. Wynika to z braku spójnych i systemowych działań w zakresie monitorowania i przeciwdziałania zagrożeniom występującym w cyberprzestrzeni.

NIK podkreśla, że kierownictwo najważniejszych instytucji publicznych nie było świadome niebezpieczeństw związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z tego faktu nowych zadań administracji państwowej. W rezultacie:

---

[14] Rodzaj oprogramowania używanego w przestępczości internetowej. Przestępca wnika do wnętrza atakowanego komputera i zaszyfrowuje dane należące do użytkownika. Następnie program umieszcza w komputerze notatkę, w której przestępca informuje co użytkownik ma zrobić, aby je odzyskać.

[15] Bezpieczeństwo cyberprzestrzeni rozumiane jest jako zapobieganie i minimalizacja skutków incydentów.

- nie podjęto dotychczas spójnych i systemowych działań, mających na celu monitorowanie i przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni oraz minimalizowanie skutków incydentów,
- nie oszacowano ryzyk dla krajowej infrastruktury teleinformatycznej oraz nie wypracowano narodowej strategii ochrony cyberprzestrzeni, stanowiącej podstawę dla działań podnoszących bezpieczeństwo teleinformatyczne,
- nie określono struktury i ram prawnych krajowego systemu ochrony cyberprzestrzeni, nie zdefiniowano obowiązków i uprawnień jego uczestników oraz nie przydzielono zasobów niezbędnych do skutecznej realizacji zadań,
- nie przygotowano procedur reagowania w sytuacjach kryzysowych związanych z cyberprzestrzenią,
- nie zorganizowano systemu zbierania i rejestrowania informacji o incydentach występujących w cyberprzestrzeni oraz nie wprowadzono prawnego obowiązku zgłaszania incydentów skierowanego do wszystkich najważniejszych użytkowników i administratorów cyberprzestrzeni.

W związku z tym administracja państwowa nie dysponuje nawet ogólną wiedzą na temat skali i rodzaju incydentów, a zatem nie ma możliwości podejmowania i koordynowania odpowiednich działań.

W ocenie NIK, istotnym czynnikiem wpływającym negatywnie na realizację zadań w obszarze bezpieczeństwa w cyberprzestrzeni był m.in. brak rozstrzygania kwestii spornych między poszczególnymi urzędami oraz zapewnienia współdziałania organów i instytucji związanych z bezpieczeństwem teleinformatycznym państwa.

W ramach zaleceń NIK określiła szereg działań związanych z ochroną cyberprzestrzeni RP, które powinny być zrealizowane przez wskazane podmioty i jednostki państwowe, w szczególności: Radę Ministrów, Ministra Administracji i Cyfryzacji (obecnie Minister Cyfryzacji), Ministra Spraw Wewnętrznych (obecnie Minister Spraw Wewnętrznych i Administracji), Agencję Bezpieczeństwa Wewnętrznego, Ministra Obrony Narodowej, Policję oraz CERT Polska[16] i inne zespoły powołane w celu reagowania na zdarzenia i incydenty w cyberprzestrzeni. Treść zaleceń znajdą Państwo w raporcie.

PODSTAWOWE REGULACJE PRAWNE

NIK zwróciła uwagę na brak odpowiednich polityk, aktów prawnych i wytycznych regulujących kwestie ochrony cyberprzestrzeni RP. Wśród obowiązujących krajowych przepisów jako kluczowe dla tego obszaru wskazała następujące regulacje prawne:

1. **Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[17]** określającą wymogi dla państwowych

[16] Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej), jest to pierwszy powstały w Polsce zespół reagowania na incydenty (Computer Emergency Response Team).

[17] Dz. U. z 2014 r. poz. 1114, z późn. zm.

systemów i rejestrów informatycznych. Zakres przedmiotowy ww. regulacji dotyczy przede wszystkim zapewnienia interoperacyjności (tj. współdziałania i wymiany danych) między różnymi systemami i bazami danych wykorzystywanymi przez podmioty państwowe do realizacji zadań publicznych.

2. **Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[18]** regulujące zagadnienia dotyczące bezpieczeństwa danych przetwarzanych za pomocą systemów informatycznych. Zgodnie z § 20 ww. rozporządzenia, podmioty realizujące zadania publiczne zostały zobowiązane do wdrożenia i doskonalenia systemów zarządzania bezpieczeństwem informacji zapewniających poufność, dostępność, integralność i rozliczalność przetwarzanych informacji[19].

