

## ЗАТВЕРДЖЕНО

Наказ Секретаря Рахункової палати –  
керівника апарату

« 09 » грудня 2021 року № 347-к

### УМОВИ

#### проведення конкурсу на зайняття вакантної посади головного спеціаліста відділу системного адміністрування та інформаційної безпеки управління ІТ забезпечення (категорія «В»)

<b>Загальні умови</b>	
Посадові обов'язки	<ul style="list-style-type: none"><li>- здійснення адміністрування системи електронного документообігу Megapolis DocNet, організація підтримки користувачів системи (у частині питань з системного адміністрування, ІТ безпеки, застосування кваліфікованого електронного підпису);</li><li>- впровадження механізмів контролю та контроль прав доступу користувачів у Megapolis DocNet;</li><li>здійснення робіт із обслуговування системного програмного забезпечення, встановленого на засобах обчислювальної техніки Рахункової палати, та ліквідації системних збоїв (у частині питань з системного адміністрування та ІТ безпеки). Участь у зборі та аналізі інформації щодо надійності і сумісності складових програмно-технічних комплексів (у частині питань з системного адміністрування та ІТ безпеки);</li><li>- здійснення обслуговування програмно-технічних комплексів у частині технічних засобів та системного програмного забезпечення (у частині питань з системного адміністрування та ІТ безпеки). Здійснення оновлення системного програмного забезпечення та виконання заходів щодо його зберігання та контролю версій;</li><li>- надання консультативної та методичної допомоги структурним підрозділам Рахункової палати з питань використання апаратно-програмного забезпечення (у частині питань з системного адміністрування та ІТ безпеки);</li><li>- здійснення актуалізації бази даних захисту інформації (матриці доступу, класифікаційні мітки об'єктів, ідентифікатори користувачів тощо). Участь у підготовці пропозицій щодо удосконалення порядку забезпечення захисту інформації в АС, впровадження нових технологій захисту і модернізації КСЗІ. Участь у проведенні заходів з модернізації КСЗІ та АС, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій АС або КСЗІ. Моніторинг та аналіз щоденних протоколів інформаційної безпеки на мережевому обладнанні;</li><li>- здійснення заходів щодо керування доступом до ресурсів АС Рахункової палати (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів тощо). Впровадження механізмів</li></ul>

	<p>контролю прав доступу користувачів до даних в автоматизованих інформаційно-аналітичних системах;</p> <ul style="list-style-type: none"> <li>- складання кошторису витрат на закупівлю послуг для підтримки безперебійного функціонування ІТ інфраструктури Рахункової палати (у частині питань з системного адміністрування та ІТ безпеки). Участь у контролі за виконанням укладених договорів з надання послуг підтримки безперебійного функціонування ІТ інфраструктури Рахункової палати (у частині питань з системного адміністрування та ІТ безпеки);</li> <li>- надання пропозицій щодо впровадження технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання таких засобів для потреб Рахункової палати.</li> </ul>
Умови оплати праці	<ul style="list-style-type: none"> <li>- посадовий оклад 14300 грн. відповідно до постанови Кабінету Міністрів України від 18.01.2017 № 15 «Питання оплати праці працівників державних органів»;</li> <li>- надбавки відповідно до статті 52 Закону України «Про державну службу».</li> </ul>
Інформація про строковість чи безстроковість призначення на посаду	<p>безстроково</p> <p>строк призначення особи, яка досягла 65-річного віку, становить один рік з правом повторного призначення без обов'язкового проведення конкурсу щороку</p>
Перелік інформації, необхідної для участі в конкурсі, та строк її подання	<ol style="list-style-type: none"> <li>1) заяву про участь у конкурсі із зазначенням основних мотивів щодо зайняття посади за формою згідно з додатком 2 Порядку проведення конкурсу на зайняття посад державної служби;</li> <li>2) резюме за формою згідно з додатком 2<sup>1</sup> Порядку проведення конкурсу на зайняття посад державної служби, в якому обов'язково зазначається така інформація: <ul style="list-style-type: none"> <li>- прізвище, ім'я, по батькові кандидата;</li> <li>- реквізити документа, що посвідчує особу та підтверджує громадянство України;</li> <li>- підтвердження наявності відповідного ступеня вищої освіти;</li> <li>- відомості про стаж роботи, стаж державної служби (за наявності), досвід роботи на відповідних посадах у відповідній сфері, визначеній в умовах конкурсу, та на керівних посадах (за наявності відповідних вимог);</li> </ul> </li> <li>3) заяву, в якій повідомляє, що до неї не застосовуються заборони, визначені частиною третьою або четвертою статті 1 Закону України «Про очищення влади», та надає згоду на проходження перевірки та на оприлюднення відомостей стосовно неї відповідно до зазначеного Закону. Подача додатків до заяви не є обов'язковою;</li> </ol>

