



NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy

LBY.410.016.04.2022

Pan
Mikołaj Bogdanowicz
Wojewoda Kujawsko-Pomorski
Kujawsko-Pomorski Urząd Wojewódzki
ul. Jagiellońska 3
85-950 Bydgoszcz

KUJAWSKO-POMORSKI
Wydzi:
Wpłynęło: <input type="checkbox"/>
Nr:

WYSTĄPIENIE POKONTROLNE

P/22/082/LBY Zarządzanie oprogramowaniem komputerowym przez administrację publiczną

NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy
ul. Wały Jagiellońskie 12, 85-950 Bydgoszcz
T +48 52 567 58 00, F +48 52 567 58 60
lby@rik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Kujawsko-Pomorski Urząd Wojewódzki, ul. Jagiellońska 3, 85-950 Bydgoszcz ¹ ,
Kierownik jednostki kontrolowanej	Mikołaj Bogdanowicz, Wojewoda Kujawsko-Pomorski ² , od 9 grudnia 2015 r.
Zakres przedmiotowy kontroli	1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym. 2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem.
Okres objęty kontrolą	Lata 2019-2022 do dnia zakończenia kontroli ³ , z wykorzystaniem dowodów wytworzonych przed i po tym okresie, jeżeli miały one istotny wpływ dla ustaleń i ocen kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli ⁴
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Bydgoszczy
Kontroler	Elżbieta Warda-Fereniec, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/113/2022 z 30 czerwca 2022 r. <p style="text-align: right;">(akta kontroli str. 1-3)</p>

II. Ocena ogólna⁵ kontrolowanej działalności

OCENA OGÓLNA

W ocenie Najwyższej Izby Kontroli, w Urzędzie w ograniczonym zakresie sprawowano nadzór nad oprogramowaniem komputerowym. Nie zostały określone szczegółowe zasady zarządzania licencjami obejmujące wszystkie elementy i wymagane czynności niezbędne do zarządzania oraz nadzoru nad pełnym cyklem życia oprogramowania. Pracownicy Urzędu odpowiedzialni za zarządzanie oprogramowaniem nie posiadali pełnej wiedzy na jego temat. Wynikało to z faktu, że stosowane *inventory tool*⁶ nie zapewniało kompletności danych odnoszących się do posiadanych i wykorzystywanych licencji. Wygenerowane na jego podstawie raporty obarczone były błędami, a zestawienia nie były kompletne. W jednostce nie weryfikowano systematycznie wszystkich posiadanych zasobów pod kątem instalowania i korzystania przez pracowników z nielegalnego oprogramowania, mimo obowiązków w tym zakresie wynikających z obowiązującej Polityki Bezpieczeństwa Informacji⁷. Nie zapewniono także rozwiązań technicznych umożliwiających skuteczne i rzeczywiste zarządzanie posiadanymi zasobami, takimi jak urządzenia mobilne typu smartfon, czy tablet pod kątem instalowania oprogramowania.

Zakupy realizowano tylko na niezbędne oprogramowanie, nie zidentyfikowano przypadków wolnego oprogramowania, które nie zostało zainstalowane na urządzeniach Urzędu. W toku kontroli stwierdzono pojedyncze przypadki

¹ Dalej: „Urząd” lub „KPUW”.

² Dalej: „Wojewoda”.

³ Tj. 6 października 2022 r.

⁴ Dz. U. z 2022 r. poz. 623, dalej: „ustawa o NIK”.

⁵ Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

⁶ Narzędzie do przeprowadzania inwentaryzacji oprogramowania.

⁷ Dalej: „PBI” lub „Polityka”.

oprogramowania niezwiązanego z realizacją obowiązków służbowych, wycofanego albo wymagającego aktualizacji.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe⁸ kontrolowanej działalności

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym

Opis stanu faktycznego

1.1. Zgodnie z regulaminem organizacyjnym Urzędu, będącym załącznikiem do zarządzenia Wojewody⁹, zadaniami realizowanymi przez Zespół Bezpieczeństwa Informatyki i Informatyki¹⁰, było m.in.:

- analizowanie i bilansowanie potrzeb Urzędu w dziedzinie informatyzacji, inicjowanie usprawnień, przedstawianie propozycji w zakresie e-administracji;
- monitorowanie i nadzorowanie prawidłowego funkcjonowania od strony informatycznej systemów komputerowych, administracja serwerami, bazami danych oraz urządzeniami sieciowymi działającymi w Urzędzie;
- nadawanie użytkownikom uprawnień do systemów IT- oraz zapewnienie ciągłości działania tych systemów, w tym zabezpieczenie danych przechowywanych w systemach przed ich utratą, w szczególności utrzymanie baz danych w stałej sprawności, ich archiwizowanie oraz odpowiednie przechowywanie kopii bezpieczeństwa.

Nadzór nad ZBII sprawował Wojewoda.

W wewnętrznej strukturze organizacyjnej oraz szczegółowym zakresie działania ZBII z 12 lipca 2021 r., określonych na podstawie § 14 ust. 2 ww. zarządzenia Wojewody wskazano, że do zadań Oddziału Informatyki i Telekomunikacji¹¹ należało w szczególności: monitorowanie i nadzorowanie prawidłowego funkcjonowania od strony informatycznej systemów komputerowych, administracja serwerami, bazami danych oraz urządzeniami sieciowymi działającymi w Urzędzie, nadawanie użytkownikom uprawnień do systemów IT oraz zapewnienie ciągłości działania tych systemów, w tym zabezpieczenie danych przechowywanych w systemach przed ich utratą, a w szczególności utrzymanie baz danych w sprawności, ich archiwizowanie oraz odpowiednie przechowywanie kopii bezpieczeństwa, zarządzanie licencjami na oprogramowanie Urzędu.

Kierownikowi Oddziału przypisano, m.in.: analizowanie i bilansowanie potrzeb Urzędu w dziedzinie informatyzacji, nadzór oraz monitorowanie zadań związanych z funkcjonowaniem od strony informatycznej systemów komputerowych, serwerów, baz danych oraz urządzeń sieciowych, nadzór oraz monitorowanie zadań związanych z zarządzaniem licencjami na oprogramowanie Urzędu.

Zadania związane z administrowaniem i nadzorem nad licencjami dotyczące oprogramowania i aplikacji informatycznych przypisano OIT, jednakże realizował je również Wydział Bezpieczeństwa i Zarządzania Kryzysowego¹² w zakresie zakupu licencji na potrzeby Wydziału, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 4-125, 546-548, 559-560, 649-654, 771-782)

⁸ Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

⁹ Zarządzenie nr 98 z dnia 25 maja 2021 r. ze zmianami.

¹⁰ Dalej: „ZBII” lub „Zespół”.

