

Urząd Zamówień Publicznych w Warszawie

02-676 Warszawa ul. Postępu 17A

Ogłoszenie nr 157860 / 04.11.2025

Główny Specjalista

Do spraw: infrastruktury i sieci w Wydziale Informatyki i Bezpieczeństwa Systemów Teleinformatycznych w Departamencie Danych i Informatyzacji

#administracja publiczna #IT

Pierwszeństwo dla osób z niepełnosprawnościami



Liczba stanowisk

2

Wymiar etatu

1

Status

nabór w toku

Miejsce pracy

Warszawa
ul. Postępu 17A

Ważne do

18 listopada
2025 r.

Wynagrodzenie
zasadnicze

od 9659,90 zł
do 10487,89 zł
brutto

Czym będziesz się zajmować

Osoba na tym stanowisku:

- Projektuje i wdraża architekturę sieciową Urzędu, w tym definiuje kierunki rozwoju infrastruktury sieciowej, segmentację sieci, konfigurację urządzeń sieciowych (przełączniki, routery, NGFW, WAF) oraz zapewnia bezpieczeństwo na poziomie sieci poprzez implementację rozwiązań typu Zero Trust.
- Opracowuje strategie rozwoju infrastruktury sieciowej w oparciu o analizę realnych połączeń między maszynami i systemami, uwzględniając potrzeby biznesowe Urzędu, wymogi bezpieczeństwa oraz trendy technologiczne, w tym planuje i nadzoruje modernizację infrastruktury.
- Zarządza bezpieczeństwem sieci poprzez konfigurację i utrzymanie systemów SIEM, monitorowanie i analizę zdarzeń bezpieczeństwa, implementację mechanizmów ochronnych oraz reaguje na incydenty bezpieczeństwa w czasie rzeczywistym.
- Projektuje, konfiguruje i zarządza rozwiązaniami VPN (w tym SaaS VPN/ZTNA), tunelami sieciowymi oraz połączeniami do środowisk chmurowych, zapewniając szyfrowane kanały komunikacji między aplikacjami i systemami.
- Opracowuje i aktualizuje dokumentację techniczną infrastruktury sieciowej, w tym diagramy topologii, architekturę i segmentację sieci oraz procedury operacyjne.
- Konfiguruje i zarządza zaawansowanymi urządzeniami bezpieczeństwa sieci, w tym Next Generation Firewall (NGFW), Web Application Firewall (WAF), systemami IPS/IDS oraz mechanizmami filtrowania ruchu sieciowego na różnych poziomach OSI.
- Buduje i utrzymuje architekturę monitorowania sieci, w tym konfiguruje systemy SIEM, koreluje zdarzenia bezpieczeństwa, analizuje logi oraz tworzy reguły detekcji zagrożeń i alertów bezpieczeństwa.
- Współpracuje z podmiotami realizującymi projekty informatyczne oraz prowadzi szkolenia dla pracowników w zakresie bezpieczeństwa sieci i najlepszych praktyk cyberbezpieczeństwa.

Kogo poszukujemy

Potrzebne ci będą (wymagania niezbędne)

- Wykształcenie: wyższe
- Doświadczenie: powyżej 2 lat w obszarze informatycznym
- Znajomość języków obcych: język angielski – poziom wystarczający do czytania i rozumienia dokumentacji technicznych oraz posługiwania się anglojęzycznymi stronami internetowymi
- Wiedza: zaawansowana w zakresie projektowania architektury sieci i definiowania kierunków jej rozwoju
- Wiedza: dogłębna znajomość protokołów sieciowych i mechanizmów bezpieczeństwa na wszystkich warstwach OSI
- Wiedza: znajomość rozwiązań vpn, w tym saas vpn i zabezpieczania ruchu pochodzącego z internetu
- Wiedza: znajomość koncepcji Zero Trust i jej implementacji w architekturze sieci
- Umiejętności: praktyczne w zakresie konfiguracji urządzeń sieciowych (przełączniki, routery, NGFW, WAF)
- Umiejętność: znajomość i umiejętność konfiguracji systemów SIEM (np. Splunk, QRadar, ArcSight, Elastic SIEM)
- Umiejętność: analizy zdarzeń bezpieczeństwa i korelacji logów z różnych źródeł
- Umiejętność: mapowania i analizy realnych połączeń między systemami i aplikacjami
- Umiejętność: rozwiązywania złożonych problemów technicznych
- Umiejętności: myślenie analityczne i systemowe
- Aktualne poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą „poufne” albo zgoda na poddanie się procedurze sprawdzającej.
- Niepracowanie lub niepełnienie służby zawodowej w organach bezpieczeństwa państwa wymienionych w art. 2 ustawy z 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990 oraz treści tych dokumentów (Dz. U z 2023 r. poz. 342, 497 i 1195), ani niebycie ich współpracownikiem – dotyczy kandydatów urodzonych przed 1 sierpnia 1972 r.
- Posiadanie obywatelstwa polskiego
- Korzystanie z pełni praw publicznych
- Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

