

Технічні вимоги

на

«Технічне переоснащення системи моніторингу роботи свердловин»

ПАТ «Укргазвидобування»

1. ЗАГАЛЬНІ ВІДОМОСТІ

1.1. ПОВНЕ НАЙМЕНУВАННЯ РОБІТ.

Виконання проектних і будівельних робіт (розробка проектно-кошторисної документації, укомплектування необхідним устаткуванням та матеріалами, будівельно-монтажні роботи, придбання та розробка програмного забезпечення, пусконаладжувальні роботи) по об'єкту будівництва «Технічне переоснащення системи моніторингу роботи свердловин» (далі – Система).

2. МЕТА ТА ПРИЗНАЧЕННЯ ВПРОВАДЖЕННЯ СИСТЕМИ

2.1. МЕТА ВПРОВАДЖЕННЯ СИСТЕМИ

Система впроваджується з метою:

- Контролю за режимами роботи свердловин;
- Своєчасне виявлення і попередження нештатної роботи свердловини для недопущення зниження видобутку вуглеводнів;
- Підвищення ефективності використання технологічного обладнання, оперативне реагування при змінах режимів, попередження позаштатних ситуацій та надійності керування процесом видобутку вуглеводнів;
- Підвищення ефективності обслуговування, зменшення часу на ТО та ремонт технологічного обладнання;
- Забезпечення автоматизованого телеконтролю, телесигналізації, аналізу роботи технологічних процесів та устаткування в режимі реального часу;
- Збирання, оброблення, зберігання, відображення інформації (телевимірювання – ТВ, телесигналізації – ТС) технологічних процесів та устаткування, формування масивів інформації і передачі технологічної інформації на вищий рівень, вирішення задач, що забезпечують безпеку функціонування об'єкту телеметрії в заданих регламентом режимах роботи;
- Створення електронної бази реального часу про режим роботи свердловин протягом тривалого часу та мати абсолютну сумісність з системами управління підприємством (ERP).

2.2. ПРИЗНАЧЕННЯ СИСТЕМИ

Система повинна забезпечувати виконання наступних завдань:

- Забезпечення телеметрії процесу видобутку в заданому обсязі функцій та можливість їх подальшого розширення (збирання, оброблення, структурування, зберігання, відображення, архівування, документування технологічної інформації з використанням уніфікованих сигналів та протоколів передачі даних), аналізу роботи технологічних процесів та устаткування видобутку вуглеводнів в режимі реального часу, вирішення задач, що забезпечують безпеку функціонування об'єкту в заданих регламентом режимах роботи;
- Можливість передачі даних вимірюваних параметрів в єдину інфраструктуру збору даних;
- Миттєвий доступ в єдиний інформаційний простір до структурованої інформації (актуальною і ретроспективною) з метою її аналізу і прийняття рішень;

- Надавати можливість користувачам виконувати аналіз показників згідно з певними заданими критеріями, проводити порівняльний аналіз показників різних технологічних об'єктів і формувати як стандартні звіти, так і звіти за довільним набором показників за запитом користувачів;

3. ВИМОГИ ДО СИСТЕМИ

3.1. СКЛАД СИСТЕМИ

До складу комплексу Системи повинні входити:

Підсистема нижнього рівня

Контрольований пункт телеметрії одиночної свердловини (КП ТОС) з контрольно-вимірювальними приладами (КВП):

- Контрольований пункт телеметрії одиночної свердловини (КП ТОС), що складається з:
 - Шафи КП ТОС;
 - Системи живлення КП ТОС;
 - Контролера RTU;
 - Системи передачі даних;
 - Засоби безпеки КП ТОС.
- Контрольно-вимірювальні прилади (КВП) з *дротовими та/або бездротовими каналами передачі даних до КП ТОС, що складаються з:
 - перетворювачі тиску для вимірювання:
 - трубного та затрубного тисків – 2 шт.;
 - між експлуатаційною та проміжною колонами – 2 шт.;
 - тиску в шлейфі після регулюючого штуцера – 1 шт.;
 - перетворювачі температури для вимірювання температури флюїду – 2 шт.;
 - манометри – 2 шт.

**Бездротовий канал можливо застосовувати для кустових свердловин, розташованих на відстані не більше 500 метрів одна від одної, можливість використання бездротового КВП визначається проектом.*

Підсистема верхнього рівня

Підсистема верхнього рівня – Автоматизована система оперативного диспетчерського моніторингу (АСОДМ) роботи свердловин (РС) складається з наступного програмного забезпечення (ПЗ):

Прикладне ПЗ:

- Клієнт середовища розробки прикладного ПЗ
- Єдиний репозиторій прикладного ПЗ

Технологічне ПЗ, що реалізує «клієнт-серверну» архітектуру та складається з наступних модулів:

- Модулі введення-виведення даних;
- Модулі додатків реального часу;
- Модулі локальних технологічних архівів;
- Модулі консолідованих технологічних архівів;
- Модулі тонких клієнтів;
- Модулі звітності;
- Робочі місця, клієнти аналізу, управління та звітів технологічних процесів.

Можлива альтернативна «клієнт-серверна» архітектура в якій один модуль містить у собі функції декількох вищенаведених модулів.

