Технічні, якісні та кількісні характеристики
«Впровадження телеметричного програмного комплексу IoT»

Зміст

1. АНОТАЦІЯ 3

2. ПЕРЕЛІК ВИЗНАЧЕНЬ ТА СКОРОЧЕНЬ 4

3. АКТУАЛЬНІСТЬ 6

4. МЕТА ТА ПРИЗНАЧЕННЯ 7

5. ЗАГАЛЬНІ ВИМОГИ ДО ТЕЛЕМЕТРИЧНОЇ IoT-ПЛАТФОРМИ 9

6. ВИМОГИ ДО АРХІТЕКТУРИ ТЕЛЕМЕТРИЧНОЇ IoT-ПЛАТФОРМИ 11

7. ВИМОГИ ДО ПРОГРАМНИХ МОДУЛІВ ТЕЛЕМЕТРИЧНОЇ IoT-ПЛАТФОРМИ 12

7.1. Модуль прийому даних 12

7.1.1 Модуль прийому даних NB-IoT, GSM/GPRS 12

7.1.2 Модуль прийому даних LoRaWAN 13

7.2. Модуль обробки та фільтрації даних 14

7.3. Модуль репозиторію 16

7.4. Модуль зберігання даних 17

7.5. Модуль аналітики та візуалізації 17

7.6. Геоінформаційний модуль 19

7.7. Модуль подій 20

7.8. Модуль сповіщень та повідомлень 20

7.9. Модуль асинхронних завдань 20

7.10. Модуль інтеграції 21

7.11. Модуль безпеки та автентифікації 21

8. СХЕМА РОЗГОРТАННЯ 22

9. ВИМОГИ ДО ЗАХИСТУ ІНФОРМАЦІЇ 24

10. ВИМОГИ ДО ДОКУМЕНТАЦІЇ 26

11. ТЕХНІЧНІ ВИМОГИ ДО АПАРАТНОЇ ЧАСТИНИ 27

11.1. Вимоги до мережевого пристрою безпеки (NGFW) ..... **Error! Bookmark not defined.**

11.2. Вимоги до системи централізованого збору та аналізу журнальних файлів (віртуалізоване рішення) ..... **Error! Bookmark not defined.**

11.3. Вимоги до програмного забезпечення системи захисту веб-сервісів (віртуалізоване рішення) ..... **Error! Bookmark not defined.**

1. АНОТАЦІЯ

Цей документ є технічними вимогами на впровадження телеметричного програмного комплексу IoT, яка містить набір технологічних інструментів для збору, аналізу, обробки, зберігання телеметричних даних зі спеціалізованого обладнання (цифрові датчики, сенсори, лічильники та інші пристрої обліку та вимірювання), побудови на базі програмного комплексу системи автоматизованого обліку газу та телеметричного контролю системи транспортування газу з метою забезпечення моніторингу споживання газу в режимі реального часу.

Документ визначає загальні функціональні та технічні вимоги до програмного комплексу та її модулів.

Перелік задач в технічних вимогах не є вичерпним та може бути уточненим в процесі побудови програмного комплексу відповідно до потреб Замовника.

2. ПЕРЕЛІК ВИЗНАЧЕНЬ ТА СКОРОЧЕНЬ

У цьому документі терміни та скорочення викладені в наступному значенні:

IoT-платформа (далі – платформа) – програмно-телеметрична платформа, програмний комплекс, що містить набір технологічних інструментів для збору, аналізу, обробки, зберігання даних з необхідних цифрових датчиків, сенсорів, лічильників, пристроїв перетворення об’єму та інші пристрої обліку та вимірювання.

Адміністрування – інструмент для додавання, редагування та налаштування прав доступу, керування користувачами та об‘єктами спостереження (обладнанням).

ПЗ (програмне забезпечення) – клієнт-серверне програмне забезпечення, яке складається з бази даних та серверного програмного забезпечення, яке дозволяє отримувати, обробляти, зберігати дані, отримані від обладнання у базі даних; здійснювати моніторинг даних від обладнання та відправки команд до обладнання за допомогою веб-інтерфейсу системи.

База даних – центральне сховище даних, у якому зберігаються всі дані, отримані від обладнання та інші сутності програмного забезпечення системи.

Сервер – віддалений комп'ютер, розміщений у фізичному чи віртуалізованому середовищі ІТ-інфраструктури Замовника, призначений для розміщення бази даних, серверного програмного забезпечення та веб-інтерфейсу, до якого звертаються користувачі системи.

Веб-інтерфейс – елемент програмного забезпечення системи, який за допомогою веб-браузеру та мережі Інтернет надає можливість користувачам здійснювати моніторинг даних.

Вузол обліку природного газу/вузол обліку/ВОГ – сукупність засобів вимірювальної техніки, зокрема лічильник газу або звужуючий пристрій, та допоміжних засобів, призначених для вимірювання, реєстрації результатів вимірювання та розрахунків об’єму природного газу, зведених до стандартних умов, визначених законодавство

API – інтерфейс програмного забезпечення системи, що використовується для передачі даних з бази даних до веб-інтерфейсу, або у сторонні системи та сервіси.

Користувач – визначений працівник Замовника, який може взаємодіяти із програмним забезпеченням через веб-інтерфейс та/або програмного забезпечення, встановленого на операційних системах мобільних застосунків.

Адміністратор – користувач із розширеними правами доступу, який забезпечує технічний та технологічний супровід програмного забезпечення системи.

ГРМ (газорозподільні мережі) – виробничий комплекс, що складається з організаційно і технологічно пов’язаних між собою об’єктів, призначених для розподілу природного газу від газорозподільних станцій безпосередньо споживачам.

ЕХЗ - електрохімічний захист, використовується для захисту трубопроводу від підземної корозії.

ПРГ (пункт редукування природного газу) **—** комплекс обладнання для зниження тиску природного газу та підтримання його на заданому рівні, а саме: газорегуляторний пункт, газорегуляторний пункт блоковий, шафовий газорегуляторний пункт, газорегуляторна установка, підземний газорегуляторний пункт.

Пристрої – датчики, сенсори, лічильники, пристроїв перетворення об’єму та інші пристрої обліку та вимірювання.

Білий список – перелік пристроїв з серійними номерами, зазначенням типу пристрою та збереженням ключів шифрування, якщо пристрій використовує шифрування інформації.

"В режимі, наближеному до реального часу" - означає, що процес або система працює з мінімальною затримкою, максимально наближеною до миттєвої реакції. Це дозволяє отримувати результати або здійснювати дії майже одразу після їхнього запуску, затримка залежить від технології передачі даних та налаштування обладнання.

СКБД - набір взаємопов'язаних даних (база даних) і програм для доступу до цих даних. Надає можливості створення, збереження, оновлення та пошуку інформації в базах даних з контролем доступу до даних.

SDK - набір із засобів розробки, утиліт і документації, який дає програмістам змогу створювати прикладні програми за визначеною технологією або для певної платформи (програмної або програмно-апаратної).

3. АКТУАЛЬНІСТЬ

В умовах зростаючої потреби в ефективності та безпеці ГРМ значно збільшилася необхідність у уніфікованому зборі, консолідації та отриманні інформації про облік споживаного газу «в режимі, наближеному до реального часу». Наразі відповідні дані або не збираються зовсім, або ведуться вручну, що підвищує ризик впливу людського фактору, нівелюючи релевантність та актуальність інформації. Галузь гостро потребує впровадження єдиного програмного рішення для збору, управління, обробки та аналізу таких даних, що дозволить приймати обґрунтовані управлінські рішення на основі актуальної, об'єктивної та оперативної інформації.

