ОБҐРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ

(оприлюднюється на виконання постанови КМУ № 710 від 11.10.2016 «Про ефективне використання державних коштів» (зі змінами))

**Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб — підприємців та громадських формувань, його категорія: Держмитслужба м. Київ , вул. Дегтярівська, 11г, ЄДРПОУ 43115923.**

**Вид та ідентифікатор процедури закупівлі:** UA-2024-11-01-008136-a.

1. Предмет закупівлі: (зазначається назва предмета закупівлі та код ДК 021:2015 із застосуванням Єдиного закупівельного словника (див. пункт 2.3 розділу ІІ Порядку організації планування та проведення публічних закупівель в Державній митній службі України)).

Послуги з постачання програмного забезпечення для системи моніторингу інформаційних систем та електронного комунікаційного обладнання та послуги з його впровадження за кодом ДК 021:2015-72260000-5 «Послуги, пов’язані з програмним забезпеченням**»**

2.Обґрунтування доцільності закупівлі (чим зумовлена необхідність закупівлі, мета Постачання програмного забезпечення для системи моніторингу інформаційних систем та електронного комунікаційного обладнання та послуги з його впровадження, код ДК 021:2015-72260000-5 (Послуги, пов’язані з програмним забезпеченням)

Підпунктом 2.4.2. пункту 2.4. «Здійснення інституційних, організаційно-технічних змін у митних органах в частині функціонування ІТ-систем» Портфелю проєктів цифрового розвитку, цифрових трансформацій і цифровізації у митній справі до кінця 2023 року до Стратегічного плану цифрового розвитку, цифрових трансформацій і цифровізації Державної митної служби України, затвердженого наказом Міністерства фінансів України від 15.12.2022 № 435 "Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами" (далі – Портфель проєктів) передбачено проєкт закупівлі ліцензій на програмне забезпечення системи моніторингу інформаційних систем та електронного комунікаційного обладнання. Враховуючи відсутність фінансування протягом 2022-2023 років зазначений підпункт 2.4.2. пункту 2.4 не було виконано.

Основною метою закупівлі програмного забезпечення для системи моніторингу інформаційних систем та електронного комунікаційного обладнання (далі – система Моніторингу) є забезпечення підтримки ефективності, безпеки та стабільності інформаційної інфраструктури ЄАІС.

В результаті впровадження буде отримано сучасну систему Моніторингу, яка являє собою програмне забезпечення, призначене для керування, моніторингу та організації доступу до мережевої інфраструктури Замовника, що призначене для обслуговування та підтримки працездатності інформаційних, аналітичних, комунікаційних автоматизованих систем розгорнутих на серверній та мережевій інфраструктурі Замовника.

Також, наразі в Державній митній службі України впроваджується, за рахунок коштів міжнародної технічної допомоги, система HelpDesk. Інтеграція системи Моніторингу з системою HelpDesk дозволить проактивно виявляти проблеми (інцинденти), аналізувати продуктивність, покращувати комунікацію з користувачами та ефективно управляти ресурсами, що в свою чергу підвищить загальну якість обслуговування техніки та користувачів.

Завдяки моніторингу, інформація про статус ІТ-ресурсів надходить до команди HelpDesk миттєво, що дозволяє швидко усувати несправності, зменшуючи час простою для користувачів.

Система моніторингу надає статистичні дані, які можуть бути використані системою HelpDesk для аналізу частоти та типу інцидентів. Це дозволяє виявляти повторюванні проблеми, що підвищує ефективність обслуговування.

Загалом, інтеграція системи моніторингу з системою HelpDesk значно підвищить ефективність роботи обох систем, забезпечуючи проактивний підхід до управління ІТ-послугами та покращуючи задоволеність користувачів.

Система моніторингу надає можливість виявляти проблеми або аномалії до того, як вони вплинуть на продуктивність. Це дозволяє забезпечити притаманну реакцію та уникнути серйозних негараздів. За допомогою системи моніторингу можна визначити слабкі місця в інфраструктурі та програмному забезпеченні, що сприяє подальшій оптимізації ресурсів та підвищенню продуктивності.

Система моніторингу є важливим інструментом для підтримки ефективності, безпеки та стабільності інформаційної інфраструктури Держмитслужби.

