NAJWYŻSZA IZBA KONTROLI

Delegatura w Kielcach

LKI.410.6.2.2025

Agnieszka Rogalińska
Starosta Ostrowiecki
Starostwo Powiatowe
w Ostrowcu Świętokrzyskim
ul. Iłżecka 37
27-400 Ostrowiec Świętokrzyski

WYSTĄPIENIE POKONTROLNE

P/25/003 Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Delegatura w Kielcach
ul. gen. T. Kościuszki 6, 25-310 Kielce
T +48 41 249 91 00, F +48 41 249 91 05
lki@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Ostrowcu Świętokrzyskim (dalej: Starostwo lub SP), ul. Iłżecka 37, 27-400 Ostrowiec Świętokrzyski.
Kierownik jednostki kontrolowanej	Agnieszka Rogalińska, Starosta Ostrowiecki (dalej: Starota), od 15 maja 2024 r., wcześniej Starostą Ostrowieckim była Marzena Dębnika, od 22 listopada 2018 r. do 14 maja 2024 r.
Zakres przedmiotowy kontroli	Realizacja przez powiat działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych, tj. 10 czerwca 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Kielcach.
Kontroler	Piotr Fatalski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKI/42/2025 z 28 kwietnia 2025 r. (akta kontroli str. 1-4)

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Powiat Ostrowiecki, w ramach projektu grantowego *Cyberbezpieczny Samorząd Zwiększenie poziomu cyberbezpieczeństwa*[3] *Powiatu Ostrowieckiego*, podjął działania w celu zwiększenia poziomu bezpieczeństwa informacji. W dokumentach strategicznych Powiatu Ostrowieckiego nie ujęto zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa. Potrzeby w zakresie cyberbezpieczeństwa zostały rozpoznane dopiero na potrzeby projektu pn. *Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego* (dalej: Projekt).

W ramach projektu grantowego Starostwo pozyskało z Centrum Projektów Polska Cyfrowa 850 tys. zł na realizację Projektu. Poza Starostwem w Projekcie uczestniczyły również Powiatowy Urząd Pracy w Ostrowcu Św. (dalej: PUP) oraz Powiatowe Centrum Pomocy Rodzinie w Ostrowcu Św. (dalej: PCPR). Do zakończenia kontroli, tj. do 10 czerwca 2025 r. Starostwo realizowało Projekt zgodnie z zapisami umowy o powierzenie grantu. SP terminowo przekazało, za pośrednictwem ePUAP do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (dalej: NASK) uzupełnione *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego* wykonane oddzielnie dla Starostwa, PUP i PCPR. W ramach projektu wydatkowano 528 389,64 zł, tj. 62,2% zaplanowanych środków. SP zakupiło cały zaplanowany sprzęt, zamówiło oprogramowanie. Na potrzeby Projektu Starostwo wyodrębniło ewidencję księgową oraz posiadało wyodrębniony rachunek bankowy umożliwiający identyfikację wszystkich transakcji oraz poszczególnych operacji bankowych związanych z Projektem. Zrealizowane w ramach Projektu zakupy zostały dokonane zgodnie z §4 ust. 1 pkt 5 umowy o udzielenie grantu, tj. z należytą starannością, w szczególności ponosząc wydatki celowo, rzetelnie, racjonalnie i oszczędnie z zachowaniem zasady uzyskiwania najlepszych efektów z danych nakładów. Zakupiony sprzęt był użytkowany. Do realizacji pozostały szkolenia, audyt zgodności z KRI[4]-KSC[5] dla PUP i PCPR, aktualizacje SZBI[6] dla SP i PUP, opracowanie SZBI dla PCPR, audyt końcowy dla SP, PUP i PCPR oraz działania promocyjne. Ustalony na 6 maja 2026 r. termin realizacji Projektu wydaje się być niezagrożony. Starosta zapewnił stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu. Starostwo prawidłowo realizowało, wynikający z umowy o powierzenie grantu, obowiązek informowania obywateli o fakcie otrzymania dofinansowania na realizację Projektu.

W Starostwie nie było opracowanego i wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji, w rozumieniu § 19 ust. 1 w związku z ust. 3 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

---

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

[3] Dziedzina wiedzy zajmująca się zapewnieniem odporności: systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność posiadanych i przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

[4] Krajowe Ramy Interoperacyjności.

[5] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

[6] System Zarządzania Bezpieczeństwem Informacji.

informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7] (dalej: rozporządzenie KRI).

W 2023 r. SP nie przeprowadziło audytu z zakresu bezpieczeństwa informacji, pomimo że zgodnie z § 19 ust. 2 pkt 14 rozporządzenia KRI audyt taki należało przeprowadzać nie rzadziej niż raz w roku.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

Opis stanu faktycznego

1. W przyjętej przez Radę Powiatu Ostrowieckiego Strategii Zrównoważonego Rozwoju Powiatu Ostrowieckiego do roku 2030+[9] ani innych dokumentach wskazujących kierunki rozwoju nie ujęto zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa.

(akta kontroli str. 41-42)

Starosta wyjaśniła m.in.: *Choć w „Strategii Zrównoważonego Rozwoju Powiatu Ostrowieckiego do roku 2030+" nie uwzględniono bezpośrednio zagadnienia cyberbezpieczeństwa, kwestia wzmocnienia bezpieczeństwa systemów informacyjnych zarówno Starostwa Powiatowego, jak i powiatowych jednostek organizacyjnych traktowana jest przez Zarząd Powiatu Ostrowieckiego priorytetowo. Powiat aktywnie realizuje działania w zakresie zwiększenia poziomu cyberbezpieczeństwa, czego doskonałym przykładem jest projekt pn.: „Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego", dofinansowany przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021–2027, na realizację którego powiat otrzymał 850 000,00 zł. (...) Brak bezpośredniego odniesienia do cyberbezpieczeństwa w ww. dokumencie strategicznym, wynika również z faktu, że dokument ten koncentruje się głównie na szeroko pojętym zrównoważonym rozwoju a kwestie techniczne, w tym związane z cyberbezpieczeństwem, zostały ujęte pośrednio jako element zapewnienia nowoczesnego i efektywnego zarządzania. Ich szczegółowa realizacja odbywa się w ramach odrębnych programów i projektów operacyjnych. Jako, że celem nadrzędnym przedmiotowego dokumentu jest poprawa jakości życia mieszkańców oraz zrównoważony rozwój społeczno–gospodarczy Powiatu Ostrowieckiego, obejmujący przede wszystkim aspekty społeczne, gospodarcze i środowiskowe, cyberbezpieczeństwo, choć w ostatnim czasie bardzo istotne, traktowane jest jako element wspierający główne cele, a nie jako odrębny priorytet. Powyższe powoduje, że podejmowane przez Powiat Ostrowiecki działania w zakresie zwiększenia poziomu cyberbezpieczeństwa, wpisują się w następujący obszar i cel strategiczny, ujęty w ww. strategii:*

- *Obszar strategiczny: ZARZĄDZANIE ROZWOJEM*
- *Cel strategiczny: Partnerskie zarządzanie sprawami publicznymi, wykorzystujące nowoczesne instrumenty polityki rozwoju*
- *Cel operacyjny 4.1. Rozwój zarządzania strategicznego powiatem*

---

[7] Dz. U. poz. 773. Do dnia 22 maja 2024 r. § 20 ust. 1 w związku z ust. 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) dalej: stare rozporządzenie KRI.

