Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі

(відповідно до пункту 4^1 постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами))

1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань, його категорія:

Державна установа «Держгідрографія»; вул. Електриків, 26, м. Київ, 04176; код за ЄДРПОУ – 21720000

2. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником:

ДК 021:2015 - 48820000-2 Сервери (обладнання для єдиного апаратного комплексу центру обробки даних ДУ "Держгідрографія") з монтажними та пусконалагоджувальними роботами.

3. Ідентифікатор закупівлі: UA-2021-04-29-005226-a

4. Обґрунтування технічних та якісних характеристик предмета закупівлі.

Обґрунтуванням закупівлі є висновки проведених в ДУ «Держгідрографія» аудитів та проєктування інформаційної інфраструктури з метою забезпечення якісного виконання покладених функцій установою.

Результати проведення технічного аудиту серверної та мережевої інфраструктури та аналізу систем інформаційної безпеки ДУ «Держгідрографія» (далі – Установа).

На виконання службових записок від 13.01.2021 № 31-Сз та від 14.01.2021 № 37-Сз, згідно з договорами від 16.01.2021 № 03/21, № 04/21 було проведено аудит серверної та

мережевої інфраструктури і систем інформаційної безпеки ДУ «Держгідрографія». За результатами аудиту, що проходив з 17.01.2021 до 27.01.2021, надано звіти та підсипано акти від 27.01.2021.

Висновки аудиту серверної та мережевої інфраструктури:

1) Відсутня централізована система моніторингу, це не дозволяє стежити за всім важливим, з точки зору бізнес-процесів, обладнанням й унеможливлює підтримання актуальності даних про стан систем. Зокрема, щодо використовуваних/вільних ресурсів, навантаженнь (середніх, пікових), стан підключення, відключеня сервісів та інше.
2) Відсутня система резервного копіювання даних. Відсутність політик і регламентів резервного копіювання та самої централізованої та автоматизованої системи резервного копіювання є критичним, оскільки унеможливлює відновлення працездатності сервісів (зокрема відновлення даних), у разі відмови обладнання, збою ПЗ або в результаті кібератаки.
3) Відсутня централізована система надання доступу до інформаційних систем. З використанням сервісу каталогів Active Directory можна гнучко, а головне, стандартизовано і централізовано керувати доступом працівників до зовнішніх ресурсів та ресурсів Установи.
4) Відсутні централізовані та стандартизовані правила й описи процесу відновлення IT-систем Установи.
5) Інфраструктуру Установи реалізовано без попереднього планування. Пакет документів «Супровідна документація IT-систем», призначений для структурованості і підконтрольності IT-систем, відсутній, що ускладнює обслуговування системи.
6) Відсутня централізована і стандартизована карта доступів в Установі. Централізоване управління доступом всередині локальних доменів, там, де це наявне, налаштоване некоректно або не використовується за призначенням. Політики AD GPO (Active Directory Group Policy Object) повноцінно не використовуються, оскільки на багатьох пристроях наявні користувачі (в тому числі і локальні), додані вручну, без використання методик автоматизації та централізованості процесу, передбачених службою каталогів корпорації Microsoft.
7) Загальна схема побудови інформаційної системи не централізована і стандартизована для всієї інфраструктури. Відсутні єдині засоби адміністрування та моніторингу сервісів, пристроїв і ресурсів.
8) Серверна інфраструктура у філіях не має середовищ віртуалізації. Це унеможливлює імплементацію в сучасні інфраструктури централізованого моніторингу, управління

ресурсами, управління даними, а також зводить нанівець можливість забезпечення відмовостійкості серверного обладнання, сервісів і бізнес-процесів.

9) Дизайн інфраструктури окремо розглянутих філій, топології, в більшості ідентичні і містять ряд схожих проблем, які необхідно виправити для коректного і безпечного функціонування ІТ-систем. Насамперед це стосується відсутності логічного розмежування сегментів мережі в будь-якому вигляді і в будь-якій імплементації. Це ставить під загрозу стабільність інфраструктури, її відмовостійкість, а також безпеку, як перед зовнішніми, так і перед внутрішніми факторами загроз.