Система моніторингу – це комплекс програмних та апаратних засобів, спрямований на постійне відстеження та контроль за різними аспектами діяльності системи або організації. Вона забезпечує нагляд, аналіз та інформування про роботу апаратного та програмного забезпечення, стан безпеки, продуктивність та доступність ресурсів.

Комплексність інформаційних систем: З огляду на розвиток технологій та збільшення складності ІТ-інфраструктури, система моніторингу стає важливим інструментом для управління та забезпечення безперебійної роботи систем.

Безпека інформації: Зростання кількості кіберзагроз та вразливостей вимагає постійного моніторингу для вчасного виявлення аномалій та захисту від потенційних атак. Наявність системи моніторингу передбачено Технічним завданням на побудову комплексної системи захисту інформації на ЄАІС.

Ефективне використання ресурсів: З метою економії коштів та оптимізації ресурсів, система моніторингу дозволяє визначати та усувати резерви та непотрібні витрати.

Глобалізація та робота в режимі 24/7: З урахуванням необхідності постійної доступності, система моніторингу стає ключовою для уникнення перерв у наданні послуг та ефективного вирішення проблем.

Аналіз та планування: Здатність аналізувати статистичні дані та прогнозувати можливі проблеми робить систему моніторингу інструментом для стратегічного планування та управління.

Усе це підкреслює важливість та актуальність завдання системи моніторингу в сучасному інформаційному середовищі.

3.Обґрунтування обсягів закупівлі (відповідно до чого визначено обсяги закупівлі або підставі чого обраховано).

Обсяги закупівель визначені відповідно до потреб замовника на 2024 рік.

4. Обґрунтування очікуваної вартості закупівлі: 10 142 260,00 грн, вартість послуг сформовано відповідно до примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275, а саме на підставі проведеного аналізу цін на аналогічні за технічними характеристиками послуги шляхом направлення запитів на отримання цінових пропозицій від виробників, офіційних представників та дилерів з постачання програмного забезпечення.

**ТЕХНІЧНІ ВИМОГИ**

1.  **Загальні відомості**

1.1. Предметом закупівлі є послуги з постачання програмного забезпечення для системи моніторингу інформаційних систем та електронного комунікаційного обладнання та послуги з його впровадження (далі - система Моніторингу).

1.2. Всі посилання на конкретну торгівельну марку чи фірму, патент, конструкцію або тип предмета закупівлі, джерело його походження або виробника, слід читати з виразом «або еквівалент».

1.3. Якісні та кількісні характеристики щодо обсягу відповідних послуг визначаються цими Технічними вимогами.

**2.** **Мета впровадження програмного забезпечення системи Моніторингу**

Метою впровадження системи Моніторингу є отримання сучасного та зручного інструменту, який надасть можливість запровадити автоматизацію процесів моніторингу та організацію доступу до мережевої інфраструктури Замовника.

В результаті впровадження буде отримано сучасну систему Моніторингу, яка являє собою програмне забезпечення, призначене для керування, моніторингу та організації доступу до мережевої інфраструктури Замовника, що призначене для обслуговування та підтримки працездатності інформаційних, аналітичних, комунікаційних автоматизованих систем розгорнутих на серверній та мережевій інфраструктурі Замовника згідно з Довгостроковим національним стратегічним планом цифрового розвитку, цифрових трансформацій і цифровізації Державної митної служби України та її територіальних підрозділів на основі Багаторічного стратегічного плану електронної митниці ЄС (Multi-annual strategic plan for electronic customs, MASP-C), затвердженого наказом Міністерства фінансів України
від 09.02.2024 № 63 «Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами».

Додатково від впровадження системи Моніторингу очікується:

підвищення технічної підтримки користувачів автоматизованих систем та відповідних програмно-апаратних комплексів;

підвищення ефективності процесів керування та моніторингу автоматизованих систем та відповідних програмно-апаратних комплексів;

підвищення рівня аналітичної обробки інформації про процеси, які супроводжують обслуговування автоматизованих систем та відповідних програмно-апаратних комплексів;

покращення інформаційного середовища, яке стосується технічних статусів та відповідного рівня керування інформаційно-аналітичних, автоматизованих, телекомунікаційних систем та відповідних програмно-апаратних комплексів.

