6.2

Виконуючому обов'язки директора Спеціалізованого комунального підприємства «Київтелесервіс» Волощуку Олександру Олександровичу

Начальника відділу інформаційної безпеки Стревалюка Антона Сергійовича

С Л У Ж Б О В А З А П И С К А

місто Київ «18» березня 2025 року

Конкретна назва предмета закупівлі – Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури; 48730000-4 – Пакети програмного забезпечення для забезпечення безпеки за ДК 021:2015 Єдиного закупівельного словника

Обґрунтування доцільності закупівлі:

6.2 «Створення, розвиток та модернізація мережевої інфраструктури, сервісної мережевої інфраструктури, платформи Інтернету речей (IoT), мереж доступу, радіомереж, системи отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку» переліку завдань і заходів Комплексної міської цільової програми «Цифровий Київ» 2024-2027 роки» (у редакції від 12 грудня 2024 року № 449/10257), згідно із зверненням КП "Інформатика" № 075/3-410 від 12.02.2025.

Обґрунтування обсягів закупівлі:

З метою забезпечення коректної працездатності, забезпечення доступу до оновлень програмного забезпечення, сигнатур та підтримки виробником систем міської мережевої інфраструктури, для забезпечення захисту міської мережевої інфраструктури має бути передбачено постачання програмної продукції (придбання ліцензійного програмного забезпечення з доступом до оновлень та підтримки з боку виробника) для підсистем безпеки міської мережевої інфраструктури.

Обґрунтування якісних характеристик закупівлі:

З метою забезпечення коректної працездатності, забезпечення доступу до оновлень програмного забезпечення, сигнатур та підтримки виробником зазначених нижче систем міської мережевої інфраструктури, для забезпечення захисту міської мережевої інфраструктури має бути передбачено постачання програмної продукції (оновлення ПЗ, подовження терміну дії ПЗ та підтримки виробником) для підсистем захисту міської мережевої інфраструктури.

Існуюча система захисту міської мережевої інфраструктури у своєму складі має наступні системи виробництва компанії Fortinet:

1. Мережевий екран FortiGate FG-1000D.
2. Мережевий екран FortiGate FG-3000D.
3. Мережевий екран FortiGate FG-200F.
4. Мережевий екран FortiGate FG-80F.
5. Мережевий екран FortiGate FG-40F.
6. Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E.
7. Система керування FortiManager FMG-VM with 450 device license.
8. Віртуальний пристрій FortiAuthenticator-VM with 1100 user license.
9. Система захисту FortiSandbox-VM.

10. Система захисту FortiMail-VM.
11. Система захисту Web Application Firewall.
12. Система FAD-100F Application Delivery Controller.
13. Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G
14. Віртуальний пристрій FortiEMS-VM with 500 user license.

Технічні вимоги до предмета закупівлі рекомендовані протоколом № 20 від 14 березня 2025 року засідання робочої групи з розробки та погодження технічних вимог до закупівель, робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024 – 2027 роки.

Очікувана вартість предмета закупівлі, згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, становить 25 157 884 грн. 18 коп. (двадцять п'ять мільйонів сто п'ятдесят сім тисяч вісімсот вісімдесят чотири грн. 18 коп.) з ПДВ, є середньоарифметичним значенням отриманих комерційних пропозицій і не перевищує розмір бюджетного призначення.

Розмір бюджетного призначення визначено паспортом бюджетної програми на 2025 рік відповідно до заходів Комплексної міської цільової програми «Цифровий Київ» на 2024 – 2027 роки.

Джерело фінансування закупівлі – місцевий бюджет, КЕКВ 2610 Субсидії та поточні трансферти підприємствам (установам, організаціям).

Процедура закупівлі – відкриті торги.

Вид предмету закупівлі – товар.

Кількість товарів – 474 (чотириста сімдесят чотири) штуки.

Місце поставки товарів – 03113, Україна, Київська область, місто Київ, вулиця Дегтярівська, будинок 37 (ЦОД КМДА).

Строк поставки товарів – до 18 квітня 2025 року.

Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги)
2. Додаток 2. Кваліфікаційні критерії до учасників
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін).

Ініціатор закупівлі **А. С. Стревалюк**

«ПОГОДЖЕНО»:

Начальник відділу -
Головний бухгалтер **Г. А. Букша**

Заступник начальника відділу з
економічних питань **Ю.В.Волочаєва**

Заступник директора з юридичних питань **О. Є. Юрко**

Заступник директора з технічних питань **О.Ф. Поліщук**

Засідання в онлайн режимі
із використанням Microsoft
Teams

ПРОТОКОЛ № 20

засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки

м. Київ «14» березня 2025 року

ПРИСУТНІ:

Члени робочої групи:
О. Грекалов
В. Жучков
М. Клюєва
С. Осіпов
О. Поліщук
Т. Самойленко
Д. Цвігун

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257) (далі – Програма), у 2025 році, а саме:

1.1 проєкт технічних вимог до закупівлі «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури» (пункт 6.2 «Створення, розвиток та модернізація мережевої інфраструктури, сервісної мережевої інфраструктури, платформи Інтернету речей (IoT), мереж доступу, радіомереж, системи отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку» переліку завдань і заходів Програми);

1.2 проєкт технічних вимог до закупівлі «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури» (пункт 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Програми).

2. Різне.

По пунктах 1.1 – 1.2 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував, що для підтримки працездатності та захисту міської мережевої інфраструктури, зокрема обладнання компанії Fortinet, необхідно забезпечити доступ до оновлень та сигнатур відповідного програмного забезпечення, подовження терміну його дії, підтримки виробником підсистем захисту міської мережевої інфраструктури тощо та представив проєкти технічних вимог «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури» (пункт 6.2 переліку завдань і заходів Програми) та «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні проєктів технічних вимог брали участь: Д. Цвігун, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури» (пункт 6.2 переліку завдань і заходів Програми) та «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури» (пункт 6.5 переліку завдань і заходів Програми), використовувати проєкти технічних вимог, розглянуті на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 7, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-614 **Дата реєстрації** 14.03.2025
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 14.03.2025 (Протокол № 20 від 14.03.2025)

Кількість файлів: 3 **Кількість ЕП:** 21

ДОКУМЕНТ СЕД АСКОД ГТС СПК

Департамент інформаційно-комунікаційних технологій
14.03.2025 № 075-614

Перелік електронних підписів

ПІБ	Дати і час накладення ЕП	Погодження	Час останнього накладення ЕП
Жучков Василь Анатолійович **Кількість ЕП:** 3	17.03.2025 11:04:08 ; 17.03.2025 11:04:10 ; 17.03.2025 11:04:11 ;	17.03.2025 11:04:11 Погодив;	17.03.2025 11:04:11 Погодив
КЛЮСВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 3	17.03.2025 10:57:05 ; 17.03.2025 10:57:06 ; 17.03.2025 10:57:09 ;	17.03.2025 10:57:09 Погодив;	17.03.2025 10:57:09 Погодив
Грекалов Олександр Сергійович **Кількість ЕП:** 3	17.03.2025 10:38:23 ; 17.03.2025 10:38:25 ; 17.03.2025 10:38:26 ;	17.03.2025 10:38:26 Погодив;	17.03.2025 10:38:26 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 3	14.03.2025 15:39:42 ; 14.03.2025 15:39:43 ; 14.03.2025 15:39:44 ;	14.03.2025 15:39:44 Погодив;	14.03.2025 15:39:44 Погодив
Поліщук Олег Федорович **Кількість ЕП:** 3	14.03.2025 14:09:25 ; 14.03.2025 14:09:26 ; 14.03.2025 14:09:27 ;	14.03.2025 14:09:27 Погодив;	14.03.2025 14:09:27 Погодив

Самойленко Тамара Анатоліївна **Кількість ЕП:** 3	14.03.2025 14:06:19 ; 14.03.2025 14:06:20 ; 14.03.2025 14:06:21 ;	14.03.2025 14:06:21 Погодив;	14.03.2025 14:06:21 Погодив
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 3	14.03.2025 14:05:55 ; 14.03.2025 14:05:56 ; 14.03.2025 14:05:58 ;	14.03.2025 14:05:58 Погодив;	14.03.2025 14:05:58 Погодив

ТЕХНІЧНІ ВИМОГИ

Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури; 48730000-4 – Пакети програмного забезпечення для забезпечення безпеки за ДК 021:2015 Єдиного закупівельного словника

На виконання пункту 6.2 «Створення, розвиток та модернізація мережевої інфраструктури, сервісної мережевої інфраструктури, платформи Інтернету речей (IoT), мереж доступу, радіомереж, системи отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку» переліку завдань та заходів в Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257).

1. Загальні відомості про зміст робіт:

1.1. Повне найменування об'єкта інформатизації

Міська мережева інфраструктура, у складі якої наявне обладнання виробника Fortinet.

1.2. Найменування сторін:

- Замовник – СКП «Київтелесервіс»;
- Виконавець – визначається за результатом проведення закупівлі послуг відповідно до вимог законодавства України у сфері публічних закупівель.

1.3. Перелік документів, які мають враховуватись під час розробки.

- Закон України «Про Національну програму інформатизації»;
- Постанова Кабінету Міністрів України від 21.02.2025 №205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації»;
- Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Постанови Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

2. Призначення та цілі інформатизації:

2.1. Призначення

- Забезпечення доступу обладнання Fortinet до оновлення сигнатур та компонентів системи захисту;
- Забезпечення доступа до оновлення мікрокодів обладнання Fortinet;
- Забезпечення підтримки від виробника для обладнання Fortinet.