Powyższe regulacje mają jednak ramowy charakter i ograniczają się tylko do systemów wykorzystywanych do realizacji zadań publicznych.

Dodatkowo NIK wskazała **ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym**. Jednak termin zarządzanie kryzysowe obejmuje działalność organów administracji publicznej będącą elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej. Ustawa ta ma zatem ograniczone zastosowanie.

ZAGROŻENIA W CYBERPRZESTRZENI I ICH ŹRÓDŁA

Istotne dla przeciwdziałania, wykrywania i podejmowania właściwych reakcji na incydenty w cyberprzestrzeni jest posiadanie odpowiedniej wiedzy w tym zakresie. Obejmuje ona m.in. rodzaje zagrożeń i ich źródła.

Źródła zagrożeń

Podstawowy podział zagrożeń występujących w cyberprzestrzeni związany jest z celami, jakie przyświecają pojedynczym ludziom, czy też organizacjom. Według tego kryterium NIK przytoczyła w raporcie następujące zagrożenia:

1. Cyber-chuligani – pojedyncze osoby lub niewielkie grupy prowadzące działania w celu sprawdzenia lub udowodnienia swoich umiejętności, dokonania odwetu, na przykład na adwersarzu lub byłym pracodawcy.

[18] Dz. U. poz. 526, z późn. zm., dalej jako: rozporządzenie KRI.

[19] Więcej na ten temat w Biuletynie Nr 4 (9)/2013 *„Zapewnienie okresowego audytu wewnętrznego w zakresie systemu bezpieczeństwa informacji w JST”* oraz Biuletynie Nr 2 (7)/2013 *„Audyt bezpieczeństwa informacji”.*

2. Cyber-aktywiści – grupy osób prowadzące działania w celu wsparcia jakiejś idei, dążące do jej rozpowszechnienia za pomocą spektakularnych działań o dużym zasięgu i zakresie, które mają godzić w czyjś wizerunek. Działania takie nie powinny, w mniemaniu atakujących, powodować istotnych strat finansowych.
3. Cyber-przestępcy – pojedyncze osoby lub grupy osób prowadzące działania w celu uzyskania korzyści materialnej, dokonujące przeważnie klasycznego oszustwa lub wyłudzenia z wykorzystaniem środków, metod i narzędzi dostępnych w cyberprzestrzeni.
4. Cyber-terroryści – pojedyncze osoby, grupy osób lub organizacje polityczne prowadzące działania w cyberprzestrzeni dla wsparcia swoich celów politycznych, dążące do ich osiągnięcia poprzez zastraszenie i wywołanie stanu zagrożenia. Wykorzystujące również cyberprzestrzeń jako narzędzie komunikacji, propagandy, gromadzenia środków finansowych oraz werbunku i szkolenia.
5. Cyber-szpiedzy – organizacje lub firmy pracujące na rzecz biznesu lub resortów siłowych prowadzące działania w cyberprzestrzeni w celu skrytego pozyskania wiedzy lub wywarcia wpływu. Wiele państw (w tym szczególnie Chiny, USA, Rosja) na szeroką skalą wykorzystują cyberprzestrzeń do zbierania informacji, szczególnie gospodarczych i technologicznych. Jest to niezwykle tania, efektywna i łatwa do ukrycia forma działalności wywiadowczej.
6. Cyber-żołnierze – organizacje najemnicze lub oddziały wojskowe przeznaczone do prowadzenia działań zbrojnych w cyberprzestrzeni. Mogą być one prowadzone samodzielnie lub we współpracy z innymi rodzajami sił zbrojnych.

Jak podkreśla NIK powyższy podział ma jedynie charakter umowny, a w wielu wypadkach jednoznaczne zakwalifikowanie źródeł zagrożeń jest utrudnione lub niemożliwe, co wynika m.in. z celowych zabiegów atakującego lub błędów w przeprowadzonej analizie.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

1. Użycie szkodliwego oprogramowania (wirusy, robaki, konie trojańskie, tylne wejścia, programy szpiegujące, procedury wykorzystujące znane lub ukrywane luki w programach komercyjnych).
2. Kradzież i wykorzystywanie cudzych danych osobowych.
3. Wyłudzanie, kradzież, fałszowanie lub niszczenie danych.
4. Blokowanie dostępu do usług (bomby pocztowe, przeciążanie aplikacji i serwisów, masowe zawłaszczanie systemów komputerowych w celu wykorzystywania ich do prowadzenia takich przeciążeń).
5. Przesyłanie niepotrzebnej lub niechcianej informacji.
6. Ataki socjotechniczne (wyłudzanie informacji poprzez podszywanie się pod instytucję lub osobę zaufaną).

