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

Начальника відділу інформаційної безпеки Стревалюка Антона Сергійовича

СЛУЖБОВА ЗАПИСКА

місто Київ «23» лютого 2026 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 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), згідно із зверненням КП "Інформатика" № 075/3-223 від 30.01.2026.

Обґрунтування обсягів закупівлі:

З метою забезпечення коректної працездатності, забезпечення доступу до оновлень програмної продукції, сигнатур та підтримки виробником систем міської мережевої інфраструктури, для забезпечення захисту міської мережевої інфраструктури має бути передбачено постачання програмної продукції (придбання ліцензійного програмної продукції 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 продукції, 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 програмної продукції 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 керування FortiManager FMG-VM with 450 device license.
7. Віртуальний пристрій FortiAuthenticator-VM with 1100 user license.
8. Система захисту FortiSandbox-VM.

Отримано 25.02.2026

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

Технічні вимоги до предмета закупівлі рекомендовані протоколом №5 від 03.02.2026 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 сформована Ініціатором закупівлі відповідно до «Порядку визначення очікуваної вартості предмета закупівлі в спеціалізованому комунальному підприємстві «Київтелесервіс»», розробленого на основі Примірної методики визначення очікуваної вартості предмета закупівлі (наказ Мінекономіки від 18.02.2020 № 275) та затвердженого наказом СКП «Київтелесервіс» №68 від 21.08.2023, з використанням методу порівняння ринкових цін у спосіб, що передбачає направлення не менше 3-х письмових запитів цінових пропозицій (електронною поштою) виробникам, офіційним представникам та дилерам, постачальникам конкретного товару, надавачам послуг.

Очікувана вартість предмета закупівлі становить 29 312 273,41 грн. (двадцять дев'ять мільйонів триста дванадцять тисяч двісті сімдесят три грн. сорок коп.) з ПДВ, є середньоарифметичним значенням отриманих комерційних пропозицій і не перевищує розмір бюджетного призначення.

Розмір бюджетного призначення визначено паспортом бюджетної програми на 2026 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 – 499 (чотириста дев'яноста дев'ять) штук.

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

Строк поставки товарів – до 20 березня 2026 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**

Перший заступник директора _____ **С.П. Пашков**

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 – спеціалізоване комунальне підприємство «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»;
- Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- Постанова Кабінету Міністрів України від 21.02.2025 №205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» » (у редакції постанови Кабінету Міністрів України від 15.07.2025 № 893 зі змінами);
- Постанови Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем».
- Цей перелік документів не є вичерпним і може бути доповнений та уточнений під час укладання договору про **підтримку програмної продукції для підсистем захисту міської мережевої інфраструктури**.

2. Призначення та цілі інформатизації:

2.1. Призначення

- Забезпечення доступу обладнання Fortinet до оновлення сигнатур та компонентів системи захисту;
- Забезпечення доступу 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 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.

3.7. 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.

3.8. 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.

3.9. 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.

3.10. 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.

3.11. 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.

3.12. 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.

3.13. 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	Кіль-кість	Термін підтримки

1	**Мережевий екран FortiGate FG-1000D**	шт.	2	
	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) або еквівалент			не менш ніж 12 міс.

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-комунікаційних 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	Кіль-кість	Термін підтримки
1	**Мережевий екран FortiGate FG-3000D**	шт.	2	не менш ніж 12 міс.
	Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D : FortiGate-3000D 1 Year FortiCare Premium Support або еквівалент			
2	**Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D :** FortiGate-3000D 1 Year FortiGuard URL, DNS & Video Filtering Service 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 ПП через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника.
- Отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та інших оновлень для сервісів безпеки.
- 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-комунікаційних 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	Кіль-кість	Термін підтримки
1	**Мережевий екран FortiGate FG-200F**	шт.	4	не менш ніж 12 міс.
	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			

