NAJWYŻSZA IZBA KONTROLI
Delegatura w Rzeszowie

LRZ.410.020.04.2022

Robert Bugaj
Dyrektor
Podkarpackiego Oddziału Wojewódzkiego
Narodowego Funduszu Zdrowia
z siedzibą w Rzeszowie
ul. Zamkowa 8, 35-032 Rzeszów

WYSTĄPIENIE POKONTROLNE

P/22/082 Zarządzanie oprogramowaniem komputerowym przez administrację publiczną

NAJWYŻSZA IZBA KONTROLI
Delegatura w Rzeszowie
ul. Kraszewskiego 8, 35-016 Rzeszów
T +48 17 780 23 00, F +48 17 780 23 06
lrz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Podkarpacki Oddział Wojewódzki Narodowego Funduszu Zdrowia z siedzibą w Rzeszowie[1],

35-032 Rzeszów, ul. Zamkowa 8.

Kierownik jednostki kontrolowanej

Robert Bugaj, dyrektor POW NFZ od 4 lipca 2016 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, 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[2].

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Rzeszowie

Kontroler

1. Edyta Niegowska-Buko, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LRZ/108/2022 z 7 lipca 2022 r.

(akta kontroli Tom I str.1-3)

[1] Dalej: POW NFZ lub Oddział
[2] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W ocenie Najwyższej Izby Kontroli POW NFZ podejmował działania w celu zapewnienia właściwego zarządzania oprogramowaniem, niemniej jednak nie zawsze były one skuteczne.

Uzasadnienie oceny ogólnej

W Oddziale obowiązywały zasady zarządzania oprogramowaniem opracowane w Centrali NFZ. Nie zawierały one jednak szczegółowych uregulowań obejmujących m.in.: przechowywanie nośników i kluczy licencyjnych, monitorowania używanego oprogramowania pod względem zgodności z posiadanymi licencjami, identyfikacji nieautoryzowanego oprogramowania, nabywania i wykorzystywania programów typu SaaS.

Zadania z zakresu zarządzania oprogramowaniem wykonywali wyznaczeni pracownicy Wydziału Informatyki.

Prowadzone w Oddziale wykazy licencji nie były kompletne, a posiadane narzędzia do monitorowania oprogramowania nie były wykorzystywane do regularnego skanowania całego oprogramowania. Monitoringiem oprogramowania nie objęto służbowych telefonów komórkowych, na podstawie wewnętrznych uregulowań NFZ. W POW NFZ nie wykonywano audytów zasobów IT, w tym pod kątem wykrycia nieautoryzowanego oprogramowania.

W toku kontroli stwierdzono przypadki użycia niedozwolonego w NFZ oprogramowania (darmowe do użytku prywatnego, domowego) oraz przypadki instalacji wersji określonej jako EOL[4].

W Oddziale były zainstalowane systemy operacyjne w różnych wersjach, w tym EOL oraz różne wersje tych samych programów ponieważ nie prowadzono bieżącej ich aktualizacji.

W procesie nabywania oprogramowania uwzględniane były faktyczne potrzeby Oddziału, które weryfikowano i oceniano pod kątem zasadności/celowości wykorzystania oprogramowania, przy jednoczesnym uwzględnieniu możliwości finansowych. W jednym przypadku nie odnowiono wsparcia dla oprogramowania NetSupport Notify po 31 maja 2022 r.

Nabywane w POW NFZ oprogramowanie typu SaaS nie było weryfikowane pod katem spełnienia wymogów bezpieczeństwa i poufności danych ani oceny wiarygodności dostawcy i zapewnienia wsparcia technicznego. Były to jednak programy wykorzystywane już w Centrali NFZ i innych oddziałach lub takie, które Oddział użytkował wcześniej.

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[4] End of life. Dalej: EOL

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym.

Opis stanu faktycznego

1.1 Zgodnie z Regulaminem Organizacyjnym POW NFZ[6] za prowadzenie spraw związanych z budową, utrzymaniem i rozwojem systemów informatycznych i infrastruktury teleinformatycznej odpowiadał Wydział Informatyki, w którego skład wchodzą: Sekcja Aplikacji i Sekcja Eksploatacji i Infrastruktury[7] Bezpośredni nadzór nad WI-E sprawuje Dyrektor POW NFZ. Do zadań Sekcji Aplikacji należy zarządzanie i administrowanie bazami danych w zakresie Systemu Informatycznego Wspomagania Działalności Narodowego Funduszu Zdrowia[8]. Zapewnia ona głównie nadzór nad prawidłowym działaniem obsługiwanych elementów SIWD NFZ, wsparcie techniczne dla użytkowników wewnętrznych w zakresie poszczególnych modułów tego systemu oraz dla użytkowników zewnętrznych portali NFZ w tym obszarze.
Do zadań WI-E należy, m.in.:
- planowanie finansowe i rzeczowe dla obszaru technologii informatycznych;
- zapewnienie infrastruktury serwerowej, sieciowe oraz stacji roboczych i urządzeń peryferyjnych;
- zapewnienie budowy, utrzymania i rozwoju dedykowanych systemów informatycznych wspierających pracę POW NFZ;
- zapewnienie utrzymania i rozwoju systemów standardowych wspierających pracę Oddziału;
- zarządzanie, realizacja i nadzór nad umowami w obszarze technologii informatycznych;
- współpraca w zakresie prowadzenia i zarządzania programami i projektami informatycznymi;
- udział w postępowaniu o udzielenie zamówień publicznych w zakresie zadań Wydziału;
- współpraca z dostawcami sprzętu i systemów teleinformatycznych, a także operatorami telekomunikacyjnymi świadczącymi usługi dla Oddziału;
- realizacja wsparcia technicznego dla użytkowników (wewnętrznych i zewnętrznych) systemów informatycznych NFZ;
- administrowanie aplikacją kancelaryjną elektronicznego obiegu dokumentów Oddziału.

(akta kontroli Tom I str.4-90)

Zarządzeniem Nr 17/2017/GPF Prezesa Narodowego Funduszu Zdrowia z dnia 9 marca 2017 r.[9] wprowadzony został w NFZ Zintegrowany System Zarządzania[10], którego wdrożenie realizowane jest na podstawie Polityki Zintegrowanego Systemu Zarządzania[11] określającej zasady zarządzania bezpieczeństwem informacji, zgodnie

[5] 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.
[6] Zarządzenie Nr 87/2022/WO Dyrektora POW NFZ z dnia 29 kwietnia 2022 r. w sprawie nadania Regulaminu Organizacyjnego POW NFZ z siedzibą w Rzeszowie. Wcześniej obowiązywały Zarządzenia: Nr 2/2021/WO z 5 stycznia 2021 r., Nr 86/2020 z 1 października 2020 r., Nr 251/2019 z 16 grudnia 2019 r., Nr 112/2019 z 17 czerwca 2019 r., Nr 27/2019 z dnia 1 lutego 2019 r. oraz Nr 139/2018 z dnia 25 maja 2018 r.
[7] Dalej: WI-E.
[8] Dalej: SIWD NFZ lub system dziedzinowy. Główne oprogramowanie do wykonywania statutowych obowiązków NFZ, zakupione centralnie dla wszystkich oddziałów NFZ.
[9] Zarządzenie Nr 17/2017/GPF Prezesa NFZ z dnia 9 marca 2017 r. w sprawie wdrożenia Zintegrowanego Systemu Zarządzania w Narodowym Funduszu Zdrowia.
[10] Dalej: ZSZ.
[11] Dalej: Polityka ZSZ.

z normą ISO/IEC 27001:2014 oraz zarządzania ciągłością działania zgodnie z normą ISO/IEC 22301:2012.

Polityka ZSZ odnosi się do polityk dziedzinowych, gdzie w obszarze zarządzania oprogramowaniem zdefiniowano dokument PZSZ/014 *Polityka zarządzania bezpieczeństwem teleinformatycznym w NFZ*[12]*,* określająca minimalne wymagania w zakresie zarządzania bezpieczeństwem teleinformatycznym w NFZ.

