ОБҐРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, його очікуваної вартості та/або розміру бюджетного призначення в межах закупівлі

UA-2026-10-28-011284-a

Замовник: Державна установа «Урядовий контактний центр» (далі-Центр) (ЄДРПОУ 36521731)

Місцезнаходження замовника: 01001, м. Київ, вул. Еспланадна, буд. 8/10

Категорія замовника: юридична особа, яка забезпечує потреби держави або територіальної громади.

Підстава для публікації: постанова Кабінету Міністрів України «Про ефективне використання державних коштів» від 11 жовтня 2016 р. № 710»

Предмет закупівлі: 72250000-2 Послуги, пов’язані із системами та підтримкою (послуги з побудови та налаштування відмовостійкого кластера ПТК НСОЗ із впровадженням альтернативної системи IP-телефонії)
ДК 021:2015: 72250000-2 Послуги, пов’язані із системами та підтримкою.

Інформація про технічні, якісні та кількісні характеристики предмета закупівлі

1. ЗАГАЛЬНІ ВІДОМОСТІ
1.1. Визначення, позначення та скорочення:

Терміни та скорочення	Опис
ПТК НСОЗ, Система	Програмно-технічний комплекс Національної системи опрацювання звернень до органів виконавчої влади, включно з компонентами та залежностями, необхідними для його роботи.
Замовник, УКЦ	Державна установа «Урядовий контактний центр».
Виконавець	Суб’єкт господарювання, з яким укладено договір про закупівлю послуг.
CRM	Прикладна система опрацювання звернень у складі ПТК НСОЗ.
Відмовостійкий кластер	Сукупність основних і резервних вузлів, засобів реплікації, контролю стану та переключення сервісів, що забезпечують відновлення роботи після відмови компонента.
DR, резервний майданчик	Географічно відокремлений контур аварійного відновлення, здатний забезпечити роботу визначених сервісів без ресурсів основного майданчика.
RPO	Максимально допустимий період втрати даних, визначений відносно моменту інциденту.
RTO	Максимально допустимий час відновлення погоджених функцій сервісу після інциденту.
Failover, failback	Переключення на резервний контур і контрольоване повернення на основний контур відповідно.
Fencing, split-brain	Ізоляція вузла від запису; небезпечний стан одночасного незалежного запису в основному та резервному контурах.
SIP, DID, IVR, ACD	Протокол телефонного зв’язку; номер вхідної лінії; інтерактивне голосове меню; автоматичний розподіл викликів.
CDR, API, VIP	Обліковий запис про виклик; програмний інтерфейс; логічна віртуальна адреса доступу до сервісу.

1.2. Перелік документів, на основі яких надаються послуги:
1. Постанова Кабінету Міністрів України від 27 листопада 2019 року № 976 «Деякі питання Єдиної системи опрацювання звернень» (зі змінами).
2. Постанова Кабінету Міністрів України від 27 листопада 2019 року № 972 «Про реалізацію експериментального проекту із створення “єдиного входу” опрацювання звернень громадян та запитів на публічну інформацію» (зі змінами).
1.3. Перелік нормативно-технічних документів, методичних матеріалів:

1. Постанова Кабінету Міністрів України від 21 лютого 2025 року № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» (зі змінами).
2. Закон України від 1 червня 2010 року № 2297-VI «Про захист персональних даних» (зі змінами).
3. Закон України від 5 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах» (зі змінами).
4. НД ТЗІ 3.7-003-2023 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі», затверджений Наказом Адміністрації Держспецзв'язку № 924 від 28.10.2023 року — у частині, що застосовується до наявної системи захисту інформації та змін, які виконуються під час надання послуг, і не суперечить чинному законодавству.
5. Експлуатаційна документація виробників програмного забезпечення та обладнання, що використовується у ПТК НСОЗ, з питань кластеризації, реплікації, резервного копіювання, відновлення, мережевої взаємодії та IP-телефонії.
6. Політики інформаційної безпеки, правила доступу та експлуатаційні регламенти Замовника, надані Виконавцю в частині, необхідній для надання послуг.
Нормативні документи застосовуються в чинних редакціях та в межах, що поширюються на об’єкт і склад послуг. Повинно бути забезпечено врахування вимог до захисту інформації та кіберзахисту під час зміни архітектури, розміщення резервних компонентів і налаштування доступу.
1.4. Мета та предмет надання послуг
Метою надання послуг є забезпечення стійкої роботи ПТК НСОЗ, збереження критичних даних та відновлення обслуговування звернень у разі відмови окремого вузла, порушення міжмайданчикового зв’язку або повної недоступності основного майданчика. Результатом повинні бути налаштований і випробуваний відмовостійкий кластер, працездатний резервний контур та інтегрована альтернативна система IP-телефонії.
Послуги повинні охоплювати обстеження, проєктування, розгортання, конфігурування, інтеграцію, перенесення необхідних налаштувань і даних, автоматизацію та випробування. Упровадження альтернативної телефонії має забезпечувати паралельну роботу з чинною Cisco-інфраструктурою та можливість обслуговування викликів незалежно від неї в аварійному режимі.
1.5. Склад та умови надання послуг
Об’єктом налаштування є наявний ПТК НСОЗ та пов’язані продуктивні компоненти: бази даних, CRM API і middleware, інтеграційний модуль, черги повідомлень, кешування, пошук, reverse proxy, публічні сервіси, засоби автентифікації, DNS, віддалений доступ і телефонія. СЕД та аварійна пошта включаються як залежні сервіси забезпечення безперервності роботи відповідно до пункту 2.8.
Фактичні версії Oracle, PostgreSQL, MySQL/MariaDB, Cisco CUCM та інших компонентів повинні бути підтверджені обстеженням. Під час налаштування повинні бути враховані всі продуктивні системи та залежності, необхідні для їх роботи. Основні відомості про налаштовані компоненти зазначаються у довідці для адміністратора. Уточнення інвентарних даних не повинно призводити до виключення обов’язкових функцій, установлених цими вимогами.
Повинно бути забезпечено визначення необхідних обчислювальних ресурсів, місткості й продуктивності сховищ, пропускної здатності каналів, програмних компонентів та ліцензій для роботи основного і резервного контурів. Розгортання та налаштування здійснюються на ресурсах, визначених договором. Використання ресурсів і порядок надання доступів погоджуються із Замовником у робочому порядку до початку змін у продуктивному середовищі, без оформлення окремого плану впровадження.
1.6. Вимоги до застосованих рішень
Послуги повинні надаватися з дотриманням застосовних вимог законодавства України, внутрішніх політик захисту інформації Замовника, вимог до обробки персональних даних та ліцензійних умов використання програмного забезпечення. Технологічні рішення повинні бути сумісними з фактичними версіями продуктивних компонентів.

Усі компоненти, що впроваджуються, повинні забезпечувати виконання встановлених функціональних вимог, сумісність із наявною інфраструктурою та можливість подальшого адміністрування Замовником. Для нових компонентів, наведених із зазначенням торговельних назв, допускається застосування еквівалентних рішень за умови виконання всіх установлених технічних характеристик. Назви наявних продуктів визначають середовище, з яким повинна бути забезпечена сумісність.

2. ОСНОВНІ ТЕХНІЧНІ ВИМОГИ

Повинно бути забезпечено створення цілісного контуру відмовостійкості, в якому резервуються не лише віртуальні машини, а й дані, прикладні функції та залежності ПТК НСОЗ. Відмова компонента повинна виявлятися засобами контролю, а відновлення здійснюватися за визначеною процедурою з перевіркою працездатності сервісів.

Локальна відмовостійкість і аварійне відновлення при втраті майданчика повинні бути реалізовані як окремі узгоджені сценарії. Автоматичне переключення допускається за наявності надійного механізму визначення активного вузла та запобігання одночасному запису. Аварійне підвищення ролі репліки бази даних виконується контрольовано після перевірки передумов та ізоляції попереднього активного контуру.

Альтернативна IP-телефонія повинна бути функціонально пов’язана з CRM, обліковими записами операторів і резервним майданчиком. Резервна телефонія не повинна залежати від доступності основної Cisco-платформи, її службових API або міжмайданчикового каналу для приймання нових викликів після активації аварійного режиму.

2.1. Обстеження та проєктування відмовостійкого контуру

Виконавець повинен виконати інвентаризацію вузлів, сервісів, баз даних, файлових ресурсів, мережевих маршрутів, сертифікатів, облікових записів, інтеграцій та зовнішніх залежностей. Для кожного критичного сервісу необхідно встановити власника, джерело даних, залежні компоненти, обсяг, темп приросту та допустимі режими зупинки.

За результатами обстеження повинні бути визначені склад і взаємодія компонентів основного та резервного контурів, необхідні ресурси, порядок резервування й послідовність упровадження. Під час налаштування повинні бути враховані штатне та пікове навантаження, відмова одного вузла, реплікація, резервне копіювання та зберігання записів розмов. Основні параметри налаштованого рішення відображаються у довідці для адміністратора без підготовки окремих схем, матриць і розрахункових документів.

Для CRM, телефонії, автентифікації, VPN, інтеграцій та публічних сервісів повинні бути визначені допустимий час відновлення (RTO), початкова й кінцева події його вимірювання та послідовність відновлення. Числові значення RTO погоджуються із Замовником у робочому порядку до початку впровадження, зазначаються у довідці для адміністратора та перевіряються під час приймання. Окрема матриця відновлення не складається.

Повинно бути забезпечено окреме визначення часу виявлення відмови, виконання процедур переключення та відновлення користувацької функції. Для критичних продуктивних баз даних допустимий період втрати даних (RPO) не повинен перевищувати 15 хвилин. Для допоміжних даних нижчого пріоритету RPO не повинен перевищувати однієї години. Належність даних до відповідного рівня критичності та спосіб перевірки RPO погоджуються із Замовником до початку впровадження; погоджені значення зазначаються у довідці для адміністратора.

