MINISTER
NAUKI I SZKOLNICTWA WYŻSZEGO

BKA.WK.0912.9.2019.BŁ
ala

Warszawa, dnia 8 lipca 2019 r.

Pan
dr Olaf Gajl
Dyrektor
Ośrodka Przetwarzania Informacji –
Państwowego Instytutu Badawczego

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 6 ust. 3 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1], art. 25 ust. 1 pkt 3 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[2] oraz art. 35 ustawy z dnia 30 kwietnia 2010 r. *o instytutach badawczych*[3], Minister Nauki i Szkolnictwa Wyższego (dalej: Minister) przeprowadził kontrolę w Ośrodku Przetwarzania Informacji – Państwowym Instytucie Badawczym, Al. Niepodległości 188B, 00-608 Warszawa (dalej: OPI-PIB, Instytut) w zakresie *działania systemów teleinformatycznych używanych do realizacji zadań publicznych oraz realizacji obowiązków wynikających z art. 13 ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.*

Zgodnie z art. 47 w związku z art. 46 ust. 1 *ustawy o kontroli w administracji rządowej*, przekazuję Panu Dyrektorowi *Wystąpienie pokontrolne*, zawierające ustalenia i ocenę skontrolowanej działalności wraz z zaleceniami pokontrolnymi.

Kontrola została przeprowadzona[4] w trybie zwykłym określonym *ustawą o kontroli w administracji rządowej* i obejmowała okres od dnia 1 stycznia 2018 r. do dnia rozpoczęcia kontroli, z możliwością zasięgania informacji z okresów wcześniejszych, jeżeli miały wpływ na kontrolowaną działalność.

Celem kontroli było racjonalne zapewnienie, że systemy teleinformatyczne wykorzystywane do realizacji zadań publicznych, w tym rejestry publiczne, spełniają minimalne wymagania w zakresie elektronicznej wymiany informacji (interoperacyjności), są bezpieczne i dostępne dla wszystkich obywateli.

ul. Wspólna 1/3, 00-529 Warszawa
tel. (22) 628 19 44, faks: (22) 529 26 21, e-mail: sekretariat.minister@nauka.gov.pl, www.nauka.gov.pl

W szczególności kontrola miała za zadanie ocenić stopień:

- zapewnienia spójności rejestrów publicznych oraz współdziałania różnych systemów teleinformatycznych poprzez właściwą organizację wymiany informacji w postaci elektronicznej, współpracę z innymi systemami/rejestrami informatycznymi oraz procesy wspomagania świadczenia usług drogą elektroniczną,
- zapewnienia skutecznego zarządzania bezpieczeństwem informacji dla badanych systemów teleinformatycznych bezpieczeństwa, w tym zapewnienia dostępności, autentyczności, poufności, niezawodności i integralności danych przetwarzanych przez te systemy,
- zapewnienia dostępności treści zawartych na stronach internetowych dla osób z niepełnosprawnościami.

Analizie poddano funkcjonujący w Instytucie System Zarządzania Bezpieczeństwem Informacji (SZBI), 2 z 14 systemów teleinformatycznych OPI-PIB, tj.:

1. Zintegrowany System Informacji o Szkolnictwie Wyższym i Nauce POL-on,
2. System wspomagania innowacyjności Inventorum,

oraz stronę internetową OPI-PIB: https://www.opi.org.pl/.

Wybierając systemy do kontroli, zastosowano dobór celowy oparty o wybór systemów krytycznych z punktu widzenia realizacji celów statutowych Instytutu.

(Dowód: akta kontroli str. 43-52)

OCENA OGÓLNA

W niniejszej kontroli zastosowano mierniki i skalę ocen, o których mowa w części III pkt 7 *Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych*, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r. Biorąc pod uwagę kryterium legalności, celowości i rzetelności, działalność niżej wymienionych obszarów oceniono[5]:

---

[1] Dz. U. Nr 185, poz. 1092, ze zm., dalej: *ustawa o kontroli w administracji rządowej.*
[2] Dz. U. z 2019 r., poz. 700, dalej: *ustawa o informatyzacji.*
[3] Dz. U. z 2018 r., poz. 736, ze zm.
[4] Czynności kontrolne prowadzone były w dniach 9 maja 2019 r. – 7 czerwca 2019 r. przez Barbarę Łukasik i Jerzego Przybyłowskiego, głównych specjalistów w Biurze Kontroli i Audytu MNiSW. Ze względu na konieczność zbadania w toku kontroli zagadnień wymagających wiedzy specjalistycznej, do udziału w kontroli, na podstawie art. 33 *ustawy o kontroli w administracji rządowej*, powołano w charakterze biegłego Pana Bogdana Kowalczyka.
[5] Na potrzeby niniejszej kontroli, w MNiSW przyjęto 4-stopniową skalę ocen: pozytywna, pozytywna z uchybieniami, pozytywna z nieprawidłowościami, negatywna.

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną – pozytywnie;
2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych – pozytywnie z uchybieniami;
3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami – pozytywnie.

Podsumowując wyniki analizy dokumentacji źródłowej, oględzin na miejscu w siedzibie Instytutu oraz uzyskanych wyjaśnień, pod kątem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych oraz przestrzegania wymagań Krajowych Ram Interoperacyjności, działalność OPI-PIB w badanym zakresie oceniono **pozytywnie z uchybieniami.**

SZCZEGÓŁOWE USTALENIA KONTROLI

Wykaz skrótów i pojęć:

BIP — Biuletyn Informacji Publicznej;
BI — bezpieczeństwo informacji;
baza konfiguracji CMDB — baza danych zarządzania konfiguracją (*Configuration Management DataBase*), centralny rejestr zasobów informatycznych, ich konfiguracji i relacji pomiędzy elementami konfiguracji;
CRWDE — centralne repozytorium wzorów dokumentów elektronicznych;
ePUAP — Elektroniczna Platforma Usług Administracji Publicznej. System teleinformatyczny udostępniający usługi elektroniczne administracji publicznej dla obywateli i podmiotów prowadzony przez ministra właściwego do spraw informatyzacji;
ESP — elektroniczna skrzynka podawcza;
rozporządzenie KRI — 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*[6]*;*
KRI — Krajowe Ramy Interoperacyjności stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą;
dostępność — właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;

[6] Dz. U. z 2016 r., poz. 113, z późn. zm.

integralność — zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
interoperacyjność — 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; osiąganie interoperacyjności następuje poprzez ciągłe doskonalenie jednostki w zakresie zarządzania systemami informatycznymi;
model usługowy — model architektury systemu informatycznego, w którym dla użytkowników (klientów/odbiorców) zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji;
polityka bezpieczeństwa informacji, polityka BI, PBI — zestaw praw, reguł i praktycznych doświadczeń, regulujących sposób zarządzania, ochrony i dystrybucji informacji wewnątrz określonej organizacji;
poufność — zapewnienie, że informacja jest dostępna tylko dla osób do tego upoważnionych;
usługa elektroniczna — w myśl art. 2 pkt 4 ustawy z dnia 8 lipca 2002 r. *o świadczeniu usług drogą elektroniczną*[7], jest to usługa świadczona bez jednoczesnej obecności stron (na odległość), poprzez przekaz informacji na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania;
współdzielenie informacji — wspólne użytkowanie tych samych zasobów przez różne osoby i/lub podmioty, np. zasobów takich jak: pliki, bazy danych, dokumenty itp.

Kontekst organizacyjny

Ośrodek Przetwarzania Informacji – Państwowy Instytut Badawczy został utworzony na mocy Zarządzenia nr 12 Ministra - Kierownika Urzędu Postępu Naukowo-Technicznego i Wdrożeń z dnia 13 grudnia 1990 r. *w sprawie utworzenia jednostki badawczo-rozwojowej*[8] jako Ośrodek Przetwarzania Informacji, któremu na mocy rozporządzenia Rady Ministrów z dnia 23 października 2013 r. nadano status państwowego instytutu badawczego[9]. OPI-PIB figuruje w rejestrze przedsiębiorców prowadzonym przez Sąd Rejonowy dla m. st. Warszawy Sąd Gospodarczy XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS: 0000127373. Posiada NIP nr 525-000-91-40 oraz REGON nr 006746090.

Dyrektorem OPI-PIB jest dr Olaf Gajl, który pełni tę funkcję od dnia 24 lutego 2005 r., z wyłączeniem okresu od 21 grudnia 2005 r. do 31 października 2007 r., kiedy przebywał

[7] Dz. U. z 2017 r., poz. 1219.
[8] Dz. Urz. Urzędu Postępu Naukowo-Technicznego i Wdrożeń Nr 4, poz. 13.
[9] Dz. U. poz. 1452.

na urlopie bezpłatnym z uwagi na pełnienie funkcji podsekretarza stanu w Ministerstwie Nauki i Szkolnictwa Wyższego (dalej: MNiSW).

