Умови
проведення добору на зайняття вакантної посади державної служби
категорії «В»
головного спеціаліста відділу з інформаційної безпеки та кіберзахисту управління інформаційних систем та електронних реєстрів
Головного управління Пенсійного фонду України в Дніпропетровській області
(місцезнаходження робочого місця:
м. Дніпро, вул. Набережна Перемоги, буд. 26,
м. Дніпро, вул. Зимових Походів, буд. 22-А,
м. Кам'янське, вул. Інститутська, буд. 4,
м. Кривий Ріг, вул. Книжна, буд. 1/1**)**

Загальні умови	
Посадові обов’язки	- забезпечення криптографічного захисту інформації та контролю за дотриманням політики безпеки при використанні засобів криптографічного захисту інформації; - контроль стану та ризиків безпеки інформації, перевірка випадків порушення стану безпеки; - здійснення заходів із забезпечення використання кваліфікованого електронного підпису; - здійснення заходів щодо кібербезпеки, кіберзахисту та інформаційної безпеки вузлів обласного рівня ІКС ПФУ; - здійснення адміністрування антивірусного захисту та засобів безпеки захисту
Умови оплати праці	Посадовий оклад – 20 795 грн. Надбавка за ранг державного службовця — від 200 до 500 грн. Надбавка за вислугу років — 2 відсотки посадового окладу державного службовця за кожний календарний рік стажу державної служби, але не більше 30 відсотків посадового окладу. Надбавки, доплати та премії відповідно до статті 52 Закону України “Про державну службу” (зі змінами)
Інформація про строковість чи безстроковість призначення на посаду	Призначення на період дії воєнного стану в Україні та до призначення конкурсу на дану посаду, але не довше 12 місяців з дня припинення чи скасування воєнного стану
Перелік інформації, необхідної для участі в конкурсі, та строк її подання	Особа, яка бажає взяти участь в доборі, подає резюме, в якому обов’язково зазначається така інформація: прізвище, ім’я, по батькові кандидата; реквізити документа, що посвідчує особу та підтверджує громадянство України; підтвердження наявності відповідного ступеня вищої освіти; відомості про стаж роботи, стаж державної

---

* *рекомендується зазначати до десяти посадових обов'язків у відповідності до посадової інструкції*

	служби (за наявності), досвід роботи на відповідних посадах у відповідній сфері, визначеній в умовах добору, та на керівних посадах (за наявності відповідних вимог). Інформація приймається до ***30.09.2026 року*** шляхом надсилання на резюме на електронну пошту управління по роботі з персоналом dpfu04@gmail.com або надання резюме за адресою: м. Дніпро, вул. Набережна Перемоги, 26, каб. 917
Дата і час початку, місце , спосіб проведення співбесіди	Про дату і час проведення співбесіди буде додатково повідомлено. м. Дніпро, вул. Набережна Перемоги, 26, (за фізичної присутності кандидатів) Кандидатам при собі необхідно мати паспорт громадянина України або інший документ, який посвідчує особу та підтверджує громадянство України
Прізвище, ім'я та по батькові, номер телефону та адреса електронної пошти особи, яка надає додаткову інформацію з питань проведення добору	Юрченко Юлія Олегівна, Копил Наталія Юріївна 067-885-90-10, dpfu04@gmail.com

Кваліфікаційні вимоги		
1.	Освіта	вища освіта не нижче бакалавра, молодшого бакалавра
2.	Досвід роботи	не потребує
3.	Володіння державною мовою	вільне володіння державною мовою
Вимоги до компетентності		
Вимога		**Компоненти вимоги**
1.	Досягнення результатів	- здатність до чіткого бачення результату діяльності; - вміння фокусувати зусилля для досягнення результату діяльності; - вміння запобігати та ефективно долати перешкоди.
2.	Відповідальність	- усвідомлення важливості якісного виконання своїх посадових обов'язків з дотриманням строків та встановлених процедур; - усвідомлення рівня відповідальності під час підготовки і прийняття рішень, готовність нести відповідальність за можливі наслідки реалізації таких рішень; - здатність брати на себе зобов'язання, чітко їх дотримуватись і виконувати
3.	Цифрова грамотність	- вміння використовувати комп'ютерні пристрої, базове офісне та спеціалізоване програмне забезпечення для

		ефективного виконання своїх посадових обов'язків; - вміння використовувати сервіси інтернету для ефективного пошуку потрібної інформації; вміння перевіряти надійність джерел і достовірність даних та інформації у цифровому середовищі; - здатність працювати з документами в різних цифрових форматах; зберігати, накопичувати, впорядковувати, архівувати цифрові ресурси та дані різних типів; - здатність уникати небезпек в цифровому середовищі, захищати особисті та конфіденційні дані; - вміння використовувати електронні реєстри, системи електронного документообігу та інші електронні урядові системи для обміну інформацією, для електронного листування в рамках своїх посадових обов'язків; - вміння використовувати спільні онлайн календарі, сервіси для підготовки та спільного редагування документів, вміти користуватись кваліфікованим електронним підписом (КЕП); - здатність використовувати відкриті цифрові ресурси для власного професійного розвитку
4.	Аналітичні здібності	- здатність до логічного мислення, узагальнення, конкретизації, розкладання складних питань на складові, виділяти головне від другорядного, виявляти закономірності; - уміння встановлювати причинно-наслідкові зв'язки; - уміння аналізувати інформацію та робити висновки, критично оцінювати ситуації, прогнозувати та робити власні умовиводи
Професійні знання		
Вимога		**Компоненти вимоги**
1.	Знання законодавства	Знання: 1. Конституції України; 2. Закону України «Про державну службу»; 3. Закону України «Про запобігання корупції» та іншого законодавства
2.	Знання законодавства у сфері	Знання: 1. Закону України «Про захист інформації в інформаційно-комунікаційних системах»; 2. Закон України «Про основні засади забезпечення кібербезпеки України»; 3. Інші нормативно-правові документи в сфері захисту інформації
3.	Знання в сфері інформаційної безпеки та кіберзахисту	Складові політики інформаційної безпеки; 1. Знання в сфері системи управління інформаційною безпекою; 2. Знання принципів та способів забезпечення конфіденційності, цілісності, доступності інформації; 3. Розуміння принципів роботи симетричного,

		асиметричного шифрування, хешування та цифрового підпису; 4. Розуміння принципів роботи сучасних комп'ютерних мереж; 5. Знання основних типів загроз безпеки інформації.