Програмна продукція для існуючого мережевого екрану, що складається з чотирьох 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-комунікаційних 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	Кіль-кість	Термін підтримки
1	**Мережевий екран FortiGate FG-80F**	шт.	43	не менш ніж 12 міс.
	Примірник програмної продукції для Мережевого екрану FortiGate FG-80F : FortiGate-80F 1 Year FortiCare Essential Support або еквівалент			

Програмна продукція для існуючого мережевого екрану, що складається з сорока трьох (23) 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 ПП 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-комунікаційних 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. вимір	Кіль-кість	Термін підтримки
1	**Мережевий екран FortiGate FG-40F**	шт.	431	не менш ніж 12 міс.
	Примірник програмної продукції для Мережевого екрану FortiGate FG-40F : FortiGate-40F 1 Year FortiCare Essential Support або еквівалент			

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 ПП 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-комунікаційних 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 керування FortiManager FMG-VM with 450 device license

Таблиця 7

№ п/п	Найменування	Од. вимір	Кіль-кість	Термін підтримкии
1	**Система керування FortiManager FMG-VM with 540 device license**	шт.	1	не менш ніж 12 міс.
	Примірник програмної продукції для Системи керування FortiManager FMG-VM with 540 device license: FortiManager - VM FortiCare Premium Support FortiCare Premium Support (1 - 1010 devices/Virtual Domains) або еквівалент			

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.

4.6.1. 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-комунікаційних 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

- 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.

4.6.7. 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 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.

4.6.9. 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.

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

Таблиця 8

№ п/п	Найменування	Од. вимір	Кіль-кість	Термін підтримки
1	**Віртуальний пристрій FortiAuthenticator-VM with 1100 user license**	шт.	2	не менш ніж 12 міс.
	Примірник програмної продукції для Віртуального пристрою FortiAuthenticator-VM with 1100 user license: FortiAuthenticator - VM License FortiCare Premium Support (1 - 1100 USERS) або еквівалент			

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.

4.7.1. 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-комунікаційних 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

- 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.

4.7.7. 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 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.

4.7.9. 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.

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

Таблиця 9

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки
1	**Система захисту FortiSandbox-VM**	шт.	4	

	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			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 антівірусного 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.

4.8.1. 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-комунікаційних 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

- 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.

4.8.7. 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 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.

4.8.9. 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.

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

Таблиця 10

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки
1	**Система захисту FortiMail-VM**	шт.	2	не менш ніж 12 міс.
	Примірник програмної продукції для Системи захисту FortiMail -VM: FortiMail-VM02 FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract або еквівалент			

Програмна продукція для існуючої системи захисту FortiMail-VM, яка складається з двох підсистем FortiMail-VM, 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;
- 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.

4.9.1. 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-комунікаційних 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

- 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.

4.9.7. 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 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.

4.9.9. 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.

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

Таблиця 11

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки
1	**Система захисту Fortinet FortiWeb-VM**	шт.	2	не менш ніж 12 міс.
	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			

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.

4.10.1. 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-комунікаційних 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

- 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.

4.10.7. 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 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.

4.10.9. 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.

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

Таблиця 12

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки
1	**Система FAD-100F Application Delivery Controller**	шт.	2	не менш ніж 12 міс.
	Примірник програмної продукції для Системи FAD-100F Application Delivery Controller:			

	FortiADC-100F 1 Year Network Security - IP Reputation and Geo-IP, AV, IPS, and FortiCare Premium або еквівалент			

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.

4.11.1. 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-комунікаційних 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

- 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.

4.11.7. 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 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.

4.11.9. 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.

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

Таблиця 13

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки
1	**Система моніторингу та контролю безпеки FortiAnalyzer FAZ- 3700G**	шт.	1	не менш ніж 12 міс.
	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			

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 ПП 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.

4.12.1. 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-комунікаційних 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

- 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.

4.12.7. 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 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.

4.12.9. 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.

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

Таблиця 14

№ п/п	Найменування	Од. виміру	Кіль-кість	Термін підтримки
1	**Віртуальний пристрій FortiEMS-VM with 500 user license**	шт.	1	не менш ніж 12 міс.
	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			

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 ПП 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.