Zgodnie z § 3 Statutu OPI-PIB[10], przedmiotem działania Instytutu jest prowadzenie badań naukowych lub prac rozwojowych oraz wdrażanie ich wyników i świadczenie usług w zakresie systemów informacyjnych, ich projektowania, eksploatacji i doskonalenia, pozyskiwania i opracowywania informacji zbiorczej, przekrojowej i syntetycznej dotyczącej badań naukowych i prac rozwojowych, transferu technologii, innowacyjności oraz edukacji, w tym dla celów statystycznych.

OPI-PIB kompleksowo tworzy systemy informatyczne wspierające rozwój nauki i szkolnictwa wyższego, począwszy od metodologii i aspektów technologicznych, przez gromadzenie informacji, ich weryfikację (organizacja procesów, przeszukiwanie sieci z analizą semantyczną włącznie), aż do agregacji danych oraz ich wizualizacji. Głównym odbiorcą wyników badań OPI-PIB jest MNiSW, któremu służą jako narzędzie wspomagające proces podejmowania decyzji. Systemy tworzone przez OPI-PIB wspierają także działania dwóch centralnych agencji finansujących badania: Narodowego Centrum Nauki oraz Narodowego Centrum Badań i Rozwoju, jak również innych resortów (np. Ministerstwa Infrastruktury, Ministerstwa Inwestycji i Rozwoju, Ministerstwa Przedsiębiorczości i Technologii), ekspertów i przedsiębiorców.

Nadzór nad funkcjonowaniem OPI-PIB sprawuje minister właściwy do spraw nauki[11], do którego kompetencji należy ocena poziomu naukowego instytutu i jakości prowadzonych w nim badań naukowych i prac rozwojowych oraz zgodności działalności instytutu z zadaniami określonymi w art. 2 ust. 1 i 2 *ustawy o instytutach badawczych.*

Budynki należące do Instytutu, znajdujące się w lokalizacjach: al. Niepodległości 188b i 186 w Warszawie, stanowią własność jednostki i znajdują się na gruncie użytkowanym wieczyście od Skarbu Państwa. Ponadto OPI-PIB korzysta z wynajmowanych powierzchni w budynku przy ul. Rychlińskiego 2 w Warszawie oraz w budynku przy ul. Wiktorskiej 63.

W kontrolowanym okresie strukturę organizacyjną Instytutu określał *Regulamin Organizacyjny Ośrodka Przetwarzania Informacji – Państwowego Instytutu Badawczego*, wprowadzony w 2017 r. Zarządzeniem Dyrektora OPI-PIB[12], do którego w 2018 r. zostały dwukrotnie wprowadzone zmiany[13].

(Dowód: akta kontroli str. 53-54, 58-90)

---

[10] Zatwierdzonego przez Ministra Nauki i Szkolnictwa Wyższego Zarządzeniem z dnia 23 października 2014 r. (Dz.U. z 2014 r., poz. 60).

[11] art. 34 *ustawy o instytutach badawczych.*

[12] Zarządzenie nr 4/2017 Dyrektora OPI-PIB z dnia 28 marca 2017 r. *w sprawie wprowadzenia Regulaminu Organizacyjnego Ośrodka Przetwarzania Informacji-Państwowego Instytutu Badawczego.*

[13] Zarządzenie nr 4/2018 Dyrektora OPI-PIB z dnia 10 kwietnia 2018 r. *w sprawie wprowadzenia zmian do Regulaminu Organizacyjnego Ośrodka Przetwarzania Informacji-Państwowego Instytutu Badawczego i Zarządzenie nr 10/2018 Dyrektora OPI-PIB z dnia 23 sierpnia 2018 r. w sprawie wprowadzenia zmian do Regulaminu Organizacyjnego Ośrodka Przetwarzania Informacji-Państwowego Instytutu Badawczego.*

Za realizację zadań wynikających z § 20 rozporządzenia KRI w kontrolowanym okresie odpowiedzialny był Dyrektor OPI-PIB, do obowiązków którego należał (zgodnie z *ustawą o informatyzacji*) m.in.: nadzór nad sprawami z zakresu administrowania bezpieczeństwem informacji. Za bezpieczeństwo informacji w OPI-PIB odpowiadali także: Zastępca Dyrektora, Kierownicy komórek organizacyjnych, Liderzy zespołów oraz osoby zajmujące samodzielne stanowiska (każdy w zakresie podległych mu obszarów), tj. Inspektor Ochrony Danych, Administrator Bezpieczeństwa Systemów, Administratorzy Systemów Informatycznych, Administratorzy Serwerów, Administratorzy Baz Danych, Administrator Kopii Zapasowych oraz Administrator Sieci. Odpowiedzialność za bezpieczeństwo informacji przetwarzanych w związku z wykonywanymi obowiązkami ponoszą także wszyscy pracownicy, współpracownicy oraz podmioty zewnętrzne (na podstawie zawartych umów).

Role, obowiązki i zakresy odpowiedzialności Dyrektora OPI-PIB oraz ww. osób w procesie ochrony zasobów informacyjnych zostały określone w Polityce Bezpieczeństwa Informacji OPI-PIB (dalej: PBI), wdrożonej Zarządzeniem Nr 6/2015 Dyrektora OPI-PIB z dnia 5 maja 2015 r. *w sprawie wprowadzenia systemu zarządzania bezpieczeństwem informacji w Ośrodku Przetwarzania Informacji – Państwowym Instytucie Badawczym,* zaktualizowanej w 2015 r.[14] oraz w 2019 r.[15]

(Dowód: akta kontroli str. 55-57, 142-313)

1. Obszar wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami/rejestrami informatycznymi i wspomagania świadczenia usług drogą elektroniczną w OPI-PIB, oceniono pozytywnie.

Przepisy dotyczące interoperacyjności mają na celu stworzenie warunków do współdziałania ze sobą systemów informatycznych jednostek realizujących zadania publiczne w celu zapewnienia szybkiej wymiany informacji, zarówno wewnątrz jednostki, jak i z urzędami administracji publicznej. Wdrożenie tych przepisów powinno przyczynić się do usprawnienia realizacji przez nie zadań, w tym załatwiania spraw obywateli i przedsiębiorców, na odległość i w krótszym czasie, bez żądania informacji będących już w posiadaniu jednostki. Jednocześnie, powinny zostać stworzone warunki korzystania z serwisów internetowych jednostki przez osoby z niepełnosprawnościami.

1.1. Obieg dokumentów

Stosowanie systemu elektronicznego zarządzania obiegiem dokumentów wpływa na porządkowanie i usprawnianie ich obiegu w jednostce, znacząco ułatwia i przyspiesza

[14] Aneks nr 2 z dnia 2 listopada 2015 r. do Zarządzenia Nr 6/2015 Dyrektora OPI-PIB z dnia 5 maja 2015 r.
[15] Zarządzenie Nr 3/2019 Dyrektora OPI-PIB z dnia 18 marca 2019 r. *w sprawie aktualizacji w systemie zarządzania bezpieczeństwem informacji w Ośrodku Przetwarzania Informacji – Państwowym Instytucie Badawczym.*

prowadzenie archiwizacji oraz zapewnia bezpośredni dostęp do dokumentów archiwalnych, co w konsekwencji przyspiesza proces załatwiania spraw i minimalizuje nakład pracy.

W OPI-PIB funkcjonuje tradycyjny (papierowy) obieg dokumentacji stanowiącej korespondencję zewnętrzną. Rejestracja dokumentów wpływających i wypływających jest wspomagana oprogramowaniem pełniącym funkcję dziennika korespondencji. Na potrzeby organizacji obiegu dokumentacji wewnętrznej, związanej z realizacją projektów informatycznych i procesów utrzymaniowych systemów informatycznych, w OPI-PIB wykorzystywane są specjalistyczne narzędzia programowe gromadzące, przetwarzające, udostępniające i archiwizujące informacje, w tym m.in. oprogramowanie Jira Software Atlassian.

