NAJWYŻSZA IZBA KONTROLI

Delegatura w Kielcach

LKI.410.6.4.2025

Pan
Ernest Kumek
Wójt Gminy
Urząd Gminy Brody
ul. Stanisława Staszica 3
27-230 Brody

WYSTĄPIENIE POKONTROLNE

P/25/003 – Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Delegatura w Kielcach
ul. gen. T. Kościuszki 6, 25-310 Kielce
tel. 48412499100, lki@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy Brody (dalej: Urząd lub Gmina), ul. Stanisława Staszica 3, 27-230 Brody.
Kierownik jednostki kontrolowanej	Ernest Kumek, Wójt Gminy Brody od 7 kwietnia 2024 r. (dalej: Wójt); w okresie od 21 października 2018 r. do 6 kwietnia 2024 r. Wójtem Gminy Brody była Agata Bernat (dalej: były Wójt).
Zakres przedmiotowy kontroli	Realizacja przez gminy i powiaty powiatowe działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych w 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.
Kontrolerzy	Monika Górniak-Napora, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LKI/49/2025 z 30 kwietnia 2025 r. Łukasz Nowakowski, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LKI/48/2025 z 30 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

Pomimo, że obowiązek opracowania, ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI) wynikał z §20 ust. 1 rozporządzenia KRI z 12 kwietnia 2012 r., zgodnie z którym *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji (...)*, System ten został wprowadzony w Gminie dopiero w dniu 18 lutego 2025 r.

SZBI, w tym Polityka Bezpieczeństwa Informacji (dalej: PBI) nie spełniały wymogów Polskiej Normy PN-ISO/IEC 27001[3]. W okresie objętym kontrolą Wójt nie przeprowadził obowiązkowego corocznego audytu w zakresie bezpieczeństwa informacji wskazanego przepisami rozporządzeń KRI[4].

W Gminie podejmowano działania informacyjne dotyczące Projektu, tj. oznaczano znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich dokumenty związane z realizacją Projektu oraz umieszczano je w informacjach podawanych do wiadomości publicznej, informacje o projekcie umieszczono na stronie internetowej Urzędu).

Nie wypełniono jednak wymogu umieszczenia przynajmniej jednego plakatu o minimalnym formacie A3 informującego opinię publiczną o fakcie otrzymania dofinansowania z Projektu, co wynikało z §11 ust. 4 pkt 2 Umowy.

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

OBSZAR

Realizacja przez gminę działań w celu zwiększenia poziomu cyberbezpieczeństwa

Opis stanu faktycznego

W okresie objętym kontrolą Gmina nie posiadała aktualnej Strategii Rozwoju Gminy Brody (dalej: Strategia). Strategia na lata 2014-2020[6] została opracowana w okresie styczeń-lipiec 2014 r., jej aktualizacji dokonano w czerwcu 2015 r. Wójt wyjaśnił, że nie sporządzono nowego dokumentu Strategii na kolejny horyzont czasowy. Przyczyną tego była przede wszystkim konieczność skoncentrowania się na realizacji bieżących zadań gminy oraz kontynuacji rozpoczętych wcześniej inwestycji i projektów ujętych w Strategii obowiązującej do 2020 roku.

W dokumentach dotyczących opracowania Strategii na lata 2025-2030, przekazanych w trakcie kontroli, nie uwzględniono zagadnień związanych z cyberbezpieczeństwem.

(akta kontroli str. 8-9, 26-53)

---

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

[3] Zgodnie z §20 ust. 3 rozporządzenia KRI z 21 maja 2024 r. *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem.*

[4] §20 ust. 2 pkt 14 rozporządzenia KRI z 12 kwietnia 2012 r., §19 ust. 2 pkt 14 rozporządzenie KRI z 21 maja 2024 r. (dalej: rozporządzenia KRI).

[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] https://bip.brody.info.pl/strategia-rozwoju-gminy-brody-na-lata-2014-2020.html? – data dostępu 7 maja 2025 r.

Były Wójt wyjaśniła: *Przywoływana w piśmie strategia była realizowana w praktyce i w ocenie osób realizujących zadania z niej wynikające, wymagała aktualizacji w terminie wskazanym w piśmie (...). Realizując wszelkie aspekty funkcjonowania Urzędu otrzymywałam więc od podległych mi pracowników zwrotne informacje o spełnianiu przez wdrożoną strategię wymagań bezpieczeństwa w tym zakresie, co dawało realne przekonanie, że Gmina jest na bieżąco przygotowana (odporna) na ewentualne zewnętrzne zagrożenia. W trakcie sprawowania przeze mnie funkcji wójta podlegli mi pracownicy nie zgłaszali żadnych, li tylko potencjalnych (możliwych) zagrożeń, ale przede wszystkim nie doszło do naruszenia stosowanych zabezpieczeń, stąd realizacja w latach 2014-2020 strategii dała solidne podstawy do jej dalszego stosowania. Strategia ta, w dalszych latach, to jest po roku 2020 była kontynuowana jako ta która została w praktyce prawidłowo wcześniej realizowana. Działania, które były wykonywane w tej materii były czynnościami faktycznie związanymi z zapewnieniem bezpieczeństwa w rozumieniu KRI, przede wszystkim poprzez zatrudnienie fachowego personelu (...).*

(akta kontroli str. 74)

Prace nad opracowaniem nowej Strategii, z uwzględnieniem aktualnych uwarunkowań społecznych, gospodarczych i technologicznych, w tym także aspektów cyberbezpieczeństwa, podjęto w Urzędzie dopiero w 2025 r. W przygotowywanych materiałach studyjnych do opracowania Strategii nie były ujęte zagadnienia dot. cyberbezpieczeństwa.

(akta kontroli str. 9-10, 26-70)

Jak wyjaśniła była Wójt działania podejmowane w celu rozpoznawania potrzeb w zakresie zwiększania poziomu cyberbezpieczeństwa były związane z podnoszeniem świadomości zarówno pracowników, jak i osób korzystających z usług Urzędu w zakresie cyberbezpieczeństwa, zapewniając właściwą obsadę pracowniczą. Podała: *Miałam bieżący kontakt z pracownikami Panem Ł. W. i Panią E. S. i posiłkowo z panią T. W., zajmującymi stanowiska odpowiedzialne za poziom cyberbezpieczeństwa, to jest osobami w kompetencjach, których było zapewnienie zarówno odpowiedniego poziomu bezpieczeństwa informatycznego, jak również przeciwdziałanie ewentualnym zewnętrznym próbom ataku informatycznego. Pracownicy ci także dbali o właściwy obieg informacji w wewnętrznej sieci Urzędu. Wybór takiego postępowania z mojej strony okazał się optymalny, ponieważ w czasie moich kadencji Gmina nie miała sytuacji kryzysowych wynikających z cyberataków, które miałyby spowodować ograniczenia w funkcjonowaniu Urzędu*.

(akta kontroli str. 74)

NIK zauważa, że opisane wyżej działania ograniczały się do bieżącego wypełniania służbowych obowiązków m. in.: Wójta, informatyka Urzędu, pracownika do spraw kadr i inspektora danych osobowych (dalej: IOD). Nie podejmowano innych, dodatkowych, czynności mających na celu rozpoznawanie potrzeb w zakresie cyberbezpieczeństwa.