4.13.1. 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-комунікаційних 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

- 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.

4.13.7. 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 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.

4.13.9. 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 ПП у кабінеті адміністратора на порталі виробника.
- Документ, який підтверджує реєстрацію у файлі формату *.pdf та на паперовому носії.
- Активація ліцензійної програмної продукції - здійснюється датою наступною від закінчення попереднього терміну ліцензування

5.3. Вимоги до гарантійної підтримки

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

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 5
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 «03» лютого 2026 року

ПРИСУТНІ:

Члени робочої групи:
А. Бухта
А. Жежера
Н. Йожиков
М. Клюєва
О. Поліщук
С. Осіпов
Т. Самойленко

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 «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 «Розвиток комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми) у частині окремих локацій вулично-транспортної мережі міста;

1.2. проєкт технічних вимог до закупівлі «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 «Розвиток комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми) у частині закладів освіти;

1.3. проєкт технічних вимог до закупівлі «Модернізація інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» у частині створення послуг (сервісів) для подання, обліку та опрацювання заяв на послуги «Оздоровлення та відпочинок дітей віком від 7 до 18 років», «Зарахування дитини до дитячо-юнацької спортивної школи (ДЮСШ)», отримання довідок та технічних

паспортів від КП КМР «Київське міське бюро технічної інвентаризації» та модернізації послуги (сервісу) «Оздоровлення дітей у супроводі дорослого» (пункт 6.1 «Створення, розвиток, впровадження та модернізація цифрових сервісів, систем та реєстрів даних» переліку завдань і заходів Програми);

1.4. 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);

1.5. проєкт технічних вимог до закупівлі «Послуга з супроводу та технічної підтримки комплексної системи відеоспостереження (засобів відеоспостереження «КАСКАД»)» (пункт 6.4 «Супровід, проведення ремонтів, обслуговування та технічна підтримка мережевої інфраструктури, сервісної мережевої інфраструктури, інфраструктури обробки даних, платформи Інтернету речей (IoT), мереж доступу, радіомереж, систем отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку, комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, систем моніторингу та кібербезпеки міських сервісів, інформаційно-комунікаційних, інформаційних (автоматизованих), електронних комунікаційних систем, платформ, вебпорталів та сервісів, обладнання, технічних засобів, модулів, програмно-апаратних комплексів, програмного забезпечення, ліцензій» переліку завдань і заходів Програми);

1.6. проєкт технічних вимог до закупівлі «Послуга з супроводу та технічної підтримки комплексної системи відеоспостереження міста Києва» (пункт 6.4 «Супровід, проведення ремонтів, обслуговування та технічна підтримка мережевої інфраструктури, сервісної мережевої інфраструктури, інфраструктури обробки даних, платформи Інтернету речей (IoT), мереж доступу, радіомереж, систем отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку, комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, систем моніторингу та кібербезпеки міських сервісів, інформаційно-комунікаційних, інформаційних (автоматизованих), електронних комунікаційних систем, платформ, вебпорталів та сервісів, обладнання, технічних засобів, модулів, програмно-апаратних комплексів, програмного забезпечення, ліцензій» переліку завдань і заходів Програми).

2. Різне.

По пунктах 1.1 -1.2 питання 1

СЛУХАЛИ:

С. Осіпова, який поінформував, що з метою запобігання виникненню надзвичайних ситуацій та ліквідації їх наслідків, а також підвищення рівня

безпеки громадян, протидії злочинності, забезпечення публічної безпеки на території міста Києва шляхом розширення зони контрольованого покриття системами відеоспостереження транспортної мережі міста Києва та території закладів освіти є необхідність закупівлі комплектів засобів для встановлення та підключення їх до комплексної системи відеоспостереження міста Києва та представив два проєкти технічних вимог до закупівель «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 переліку завдань і заходів Програми).