Беручи до уваги тенденцій щодо впровадження нових технологічних рішень на базі телеметричних IoT-систем, зазначене питання набуває особливого значення в різних сферах промисловості. Газорозподільна система (далі - ГРМ) потребує застосування та впровадження сучасних систем телеметрії на базі IoT для підвищення безпеки, підтримання ГРМ в належному стані, покращення якості послуг для споживачів, зниження операційних витрат підприємств та покращення екологічної ситуації в навколишньому середовищі.

4. МЕТА ТА ПРИЗНАЧЕННЯ

Метою є створення та впровадження телеметричного програмного комплексу IoT для побудови загальної автоматизованої системи обліку газу та контролю ГРМ з уніфікованою взаємодією спеціалізованих пристроїв та цифрових елементів (цифрових датчиків, сенсорів, лічильників, пристроїв перетворення об’єму та інші пристроїв обліку та вимірювання) з програмними комплексом, а також реалізація завдань з організації обміну даними між автоматизованими системами, програмними додатками з метою збору, консолідації та управління даними в онлайн режимі, контроль використання активів без необхідності ручного введення, коригування інформації та даних, що дозволить дистанційно збирати та обробляти дані про споживання газу, електроенергії, зменшуючи залежність від ручної праці, скоротити технологічні та комерційні втрати, а також підвищити точність і надійність обліку.

Призначення: першочергово, на базі програмного комплексу IoT має відбутися впровадження та налаштування системи автоматизованого обліку газу та електроенергії з метою забезпечення моніторингу споживання ресурсів в режимі реального часу, оперування об'єктивними даними про обсяги споживання, створення відповідних умов для забезпечення оперативного інформування про позаштатні події в ГРМ та вчасне реагування на будь-які відхилення від нормальної роботи. Наразі збір інформації у більшості випадків відбувається вручну, що не виключає можливості допущення похибок та має безпосередній вплив на актуальність та достовірність інформації.

Впровадження системи автоматизованого обліку газу на базі IoT-платформи повинно дозволити:

- відслідковувати споживання газу онлайн, що дасть можливість оперативного реагування на особливості в споживанні, виявляти витоки, або несанкціоноване використання газу, невідповідну роботу ВОГ, отримувати актуальну інформацію зі зменшенням можливого впливу людського фактору та своєчасного прийняття управлінські рішення, що призведе до зниження втрат та підвищення ефективності;
- проводити аналітичні дослідження, з метою виявляти недоліки в роботі , ГРМ оптимізувати навантаження на мережу, планувати ремонти та модернізацію, а також прогнозувати споживання для кращого планування ресурсів;

- підвищити надійність та безпеку ГРМ шляхом своєчасного виявлення та усунення аварійних ситуацій, що зменшить ризики для споживачів та навколишнього середовища;
- забезпечити можливість інтеграції даних з внутрішніми веб-сервісами та системами, у тому числі для інформування споживачів про стан ГРМ , надання їм доступу до власних даних про споживання та можливість оптимізації витрат.

5. ЗАГАЛЬНІ ВИМОГИ ДО ТЕЛЕМЕТРИЧНОЇ IoT-ПЛАТФОРМИ

Платформа повинна забезпечувати обмін даними між програмними комплексами та їх складовими, включаючи різноманітні інтерфейси апаратних та програмних модулів спеціалізованого обладнання (цифрові датчики, сенсори, лічильники, пристрої перетворення об’єму тощо) та складатися з набору програмних модулів або підсистем для автоматизації виробничих процесів відповідно до потреб.

Платформа має дозволяти побудови єдиного програмного комплексу з можливим горизонтальним масштабуванням в тому числі у віртуальному обчислювальному середовищі з можливістю підтримки різних технологій та СКБД. Забезпечувати роботу платформи в режимі 24/7 з можливістю масштабування без змін програмних модулів, налаштувань клієнтів та тривалих зупинок сервісів. Бути сумісною з розповсюдженими системами керування базами даних (MS SQL Server, Oracle Database, PostgreSQL тощо) та можливість використання інших БД за вибором замовника.

Для забезпечення таких можливостей до складу платформи мають бути включені клієнтські бібліотеки (SDK) та засоби розробки для подальшого самостійного розвитку, налаштування програмного продукту та можливість інтеграції з іншими інформаційним системами Замовника.

Одною з базових вимог – наявність інструментів бездротового прийому/передача даних та взаємодія об'єктів платформи шляхом створення єдиної мережі унікально ідентифікованих об'єктів використовуючи розповсюджені протоколи зв'язку такі як: NB-IoT, LoRaWAN, GSM/GPRS для забезпечення передачі даних у реальному часі з можливістю підтримки функції двостороннього зв'язку для віддаленого керування та оновлення програмного забезпечення пристроїв IoT.

Таким чином забезпечувати масштабність прийому даних з великої кількості (не менше 10 мільйонів) пристроїв через API платформи.

Платформа має містити реалізовані алгоритми логічної обробки отриманої інформації з пристроїв використовуючи власні математичні фільтри та інструменти їх налаштування, мати сервіси операційного аналізу даних: відображення процесів у реальному часі, побудова графіків, пошук у журналі даних, порівняння даних з різних джерел, застосування фільтрів до вхідних даних тощо

Можливість інтеграції різного обладнання за наявності протоколу передачі даних.

Програмний комплекс повинен бути розширюваним з можливістю інтегрування нових модулів, як із залученням розробника так і силами Замовника , використовуючи вбудовану середу розробки. Постачання програмного забезпечення IoT-платформи в межах цієї закупівлі має передбачати надання безстрокової невиключної ліцензії серверної частини програмного забезпечення з підтримкою необмеженої кількості підключень датчиків/сенсорів та необмеженої кількості користувачів.

Також постачання програмного забезпечення IoT-платформи в межах цієї закупівлі передбачає передачу вихідного коду: приймання, обробки, аналітики, безпеки, інтеграцій що є необхідним для забезпечення умов щодо можливого подальшого самостійного розвитку та забезпечення необхідного рівня конфіденційності та подальшого кіберзахисту функціонування програмного забезпечення.

6. ВИМОГИ ДО АРХІТЕКТУРИ ТЕЛЕМЕТРИЧНОЇ IoT-ПЛАТФОРМИ

Архітектура телеметричної IoT-платформи має відповідати наступним вимогам:

1. Мати сервіс-орієнтовану архітектура (SOA):
   - програмні модулі повинні бути побудовані на принципах SOA, для забезпечення гнучкості, масштабованості та можливості повторного використання компонентів;
   - реалізація взаємодії між розподіленими програмними підсистемами та клієнтськими додатками через стандартизовані сервіси.
2. Наявність документованих SDK/API для інтеграції. Кожен програмний модуль платформи повинен надавати доступ до своїх сервісів через документовані SDK/API, для реалізації інтеграції з іншими системами та додатками.
3. Безпека доступу та передачі даних:
   - доступ до сервісів модулів повинен вимагати автентифікації та авторизації користувачів;
   - використання тільки захищених з'єднань по HTTPS протоколу для забезпечення конфіденційності та цілісності даних.

7. ВИМОГИ ДО ПРОГРАМНИХ МОДУЛІВ ТЕЛЕМЕТРИЧНОЇ IoT-ПЛАТФОРМИ

Кожен з програмних модулів IoT - платформи має надавати доступ до своїх сервісів для інших програмних підсистем або додатків за допомогою документованих SDK/API. Для забезпечення безпеки, доступ до цих сервісів повинен вимагати автентифікації користувачів та використання захищеного з'єднання по HTTPS протоколу.