3.2. ВИМОГИ ДО ПІДСИСТЕМИ НИЖНЬОГО РІВНЯ

3.2.1. ВИМОГИ ДО КП ТОС

Вимоги до контролера

Контролер Remote Terminal Unit (RTU) з низьким енергоспоживанням, обчислювальні можливості якого дозволяють використовувати його для вимірювання нормованих значень телеметрії, виконання необхідних розрахунків, контролю параметрів телесигналізації, ретрансляції даних по цифрових інтерфейсах, відповідати наступним технічним вимогам:

- максимальне споживання енергії базового модуля 2 Вт, без модулів розширення;
- підтримувати функцію буферизації даних (обсяг даних, які зберігаються в буфері не менше 20,000 подій) з автоматичною передачею даних до серверів АСОДМ РС без втрати інформації за стандартними протоколами передачі даних DNP3 або аналогічний;
- діапазон робочих температур від -30 ... +50°C;
- працювати в режимі Ведучого пристрою (Master). Master може ініціювати запити на отримання статичних даних, подій і приймати ініціативні повідомлення від відомого пристрою (Slaves);
- мати підтримку віддаленого доступу для проведення діагностики, програмування і налагодження контролера;
- мати можливість збереження даних при порушеннях живлення;
- має підтримуватись мова релейного логіки, відповідно до стандарту IEC 61131-3;
- має підтримуватись налаштування періодичність збору даних від польових приладів КВП;
- має підтримувати передачу даних по подіям;
- мати можливість керування живленням GSM\GPRS\3G роутером;
- підтримувати додаткові модулі вводу / виводу для розширення;
- мати наступну кількість вхідних / вихідних сигналів разом з модулями розширення:
 - цифрових вхідних сигналів не менше – 12;
 - цифрових вихідних сигналів не менше – 4;
 - аналогових входів не менше - 8 (0-20/4-20 мА).
- Мати запас вхідних та вихідних сигналів – не менше ніж 20% від загальної кількості.

Вимоги до шафи КП ТОС

Конструктивне виконання шафи КП повинно складатися з двох шаф зовнішня (антивандальна) та внутрішня (корпус в корпусі) та відповідати умовам експлуатації ПТЗ, а також вимогам безпеки та забезпечувати:

- зручність обслуговування;
- зручність виконання монтажних робіт та доступу до елементів регулювання;
- взаємозамінність однотипних складових;
- надійність з'єднань і фіксації складових;
- зручність під'єднання перетворювачів, приладів та зовнішніх ліній зв'язку;

- безпеку обслуговування та проведення ремонтних робіт;
- працездатність в умовах дії атмосферних опадів, температури навколишнього середовища, прямих уражень блискавки, електромагнітної дії грозових розрядів.

***Шафа зовнішня контрольованого пункту:**

- Конструкція - вандалозахищений корпус, відсутність зовнішніх петель;
- Корпус - суцільнометалевий зварний;
- Клас опору - RC-6 відповідно до DIN EN 1627:2011 «Класифікація протизламних конструкцій»;
- Матеріал – листова сталь товщина не менше 3мм;
- Двері – двошарові сейфового типу, втоплені всередину;
- Замок – вандалозахищений внутрішній 3-х ригельний;
- Тип з'єднання до опори – заклепувальні з'єднання, діаметр не менш 15 мм;
- Розташування шафи на опорі – висота не менше 2,5 м;
- Кінцевий вимикач відкриття дверей;
- Сигналізатор вібрації шафи;
- Антикорозійне покриття – гарантія не менше 3 років

***Шафа внутрішня:**

- Конструкція – компактна розподільча шафа;
- Ступінь захисту IP – не менше IP66;
- Матеріал - листова сталь;
- Антикорозійне покриття – гарантія не менше 3 років;

Додаткові вимоги:

- Зовнішні під'єднання кабелів та ліній зв'язку до зовнішньої шафи виконати захищене в середині несучої опори через задню стінку шафи;
- Зовнішні під'єднання кабелів та ліній зв'язку до внутрішньої шафи виконати з використанням роз'ємів для важких умов експлуатації (HDC).

**Конструкцію шафи на етапі проектування погодити з департаментом Безпеки та управлінням Метрології КВП та А ПАТ «Укргазвидобування».*

Вимоги до системи зв'язку

Система зв'язку має бути у складі ПЛК або на базі промислового GSM/GPRS-роутера з підтримкою:

- мережі GSM\GPRS\3G;
- дві SIM-карти для резервування послуг, що надаються операторами зв'язку;
- моніторинг якості каналів мобільного зв'язку (втрати пакетів, затримка та інше), автоматичне переналаштування на інші канали зв'язку з кращими показниками якості передачі;
- автоматичне відстеження стану GSM-модуля і таймер захисту від програмних, апаратних збоїв;
- механізмів якості обслуговування (QoS) для забезпечення низької затримки передачі даних індустріальними протоколами такими як DPN3, ModBus;
- можливості віддаленого спостереження та контролю за пристроєм за допомогою протоколів SNMP v2, v3, MIB, Secure Shell (SSH),
- аналізу мережевих з'єднань та інспекція їх сервісів за допомогою функцій міжмережевого екрана;
- фіксації та отримання інформації о подіях інформаційної безпеки; збір та збереження журналів подій;

- апаратного забезпечення шифрування пакетів (для гарантії та стабільності часу обробки та передачі даних)
- *Можливості використання наступних криптографічних алгоритмів:*
 - Шифрування: DES, 3DES, AES-128 та AES-256
 - Автентифікація: RSA (748/1024/2048 біт), ECDSA (256/384 біт)
 - Цілісність: MD5, SHA, SHA-256, SHA-384, SHA-512
- підтримка технологій IPSEC поверх IPv4/IPv6, IPSEC Statefull Failover, DMVPN, FlexVPN
- забезпечення безпеки за допомогою цифрового підпису, верифікації програмного забезпечення, безпечної завантаження програмного коду;
- діапазоном робочих температур від -30 ° С до + 50 ° С.

Сертифікат Державної служби спеціалізованого зв'язку та захисту інформації (ДСТСЗІ) про відповідність вимогам нормативних документів систем технічного захисту інформації в Україні. Указ Президента "Про Положення про технічний захист інформації в Україні" від 27.09.1999 N 1229/99.

Вимоги до системи живлення

Живлення шафи телеметрії і всього допоміжного обладнання, повинно бути передбачено на альтернативному джерелі енергії - сонячна батарея, яка забезпечує функціонування системи в цілодобовому форматі (Основне джерелом електроживлення). Сонячна батарея повинна забезпечувати необхідним зарядом блок акумуляторних батарей (АКБ) (Резервне джерело електроживлення). Ємність АКБ повинна забезпечувати роботу системи не менше 3х днів без підзарядки.

Сонячна батарея повинна бути вбудована в вандалозахищений корпус, та відповідати наступним технічним вимогам:

- клас не нижче Tier2;
- Температурний коефіцієнт не більше - 0,4%/1°C;
- ККД панелі не менше - 15%
- Гарантія від виробника не менше -10 років.