2.2. Цілі інформатизації

Забезпечення належного рівня захисту від інформаційних загроз систем міської мережевої інфраструктури, шляхом доступу до оновлень компонентів системи захисту на обладнанні Fortinet.

3. Характеристики об'єкта інформатизації

3.1. Мережевий екран FortiGate FG-1000D.

- Забезпечує комплексний контроль доступу до мережевих ресурсів із глибоким аналізом трафіку.
- Виявляє та блокує кібератаки, включаючи експлойти, шкідливе програмне забезпечення та аномальну активність.
- Інтегрована система захисту від загроз із можливістю гнучкого налаштування політик безпеки.
- Підтримує сегментацію мережі, що дозволяє ізолювати критичні ресурси.
- Вбудована підтримка VPN-технологій для безпечного доступу віддалених користувачів.
- Автоматизоване оновлення сигнатур загроз та політик безпеки.
- Використовує аналіз поведінки для виявлення аномалій у трафіку та адаптації політик безпеки.
- Вбудована інтеграція з іншими системами кібербезпеки для підвищення рівня захисту.
- Оптимізований для роботи в середовищах із високим навантаженням і критичними сервісами.
- Підтримує шифрування трафіку та глибоку інспекцію пакетів без втрати продуктивності.

3.2. Мережевий екран FortiGate FG-3000D.

- Забезпечує комплексний контроль доступу до мережевих ресурсів із глибоким аналізом трафіку.
- Виявляє та блокує кібератаки, включаючи експлойти, шкідливе програмне забезпечення та аномальну активність.
- Інтегрована система захисту від загроз із можливістю гнучкого налаштування політик безпеки.
- Підтримує сегментацію мережі, що дозволяє ізолювати критичні ресурси.
- Вбудована підтримка VPN-технологій для безпечного доступу віддалених користувачів.
- Автоматизоване оновлення сигнатур загроз та політик безпеки.
- Використовує аналіз поведінки для виявлення аномалій у трафіку та адаптації політик безпеки.
- Вбудована інтеграція з іншими системами кібербезпеки для підвищення рівня захисту.
- Оптимізований для роботи в середовищах із високим навантаженням і критичними сервісами.
- Підтримує шифрування трафіку та глибоку інспекцію пакетів без втрати продуктивності.

3.3. Мережевий екран FortiGate FG-200F.

- Забезпечує комплексний контроль доступу до мережевих ресурсів із глибоким аналізом трафіку.
- Виявляє та блокує кібератаки, включаючи експлойти, шкідливе програмне забезпечення та аномальну активність.
- Інтегрована система захисту від загроз із можливістю гнучкого налаштування політик безпеки.
- Підтримує сегментацію мережі, що дозволяє ізолювати критичні ресурси.
- Вбудована підтримка VPN-технологій для безпечного доступу віддалених користувачів.
- Автоматизоване оновлення сигнатур загроз та політик безпеки.
- Вбудована інтеграція з іншими системами кібербезпеки для підвищення рівня захисту.
- Підтримує шифрування трафіку та глибоку інспекцію пакетів без втрати продуктивності.

3.4. Мережевий екран FortiGate FG-80F.

- Забезпечує комплексний контроль доступу до мережевих ресурсів із глибоким аналізом трафіку.
- Виявляє та блокує кібератаки, включаючи експлойти, шкідливе програмне забезпечення та аномальну активність.
- Інтегрована система захисту від загроз із можливістю гнучкого налаштування політик безпеки.
- Підтримує сегментацію мережі, що дозволяє ізолювати критичні ресурси.
- Вбудована підтримка VPN-технологій для безпечного доступу віддалених користувачів.
- Автоматизоване оновлення сигнатур загроз та політик безпеки.
- Вбудована інтеграція з іншими системами кібербезпеки для підвищення рівня захисту.
- Підтримує шифрування трафіку та глибоку інспекцію пакетів без втрати продуктивності.

3.5. Мережевий екран FortiGate FG-40F.

- Забезпечує комплексний контроль доступу до мережевих ресурсів із глибоким аналізом трафіку.
- Виявляє та блокує кібератаки, включаючи експлойти, шкідливе програмне забезпечення та аномальну активність.
- Інтегрована система захисту від загроз із можливістю гнучкого налаштування політик безпеки.
- Підтримує сегментацію мережі, що дозволяє ізолювати критичні ресурси.
- Вбудована підтримка VPN-технологій для безпечного доступу віддалених користувачів.

- Автоматизоване оновлення сигнатур загроз та політик безпеки.
- Вбудована інтеграція з іншими системами кібербезпеки для підвищення рівня захисту.
- Підтримує шифрування трафіку та глибоку інспекцію пакетів без втрати продуктивності.

3.6. **Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E.**

- Централізований збір і аналіз логів для моніторингу подій у мережі.
- Автоматичне корелювання загроз для виявлення складних атак.
- Створення детальних звітів щодо активності мережі та потенційних ризиків.
- Візуалізація мережевих подій у реальному часі для швидкого прийняття рішень.
- Підтримка інтеграції з іншими системами Fortinet для глибшого аналізу даних.

3.7. Система керування FortiManager FMG-VM with 450 device license.

- Централізоване управління політиками безпеки для великої кількості пристроїв Fortinet.
- Масштабована архітектура, що дозволяє керувати розподіленими мережами.
- Автоматизоване оновлення конфігурацій та політик без необхідності ручного втручання.
- Контроль змін у налаштуваннях та резервне копіювання конфігурацій.
- Виявлення та усунення помилок у налаштуваннях безпеки.

3.8. Віртуальний пристрій FortiAuthenticator-VM with 1100 user license.

- Автентифікація користувачів із використанням багатофакторного доступу (2FA).
- Централізоване управління обліковими записами та доступами до мережевих ресурсів.
- Інтеграція з Microsoft Active Directory та іншими ідентифікаційними системами.
- Контроль рівня доступу користувачів відповідно до їхніх ролей у компанії.
- Захист критичних систем від несанкціонованого доступу.

3.9. Система захисту FortiSandbox-VM.

- Виявлення невідомих загроз через аналіз поведінки файлів у віртуальному середовищі.
- Автоматичне блокування шкідливих файлів перед їхнім потраплянням у мережу.
- Інтеграція з міжмережевими екранами Fortinet для миттєвого реагування на загрози.
- Виявлення атак нульового дня через емуляцію виконання коду.
- Генерація звітів щодо виявлених загроз із детальним аналізом їхньої поведінки.

3.10. Система захисту FortiMail-VM.

- Захист електронної пошти від фішингових атак, спаму та шкідливих вкладень.
- Аналіз загроз у реальному часі з використанням глобальних баз загроз FortiGuard.
- Багаторівневий контроль вхідних і вихідних повідомлень для запобігання витоку даних.
- Вбудована система автентифікації відправників для мінімізації ризику підроблених листів.

- Інтеграція з іншими системами Fortinet для комплексного захисту електронної пошти.

3.11. Система захисту Fortinet FortiWeb-VM.

- Контроль трафіку веб-додатків для запобігання SQL-ін'єкціям, XSS-атакам та експлойтам.
- Захист API-інтерфейсів від автоматизованих атак та несанкціонованого доступу.
- Вбудований механізм машинного навчання для адаптації до нових загроз.
- Підтримка аналізу поведінки користувачів для виявлення підозрілої активності.
- Гнучкі політики блокування трафіку залежно від рівня загрози.

3.12. Система FAD-100F Application Delivery Controller.

- Оптимізація продуктивності веб-додатків шляхом балансування навантаження.
- Автоматичне перенаправлення трафіку на доступні сервери у разі перевантаження.
- Шифрування з'єднань для підвищення безпеки передавання даних.
- Контроль продуктивності додатків та мінімізація затримок у роботі сервісів.
- Інтеграція з Fortinet Security Fabric для комплексного контролю трафіку.

3.13. Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G

- Глибока аналітика мережевого трафіку для виявлення складних атак.
- Масштабованість для підтримки великих обсягів логів та швидкої обробки даних.
- Інтелектуальний аналіз інцидентів із автоматичним створенням кореляцій.
- Контроль ефективності політик безпеки та їхньої оптимізації.

3.14. **Віртуальний пристрій FortiEMS-VM with 500 user license.**

- Централізоване управління безпекою кінцевих пристроїв.
- Контроль відповідності пристроїв корпоративним політикам безпеки.
- Автоматичне виявлення та ізоляція заражених пристроїв.
- Моніторинг дій користувачів для запобігання витоку даних.

4. Вимоги до засобу інформатизації:

4.1. Вимоги до структури та функціонування засобу інформатизації Мережевий екран FortiGate FG-1000D

Таблиця 1

№ п/п	Найменування	Од. вимір у	Кіль - кість	Термін підтримки
1	**Мережевий екран FortiGate FG-1000D** **Примірник програмної продукції для Мережевого екрану FortiGate FG-1000D :**	шт.	2	не менш ніж 12 міс.

	FortiGate-1000D 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) або еквівалент		

Програмна продукція для існуючого мережевого екрану, що складається з двох підсистем FortiGate FG-1000D, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 1 та забезпечувати наступне:

- Отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та інших оновлень для сервісів безпеки.
- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Підтримка функцій мережевого екрану, а саме, контролю додатків, запобігання вторгненням, антивірусу, веб-фільтрації, антиспаму.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.1.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.1.2. Вимоги до безпеки

- Не застосовуються.

4.1.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.1.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.1.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: IPSec, TLS, DNSSEC.