Zgodnie z art. 16 ust. 1 oraz ust. 1a *ustawy o informatyzacji*, OPI-PIB udostępniał Elektroniczną Skrzynkę Podawczą (ESP) na platformie ePUAP pod adresem /OPIPIB/SkrytkaESP, która pozwalała na przesyłanie drogą elektroniczną korespondencji skierowanej do jednostki, w tym pism ogólnych, skarg, wniosków, zapytań itp. Na stronie podmiotowej BIP OPI-PIB znajdują się niezbędne informacje o możliwości korzystania z ESP na platformie ePUAP, w tym instrukcje i wymagania dla dokumentów elektronicznych dostarczanych do OPI-PIB. Korespondencja wpływająca za pośrednictwem ESP jest kierowana do dyrektora OPI-PIB, a następnie jest dekretowana na właściwych merytorycznie kierowników jednostek organizacyjnych.

Ze względu na specyfikę działalności statutowej, OPI-PIB, w tym nieznaczną ilość korespondencji zewnętrznej oraz stosowanie specjalistycznych narzędzi programowych dla przetwarzania dokumentacji wewnętrznej, należy uznać, że OPI-PIB zapewnił właściwy poziom bezpieczeństwa informacji, co oznacza spełnienie wymagania § 20 ust. 2 pkt 9 rozporządzenia KRI.

Funkcjonowanie tego obszaru oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48, 91-126)

1.2. Format danych udostępniany przez badane systemy informatyczne

Podmioty realizujące zadania publiczne mają obowiązek umożliwić wymianę danych pomiędzy różnymi systemami informatycznymi oraz swobodny dostęp do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików.

Zespół kontrolny stwierdził, że dla badanych systemów teleinformatycznych OPI-PIB kodowanie znaków w wysyłanych z nich dokumentach odbywa się według standardu Unicode UTF-8, co jest zgodne z § 17 ust. 1 rozporządzenia KRI. Stosowane w OPI-PIB systemy udostępniają zasoby informatyczne w formatach określonych w załączniku nr 2 do rozporządzenia KRI, tj. zgodnie z § 18 ust. 1 rozporządzenia KRI.

Powyższy obszar oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48)

1.3. Usługi elektroniczne, centralne repozytorium wzorów dokumentów elektronicznych, model usługowy oraz współpraca badanych systemów informatycznych z innymi systemami

W okresie objętym kontrolą, ze względu na specyfikę działalności statutowej, OPI-PIB:

- nie opracował i nie świadczył usług drogą elektroniczną, w związku z czym nie posiadał udokumentowanych procedur określających deklarowany poziom dostępności tych usług;
- nie korzystał, ani nie tworzył własnych wzorów dokumentów elektronicznych;
- nie realizował interaktywnych usług elektronicznych na poziomie wyższym od pierwszego (poziom informacyjny) [16];
- nie był właścicielem systemów realizujących funkcje publiczne, a jedynie administrował od strony technicznej powierzonymi systemami na rzecz ich właścicieli i nie decydował o zakresie wymiany danych pomiędzy utrzymywanymi systemami.

Zatem spełnienie wymagań rozporządzenia KRI w zakresie dotyczącym usług elektronicznych, centralnego repozytorium wzorów dokumentów elektronicznych, modelu usługowego oraz współpracy badanych systemów informatycznych z innymi systemami nie dotyczyło OPI-PIB.

W związku z powyższym zagadnienia te nie podlegały ocenie.

(Dowód: akta kontroli str. 43-48)

2. Wdrożenie i funkcjonowanie SZBI w systemach teleinformatycznych OPI-PIB oceniono pozytywnie z uchybieniami. Na ocenę tą miało wpływ m.in. to, że przeprowadzona analiza ryzyka dotycząca bezpieczeństwa informacji nie zakończyła się opracowaniem dokumentu zawierającego podsumowanie wyników tej analizy i plan postępowania z ryzykiem. W konsekwencji dobór zastosowanych zabezpieczeń informacji i systemów teleinformatycznych nie wynikał z analizy ryzyka i planu postępowania z ryzykiem. Stwierdzono również brak szczegółowych regulacji wewnętrznych dotyczących zasad postępowania z logami systemowymi oraz brak ich systematycznych przeglądów.

[16] Według klasyfikacji, opracowanej na zlecenie Komisji Europejskiej, która zawiera pięciostopniową skalę dojrzałości usług elektronicznych. Poziom pierwszy – informacyjny oznacza, że instytucje publikują informacje w Internecie, a odbiorcy (obywatele, klienci, użytkownicy) mogą się z nimi zapoznać. Kolejne poziomy kształtują się następująco: drugi – interakcyjny, trzeci – transakcyjny, czwarty – integracyjny, piąty – personalizacyjny.

Obowiązkiem podmiotu realizującego zadania publiczne jest opracowanie i ustanowienie, wdrożenie i eksploatowanie, monitorowanie i przeglądanie oraz utrzymywanie i doskonalenie systemu zarządzania bezpieczeństwem informacji (SZBI), gwarantującego poufność, dostępność i integralność przetwarzanych danych z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2.1. Dokumenty z zakresu bezpieczeństwa informacji

System Zarządzania Bezpieczeństwem Informacji został wdrożony w OPI-PIB Zarządzeniem Dyrektora OPI-PIB Nr 6/2015 z dnia 5 maja 2015 r. *w sprawie wprowadzenia systemu zarządzania bezpieczeństwem informacji w Ośrodku Przetwarzania Informacji – Państwowym Instytucie Badawczym*. Zarządzenie to wprowadziło do stosowania dwa dokumenty SZBI:

1) PBI wraz z powiązanymi dokumentami wewnętrznymi oraz
2) *Regulamin Użytkowników Systemów Teleinformatycznych.*

W 2015 roku SZBI został zaktualizowany[17], a następnie uzupełniony w 2016[18].

W momencie przeprowadzania kontroli, w OPI-PIB w zakresie stanowienia SZBI, obowiązywały zarządzenia Dyrektora OPI-PIB:

1. Zarządzenie nr 2/2019 z dnia 15 marca 2019 r. wprowadzające aktualizację *Polityki bezpieczeństwa danych osobowych Ośrodka Przetwarzania Informacji – Państwowego Instytutu Badawczego* (dalej: PBDO) i jednocześnie wprowadzające jej tekst jednolity;
2. Zarządzenie nr 3/2019 z dnia 18 marca 2019 r. w sprawie aktualizacji w SZBI OPI-PIB wprowadzające tekst jednolity zmienionej *Polityki bezpieczeństwa informacji OPI-PIB* oraz wprowadzające do SZBI dokument pn. *Polityka bezpieczeństwa teleinformatycznego* (dalej: PBT) w miejsce *Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.*

PBI zawiera deklarację Kierownictwa co do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych i przechowywanych w OPI-PIB oraz wsparcia dla podejmowanych działań uzasadnionych realizacją celów zabezpieczenia przetwarzanych danych. Ponadto, zdefiniowane zostały cele ustanowienia PBI oraz zasady organizacji, utrzymania i doskonalenia SZBI, w tym m.in. ogólne zasady ochrony informacji, zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania bezpieczeństwem informacji. Zapisano w niej także obowiązek

[17] Aneks nr 2 z dnia 2 listopada 2015 r. do Zarządzenia nr 6/2015 Dyrektora OPI PIB z dnia 5 maja 2015 r. *w sprawie wprowadzenia systemu zarządzania bezpieczeństwem informacji w Ośrodku Przetwarzania Informacji - Państwowym Instytucie Badawczym.*

[18] Aneks nr 3 z dnia 19 maja 2016 do Zarządzenia nr 6/2015 Dyrektora OPI PIB z dnia 5 maja 2015 r. *w sprawie wprowadzenia systemu zarządzania bezpieczeństwem informacji w Ośrodku Przetwarzania Informacji - Państwowym Instytucie Badawczym* (uzupełnienie dokumentacji systemowej).

zapoznania się z tym dokumentem przez wszystkie osoby, które mają dostęp do chronionych informacji w OPI-PIB, bez względu na pełnione funkcje i zajmowane stanowisko.

PBI określa hierarchiczną strukturę dokumentacji składającej się na SZBI:

- na poziomie jednostki organizacyjnej: PBI oraz odrębna PBDO;
- na poziomie systemów teleinformatycznych / informatycznych: PBT;
- na poziomie procedur, instrukcji i regulaminów: poszczególne procedury, instrukcje, regulaminy i inne dokumenty SZBI tworzone w celu uszczegółowienia zasad opisanych w politykach.

W OPI-PIB stosowane są mechanizmy służące zapewnieniu bezpieczeństwa informacji w stosunku do wszystkich przetwarzanych informacji. Elementem SZBI jest ustanowiony dokumentem PBDO system ochrony danych osobowych, który zapewnia przetwarzanie bezpieczeństwa danych osobowych w OPI-PIB w sposób zgodny z przepisami z zakresu ochrony danych osobowych oraz gwarantujący ich odpowiednie bezpieczeństwo.