7. Zaawansowane ataki celowane (prowadzone za pomocą wielu skoordynowanych i zindywidualizowanych metod ataki skierowane precyzyjnie przeciwko konkretnej osobie, organizacji lub firmie).

AUDYT I KONTROLA BEZPIECZEŃSTA TELEINFORMATYCZNEGO

NIK jako nieprawidłowość wskazała również niewykorzystanie w ramach analizy zagrożeń związanych z cyberprzestrzenią wyników zleconego audytu wewnętrznego, dotyczącego bezpieczeństwa teleinformatycznego. Audyt ten został przeprowadzony na polecenie Prezesa Rady Ministrów w 314 jednostkach administracji państwowej w okresie wrzesień – październik 2013 r.

Kontrola wykazała także, że całkowicie nie realizowano przepisów art. 25 ust. 1 pkt 3 ustawy o informatyzacji, nakładających na ministrów i wojewodów obowiązki w zakresie przeprowadzania kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych. Kontrola ta obejmowała m.in. weryfikację wymogów bezpieczeństwa tych systemów wynikających z § 20 rozporządzenia KRI.

Tymczasem regularny audyt i kontrola tego obszaru są niezbędne dla oceny przyjętych rozwiązań oraz ich usprawnienia, odpowiadającego zachodzącym zmianom.

"ZAPEWNIENIE BEZPIECZEŃSTWA DZIAŁANIA SYSTEMÓW INFORMATYCZNYCH WYKORZYSTYWANYCH DO REALIZACJI ZADAŃ PUBLICZNYCH"

Każdy urząd w ramach realizacji zadań publicznych przetwarza tysiące informacji o różnym charakterze. Coraz większa ich część znajduje się na rozmaitych nośnikach cyfrowych, w bazach danych, systemach pocztowych, archiwach, itd. Stanowią one zasób, który powinien być przez urząd odpowiednio chroniony.

NIK w kolejnej kontroli postanowiła ocenić warunki i podstawy, w szczególności formalne, stworzone w celu zapewnienia bezpieczeństwa informacji w wybranych jednostkach sektora publicznego. Kontrola nie weryfikowała natomiast zastosowanych rozwiązań technicznych.

Wobec braku centralnych zaleceń i wymagań dotyczących bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych NIK przyjęła jako wyznaczniki służące ocenie kontrolowanej działalności wskazania wynikające z Polskich Norm[20], literatury fachowej i dobrych praktyk dotyczących tego obszaru oraz minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI.

[20] PN-ISO/IEC 27001:2007.

OCENA NIK

> W ocenie NIK stopień przygotowania oraz wdrożenia Systemu Zapewnienia Bezpieczeństwa Informacji nie zapewniał akceptowalnego poziomu bezpieczeństwa danych zgromadzonych w systemach informatycznych wykorzystywanych do realizacji istotnych zadań publicznych.

Świadomość konieczności zapewnienia bezpieczeństwa informatycznego była w kontrolowanych jednostkach ograniczona, a stosowane systemy ochrony danych nie zapewniały ich bezpieczeństwa. W efekcie istnieje ryzyko, że działanie istotnych dla funkcjonowania państwa systemów teleinformatycznych zostanie zakłócone, a znajdujące się w nich dane trafią w niepowołane ręce.

W większości skontrolowanych jednostek działania były doraźne i nie zapewniały odpowiedniego, bezpiecznego i spójnego zarządzania bezpieczeństwem danych. Opierały się wyłącznie na uproszczonych lub nieformalnych zasadach wynikających z dobrych praktyk lub dotychczas zdobytego doświadczenia pracowników działów IT.

Kontrola wykazała w tym obszarze m.in.:

- brak planów zapewnienia bezpieczeństwa danych,
- niewdrożenie systemów zarządzania bezpieczeństwem informacji,
- brak niezbędnych opracowań analitycznych i procedur (w tym dotyczących incydentów, identyfikacji i ewidencji kluczowych zadań wraz z zasobami niezbędnymi do ich realizacji, dystrybucji oprogramowania antywirusowego),
- ograniczony zakres nadzoru, testowania i monitorowania bezpieczeństwa.