7.1. Модуль прийому даних

Модуль прийому даних - приймає дані від різноманітних пристроїв. Підтримує масштабований прийом інформації від пристроїв (можливість горизонтального масштабування).

7.1.1 Модуль прийому даних NB-IoT, GSM/GPRS

Програмний модуль прийому даних для технологій радіозв'язку NB-IoT та GSM/GPRS відповідає за прийом, розшифрування і парсинг даних від ВОГ, ПРГ, ЕХЗ та додаткового обладнання. Модуль отримує «сирі» дані від датчиків і ВОГ, за потреби розшифровує їх, виконує парсинг відповідно до протоколу пристрою та передає оброблені дані до модуля збереження даних.

Модуль прийому даних повинен підтримувати прийом та передачу даних по протоколам:

- TCP
- UDP
- MQTTS
- Modbus TCP

Програмне забезпечення повинно мати змогу додавання нових типів пристроїв з пропрієтарними протоколами, за наявністю протоколів.

Модуль повинен підтримувати додаткові функції пристроїв такі як:

- Синхронізація часу;
- Віддалене внесення налаштувань;
- Видачу квитанцій (стандартних звітів передбачених виробником пристроїв, а також не стандартних звітів на вимогу замовника);
- Оновлення програмного забезпечення датчиків та лічильників (за необхідності).

7.1.2 Модуль прийому даних LoRaWAN

Програмний модуль прийому даних для технологій радіо зв'язку LoRaWAN відповідає за прийом та парсинг даних від сервера керування мережею LoRaWAN. Модуль приймає сирі дані від пристроїв, проводить парсинг у відповідності до протоколу пристрою та передає, оброблені дані, в модуль збереження даних.

Модуль прийому даних повинен підтримувати прийом та передачу даних по протоколам:

- REST API
- gRPC API
- MQTTS

Програмне забезпечення повинно мати змогу додавання нових типів пристроїв з пропрієтарними протоколами.

Модуль повинен підтримувати додаткові функції пристроїв такі як:

- Синхронізація часу
- Віддалене внесення налаштувань
- Видачу квитанцій (стандартних звітів передбачених виробником пристроїв, а також не стандартних звітів на вимогу замовника)

Модуль повинен мати змогу проводити моніторинг мережі LoRaWAN, збираючи дані за допомогою REST API, або gRPC API від сервера керування мережею. Необхідно проводити збір та обробку даних о працездатності базових станцій та мережі LoRaWAN.

7.2. Модуль обробки та фільтрації даних

Модуль забезпечує логічну обробку, каскадну фільтрацію та агрегацію даних, а також застосування математичних фільтрів для обробки даних у режимі реального часу.

Основні функції:

- Обробка даних від пристроїв;
- Контроль лічильників накопичення:
  - виявлення зменшення показників;
  - відкидання некоректних даних;
  - формування повідомлень про помилки;
- Застосування математичних фільтрів;
- Агрегація та нормалізація даних.

Каскадно-кореляційний аналіз тиску:

- Аналізувати дані датчиків тиску на послідовно з’єднаних ПРГ;
- Виконувати кореляційний аналіз змін тиску;
- Визначати, чи належать події до одного інциденту.

Аналіз тиску для закільцьованих мереж:

- Враховувати альтернативні джерела газопостачання;
- Не дублювати події у разі часткового падіння тиску;
- Коректно інтерпретувати відновлення тиску.

Обробка інцидентів:

- Визначати межі інциденту з урахуванням напрямку потоків;
- Об’єднувати пов’язані події в одну логічну подію;
- Запобігати дублюванню повідомлень;

- Фіксувати перелік датчиків, залучених до події;
- Визначати первинну точку інциденту (час + топологія).

Кластеризація та залежності:

- Формування зв’язок «лічильник – датчик» (кластер);
- Прогнозування кількості відключених лічильників при падінні тиску;
- Врахування структури мережі та напрямків потоків.

Аналіз споживання та параметрів:

- Різкі зміни споживання газу (непобутові споживачі);
- Різкі зміни температури газу;
- Різкі зміни тиску газу;
- Прив’язка до ГРС та пунктів підготовки газу.

Контроль ВОГ:

- Контроль строків повірки;
- Виявлення втручання у роботу ВОГ та складових.

Логіка обробки:

- Часові інтервали між подіями;
- Напрямки потоків газу;
- Топологію мережі;
- Причинно-наслідкові зв’язки.

Додаткові умови:

Повний перелік каскадних залежностей та правил агрегації визначається та узгоджується після підписання договору.

7.3. Модуль репозиторію

Модуль репозиторію – реалізований універсальний API для управління списками датчиків, пристроїв стеження або, реєстром користувачів. API модуля репозиторію має містити набір CRUD-інтерфейсів (створення, читання, модифікація та видалення інформації) для різних типів об'єктів, наприклад для управління переліками датчиків, об'єктами спостереження, моніторингу або реєстром користувачів.

Модуль повинен мати змогу проводити менеджмент ключів шифрування даних від пристроїв обліку та сенсорів IoT. Якщо на пристрої обліку, або сенсорі використовується шифрування необхідно мати змогу активувати пристрій (додати ключи шифрування).

Необхідно реалізувати збереження, та менеджмент інформації, щодо поточного стану (в роботі, не в роботі, в ремонті/ТО тощо), переміщення (належності до філії), введення в експлуатацію, виведення з експлуатації, технічного обслуговування, ремонту, повірки, та списання приладів, із зазначенням статусів та дат зміни статусів.

Статуси лічильників, пристроїв перетворення об’єму:

- встановлений (в роботі, не в роботі, в ремонті/ТО, необхідний ремонт/ТО тощо);
- демонтований (на повірку, на ремонт/ТО, списаний тощо);
- необхідна повірка;
- необхідний ремонт/ТО.

Статуси іншого обладнання:

- встановлений;
- демонтований;
- необхідний ремонт;
- списаний.

Дані які відносяться до лічильника, пристроїв перетворення об’єму:

- показники на момент монтажу;
- дата монтажу;

- показники на момент демонтажу;
- дата демонтажу;
- строк дії повірки;
- дата повірки.

Процес монтажу та проведення.

Новий лічильник, пристрій перетворення об’єму закупається на філію, створюється в ПЗ з вказанням повірочного інтервалу та дати повірки. При монтажі вказується адреса монтажу, геопросторова точка, та початкові показники. При необхідності зняття (повірки, ремонту/ТО) записується поточний показник об’єму. Після проведення сервісних робіт, проводиться монтаж, або на стару адресу, або на нову. При монтажі вказуються поточні показники лічильника, пристрою перетворення об’єму.

Формування звітності про статус лічильника, пристрою перетворення об’єму відбувається за моделлю та серійним номером.

7.4. Модуль зберігання даних

Модуль зберігання даних - забезпечує надійне зберігання великих обсягів історичних та поточних даних. Підтримує одну, або декілька розповсюджених СКБД (MS SQL Server, Oracle Database, PostgreSQL тощо). Модуль повинен мати змогу масштабування кількості баз даних, що дозволить збільшити пропускну здатність платформи, при збільшенні кількості приладів IoT.

7.5. Модуль аналітики та візуалізації

Модуль призначений для операційного та аналітичного аналізу даних, побудови звітів, графіків і візуалізації технологічних процесів у режимі реального часу та в історичному розрізі.