***Вимоги корпусу сонячної батареї:**

- Конструкція - вандалозахищений корпус, клас опору RC-6 відповідно до DIN EN 1627:2011 «Класифікація протизламних конструкцій»;
- Матеріал – листовая сталь не менше 3мм;
- Скло – категорія міцності P1A відповідно до ДСТУ EN 356:2005 «Захисне скління. Випробування і класифікація по стійкості проти ручного зламування»;
- Тип з'єднання конструкції – заклепувальні з'єднання, діаметр не менш 15 мм;
- Тип з'єднання до опори – заклепувальні з'єднання, діаметр не менш 15 мм;
- Антикорозійне покриття – гарантія не менше 3 років;
- Запобігання конденсатоутворенню в середині корпусу;

**Конструкцію шафи на етапі проектування погодити з Департаментом Безпеки та Департаментом Метрології, КВПтаА ПАТ «Укргазвидобування».*

Системою живлення КП повинно бути передбачено:

- автоматичне перемикання з основного джерела електроживлення на резервне і зворотньо без збоїв у роботі та втрати інформації;
- автоматична зарядка АКБ;
- моніторинг поточного стану АКБ.

Максимальна повна споживана потужність складових частин технічних засобів КП ТОС має бути розрахована на етапі проектування.

АКБ повинні бути розмішені в термоізоляційному блоку під землею для забезпечення позитивної температури експлуатації.

Вимоги до засобів несанкціонованого доступу обладнання КП

Засоби безпеки КП повинні забезпечувати попередження та недопущення несанкціонованого доступу до обладнання КП, формування повідомлень та складатися з наступних елементів:

- Сигналізатор вібрації шафи КП;
- Кінцевий вимикач дверей шафи.
- Датчик руху:
 - Опціональна маска імунітету до тварин (до 36 кг);
 - Вологозахист і герметична конструкція корпусу
 - Дальність виявлення до 15 метрів;
 - Не вимагає обслуговування;
 - Корпус, стійкий до спроб руйнування.
- Сирена: потужність не менше 105 дБ, корпус стійкий до спроб руйнування ;
- Паркан із сітки-рабиці з эгозою;
- Таблички інформаційні знаки на паркані.

3.2.2. ВИМОГИ ДО КВП.

Вимоги до бездротових приладів КВП

Прилади КВП повинні складатися з наступних технічних засобів:

- безпроводні перетворювачі тиску і температури;
- мережеве обладнання (бездротові шлюзи, точки доступу).

Бездротовий польовий КВП повинен складатися з перетворювачів тиску, температури і інтелектуальних бездротових шлюзів для організації зв'язку бездротових перетворювачів з контролером.

Бездротові перетворювачі повинні працювати від внутрішнього блоку батарей. Бездротовий зв'язок повинен бути з шифруванням, забезпечувати безпечне використання і численні функції, включаючи моніторинг стану пристроїв, розширені можливості діагностики і регулювання параметрів пристрою.

Вимоги до польових перетворювачів

- клас захисту корпусу – вибухозахищений (Ex d);
- регульований інтервал часу збору і передачі даних від 1 до 60 с;
- термін служби елементів живлення – не менше 4 років (при часі поновлення від 30 с);
- забезпечувати безпечну передачу інформації з шифруванням;
- мати відкритий промисловий протокол зв'язку ISA 100.11a, Wi-Star, WirelessHART;
- базова дальність передачі даних (без використання посиленних антен) на відкритій місцевості - повинна бути не менше 500 м;
- похибка вимірювань не повинна перевищувати $\pm 0,25\%$ від шкали;
- потужність передача в базовому виконанні повинна бути не менше 10 дБм;
- діапазон робочих температур -40 ... 60°C;
- ЖК - дисплей;
- Максимальне значення верхньої границі вимірювання надлишкового тиску визначається на етапі проектування;
- Максимальний допустимий тиск не менше – 250 кг\см²;
- Діапазон вимірювання перетворювачів температури -50...+ 180 °С.

Вимоги до точки доступу (бездротового шлюзу)

Бездротова точка доступу (бездротовий шлюз) повинна бути виконана в промисловому виконанні і забезпечувати надійний зв'язок з бездротовими пристроями. Дозволяти створювати розподілену бездротову мережу, даючи можливість для ефективного управління топологією. Мати різні інтерфейси зв'язку.

Бездротова точка доступу повинна мати такі характеристики:

- кількість бездротових пристроїв які підключаються - не менше 100;
- передача даних повинна здійснюватися в діапазоні частот 2400 ... 2483,5 МГц;
- забезпечувати безпечну передачу інформації з шифруванням;
- мати один з відкритих промисловий протокол зв'язку ISA 100.11a, Wi-Star, WirelessHART сумісний з перетворювачами;
- потужність передавача не більше - 10 дБм;
- дальність зв'язку не менше - 500м;
- можливість застосування при температурі навколишнього середовища -40... +60°C;

Обладнання бездротового КВП, бездротові шлюзи, точки доступу повинні бути розміщені таким чином, щоб забезпечувати надійний прийом і передачу даних (Місця розміщення узгоджуються на етапі погодження технічних рішень).

Вимоги до провідного КВП.