Istniała duża dysproporcja pomiędzy działaniami podejmowanymi dla ochrony poszczególnych grup informacji, tj. informacji objętych ustawową ochroną (niejawnych i danych osobowych) oraz innych informacji, których ochrona nie została wprost usankcjonowana, ale które mają istotne znaczenie dla prawidłowej realizacji podstawowych zadań tych jednostek.

NIK zauważa, że tylko w jednej z kontrolowanych instytucji formalnie wdrożono System Zarządzania Bezpieczeństwem Informacji i wprowadzono wszystkie procesy wymagane dla zapewnienia bezpieczeństwa danych. Było to związane z działaniami podjętymi w celu uzyskania certyfikatu ISO 27001.

Jednakże również w systemie funkcjonującym w tej jednostce kontrola wykryła nieprawidłowości, które dotyczyły m.in.:

- rozbieżności pomiędzy deklarowanym a faktycznym poziomem zabezpieczenia informacji,
- czytelności i kompletności głównych procedur bezpieczeństwa,
- braku odpowiednich narzędzi nadzoru w przypadku powierzenia zasobów jednostki wykonawcy zewnętrznemu (np. nie określono sposobu szacowania ryzyka związanego z utratą informacji),

- braku mierników i zasobów odpowiadających celom w zakresie bezpieczeństwa,
- niekompletności systemu zbierania i analizy incydentów.

WNIOSKI I ZALECENIA DOTYCZĄCE ZARZĄDZANIA BEZPIECZEŃSTWEM IT

W zakresie zarządzania bezpieczeństwem IT NIK stwierdziła m.in.:

- niewdrożenie systemów zarządzania bezpieczeństwem informacji,
- ograniczoną wiedzę kierownictwa jednostek w zakresie konieczności ochrony bezpieczeństwa informacji i wymogów z tym związanych,
- brak niezbędnych opracowań analitycznych, planów i procedur (dotyczących incydentów, identyfikacji kluczowych zadań, dystrybucji oprogramowania antywirusowego, okresowego informowania o stanie bezpieczeństwa, itp.).

Wnioski NIK przedstawione w ramach czterech kluczowych obszarów wyodrębnionych w tym zakresie oraz odnoszące się do nich zalecenia znajdą Państwo poniżej.

Identyfikacja ryzyka

Kontrolowane jednostki w ograniczonym zakresie wykorzystywały metody identyfikacji, monitorowania i zapobiegania ryzyku związanemu z bezpieczeństwem informacji przetwarzanych w systemach teleinformatycznych.

W trzech skontrolowanych jednostkach proces ten był prowadzony jedynie w zakresie niezbędnym dla realizacji wymagań:

- Polityki Ochrony Cyberprzestrzeni[21],
- przepisów o ochronie informacji niejawnych,
- obowiązków związanych z operowaniem infrastrukturą krytyczną.

Identyfikacja ryzyka ma zasadnicze znaczenie dla rozpoznania obszarów z jednej strony „najcenniejszych" dla jednostki, a z drugiej strony najbardziej zagrożonych. Pozwala na wprowadzenie mechanizmów zabezpieczających oraz alokację zasobów odpowiednią do faktycznych potrzeb.

Proces szacowania ryzyka powinien być przeprowadzony w odniesieniu do wszystkich posiadanych i przetwarzanych informacji, z uwzględnieniem realizowanych zadań i specyfiki instytucji. Przeprowadzenie procesu szacowania ryzyka powinno być poprzedzone m.in. doborem metodyki prac, zidentyfikowaniem aktywów i określeniem ich wartości.

Zabezpieczenie informacji w kontrolowanych jednostkach

Stwierdzona dysproporcja pomiędzy działaniami podejmowanymi dla ochrony różnych grup informacji (objętych ustawową ochroną oraz pozostałych), może mieć poważne

[21] Dokument strategiczny przyjęty na podstawie uchwały Rady Ministrów z dnia 25 czerwca 2013 r., którego celem jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa.

konsekwencje dla właściwego szacowania ryzyka, dzielenia zasobów, a przede wszystkim zapewnienia ciągłości działania instytucji mających istotne znaczenie dla funkcjonowania państwa.