Zgodnie z § 44 PZSZ/014 w NFZ może być używane wyłącznie oprogramowanie licencjonowane zgodnie z udzielonymi w licencji prawami, a dla każdego podsystemu teleinformatycznego w jednostce organizacyjnej NFZ prowadzić należy ewidencję posiadanych zainstalowanych licencji na wykorzystywane oprogramowanie. Sposób ewidencji licencji ma natomiast umożliwiać wykonanie audytu faktycznie zainstalowanego lub użytkowanego oprogramowania. Eksploatowane oprogramowanie powinno być chronione przed nieautoryzowana modyfikacją, nieuprawnionym usunięciem oraz kopiowaniem.
Za zarządzanie zmianami w środowisku IT odpowiadają administratorzy poszczególnych podsystemów oraz komponentów systemu. Całość uregulowana jest w ramach PZSZ/014-07 Procedury zarządzania zmianą w systemie teleinformatycznym NFZ. Procedura ta pokrywa zmiany kluczowe, standardowe i drobne.
Zgodnie z § 9 ust. 2, 3 i 4 PZSZ/014-07 Administrator systemu zobowiązany jest do śledzenia aktualności związanych z wydawanymi aktualizacjami do administrowanych przez siebie systemów. Źródłami informacji w tym zakresie są w szczególności strony internetowe producenta oraz dedykowane portale branżowe. Każdorazowo Administrator systemu zobowiązany jest do przeanalizowania informacji o poprawce i dokonania oceny jej przydatności.

Powyższe regulacje i procedury eksploatacyjne administratorów odnoszą się do szeregu zasad w obszarze bezpieczeństwa informacji, natomiast nie definiują zarządzania oprogramowaniem w obrębie całego cyklu jego życia, w tym zasad: nabywania oprogramowania uwzględniających kryteria weryfikacji pod kątem bezpieczeństwa, przechowywania i zabezpieczania dostępu do nośników instalacyjnych, kluczy licencyjnych, dystrybucji i redystrybucji, monitorowania stanu użycia i legalności, dokonywania cyklicznego skanowania środowiska IT i dokonywania przeglądów oraz wycofywania licencji i odinstalowania oprogramowania z urządzeń.

W POW NFZ w ramach Polityki ZSZ obowiązywały m.in. dokumenty:

- PZSZ/009 – *Podstawowe zasady bezpieczeństwa w NFZ*, określają podstawowe zasady zapewniające bezpieczeństwo aktywów informacyjnych, właściwe postępowanie z nośnikami danych, zarządzanie incydentami, korzystanie ze sprzętu poza siedzibą NFZ oraz ochronę za pomocą środków kryptograficznych;

- PZSZ/011 – *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w NFZ*, określają zasady bezpieczeństwa w obszarze zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w NFZ.

W ramach regulacji wewnętrznych Dyrektor POW NFZ w zakresie użytkowania i bieżącego nadzoru nad urządzeniami mobilnymi oraz w zakresie użytkowania telefonów komórkowych wprowadził:

[12] Dalej: PZSZ/014.

- Zarządzeniem Nr 104/2019 Dyrektora POW NFZ z dnia 31 maja 2019 r. Podstawowe zasady bezpieczeństwa urządzeń mobilnych i komputerów przenośnych użytkowanych w POW NFZ z siedzibą w Rzeszowie[13];
- Zarządzeniem Nr 45/2019 Dyrektora POW NFZ z dnia 26 lutego 2019 r. Podstawowe zasady bezpieczeństwa służbowych telefonów komórkowych użytkowanych w POW NFZ z siedzibą w Rzeszowie.

W Podstawowych zasadach bezpieczeństwa urządzeń mobilnych określono odpowiedzialność Naczelnika Wydziału Informatyki za:
- organizację dystrybucji urządzeń mobilnych do pracowników POW NFZ,
- prowadzenie wydzielonej ewidencji urządzeń mobilnych,
- odpowiednią konfigurację zgodnie z Zarządzeniem Prezesa NFZ nr 17/2017/GPF z dnia 9 marca 2017 r. w sprawie wdrożenia Zintegrowanego Systemu Zarządzania w Narodowym Funduszu Zdrowia - Polityką zarządzania bezpieczeństwem teleinformatycznym NFZ (PZSZ/014).

Decyzją Prezesa NFZ z dniem 27 września 2021 r. w NFZ zostało wprowadzone Odstępstwo od zapisów w dokumentacji Systemu Zarządzania Bezpieczeństwem w zakresie wdrożenia odpowiednich zasad organizacyjnych i środków technicznych w procesie zarządzania urządzeniami mobilnymi. Wynikało ono z prac nad wdrożeniem w NFZ odpowiednich zasad organizacyjnych i środków technicznych w procesie zarządzania urządzeniami mobilnymi, w tym: wdrożeniem systemu do zarządzania urządzeniami mobilnymi klasy MDM oraz opracowaniem Polityki zarządzania urządzeniami mobilnymi. Odstępstwo obowiązuje do czasu zakończenia ww. prac i zostanie zniesione w drodze decyzji Dyrektora Biura Bezpieczeństwa Informacji i Ciągłości Działania.

W zakresie nabywania oprogramowania, planowania budżetu, jego zatwierdzania i realizacji w POW NFZ obowiązywały:
- Regulamin tworzenia rzeczowego planu wydatków inwestycyjnych Narodowego Funduszu Zdrowia, jego zatwierdzania i dokonywania zmian w trakcie jego realizacji[14];
- Regulamin udzielania zamówień publicznych w Narodowym Funduszu Zdrowia[15].

W NFZ wprowadzono *Zasady gospodarowania zbędnymi/zużytymi składnikami majątkowymi w Narodowym Funduszu Zdrowia* oraz *Zasady likwidacji zużytych składników majątkowych w NFZ*[16].

W POW NFZ nie było określonego katalogu oprogramowania dopuszczonego do instalowania na stacjach roboczych. W ramach polityki dziedzinowej PZSZ/014 Polityka zarządzania bezpieczeństwem teleinformatycznym w NFZ utworzona została jedynie lista oprogramowania kryptograficznego dla całego NFZ.

(akta kontroli str. Tom I str. 91-559)

Obowiązujące w Oddziale zasady nie ustanawiały istotnych mechanizmów kontrolnych, koniecznych do zapewnienia skutecznego i efektywnego zarządzania

[13] Dalej: Podstawowe zasady bezpieczeństwa urządzeń mobilnych.

[14] Zarządzenie Nr 26/2015/BAG Prezesa NFZ z dnia 27 maja 2015 r. w sprawie Regulaminu tworzenia rzeczowego planu wydatków inwestycyjnych Narodowego Funduszu Zdrowia, jego zatwierdzania i dokonywania zmian w trakcie jego realizacji. Dalej: Zarządzenie Prezesa NFZ w sprawie Regulaminu tworzenia rzeczowego planu wydatków.

[15] Zarządzenie Nr 85/2022/BAG Prezesa NFZ z dnia 8 lipca 2022 r. w sprawie wprowadzenia w NFZ regulaminu udzielania zamówień publicznych oraz regulaminu prac komisji przetargowych. Poprzednio obowiązywały: Zarządzenie Nr 127/2021/BAG z dnia 2 lipca 2021 r., Dalej: Zarządzenie Prezesa NFZ w sprawie wprowadzenia regulaminu udzielania zamówień publicznych; Nr 115/2020/BAG z dnia 24 lipca 2020 r., Nr 35/2015/BAG z dnia 1 lipca 2015 r., ze zm.

[16] Zarządzeniem Nr 45/2015/BAG Prezesa NFZ z dnia 7 sierpnia 2015 r. w sprawie zasad gospodarowania składnikami majątkowymi w NFZ. Dalej: Zarządzenie w sprawie zasad gospodarowania składnikami majątkowymi w NFZ.

oprogramowaniem i licencjami, o czym o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

Wydział Informatyki nie identyfikował żadnych ryzyk w obszarze zarządzania oprogramowaniem, w związku z tym nie zgłaszał ich Kierownictwu. Nie identyfikowano również potrzeb w zakresie zakupu i wdrożenia nowego oprogramowania wspierającego proces zarządzania oprogramowaniem i licencjami.

(akta kontroli Tom I 399-402, 405-423, Tom II str. 1-61)

1.2 Zadania dotyczące zarządzania licencjami i oprogramowaniem znajdują się w zakresie działalności WI-E.
W okresie objętym kontrolą w WI-E łącznie z Naczelnikiem zatrudnionych było 5 osób[17]. Pracownikom tym w Rejestrze Podsystemów Teleinformatycznych w POW NFZ przypisano role administratorów poszczególnych systemów teleinformatycznych[18]. W zakresach czynności wskazano osoby zastępujące[19], przypisano realizację zadań określonych w szczególności w Polityce zarządzania bezpieczeństwem teleinformatycznym w NFZ (PZSZ/014) oraz określono główne zadania na stanowiskach administratorów, w tym m.in.: koordynację prac związaną z zapewnieniem działania i bezpieczeństwa systemu, doraźną weryfikację uprawnień, zarządzanie hasłami, prowadzenie dzienników administracyjnych, monitorowanie zdarzeń systemowych i usług, okresową weryfikację aktywności kont, tworzenie i aktualizowanie dokumentacji eksploatacyjnej dla systemów oraz tworzenie analiz, raportów w zakresie administrowanych systemów.
Naczelnik WI wyjaśnił, że w POW NFZ nie określono częstotliwości realizacji przez daną osobę konkretnej czynności w zakresie zarządzania licencjami i oprogramowaniem, ale administratorzy systemów na bieżąco monitorują i weryfikują systemy oraz oprogramowanie, którym zarządzają.