2.2. Побудова та налаштування кластера

Повинно бути забезпечено розгортання основних і резервних екземплярів критичних прикладних сервісів та налаштування механізмів їх контрольованого переключення. Для критичного прикладного рівня повинно бути передбачено не менше двох екземплярів на різних вузлах або в незалежних доменах відмови. Розміщення двох віртуальних машин на одному фізичному вузлі без незалежного резервування не вважається достатнім підтвердженням відмовостійкості.

Для кожного рівня повинні бути визначені активні та резервні ролі, спосіб контролю працездатності, умови переключення, механізм запобігання split-brain і порядок відновлення резервування. Засоби керування кластером, балансування та зберігання даних не повинні створювати незахищену єдину точку відмови в межах погодженого сценарію.

Після відмови одного вузла залишкових ресурсів має бути достатньо для погодженого із Замовником обсягу критичних функцій. Для прикладних сервісів налаштовуються перевірки

готовності, контроль запуску та виключення непрацездатного екземпляра з обслуговування. Для компонентів зі станом має застосовуватися сумісний механізм реплікації та керування ролями.
Застосування та оновлення конфігурацій повинно бути повторюваним. Замовнику надаються доступ до налаштувань і створені в межах послуг сценарії, міграції та конфігураційні шаблони у складі налаштованого рішення. Короткі відомості про їх розміщення та використання включаються до довідки для адміністратора. Не допускається залежність від невідтворюваних ручних змін, відомих лише окремому працівнику Виконавця.

2.3. Резервний майданчик та мережева взаємодія

Повинно бути забезпечено налаштування географічно відокремленого резервного контуру у хмарному середовищі Замовника. Резервний контур повинен мати незалежний вихід до Інтернету, локально доступні DNS і засоби автентифікації, а також можливість адміністрування та роботи користувачів без обладнання основного майданчика.
Міжмайданчикова взаємодія повинна здійснюватися захищеним маршрутизованим VPN-каналом. Для наявної Cisco ASA налаштовується сумісне підключення до міжмережевого екрана резервного контуру. Мережі реплікації, керування, прикладних сервісів і публічного доступу повинні бути логічно розмежовані.
Повинні бути налаштовані та погоджені із Замовником IP-адресація, маршрутизація, NAT, firewall, DNS і синхронізація часу. Необхідні для адміністрування адреси та службові імена зазначаються у довідці для адміністратора; окремий IP-план не оформлюється. Фактична пропускна здатність і затримка міжмайданчикового каналу мають бути перевірені для необхідного обсягу реплікації; пропускна здатність доступу до Інтернету перевіряється окремо від VPN.
При втраті міжмайданчикового зв’язку система повинна формувати сповіщення, фіксувати стан реплікації та діяти за визначеною політикою. Сам факт втрати зв’язку не повинен спричиняти неконтрольований запуск другого активного контуру запису.

2.4. Реплікація та відновлення баз даних

Повинно бути забезпечено резервування всіх продуктивних баз даних, необхідних для критичних функцій ПТК НСОЗ. Для кожної БД повинні бути визначені залежні сервіси, версія й редакція СУБД, обсяг, спосіб реплікації, цільові RPO/RTO, ознаки актуальності репліки та порядок переключення. Необхідні для експлуатації відомості зазначаються у довідці для адміністратора без складання окремого реєстру БД. Копіювання віртуальної машини не замінює вимоги до реплікації БД штатними сумісними засобами.
Для Oracle CRM повинна бути налаштована фізична резервна база із передаванням і застосуванням redo/archive засобами Oracle Data Guard або іншою штатною технологією, сумісною з фактичною версією та редакцією. До налаштування перевіряються ліцензійна допустимість, режими журналювання, поточні standby, archive destinations та вплив на продуктивну БД. Використання засобів реплікації та резервування повинно відповідати ліцензійним умовам фактичної редакції Oracle.
Для PostgreSQL повинна бути налаштована фізична потокова реплікація; інший штатний механізм допускається для окремих БД за технічно обґрунтованим і погодженим із Замовником рішенням. Необхідно контролювати receive/replay position, відставання, утримання WAL і стан replication slots, а також перевірити повторний запуск реплікації після перезавантаження.
Для MySQL/MariaDB повинна бути налаштована сумісна реплікація із використанням GTID або file/position залежно від версії. Резервний вузол у штатному режимі має бути захищений від прикладного запису. Під час переключення перевіряються отримані журнали, стан потоків реплікації та актуальність даних.
Для всіх СУБД повинні бути передбачені контроль розриву реплікації, обробка накопичених журналів, контроль дискового простору, підвищення ролі резервної БД та повернення реплікації після аварії. Фактичний RPO визначається за точкою відновлених даних; у разі недоступності каналу або перевищення встановленого відставання повинні забезпечуватися фіксація події, сповіщення відповідальних осіб і контрольоване відновлення реплікації.