4.1.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Висока продуктивність із підтримкою кластеризації для балансування навантаження.
- Автоматичне збереження резервних копій налаштувань та швидке їх відновлення.
- Захист від зовнішніх атак із мінімізацією впливу на критичні сервіси.
- Підтримка механізмів гарячого резервування (HA) для безперервної роботи.
- Контроль доступу на рівні адміністрування для запобігання несанкціонованим змінам.

4.1.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.1.8. Вимоги до режимів функціонування засобу інформатизації

- Режими роботи: моніторинг, навчання, активне блокування.
- Адаптивне керування політиками безпеки та автоматична зміна конфігурації відповідно до загроз.

4.1.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Глибокий аналіз трафіку з підтримкою сигнатурного та поведінкового виявлення загроз.
- Автоматичне оновлення баз загроз і політик безпеки.
- Централізоване логування всіх подій безпеки з можливістю інтеграції з SIEM.
- Підтримка VPN-тунелів для захищеного віддаленого доступу.
- Розширений захист від складних багатовекторних атак на рівнях L3, L4 та L7.
- Вбудована система запобігання вторгненням (IPS) з можливістю адаптивного аналізу загроз.
- Інтелектуальна система аналізу поведінки користувачів і мережевого трафіку.
- Автоматизоване реагування на аномальні події та підозрілу активність.
- Підтримка високої продуктивності з мінімальним впливом на швидкість мережі.

4.2. Вимоги до структури та функціонування засобу інформатизації Мережевий екран FortiGate FG-3000D

Таблиця 2

№ п/п	Найменування	Од. вимір у	Кіль-кість	Термін підтримки
1	**Мережевий екран FortiGate FG-3000D** **Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D :** FortiGate-3000D 1 Year FortiCare Premium Support або еквівалент	шт.	2	не менш ніж 12 міс.

Програмна продукція для існуючого мережевого екрану, що складається з двох підсистем FortiGate FG-3000D, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 2 та забезпечувати наступне:

- Отримання основних та проміжних релізів ПЗ через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.2.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.2.2. Вимоги до безпеки

- Не застосовуються.

4.2.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.2.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.2.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: IPSec, TLS, DNSSEC.

4.2.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Висока продуктивність із підтримкою кластеризації для балансування навантаження.
- Автоматичне збереження резервних копій налаштувань та швидке їх відновлення.
- Захист від зовнішніх атак із мінімізацією впливу на критичні сервіси.
- Підтримка механізмів гарячого резервування (HA) для безперервної роботи.
- Контроль доступу на рівні адміністрування для запобігання несанкціонованим змінам.

4.2.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.2.8. Вимоги до режимів функціонування засобу інформатизації

- Режими роботи: моніторинг, навчання, активне блокування.
- Адаптивне керування політиками безпеки та автоматична зміна конфігурації відповідно до загроз.

4.2.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Глибокий аналіз трафіку з підтримкою сигнатурного та поведінкового виявлення загроз.
- Автоматичне оновлення баз загроз і політик безпеки.
- Централізоване логування всіх подій безпеки з можливістю інтеграції з SIEM.
- Підтримка VPN-тунелів для захищеного віддаленого доступу.
- Розширений захист від складних багатовекторних атак на рівнях L3, L4 та L7.
- Вбудована система запобігання вторгненням (IPS) з можливістю адаптивного аналізу загроз.
- Інтелектуальна система аналізу поведінки користувачів і мережевого трафіку.
- Автоматизоване реагування на аномальні події та підозрілу активність.
- Підтримка високої продуктивності з мінімальним впливом на швидкість мережі.

4.3. Вимоги до структури та функціонування засобу інформатизації Мережевий екран FortiGate FG-200F

Таблиця 3

№ п/п	Найменування	Од. вимір у	Кіль-кість	Термін підтримки
1	**Мережевий екран FortiGate FG-200F** **Примірник програмної продукції для Мережевого екрану FortiGate FG-200F:** FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) або еквівалент	шт.	2	не менш ніж 12 міс.

Програмна продукція для існуючого мережевого екрану, що складається з двох підсистем FortiGate FG-200F, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 3 та забезпечувати наступне:

- Отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та інших оновлень для сервісів безпеки.
- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Підтримка функцій мережевого екрану, а саме, контролю додатків, запобігання вторгненням, антивірусу, веб-фільтрації, антиспаму.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.3.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.3.2. Вимоги до безпеки

- Не застосовуються.

4.3.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.3.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.3.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.

- Сумісність із загальноприйнятими протоколами безпеки: IPSec, TLS, DNSSEC.

4.3.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Висока продуктивність із підтримкою кластеризації для балансування навантаження.
- Автоматичне збереження резервних копій налаштувань та швидке їх відновлення.
- Захист від зовнішніх атак із мінімізацією впливу на критичні сервіси.
- Підтримка механізмів гарячого резервування (HA) для безперервної роботи.
- Контроль доступу на рівні адміністрування для запобігання несанкціонованим змінам.

4.3.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.3.8. Вимоги до режимів функціонування засобу інформатизації

- Режими роботи: моніторинг, навчання, активне блокування.
- Адаптивне керування політиками безпеки та автоматична зміна конфігурації відповідно до загроз.

4.3.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Глибокий аналіз трафіку з підтримкою сигнатурного та поведінкового виявлення загроз.
- Автоматичне оновлення баз загроз і політик безпеки.
- Централізоване логування всіх подій безпеки з можливістю інтеграції з SIEM.
- Підтримка VPN-тунелів для захищеного віддаленого доступу.
- Розширений захист від складних багатовекторних атак на рівнях L3, L4 та L7.
- Вбудована система запобігання вторгненням (IPS) з можливістю адаптивного аналізу загроз.
- Інтелектуальна система аналізу поведінки користувачів і мережевого трафіку.
- Автоматизоване реагування на аномальні події та підозрілу активність.
- Підтримка високої продуктивності з мінімальним впливом на швидкість мережі.

4.4. Вимоги до структури та функціонування засобу інформатизації Мережевий екран FortiGate FG-80F

Таблиця 4

№ п/п	Найменування	Од. вимір у	Кіль-кість	Термін підтримки
	Мережевий екран FortiGate FG-80F			
1	**Примірник програмної продукції для Мережевого екрану FortiGate FG-80F :** FortiGate-80F 1 Year FortiCare Essential Support	шт.	20	не менш ніж 12 міс.

або еквівалент

Програмна продукція для існуючого мережевого екрану, що складається з двадцяти (20) підсистем FortiGate FG-80F, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 4 та забезпечувати наступне:

- Отримання основних та проміжних релізів ПЗ через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.4.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.4.2. Вимоги до безпеки

- Не застосовуються.

4.4.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.4.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.4.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: IPSec, TLS, DNSSEC.

4.4.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Висока продуктивність із підтримкою кластеризації для балансування навантаження.
- Автоматичне збереження резервних копій налаштувань та швидке їх відновлення.
- Захист від зовнішніх атак із мінімізацією впливу на критичні сервіси.
- Підтримка механізмів гарячого резервування (HA) для безперервної роботи.
- Контроль доступу на рівні адміністрування для запобігання несанкціонованим змінам.

4.4.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.4.8. Вимоги до режимів функціонування засобу інформатизації

- Режими роботи: моніторинг, навчання, активне блокування.
- Адаптивне керування політиками безпеки та автоматична зміна конфігурації відповідно до загроз.

4.4.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Глибокий аналіз трафіку з підтримкою сигнатурного та поведінкового виявлення загроз.
- Автоматичне оновлення баз загроз і політик безпеки.
- Централізоване логування всіх подій безпеки з можливістю інтеграції з SIEM.

- Підтримка VPN-тунелів для захищеного віддаленого доступу.
- Розширений захист від складних багатовекторних атак на рівнях L3, L4 та L7.
- Вбудована система запобігання вторгненням (IPS) з можливістю адаптивного аналізу загроз.
- Інтелектуальна система аналізу поведінки користувачів і мережевого трафіку.
- Автоматизоване реагування на аномальні події та підозрілу активність.
- Підтримка високої продуктивності з мінімальним впливом на швидкість мережі.

4.5. Вимоги до структури та функціонування засобу інформатизації Мережевий екран FortiGate FG-40F

Таблиця 5

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки
	Мережевий екран FortiGate FG-40F			
1	**Примірник програмної продукції для Мережевого екрану FortiGate FG-40F :** FortiGate-40F 1 Year FortiCare Essential Support або еквівалент	шт.	431	не менш ніж 12 міс.

Програмна продукція для існуючого мережевого екрану, що складається з чотирьохсот тридцяти однієї (431) підсистеми FortiGate FG-40F, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 5 та забезпечувати наступне:

- Отримання основних та проміжних релізів ПЗ через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.5.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.5.2. Вимоги до безпеки

- Не застосовуються.

4.5.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.5.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.5.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.

- Сумісність із загальноприйнятими протоколами безпеки: IPSec, TLS, DNSSEC.

4.5.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Висока продуктивність із підтримкою кластеризації для балансування навантаження.
- Автоматичне збереження резервних копій налаштувань та швидке їх відновлення.
- Захист від зовнішніх атак із мінімізацією впливу на критичні сервіси.
- Підтримка механізмів гарячого резервування (HA) для безперервної роботи.
- Контроль доступу на рівні адміністрування для запобігання несанкціонованим змінам.

4.5.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.5.8. Вимоги до режимів функціонування засобу інформатизації

- Режими роботи: моніторинг, навчання, активне блокування.
- Адаптивне керування політиками безпеки та автоматична зміна конфігурації відповідно до загроз.