Na potrzeby udziału w Projekcie Cyberbezpieczny Samorząd (dalej: Cyberbezpieczny Samorząd lub Projekt), na przełomie lipca i sierpnia 2023 r., sporządzony został przez informatyka Urzędu *Raport potrzeb w zakresie zwiększenia potrzeb cyberbezpieczeństwa w Urzędzie Gminy Brody, Centrum Usług Wspólnych Gminy Brody, Gminny Ośrodek Pomocy Społecznej w Brodach, Zakład Gospodarki Komunalnej w Brodach* (dalej: Raport informatyka). Określał on m.in. potrzeby w zakresie sprzętu i oprogramowania w Urzędzie i jednostkach podległych, tj. w Centrum Usług Wspólnych (dalej: CUW), Gminnym Ośrodku

Pomocy Społecznej (dalej: GOPS) i Zakładzie Gospodarki Komunalnej (dalej: ZGK), potrzeby organizacyjne i kompetencyjne, w tym opracowanie i wdrożenie SZBI zgodnego z normami ISO, udział w specjalistycznych szkoleniach, w tym w zakresie administracji aplikacjami, systemami oraz z tematyki cyberbezpieczeństwa i hackingu[7] dla obsługi informatycznej oraz szkoleń z zakresu cyberbezpieczeństwa dla wszystkich pracowników.
Podstawą sporządzenia Raport informatyka było m.in.: sprawdzenie obecnych zabezpieczeń, systemów i procedur, aby zidentyfikować słabe punkty i obszary wymagające poprawy; ocena potencjalnych zagrożeń i ich możliwych skutków dla Urzędu; konsultacje, wywiady indywidualne i grupowe z pracownikami, przegląd obowiązujących regulacji i standardów oraz najlepszych praktyk w zakresie cyberbezpieczeństwa. Raport ten stanowił podstawę do opracowania koncepcji projektu wniosku grantowego.

(akta kontroli str. 78-82)

Raport informatyka wskazał na potrzebę wdrożenia silnych zabezpieczeń technicznych, regularne ich aktualizacje i testy, szkolenia i podnoszenie świadomości pracowników, regularne tworzenie kopii zapasowych danych umożliwiających przywrócenie funkcjonowania systemów po ewentualnym ataku lub awarii. Planowanymi miernikami działań miały być: liczba zagrożeń i czas reakcji na incydenty oraz liczba przeprowadzonych szkoleń i poziom wiedzy pracowników.

(akta kontroli str. 83)

Urząd, w dniu 16 maja 2024 r. przekazał do Naukowej i Akademickiej Sieci komputerowej – Państwowego Instytutu Badawczego (dalej; NASK-PIB) wypełnioną „Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego (dalej: Ankieta Dojrzałości), tj. w ciągu 28 dniu od dnia zawarcia umowy[8] o powierzenie grantu (dalej: Umowa)[9]. Zachowany został w ten sposób termin 30 dni od dnia zawarcia Umowy, zgodnie z §4 ust. 1 pkt 4 Umowy. Ankieta Dojrzałości została przeprowadzona i przekazana na adres skrytki e-PUAP NASK-PIB[10]. Ankieta dotyczyła Urzędu i jednostek biorących udział w Projekcie. Powyższe zostało potwierdzone przeprowadzonymi w ramach kontroli oględzinami skrytki ePUAP Urzędu.

(akta kontroli str. 154-156)

W dniu 18 kwietnia 2024 r. zawarta została Umowa pomiędzy Gminą a Skarbem Państwa, w imieniu którego do umowy przystąpiło Centrum Projektów Polska Cyfrowa (dalej: CPPC). Grant pochodził ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu bezpieczeństwa. Udzielony został w wyniku rozstrzygnięcia konkursu grantowego w ramach projektu Cyberbezpieczny Samorząd nr FERC.02.02-CS.01-001/23. Konkurs przeprowadziła NASK-PIB.
Zgodnie z postanowieniami Umowy Gminie przyznane zostały środki w wysokości 847,6 tys. zł, które miały zostać wypłacone w trzech transzach:

---

[7] Działanie polegające na wykorzystywaniu luk w zabezpieczeniach systemów komputerowych lub sieci w celu uzyskania nieautoryzowanego dostępu. Obejmuje to analizę, modyfikację i manipulację systemami informatycznymi, często w sposób wykraczający poza zamierzone przez twórców użycie.

[8] Podpisanej w dniu 18 kwietnia 2024 r.

[9] FERC.02.02-CS.01-001/23/1433/FERC.02.02.-CS.01-001/23/2024

[10] ePUAPNASK-PIB:/NASKInstytut/SkrytkaESP (akronim/temat: cyberbezpieczny.samorzad.ankieta).

pierwsza transza w terminie do 60 dni kalendarzowych po zawarciu Umowy (nie wcześniej jednak niż po przesłaniu Ankiet Dojrzałości), druga - w okresie 12 miesięcy od dnia podpisania Umowy (po m.in.: osiągnięciu 70% postępu rzeczowego realizacji transzy pierwszej) oraz trzecia - wypłacana w okresie 18 miesięcy od dnia podpisania Umowy (po m.in.: osiągnięciu 70% postępu rzeczowego realizacji transzy drugiej). Za kwalifikowane uznane były wydatki ponoszone w okresie kwalifikowalności, tj. od 1 czerwca 2023 r. przez okres maksymalnie 24 miesięcy od dnia zawarcia Umowy (nie dłużej jednak niż do 30 czerwca 2026 roku).
Wydatkowanie środków zaplanowano w trzech obszarach: organizacyjnym, kompetencyjnym i technicznym.
W obszarze organizacyjnym przyznano wsparcie w wysokości 37,5 tys. zł, na wdrożenie SZBI, przeprowadzenie audytów i Ankiet Dojrzałości w Urzędzie i w jednostkach podległych. Do zakończenia czynności kontrolnych w jednostce działania w ramach obszaru organizacyjnego nie były realizowane.
W obszarze kompetencyjnym Urzędowi przyznano wsparcie w wysokości 63,1 tys. zł, na szkolenie z zakresu cyberbezpieczeństwa i szkolenie specjalistyczne dla kadry informatycznej oraz szkolenie dla IOD. Szkolenia te dotyczyły m.in. przetwarzania danych w systemach informatycznych. Gmina uzyskała również środki na budowę platformy szkoleniowej w dziedzinie ochrony zasobów informatycznych dla wszystkich pracowników Urzędu i jednostek podległych. Do dnia zakończenia czynności kontrolnych wydatkowano 16,3 tys. zł w obszarze kompetencyjnym, co stanowiło 29% kwoty przyznanych środków.