Należy zidentyfikować informacje najważniejsze dla funkcjonowania jednostki oraz dokonać ich klasyfikacji. Oprócz informacji, co do których wymóg ochrony zapisany jest wprost w przepisach prawa, należy uwzględnić inne informacje, równie ważne, o których ochronę każda jednostka także powinna zadbać. Przystępując do takiej analizy należy sobie zadać następujące pytania: Jakimi informacjami dysponuje jednostka? Które informacje należy chronić? Gdzie są zgromadzone? Kto jest ich właścicielem? Kto powinien mieć do nich dostęp? Jak są rozpowszechniane?

Odpowiedzialność za bezpieczeństwo

W żadnej ze skontrolowanych jednostek nie określono precyzyjnie zakresu odpowiedzialności poszczególnych osób za zapewnienie bezpieczeństwa danych, co prowadziło do sporów kompetencyjnych. Najczęściej odpowiedzialność w tym zakresie była powierzana komórkom IT. Skutkowało to ograniczeniem faktycznego zakresu ochrony informacji jedynie do systemów informatycznych i nośników danych oraz ograniczało, z przyczyn kompetencyjnych, możliwości budowania systemów ochrony informacji obejmujących całe instytucje. Rozwiązanie takie sprawiało również, że pozostałe komórki organizacyjne, nie czując się współodpowiedzialnymi za ochronę informacji, uznawały wymagania definiowane przez informatyków jako nieuzasadnione utrudnienia, które ich nie dotyczą. Również kierownictwa tych instytucji nie wykazując wsparcia dla realizacji delegowanych zadań, w niedostatecznym zakresie uznawały swoją rolę w kreowaniu i osiąganiu strategicznych celów dotyczących bezpieczeństwa informacji.

Tymczasem należy zauważyć, że wiele udanych ataków hakerskich wcale nie polegało na fizycznym przełamaniu zabezpieczeń informatycznych, lecz na wykorzystaniu metod socjotechnicznych w celu uzyskania dostępu do chronionych systemów.

Dlatego bardzo ważne jest, aby wszyscy pracownicy posiadali wiedzę na temat zagrożeń oraz działań jakie należy podjąć w przypadku zaistnienia incydentu. Odpowiedzialność za zapewnienie bezpieczeństwa informacji nie może spoczywać jedynie na koordynatorze wyznaczonym w jednostce, lecz na każdym użytkowniku systemów teleinformatycznych. Wraz z odpowiedzialnością musi być przypisany dostateczny poziom uprawnień legitymujący do działania w sferze zarządzania procesem i skoordynowania działań związanych z zapewnieniem bezpieczeństwa w całej jednostce.

Audyt bezpieczeństwa

We wszystkich kontrolowanych jednostkach prowadzono audyt bezpieczeństwa. Raporty z tych audytów stanowiły dla kierownictwa kontrolowanych jednostek jedyne istotne źródło informacji o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz działaniach niezbędnych do przeprowadzenia.

NIK podkreśliła pozytywny wpływ audytów na świadomość dysponentów jednostek kontrolowanych, co do konieczności podjęcia określonych działań, w tym inicjatywy w zakresie:

- poprawy jakości wykorzystywanych polityk bezpieczeństwa i towarzyszących im dokumentów,
- wdrażania Systemów Zapewnienia Bezpieczeństwa Informacji,
- modyfikowania struktur odpowiedzialnych za bezpieczeństwo,
- realizacji obowiązkowych audytów wynikających z rozporządzenia KRI,
- powołania specjalistycznych zespołów.

Istotnym problemem był jednak brak konsekwencji i zaangażowania kierownictwa kontrolowanych jednostek w realizację zaleceń audytorów, co w efekcie wymuszało powrót do realizacji jedynie rutynowych zadań.

Pozostałe zagadnienia

NIK w ramach kontroli zbadała również realizację działań kontrolowanych jednostek w odniesieniu do następujących zagadnień:

- opracowania planu zapewnienia bezpieczeństwa,
- testowania, nadzorowania i monitorowania bezpieczeństwa,
- zarządzania kluczami kryptograficznymi,
- ochrony przed złośliwymi oprogramowaniami,
- bezpieczeństwa sieciowego,
- zarządzania tożsamością i kontami użytkowników,
- ochrony technologii zabezpieczeń,
- wymiany wrażliwych danych.