Можливості:

- Візуалізація даних (графіки, таблиці, діаграми, dashboard);
- Аналіз даних у реальному часі та історії;
- Підтримка всіх типів даних від пристроїв;

- Комбінування даних у межах одного звіту;
- Експорт у формати Excel та PDF.

Дані для аналізу:

- Показники витрати (лічильники, коректори);
- Помилки та аварії на вузлах обліку;
- Стани та помилки IoT-сенсорів;
- Виходи параметрів за норми (ПРГ, ЕХЗ);
- Стан мережі LoRaWAN;
- Інші дані від пристроїв.

Ієрархія та доступ:

Товариство → Філія → УЕГГ → дільниця

Функціонал:

- Розмежування доступу за ролями;
- Drill-down / roll-up;
- Перегляд від загального до деталізованого рівня.

Рівні відображення:

- Товариство — загальний стан;
- Філія — агреговані показники;
- УЕГГ — детальні дані по об’єктах.

Конструктор звітів:

- Вибір ключових і додаткових параметрів;
- Побудова таблиць, графіків, діаграм;
- Фільтри (пристрої, структура, події);
- Вибір періоду;

- Агрегації (сума, середнє, мін/макс, кількість, медіана);
- Порівняльний аналіз.

Робота зі звітами:

- Збереження шаблонів;
- Редагування та копіювання;
- Автоматичне оновлення;
- Контроль доступу.

Використання:

- Перегляд у реальному часі та історії;
- Додавання до dashboard;
- Експорт у Excel та PDF.

7.6. Геоінформаційний модуль

Геоінформаційний модуль - наявний набір інструментів з відображення електронних карт, основних характеристик територій та позначень на карті місцезнаходження відповідного обладнання обліку, датчиків, сенсорів, телеметрії мережі (ПРГ, ЕХЗ, тощо).

Об’єкти відображанні на мапі повинні мати інтерактивне позначення робочого статусу та помилок.

Наявність документованих SDK/API для інтеграції з наявною геоінформаційною системою Замовника.

7.7. Модуль подій

Модуль подій - реалізований універсальний API для отримання різних подій щодо зміни властивостей об'єкта, факту отримання нового значень або повідомлень про початок, закінчення роботи, виконання завдань та ін.

Модуль подій має враховувати та групувати події що агреговані як каскадні, оновлювати поточну подію інформацією з датчиків по ходу руху газу. Групувати події та відображати аварію першого пристрою по руху ієрархії дерева пристроїв.

7.8. Модуль сповіщень та повідомлень

Модуль сповіщень та повідомлень - мати можливість створення сповіщень про події (наприклад, досягнення критичних значень датчиків, позаштатна робота обладнання, перевищенні ліміту). - Підтримує різні канали повідомлень: email, SMS, push-сповіщення, тощо.

Необхідно реалізувати повідомлення про стан пристроїв в мережі IoT - точки обліку, сенсори, телеметрія ГРМ (ПРГ, ЕХЗ, тощо), базові станції мережі LoRaWAN. Реалізувати повідомлення, щодо необхідності повірки, із зазначенням статусів та дат зміни статусів. Виводити попередження про спливаючий термін повірки лічильників.

7.9. Модуль асинхронних завдань

Модуль асинхронних завдань – реалізований універсальний API для запуску та контролю виконання програмних завдань тривалої дії на віддалених підсистемах.

Модуль повинен забезпечити можливість виконання об’ємних задач, таких як формування великих звітів, копіювання даних, аналіз великих масивів даних.

7.10. Модуль інтеграції

Модуль інтеграції - забезпечує взаємодію з зовнішніми інформаційними системами та сервісами. Підтримує стандартизовані протоколи та формати обміну даними.

Підключення та взаємодія з модулем відбувається за допомогою описаного REST API.

7.11. Модуль безпеки та автентифікації

Модуль безпеки та автентифікації - відповідає за автентифікацію користувачів, керування ролями та правами доступу. Забезпечує аудит дій користувачів та моніторинг безпеки системи.

8. СХЕМА РОЗГОРТАННЯ

Програмне забезпечення розгортається на серверах, які входять до поставки програмного комплексу. Всі необхідні ліцензії, для функціонування комплексу, повинні бути включені в поставку.

Платформа IoT повинна мати можливість масштабування та балансування навантаження, необхідно мати можливість розгортання декількох кластерів серверу для забезпечення відмовостійкості та можливості подальшого масштабування.

Платформа IoT розгортається з використанням системи віртуалізації Proxmox VE, кожний модуль повинен мати окрему віртуальну машину, чи контейнер для забезпечення гнучкого налаштування та балансування апаратних ресурсів.

Платформа повинна забезпечувати балансування навантаження між серверами обробки даних із використанням NGINX (або еквіваленту), що гарантує масштабованість, відмовостійкість, стабільну обробку великої кількості одночасних підключень та централізоване управління мережевим трафіком із підтримкою механізмів безпеки.

Розробник повинен надати технічні вимоги до системи віртуалізації для розгортання програмного комплексу, навантаження:

1. до 500 000 приладів з сирою вагою пакета:

Тип приладу	**Пакетів/добу**	**Розмір пакета, Б**	**Формула**	**Байт/добу**	**МіБ/добу**	**ГіБ/добу**
Телеметрія ГРП	48 000	374	48 000 × 374	17 952 000	17.12	0.017
Телеметрія СКЗ	21 000	374	21 000 × 374	7 854 000	7.49	0.007
Лічильники промисловості, тип А	4 800	6714	4 800 × 6714	32 227 200	30.73	0.030
Лічильники промисловості, тип Б	144 096	289	144 096 × 289	41 643 744	39.71	0.039
Лічильники побутові	16 267	192	16 267 × 192	3 123 264	2.98	0.003
Лічильники електроенергії	21 000	462	21 000 × 462	9 702 000	9.25	0.009
Нові прилади платформи	256 000	374*	256 000 × 374	95 744 000	95.74	0.096
Разом			Σ V_d	208 246 208	203.02	0.201

2. Гарячим сховищем даних на 31 добу;
3. Збереженням оброблених даних на 8 років;
4. Резервне копіювання віртуальних машин за схемою GFS;
5. Онлайн до 1000 користувачів.

9. ВИМОГИ ДО ЗАХИСТУ ІНФОРМАЦІЇ

Платформа IoT повинна забезпечувати безпеку збору, збереження та транспортування інформації.

Реалізувати захист відповідно до протоколу шифрування TLS 1.2 / 1.3. Забезпечити захист підключень клієнтів та приладів.

Підключення приладів повинно проходити верифікацію за серійними номерами, та типами пристроїв, запит на аутентифікацію від приладів які не внесені до «білого списку» необхідно відхиляти.

Підключення клієнтів до серверу необхідно реалізовувати завдяки HTTPS з використанням TLS 1.2 / 1.3.