Dodatkowym atutem będzie (wymagania dodatkowe)

- Wykształcenie: wyższe z zakresu nauk ścisłych lub technicznych
- Doświadczenie: powyżej 4 lat w reagowaniu na incydenty bezpieczeństwa i prowadzeniu analiz forensycznych
- Doświadczenie: powyżej 4 lat w audytach bezpieczeństwa sieci i testach penetracyjnych
- Przeszkolenie: certyfikaty z zakresu bezpieczeństwa sieci (np. CISSP, CISM) lub technologii sieciowych (np. CCNP, CCIE)
- Wiedza: znajomość technologii chmurowych (Azure, AWS) i ich integracji z siecią on-premise
- Wiedza: znajomość rozwiązań Software-Defined Networking (SDN/SD-WAN)
- Umiejętność: programowania skryptowego (PowerShell, Bash, Python)

Co oferujemy

- zatrudnienie na podstawie umowy o pracę,
- **częściowe wykonywanie pracy poza siedzibą urzędu (praca zdalna) - do 50% dni roboczych w miesiącu, w tym ruchomy czas rozpoczęcia pracy zdalnej pomiędzy 7.00 a 9.00,**
- indywidualny rozkład czasu pracy – na wniosek pracownika,
- ruchomy czas pracy wykonywanej w siedzibie – na wniosek pracownika,
- dodatek za wysługę lat (powyżej 5 lat) od 5 do 20% wynagrodzenia zasadniczego w zależności od udokumentowanego stażu pracy,
- dodatkowe wynagrodzenie roczne (tzw. trzynastka),

- możliwość dofinansowania do zakupu okularów lub soczewek korekcyjnych do pracy przy komputerze,
- wsparcie w podnoszeniu kwalifikacji zawodowych,
- pakiet socjalny (np. dofinansowanie do wypoczynku dla pracownika i jego dzieci, niskooprocentowane pożyczki na cele mieszkaniowe, wsparcie finansowe w trudnych sytuacjach),
- możliwość wykupienia dodatkowego ubezpieczenia na życie.

Dostępność

- Nasz urząd jest pracodawcą równych szans. Aplikacje rozważane są z równą uwagą bez względu na płeć, wiek, niepełnosprawność, rasę, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, orientację seksualną czy też jakąkolwiek inną cechę prawnie chronioną.
- Jako osoba z niepełnosprawnością możesz skorzystać z pierwszeństwa w zatrudnieniu – złóż wówczas kopię dokumentu potwierdzającego niepełnosprawność.
W miesiącu poprzedzającym datę upublicznienia ogłoszenia wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie, w rozumieniu przepisów ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, był mniejszy niż 6%.
- Do składania dokumentów zachęcamy również osoby ze szczególnymi potrzebami, które spełniają wymagania określone w niniejszym ogłoszeniu.
- Jako osoba ze szczególnymi potrzebami możesz je zgłosić na etapie składania dokumentów.
- Dostosowujemy materiały używane podczas naboru do potrzeb osób ze szczególnymi potrzebami (np. większa czcionka w materiałach drukowanych).