Склад приладів КВП:

- Перетворювачі тиску;
- Перетворювачі температури;
- манометр технічний;

Спеціалізований антивандальний корпус з сигналізацією про відкриття, можливістю пломбування;

***Вимоги до антивандальної шафи розміщення КВП:**

- Конструкція - вандалозахисений корпус, відсутність зовнішніх петель, суцільнометалевий зварний
- Клас опору - RC-6 відповідно до DIN EN 1627:2011 «Класифікація протизламних конструкцій»;
- Кріплення - кріплення на трубопровід за допомогою хомутів максимально захищеного від руйнування при зломі, або виносна конструкція.
- Матеріал – листовая сталь не менше 3мм;
- Двері – листовая сталь не менше 3мм;
- Замок – внутрішній 2-х ригельний (замки з однаковим ключем на всі антивандальні шафи розташовані на одній свердловині);
- Тип з'єднання конструкції – заклепувальні з'єднання, діаметр не менш 15 мм або зварна;
- Кінцевий вимикач дверей шафи;
- Антикорозійне покриття – гарантія не менше 3 років;

**Конструкцію шафи на етапі проектування погодити з Департаментом Безпеки та Департаментом Метрології КВПтаА ПАТ «Укргазвидобування».*

Вимоги до перетворювачів тиску:

- Вихідні сигнали (0-20/4-20 мА);
- Вибухозахист - клас Exd;
- Матеріал деталей, що контактують із середовищем – SST316L;

- Енергоспоживання - знизеним енергоспоживанням;
- Діапазон вимірювань – визначається на етапі проектування ;
- Максимальний допустимий тиск не менше – 250 кг\см²;
- можливість застосування при температурі навколишнього середовища -40 ... +60 °С;
- Похибка вимірювань - 0,25%;
- Габарити – малогабаритні;

Вимоги до перетворювачів температури:

- Вимірювальні елементи Pt100/Pt1000;
- Температурний діапазон -50... +150 °С;
- Перетворювач з вихідним сигналом - 4 ... 20 мА;
- Вибухозахист - клас Exd.

Вимоги до манометрів:

- тип-манометр технічний;
- клас точності - не гірше 1,5;
- ступінь захисту - не гірше IP-53;
- діапазон вимірювань - визначається на етапі проектування;
- приєднання-радіальне, М20х1,5;
- діапазон робочих температур -40 до +60 °С.

3.3. ВИМОГИ ДО ПІДСИСТЕМИ ВЕРХНЬОГО РІВНЯ

Програмне забезпечення повинно мати абсолютну сумісність з системами управління підприємством (ERP) на базі вимог стандарту ISA-95\IEC62264 (Інтеграція систем управління підприємством). Для забезпечення мережевої взаємодії між Технологічні об'єкти (УКПГ,УКПН та інші) та серверами збору даних АСОДМ РС використовується існуюча корпоративна інфраструктура. Для забезпечення мережевої взаємодії між КП ТОС та серверами збору даних використовується окрема резервована мережа моніторингу на базі технології M2M. Вся зібрана інформація в АСОДМ РС повинна являти собою єдиний структурований інформаційний простір, що автоматично гарантує унікальність і ієрархічність ідентифікатора для кожної одиниці Системи. Наприклад: «УГВ.ПГВ.ЦВНГК.ЯБЛУНІВСЬКИЙ.УКПГ.Яблунівка.Свердловина №345. тиску в шлейфі після регулюючого штуцера». З точки зору клієнтських функцій, ПАТ, ГПУ, ЦВНГК та Технологічні об'єкти є рівнозначними інформаційними вузлами АСОДМ РС, в яких будь-який рівень доступу користувачів (крім адміністраторського) до єдиного інформаційного простору визначається виключно призначеними правами, а не технічною можливістю.

3.3.1. ЗАГАЛЬНІ ВИМОГИ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Для досягнення цілей інтеграції і функціональної сумісності різних систем в складі захищеної інформаційної інфраструктури та заради економічного ефекту, обумовленого мінімізацією при модернізації і розширенні, Система повинна впроваджуватись на основі принципу відкритих систем та відповідати загальним вимогам до побудови складних ієрархічних систем. В прив'язці до конкретних завдань Системи, необхідно забезпечити наступні принципи її побудови:

- програмне забезпечення Системи повинно мати відкриту архітектуру, що забезпечить можливість незалежної розробки (доброби) окремих функціональних підсистем різними організаціями – виконавцями робіт, а також спеціалістами Компанії;
- розробка програмної частини Системи повинна супроводжуватися необхідними коментарями коду та бути логічною структурованою і зрозумілою;
- логічна структура Системи та її внутрішні та зовнішні взаємодії повинні бути побудовані на принципах швидкодії, економічності та простоти роботи;
- зміни в окремих модулях чи окремих частинах програмної частини Системи не повинні приводити до змін в інших, незалежних від даної, частинах системи;
- наявність єдиної інформаційної бази даних, що забезпечить виключення дублювання інформації, виконання схожих функцій в різних підсистемах;
- працездатність Системи має бути забезпечена на стандартизованих комплектах апаратних засобів (сервера, робочі станції, мережне та телекомунікаційне обладнання, засоби резервного архівування даних тощо), з можливістю подальшого розширення та модернізації;
- здатність системи як в цілому, так і окремих її складових частин до масштабування;
- використання уніфікованих загальносистемних та прикладних програмних рішень з метою оптимального використання парку комп'ютерної техніки;
- використання спільної для всіх підсистем, уніфікованої системи обміну інформацією;
- логічність, простота інтерфейсу та наглядна функціональність для користувачів системи (usability);
- ведення повної історії дій кожного користувача та запис цих дій до архіву (журналу) дій;