10) Система віртуалізації має некоректну конфігурацію, а саме:

- багато із серверів не є віртуалізованими;
- vCenter (управління середовищем віртуалізації) відсутній;
- крім VMware vSphere, є рішення на базі Proxmox;
- відсутнє резервування LAN-з'єднання.

11) Мережеве обладнання, що використовується, не здатне забезпечити повноцінну інформаційну безпеку інфраструктури, оскільки не є UTM або NGFW, а виконує лише базові функції брандмауера, тобто не може забезпечити вебфільтрацію, IPS/IDS (Intrusion Prevention System/Intrusion Detection System), контроль додатків, сигнатурний аналіз пакетів L7 рівня.

12) Не використовується логічний поділ мережі на підмережі та віртуальні підмережі (vlan), що забезпечує в теорії і на практиці доступ усіх пристроїв до всіх пристроїв, що є недопустимим при побудові рекомендованої або хоча б мінімально захищеної топології мережі.

13) Переважно не використовується середовище віртуалізації, що не дозволяє реалізувати відмовостійкість бізнес-процесів і централізоване (або навіть розподілене) управління обчислювальними ресурсами і ресурсами сховищ, а також можливість швидкого відновлення систем у разі їх виходу з ладу.

14) На більшості серверів виявлено засоби щодо забезпечення безпеки кінцевих точок. Проте вони є стандартними та непоновлюваними, із застарілими сигнатурними базами (Windows Defender, Security Essentials) або безкоштовними (Comodo, 360 Total Security). В інфраструктурі філій і апарату управління відсутні центри контролю та управління антивірусною системою. З огляду на те, що мережеве обладнання, яке використовується в Установі, не може забезпечити виконання необхідного функціонала, захист кінцевих точок практично не використовується, загальна інфраструктура піддається ще більшій небезпеці.

15) Серверне обладнання, що використовується, не є повністю стандартизованим і його централізований моніторинг і облік не ведуться. Значна частина серверного обладнання використовується більше за рекомендований термін служби (4–7 років), що спричиняє потенційні проблеми, пов'язані з надійністю апаратних ресурсів, особливо з урахуванням

того, що управління і резервування апаратних потужностей фактично ніде не використовується і не реалізується. Також варто зазначити, що наявна велика кількість обладнання (CPU, HDD), не призначеного для використання в серверній інфраструктурі (сюди входять лінійки процесорів Intel Pentium, Atom, i3, i5 і SATA HDD (7200 rpm, або навіть 5500 rpm), особливо ті, які не перебувають у конфігурації RAID).

16) У серверній інфраструктурі використовуються як серверні ОС (Windows Server 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016), так і системи для персональних комп'ютерів і робочих станцій (Windows XP, Windows 7, Windows 8, Windows 10). Подібна різноманітність ускладнює можливість потенційного розгортання централізованого контролю й управління інфраструктурою, а що стосується застарілих ОС, то на додачу до всього становить чималу загрозу для безпеки бізнес-процесів та інфраструктури в цілому, оскільки оновлення безпеки на застарілі ОС не поширюються.

17) У філіях відсутні локальні контролери домену (AD) або такі, що підпорядковуються контролерам домену апарату управління. Всі працівники використовують локальні облікові записи з адміністративними правами. Така топологія взаємодії тягне за собою неможливість гнучкого централізованого управління доступами і інфраструктурою в цілому. Відсутні будь-які політики GPO, розподіл доступів до корпоративних або зовнішніх ресурсів не реалізований.

18) Переважно використовується обладнання Mikrotik, яке, хоч і має функціонал брандмауера, не може рекомендуватися як таке, що не відповідає вимогам інформаційної безпеки, оскільки не може забезпечити необхідного захисту й аналізу через відсутність web filtering, ips/ids, application control, AV instpection, traffic shaping based on L7 signatures тощо. Відсутня централізована система захисту локальної мережі. На кінцевих пристроях, як правило, відсутні актуальні засоби захисту, а оновлення безпеки для ОС також не встановлені. Моніторинг основних вузлів (серверних і мережевих) не використовується. Управління доступом відсутнє.