Warunki pracy

- konieczność reagowania na incydenty bezpieczeństwa poza standardowymi godzinami pracy,
- praca biurowa przy komputerze powyżej 4 godzin dziennie,
- opis dostępności budynku dla osób z niepełnosprawnością znajduje się na stronie urzędu
<https://www.gov.pl/web/uzp/deklaracja-dostepnosc>

Dodatkowe informacje

- w służbie cywilnej nie może być zatrudniona osoba, która w okresie od dnia 22 lipca 1944 r. do dnia 31 lipca 1990 r. pracowała lub pełniła służbę w organach bezpieczeństwa państwa lub była współpracownikiem tych organów w rozumieniu przepisów ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów - nie dotyczy kandydatek/kandydatów urodzonych 1 sierpnia 1972 r. lub później. Osoba wybrana do zatrudnienia będzie musiała złożyć oświadczenie lustracyjne, jeśli urodziła się przed 1 sierpnia 1972 r.,
- przed wysłaniem aplikacji prosimy o upewnienie się, że spełnienie wymagań jednoznacznie wynika z przesłanych dokumentów,
- dokumenty należy przygotować w języku polskim - do dokumentów w języku obcym należy dołączyć również ich tłumaczenie na język polski; w przypadku ukończenia studiów wyższych na uczelni zagranicznej prosimy o przesłanie kopii pisemnej informacji o zagranicznym dyplomie wydanej przez Narodową Agencję Wymiany Akademickiej,
- nie rozpatrzymy oferty, którą otrzymamy po terminie (decyduje data wpływu do UZP – w przypadku złożenia oferty drogą pocztową za datę złożenia oferty uważamy datę jej wpływu do Urzędu Zamówień Publicznych),
- jeżeli ofertę składasz elektronicznie na adres mailowy, wymagane w ogłoszeniu oświadczenia muszą być podpisane własnoręcznie z aktualną datą i przesłane w formie skanów/zdjęć lub podpisem elektronicznym kwalifikowanym lub podpisem zaufanym,

- jeśli zostaniesz zakwalifikowany do kolejnego etapu, powiadomimy Cię o tym mailowo (lub telefonicznie – jeżeli nie podałeś adresu e-mail),
- nie przysyłaj wszystkich dokumentów, które uznasz, że mogą Ci pomóc w naborze - prześlij tylko te, których wymagamy lub zalecamy,
- zwróć uwagę na warunki pracy, które wskazaliśmy w ogłoszeniu – rzetelnie oceń, czy odpowiada Ci taka praca,
- informacje na temat zgłoszeń dotyczących naruszeń prawa znajdują się na stronie:
<https://www.gov.pl/web/uzp/zgloszenia-dotyczace-naruszen-prawa>

Planujemy następujące metody/techniki naboru:

- weryfikacja formalna ofert
- rozmowa kwalifikacyjna

Twoja aplikacja musi zawierać (dokumenty niezbędne)

- CV
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie wykształcenia
- Kopie dokumentów potwierdzających wymagane doświadczenie powyżej 2 lat w obszarze informatycznym
- Kopię posiadanego poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli "poufne" lub oświadczenie o wyrażeniu zgody na przeprowadzenie postępowania sprawdzającego w celu uzyskania dostępu do informacji niejawnych o klauzuli „poufne”, zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
- Dotyczy kandydatek/kandydatów urodzonych przed 1 sierpnia 1972 r. - oświadczenie, że w okresie od dnia 22 lipca 1944 r. do dnia 31 lipca 1990 r. kandydatka/kandydat nie pracowała/ł, nie pełniła/ł służby w organach bezpieczeństwa państwa i nie była/był współpracownikiem tych organów w rozumieniu przepisów ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów
- Najpóźniej w dniu rozmowy kwalifikacyjnej, kandydaci, którzy złożyli wymagane oświadczenia elektronicznie w formie skanów/zdjęć przekazują wszystkie oświadczenia w oryginale (skorzystaj z przygotowanego wzoru <https://www.gov.pl/web/uzp/pracuj-z-nami3>)
- Oświadczenie o posiadaniu obywatelstwa polskiego
- Oświadczenie o korzystaniu z pełni praw publicznych
- Oświadczenie o nieskazaniu prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

Dołącz, jeśli posiadasz (dokumenty dodatkowe)

- Kopia dokumentu potwierdzającego niepełnosprawność - w przypadku kandydatek/kandydatów, zamierzających skorzystać z pierwszeństwa w zatrudnieniu w przypadku, gdy znajdą się w gronie najlepszych kandydatek/kandydatów
- Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie wykształcenia
- Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie powyżej 4 lat w reagowaniu na incydenty bezpieczeństwa i prowadzeniu analiz forensycznych
- Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie powyżej 4 lat w audytach bezpieczeństwa sieci i testach penetracyjnych
- Kopie certyfikatów potwierdzających spełnienie wymagania dodatkowego z zakresu bezpieczeństwa sieci (np. CISSP, CISM) lub technologii sieciowych (np. CCNP, CCIE)