[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] Uchwała LIX/367/2022 z 29 czerwca 2022 r.

– *Kierunki interwencji (kluczowe działania): 4.1.1. Doskonalenie jakości usług publicznych i sprawności administracyjnej*

Podsumowując, pomimo, że zagadnień oraz działań dotyczących zwiększenia poziomu cyberbezpieczeństwa nie uwzględniono bezpośrednio w ww. strategii rozwoju powiatu do roku 2030+ oraz w pozostałych dokumentach strategicznych, jest ono traktowane jako kluczowy element zapewniający bezpieczne, sprawne i efektywne funkcjonowanie administracji publicznej samorządu powiatowego. Jednocześnie zapewniam, że w przypadku konieczności przystąpienia do aktualizacji posiadanych dokumentów strategicznych lub opracowania nowych po upływie okresu ich obowiązywania, zagadnienia związane ze zwiększeniem poziomu cyberbezpieczeństwa zostaną bezpośrednio uwzględnione w aktualizowanych/opracowywanych dokumentach.

(akta kontroli str. 564-565)

2. W Starostwie nie sporządzono pisemnej analizy potrzeb SP w zakresie zwiększenia poziomu cyberbezpieczeństwa. We wniosku o dofinansowanie projektu pn. *Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego* wskazano, że koncepcja realizacji projektu opracowana została na podstawie analizy potrzeb (luk) jednostek w zakresie cyberbezpieczeństwa w obszarze organizacyjnym, kompetencyjnym oraz technicznym w oparciu o posiadaną dokumentację, opracowane Ankiety Dojrzałości Cyberbezpieczeństwa, badanie stanu infrastruktury technicznej oraz kompetencji pracowników w zakresie cyberbezpieczeństwa. We wniosku wskazano, że:

– regulacje ujęte w PBI[10]/SZBI Starostwa, PUP i PCPR nie uwzględniały obszaru cyberbezpieczeństwa;
– w PBI/SZBI w PUP występowały istotne luki w obszarze procedur dotyczących badania i zarządzania podatnościami, ryzykami oraz zagrożeniami;
– wszystkie jednostki nie organizowały szkoleń dla pracowników w zakresie cyberbezpieczeństwa. Infrastruktura sieciowa wymagała wzmocnienia.

(akta kontroli str. 5-15, 41)

Starosta wyjaśniła: *Analiza potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa dla jednostek objętych wsparciem w ramach realizowanego projektu, tj. Starostwa Powiatowego, PUP oraz PCPR została przeprowadzona w oparciu o posiadaną dokumentację, ocenę stanu infrastruktury informatycznej jednostek, kompetencje pracowników w zakresie cyberbezpieczeństwa oraz opracowane Ankiety Dojrzałości Cyberbezpieczeństwa dla poszczególnych jednostek objętych projektem. Zgodnie z wytycznymi dokumentacji konkursowej, koncepcja realizacji projektu wraz z zaproponowanymi w niej rozwiązaniami, została opracowana w oparciu o poradnik Cyberbezpieczny Samorząd. Jako, że analiza ta została przeprowadzona, ale nie została sformalizowana odrębnym dokumentem stanowiącym stricte „analizę potrzeb", informacje pozyskane w wyniku jej przeprowadzenia stanowiły podstawę do opracowania koncepcji projektu, co z kolei znalazło swoje odzwierciedlenie we wniosku o dofinansowanie. W procesie identyfikacji potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa uczestniczyli informatycy PUP i PCPR oraz z ramienia Starostwa Powiatowego – przedstawiciel firmy, prowadzącej obsługę informatyczną Starostwa Powiatowego.*

[10] Polityka Bezpieczeństwa Informacji.

Współpraca tych jednostek umożliwiła opracowanie koncepcji działań projektowych, odpowiadających realnym potrzebom ww. podmiotów. Ostateczny zakres zaplanowanych w ramach projektu działań w ramach poszczególnych obszarów został poprzedzony wieloma konsultacjami, spotkaniami i szkoleniami ww. osób ze specjalistycznymi firmami doradczymi specjalizującymi się w obszarze cyberbezpieczeństwa. Informuję również, że ostateczna analiza zidentyfikowanych potrzeb w przedmiotowym zakresie, która została ujęta w złożonym wniosku, została przeprowadzona z udziałem zewnętrznej firmy doradczej. Wszystkie poczynione w ramach dokonanych analiz i uzgodnień na potrzeby jednostek w zakresie cyberbezpieczeństwa przed ostatecznym złożeniem wniosku o dofinansowanie zostały zaakceptowane przez Sekretarza urzędu.

(akta kontroli str. 565)

3. Starostwo, w związku z § 4 ust. 1 pkt 4 umowy o powierzenie grantu na realizację zadania pn. *Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego*, przekazało w dniu 29 maja 2024 r. za pośrednictwem ePUAP do NASK uzupełnione w formacie .xlsx *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego* wykonane oddzielnie dla Starostwa, PUP i PCPR.

(akta kontroli str. 73-75)

4. Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0673/FERC.02.02-CS.01-001/23/2024, ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), w ramach Priorytetu II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, konkurs grantowy w ramach projektu grantowego „Cyberbezpieczny Samorząd" została zawarta pomiędzy Powiatem Ostrowieckim (dalej: Powiat) a Skarbem Państwa, w którego imieniu działało Centrum Projektów Polska Cyfrowa (dalej: CPPC lub Grantodawca) w dniu 6 maja 2024 r. Grantodawca przyznał Powiatowi dofinansowanie[11] na realizację projektu pn. *Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego* (dalej: Projekt) w kwocie 850 tys. zł[12]. W ramach projektu Starostwo przewidziało wydatki na zadanie nr 1 – *Obszar kompetencyjny* w kwocie 61 007 zł[13], na zadanie nr 2 – *Obszar organizacyjny* w kwocie 114 390 zł[14] i na zadanie nr 3 – *Obszar techniczny* w kwocie 674 603 zł[15]. Udział procentowy poszczególnych zadań w kwocie ogółem wynosił odpowiednio 7,2%, 13,5% i 79,4%. Powiat zobowiązał się zrealizować projekt w okresie maksymalnie 24 miesięcy od dnia wejścia w życie umowy, tj. do 6 maja 2026 r.