W okresie objętym kontrolą w OPI-PIB, w zakresie przeglądu SZBI, funkcjonowała *Procedura – Przegląd zarządzania* z dnia 14 kwietnia 2017 r., opisująca sposób przygotowania i przeprowadzenia przez Kierownictwo OPI-PIB przeglądu zarządzania oraz dokumentowania wyników tego przeglądu. Z analizy okazanych do kontroli raportów z przeglądów SZBI, przeprowadzonych w latach 2017-2019, wynika, że przeglądy te były dokonywane, zgodnie z ww. procedurą, co najmniej raz w roku i obejmowały m.in. wyniki audytów, przeglądu aktualności dokumentacji SZBI, wyniki szacowania ryzyka, propozycje działań usprawniających.

Zarządzanie bezpieczeństwem informacji w OPI-PIB realizowane jest w szczególności przez zapewnienie przez Kierownictwo OPI-PIB warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji, opisanych w PBI i w dokumentach wykonawczych, zgodnie z § 20 ust. 2 pkt 1 rozporządzenia KRI. Kierownictwo OPI-PIB jest w sposób bieżący i bezpośredni zaangażowane w proces utrzymania i monitorowania SZBI, zgodnie z § 20 ust. 1 rozporządzenia KRI.

Należy zatem stwierdzić, że działania Kierownictwa OPI-PIB podejmowane w celu stworzenia warunków aktualizacji regulacji wewnętrznych dotyczących SZBI w zakresie dotyczącym zmieniającego się otoczenia, zgodnie z wymaganiem § 20 ust. 2 pkt 1 rozporządzenia KRI, były prowadzone systematycznie i wpływały na doskonalenie SZBI.

W związku z tym dokumenty z zakresu bezpieczeństwa informacji ocenia się pozytywnie.

(Dowód: akta kontroli str. 43-48, 145-325)

2.2. Dokonywanie analizy zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, które obejmują identyfikację, szacowanie, a następnie określenie sposobu postępowania z ryzykiem oraz deklarację stosowania zabezpieczeń będącą podstawą podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy. Analiza ryzyka pozwala na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń (w oparciu o plan postępowania z ryzykiem) adekwatnych do oszacowanego poziomu ryzyka.

W OPI-PIB zarządzanie ryzykiem w ramach SZBI reguluje pkt. 4.2.1. PBI oraz dokumenty wykonawcze:

1) Metodyka analizy ryzyka zasobów informacyjnych OPI-PIB dla infrastruktury informatycznej i cyberprzestrzeni z dnia 5 maja 2015 r.,
2) PBI-R3 *Procedura zarządzania ryzykiem bezpieczeństwa aktywów informacyjnych OPI-PIB* z dnia 16 maja 2018 r.

Procedura PBI-R3 przewiduje przeprowadzenie przynajmniej raz w roku analizy ryzyka w obszarze bezpieczeństwa informacji. Analiza ryzyka konieczna jest także w sytuacji zaistnienia istotnych zmian w infrastrukturze IT lub w funkcjonowaniu organizacji.

Z przedstawionej do kontroli dokumentacji wynika, że w okresie objętym kontrolą przeprowadzono w OPI-PIB jedną analizę ryzyka w wyżej wskazanym obszarze (maj 2018 r.), której wyniki zostały zawarte w dokumentach pn. *Karty ryzyka*, zakładanych oddzielnie dla każdego zagrożenia / podatności, zidentyfikowanych w ramach poszczególnej grupy informacji i aktywów informacyjnych. W *Kartach ryzyka* przedstawiono informacje o oszacowanym poziomie ryzyka oraz o sposobie postępowania ze zidentyfikowanym ryzykiem. Zbiór *Kart ryzyka* stanowił rejestr ryzyka, a tym samym rejestr ten był rozproszony.

Zastrzeżenia związane z przeprowadzoną analizą ryzyka w OPI-PIB dotyczą braku dokumentu stanowiącego podsumowanie jej wyników i plan postępowania z ryzykiem, zawierającego m.in. uszeregowanie zidentyfikowanych ryzyk pod względem ich istotności oraz określenie sposobu postępowania z ryzykiem, gdy wymagane jest podjęcie działań zapobiegawczych.

W zakresie realizacji przepisów rozporządzenia RODO[19], w toku czynności kontrolnych udostępniono wyciąg z „Rejestru czynności przetwarzania Ośrodka Przetwarzania Informacji – Państwowego Instytutu Badawczego", zawierający kategorie danych osobowych

[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych).

przetwarzanych w poszczególnych procesach przez OPI-PIB i osób, których te dane dotyczą wraz z oceną skutków dla ich ochrony, stanowiącą analizę ryzyka z punktu widzenia podmiotu (osoby), którego dane są przetwarzane. Z informacji uzyskanych w toku kontroli wynika, że kolejna analiza ryzyka zostanie przeprowadzona w 2019 r.

Należy zaznaczyć, że zarówno procedury, jak i wyniki analizy i szacowania ryzyka pozwalają na stwierdzenie, iż OPI-PIB skutecznie zarządza ryzykiem utraty integralności, dostępności i poufności informacji, oraz że podejmowane są działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy. W związku z powyższym spełnione zostały wymagania określone w § 20 ust. 2 pkt 3 rozporządzenia KRI.

Jednakże, z uwagi na brak dokumentu podsumowującego wyniki analizy ryzyka bezpieczeństwa informacji, zawierającego plan postępowania z ryzykiem, badany obszar ocenia się pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 43-48, 329-425)

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Baza inwentaryzacyjna powinna zawierać wszystkie zidentyfikowane aktywa informatyczne, przez co możliwe będzie ich odtworzenie w przypadku np.: katastrofy. Baza inwentaryzacyjna jest niezbędna przy wprowadzaniu wszelkich zmian w środowisku teleinformatycznym urzędu ograniczając możliwość zaistnienia zakłóceń w pracy, które wynikałyby z błędnych decyzji i podejmowanych działań, będących skutkiem braku aktualnej i kompleksowej wiedzy o stanie infrastruktury teleinformatycznej.

W OPI-PIB prowadzony jest rejestr środków trwałych zgodnie z ustawą z dnia 29 września 1994 r. *o rachunkowości*[20].

W OPI-PIB zarządzanie sprzętem informatycznym i oprogramowaniem w ramach SZBI zostało opisane w PBT. Dodatkowo, z dniem 25 marca 2019 r. została wdrożona procedura PBI-4 *Zarządzanie konfiguracją (Baza CMDB)*, doprecyzowująca zapisy PBT w zakresie zasad zarządzania konfiguracją systemów teleinformatycznych OPI-PIB. W szczególności procedura ta opisuje sposób zarządzania aktywami informatycznymi, zawartość merytoryczną bazy CMDB, a także sposób audytu oraz wskazuje osoby odpowiedzialne za utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania. Rejestr aktywów informatycznych w OPI-PIB prowadzony był w formie elektronicznej, wspomagany specjalizowanym oprogramowaniem. Aktualizacja rejestru aktywów informatycznych, w tym rejestru oprogramowania oraz rejestru konfiguracji sprzętowej, odbywała się na bieżąco, zgodnie z zapisami zawartymi w pkt 4.4. PBT. W bazie CMDB zinwentaryzowano topologię sieci,

[20] Dz. U. z 2016 r., poz. 1047, ze zm.

urządzenia aktywne, adresację IP, usługi sieciowe, podstawowe parametry sprzętu informatycznego (stacje robocze, serwery itp.), a także zawarto informacje o osobach, którym dany zasób informatyczny został powierzony. Z uzyskanych informacji wynika, że współczynnik amortyzacji informatycznych środków trwałych w OPI-PIB wynosi 30% w skali roku, co oznacza dużą dynamikę zmian w bazie CMDB.

Analiza przedłożonej dokumentacji świadczy o skutecznym zarządzaniu zasobami teleinformatycznymi w OPI-PIB, zgodnie z wymaganiem z § 20 ust. 2 pkt 2 rozporządzenia KRI, a zatem powyższe zagadnienie oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48, 432-493)

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

W okresie objętym kontrolą, zarządzanie uprawnieniami dostępu do aktywów (zasobów informacyjnych) w OPI-PIB zostało uregulowane w pkt 4.2.6. PBI oraz w pkt 3 i 9 PBT. Nadawanie, modyfikacja lub odebranie uprawnień użytkownikom systemów teleinformatycznych opisywała *Procedura nadawania i rejestrowania uprawnień do przetwarzania danych w systemie informatycznym* (P-5) z dnia 1 czerwca 2016 r. Dodatkowo, obowiązywały regulacje zawarte w *Procedurze upoważniania osób do przetwarzania danych osobowych* (P-4) z dnia 1 czerwca 2016 r. oraz w *Procedurze dostępu systemów teleinformatycznych w pracach projektowych wykonywanych w ramach tworzonych systemów informacyjnych* (P-6) z dnia 8 sierpnia 2018 r.