Zapoznanie się z wnioskami w tym zakresie może pomóc w zweryfikowaniu i usprawnieniu rozwiązań przyjętych w Państwa jednostce.

PODSUMOWANIE

We wszystkich kontrolowanych obszarach bardzo istotne znaczenie ma świadomość odnośnie do możliwości oraz zagrożeń jakie niesie ze sobą korzystanie z nowoczesnych narzędzi informatycznych. Dlatego niezbędne są działania edukacyjne i promocyjne zarówno na poziomie ogólnopolskim, jak i poszczególnych jednostek.

W zakresie cyberbezpieczeństwa NIK rekomenduje opracowanie i wprowadzenie na szczeblu centralnym generalnych zaleceń i wymagań dotyczących zapewnienia bezpieczeństwa IT, obowiązujących wszystkie podmioty publiczne. Ministerstwo Cyfryzacji podjęło szereg działań, które mają być kontynuowane. Jednym z nich jest opracowanie dokumentu „Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej

Polskiej", opracowanej przez Zespół zadaniowy Ministerstwa Cyfryzacji w lutym 2016 r.[22]

Zapewnienie wdrożenia tych regulacji wymaga jasnego określenia ról w systemie oraz wskazania koordynatora działań. Dotyczy to zarówno systemu ogólnopolskiego, jak i poszczególnych urzędów administracji publicznej, w których również powinny zostać opracowane odpowiednie procedury.

Podstawą dla odpowiedniego zaprojektowania systemu bezpieczeństwa jest identyfikacja najważniejszych informacji, ich klasyfikacja oraz ocena ryzyk, dzięki czemu wzrasta prawdopodobieństwo, że informacja będzie przetwarzana zgodnie z przeznaczeniem przy zachowaniu dostępności, integralności i poufności tego procesu. W konsekwencji wydatki na ochronę będą koncentrowane tam, gdzie jest to wymagane.

Rozwój cyberprzestrzeni pociąga za sobą konieczność regularnej oceny i aktualizacji przyjętych rozwiązań w jednostkach. Istotnym źródłem informacji nt. kluczowych potrzeb w tym zakresie powinien być audyt bezpieczeństwa informacji.

Bardzo ważne jest również zapoznawanie się z przykładami dobrych praktyk oraz wymiana doświadczeń.

Jak twierdzi NIK zapewnienie bezpieczeństwa informacji na zakładanym poziomie wymaga systemowej i ciągłej realizacji odpowiednich procesów.

ŹRÓDŁA:

1. Raporty i informacje opublikowane na stronie internetowej NIK:
   - „Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego", https://www.nik.gov.pl/plik/id,10420,vp,12749.pdf ,
   - Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP", https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf ,
   - „Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych", https://www.nik.gov.pl/plik/id,10771,v,artykul_12904.pdf .
2. Strategia „Sprawne Państwo 2020, http://administracja.mac.gov.pl/adm/departament-administra/strategia-sprawne-panst/8085,Strategia-Sprawne-Panstwo-2020.html .
3. Prezentacja Prezesa NIK przedstawiona podczas Konferencji CyberGOV 2016, https://cybergov.pl/cybergov-2016/ .

Opracowanie: Departament Polityki Wydatkowej Ministerstwa Finansów.

[22] https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf .

PUBLIKACJE NA STRONIE INTERNETOWEJ MINISTERSTWA FINANSÓW

Zachęcamy do zapoznania się z materiałami przygotowanymi przez Departament Polityki Wydatkowej MF opublikowanymi na stronie internetowej Ministerstwa Finansów.

OCENA FUNKCJONOWANIA AUDYTU WEWNĘTRZNEGO W JEDNOSTKACH SEKTORA FINANSÓW PUBLICZNYCH W ROKU 2015

Departament Polityki Wydatkowej MF, w ramach realizacji zadań Ministra Finansów w zakresie koordynacji kontroli zarządczej i audytu wewnętrznego w sektorze publicznym[23], dokonał oceny funkcjonowania audytu wewnętrznego w jednostkach sektora finansów publicznych w roku 2015.

Ocena dotyczy następujących obszarów:

- organizacji komórki audytu wewnętrznego,
- planowania i przeprowadzania audytu wewnętrznego,
- efektywności audytu wewnętrznego,
- jakości audytu wewnętrznego.

