MINISTER
NAUKI I SZKOLNICTWA WYŻSZEGO

BKA.WK.1942.2.2018.BŁ

Warszawa, dnia 18 grudnia 2018 r.

Pan
prof. dr hab. inż. Maciej Chorowski
Dyrektor Narodowego Centrum
Badań i Rozwoju

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. 34 ustawy z dnia 30 kwietnia 2010 r. *o Narodowym Centrum Badań i Rozwoju*[3], Minister Nauki i Szkolnictwa Wyższego (dalej: Minister) przeprowadził kontrolę w Narodowym Centrum Badań i Rozwoju[4] (dalej: NCBR, Centrum) 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*, przekazuję Panu Dyrektorowi *Wystąpienie pokontrolne*, zawierające ustalenia i ocenę skontrolowanej działalności wraz z zaleceniami pokontrolnymi.

Kontrola została przeprowadzona[5] w trybie zwykłym, określonym *ustawą o kontroli w administracji rządowej* i obejmowała okres od dnia 1 stycznia 2017 r. do dnia 30 czerwca

[1] Dz. U. Nr 185, poz. 1092, dalej: *ustawa o kontroli w administracji rządowej.*
[2] Dz. U. z 2017 r., poz. 570, z późn. zm., dalej: *ustawa o informatyzacji.*
[3] t. j. Dz. U. z 2018 r., poz. 1249, dalej: *ustawa o NCBR.*
[4] Narodowe Centrum Badań i Rozwoju, ul. Nowogrodzka 47a, 00-695 Warszawa.
[5] Czynności kontrolne w NCBR prowadzone były w dniach 23 - 24 października 2018 r. przez zespół kontrolny w składzie: Barbara Łukasik – główny specjalista w Biurze Kontroli i Audytu MNiSW - upoważnienie nr 1/2/KN/2018/BKA; Łukasz Abramowicz – główny specjalista w Biurze Kontroli i Audytu MNiSW - upoważnienie nr 2/2/KN/2018/BKA; Bogdan Kowalczyk – biegły powołany w skład zespołu kontrolnego na podstawie art. 33 *ustawy o kontroli w administracji rządowej* - upoważnienie nr 3/2/KN/2018/BKA.

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

2018 r., z możliwością zasięgania informacji z okresów wcześniejszych, jeżeli miały wpływ na kontrolowane zagadnienia.

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.

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.

Zespół kontrolny poddał analizie funkcjonujący w Centrum System Zarządzania Bezpieczeństwem Informacji (SZBI) oraz 3 z 9 systemów teleinformatycznych eksploatowanych w NCBR, tj.:

1. Lokalny System Informatyczny (LSI) – obsługa naboru wniosków o dofinansowanie oraz procesu oceny wniosków, obsługi protestów i generowania umów;
2. OSF/ZSUN – obsługa naboru wniosków o dofinansowanie oraz procesu oceny wniosków i generowania umów w Programach Strategicznych, Obronnych oraz innych, finansowanych ze źródeł krajowych;
3. Strona internetowa NCBR – www.ncbr.gov.pl.

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

(Dowód: akta kontroli str. 42-52)

OCENA OGÓLNA

Biorąc pod uwagę kryterium legalności, celowości i rzetelności, zespół kontrolny sformułował ocenę[6] niżej wymienionych obszarów:

[6] Na potrzeby niniejszej kontroli, w MNiSW przyjęto 4-stopniową skalę ocen:
- ocena pozytywna,
- ocena pozytywna z uchybieniami,
- ocena pozytywna z nieprawidłowościami,
- ocena negatywna.

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

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

SZCZEGÓŁOWE USTALENIA KONTROLI

Słownik

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;
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;
RI — Repozytorium Interoperacyjności — część zasobów ePUAP przeznaczona do udostępniania informacji służących osiąganiu interoperacyjności;
rozporządzenie ePUAP — rozporządzenie Ministra Administracji i Cyfryzacji z dnia 5 października 2016 r. *w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej*[7];
rozporządzenie KRI — rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów*

[7] Dz. U. z 2016 r., poz. 1626.

publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[8]*;*

dostępność — właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;

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*[9], 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

Narodowe Centrum Badań i Rozwoju jest agencją wykonawczą w rozumieniu ustawy z dnia 27 sierpnia 2009 r. *o finansach publicznych*[10], powołaną do realizacji zadań z zakresu polityki naukowej, naukowo-technicznej i innowacyjnej państwa.

W kontrolowanym okresie dyrektorem NCBR był prof. dr hab. inż. Maciej Chorowski, który pełni tę funkcję od dnia 13 kwietnia 2016 r.

Do zadań Centrum należy zarządzanie strategicznymi programami badań naukowych i prac rozwojowych (w tym na rzecz obronności i bezpieczeństwa państwa), finansowanie lub współfinansowanie tych programów, a także pobudzanie inwestowania przez przedsiębiorców w działalność badawczo-rozwojową, w szczególności poprzez współfinansowanie

[8] Dz. U. z 2016 r., poz. 113, z późn. zm.
[9] Dz. U. z 2017 r., poz. 1219.
[10] Dz. U. z 2018 r., poz. 62, z późn. zm.

przedsięwzięć prowadzonych przez podmiot posiadający zdolność do zastosowania wyników projektu w praktyce oraz wspieranie pozyskiwania przez jednostki naukowe środków na działalność badawczo-rozwojową pochodzących z innych źródeł niż budżet państwa.

Siedziba Narodowego Centrum Badań i Rozwoju mieści się w budynku przy ul. Nowogrodzkiej 47a w Warszawie, kod pocztowy 00-695. NCBR jest najemcą pomieszczeń zlokalizowanych na piętrach 1 – 7 w budynku, którego administratorem i operatorem jest Roma Office Center Sp. z o.o. Budynek jest objęty całodobową ochroną fizyczną, którą zapewnia administrator obiektu. Newralgiczne przestrzenie, tj. wejścia z klatki schodowej do pomieszczeń biurowych monitorowane są systemem telewizji przemysłowej nadzorowanej przez administratora budynku. Wejścia do przestrzeni biurowej NCBR są zabezpieczone elektronicznym systemem kontroli dostępu z zastosowaniem czytników kart zbliżeniowych przy drzwiach wejściowych oraz w strefach podwyższonej ochrony. Elektroniczny system kontroli dostępu administrowany jest przez administratora obiektu. NCBR dysponuje dwoma serwerowniami, ulokowanymi w pomieszczeniach technicznych, w obrębie przestrzeni biurowych zajmowanych przez NCBR. Zespół kontrolny uzyskał informacje, że NCBR prowadzi prace związane z adaptacją jednego z pomieszczeń w obrębie przestrzeni biurowej zajmowanej przez NCBR z przeznaczeniem na nową serwerownię.

(Dowód: akta kontroli str. 53-57)

Za realizację zadań wynikających z § 20 rozporządzenia KRI w kontrolowanym okresie odpowiedzialny był Dyrektor NCBR, do obowiązków którego należał (zgodnie z *ustawą o informatyzacji*) m.in.: nadzór nad sprawami z zakresu administrowania bezpieczeństwem informacji. W NCBR za bezpieczeństwo informacji odpowiadali:

- Pełnomocnik Dyrektora NCBR ds. Zarządzania Bezpieczeństwem Informacji – Dyrektor Działu Administracyjno-Gospodarczego, który pełnił tę funkcję w okresie od dnia 13 maja 2016 r. do dnia 23 sierpnia 2018 r., oraz – Kierownik Sekcji Infrastruktury Teleinformatycznej w Dziale Systemów Informatycznych, który pełni tę funkcję od dnia 23 sierpnia 2018 r.,
- Administrator Bezpieczeństwa Informacji (ABI) – Kierownik Sekcji Informacji Niejawnych i Danych Osobowych w Biurze Dyrektora Centrum,
- Administrator Bezpieczeństwa Systemów Informatycznych (ABSI) – – Kierownik Sekcji Infrastruktury Teleinformatycznej w Dziale Systemów Informatycznych.

Role, obowiązki i zakresy odpowiedzialności Dyrektora NCBR oraz ww. osób w procesie ochrony zasobów informacyjnych zostały określone w Polityce Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju z dnia 21 marca 2016 r.