(akt kontroli str. 5-40, 43-72)

W Projekcie uczestniczyły również PUP i PCPR. Jednostki nie korzystały z wspólnych zasobów informatycznych i systemów teleinformatycznych ze Starostwem.

W Projekcie w celu likwidacji luk w obszarze organizacyjnym w Starostwie oraz PUP przewidziano przeprowadzenie przeglądu zgodności polityk z KRI i KSC oraz

[11] W tym dofinansowanie ze środków Unii Europejskiej w wysokości 82% i z budżetu państwa w wysokości 18%.

[12] W tym Starostwo – 551 751 zł, PCPR – 143 910 zł i PUP – 154 339 zł.

[13] W tym Starostwo – 19 680 zł, PCPR – 20 049 zł i PUP – 21 278 zł.

[14] W tym Starostwo – 73 800 zł, PCPR – 20 295 zł i PUP – 20 295 zł.

[15] W tym Starostwo – 458 271 zł, PCPR – 103 566 zł i PUP – 112 766 zł.

aktualizacje SZBI. Dla PCPR przewidziano opracowanie całościowego SZBI. Na zakończenie projektu dla wszystkich jednostek przewidziano wykonanie audytu powdrożeniowego wraz z raportem. Powyższe zadania miały być zrealizowane z wykorzystaniem podmiotów zewnętrznych posiadających odpowiednie doświadczenie oraz kwalifikacje. Przewidziano także wsparcie w zakresie przygotowania projektu przez podmiot zewnętrzny wyspecjalizowany w przygotowaniu i zarządzaniu projektami ICT[16] finansowanymi ze środków pomocowych. W zakresie organizacyjnym przewidziano również przeprowadzenie działań promocyjnych zgodnie z wymaganiami ustawowymi oraz zapisami umowy o Powierzenie Grantu.

W ramach Projektu w obszarze kompetencyjnym przewidziano szkolenia w zakresie podstaw cyberbezpieczeństwa wszystkich pracowników Starostwa, PUP i PCPR. Dla kadry kierowniczej dodatkowo przewidziano szkolenia w zakresie polityki, procedur oraz regulacji wewnętrznych i zewnętrznych dotyczących bezpieczeństwa informacji, systemu zarządzania bezpieczeństwem informacji, a także zagadnień związanych z identyfikacją i zarządzaniem ryzykiem oraz incydentami. W przypadku Starostwa oraz PUP szkolenia mają być przeprowadzone dwukrotnie: w trakcie i na zakończenie projektu. Dodatkowo przewidziano szkolenie specjalistyczne dla pracowników IT[17] PUP i PCPR w zakresie zarządzania urządzeniami sieciowymi firmy Fortigate. Starostwo Powiatowe nie posiadało etatowego pracownika IT, więc w projekcie nie przewidziano szkolenia IT dla tej jednostki.

W Projekcie w obszarze technicznym przewidziano wzmocnienie w Starostwie infrastruktury sieciowej. Przewidziano zakup UTM[18] łącznie z rozbudową oprogramowania e-Audytor[19], co miało umożliwić inwentaryzację aktywów IT jednostki, monitorowanie sieci i jej użytkowników, dokumentowanie działań i zdarzeń, a także pozwolić na ochronę sieci przed wyciekami danych. Pasywne skanowanie podatności sieci miało być realizowane przez moduł na UTM. Dodatkowo, zapewnienie bezpieczeństwa plików systemowych, monitorowanie sieci oraz wykrywanie i reagowanie na incydenty na poziomie endpoint miało być realizowane przez zakupione w ramach projektu oprogramowanie antywirusowe z modułem EDR[20]. Zostanie ono zainstalowane na zakupionym w ramach projektu serwerze, który będzie stanowił także platformę pod maszyny wirtualne obsługujące m.in. system archiwizacji danych, logów i działań w systemie. System archiwizacji Starostwa miał być wzmocniony poprzez zakup macierzy dyskowej wraz z oprogramowaniem do zarządzania kopiami zapasowymi, a także NAS[21] do przechowywania kopii zapasowych. Zasilanie dla serwera oraz przełączników miał zapewniać zakupiony w ramach projektu UPS[22]. W PUP przewidziano zakup trzech przełączników zarządzalnych klasy enterprise umożliwiających segmentację sieci jednostki. Integracja nowych przełączników

[16] Ang. Information and Communication Technologies – Technologie Informacyjno-Komunikacyjne.
[17] Ang. Information Technology (technika informatyczna).
[18] Ang. Unified Threat Management (wielofunkcyjna zapora sieciowa zintegrowana w postaci jednego urządzenia).
[19] System do zarządzania i monitorowania infrastruktury IT.
[20] Ang. Endpoint Detection and Response (narzędzie służące wykrywaniu i reagowaniu na podejrzane aktywności na urządzeniach końcowych)
[21] Ang. Network Attached Storage (technologia umożliwiająca podłączenie zasobów pamięci dyskowych bezpośrednio do sieci komputerowej).
[22] Ang. Uninterruptible Power Supply (zasilacz awaryjny).

z posiadanymi przez PUP urządzeniami firmy Fortinet umożliwi kompleksową ochronę sieci łącząc zabezpieczenia na różnych poziomach infrastruktury oraz wdrożenie polityki bezpieczeństwa na poziomie portów i protokołów, co zwiększy kontrolę nad ruchem w sieci. Przełączniki klasy enterprise mają zapewnić funkcję kontroli dostępu i jego ograniczenia tylko dla uprawnionych użytkowników i urządzeń. Do podtrzymania zasilania przełączników zaplanowano zakup dwóch zasilaczy UPS zapewniających urządzeniom ciągłość działania. Wykrywanie, zapobieganie, monitorowanie i wyszukiwanie zagrożeń oraz monitorowanie działań w sieci w czasie rzeczywistym na endpointach miało być realizowane przez chmurowe (SaaS) oprogramowanie antywirusowe nowej generacji z funkcjonalnością EDR.
Dla PCPR w projekcie zaplanowano unowocześnienie infrastruktury IT poprzez zakup nowego, zarządzalnego przełącznika, a także serwera (wraz z systemem operacyjnym oraz licencjami dostępowymi), na którym zostanie zainstalowane oprogramowanie e-Audytor. Realizację polityki ochrony danych w zakresie bezpiecznego przechowywania kopii zapasowych ma zapewnić zakupiony w ramach Projektu serwer NAS, a do podtrzymania zasilania zaplanowano zakup zasilacza UPS. Wsparcie w zakresie inwentaryzacji, monitorowania oraz zarządzania bezpieczeństwem infrastruktury IT jednostki realizowane będzie przez zakupione w ramach projektu oprogramowanie e-Audytor.
Wskazane we wniosku o dofinansowanie koszty spełniały warunki kwalifikowalności określone w § 4 pkt 7 regulaminu konkursu grantowego pn. *Cyberbezpieczny Samorząd*.