- забезпечення можливості поетапного розвитку та впровадження.
- оперативне забезпечення співробітників Компанії достовірною інформацією, необхідною для прийняття рішень;
- можливість інтеграції всіх вже існуючих автоматизованих, інформаційних та інформаційно-аналітичних систем, програмних комплексів та баз даних у єдину інфраструктуру із скороченням кількості обслуговуючого персоналу та чергових змін для економії коштів Компанії на їх утримання;
- впровадження ідентифікації та автентифікації користувачів Системи, регламентованого доступу і обміну даними, забезпечення необхідного рівня захисту інформації;
- використання типових рішень щодо інформаційної інтеграційної складової для всіх рівнів інформаційного забезпечення;
- ПЗ повинно бути сертифіковане на відповідність міжнародним стандартам ISA-95, IEC 62264, який регламентує склад, зміст і взаємодія виробничих інформаційних моделей, систем;
- Постачальник ПЗ Системи повинен бути офіційним представником та мати необхідний рівень сервісної підтримки в Україні;
- ПЗ повинно мати відповідні ліцензії і, як мінімум, 12 місяців прямої підтримки від Розробника АСОДМ РС з моменту здачі Системи в експлуатацію.
- ПЗ повинно використовувати високопродуктивну базу даних реального часу для зберігання виробничої і технологічної інформації;
- Резервування всіх компонентів системи (Резервування серверів додатків, Резервування серверів вводу-виводу, Резервування сервера історичних даних, Резервування клієнтів);
- Графічний інтерфейс користувача АСОДМ РС повинен адаптуватися під різну розподільну здатність екрану на робочому місці користувача (як мобільного пристрою, так і ноутбука, так і окремого монітору).
- Постачальником ПЗ повинно бути розгорнуто окреме тестове та продуктивне середовища. Використання ПЗ на тестовому середовищі не повинно вимагати окремого ліцензування та витрат, або повинно бути включено в ліцензійне використання ПЗ продуктивного середовища.
- У разі наявності ліцензійних ключів на ПЗ, ключі не повинні бути прив'язані до апаратної частини Замовника для забезпечення безперешкодної заміни обладнання на якому працює ПЗ. У разі прив'язки ключів до апаратної частини, персонал Замовника повинен мати можливість самостійно перенести ключі на іншу апаратну частину, відповідну документацію та тренінги з цього функціоналу забезпечує Постачальник ПЗ.
- Кількість фізичних серверів і робочих станцій визначається на етапі проектування. Різні логічні компоненти системи можуть групуватися на одних і тих же фізичних серверах.
-

3.3.2. ЗАГАЛЬНІ ВИМОГИ ДО ФУНКЦІОНАЛЬНИХ МОДУЛІВ ПЗ

- ПЗ має забезпечувати модульний підхід при єдиному інформаційному просторі і не менше 250 серверів додатків географічно розподіленої середовища виконання.

- ПЗ має дозволяти реалізувати Систему на базі архітектури «клієнт-сервер», з можливістю підключення до серверної частини системи одночасно не менше 250 клієнтських робочих місць, з використанням стека протоколу TCP/ IP.
- ПЗ повинно забезпечувати доступ до системи з використанням WEB технології за допомогою клієнтських робочих місць, що працюють на платформі MICROSOFT.
- ПЗ має надавати безперервний доступ до системи.
- Серверна частина ПЗ повинна мати службу автентифікації та авторизації користувачів та надавати засоби для адміністрування облікових записів
- Всі функції, пов'язані з обміном даними, обчисленням розрахункових параметрів, передачі даних, формування звітів і мнемосхем, повинні бути реалізовані на серверній частині ПЗ. Клієнтські частини надають тільки функції користувальницького інтерфейсу.

3.3.3. ВИМОГИ ДО СУМІСНОСТІ З СИСТЕМНИМ ПЗ

- Використання промислової СКБД (MS SQL або Oracle).
- Аудит:
 - Можливість аудиту дій користувачів.
 - Можливість аудиту операцій
 - Можливість аудиту змін значень реквізитів
 - Можливість перегляду реєстрів аудиту
- Можливість інтеграції з іншими системами на рівні сервера застосувань.
- Наявність функції відправлення повідомлень на електронну пошту.
- Промисловий рівень надійності та цілісності даних. Високий рівень масштабованості системи. Можливість збільшення кількості працюючих із системою користувачів шляхом модернізації існуючих та додавання додаткових серверних компонентів.
- Наявність розмежування прав користувачів засобами Системи. Наявність рольової моделі доступу в Системі.
- Система повинна підтримувати наступну автентифікацію:
 - традиційне введення облікового імені та паролю в системі.
 - можливість інтеграції з AD (Microsoft Active Directory) .
- Під час розгортання модулів продуктивного середовища – ПЗ АСОДМ РС Виконавцю провести із ІТ персоналом Замовника перевірку відмовостійкості розгорнутої системи (апаратні, програмні, мережеві та інші відмови). Під час впровадження проекту провести із ІТ персоналом Замовника всі практичні дії зафіксовані у документації щодо загальносистемного адміністрування.
- Серверна частина Системи повинна працювати у відмовостійкій конфігурації з можливістю балансування навантаження.
- Система повинна працювати у локальній обчислювальній мережі замовника за протоколом TCP/IP. При необхідності система повинна працювати з мережевими з'єднаннями на низьких швидкостях (GPRS\EDGE модемні з'єднання).
- Підтримка можливості роботи на обчислювальному обладнанні під управлінням операційних систем сімейства Microsoft Windows (7, 8.1, 10 –для клієнтських місць; 2008R2, 2012R2, 2016 – для серверів).
- Підтримка серверної частини (а також апаратних ліцензійних ключів при їх наявності) у віртуальному середовищі – VMware.
- Серверна операційна система – Microsoft Windows.

- ПЗ АСОДМ РС повинно мати можливість розгортання та експлуатації з використанням зовнішніх хмарних потужностей (наприклад: Microsoft Azure, VMware vCloud та інші)
- Низькі вимоги до програмного забезпечення клієнтського робочого місця (користувач повинен працювати на клієнтському робочому місці під звичайним користувачем без будь яких адміністративних прав, а також інсталювати оновлення клієнтської частини), підвищення безпеки даних. Повинні бути доступні для друку як локальні так і мережеві пристрої друку включаючи ті, що функціонують через сервер друку (print server).
- Клієнти Системи повинні працювати на клієнтському робочому місці на якому працює корпоративна антивірусна система.

3.3.4. ВИМОГИ ДО МОДУЛІВ ПЗ

Єдиний репозиторій прикладного ПО

- Зберігання табличних і текстових частин проектів прикладного ПЗ в реляційній СУБД на базі системного ПЗ;
- Зберігання графічної частини в файлах векторного формату;
- Можливість роботи необмеженої кількості клієнтів середовища розробки;
- Створення, конфігурація і адміністрування всього прикладного ПЗ в рамках одного середовища розробки;
- Централізоване віддалене розгортання всього проекту по розподіленій інфраструктурі і середовищі виконання.