2.5. Відмовостійкість CRM та інтеграцій

Повинно бути забезпечено налаштування резервних компонентів CRM API, middleware, reverse proxy та інтеграційного модуля, необхідних для входу користувачів, пошуку, перегляду,

створення й оновлення звернень. Параметри підключення повинні використовувати сервісні імена або погоджені логічні endpoint, що змінюються без перекомпіляції застосунків.
Порядок запуску має враховувати залежності між БД, чергами повідомлень, кешами, пошуком, API та зовнішніми споживачами. Перехід до наступного етапу запуску повинен виконуватися після перевірки готовності необхідних залежностей. Формальна доступність TCP-порту не повинна бути єдиним критерієм працездатності CRM.
Для RabbitMQ повинні бути визначені механізми збереження критичних повідомлень і підтверджень обробки, відновлення споживачів та повторної доставки. Для Redis необхідно розмежувати кеш і дані, втрата яких впливає на бізнес-операції; для останніх налаштовується збереження або відновлення стану. Для Elasticsearch налаштовуються реплікація або snapshot/restore та перевіряється працездатність пошуку після відновлення.
Переключення повинно запобігати одночасному виконанню однакових фонових завдань у двох контурах і запису в неактивні продуктивні endpoint. Потрібно забезпечити виявлення дублів і незавершених інтеграційних операцій, їх журналювання та контрольоване повторне виконання. Для перевірки застосовується наскрізна контрольна операція із відстеженням її результату в усіх задіяних компонентах.
2.6. Сервісні адреси та балансування
Для CRM, API, інтеграцій, БД і публічних сервісів повинні бути налаштовані стабільні сервісні DNS-імена та/або VIP. Переключення не повинно вимагати масового ручного редагування адрес у конфігураціях користувацьких робочих місць і залежних серверів.
Механізм балансування має використовувати перевірки прикладної готовності та виключати несправні вузли. Якщо хмарна мережа не підтримує VRRP/GARP, застосовується підтримуваний механізм балансувальника, NAT або DNS. Для DNS-переключення враховуються TTL, кешування та фактичний час оновлення адрес у споживачів.
Endpoint БД переводиться на резервний контур лише після перевірки активної ролі та виконання fencing. Втрата доступності основної БД сама по собі не є дозволом автоматично спрямовувати запис у standby. Короткий порядок переведення endpoint та повернення до попереднього стану зазначається у довідці для адміністратора.
2.7. Впровадження альтернативної IP-телефонії
Повинно бути забезпечено впровадження та налаштування альтернативної системи IP-телефонії на базі Asterisk або функціонально еквівалентного рішення. Система має підтримувати SIP-підключення до операторів зв’язку, реєстрацію робочих місць, IVR, черги, ACD, вхідні та вихідні виклики, запис розмов і CDR. В аварійному режимі ці функції повинні виконуватися без основної Cisco-інфраструктури.
Повинна бути забезпечена підтримка не менше 150 одночасно авторизованих операторських сесій та не менше 100 одночасних голосових сесій у погодженому режимі обслуговування. До приймального профілю включаються одночасний запис, робота IVR і черг та операторський інтерфейс. Облік зовнішніх викликів і внутрішніх медіаканалів, зокрема консультацій та конференцій, визначається окремо, щоб не підмінювати цільову кількість викликів кількістю технічних з’єднань.
Для оператора повинні бути налаштовані єдина автентифікація, індикація реєстрації телефонії, стани Ready, Not Ready, On Call, Wrap-up та Offline, приймання і завершення виклику, утримання, DTMF, сліпе й консультаційне переведення, а також фіксація результату обслуговування. Вихід із системи повинен унеможливлювати направлення нових викликів на неактивну сесію.
Робоче місце повинно забезпечувати голос через браузер із WebRTC та/або сумісний SIP-клієнт у складі рішення. Для браузерного режиму налаштовуються HTTPS/WSS, ICE, DTLS-SRTP, STUN/TURN і перевіряється двосторонній звук за NAT/VPN. Не допускається конфліктна одночасна реєстрація одного робочого місця в кількох голосових режимах.
Повинні бути налаштовані черги, групи операторів, skills, пріоритети, правила розподілу, максимальний час очікування, overflow, робочі години, свята та сценарії неробочого часу. IVR має підтримувати привітання, меню, введення цифр, направлення до черг або зовнішніх номерів та завершення виклику. Налаштування DID, транків, маршрутів і сценаріїв повинно виконуватися керовано, із перевіркою параметрів, журналюванням і можливістю відновлення попередньої конфігурації.