¹¹ Dalej: „OIT”, lub „Oddział”.

¹² Dalej: „WBZK” lub „Wydział”.

W Urzędzie opracowano Politykę Bezpieczeństwa Informacji, która została zatwierdzona 29 grudnia 2021 r. przez Wicewojewodę. Zawarto w niej m.in. reguły użytkowania sprzętu IT i legalności oprogramowania. W Urzędzie natomiast nie było sformalizowanej procedury dotyczącej zarządzania oprogramowaniem komputerowym. Ustanowione w Urzędzie zasady nie uwzględniały wszystkich etapów życia oprogramowania, w tym zasad monitorowania i nadzoru nad stanem użycia i legalności, w tym na urządzeniach typu smartfon/tablet, konieczności weryfikacji pod kątem bezpieczeństwa nabywanych licencji, w tym również w modelu SaaS¹³ oraz dopuszczania do instalacji programów darmowych, przechowywania i zabezpieczania kluczy instalacyjnych, ewidencjonowania posiadanych i używanych licencji, wycofywania/odinstalowywania licencjonowanego oprogramowania, odniesienia do zmian licencyjnych, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 126-262,561-624)

1.2. W latach 2019-2021 w Urzędzie zostały przeprowadzone dwa audyty: wewnętrzny i zewnętrzny, w których zawarto również kwestie dotyczące zarządzania oprogramowaniem. Audytor Urzędu przeprowadził w 2019 r. „Audyty wewnętrzny w zakresie bezpieczeństwa informacji”, a następnie w sprawozdaniu z zadania zapewniającego sformułował dziewięć zaleceń. Pełnomocnik Wojewody ds. cyberbezpieczeństwa pismami ze stycznia i kwietnia 2022 r. informował audytora o stopniu ich realizacji.

Audyty zewnętrzny został przeprowadzony przez Agencję Bezpieczeństwa Wewnętrznego¹⁴ w 2021 r. i obejmował sprawdzenie systemów IT w Urzędzie. W korespondencji e-mail Urzędu z ABW przekazano wiadomość, że nie wykazano podatności zagrażających bezpieczeństwu systemów IT w KPUW.

W dniu 8 sierpnia 2022 r. zostały przekazane przez ABW końcowe wyniki z tego audytu. Ocena pozostała bez zmian, a zalecenia zostały wdrożone przez Urząd.

(akta kontroli str. 263-266, 358-385, 636)

1.3. Zarządzeniem Dyrektora Generalnego Urzędu nr 17/2014 z 19 listopada 2014 r.¹⁵ określono, w regulaminie udzielania zamówień publicznych, zasady nabywania m.in. oprogramowania. W obowiązujących w Urzędzie procedurach nie określono jednak wszystkich kwestii dot. jego zarządzania, np. nie określono zasad zarządzania, wdrażania, użytkowania i bieżącego nadzorowania oprogramowania komputerowego.

W latach 2019-2022 w ZBII zatrudnionych było od dziewięciu do 10 pracowników. W trzech postępowaniach konkursowych oraz poza procedurą konkursową zatrudniono osiem osób, jednakże w tym samym okresie odeszło z pracy siedem osób. Wicewojewoda podał, że Urząd boryka się z problemem fluktuacji i pozyskiwania nowych pracowników. W ostatnim czasie odeszło z pracy dwóch informatyków i kolejni zgłaszają chęć zmiany pracy oraz odejścia z powodu niezadowolenia z wysokości wynagrodzenia.

(akta kontroli str. 386-449)

Nadzór oraz monitorowanie zadań związanych z zarządzaniem licencjami na oprogramowanie przypisano kierownikowi OIT. Prowadzenie ewidencji licencji na

¹³ SaaS - Oprogramowanie jako usługa (Software as a Service) to model udostępniania oprogramowania w chmurze, w którym dostawca chmury rozwija i utrzymuje aplikacje chmurowe, zapewnia ich automatyczne aktualizacje i udostępnia oprogramowanie swoim klientom za pośrednictwem Internetu na zasadzie „pay-as-you-go”, czyli w zależności od wykorzystania zasobów.

¹⁴ Dalej: „ABW”.

¹⁵ Zarządzenie zmieniono czterokrotnie: 8 lutego 2016 r. – zarządzenie nr 5/2016, 20 maja 2020 r. – zarządzenie nr 6/2020, 1 lipca 2020 r. – zarządzenie nr 10/2020 i 31 sierpnia 2020 r. – zarządzenie nr 13/2020.

oprogramowanie będących w posiadaniu Urzędu przypisano ośmiu informatykom Oddziału. Ponadto w Wydziale Bezpieczeństwa i Zarządzania Kryzysowego¹⁶ zadania związane z zarządzaniem licencjami/oprogramowaniem w zakresie ograniczonym zapisami przyjętej Polityki przypisano pięciu pracownikom: dwóm administratorom wojewódzkim systemu SI CPR¹⁷, dwóm administratorom wojewódzkim systemu SWD PRM¹⁸, jednemu pracownikowi WBZK, który realizuje nadzór merytoryczny nad oprogramowaniem dedykowanym dla Wydziału.

W okresie objętym kontrolą wszyscy pracownicy ZBII¹⁹, którym przypisano do realizacji zadania dotyczące zarządzanie oprogramowaniem, uczestniczyli w szkoleniach podnoszących kwalifikacje zawodowe. Łącznie w latach 2019-2022 odbyło się 18 szkoleń, w tym cztery nieodpłatne, w których wzięli udział aktualnie zatrudnieni (dziewięć osób) i byli pracownicy (trzy osoby) ZBII. Łączny koszt tych szkoleń wynosił 39 037 zł. Szkolenia m.in. dotyczyły analizy ryzyka, dostępności cyfrowej, zamówień publicznych, jednak żadne ze szkoleń nie dotyczyło zarządzania licencjami.

(akta kontroli str. 4-80, 386-449)

Analiza dokumentacji 12 wykorzystywanych przez Urząd licencji na oprogramowanie wykazała, że we wszystkich przypadkach Urząd posiadał dowody ich zakupu.

Posiadane przez Urząd klucze licencyjne zebrane były w arkuszu Excel, prowadzonym przez pracownika IT, z podziałem na zainstalowane na PC i laptopach. Zawierający dane arkusz chroniony był hasłem dostępu.

Klucze licencyjne, które są w posiadaniu IT, przechowywane były w zasobie sieciowym. Natomiast klucze licencyjne będące w posiadaniu m.in. WBZK, jak i licencje przypisane do poszczególnych pracowników, były przechowywane w danym wydziale lub przez użytkującego program pracownika.