Aplikuj do: 18 listopada 2025

Aplikuj mailowo na adres: **rekrutacja@uzp.gov.pl**, w temacie wpisz: **Ogłoszenie nr 157860 / 04.11.2025.**

Lub w formie papierowej na adres: **URZĄD ZAMÓWIEŃ PUBLICZNYCH, ul. Postępu 17A, 02-676 Warszawa -**

osobiście lub pocztą (z dopiskiem na aplikacji stanowiska i nr ogłoszenia)

- w formie elektronicznej - za pośrednictwem platformy ePUAP:

<https://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/opis-uslugi/skargi-wnioski-zapytania-do-urzedu/UZP>

Uwaga: załączniki udostępnione w internecie w przestrzeni dyskowej nie będą pobierane.

Zapraszamy również do kontaktu mailowego: **rekrutacja@uzp.gov.pl**

Więcej o pracy na stronie urzędu: **<https://www.gov.pl/web/uzp/pracuj-z-nami3>**

- Dokumenty należy złożyć do: **18.11.2025**
- Decyduje data: **wpływu oferty do urzędu**
- Aplikując, oświadczasz, że znana Ci jest treść informacji na temat przetwarzania danych osobowych w naborze

Przetwarzanie danych osobowych

DANE OSOBOWE - KLAUZULA INFORMACYJNA

Dane osobowe są przetwarzane zgodnie z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

Administrator: Administratorem danych osobowych jest Prezes Urzędu Zamówień Publicznych, ul. Postępu 17a, 02-676 Warszawa.

Inspektor ochrony danych: w sprawach danych osobowych można się kontaktować z inspektorem ochrony danych: Urząd Zamówień Publicznych, ul. Postępu 17a, 02-676 Warszawa; e-mail: IOD@uzp.gov.pl

Cel przetwarzania danych: przeprowadzenie naboru na stanowisko pracy w służbie cywilnej oraz archiwizacja dokumentów po przeprowadzeniu naboru.

Informacje o odbiorcach danych: podmioty upoważnione na podstawie przepisów prawa.

Okres przechowywania danych: czas niezbędny do przeprowadzenia naboru na stanowisko pracy w służbie cywilnej (z uwzględnieniem 3 miesięcy, w których dyrektor generalny urzędu ma możliwość wyboru kolejnego wyłonionego kandydata, w przypadku, gdy ponownie zaistnieje konieczność obsadzenia tego samego stanowiska), a następnie przez czas wynikający z przepisów o archiwizacji.

Uprawnienia:

- prawo dostępu do swoich danych oraz otrzymania ich kopii;
- prawo do sprostowania (poprawiania) swoich danych osobowych;
- prawo do ograniczenia przetwarzania danych osobowych;
- prawo do usunięcia danych osobowych: żądanie realizacji tych praw należy przesłać w formie pisemnej na adres kontaktowy administratora danych, podany powyżej;
- prawo do wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa).

Podstawa prawna przetwarzania danych:

- art. 6 ust. 1 lit. b RODO;
- art. 221 Kodeksu pracy, ustawa z dnia 21 listopada 2008 r. o służbie cywilnej oraz ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach w zw. z art. 6 ust. 1 lit. c RODO;
- art. 6 ust. 1 lit. a RODO oraz art. 9 ust. 2 lit. a RODO.

Informacje o wymogu podania danych: podanie danych osobowych w zakresie wynikającym z art. 221 Kodeksu pracy oraz ustawy o służbie cywilnej jest dobrowolne, jednak niezbędne, aby uczestniczyć w procesie naboru na stanowisko pracy w służbie cywilnej. Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie. Jeżeli podane dane będą obejmowały szczególne kategorie danych, o których mowa w art. 9 ust. 1 RODO, konieczna będzie wyraźna zgoda na ich przetwarzanie, która może zostać odwołana w dowolnym czasie.

Inne informacje: podane dane nie będą podstawą do zautomatyzowanego podejmowania decyzji, nie będą też profilowane.