(akta kontroli str. 11-13, 86-97, 98-127, 131-13)

W obszarze technicznym Urząd otrzymał 747 tys. zł na sprzęt: cztery przełączniki sieciowe dla Urzędu, urządzenia UTM[11], urządzenia NAS[12] do przechowywania kopii zapasowych, rozwiązania zasilania awaryjnego UPS[13], nabycie serwerów wraz z systemami operacyjnymi oraz licencjami dostępowymi dla użytkowników (dwa urządzenia dla Urzędu i po jednym dla jednostek podległych). Ponadto Urząd postanowił przeznaczyć środki na oprogramowanie:

- do inwentaryzacji aktów, ich konfiguracji, zarządzania nośnikami wymiennymi oraz wykrywania niepożądanych zdarzeń w infrastrukturze IT wraz ze wsparciem na czas trwania projektu (licencja bezterminowa, infrastruktura informatyczna Urzędu),
- system zabezpieczający przed wyciekiem danych (licencja bezterminowa, 65 stanowisk),
- oprogramowanie antywirusowe (licencja bezterminowa, 110 stanowisk)
- system do gromadzenia i analizy zapisów działań w systemach logów, (licencja bezterminowa, 65 stanowisk)
- system kopii zapasowych dla Urzędu (licencja bezterminowa, 65 stanowisk w tym sześć serwerów).

[11] Urządzenie UTM, czyli Unified Threat Management, to zintegrowane rozwiązanie do zarządzania zagrożeniami, które umożliwia ochronę sieci. Jest to urządzenie sprzętowe, które łączy wiele narzędzi cyberbezpieczeństwa – po jednym urządzeniu dla Urzędu i każdej z jednostek podległych

[12] Serwery NAS (Network-Attached Storage) to specjalne urządzenia lub rozwiązania komputerowe, które służą do przechowywania danych i udostępniania ich w sieci lokalnej lub internetowej - po jednym urządzeniu dla Urzędu i każdej z jednostek podległych

[13] Zasilanie awaryjne UPS (Uninterruptible Power Supply) to urządzenie, które zapewnia ciągłość zasilania w przypadku zaniku lub spadku napięcia w sieci elektrycznej – dwa urządzenia dla Urzędu i po jednym dla jednostek podległych.

Do zakończenia czynności kontrolnych w jednostce Urząd nabył oprogramowanie, dokonując wydatków na kwotę 143,7 tys. zł w w/w obszarze, co stanowiło 19% kwoty przyznanych środków. Zakupiono: oprogramowanie antywirusowe[14], oprogramowanie menedżera logów[15], oprogramowanie przeciwdziałające wyciekowi danych[16]. Łącznie w ramach realizacji Projektu do dnia zakończenia kontroli Urząd wydatkował 162 tys. zł (19% kwoty grantu). Nie zakupiono żadnych urządzeń i sprzętu, przeprowadzono natomiast szkolenia dla dwóch osób, tj. informatyka Urzędu oraz IOD. Wójt wyjaśnił, że brak zakupu sprzętu na wczesnym etapie realizacji projektu był świadomą decyzją organizacyjną, uzasadnioną m.in.: potrzebą zapewnienia zgodności technicznej pomiędzy wdrażanym oprogramowaniem a planowaną infrastrukturą. Odnośnie szkoleń podał, że były one konieczne dla przygotowania personelu do dalszej realizacji zadań.
Wszystkie wskazane powyżej wydatki były wydatkami kwalifikowanymi zgodnie z §4 ust. 7 Regulaminu. Finansowanie ze środków Unii Europejskiej było na poziomie 82%, a z budżetu państwa - 18%.

(akta kontroli str. 12-13, 86-97, 98-127,131-134, 268, 271, 274, 277, 280)

W dniu 5 września 2024 r. Wójt, działając na podst. §2 ust. 8 Umowy zwrócił się do NASK-PIB o wypłatę całości dofinansowania motywując wniosek planowaną realizacją Umowy do końca 2024 r. Transze wypłacono: dnia 4 czerwca 2024 r. (dwie operacje: 45,8 tys. zł oraz 208,5 tys. zł) oraz 31 października 2024 r. (dwie operacje: 486,5 tys. zł i 106,8 tys. zł). Tym samym Urząd otrzymał środki przeznaczone na realizację Projektu w pełnej wysokości.

(akta kontroli str. 128-130, 290-294)

Jak wyjaśnił Informatyk Urzędu, Projekt został zrealizowany maksymalnie w 30% - w ujęciu ilościowym[17]. Wskazał, że Urząd nie sporządził formalnego harmonogramu Projektu na etapie składania wniosku, niemniej informatyk Urzędu stworzył plan pracy porządkujący działania planowane w celu wykonania Umowy. Wójt zadeklarował, że Projekt zostanie zrealizowany zgodnie z Umową.

(akta kontroli str. 12-13, 131-134, 319-320)

W odpowiedzi na pytanie o harmonogram Projektu, Wójt wyjaśnił: *W pierwszej fazie realizacji projektu główny nacisk został położony na przeprowadzenie diagnozy dojrzałości cyberbezpieczeństwa zgodnie z wymaganiami projektu. Dopiero na podstawie wyników tej diagnozy możliwe było określenie priorytetów, zakresu działań oraz realistycznych terminów ich wdrożenia. Z tego względu harmonogram działań nie został stworzony na etapie składania wniosku o dofinansowanie ani bezpośrednio po podpisaniu umowy. (...) W październiku 2024 r., na podstawie zarządzenia 178/2024 Wójta gminy Brody, formalnie powołano zespół ds. realizacji projektu. W ślad za tym opracowano wewnętrzny harmonogram (...).*

(akta kontroli str. 10-11)

NIK zwraca uwagę, że ze względu na upływ czasu przeznaczony na realizację Umowy (ponad połowa okresu), przy realizacji Projektu w tym czasie na poziomie 30%, nie pozwala wykluczyć ryzyka niedotrzymania terminów realizacji Umowy.

---

[14] Bitdefender GravityZone Business Security Enterprise (Ultra).
[15] Safetica PRO on-prem.
[16] Energy Logserver Energy SIEM Lite.
[17] Na dzień 14 maja 2025 r.

W dniu 25 października 2024 r. Gmina zwróciła się do NASK-PIB o przedłużenie terminu realizacji Umowy do 30 czerwca 2026 r. Uzasadniając wniosek Wójt wskazał: *Powyższą prośbę motywuję tym, iż Gmina Brody ogłosiła już postępowanie przetargowe i jest po wyborze najkorzystniejszej oferty na zakup oprogramowań, w których w opisie przedmiotu zamówienia określiła, iż systemy mają posiadać wsparcie techniczne do 30.06.2026 r. (...) prosimy Państwa o wyrażenie zgody na aneksowanie terminu realizacji grantu do 30.06.2026 r., ponieważ w przypadku odmowy zmuszeni będziemy unieważnić przetarg*. Wyjaśnił również: *Wniosek o przedłużenie okresu realizacji grantu do czerwca 2026 r. był efektem trudności organizacyjno-kadrowych i chęci zapewnienia jakościowego wdrożenia wszystkich działań projektowych. Pomimo formalnych ograniczeń zawartych w umowie, Gmina Brody uznała za zasadne wystąpienie o zgodę na przesunięcie terminu*.
Do dnia zakończenia czynności kontrolnych Urząd nie uzyskał od NASK-PIB zgody na przedłużenie terminu realizacji Projektu. Nie podjęto innych działań w celu uzyskania od NASK odpowiedzi na prośbę o przedłużenie terminu realizacji Umowy.