В обговоренні проєктів технічних вимог брали участь: О. Поліщук, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури двох закупівель «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 переліку завдань і заходів Програми) використовувати проєкти технічних вимог, розглянуті на засіданні робочої групи.

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

По пункту 1.3 питання 1

СЛУХАЛИ:

А. Жежеру, який поінформував про модернізацію та удосконалення функціональних можливостей інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» щодо створення електронних послуг «Оздоровлення та відпочинок дітей віком від 7 до 18 років», «Зарахування дитини до дитячо-юнацької спортивної школи (ДЮСШ)», подання заяв на отримання довідок та технічних паспортів від КП КМР «Київське міське бюро технічної інвентаризації», модернізації електронної послуги «Оздоровлення дітей у супроводі дорослого», налаштування електронної інформаційної взаємодії із зовнішньою інформаційною системою Єдиний державний вебпортал електронних послуг та автоматизованою системою взаємозв'язків між учасниками освітнього процесу та спортивної діяльності в місті Києві та представив технічні вимоги до закупівлі «Модернізація інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» у частині створення послуг (сервісів) для подання, обліку та опрацювання заяв на послуги «Оздоровлення та відпочинок дітей віком від 7 до 18 років», «Зарахування дитини до дитячо-юнацької спортивної школи (ДЮСШ)», отримання довідок та технічних паспортів від КП КМР «Київське міське бюро технічної інвентаризації» та модернізації послуги (сервісу) «Оздоровлення дітей у супроводі дорослого» (пункт 6.1 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: С. Осіпов, О. Поліщук, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Головний інформаційно-обчислювальний центр» під час процедури закупівлі «Модернізація інформаційно-комунікаційної системи «Програмна платформа для надання електронних послуг, у тому числі адміністративних» у частині створення послуг (сервісів) для подання, обліку та опрацювання заяв на послуги «Оздоровлення та відпочинок дітей віком від 7 до 18 років», «Зарахування дитини до дитячо-юнацької спортивної школи (ДЮСШ)», отримання довідок та технічних паспортів від КП КМР «Київське міське бюро технічної інвентаризації» та модернізації послуги (сервісу) «Оздоровлення дітей у супроводі дорослого» (пункт 6.1 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По пункту 1.4 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував, що для забезпечення належного рівня захисту від інформаційних загроз систем міської мережевої інфраструктури необхідно забезпечити доступ до оновлень компонентів системи захисту на обладнанні Fortinet та представив проєкт технічних вимог до закупівлі «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури» (пункт 6.2 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: С. Осіпов, 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) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По пункту 1.5 питання 1

СЛУХАЛИ:

С. Осіпова, який поінформував, що для створення безпечного середовища в місті Києві необхідно забезпечувати супровід і технічну підтримку засобів

відеоспостереження «КАСКАД» (комплексів автоматичної фото/відеофіксації правопорушень у сфері безпеки дорожнього руху, у складі реєстраційного та телекомунікаційного блоків) та представив проєкт технічних вимог до закупівлі «Послуга з супроводу та технічної підтримки комплексної системи відеоспостереження (засобів відеоспостереження «КАСКАД»)» (пункт 6.4 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: О. Поліщук, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури закупівлі «Послуга з супроводу та технічної підтримки комплексної системи відеоспостереження (засобів відеоспостереження «КАСКАД»)» (пункт 6.4 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По підпункту 1.6 питання 1

СЛУХАЛИ:

С. Осіпова, який поінформував, що для створення безпечного середовища в місті Києві необхідно забезпечувати супровід і технічну підтримку комплексної системи відеоспостереження міста Києва в частині засобів відеофіксації (засобів зв'язку (відеозв'язку/відеофіксації)) та супутнього обладнання, розміщених на території освітніх закладів, та представив проєкт технічних вимог до закупівлі «Послуга з супроводу та технічної підтримки комплексної системи відеоспостереження міста Києва» (пункт 6.4 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: О. Поліщук, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури закупівлі «Послуга з супроводу та технічної підтримки комплексної системи відеоспостереження міста Києва» (пункт 6.4 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-265
Дата реєстрації 03.02.2026
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Материали засідання робочої групи 03.02.2026 (Протокол № 5 від 03.02.2026)