Zgodnie z obowiązującym Regulaminem Organizacyjnym NCBR[11], obsługę informatyczną procesów wewnętrznych NCBR zapewnia Dział Systemów Informatycznych (DSI), kierowany przez Pod opieką DSI znajdują się m.in.: systemy informatyczne Centrum (w tym Lokalny System Informatyczny, aplikacje biurowe, poczta elektroniczna, system Elektronicznego Zarządzania Dokumentacją EZD), usługi katalogowe, środowiska sprzętowo-programowe pracy aplikacji NCBR, sieć lokalna, stacje robocze i drukarki. Za administrowanie i rozwój strony internetowej oraz serwisu BIP NCBR odpowiada Dział Komunikacji i Promocji.

Realizację zadań statutowych NCBR wspomagają dwa systemy dedykowane do obsługi naboru wniosków o finansowanie oraz procesu oceny wniosków w zakresie badań finansowanych przez NCBR, tj.: system LSI oraz system OSF/ZSUN, którego utrzymanie zapewnia Ośrodek Przetwarzania Informacji - Państwowy Instytut Badawczy (OPI-PIB)[12].

(Dowód: akta kontroli str. 42-52, 58-64, 65-351)

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

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. Usługi elektroniczne

Celem stosowania usług elektronicznych jest ułatwienie dostępu do usług poprzez wyeliminowanie korespondencji papierowej obywatela/podmiotu z jednostką, zastąpienie

---

[11] Zarządzenie Nr 2/2016 Dyrektora NCBR z dnia 14 stycznia 2016 r. zmieniające Zarządzenie Nr 23/2015 *w sprawie ustanowienia Regulaminu organizacyjnego Biura Narodowego Centrum Badań i Rozwoju*; Zarządzenie Nr 39/2016 Dyrektora NCBR z dnia 22 lipca 2016 r. *w sprawie ustanowienia Regulaminu organizacyjnego Biura Narodowego Centrum Badań i Rozwoju*, zmienione Zarządzeniem Nr 24/2017 Dyrektora NCBR z dnia 7 marca 2017 r., Zarządzeniem Nr 40/2017 Dyrektora NCBR z dnia 20 kwietnia 2017 r., Zarządzeniem Nr 47/2017 Dyrektora NCBR z dnia 23 maja 2017 r. oraz Zarządzeniem Nr 72/2017 Dyrektora NCBR z dnia 19 lipca 2017 r.; Zarządzenie Nr 82/2017 Dyrektora NCBR z dnia 31 sierpnia 2017 r. *w sprawie ustanowienia Regulaminu organizacyjnego Biura Narodowego Centrum Badań i Rozwoju*, zmienione Zarządzeniem Nr 124/2017 Dyrektora NCBR z dnia 7 grudnia 2017 r. oraz Zarządzeniem Nr 43/2018 Dyrektora NCBR z dnia 8 maja 2018 r.

[12] OPI-PIB jest jednostką nadzorowaną przez MNiSW.

druków i formularzy papierowych ich odpowiednikami elektronicznymi, dostępnymi do wypełnienia na platformie usług elektronicznych, a także wyeliminowanie papierowych dokumentów kierowanych do obywatela/podmiotu i zastąpienie ich odpowiednikami elektronicznymi, przesyłanymi drogą elektroniczną, np. na skrytkę na platformie ePUAP.

Zgodnie z art. 16 ust. 1 oraz ust. 1a *ustawy o informatyzacji*, NCBR udostępniało Elektroniczną Skrzynkę Podawczą (ESP) na platformie ePUAP pod adresem /NCBR/SkrytkaESP, która pozwalała na przesyłanie drogą elektroniczną korespondencji skierowanej do jednostki, w tym pism ogólnych, skarg, wniosków, zapytań itp. Na stronie podmiotowej BIP NCBR znajdują się niezbędne informacje o możliwości korzystania z ESP na platformie ePUAP, w tym instrukcje i wymagania dla dokumentów elektronicznych dostarczanych do NCBR. Korespondencja wpływająca za pośrednictwem ESP wprowadzana jest do systemu Elektronicznego Zarządzania Dokumentacją (EZD). Pracownik kancelarii ogólnej kieruje korespondencję do właściwych dyrektorów/kierowników jednostek organizacyjnych, następnie korespondencja jest dekretowana.

Ze względu na specyfikę działalności statutowej, NCBR nie opracowało i nie świadczyło usług drogą elektroniczną, w związku z czym nie posiadało udokumentowanych procedur określających deklarowany poziom dostępności tych usług. Niemniej jednak Centrum realizowało pewną formę elektronicznej komunikacji z interesariuszami poprzez udostępnianie możliwości dostarczania do NCBR dokumentów w postaci elektronicznej przy użyciu systemu OSF (w zakresie obsługi formalnej wniosków o finansowanie badań podstawowych).

Zespół kontrolny stwierdził, że NCBR nie dostarcza interaktywnych usług elektronicznych na poziomie wyższym od pierwszego[13] (poziom informacyjny[14]). Stwierdził również, że NCBR nie przeprowadziło inwentaryzacji i analizy tych usług, która skutkowałaby decyzją o podniesieniu ich na wyższy poziom dojrzałości.

(Dowód: akta kontroli str. 44-52)

---

[13] Portal NCBR: https://www.ncbr.gov.pl.

[14] Poziom pierwszy – informacyjny: instytucje publikują informacje w Internecie, a odbiorcy (obywatele, klienci, użytkownicy) mogą się z nimi zapoznać.
Poziom drugi – interakcyjny: odbiorcy przekazują informacje instytucji drogą elektroniczną, ale nie we wszystkich przypadkach instytucja im odpowiada tą samą drogą (komunikacja jest jednostronna).
Poziom trzeci – transakcyjny: odbiorca komunikuje się z instytucjami drogą elektroniczną, a one odpowiadają mu tą samą drogą (komunikacja jest dwustronna).
Poziom czwarty – integracyjny: odbiorcy wykorzystują specjalne portale, w których udostępniane są informacje pochodzące z różnych instytucji. Jest to możliwe dzięki zintegrowaniu danych z różnych źródeł. Połączenie danych umożliwia przejście przez cały proces załatwiania danej sprawy zdalnie i elektronicznie. Dzięki internetowemu portalowi odbiorca uzyskuje informacje, uzupełnia dane w formularzach, przesyła je, wnosi opłaty i uzyskuje decyzje (zaświadczenia, zezwolenia itp.) od instytucji.
Poziom piąty – personalizacyjny: odbiorcy oferowane są usługi dostosowane do ich indywidualnych potrzeb i sytuacji. Dzięki wdrożeniu odpowiednich algorytmów przetwarzania danych usługi są zautomatyzowane i świadczone proaktywnie (czyli to instytucja wychodzi do odbiorcy z inicjatywą świadczenia usług).

1.2. Centralne repozytorium wzorów dokumentów elektronicznych

Na podstawie art. 19b ust. 1 *ustawy o informatyzacji*, w CRWDE przechowywane są wzory dokumentów elektronicznych, opracowanych i używanych do realizacji usług świadczonych drogą elektroniczną przez urzędy i jednostki realizujące zadania publiczne. W przypadku uruchamiania usługi elektronicznej, która już funkcjonuje w innym urzędzie, należy skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych znajdujące się w CRWDE. W przypadku uruchamiania usługi, dla której nie ma opublikowanych wcześniej wzorów dokumentów w CRWDE, należy opracować i przekazać do CRWDE wzory dokumentów elektronicznych związanych z nową usługą.

Zespół kontrolny stwierdził, że NCBR dopuszcza korzystanie z opublikowanych w CRWDE wzorów dokumentów elektronicznych w kontaktach z interesariuszami za pośrednictwem ESP na platformie ePUAP i w EZD, traktując je jako pisma ogólne, lecz nie korzystało z nich, ani nie tworzyło własnych wzorów.

(Dowód: akta kontroli str. 44-52)

1.3. Model usługowy

Rozporządzenie KRI w § 2 pkt 8 określa model usługowy jako model architektury, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji, inaczej: system zorientowany na usługi. Zarządzanie usługami elektronicznymi w oparciu o model usługowy wymaga posiadania i stosowania wewnętrznych procedur obsługi danych usług oraz dostarczania ich na zadeklarowanym poziomie, zgodnie z wymaganiami § 15 ust. 2 rozporządzenia KRI.