Metody uwierzytelniania oraz sposób zarządzania środkami uwierzytelniania, w tym procedury związane z ich zarządzaniem i użytkowaniem, zostały szczegółowo opisane w pkt 8 PBT. Procedury definiują sposób zarządzania uprawnieniami użytkowników, w tym także przeprowadzania okresowego przeglądu nadanych uprawnień dostępu do systemów teleinformatycznych w OPI-PIB.

Proces zarządzania uprawnieniami dostępu do zasobów informatycznych (nadawanie, zmiana, odbieranie uprawnień) realizowany był w oparciu o dedykowane formularze. Wnioski o nadanie uprawnień przechodziły ścieżkę dekretacji i podlegały archiwizacji. Dodatkowo użytkownicy systemów, w których przetwarzane są dane osobowe, otrzymywali upoważnienia do przetwarzania danych osobowych, zgodnie z *PBDO*.

W OPI-PIB był prowadzony elektroniczny rejestr uprawnień do systemów teleinformatycznych, zawierający szczegółowe informacje: imię i nazwisko użytkownika, zakres i datę ważności uprawnienia.

Pracownicy OPI-PIB uzyskiwali dostęp do zasobów informatycznych po podaniu unikalnego loginu i hasła. Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie działań zastrzeżonych dla administratorów systemów. W OPI-PIB na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 20 ust. 2 pkt 4 rozporządzenia KRI. Konta byłych pracowników w systemach informatycznych OPI-PIB w okresie objętym badaniem były sukcesywnie blokowane, zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI.

Działania w powyższym zakresie oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48, 494-597)

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Szkolenia z zakresu BI powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów związanych z BI. Szkolenia pracowników w zakresie bezpieczeństwa informacji powinny być powtarzane w regularnych odstępach czasu.

W badanym okresie kwestie związane ze szkoleniem pracowników zaangażowanych w proces przetwarzania informacji w OPI-PIB zostały uregulowane w pkt. 4.2.8. i pkt 6 PBI.

Analiza przedstawionej do kontroli dokumentacji dotyczącej szkoleń pracowników OPI-PIB wykazała, że dla wszystkich nowozatrudnionych pracowników organizowane są szkolenia w zakresie zasad bezpieczeństwa informacji. Ponadto, cyklem szkoleń utrzymujących wiedzę z zakresu bezpieczeństwa informacji i znajomości procedur SZBI, organizowanych w okresie od czerwca do października 2018 r., zostali objęci wszyscy pracownicy OPI-PIB zaangażowani w proces przetwarzania informacji w systemach teleinformatycznych.

Dodatkową formą uświadamiania pracowników o potencjalnych zagrożeniach w obszarze bezpieczeństwa teleinformatycznego (np. cyberataki, wymuszenia danych) było bieżące informowanie za pośrednictwem poczty elektronicznej o ww. zagrożeniach.

Powyższe oznacza, że wymaganie wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI zostało spełnione, a zatem kwestię szkoleń z bezpieczeństwa informacji dla pracowników OPI-PIB oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48, 598-646)

2.6. Praca na odległość i mobilne przetwarzanie danych

Wobec możliwości technicznych związanych z pracą na odległość z wykorzystaniem urządzeń mobilnych, takich jak laptopy, tablety, smartfony, pojawiają się nowe zagrożenia BI. Konieczne jest opisanie zasad określających sposoby zabezpieczenia urządzeń mobilnych i danych w nich zawartych przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także zasad korzystania z ogólnodostępnych sieci.

W kontrolowanym okresie zasady zarządzania dostępem zdalnym do systemów przetwarzających informacje oraz zasady bezpiecznego użytkowania przenośnych komputerów i przenośnych nośników danych w OPI-PIB zostały określone w pkt. 4.2.6. PBI, oraz w pkt 10, 11, 15, 20 i 21 PBT. Dodatkowo, w celu zapewnienia bezpieczeństwa w zdalnym nadzorze teleinformatycznym realizowanym przez administratorów, opracowana i wdrożona została *Procedura – Bezpieczny dostęp teleinformatyczny* z dnia 14 kwietnia 2017 r.

Sprzęt komputerowy wykorzystywany do pracy na odległość był konfigurowany przez administratora systemów informatycznych (ASIp), a jego wydanie i zwrot pracownikowi było ewidencjonowane wraz ze stosowną adnotacją w bazie CMDB.

Dostęp zdalny przydzielany był zgodnie z procedurą nadawania uprawnień do przetwarzania danych na podstawie formalnego wniosku o przyznanie praw dostępu. W OPI-PIB prowadzony był rejestr osób, którym przyznany został dostęp zdalny do sieci OPI-PIB przy wykorzystaniu VPN (*Virtual Private Network*).

Obowiązujące w OPI-PIB regulacje dotyczące BI określały podstawowe zasady bezpiecznej pracy przy mobilnym przetwarzaniu informacji oraz pracy na odległość, zgodnie z wytycznymi § 20 ust. 2 pkt 8 rozporządzenia KRI.

Powyższy obszar oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48, 647-654)

2.7. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o znaczeniu krytycznym dla podmiotu realizującego zadania publiczne niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego, systemowego, sprzętu i rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii. Umowy powinny posiadać klauzule prawne zabezpieczające BI w przypadku wejścia w ich posiadanie przez firmy serwisujące.

Zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu systemów teleinformatycznych regulowały postanowienia zawarte w pkt. 5 PBT, zaś zasady dostępu do zasobów teleinformatycznych określała *Procedura kontroli dostępu (PBI-6)* oraz PBDO.

Powyższe regulacje wymagały od podmiotu zewnętrznego podpisania zobowiązania do zachowania poufności, a w przypadku dostępu do danych osobowych, do zawarcia umowy powierzenia przetwarzania danych osobowych. Pracownicy firm zewnętrznych mogli wykonywać prace wyłącznie pod nadzorem pracowników OPI-PIB.

W konkretnych umowach z dostawcami produktów i usług zapisy dotyczące bezpieczeństwa informacji były indywidualnie negocjowane przez strony umowy i były adekwatne do charakteru usług. Udostępnione zespołowi kontrolnemu umowy serwisowe zawarte przez OPI-PIB uwzględniały postanowienia zapewniające w kontaktach z firmami zewnętrznymi odpowiedni poziom bezpieczeństwa informacji oraz wydajności i dostępności systemów zgodnie z zakresem usług oraz parametrami SLA (*Service Level Agreement*), co wypełnia wymagania § 20 ust. 2 pkt 10 rozporządzenia KRI.

Mając na uwadze powyższe, badane zagadnienie ocenia się pozytywnie.

(Dowód: akta kontroli str. 43-48, 655-933)

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Pomimo stosowania zabezpieczeń pozwalających na ograniczanie ryzyka związanego z przetwarzaniem informacji, w podmiocie realizującym zadania publiczne istnieje ryzyko szczątkowe, świadomie akceptowane przez kierownictwo. W ramach ryzyka szczątkowego, a także ryzyka nieobjętego analizą ryzyka mogą pojawić się incydenty naruszenia BI. Incydenty te powinny być bezzwłocznie zgłaszane w sposób z góry ustalony, a także powinien być opisany sposób reakcji na te incydenty przez wyznaczone osoby, skutkujący szybkim podjęciem działań korygujących.

W okresie objętym kontrolą ogólne zasady postępowania z incydentami naruszenia bezpieczeństwa informacji zostały opisane w pkt. 11 PBI oraz w *Regulaminie Użytkowników Systemów Teleinformatycznych*, zaś szczegółowy tryb postępowania w przypadku wystąpienia incydentu określał *Regulamin zarządzania incydentami* z dnia 2 listopada 2015 r., a od dnia 25 marca 2019 r. - *Procedura postępowania z incydentami i naruszeniami (PBI-7).*

Powyższe regulacje precyzyjnie określają sposób zarządzania incydentami naruszenia bezpieczeństwa informacji w ramach SZBI, w tym: przypadki wystąpienia incydentu informatycznego naruszającego BI, sposób zgłaszania oraz postępowania z incydentami, osoby odpowiedzialne za właściwe postępowanie, działania korygujące oraz przygotowanie materiałów dowodowych. Procedura zawiera wykaz potencjalnych incydentów naruszenia bezpieczeństwa informacji, wzór raportu z incydentu oraz wzór rejestru incydentów.