**3. Вимоги чинного законодавства**

1. Конституція України;
2. Закон України «Про електронну ідентифікацію та електронні довірчі послуги»;
3. Закон України «Про інформацію»;
4. Закон України «Про електронні документи та електронний документообіг»;
5. Закон України «Про доступ до публічної інформації»;
6. Закон України «Про захист персональних даних»;
7. Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
8. Митний кодекс України;
9. Постанова Кабінету Міністрів України від 12 березня 2022 року № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану»;
10. Постанова Кабінету Міністрів України від 08 вересня 2016 року № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів»;
11. Постанова Кабінету Міністрів України від 02 лютого 2024 року № 119 «Деякі питання Національної програми інформатизації»;
12. Постанова Кабінету Міністрів України від 4 лютого 1998 року № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»
13. Розпорядження КМУ «Деякі питання реалізації концептуальних напрямів реформування системи органів, що реалізують державну митну політику»
від 13 травня 2020 р. № 569-р;
14. Довгостроковий національний стратегічний план цифрового розвитку, цифрових трансформацій і цифровізації Державної митної служби України та її територіальних підрозділів на основі Багаторічного стратегічного плану електронної митниці ЄС (Multi-annual strategic plan for electronic customs, MASP-C), затвердженого наказом Міністерства фінансів України від 09.02.2024 № 63 «Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами».

**4. Вимоги до постачання Програмного забезпечення**

Виконавець протягом 40 (сорока) календарних днів з дати укладання Договору передає Замовнику програмне забезпечення системи Моніторингу та здійснює:

* розгортання системи Моніторингу на ресурсах Замовника, початкове налаштування та здійснення оновлення;
* налаштування моніторингу вузлів відомчої комутаційної мережі Держмитслужби з здійсненням моніторингу різних інтерфейсів обладнання (маршрутизаторів/комутаторів) – 200 вузлів;
* налаштування моніторингу обладнання локальної обчислювальної мережі – 30 шт;
* налаштування моніторингу пристроїв WiFi -150 шт;
* налаштування моніторингу мережевого трафіку (NetFlow) на зазначених пристроях;
* налаштування моніторингу поштових серверів – 10 шт;
* налаштування моніторингу серверів додатків та Web-серверів – 10 шт;
* побудови інтерактивної карти мережі з відображенням залежності між пристроями;
* налаштування сигналів тривоги, при збоях в роботі обладнання;
* налаштування звітів по роботі вузлів мережі.

Разом з програмним забезпеченням Виконавець повинен надати Замовнику:

- інструкцію з розгортання та налаштування програмного забезпечення;

- керівництво оператора.

Після впровадження системи Моніторингу Виконавець повинен провести навчання не менше 4-х співробітників Замовника по експлуатації та роботі з програмним забезпеченням.

**5. Функціональні вимоги до Програмного забезпечення**

Програмне забезпечення системи Моніторингу повинно:

5.1. забезпечувати виконання наступних вимог:

* ліцензія має надавати можливість виконувати моніторинг не менше ніж 20000 фізичних пристроїв, додатків та джерел аналізу трафіку;
* мати безагентну архітектуру та вбудований уніфікований інтерфейс без необхідності додавання або встановлення додаткових модулів/функцій/стороннього ПЗ;
* надавати можливість автоматичного та користувальницького присвоєння пристрою головної та другорядних ролей цього пристрою в інфраструктурі і мережі;
* інтерфейс має бути налаштовано українською або англійською мовами.

5.2.забезпечувати оперативний контроль стану обладнання та сервісів, мати графічний інтерфейс і набір інструментів для запису та аналізу подій, що відбуваються в ІТ-інфраструктурі, у тому числі:

1) моніторинг та контроль працездатності, доступності та продуктивності мережевого обладнання різних виробників;

2) моніторинг стану апаратного забезпечення на основі стандарту Redfish, включаючи системи виробництва Cisco, HP, Dell, Lenovo, Supermicro, Fujitsu, IBM та інших;

3) моніторинг та контроль працездатності, доступності та продуктивності серверів, робочих станцій різних виробників;

4) моніторинг та аналіз роботи, запитів, черги на читання / запис для баз даних різних виробників;

5) моніторинг та контроль працездатності, доступності та продуктивності жорстких дисків та систем зберігання даних різних виробників.