(akta kontroli str. 14, 98-127, 306-318)

NIK zauważa, że termin realizacji umów dotyczących zakupu oprogramowania wraz ze wsparciem będzie przekraczał okres realizacji Projektu wskazany w §3 ust. 1 Umowy. Określono w nim, że *Grantobiorca zobowiązuje się zrealizować Projekt 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 30.06.2026 r.*
Postanowienia Umowy przewidują realizację Projektu maksymalnie do dnia 18 kwietnia 2026 r., gdyż Umowę zawarto dnia 18 kwietnia 2024 r.
Zgodnie z warunkami określonymi w Umowie[18], Urząd utworzył odrębny rachunek bankowy dla Projektu oraz dokonał faktycznego wyodrębnienia ewidencji księgowej[19].

(akta kontroli str. 108, 128-130, 135-144, 167-287)

We wniosku o przyznanie grantu[20] wskazano, że dofinansowaniem objęte zostaną działania podejmowane w celu zwiększenia poziomu cyberbezpieczeństwa, także w jednostkach podległych[21], tj. w GOPS, CUW oraz ZGK. W każdej z wyżej wymienionych jednostek przewidziano wdrożenie SZBI i wykonanie audytów oraz Ankiet Dojrzałości, a także utworzenie platformy szkoleniowej z zakresu cyberbezpieczeństwa – wspólnej dla Urzędu i jednostek podległych – umożliwiającej wszystkim pracownikom dostęp do szkoleń oraz aktualnych materiałów w zakresie cyberbezpieczeństwa.

(akta kontroli str. 86-89, 91-95, 133-134)

Zgodnie z wyjaśnieniami udzielonymi przez Wójta, w CUW planowane było wdrożenie dodatkowych zabezpieczeń w systemie obsługi finansowo-kadrowej i zarządzania oświatą, w GOPS - zabezpieczenie systemów obsługujących dane osobowe beneficjentów świadczeń, a w ZGK - zastosowanie rozwiązań

---

[18] §5 ust. 1 i §4 ust. 1 pkt 6.
[19] Zarządzenie Nr 248/2024 Wójta Gminy Brody z dnia 31 grudnia 2024 r. w sprawie prowadzenia wyodrębnionej ewidencji księgowej dla zadania „Cyberbezpieczny Samorząd" (dalej: Zarządzenie dotyczące odrębnej ewidencji księgowej).
[20] Wniosek o przyznanie Gminie Brody grantu w programie Cyberbezpieczny Samorząd, nr naboru FERC.02.02-CS.01-001/23.
[21] Stosownie do §3 ust. 1 Regulaminu Konkursu Grantowego: jednostki sektora publicznego z wyłączeniem placówek ochrony zdrowia.

zwiększających odporność systemów obsługujących infrastrukturę komunalną (np. kontrola dostępu do danych, segmentacja sieci). Dla każdej z w/w jednostek Wójt zaplanował zakup następującego sprzętu informatycznego:

- serwer wraz z systemem operacyjnym oraz licencjami dostępowymi dla użytkowników,
- rozwiązań zasilania awaryjnego UPS,
- urządzenia NAS do przechowywania kopii,
- urządzenie UTM wraz ze wsparciem serwisowym.

Do dnia zakończenia czynności kontrolnych, nie zakupiono sprzętu dla wskazanych jednostek.

(akta kontroli str. 14-16, 86-89, 91-95)

Urzędy i jednostki organizacyjne Gminy korzystały ze wspólnych zasobów informatycznych w ograniczonym zakresie, głównie w postaci: - połączenia lokalnej sieci komputerowej w której jednostki nie funkcjonują w ramach wspólnej sieci V-LAN[22], korzystania z poczty elektronicznej w ramach wspólnej domeny gminnej, współdzielonego dostępu do części usług administracyjnych (np. BIP). System zarządzania bezpieczeństwem informacji w Gminie funkcjonował głównie w ramach struktur Urzędu. SZBI nie obejmował swoim zasięgiem jednostek organizacyjnych Urzędu. Jednostki te nie posiadały odrębnych polityk.
Wójt wyjaśnił: (...) *Formalna integracja SZBI dla całej gminy nie została jeszcze zakończona. Wynika to z ograniczeń kadrowych i technicznych, które będą sukcesywnie eliminowane w toku dalszej realizacji projektu i planowanych działań wewnętrznych.*

(akta kontroli str. 16-17)

W zakresie obowiązków służbowych, uprawnień i odpowiedzialności głównego specjalisty ds. informatyki i bezpieczeństwa[23] w części dotyczącej szczegółowego zakresu obowiązków służbowych określono m.in. zadania w zakresie bezpieczeństwa informacji. Wskazano w nim m.in. udział w określaniu BPI, opracowywanie procedur w ramach SZBI.
W związku z realizacją grantu w Urzędzie, zarządzeniem 178/2024 Wójta Gminy Brody z dnia 14 października 2024 r.[24] powołano Zespół ds. Projektu „Wzmocnienie systemu cyberbezpieczeństwa w Urzędzie Gminy w Brodach" (dalej: Zespół ds. Projektu). W jego skład weszło osiem osób (sekretarz Gminy, Koordynator Projektu – główny specjalista ds. Informatyki i Bezpieczeństwa Informacji, Kierownik Referatu Organizacyjnego, Inspektor ds. Inwestycji i Zamówień Publicznych oraz Kierownik Referatu Finansowego). Zgodnie z wyjaśnieniami Wójta zadania i obowiązki pracowników Urzędu oraz członków Zespołu ds. Projektu, były przydzielane w formie ustnych poleceń służbowych oraz indywidualnych uzgodnień z bezpośrednimi przełożonymi, w tym z Sekretarzem Gminy oraz Koordynatorem Projektu. Wójt wyjaśnił również: *Obecnie, w celu uporządkowania dokumentacji i zapewnienia zgodności z zasadami realizacji projektu grantowego, trwają prace nad uzupełnieniem – poszerzeniem zakresów czynności (...).*
W zarządzeniu w sprawie powołania Zespołu ds. Projektu (§2) wskazano, że do jego zadań należało: czuwanie nad finansową, merytoryczną i zgodną

[22] VLAN (Virtual Local Area Network - wirtualna sieć lokalna) to technologia sieciowa, która pozwala na logiczne podzielenie jednej fizycznej sieci LAN na kilka niezależnych od siebie, wirtualnych sieci.
[23] Dokument z dnia 4 października 2024 r.
[24] Ze zmianą zarządzeniem nr 26/2025 Wójta gminy Brody z dnia 17 lutego 2025 r. ze względu na zmianę personalną na stanowisku inspektora ds. zamówień publicznych.