19) Наявна реалізація поштового сервера не є стабільною, відмовостійкою і здатною забезпечити необхідний функціонал, оскільки схема побудови не відповідає будь-яким BestPractice від будь-якого виробника. Більше того, поштовий сервіс нецентралізований і в різних філіях реалізований з використанням різного ПЗ MS Exchange, Zimbra, Mdaemon тощо. Відсутній рекомендований розподіл ролей і навантажень для поштового сервісу (EDGE, WAP, DataBases).

20) Наявні бази даних нецентралізовані і в своїй більшості рознесені по філіях. Централізовані і стандартизовані регламентні роботи не проводяться. Централізоване та регламентоване резервування даних відсутнє.

21) Сервіс централізованого і безпечного оновлення ПЗ у всіх філіях і апараті управління відсутній.

Висновки аналізу систем інформаційної безпеки:

1) Модель і еталонний план IT-безпеки в Установі не розроблений. Безпека реалізована за використання програмно-апаратного забезпечення мінімального рівня захисту. Топологію мережевої інфраструктури та інфраструктури мережевої безпеки не спроєктовано. На сьогоднішній день системи мережевої безпеки не забезпечують необхідного рівня надійності інформаційної безпеки Установи.

2) Обмін критичними даними використовує, в тому числі, не захищені канали передавання даних, це тягне за собою високу зону ризику.

3) Виступаючи периметром мережі, таке обладнання, як MikroTik, D-Link або TP-Link, вимушене виконувати роль Firewall, проте це обладнання не розроблялося з такою метою та не може надати необхідного рівня ані захисту, ані функціонала. Також у цьому обладнанні відсутні аналіз трафіку, сегментація, контроль входу і виходу мережевих пакетів тощо.

4) Відсутність сегментації у внутрішній інфраструктурі в межах Установи на різні віртуальні (логічні) підмережі також є загрозою для всієї IT-інфраструктури, оскільки при компрометації однієї системи наявний легкий доступ до всіх інших систем і сервісів Установи. Така ситуація спостерігається у всіх філіям та апараті управління.

5) Відсутній поділ на віртуальні підмережі в мережах, що поширюються по Wi-Fi, що є необхідним.

6) Відсутня будь-яка стандартизація використовуваного обладнання. Наявне мережеве обладнання від різних вендорів, таких як MikroTik, TP-Link, Keenetic, Tenda, D-Link, Asus, Hpe, які виконують роль маршрутизаторів та комутаторів рівня доступу.

7) Централізоване управління та централізований моніторинг такої інфраструктури неможливі.

8) Управління доступами працівників як локальними (LAN), так і глобальними (WAN)) відсутнє.

9) Не дотримано логіки в розміщенні мережевого обладнання в локальній мережевій інфраструктурі у філіях та апараті управління.

10) Доступ між різними середовищами функціонування Установи не заблокований.

11) Не виділено окремі сегменти для доступу в мережу працівників підрядних організацій, аудиторів та інших осіб, які не є працівниками Установи.

12) Не виділено окремі сегменти для різного типу обладнання, що використовується в Установі (окремий VLAN для CCTV, окремий VLAN для телефонії, окремий VLAN для серверного обладнання, окремий VLAN для адміністрування систем).

13) На інтерфейсах, підключених до провайдерів, не налаштовано базові списки доступів, які забезпечують базовий захист від атак з мереж провайдера.

14) Не використовуються міжмережеві екрани для контролю доступу користувачів до додатків інформаційних ресурсів, а також забезпечення сегментації мережі на зони безпеки, щоб запобігти несанкціонованому доступу.

15) Не використовуються системи виявлення/запобігання мережевим атакам як на периметрі мережі, так і в локальній мережі за допомогою SPAN-порту комутатора. Сигнатури не регулярно оновлюються.