W badanym okresie NCBR nie realizowało interaktywnych usług elektronicznych na poziomie wyższym od pierwszego[15] (poziom informacyjny), a dla kontaktów z interesariuszami poprzez system OSF realizowało nieformalne procedury pozwalające na identyfikację właściciela merytorycznego, ustalenie odpowiedzialności za realizację, zadeklarowanych terminów realizacji oraz monitoring dotrzymywania tych terminów. Ponieważ NCBR nie świadczy interaktywnych usług elektronicznych na poziomie wyższym od pierwszego (poziom informacyjny), o czym mowa w pkt 1.1 niniejszego wystąpienia pokontrolnego, spełnienie wymagania § 15 ust. 2 rozporządzenia KRI nie dotyczy NCBR.

(Dowód: akta kontroli str. 44-52)

[15] https://www.ncbr.gov.pl/

1.4. Współpraca badanych systemów informatycznych z innymi systemami

Ułatwieniem w załatwieniu spraw dla obywatela/podmiotu jest odwoływanie się systemu informatycznego bezpośrednio do danych o obywatelu/podmiocie (PESEL, REGON, NIP, dane adresowe) gromadzonych w innych systemach/rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

W NCBR niektóre systemy informatyczne przekazują sobie wzajemnie informacje np. zasilanie systemu LSI danymi o ekspertach z systemu eCentrum, pobieranie danych z REGON do systemu eCentrum, wymiana danych pomiędzy systemem LSI a systemem centralnym SL2014, pobieranie danych z systemu Sowa do LSI, wymiana danych pomiędzy Hurtownią Danych NCBR a systemem POL-on, pobieranie danych z systemu OSF do Hurtowni Danych NCBR. Ponadto, użytkowany w NCBR system EZD komunikuje się w standardowy sposób z platformą ePUAP.

Interfejsy programowe pomiędzy systemami w NCBR powinny posiadać stosowną dokumentację opisującą sposób ich funkcjonowania, w tym zastosowane mechanizmy bezpieczeństwa. NCBR nie posiada regulacji wewnętrznych, które zawierałyby wymagania co do sposobu ich budowy i niezbędnych mechanizmów bezpieczeństwa, a także konieczności ich pełnego dokumentowania. W związku z powyższym w NCBR nie w pełni realizowane są wymagania określone w § 16 ust. 1 oraz § 5 ust. 3 pkt 3 rozporządzenia KRI, zatem ocenia się ten obszar pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 42-43,44-52)

1.5. Obieg dokumentów

Stosowanie systemu elektronicznego zarządzania obiegiem dokumentów wpływa na porządkowanie i usprawnianie ich obiegu w jednostce, znacząco ułatwia i przyspiesza prowadzenie archiwizacji oraz zapewnia bezpośredni dostęp do dokumentów archiwalnych, co w konsekwencji przyspiesza proces załatwiania spraw i minimalizuje nakład pracy.

W okresie od dnia 15 listopada 2017 r. do dnia 30 marca 2018 r., w miejsce dotychczas stosowanego w NCBR systemu SWP/intraDok do obsługi czynności kancelaryjnych i zarządzania obiegiem dokumentacji, trwało wdrażanie elektronicznego systemu zarządzania dokumentacją – EZD, a od dnia 1 kwietnia 2018 r. system ten ustanowiono jako podstawowy sposób dokumentowania przebiegu załatwiania spraw oraz dokonywania czynności kancelaryjnych w NCBR. W związku z tym, z dniem 1 kwietnia 2018 r. [16] wprowadzono

[16] Zarządzenie Nr 32/2018 Dyrektora Narodowego Centrum Badań i Rozwoju z dnia 28 marca 2018 r. *zmieniające zarządzenie w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt, instrukcji w sprawie organizacji i zakresu archiwum zakładowego Narodowego Centrum Badań i Rozwoju.*

do stosowania zmienioną instrukcję kancelaryjną, jednolity rzeczowy wykaz akt oraz instrukcję w sprawie organizacji i zakresu działania archiwum zakładowego NCBR.

Zakres i sposób stosowania elektronicznego systemu zarządzania obiegiem dokumentów zostały kompleksowo określone w Zarządzeniu Nr 34/2018 Dyrektora Narodowego Centrum Badań i Rozwoju z dnia 30 marca 2018 r. *w sprawie stosowania teleinformatycznego systemu Elektronicznego Zarządzania Dokumentacją (EZD) w Narodowym Centrum Badań i Rozwoju.* Regulacja ta wspiera zapewnianie właściwego poziomu bezpieczeństwa informacji, co oznacza spełnienie wymagania § 20 ust. 2 pkt 9 rozporządzenia KRI.

Funkcjonowanie tego obszaru oceniono pozytywnie.

(Dowód: akta kontroli str. 352-540)

1.6. 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 NCBR 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 NCBR 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. 44-52)

Podsumowanie ustaleń:

1. W badanym okresie NCBR nie świadczyło usług elektronicznych na poziomie wyższym od pierwszego (poziom informacyjny). Elektroniczna skrzynka podawcza NCBR na platformie ePUAP wykorzystywana była wyłącznie do przesyłania pism ogólnych. Nie przeprowadzono inwentaryzacji i analizy usług NCBR, która skutkowałaby decyzją o ich podniesieniu na wyższy poziom dojrzałości.
2. NCBR nie tworzyło i nie przekazywało wzorów dokumentów elektronicznych do CRWDE, jak również nie udostępniało tych wzorów na stronie podmiotowej BIP NCBR, gdyż nie realizowało usług elektronicznych w oparciu o dokumenty elektroniczne.
3. Wobec braku interaktywnych usług elektronicznych na poziomie wyższym niż pierwszy (poziom informacyjny), spełnienie wymagania § 15 ust. 2 rozporządzenia KRI nie było możliwe.
4. Pomimo eksploatowania wielu interfejsów programowych, NCBR nie posiada regulacji wewnętrznych, które zawierałyby wymagania co do sposobu ich budowy

i niezbędnych mechanizmów bezpieczeństwa, a także konieczności ich pełnego dokumentowania. W związku z powyższym, w NCBR nie w pełni realizowane są wymagania określone w § 16 ust. 1 oraz § 5 ust. 3 pkt 3 rozporządzenia KRI.

5. W NCBR funkcjonuje system EZD, a regulacje wewnętrzne kompleksowo opisują zakres i sposób stosowania elektronicznego obiegu dokumentów i ich archiwizacji, zapewniając właściwy poziom bezpieczeństwa informacji w nim przetwarzanych, zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI.
6. Dla kontrolowanych systemów kodowanie znaków w wysyłanych z nich dokumentach odbywa się według standardu Unicode UTF-8, zgodnie z § 17 ust. 1 rozporządzenia KRI, a ich udostępnianie odbywa się w formatach danych określonych w załączniku nr 2 do rozporządzenia KRI, zgodnie z § 18 ust. 1 rozporządzenia KRI.

Zdaniem zespołu kontrolnego, obszar dotyczący wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną w NCBR, należy ocenić **pozytywnie z uchybieniami.**

2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

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

Dokumentacja SZBI w NCBR została przyjęta w 2016 roku, tj. po 4 latach funkcjonowania Rozporządzenia KRI. Wprawdzie przed ustanowieniem SZBI, w NCBR obowiązywało Zarządzenie Nr 14/2015 Dyrektora Narodowego Centrum Badań i Rozwoju z dnia 22 kwietnia 2015 r. *w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Narodowym Centrum Badań i Rozwoju*, jednakże dokumenty te nie regulowały całościowo wszystkich obszarów bezpieczeństwa informacji, wymaganych Rozporządzeniem KRI.

W okresie objętym kontrolą, w NCBR obowiązywało Zarządzenie Nr 20/2016 Dyrektora NCBR z dnia 6 maja 2016 r. *w sprawie przyjęcia Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju*, które ustanowiło SZBI oraz wprowadziło do stosowania Politykę Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju (PBI) z dnia 21 marca 2016 r. Zawiera ona deklarację

kierownictwa co do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych i przechowywanych w Centrum oraz wsparcia działań podnoszących poziom ich bezpieczeństwa. Ponadto, zdefiniowane zostały cele PBI oraz wskazano na potrzebę aktualizacji oraz zakomunikowania PBI wszystkim osobom, które mają dostęp do informacji w NCBR. PBI opisuje sposób organizacji SZBI w NCBR, ogólne zasady ochrony informacji, zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania ich bezpieczeństwem.