z wnioskiem realizacją Projektu, analiza postępów rzeczowych i finansowych projektu, reagowanie na ewentualne problemy w trakcie jego realizacji, analiza ankiet oraz stopnia osiągniecia założonych wskaźników. Nadzór na realizacją przedmiotowego zarządzenia pełnił Sekretarz Gminy Brody. Zespół ds. Projektu obradował dwukrotnie: w październiku 2024 i listopadzie 2024 r. Na spotkaniu omawiane były m.in. problemy kadrowe, terminy kwalifikowalności wydatków, ryzyka uchybienia terminom w postępowaniach w zakresie zamówień publicznych. W październiku 2024 r. Zespół ds. Projektu podjął decyzję o przesunięciu działań związanych z realizacją Projektu na 2025 r., o czym Wójt poinformował NASK-PIB w dniu 16 października 2024 r.
Mimo, że od dnia podpisania Umowy do czasu powołania Zespołu ds. Projektu minęło sześć miesięcy, to - jak wyjaśnił Wójt - jego członkowie (w tymczasowych strukturach) realizowali działania przygotowawcze. Wójt nie przekazał jednak żadnej dokumentacji potwierdzającej podejmowanie jakichkolwiek działań w tym zakresie.
Wójt wyjaśnił również, że opóźnienie związane z utworzeniem Zespołu ds. Projektu wynikało z kumulacji następujących czynników organizacyjno-kadrowych: - zmiany na stanowisku Wójta Gminy, która miała wpływ na ciągłość realizacji zadań strategicznych, w tym projektów finansowanych z funduszy zewnętrznych; - braki kadrowe w Urzędzie Gminy które ograniczały możliwości wyznaczenia zespołu projektowego; - fluktuacja pracowników i zmiany kadrowe, w tym zmiany na stanowiskach kierowniczych i technicznych, odpowiedzialnych za realizację i nadzór nad komponentami Projektu; - konieczność ponownej weryfikacji i dostosowania zakresu Projektu do realnych możliwości operacyjnych Gminy w zmieniających się warunkach organizacyjnych.
Wójt wyjaśnił, że prowadzony był monitoring działań podejmowanych w ramach realizacji grantu, który zdaniem Wójta polegać miał na bieżącej sprawozdawczości oraz na weryfikacji wdrażanych rozwiązań technicznych przez Koordynatora Projektu.
Urząd nie przedłożył dokumentów potwierdzających przebieg prac Zespołu ds. Projektu, które mogłyby pozwolić na odtworzenie monitoringu działań dotyczącego jednostek podległych.
(akta kontroli str. 14-19, 85-86, 91-95, 172-173,178-179, 209, 297)

W trakcie realizacji Projektu wystąpiły trudności kadrowe, które miały wpływ na sprawność i terminowość wdrażania zaplanowanych działań. Problemy te dotyczyły zarówno Urzędu jak i jednostek organizacyjnych biorących udział w Projekcie. Wójt wskazał: *Zmiana na stanowisku wójta, wymusiła potrzebę przeglądu stanu zaawansowania Projektu, jego założeń oraz dostosowania działań (...) do możliwości organizacyjnych. Proces ten wpłynął na przesunięcie części kluczowych decyzji i działań projektowych.* Umowę podpisaną przez byłego Wójta, realizował obecny Wójt[25]. Został on wybrany dnia 9 kwietnia 2024 r., a w dniu 15 lipca 2024 r. zawarł umowę dotyczącą przeglądu, aktualizacji i wykonania SZBI. W dniu 19 września 2024 r. ogłoszono przetarg na zakup i dostawę oprogramowania, a 7 listopada 2024 r. Wójt podpisał umowy w tym zakresie. W dniu 14 października 2024 r. Wójt powołał Zespół ds. realizacji Projektu, opisanym w pkt 6 niniejszego wystąpienia.
Zarówno w Urzędzie, jak i w jednostkach podległych występowały braki kadrowe, długie absencje chorobowe osób zaangażowanych w zadania związane z realizacją zadań projektowych oraz rotacje na stanowiskach urzędniczych (w szczególności w zakresie zamówień publicznych) i administracyjnych.

[25] Zaświadczenie o wyborze Wójta Gminy Brody z dnia 9 kwietnia 2024 r.

W związku z fluktuacją kadr i pomimo powołania Zespołu ds. Projektu, wystąpiły opóźnienia w jego realizacji.
Ponadto, za realizację grantu, w tym również przygotowanie i prowadzenie postępowań o udzielenie zamówień publicznych, odpowiadało dwóch pracowników Urzędu, którzy wykonywali również inne obowiązki służbowe, niezwiązane z Projektem.
Wójt wyjaśnił, że z uwagi na ograniczone zasoby ludzkie i zakres obowiązków wykraczający poza sam Projekt, niemożliwe było równoległe, sprawne prowadzenie wszystkich zaplanowanych działań w założonym pierwotnie tempie. W konsekwencji formalne powołanie Zespołu ds. Projektu nastąpiło dopiero w październiku 2024 r.
Wójt wyjaśnił: *Problemy kadrowe, zmiany personalne oraz konieczność łączenia obowiązków związanych z projektem i zamówieniami publicznymi (...) istotnie wpłynęły na tempo i organizację wdrażania grantu. Pomimo tych trudności działania były sukcesywnie podejmowane zgodnie z zapisami umowy oraz wytycznymi NASK, a Gmina podejmuje dalsze kroki w celu pełnej realizacji projektu.*
W realizację grantu od początku jego realizacji zaangażowanych było 16 osób.
(akta kontroli str. 8, 19, 84-85, 167-170)

Zgodnie z Załącznikiem nr 9 do Regulaminu Konkursu Grantowego *Cyberbezpieczny Samorząd*[26] (dalej: Załącznik nr 9 do Regulaminu) we wniosku o przyznanie grantu określono następujące wskaźniki Projektu:

- liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym w podziale Kobiety/Mężczyźni (planowane przeszkolenie jednej osoby – informatyka Urzędu) - wsparciem szkoleniowym podnoszącym umiejętności z zakresu ICT[27]objęto informatyka Urzędu w zakresie wdrażanych rozwiązań technicznych oraz audytu SZBI. a także IOD w zakresie bezpieczeństwa przetwarzania danych w systemach informatycznych;
- liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym w podziale Kobiety/Mężczyźni (planowane przeszkolenie IOD dotyczące bezpieczeństwa sprzętu i danych oraz obowiązujących przepisów prawa, a także szkolenia dla wszystkich pracowników Urzędu pod kątem budowania świadomości występowania zagrożeń cyberbezpieczeństwa) - wsparciem szkoleniowym podnoszącym umiejętności z zakresu ICT objęto dotychczas IOD w zakresie bezpieczeństwa przetwarzania danych w systemach informatycznych;
- liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji. Urząd zaplanował zakup pięciu systemów służących zwiększeniu poziomu bezpieczeństwa informacji, tj.:
  - oprogramowania do inwentaryzacji aktywów, ich konfiguracji, zarządzania nośnikami wymiennymi oraz wykrywaniem niepożądanych zdarzeń w infrastrukturze IT,
  - systemu zabezpieczający przed wyciekiem danych,
  - oprogramowanie antywirusowe,
  - system do gromadzenia i analizy logów,
  - system kopii zapasowych;

[26] https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (data dostępu 15 maja 2025 r.).
[27] Skrót od *Information and Comunications Technology* – technologie informacyjne i komunikacyjne lub technologie komunikacyjno-informacyjne.

– użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych – realizację tego wskaźnika rezultatu Urząd miał wskazać na etapie wniosku;
liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST[28] (planowane wsparcie trzech jednostek podległych, w szczególności zakup sprzętu).

(akta kontroli str. 86-97, 131-132, 331-342)

Opis wskaźnika określającego liczbę podmiotów wspartych w zakresie cyberbezpieczeństwa nie zawierał wymogu odnośnie minimalnej liczby jednostek objętych finansowaniem. Udział jednostek podległych został opisany w pkt 5 niniejszego wystąpienia. Wskaźnikiem rezultatu była liczba użytkowników nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych podana w formacie *użytkownicy na rok* obejmujących pracowników Urzędu i jednostek podległych. Realizację tego wskaźnika Urząd miał wskazać na etapie wniosku rozliczającego.
Wskaźniki Projektu (produktu i rezultatu) określono zgodnie z Załącznikiem nr 9 do Regulaminu. W opisie wskaźników Projektu określono minimalną liczbę pracowników podmiotów wykonujących zadania publiczne (będących pracownikami IT – minimum jedna osoba oraz niebędących pracownikami IT – minimum jedna osoba), objętych wsparciem szkoleniowym. W Urzędzie szkoleniami objęto jedną kobietę i jednego mężczyznę[29].

(akta kontroli str. 86-97, 331-342)

Brak liczbowego wskaźnika rezultatu[30] Wójt wyjaśnił następująco: *Część wskaźników rezultatu nie została określona liczbowo, ponieważ projekt miał charakter modułowy i oparty na diagnozie dojrzałości cyberbezpieczeństwa, która była przeprowadzana po podpisaniu umowy. Szczegółowe mierniki dostosowano do potrzeb i możliwości Gminy Brody na etapie realizacji, co było zgodne z elastycznym charakterem programu.* Zgodnie z wnioskiem celem Projektu była: (...) *poprawa cyberbezpieczeństwa JST, która zostanie osiągnięta do końca realizacji projektu i potwierdzona audytem SZBI i ankietami.*

(akta kontroli str. 11-12, 86-97)

Zakupione w ramach grantu oprogramowanie zostało uruchomione, co zostało potwierdzone przeprowadzonymi, w ramach kontroli, oględzinami. Audyt, zgodnie z aneksem nr 1 do umowy Nr 7/CS/2024 zawartej w dniu 15 lipca 2024 r. przewidziano do zrealizowania w terminie do dnia 31 marca 2026.

(akta kontroli str. 157-166, 323-329)

Na dzień zakończenia kontroli Projekt był w trakcie realizacji i nie przewidziano działań w celu utrzymania poziomu cyberbezpieczeństwa po zakończeniu realizacji grantu. Cyberbezpieczny Samorząd miał być realizowany w okresie maksymalnie 24 miesięcy od dnia wejścia w życie Umowy, nie dłużej jednak niż do 30 czerwca 2026 r.

(akta kontroli str. 104-105)

---

[28] Jednostka samorządu terytorialnego.
[29] IOD i informatyk Urzędu.
[30] Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych.

W Urzędzie ustanowiono i wdrożono PBI zgodnie z §20 ust. 2 pkt 12 lit. h rozporządzenia KRI z dnia 12 kwietnia 2012 r. Podstawowym dokumentem było Załącznik nr 1 do Zarządzenia Nr 165/2019 Wójta Gminy Brody z dnia 31 października 2019 r.[31] (dalej: zarządzenie PBI). Określała ona m.in. zadania i odpowiedzialność pracowników w zakresie bezpieczeństwa informacji, podstawowe zasady jego zapewnienia, sposoby reagowania na incydenty bezpieczeństwa informacji.
Pracownicy Urzędu zapoznali się z dokumentem, potwierdzając to własnoręcznym podpisem na liście osób lub poprzez złożenie oświadczenia. PBI nie miało ustalonego właściciela odpowiadającego za jej opracowanie, wdrożenie, ocenę, przegląd i modyfikację, tj. komórkę organizacyjną lub osobę odpowiedzialną za wszelkie zmiany w dokumencie. Wójt wyjaśnił, że zadania te realizowane były wspólnie przez: IOD (odpowiadał za zgodność z przepisami o ochronie danych osobowych), Referat Organizacyjny (odpowiedzialny był za koordynację działań związanych z wdrażaniem dokumentów wewnętrznych) oraz informatyka (odpowiadał za techniczne aspekty zabezpieczeń systemów informatycznych).
Wójt wyjaśnił: *W związku z trwającymi pracami nad uporządkowaniem dokumentacji projektowej i wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostkach podległych, planowane jest formalne przypisanie odpowiedzialności za PBI konkretnej osobie lub komórce organizacyjnej, co zostanie uregulowane w wewnętrznych aktach prawa miejscowego.*

(akta kontroli str. 182-207, 209)

Zarządzeniem Nr 179/2024 Wójta Gminy Brody z dnia 17 października 2024 r. ustanowiono Pełnomocnika Wójta Gminy do spraw systemu zarządzania bezpieczeństwem informacji (dalej: Pełnomocnik) oraz powołano czteroosobowy zespół wdrożeniowy do spraw Systemu Zarządzania Bezpieczeństwem Informacji. Do zadań Pełnomocnika należała realizacja obowiązków wynikających z rozporządzenia KRI, w tym m.in. koordynacja, opracowanie i aktualizacja dokumentów SZBI, opracowanie i aktualizacja procesów dotyczących bezpieczeństwa informacji, koordynacja przeglądów SZBI oraz nadzór nad realizacją ustaleń wynikających z przeglądów zarządzania SZBI, inicjowanie oraz nadzorowanie działań wdrożeniowych, korygujących i zapobiegawczych w zakresie bezpieczeństwa informacji.

(akta kontroli str. 180-182)

SZBI został wprowadzony w Gminie dopiero w dniu 18 lutego 2025 r. Obowiązek jego opracowania, ustanowienia i wdrożenia wynikał z rozporządzeń KRI[32]. Szerzej na powyższy temat w sekcji *Stwierdzone nieprawidłowości.*
SZBI został zatwierdzony i zakomunikowany pracownikom Urzędu. Pracownicy potwierdzili zapoznanie się z dokumentem własnoręcznym podpisem na liście lub poprzez złożenie stosownego oświadczenia.
Integralną częścią SZBI były m.in.: PBI, Procedurę bezpieczeństwa teleinformatycznego, Procedurę użytkowania zasobów teleinformatycznych wraz z załącznikami, Procedurę zarządzania ciągłością działania wraz z załącznikami, Procedurę zarzadzania Incydentami Cyberbezpieczeństwa wraz