Повинні бути забезпечені автоматичний запис відповідно до політики Замовника, каталог записів, пошук за часом, оператором, чергою та ідентифікатором виклику, прослуховування за правами та аудит доступу. Кожний запис має бути пов'язаний із CDR. Для конфіденційних фрагментів повинна бути доступна керована пауза або вимкнення запису із фіксацією дії.
Для супервізора повинні бути налаштовані перегляд станів операторів і черг, показники очікування й обслуговування, доступ до CDR та записів, а також службові режими прослуховування, підказки оператору та підключення до розмови за наданими правами. Звіти мають містити вхідні, прийняті, пропущені й вихідні виклики, тривалість розмов, очікування та стани операторів із погодженими правилами обчислення й експортом даних.
Резервування телефонної платформи, конфігурації, її БД і записів повинно бути включено до загальної архітектури кластера. Для відмови телефонного вузла та втрати майданчика окремо визначаються відновлення приймання нових викликів, повторна реєстрація операторів і доля активних розмов. Фактична поведінка активних розмов під час відмови повинна бути перевірена в присутності представника Замовника. Можливі переривання та особливості відновлення зазначаються у довідці для адміністратора.
2.8. Відновлення залежних сервісів і віддалений доступ
У резервному контурі повинні бути забезпечені незалежний VPN-доступ, локальні DNS і синхронізація часу. За використання Active Directory налаштовується резервний контролер домену з необхідними службами та перевіркою автентифікації користувачів за недоступності основних контролерів. Для критичних адміністративних дій передбачаються контрольовані аварійні облікові записи та захищений порядок доступу до них.
Для публічних сервісів, пов'язаних із ПТК НСОЗ, налаштовується резервний ланцюжок reverse proxy, portal/cabinet/API та залежних БД зі збереженням користувацьких URL і TLS. За наявності Cloudflare готується контрольована процедура зміни origin, перевірка доступності з Інтернету та повернення на основний контур.
Для СЕД повинні бути визначені й відновлені компоненти, необхідні для погоджених операцій обміну з ПТК НСОЗ: БД, файлові ресурси, автентифікація, сертифікати та інтеграції. Приймальна перевірка включає вхід і контрольну операцію з документом у резервному контурі.
Повинна бути налаштована незалежна аварійна електронна пошта для погодженого переліку службових користувачів. До активації визначаються домен або піддомен, доставка, DNS/MX, SPF/DKIM/DMARC та порядок повернення. Повинні бути визначені порядок збереження та перенесення листів, отриманих в аварійному контурі, після повернення до штатної схеми. Обсяг відновлення поштових даних і перелік аварійних скриньок погоджуються із Замовником до налаштування.
2.9. Інтеграція телефонії з Cisco та CRM
Повинна бути забезпечена можливість паралельної експлуатації чинної Cisco-телефонії та альтернативного контуру з поетапним перенесенням груп операторів і ліній. Для кожного етапу визначаються маршрути між платформами, правила нумерації, Caller ID, transfer, запобігання петлям і повернення перенесених маршрутів у попередній стан.
Повинна бути налаштована синхронізація користувачів, пристроїв, номерів і їх зв'язків із Cisco CUCM через офіційні програмні інтерфейси. AXL використовується для конфігураційних об'єктів, RisPort/Serviceability — для станів реєстрації; сумісність підтверджується для фактичної версії CUCM. Прямий несанкціонований доступ до БД Cisco не допускається.
Інтервали оновлення повинні бути конфігурованими; базово передбачаються оновлення користувачів, пристроїв і ліній кожні 15 хвилин, реєстраційних станів кожні 5 хвилин та повна звірка щодоби. Перед масовим застосуванням має бути доступний попередній перегляд. Імпорт секретів SIP або паролів CUCM не виконується.
Пріоритети атрибутів між CUCM, AD та локальною системою повинні бути погоджені із Замовником і зазначені у довідці для адміністратора. Ролі, команди та skills не повинні безумовно перезаписуватися даними зовнішнього каталогу. Дублі та суперечливі асоціації повинні потрапляти на розгляд адміністратора; видалення в джерелі не повинно призводити до негайного фізичного видалення історії оператора.
Для CRM повинні бути налаштовані відкриття картки або пошуку за номером абонента, передавання ідентифікатора виклику та подій початку, відповіді й завершення виклику, а також зв'язок із записом розмови. Механізм може використовувати URL, iframe, REST API та підписані