Zgodnie z przyjętą w Urzędzie praktyką, osobą odpowiedzialną za wprowadzanie danych dotyczących kluczy licencyjnych i ich aktualizację był jeden z pracowników IT. W razie jego nieobecności uprawnienia posiadał również kierownik lub osoba przez niego wskazana. Dostęp do kluczy licencyjnych, będących w posiadaniu IT miało ośmiu pracowników działu w Bydgoszczy. Badanie pięciu licencji wykazało, że klucze licencyjne przechowywano w sposób prawidłowy.

W przypadku WBZK Wydział nie posiadał specjalistycznego narzędzia do zarządzania oprogramowaniem. Liczba wykorzystywanego oraz wolnego oprogramowania była weryfikowana przez pracownika Wydziału. Dyrektor WBZK wyjaśnił, że Wydział nadzoruje licencje specjalistyczne, które są w jego posiadaniu, tj. aplikacje rządowe.

KPUW nie monitorował instalacji oprogramowania na urządzeniach typu smartfony/tablety. Nie posiadał dedykowanego narzędzia do ich monitoringu, a *inventory tool* wykorzystywany przez Urząd, nie posiadał takiej funkcjonalności, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

W Urzędzie nie prowadzono jednego kompletnego spisu oprogramowania. Spisy zakupionego oprogramowania znajdowały się w trzech komórkach organizacyjnych Urzędu: w ZBII, WBZK oraz ujmowane przez Biuro Finansowo-Inwestycyjne²⁰

¹⁶ Dalej: „WBZK”.

¹⁷ System Informatyczny Powiadomiania Ratunkowego – tel. 112.

¹⁸ System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego.

¹⁹ Z wyjątkiem jednego, który rozpoczął pracę w Zespole w kwietniu 2021 r.

²⁰ Dalej: „BFI”.

w systemie finansowo-księgowym²¹, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 297-302, 316-323, 450-474, 559-560, 649-659, 763-791)

Oprogramowanie typu *inventory tool* zostało zainstalowane w Urzędzie w III kwartale 2018 r. W pierwotnej wersji oprogramowanie było aktualizowane ręcznie, przez zbieranie informacji ze wszystkich dostępnych na etapie wprowadzania informacji do systemu. Aktualizacja była wykonywana w momencie wykonywania czynności na danej stacji. W kolejnym etapie oprogramowanie zostało zautomatyzowane poprzez instalację agentów na stacjach podłączonych do sieci komputerowej Urzędu co pozwoliło na bieżąco aktualizować informacje. Wykorzystywane oprogramowanie jest darmowe, dystrybuowane na licencji GNU GPL, co uprawnia użytkownika do komercyjnego wykorzystania. Od czasu zautomatyzowania procesu zbierania informacji, dane wykorzystywane są w sytuacji konieczności przeglądu oprogramowania zainstalowanego na stacji np. w przypadku konieczności reinstalacji. Dane zbierane automatycznie wskazują jakie oprogramowanie zostało zainstalowane oraz w jakiej wersji. Zainstalowany agent nie jest w stanie zebrać informacji odnośnie daty zakupu oraz daty ważności oprogramowania. Dane dotyczące zakupu w tym długość ważności subskrypcji należy wprowadzić ręcznie do systemu. System zbiera informacje ze stacji podłączonych do sieci wewnętrznej Urzędu jednak nie pozwala na identyfikację wykorzystywanych/wolnych licencji. Prowadzony jest dodatkowy spis w postaci arkusza kalkulacyjnego Excel, który zawiera informacje o wykorzystanych oraz wolnych licencjach. W trakcie badania nie stwierdzono wolnego oprogramowania. Wszystkie zakupione licencje były zainstalowane na komputerach.

(akta kontroli str. 519-522, 559-560, 624a, 637-770)

W latach 2019-2022 (do dnia 9 września 2022 r. – data sporządzenia wykazu) 74 osoby zmieniły stanowisko służbowe w Urzędzie. I tak: 24 osoby w 2019 r., 15 w 2020 r., osiem w 2021 i 27 w 2022 r. Na podstawie przygotowanego przez Urząd wykazu osób, u których nastąpiła zmiana stanowiska pracy, wybrano w sposób celowy 10 takich zmian. Analiza wykazała, że komputer stacjonarny (PC) wraz z zainstalowanym na nim oprogramowaniem przypisany był do konkretnego pracownika, a w przypadku zmiany stanowiska tego pracownika, komputer zostawał w dziale/wydziale, do którego był przypisany. W przypadku zmiany stanowiska (wydziału) przez użytkowników laptopów, awansowani pracownicy zabierali je ze sobą na nowe stanowisko, wraz z zainstalowanym na nim oprogramowaniem. Nie stwierdzono przypadku aby okres pozostawiania komputera bez przydziału trwał dłużej niż 6 miesięcy.

(akta kontroli str. 513-518, 524-530)

W latach 2019-2022 (do dnia 31 sierpnia 2022 r.) 245 osób odeszło z pracy w Urzędzie. I tak: 75 osób w 2019 r., 50 w 2020 r., 73 w 2021 i 47 w 2022 r. Na podstawie przygotowanego przez Urząd wykazu osób, z którymi nastąpiło rozwiązanie stosunku pracy, wybrano w sposób celowy 20 osób (z 2019 r. – cztery, z 2020 r. – jedną, z 2021 r. – sześć i z 2022 r. – dziewięć osób). Analiza wykazała, że siedem osób, które już nie pracują w Urzędzie, mają cały czas aktywne konta użytkowników i dostęp do system informatycznego Urzędu (cztery z 2021 r. i trzy z 2022 r.). Pozostałym 13 osobom z badanej próby dostęp do systemu informatycznego Urzędu został odebrany. Szerzej opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 495-512, 531-538)

²¹ W ewidencji środków trwałych, pozostałych środków trwałych i wartościach niematerialnych i prawych.

W Urzędzie użytkowany był jeden program na portalu Wydziału Koordynacji Świadczeń, zawierający m.in. system kolejkowy oraz rejestry wydawanych rozstrzygnięć, którego autorem był pracownik Urzędu. Tworzenie tej strony internetowej odbyło się w ramach umowy o pracę, a właścicielem strony jest Urząd. Również kody dostępu były przechowywane na serwerach Urzędu.

(akta kontroli str. 386-395)

1.4. W PBI zawarto m.in. reguły użytkowania oprogramowania w Procedurze nr KPUW-PBI-08 - *Procedura zasad użytkowania i zarządzania sprzętem informatycznym i legalnością oprogramowania*. Dodatkowo aby uniemożliwić instalowanie oprogramowania użytkownicy nie posiadali uprawnień administratora systemu. Tylko pracownicy komórki odpowiedzialnej za obsługę informatyczną Urzędu mieli stosowne uprawnienia do jego instalowania. Pełnomocnik ds. Ochrony Informacji Niejawnych²² wyjaśnił, że pracownicy Urzędu mają obowiązek stosowania ww. procedury, co w połączeniu z brakiem uprawnień administratora systemu uniemożliwia instalację nielegalnego oprogramowania. Wyjaśnił również, że w KPUW nie przeprowadzano audytu legalności oprogramowania. Oprogramowanie było sprawdzane w momencie wykonywania czynności na danej stacji roboczej.