16) В Установі відсутня задокументована політика управління доступом, процес реєстрації доступу користувачів не врегульовано. Відсутній процес перегляду прав доступу користувачів до інформаційних ресурсів на регулярній основі і процес, який гарантує, що права доступу до інформації та засобів обробки інформації всіх працівників і представників сторонніх організацій були видалені або змінені після закінчення їх відносин (трудових, контрактних, договірних). Немає задокументованого процесу, що описує методи організації доступу та використання конфіденційної інформації. Не визначено вимог щодо складності паролів для користувачів і адміністраторів.

17) Дані обробляються на застарілих серверних і програмних продуктах, цілісність, доступність, надійність і стабільність роботи забезпечити неможливо.

18) Немає задокументованої політики резервного копіювання. Резервне копіювання даних/систем/сервісів не здійснюється.

19) Не ведуться відповідні журнали подій. Журнали дій системних адміністраторів/операторів не контролюються.

20) Немає політики або регламенту архівування даних. Централізоване архівування даних не проводиться.

21) Системи інформаційної безпеки бізнесу відсутні.

Висновки аудиту мережевої структури та систем інформаційної безпеки, що проводилися у 2019-2020 роках ДП «Галузевий центр цифровізації та кібербезпеки»:

Фахівцями ДП «Галузевий Центр Цифровізації та Кібербезпеки» згідно договору №47/19 від 06.062019 було надано послуги у сфері локальних мереж, а саме розробка детальної топології локальної обчислювальної мережі, сканування локальної обчислювальної мережі на вразливості на надання детального консолідованого звіту за даними роботами.

Також згідно договору «32 від 16.04.2020 року, ДП «Галузевий Центр Цифровізації та Кібербезпеки» проводило аналіз стану інформаційно-комунікаційних систем Установи.

В результаті досліджень було надано наступні висновки:

Фахівцями ДП «Галузевий центр цифровізації та кібербезпеки» згідно з договором від 06.062019 № 47/19 було надано послуги у сфері локальних мереж, а саме: розробка детальної топології локальної обчислювальної мережі, сканування локальної обчислювальної мережі на вразливості та надання детального консолідованого звіту щодо виконання цих робіт. Також відповідно до договору від 16.04.2020 № 32 ДП «Галузевий центр цифровізації та кібербезпеки» проводило аналіз стану інформаційно-комунікаційних систем Установи.

У результаті досліджень було надано такі висновки:

1) Сегментація мережі відсутня, топологія на момент проведення аналізу однорангова. Сегменти мережі здатні взаємодіяти один з одним та неізольовані.

2) Підключення сторонніх пристроїв до мережі не обмежується. Повноцінний доступ до мережі можливо отримати з будь-якого пристрою з портом Ethernet, перебуваючи в периметрі Установи та підключившись до вільної активної розетки.

3) На мережевому обладнанні рівня доступу не включено захисту від атак типу ARP spoofing (зміна ARP таблиці жертви), що дозволяє організувати атаку типу MITM (людина посередині).

4) На мережевому обладнанні рівня доступу не включено захисту від атак типу dhcp spoofing – організація роботи не авторизованого сервера DHCP (динамічного налаштування клієнтських вузлів), що дозволяє організувати атаку типу MITM (людина посередині).

5) Для багатьох сучасних ОС IPv6 активовано за замовчуванням, але не використовується. Як правило, адміністратори безпеки звертають увагу на захист IPv4 підключень і не враховують безпеку IPv6.

6) У мережевій архітектурі єдина точка відмови комутаторів агрегації каналів. У схемі роботи відсутнє резервне обладнання.

7) Відсутня URL-фільтрація і контроль роботи додатків, механізмів захисту від шкідливого коду.

8) Відсутня статистика і телеметрія підключень до мережі.

9) Відсутній процес системного зберігання контрольних журналів мережевого серверного обладнання, операційних систем і баз даних.