4.5.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Глибокий аналіз трафіку з підтримкою сигнатурного та поведінкового виявлення загроз.
- Автоматичне оновлення баз загроз і політик безпеки.
- Централізоване логування всіх подій безпеки з можливістю інтеграції з SIEM.
- Підтримка VPN-тунелів для захищеного віддаленого доступу.
- Розширений захист від складних багатовекторних атак на рівнях L3, L4 та L7.
- Вбудована система запобігання вторгненням (IPS) з можливістю адаптивного аналізу загроз.
- Інтелектуальна система аналізу поведінки користувачів і мережевого трафіку.
- Автоматизоване реагування на аномальні події та підозрілу активність.
- Підтримка високої продуктивності з мінімальним впливом на швидкість мережі.

4.6. Вимоги до структури та функціонування засобу інформатизації Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E

Таблиця 6

№ п/п	Найменування	Од. вимір у	Кіль - кість	Термін підтримки
1	**Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E** **Примірник програмної продукції для Системи моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E:**	шт.	1	не менш ніж 12 міс.

FortiAnalyzer-400E Support або еквівалент	FortiCare	Premium	

Програмна продукція для існуючої системи моніторингу та контролю безпеки FortiAnalyzer FAZ 400E повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 6 та забезпечувати наступне:

- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.6.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.6.2. Вимоги до безпеки

- Не застосовуються.

4.6.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.6.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.6.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.6.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Захищене зберігання логів із використанням криптографічних методів.
- Автоматичне реплікування даних на резервні сервери.
- Захист від несанкціонованого доступу завдяки шифруванню та контролю доступу.
- Резервування дискових ресурсів для запобігання втраті даних.
- Вбудовані механізми самовідновлення у разі пошкодження логів.

4.6.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.6.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим реального часу** – збір і обробка логів у режимі безперервного моніторингу.
- **Режим архівування** – збереження історичних даних про події безпеки.
- **Режим аналітики** – виявлення кореляцій між подіями для побудови звітів про загрози.
- **Режим інтеграції** – передача даних до зовнішніх систем SIEM.

4.6.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Централізоване логування та аналіз подій безпеки у реальному часі.

- Автоматичне корелювання подій для виявлення складних атак.
- Інтеграція з SIEM-системами для спрощення моніторингу та звітності.
- Побудова детальних звітів з аналізу мережевої безпеки.
- Підтримка автоматичних дашбордів для візуалізації загроз.

4.7. Вимоги до структури та функціонування засобу інформатизації Система керування FortiManager FMG-VM with 450 device license

Таблиця 7

№ п/п	Найменування	Од. вимір у	Кіль - кість	Термін підтримки
	Система керування FortiManager FMG-VM with 450 device license			
1	**Примірник програмної продукції для Системи керування FortiManager FMG-VM with 450 device license:** FortiManager - VM FortiCare Premium Support FortiCare Premium Support (1 - 1010 devices/Virtual Domains) або еквівалент	шт.	1	не менш ніж 12 міс.

Програмна продукція для існуючої системи керування FortiManager FMG-VM повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 7 та забезпечувати наступне:

- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.7.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.7.2. Вимоги до безпеки

- Не застосовуються.

4.7.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.7.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.7.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.

- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.7.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Автоматичне створення резервних копій налаштувань усіх підключених пристроїв.
- Надійний контроль версій конфігурацій для швидкого відновлення після збоїв.
- Захищене адміністрування з можливістю двофакторної автентифікації.
- Можливість швидкого масштабування без ризику перевантаження системи.

4.7.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.7.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим централізованого керування** – управління всіма підключеними пристроями з однієї платформи.
- **Режим групового оновлення** – автоматичне оновлення прошивок і політик безпеки.
- **Режим аварійного відновлення** – відкат змін у конфігураціях у разі помилки.
- **Режим автоматизації** – застосування політик на основі сценаріїв та тригерів.

4.7.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Централізоване управління налаштуваннями безпеки для великої кількості пристроїв.
- Масштабоване розгортання та моніторинг політик на сотнях пристроїв одночасно.
- Контроль доступу до налаштувань з аудитом змін конфігурації.
- Автоматичне оновлення прошивок і політик безпеки.
- Забезпечення відповідності корпоративним стандартам безпеки.

4.8. Вимоги до структури та функціонування засобу інформатизації Віртуальний пристрій FortiAuthenticator-VM with 1100 user license

Таблиця 8

№ п/п	Найменування	Од. вимір у	Кіль - кість	Термін підтримки
	Віртуальний пристрій FortiAuthenticator-VM with 1100 user license			
1	**Примірник програмної продукції для Віртуального пристрою FortiAuthenticator-VM with 1100 user license:** FortiAuthenticator - VM License FortiCare Premium Support (1 - 1100 USERS) або еквівалент	шт.	3	не менш ніж 12 міс.

Програмна продукція для існуючого віртуального пристрою FortiAuthenticator-VM with 1100 user license (забезпечення сервісу не менше ніж для 1100 користувачів) повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 8 та забезпечувати наступне:

- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.

4.8.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.8.2. Вимоги до безпеки

- Не застосовуються.

4.8.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.8.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.8.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.8.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Надійний захист автентифікаційних даних та шифрування токенів доступу.
- Вбудована підтримка резервного копіювання даних автентифікації.
- Контроль доступу за допомогою багаторівневої автентифікації.
- Захищений обмін даними між клієнтами та серверами через TLS/SSL.
- Автоматичне відновлення у разі виявлення порушень у системі.

4.8.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.8.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим стандартної автентифікації** – перевірка облікових записів користувачів за стандартними правилами.
- **Режим багатофакторної автентифікації (MFA)** – додатковий рівень перевірки користувачів.
- **Режим інтеграції з Active Directory** – централізоване управління автентифікацією через AD.

- **Режим аварійного доступу** – тимчасове розширення прав доступу у разі відмови основних сервісів.

4.8.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Підтримка багатофакторної автентифікації (2FA) для користувачів.
- Централізоване управління доступом на основі ролей та груп.
- Інтеграція з Microsoft Active Directory та іншими IDM-рішеннями.
- Контроль доступу до корпоративних ресурсів за допомогою політик автентифікації.
- Захист від несанкціонованого доступу до критичних сервісів.

4.9. Вимоги до структури та функціонування засобу інформатизації Система захисту FortiSandbox-VM

Таблиця 9

№ п/п	Найменування	Од. вимір у	Кіль - кість	Термін підтримки
1	**Система захисту FortiSandbox-VM** **Примірник програмної продукції для Системи захисту FortiSandbox-V:** FortiSandbox VM00 Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs. або еквівалент	шт.	4	не менш ніж 12 міс.

Програмна продукція для існуючої системи захисту FortiSandbox-VM, яка складається з чотирьох підсистем FortiSandbox-VM, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 9 та забезпечувати наступне:

- Отримання актуальних репутаційних баз, сигнатур антивірусного захисту та інших оновлень для сервісів безпеки.
- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.
- Підтримку функцій антивірусного захисту, системи запобігання вторгненням, системи перевірки файлів.

4.9.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.9.2. Вимоги до безпеки

- Не застосовуються.

4.9.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.9.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.9.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.9.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Вбудований механізм ізоляції загроз для запобігання поширенню атак.
- Автоматичне видалення шкідливих файлів після аналізу без залишкових слідів.
- Захист конфіденційних даних шляхом обмеження доступу до звітів про загрози.
- Резервне збереження аналітичних даних для подальшого аналізу інцидентів.
- Підтримка розподіленої архітектури для підвищення надійності роботи.

4.9.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.9.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим ізоляції загроз** – тестування файлів у захищеному середовищі.
- **Режим поведінкового аналізу** – виявлення загроз без сигнатурного аналізу.
- **Режим глибокого аналізу** – емуляція виконання шкідливого коду для виявлення складних атак.
- **Режим інтеграції** – обмін інформацією про загрози з іншими системами Fortinet.

4.9.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Виявлення та аналіз нових шкідливих програм у віртуальному середовищі.
- Автоматичне блокування загроз на рівні міжмережевого екрану та поштових серверів.
- Аналіз поведінки файлів для виявлення атак нульового дня.
- Інтеграція з антивірусними системами та мережевими засобами захисту.
- Формування звітів про шкідливу активність та потенційні загрози.

4.10. Вимоги до структури та функціонування засобу інформатизації Система захисту FortiMail-VM

Таблиця 10

№ п/п	Найменування	Од. вимір у	Кіль-кість	Термін підтримки
1	**Система захисту FortiMail-VM**	шт.	2	

	Примірник програмної продукції для Системи захисту FortiMail -VM: FortiMail-VM02 FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract або еквівалент		не менш ніж 12 міс.

Програмна продукція для існуючої системи захисту FortiMail-VM, яка складається з двох підсистем FortiMail-VM, повинна включати в себе підтримку від виробника у режимі 24х7 строком дії відповідно до Таблиці 1 та забезпечувати наступне:

- Отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та інших оновлень для сервісів безпеки.
- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника;
- Підтримку функцій антивірусного захисту, антиспаму, служби захисту від вірусних епідемій, системи видалення загрози в повідомленні, системи захисту від «натискання на посилання».
- Доступ до системи захисту мережі від розширених загроз, що розгорнута у хмарному сервісі виробника.

4.10.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.10.2. Вимоги до безпеки

- Не застосовуються.