Zasady obejmujące użycie służbowych zasobów IT zostały określone w PBI, którą każdy pracownik ma obowiązek znać i potwierdzić wypełnieniem stosownego oświadczenia dołączonym do akt osobowych. Opisują to m.in.: Procedura nr KPUW-PBI-03, *zasady dostępu do sieci i korzystanie z poczty elektronicznej*, Procedura nr KPUW-PBI-07- *zasady użytkowania urządzeń mobilnych*, Procedura nr KPUW-PBI-08 - *zasady użytkowania i zarządzania sprzętem informatycznym i legalnością oprogramowania*. W pkt. 3 tej Procedury opisano zasady użytkowania oprogramowania, w niej zapis, że: *Pracownicy mogą korzystać jedynie z oprogramowania, na które Urząd posiada aktualne licencje*.

W okresie objętym kontrolą nie przeprowadzano przeglądu oprogramowania i licencji, w związku z czym jednostka nie przedstawiła stosownych raportów, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*.

Licencje na środowisko wirtualne w okresie objętym kontrolą obejmuje środowisko VMware, na które licencja została zakupiona na okres 3 lat i wygaśnie w 2024 r. W Urzędzie brak było środowisk deweloperskich, testowych czy szkoleniowych. Zasoby sieciowe wykorzystywane były jako repozytoria do systemu kopii zapasowych lub jako folder plików.

W trakcie kontroli ujawniono pojedyncze przypadki oprogramowania wycofanego z użycia, wymagającego aktualizacji lub niezwiązanego z realizacją obowiązków służbowych. Ponadto na urządzeniach będących własnością Urzędu zainstalowane było różnego typu oprogramowanie do łączenia się i zarządzania innymi komputerami, które nie były wykazane w przekazanym kontroli spisie licencji. Szerzej opisano w sekcji *Stwierdzone nieprawidłowości*.

Oprogramowanie, dla którego wygasła subskrypcja było wycofywane z użytkowania²³. Pełnomocnik wyjaśnił, że nie ma możliwości użytkowania takiego oprogramowania. W sytuacji uzyskania informacji o podatnościach, mogących mieć wpływ na bezpieczeństwo systemów, wdrażano czynności mające na celu wyeliminowanie zagrożenia. Działania te miały na celu przede wszystkim ochronę zasobów IT przed oprogramowaniem ransomware, którego destruktoryjne działanie miałyby wpływ na bezpieczeństwo zasobów. Informację o podatnościach wykrytych w aplikacjach, systemach operacyjnych, oprogramowaniu narzędziowym było

²² Dalej: „Pełnomocnik”.

²³ M.in. m.in. AutoCAD i Symantec.

przesyłane z CSIRT²⁴ wraz ze zaleceniami. Wszelkie informacje mogące mieć wpływ na bezpieczeństwo IT były zamieszczane na wewnętrznej stronie Intranetu z zaleceniami dla użytkowników.

Zgodnie z PBI incydenty są zgłaszane do Pełnomocnika ds. Cyberbezpieczeństwa, który podejmuje stosowne kroki w celu wyeliminowania zagrożenia. Urząd jest użytkownikiem systemu Arakis, dzięki któremu na bieżąco są przekazywane informacje o podatnościach. W przypadku WBZK, Wydział nie posiada oprogramowania do skanowania sieci, nie ma więc możliwości wygenerowania raportu. Dyrektor WBZK wyjaśnił, że w systemie Urzędu nie są wpięte komputery, na których zainstalowane jest oprogramowanie dotyczące centrum powiadamiania ratunkowego (CPR) oraz dyspozytorni medycznych, które są nadzorowane przez system wspomaganie dowodzenia ratownictwa medycznego, będącego w dyspozycji MSWiA. W CPR w przypadku wykrycia naruszenia zasad użytkownika wykonywane są stosowne kroki mające na celu eliminację ewentualnych luk w zabezpieczeniach. W pozostałych Oddziałach WBZK (w miejscu) postępowanie w przypadku wykrycia ewentualnej nieprawidłowości jest zgodne z PBI, a wszelkie ewentualne naruszenia są zgłaszane Pełnomocnikowi Wojewody ds. Cyberbezpieczeństwa oraz ZBII.

W okresie objętym kontrolą Urząd nie zbywał żadnego sprzętu, ani oprogramowania. Zainstalowane na sprzęcie do likwidacji oprogramowanie nie podlegało ponownej instalacji na innym sprzęcie komputerowym.

Pełnomocnik wyjaśnił, że przestarzałe oprogramowanie zainstalowane na stacjach roboczych, które było niebezpieczne ze względu na pojawiające się luki oraz brak wsparcia producenta, zostało wycofane z użytku wraz ze starą stacją roboczą, nienadającą się do dalszej pracy. Zgodnie z obowiązującą procedurą z nośników zostały usunięte dane użytkowników, a dyski wymontowane. Oprogramowanie²⁵ znajdujące się na tych nośnikach w związku z brakiem możliwości ponownego wykorzystania, zostaje trwale usunięte w procesie demagnetyzacji oraz fizycznego uszkodzenia nośników.

(akta kontroli str. 126-262, 316-323, 465-492)

Pełnomocnik i Dyrektor WBZK podali, że w Urzędzie nie stosuje się oprogramowania typu SaaS.

(akta kontroli str. 552, 559-560)

1.5. Na podstawie opisanej wyżej wybranej próby 12 zakupów oprogramowania stwierdzono, że liczba użytkowników nie przekraczała liczby nabytych licencji a licencje te były używane w terminach ich ważności.

(akta kontroli str. 173-262, 637-770, 624a)

Stwierdzone
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości.

1. Brak w Urzędzie monitoringu zainstalowanego oprogramowania na urządzeniach typu smartfon/tablet.

Pełnomocnik wyjaśnił, że użytkowany przez Urząd program *inventory tool* nie posiadał takiej funkcjonalności. Podał, że ZBII będzie wnioskował w najbliższym czasie o zakup stosownego oprogramowania umożliwiającego zinwentaryzowanie urządzeń przenośnych typu smartfon/tablet.

(akta kontroli str. 263-266, 628-630)

²⁴ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego.