W toku czynności kontrolnych przedłożono wyciąg z *Rejestru naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych* i dwa „Raporty wystąpienia zdarzenia lub incydentu w zakresie bezpieczeństwa informacji/danych osobowych", zawierające

szczegółowe informacje o przyczynach, skutkach i podjętych działaniach zaradczych. W 2018 roku zgłoszono 7 zdarzeń wpływających na bezpieczeństwo informacji w OPI-PIB. Sposób obsługi ww. incydentów, związanych z bezpieczeństwem informacji w OPI-PIB, pozwala stwierdzić, że wymagania zawarte w § 20 ust. 2 pkt 13 rozporządzenia KRI zostały spełnione.

Powyższy obszar oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48, 934-961)

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Wymogiem SZBI jest regularne (nie rzadziej niż raz na rok) przeprowadzanie audytów wewnętrznych w zakresie BI w systemach informatycznych, co pozwoli na ewentualne ujawnienie słabości SZBI i jego doskonalenie.

W OPI-PIB kwestia przeprowadzania audytów z zakresu bezpieczeństwa informacji została uregulowana w PBI, która w pkt. 4.2.2. stanowi, że SZBI jest monitorowany m.in. poprzez wykonywanie audytów wewnętrznych i zewnętrznych. Za opracowanie planów audytów, wykonywanie audytów wewnętrznych SZBI i udział w prowadzonych audytach zewnętrznych odpowiada Inspektor Ochrony Danych.

W 2017 roku w OPI-PIB został przeprowadzony audyt zewnętrzny bezpieczeństwa i ochrony informacji w kontekście wymagań normy PN ISO/IEC 27001:2014-12, aktualnych wymagań Krajowych Ram Interoperacyjności i ochrony danych osobowych. Realizacja zawartych w raporcie z audytu[21] rekomendacji działań naprawczych i korygujących dla SZBI wpłynęła na podniesienie poziomu bezpieczeństwa poprzez usprawnienie procedur przetwarzania informacji w OPI-PIB.

W 2018 roku przeprowadzono 2 audyty:

- zewnętrzny w zakresie ochrony danych osobowych; w sprawozdaniu z audytu[22] wykazano wysoki stopień zgodności z obowiązującymi wymogami prawnymi w zakresie bezpieczeństwa i ochrony danych oraz wymaganiami art. 20 KRI oraz szereg obszarów doskonalenia dla prawidłowego spełnienia wymogów w obszarze bezpieczeństwa informacji, realizacja których wpłynęła na podniesienie ich bezpieczeństwa;

[21] Raport z audytu bezpieczeństwa i ochrony informacji w kontekście wymagań normy PN ISO/IEC 27001:2014-12, aktualnych wymagań Krajowych Ram Interoperacyjności i ochrony danych osobowych z dnia 30.01.2017 r., opracowany przez Volvox Consulting.

[22] Sprawozdanie ze sprawdzenia w obszarze ochrony danych osobowych w zakresie zgodności bieżącej działalności Ośrodka Przetwarzania Informacji-Państwowego Instytutu Badawczego z RODO/GDPR z dnia 14.03.2018 r., opracowane przez JDS Consulting sp. z o.o. sp. k.

- wewnętrzny dotyczący ochrony danych osobowych i bezpieczeństwa informacji w obszarze HR; raport z audytu[23] zawiera szereg rekomendacji dotyczących głównie wdrożenia w OPI-PIB przepisów rozporządzenia RODO i ochrony danych osobowych.

Zgodnie z *Planem sprawdzeń i audytów w Ośrodku Przetwarzania Informacji – Państwowym Instytucie Badawczym z zakresu ochrony danych osobowych i bezpieczeństwa informacji w roku 2019,* kontynuowany jest rozpoczęty w listopadzie 2018 r. wieloetapowy audyt zewnętrzny w zakresie bezpieczeństwa systemów teleinformatycznych i sieci informatycznej, w tym przeprowadzenie testów penetracyjnych, wskazanie podatności i słabości audytowanych systemów teleinformatycznych, sieci i środowiska informatycznego, w którym funkcjonują. Zakończenie tego audytu jest przewidziane po upływie 23 tygodni od rozpoczęcia prac. Na rok 2019 zaplanowano także inne audyty wewnętrzne, m.in. w obszarach: bezpieczeństwa fizycznego, aktualności procedur, wielu aspektów ochrony danych osobowych oraz uprawnień dostępu do systemów teleinformatycznych.

Stwierdzono, że zakres i wyniki dotychczas przeprowadzonych audytów spełniają wymagania § 20 ust. 2 pkt 14 rozporządzenia KRI, zatem działalność OPI-PIB w tym zakresie ocenia się pozytywnie.

(Dowód: akta kontroli str. 43-48, 962-1038)

2.10. Kopie zapasowe

Kopie zapasowe (bezpieczeństwa) danych powinny być właściwie tworzone, przechowywane i testowane. Celem ich tworzenia jest możliwość przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system np. w bazie danych. Wymóg ten można osiągnąć poprzez regularne wykonywanie kopii całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych, regularne odtwarzanie systemu z kopii na niezależnym środowisku sprzętowym oraz testowanie pracy użytkowej tak odtworzonego systemu.

W okresie objętym kontrolą w OPI-PIB obowiązywały regulacje zawarte w pkt 18 PBT (w zakresie wykonywania kopii zapasowych) oraz pkt 19 PBT (w zakresie przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz ich kopii zapasowych). Nie funkcjonowała odrębna procedura wykonywania i testowania kopii bezpieczeństwa, doprecyzowująca zapisy PBT.

Zespół kontrolny stwierdził, że w OPI-PIB w badanym okresie kopie bezpieczeństwa były skutecznie wykonywane i testowane. Kopie bezpieczeństwa wykonywane były w sposób

[23] Analiza obszaru ochrony danych osobowych i bezpieczeństwa informacji w Dziale Zarządzania Kapitałem Ludzkim Ośrodka Przetwarzania Informacji-Państwowego Instytutu Badawczego z dnia 23.11.2018 r.

automatyczny i według zdefiniowanego harmonogramu, przy wykorzystaniu specjalizowanego oprogramowania. Do kontroli okazano wydruk harmonogramu wykonania kopii zapasowych, zawierający nazwy serwerów i plików przeznaczonych do przeniesienia na nośniki stanowiące kopie zapasowe. Kontrola wykonania kopii była potwierdzana raportami zawierającymi informacje o prawidłowości przeprowadzenia procedury wykonywania kopii zapasowych obiektów systemowych, w tym serwerów, plików i logów. Zgodnie z przedłożonymi raportami z odtwarzania backup-u z taśm dla projektów OPI/OSF/Pol-on/LIL, w OPI-PIB przeprowadzano testy kopii zapasowych poprzez odtworzenie z kopii systemów użytkowych i baz danych oraz sprawdzenie działania funkcji użytkowych odtworzonych systemów. Utworzone kopie zapasowe były przechowywane w niezależnych lokalizacjach (innych niż serwerownie, w których znajdują się zabezpieczane systemy).

OPI-PIB dysponuje procedurą *Plan ciągłości działania w sytuacjach kryzysowych dla zasobów informatycznych OPI-PIB (PBI-R2)* z dnia 14 kwietnia 2017 r. oraz zatwierdzonymi planami awaryjnymi na wypadek wystąpienia incydentów krytycznych (tzw. *Karty PCD*). Zdefiniowano w nich różne czynniki ryzyka (zagrożenia) oraz opisano szczegółowo procedury działania w sytuacji zmaterializowania się danego ryzyka. Głównym elementem ww. planów awaryjnych, z punktu widzenia bezpieczeństwa informacji, jest dysponowanie zabezpieczeniem przed utratą ciągłości działania jakim jest Zapasowe Centrum Danych[24], umożliwiające kontynuowanie, w sytuacjach kryzysowych, działalności operacyjnej OPI-PIB w zakresie systemów o znaczeniu krytycznym. Plan Ciągłości Działania zakłada, że w przypadku wystąpienia awarii w ośrodku podstawowym, następuje przełączenie pracy systemów krytycznych na ośrodek zapasowy. Z oświadczenia Inspektora Ochrony Danych wynika, że w ośrodku zapasowym znajdują się następujące systemy teleinformatyczne oraz bazy możliwe do uruchomienia w trybie awaryjnym: ZSUN/OSF, Baza danych POL-on, Baza danych ORPPD, Bazy danych systemów Pstryk, Recenzenci, Aparatura, Inventorum, Nauka Polska, System RAD-on w zakresie MCL oraz JSA.