(akta kontroli str. 5-40)

W Starostwie nie sporządzono harmonogramu realizacji projektu.

(akta kontroli str. 41)

Starosta wyjaśniła: *Harmonogram realizacji projektu pn. „Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego" nie został sporządzony w formie odrębnego dokumentu przede wszystkim z uwagi na brak wymogu w przedmiotowym zakresie, wynikającego m.in. z dokumentacji konkursowej na etapie naboru wniosków o dofinansowane w ramach przeprowadzonego konkursu grantowego. Również żaden z dokumentów stanowiących załączniki do umowy o dofinasowanie na etapie składania wniosku o dofinansowanie dla ww. projektu, nie stanowił wzoru harmonogramu, do sporządzenia którego Grantobiorca zostałby zobligowany. Jednocześnie informuję, że prowadzone w ramach przedmiotowego projektu grantowego działania realizowane są zgodnie z terminami wynikającymi z umowy o dofinansowanie oraz w oparciu o zapisy dokumentacji konkursowej dla Działania 2.2 „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027. Z uwagi na stosunkowo prostą strukturę projektu, ograniczoną liczbę zadań oraz jasno określone terminy realizacji w dokumentacji konkursowej, funkcję harmonogramu pełnią wytyczne wynikające z wyżej wspomnianej dokumentacji oraz zapisy zawarte w umowie o dofinansowanie. Zgodnie z § 3 ust. 1 zawartej w dniu 06.05.2024 r. umowy o powierzenie grantu o numerze FERC.02.02-CS.01- 001/23/0673/FERC.02.02-CS.01-001/23/2024, Grantobiorca zobowiązany jest do realizacji projektu w zakresie rzeczowym wynikającym z wniosku o przyznanie grantu w okresie maksymalnie 24 miesięcy od dnia wejścia w życie umowy, ale nie dłużej niż do dnia 30 czerwca 2026 r., co w naszym przypadku oznacza, że realizowany projekt musi zostać zakończony w terminie do dnia 6 maja 2026 r. Zaznaczam, że prowadzone w ramach*

projektu działania realizowane są etapowo, z bieżącym monitoringiem postępu i zgodności z wymaganiami programu FERC oraz zapisami umowy o dofinansowanie. Wszystkie zaplanowane zadania, w tym zakup sprzętu i oprogramowania, przeprowadzenie szkoleń oraz wdrożenie procedur zwiększających odporność na cyberzagrożenia, są wykonywane zgodnie z założeniami projektowymi. W związku z powyższym, formalne opracowanie dodatkowego harmonogramu w postaci osobnego dokumentu nie jest niezbędne do skutecznego zarządzania projektem. Realizacja zadań jest na bieżąco monitorowana wewnętrznie, a wszystkie działania prowadzone są zgodnie z przyjętym wewnętrznie planem rzeczowo-finansowym i terminami wynikającymi z umowy.

(akta kontroli str. 565-566)

NASK przekazał środki na realizację Projektu w dwóch ratach. Na wyodrębniony na potrzeby Projektu rachunek bankowy Starostwa 13 czerwca 2024 r. wpłynęła kwota 255 000 zł[23], a w dniu 8 lipca 2024 r. pozostałe środki w wysokości 595 000 zł[24].

(akta kontroli str. 288, 434-437)

Na dzień zakończenia czynności kontrolnych, tj. 10 czerwca 2025 r. Starostwo nie zrealizowało szkoleń przewidzianych w zadaniu nr 1 – *Obszar kompetencji*. Szkolenia dla pracowników i kadry kierowniczej zostały zaplanowane do realizacji w III kwartale 2025 r. i I kwartale 2026 r. Starostwo dokonało wyboru oferty na szkolenie dla informatyków z PCPR i PUP. Na dzień 10 czerwca 2025 r. umowa nie została jeszcze podpisana. W ramach zadania nr 2 – *Obszar organizacyjny* zakupiono:

- usługę doradztwa specjalistycznego – przygotowanie projektu. Usługę zrealizowano w zakresie przygotowania koncepcji projektu. Dokonano zapłaty 14 760 zł, pozostała kwota 3690 zł zostanie zapłacona po zakończeniu realizacji projektu;
- audyt zgodności z KRI-KSC dla SP, PUP i PCPR. Usługa została zrealizowana w zakresie dotyczącym Starostwa, trwają przygotowania do zrealizowania przez podmiot zewnętrzny audytu dla PUP i PCPR. Dokonano zapłaty 9840 zł, pozostało do zapłaty 4920 zł;

Na dzień 10 czerwca 2025 r. na zadanie nr 2 – *Obszar organizacyjny* wydatkowano 24 600 zł, co stanowiło 21,5% środków przeznaczonych na realizację zadania. W ramach zadania nr 2 pozostały do realizacji aktualizacje SZBI dla SP i PUP, opracowanie SZBI dla PCPR, audyt końcowy dla SP, PUP i PCPR oraz działania promocyjne. Aktualizacje i opracowanie SZBI oraz działania promocyjne zaplanowano na III kwartał 2025 r., a audyty końcowe na zakończenie realizacji projektu.

W ramach zadania nr 3 – *Obszar techniczny* zakupiono dla:

- Starostwa:
  - UTM Stormshekd SN 520 z pakietami za kwotę 54 783,02 zł;
  - dwa przełączniki 48p zarządzalne za kwotę 13 072,44 zł;
  - serwer 2x Silver 8 rdzeni, 512 RAM, 24 dysk SSD oraz SAS HDD, porty 10Gb, Windows Datacenter za kwotę 121 278,00 zł;

[23] W tym z budżetu UE – 209 100 zł i budżetu państwa – 45 900 zł.
[24] W tym z budżetu UE – 487 900 zł i budżetu państwa – 107 100 zł.

- macierz dyskowa 24x 2,4 TB SAS HDD wraz z osprzętem i instalacją za kwotę 87477,60 zł;
- serwer NAS, 16x8TB za kwotę 35 734,71 za kwotę 35 734,71 zł;
- UPS 3kVA- 3kW za kwotę 6412,51 zł;
- przedłużenie wsparcia oraz dodatkowe moduły E- Audytor za kwotę 20 937,06 zł;
- przedłużenie oraz rozszerzenie licencji ESET o moduł EDR dla 140 użytkowników za kwotę 35 977,50 zł[25];

– PUP:
- trzy przełączniki 48p zarządzalne Fortinet FortiSwitch 148F za kwotę 19 778,40 zł
- dwa UPS 3kVA- 3kW za kwotę 10 629,66 zł

– PCPR:
- przełącznik 48p zarządzalny z wkładką SFP za kwotę 3044,25 zł;
- serwer 128GB RAM 2x960GB SSD, 6x2.4tb, SAS zasilacze 2x800W, Windows 2022STD za kwotę 54 556,65 zł;
- licencja Windows Server Standard Device 55 CAL za kwotę 12 939,60 zł;
- UPS 3kVA-2,250kW za kwotę 4041,78 zł;
- Serwer NAS TS-855eU, 6x SSD DC500 3.84 TB 2.5 za kwotę 23 126,46 zł.