10) Відсутня політика періодичної зміни паролів доступу до мережевого обладнання.

11) Облікові записи адміністратора до мережевого устаткування не персоналізовані.

12) Операційні системи мережевого обладнання періодично не оновлюються.

13) Не виконується періодична перевірка інформаційних активів Установи на наявність вразливостей програмного забезпечення.

14) Декілька користувачів має необмежені права на робочих станціях.

15) Процес управління вразливостями не впроваджений.

16) Дані частини користувачів зберігаються на робочих станціях і не виконується резервне копіювання цих даних.

17) Відсутні контрольні журнали ПО і журнали аудиту.

18) Створення резервних копій не систематизовано.

19) Стадія планування допомагає організувати процес у разі настання ризику.

20) Підвищення обізнаності працівників у контексті інформаційної безпеки не проводиться.

21) В існуючій ІТС відсутній порядок присвоєння пароля для користувачів. Також відсутнє розмежування кінцевих користувачів і систем мережевого та серверного обладнання, що є критичним недоліком мережевої архітектури.

22) Облікові записи користувачів, а разом з тим і їх спільні папки, не захищені паролями, що дає змогу заволодіти конфіденційною інформацією.

23) У локальній мережі трафік не шифрується.

24) Контроль доступу до мережі Інтернет через Blacklist/Whitelist не використовується.

Загальні висновки аналізу стану інформаційної інфраструктури Установи, можливі наслідки відсутності модернізації системи та рекомендації із модернізації.

1) Інформаційна інфраструктура Установи працює в режимі максимального навантаження, про що свідчать постійні інциденти в роботі обладнання.

2) Інформаційна інфраструктура Установи не є спроєктованою системою і не може бути надійною через відсутність централізованості та стандартизації.

3) Інформаційна інфраструктура Установи не має систем інформаційної безпеки.

4) Інформаційна інфраструктура Установи не має надійних систем резервного копіювання.

5) Інформаційна інфраструктура Установи не має скоординованої системи антивірусного захисту.

6) Мережева інфраструктура не є правильно спланованою та працює на ненадійному обладнанні, яке не має функцій захисту інформації.

Це може мати негативні наслідки для Установи, зокрема:

1) загроза відмови обладнання, яке підтримує виконання основних функцій Установи – підтримання безпеки судноплавства, функціонування системи NAVTEX, AIC та системи моніторингу ЗНО;

2) вихід з ладу елементів серверної інфраструктури може спричинити зупинку роботи Установи через відсутність відмовостійкості та кластеризації;

3) через відсутність технічних ресурсів,серверна архітектура Установи спроєктована некоректно, що тягне за собою ризики доступності, безпеки і функціональних можливостей;

4) існуюча архітектура не дозволяє коректно масштабувати і розширювати технічні потужності, а значить й інформаційні сервіси Установи;

5) використання ненадійного серверного та програмного забезпечення тягне за собою істотні ризики можливості злому, дискредитації даних та інформації, часткової або повної зупинки функціонування сервісу;

6) недостатній рівень автоматизованої системи резервного копіювання тягне за собою ризик втрати даних;

7) недостатній рівень сегментації мережевої інфраструктури тягне за собою ризики поширення шкідливого коду і шпигунських програм;

8) недостатній рівень захисту периметра мережі і недостатній рівень захисту поштового сервісу тягне за собою ризик несанкціонованого доступу до ресурсів Установи;

9) відсутні необхідні функціональні інструменти для реалізації надійної, безпечної мережевої інфраструктури, що може спричинити вихід з ладу елементів мережевої інфраструктури та призвести до зупинки роботи Установи.

Мета і призначення закупівлі

Мета створення програмно-апаратного комплексу центру обробки даних ДУ «Держгідрографія».

З огляду на результати аудиту серверної та мережевої інфраструктури та аналізу систем інформаційної безпеки, на виконання службової записки від 28.01.2021 № 88-Сз було укладено договір від 02.02.2021 № 06/21 на проєктування програмно-апаратного комплексу центру обробки даних ДУ «Держгідгографія». За результатами виконання договору надано проєкт центру обробки даних Установи та підписано акти про виконані роботи від 09.02.2021.