Кількість файлів: 7
Кількість ЕП: 49

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
03.02.2026 № 075-265

Перелік електронних підписів

П.І.Б.	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 7	04.02.2026 12:15:04 ; 04.02.2026 12:15:05 ; 04.02.2026 12:15:07 ; 04.02.2026 12:15:09 ; 04.02.2026 12:15:10 ; 04.02.2026 12:15:11 ; 04.02.2026 12:15:13 ;	04.02.2026 12:15:13 Погодив;	04.02.2026 12:15:13 Погодив
Бухта Андрій Миколайович **Кількість ЕП:** 7	04.02.2026 08:33:47 ; 04.02.2026 08:33:48 ; 04.02.2026 08:33:49 ; 04.02.2026 08:33:49 ; 04.02.2026 08:33:50 ; 04.02.2026 08:33:51 ; 04.02.2026 08:33:52 ;	04.02.2026 08:33:53 Погодив;	04.02.2026 08:33:52
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 7	03.02.2026 17:05:54 ; 03.02.2026 17:05:55 ; 03.02.2026 17:05:56 ; 03.02.2026 17:05:57 ; 03.02.2026 17:05:59 ; 03.02.2026 17:06:00 ; 03.02.2026 17:06:01 ;	03.02.2026 17:06:01 Погодив;	03.02.2026 17:06:01 Погодив
Поліщук Олег Федорович **Кількість ЕП:** 7	03.02.2026 17:01:43 ; 03.02.2026 17:01:45 ; 03.02.2026 17:01:46 ; 03.02.2026 17:01:47 ; 03.02.2026 17:01:48 ; 03.02.2026 17:01:49 ; 03.02.2026 17:01:50 ;	03.02.2026 17:01:50 Погодив;	03.02.2026 17:01:50 Погодив
Йожиков Нікіта Сергійович **Кількість ЕП:** 7	03.02.2026 16:33:37 ; 03.02.2026 16:33:38 ; 03.02.2026 16:33:38 ; 03.02.2026 16:33:39 ; 03.02.2026 16:33:40 ; 03.02.2026 16:33:41 ;	03.02.2026 16:33:42 Погодив;	03.02.2026 16:33:42 Погодив

	03.02.2026 16:33:42 ;		
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 7	03.02.2026 16:00:38 ; 03.02.2026 16:00:39 ; 03.02.2026 16:00:39 ; 03.02.2026 16:00:40 ; 03.02.2026 16:00:41 ; 03.02.2026 16:00:42 ; 03.02.2026 16:00:44 ;	03.02.2026 16:00:44 Погодив;	03.02.2026 16:00:44 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 7	03.02.2026 15:57:37 ; 03.02.2026 15:57:38 ; 03.02.2026 15:57:38 ; 03.02.2026 15:57:39 ; 03.02.2026 15:57:40 ; 03.02.2026 15:57:40 ; 03.02.2026 15:57:41 ;	03.02.2026 15:57:41 Погодив;	03.02.2026 15:57:41 Погодив

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**

ALESTA

ТОВ «АЛЕСТА»
ЄДРПОУ 42232756 | **ІПН** 422327526530
alesta.ua | info@alesta.ua | +380 44 377 73 11
01135, Україна, Київ, вул. Дмитрівська 66а, офіс 65

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/197
Від 19.02. 2026 р.