	<p>4) копію Державного сертифіката про рівень володіння державною мовою (витяг з реєстру Державних сертифікатів про рівень володіння державною мовою), що підтверджує рівень володіння державною мовою, визначений Національною комісією зі стандартів державної мови.</p> <p>За бажанням можна подавати додаткову інформацію, яка підтверджує відповідність встановленим вимогам, зокрема стосовно попередніх результатів тестування, досвіду роботи, професійних компетентностей, репутації (характеристики, рекомендації, наукові публікації тощо).</p> <p><b>Інформація для участі в конкурсі приймається до 17 год. 00 хв. 17.12.2021 в електронному вигляді з накладенням кваліфікованого електронного підпису кандидата – через Єдиний портал вакансій державної служби за адресою: <a href="https://www.career.gov.ua">https://www.career.gov.ua</a></b></p>
Додаткові (необов'язкові документи)	заява щодо забезпечення розумним пристосуванням за формою згідно з додатком 3 до Порядку проведення конкурсу на зайняття посад державної служби
<p>Дата і час початку проведення тестування кандидатів</p> <p>Місце або спосіб проведення тестування.</p> <p>Місце або спосіб проведення співбесіди (із зазначенням електронної платформи для комунікації дистанційно)</p> <p>Місце або спосіб проведення співбесіди з метою визначення суб'єктом призначення або керівником державної служби переможця (переможців) конкурсу (із зазначенням електронної платформи для комунікації дистанційно)</p>	<p>23.12.2021 о 10 год. 00 хв.</p> <p>м. Київ, вул. М. Коцюбинського, 7 (проведення за фізичної присутності кандидатів)</p> <p>м. Київ, вул. М. Коцюбинського, 7 (проведення за фізичної присутності кандидатів)</p> <p>м. Київ, вул. М. Коцюбинського, 7 (проведення за фізичної присутності кандидатів)</p>
Прізвище, ім'я та по батькові, номер телефону, адреса електронної пошти	Дяченко Ірина Анатоліївна, тел. 206-07-46, Diachenko_IA@rp.gov.ua

особи, яка надає додаткову інформацію з питань проведення конкурсу		
<b>Кваліфікаційні вимоги</b>		
1.	Освіта	вища за освітнім ступенем не нижче бакалавра
2.	Досвід роботи	не потребує
3.	Володіння державною мовою	вільне
<b>Вимоги до компетентності</b>		
	<b>Вимога</b>	<b>Компоненти вимоги</b>
1.	Досягнення результатів	<ul style="list-style-type: none"> <li>- здатність до чіткого бачення результату діяльності;</li> <li>- вміння фокусувати зусилля для досягнення результату діяльності;</li> <li>- вміння запобігати та ефективно долати перешкоди</li> </ul>
2.	Відповідальність	<ul style="list-style-type: none"> <li>- усвідомлення важливості якісного виконання своїх посадових обов'язків з дотриманням строків та встановлених процедур;</li> <li>- усвідомлення рівня відповідальності під час підготовки і прийняття рішень, готовність нести відповідальність за можливі наслідки реалізації таких рішень;</li> <li>- здатність брати на себе зобов'язання, чітко їх дотримуватись і виконувати.</li> </ul>
3.	Цифрова грамотність	<ul style="list-style-type: none"> <li>- вміння працювати з комп'ютерним обладнанням та програмним забезпеченням призначеним для захисту інформації;</li> <li>- знання з основ побудови комп'ютерних мереж, а також державних стандартів у сфері захисту інформації та побудови інформаційних систем;</li> <li>- вміння працювати з технічною документацією;</li> <li>- здатність передбачати небезпеки в цифровому середовищі, вміння реагувати на інциденти з порушення безпеки обробки даних;</li> <li>- вміння використовувати інформаційні системи, системи електронного документообігу та інші електронні інструменти та сервіси для електронного листування або обміну інформацією.</li> </ul>
<b>Професійні знання</b>		
	<b>Вимога</b>	<b>Компоненти вимоги</b>
1.	Знання законодавства	<ol style="list-style-type: none"> <li>1. Конституція України;</li> <li>2. Закон України «Про державну службу»;</li> <li>3. Закон України «Про запобігання корупції»</li> </ol>
2.	Знання законодавства у сфері	<ol style="list-style-type: none"> <li>1. Закон України «Про Рахункову палату»;</li> <li>2. Закон України «Про електронні документи та електронний документообіг»;</li> <li>3. Закон України «Про електронні довірчі послуги»;</li> <li>4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;</li> </ol>

		<p>5. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;</p> <p>6. Регламент організації взаємодії органів виконавчої влади в електронній формі затвердженого постановою Кабінету Міністрів України від 17.01.2018 №55,</p> <p>7. Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затверджених наказом Міністерства юстиції України від 18.06.2015 №1000/5.</p> <p>8. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373;</p> <p>9. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (НД ТЗІ 3.7-003 -2005).</p> <p>10. Знання:  ДСТУ ISO/IEC 27001:2015, Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги.  ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.</p>
--	--	---