W Oddziale nie określono wprost odpowiedzialności za weryfikację umów licencyjnych i utrzymanie zgodności z przepisami praw autorskich i praw pokrewnych na wszystkich zasobach sprzętowych.

(akta kontroli str. Tom II str.1- 61, 399-402)

WI-E w zakresie zarządzania oprogramowaniem telefonów komórkowych dokonuje jedynie pierwszego uruchomienia, wstępnej konfiguracji i aktualizacji oraz realizuje zadania w przypadku awarii urządzenia. Ewidencja i gospodarka prowadzona jest w Wydziale Administracyjno-Gospodarczym POW NFZ. Umowy w zakresie telefonii komórkowej realizowane są w Centrali NFZ.

W POW NFZ nie ma wdrożonego systemu zarządzania i monitorowania oprogramowania na telefonach służbowych.

Dyrektor POW NFZ wyjaśnił, że w Centrali NFZ trwają prace nad wdrożeniem odpowiednich zasad organizacyjnych i środków technicznych w procesie zarządzania urządzeniami mobilnymi, w tym: wdrożeniem systemu do zarządzania urządzeniami mobilnymi klasy MDM oraz opracowaniem Polityki zarządzania urządzeniami.

[17] W związku z przejściem jednego pracownika na emeryturę w okresie od 1 lutego2022 r. do 28 lutego 2022 r. zatrudnione były 4 osoby.

[18] Zarządzenie Nr 71/2019 Dyrektora POW NFZ z dnia 1 kwietnia 2019 r. w sprawie wprowadzenia dokumentu pt.: „Rejestr Podsystemów Teleinformatycznych, Rejestr Komponentów Teleinformatycznych oraz Dzienniki Administracyjne Podsystemów w Podkarpackim Oddziale Wojewódzkim Narodowego Funduszu Zdrowia z siedzibą w Rzeszowie" ze zm. wprowadzonymi Zarządzeniem Nr 2/2020 Dyrektora POW NFZ z dnia 3 stycznia 2020 r. oraz Zarządzeniem Nr 183/2022/WI Dyrektora POW NFZ z dnia 19 lipca 2022 r.

[19] W przypadku Naczelnika Wydziału w zakresie czynności zapisano, że zastępstwo pełni wyznaczona przez niego osoba lub osoba wskazana jako drugi administrator danego podsystemu teleinformatycznego. Wskazanie osoby zastępującej następuje również w formie pisemnej na wniosku urlopowym.

(akta kontroli Tom II str.62-67)

W latach 2019-2022 (I półrocze) wszyscy pracownicy WI-E odbywali szkolenia z zakresu realizowanych przez nich zadań, w tym dotyczących systemów teleinformatycznych.
W okresie objętym kontrolą pracownicy WI-E odbyli łącznie 33 szkolenia, w tym 10 szkoleń płatnych, na które wydatkowano 3 653 zł, z tego:
- w 2019 r. – 14 szkoleń[20], w tym 5 płatnych, na które wydatkowano 1 985 zł;
- w 2020 r. – 8 szkoleń[21], w tym 2 płatne, na które wydatkowano 710 zł;
- w 2021 r. – 7 szkoleń[22], w tym 3 płatne, na które wydatkowano 958 zł;
- w 2022 r. (I półrocze) - 4 szkolenia[23] - wszystkie bezpłatne.

Szkolenia te nie obejmowały zagadnień dotyczących zarządzania licencjami komputerowymi.
Naczelnik WI-E wyjaśnił, że pracownicy WI nie brali udziału w szkoleniach w zakresie zarządzania licencjami i oprogramowaniem, gdyż zakupem większości systemów zajmuje się Centrala NFZ. Podkarpacki Oddział NFZ kupuje jedynie pojedyncze oprogramowanie narzędziowe i zabezpieczające.

(akta kontroli Tom II str.68-88, 399-402)

W latach 2019-2022 POW NFZ nie korzystał z outsourcingu w zakresie audytu oprogramowania. Nie planował i nie planuje zewnętrznej usługi w tym zakresie.

(akta kontroli str. Tom II str.1-2)

1.3 POW NFZ nie posiada globalnego repozytorium licencji i oprogramowania. Spis posiadanych licencji prowadzony był w module Systemu Informatycznego NFZ Środki Trwałe. Od 2019 r. w Rejestrze komponentów aplikacyjnych ujęta była część oprogramowania na serwerach. Nie wykazywano w nim oprogramowania, które nie było objęte licencjonowaniem, darmowego lub dostarczonego wraz z nabywanym sprzętem komputerowym. Dodatkowo administratorzy poszczególnych systemów prowadzili rejestry zawierające informacje o przydzielonych użytkownikom licencjach zakupionych wraz ze sprzętem.

W POW NFZ nie prowadzono spisu całego oprogramowania, w tym subskrypcji czy oprogramowania chmurowego. Rejestry nie zawierały również dat wygaśnięcia licencji, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli Tom II str.90-195)

W okresie od 2019 r. do lutego 2022 r. w POW NFZ użytkowane było darmowe oprogramowanie typu inventory tool, tj. Open Computer and Software Inventory Next Generation (OCS Inventory NG). System wykorzystywany był do bieżącego monitorowania oprogramowania oraz zasobów na stacjach roboczych. Nie były sporządzane okresowe przekrojowe raporty z oprogramowania[24].
W lutym 2022 r. w POW NFZ wdrożony został Microsoft System Center Configuration Manager (SCCM) posiadający m.in. funkcję inwentaryzacji i bieżącego monitorowania oprogramowani na stacjach[25]. Oddział nie ponosił kosztów wdrożenia, gdyż system zainstalowano w ramach posiadanej przez NFZ subskrypcji Miscrosoft M365 E3[26]. W okresie tym nie były wykonywane ani przechowywane okresowe przekrojowe raporty w zakresie oprogramowania.
Oddział posiadał również oprogramowanie NetCrunch, które wykorzystywał jedynie do monitorowania sieci pod kątem wydajności i dostępności urządzeń sieciowych

[20] W szkoleniach uczestniczyło od 1 do 2 pracowników WI-E.
[21] W szkoleniach uczestniczyło od 1 do 5 pracowników WI-E.
[22] W szkoleniach uczestniczyło od 1 do 2 pracowników WI-E.
[23] W szkoleniach uczestniczyło od 1 do 2 pracowników WI-E.
[24] Zachowany został dostęp do częściowych danych archiwalnych (raporty zasobów stacji).
[25] Funkcjonuje w obrębie systemów Microsoft.
[26] Umowa 154/2019 zawarta przez Centralę NFZ w dniu 31 grudnia 2019 r.

i serwerów. W latach 2019-2022 (30 czerwca) koszty użytkowania oprogramowania wynosiły 25,98 tys. zł.
Dane w spisach POW NFZ nie umożliwiały uzyskania informacji odnośnie daty wygaśnięcia licencji.

Kierownik WI wyjaśnił, że: Oddział zamierza uzupełnić w Rejestrze komponentów aplikacyjnych również o dane dotyczące daty wygaśnięcia licencji.

Wykorzystywane w POW NFZ programy SCCM i NetCrunch również nie zawierały pełnej informacji, co do posiadanych licencji.
NetCrunch umożliwia po wprowadzeniu pełnych informacji odnoszących się do posiadanych licencji bieżące i w sposób zautomatyzowany monitorowanie czy liczba posiadanych licencji jest odpowiednia dla zainstalowanego oprogramowania, które jest wykorzystywane w Oddziale.
Kierownik WI wyjaśnił, że ze względu na liczbę licencji, Netcrunch nie jest wykorzystywany do monitorowania stacji roboczych, a jedynie do monitorowania urządzeń sieciowych (przełączniki sieciowe, routery itp.) i serwerów. Do monitorowania stacji roboczych wykorzystywany jest SCCM.

(akta kontroli Tom II str.90-92, 194-204)

W POW NFZ nie dokonywano przeniesienia licencji między użytkownikami/stanowiskami i nie uwzględniano tego w spisie. Licencje przypisywano do urządzenia, wgrywając oprogramowanie z obrazu, który zawierał wszystkie wymagane do pracy programy. Urządzenia IT przypisywano do Wydziałów. Odejście pracownika lub zmiana stanowiska wynikająca z przeniesienia do innej komórki organizacyjnej było zgłaszane do WI w celu zagospodarowania sprzętu. Komputer w zależności od uzgodnień WI z kierownikami komórki, z której pracownik odchodził albo pozostawał w tym wydziale, albo był przekazywany do WI. Licencja pozostawała na komputerze.