4.10.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.10.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.10.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.10.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Багаторівневий захист електронної пошти від спаму та атак нульового дня.
- Надійне шифрування листів для запобігання перехопленню даних.
- Автоматичне карантинування потенційно небезпечних повідомлень.
- Вбудовані механізми резервного копіювання налаштувань безпеки.
- Інтеграція з антивірусними базами для підвищення рівня захисту.

4.10.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.10.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим фільтрації спаму** – автоматичне відсіювання небажаних листів.
- **Режим блокування фішингових атак** – виявлення підроблених електронних листів.
- **Режим карантину** – ізоляція підозрілих повідомлень для подальшого аналізу.
- **Режим наскрізного шифрування** – захист вмісту листів під час передачі.

4.10.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Захист корпоративної пошти від фішингових атак, спаму та шкідливих вкладень.
- Інтелектуальний аналіз листів для виявлення підозрілих повідомлень.
- Контроль вхідного та вихідного трафіку для запобігання витоку даних.
- Інтеграція з системами автентифікації для перевірки відправників.
- Автоматичне карантинування потенційно небезпечних повідомлень.

4.11. Вимоги до структури та функціонування засобу інформатизації Система захисту Fortinet FortiWeb-VM

Таблиця 11

№ п/п	Найменування	Од. вимір у	Кіль - кість	Термін підтримки
	Система захисту Fortinet FortiWeb-VM			
1	**Примірник програмної продукції для Система захисту Fortinet FortiWeb-VM:** FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation) або еквівалент	шт.	2	не менш ніж 12 міс.

Програмна продукція для існуючої системи захисту FortiWeb-VM, яка складається з двох підсистем FortiWeb-VM, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 11 та забезпечувати наступне:

- Отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та інших оновлень для сервісів безпеки.
- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.
- Підтримку функцій антивірусу та безпеки веб-додатків (механізмів виявлення вразливостей та ботів, шаблонів URL-адрес, типів даних).

- Отримання оновлень списку відомих компрометованих, підозрілих та шкідливих IP адрес.

4.11.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.11.2. Вимоги до безпеки

- Не застосовуються.

4.11.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.11.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.11.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.11.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Захист веб-додатків від атак та вразливостей з використанням самонавчання.
- Контроль доступу до веб-додатків та виявлення аномальної активності.
- Автоматичне оновлення політик безпеки для відповідності актуальним загрозам.
- Вбудована підтримка резервування конфігурацій і відновлення після атак.
- Захист від несанкціонованих змін у веб-додатках.

4.11.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.11.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим базового захисту** – блокування загроз на основі сигнатур.
- **Режим поведінкового аналізу** – динамічне виявлення атак на веб-додатки.
- **Режим адаптивного навчання** – оновлення політик на основі трафіку.
- **Режим інтеграції з SIEM** – передача даних про загрози в реальному часі.

4.11.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Захист веб-додатків від атак типу SQL-ін'єкцій, XSS та CSRF.
- Контроль API-запитів для запобігання експлуатації вразливостей.
- Аналіз поведінки користувачів для виявлення автоматизованих атак.
- Динамічне оновлення правил безпеки для блокування нових загроз.
- Інтеграція з іншими рішеннями Fortinet для централізованого управління загрозами.

4.12. Вимоги до структури та функціонування засобу інформатизації Система FAD-100F Application Delivery Controller

Таблиця 12

№ п/п	Найменування	Од. вимір у	Кіль-кість	Термін підтримки
	Система FAD-100F Application Delivery Controller			
1	**Примірник програмної продукції для Системи FAD-100F Application Delivery Controller:** FortiADC-100F 1 Year Standard Bundle (FortiCare Premium plus IP Reputation and FortiADC WAF Security Service) або еквівалент	шт.	2	не менш ніж 12 міс.

Програмна продукція для існуючої системи FAD-100F Application Delivery Controller, яка складається з двох підсистем FAD-100F Application Delivery Controller, повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 12 та забезпечувати наступне:

- Отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та інших оновлень для сервісів безпеки.
- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.
- Оновлення бази компрометованих, підозрілих та шкідливих IP адрес.

4.12.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.12.2. Вимоги до безпеки

- Не застосовуються.

4.12.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.12.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.12.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.12.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Забезпечення безперервної роботи додатків завдяки балансуванню навантаження.
- Контроль стану серверів із автоматичним перемиканням у разі збою.
- Захист від DDoS-атак та перевантаження ресурсів додатків.
- Автоматизоване керування політиками доступу та безпеки.
- Можливість резервного копіювання налаштувань для швидкого відновлення.

4.12.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.12.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим балансування навантаження** – рівномірний розподіл трафіку між серверами.
- **Режим аварійного переключення** – автоматичне перенаправлення трафіку при збоях.
- **Режим продуктивності** – оптимізація з'єднань для мінімізації затримок.
- **Режим контролю безпеки** – аналіз та фільтрація трафіку на рівні додатків.

4.12.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Балансування навантаження між серверами для забезпечення безперебійної роботи.
- Контроль продуктивності додатків та мінімізація часу відгуку.
- Інтелектуальне кешування контенту для оптимізації швидкості завантаження.
- Автоматичне переключення на резервні сервери у разі збою.
- Підтримка шифрування трафіку для безпечної передачі даних.

4.13. Вимоги до структури та функціонування засобу інформатизації Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G

Таблиця 13

№ п/п	Найменування	Од. вимір у	Кіль - кість	Термін підтримки
	Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G			
1	**Примірник програмної продукції для Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G:** FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service) або еквівалент	шт.	1	не менш ніж 12 міс.

Програмна продукція для існуючої системи моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 13 та забезпечувати наступне:

- Отримання основних та проміжних релізів ПЗ через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.
- Доступ до обміну і оновлення індикаторів компрометації (IOC).
- Можливість створення та виконання не менш ніж 100 автоматичних дій (реакцій на інциденти).
- Доступ до інформації про новітні загрози та вектори атаки.

4.13.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.13.2. Вимоги до безпеки

- Не застосовуються.

4.13.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.13.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.13.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.13.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Захищене збереження логів без можливості їх модифікації.
- Контроль відповідності безпеки корпоративним стандартам та нормативним вимогам.
- Розширене шифрування логів для захисту від несанкціонованого доступу.
- Вбудовані механізми виявлення збоїв та самовідновлення.
- Автоматична реплікація даних для забезпечення безперервності роботи.

4.13.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.13.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим реального часу** – негайний аналіз логів із попередженням про загрози.
- **Режим довготривалого зберігання** – архівування логів для історичного аналізу.
- **Режим автоматичної кореляції** – аналіз подій для виявлення складних атак.
- **Режим аварійного дублювання** – резервування логів на віддалені сервери.

4.13.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Розширене збирання та аналіз логів з урахуванням поведінкових патернів.
- Виявлення складних атак за допомогою машинного навчання.
- Автоматичне корелювання подій для швидкого реагування на загрози.
- Створення звітів для оцінки безпеки та відповідності стандартам.
- Інтеграція з іншими системами Fortinet для комплексного аналізу загроз.

4.14. Вимоги до структури та функціонування засобу інформатизації Віртуальний пристрій FortiEMS-VM with 500 user license

Таблиця 14

№ п/п	Найменування	Од. вимір у	Кіль-кість	Термін підтримки
	Віртуальний пристрій FortiEMS-VM with 500 user license			
1	**Примірник програмної продукції для Віртуальний пристрій FortiEMS-VM with 500 user license:** Endpoint-based Licenses - EPP/ATP (On Premise Deployments) 1 Year FortiClient EPP/ATP Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/ATP on-prem EMS with FortiCare Premium. або еквівалент	шт.	1	не менш ніж 12 міс.

Програмна продукція для існуючого віртуального пристрою FortiEMS-VM with 500 user license (забезпечення сервісу не менше ніж для 500 користувачів) повинна включати в себе підтримку від виробника у режимі 24x7 строком дії відповідно до Таблиці 14 та забезпечувати наступне:

- Отримання основних та проміжних релізів ПЗ через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Постійний (24 години х 7 днів на тиждень) авторизований доступ до сайту виробника.
- Забезпечення перевірки на відповідність для не менш ніж 500 користувачів, при підключенні через VPN клієнт додатків
- Забезпечення доступу до оновлення сигнатур безпеки (AV, IPS) для не менш ніж 500 клієнт-додатків.

4.14.1. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.14.2. Вимоги до безпеки

- Не застосовуються.

4.14.3. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.14.4. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

4.14.5. Вимоги до стандартизації та уніфікації

- Використання міжнародних стандартів безпеки: ISO/IEC 27001, NIST SP 800-53.
- Підтримка національних вимог захисту інформації згідно з НД ТЗІ 3.6-001-2000.
- Сумісність із загальноприйнятими протоколами безпеки: TLS, DNSSEC.

4.14.6. Вимоги до надійності засобу інформатизації та збереженості інформації

- Захист кінцевих пристроїв від несанкціонованого доступу та атак.
- Контроль оновлень безпеки та відповідності пристроїв корпоративним стандартам.
- Вбудовані механізми резервного копіювання та швидкого відновлення.
- Інтеграція з антивірусними системами та мережевими засобами контролю.

4.14.7. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- Відповідність вимогам НД ТЗІ 3.6-001-2000 щодо інформаційного обміну між компонентами системи.

4.14.8. Вимоги до режимів функціонування засобу інформатизації

- **Режим централізованого контролю** – управління безпекою кінцевих пристроїв.
- **Режим відповідності політикам** – перевірка дотримання правил безпеки.
- **Режим автоматичного виявлення загроз** – блокування заражених пристроїв.
- **Режим моніторингу активності** – аудит дій користувачів у корпоративній мережі.

