| Номер тендеру в ЦБД | Тип процедури | Предмет закупівлі | Класифікація | Обгрунтування технічних та якісних характеристик предмету закупівлі | Обгрунтування розміру бюджетного призначення та очікуваної вартості закупівлі |
|---|---|---|---|---|---|
| UA-2021-10-23-006423-b | Відкриті торги | Послуги з побудови комплексної системи захисту інформації на автоматизовану систему класу 3 четвертої категорії та організація проведення додаткової державної експертизи у сфері технічного захисту інформації інформаційно-телекомунікаційної системи «Центральна база даних електронної системи охорони здоров'я» | ДК 021:2015: 71310000-4: Консультаційні послуги у галузях інженерії та будівництва | 71310000-4 - Консультаційні послуги у галузях інженерії та будівництва (Послуги з побудови комплексної системи захисту інформації на автоматизовану систему класу 3 четвертої категорії та організація проведення додаткової державної експертизи у сфері технічного захисту інформації інформаційно-телекомунікаційної системи «Центральна база даних електронної системи охорони здоров'я»)<br><br>У зв'язку із модернізацією інформаційно-телекомунікаційної системи «Центральна база даних електронної системи охорони здоров'я (далі – Система) метою закупівлі є створення комплексної системи захисту інформації (далі – КСЗІ) Системи (далі разом – КСЗІ Системи) та досягнення максимальної ефективності захисту за рахунок одночасного цільового використання усіх необхідних ресурсів, методів і засобів, що виключатимуть несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно-правових актів України у сфері захисту інформації: Закони України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».<br>В результаті виконання проекту буде реалізовано:<br>1. Забезпечення максимального рівня ефективного захисту інформації в Системі.<br>2. Забезпечення недопущення блокування інформації, несанкціонованого доступу до неї та/або її модифікації в Системі за рахунок одночасного використання усіх необхідних ресурсів, методів і засобів.<br>3. Досягнення максимальної ефективності захисту інформації за рахунок одночасного використання усіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до нормативно-правових актів України у сфері захисту інформації.<br><br>Обгрунтування технічних та якісних характеристик предмета закупівлі:<br>На виконання положень Законів України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», Загальних вимог до кіберзахисту об'єктів критичної інфраструктури затверджених постановою КМУ від 19.06.2019 №518, Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою КМУ від 29.03.2006 № 373, Указів Президента України від 26 серпня 2021 року №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», від 16 січня 2017 року № 8/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», від 13 лютого 2017 року №32/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», від 30 серпня 2017 року № 254/2017 Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32,<br>для забезпечення сталого, безперебійного та захищеного функціонування Системи необхідно організувати роботи щодо побудови КСЗІ Системи та проведення її додаткової державної експертизи. Метою створення КСЗІ Системи є забезпечення конфіденційності, цілісності та доступності інформації, яка циркулює в Системи, від несанкціонованої модифікації або знищення шляхом здійснення протидії загрозам від дій потенційного порушника. Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування Системи. КСЗІ Системи з метою здійснення захисту інформації на всіх стадіях її життєвого циклу повинна передбачати застосування наступних заходів та засобів захисту інформації: - організаційні заходи, які реалізуються поза межами Системи;<br>- технічні заходи, що реалізуються поза межами Системи;<br>- апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу до інформації, яка обробляється та зберігається в Системи.<br>КСЗІ Системи призначена для:<br>- реалізації політики безпеки інформації, прийнятої в Системи;<br>- забезпечення конфіденційності, цілісності та доступності інформації під час експлуатації Системи;<br>- ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів Системи, причин та умов, які спричиняють або можуть привести до порушення її нормального функціонування;<br>- керування засобами захисту інформації, розмежування доступу користувачів до ресурсів Системи, контроль за їх роботою з боку осіб, які відповідають за забезпечення безпеки інформації в Системи ;<br>- створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування Системи;<br>- організації обліку, зберігання, обігу інформації, яка потребує захисту, та матеріальних носіїв, на яких вона накопичується;<br>- реєстрації, збору, зберігання, обробки даних про всі події в Системи, які мають відношення до безпеки інформації;<br>- забезпечення доступності ресурсів Системи для авторизованих користувачів.<br>Для досягнення вказаної мети необхідно здійснити наступні заходи:<br>1. Обстеження середовища функціонування Системи, визначення потенційних загроз, внесення відповідних змін до документів модель загроз та модель порушника, або розробка нових.<br>2. Аналіз актуальності технічного завдання на створення КСЗІ Системи, внесення відповідних змін, або розробка нового технічного завдання на створення КСЗІ Системи за необхідністю.<br>3. Аналіз актуальності плану захисту інформації в КСЗІ Системи, внесення відповідних змін, або розробка нового плану захисту інформації в КСЗІ Системи за необхідністю.<br>4. Постачання та впровадження засобу захисту інформації.<br>5. Аналіз актуальності технороботочого проекту на КСЗІ Системи, несення відповідних змін, або розробка нового технороботочого проекту на КСЗІ Системи за необхідністю.<br>6. Попередні випробування КСЗІ Системи.<br>7. Дослідна експлуатація КСЗІ Системи.<br>8. Організація проведення додаткової державної експертизи у сфері технічного захисту інформації КСЗІ Системи. | Розмір бюджетного призначення для надання послуг з впровадження КСЗІ відповідає розрахунку видатків до кошторису НСЗУ на 2021 рік. Кошти заплановані за КПКВК 2308060 на 2021 рік, КЕКВ 2240 Оплата послуг (крім комунальних).<br>Очікувана вартість предмета закупівлі визначена у межах видатків, передбачених для НСЗУ кошторисом на 2021 рік за бюджетною програмою КПКВК 2308060, КЕКВ 2240 Оплата послуг (крім комунальних) відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18 лютого 2020 року №275. |