Ocena została sporządzona na podstawie informacji uzyskanych z jednostek administracji rządowej[24], jednak wnioski z niej wynikające mogą mieć zastosowanie również do jednostek samorządowych.

Dokument ten został opublikowany na stronie Internetowej MF http://www.mf.gov.pl w zakładce: Działalność/Finanse publiczne/Kontrola zarządcza i audyt wewnętrzny/Audyt wewnętrzny w sektorze publicznym/Ocena audytu wewnętrznego.

RAPORT BENCHMARKINGOWY ZA ROK 2015

Departament Polityki Wydatkowej MF po raz piąty opublikował Raport benchmarkingowy, przedstawiający podsumowanie badania wybranych wskaźników opisujących komórki audytu wewnętrznego i usługodawców oraz wyniki ich pracy.

Celem Raportu, podobnie jak w latach ubiegłych, jest umożliwienie audytorom wewnętrznym porównania własnej pracy z obliczonymi wskaźnikami.

Wskaźniki zastosowane w raporcie zostały opracowane podobnie jak w przypadku *Oceny funkcjonowania audytu wewnętrznego w jednostkach sektora finansów*

[23] Art. 292 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2013 r. poz. 885, z późn. zm.).

[24] Termin „jednostki administracji rządowej" odnosi się do jednostek, o których mowa w art. 274 ust. 1, 2, 5 i 6 ustawy oraz jednostek nienależących do administracji samorządowej, których kierownicy jednostek podjęli decyzję o prowadzeniu audytu wewnętrznego.

publicznych, w oparciu o dane przekazane Ministrowi Finansów przez jednostki administracji rządowej. Jednak wyniki raportu benchmarkingowego mogą być również wykorzystane przez audytorów wewnętrznych jednostek samorządowych.

Dokument ten został opublikowany na stronie MF http://www.mf.gov.pl w zakładce: Działalność/Finanse publiczne/Kontrola zarządcza i audyt wewnętrzny/Audyt wewnętrzny w sektorze publicznym/Baza wiedzy/Benchmarking audytu wewnętrznego raporty.

PUBLIKACJE NA TEMAT SPOTKAŃ AUDYTORÓW WEWNĘTRZNYCH JSFP

W dniu 28 kwietnia 2016 r. w Ministerstwie Finansów odbyło się spotkanie audytorów wewnętrznych jednostek sektora finansów publicznych poświęcone tematyce zamówień publicznych. Podczas spotkania zostało omówione:

- stosowanie klauzul prospołecznych w zamówieniach publicznych na przykładzie praktyk Ministerstwa Finansów oraz
- realizowanie zamówień publicznych poniżej progu 30.000 euro na przykładzie rozwiązań stosowanych w Urzędzie Miejskim w Dąbrowie Górniczej.

Notatka oraz prezentacje ze spotkania zostały opublikowane na stronie internetowej MF http://www.mf.gov.pl w zakładce: Działalność/Finanse Publiczne/Audyt wewnętrzny i kontrola zarządcza w sektorze publicznym/ Audyt wewnętrzny w sektorze publicznym/Spotkania audytorów.

OD REDAKCJI

Serdecznie zapraszamy Państwa do lektury publikowanych materiałów i kontaktów z naszym Departamentem. Chętnie służymy Państwu wsparciem merytorycznym.

Zachęcamy również do dzielenia się własnymi dobrymi praktykami, których publikacja pozwoli innym jednostkom na usprawnienie systemów kontroli zarządczej. Będziemy wdzięczni za wszystkie Państwa sugestie, propozycje i uwagi w sprawie *Biuletynu.*

MINISTERSTWO FINANSÓW; ŚWIĘTOKRZYSKA 12; 00-960 WARSZAWA

WYDAWCA: MINISTER FINANSÓW

REDAKTOR NACZELNY – Katarzyna Szarkowska, Dyrektor Departamentu Polityki Wydatkowej MF

REDAKTOR PROWADZĄCY – Monika Kos, Radca Ministra w Departamencie Polityki Wydatkowej MF

REDAKCJA: Wydział Standardów Zarządzania w Sektorze Publicznym Departamentu Polityki Wydatkowej MF

KONTAKT:

tel.: 22 694 42 42

fax: 22 694 47 41

e-mail:RedakcjaBKZ@mf.gov.pl

lub SekretariatPW@mf.gov.pl