4.14.9. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

- Централізоване управління безпекою кінцевих пристроїв.
- Контроль відповідності пристроїв політикам безпеки організації.
- Автоматичне виявлення та ізоляція заражених пристроїв.
- Захист корпоративних пристроїв навіть поза межами локальної мережі.
- Моніторинг дій користувачів для запобігання витоку даних.

5. Вимоги до розробки та передачі послуг

5.1. Вимоги до розробки

- Відсутні

5.2. **Вимоги до передачі;**

- Забезпечення відображення примірників ІІЗ у кабінеті адміністратора на порталі виробника;
- Код активації у файлі формату *.pdf та на паперовому носії.

5.3. Вимоги до гарантійної підтримки

- Забезпечення режиму підтримки 24x7, строком дії відповідно до Таблиць 1 - 14.

6. **Висновки.**

- Призначення та цілі інформатизації відповідно до цих Технічних вимог забезпечують якісну реалізацію визначених планових потреб Замовника та забезпечення функціонування засобу інформатизації і гарантує відповідність набору критеріїв, які описують засіб інформатизації.

7. **Додатки.**

- Відсутні.

8. **Заявка на модернізацію (модифікацію, розвиток).**

- Не передбачена.

Додаток 2

Кваліфікаційні критерії процедури закупівлі та перелік документів, що підтверджують інформацію учасників про відповідність їх таким критеріям

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	**Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) договору (договорів)**	Довідка в довільній формі за підписом уповноваженої особи учасника, завірена печаткою (у разі її використання), на фірмовому бланку (у разі наявності) про наявність досвіду виконання аналогічного (аналогічних) договору (договорів)* із зазначенням: найменування контрагента, предмету договору, дати укладання. На підтвердження виконання аналогічного (аналогічних) договору (договорів), який (які) зазначений (зазначені) в довідці, надаються копії: виконаного договору, видаткової (видаткових) накладної (накладних) або акту (актів), листа-відгука від замовника, або інші документи, що підтверджують його виконання. ** Під аналогічним договором розуміється договір подібний за предметом закупівлі за період з 2014 року по теперішній час. Якщо в довідці учасник вказує декілька аналогічних договорів, то всі документи щодо підтвердження виконання таких договорів надаються щодо кожного із вказаних в довідці договорів.*
2.	**Інформація про технічні, якісні та кількісні характеристики предмета закупівлі**	Для підтвердження відповідності тендерної пропозиції технічним, якісним та кількісним характеристикам (вимогам) замовника Учасник у складі тендерної пропозиції повинен надати: 1) інформацію про можливість поставки товару відповідно до технічної специфікації із зазначенням конкретної назви програмної продукції та терміну її дії, що пропонується учасником; 2) авторизаційний лист (авторизаційна форма тощо) від виробника товару або його офіційного представника, дистриб'ютора в Україні, який підтверджує наявність у Учасника статусу партнера та права на здійснення продажу запропонованого Учасником товару, виданий на адресу Замовника із посиланням на процедуру закупівлі.

У разі участі об'єднання учасників підтвердження відповідності кваліфікаційним критеріям здійснюється з урахуванням узагальнених об'єднаних показників кожного учасника такого об'єднання на підставі наданої об'єднанням інформації.

Ініціатор закупівлі **А. С. Стревалюк**

ВИКОНАВЧИЙ ОРГАН КИЇВСЬКОЇ МІСЬКОЇ РАДИ
(КИЇВСЬКА МІСЬКА ДЕРЖАВНА АДМІНІСТРАЦІЯ)
ДЕПАРТАМЕНТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
КОМУНАЛЬНЕ ПІДПРИЄМСТВО «ІНФОРМАТИКА»
(КП «ІНФОРМАТИКА»)

State Enterprise
Informatics

вул. Левка Лук'яновича, буд. 3, м. Київ, 03186, тел.: (044) 366-86-54 E-mail: informatika@kmda.gov.ua
Код ЄДРПОУ 31024875

12.02.2025 № 075/3-401

Департамент
інформаційно-комунікаційних
технологій виконавчого органу
Київської міської ради (Київської
міської державної адміністрації)

Щодо продовження терміну дії ліцензій

Комунальне підприємство «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) (далі – КП «Інформатика») та Спеціалізоване комунальне підприємство «Київтелесервіс» (далі – СКП «Київтелесервіс») є учасниками (співвиконавцями) Комплексної міської цільової програми «Цифровий Київ» на 2024 - 2027 роки (далі - Програма), затвердженої рішенням Київської міської ради від 7 грудня 2023 року № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257) та виконують передбачені нею заходи.

На балансі КП «Інформатика», перебуває віртуальний пристрій FortiAuthenticator-VM with 500 user license у складі: FortiAuthenticator-VM License 24x7 FortiCare Contract (1 – 1100 USERS) та віртуальний пристрій FortiEMS-VM with 500 user (FortiClient) license у складі: Endpoint-based Licenses - EPP/APT (On Premise Deployments) FortiClient EPP/APT Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/APT, on-prem EMS with FortiCare Premium.

Вказані віртуальні пристрої, потребують ліцензійної підтримки для подальшої їх роботи.

Враховуючи вищевикладене та з урахуванням що заходами Програми на СКП «Київтелесервіс» покладається придбання ліцензійного програмного забез-

печення, просимо Вас посприяти у забезпеченні ліцензійною підтримкою зазначені віртуальні пристрої строком дії не менш ніж 12 місяців відповідно до наведеної таблиці:

Віртуальний пристрій FortiAuthenticator-VM with 500 user license :			
FortiAuthenticator - VM License 24x7 FortiCare Contract (1 - 1100 USERS)	шт.	1	не менш ніж 12 місяців
Віртуальний пристрій FortiEMS-VM with 500 user (500 FrotiClient) license :			
Endpoint-based Licenses - EPP/APT (On Premise Deployments) FortiClient EPP/APT Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/APT, on-prem EMS with FortiCare Premium.	шт.	1	не менш ніж 12 місяців

В.о. генерального директора Микола ЖАНДОРОВ

Олег Заграй
0504012012

УКРІНФОСИСТЕМИ
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «УКРАЇНСЬКІ ІНФОСИСТЕМИ»
Місцезнаходження - 04112, м.Київ, вулиця Олени Теліги, будинок 4
Поштова адреса - 04112, м.Київ, вул. Олени Теліги, будинок 4, тел. +38 (044) 422-55-33
web: http://ukrinfosystems.com.ua, e-mail: info@ukrinfosystems.com.ua
IBAN UA463006140000026005500095615, АТ «КРЕДІ АГРІКОЛЬ БАНК», МФО 300614
код ЄДРПОУ 39210567, ІПН 392105626584

№ 39 від 17.03.2025р.
на № 67-2025 від 14.03.2025р.

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 69/2025
Від 17.03. 2025 р.

В.о. директора
СПЕЦІАЛІЗОВАНОГО
КОМУНАЛЬНОГО
ПІДПРИЄМСТВА «КИЇВТЕЛЕСЕРВІС»
Олександру ВОЛОЩУКУ

ЦІНОВА ПРОПОЗИЦІЯ

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «УКРАЇНСЬКІ ІНФОСИСТЕМИ», у відповідь на Ваш Запит № 67-2025 від 14.03.2025р. та ознайомившись з технічними вимогами до предмету закупівлі «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури; 48730000-4 – Пакети програмного забезпечення для забезпечення безпеки за ДК 021:2015 Єдиного закупівельного словника» надає свою цінову пропозицію:

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки	Ціна за одиницю, грн. (без ПДВ)	Сума, грн. (з ПДВ)
1	**Мережевий екран FortiGate FG-1000D** **Примірник програмної продукції для Мережевого екрану FortiGate FG-1000D:** FortiGate-1000D 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	шт.	2	12 місяців	918 241,50	2 203 779,60
2	**Мережевий екран FortiGate FG-3000D** **Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D:** FortiGate-3000D 1 Year FortiCare Premium Support	шт.	2	12 місяців	633 722,85	1 520 934,84
3	**Мережевий екран FortiGate FG-200F** **Примірник програмної продукції для Мережевого екрану FortiGate FG-200F:** FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	шт.	2	12 місяців	210 881,00	506 114,40
4	**Мережевий екран FortiGate FG-80F** **Примірник програмної продукції для Мережевого екрану FortiGate FG-80F:** FortiGate-80F 1 Year FortiCare Essential Support	шт.	20	12 місяців	12 435,50	298 452,00
5	**Мережевий екран FortiGate FG-40F** **Примірник програмної продукції для Мережевого екрану FortiGate FG-40F:** FortiGate-40F 1 Year FortiCare Essential Support	шт.	431	12 місяців	4 005,85	2 071 825,62
6	**Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E** **Примірник програмної продукції для Системи моніторингу та контролю безпеки FortiAnalyzer FAZ-400E:** FortiAnalyzer-400E FortiCare Premium Support	шт.	1	12 місяців	134 944,35	161 933,22
7	**Система керування FortiManager FMG-VM with 450 device license** **Примірник програмної продукції для Системи керування FortiManager FMG-VM**	шт.	1	12 місяців	1 020 477,35	1 224 572,82