Zakupiony na potrzeby PUP i PCPR przez Starostwo sprzęt został przekazany do jednostek protokołem przekazania.

(akta kontroli str. 76-104, 550-557)

Zakup sprzętu wraz z oprogramowaniem został dokonany w trybie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych[26] oraz na podstawie uregulowań wewnętrznych w tym zakresie[27]. Pozostałe zakupy:

– usługi doradztwa w zakresie przygotowania projektu;
– wykonania audytu bezpieczeństwa informacji;
– przedłużenie oraz rozszerzenie licencji ESET o moduł EDR dla 140 użytkowników;
– przedłużenie wsparcia oraz dodatkowe moduły E- Audytor,

zostały przeprowadzone zgodnie z obowiązując w Starostwie regulaminem udzielania zamówień publicznych o wartości poniżej 130 000 zł netto.

Zrealizowane w ramach Projektu zakupy zostały dokonane zgodnie z §4 ust. 1 pkt 5 umowy o udzielenie grantu, tj. z należytą starannością, w szczególności ponosząc wydatki celowo, rzetelnie, racjonalnie i oszczędnie z zachowaniem zasady uzyskiwania najlepszych efektów z danych nakładów, zasady optymalnego doboru metod i środków służących osiągnięciu założonych celów, zgodnie z obowiązującymi przepisami prawa i zasadami obowiązującymi w ramach Programu oraz w sposób, który zapewni prawidłową i terminową realizację Projektu oraz osiągnięcie celów zakładanych we wniosku o przyznanie grantu.

---

[25] Całkowita wartość subskrypcji na dwa lata, tj. od 1 styczeń 2025 r. do 31 grudnia 2026 r. stanowi kwotę 47 970,00 zł. Wartość subskrypcji za okres od 1 lipca 2026 r. do 31 grudnia 2026 r. w kwocie 11 992,50 zł stanowi koszt niekwalifikowalny i została poniesiona ze środków własnych Powiatu Ostrowieckiego.

[26] Dz. U. z 2024 r. poz. 1320 ze zm.

[27] Regulaminy udzielania zamówień publicznych o wartości równej lub wyższej od 130 000 zł netto wprowadzone zarządzeniami Starosty nr Or.I.120.1.5.2021 z 21 stycznia 2021 r. i Or.I.120.1.122.2024 z 4 grudnia 2024 r.

(akta kontroli str. 43-72, 105-287)

Zarządzeniem Nr OR.I.120.1.63.2024 z 2 lipca 2024 r. Starosta wprowadził zasady rachunkowości i plan kont dla Projektu. Ewidencja księgowa dla Projektu była wyodrębniona i umożliwiała identyfikację wszystkich operacji finansowych, co było zgodne z § 4 ust. 1 pkt 6 umowy o udzielenie grantu.

(akta kontroli str. 289-297)

Na dzień 10 czerwca 2025 r. na zadanie nr 3 – *Obszar techniczny* wydatkowano 503 789,64 zł, co stanowiło 74,7% środków przeznaczonych na realizację zadania. Łącznie w ramach projektu wydatkowano 528 389,64 zł, tj. 62,2% zaplanowanych środków. Zakupiono wszystkie zaplanowane urządzenia. Umowy zawarto na zakup pozostałych licencji i oprogramowania, tj.:

- oprogramowania do backupu i archiwizacji danych (licencja 2 lata) dla SP o wartość według złożonej oferty 13 510,32 zł;
- oprogramowanie EDR CrowdStrike (licencja 2 lata) dla PUP o wartość według złożonej oferty 29 483,10 zł;
- licencja na oprogramowanie e-Auditor dla PCPR o wartość według złożonej oferty 20 496,72 zł.

Łącznie na wykonanie całego zadania nr 3 (zakupiony lub objęty umowami sprzęt i oprogramowanie) wykorzystano 579 272,28 zł, co stanowi 85,9% zakładanych środków. Podczas realizacji zadania nr 3 powstały oszczędności w kwocie 95 330,72 zł.

(akta kontroli str. 76-77, 516-549)

5. Starostwo nie posiadało dokumentów potwierdzających prowadzenie monitoringu działań realizowanych przez PUP i PCPR.

(akta kontroli str. 41)

Sekretarz Powiatu Ostrowieckiego (dalej: Sekretarz) poinformował m.in.: mając na uwadze, że wsparciem w ramach przedmiotowego projektu zostały objęte trzy jednostki organizacyjne Powiatu Ostrowieckiego, tj. Starostwo Powiatowe, PUP oraz PCPR, działania założone w ramach projektu realizowane są przez pracowników Starostwa Powiatowego w ścisłej i bieżącej współpracy z informatykami ww. jednostek podległych oraz przedstawicielem firmy, prowadzącej obsługę informatyczną Starostwa Powiatowego Wszelkie czynności związane z przygotowaniem i realizacją projektu są na bieżąco monitorowane przez komórkę organizacyjną Starostwa Powiatowego, prowadzącą obsługę merytoryczną i administracyjną projektu, tj. Wydział Inwestycji, Infrastruktury i Transportu, w strukturach którego funkcjonuje Referat Inwestycji i Rozwoju Powiatu. Wyżej wskazana komórka organizacyjna Starostwa Powiatowego, w ramach zawieranych umów z wyłonionymi wykonawcami na dostawę sprzętu i oprogramowania, koordynowała przeprowadzone dostawy sprzętu i oprogramowania. Kierownik referatu wraz z przedstawicielem firmy prowadzącej obsługę informatyczną uczestniczyli w odbiorach dokonanych dostaw na potrzeby Starostwa Powiatowego zgodnie z podpisanymi protokołami odbiorów. W przypadku dostaw sprzętu i oprogramowania dedykowanych PUP oraz PCPR, były one bezpośrednio dostarczane przez wybranych wykonawców do siedzib ww. instytucji z udziałem informatyków tych jednostek. Proces dostaw i odbiorów przez cały czas był monitorowany drogą telefoniczną oraz w ramach bezpośrednich spotkań z informatykami jednostek objętych wsparciem przez Referat Inwestycji i Rozwoju Powiatu, dzięki czemu wszystkie dostawy zostały przeprowadzone w terminie