[31] Zarządzeniem Nr 165/20219 Wójta Gminy Brody z dnia 31 października 2019 r. ustanowiono i wdrożono PBI r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji dla Urzędu Gminy w Brodach
[32] §20 ust. 1 rozporządzenia KRI z dnia 12 kwietnia 2012 r. oraz §19 ust. 1 rozporządzenia KRI z dnia 21 maja 2024 r.

z załącznikami, Procedurę szacowania ryzyka bezpieczeństwa informacji, w tym danych osobowych.
W wyniku przeprowadzonej przez Pełnomocnika wewnętrznej analizy oraz przeglądu dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji stwierdzono, że dokumentacja ta nie spełnia wszystkich wymagań określonych przez normę ISO/IEC 27001. Wskazano następujące niezgodności: - niekompletną analizę ryzyka oraz brak stosownej dokumentacji potwierdzającej jej przeprowadzenie; - niekompletną dokumentację dotyczącą procedur zarządzania ciągłością działania; - nieprzeprowadzenie audytu po wdrożeniu SZBI potwierdzającego zgodność z wymaganiami wskazanej normy.
o czym więcej w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 182-201, 206-207, 210, 266, 343-349)

12. KRI wymaga aktualizacji i przeglądu SZBI i powiązanych z nim dokumentów. Biorąc pod uwagę, że SZBI wprowadzono w Gminie w 2025 r. najbliższa aktualizacja będzie wymagana w 2026 r. W Gminie była ustanowiona PBI jednak nie była ona częścią SZBI, tym samym przepis z §4 ust. 1 i 2 Załącznika Nr 1 do zarządzenie PBI, nie miał tu zastosowania.

(akta kontroli str. 186, 202-203, 343-349)

13. W Urzędzie, w 2024 r., nie przeprowadzono okresowego audytu z zakresu bezpieczeństwa informacji, który wynikał z §20 ust. 2 pkt 14 rozporządzenia KRI z dnia 12 kwietnia 2012 r. oraz §19 ust. 2 pkt 14 rozporządzenia KRI 21 maja 2024 r., o czym szerzej *w sekcji Stwierdzone nieprawidłowości.*

(akta kontroli str. 215-249)

14. Urząd informował opinię publiczną o fakcie otrzymania dofinansowania na realizację Projektu, m.in.: poprzez oznaczanie znakiem Unii Europejskiej, barwy Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich dokumentów związanych z realizacją Projektu, w tym dokumentacji z postępowań przetargowych (tj.: korespondencji z wykonawcami, protokołów odbioru i realizacji usług) oraz w informacjach podawanych do wiadomości publicznej.
W ramach podejmowanych działań informacyjnych na stronie internetowej Urzędu, w zakładce *Aktualności,* zamieszczono informacje o Projekcie Cyberbezpieczny Samorząd: - z dnia 30 kwietnia 2024 r. pn.: „Kolejny krok w stronę cyberbezpieczeństwa" o zawarciu Umowy wraz z krótkim opisem Projektu, jego celów i kosztów, warunków dofinansowania i terminów realizacji; - z dnia 31 października 2024 r. o udziale Gminy w Projekcie, ze wskazaniem celów i zakresu projektu, warunków dofinansowania oraz uzasadnieniem udziału w projekcie.
Informacje o przystąpieniu Gminy do Projektu i jego realizacji nie znalazły się na tablicach informacyjnych Urzędu, nie było również ulotek i broszur. Nie umieszczono również wymaganego przynajmniej jednego plakatu o minimalnym formacie A3, co wynikało z zawartej Umowy (§11 ust. 4 pkt 2), o czym szerzej w sekcji *Stwierdzone nieprawidłowości.*
Na stronie internetowej Urzędu utworzona była zakładka pn. Cyberbezpieczeństwo, które mimo, że nie odnosiła się bezpośrednio do realizowanego projektu, to zawierała podstawowe informacje i definicje dotyczące bezpieczeństwa cybernetycznego oraz informacje odnośnie: najpopularniejszych zagrożeń w cyberprzestrzeni, sposobów zabezpieczenia się przed zagrożeniami, linki do stron zawierających porady dotyczące cyberbezpieczeństwa.

(akta kontroli str. 120, 253-265)

Stwierdzone nieprawidłowości

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

1. Obowiązek opracowania, ustanowienia i wdrożenia SZBI wynikał z §19 ust. 1 rozporządzenia KRI z 12 kwietnia 2012 r., zgodnie z którym *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.*
   Wójt wprowadził SZBI dopiero w dniu 18 lutego 2025 r. (zarządzenie Wójta nr 31/2025)

   (akta kontroli str. 202-203)

   Były Wójt wyjaśniła: *Według mojej najlepszej wiedzy, system obiegu informacji, w tym dotyczący cyberbezpieczeństwa był realizowany w praktyce i wypełniał przesłanki wymagane dla systemu zarządzania bezpieczeństwem informacji zapewniając poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, czyli te, które wymaga rozporządzenie KRI.*

   (akta kontroli str. 75)

   Odnośnie zbyt późnego opracowania SZBI Wójt wyjaśnił, że przyczyną były: *a) zmiana na stanowisku Wójta Gminy Brody w 2024 r. wpłynęła na reorganizację i ponowną ocenę stanu realizacji projektów, w tym grantu „Cyberbezpieczny Samorząd". Nowe kierownictwo wymagało czasu na przegląd dokumentacji oraz przywrócenie płynności decyzyjnej; b) Znaczące braki kadrowe i zmiany personalne: W drugiej połowie 2024 r. doszło do odejścia pracownika merytorycznie odpowiedzialnego za projekt, - równolegle pracownik prowadzący postępowania o udzielenie zamówień publicznych od listopada 2024 roku przebywa na zwolnieniu lekarskim, co wstrzymało kluczowe działania wdrożeniowe, - w tym czasie obowiązki realizacji grantu i wdrożenia SZBI były dzielone przez innych pracowników, co w praktyce nie pozwalało na sprawne i jednoczesne prowadzenie wszystkich etapów prac.*
   Wyjaśnił również: *Po ustabilizowaniu sytuacji kadrowej, w lutym 2025 r. zakończono formalne ustanowienie SZBI, obejmujące: politykę bezpieczeństwa informacji, plan zarządzania incydentami, politykę klasyfikacji informacji, danych osobowych, analizę ryzyka, plan ciągłości działania oraz inne dokumenty wymagane przepisami KRI. System został wdrożony w sposób obejmujący Urząd (...).*

   (akta kontroli str. 22-23)

   W związku z wprowadzeniem SZBI, NIK odstępuje od formułowania wniosku w tym zakresie.

2. Dokumentacja SZBI nie spełniała wszystkich wymagań określonych przez normę ISO/IEC 27001. Wskazano następujące niezgodności: - niekompletną analizę ryzyka oraz brak stosownej dokumentacji potwierdzającej jej przeprowadzenie; - niekompletną dokumentację dotyczącą procedur zarządzania ciągłością działania; - nieprzeprowadzenie audytu po wdrożeniu SZBI potwierdzającego

zgodność z wymaganiami wskazanej normy. Jak wskazano w rozporządzeniu KRI[33]: *wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: 1) PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń; 2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem; 3) PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania*. Było to działanie nierzetelne.