Kierownik WI wyjaśnił, że w Active Directory przy nazwie komputera (tożsamej z numerem inwentarzowym) przypisywani byli użytkownicy, którym powierzono dany sprzęt.

Analiza 10 komputerów użytkowanych przez pracowników, którzy zostali zwolnieni lub zmienili wydział w okresie 2019-2022 (I półrocze) wykazała, że w 7 przypadkach zostały one przekazane do WI[27], a w 3 zostały na stanie wydziału i przydzielono je innym osobom. W toku kontroli nie stwierdzono przypadków przestoju w wykorzystaniu oprogramowania powyżej 6 miesięcy.

(akta kontroli Tom II str. 205-224)

Analiza dokumentacji 10 wykorzystywanych licencji oprogramowania[28], wykazała, że w odniesieniu do 9 Oddział posiadał dowody zakupu. W przypadku jednego oprogramowania dowodu zakupu nie posiadano, gdyż było to oprogramowanie darmowe, tj. 7-zip. Zostało ono dopuszczone w NFZ do stosowania poprzez umieszczenie go na liście oprogramowania kryptograficznego w PZSZ/014-06-02.
Klucze licencyjne dla 6 programów objętych badaniem[29] przechowywano w WI na zasobach sieciowych, serwerach i w EZD. Dostęp mieli wszyscy pracownicy WI, tj. 10 osób, a nie wyłącznie pracownicy WI-E, których wyznaczono jako administratorów systemów.

[27] 6 z przeznaczeniem jako komputery rezerwowe, a 1 z przeznaczeniem do likwidacji.
[28] McAfee Data Protection Advanced (DLP), NetSupport Notify, TOAD for Oracle, PL/SQL Developer, Symantec Endpoint Protection, Adobe Acrobat Pro, 7-zip, Cisco Webex, Platforma eZamawiający, LEX Omega
[29] McAfee Data Protection Advanced (DLP), NetSupport Notify, TOAD for Oracle, PL/SQL Developer, Symantec Endpoint Protection, Adobe Acrobat Pro.

Kierownik WI wyjaśnił, że: „wszystkie osoby w WI były upoważnione do dostępu do kluczy licencyjnych. W trakcie kontroli uznałem jednak, że warto ograniczyć dostęp tylko do pracowników WI-E".

POW NFZ nie posiadał oprogramowania tworzonego przez pracowników Oddziału. W Oddziale nie było możliwości wygenerowania całościowego raportu dla wszystkich posiadanych licencji oraz subskrypcji.

(akta kontroli Tom II str.225-238, 239)

Analiza 10 programów komputerowych[30] wykorzystywanych w NFZ wykazała, że w przypadku 4 programów licencje nie są wykorzystywane w 100%, tj.:

- dla McAfee Data Protection – Advanced (DPL) wykorzystywano 225 z 300 licencji dożywotnich na urządzenie, tj.: 75%,

- dla NetSupport Notify - wykorzystywano 217 z 250 licencji dożywotnich na urządzenie, tj.: 86,80%,

- dla PL/SQL Developer wykorzystywano 6 z 8 licencji dożywotnich na użytkownika, tj. 75%,

- dla Symantec Endpoint Protection wykorzystywano 293 z 350 licencji, w tym 290 dożywotnich na urządzenie i 60 subskrypcji rocznych, tj. 83,71%.

Naczelnik WI wyjaśnił, że: Programu MCAfee Data Protection Advanced (DPL), który służy do ochrony przed wyciekiem danych, więc zabezpieczono komputery użytkowane na co dzień. Pozostałe licencje traktowano jako rezerwę i planowano wykorzystać w sytuacji konieczności uruchomienia dodatkowych urządzeń będących w magazynie. Brak wykorzystania 33 licencji NetSupport Notify może wynikać z faktu, że nie wgrano jeszcze agenta na stacjach, które wymagały reinstalacji systemu. Dla PL/SQL Developer obecnie wykorzystujemy 6 licencji na użytkownika, 2 licencje stanowią rezerwę na wypadek konieczności podłączenia kolejnej osoby. Niewykorzystane 57 licencji Symantec Endpoint Protection przeznaczonych jest do instalacji na urządzeniach będących w rezerwie w przypadku konieczności wydania ich na pracę zdalną.

(akta kontroli Tom II str. 240-294, 355-356)

1.4 W POW NFZ ustalono zasady akceptowalnego użycia służbowych zasobów IT, z zasadami tymi zapoznano pracowników, którzy potwierdzili to swoim podpisem.
W Oddziale zgodnie z wewnętrznymi regulacjami i praktykami zatrudniani pracownicy odbywają obowiązkowe szkolenia z zakresu ochrony danych osobowych i wewnętrznych regulacji ZSZ[31]. Podczas szkolenia pracownicy zapoznawali się m.in. z zagadnieniami Polityki zarządzania bezpieczeństwem teleinformatycznym w NFZ (PZSZ/014).
Dodatkowo pracownicy, którym przydzielono komputery przenośne i telefony komórkowe na protokołach ich odbioru potwierdzali zapoznanie się z obowiązującymi w POW NFZ zasadami bezpieczeństwa urządzeń mobilnych i komputerów przenośnych oraz służbowych telefonów komórkowych[32].

(akta kontroli Tom II str. 295-298)

[30] McAfee Data Protection Advanced (DLP), NetSupport Notify, TOAD for Oracle, PL/SQL Developer, Symantec Endpoint Protection, Adobe Acrobat Pro, 7-zip, Cisco Webex, Platforma eZamawiający, LEX Omega

[31] Szkolenia realizowane są w ramach Zespołu Bezpieczeństwa Informacji i Ciągłości Działania w POW NFZ. Fakt odbycia szkolenia pracownik potwierdza podpisem na liście obecności oraz w „karcie szkolenia wstępnego z zakresu bezpieczeństwa informacji".

[32] Podstawowe zasady bezpieczeństwa urządzeń mobilnych i komputerów przenośnych użytkowanych w Podkarpackim Oddziale Wojewódzkim Narodowego Funduszu Zdrowia z siedzibą w Rzeszowie oraz Podstawowe zasady bezpieczeństwa służbowych telefonów komórkowych użytkowanych w Podkarpackim Oddziale Wojewódzkim Narodowego Funduszu Zdrowia z siedzibą w Rzeszowie.

W latach 2019-2022 (I półrocze) w POW NFZ nie przeprowadzono żadnych audytów ani kontroli wewnętrznych dotyczących oprogramowania i sprzętu komputerowego[33]. Nie było też w tym zakresie kontroli zewnętrznych.
WI prowadził przy okazji rocznych inwentaryzacji jedynie przeglądy licencji ujętych w spisie Środki Trwałe. Z inwentaryzacji sporządzano protokół weryfikacji aktywów – wartości niematerialnych i prawnych. Przeglądów tych nie prowadzono pod kątem sprawdzenia czy Oddział posiada licencje na każde zainstalowane oprogramowanie. Nie było przeglądów pod kątem nieautoryzowanego oprogramowania, które obejmowałyby stacje robocze, urządzenia mobilne (laptopy, smartfony), udostępnione udziały sieciowe, środowiska wirtualne i nieprodukcyjne.

POW NFZ posiadał narzędzia do monitorowania stacji roboczych (SCCM) i do monitorowania serwerów i urządzeń sieciowych (Netcrunch). Nie prowadził jednak monitoringu legalności korzystania z oprogramowania, ani analizy pod kątem używania różnych wersji programów, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*
Nie było wdrożonego narzędzia np. klasy MDM ani EMM, które umożliwiałoby skanowanie wszystkich urządzeń, w tym mobilnych (np. telefony).

(akta kontroli Tom II str. 299-315)

W okresie objętym kontrolą POW NFZ nie ponosił kar za nielegalne użytkowanie oprogramowania. Niemniej jednak w wyniku przeprowadzonego przez powołanego postanowieniem p.o. Dyrektora Delegatury NIK w Rzeszowie z dnia 31 sierpnia 2022 r. Biegłego[34] z dziedziny audytu systemów informatycznych badania, w POW NFZ stwierdzono przypadki użycia nielegalnego oprogramowania shareware, na które Oddział nie posiada licencji. Stwierdzono również przypadki braku aktualizacji systemów operacyjnych oraz wykorzystywanych bez wsparcia, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*
W POW NFZ występowały również przypadki instalacji na komputerach różnych wersji tych samych programów (IZArc, 7-zip, Acrobar Reader, Filezilla, PuTTY, WinSCP) oraz instalacji różnego oprogramowania VNC umożliwiającego zdalne łączenie się do komputerów.