umownym. Zgodnie z podpisanymi protokołami odbioru zrealizowanych dostaw, strony dokonujące odbioru oświadczyły, że dostawy stanowiące przedmiot poszczególnych zamówień zostały zrealizowane przez Wykonawców zgodnie z postanowieniami SWZ i ofertami Wykonawców oraz funkcjonują prawidłowo, a dostawy zostały zrealizowane zgodnie z zapisami zawartych umów. Jednocześnie, strony odbierające potwierdziły, że dostarczone urządzenia/oprogramowania zostały odebrane przez uprawnionych pracowników bez zastrzeżeń jako w pełni sprawne. (…) Odnosząc się do powyższego, informuję, że dzięki właściwie prowadzonej współpracy jednostek, w których realizowane są działania na rzecz poprawy cyberbezpieczeństwa w ramach realizowanego projektu grantowego oraz zaangażowaniu pracowników Starostwa Powiatowego, odpowiedzialnych za realizację przedmiotowego zakresu projektu, monitorowanie postępu podejmowanych działań przez cały okres realizacji projektu przebiega właściwie. Dotychczas w ramach prowadzonego monitoringu projektu, polegającego na systematycznym śledzeniu postępu prac, jego zgodności z zapisami wniosku o dofinansowanie oraz skuteczności wdrażanych rozwiązań w celu zapewnienia, że projekt osiąga swoje cele w sposób bezpieczny, efektywny i zgodny z założeniami i wymaganiami, nie stwierdzono żadnych niezgodności oraz uchybień.

(akta kontroli str. 379-380)

6. Zarząd Powiatu Ostrowieckiego 6 marca 2024 r. udzielił pełnomocnictwa Kierownikowi Referatu Rozwoju i Inwestycji Starostwa do podejmowania w imieniu Powiatu Ostrowieckiego wszelkich czynności związanych z przygotowaniem, realizacją oraz trwałością projektu w ramach konkursu grantowego Cyberbezpieczny Samorząd realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Pełnomocnictwo w szczególności obejmowało:

- złożenie oraz aktualizację wniosku o przyznanie grantu;
- składanie wyjaśnień, uzupełnień i poprawek do wniosku o przyznanie grantu i załączników;
- składanie wniosków o płatność wraz z załącznikami;
- wykonywanie innych prac niezbędnych do prawidłowej realizacji i rozliczenia wniosku o przyznanie grantu.

Pełnomocnictwo zostało udzielone na okres realizacji oraz trwałości projektu w ramach konkursu Cyberbezpieczny Samorząd.

Poza kierownikiem Referatu Inwestycji i Rozwoju Powiatu w bezpośrednią oraz merytoryczną realizację projektu zaangażowani byli Naczelnik Wydziału Inwestycji, Infrastruktury i Transportu oraz dwóch Inspektorów ds. zamówień publicznych i przetargów, z tym że jeden od 1 lutego 2025 r. został przeniesiony do innej jednostki samorządowej. Zakres merytoryczny spraw prowadzonych w ramach realizowanego projektu przez każdego z ww. pracowników Starostwa wynikał z obowiązujących zakresów czynności. Pracownicy posiadali niezbędne kompetencje do realizacji projektu.

Starostwo nie zatrudniało pracownika etatowego na stanowisku informatyka. Obsługę informatyczną Starostwa, na podstawie zawartej umowy prowadziła firma zewnętrzna. Zgodnie z zapisami umowy, firma sprawowała rolę administratora technicznego, do którego zadań należało m.in.:

- administrowanie siecią lokalną i urządzeniami UTM;
- zabezpieczenie zbiorów danych od strony technicznej;

- współpraca z inspektorem ochrony danych osobowych w zakresie ochrony dostępu do danych;
- konfigurowanie serwerów, sieci komputerowych, oprogramowania systemowego i aplikacji w stopniu umożliwiającym zabezpieczenie danych przed nieupoważnionym dostępem oraz nieuprawnionym modyfikowaniem;
- nadzorowanie systemów zarządzających używaniem haseł;
- rekomendowanie zakupu programów komputerowych, ich wdrażanie, kontrola funkcjonowania i przydatności użytkowej oraz ich aktualizacja;
- pełnienie roli administratora systemów informatycznych.

Przedstawiciel firmy zewnętrznej brał merytoryczny udział przez cały okres realizacji projektu, z uwzględnieniem etapu aplikowania o środki grantu.

(akta kontroli str. 16, 298-378)

Sekretarz poinformował: *zarówno na etapie czynności związanych z przygotowaniem, jak również realizacją projektu, zaangażowani byli również informatycy PUP oraz PCPR, będący etatowymi pracownikami poszczególnych jednostek organizacyjnych*.

(akta kontroli str. 381-382)

7. Podczas realizacji Projektu nie wystąpiła istotna rotacja personelu, która mogłaby mieć wpływ na sprawną realizację projektu. Spośród osób biorących udział w realizacji Projektu jedynie jeden Inspektor ds. zamówień publicznych i przetargów odszedł do innej jednostki organizacyjnej.

(akta kontroli str. 381-382)

8. Starostwo nie określiło minimalnych wartości wskaźników produktu i rezultatu projektu wskazanych w załączniku nr 9 do Regulaminu Konkursu Grantowego.

(akta kontroli str. 41)

Starosta wyjaśniła: *Zgodnie z dokumentacją przeprowadzonego konkursu grantowego, w szczególności z Załącznikiem nr 9 - Opis wskaźników projektu Cyberbezpieczny Samorząd, Wnioskodawca na etapie składania wniosku o dofinansowanie zobowiązany był do określenia wskaźników produktu i rezultatu, które miały być adekwatne i mierzalne, jednak sam regulamin, jak również formularz wniosku aplikacyjnego nie nakładał obowiązku wskazania minimalnych wartości liczbowych dla wskaźników rezultatu na etapie składania wniosku. Biorąc pod uwagę, że nie było jednoznacznego wymogu przypisywania tym wskaźnikom konkretnych, liczbowych wartości minimalnych, zaś uwzględniając, że opis i sposób weryfikacji poszczególnych wskaźników pozwoli na ocenę osiągnięcia zakładanych celów po zrealizowaniu projektu, wskazanie konkretnych wartości liczbowych na etapie składania wniosku o dofinansowanie byłoby niemożliwe do wykonania, gdyż określenie efektów jakościowych czy podanie konkretnej liczby pracowników, którzy zostaną przeszkoleni w ramach projektu, było trudne do określenia przed rozpoczęciem projektu, chociażby z uwagi na proces fluktuacji wśród pracowników jednostek objętych wsparciem. Jednocześnie podkreślam, że na etapie przygotowania wniosku o dofinansowanie, w celu oszacowania wartości kosztów dla działań przypisanych do poszczególnych obszarów, założono szacunkowe wartości dla określonych wskaźników, które zostały przyjęte w formie roboczej i nie stanowią oficjalnego dokumentu dla realizowanego projektu. Niezależnie od braku minimalnych wartości liczbowych, projekt przewiduje konkretne działania i produkty*

(np. przeszkolenie pracowników, opracowanie polityk bezpieczeństwa), których realizacja bezpośrednio przekłada się na osiągnięte rezultaty projektu.