Jak wynika z zapisów w *Rejestrze naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych,* w kontrolowanym okresie nie było konieczności przełączenia pracy z ośrodka podstawowego do zapasowego w trybie awaryjnym. W celu uzyskania zapewnienia o skuteczności zabezpieczeń na wypadek potencjalnych incydentów powodujących niedostępność ośrodka podstawowego w OPI-PIB, przeprowadzono trzy przełączenia testowe na pracę w ośrodku zapasowym. Z przedłożonych raportów z testów wynika, że osiągnięto pozytywny wynik przeprowadzonych sprawdzeń (przełączenia były skuteczne).

Podsumowując, należy stwierdzić, że w OPI-PIB, pomimo braku odrębnej całościowej procedury wykonywania i testowania kopii bezpieczeństwa eksploatowanych systemów, kopie te były wykonywane i testowane w oparciu o procedury opisane w dokumentacji

[24] Ośrodek zapasowy jest zlokalizowany poza siedzibą OPI-PIB.

technicznej poszczególnych systemów. OPI-PIB posiadał plany awaryjne, w tym ośrodek zapasowy stanowiący główny element zabezpieczenia przed utratą ciągłości działania oraz testował skuteczność pracy z jego wykorzystaniem. Powyższe oznacza zgodność z wymaganiem § 20 ust. 2 pkt 12 lit b rozporządzenia KRI, zatem działalność OPI-PIB w tym zakresie ocenia się pozytywnie.

(Dowód: akta kontroli str. 43-48, 1039-1194)

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Bezpieczeństwo systemu teleinformatycznego w dużym stopniu zależy od jego budowy. Stąd wymagania, aby system teleinformatyczny został zaprojektowany i zbudowany zgodnie z zasadami BI opisanymi w obowiązujących normach i standardach przemysłowych.

OPI-PIB, w ramach realizacji zadań statutowych, prowadził prace związane z tworzeniem i utrzymywaniem unikatowych systemów informatycznych oraz prowadzeniem prac rozwojowych w zakresie eksploatowanych systemów informatycznych.

W okresie objętym kontrolą, projektowanie, wdrażanie i eksploatacja systemów informatycznych w OPI-PIB odbywało się m.in. na podstawie nw. regulacji wewnętrznych, określających szczegółowe wymagania techniczne, bezpieczeństwa i eksploatacyjne:

1. *Standardy zarządzania projektami i zespołem oraz projektowania, wykonywania i utrzymania systemów informatycznych w Laboratorium Inteligentnych Systemów Informatycznych OPI-PIB* – opisujące sposób zarządzania projektami informatycznymi; dokument ten wskazuje na konieczność stosowania standardowych metodyk zarządzania projektami, jak PRINCE2 czy AGILE-SCRUM oraz opisuje role, system monitoringu i kontroli, zarządzanie incydentami, ryzykiem i jakością w celu skutecznego zakończenia projektu;
2. *Projektowanie, wdrażanie i utrzymanie systemów PBN, Pol-index, ZSUN Helpdesk i JSA* – dokument opisujący procedury i narzędzia wspomagające projektowanie, wdrażanie oraz utrzymanie ww. systemów, w którym określono szczegółowe wymagania techniczne i eksploatacyjne w zakresie projektowania, wdrażania i odbioru systemów informatycznych planowanych do wdrożenia, sposoby dostarczenia i instalacji systemu informatycznego oraz wymagania sprzętowe, środowiskowe i dokumentacyjne dla systemów, sposób i zakres testów, a także warunki i kryteria odbioru;
3. P*rojektowanie systemu informatycznego* – procedura obejmująca działania związane z analizą biznesową, analizą wewnętrzną wymagań funkcjonalnych, przygotowaniem projektu przedsięwzięcia, przygotowaniem i akceptacją zamówienia oraz planowaniem;

4. *Standardy tworzenia interfejsu użytkownika w systemie ZSUN/moduł OSF* – dokument, w którym określono wymagania techniczne dla systemów informatycznych w celu zapewnienia łatwości ich obsługi, przejrzystości danych i spójnego systemu nawigacji;
5. *Procedura Testowania Systemu Informatycznego*, która określała sposób przedstawiania informacji dotyczących przygotowania, przeprowadzania i dokumentowania prac testowych dla realizowanych projektów rozwiązań informatycznych;
6. *Procedura Eksploatacji Systemu Informatycznego*, opisująca działania w celu zapewnienia stabilności w codziennych działaniach i procesach organizacyjnych oraz ciągłą poprawę usług, przy jednoczesnym redukowaniu kosztów i utrzymaniu stabilności. Ponadto, procedura opisuje sposób diagnozy i rozwiązywania problemów związanych z awariami systemów teleinformatycznych;
7. *Procedura monitorowania wydajności, integralności i podatności systemów teleinformatycznych* z dnia 25 marca 2019 r., która reguluje proces administrowania systemami eksploatowanymi w OPI-PIB, w szczególności opisuje sposób postępowania w zakresie monitorowania pojemności, wydajności i integralności systemów informatycznych dla sieci, serwerów sprzętowych, serwerów aplikacji i baz danych;
8. *Procedura - zarządzanie zmianą* z dnia 14 kwietnia 2017 r., która reguluje proces zarządzania zmianami w OPI-PIB, w szczególności opisuje sposób wprowadzania i nadzorowania zmian dokonywanych w systemach teleinformatycznych administrowanych przez OPI-PIB, w tym zasady nadzoru nad zmianą konfiguracji, funkcjonalności i kluczowych komponentów systemów informatycznych;
9. *Procedura dostępu systemów teleinformatycznych w pracach projektowych wykonywanych w ramach tworzonych systemów informacyjnych* z dnia 8 sierpnia 2018 r., określająca sposób udzielania dostępu dla systemu teleinformatycznego do innych systemów teleinformatycznych.

Z informacji uzyskanych w toku kontroli wynika, że wymagania dotyczące projektowania, wdrażania i odbioru systemów są określane w taki sposób, aby systemy były zaprojektowane i wdrożone z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności i pielęgnowalności.

W OPI-PIB realizowany był ciągły proces zarządzania i monitorowania systemów informatycznych i środowiska ich pracy pod kątem bezpieczeństwa wydajności i pojemności. W pomieszczeniu zarządzania eksploatacją IT realizowany był proces monitorowania parametrów pracy sieci, urządzeń i aplikacji, m. in.: utylizacji serwerów, obciążenia łączy zewnętrznych, urządzeń sieciowych, alertów bezpieczeństwa, graficznej prezentacji sieci LAN, w tym statusu urządzeń pracujących w sieci, itp. Proces administrowania technicznego i monitorowania określonych obszarów (systemy, aplikacje, dane, infrastruktura sieciowa, stacje robocze) był przypisany konkretnym pracownikom pionu IT. Proces monitorowania

i diagnostyki pozwalał na przewidywanie i zapobieganie ewentualnym problemom związanym z awariami, wyciekami danych, bądź ich utratą.

Powyższe pozwala stwierdzić, że OPI-PIB spełnił wymaganie § 15 ust. 1 rozporządzenia KRI, zatem badany obszar oceniono pozytywnie.

(Dowód: akta kontroli str. 43-48, 1195-1393)

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

W celu uzyskania odpowiedniego poziomu BI przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników, stosowanych jest szereg zabezpieczeń informatycznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także przed m.in. kradzieżą środków przetwarzania informacji. Zastosowane zabezpieczenia powinny być adekwatne do poziomu ryzyka wynikającego z analizy ryzyka BI.

W okresie objętym kontrolą kwestie dotyczące stosowanych w OPI-PIB zabezpieczeń dostępu do informacji zostały wieloaspektowo ujęte w PBI, PBT, PBDO oraz w procedurach wykonawczych.

Zgodnie z § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, w OPI-PIB zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami oraz ustalono zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie m.in. poprzez:

a) zabezpieczenie dostępu do informacji poprzez wymuszone logowanie użytkowników z podaniem unikalnego hasła do systemów teleinformatycznych;

b) kontrolę i monitorowanie ruchu osobowego, zabezpieczenia fizycznego dostępu do pomieszczeń;

c) podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę zgłoszeń serwisowych, analizę incydentów naruszenia BI;

d) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji poprzez stosowanie: systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, zabezpieczeń kryptograficznych, systemów antywirusowych i antyspamowych, zapór sieciowych typu *firewall*.

W OPI-PIB stosowano procedury postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, co było zgodne z § 20 ust. 2 pkt 11 rozporządzenia KRI.