webhooks за сумісністю CRM. Повторна доставка події не повинна неконтрольовано дублювати результат у CRM.
Для кожного SIP-провайдера повинні бути визначені порядок переключення DID/маршрутів, необхідні дії сторін, контрольні номери й спосіб перевірки завершення переключення. Короткі відомості, необхідні адміністратору для виконання цих дій, включаються до довідки для адміністратора. Недоступність Cisco Sync не повинна блокувати роботу вже налаштованих операторів в аварійному контурі.
2.10. Резервне копіювання та контрольне відновлення
Повинні бути налаштовані окремі резервні копії баз даних, конфігурацій, IVR prompts, необхідних файлових ресурсів, метаданих і файлів записів відповідно до погодженої політики. Резервне копіювання повинно виконуватися незалежно від реплікації та забезпечувати відновлення даних у разі їх пошкодження або помилкового видалення в основному й реплікованому середовищах.
Періодичність копіювання, строки зберігання, місце розміщення копій, шифрування, повноваження на видалення та порядок доступу до ключів повинні бути погоджені із Замовником, реалізовані у налаштуваннях і стисло зазначені у довідці для адміністратора. Копії повинні бути захищені від одночасної втрати з основним і резервним контурами; для критичних даних застосовується ізольоване або незмінюване зберігання, сумісне з інфраструктурою Замовника.
Для СУБД повинна бути перевірена можливість відновлення на визначену точку часу в межах підтримуваного механізму та політики зберігання журналів. До приймання Виконавець виконує контрольне відновлення з окремої копії та демонструє Замовнику прикладну доступність відновлених даних. Короткий підсумок перевірки, відновлена точка даних і фактична тривалість відновлення зазначаються у довідці для адміністратора.
2.11. Автоматизація аварійного переключення та повернення
Повинні бути налаштовані та перевірені аварійне переключення (failover) і повернення до штатного режиму (failback). Короткий порядок дій адміністратора зазначається у довідці для адміністратора. Він повинен охоплювати перевірку ізоляції основного контуру, стану реплік і фактичного RPO, підвищення ролі БД, активацію endpoint, запуск залежних сервісів, переключення телефонії та перевірку працездатності. Окремі інструкції failover і failback не оформлюються.
Повторювані перевірки та операції повинні бути автоматизовані сценаріями або playbook. Сценарії повинні мати конфігураційні параметри, журналювання, зрозумілі коди завершення, захист від повторного паралельного запуску та режим попередньої перевірки для небезпечних дій. Підвищення ролі БД повинно вимагати явного дозволу адміністратора і завершуватися без змін при невиконанні обов’язкових передумов.
Failback виконується після підтвердження готовності основного майданчика, зворотної синхронізації актуальних даних, перевірки цілісності та погодження фінального переключення. Автоматичне повернення запису на основний контур лише за фактом його появи в мережі не допускається. Після повернення відновлюється штатна реплікація та повторно перевіряються CRM, інтеграції, публічні сервіси й телефонія.
2.12. Моніторинг та журналювання
Повинен бути забезпечений централізований контроль стану вузлів, прикладних сервісів, БД, реплікації, VPN, DNS, SIP-транків, реєстрації операторів, сховища записів і резервного копіювання з інтеграцією із системою моніторингу Замовника. Для кожної критичної події встановлюються поріг, одержувач сповіщення та порядок реагування.
Контролю підлягають ролі БД, transport/apply lag, стан журналів і реплікаційних потоків, накопичення повідомлень, помилки споживачів, місце на дисках, CPU/RAM, строк дії сертифікатів і результати контрольних перевірок. Засоби сповіщення про втрату основного майданчика повинні залишатися доступними поза ним.
Журнали повинні фіксувати час, суб’єкта дії, об’єкт, операцію, результат і помилку. Для інтеграцій та викликів застосовуються ідентифікатори кореляції. Доступ до записів розмов, зміни ролей, конфігурацій, маршрутів, реплікації та ручні переключення повинні аудитуватися. Паролі, токени, приватні ключі та повні чутливі дані не повинні потрапляти у звичайні журнали.
2.13. Випробування та підтвердження результату

До введення в експлуатацію повинні бути проведені функціональні, навантажувальні та аварійні перевірки за сценаріями, погодженими із Замовником у робочому порядку. Працездатність повинна бути продемонстрована представнику Замовника, з вимірюванням фактичних RTO та RPO критичних сервісів. Короткі підсумки перевірок зазначаються у довідці для адміністратора. Обов'язково перевіряються відмова одного прикладного вузла, відмова активного вузла БД, втрата міжмайданчикового каналу, логічна повна недоступність основного майданчика, контрольоване повернення та відновлення з backup. Перевірка лише ping, запуску віртуальних машин або наявності реплік не є достатньою.

У резервному контурі повинні бути підтверджені VPN-доступ з Інтернету, незалежна автентифікація і DNS, вхід у CRM, пошук, відкриття, створення та оновлення тестового звернення, наскрізна інтеграційна операція, погоджена операція СЕД, доступ до публічних URL і тестова доставка аварійної пошти. Повторні операції не повинні спричиняти неконтрольованих дублів або запису в ізольований контур.

Для телефонії перевіряється повний цикл: вхідний DID → IVR → черга → оператор → двостороння розмова → transfer за сценарієм → завершення → CDR → відтворення запису → відображення події у CRM. Окремо перевіряються вихідний дзвінок, робочий час, права доступу, робота за NAT/VPN та переключення SIP/DID без участі основної Cisco-платформи.