В.о. директора
СКП "КИЇВТЕЛЕСЕРВІС"
Олександру ВОЛОЩУКУ

Комерційна пропозиція

ТОВ «АЛЕСТА» вдячне Вам за можливість взяти участь у 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» та у відповідь на ваш запит 075/2-262 від 18.02.2026 надає до розгляду наступну пропозицію:

№	Назва / опис	К-ть	Ціна за од. (грн без ПДВ)	Сума (грн без 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).	2	952 326,00	1 904 652,00
2	**Мережевий екран FortiGate FG-3000D** Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D : FortiGate-3000D 1 Year FortiCare Premium Support.	2	657 268,00	1 314 536,00
3	Примірник програмної продукції для Мережевого екрану FortiGate FG-3000D : FortiGate-3000D 1 Year FortiGuard URL, DNS & Video Filtering Service.	2	985 903,00	1 971 806,00
4	**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).	4	218 703,00	874 812,00
5	**Мережевий екран FortiGate FG-80F** Примірник програмної продукції для Мережевого екрану FortiGate FG-80F : FortiGate-80F 1 Year FortiCare Essential Support.	43	12 933,00	556 119,00
6	**Мережевий екран FortiGate FG-40F** Примірник програмної продукції для Мережевого екрану FortiGate FG-40F : FortiGate-40F 1 Year FortiCare Essential Support.	431	4 184,00	1 803 304,00
7	**Система керування FortiManager FMG-VM with 450 device license** Примірник програмної продукції для Системи керування FortiManager FMG-VM with 540 device license: FortiManager - VM FortiCare Premium Support FortiCare Premium Support (1 - 1010 devices/Virtual Domains) .	1	1 058 347,00	1 058 347,00
8	**Віртуальний пристрій FortiAuthenticator-VM with 1100 user license** Примірник програмної продукції для Віртуального пристрою FortiAuthenticator-VM	2	86 899,00	173 798,00

ALESTA

ТОВ «АЛЕСТА»
ЄДРПОУ 42232756 | **ІПН** 422327526530
alesta.ua | info@alesta.ua | +380 44 377 73 11
01135, Україна, Київ, вул. Дмитрівська 66а, офіс 65

	with 1100 user license: FortiAuthenticator - VM License FortiCare Premium Support (1 - 1100 USERS).			
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.	4	317 325,00	1 269 300,00
10	**Система захисту FortiMail-VM** Примірник програмної продукції для Системи захисту FortiMail -VM: FortiMail-VM02 FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract.	2	359 167,00	718 334,00
11	**Система захисту Fortinet FortiWeb-VM** 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).	2	1 122 648,00	2 245 296,00
12	**Система FAD-100F Application Delivery Controller** Примірник програмної продукції для Системи FAD-100F Application Delivery Controller: FortiADC-100F 1 Year Network Security - IP Reputation and Geo-IP, AV, IPS, and FortiCare Premium.	2	116 091,00	232 182,00
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).	1	9 624 025,00	9 624 025,00
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.	1	568 058,00	568 058,00
			Разом (грн без ПДВ)	**24 314 569,00**
			ПДВ (грн)	**4 862 913,80**
			Разом (грн з ПДВ)	**29 177 482,80**

Термін підтримки – 12 місяців

19.02.2026 року
Директор ТОВ «АЛЕСТА» Анатолій БЛІНОВ

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 12:20:26 19.02.2026

Назва файлу з підписом: Алеста_пропозиція.pdf.p7s
Розмір файлу з підписом: 18.4 КБ

Перевірені файли:
Назва файлу без підпису: Алеста_пропозиція.pdf
Розмір файлу без підпису: 128.6 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Блінов Анатолій Анатолійович
П.І.Б.: Блінов Анатолій Анатолійович
Країна: Україна
РНОКПП: 2771400236
Організація (установа): Товариство з обмеженою відповідальністю "АЛЕСТА"
Код ЄДРПОУ: 42232756
Посада: директор
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 12:20:25 19.02.2026
Сертифікат виданий: КНЕДП ТОВ "Центр сертифікації ключів "Україна"
Серійний номер: 340A32080000000000000000000000000000000001
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в окремих файлах (CAdES detached)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.08.25 13:00

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№ 021826/3 від 18.02.2026
На № 075/2-242 від 16.02.2026

Спеціалізованому комунальному підприємству «Київтелесервіс»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Товариство з обмеженою відповідальністю «ОПТІДАТА» надає комерційну пропозицію, у відповідь на Ваш запит, стосовно закупівлі «Підтримка програмної продукції для підсистем захисту міської мережевої інфраструктури».