PBI wprowadza hierarchiczną strukturę dokumentacji składającej się na SZBI:

- na pierwszym poziomie – Polityka Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju jako dokument nadrzędny,
- na drugim poziomie – Polityki grupy informacji (Polityka Bezpieczeństwa Danych Osobowych Narodowego Centrum Badań i Rozwoju),
- na trzecim poziomie – Polityki systemu informatycznego (Polityka Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju – dokument opatrzony klauzulą „zastrzeżone").

Ponadto, dokumentację SZBI w NCBR stanowią:

1. Regulamin Użytkownika Systemu Informatycznego Narodowego Centrum Badań i Rozwoju,
2. Regulamin Ochrony Informacji dla Wykonawcy Narodowego Centrum Badań i Rozwoju,
3. PZ1-1 *Procedura Identyfikacja i klasyfikacja aktywów oraz zasobów informacyjnych*,
4. PZ1-2 *Procedura audytu i przeglądu SZBI*,
5. PZ1-3 *Procedura kontroli dostępu*,
6. PZ1-4 *Procedura niszczenia nośników*,
7. PZ1-5 *Procedura pomiaru i monitorowania zabezpieczeń*,
8. PZ1-6 *Procedura kontroli dostępu do budynków i pomieszczeń*,
9. PZ1-7 *Procedura zachowania ciągłości działania SI*,
10. PZ1-8 *Procedura zarządzania incydentami naruszenia bezpieczeństwa informacji*,
11. PZ1-9 *Procedura zarządzania zmianami oraz konfiguracją*,
12. PZ1-10 *Procedura zarządzania oprogramowaniem*,
13. PZ1-11 *Procedura wykonywania kopii zapasowych w systemie informatycznym*.

Należy zwrócić uwagę, że procedury wymienione w punktach 3 - 13 zostały opatrzone klauzulą „zastrzeżone", ponieważ, jak wynika z treści przywołanego zarządzenia, „zawierają informacje niejawne o klauzuli „zastrzeżone" w rozumieniu art. 5 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., Nr 182,

poz.1228 ze zm.)". Są one przechowywane w kancelarii tajnej NCBR, a dostęp do nich, zgodnie z pismem Pełnomocnika ds. SZBI z dnia 1 sierpnia 2016 r., posiadało jedynie 5 pracowników (w tym Dyrektor DSI, dwóch Kierowników Sekcji, Główny Informatyk i Główny Specjalista). Taki zakres ochrony dokumentacji SZBI spowodował to, że procedury nie były znane pracownikom wykonującym zadania w nich opisane. Tym samym niemożliwe było spełnienie np. wymogu zapisanego w dokumencie PZ1-8 *Procedura zarządzania incydentami naruszenia bezpieczeństwa informacji*, że „wszyscy pracownicy Sekcji Teleinformatyki oraz Sekcji ds. Rozwoju Narzędzi Informatycznych powinni znać treść niniejszej procedury i postępować zgodnie z jej zaleceniami". Zgodnie z obowiązującą praktyką możliwe i wskazane do opatrzenia klauzulą „zastrzeżone" są jedynie dane zawierające informacje wrażliwe ze względów bezpieczeństwa systemu informatycznego.

W NCBR stosowane są mechanizmy służące zapewnieniu bezpieczeństwa informacji w stosunku do wszystkich przetwarzanych w Centrum informacji. Dodatkowo zapewnienie bezpieczeństwa danych osobowych zostało szczegółowo opisane w Polityce Bezpieczeństwa Danych Osobowych NCBR.

Zespół kontrolny stwierdził również, że zarządzanie bezpieczeństwem informacji w NCBR realizowane jest w szczególności poprzez zapewnienie przez kierownictwo Centrum warunków umożliwiających realizację i egzekwowanie działań związanych z BI, opisanych w PBI i w dokumentach wykonawczych, zgodnie z § 20 ust. 2 pkt 1 rozporządzenia KRI. Kierownictwo NCBR jest w sposób bieżący i bezpośredni zaangażowane w proces utrzymania i monitorowania SZBI, zgodnie z § 20 ust. 1 rozporządzenia KRI.

Dyrektor NCBR powołał w 2017 r. Zespół ds. inicjowania oraz walidacji działań podejmowanych na rzecz Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju[17], do zadań którego należy koordynacja SZBI oraz zapewnienie jego prawidłowego funkcjonowania, w szczególności m.in. sprawowanie nadzoru nad opracowaniem, aktualizacją, archiwizacją dokumentacji SZBI w sposób zapewniający jej integralność (spójność) oraz bezpieczeństwo przetwarzanych i przechowywanych dokumentów. Jednakże, w zarządzeniu ustanawiającym Zespół nie określono terminu realizacji przez niego poszczególnych zadań, co oznacza brak mechanizmów kontrolnych pozwalających na rozliczanie efektów pracy i zapewnienie skuteczności realizowanych działań Zespołu. Udostępnione zespołowi kontrolnemu harmonogramy prac Zespołu z kolejnych lat wskazują na coroczne przesuwanie terminów działań zaplanowanych na dany rok, niewykonanych zgodnie z harmonogramem. Zdaniem zespołu kontrolnego stanowi to konsekwencję braku opisanych wyżej mechanizmów kontrolnych.

---

[17] Zarządzenie Nr 125/2017 Dyrektora Narodowego Centrum Badań i Rozwoju z dnia 12.12.2017 r. *w sprawie ustanowienia Zespołu ds. inicjowania oraz walidacji działań podejmowanych na rzecz Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju.*

W NCBR obowiązuje dokument PZ3-4 *Procedura*: *Nadzór nad dokumentacją opisującą procesy* z dnia 21 marca 2016 r., który reguluje sposób opracowywania, ustanawiania i utrzymywania dokumentacji procesowej, w tym dokumentacji SZBI. Procedura opisuje warunki, sposób oraz osoby odpowiedzialne m.in. za aktualizację dokumentacji, w tym dotyczącej SZBI.

Niemniej jednak, pomimo powołania w NCBR Zespołu ds. inicjowania oraz walidacji działań podejmowanych na rzecz SZBI, jak i posiadania procedury PZ3-4, obowiązująca dokumentacja SZBI jest w znacznym stopniu nieaktualna, a działania związane z jej aktualizacją należy uznać za niewystarczające. Procedury zapewniające bezpieczeństwo informacji nie uwzględniają kolejnych zmian organizacyjnych NCBR, przez co figurują w nich nieaktualne już zapisy dotyczące nieistniejących już komórek organizacyjnych NCBR. Przykładowo, w strukturze Działu Systemów Informatycznych (DSI) do dnia 10 grudnia 2017 r. funkcjonowała Sekcja Teleinformatyki i Sekcja ds. Rozwoju Narzędzi Informatycznych, zaś od dnia 11 grudnia 2017 r. do dnia zakończenia czynności kontrolnych, w skład DSI wchodziły: Sekcja Wsparcia Narzędzi Informatycznych, Sekcja Rozwoju Oprogramowania i Sekcja Infrastruktury Teleinformatycznej. Zatem należy stwierdzić, że działania kierownictwa podejmowane w celu stworzenia warunków dla aktualizacji regulacji wewnętrznych dotyczących SZBI w zakresie dotyczącym zmieniającego się otoczenia, zgodnie z wymaganiem § 20 ust. 2 pkt 1 rozporządzenia KRI, nie były prowadzone systematycznie i nie wpływały na doskonalenie SZBI. W związku z tym dokumenty z zakresu bezpieczeństwa informacji ocenia się pozytywnie z nieprawidłowościami.

Zespół kontrolny przyjął wyjaśnienia złożone w toku kontroli, że w NCBR planowane jest takie skonstruowanie polityk i procedur, aby były one jawne i ogólnie znane wszystkim pracownikom NCBR, z wyłączeniem pojedynczych instrukcji zawierających dane systemów, które ze względów bezpieczeństwa nie powinny być publicznie znane.