Навантажувальна перевірка повинна підтвердити 150 операторських сесій та не менше 100 голосових сесій із записом. Тривалість, інтенсивність надходження викликів, середня тривалість, частка transfer, допустимі затримки й помилки погоджуються із Замовником у робочому порядку до початку перевірки. Критичні функції додатково перевіряються після відмови одного вузла в межах погодженого профілю. Працездатність у штатному й аварійному режимах демонструється Замовнику без складання окремих звітів.

Випробування повинні проводитися без неконтрольованого впливу на продуктивні звернення та номери. До завершення надання послуг повинні бути усунені дефекти, що порушують обов'язкові функції, цілісність даних або досягнення погоджених показників. Результат перевіряється Замовником під час демонстрації роботи налаштованого рішення.

2.14. Довідка для адміністратора та практичний інструктаж

Виконавець повинен надати Замовнику одну коротку довідку для адміністратора в електронній формі. Довідка повинна містити основні відомості про налаштовані компоненти й адреси доступу, розміщення конфігурацій та засобів автоматизації, контроль працездатності й реплікації, порядок резервного копіювання та відновлення, аварійного переключення й повернення, особливості телефонної маршрутизації, погоджені RTO/RPO та короткі підсумки перевірок. Інформація викладається стисло, в обсязі, необхідному для повсякденного адміністрування та виконання аварійних дій.

Усі технічні відомості, передбачені цими вимогами для передачі Замовнику, включаються до зазначеної довідки адміністратора. Налаштування, конфігурації, створені сценарії та програмні доопрацювання передаються у складі налаштованого рішення без підготовки окремих описових документів. Облікові дані й секрети надаються окремим захищеним способом. Документи приймання послуг оформлюються відповідно до договору.

Повинен бути проведений практичний інструктаж адміністраторів із керування кластером, реплікацією, резервним копіюванням, відновленням і телефонією, а також ознайомлення операторів і супервізорів із роботою альтернативного контуру.

3. ЗАГАЛЬНІ ВИМОГИ

3.1. Сумісність і збереження працездатності

Усі налаштування повинні виконуватися з урахуванням чинної архітектури ПТК НСОЗ, структури даних, інтеграцій та обмежень продуктивних систем. Повинні бути збережені необхідні зв'язки між зверненнями, документами, подіями та записами розмов. Масові зміни допускаються після перевірки, створення потрібних резервних копій і визначення порядку відкату.

Упровадження повинно здійснюватися поетапно з пілотною перевіркою та погодженими вікнами змін. Планові перерви, їх тривалість і дії користувачів погоджуються заздалегідь. Тестування повинно проводитися у виділеному контурі або в погоджені вікна із забезпеченням можливості повернення діючої Cisco-телефонії та CRM до попереднього працездатного стану.

3.2. Захист інформації та розмежування доступу
Повинні бути налаштовані рольовий доступ, мінімально необхідні права службових облікових записів, захищені канали передавання, обмеження адміністративних інтерфейсів і журналювання змін. Адміністративний доступ через відкритий Інтернет без захищеного механізму не допускається; для привілейованого віддаленого доступу повинна бути застосована багатофакторна автентифікація.
Публічні вебінтерфейси повинні використовувати TLS; службові API, СУБД і керування телефонією розміщуються у внутрішніх або керуючих сегментах. Доступ SIP/RTP обмежується необхідними напрямками й діапазонами. Для інтеграцій передбачаються перевірка автентичності запитів, керування секретами та контроль повторного виконання.
Секрети не повинні міститися у відкритому вигляді в репозиторіях, сценаріях, звичайних журналах або документації. Повинні бути визначені їх захищене зберігання, резервування, ротація та доступ у разі втрати основного майданчика. Доступ до продуктивних даних під час робіт здійснюється лише в межах повноважень, наданих Замовником.
3.3. Надійність та керованість
Відновлення повинно бути відтворюваним підготовленим персоналом Замовника з використанням переданих налаштувань, засобів автоматизації та короткого порядку дій у довідці для адміністратора. Ручні операції повинні мати зрозумілі передумови й ознаки успішного виконання. Некритична несправність моніторингу або синхронізації не повинна неконтрольовано зупиняти вже працездатне обслуговування звернень.
Після відмови або оновлення повинен відновлюватися не лише прикладний сервіс, а й стан резервування та контроль його актуальності. Зміни конфігурації, розкладів і маршрутів повинні бути простежуваними; операції синхронізації та регламентні завдання повинні мати історію виконання й захист від дубльованого запуску.
3.4. Ліцензії та передача результатів
Відомості про використані програмні компоненти, їх версії, ліцензії, необхідні підписки й обмеження, включно з можливими витратами після завершення договору, зазначаються у довідці для адміністратора без складання окремого переліку. Права використання повинні забезпечувати експлуатацію погодженого складу основного та резервного контурів.
Замовнику передаються всі створені в межах послуг сценарії, шаблони, інтеграційні модулі та вихідний код розроблених доопрацювань у складі налаштованого рішення. Необхідні команди або порядок їх запуску й розгортання зазначаються у довідці для адміністратора. Для стороннього ПЗ передаються передбачені ліцензією права та засоби адміністрування. Експлуатація не повинна залежати від особистих облікових записів працівників Виконавця або непереданих ключів доступу.