Програмне забезпечення повинно мати засоби криптографічного захисту передачі інформації, що знаходяться у реєстрі Державної служби спеціального зв'язку та захисту інформації України відповідно до наступних вимог:

№	Підсистема та вимоги до неї	Деталізація вимог
1. Підсистема захисту інформації між користувачами і Платформою IoT (без використання VPN клієнта)		
1.1	Реалізація шлюзів у вигляді образу віртуальної машини (virtual appliance) з попередньо налаштованими операційною системною та програмним забезпеченням у віртуальній інфраструктурі Платформи IoT	Постачання у вигляді Virtual Appliance для середовищ віртуалізації
1.2	Завдання на захист конфіденційності і автентичності трафіку між Платформою IoT та користувачами покладається на web-сервери, для побудови HTTPS з'єднання	Обов'язково з використанням TLS v1.2+
1.3	Можливість горизонтального масштабування пропускної здатності за рахунок збільшення кількості серверів (virtual appliance).	Без обмежень на кількість
1.4	Забезпечення пропускної здатності захищеного каналу між користувачами та Платформи IoT (за умови наявності якісного Інтернет з'єднання між web-браузером користувача і web-серверами Платформи IoT)	Не менше 100 Мбіт/с між користувачем і web-серверами Платформи IoT

1.5	Можливість роботи через HTTP-proxy	Обов’язково
1.6	Засоби КЗІ, які використовуються для побудови TLS v1.2 на боці web-серверів Платформи IoT повинні мати відповідний діючий позитивний експертний висновок Держспецзв’язку України у галузі криптографічного захисту інформації.	Обов’язково
1.7	Кількість Virtual Appliance з засобами КЗІ	1 шт, з можливістю масштабування до 4 шт

10. ВИМОГИ ДО ДОКУМЕНТАЦІЇ

IoT платформа повинна бути передана разом з технічною та експлуатаційною документацією, а саме:

- технічний опис функціоналу платформи;
- інструкція розробника, в якій описані інструменти та їх можливості;
- інструкція адміністратора, в якій описані механізми розгортання, конфігурування, налаштування та адміністрування платформи;
- інструкція користувача;
- опис всіх програмних інтерфейсів (API) для інтегрування та обміну даними як внутрішніми так і зовнішніми системами та сервісами.

11. ВИМОГИ ДО АПАРАТНОЇ ЧАСТИНИ

Найменування/назва	Вимоги
11. Модуль обміну даними	**1 комплект**
До складу входять:	
11.1. Мережевий пристрій безпеки (NGFW)	Не менше 2 шт.
Загальні вимоги	• Мережевий пристрій безпеки що пропонується, повинен являти собою міжмережевий екран наступного покоління (NGFW) та здійснювати інспекцію мережевого трафіку та захист корпоративної інфраструктури відповідно до нижченаведених вимог • Якщо відповідно до функціональності пристроїв/систем або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то вони усі мають бути у комплекті поставки рішення з урахуванням вимог до строку та функціональності технічної підтримки • Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення • На обладнання не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника
Архітектура та форм-фактор	• Програмно-апаратний комплекс (ПАК) для встановлення в стандартну монтажну шафу 19", 1U
Інтерфейси	• Не менше ніж 16 × GE RJ45 порти • Не менше ніж 1 × GE RJ45 Management порт • Не менше ніж 1 × GE RJ45 HA порт • Не менше ніж 8 × GE SFP слоти • Не менше ніж 4 × 10 GE SFP+ uplink слоти • Не менше ніж 1 × USB порт • Не менше ніж 1 × RJ45 консольний порт
Живлення	• Два вбудованих блоки живлення з резервуванням 1+1 (100–240V AC, 50/60 Hz)
Продуктивність сервісів безпеки	• Пропускна здатність сервісу Stateful Firewall (на пакетах розміром 1518 байт, UDP): не менше ніж 39 Гбіт/с • Кількість одночасних TCP-сесій: не менше ніж 3 000 000 • Кількість нових TCP-сесій/секунду: не менше ніж 140 000 • Пропускна здатність на пакетах розміром 450 байт або

	Enterprise Testing Conditions / Enterprise traffic mix / APPMIX (з включеними сервісами FW+App Control+IPS+Malware Protection): не менше ніж 2,8 Гбіт/с • Пропускна здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 3 Гбіт/с
Продуктивність VPN	• Пропускна здатність IPSec VPN: не менше ніж 35 Гбіт/с • Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 16 000 • Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 2 000
Модуль довіреної платформи (TPM)	• Апаратний механізм захисту, створення, зберігання та автентифікації криптографічних ключів
Віртуалізація	• Віртуальні FW (Virtual Systems/Security contexts/Virtual Domains), що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами тощо: не менше ніж 10
Висока доступність (High Availability)	• Active-Active • Active-Standby
L2 функціонал та мережеві служби	• Агрегація портів (802.3ad) • VLAN (802.1Q та Trunking) • Вбудований DHCP, NTP, DNS-сервер
NAT	• Статичний NAT • Динамічний NAT • PAT
Multicast	• Sparse та dense режим • Підтримка PIM
Сервіси безпеки	• Stateful Firewall • Ідентифікація та контроль застосувань (AC/AVC) • Захист від загроз на основі сигнатурного аналізу (IPS) • Захист від malware (Antivirus/AMP) • Web та DNS-фільтрація • Anti-Spam • Інспектування/сканування SSL/TLS трафіку на загрози • Захист від невідомих загроз (0-day) • Захист від DoS-атак • IPSec VPN
Stateful Firewall	• Режими роботи: • NAT/маршрутизатор • прозорий режим (міст)

	• Підтримка VoIP трафіку: глибока інспекція та захист від атак на протокол SIP • Виконання ролі проксі для аналізу, інспектування та забезпечення коректної роботи сесій різних протоколів (session helpers, application layer gateway)
Ідентифікація та контроль застосувань (AC/AVC)	• Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control) • Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур • Конфігурація виключень у діях з певними додатками (exemption/override) • Створення користувацьких сигнатур додатків
Захист від загроз на основі сигнатурного аналізу (IPS)	• Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (Intrusion Prevention System) • Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур • Конфігурація виключень у діях з певними сигнатурами (exemption/override)
Захист від malware (Antivirus/AMP)	• Anti-Virus / Anti-malware захист • Виявлення та блокування небажаних програм або файлів (grayware) • Виявлення та блокування файлів на основі налаштованих порогових значень їх розміру для різних протоколів • Захист від зловмисних програм для мобільних пристроїв • Content Disarm and Reconstruct (CDR) — знешкодження потенційно шкідливого вмісту у файлах документів перед їх доставкою
Web та DNS-фільтрація	• Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фільтрація) • Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація) • Фільтрація відеоконтенту за категоріями (Video Filtering) • Виявлення та блокування доступу до Botnet мереж та C2 серверів • Блокування підключень з використанням шкідливих SSL/TLS-сертифікатів • Статичні blacklists та whitelists
SSL/TLS-інспекція	• Перехоплення, розшифрування та інспекція HTTPS, IMAPS, POP3S, SMTPS, FTPS-сесій • Конфігурація виключень з SSL/TLS-інспекції певних IP-

	адрес, URL тощо (exemption/override) • Інспектування SSL/TLS-сертифікату на відповідність певному web-ресурсу та строку дійсності (SSL/TLS Certificate Inspection) • Повноцінне інспектування контенту зашифрованих сесій (Full SSL/TLS Inspection) • Інспектування SSL/TLS-трафіку має включати: IPS, AC/AVC, AV/AMP, Web-фільтрацію
Захист від невідомих загроз (0-day)	• Інтеграція з системою захисту від складних атак нульового дня (у вигляді хмарного сервісу — Cloud Sandbox) • Відправка файлів з користувацького трафіку на аналіз у Cloud Sandbox для виявлення невідомих загроз класу «0-day» • Ліцензування має дозволяти інспектувати у Cloud Sandbox не менше ніж 14 400 файлів на день (24 години)
Захист від DoS-атак	• Можливість розпізнавання та блокування DoS-атак: • TCP Syn flood • TCP/UDP/SCTP port scan • ICMP sweep • TCP/UDP/SCTP/ICMP session flooding
IPSec VPN	• Алгоритми шифрування: 3DES, AES128, AES192, AES256 • Алгоритми хешування: MD5, SHA256, SHA384, SHA512 • Diffie-Hellman Group: 1, 2, 5, 14 • Підтримка Hub & Spoke топології, Spoke & Spoke (mesh) топології, DMVPN/ADVPN або аналог
QoS	• Traffic Shaping • Traffic Policing
Маршрутизація та SD-WAN	• Статична маршрутизація та маршрутизація по політиках (PBR) • Динамічні протоколи маршрутизації: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4 • Об'єднання фізичних та логічних інтерфейсів з різнотипними підключеннями (MPLS, broadband Internet, LTE тощо) • Оцінка якості каналів зв'язку SD-WAN шляхом відправлення пакетів або запитів до певних вузлів у мережі або пасивними методами • Контроль характеристик каналів зв'язку в режимі реального часу (packet loss, jitter, latency) та їх графічне відображення • Вибір та переключення каналів зв'язку на основі заданих порогових значень характеристик якості