6) моніторинг та контроль працездатності, доступності та продуктивності веб-сайтів за сценарієм;

7) моніторинг та контроль працездатності різноманітних сервісів, їхньої доступності та продуктивності;

8) централізоване збирання, зберігання та обробка журналів подій з обладнання та сервісів;

9) підвищення операційної ефективності та прискореної ідентифікації проблем в роботі ІТ-інфраструктури, їх вирішення за допомогою попередньо встановлених і налаштованих панелей моніторингу, вбудованих систем оповіщення та звітності.

10) покращення рівня обслуговування та зменшення простоїв;

11) керування всіма модулями з однієї платформи.

5.3. В ході функціонування:

1) мати можливість автоматично виявляти об’єкти ІТ-інфраструктури;

2) вміти автоматично сканувати мережу, включаючи ідентифікацію мережевих пристроїв, проводити моніторинг критичного обладнання та автоматизувати процеси за допомогою інструментів та планування процесів;

3) має надавати можливість відображення топології мережі L2 та L3 з усіма зазначеними елементами в одному вікні без необхідності перемикання між функціональними панелями:

* фізичні сервери;
* мережеве обладнання (маршрутизатори, комутатори, фаерволи, контролери точок доступу, точки доступу);
* пристрої, що ідентифікуються як кінцеві точки користувача;
* принтери;
* елементи середовища віртуалізації (гіпервізори, віртуальні машини, кластери тощо);
* додатки;
* навантаження на інтерфейси мережевих пристроїв;
* залежності між пристроями та елементами віртуальних середовищ;
* залежності між елементами віртуальних середовищ;
* залежності мiж елементами, що забезпечують роботу WiFi мереж: контролери точок доступу та точки доступу;
* залежності між точками доступу та клієнтами точок доступу;
* зображення у форматах png., jpg., jpeg., svg.;
* текст;
* стан кожного елемента мережі;
* детальна інформація про події у реальному часі із зазначенням пристрою, часу та події, із вказанням ступеня її критичності;

4) надавати можливість використовувати вбудовані шаблони для моніторингу пристроїв Cisco Meraki;

5) надавати можливість автоматично визначати тип, головну роль та другорядні ролі пристрою в інфраструктурі;

6) надавати можливість створювати шаблони для визначення типу, головної ролі та другорядних ролей пристрою з присвоєнням елементів моніторингу, атрибутів, правил сканування та виконання системних задач кожному шаблону;

7) підтримувати гетерогенні мережі та пристрої провідних виробників обладнання;

8) відстежувати продуктивність та наявність мережевого і серверного обладнання.

5.4. підтримувати наступні протоколи та стандарти, але може не обмежуватись ними:

* SNMP-trap;
* SNMP v1/v2/v3;
* SYSLOG;
* ICMP;
* SSH;
* WMI;
* LLDP;
* CDP;
* JDP;
* Windows Event Log;
* NetFlow, jFlow;
* Redfish.

5.5. мати графічний інтерфейс користувача на базі веб-консолі з наступними налаштуваннями:

* високоякісний графічний інтерфейс користувача з асинхронним оновленням;
* можливості налаштування параметрів по додаванню / видаленню секцій веб-сторінок;
* забезпечення доступу користувачу / оператору за допомогою веб-консолі яка повинна:

1) бути доступною як централізовано, так і дистанційно;

2) надавати одночасний вхід декільком користувачам та підтримувати не менше ніж 25 одночасних сесій користувачів без втрати працездатності;

3) швидко виявляти та сповіщати про проблемні додатки, ґрунтуючись на різних властивостях, таких як непрацюючі додатки, додатки з параметрами високого завантаження ЦП, використання пам’яті і т. д.;

4) виявляти та сповіщати про проблемні пристрої, ґрунтуючись на різних властивостях, таких як час відгуку, завантаження процесора, використання пам’яті, високе завантаження інтерфейсу і т. д.;

5) бути доступна через стандартні браузери такі як Chrome, Mozila та Edge;

6) бути простою у використанні та зрозумілою, мати функції деталізації інформації;

7) мати можливість горизонтального масштабування при одночасному вході великої кількості користувачів;

8) мати можливість інтеграції з інструментами моніторингу платформ віртуалізації для автоматичної візуалізації систем, сервісів та додатків з об’єктами зберігання, таких як луни та відповідними об’єктами віртуальної інфраструктури, таким як сховища даних і кластери;

9) надавати можливість користувачу створення панелей моніторингу для різних цілей: продуктивність, планування обчислювальної потужності і т.д.