(akta kontroli str. 570)

Starostwo zgodnie z § 7 ust. 2 umowy przekazał sprawozdanie za okres 12 miesięcy, tj. od 6 maja 2024 r. do 14 maja 2025 r. W sprawozdaniu nie uzupełniono wskaźników rezultatu za wyjątkiem liczby podmiotów wspartych w zakresie cyberbezpieczeństwa. Opis wykonanych działań był tożsamy z przedstawionym we wcześniejszej części niniejszego wystąpienia.

(akta kontroli str. 383-385)

Starosta wyjaśniła m.in.: *Zgodnie z udostępnionym na stronie internetowej projektu Cyberbezpieczny Samorząd dokumentem, stanowiącym instrukcję dotyczącą dokumentacji rozliczającej w projekcie „Cyberbezpieczny Samorząd" (zakładka „Materiały dodatkowe"), wartości bazowe dla przypisanych wskaźników rezultatu należy, podobnie jak wartości osiągnięte dla tych wskaźników, wykazać na etapie wniosku rozliczającego zaliczkę, który zostanie przedłożony Grantodawcy po zrealizowaniu projektu, jednak w terminie nie późniejszym niż do dnia 30 czerwca 2026 r.*

(akta kontroli str. 570-571)

9. Przeprowadzone oględziny wykazały, że zakupiony w ramach projektu sprzęt znajduje się w Starostwie, PUP oraz PCPR. W serwerowni Starostwa, w szafie serwerowej, zamontowane były: serwer Dell, macierz Dell, przełącznik sieciowy, serwer NAS, UMT Stormshield oraz zasilacz UPS. Na serwerze zainstalowane było oprogramowanie E-Audytor (przedłużenie wsparcia oraz dodatkowe moduły) oraz ESET (przedłużenie oraz rozszerzenie licencji). W budynku PCPR w serwerowni zamontowane były w szafie serwerowej: serwer Dell R760xs, serwer plików NAS oraz zasilacz UPS. Natomiast w rozdzielni zamontowany był switch Ubiquiti. Sprzęt był użytkowany. W budynku PUP w serwerowniach znajdowały się trzy przełączniki sieciowe Fortiner oraz dwa zasilacze awaryjne UPS. Dwa przełączniki sieciowe i jeden UPS były zamontowane w szafie serwerowej. Pozostały sprzęt znajdował się w serwerowni i nie był zainstalowany.

(akta kontroli str. 386-387)

Sekretarz Powiatu poinformował: *w przypadku jednostki PUP, na potrzeby przeprowadzonych w dniu 13 maja br. oględzin zakupionego sprzętu i oprogramowania, sprzęt w postaci zasilacza UPS (1 szt.) oraz przełącznika sieciowego Fortiner (1 szt.), znajdujący się w szafie serwerowej w pomieszczeniu na kondygnacji piwnic, w celu udostępnienia do weryfikacji osoby kontrolującej projekt, został wymontowany do oględzin, po czym ponownie zainstalowany przez informatyka jednostki w miejscach przeznaczenia.*

(akta kontroli str. 380)

W dniu 16 lipca 2024 r. firma zewnętrzna przeprowadziła audyt bezpieczeństwa informacji w Starostwie[28]. Celem audytu było przedstawienie zaobserwowanego przez audytorów stanu bezpieczeństwa informacji w jednostce oraz wskazanie ewentualnych podatności mających wpływ na przetwarzanie danych. Audyt został przeprowadzony pod kątem zgodności z obowiązującymi przepisami

[28] Raport z audytu sporządzono 20 sierpnia 2024 r.

prawa w zakresie przetwarzania informacji oraz dobrych praktyk i standardów bezpieczeństwa. Z audytu sporządzono 87 rekomendacji, w tym 28 rekomendacji zalecających utrzymanie bieżącego stanu. W czasie audytu zidentyfikowano również siedem zagrożeń.

Do rozpoczęcia kontroli, tj. przez 286 dni od sporządzenia audytu, Starostwo nie zrealizowało większości rekomendacji istotnych dla zapewnienia bezpieczeństwa informacji.

(akta kontroli str. 388-433)

Starosta wyjaśniła m.in.: *Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i opracowanie kompleksowych regulacji wewnętrznych to proces złożony, czasochłonny i wymagający specjalistycznej wiedzy oraz znacznych zasobów wewnętrznych. Obejmuje on swoim zakresem tworzenie polityk, definiowanie procesów i ich ciągłe dostosowywanie. Występuje niedobór wewnętrznego personelu z niezbędną wiedzą w zakresie zarządzania bezpieczeństwem informacji i dokumentacji. Chociaż realizowany projekt Cyberbezpieczny Samorząd obejmuje działania szkoleniowe w ramach obszaru kompetencyjnego, wpływ tych szkoleń na rozwój założonych SZBI może nie być natychmiastowy. Mimo że realizowany projekt grantowy uwzględnia komponent organizacyjny, dotychczasowe działania koncentrowały się przede wszystkim na aspektach technicznych. W najbliższym czasie zostaną przeprowadzone działania związane z realizacją pozostałych zamierzeń, zaplanowanych w projekcie, jak na przykład dotyczących dokumentacji SZBI. (...)* Powszechnym wyzwaniem dla samorządów jest „Brak spójnego systemu identyfikacji i oceny ryzyka". Bez jasnej metodologii i narzędzi, przeprowadzanie regularnych analiz jest trudne. Analiza ryzyka wymaga przeszkolonego personelu i potencjalnie specjalistycznego oprogramowania, których brakuje. Jest to proces ciągły, a nie jednorazowe zadanie to wymaga stałego zaangażowania i zasobów, które są przekierowywane na bardziej pilne „techniczne" poprawki. Chociaż KSC nakłada obowiązek szacowania ryzyka w ciągu 3 miesięcy dla operatorów usług kluczowych, praktyczne wdrożenie może być wyzwaniem ze względu na istniejące braki zasobowe i kompetencyjne.

(akta kontroli str. 571-573)

NIK zwraca uwagę, że od przeprowadzenia audytu upłynęło 286 dni, a Starostwo nie wprowadziło szeregu zmian w zakresie zapewnienia bezpieczeństwa informacji tym samym nie minimalizowano istotnych ryzyk w tym zakresie.