	with 450 device license: FortiManager - VM FortiCare Premium Support FortiCare Premium Support (1 - 1010 devices/Virtual Domains)					
8	**Віртуальний пристрій FortiAuthenticator-VM with 1100 user license** **Примірник програмної продукції для Віртуального пристрою FortiAuthenticator-VM with 1100 user license:** FortiAuthenticator - VM License FortiCare Premium Support (1 - 1100 USERS)	шт.	3	12 місяців	41 869,65	150 730,74
9	**Система захисту FortiSandbox-VM** **Примірник програмної продукції для Системи захисту FortiSandbox-V:** FortiSandbox VM00 Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs.	шт.	4	12 місяців	305 976,00	1 468 684,80
10	**Система захисту FortiMail-VM** **Примірник програмної продукції для Системи захисту FortiMail -VM:** FortiMail-VM02 FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract	шт.	2	12 місяців	346 313,00	831 151,20
11	**Система захисту Fortinet FortiWeb-VM** **Примірник програмної продукції для Системи захисту Fortinet FortiWeb-VM:** FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)	шт.	2	12 місяців	1 082 480,65	2 597 953,56
12	**Система FAD-100F Application Delivery Controller** **Примірник програмної продукції для Системи FAD-100F Application Delivery Controller:** FortiADC-100F 1 Year Standard Bundle (FortiCare Premium plus IP Reputation and FortiADC WAF Security Service)	шт.	2	12 місяців	111 919,50	268 606,80
13	**Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G** **Примірник програмної продукції для Системи моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G:** FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service)	шт.	1	12 місяців	9 279 878,65	11 135 854,38
14	**Віртуальний пристрій FortiEMS-VM with 500 user license** **Примірник програмної продукції для Віртуального пристрою FortiEMS-VM with 500 user license:** Endpoint-based Licenses - EPP/ATP (On Premise Deployments) 1 Year FortiClient EPP/ATP Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/ATP on-prem EMS with FortiCare Premium.	шт.	1	12 місяців	547 719,35	657 263,22
					Всього без ПДВ:	**20 914 881,00**
					Всього ПДВ:	**4 182 976,20**
					Всього з ПДВ:	**25 097 857,20**

Загальна вартість цінової пропозиції становить 25 097 857,20 грн. в тому числі ПДВ 20% - 4 182 976,20 грн.

З повагою,
директор ТОВ «УКРІНФОСИСТЕМИ» Андрій ПЯТОВ

ТОВ «ОПТІДАТА»
04071, м. Київ, вул. Межигірська, 22,
UA103226690000026004300941299
у філії ГУ по м. Києву та Київської області,
АТ «Ощадбанк» ТВБВ 10026/020, МФО:
322669, ЄДРПОУ: 39693067

Вих№ 031725/9 від 17.03.2025
На № 68-2025 від 14.03.2025

Спеціалізованому комунальному підприємству «Київтелесервіс»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Товариство з обмеженою відповідальністю «ОПТІДАТА» надає комерційну пропозицію, у відповідь на Ваш запит, стосовно закупівлі Пакети програмного забезпечення для підсистем захисту міської мережевої інфраструктури; 48730000-4 – Пакети програмного забезпечення для забезпечення безпеки.

№	Назва	Од. виміру	К-ть	Ціна за од., грн. з ПДВ	Всього, грн. з ПДВ
1	Мережевий екран FortiGate FG-1000D				
	Примірник програмної продукції для Мережевого екрану FortiGate FG-1000D : FortiGate-1000D 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	шт	2	1 107 162,00	2 214 324,00
2	Мережевий екран FortiGate FG-3000D				
	Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D : FortiGate-3000D 1 Year FortiCare Premium Support	шт	2	764 106,00	1 528 212,00
3	Мережевий екран FortiGate FG-200F				
	Примірник програмної продукції для Мережевого екрану FortiGate FG-200F: FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	шт	2	254 268,00	508 536,00
4	Мережевий екран FortiGate FG-80F				
	Примірник програмної продукції для Мережевого екрану FortiGate FG-80F: FortiGate-80F 1 Year FortiCare Essential Support	шт	20	14 994,00	299 880,00
5	Мережевий екран FortiGate FG-40F				

info@optidata.com.ua
www.optidata.com.ua

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 71/2025
від 17.03. 2025

Opti Data
Enforce your security

ТОВ «ОПТІДАТА»
04071, м. Київ, вул. Межигірська, 22,
UA103226690000026004300941299
у філії ГУ по м. Києву та Київської області,
АТ «Ощадбанк» ТВБВ 10026/020, МФО:
322669, ЄДРПОУ: 39693067

	Примірник програмної продукції для Мережевого екрану FortiGate FG-40F : FortiGate-40F 1 Year FortiCare Essential Support	шт	431	4 830,00	2 081 730,00
6	Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E				
	Примірник програмної продукції для Системи моніторингу та контролю безпеки FortiAnalyzer FAZ 400E: FortiAnalyzer-400E FortiCare Premium Support	шт	1	162 708,00	162 708,00
7	Система керування FortiManager FMG-VM with 450 device license				
	Примірник програмної продукції для Системи керування FortiManager FMG-VM with 450 device license: FortiManager - VM FortiCare Premium Support FortiCare Premium Support (1 - 1010 devices/Virtual Domains)	шт	1	1 230 432,00	1 230 432,00
8	Віртуальний пристрій FortiAuthenticator-VM with 1100 user license				
	Примірник програмної продукції для Віртуального пристрою FortiAuthenticator-VM with 1100 user license: FortiAuthenticator - VM License FortiCare Premium Support (1 - 1100 USERS)	шт	3	50 484,00	151 452,00
9	Система захисту FortiSandbox-VM				
	Примірник програмної продукції для Системи захисту FortiSandbox-V: FortiSandbox VM00 Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs.	шт	4	368 928,00	1 475 712,00
10	Система захисту FortiMail-VM				
	Примірник програмної продукції для Системи захисту FortiMail -VM: FortiMail-VM02 FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract	шт	2	417 564,00	835 128,00
11	Система захисту Fortinet FortiWeb-VM				
	Примірник програмної продукції для	шт	2	1 305 192,00	2 610 384,00

Opti Data
Enforce your security

ТОВ «ОПТІДАТА»
04071, м. Київ, вул. Межигірська, 22,
UA103226690000026004300941299
у філії ГУ по м. Києву та Київської області,
АТ «Ощадбанк» ТВБВ 10026/020, МФО:
322669, ЄДРПОУ: 39693067

	Система захисту Fortinet FortiWeb-VM: FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)				
12	Система FAD-100F Application Delivery Controller				
	Примірник програмної продукції для Системи FAD 100F Application Delivery Controller: FortiADC-100F 1 Year Standard Bundle (FortiCare Premium plus IP Reputation and FortiADC WAF Security Service)	шт	2	134 946,00	269 892,00
13	Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G				
	Примірник програмної продукції для Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G: FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service)	шт	1	11 189 136,00	11 189 136,00
14	Віртуальний пристрій FortiEMS-VM with 500 user license				
	Примірник програмної продукції для Віртуальний пристрій FortiEMS-VM with 500 user license: Endpoint-based Licenses - EPP/ATP (On Premise Deployments) 1 Year FortiClient EPP/ATP Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/ATP on prem EMS with FortiCare Premium.	шт	1	660 408,00	660 408,00
ПДВ (20%):					**4 202 989,00**
Разом, грн з ПДВ:					**25 217 934,00**

З повагою,
Генеральний директор
ТОВ «ОПТІДАТА» Білик М.А.

info@optidata.com.ua
www.optidata.com.ua

www.tb.ua

ТОВ "ТЕХНОЛОГІЇ ДЛЯ БІЗНЕСУ"
вул. Угорська, буд. 12, офіс 21, м. Львів, 79034
БЦ Grand Step, вул. Польова, 24Д, м. Київ, 03056
tb@tb.ua

TECHNOLOGY for BUSINESS

Вих.№250317/2 від 17.03.2025	В.о. директора СКП «КИЇВТЕЛЕСЕРВІС» Олександру ВОЛОЩУКУ

щодо запиту цінової пропозиції

У відповідь на Ваш запит №70-2025 від 14.03.2025р. надаємо інформацію щодо орієнтовної вартості засобів інформатизації «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури; 48730000-4 – Пакети програмного забезпечення для забезпечення безпеки за ДК 021:2015 Єдиного закупівельного словника», відповідно до технічних вимог, наданих Вами у Додатку.