4. ВИМОГИ ДО ЯКОСТІ ПОСЛУГ ТА ГАРАНТІЙНІ ЗОБОВ’ЯЗАННЯ

4.1. Послуги повинні бути надані в повному обсязі, у строки, визначені договором, із дотриманням цих технічних вимог та погоджених із Замовником умов упровадження.
4.2. Належна якість послуг підтверджується працездатністю кластера, резервного контуру й альтернативної телефонії, виконанням погоджених показників та успішною демонстрацією функціональних сценаріїв у штатному й аварійному режимах. Замовнику повинні бути передані довідка для адміністратора, налаштування та засоби адміністрування.
4.3. Гарантійний строк на результати наданих послуг становить не менше 6 місяців із дати підписання документа про приймання. Гарантія поширюється на дефекти виконаних налаштувань, інтеграцій, автоматизації та розроблених доопрацювань.
4.4. У разі виявлення протягом гарантійного строку недоліків Виконавець повинен усунути їх без додаткової оплати протягом 5 календарних днів із дня повідомлення Замовником. Для інцидентів, що зупиняють критичні функції, порядок оперативного реагування та тимчасового відновлення встановлюється договором окремо; строк гарантійного виправлення не замінює погодженого RTO.
4.5. Виправлення повинно супроводжуватися перевіркою відновленої функції та, за потреби, актуалізацією налаштувань і довідки для адміністратора. Відповідальність за неналежне виконання гарантійних зобов’язань визначається договором.

5. ОРГАНІЗАЦІЙНІ ПОЛОЖЕННЯ

5.1. Послуги надаються поетапно: обстеження та підготовка; налаштування ресурсів і мережі; побудова кластера та реплікації; налаштування прикладних сервісів; упровадження й інтеграція альтернативної телефонії; перевірка працездатності; дослідна експлуатація; передача результатів. Строки, місце надання та тривалість дослідної експлуатації визначаються договором. Послідовність дій і вікна змін погоджуються із Замовником у робочому порядку без окремих календарних планів та звітів за етапами.

5.2. Параметри налаштування, порядок переключення й відновлення та сценарії перевірок погоджуються із Замовником у робочому порядку до виконання відповідних змін. Окреме документальне оформлення результатів кожного етапу не вимагається. Основні відомості про остаточно налаштоване рішення включаються до довідки для адміністратора. Погодження технічних деталей не повинно зменшувати обсяг обов'язкових функцій і результатів, установлених цими вимогами.

5.3. Замовник забезпечує погоджені доступи та участь відповідальних працівників. Необхідні доступи, ресурси й дії третіх сторін узгоджуються в робочому порядку. Роботи, що можуть вплинути на продуктивні сервіси, виконуються лише в погоджені вікна зі збереженням можливості повернення до попереднього працездатного стану.

5.4. Довідка для адміністратора надається українською мовою одним електронним документом. Назви технологій, параметри конфігурацій, програмні ідентифікатори та документація виробників можуть зберігатися мовою оригіналу.

5.5. Завершення послуг підтверджується перевіреною Замовником працездатністю налаштованого рішення, досягненням погоджених показників, передачею довідки для адміністратора, налаштувань і доступів та підписанням документа про приймання послуг, передбаченого договором. Відомі обмеження й особливості експлуатації зазначаються в довідці для адміністратора; вони не можуть підмінювати виконання обов'язкових вимог.

Учасник підтверджує відповідність запропонованих послуг з побудови та налаштування відмовостійкого кластера ПТК НСОЗ із впровадженням альтернативної системи IP-телефонії технічним вимогам Замовника:

Обґрунтування очікуваної вартості предмета закупівлі, розміру бюджетного призначення:
Очікувана вартість закупівлі формувалась із середніх цін комерційних пропозицій, наданих суб'єктами господарювання.

Очікувана вартість

Комерційні пропозиції учасників надані з урахуванням податку на додану вартість (ПДВ). Середнє арифметичне значення отриманих цінових пропозицій становить **2 500 000,00 грн**.

Відповідно до пункту 14 Особливостей, очікувана вартість предмета закупівлі, що зазначається в річному плані закупівель, визначена в межах граничного ліміту кошторисних призначень Замовника і становить: **2 500 000,00 грн (два мільйони п'ятсот тисяч гривень 00 копійок) з ПДВ.**

Відповідно до пункту 26 Особливостей, очікувана вартість предмета закупівлі в оголошенні про проведення відкритих торгів зазначається без урахування податку на додану вартість (ПДВ є нарахуванням на чисту вартість пропозиції переможця-платника при укладанні договору) і становить: **2 083 333,33 грн (два мільйони вісімдесят три тисячі триста тридцять три гривні 33 копійки) без ПДВ**.