	• Визначення SLA для користувацьких додатків (applications) з використанням характеристик каналів зв'єднання (packet loss, jitter, latency) • Визначення різнопланових стратегій вибору каналів зв'язку для маршрутизації трафіку додатків та сервісів виходячи з критеріїв відповідності SLA, кращих значень характеристик каналів зв'язку тощо • Визначення правил маршрутизації трафіку додатків та сервісів через канали SD-WAN з урахуванням стратегій та SLA • Автоматичне балансування навантаження, переключення і резервування каналів зв'язку для користувацьких додатків та сервісів при зміні характеристик мережевих з'єднань (loss, jitter, latency) в реальному часі • Динамічне виправлення втрати пакетів або відновлення пакетів з помилками, що викликані несприятливими умовами WAN-каналів під час роботи через VPN (Forward Error Correction) • Балансування пакетів однієї сесії через декілька IPSec VPN тунелів
Автентифікація, авторизація та облік (AAA)	• Локальна база даних користувачів • Підтримка протоколів LDAP, RADIUS, TACACS+ • Підтримка 2-факторної автентифікації (two-factor authentication) на основі програмних токенів • Не менше ніж 2 програмні токени для встановлення на мобільні пристрої (смартфони) • Single Sign-On: інтеграція з Windows AD • PKI та сертифікати: X.509, SCEP support, створення Certificate Signing Request (CSR), автоматичне поновлення сертифікатів до закінчення терміну дії, підтримка OCSP
Керування, звітність, інтеграція	• Графічний веб-інтерфейс (Web GUI) • Інтерфейс командного рядка (CLI) • Підтримка централізованої системи керування • Ролевий доступ адміністраторів (RBAC) • Підтримка REST API • Централізоване ведення журналів та звітності (logging and reporting) • Функціонал запису пакетів з мережевих інтерфейсів (packet capture) • Функціонал резервного копіювання та відновлення файлів конфігурації • SNMP v1, v2, v3 • sFlow v5 / NetFlow v9, syslog

Технічна сервісна підтримка	• Рішення повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 12 місяців з рівнем сервісу 24*7 • Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7 • Постійний авторизований доступ до сайту виробника 24*7 • Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки • Отримання основних та проміжних релізів програмного забезпечення • Можливість реєстрації сервісних випадків в режимі 24*7*365, доставку і заміну запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника)
11.2. Система централізованого збору та аналізу журнальних файлів (віртуалізоване рішення)	Не менше 1
Загальні вимоги	• Система являє собою централізовану систему збору журнальних файлів (логів), їх аналізу та побудови звітів з мережевих пристроїв безпеки • Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових ліцензій, то вони усі мають бути у комплекті поставки рішення з урахуванням вимог до строку та функціональності технічної підтримки • Для системи не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника
Архітектура та форм-фактор	• Ліцензія має бути безстрокова • Система має бути у вигляді віртуалізованого рішення, що встановлюється на апаратних ресурсах (серверах) замовника (під VMWare/Hyper-V/KVM) • Мінімальна кількість виділених vCPU: не менше ніж 4 • Мінімальний обсяг оперативної пам'яті: не менше ніж 16 ГБ • Підтримка до 12 мережевих інтерфейсів (vNIC)
Ліцензування	• Система має бути спроможна (ліцензована) приймати для обробки та аналізу не менше 5 ГБайт логів на день • Система має бути ліцензована для автоматичного завантаження пакетів для виявлення найновішого зловмисного програмного забезпечення включно зі звітами

	про спалахи (Outbreaks), обробниками подій і шаблонами звітів для виявлення спалахів • Система має бути ліцензована для виявлення у журнальних файлах сигнатур IOC та ідентифікації скомпрометованих пристроїв/користувачів • Система має бути ліцензована для інтеграції з сервісом обміну розвідданими про загрози, що забезпечує отримання актуальних даних про IOC, зловмисні домени/URL та хеші шкідливого ПЗ у режимі реального часу • Система має бути ліцензована сервісом автоматичної оцінки безпеки та відповідності, що допомагає командам безпеки розробляти, впроваджувати та підтримувати рівень безпеки та надавати дієві рекомендації щодо конфігурації, а також відображати ключові показники ефективності та ризику
Загальні вимоги до системи	• Система має виконувати функції збору, аналізу та кореляції подій з журнальних файлів (log data) з мережевих пристроїв та систем • Журнальні файли мають відправлятись з пристроїв на систему через шифровані з'єднання / з використанням протоколів шифрування • Аналіз журнальних файлів та побудова звітів • Створення зведених графічних звітів з пристроїв, що надсилають дані • Забезпечення створення звітів по мережевій активності, системним подіям, загрозам, web-фільтрації, тощо • Наявність вбудованих шаблонів для швидкого створення найбільш затребуваних звітів • Підтримка імпорту та експорту шаблонів звітів • Підтримка різних форматів звітів
Режими роботи	• Режим збору журнальних файлів та відправки їх на аналіз та для побудови звітів на іншу систему • Режим збору, аналізу та побудови звітів на основі журнальних файлів
Загальні вимоги до роботи з журнальними файлами (logs)	• Прийом усіх можливих журнальних файлів з мережевих пристроїв та систем • Пошук та фільтрація у журнальних файлах за різними критеріями (проміжки часу, тип пристрою, тощо) • Збереження критеріїв фільтрації у шаблон, який у подальшому можливо запускати для здійснення швидкого пошуку • Визначення граничних розмірів журнальних файлів для їх

	автоматичного архівування • Визначення автоматичного архівування журнальних файлів за розкладом • Збереження журнальних файлів на адміністративній станції або на мережевому сервері з використанням протоколів FTP, SCP, SFTP • Відновлення журнальних файлів з адміністративної станції або з мережевого серверу з використанням протоколів FTP, SCP, SFTP • Конфігурація автоматичного стиснення (gzip) журнальних файлів перед відправкою на сторонні сервери • Конфігурація автоматичного видалення журнальних файлів після відправки на сторонні сервери • Конфігурація автоматичного видалення журнальних файлів через певний проміжок часу • Пересилка журнальних файлів на сторонні сервери за протоколом syslog, CEF у режимі реального часу та за розкладом • Фільтрація по типам журнальних файлів та по типам пристроїв, для визначення які журнальні файли та з яких пристроїв пересилати на сторонні сервери • Додавання хеш-сум журнальних файлів під час їх архівування та передачі на сторонні сервери для збереження цілісності журнальних файлів • При досягненні граничного значення ємності системи зберігання журнальних файлів система має (в залежності від налаштувань): • припинити прийом журнальних файлів • перезаписувати найбільш старі журнальні файли
Обробники подій у журнальних файлах	• Автоматичний пошук у журнальних файлах інформації щодо певних подій та сповіщення адміністраторів про її виявлення • Такі сповіщення мають надсилатись по електронній пошті, як SNMP-trap, на сервер syslog • Наявність у системі попередньо визначених обробників подій у журнальних файлах • Конфігурація власних обробників подій у журнальних файлах
Аналітика журнальних файлів	• Журнальні файли, що приймаються з пристроїв, мають бути проіндексовані та розміщені у базі даних для проведення аналітики • Видалення аналітичних журнальних файлів з бази даних через визначений проміжок часу