№	Найменування засобів зв'язку	Кіль-кість	Од. вим.	Ціна грн без ПДВ	Сума, грн без ПДВ
1	Програмна продукція FortiGate-1000D 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	2	шт	955 621,50	1 911 243,00
2	Програмна продукція FortiGate-3000D 1 Year FortiCare Premium Support	2	шт	659 542,50	1 319 085,00
3	Програмна продукція FortiGate-3000D 1 Year FortiGuard URL, DNS & Video Filtering Service	2	шт	989 314,00	1 978 628,00
4	Програмна продукція FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	4	шт	219 459,50	877 838,00
5	Програмна продукція FortiGate-80F 1 Year FortiCare Essential Support	43	шт	12 978,00	558 054,00
6	Програмна продукція FortiGate-40F 1 Year FortiCare Essential Support	431	шт	4 199,00	1 809 769,00
7	Програмна продукція FortiManager - VM FortiCare Premium Support 1 Year FortiCare Premium Support (1 - 1010 devices/Virtual Domains)	1	шт	1 062 009,00	1 062 009,00
8	Програмна продукція FortiAuthenticator - VM License 1 Year FortiCare Premium Support (1 - 1100 USERS)	2	шт	87 200,00	174 400,00
9	Програмна продукція FortiSandbox VM00 1 Year Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial	4	шт	318 423,00	1 273 692,00

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

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

	Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs.				
10	Програмна продукція FortiMail-VM02 1 Year FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract	2	шт	360 410,00	720 820,00
11	Програмна продукція FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)	2	шт	1 126 532,50	2 253 065,00
12	Програмна продукція FortiADC-100F 1 Year Network Security - IP Reputation and Geo-IP, AV, IPS, and FortiCare Premium	2	шт	116 493,00	232 986,00
13	Програмна продукція FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, FortiTIP SaaS Extension, and FortiGuard Outbreak Service)	1	шт	9 657 326,50	9 657 326,50
14	Програмна продукція 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.	1	шт	570 024,00	570 024,00
Сума, грн без ПДВ:					**24 398 939,50**
ПДВ:					**4 879 787,90**
Сума, грн з ПДВ:					**29 278 727,40**

З повагою,
Генеральний директор
ТОВ «ОПТІДАТА»

Україна * Київська обл. * м. Біла Церква * ТОВ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ОПТІДАТА» Ідентифікаційний код 39693067

Білик М.А.

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

ТОВ «ВІ ЄМ ДЖІ»
ЄДРПОУ 40844268
+380 96 001 01 61
info@wmgroup.com.ua
wmgroup.com.ua

18/02/26 вих 12

КТС

Комерційна Пропозиція

Компанія "ВІ ЄМ ДЖІ" вдячна Вам за довіру та проявлений інтерес до нашої продукції. Отримавши Ваш запит, ми готові надати Вам повний спектр IT-послуг на самих вигідних для Вас умовах. Нижче пропонуємо Вашій увазі пропозицію згідно Ваших технічних вимог:

№ з/п	Найменування	Од. вим.	Кіль - кість	Ціна грн з ПДВ	Сума, грн з ПДВ
1	Примірник ПЗ 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	1 159 926,72	2 319 853,44
2	Примірник ПЗ FortiGate-3000D 1 Year FortiCare Premium Support	шт	2	800 548,32	1 601 096,64
3	Примірник ПЗ FortiGate-3000D 1 Year FortiGuard URL, DNS & Video Filtering Service	шт	2	1 200 822,48	2 401 644,96
4	Примірник ПЗ FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	шт	4	266 378,16	1 065 512,64
5	Примірник ПЗ FortiGate-80F 1 Year	шт	43	15 752,88	677 373,84