10) інтегруватися з Active Directory/LDAP, Cisco ACS, OpenID для автентифікації та авторизації користувачів в системі;

11) надавати можливість створення динамічної панелі моніторингу, яка забезпечує детальну видимість і зіставлення різних історичних точок даних в різних частинах інфраструктури. Результат повинен мати можливість бути експортованим в форматі таблиці;

12) забезпечувати єдине уявлення про попередження і події;

13) забезпечувати інтерактивне складання діаграм для вузлів, інтерфейсів, графіків обсягу і т. д.;

14) оперативно виявляти та інформувати про проблемні пристрої;

15) оперативно виявляти та інформувати про проблемні пристрої, ґрунтуючись на різних властивостях, таких як загальний показник IOPS, час затримки, читання та запис;

16) дозволяти створювати панелі моніторингу для користувача і обмежувати уявлення для користувачів на основі додатків, тобто мати рольовий доступ;

17) надавати можливість оператору вирішувати проблем з використанням обчислювальних ресурсів віртуальної машини без переходу в додаткові консолі через інтерфейс системи;

18) надавати уніфіковане уявлення багатоадресної інформації, інформації про маршрут та інформації про пристрій;

19) надавати на одній сторінці уніфіковане уявлення про попередження та події;

20) надавати на одній сторінці уніфіковане уявлення про попередження, пастки, події і повідомлення системного журналу;

21) реєструвати дії і події користувачів в веб-консолі для аудиту з подальшим доступом для оповіщення і звітності.

5.6. мати засоби попереджень про інциденти в роботі обладнання та сервісів, що забезпечить швидке виявлення і надання необхідної інформації для вирішення проблем з продуктивністю за допомогою налаштування і комплексних рекомендацій, а саме можливості:

1) динамічного компонування статистичних даних і автоматичного встановлення порога попередження і критичного порога;

2) надавати оповіщення про можливі проблеми з базою даних за різними категоріями: час очікування, ресурси, адміністративні налаштовані користувачем метрики;

3) відключати попередження під час планового обслуговування;

4) використовувати різні дії, не обмежуючись ними: відправляти повідомлення у SMS, Email; створювати звуковий сигнал; запускати команди у PowerShell, SSH; автоматично робити зупинку, запуск, перезапуск, зняття снепшоту віртуальної машини, автоматично робити зупинку, запуск, перезапуск сервісів;

5) розсилати електронною поштою оповіщення, які вміщують повну інформацію про інцидент;

6) створювати нові попередження не використовуючи існуючи рекомендовані сповіщення, а також мати змогу вносити зміни та налаштовувати порогові значення для вже існуючих сповіщень;

7) створювати оповіщення, враховуючи інформацію про тривалі стани роботи;

8) надавати попередження при виникненні конфлікт IP-адрес на основі MAC-адреси, коли області DHCP збігаються з існуючою IP-адресою, коли є висока завантаженість підмережі і т. д.;

9) надавати інформацію про попередження і події, яка має бути внесена в базу даних для подальшого використання.

10) визначати додаткові параметри та групи параметрів для звуження умов створення попередження для оператора про настання інциденту;

11) керування і відображення подій і попереджень у веб-консолі.

5.7. надавати готові звіти за поточними або історичним статистичними даними про інциденти в роботі обладнання та сервісів, створювати звіти за допомогою веб-консолі та надавати, але не обмежуючись, такі можливості:

1) генерувати статистичні звіти, які можуть бути використані для майбутнього планування і усунення неполадок в роботі;

2) групувати кілька звітів в один комплексний;

3) поміщати діаграми і таблиці в один звіт;

4) розширеного налаштування, надаючи параметри для введення запитів користувача для безпосереднього запиту бази даних;

5) застосовувати велику кількість вбудованих правил для негайного використання і налаштування;

6) застосовувати параметри для імпортування та експортування звітів, створених іншими користувачами;

7) налаштовувати звіти шляхом додавання / видалення стовпців, установки фільтрів, вказівки тимчасових рамок, групування стовпців і т. д.;

8) підтримувати інтеграцію з зовнішніми програми;

9) підтримувати налаштування умов сповіщень з налаштованою областю джерел сповіщень;

10) пересилання повідомлень в систему моніторингу NOC або інші системи;

11) підтримувати різні формати: txt, xlsx, HTML і CSV;