Архівування журнальних файлів	• При досягненні певного розміру журнальні файли, що приймаються з пристроїв, мають архівуватися • Видалення архівних журнальних файлів через визначений проміжок часу
Оповіщення (alert generation)	• Генерація сповіщень при знаходженні у журнальних файлах певних повідомлень • Відображення сповіщень в GUI системи • Відправка сповіщень адміністраторам по email, SNMP, syslog
Хмарне зберігання журнальних файлів	• Підтримка відправлення журнальних файлів на збереження у хмарний сервіс виробника (при додатковому ліцензуванні)
Побудова звітів (reporting)	• Обробка журнальних файлів та створення звітів на основі зібраних даних • Наявність у системі попередньо створених звітів/шаблонів звітів • Конфігурація власних звітів/шаблонів звітів • Формування звітів на основі певних даних та з використанням визначених форматів відображення (кругові діаграми, гістограми, таблиці, тощо) • Запуск створення звітів за розкладом та у ручному режимі • Збереження звітів на мережевому сервері з використанням протоколів FTP, SCP, SFTP • Відновлення звітів з мережевого серверу з використанням протоколів FTP, SCP, SFTP • Відправлення звітів по email • Збереження звітів у різних форматах (PDF, HTML, XML, тощо) • Підтримка отримання архівних журнальних файлів з іншої аналогічної системи для її розвантаження та локального виконання запитів і генерування звітів • Фільтрація, під час запиту на отримання архівних журнальних файлів з іншої аналогічної системи, на основі різних критеріїв (тип пристрою, часовий проміжок, тощо)
Security Rating and Compliance Service	• Забезпечення командам безпеки можливості розробляти, впроваджувати та підтримувати безпекову позицію, надаючи практичні рекомендації щодо конфігурації, а також ключові показники ефективності та ризику
IOC, Outbreak Detection та хмарний сервіс обміну розвідданими про загрози	• Виявлення у журнальних файлах сигнатур IOC та ідентифікація скомпрометованих пристроїв/користувачів • Виявлення найновішого зловмисного програмного забезпечення включно зі звітами про спалахи (Outbreaks)

	• Надання хмарного сервісу з розвідки загроз для захисту від сучасних кіберзагроз, забезпечуючи у реальному часі дані про зловмисників, індикатори компрометації (IOC), хеші шкідливого ПЗ та фішингові домени/URL • Сервіс має оптимізувати розслідування та реагування на інциденти за допомогою розширеної аналітики, сповіщень про спалахи загроз та автоматизованих робочих процесів
Звітність у реальному часі	• Графічне відображення заздалегідь створених інформаційних панелей (dashboard), що містять інформацію з різних web-віджетів (widgets) стосовно загроз, трафіку, додатків, скомпрометованих вузлів, працездатності системи, тощо • Створення власних інформаційних панелей для графічного відображення інформації з журнальних файлів • Відтворення різних інформаційних панелей (dashboard) на різних моніторах адміністраторів
Ролевий доступ	• Адміністрування системи на основі ролевого доступу з різним рівнем повноважень (admin profiles) • Визначення довірених вузлів/підмереж з яких дозволяється підключення до системи (Web GUI, SSH)
Адміністративні домени (Multi-Tenancy)	• Створення окремих ізольованих між собою адміністративних доменів для розподілення між ними пристроїв та відповідних адміністраторів (Multi-Tenancy) • Розподілення до адміністративних доменів як фізичних так і віртуальних пристроїв • Розподіл дискового простору системи між адміністративними доменами • Визначення терміну зберігання журнальних файлів • Визначення дискового простору для аналітичних журнальних файлів та архівних журнальних файлів
Функціонал керування, налаштування та моніторингу	• Керування через графічний веб-інтерфейс (Web GUI) з використанням HTTPS • Керування через CLI з використанням SSH-підключення • Конфігурування політик стійкості паролів (password policy) для локальних записів (local accounts) • Автентифікація адміністраторів на основі локальної бази, LDAP, RADIUS, TACACS+, PKI • Підтримка двофакторної автентифікації • SAML SSO для забезпечення наскрізної аутентифікації адміністратора поміж декількох пристроїв, що входять в один домен безпеки • Моніторинг стану системи (status та health), частки використаних апаратних ресурсів (CPU, Memory, Disk)

	• Моніторинг швидкості надходження журнальних файлів • Відображення ліцензійної інформації • Статична маршрутизація • JavaScript Object Notation (JSON) API
Резервне копіювання та відновлення системи (Backup та restore)	• Резервне копіювання конфігураційних файлів • Шифрування конфігураційних файлів, що зберігаються, з використанням паролів • Відновлення системи з резервних конфігураційних файлів • Оновлення програмного забезпечення системи
Спостереження за роботою системи	• Відображення стану системних завдань, що виконуються адміністраторами у системі • Фільтрація серед списку цих завдань за статусом чи станом їх виконання • Відміна (delete) виконання певних завдань • Ведення журналу подій (event log) які виникають під час роботи системи • Відображення подій з заданим рівнем важливості (severity) • Збереження журналу подій для подальшого аналізу • Фільтрація та пошук у журналі подій за різними критеріями
Пошук неполадок (troubleshooting)	• Відображення завантаження та використання основних апаратних елементів (cpu, memory, hdd, тощо) системи • Відображення інформації стосовно частоти прийому журнальних файлів та швидкості їх індексації у базі • Наявність packet sniffer для виявлення неполадок шляхом збору та аналізу мережевого трафіку
Технічна сервісна підтримка	• Рішення повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 12 місяців з рівнем сервісу 24*7 • Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7 • Постійний авторизований доступ до сайту виробника 24*7 • Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки • Отримання основних та проміжних релізів програмного забезпечення • Можливість реєстрації сервісних випадків в режимі 24*7
11.3. Програмне забезпечення системи захисту веб-сервісів (віртуалізоване рішення)	Не менше 1 шт

Загальні вимоги	• Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки • Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення • На запропоноване рішення не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника • Усі функціональні вимоги та кількісні показники продуктивності повинні мати підтвердження у документації виробника
Архітектура та форм-фактор	• Система має поставлятись як віртуальна машина (VM), що буде встановлюватися на відповідний сервер з системою віртуалізації, які надаються замовником • Система має підтримувати роботу з однією з систем віртуалізації: VMware ESXi, Microsoft Hyper-V, KVM • Кількість виділених віртуальних процесорів (vCPU): не менше ніж 1 vCPU
Продуктивність (Throughput)	• Продуктивність обробки HTTP-трафіку не менше ніж 25 Мбіт/с • Продуктивність обробки HTTPS-трафіку (SSL/TLS) не менше ніж 10 Мбіт/с
Ліцензування	• Необмежена кількість веб-додатків що захищаються • Ліцензія захисту від botnet, malicious IP, phishing URLs, anonymous proxies, Trojan, ddos sources • Ліцензія для балансування навантаження на сервери на 7 рівні (Load balancing) • Інші ліцензії, що потребують задоволення наведених функціональних вимог
Резервування, відмовостійкість	• Active / Passive • Active / Active
Режими функціонування	• Зворотний проксі (Reverse Proxy) • Прозорий режим (Transparent / Bridge) • Прозорий проксі режим (Transparent Reverse Proxy) • Офлайн-режим (Non-inline sniffer / Off-line Sniffing) • WCCP
Мережевий функціонал	• Статична маршрутизація (Static routing) • Маршрутизація на основі політик (Policy-based routing)