Клієнти середовища розробки прикладного ПЗ та конфігурації виробничих процесів

- об'єктно-орієнтований підхід до створення інформаційних моделей відповідно до міжнародних стандартів ISA-95, IEC 62264;
- Можливість створення типізованих шаблонів сутностей (місця розташування, обладнання, потоків, процесів), що включають в себе масиви даних, методи їх обробки і повний набір анімованої графіки для подальшого тиражування;
- Повне, або часткове успадкування властивостей і методів типізованих шаблонів як в наступних шаблонах, так і примірниках сутностей;
- Наявність вбудованого редактора векторної графіки.

Модулі введення-виведення повинні забезпечувати:

- централізований обмін даними з усіма апаратно-програмними засобами КП ТОС за допомогою комунікаційних драйверів протоколів ПЛК;
- Підтримувані драйвери: DNP3, Modbus, SNMP, OPC DA, OPC HDA, OPC UA та інші;
- наявність в складі цього модуля інструментарію швидкої розробки призначених для користувача драйверів для обміну по COM, UDP, TCP портів;
- гаряче резервування.

Модулі додатків реального часу повинні забезпечувати:

- Синхронне і асинхронне багатопотокове виконання прикладного ПЗ;
- Вбудовану систему контролю коректності ходу виконання прикладного ПЗ для кожного потоку;

- Автоматичне гаряче резервування і перезапуск (watchdog) кожного потоку в разі некоректного ходу виконання прикладного ПЗ;
- Розвинене середовище розробки додатків з централізованим репозиторієм проектів;
- Автоматичне гаряче резервування джерел даних (серверів введення-виведення)
- Дублювання потоків архівних даних і подій – підтримка одночасно двох незалежних локальних технологічних архівів
- Буферизація історичних даних і подій з подальшою автоматичною передачею в сервери локальних технологічних архівів.

Модулі локальних архівів

- Зберігання конфігураційних даних, що включають інформаційні моделі в реляційної СУБД на базі системного ПО
- Доступ до архівних даних за допомогою стандартних SQL запитів до реляційної СУБД на базі системного ПО
- Вбудовані функції накопичення статистичних даних
- Розширений інструментарій аналізу часових рядів даних і подій у вигляді графіків і таблиць
- Автоматична реплікація інформації в сервери архівів підприємства які розташовані в мережевому сегменті, що виконує роль DMZ («демілітаризованої зони»).

Модулі архівів підприємства

- Зберігання конфігураційних даних, що включають інформаційні моделі в реляційної СУБД на базі системного ПЗ;
- Доступ до архівних даних за допомогою стандартних SQL запитів до реляційної СУБД на базі системного ПЗ;
- Вбудовані функції накопичення статистичних даних;
- Розширений інструментарій аналізу часових рядів даних і подій у вигляді графіків і таблиць.

Модулі клієнтів

Модулі клієнтів повинні підтримувати наступні типи робочих місць:

- Стаціонарні робочі станції – потребує спеціалізованого програмного забезпечення НМІ - Людино-машинний інтерфейс;
- Тонкі клієнти – отримують доступ до інформації модулів клієнтів за допомогою служб віддаленого робочого столу за протоколом RDP;
- WEB-клієнти - Віддалений доступ до візуалізації і звітності з повною функціональністю за допомогою будь-якого браузера з підтримкою HTML5.

Підтримка різних варіантів ліцензування клієнтів: на пристрій, на користувача, за кількістю одночасно активних сесій

Модулі звітності

- Генерація звітів:
 - автоматично за розкладом, по події;
 - за необхідністю;
- Конструювання звітів;
- Конфігурування агрегованих даних;
- Наявність власного WEB інтерфейсу з підтримкою за допомогою будь-якого браузера з підтримкою HTML5 в якості штатного клієнта.

Клієнти аналізу та управління процесами

- Підтримка всіх можливих для системного ПЗ мультимоніторних режимів виведення інформації
- Забезпечення санкціонованого доступу до Мнемосхеми і звітів
- Логування дій користувачів

3.3.5. ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТА КІЛЬКІСТЬ МОДУЛІВ ПЗ

АСОДМ РС являється єдиним інформаційним вузлом з наступними функціональними можливостями:

Модулі розташовані в мережі моніторингу:

- **Модулі введення-виведення:**
 - Кількість – 2;
 - Об'єми обміну по Інтерфейсах DNP3 або аналогічних відповідно до «Завдання на проектування».
- **Модулі додатків реального часу:**
 - Кількість – 2.
- **Модулі локальних архівів:**
 - Кількість – 1;
 - Кількість звітних форм визначається на етапі проектування;
- **Модулі архівів підприємства:**
 - Кількість – 1;
 - Кількість звітних форм визначається на етапі проектування;
- **Репозиторій прикладного ПО**
 - Кількість – 1
- **АРМ адміністратора АСОДМ РС (Клієнт середовища розробки прикладного ПЗ та конфігурації виробничих процесів)**
 - Кількість – 2
 - Кількість моніторів (дисплеїв з роздільною здатністю 1920x1080) - 2
 - Конфігурація всіх математичних моделей єдиного інформаційного простору АСОДМ РС
 - Конфігурація засобів і методології обробки інформації
 - Конфігурація засобів і складу інформації, що збирається
 - Конфігурація засобів архівування та аналізу зібраної інформації
 - Конфігурація клієнтських засобів доступу до інформації
 - Управління правами всіх користувачів АСОДМ РС на базі доменних політик безпеки Windows.

Модулі розташовані в мережі DMZ:

- **Модулі звітності:**
 - Кількість – 1;
 - Кількість звітних форм визначається на етапі проектування.
- **Модулі тонких клієнтів**
 - Кількість – 1
- **АРМи фахівців:**
 - Кількість – відповідно до «Завдання на проектування»;
 - Використання в якості тонкого клієнта будь-якого WEB-браузера з підтримкою HTML-5.

АРМи, клієнти розташовані в корпоративній мережі:

- **АРМи оперативного персоналу (ОП):**
 - Кількість – відповідно до «Завдання на проектування».
 - Стаціонарні робочі станції – НМІ клієнти;
 - Тонкі клієнти.
- **Клієнти звітності:**
 - Кількість – відповідно до «Завдання на проектування».
 - Онлайн доступ до серверів звітності за допомогою WEB браузера.
 - Доступ до файлового сховища незмінних звітів, сформованих за розкладом.
 - Індивідуальна підписка на розсилки звітів за розкладом.