Запропонований проєктом центр обробки та збереження даних (далі – ЦОД) має виконувати функції обробки і зберігання інформації; він орієнтований на вирішення завдань Установи шляхом надання інформаційних послуг і забезпечення безперервної роботи систем

та сервісів Установи. Консолідація обчислювальних ресурсів і засобів зберігання даних у ЦОД дозволяє скоротити сукупну вартість утримання ІТ-інфраструктури за рахунок можливості ефективного використання технічних засобів, наприклад, відмови від використання сторонніх сервісів обробки даних, хмарних сервісів, перерозподілу навантажень, а також за рахунок скорочення витрат на адміністрування.

Рекомендовані програмно-апаратні рішення інформаційної інфраструктури

Рішення з інтеграції систем	Переваги рішення
Обчислювальні системи і системи зберігання даних	Організація надійного зберігання, обробки інформаційних ресурсів і надання доступу до них
Платформа віртуалізації	Організація уніфікованого, централізованого, відмовостійкого, контрольованого середовища з можливістю масштабування
Системи резервного копіювання	Відновлення даних у разі їх пошкодження або знищення
Мережева інфраструктура	Основа для ефективного обміну інформацією між користувачами, ПЗ, сервісами, серверами
Системи захисту периметра мережі	Запобігання атакам на ІТ-ресурси і реалізація безпечного доступу працівників до зовнішніх мереж і віддалених корпоративних ресурсів
Системи захисту даних	Забезпечення управління доступами до даних, реєстрація подій безпеки, перевірка цілісності інформації, захист від витоку даних
Системи захисту серверних операційних систем	Ідентифікація та автентифікація суб’єктів доступу, ідентифікація об’єктів доступу, управління доступами, обмеження використання програмного середовища, виявлення (запобігання) вторгнень, антивірусний захист
Системи захисту робочих станцій і мобільних пристроїв	Антивірусний захист, реєстрація подій безпеки, виявлення (запобігання) вторгнень, захист і аналіз носіїв інформації
Системи централізованого управління ідентифікацією та доступами	Перевірка автентичності користувача, управління доступом. Забезпечення уніфікованого механізму управління інфраструктурою, доступами, налаштування для користувача робочого середовища
Системи централізованого	Автоматизоване централізоване управління

управління мережевою безпекою	мережевою інфраструктурою, застосування політик, оновлення і моніторинг пристроїв
Системи централізованого управління мережевою інфраструктурою	Автоматизація основних процесів з контролю і управління IT-ресурсами, можливість проактивного виявлення та локалізації інцидентів, сервісний підхід в управлінні IT-інфраструктурою
Системи централізованого моніторингу	Забезпечення централізації й актуалізації даних про стан IT-систем
Системи централізованого оновлення	Централізоване управління оновленнями серверів і робочих станцій, економія зовнішнього трафіку
Операційні системи серверного забезпечення	Управління додатками, що обслуговують усіх користувачів корпоративної мережі. Забезпечення безперервності і стабільності функціонування
Системи відмовостійкості та балансування навантаження бізнес-додатків	Управління навантаженнями і забезпечення безперервності функціонування критично важливих бізнес-процесів

Якісні та кількісні характеристики ЦОД і його складових розраховані з урахуванням вимог до обладнання, що потребують сервіси, які використовує та надає Установа – підтримка безпеки судноплавства, сталого функціонування та відмовостійкості систем NAVTEX, навігаційних сервісів AIC та системи моніторингу ЗНО.

Переваги ЦОД:

- Централізоване управління
- Відмова від сторонніх сервісів
- Високий рівень інформаційної безпеки
- Надійність програмно-апаратного забезпечення
- Надійна система резервного копіювання
- Сучасність інформаційних рішень, що суттєво підвищить ефективність роботи всієї Установи.