(akta kontroli Tom II str. 316-320, 405-423)

Zasady zbywania i przekazywania oprogramowania w POW NFZ uregulowane zostały w Zarządzeniu w sprawie zasad gospodarowania składnikami majątkowymi w NFZ.
W POW NFZ wszystkie nośniki danych ze sprzętu przeznaczonego do likwidacji lub zbycia – niezależnie od ich stanu technicznego podlegają niszczeniu przez firmę zewnętrzną. Ostatnia taka likwidacja dysków miała miejsce w 2018 r. [35]
W POW NFZ w latach 2019-2022 (I półrocze) zlikwidowano lub zbyto 76 urządzeń IT i zlikwidowano 1 oprogramowanie, z tego:

- w 2019 r. 50 urządzeń IT (46 zlikwidowano, 4 zbyto), w których:

  40 dysków wymontowano z urządzeń zlikwidowanych, z czego:

  - 35 nośników zarejestrowano w rejestrze nośników do likwidacji,

  - 5 nośników pozostaje w dyspozycji WI.

  10 urządzeń IT nie posiadało nośników (np. drukarki, komputer bez dysku);

[33] W planie audytu wewnętrznego NFZ na rok 2022 r. (III i IV kw.) ujęte zostały dwa zadania audytowe związane z obszarem zarządzania oprogramowaniem, tj.: Zarządzanie uprawnieniami do SI oraz Efektywność wykorzystania systemów informatycznych- optymalizacja, integracja.
[34] Dalej: Biegły.
[35] W dniach 30 lipca 2018 r. – 1 sierpnia 2018 r. dokonano zdemagnetyzowania i zniszczenia fizycznego urządzeń przeznaczonych do likwidacji przez firmę zewnętrzną

- w 2021 r. 26 urządzeń IT i 1 oprogramowanie zlikwidowano, w tym:
  - system antywirusowy McAfee[36];
  - 22 urządzenia IT nie posiadały nośników (np. drukarki, skanery),
  - z 4 urządzeń przeznaczonych do likwidacji wymontowano 5 dysków z czego:
  - 2 dyski zarejestrowano w rejestrze nośników do likwidacji,
  - 3 dyski pozostają w dyspozycji WI[37];

W okresie tym nie przekazano żadnego sprzętu IT do ponownego użycia innym jednostkom.

Zlikwidowane oprogramowanie system antywirusowy McAfee zostało wycofane z użycia.

(akta kontroli Tom II str. 321-351)

1.5 Analiza 10 zakupionych i wykorzystywanych w POW NFZ programów komputerowych[38] wykazała, że Oddział korzystał z oprogramowania zgodnie z warunkami nabycia bądź użytkowania określonymi w zawieranych umowach.

(akta kontroli str. Tom II, str. 294, 352-355)

Stwierdzone nieprawidłowości

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

1. Obowiązujące w Oddziale przepisy nie ustanawiały istotnych mechanizmów kontrolnych, koniecznych do zapewnienia skutecznego i efektywnego zarządzania oprogramowaniem i licencjami. Regulacje te nie obejmowały (w odniesieniu do całego cyklu życia licencji i oprogramowania) procedur dotyczących:

   - nabywania oprogramowania uwzględniających kryteria (zakres) weryfikacji pod kątem bezpieczeństwa,
   - przechowywania i zabezpieczania dostępu do nośników instalacyjnych, kluczy licencyjnych i innych dokumentów licencyjnych (w tym utrzymywanych w środowiskach chmurowych),
   - ewidencjonowania posiadanych i używanych licencji dotyczących oprogramowania nabywanego w modelu SaaS,
   - dystrybucji i redystrybucji licencji,
   - monitorowania (stanu użycia i legalności licencji) oraz zasad wykonywania cyklicznych przeglądów licencji (określenie cyklu, monitorowanie poziomu wykorzystania i daty ważności - szczególnie w przypadkach czasowych subskrypcji, wymagany sposób i elementy raportowania),
   - dokonywania przeglądów na wszystkich wykorzystywanych w Oddziale urządzeniach (serwery, stacje robocze, laptopy, smartfony) oraz objęcia szczególnym nadzorem hostów użytkowników posiadających uprawnienia administracyjne,
   - dokonywania cyklicznego skanowania środowiska IT (stacje robocze, serwery, urządzenia mobilne) pod kątem identyfikacji nieautoryzowanego oprogramowania, a w przypadku jego identyfikacji przedstawiania w raportach pokontrolnych przyczyn takich sytuacji oraz (jeśli konieczne) wskazywania rekomendacji systemowych,
   - dokonywania przeglądów lokalnych i serwerowych zasobów plikowych pod kątem przechowywania danych multimedialnych i innych plików, których

[36] Protokół likwidacji 1/N/2021 z dnia 29 czerwca 2021 r., zniszczenie nośnika w dniu 1 lipca 2021 r.

[37] W tym 1 dysk zarchiwizowano w WI - dysk zawiera dane archiwalnego systemu - przechowywany w sejfie WI.

[38] McAfee Data Protection Advanced (DLP), NetSupport Notify, TOAD for Oracle, PL/SQL Developer, Symantec Endpoint Protection, Adobe Acrobat Pro, 7-zip, Cisco Webex, Platforma eZamawiający, LEX Omega

przechowywanie prowadzi do naruszenia praw do własności intelektualnej oraz innych treści nielegalnych.

Brak ustanowienia w Urzędzie powyższych zasad potwierdził również biegły po przeprowadzeniu badań w jednostce

Kierownik WI wskazał, że szczegółowe procedury dotyczące zarządzania licencjami, w tym dotyczące m.in. zasad monitorowania (stanu użycia i legalności) oraz wykonywania cyklicznych przeglądów i cyklicznego skanowania zasobów ułatwiłyby bieżącą pracę w zakresie zarządzania licencjami. Pozwoliłyby na rozliczenie z wykonania poszczególnych zadań osób, którym je przypisano wg precyzyjne i szczegółowo opisanych czynności.

(akta kontroli Tom I 399-402, 405-423, Tom II str. 1-61)

2. Prowadzone w POW NFZ rejestry nie zawierały całego posiadanego oprogramowania ani dat wygaśnięcia licencji. Zgodnie z zapisami § 44 ust. 2 PZSZ/014 dla każdego podsystemu prowadzi się ewidencję posiadanych i zainstalowanych licencji na wykorzystywane oprogramowanie. Sposób ewidencji powinien umożliwiać wykonanie audytu faktycznie zainstalowanego lub użytkowanego oprogramowania.

   Dyrektor wyjaśnił że prowadzony rejestr zostanie w najbliższym czasie uzupełniony o spis całego oprogramowania użytkowanego w POW NFZ.

   Kierownik WI wyjaśnił, że: Oddział zamierza uzupełnić w Rejestrze komponentów aplikacyjnych również o dane dotyczące daty wygaśnięcia licencji.

   (akta kontroli Tom II str.194-195, 204, 401)

3. Oddział pomimo posiadanych narzędzi do inwentaryzacji oprogramowania[39]. nie wykonywał skanowania wszystkich urządzeń w sieci pod tym kątem zainstalowanych programów[40]. Nie przeprowadzano audytów w zakresie wykrycia nielegalnego oprogramowania, co skutkowało tym, że jednostka nie miała wiedzy, czy takie oprogramowanie jest zainstalowane.

   Kierownik WI wyjaśnił iż: nie prowadzono takiego monitoringu, zakładając, że prawo do instalacji na urządzeniach posiadają wyłącznie administratorzy (pracownicy WI-E) i użytkownicy nie mogą instalować żadnego oprogramowania. Nie analizowano oprogramowania pod kątem używania różnych jego wersji, ze względu na obciążenie pracowników WI-E wieloma różnymi zadaniami.

   (akta kontroli Tom II str. 90-138, 239, 299-315)

4. W POW NFZ stwierdzono przypadki użycia oprogramowania shareware[41], na które Oddział nie posiada licencji, a które nie zostało odinstalowane po testach, tj. LanTopLog 2, Tenable Nessuss, AVG PC Tuneup.

   Kierownik WI wyjaśnił, że oprogramowanie to nie zostało odinstalowane po testach przez zapomnienie.

   (akta kontroli Tom II str. 90-92, 239, 357-423)

5. W Oddziale stwierdzono przypadki braku aktualizacji systemów operacyjnych oraz wykorzystywanych bez wsparcia, instalacje aplikacji w nieaktualnej wersji oraz różne wersje tych samych programów.

   W wyniku analizy oprogramowania na siedmiu serwerach stwierdzono:

[39] Do monitorowania stacji roboczych od lutego 2022 r. - SCCM (wcześniej OSC Inventory) i do monitorowania serwerów i urządzeń sieciowych - Netcrunch.