Podkreślić jednak należy, że dobór zastosowanych zabezpieczeń nie wynikał z analizy ryzyka i planu postępowania z ryzykiem, w związku z czym działalność OPI-PIB w tym zakresie ocenia się pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 43-48, 368-429, 1316-1321, 1394-1395)

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosowanie zabezpieczeń techniczno-organizacyjnych dotyczących środowiska teleinformatycznego powinno wynikać z analizy ryzyka i powstałego w jej wyniku planu postępowania z ryzykiem oraz deklaracji stosowania tych zabezpieczeń.

W okresie objętym kontrolą w OPI-PIB funkcjonowały następujące regulacje wewnętrzne dotyczące zabezpieczeń techniczno-organizacyjnych systemów informatycznych:

- na pierwszym poziomie – PBI,
- na drugim poziomie – polityki, regulaminy i procedury regulujące poszczególne obszary objęte SZBI.

W OPI-PIB sporządzono listę środków techniczno-organizacyjnych[25], jakie zostały zastosowane w celu zapewnienia bezpieczeństwa zgodnie z wymaganiem rozporządzenia RODO.

Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia KRI, w OPI-PIB zapewniono odpowiedni poziom bezpieczeństwa systemów teleinformatycznych poprzez:

a) aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (poprzez wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy);

b) minimalizowanie ryzyka utraty informacji w wyniku awarii oraz ochronę przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnienie bezpieczeństwa plików systemowych (poprzez zastosowanie redundantnych rozwiązań sprzętowych, w tym: bezprzerwowego zasilania, redundantnej klimatyzacji, zastosowanie serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci);

c) zastosowanie mechanizmów kryptograficznych dla transmisji danych i poczty elektronicznej.

[25] Załącznik nr 1 do „Rejestru czynności przetwarzania danych" - Opis Środków Techniczno-Organizacyjnych.

OPI-PIB posiada trzy serwerownie, które powstały poprzez adaptowanie pomieszczeń biurowych, co jest powodem istnienia opisanych w protokole z oględzin[26] ryzyk, które należy uwzględniać w analizie ryzyka. Stan bezpieczeństwa serwerowni należy ocenić pozytywnie.

Na podstawie umowy z podmiotem zewnętrznym, OPI-PIB korzysta z Zapasowego Centrum Danych oraz Platformy Sprzętowo-Programowej wraz z niezbędną infrastrukturą techniczną (ośrodek zapasowy).

Z uwagi na fakt, że dobór zastosowanych w OPI-PIB zabezpieczeń techniczno-organizacyjnych systemów informatycznych nie wynikał z analizy ryzyka i planu postępowania z ryzykiem, obszar ten ocenia się pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 43-48, 1293-1297, 1394-1395, 1488-1491)

2.14. Rozliczalność działań w systemach informatycznych

Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby w ustalonym zakresie. Dokumentowaniu w postaci zapisów w dziennikach systemów (logi) podlegają wszelkie działania związane z przetwarzaniem informacji, a także działania administracyjne, co zapewnia rozliczalność tych operacji, tj. informację kto, kiedy i co wykonał w systemie teleinformatycznym. Informacje zawarte w logach powinny być regularnie przeglądane w celu wykrycia działań niepożądanych i powinny być przechowywane w bezpieczny sposób przez okres wskazany w odrębnych przepisach, a w przypadku ich braku przez dwa lata.

Podczas kontroli OPI-PIB udostępnił dokument pn. *Polityka przechowywania logów w OPI-PIB*, który zawiera zalecenia dotyczące przechowywania logów w podziale na dwie kategorie: logi projektowe i logi systemów zewnętrznych i określa podmiotowo systemy, z których logi powinny być gromadzone (zapisywane) ze wskazaniem okresów retencji, określonych niezgodnie z wymaganiem KRI. Dokument ten nie stanowi jednak procedury zatwierdzonej przez Kierownictwo OPI-PIB i formalnie wdrożonej do stosowania w organizacji. Ponadto, nie zawiera on koniecznych wymagań, w których zostałyby określone zasady postępowania z logami systemowymi, w tym sposób i miejsce ich gromadzenia, prawidłowo określony okres ich przechowywania, a także sposób ich systematycznego przeglądania oraz analizy w celu wykrycia działań niepożądanych.

W toku czynności kontrolnych stwierdzono, że logi systemowe, o których mowa w wyżej przywołanym dokumencie, są doraźnie przeglądane przez administratorów sieci, serwerów i baz danych. Nie są one jednak systematycznie archiwizowane i przeglądane, jak wymaga tego rozporządzenie KRI. Brak regulacji wewnętrznych dotyczących zasad postępowania

[26] Protokół z oględzin serwerowni w Ośrodku Przetwarzania Informacji – Państwowym Instytucie Badawczym przeprowadzonych przez Zespół kontrolny MNiSW w dniu 10.05.2019 r.

z logami systemowymi oraz brak ich systematycznych przeglądów oznacza jedynie częściową zgodność z wymaganiem określonym w § 21 ust. 1 i 2 rozporządzenia KRI.

Działania OPI-PIB w badanym zakresie oceniono pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 43-48, 1396-1409)

3. Zapewnienie dostępności dla osób z niepełnosprawnościami informacji zawartych na stronach internetowych OPI-PIB oceniono pozytywnie.

W eksploatowanych systemach teleinformatycznych powinny zostać zastosowane rozwiązania techniczne umożliwiające osobom z niepełnosprawnościami zapoznanie się z treścią publikowanych informacji m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu, czy też odsłuchanie wyświetlanej treści, zgodnie ze standardem WCAG 2.0[27]. Termin dostosowania systemów teleinformatycznych do prezentacji zasobów informacyjnych według powyższego standardu upłynął z dniem 30 maja 2015 r.

W OPI-PIB opracowano wewnętrzną instrukcję zawierającą wytyczne implementacji wymagań WCAG 2.0[28]. Instrukcja zawiera praktyczne wskazówki i przykładowe rozwiązania wdrożenia wymagań WCAG 2.0 w systemach tworzonych w OPI-PIB.

Analiza sposobu prezentacji treści na stronach internetowych w systemach OPI-PIB wskazała, że strony zostały dostosowane do odbioru ich treści przez osoby z niepełnosprawnościami (w zakresie możliwym do uzyskania), co oznacza spełnienie wymagań określonych w § 19 rozporządzenia KRI.

(Dowód: akta kontroli str. 1410-1487)

ZALECENIA POKONTROLNE

Biorąc pod uwagę ustalenia, uwagi i oceny zawarte w niniejszym *Wystąpieniu pokontrolnym*, działając na podstawie art. 46 ust. 3 pkt 1 *ustawy o kontroli w administracji rządowej*, zalecam:

1. Opracowywanie każdorazowo po przeprowadzeniu analizy ryzyka bezpieczeństwa informacji dokumentu podsumowującego jej wyniki i zawierającego plan postępowania z ryzykiem.
2. Uwzględnianie wyników analizy ryzyka przy podejmowaniu decyzji o doborze zabezpieczeń dostępu do informacji oraz zabezpieczeń techniczno-organizacyjnych

[27] System wymagań *Web Content Accessibillity Guidelines* 2.0.
[28] Praktyczne wskazówki zgodności ze standardami WCAG 2.O (Web Content Accessibility Guidelines) - instrukcja dla pracowników LSB OPI-PIB.

systemów teleinformatycznych OPI-PIB, używanych do realizacji zadań publicznych.

3. Opracowanie i wdrożenie regulacji wewnętrznych dotyczących zasad postępowania z logami systemowymi.
4. Dokonywanie systematycznych przeglądów logów systemowych oraz dokumentowanie tych czynności.

Na podstawie art. 49 w związku z art. 46 ust. 3 pkt 3 *ustawy o kontroli w administracji rządowej*, proszę o poinformowanie Ministra o sposobie wykonania powyższych zaleceń pokontrolnych, a także o podjętych działaniach w celu usunięcia stwierdzonych uchybień lub przyczynach ich niepodjęcia, w terminie 30 dni licząc od daty otrzymania niniejszego dokumentu. Proszę również o sukcesywne przekazywanie informacji oraz dokumentacji potwierdzającej zrealizowanie zaleceń pokontrolnych aż do całkowitego usunięcia stwierdzonych uchybień. Informuję, że realizacja wskazanych zaleceń może być przedmiotem ponownej kontroli.

Jednocześnie informuję, że zgodnie z art. 48 *ustawy o kontroli w administracji rządowej,* od *Wystąpienia pokontrolnego* nie przysługują środki odwoławcze.

z up. Ministra
PODSEKRETARZ STANU
dr hab. Sebastian SKUZA
Minister Nauki i Szkolnictwa Wyższego