²⁵ Tj. m.in.: Office 2003, 2007, 2010, Windows XP, Vista, 7 Pro oraz wersje OEM przypisane do uszkodzonego urządzenia. Telefony zostają przywrócone do ustawień fabrycznych, przed przekazaniem ich do utylizacji.

NIK zauważa, że brak szczegółowych regulacji dotyczących monitorowania urządzeń mobilnych (np. dotyczących np. częstotliwości weryfikacji legalności oprogramowania instalowanego na tych urządzeniach), skutkowało brakiem nadzoru nad oprogramowaniem zainstalowanym na tego typu urządzeniach.

2. Brak pełnych danych o posiadanych przez Urząd licencjach. Stosowane w Urzędzie *inventory tool* nie zapewniało kompletności danych odnoszących się do posiadanych i wykorzystywanych licencji, wygenerowane na jego podstawie raporty obarczone były błędami, a zestawienia nie były pełne. W Urzędzie brak było zautomatyzowanych rozwiązań zapewniających dostępność kompletnych i aktualnych informacji o posiadanych i wykorzystywanych licencjach w ramach wszystkich użytkowanych zasobów sprzętowych. W związku z tym w okresie od 2019-2022 roku Urząd nie posiadał pełnej informacji na temat wszystkich zakupionych licencji. Prowadzone przez pracowników Urzędu rejestry były nierzetelne, żaden z nich nie był kompletny. W spisie przedstawionym przez IT brakowało dwóch licencji a przez WBZK i BFI – po trzy licencje. W trakcie trwania kontroli wszystkie rejestry zostały uaktualnione.

Pełnomocnik wyjaśnił, że w trakcie kontroli sporządzono korekty do zestawienia zakupionego oprogramowania w latach 2019-2022. Dyrektor WBZK wyjaśnił, że omyłkowo zostały wpisane do zestawienia tylko licencje zakupione w 2021 r.

(akta kontroli str. 297-302, 316-323, 450-474, 559-560, 649-659, 763-791)

3. Nieprawidłowe postępowanie z zainstalowanym oprogramowaniem:

a) w trakcie kontroli ujawniono, na wybranych losowo urządzeniach, przypadki instalacji wersji demo, testowych, które powinny być odinstalowane. Ponadto odinstalowane powinno zostać również oprogramowanie EOL (end of life), czyli takie, które zostało oficjalnie wycofane ze względu na luki w bezpieczeństwie.

Pełnomocnik wyjaśnił, że pomimo usunięcia ww. oprogramowania system *inventory tool* nadal wykazuje, że na wskazanych stacjach roboczych te programy się znajdują. Problemem jest niekompletna deinstalacja instalatora producenta wskazanego oprogramowania, która nie usuwała wszystkich wpisów, w związku z czym agent systemu *inventory tool* odczytywał oprogramowanie jako nadal zainstalowane. Rozwiązaniem byłby zakup dedykowanego, płatnego rozwiązania po rozpoznaniu rynku. Pełnomocnik wyjaśnił również, że oprogramowanie niewspierane przez producenta, jest odinstalowywane sukcesywnie ze stacji roboczych. Braki kadrowe uniemożliwiają jednak wykonywanie regularnych przeglądów. Wskazane oprogramowanie jako plugin został wyłączony z użytku w kolejnych wersjach przeglądarek internetowych z racji nie wspierania przez producenta. W związku z zakończeniem subskrypcji na oprogramowanie antywirusowe, zakupiono oprogramowanie innego producenta, które na chwilę obecną jest w końcowym etapie wdrożenia. Jedną z jego funkcjonalności jest możliwość wyszukania oprogramowania wycofanego ze wsparcia producenta lub nieaktualnego.

(akta kontroli str. 296-299, 316-324, 334-357, 461-464, 561-624)

b) korzystanie ze starych wersji aplikacji, wymagających aktualizacji.

Pełnomocnik wyjaśnił, że w Urzędzie od 2016 roku jest wdrożony system, który zabezpiecza sieć KPUW i w przypadku wystąpienia zagrożenia generuje stosowne alerty. Dodatkowo ostrzeżenia o zagrożeniach oraz podatnościach są przesyłane przez CSIRT GOV. Po uzyskaniu takiej informacji sprawdzane są wersje oprogramowania pod kątem zagrożenia bezpieczeństwa. W sytuacji wykrycia luki, oprogramowanie podatne jest aktualizowane do najnowszej wersji, bądź w sytuacji braku możliwości aktualizacji, jest odinstalowane. Oprogramowanie systemowe

(systemy operacyjne), pakiety biurowe są aktualizowane na bieżąco pozostałe oprogramowanie jest zaktualizowane sukcesywnie. Na chwilę obecną Urząd jest na etapie wdrożenia nowo zakupionego oprogramowania pozwalającego zweryfikować aktualność zainstalowanego oprogramowania co pozwoli w przyszłości kompleksowo wyszukać oprogramowanie przestarzałe lub niewspierane, które docelowo zostanie zaktualizowane bądź odinstalowane.

(akta kontroli str. 561-624)

c) Zainstalowanie na urządzeniach będącym własnością Urzędu różnego oprogramowania do łączenia się i zarządzania innymi komputerami np. *UltraVNC*, *AnyDesk* oraz *TeamViewer*, które nie były wykazane w przekazanym kontroli spisie licencji.

Pełnomocnik wyjaśnił, że UltraVNC jest oprogramowaniem rozpowszechnianym na licencji GNU GPL, co oznacza, że jest darmowe dla użytku prywatnego jak i komercyjnego. UltraVNC jest wykorzystywane przez pracowników Oddziału Informatyki i Telekomunikacji do łączenia się zdalnie ze stacjami użytkowników w ramach sieci Urzędu. TeamViewer zainstalowany na stacjach roboczych jest wersją klienta, który tylko pozwala połączyć się z daną stacją. Pełnomocnik podał, że jest to wersja, którą instalują w związku z koniecznością świadczenia usługi wsparcia przez firmy, z którymi Urząd posiada umowy a posiadanie licencji na oprogramowanie leży po stronie firmy zewnętrznej. Oprogramowanie AnyDesk zainstalowane jest na komputerach stanowiących wyposażenie stanowisk dyspozytorów medycznych w Dyspozytorni Medycznej w Toruniu i stanowisk wyniesionych w Bydgoszczy. Komputery stanowiskowe Dyspozytorni Medycznej pracują w sieci wydzielonej (zamkniętej) SWD PRM administrowanej centralnie przez administratora w Krajowym Centrum Monitorowania Systemu Państwowego Ratownictwa Medycznego. Niezależnie od powyższego na potrzeby realizacji zadań przez dwóch administratorów wojewódzkich SWD PRM zakupiono dwie licencje na oprogramowanie AnyDesk, które zainstalowane jest na dwóch laptopach i dwóch stacjach desktop zlokalizowanych w pomieszczeniach dyspozytorni medycznej „w budowie” w Bydgoszczy, przy ul. Szubińskiej 4. Ponadto wyjaśnił, że w przekazanych spisach skupiono się przede wszystkim na programach płatnych, za które Urząd musiał ponieść określone koszty.