[40] Podczas kontroli przedłożono dwa archiwalne raporty skanowania zasobów programem OSC Inventory dwóch stacji roboczych.

[41] Oględzinom poddano 7 serwerów i 6 stacji roboczych

- na 4 serwerach - brak aktualizacji serwerowych systemów operacyjnych, wśród których zidentyfikowano systemy EOL, np. Linux Red Hat 5 i Windows Server 2008 R2,
- na 5 serwerach - wykorzystywanie systemów operacyjnych bez wsparcia, np. Microsoft Windows 7(32-bit).

W POW NFZ występowały również przypadki instalacji na komputerach oprogramowania określanego jako EOS[42], które nie posiada już wsparcia producenta, czy EOL- czyli takie, które zostało oficjalnie wycofane (Adobe Shockwave Player) ze względu na luki w bezpieczeństwie[43].

Kierownik WI wyjaśnił, że braki i instalacje w różnych wersjach oraz inne niedociągnięcia wynikają z niewielkiej liczby osób w WI-E (4 pracowników i Naczelnik) oraz dużego obciążenia WI-E zadaniami helpdesk. Zdarza się, że trzeba odłożyć część czynności administracyjnych na rzecz awarii urządzeń, bieżącej obsługi użytkowników, prowadzonych prac w ramach różnych zespołów zadaniowych oraz wymiany sprzętu komputerowego.

(akta kontroli Tom II str.357-363, 399-402, 405-423)

OCENA CZĄSTKOWA

NIK ocenia negatywnie realizację zadań związanych z organizacją i nadzorem nad oprogramowaniem. Oddział wykorzystywał zakupione przez siebie oprogramowanie zgodnie z warunkami licencji.

W POW NFZ obowiązywały polityki zarzadzania oprogramowaniem wprowadzone przez Centralę NFZ. Nie zawierały one jednak szczegółowych zasad zarządzania licencjami. Pracownikom WI-E przydzielono zadania w tym zakresie.

Oddział posiadał narzędzia do monitorowania oprogramowania jednak go nie wykorzystywał do skanowania posiadanych zasobów. Nie wykonywano audytów (przeglądów) całości zasobów pod kątem wykrycia nielegalnego oprogramowania.

Prowadzone w POW NFZ spisy nie zawierały całego oprogramowania ani dat wygaśnięcia licencji. W toku kontroli stwierdzono również przypadki użycia niedozwolonego w NFZ oprogramowania (darmowe do użytku prywatnego, domowego), przypadki instalacji wersji określonej jako EOL.

OBSZAR

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

Opis stanu faktycznego

2.1 W POW NFZ na podstawie inwentaryzacji posiadanych zasobów informatycznych, zgłaszanych potrzeb dokonywano analizy w celu zaplanowania wydatków w zakresie nabycia i utrzymania licencji komputerowych.

W NFZ w dniu 28 marca 2019 r. przyjęto Strategię NFZ na lata 2019-2023, w której w pkt 61 określono Cel 7.3 Rozwój infrastruktury i systemów IT. Jako główny cel w obszarze technologii informatycznych wskazano zbudowanie nowego systemu teleinformatycznego i ograniczenie uzależnienia organizacji od zewnętrznych dostawców IT. Jako niezbędny element zmian w tym zakresie wskazano doskonalenie systemu zarządzania bezpieczeństwem i ciągłości działania.

Zasady dokonywania zakupów w POW NFZ określały procedury zawarte w *Regulaminie tworzenia rzeczowego planu wydatków* oraz *Regulaminie udzielania zamówień publicznych.*

[42] End of Support. Dalej: EOS.
[43] Raport skanowania (SCCM) z 27.07.2022 r.

W latach 2019-2022 za realizację zakupów ujętych w rzeczowym planie wydatków inwestycyjnych w POW NFZ odpowiedzialne były kolejno dwa działy: WI-E i Wydział Administracyjno-Gospodarczy[44] tj.:

- do 1 sierpnia 2021 r. – WAG, który realizował zadania w z zakresu zakupów przy współpracy i wsparciu WI-E;
- od 2 sierpnia 2021 r. w zależności od wielkości wydatkowanych środków:
  - do 130 tys. zł netto – WI-E we współpracy z WAG,
  - powyżej 130 tys. zł netto - WAG we współpracy z WI-E.

W okresie objętym kontrolą, POW NFZ w rzeczowym planie wydatków inwestycyjnych zatwierdzanym przez Departament Informatyki w Centrali NFZ oraz Radę Funduszu w poz. E.1 Wartości niematerialne i prawne, otrzymywał corocznie budżet w wysokości 20 tys. zł na wydatki dotyczące zakupu oprogramowania i licencji, które mógł realizować bez konieczności zmiany w planie wydatków inwestycyjnych.

W planie na 2019 r. przyjęto wydatki w wysokości po 20 tys. zł z przeznaczeniem na zakup pakietów oprogramowania i systemów informatycznych. Środków tych nie wydatkowano.

W planie na 2020 r przyjęto wydatki w wysokości 210 tys. zł, ujmując oprócz 20 tys. zł 150 tys. zł, z przeznaczeniem na zakup systemu o funkcjonalności DLP – McAfee Complete Data Protection - Advanced. W trakcie roku Oddział wystąpił o zwiększenie środków o 41 tys. zł, z przeznaczeniem na rozszerzenie licencji na liczbę połączeń VPN z 50 do 200[45].

W roku tym Oddział wydatkował 161,17 tys. zł, w tym na:

- NetSupport Notify – 4,55 tys. zł. Zakupiono z dniu 22 maja 2020 r. od firmy ALWO W. Prokopczuk w Warszawie 250 licencji wieczystych na urządzenia z 2 letnim wsparciem;

- McAfee Complete Data Protection - Advanced (DLP) - 124,64 tys. zł[46]. Zakupiono w dniu 17 listopada 2020 r. od firmy Stinet Sp. z o.o. w Warszawie, 300 licencji wieczystych na urządzenia z 3-letnim wsparciem od firmy;

- licencje VPN - 31,98 tys. zł. Zakupiono w dniu 15 maja 2020 r. od firmy COMP S.A. w Warszawie, 150 licencji wieczystych na ilość jednoczesnych połączeń.

Na powyższe zakupy zapotrzebowanie zgłaszał WI i były one realizowane przez WAG przy współpracy z WI.

W planie na 2021 r. przyjęto wydatki w wysokości 112 tys. zł, ujmując oprócz 20 tys. zł z przeznaczeniem na zakup pakietów oprogramowania i systemów informatycznych 92 tys. zł na zakup licencji umożliwiającej uruchomienie środowiska wirtualnych stacji roboczych. Z zaplanowanej łącznej kwoty 112 tys. zł Oddział nie wydatkował żadnych środków.

W planie na 2022 r. ujęto wydatki w wysokości po 20 tys. zł z przeznaczeniem na zakup pakietów oprogramowania i systemów informatycznych. Do chwili zakończenia kontroli środków tych nie wydatkowano.

(akta kontroli Tom III str. 1-136)

Kierownik IT wyjaśnił, że w 2021 r. zrezygnowano z zakupu licencji do uruchomienia środowiska wirtualnych stacji, gdyż producenci zmienili zasady sprzedaży na formę subskrypcji, co uniemożliwiło sfinansowanie zadania z rzeczowego planu wydatków inwestycyjnych. Ostatecznie zrezygnowano z realizacji zadania, ze względów technicznych. W roku 2019 i 2021 nie wykorzystano środków na zakup pakietów

[44] Dalej: WAG
[45] Wynikało to konieczności pracy zdalnej podczas epidemii COVID-19.
[46] W tym zakup licencji za kwotę 99,71 tys. zł i zakup instruktarzu ze szkoleniem 24,93 tys. zł

oprogramowania i systemów informatycznych ze środków ujętych w rzeczowym planie inwestycyjnym, gdyż uważano, że oprogramowanie, które posiadano jest wystarczające.

(akta kontroli Tom III str.137)

W POW NFZ stwierdzono przypadek nieodnowienia wsparcia dla jednego programu, o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. Tom II, str. 294, 352-355)

2.2 W POW NFZ nie dokonywano pomiarów efektywności posiadanego oprogramowania. Weryfikowano i raportowano wykorzystywane przez Oddział oprogramowanie, przy planowanym odnowieniu wsparcia oraz na zapytania Centrali NFZ[47].

Większość oprogramowania wymagającego wdrożenia, w tym oprogramowanie dziedzinowe SIDW NFZ, nabywana jest przez Centralę NFZ i wdrażane na zasadach opisanych w umowach zawieranych przez Centralę NFZ[48].