(akta kontroli str. 182-198, 343-349)

Wójt wyjaśnił: *Po pełnym wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji we wszystkich jednostkach organizacyjnych gminy (CUW, GOPS, ZGK), planuje się ujednolicenie dokumentacji oraz dostosowanie SZBI i PBI do wymagań ww. norm, zgodnie z § 19 ust. 3 rozporządzenia KRI z dnia 21 maja 2024 r. W tym celu przewiduje się opracowanie kompleksowej metodyki zarządzania ryzykiem oraz doboru zabezpieczeń w oparciu o wytyczne PN-ISO/IEC 27005 oraz 27002 (...). Na dzień dzisiejszy wdrożenie SZBI jest w toku, a dalsze działania są sukcesywnie realizowane zgodnie z harmonogramem działań przyjętym przez Zespół ds. projektu "Cyberbezpieczny Samorząd". Zakończenie pełnej implementacji dokumentacji SZBI i rozpoczęcie cyklicznych przeglądów zgodnych z normami ISO planowane jest na II połowę 2025 roku.*

(akta kontroli str. 211)

Odnośnie SZBI Pełnomocnik wyjaśnił, że rozpoczęto działania naprawcze mające na celu dostosowanie dokumentacji do wymagań określonych przez normę ISO/IEC 27001.

(akta kontroli str. 266)

3. Wójt nie przeprowadził okresowego audytu bezpieczeństwa informacji nie rzadziej niż raz na rok. Obowiązek ten wynikał rozporządzeń KRI[34].

Były Wójt wyjaśniła: *Według mojej najlepszej wiedzy, był prowadzony zewnętrzny audyt, to jest przez podmiot niebędący w strukturach organizacyjnych Urzędu. Ponieważ obecnie nie mam dostępu do akt oraz infrastruktury urzędu gminy, to nie mogę podać konkretnej daty oraz treści pism związanych z audytem, ale były prowadzone zgodnie z zasadami wynikającymi z regulaminu organizacyjnego urzędu, więc nie powinno być problemu z ich wskazaniem przez obecne władze Gminy, poza tym pracownicy, którzy merytorycznie zajmowali się sprawami informatycznymi nadal są zatrudnieni w urzędzie gminy i z tego co mi jest wiadome nawet zostali awansowani, co tylko potwierdza mój uprzedni wybór, a ich fachowość. Działania moje wypełniały dyspozycje przywołanej w piśmie normy prawnej, która zawiera otwarty katalog możliwych do podjęcia działań, a w szczególności zgodne są pkt 14 - właściwym podmiotem, który*

[33] §20 ust. 3 rozporządzenia KRI z 12 kwietnia 2012 r. i §19 ust. 3 rozporządzenia KRI z 21 maja 2024 r.

[34] §20 ust. 2 pkt 14 rozporządzenia KRI z dnia 12 kwietnia 2012 r. oraz §19 ust. 2 pkt 14 rozporządzenia KRI z 21 maja 2024 r.

realizował audyt był tym wskazanym w tej jednostce redakcyjnej rozporządzenia.

(akta kontroli str. 74)

Wójt wyjaśnił: *W ramach realizacji projektu „Cyberbezpieczny Samorząd", w Gminie Brody przeprowadzono audyt wstępny (tzw. diagnozę dojrzałości w zakresie cyberbezpieczeństwa), który obejmował również elementy oceny zgodności z wymaganiami określonymi w rozporządzeniu KRI, w tym dotyczące systemów teleinformatycznych oraz poziomu zabezpieczeń informacji. 1) Diagnoza ta obejmowała ocenę stosowanych procedur i polityk bezpieczeństwa: analizę zabezpieczeń technicznych i organizacyjnych, wskazanie niezgodności i obszarów wymagających poprawy, opis planowanego zakresu zmian, które stanowiły podstawę do dalszych działań w ramach projektu. 2) Audyt Gminy Brody został przeprowadzony na przełomie maj/czerwiec 2024 r., po wyborach samorządowych w 2024 roku. (...). Raport z audytu stanowił integralny element dokumentacji potwierdzającej braki w polityce bezpieczeństwa – brak SZBI. (...) 3) Dnia 5 sierpnia powstał Raport z badania dojrzałości organizacyjnej opracowany przez firmę zewnętrzną Fortcyber zawierający opis poziomu dojrzałości JST w obszarach – IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER wraz z Ankietą Techniczną w zakresie wdrożenia usługi. (...) Pełny audyt końcowy zostanie zrealizowany po zakończeniu prac wdrożeniowych, zgodnie z dobrą praktyką oraz celem zapewnienia zgodności z przepisami.*

(akta kontroli str. 21-22)

NIK wskazuje, że audyty, które wskazano w wyjaśnieniach nie zostały przeprowadzone na podstawie §19 ust. 2 pkt 14 rozporządzenia KRI z dnia 21 maja 2024 r.

4. Wójt nie dopełnił obowiązku z Umowy w zakresie umieszczenia przynajmniej jednego plakatu o minimalnym formacie A3. Obowiązek ten wynikał z §11 ust. 4 pkt 2 Umowy.

(akta kontroli str. 120, 253)

Wójt wyjaśnił, że przyczynami braku umieszczenia plakatu były: - problemy kadrowe, wyjaśnił: (...) *W Urzędzie wystąpiły istotne braki kadrowe oraz zmiany personalne, w tym zmiana Wójta, a także rotacja pracowników odpowiedzialnych za projekt i zamówienia publiczne. Zmiana Kierownika Referatu Organizacyjnego, dlatego też, zadania związane z promocją nie zostały odpowiednio rozdzielone i przypisane; - skoncentrowanie działań na wdrożeniu technicznym i merytorycznym – w tym okresie priorytetem była realizacja zakupów, procedur bezpieczeństwa oraz szkoleń - planowana przebudowa strony internetowej Urzędu – z uwagi na planowaną modernizację serwisu internetowego, zrezygnowano tymczasowo z publikacji plakatu*. (...) Wyjaśnił również: *(...) Gmina podjęła starania o wykonanie plakatu informacyjnego w formacie A3, zgodny z wymaganiami dotyczącymi identyfikacji wizualnej i umieści go w widocznym miejscu w siedzibie Urzędu Gminy. (...)*

(akta kontroli str. 24)

IV. Uwagi i wnioski

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

Wnioski

1. Uzupełnić dokumentację SZBI o brakujące elementy wynikające z wymagań określonych w rozporządzeniu KRI.
2. Zapewnić okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
3. Umieścić przynajmniej jeden plakat o minimalnym formacie A3 informujący opinię publiczną o fakcie otrzymania dofinansowania z Projektu.

Uwagi

NIK nie formułuje uwag.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w postaci elektronicznej.

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 wniosków

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

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

Kielce, 4 lipca 2025 r.

Kontrolerzy

Monika Górniak-Napora

starszy inspektor kontroli państwowej

/podpisano elektronicznie/

Łukasz Nowakowski

starszy inspektor kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Delegatura w Kielcach

Dyrektor

Grzegorz Walendzik

/podpisano elektronicznie/