(Dowód: akta kontroli str. 65-351, 541-671, 760-764, 828-838)

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 NCBR zarządzanie ryzykiem w ramach SZBI reguluje PBI oraz dokument PZ3-1 *Procedura*: *Zarządzanie ryzykiem* z dnia 28 czerwca 2018 r. (wersja: 05/01). Procedura

zakłada przeprowadzenie przynajmniej raz w roku analizy ryzyk związanych z realizacją celów strategicznych oraz celów operacyjnych NCBR.

W okresie objętym kontrolą przeprowadzono w NCBR jedną analizę ryzyka zakończoną raportem z dnia 28 grudnia 2017 r. Z informacji uzyskanych w toku kontroli wynika, że kolejna analiza ryzyka (dotycząca roku 2018) zostanie przeprowadzona w IV kwartale 2018 r.

Zdaniem zespołu kontrolnego przeprowadzona analiza ryzyka nie spełniła oczekiwanego celu, gdyż nie została zakończona opracowaniem planu postępowania z ryzykiem mimo, że procedura PZ3-1 w pkt 6.5 i 6.6 wskazuje na konieczność opracowania planu postępowania z ryzykiem oraz wdrożenia takiego planu. Dopiero w notatce służbowej z dnia 24 października 2018 r. (uzyskanej w toku kontroli) opisano szereg działań, jakie zostały podjęte w wyniku ww. analizy ryzyka przeprowadzonej w grudniu 2017 r. Powyższe potwierdza jednoznacznie brak planu postępowania z ryzykiem w NCBR finalizującego przeprowadzoną analizę, w związku z czym jedynie częściowo spełnione zostały wymagania określone w § 20 ust. 2 pkt 3 rozporządzenia KRI. Zatem dokonywanie analizy zagrożeń związanych z przetwarzaniem informacji ocenia się pozytywnie z nieprawidłowościami.

(Dowód: akta kontroli str. 776-827, płyta CD)

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.: wystąpienia katastrofy. Baza inwentaryzacyjna jest niezbędna przy wprowadzaniu wszelkich zmian w środowisku teleinformatycznym podmiotu 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 NCBR prowadzony był rejestr środków trwałych. Jego funkcjonowanie wynika z ustawy z dnia 29 września 1994 r. *o rachunkowości*[18].

Sposób zarządzania sprzętem informatycznym i oprogramowaniem został opisany w dokumencie PZ1-9 *Procedura zarządzania zmianami oraz konfiguracją,* a także w dokumencie PZ1-10 *Procedura zarządzania oprogramowaniem*. Procedury te w sposób szczegółowy opisują sposób zarządzania aktywami informatycznymi, w tym opis bazy konfiguracji CMDB. W NCBR prowadzony był rejestr aktywów informatycznych. Aktualizacja rejestru aktywów informatycznych, w tym oprogramowania oraz konfiguracji sprzętowej odbywała się na bieżąco i była wspomagana specjalizowanym oprogramowaniem.

[18] Dz. U. z 2016 r., poz. 1047, z późn. zm.

Zinwentaryzowana była topologia sieci, urządzenia aktywne, adresacja IP, usługi sieciowe i role serwerów.

Zespół kontrolny stwierdza, że przedłożona dokumentacja świadczy o skutecznym zarządzaniu zasobami teleinformatycznymi w NCBR, zgodnie z wymaganiem z § 20 ust. 2 pkt 2 rozporządzenia KRI. Powyższe oceniono pozytywnie.

(Dowód: akta kontroli str. 915-916, płyta CD)

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Ma ono 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 badanym okresie zarządzanie uprawnieniami dostępu do przetwarzania danych w NCBR zostało uregulowane w Polityce Bezpieczeństwa Danych Osobowych NCBR, Polityce Bezpieczeństwa Systemu Informatycznego NCBR, Regulaminie Użytkownika Systemu Informatycznego NCBR oraz w dokumencie PZ1-3 *Procedura kontroli dostępu.* Regulacje te w sposób kompleksowy definiują sposób zarządzania uprawnieniami użytkowników, w tym także przeprowadzania okresowego przeglądu nadanych uprawnień dostępu do systemów teleinformatycznych w NCBR.

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.

W NCBR był prowadzony elektroniczny rejestr uprawnień do systemów teleinformatycznych, zawierający szczegółowe informacje, jak imię i nazwisko użytkownika oraz zakres i data ważności uprawnienia.

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

Działania w powyższym zakresie oceniono pozytywnie.

(Dowód: akta kontroli str. 923-927, płyta CD)

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Szkolenia z zakresu BI powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać im 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 NCBR kwestię szkoleń dotyczących BI uregulowano w Polityce Bezpieczeństwa Informacji NCBR (pkt 7.2).

Analiza przedstawionej do kontroli dokumentacji dotyczącej szkoleń dla pracowników NCBR wskazała, że w kontrolowanym okresie nie zapewniono okresowych szkoleń dla użytkowników zaangażowanych w proces przetwarzania informacji w systemach informatycznych. Podstawowe szkolenia z zakresu bezpieczeństwa informacji przechodzili jedynie pracownicy nowozatrudnieni, co oznacza częściowe spełnienie wymagań § 20 ust. 2 pkt 6 rozporządzenia KRI.

Powyższe zagadnienie oceniono pozytywnie z nieprawidłowościami.

(Dowód: akta kontroli str. 936-1015, płyta CD)

2.6. Praca na odległość i mobilne przetwarzanie danych

W okresie objętym kontrolą w NCBR w zakresie zabezpieczenia urządzeń mobilnych i danych w nich zawartych przed kradzieżą oraz nieuprawnionym dostępem poza siedzibą jednostki, funkcjonowały: Regulamin Użytkownika Systemu Informatycznego w NCBR, dokument PZ1-3 *Procedura kontroli dostępu*, a także Regulamin ochrony informacji dla wykonawcy (stosowany w przypadku potrzeby zapewnienia dostępu zdalnego do zasobów NCBR przez zewnętrznego dostawcę usług na podstawie stosownej umowy).

Sprzęt komputerowy wykorzystywany do pracy na odległość był konfigurowany przez pracowników DSI, a jego wydanie i zwrot pracownikowi były każdorazowo ewidencjonowane. Niezależnie od powyższego prowadzony był rejestr osób, którym przyznany został dostęp zdalny do sieci NCBR z wykorzystaniem VPN (*Virtual Private Network*). Oddzielny rejestr był prowadzony dla udzielonych dostępów VPN dla pracowników zewnętrznych dostawców usług dla NCBR. Obowiązujące w NCBR regulacje dotyczące BI określały podstawowe zasady bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, zgodnie z wytycznymi § 20 ust. 2 pkt 8 rozporządzenia KRI.

Powyższy obszar ocenia się pozytywnie.

(Dowód: akta kontroli str. 917-922, płyta CD)

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 posiadania przez firmy serwisujące.

W NCBR w zakresie serwisu i rozwoju systemów teleinformatycznych obowiązywał Regulamin ochrony informacji dla wykonawcy. Powyższa regulacja wymagała 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 jedynie pod nadzorem pracowników NCBR.

W konkretnych umowach z dostawcami produktów i usług zapisy dotyczące BI były indywidualnie negocjowane przez strony umowy i były adekwatne do charakteru usług. Udostępnione zespołowi kontrolnemu umowy serwisowe, zawarte przez NCBR, zawierały zapisy zapewniające odpowiedni poziom bezpieczeństwa informacji w kontaktach z firmami zewnętrznymi, co wypełnia wymagania § 20 ust. 2 pkt 10 rozporządzenia KRI.

Mając na uwadze powyższe, badane zagadnienie ocenia się pozytywnie.

(Dowód: akta kontroli str. 839-875, płyta CD)

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 ustalony z góry sposób, a także powinien być opisany sposób reakcji na te incydenty przez wyznaczone osoby, skutkujący szybkim podjęciem działań korygujących.

W okresie objętym kontrolą w zakresie obsługi incydentów naruszenia BI w NCBR obowiązywały regulacje opisane w PBI oraz w dokumencie PZ1-8 *Procedura zarządzania incydentami naruszenia bezpieczeństwa informacji.*

Powyższe regulacje szczegółowo 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 PZ1-8 zawiera wykaz potencjalnych incydentów naruszenia bezpieczeństwa informacji, wzór raportu z incydentu oraz wzór rejestru incydentów.