12) дозволяти виконувати відправку по електронній пошті панелей моніторингу, створених в веб-консолі;

13) дозволяти виконувати розсилання звітів за  розкладом: щодня, щотижня, щомісяця;

14) планування звітів для подальшої автоматичної відправки;

15) надавати звіти про управління роботою, що містять інформацію про все обладнання;

16) надавати можливість перегляду вбудованого звіту, що надає інформацію щодо спрогнозованого майбутнього споживання ресурсів кожного пристрою, включаючи навантаження на процесор, використання оперативної пам’яті, заповнення диску, інтерфейс;

17) надавати можливість перегляду вбудованого звіту про встановлене ПЗ на усіх пристроях у мережі. Дані для аналізу стану та роботи обладнання мають збиратися без встановлення агентів на пристроях;

18) надавати можливості керувати конфігураціями мережевих пристроїв, робити копіювання конфігурацій, сповіщати про зміни в конфігурації, проводити їх аудит за допомогою вбудованих шаблонів аудиту для виробника Cisco та надавати можливості для створення користувацьких шаблонів;

19) надавати звіти про встановлене ПЗ на усіх пристроях у мережі без встановлення агентів або іншого стороннього ПЗ на цих пристроях.

20) надавати звіти про оновлення ПЗ на пристроях с ОС сімейства Windows, без встановлення агентів або іншого стороннього ПЗ на цих пристроях.

21) забезпечувати функціонал та можливість використовувати інструменти для зберігання, фільтрування, обробки журналів подій, такі як: Syslogs та WinEvents;

22) надавати параметри для збереження налаштованих звітів з подальшим доступом до них в веб-консолі;

23) надавати шаблони для простого створення звітів про роботу різних баз даних.

5.8. мати можливість групування інформаційних об’єктів та забезпечувати можливості:

1) групувати додатки за типом додатку: веб-додаток, поштовий додаток, додаток для голосової телефонії і т.д.; за виробником: Microsoft, IBM, Dell і т.д;

2) об’єднання учасників у динамічні групи на основі їх атрибутів: виробник, стан пристрою, тип пристрою;

3) визначення залежностей між серверами і додатками задля уникнення зайвих сповіщень;

4) відображення зв’язків між підключеними ресурсами в часі, залежностей між віртуальними об’єктами центру обробки даних, такими як віртуальні машини, хости, сховища даних, кластери і віртуальні додатки;

5) пошук, фільтрація і сортування за зібраними атрибутам конфігурації, виробника, типу обладнання і місцезнаходженням.

5.9. мати можливість будувати топологічні карти різних систем та сервісів з наступними можливостями:

1) побудування топології мережі з усіма можливими елементами мережі на одному зображенні без додаткового встановлення модулів/функцій для подальшої обробки;

2) автоматичне побудування топології мережі на L2 та L3, можливість редагування карти мережі та додавання окремих елементів, таких як план поверху, будівлі;

3) автоматичного підключення пристроїв за допомогою топологічної інформації, зібраної під час автоматичного пошуку за допомогою протоколів CDP(Cisco Discovery Protocol)/LLDP(Link Layer Discovery Protocol) та/або інших;

4) зміни фону, іконок, а також вкладення кількох карт з можливістю деталізації;

5) інтеграції  стану каналів зв’язку між територіально рознесеними точками;

6) відображення місця розташування пристроїв на карті місцевості;

7) відображення стану вузлів або агрегованої групи вузлів;

8) перегляду топології мережі з використанням інформації списку пристроїв у висхідному і низхідному напрямках;

9) надавати відображення стану будь-якої деталі, отриманої за допомогою призначеного для користувача опитування MIB;

10) отримання через карту топології мережі доступу до інформації відносно усіх елементів інфраструктури.

5.10. мати можливість підтримки різних виробників обладнання та сервісів, в тому числі:

1) контролювати різні пристрої зберігання даних: Dell, Dell EMC, NetApp, і т. д.;

2) виявляти додатки та контролювати їх за допомогою вбудованих шаблонів моніторингу, створених на основі кращих рекомендацій і досвіду експлуатації;

3) використовувати вбудовані шаблони додатків та мати можливість редагувати їх;

4) створювати користувацькі шаблони додатків, із можливістю додавання до шаблону окремих елементів, таких як: збір метрик через SNMP, WMI, Windows Performance Counters; перевірка працездатності сервісу та процесу; запуск користувацьких команд в SSH та PowerShell; перевірка роботи порту; збір значень за допомогою Rest API.