10. Zgodnie z §13 umowy o powierzenie grantu „*Grantobiorca jest zobowiązany do utrzymania efektów Projektu, w tym do opracowania oraz wdrożenia procedury monitorowania utrzymania efektów Projektu tj. utrzymania środków trwałych i usług nabytych w ramach projektu przez okres min. 2 lat od zakończenia Projektu oraz utrzymania trwałości Projektu*". Zgodnie z umową o powierzeniu grantu Projekt ma być zrealizowany do 6 maja 2026 r.

(akta kontroli str. 43-72)

11. W Starostwie nie było opracowanego i wdrożonego SZBI, w rozumieniu § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

Zarządzeniem Nr Or.I.120137.2018 Starosty Ostrowieckiego z dnia 23 października 2018 r. wprowadzono *Instrukcję Zarządzania Systemem*

Informatycznym Starostwa Powiatowego w Ostrowcu Świętokrzyskim. Instrukcja dotyczyła m.in.:

- bezpieczeństwa eksploatacji sprzętu i oprogramowania;
- procedury korzystania z Internetu i poczty elektronicznej;
- procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych;
- metod i środków uwierzytelniania;
- procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie;
- procedur tworzenia kopii zapasowych;
- sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków;
- zasad udostępniania oraz przekazywania danych osobowych innym osobom i instytucją;
- procedur wykonywania przeglądów i konserwacji systemów.

Zarządzeniem Nr Or.I.120.1.22.2019 Starosty Ostrowieckiego z 20 maja 2019 r. wprowadzono *Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Starostwie Powiatowym w Ostrowcu Świętokrzyskim*, która została zmieniona zarządzeniem Nr Or.I.120.1.85.2021 Starosty Ostrowieckiego z 22 września 2021 r.

Obowiązujące w SP *Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Starostwie Powiatowym w Ostrowcu Świętokrzyskim* oraz *Instrukcja Zarządzania Systemem Informatycznym Starostwa Powiatowego w Ostrowcu Świętokrzyskim* dotyczyły bezpieczeństwa danych osobowych.

(akta kontroli str. 438-514, 579-580)

12. W okresie objętym kontrolą poza audytem przeprowadzonym na potrzeby Projektu nie przeprowadzono żadnego audytu z zakresu bezpieczeństwa informacji, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 578)

13. Starostwo wypełniało określone w § 11 umowy o powierzenie grantu dotyczące informacji i promocji o otrzymaniu grantu. Na facebook'u na profilu Powiatu Ostrowieckiego dnia 2 września 2024 r. zamieszczono informacje o realizacji projektu pn. Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego w ramach projektu grantowego Cyberbezpieczny Samorząd. Również na stronie internetowej Powiatu Ostrowieckiego zamieszczono informacje o Projekcie oraz w wersji elektronicznej plakat i logotyp. Na tablicach informacyjnych i drzwiach serwerowni w SP, PUP i PCPR zamieszczono plakaty informujące o wsparciu finansowym otrzymanym w ramach projektu Cyberbezpieczny Samorząd. Na zakupionym sprzęcie zamieszczono informacje, że zakup współfinansowany jest ze środków Unii Europejskiej. Wszystkie dokumenty związane z realizacją Projektu oznaczone były znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich.

(akta kontroli str. 386-387, 558-561)

Stwierdzone nieprawidłowości

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

1. W Starostwie nie było opracowanego i wdrożonego SZBI, w rozumieniu § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI.

(akta kontroli str. 438-514)

Starosta wyjaśniła: *W Starostwie Powiatowym w Ostrowcu Świętokrzyskim została opracowana i wdrożona Polityka Bezpieczeństwa w rozumieniu przepisów RODO, obejmująca szereg procedur oraz zabezpieczeń organizacyjnych i technicznych, mających na celu ochronę przetwarzanych danych osobowych. Dodatkowo funkcjonują inne regulacje dotyczące bezpieczeństwa systemów teleinformatycznych, jednakże nie zostały one dotąd ujęte w formie jednolitej, kompleksowej polityki bezpieczeństwa informacji w rozumieniu § 19 ust. 1 w związku z ust. 3 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności. Brak jednolitej polityki bezpieczeństwa informacji wynikał dotychczas z przekonania, że istniejące dokumenty i procedury częściowo realizują wymagania ww. rozporządzenia. Niemniej jednak, w związku z obowiązującymi przepisami oraz w trosce o pełną zgodność z KRI, Starostwo Powiatowe podjęło działania zmierzające do opracowania i wdrożenia polityki bezpieczeństwa informacji w wymaganym zakresie, jako odrębnego dokumentu obejmującego wszystkie elementy wskazane w § 20 ust. 2 przedmiotowego rozporządzenia i uwzględniło to działanie w ramach realizowanego projektu grantowego pn.: „Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego". Mając powyższe na uwadze, informuję, że w najbliższym czasie zostanie wdrożona w życie kompleksowa i spójna Polityka Bezpieczeństwa.*

(akta kontroli str. 566)

2. W SP nie przeprowadzono audytu z zakresu bezpieczeństwa informacji w 2023 r., pomimo że zgodnie z § 19 ust. 2 pkt 14 rozporządzenia KRI audyt taki powinien być przeprowadzany nie rzadziej niż raz w roku.

(akta kontroli str. 578)

Starosta wyjaśniła: *jako, że w ramach planowanego do realizacji projektu grantowego Cyberbezpieczny Samorząd założono przeprowadzenie audytu z zakresu bezpieczeństwa informacji w Starostwie Powiatowym, uznano, że w związku z ograniczonymi możliwościami sfinansowania jego wykonania ze środków własnych Powiatu, audyt ten zostanie zlecony w ramach przyznanego grantu, w związku z czym odstąpiono wówczas od jego przeprowadzenia.*

(akta kontroli str. 574)

Z § 19 ust. 2 pkt 14 rozporządzenia KRI wynika coroczny obowiązek przeprowadzania audytu.

NIK odstępuje od formułowania wniosku pokontrolnego w powyższym zakresie, ponieważ w 2024 r. przeprowadzono audyt z zakresu bezpieczeństwa informacji.

IV. Uwagi i wnioski

Wniosek

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK wnioskuje o opracowanie i wdrożenie SZBI spełniającego wymogi określone w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI.

Uwagi

NIK nie formułuje uwag.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne sporządzono w postaci elektronicznej z użyciem kwalifikowanych podpisów elektronicznych.

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 Kielcach. 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 wniosku

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

Kielce, 2 lipca 2025 r.

Najwyższa Izba Kontroli
Delegatura w Kielcach
Dyrektor
Grzegorz Walendzik

/podpisano elektronicznie/

Kontroler

Piotr Fatalski

Główny specjalista kontroli państwowej

/podpisano elektronicznie/