Zespołowi kontrolnemu przedłożono rejestr incydentów BI oraz trzy raporty z 2018 r. dotyczące naruszeń zasad bezpieczeństwa systemu informatycznego NCBR, a także dwie notatki z 2017 r. w sprawie zgłoszonych naruszeń bezpieczeństwa informacji. Raporty i notatki zawierają szczegółowe informacje o przyczynach, skutkach i działaniach korygujących podjętych w stosunku do zaistniałych incydentów naruszenia BI. Ponadto, w NCBR był prowadzony oddzielny rejestr naruszeń ochrony danych osobowych.

Sposób obsługi incydentów związanych z bezpieczeństwem informacji w NCBR pozwala stwierdzić, że spełnione są wymagania § 20 ust. 2 pkt 13 rozporządzenia KRI, a zatem obszar ten oceniono pozytywnie.

(Dowód: akta kontroli str. 876-885)

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 NCBR w powyższym zakresie funkcjonował dokument PZ1-2 *Procedura audytu i przeglądu SZBI.*

Zgodnie z *Planem audytu na rok 2017*[19], audytor wewnętrzny NCBR przeprowadził audyt wewnętrzny w zakresie bezpieczeństwa informacji i działalności w zakresie zarządzania bezpieczeństwem systemów informatycznych[20], w wyniku którego zostało sporządzone „Sprawozdanie z zadania audytowego" z dnia 28 grudnia 2017 r.

Na rok 2018 zostało zaplanowane[21] zadanie zapewniające pn. „Stan bezpieczeństwa teleinformatycznego w Narodowym Centrum Badań i Rozwoju", którego wykonanie przez komórkę audytu wewnętrznego NCBR planowane jest na IV kwartał 2018 r.

Niezależnie od ww. planu audytu wewnętrznego, w I kwartale 2017 r. w NCBR został przeprowadzony przez trójetapowy audyt[22] dotyczący bezpieczeństwa elementów infrastruktury teleinformatycznej NCBR. Audyt skupiał się na bezpieczeństwie środowiska

[19] Wyciąg z planu audytu wewnętrznego NCBR na rok 2017.
[20] Nr zadania audytowego: SAK.0921.4.2017.KB1.
[21] Wyciąg z planu audytu wewnętrznego NCBR na rok 2018.
[22] Raport z wykonania badań bezpieczeństwa elementów infrastruktury teleinformatycznej dla NCBR Etap I - luty 2017, Etap II - marzec 2017, Etap III - retesty - październik 2017.

pracy kluczowych aplikacji, a jego wyniki znacząco wpłynęły na podniesienie bezpieczeństwa informacji w NCBR.

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

(Dowód: akta kontroli str. 720-733, 744-756, 765-769; płyta CD)

2.10. Kopie zapasowe

Kopie zapasowe (bezpieczeństwa) powinny być właściwie tworzone, przechowywane i testowane. Celem tworzenia kopii zapasowych danych 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 zakresie wykonywania kopii zapasowych w NCBR obowiązywały następujące regulacje wewnętrzne: Regulamin Użytkownika Systemu Informatycznego NCBR, Polityka Bezpieczeństwa Danych Osobowych, dokument PZ1-11 *Procedura wykonywania kopii zapasowych w systemie informatycznym* oraz PZ1-7 *Procedura zachowania ciągłości działania SI.*

Zespół kontrolny stwierdził, że procedury wykonywania kopii zapasowych były na bieżąco stosowane. Kopie bezpieczeństwa w ramach SZBI wykonywane były przy wykorzystaniu specjalizowanego oprogramowania w sposób automatyczny i według zdefiniowanego harmonogramu. W toku kontroli okazano przykładowy wydruk harmonogramu wykonania kopii zapasowych zawierający nazwy 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. Utworzone kopie zapasowe były przechowywane w dwóch niezależnych lokalizacjach. W okresie od grudnia 2017 r. do marca 2018 r. w NCBR przeprowadzono odtworzenie środowiska systemu , co potwierdza skuteczność wykonywania kopii zapasowych. Ponadto, stwierdzono liczne przypadki odtwarzania na wniosek użytkowników, pojedynczych plików z kopii zapasowej. Nie stwierdzono jednak wykonywania okresowych planowanych testów polegających na odtworzeniu systemów z kopii zapasowych. Brakowało także regulacji wewnętrznych

opisujących procedury przeprowadzania takich testów. Powyższe oznacza jedynie częściową zgodność z wymaganiem § 20 ust. 2 pkt 12 lit b rozporządzenia KRI, zatem działalność NCBR w tym zakresie ocenia się pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 928-935)

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.

NCBR, ze względu na ściśle zdefiniowany zakres zadań statutowych, nie prowadziło samodzielnie znaczących prac rozwojowych w zakresie rozwoju eksploatowanych systemów informatycznych. W związku z powyższym, w badanym okresie, NCBR nie posiadało regulacji wewnętrznych określających szczegółowe wymagania techniczne i eksploatacyjne w zakresie projektowania, wdrażania i odbioru systemów informatycznych planowanych do wdrożenia, jak wymagana architektura systemu, sposób licencjonowania i wykorzystania praw autorskich, zgodność z obowiązującymi przepisami prawa (m.in. z ustawą z dnia 16 lipca 2014 r. *Prawo telekomunikacyjne*[23] i *ustawą o informatyzacji*), sposób i poziom zabezpieczeń, zastosowanie norm i standardów przemysłowych, wydajność, poziom niezawodności SLA, mechanizmy kontroli i audytu, sposoby dostarczenia i instalacji systemu informatycznego oraz wymagania sprzętowe i środowiskowe dla systemu, sposób i zakres testów oraz dokumentacji, a także warunki i kryteria odbioru. Wymagania dla nowych systemów informatycznych lub modyfikacji istniejących systemów są formułowane w sposób doraźny w oparciu o wzory umów wykonawców oraz w odpowiedzi na bieżące potrzeby zamawiającego, w tym analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany. Wymagania dotyczące projektowania, wdrażania i odbioru systemów są określane w taki sposób, aby eksploatowane systemy były zaprojektowane i wdrożone z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności i pielęgnowalności. Powyższe atrybuty zostały zabezpieczone w umowach wykonawczych i serwisowych.

W NCBR proces zarządzania zmianami został uregulowany w dokumencie PZ1-9 *Procedura zarządzania zmianami oraz konfiguracją.*

W procesie rozwoju systemów pracownicy NCBR przygotowywali specyfikacje zmian, a następnie aktywnie uczestniczyli w testach akceptacyjnych wdrożonych zmian, co należy uznać za działania pozytywne i racjonalne z punktu widzenia podnoszenia jakości narzędzi informatycznych wspomagających pracę NCBR.

[23] Dz. U. z 2016 r., poz. 1489, z późn. zm.

W 2018 roku w NCBR zmieniono model utrzymania i zarządzania rozwojem kluczowego dla funkcjonowania NCBR systemu informatycznego LSI, co oznaczało przejęcie przez NCBR (DSI) zadań (usług) wcześniej zleconych podmiotowi zewnętrznemu. System LSI został wytworzony i wdrożony przez Firmę '. NCBR posiadał umowę serwisową[24] z ww. firmą na usługi związane z bieżącym utrzymaniem (obsługa błędów) i rozwojem systemu (nowe funkcjonalności). Twórca systemu LSI został zatrudniony w NCBR na stanowisku kierownika Sekcji Rozwoju Oprogramowania odpowiedzialnym za ww. obszar. Zmiana modelu spowodowała obniżenie kosztów utrzymania i rozwoju systemu oraz zwiększenie efektywności procesu zmian (nowe funkcjonalności lepiej dostosowane do potrzeb i szybciej wprowadzane).

Należy zauważyć, że Firma jest twórcą dwóch innych aplikacji używanych w NCBR o znaczeniu pomocniczym:
oraz , zapewniając w ramach pełnionych obowiązków ich rozwój. Pewne ryzyko związane jest z koncentracją kompetencji, jednakże jest ono mitygowane przez proces szkoleń wewnętrznych podnoszących kompetencje zespołu zajmującego się rozwojem aplikacji i systemów w NCBR.