(akta kontroli str. 561-624)

Skutkiem braku posiadania sprawnego narzędzia do prowadzenia ewidencji licencji oprogramowania był m.in. brak prowadzenia przeglądów oprogramowania i licencji pod kątem kompletności i aktualności tej ewidencji oraz istotne utrudnienie możliwości potwierdzenia, że oprogramowanie, którego licencje wygasły, faktycznie zostało wycofane z użycia.

4. Brak okresowych kontroli (raz na sześć miesięcy) i sporządzania raportów oraz braku egzekwowania tego obowiązku, pomimo zapisów w Polityce obligujących do tego pracowników Urzędu.

Pełnomocnik wyjaśnił, że kontrola dostępu do zasobu, zgodnie z zapisem procedury, była wykonywana na bieżąco, w chwili otrzymania wniosku bądź uzyskania informacji. Brak raportów we wskazanym okresie był spowodowany pandemią COVID-19, co wymusiło konieczność zmiany organizacji pracy Urzędu i przejście na pracę zdalną. Wymusiło to na pracownikach działu IT konieczność skonfigurowania dostępu zdalnego do zasobów oraz monitorowanie pracy użytkowników. W dniu 24 lutego 2022 r. wprowadzono stopień alarmowy Charlie-CRP na terenie całego kraju co spowodowało przesunięcie części pracowników do wykonywania zadań związanych z wprowadzonym stopniem w systemie 24/7. Przełożyło się to na braki kadrowe

uniemożliwiające kompleksowe prowadzenie czynności wskazanych w przedmiotowej procedurze. W związku z tymi zdarzeniami część zespołu była zaangażowana w przygotowanie, obsługę (wielokrotnie wyjazdowych) konferencji, wideokonferencji, co wiązało się z dużymi problemami kadrowymi.

(akta kontroli str. 561-624)

5. Nieuwzględnienie w ustanowionej w Urzędzie procedurze w szczególności zasad dotyczących:

- monitorowania i nadzoru nad stanem użycia i legalności oprogramowania oraz nadzoru nad realizacją procedury związanej z zarządzaniem licencjami, w tym na urządzeniach typu smartfony/tablety;
- zakresu konieczności weryfikacji pod kątem wymagań bezpieczeństwa w ramach nabywania licencji, w tym oprogramowania w modelu SaaS oraz zasad dopuszczania programów do instalacji np. darmowych;
- przechowywania i zabezpieczania dostępu do nośników instalacyjnych, w tym kluczy licencyjnych i innych dokumentów licencyjnych, w tym utrzymywanych w środowiskach chmurowych;
- zasad ewidencjonowania wszystkich posiadanych i używanych licencji, w tym oprogramowania w modelu SaaS, w taki sposób, aby spis zapewniał dostępność aktualnych informacji na temat liczby posiadanych oraz wykorzystywanych licencji dla osób odpowiedzialnych za instalację;
- wycofywania/odinstalowywania (z uwzględnieniem wszystkich rodzajów urządzeń końcowych) licencjonowanego oprogramowania, którego termin ważności licencji się kończy i konieczności użycia właściwego dla danego oprogramowania narzędzia deinstalacji;
- odniesienia do zmian licencyjnych pojawiających się na rynku oprogramowania, np. monitorowania środowiska JAVA.

Pełnomocnik wyjaśnił, że PBI została zaktualizowana w grudniu 2021 r. W związku z pandemią COVID-19, w celu zapobiegania rozprzestrzenianiu choroby, wysyłano pracowników do świadczenia pracy zdalnej, a przy tym zaktualizowano procedury związane z jej świadczeniem. W ramach prac zaktualizowano i uzupełniono pozostałe procedury. Do końca maja 2022 r. Polityka została zaktualizowana²⁶. Kolejnym etapem będzie aktualizacja PBI planowana do końca 2022 r. W ramach prac nad aktualizacją wskazane powyżej zasady zostaną uwzględnione.

(akta kontroli str. 561-624, 635)

6. Nieusunięcie siedmiu kont pracowników z dostępem do systemu informatycznego Urzędu, którzy odeszli z pracy. Analiza wykazała, że siedem osób, które już nie pracują w Urzędzie, mają cały czas aktywne konta użytkowników i dostęp do system informatycznego Urzędu (cztery z 2021 r. i trzy z 2022 r.). Były to trzy osoby, które zostały przeniesione służbowo na podst. art. 64 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej²⁷, w przypadku dwóch osób nastąpiło rozwiązanie umowy o pracę na podstawie art. 53 Kodeksu pracy²⁸, w przypadku jednej osoby upłynął czas umowy, a jedna osoba odeszła z pracy na skutek porozumienia stron.

Pełnomocnik wyjaśnił, że wskazane konta są widoczne w systemie Active Directory, jednak zostały one wyłączone, w związku z powyższym brak jest możliwości zalogowania się użytkownika. ZBI1 wykonuje czynności blokowania/usuwania kont

²⁶ Został z niej usunięty Zespół Bezpieczeństwa Informacji, w związku z uchynieniem zarządzenia Dyrektora Generalnego.

²⁷ Dz. U. z 2022 r., poz. 1691.

²⁸ Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz. U. z 2022 r. poz. 1510 ze zm.

użytkowników na podstawie kart obiegowych, bądź na wniosek dyrektora biura/oddziału/wydziału. W przypadku braku informacji o zmianie/ustaniu stosunku pracy czynność odebrania uprawnień/zamknięcia konta, nie jest wykonywana.

W trakcie trwania kontroli dostęp do tych kont został odebrany.

(akta kontroli str. 495-512, 531-538, 539-543, 552-558)

7. Realizowanie zakupów licencji na oprogramowanie przez WBZK z pominięciem przyjętej w Urzędzie procedury. Zgodnie z PBI w Urzędzie obowiązuje centralizacja zakupów, a pracownicy nie mogą samodzielnie dokonywać zakupu oprogramowania. W latach 2019-2021 WBZK dokonywał zakupów licencji na oprogramowanie samodzielnie z pominięciem OIT.