Стислий опис предмета закупівлі

До складу апаратної частини ЦОД входять такі системи:

- Апаратний комплекс серверного обладнання

- Системи збереження даних і системи резервного копіювання даних
- Апаратний комплекс мережевого обладнання
- Система енергозабезпечення
- Апаратний комплекс мережевого захисту та інформаційної безпеки

Проєкт ЦОД описує розроблену структуру інформаційної системи Установи та має перелік обладнання, програмного забезпечення і необхідних послуг із впровадження, що включає:

- Серверне шасі
- Сервери
- Систему зберігання даних
- Дискову систему резервного копіювання
- Комутатори ядра
- Комутатори доступу
- Безпроводові точки доступу
- Централізовану система логування подій
- Міжмережеві екрани (NGFW)
- Централізовану систему керування мережевими пристроями безпеки
- Систему захисту поштової системи
- Міжмережевий екран для захисту вебдодатків
- Джерела безперебійного живлення
- Підсистему антивірусного захисту кінцевих точок
- Підсистему управління інформацією та інцидентами інформаційної безпеки
- Шафи для монтажу обладнання
- Ліцензії на програмне забезпечення
- Монтаж та пусконалагоджувальні роботи
- Роботи з налаштування програмного середовища (інтеграції)

Очікуваний ефект від впровадження ЦОД

Проведена закупівля надасть такі можливості використання інформаційного середовища:

- Впровадження відмовостійкої надійної мережевої та серверної інфраструктури, що забезпечує виконання основних функцій Установи – підтримання безпеки судноплавства, функціонування систем NAVTEX, AIC та системи моніторингу ЗНО.

- Коректна побудова та впровадження сучасних інформаційних систем і забезпечення їх необхідними технічними параметрами для стабільного функціонування та виконання своїх прямих завдань з можливістю розширення і збільшення технічних потужностей.
- Впровадження інформаційних систем забезпечення безпеки інформаційних систем Установи, даних, серверів, сервісів і користувачів.
- Забезпечення надійної системи резервного копіювання.
- Впровадження систем централізованого управління, відстеження і контролю за інформаційними системами і сервісами з метою забезпечення безперервного функціонування й адміністрування.
- Консолідація сервісів і даних усіх структурних підрозділів Установи.
- Стандартизація інформаційної системи Установи.

5. Очікувана вартість предмета закупівлі: 59 068 684,48 грн з ПДВ.

6. Обґрунтування очікуваної вартості предмета закупівлі:

Очікувано вартість предмету закупівлі визначено відповідно до примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом №275 від 18.02.2020 міністерства розвитку економіки, торгівлі та сільського господарства України (далі – Методика).

Метод, що застосовано відповідно до Методики: **Метод порівняння ринкових цін**, який передбачає визначення очікуваної вартості на підставі даних ринку, а саме інформації з отриманих цінових пропозицій на момент вивчення ринку.

Згідно із застосованим методом було **направлено запити цінових пропозицій до п’яти учасників ринку**, які **містили інформацію про технічні та якісні характеристики предмета закупівлі**, відображені у тендерній документації до предмета закупівлі, та отримано відповідні комерційні пропозиції. Отримано 4 відповіді з пропозиціями від учасників ринку, на основі яких зроблено прорахунок орієнтовної вартості.

З метою приведення всіх цін, наведених у комерційних пропозиціях, до єдиних умов, аналізуються загальні суми пропозицій, які розглядаються як ціна за одиницю. Отже, обсяг послуг (V) буде дорівнювати 1.

Таким чином очікувана вартість за одиницю становить:

Цод = (Ц1 + Ц2 + Ц3 + Ц4) / К = (59 801 981,00 + 58 970 000,60 + 59 235 756,00 + 58 267 000,30) / 4 = 59 068 684,48.

За результатами застосування методу порівняння ринкових цін, очікувана вартість Послуги становить:

ОВ = Цод х V = 59 068 684,48 х 1 = 59 068 684,48 грн.