POW NFZ dokonał jednego zakupu gotowego oprogramowania wraz z wdrożeniem, w 2020 r. Nabyty system o funkcjonalności DLP - McAfee Complete Data Protection – Advanced (300 licencji), miał wzmocnić ochronę danych w postaci elektronicznej. Zasady jego wdrożenia zostały określone w umowie z wykonawcą oraz na wniosku o zmianę w systemie[49].
Liczba zakupionych licencji ww. oprogramowania oraz licencji Symantec Endpoint Protection różniła się względem liczby komputerów w Oddziale.
Dla oprogramowania McAfee Complete Data Protection – Advanced liczba zakupionych licencji była mniejsza niż liczba komputerów w Oddziale -315, a liczba instalacji -225, mniejsza niż liczba komputerów wykorzystywanych - 252 (nawet po odjęciu rezerwy). W okresie objętym kontrolą wydatki na ww. oprogramowanie dotyczące nabycia oprogramowania oraz instruktażu ze szkoleniem wyniosły 124,64 tys. zł[50].
Dla oprogramowania antywirusowego Symantec Endpoint Protection, na które Oddział posiada 350 licencji (w okresie objętym kontrola do 290 posiadanych licencji dokupiono 60) liczba instalacji – 293, również była mniejsza niż liczba komputerów w Oddziale. W okresie objętym kontrolą wydatki na ww. oprogramowanie dotyczące zakupu 60 subskrypcji rocznych oraz wsparcia wyniosły 112,79 tys. zł[51].
Powyższe systemy powinny być zainstalowane na wszystkich komputerach wykorzystywanych przez użytkowników.
Naczelni WI wyjaśnił, że: *Przyjęto, że na stacjach rezerwowych nie będzie wgrywany DLP, a będziemy wgrywać program antywirusowy. Nie potrafię wyjaśnić tych nieścisłości. Nie jestem w stanie określić konkretnej liczby sprzętu wymagającego zabezpieczeń.*

(akta kontroli str. Tom II str. 352-354, 399-423, Tom III, str. 140-151, 168-170)

Zasadniczy zintegrowany system funkcjonujący w POW NFZ (SIWD NFZ) został zakupiony i jest utrzymywany centralnie. Błędy w zakresie jego funkcjonowania

[47] Proces realizowany był przez administratora danego systemu, przy współpracy pozostałych administratorów.
[48] Zasady wdrażania w POW NFZ określa Procedura zarządzania zmianami w systemie teleinformatycznym w NFZ PSZS/014-07 stanowiąca element polityki dziedzinowej PSZ/014 dotyczącej zarządzania bezpieczeństwem teleinformatycznym w NFZ.
[49] Umowa nr WAG.261.207.2020 r. z dnia 17 listopada 2020 r. dotycząca dostawy i wdrożenia systemu DLP wraz z asystą dla POW NFZ.
[50] Zakup oprogramowania (99,71 tys. zł) i instruktażu ze szkoleniem w związku z nabytą licencją (24,93 tys. zł) zrealizowany został w 2020 r.
[51] Zakup 60 rocznych subskrypcji (14,09 tys. zł, w tym: w 2021 r. – 4,95 tys. zł i w 2022 r. – 9.14 tys. zł) i wsparcie (98,70 tys. zł – za lata 2019-2022).

zgłaszane przez użytkowników raportowane są przez pracowników WI poprzez dedykowany system zgłoszeń (JIRA) do producenta oprogramowania.
W okresie objętym kontrolą było to 1610 zgłoszeń, w zakresie błędów, konsultacji serwisowych oraz nadzorów serwisowych, w tym: w 2019 r.- 313 zgłoszeń, w 2020 r. – 415 zgłoszeń, w 2021 r. - 510 zgłoszeń i w 2022 r.- 372 zgłoszenia.
Główne problemy dotyczyły niedziałania modułów (błędy techniczne uniemożliwiające pracę w module) oraz nieprawidłowego działania części funkcjonalności w modułach. Problemy z funkcjonowaniem i użytkowaniem pozostałego oprogramowania w Oddziale zgłaszano do WI, który samodzielnie lub przy wsparciu producentów podejmował działania w celu ich rozwiązania[52].

W okresie objętym kontrolą Oddział wykorzystywał trzy zakupione we własnym zakresie oprogramowania typu Saas[53], tj.:

- Cisco Webex z jedną licencją umożliwiająca uruchomienie jednej wideokonferencji w tym samym czasie. W okresie ostatnich 6-m-cy w Oddziale utworzono 16 spotkań, w których średnio uczestniczyło 18 osób. Dostęp do konta umożliwiającego założenie spotkania posiadało 5 osób (pracownicy WI-E i Naczelnik WI);

- platformę eZamawiający, z jedną usługą umożliwiającą publikację do 10 postępowań w rocznym okresie użytkowania. Uprawnienia przyznano 3 pracownikom Wydziału Administracyjno-Gospodarczego. W latach 2019-2022 (30 czerwca) opublikowano w kolejnych okresach obowiązywania umowy łącznie 19 postępowań, z tego:
- w okresie: 28 września 2020 r. – 27 września 2021 r. - 8 postępowań;
- w okresie: 28 września 2021 r. – 27 września 2022 r. - 11 postępowań[54];

- LEX Medica Optimum/Premium On-line[55] - z ośmioma licencjami imiennymi, wykorzystywanymi przez ośmiu pracowników (czterech Wydziału Prawnego, dwóch Wydziału Spraw Pracowniczych oraz dwóch pracowników Wydziału Administracyjno-Gospodarczego).

POW NFZ wykorzystywał również system MS Teams udostępniony od września 2021 r. przez Centralę.
Od września 2021 r. Oddział zaczął częściowo wykorzystywać usługę MS Teams w ramach licencji produktów Microsoft zakupionych przez Centralę NFZ. Rozpoczęto wówczas rekonfigurację kont użytkowników ActiveDirectory. Do końca 2022 r. Oddział planuje umożliwienie korzystania z MS Teams wszystkim użytkownikom. W związku z tym nie planuje przedłużenia subskrypcji usługi Cisco Webex w kolejnym roku.

POW NFZ nie nabywał oprogramowania finansowanego ze środków UE.

(akta kontroli str. Tom III, str. 142, 152-167)

2.3 POW NFZ w latach 2019-2022 ponosił wydatki na nabycie i utrzymanie oprogramowania komputerowego odpowiednio:
- w 2019 r. w wysokości 230,54 tys. zł, w tym na:
  - dostosowanie lub zaktualizowanie programów komputerowych - 94,71 tys. zł;
  - subskrypcje licencji – 51,82 tys. zł;
  - opłaty za wsparcie i asysty techniczne – 82,3 tys. zł;
  - inne[56] – 1,71 tys. zł;

[52] Oddział nie prowadzi ewidencji takich zgłoszeń.
[53] Oprogramowanie jako usługa (Software as a Service)
[54] 10 publikacji zrealizowano w ramach umowy obowiązującego okresu. Po automatycznym zablokowaniu dostępu do kolejnych publikacji (po wyczerpaniu limitu) uzgodniono z producentem przeniesienie jednego postępowania z nowego okresu rozliczeniowego do bieżącego. Aneksem nr 3 z dnia 14 lipca 2022 przedłużono okres trwania umowy o kolejny rok.
[55] Wykorzystywany od 8 kwietnia 2022 r. Wcześniej Oddział korzystał z abonamentu LEX Kadry Premium do 28 sierpnia 2021 r. oraz LEX Omega do 30 września 2021 r.
[56] Ubezpieczenie oprogramowania.

- w 2020 r. w wysokości 641,62 tys. zł, w tym na:
  - dostosowanie lub zaktualizowanie programów komputerowych - 12,30 tys. zł;
  - subskrypcje licencji – 61,89 tys. zł;
  - opłaty za wsparcie i asysty techniczne – 404,55 tys. zł;
  - instruktaż ze szkoleniem w związku z nabytą licencją – 24,93 tys. zł;
  - inne[57] – 137,95 tys. zł;
- w 2021 r. w wysokości 117,81 tys. zł, w tym na:
  - dostosowanie lub zaktualizowanie programów komputerowych - 12,3 tys. zł;
  - subskrypcje licencji – 14,48 tys. zł;
  - opłaty za wsparcie i asysty techniczne – 85,7 tys. zł;
  - inne[58] – 5,33 tys. zł;
- w 2022 r. (do 30 czerwca) w wysokości 321,49 tys. zł, w tym na:
  - subskrypcje licencji – 46,03 tys. zł;
  - opłaty za wsparcie i asysty techniczne –271,96 tys. zł.
  - inne[59] – 3,5 tys. zł.

W latach 2019-2022 (I półrocze) POW NFZ nie ponosił wydatków wynikających z nielegalnego użytkowania licencji i oprogramowania.