Автоматична одностороння реплікація інформації в сервери архівів підприємства які розташовані в мережевому сегменті, що виконує роль DMZ («демільтаризованої зони»). Усі модулі розташовані в мережевому сегменті DMZ не мають можливості запису інформації в мережу моніторингу.

3.3.6. НЕОБХІДНІ ПОТУЖНОСТІ ДЛЯ СЕРВЕРІВ НА ЯКИХ ВИКОНУЮТЬСЯ МОДУЛІ ПЗ

ПЗ встановлюється на сервера Замовника. Для виділення потужностей на серверах, Виконавцю необхідно надати розрахунок потужностей (відповідно Таблиці Додаток 1.) які забезпечать коректну роботу модулів ПЗ.

4. ВИМОГИ В ЧАСТИНІ ЗВ'ЯЗКУ ТА ІНФОРМАЦІЙНИХ СИСТЕМ.

- При віддаленому зборі даних, передача даних повинна здійснюватися по каналах зв'язку, які забезпечують збір та обмін по стандартним інтерфейсах та протоколах обміну. Обов'язкове використання шифрування та сучасної методики автентифікації на різних рівнях.
- Використання сегменту мережі моніторингу для каналів зв'язку нижнього рівня, або захищених сегментів, у випадках, коли використовується не мережа моніторингу.
- При виборі основного\резервного каналу зв'язку слід походити від територіального розташування об'єктів технологічного контролю.
- Канали передачі даних повинні забезпечити стійке з'єднання між елементами системи, мати резервування та можливість автоматичного перемикавання на резервний канал зв'язку та навпаки при подальшому відновленні. Вибір одного з каналів у якості основного повинен здійснюватися на етапі проектування.
- Система повинна мати можливість діагностування якості зв'язку.
- Детальні вимоги до засобів та каналів будуть сформовані на етапі проектування.
- Проектні рішення погодити з Департаментом Інформаційних технологій ПАТ «Укргазвидобування».

5. ВИМОГИ ДО ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

- Необхідно забезпечити достатній рівень безпеки Інформаційної мережі та мережі моніторингу Системи від незахищених і ненадійних зовнішніх мереж у відповідності до міжнародних стандартів інформаційної безпеки ISO 27000-series, ISA099-series і ІЕС- 62443.
- Повинні бути передбачені засоби захисту від несанкціонованого доступу до інформації, руйнування інформації, в тому числі по шляхах доступу через людино-машинний інтерфейс, зовнішні носії інформації, корпоративні комп'ютерні мережі.

- Повинна бути виключена можливість внесення змін до інформаційних баз даних Системи.
- В процесі впровадження системи повинні бути розроблені заходи, що забезпечують захищеність інформації та обладнання від факторів, що представляють загрозу для конфіденційності, цілісності, доступності інформації.
- У всіх елементах системи має бути передбачено використання технології і реалізації процедур ідентифікації і автентифікації. У компонентах Системи має бути забезпечено використання довіреного програмно-апаратного середовища.
- Обмін трафіком з мережами загального призначення повинен реалізовуватися через прикордонні міжмережеві екрани, що забезпечують функції вибіркового пропуску лише того трафіка, який ставиться до ідентифікованих інтерфейсів міжрівневої взаємодії. Увесь інший трафік повинен блокуватися (політика «заборонене все, що явно не дозволене»).
- Для реалізації взаємодії з мережами загального призначення необхідно організувати окремий мережевий сегмент, що виконує роль DMZ («демілітаризованої зони»). У цей сегмент повинні бути включені внутрішні (inside) інтерфейси міжмережевих екранів, а також виділені інтерфейси тих компонентів Системи, яким необхідна інформаційна взаємодія із засобами мереж загального призначення.
- Міжмережеві екрани мають забезпечувати контроль промислових застосувань: DNP3 та Modbus.
- Міжмережеві екрани мають виявляти атаки на промислові протоколи (DNP3, Modbus) та надавати вбудовану підтримку створення та редагування правил/сигнатур на мові SNORT.
- Міжмережеві екрани мають включати усі необхідні підписки, ліцензії для функціонування системи захисти від атак та сервісна підтримка на термін не менше 3 років. Використання функціональності системи захисту від атак не повинно впливати на пропускову здатність та швидкість функціонування міжмережевого екрану.
- Міжмережеві екрани мають постачатися в відмовостійкій конфігурації (основний та резервний екрани з можливістю автоматичного переключення)
- Міжмережеві екрани повинні підтримувати встановлення додаткових мережевих інтерфейсів.
- Моніторинг і керування активним устаткуванням мережі моніторингу.
- Міжмережеві екрани повинні мати Сертифікат Державної служби спеціалізованого зв'язку та захисту інформації (ДСТСЗІ) про відповідність вимогам нормативних документів систем технічного захисту інформації в Україні. [Указ Президента "Про Положення про технічний захист інформації в Україні" від 27.09.1999 N 1229/99](#)

6. ВИМОГИ ДО ПАТЕНТНОЇ ЧИСТОТИ

Проектні рішення побудови Системи мають відповідати вимогам щодо патентної чистоти згідно чинного законодавства і розпорядчим документам, що регламентують створення Системи.

Уточнення вимог по патентної чистоти має здійснюватися в договорах на проведення робіт по створенню Системи, її складових та компонентів. При цьому розробникам необхідно навести відомості про наявність ліцензій на інструменти розробки програмного забезпечення, які використовуються, СУБД та інші програмні продукти третіх сторін.

Всі програмно-технічні засоби загального програмного забезпечення, які гарантують працездатність Системи повинні мати дозвіл на використання (ліцензію) з необхідною кількістю користувачів.

7. НАВЧАННЯ ПО ОБСЛУГОВУВАННЮ СИСТЕМИ

Виконавець надає послуги з проведення тренінгів з:

- загальносистемного адміністрування:
 - по розгортанню, конфігуруванню, резервному копіюванню і відновленню системи (повне і часткове), встановленню та відкату оновлень, логування з аналізом серверної частини Програмної Продукції.
 - по розгортанню, конфігуруванню клієнтської частини Програмної Продукції, встановленню та відкату оновлень.
- налаштування, конфігурування, встановлення оновлень обладнання підсистема нижнього рівня.