Dyrektor WBZK wyjaśnił, że kluczowym zadaniem Wydziału jest utrzymanie w stanie gotowości systemów zarządzania sytuacjami kryzysowymi, powiadamiania ratunkowego i ratownictwa medycznego. Podał, że: *Wprawdzie nie dostosowaliśmy się do procedury, ale spowodowane było to „siłą wyższą”. Obecnie realizujemy zamówienia zgodnie z procedurą.*

(akta kontroli str. 4-125, 546-548, 559-560, 649-654, 771-782)

NIK zauważa, że Urząd zobowiązany jest do dokonywania zakupów licencji na oprogramowanie zgodnie z przepisami PBI niezależnie od sytuacji albowiem procedura ta nie przewiduje odstępstw od jej stosowania.

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli wskazuje, że pracownicy Urzędu odpowiedzialni za zarządzanie oprogramowaniem nie posiadali pełnej wiedzy na temat używanego oprogramowania. Wynikało to z faktu, że nie weryfikowano systematycznie wszystkich posiadanych zasobów, nie sporządzano raportów oraz nie badano pod kątem instalowania i korzystania przez pracowników z nielegalnego oprogramowania lub korzystania ze starych wersji aplikacji. Nie prowadzono monitoringu urządzeń typu smartfon czy tablet. W Urzędzie posiadano ograniczoną zdolność do sprawowania nadzoru nad procesem związanym z zarządzaniem licencjami. Pomagały w tym wprowadzone procedury zebrane w Polityce jednak wymagała ona uzupełnienia. Nie znalazły się w niej zapisy dotyczące m.in.: monitorowania i nadzoru nad stanem użycia i legalności oprogramowania, zarządzania licencjami na oprogramowanie, weryfikacji pod kątem bezpieczeństwa nabywanych licencji, w tym oprogramowania w modelu SaaS²⁹, dopuszczania do instalacji programów darmowych, ewidencjonowania wszelkich posiadanych i używanych licencji, w tym oprogramowania w modelu SaaS, wycofywania/odinstalowywania oprogramowania, którego termin ważności się kończy. Ponadto nie usunięto wszystkich kont pracowników, którzy odeszli już z pracy w Urzędzie oraz realizowano zakupy licencji z pominięciem przyjętej w Urzędzie procedury.

OBSZAR

2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem

Opis stanu faktycznego

2.1. W latach 2019-2021, na koniec każdego roku komórki organizacyjne Urzędu składały do BFI *Plan zapotrzebowania* na kolejny rok budżetowy, w ramach którego określały swoje potrzeby. Na podstawie złożonych zapotrzebowań oraz środków

²⁹ SaaS - Oprogramowanie jako usługa (Software as a Service) to model udostępniania oprogramowania w chmurze, w którym dostawca chmury rozwija i utrzymuje aplikacje chmurowe, zapewnia ich automatyczne aktualizacje i udostępnia oprogramowanie swoim klientom za pośrednictwem Internetu na zasadzie „pay-as-you-go”, czyli w zależności od wykorzystania zasobów.

ujętych w *Planie finansowym* danego rozdziału, sporządzany był *Plan postępowań o udzielenie zamówienia publicznego*, który następnie publikowano na stronie BIP. W *Planie postępowań o udzielenie zamówienia publicznego* ujmowano tylko te zakupy, na które zostanie ogłoszony przetarg w trybie podstawowym. Pozostałe zakupy realizowane były sukcesywnie, w ramach posiadanych możliwości finansowych Urzędu oraz wydziałów, w trybach pozaustawowych czyli tzw. zamówieniach klasycznych, których wartość zamówienia jest równa lub przekracza kwotę 130 000 zł. Zakupy realizowano tylko na niezbędne oprogramowanie. Nie zidentyfikowano oprogramowania, które nie zostało zainstalowane.

Zgodnie z Regulaminem udzielania zamówień publicznych w KPUW weryfikacji potrzeb wydziałów w zakresie asortymentu informatycznego dokonywał ZBII. Wicewojewoda wyjaśnił, że dzięki oszczędnościom, powstałym po prowadzonych postępowaniach przetargowych, w związku z niższą kwotą oferty czy też rezygnacji z realizacji niektórych zadań, możliwe było dokonanie dalszych zakupów zgodnie z zapotrzebowaniem Urzędu.

(akta kontroli str. 450-464)

Na przeprowadzone w Urzędzie w okresie objętym kontrolą 64 postępowania dotyczące nabycia oprogramowania na łączną kwotę 2 424,3 tys. zł, w czterech przypadkach przeprowadzone było postępowanie o udzielenie zamówienia publicznego w formie przetargu nieograniczonego³⁰. Pozostałe postępowania były poniżej ustawowego progu.

W okresie objętym kontrolą Urząd nie został obciążony przez producentów dodatkowymi fakturami za nadmierne korzystanie z licencji.

(akta kontroli str. 450-464, 792-793)

2.2. W okresie objętym kontrolą w Urzędzie nie dokonywano analiz efektywności posiadanego oprogramowania. Wdrożono natomiast system Microsoft Active Directory³¹, który umożliwia użytkownikom zalogowanie się i korzystanie z zainstalowanego oprogramowania na każdym sprzęcie komputerowym, będącym w zarządzaniu przez serwery Active Directory.

W sytuacji zgłaszania problemów przez użytkowników przekazywane są one w utworzonym systemie Helpdesk lub co jest podstawą do podejmowania odpowiednich czynności przez OIT, który w ramach zakresu działania rozwiązuje zgłaszane usterki. Zgłoszenia z komórek Urzędu dotyczą głównie oprogramowania Microsoft (systemy operacyjne, pakiety biurowe), systemu obiegu dokumentów *Edok*, z którym wiążą się min. problemy z aplikacją, codziennym użytkowaniem oraz modyfikacją funkcjonalności, uprawnień, integracją z systemem Epuap, certyfikatami.

Pełnomocnik wyjaśnił, że problemy z systemem obiegu dokumentów *Edok* były rozwiązywane samodzielnie przez dział IT Urzędu lub w konsultacji z Centralnym Ośrodkiem Informatyki (COI), który jest dostawcą oprogramowania gdzie problemy zgłasza się na dedykowanej platformie *Atmosfera*. Kolejnymi problemami z jakimi dział IT zmagał się w codziennej pracy były problemy ze środowiskiem serwerowym oraz sieciowym (zarządzalne przełączniki sieciowe, macierze dyskowe, serwery, serwery NAS). Wskazane powyżej problemy były rozwiązywane przez dział IT lub

³⁰ Zakup systemu Backup za kwotę 365 592,90 zł, serwera NTT – system druku podążającego za kwotę 91 488,63 zł, systemu filtrowania poczty e-mail za kwotę 194 910,72 zł, systemu bezpieczeństwa Firewall za kwotę 284 956,56 zł. Komórką składającą zapotrzebowanie było ZBII.