(akta kontroli str. Tom III, str. 171-281)

2.4-2.5 W POW NFZ nie określono formalnych wymagań bezpieczeństwa, jakie muszą spełniać aplikacje czy systemy informatyczne dopuszczone do przetwarzania informacji. Oddział nie posiadał również procedur weryfikacji oprogramowania przed jego zakupem. Oprogramowanie nabywane lub wdrażane centralnie mogło być poddawane analizie w Biurze Bezpieczeństwa i Ciągłości Działania przy współpracy Departamentu Informatyki w Centrali NFZ[60].

W okresie objętym kontrolą POW NFZ zakupił trzy gotowe oprogramowania typu SaaS, tj.:
- w 2020 r. Cisco Webex, w formie rocznego abonamentu usługi umożliwiającej uruchomienie jednej wideokonferencji w danym czasie za kwotę 2 164,80 zł[61], którego zakup podyktowany był koniecznością zapewnienia odpowiedniego poziomu komunikacji ze świadczeniodawcami w okresie pandemii COVID-19;
- w 2020 r. e-Zamawiający, w formie rocznego abonamentu do platformy wspomagającej elektroniczne prowadzenie do 10 postępowań o udzielenie zamówień publicznych za kwotę 4 797 zł[62].
- w 2022 r. LEX Medica Optimum/Premium On-line w formie rocznego dostępu do informacji prawnej w zakresie ochrony zdrowia dla 8 użytkowników za kwotę 36 885,24 zł[63].

Przed zakupem powyższych usług chmurowych w POW NFZ nie dokonywano ich oceny pod kątem spełnienia wymogów bezpieczeństwa i poufności danych czy wiarygodności dostawcy i zapewnienia wsparcia technicznego.

---

[57] Dokupienie licencji VPN, zakup oprogramowania NetSupport Notify oraz McAfee Complete Data Protection Advanced (DLP) oraz ubezpieczenie oprogramowania.

[58] Ubezpieczenie oprogramowania.

[59] Ubezpieczenie oprogramowania.

[60] W latach 2019-2022 (I półrocze) taką analizę przeprowadzono w Centrali, przed uruchomieniem w POW NFZ następujących aplikacji: DaVinci Resolve - Oprogramowanie do edycji plików video dla Zespołów Profilaktyki Zdrowotnej, SQL Server Express z Management Studio, MS Teams.

[61] Faktura za nabycie nr FA/12/11/2020 z dnia 6 listopada 2020 r., faktury za przedłużenie subskrypcji: nr FA/41/10/2021 z 28 października 2021 r. na kwotę 2 164,80 zł.

[62] Faktura nr FSEZ/20/0468 z dnia 20 października 2020 r. za usługi w okresie rocznym, faktura FSEZ/21/0640 z 12 maja 2021 r. za dodatkowy moduł do weryfikacji podpisu do 100 dokumentów na kwotę 615 zł, faktura nr FSEZ/21/1056 z 28 września 2021 r. za usługę w kolejnym okresie rocznym na kwotę 5 412 zł.

[63] Od 8 kwietnia 2022 r. do 7 kwietnia 2023 r. Oddział korzysta z pakietu Lex Medica Optimum/Premium On-line. W latach 2019-2021 korzystano z: Lex Kadry Premium do 23 sierpnia 2021 r. i Lex Omega do 30 września 2021 r. Od 1 października 2021 r. do 7 kwietnia 2022 r. w Oddziale nie było zakupione ww. oprogramowanie.

Były to programy wykorzystywane już w Centrali NFZ i innych oddziałach lub takie jak LEX, który Oddział użytkował wcześniej.
Za analizę potrzeb zakupu ww. oprogramowania odpowiadały komórki POW NFZ zgłaszające zapotrzebowanie, tj. w przypadku: Cisco Webex -WI, e-Zamawiający – WAG i LEX Medica Optimum/Premium On-line – Wydział Prawny.
W POW NFZ nie określono zasad wprowadzających szczegółowe zadania i odpowiedzialności w zakresie nabywania i wykorzystywania oprogramowania w modelu SaaS. Nie monitorowano w sposób ciągły kto wykorzystuje lub rozpoczął wykorzystywanie tego typu usługi.

Naczelnik WI wyjaśnił, że identyfikacja tego typu zdarzeń może znacząco podnieść jakość zarządzania systemami IT.
(akta kontroli str. Tom III, str. 328)

(akta kontroli str. Tom III, str. 283-328)

Stwierdzone nieprawidłowości

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

1. W POW NFZ stwierdzono jeden przypadek braku odnowienia wsparcia dla zakupionego programu[64]. Dotyczył on oprogramowania NetSupport Notify zakupionego wraz z 2-letnim wsparciem w dniu 1 czerwca 2020 r. za kwotę 4,55 tys. zł. Po 31 maja 2022 r. tego wsparcia Oddział nie odnowił.
   Naczelnik WI wyjaśnił, że *opóźnienie w działaniach dotyczących zapewnienia wsparcia wynikało z przeoczenia. Zakupiony w 2020 r. produkt miał 2-letnie wsparcie i po raz pierwszy miało być ono dokupione. Podjęliśmy próbę jego zakupu składając wniosek 8 sierpnia 2022 r. i opublikowaliśmy postępowanie przetargowe na BIP NFZ w dniu 5 września 2022 r. W związku z tym, iż nie wybrano oferty spełniającej wymagania zamówienia, Oddział podejmie kolejną próbę zakupu.*
   (akta kontroli Tom II str.352-356, Tom III str. 279-282)

OCENA CZĄSTKOWA

W Oddziale wprowadzono do stosowania regulacje uwzględniające mechanizm kontrolny zapewniający, że zapotrzebowanie na licencje jest weryfikowane i oceniane pod kątem zasadności/celowości wykorzystania oprogramowania, przy jednoczesnym uwzględnieniu możliwości finansowych.
Stwierdzono jednak przypadek nieodnowienia wsparcia dla jednego oprogramowania w wymaganym terminie.
Zmiany w rzeczowym planie wydatków inwestycyjnych dotyczące zakupów oprogramowania były jednostkowe i dotyczyły: zakupu dodatkowych licencji na liczbę połączeń VPN, co wynikało z konieczności pracy zdalnej podczas epidemii COVID-19 oraz z rezygnacji z zakupu licencji do uruchomienia środowiska wirtualnych stacji, wynikającej ze zmiany zasad sprzedaży na formę subskrypcji.
Nabywane w POW NFZ oprogramowanie typu SaaS nie było weryfikowane pod kątem spełnienia wymogów bezpieczeństwa i poufności danych ani oceny wiarygodności dostawcy i zapewnienia wsparcia technicznego. Były to jednak programy wykorzystywane już w Centrali NFZ i innych oddziałach lub takie, które Oddział użytkował wcześniej.
W POW NFZ nie określono zasad nabywania i wykorzystania oprogramowania typu SaaS. Nie było wymogu weryfikacji bezpieczeństwa dostawcy i oprogramowania w procesie jego zakupu. Brak takiej weryfikacji stwarza szereg ryzyk związanych m.in. z nabyciem oprogramowania od niewiarygodnych dostawców, brakiem ciągłości

[64] W okresie objętym kontrolą w Oddziale wystąpiło łącznie 47 przypadków odnowienia wsparcia, z tego: w 2019 – 7, w 2020 – 22, w 2021 – 4, w 2022 -14.

usług wsparcia technicznego i bezpieczeństwa, brakiem reakcji i rozwiązywania, problemów/awarii przez dostawcę w akceptowalnym przez organizację czasie, niespełnieniem podstawowych wymagań dotyczących zarządzania danymi, kontroli dostępu czy bezpieczeństwa.

IV. Wnioski

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

Wnioski

1. Podjęcie działań w celu uzupełnienia wewnętrznych regulacji dotyczących zarządzania licencjami/oprogramowaniem komputerowym.
2. Zapewnienie ujęcia w ewidencji wszystkich posiadanych licencji.
3. Podjęcie działań w celu weryfikacji zainstalowanego oprogramowania pod kątem zgodności z posiadanymi licencjami oraz przydatności oprogramowania w nieaktualnych wersjach
4. Usunięcie programów, na które Oddział nie posiada licencji lub są niepożądane.
5. Zapewnienie aktualizacji oprogramowania zgodnie z wewnętrznymi regulacjami.
6. Zapewnienie terminowego odnawiania wsparcia dla posiadanych programów.

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 Rzeszowie. 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 wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i 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.

Rzeszów, dnia 28 października 2022 r.

Najwyższa Izba Kontroli
Delegatura w Rzeszowie
Dyrektor
Wiesław Motyka

/-/

Kontroler
Edyta Niegowska-Buko
Główny specjalista kontroli państwowej

/-/