5) виявлені пристрої повинні бути визначені як пристрої певного виробника і класифіковані автоматично;

5.11. мати можливість розширення функціоналу, для чого повинно:

1) мати API, доступний для програмного імпорту / експорту вузлів і виконання аналогічних функцій;

2) мати можливість отримувати властивості з пристроїв без необхідності імпорту MIB пристроїв в базу даних MIB;

3) мати можливість отримання інформації про події у віртуальному середовищі через vSphere API

4) надавати можливість інтеграції з іншим ПЗ за допомогою таких методів Rest API як: GET/POST/PUT/PATCH/DELETE;

5) дозволяти користувачам налаштовувати метрики, попередження та звіти для розширення стандартних можливостей;

6) отримувати в реальному часі значення, діаграми, а також оповіщення по цим налаштованим властивостями;

7) мати можливість пошуку всіх кінцевих точок в підмережі;

8) дозволяти користувачу використовувати сценарії для розширення можливостей управління додатками;

9) збирати інформацію про класифікацію даних з різних пристроїв, які не підтримуються за замовчуванням;

10) збирати властивості з пристроїв, що підтримують SNMP, шляхом вказівки OID характеристик.

5.12. мати засоби моніторингу продуктивності обладнання, систем та сервісів з наступними вимогами:

1) забезпечувати можливість надавати інформацію моніторингу трафіку відповідно до політик QoS

2) мати можливість відображення агрегованих метрик для кожного додатка / вузла;

3) забезпечувати інформацію щодо виконання SLA для додатків та IP-телефонії

5.13. забезпечувати інтеграції з інфраструктурою, для чого мати можливості:

1) інтегруватися з програмним забезпеченням для моніторингу платформ віртуалізації для забезпечення детального уявлення продуктивності додатків від додатка до віртуальної машини і до хоста;

2) управління журналами та безпосередньо інтегруватися з рішенням для  моніторингу мережевої інфраструктури і відображати дані журналів поряд з продуктивністю мережі і систем на одній панелі моніторингу;

3) інтеграції з сервіс-деск системою IVANTI Neurons for ITSM (Ivanti Service Management) яка використовується Замовником, з можливістю автоматичного створення інцидентів і двобічної синхронізації підтвердження інцидентів;

4) інтеграції з інструментами, які призначено моніторингу режимів роботи всіх компоненті ІТ-інфраструктури (мережа передавання даних, системи, сервіси, додатки, бази даних, віртуалізація, системи зберігання даних, різни портали) та забезпечувати перегляд всіх даних з одного вікна;

5) забезпечувати динамічну панель моніторингу, яка детально відображає час очікування, метрики бази даних і зіставляє різні історичні точки даних в різних частинах інфраструктури;

6) експорту результатів в форматі таблиці;

7) інтегруватися з програмним забезпеченням моніторингу віртуалізації для забезпечення наскрізного уявлення про продуктивність комплексного додатка: від додатка до віртуальної машини і до хоста;

8) інтеграцію зі сторонніми додатками на рівні користувача інтерфейсу за допомогою обміну повідомленнями та API;

9) підтримувати інтеграцію з Active Directory/LDAP для розмежування доступу до консолі.

10) надавати можливість відображати події у віртуальному середовищі за допомогою vSphere API.

11) автоматизація відстеження записів DNS віртуальної машини.

12) спрощення управління IP-адресами віртуальних машин;

13) автоматизація виявлення IP-адрес віртуальних машин;

5.14. розгортатись з урахуванням наступних вимог:

1) мати активну панель моніторингу, що забезпечує самостійну перевірку платформи моніторингу і відображення рекомендацій щодо виправлення невідповідних елементів;

2) підтримувати безагентне розгортання;

3) підтримувати централізоване оновлення всіх віддалених компонентів (наприклад, віддалених збирачів даних, веб-консолей) без додаткового управління на віддалених серверах;

4) надавати підтримку розгортання системи на усіх нижчезазначених версіях операційних систем:

* Microsoft Windows Server 2019;
* Microsoft Windows Server 2016;

5) пітримувати розгортання на таких базах данних:

* Microsoft SQL Server 2016 Standard or Enterprise;
* Microsoft SQL Server 2017 Standard or Enterprise;
* Microsoft SQL Server 2019 Standard or Enterprise;

6) надавати можливість використовувати для зберігання даних  Microsoft  SQL Server Express і має бути вбудованим у перелік складових системи моніторингу.