W NCBR 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, alerty bezpieczeństwa, graficzna prezentacja sieci LAN, w tym statusu urządzeń pracujących w sieci itp. W pomieszczeniu obsługi użytkowników (Service-desk) realizowano proces wsparcia użytkowników, monitorowania i rejestracji obrazu z kamer telewizji przemysłowej, zainstalowanych w serwerowniach i punktach dystrybucyjnych sieci LAN. Proces administrowania technicznego i monitorowania określonych obszarów (systemy, aplikacje, dane, infrastruktura sieciowa, stacje robocze) był przypisany konkretnym pracownikom DSI. Proces monitorowania i diagnostyki pozwalał na przewidywanie i zapobieganie ewentualnym problemom związanym z awariami, wyciekami danych, bądź ich utratą, co oznacza, że pomimo braku regulacji wewnętrznych dotyczących projektowania i wdrażania systemów, spełnione zostało wymaganie określone w § 15 ust. 1 rozporządzenia KRI. Działalność NCBR w tym zakresie oceniono pozytywnie.

(Dowód: akta kontroli str. 42-43, 839, płyta CD)

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników, należy stosować szereg zabezpieczeń

[24] Umowa nr 202/16/PU oraz nr 219/17/PU, zmodyfikowana porozumieniem z dnia 14 marca 2018 r.

informatycznych. Celem tych zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także przed kradzieżą środków przetwarzania informacji. Zastosowane zabezpieczenia powinny być adekwatne do poziomu ryzyka wynikającego z analizy ryzyka BI.

W okresie objętym kontrolą w NCBR funkcjonowały regulacje wewnętrzne dotyczące zabezpieczeń dostępu do informacji, opisane w PBI oraz w Polityce Bezpieczeństwa Systemu Informatycznego NCBR (opatrzonej klauzulą „zastrzeżone").

Zgodnie z § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, w NCBR 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 poprzez:

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

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/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, stosowanie zabezpieczeń kryptograficznych, systemów antywirusowych i antyspamowych oraz zapór sieciowych typu *firewall*.

W NCBR 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 NCBR w tym zakresie ocenia się pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 546-573, 793-823)

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

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

W okresie objętym kontrolą w NCBR 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 (dokumenty wykonawcze).

Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia KRI, w NCBR 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). Zastrzeżenie dotyczy braku rejestru zmian w oprogramowaniu;

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, zastosowanie 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.

W wyniku oględzin w siedzibie NCBR stwierdzono, że użytkowane są dwie serwerownie, a kolejna jest w trakcie przygotowania[25]. Z uwagi na fakt, że zastosowane zabezpieczenia techniczno-organizacyjne systemów informatycznych nie wynikały z analizy ryzyka i planu postępowania z ryzykiem, obszar ten ocenia się pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 886-888)

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

[25] Notatka z wizji lokalnej w serwerowniach NCBR z dnia 24 października 2018 r.

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 przepisach odrębnych, a w przypadku ich braku przez dwa lata.

W badanym okresie NCBR nie posiadało regulacji wewnętrznych, w których zostałyby określone zasady postępowania z logami systemowymi, w tym sposób ich gromadzenia, miejsce i okres ich przechowywania, a także sposób ich systematycznego przeglądania oraz analizy w celu wykrycia działań niepożądanych. W NCBR przystąpiono do wdrożenia specjalistycznego oprogramowania klasy SIEM (*Security Information and Event Management*), co pozwoli na monitorowanie zdarzeń w tym również logów, w trybie non stop. Narzędzie to pozwala na gromadzenie rozproszonych logów, następnie ich analizę i raportowanie, co zapewnia pełną wiedzę o bieżącej sytuacji, niezbędną do efektywnego zarządzania ryzykiem operacyjnym IT.

Brak regulacji wewnętrznych dotyczących zasad postępowania z logami systemowymi oznacza jedynie częściową zgodność z wymaganiem określonym w § 20 ust. 1 pkt 1 w zw. z § 21 ust. 1 i 2 rozporządzenia KRI. Działania NCBR w tym zakresie oceniono pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 44-52, 824-827, 889-914)

Podsumowanie ustaleń:

1. W NCBR funkcjonuje SZBI. Kierownictwo NCBR jest w sposób bieżący i bezpośredni zaangażowane w proces utrzymania i monitorowania SZBI w NCBR, zgodnie z § 20 ust. 1 rozporządzenia KRI. Dokumentacja SZBI (jawna i niejawna) została opracowana i zatwierdzona w 2016 r. Pomimo powołania zespołu do jej aktualizacji oraz funkcjonowania procedury, w której opisano mechanizmy aktualizacji dokumentacji, wytworzona w NCBR dokumentacja SZBI jest w znacznym stopniu zdezaktualizowana. Działania związane z jej aktualizacją należy uznać za niewystarczające. Część procedur została opatrzona klauzulą „zastrzeżone", co utrudnia, a często nawet uniemożliwia ich stosowanie. Zatem należy stwierdzić, że działania kierownictwa podejmowane w celu stworzenia warunków dla aktualizacji regulacji wewnętrznych dotyczących SZBI w zakresie dotyczącym zmieniającego się otoczenia, zgodnie z wymaganiem § 20 ust. 2 pkt 1 rozporządzenia KRI, nie były prowadzone systematycznie i nie wpływały na doskonalenie SZBI.
2. W NCBR istnieją regulacje wewnętrzne dotyczące analizy ryzyka na potrzeby SZBI, jednak przeprowadzona analiza ryzyka nie spełnia celu podniesienia bezpieczeństwa SZBI, gdyż nie kończy się opracowaniem planu postępowania z ryzykiem i jego wdrożeniem. Zatem jedynie częściowo spełnione zostały wymagania określone w § 20 ust. 2 pkt 3 rozporządzenia KRI.

3. NCBR posiada stosowne regulacje wewnętrzne dotyczące inwentaryzacji aktywów IT na potrzeby SZBI, a przedłożona dokumentacja świadczy o skutecznym zarządzaniu zasobami teleinformatycznymi w NCBR, zgodnie z wymaganiem z § 20 ust. 2 pkt 2 rozporządzenia KRI.
4. Zarządzanie uprawnieniami do pracy w systemach informatycznych NCBR było skuteczne. Na bieżąco monitorowano dostęp do zasobów informatycznych, co jest zgodne z wymaganiami § 20 ust. 2 pkt 4 rozporządzenia KRI. Konta byłych pracowników w systemach informatycznych NCBR były w okresie objętym kontrolą sukcesywnie blokowane, zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI.
5. W kontrolowanym okresie nie potwierdzono przeprowadzania okresowych szkoleń dla użytkowników zaangażowanych w proces przetwarzania informacji w systemach informatycznych NCBR. Podstawowe szkolenia z zakresu bezpieczeństwa informacji przechodzili jedynie pracownicy nowozatrudnieni, co oznacza jedynie częściowe spełnienie wymagań § 20 ust. 2 pkt 6 rozporządzenia KRI.
6. W NCBR funkcjonowały regulacje wewnętrzne w zakresie bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, a sprzęt teleinformatyczny wykorzystywany do takiej pracy był konfigurowany i zarządzany zgodnie z obowiązującymi regulacjami, co jest zgodne z wymaganiem określonym w § 20 ust. 2 pkt 8 rozporządzenia KRI.
7. Umowy serwisowe zawarte przez NCBR ze stronami trzecimi, dotyczące badanych systemów, zawierały zapisy zapewniające odpowiedni poziom bezpieczeństwa informacji. Udostępnione zespołowi kontrolnemu umowy serwisowe zawierały zapisy zapewniające odpowiedni poziom bezpieczeństwa informacji w kontaktach z firmami zewnętrznymi, co wypełnia wymagania § 20 ust. 2 pkt 10 rozporządzenia KRI.
8. W NCBR funkcjonowały regulacje wewnętrzne w zakresie zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji. Sposób obsługi incydentów związanych z bezpieczeństwem informacji w NCBR pozwala stwierdzić, że spełnione są wymagania określone w § 20 ust. 2 pkt 13 rozporządzenia KRI.
9. W NCBR funkcjonowały odrębne regulacje wewnętrzne określające zasady wykonywania audytów wewnętrznych systemów informatycznych na potrzeby SZBI. W 2017 r. zostały przeprowadzone dwa audyty w zakresie bezpieczeństwa informacji, a kolejny został zaplanowany do przeprowadzenia w IV kwartale 2018 r., co oznacza, że zakres i wyniki dotychczas przeprowadzonych audytów spełniają wymagania § 20 ust. 2 pkt 14 rozporządzenia KRI.
10. Kopie bezpieczeństwa w ramach SZBI wykonywane były przy wykorzystaniu specjalizowanego oprogramowania w sposób automatyczny według zdefiniowanego kalendarza. Utworzone kopie zapasowe były przechowywane w dwóch niezależnych lokalizacjach. Nie stwierdzono jednak wykonywania okresowych testów polegających na odtworzeniu systemów z kopii zapasowych oraz regulacji wewnętrznych

opisujących procedury dotyczące takich testów. Powyższe oznacza jedynie częściową zgodność z wymaganiem § 20 ust. 2 pkt 12 lit b rozporządzenia KRI.