Цінова пропозиція

№	Найменування	Од. вим.	К-сть	Термін підтримки	Ціна за од., грн з ПДВ	Сума, грн з ПДВ
1	Мережевий екран FortiGate FG-1000D	шт	2	12 міс.	1 115 070,00	2 230 140,00
	Примірник програмної продукції для Мережевого екрану FortiGate FG-1000D : FortiGate-1000D 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)					
2	Мережевий екран FortiGate FG-3000D	шт	2	12 міс.	769 563,90	1 539 127,80
	Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D : FortiGate-3000D 1 Year FortiCare Premium Support					
3	Мережевий екран FortiGate FG-200F	шт	2	12 міс.	256 084,2	512 168,40
	Примірник програмної продукції для Мережевого екрану FortiGate FG-200F: FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)					
4	Мережевий екран FortiGate FG-80F	шт	20	12 міс.	15101,10	302 022,00
	Примірник програмної продукції для Мережевого екрану FortiGate-80F: FortiGate-80F 1 Year FortiCare Essential Support					
5	Мережевий екран FortiGate FG-40F	шт	431	12 міс.		2 096 599,50

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 68/2025
Від 17.03. 2025 р.

www.tb.ua

ТОВ "ТЕХНОЛОГІЇ ДЛЯ БІЗНЕСУ"
вул. Угорська, буд. 12, офіс 21, м. Львів, 79034
БЦ Grand Step, вул. Польова, 24Д, м. Київ, 03056
tb@tb.ua

TECHNOLOGY for BUSINESS

	Примірник програмної продукції для Мережевого екрану FortiGate-40F: FortiGate-40F 1 Year FortiCare Essential Support				4864,50	
6	Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E	шт	1	12 міс.	163 870,20	163 870,20
	Примірник програмної продукції для Системи моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E: FortiAnalyzer-400E FortiCare Premium Support					
7	Система керування FortiManager FMG-VM with 450 device license	шт	1	12 міс.	1 239 221,00	1 239 221,00
	Примірник програмної продукції для Системи керування FortiManager FMG-VM with 450 device license: FortiManager - VM FortiCare Premium Support FortiCare Premium Support (1 - 1010 devices/Virtual Domains)					
8	Віртуальний пристрій FortiAuthenticator-VM with 1100 user license	шт	3	12 міс.	50 844,6	152 533,80
	Примірник програмної продукції для Віртуального пристрою FortiAuthenticator-VM with 1100 user license: FortiAuthenticator - VM License FortiCare Premium Support (1 - 1100 USERS)					
9	Система захисту FortiSandbox-VM	шт	4	12 міс.	371 563,2	1 486 252,80
	Примірник програмної продукції для Системи захисту FortiSandbox-V: FortiSandbox VM00 Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs.					
10	Система захисту FortiMail-VM	шт	2	12 міс.	420 546,60	841 093,2
	Примірник програмної продукції для Системи захисту FortiMail -VM: FortiMail-VM02 FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract					
11	Система захисту Fortinet FortiWeb-VM	шт	2	12 міс.	1 314 515,00	2 629 030,00
	Примірник програмної продукції для Системи захисту Fortinet FortiWeb-VM FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)					

www.tb.ua

ТОВ "ТЕХНОЛОГІЇ ДЛЯ БІЗНЕСУ"
вул. Угорська, буд. 12, офіс 21, м. Львів, 79034
БЦ Grand Step, вул. Польова, 24Д, м. Київ, 03056
tb@tb.ua

TECHNOLOGY for BUSINESS

12	Система FAD-100F Application Delivery Controller	**шт**	**2**	12 міс.	135 909,90	271 819,80
	Примірник програмної продукції для Системи FAD-100F Application Delivery Controller: FortiADC-100F 1 Year Standard Bundle (FortiCare Premium plus IP Reputation and FortiADC WAF Security Service)					
13	Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G	**шт**	**1**	12 міс.	11 269 058,00	11 269 058,00
	Примірник програмної продукції для Системи моніторингу та контролю безпеки FortiAnalyzer-3700G: FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service)					
14	Віртуальний пристрій FortiEMS-VM with 500 user license	**шт**	**1**	12 міс.	665 125,2	665 125,2
	Примірник програмної продукції для Віртуального пристрою FortiEMS-VM with 500 user license: Endpoint-based Licenses - EPP/ATP (On Premise Deployments) 1 Year FortiClient EPP/ATP Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/ATP on-prem EMS with FortiCare Premium.					
					Всього грн. з ПДВ	25 398 061,70

З повагою
Генеральний директор **Валерій МИКОЛАЙЧУК**

CONSTRUCTION

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ВМ КОНСТРАКШН УКРАЇНА»

Вих.№ 2/032025 від 17.03.2025

В.о. Директора
СКП "КИЇВТЕЛЕСЕРВІС"
О. ВОЛОЩУКУ

Щодо надання цінової пропозиції

Шановний пане Олександре!

ТОВ «ВМ КОНСТРАКШН УКРАЇНА» засвідчує свою повагу за плідну співпрацю та у відповідь на ваш запит від 14.03.2025 року № 71-2025 надає орієнтовну вартість щодо закупівлі «Пакети програмного забезпечення для підсистем захисту міської мережевої інфраструктури; 48730000-4 – Пакети програмного забезпечення для забезпечення безпеки за ДК 021:2015 Єдиного закупівельного словника», на виконання пункту 6.2 «Створення, розвиток та модернізація мережевої інфраструктури, сервісної мережевої інфраструктури, платформи Інтернету речей (IoT), мереж доступу, радіомереж, системи отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку» переліку завдань та заходів Комплексної міської цільової програми «ЦИФРОВИЙ КИЇВ» на 2024 - 2025 роки затвердженої рішенням Київської міської ради від 07 грудня 2023 року № 7516/7557 у відповідності до технічних вимог, яка складає **24 917 683, 80 грн. (Двадцять чотири мільйони дев'ятсот сімнадцять тисяч шістсот вісімдесят три гривні 80 копійок)** з ПДВ.

Специфікація та ціна наведена у таблиці:

№ п/п	Найменування	Од. виміру	Кількість	Термін підтримки	Ціна за одиницю без ПДВ, грн.	Вартість без ПДВ, грн.	Вартість з ПДВ, грн.
1	**Мережевий екран FortiGate FG-1000D**						

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 70/2025
від 17.03 2025 р.

ЄДРПОУ 39576191

п/р UA09 3806 3400000 26003107684001 в ПуАТ КБ «АКОРДБАНК», ІПН 395761926591

вул. Глибочицька, буд. 17, корпус 1А, нежитлове приміщення 417, м. Київ, 04052, Україна

www.vmcu.com.ua, office@vmcu.com.ua . Тел: +38 (044) 33 88 640

	Примірник програмної продукції для Мережевого екрану FortiGate FG-1000D : FortiGate-1000D 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	шт.	2	12 місяців	911 651,50	1 823 303,00	2 187 963,60
2	**Мережевий екран FortiGate FG-3000D** **Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D :** FortiGate-3000D 1 Year FortiCare Premium Support	шт.	2	12 місяців	629 174,50	1 258 349,00	1 510 018,00
3	**Мережевий екран FortiGate FG-200F** **Примірник програмної продукції для Мережевого екрану FortiGate FG-200F:** FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	шт.	2	12 місяців	209 367,50	418 735,00	502 482,00
4	**Мережевий екран FortiGate FG-80F** **Примірник програмної продукції для Мережевого екрану FortiGate FG-80F:** FortiGate-80F 1 Year FortiCare Essential Support	шт.	20	12 місяців	12 346,50	246 930,00	296 316,00
5	**Мережевий екран FortiGate FG-40F** **Примірник програмної продукції для Мережевого екрану FortiGate FG-40F :** FortiGate-40F 1 Year FortiCare Essential Support	шт.	431	12 місяців	3 977,00	1 714 087,00	2 056 904,40
6	**Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 400E**	шт.	1	12 місяців	133 976,00	133 976,00	160 771,20

	Примірник програмної продукції для Системи моніторингу та контролю безпеки FortiAnalyzer FAZ-400E: FortiAnalyzer-400E 1 Year FortiCare Premium Support						
7	**Система керування FortiManager FMG-VM with 450 device license** **Примірник програмної продукції для Системи керування FortiManager FMG-VM with 450 device license:** FortiManager - VM FortiCare Premium Support 1 Year FortiCare Premium Support (1 - 1010 devices/Virtual Domains)	шт.	1	12 місяців	1 013 153,50	1 013 153,50	1 215 784,20
8	**Віртуальний пристрій FortiAuthenticator-VM with 1100 user license** **Примірник програмної продукції для Віртуального пристрою FortiAuthenticator-VM with 1100 user license:** FortiAuthenticator - VM License 1 Year FortiCare Premium Support (1 - 1100 USERS)	шт.	3	12 місяців	41 569,00	124 707,00	149 648,40
9	**Система захисту FortiSandbox-VM** **Примірник програмної продукції для Системи захисту FortiSandbox-V:** FortiSandbox VM00 1 Year Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs.	шт.	4	12 місяців	303 780,00	1 215 120,00	1 458 144,80
10	**Система захисту FortiMail-VM**	шт.	2	12 місяців	343 827,50	687 655,00	825 186,00

	Примірник програмної продукції для Системи захисту FortiMail -VM: FortiMail-VM02 1 Year FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract						
11	**Система захисту Fortinet FortiWeb-VM** **Примірник програмної продукції для Системи захисту Fortinet FortiWeb-VM :** FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)	шт.	2	12 місяців	1 074 711,50	2 149 423,00	2 579 307,60
12	**Система FAD-100F Application Delivery Controller** **Примірник програмної продукції для Системи FAD- 100F Application Delivery Controller:** FortiADC-100F 1 Year Standard Bundle (FortiCare Premium plus IP Reputation and FortiADC WAF Security Service)	шт.	2	12 місяців	111 116,50	222 233,00	266 679,60
13	**Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G** **Примірник програмної продукції для Система моніторингу та контролю безпеки FortiAnalyzer FAZ-3700G:** FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service,Security Automation Service, and FortiGuard Outbreak Service)	шт.	1	12 місяців	9 213 276,50	9 213 276,50	11 055 931,80
14	**Віртуальний пристрій FortiEMS-VM with 500 user license**	шт.	1	12 місяців	543 788,50	543 788,50	652 546,20

	Примірник програмної продукції для Віртуальний пристрій FortiEMS-VM with 500 user license: Endpoint-based Licenses - EPP/ATP (On Premise Deployments) 1 Year FortiClient EPP/ATP Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/ATP on-prem EMS with FortiCare Premium.						
Всього без ПДВ:							**20 764 736,50**
ПДВ:							**4 152 947,30**
Всього з ПДВ:							**24 917 683,80**

З повагою,
Директор **Сергій Мороз**