	• Трансляція IP-адрес (NAT) • Віртуальні мережі (VLAN - IEEE 802.1Q) • Агрегація групи фізичних інтерфейсів в один логічний інтерфейс (LACP - IEEE 802.3ad)
SSL/TLS-обробка	• Обробка SSL/TLS (якщо для цього потрібні додаткові ліцензії, вони мають бути у комплекті поставки) • Дешифрування та інспектування SSL/TLS (SSL off-loading)
Створення еталонної моделі функціонування веб-додатків	• Створення еталонної моделі функціонування веб-додатків шляхом автоматичного навчання (auto learn) або машинного навчання (machine learning), які базуються на основі запитів користувачів до веб-додатків • Підтримка автоматизованого динамічного профілювання веб-додатків • Підтримка автоматизованого внесення змін в еталонну модель при зміні веб-додатків
Комплексний захист від атак OWASP top 10 та перевірка на вразливості	• Виявлення та попередження OWASP top 10 атак (https://www.owasp.org/index.php/Top_10-2017_Top_10) • Наявність вбудованого сканеру вразливостей або інтеграція зі стороннім рішенням даного типу (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічною підтримкою на такий самий термін, що й запропонована учасником система захисту веб-серверів)
Захист від DOS/DDOS-атак, Bot-protection	• Виявлення та захист від атак повного перебору на облікові дані користувачів (Brute Force Login) • Захист від DoS-атак на 3/4 рівні OSI (TCP Flood Prevention) • Захист від DoS-атак на 7 рівні OSI (HTTP Flood Prevention) • Розпізнавання підключення до сайту програми (bot) чи людини за допомогою CAPTCHA-запиту (CAPTCHA request) чи з використанням тесту (Real Browser Enforcement / Bot Protection)
Відстеження користувачів та їх пристроїв	• Відстеження користувацьких сесій та поведінки користувачів після їх вдалої автентифікації (User Tracking) • Профілювання та відстеження пристроїв користувачів, визначення їх репутації безпеки на основі порушення ними політик безпеки та автоматизація відповідної реакції у реальному часі (Device Intelligence Service / Device identification tracking)
Функції захисту веб-додатків та веб-сайтів	• Розмежування та обмеження доступу на основі whitelist та blacklist • Захист від Botnet, Anonymous proxy, Phishing, tor, spam,

	ddos та інше на основі баз IP-репутації (IP Reputation) • Розмежування та обмеження доступу на основі баз IP-геолокації (IP Geolocation) • Перевірка відповідності HTTP RFC (Protocol validation) • Захист від відомих атак на основі сигнатур для веб-сервісів/додатків (Web services signatures) • Створення користувацьких сигнатур для захисту від атак на веб-сервіси/додатки (Custom signatures) • Додавання системних cookie у HTTP-запити без їх шифрування • Додавання системних cookie у HTTP-запити з їх шифруванням • Міжмережевий екран на 4 рівні OSI або списки керування доступом на 4 рівні OSI (Stateful Firewall / Access control lists / IP Filters) • Виявлення та блокування шкідливих програм (Malware detection) завдяки вбудованому антивірусу або завдяки інтеграції зі стороннім рішенням даного типу (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічною підтримкою на такий самий термін, що й запропонована учасником система захисту веб-сервісів) • Аналіз команд протоколу FTP (Allowed / Blocked commands) при доступі до сайту та перевірка на наявність шкідливих програм у файлах що завантажуються "на" чи "з" сервера (upload or download)
Визначення логіки, порядку доступу до ресурсів сайту та цілісності структури сайту	• Визначення URL сайту, з якого має розпочинатись доступ до контенту сайту (Start Page Enforcement) • Визначення URL сайту, що мають бути доступні у певній черзі (Page Order Rules) • Дозвіл чи блокування доступу до певних URL сайту (URL access) • Дозвіл чи блокування певних методів доступу HTTP до сайту / URL (Allow / Deny HTTP Method) • Виявлення видалення, додавання чи зміни файлів на веб-сайті та автоматичне відновлення структури та контенту сайту (Web Defacement Protection)
Доставка та маршрутизація контенту додатків	• Переписування або переправлення запитів і відповідей HTTP (URL Rewriting, redirecting) • Маршрутизація запитів до серверів на основі HTTP контенту (HTTP content routing) • Можливість додавання чи зчитування оригінальної IP-адреси ініціатора сеансу з HTTP-заголовку (X-Forwarded-For / X-Real-IP / True-Client-IP)

	• Балансування навантаження на сервери на 7 рівні (Load balancing) • Перевірка доступності серверів (Health Check) для балансування навантаження за допомогою ICMP, TCP, HTTP • Стиснення файлів (Content compression) • Кешування контенту (Content caching) • SSL/TLS off-loading • Модернізація сторінок, що відображають код помилки при порушенні користувачами політик безпеки, недоступності веб-сайту, перевірки captcha
Підтримка та аналіз протоколів	• Підтримка та аналіз протоколів XML, JSON • Підтримка та аналіз протоколів HTTP/2 • Підтримка та аналіз протоколу WebSocket
Автентифікація	• Підтримка протоколів LDAP, RADIUS, TACACS+ • Підтримка 2-факторної автентифікації (two-factor authentication) • Підтримка єдиної автентифікації користувачів (single sign-on) через систему захисту веб-серверів для доступу до декількох веб-додатків в одному домені • Автентифікація на основі SSL-сертифікатів користувачів • Інтеграція з Public Key Infrastructure (PKI) • Модернізація сторінок автентифікації користувачів
Управління, звітність, інтеграція	• Графічний веб-інтерфейс (Web GUI) • Інтерфейс командного рядка (CLI) • Підтримка системи централізованого керування для декількох пристроїв • Підтримка REST API • Централізоване ведення журналів та звітності (logging and reporting) • Розмежування доступу різних груп адміністраторів, призначаючи їм різні адміністративні привілеї для підмножини політик і захищених імен хостів (Administrative domain / Administrative Partitions / Virtual domain) • Ролевий доступ адміністраторів (RBAC) • Повідомлення про події за допомогою SNMP, Syslog та Email • Пересилання та зберігання журналів подій на виділений пристрій за допомогою FTP/TFTP, Email • Функціонал запису пакетів з мережевого інтерфейсу для подальшого їх аналізу (packet capture) • Функціонал резервного копіювання та відновлення файлів

	конфігурації на виділений пристрій за допомогою FTP • Графічний інтерфейс відображення інформації щодо працездатності та основних характеристик системи у реальному часі • Інтегровані звіти
Технічна сервісна підтримка від виробника	• Рішення повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 12 місяців з рівнем сервісу 24*7 • Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7 • Постійний авторизований доступ до сайту виробника 24*7 • Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки • Отримання основних та проміжних релізів програмного забезпечення • Можливість реєстрації сервісних випадків в режимі 24*7