11. Ze względu na zakres działalności NCBR, w badanym okresie nie funkcjonowały regulacje wewnętrzne określające szczegółowe wymagania techniczne, bezpieczeństwa i eksploatacyjne w zakresie projektowania, wdrażania i odbioru systemów teleinformatycznych, a podejmowane działania w tym obszarze miały charakter doraźny. Jednocześnie realizowany był ciągły proces zarządzania i monitorowania systemów informatycznych i środowiska ich pracy, co oznacza, że pomimo braku regulacji wewnętrznych dotyczących projektowania i wdrażania systemów, spełnione zostało wymaganie § 15 ust. 1 rozporządzenia KRI.
12. Zgodnie z § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, w NCBR zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami oraz wdrożono zabezpieczenia informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Podkreślić jednak należy, że stosowane zabezpieczenia nie wynikały z analizy ryzyka i planu postępowania z ryzykiem.
13. Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia KRI w NCBR zapewniono odpowiedni poziom bezpieczeństwa systemów teleinformatycznych pomimo, iż stosowane zabezpieczenia nie wynikały z analizy ryzyka i planu postępowania z ryzykiem.
14. W NCBR przystąpiono do wdrożenia specjalistycznego oprogramowania klasy SIEM, co pozwoli na monitorowanie zdarzeń, w tym logów systemowych, w trybie non stop. Brak regulacji wewnętrznych dotyczących zasad postępowania z logami systemowymi oznacza jedynie częściową zgodne z w § 20 ust. 1 pkt 1 w zw. z § 21 ust. 1 i 2 rozporządzenia KRI.

W świetle powyższych ustaleń, obszar dotyczący wdrożenia systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych w NCBR należy ocenić pozytywnie z nieprawidłowościami. Na ocenę tę miało wpływ przede wszystkim to, że obowiązująca dokumentacja SZBI jest w znacznym stopniu nieaktualna, a procedury wchodzące w skład dokumentacji SZBI są dokumentami niejawnymi, dostępnymi jedynie dla 5 pracowników, przez co nie były znane pracownikom wykonującym zadania w nich opisane. Ponadto, po przeprowadzeniu analizy ryzyka nie opracowano planu postępowania z ryzykiem i nie wdrożono takiego planu. Oznacza to, że kierownictwo NCBR nie mogło sprawować skutecznego nadzoru nad podjęciem działań adekwatnych do stopnia oszacowanego ryzyka. Proces zarządzania i monitorowania systemów teleinformatycznych był realizowany w sposób ciągły, niemniej jednak stwierdzono brak regulacji wewnętrznych dotyczących zasad postępowania z logami systemowymi oraz dotyczących projektowania i wdrażania systemów. Nie zapewniono również cyklicznych szkoleń dla użytkowników zaangażowanych

w proces przetwarzania informacji w systemach informatycznych, a szkoleniami objęto jedynie nowozatrudnionych.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami

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[26]. Termin dostosowania systemów teleinformatycznych do prezentacji zasobów informacyjnych według powyższego standardu upłynął z dniem 30 maja 2015 r.

Analiza sposobu prezentacji treści na stronach internetowych w systemach NCBR wskazała, że zostały one częściowo dostosowane do odbioru ich treści przez osoby z niepełnosprawnościami, m.in. możliwe jest zwiększenie kontrastu i wielkości liter. Jednocześnie, NCBR nie dysponuje dokumentacją dotyczącą wymagań i zastosowanych rozwiązań, co oznacza częściowe spełnienie wymagań określonych w § 19 rozporządzenia KRI.

Ustalenie:

1. Systemy NCBR będące przedmiotem badania zostały częściowo dostosowane do odbioru prezentowanych treści przez osoby z niepełnosprawnościami, co oznacza częściowe spełnienie wymagań określonych w § 19 rozporządzenia KRI.

Działania NCBR w zakresie zapewnienia dostępności informacji zawartych na stronach internetowych NCBR ocenia się pozytywnie z uchybieniami.

(Dowód: akta kontroli str. 44-52)

[26] system wymagań *Web Content Accessibillity Guidelines*

ZALECENIA POKONTROLNE

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

1. Podjęcie działań doskonalących SZBI, w tym w szczególności systematyczne aktualizowanie regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia oraz zapewnienie, by dokumentacja SZBI była jawna i dostępna dla osób zaangażowanych w proces przetwarzania informacji.
2. Cykliczne analizowanie zagrożeń związanych z przetwarzaniem informacji i opracowywanie na tej podstawie planu postępowania z ryzykiem z uwzględnieniem zabezpieczeń adekwatnych do poziomu ryzyka wynikającego z analizy ryzyka BI, zgodnie z wymaganiem określonym w § 20 ust. 2 pkt 3 rozporządzenia KRI.
3. Podnoszenie świadomości pracowników w zakresie bezpieczeństwa informacji, m.in. poprzez zapewnienie cyklicznych szkoleń okresowych, dostarczających aktualnej wiedzy o zagrożeniach bezpieczeństwa informacji, skutkach naruszeń zasad bezpieczeństwa informacji oraz stosowanych zabezpieczeniach, zgodnie z wymaganiem określonym w § 20 ust. 2 pkt 6 rozporządzenia KRI.
4. Przeprowadzenie inwentaryzacji i analizy interaktywnych usług elektronicznych pod kątem możliwości świadczenia ich na poziomie dojrzałości wyższym od pierwszego (poziom informacyjny), uwzględniając model usługowy, zgodnie z wymaganiem określonym w § 15 ust. 2 rozporządzenia KRI.
5. Opracowanie i wdrożenie regulacji wewnętrznych określających zasady testowania kopii zapasowych oraz systematyczne, okresowe testowanie ich jakości, zgodnie z wymaganiem § 20 ust. 2 pkt 12 lit b rozporządzenia KRI.
6. Opracowanie i wdrożenie regulacji wewnętrznych określających zasady prowadzenia i wykorzystania dzienników systemów (logów), zgodnie z wymaganiem określonym w § 21 rozporządzenia KRI.
7. Opracowanie i wdrożenie regulacji wewnętrznych określających zasady projektowania, wdrażania i eksploatacji nowych oraz istniejących systemów informatycznych, z uwzględnieniem wymagań wskazanych w § 15 ust. 1 rozporządzenia KRI.
8. Opracowanie i wdrożenie regulacji wewnętrznych określających wymagania co do sposobu budowy interfejsów programowych pomiędzy systemami NCBR, niezbędnych mechanizmów bezpieczeństwa oraz konieczności ich pełnego dokumentowania, zgodnie z § 16 ust. 1 oraz § 5 ust. 3 pkt 3. KRI.
9. Dostosowanie systemów teleinformatycznych NCBR, zgodnie ze standardem WCAG 2.0., do odbioru prezentowanych w nich treści osobom z niepełnosprawnościami.

Na podstawie art. 49 w zw. 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 nieprawidłowości lub przyczynach ich niepodjęcia, w terminie 60 dni licząc od dnia otrzymania niniejszego dokumentu.

Proszę również o sukcesywne przekazywanie informacji oraz dokumentacji potwierdzającej zrealizowanie zaleceń pokontrolnych, aż do całkowitego usunięcia stwierdzonych nieprawidłowości i uchybień.

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