8. ПОРЯДОК КОНТРОЛЮ ТА ПРИЙМАННЯ СИСТЕМИ

- Введення в дію Системи виконує Постачальник спільно з Замовником та залученням спеціалізованих будівельно-монтажних та пусконаладжувальних організацій у відповідності до погодженого графіка виконання робіт. Введення в експлуатацію Системи повинно здійснюватися з дотриманням вимог охорони праці та промислової безпеки, викладених у НПАОП 0.00-1.35, НПАОП 23.2-1.10, НПАОП 11.1-1.14, НПАОП 11.2-1.18, НПАОП 11.1-1.01, НПАОП 60.3-1.01, НПАОП 63.2-1.06, СОУ-Н МПЕ 60.3.006:2005, ДБН В.2.5-20-2001 та інших нормативно-правових актах з охорони праці та промислової безпеки..
- Введення в дію Системи відповідно до СОУ 09.1-30019775-272:2017 «Системи і засоби автоматизації, телеметрії та телемеханізації. Прийняття в промислову експлуатацію виробничих об'єктів».

9. ВИМОГИ ДО ДОКУМЕНТУВАННЯ.

- У складі Системи необхідно постачати комплект технічної документації, який використовується під час виконання монтажних робіт, налагодження та експлуатування. Технічна документація повинна використовуватися для освоєння технічних характеристик та конструкції Системи, вивчення правил її експлуатування (використання за призначенням, складу та термінів технічного обслуговування, ремонтування, умов зберігання тощо). Технічна документація має містити вказівки щодо дій експлуатаційного та обслуговуючого персоналу в аварійних ситуаціях або в разі порушення умов експлуатування Системи та не містити положень, які допускають неоднозначне тлумачення.
- **Документація по загальносистемному адмініструванню**
 - а) Надання документації по загальносистемному адмініструванню, а саме:
 - Архітектура системи (включаючи чіткий перелік мережевих з'єднань, протоколів та портів необхідних для функціонування Програмної Продукції),
 - Керівництво загальносистемного адміністратора з розгортання, конфігурування, резервного копіювання і відновлення системи (повне і часткове), встановлення та

відкат оновлень, логування з аналізом, зміна існуючих та додавання додаткових елементів системи при зростанні навантаження та кількості користувачів для серверної частини Програмної Продукції.

- Керівництво загальносистемного адміністратора з розгортання, конфігурування клієнтської частини Програмної Продукції, встановленню та відкату оновлень .
- b) Документація має бути на українській мові.
- c) Розроблена документація підлягає узгодженню із ІТ підрозділом Замовника.
- d) Остаточне узгодження документації з боку ІТ підрозділу Замовника проводиться після проведення тренінгів та відпрацювання практичних дій.
- Обов'язковий комплект технічної документації, який передається Замовнику:
 - e) проектно-кошторисна документація (постачається Проектувальником) згідно з ДСТУ Б А.2.4-4:2009 «СПДБ. Основні вимоги до проектною та робочою документації»:
 - 1) робочі кресленики, призначені для проведення будівельних та монтажних робіт;
 - 2) специфікації обладнання, виробів та матеріалів;
 - 3) кошторисну документацію;
 - f) Експлуатаційна документація (ЕД) згідно з ДСТУ ГОСТ 2.601:
 - 1) відомість експлуатаційних документів;
 - 2) формуляр;
 - 3) настанова з експлуатації;
 - 4) специфікація обладнання;
 - 5) відомість ЗІП;
 - g) експлуатаційна програмна документація:
 - 1) відомість експлуатаційних документів ПЗ;
 - 2) формуляр;
 - 3) настанова системного програміста;
 - 4) настанова оператора;
 - 5) настанова з технічного обслуговування;
 - h) конструкторська документація:
 - 1) таблиця електрична підключення;
 - 2) схема електрична принципова;
 - 3) таблиця з'єднань;
 - 4) габаритний кресленик.
- На ПТЗ та складові частини імпортного виробництва необхідно надати документацію заводів-виробників та її переклади українською (або російською) мовою, а також відповідні сертифікати відповідності.
- Обов'язковими є документи (або розділи в настанові з експлуатації (НЕ):
 - регламенти і форма проведення технічного обслуговування;
 - рекомендації щодо нормативів запасу ЗІП, що не знижується;
 - рекомендації щодо нормативів витрат матеріалів на технічне обслуговування;
 - порядок виводу Системи в ремонт або обслуговування з тимчасовою втратою функцій;
 - перелік обладнання для проведення перевірок засобів вимірювання (сервісне обладнання);
 - інструкція з повірення та калібрування каналів Системи;
 - інструкція урахування, зберігання та обігу носіїв прикладного ПЗ.
- Постачальник (Розробник) передає Замовнику експлуатаційну та конструкторську документацію у двох примірниках.

Розрахунок потужностей серверів

Модуль ПЗ	Кіл-ть віртуальних серверів , шт	Частота процесора базова, GHz	Кіл-ть фізичних процесорних ядер для кожного сервера, шт	Оперативна пам'ять RAM для кожного сервера, GB	Місткість накопичувача корисна, GB	Тип накопичувача (SSD, SAS 15k, SAS 10k, SATA)	Тип RAID для накопичувача (0, 1, 10, 5, 6 інше)	Мережа, Гбіт/с
Модуль додатків реального часу								
Модуль архівів								
Модуль тонких клієнтів								
Модуль звітів								
Репозиторій прикладного ПО								
АРМ оперативного персоналу								

Заповнюється у відповідності до наявних модулів в ПЗ та вимог до серверного обладнання.

У разі якщо СУБД серверів архівів окремо ліцензується – не входить до ПЗ АСОДМ РС, необхідно надати тип та кількість ліцензій для коректної роботи ПЗ АСОДМ РС.

Схема АСОДМ РС