³¹ System ten zarządza centralnie m.in. poświadczeniami użytkowników, co daje możliwość wykorzystania własnych poświadczeń na każdej stacji roboczej, zarządzanej przez system. Dzięki temu, każdy użytkownik ww. systemu może skorzystać z oprogramowania zainstalowanego na innej stacji roboczej.

w ramach bezpłatnego wsparcia w związku zakupionymi rozwiązaniami informatycznymi.

(akta kontroli str.628-635)

Wojewoda Kujawsko-Pomorski w latach:

- 2017-2018 był beneficjentem projektu nr 15/7-2017/OG-FAMI pn. „Wzmocnienie zdolności administracyjnych Wojewody Kujawsko-Pomorskiego w procesie integracji obywateli państw trzecich” dofinansowywanego ze środków Funduszu Azylu, Migracji i Integracji³². W ramach projektu zostały nabyte: 27 licencji, infokiosk wraz z oprogramowaniem, cztery routery oraz dwa notebooki wraz z oprogramowaniem.

Zakupione w ramach FAMI oprogramowanie jest wykorzystywane w zakresie zadań realizowanych przez Wojewodę zgodnie z projektem. Z notebooków korzystają członkowie Zespołu. Pozostałe oprogramowania wykorzystywane są przez WSOC do obsługi cudzoziemców.

- 2017-2018 był beneficjentem projektu nr 8/8-2017/OG-FAMI pn. „Masz prawo wiedzieć” dofinansowywanego ze środków FAMI. W ramach projektu zostało nabyte jedno oprogramowanie Microsoft Office, które jest wykorzystywane zgodnie z projektem przez WPS.

- 2019-2021 był beneficjentem projektu nr 1/10-2019/OG- FAMI „Wzmocnienie zdolności administracyjnych Wojewody Kujawsko- Pomorskiego w procesie integracji obywateli państw trzecich- etap II” dofinansowywanego ze środków FAMI. W ramach projektu zostało nabyte 20 licencji, system kolejowania, dwa serwery, system filtrowania poczty, system bezpieczeństwa Firewall, system druku podążającego oraz 10 notebooków łącznie z oprogramowaniem. Zakupione w ramach FAMI oprogramowanie jest wykorzystywane zgodnie z projektem, przez WSO i do obsługi cudzoziemców.

(akta kontroli str. 450-464)

2.3. W latach 2019-2022 (do 30 czerwca 2022 r.) Urząd poniósł wydatki w związku z nabyciem i korzystaniem z oprogramowania komputerowego w łącznej kwocie 2 423,3 tys. zł, z tego w:

- 2019 r. – 480, 7 tys. zł na zakup 119 sztuk oprogramowania i licencji³³ na podstawie zapotrzebowań złożonych przez Wydział Polityki Społecznej, ZBII, WBZK, Biuro Kadrowo-Organizacyjne³⁴, Wydział Zdrowia oraz Wydział Koordynacji Świadczeń³⁵;

- 2020 r. – 1 614,7 tys. zł za zakup 94 szt. oprogramowania i licencji³⁶ na podstawie zapotrzebowań złożonych przez Wydział Spraw Obywatelskich i Cudzoziemców, Państwową Straż Łowiecką³⁷, Biuro Wojewody³⁸, ZBII, WBZK, BKO i WKS;

- 2021 r. – 302,9 tys. zł za zakup 277 szt. oprogramowania i licencji³⁹ na podstawie zapotrzebowań złożonych przez Wydział Polityki Społecznej⁴⁰, WBZK, ZBII, PSL, BKO i BFI;

- 2022 r. – 12,8 tys. zł za zakup 39 szt. oprogramowania i licencji⁴¹ zakupionych na podstawie złożonych zapotrzebowań przez WBZK, BKO i BW.

³² Dalej: „FAMI”.

³³ W tym 47 szt. zestawów do składania podpisu kwalifikowalnego.

³⁴ Dalej: „BKO”.

³⁵ Dalej: „WKS”.

³⁶ W tym 38 szt. zestawów do składania podpisu kwalifikowalnego.

³⁷ Dalej: „PSL”.

³⁸ Dalej: BW”.

³⁹ W tym 60 szt. zestawów do składania podpisu kwalifikowalnego.

⁴⁰ Dalej: „WPS”.

⁴¹ W tym 27 szt. zestawów do składania podpisu kwalifikowalnego.

W latach 2019-2022 wartość sprzętu zakupionego łącznie z oprogramowaniem wynosiła 1 308,1 tys. zł. Urząd nabył 220 szt. takich zestawów.

Ponoszone przez KPUW wydatki dotyczące zakupu licencji czy oprogramowania komputerowego ujmowane były w systemie Finansowo-Księgowym Księgowość Budżetowa na podstawie faktur VAT. Wicewojewoda wyjaśnił, że system ten służy do prowadzenia ksiąg rachunkowych Urzędu, a nie do zarządzania licencjami. W BFI prowadzona była elektroniczna ewidencja środków trwałych, w której ujmowane były poszczególne składniki zakupionego asortymentu, w tym również wartości niematerialne i prawne, jednak nie można uznać tego rejestru za rejestr licencji.

Podał również, że każdy Wydział prowadzi księgi inwentarzowe, w których ujmuje składniki majątku będące w jego dyspozycji.

(akta kontroli str. 450-457, 789-791)

Stwierdzone
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli pozytywnie ocenia dokonywanie zakupu wyłącznie niezbędnych i wykorzystywanych programów komputerowych, jednakże zauważa, że nierzetelnie prowadzenie spisów licencji było m.in. przeszkodą do ustalenia stanu wolnego oprogramowania.

IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące uwagi i wnioski:

Uwagi

NIK nie formułuje uwag.

Wnioski

1. Wdrożenie szczegółowych zasad zarządzaniem oprogramowaniem i jego licencjami.
2. Wdrożenie narzędzia umożliwiającego stworzenie pełnej ewidencji oprogramowania i jego licencji.
3. Objęcie regularnym monitorowaniem całego oprogramowania, w tym instalowanego na urządzeniach mobilnych, dokumentowanie podejmowanych czynności, w tym działań naprawczych.
4. Realizowanie zakupów oprogramowania komputerowego zgodnie z zapisami PBI.
5. Niezwłoczne usuwanie kont dostępowych do systemu informatycznego Urzędu pracowników, którzy odeszli z pracy.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia
zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Bydgoszczy. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

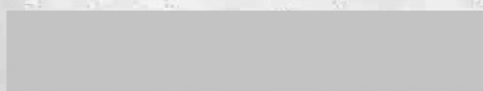
Obowiązek
poinformowania
NIK o sposobie
wykonania
wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Bydgoszcz, 27 października 2022 r.

Kontroler
Elżbieta Warda-Fereniec
główny specjalista kontroli państwowej



.....
podpis

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy
p.o. Dyrektor
Tomasz Sobecki



.....
podpis