	FortiCare Essential Support				
6	Примірник ПЗ FortiGate-40F 1 Year FortiCare Essential Support	шт	431	5 096,52	2 196 600,12
7	Примірник ПЗ FortiManager - VM FortiCare Premium Support 1 Year FortiCare Premium Support (1 - 1010 devices/Virtual Domains)	шт	1	1 289 059,20	1 289 059,20
8	Примірник ПЗ FortiAuthenticator - VM License 1 Year FortiCare Premium Support (1 - 1100 USERS)	шт	2	105 842,88	211 685,76
9	Примірник ПЗ 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	386 499,48	1 545 997,92
10	Примірник ПЗ FortiMail-VM02 1 Year FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract	шт	2	437 463,36	874 926,72
11	Примірник ПЗ FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)	шт	2	1 367 377,44	2 734 754,88
12	Примірник ПЗ FortiADC-100F 1 Year Network Security - IP Reputation and Geo-IP,	шт	2	141 398,40	282 796,80

	AV, IPS, and FortiCare Premium				
3 1	Примірник ПЗ FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, FortiTIP SaaS Extension, and FortiGuard Outbreak Service)	шт	1	11 721 996,00	11 721 996,00
4 1	Примірник ПЗ 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	691 891,20	691 891,20

Разом, грн з ПДВ: **29 615 190,12**

З повагою. Комерційний директор ТОВ «ВІ ЄМ ДЖІ» **Комар О.Л**

ESKA your ITeam

Комерційна пропозиція на постачання Fortinet

Спеціалізоване комунальне підприємство «Київтелесервіс»

20.02.2026 р.

SKU	Description	Q-ty	Price	Total
FC2-10-0ACVM-248-02-12	FortiAuthenticator - VM License 1 Year FortiCare Premium Support (1 - 1100 USERS)	2	$2 405,52	$4 811,04
FC-10-A100F-730-02-12	FortiADC-100F 1 Year Network Security - IP Reputation and Geo-IP, AV, IPS, and FortiCare Premium	2	$3 213,60	$6 427,20
FC-10-0VM02-643-02-12	FortiMail-VM02 1 Year FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract	2	$9 942,35	$19 884,70
FC-10-F200F-950-02-12	FortiGate-200F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	4	$6 054,05	$24 216,20
FC-10-01006-950-02-12	FortiGate-1000D 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	2	$26 361,97	$52 723,94
FC-10-0040F-314-02-12	FortiGate-40F 1 Year FortiCare Essential Support	431	$115,83	$49 922,73
FC-10-0080F-314-02-12	FortiGate-80F 1 Year FortiCare Essential Support	43	$358,02	$15 394,86
FC-10-L3K7G-1263-02-12	FortiAnalyzer-3700G 1 Year Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, FortiTIP SaaS Extension, and FortiGuard Outbreak Service)	1	$266 409,00	$266 409,00
FC4-10-M3004-248-02-12	FortiManager - VM FortiCare Premium Support 1 Year FortiCare Premium Support (1 - 1010 devices/Virtual Domains)	1	$29 296,80	$29 296,80
FC-10-FSV00-500-02-12	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.	4	$8 784,08	$35 136,32
FC-10-VVM08-936-02-12	FortiWeb-VM08 1 Year Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)	2	$31 076,76	$62 153,52
FC-10-03007-247-02-12	FortiGate-3000D 1 Year FortiCare Premium Support	2	$18 194,28	$36 388,56
FC2-10-EMS04-429-01-12	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.	1	$15 724,80	$15 724,80
FC-10-03007-112-02-12	FortiGate-3000D 1 Year FortiGuard URL, DNS & Video Filtering Service	2	$27 291,42	$54 582,84
				$673 072,51

29 177 695,31

Ціна вказа в доларах США з ПДВ, термін постачання 5-10 робочих днів

Курс розрахунку 43.35

Директор ТОВ «ЕСКА-СОФТ»

І.В. Скрипка

ЕСКА-СОФТ
ідентифікаційний код 38507604

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 045/2/102
Від 20.02. 2026 р.