4.15. отримувати оновлення та підтримку, в тому числі:

1) повідомляти в веб-консолі про наявність нових версій;

2) надавати нові функції не менш ніж раз в рік або частіше.

5.16. забезпечувати моніторинг мережевої інфраструктури з урахуванням наступних вимог:

1) виявляти несправності мережевих шляхів для конкретного TCP-зв’язку як в локальному, так і в хмарному середовищі;

2) опитувати устаткування з використанням SNMP v1, v2, v3, WMI та SSH;

3) визначати параметри для автоматизації та планування процесу виявлення;

4) встановлювати параметри для налаштування інтервалів опитування за необхідністю;

5) визначати параметри для визначення доступності пристрою, використовуючи тільки SNMP;

6) використовувати отримані відомості для створення топологічних карт;

7) відслідковувати стан обладнання популярних постачальників, таких як Cisco, DELL, HP і т. д., а також надавати оповіщення та звіти з моніторингу стану обладнання;

8) відображати в веб-консолі повідомлення про виявлення нових пристроїв в мережі;

9) відображати дані в реальному часі;

10) відображати різними кольорами статус пристрою і статус інтерфейсу для відображення попередження і критичного стану;

11) відображати статистичні дані:

* пропускна здатність інтерфейсу;
* поточний трафік (біт/с);
* загальна кількість прийнятих / відправлених байтів;

12) дозволяти фільтрацію інтерфейсів за результатами виявлення для виключення віртуальних інтерфейсів і портів доступу, а також вибору інтерфейсів на основі зіставлення шаблонів;

13) надавати підтримку в моніторингу інформації щодо багатоадресного трафіку, попередженнях, топології, багатоадресної передачі, маршрутах, багатоадресних помилках і т. д.;

14) не повинно додавати пристрої з декількома IP-адресами в якості дублюючих вузлів, але повинно надавати список всіх відомих IP-адрес для вузла;

15) виявляти мережі.

16) отримувати дані від:

* маршрутизаторів;
* комутаторів;
* міжмережевих екранів;
* бездротових пристроїв;
* серверів;
* інших пристроїв з підтримкою SNMP;

17) забезпечувати автоматичне виявлення пристроїв в мережі з можливостями SNMP і ICMP:

* діапазони IP-адрес;
* підмережі;
* окремі IP-адреси.

18) надавати можливість виступати сервером Syslog в мережі, що забезпечить відсутність необхідності встановлення додаткового такого серверу для збору Syslogs з мережевих пристроїв.

**6. Загальні вимоги до технічної підтримки**

1. Термін технічної підтримки програмного забезпечення, що поставляється за Договором складає не менше ніж 36 місяців від дати підписання Акту приймання-передачі послуг відповідно до умов договору.
2. Надання консультацій телефоном та електронною поштою з питань налаштування та експлуатації обладнання в робочі дні з 9.00 до 18.00 години. Послуги даного типу (консультації) являють собою рекомендації та/або відповіді на запитання Замовника стосовно особливостей налагодження, адміністрування Програмного забезпечення.
3. Реагування на запити на обслуговування протягом 1-єї години з моменту отримання запиту на обслуговування.
4. Постійний доступ до Центру технічної підтримки виробника програмного забезпечення, що працює в режимі: 24х7х365 (цілодобово (00:00-24:00) з понеділка по неділю включно, 365 днів на рік з можливістю звернення по телефону, через веб-сайт або електронну пошту (e-mail).
5. Учасник повинен надати Замовнику перелік телефонів, веб-сайт або електронну пошту (e-mail) Центру технічної підтримки виробника Програмного забезпечення протягом 3-х календарних днів з моменту підписання Договору.
6. Доступ до закритої частини сайту виробника і онлайн бази знань виробника з технічною інформацією та корисними інструментами.
7. Надання Замовнику основних та перехідних версій програмного забезпечення Виробника за допомогою веб-сайту виробника.
8. Надання рекомендацій по налаштуванню політик, що застосовуються в роботі програмного забезпечення. Надання допомоги у пошуку рішень відомих проблем в базі знань виробника програмного забезпечення та в інших джерелах.