ЗАТВЕРЖДЕНО
Директор ОП УМІЦ
Адміністратор домену .УКР

_____ Ю. Гончарук
«13» вересня 2013 року

Вимоги до Оператора реєстру домену .УКР

м. Київ
2013 рік

Зміст

1. Загальні положення.

1.1. Мета цього документу – визначити організаційні, технічні (технологічні), та кваліфікаційні вимоги до організації-претендента, що бажає стати Оператором реєстру домену .УКР (далі – Претендента), який буде зобов'язаний забезпечити розробку, впровадження та стале і безперебійне обслуговування системи реєстрацій доменних імен в домені .УКР, функціонування системи доменних імен, інших обов'язкових підсистем (далі разом – Система), включаючи:

1) усі публічно доступні служби, що пов'язані з процесами обслуговування реєстру домену .УКР;
2) підсистеми, що відповідає за документарний та електронний супровід транзакцій, що здійснюються на усіх етапах життєвого циклу доменних імен, а також внутрішніх транзакцій під час супроводу реєстру домену .УКР.

1.2. В цьому документі визначатимуться мінімальні параметри архітектури технічної бази Оператора реєстру та базові організаційні процедури, які Оператор реєстру зобов'язаний буде виконувати під час взаємодії з Адміністратором домену .УКР (далі – Адміністратором), Реєстраторами, Комісією з досудового розв'язання доменних спорів (далі – Комісією зі спорів) у відповідності до Правил реєстрацій і користування доменними іменами в домені .УКР (далі – Правил), що схвалюються Координаційною радою. Оператор реєстру також буде зобов'язаний розробити і дотримуватись вимог, що визначатимуться в Технічному регламенті, який затверджуватиметься Адміністратором.

1.3. Пропозиції щодо посилення значень технічних та інших параметрів Системи, що можуть покращити її властивості та можливості обслуговування реєстру домену .УКР, а також пропозиції з вдосконалення організаційних процедур щодо взаємодії та партнерства з Адміністратором, Реєстраторами, Комісією зі спорів тощо будуть вважатись додатковими перевагами для Претендента.

1.4. Претендент подає до Адміністратора заяву про свій намір стати Оператором реєстру домену .УКР впродовж 30 днів з дня розміщення на сайті Адміністратора оголошення про прийом відповідних пропозицій щодо здійснення функцій Оператора реєстру домену .УКР.

Заява Претендента та додатки до неї повинні містити:

1) засвідчені належним чином копії установчих документів та відповідного рішення засновників/учасників про намір здійснювати на виключній основі діяльність як Оператора реєстру домену .УКР;
2) відомості про відповідність Претендента встановленим вимогам, що визначаються у цьому документі (Вимогах до оператора реєстру домену .УКР) та у документах, дотримання яких є обов'язковим для виконання обов'язків Оператора реєстру домену .УКР;

3) відомості про існуючий досвід Претендента та його можливості, включаючи загальний опис технічних систем, власником яких є Претендент, організаційних можливостей та кваліфікації персоналу щодо виконання зобов'язань Оператора реєстру домену .УКР;
4) ескізний проект Системи з описом та архітектурою кожної з підсистем, щодо яких встановлюються вимоги у цьому документі, документах ICANN та у відповідних стандартах Інтернет;
5) відповідне ескізному проекту технічне завдання на розробку та впровадження Системи;
6) технічне завдання на розробку і впровадження комплексної системи захисту інформації у реєстрі домену .УКР та відповідні посадові інструкції;
7) документ «Опис API EPP»;
8) план по відновленню працездатності Системи та/або підсистем у разі виникнення позаштатних ситуацій (катастроф, аварій тощо) та відповідні посадові інструкції;
9) план-графік дій, що передбачені підпунктами 6) та 7) пункту 1.5 цього документу, у разі, якщо такі дії є необхідними.

1.5. Претендент, на момент подачі заяви про своє бажання стати Оператором реєстру, повинен відповідати таким наступним вимогам:

1) бути юридичною особою, що створена і зареєстрована згідно законодавства України не менше ніж за 2 роки до подачі заяви відповідно з пунктом 1.4;
2) не мати у своєму статутному капіталі частки або голосів для управління, що належить іноземній компанії або особі, що діє в інтересах іноземної особи, у розмірі більше ніж 10%;
3) не бути державним або комунальним підприємством або таким, у статутному капіталі якого частка, що належить державі, перевищує 50%;
4) мати розгорнутий та працюючий програмно-апаратний комплекс із встановленим програмним забезпеченням для обслуговування реєстру домену .УКР, у тому числі підтримки серверів доменних імен (DNS) із промисловим способом дистрибуції файлу зони, службу WHOIS із стандартним та веб-інтерфейсом, підтримку протоколу EPP (Extensible Provisioning Protocol), що призначений для управління реєстраційною інформацією, мати вбудований програмний інтерфейс та мати веб-інтерфейс для Реєстраторів;
5) відповідати вимогам ICANN, які пред'являються до операторів реєстрів доменів верхнього рівня , типу ccTLD/gTLD , що може бути підтверджено інформацією від ICANN,
6) або бути ICANN-акредитованим реєстратором у gTLD, виробничий комплекс якого може бути організаційно, технічно і кваліфікаційно відділений від діяльності з реєстрації доменних імен у gTLD і приведений у відповідність з вимогами до оператора реєстру ccTLD,

а також з вимогами до Оператора реєстру домену . УКР, що викладені в цьому документі, в строк не більше 2 -х місяців,

7) або бути фактично діючим оператором реєстру іншого домену верхнього рівня ccTLD, виробничий комплекс якого може бути технічно і кваліфікаційно відділений від діяльності з реєстрації доменних імен в іншому ccTLD і приведений у відповідність з вимогами до Оператора реєстру домену . УКР, що викладені в цьому документі, в строк не більше 2 -х місяців;
8) мати не менше ніж 5 (п’ять) технологічних майданчиків (груп логічно пов’язаних серверів і мережевого обладнання, які підключені кількома каналами до Інтернет і забезпечені безперебійним електроживленням) і які вже функціонують у робочому режимі, з яких не менш ніж один повинен знаходитись поза межами України і не менш ніж два повинні знаходитись в Україні. Усі технологічні майданчики (комплекси) повинні базуватись на власних апаратних ресурсах Претендента;
9) мати щонайменше 3 (три) блоки IPv4-адресов мінімально /24 у різних мережах класу С;
10) щонайменше 1 (один) з блоків IP-адрес, що вказані в підпункті 9) повинен також мати підтримку (адресацію) IPv6.

1.6. Для перевірки відповідності визначеним вимогам Претендент разом із заявою та додатками до неї передає Адміністраторові коди доступу до кожного з серверів та іншого обладнання, що мають бути задіяні у обслуговуванні реєстру домену .УКР та усіх його підсистем, на паперовому та електронному носії.

1.7. На момент подання заяви Претендент повинен мати розроблені і задокументовані процедури, у відповідності з якими він, як можливий Оператор реєстру, буде зобов’язаний із дотриманням вимог законодавства України здійснювати наступне:

1) **дотримуватись відповідних застосовних стандартів, рекомендацій та положень документів ICANN з імплементації IDN ccTLD**, Правил реєстрації та використання доменних імен в домені. УКР, Технічного регламенту, Положення (порядку) розв’язання доменних спорів, а також умов договорів з Адміністратором, Реєстраторами, Комісією з досудового вирішення спорів.
   Під відповідними застосовними стандартами розуміються стандарти RFC «standards - track» або «best current practice», впроваджені Групою інженерних проблем Інтернету (IETF) ;
2) **підтримувати файл зони домену .УКР/.xn--j1amh в актуальному стані** – створення регулярних поновлень даних у файлі зони повинно здійснюватися згідно відповідних стандартів, як визначено підпунктом 1);

3) **забезпечувати роботу служби доменних імен домену .УКР/.xn--j1amh –** забезпечення стабільної роботи усіх авторитативних серверів доменних імен домену .УКР, забезпечення можливості отримання адресації в домені .УКР усіма користувачами Інтернет згідно діючих стандартів;
4) **підтримувати точність, актуальність і повноту інформації**, що відноситься до будь-яких змін реєстраційних та/або службових даних щодо призначених адміністративних, технічних, фінансових контактах Оператора реєстру і Реєстраторів. Зміни будь-яких контактних і комунікативних даних Оператора реєстру повинні доводитись до Адміністратора впродовж 1 години з моменту зміни таких даних;

2. Технічні вимоги.

Претендент повинен представити рішення, які забезпечують безвідмовну та безперервну роботу усіх підсистем та елементів реєстру домену .УКР та Системи в цілому.

З метою забезпечення безвідмовності роботи Системи у випадках збоїв в роботі основних серверів та іншого обладнання, що задіяні у постійному режимі роботи підсистем DNS та/або WHOIS, баз даних, усі сервери та інше обладнання зобов'язані синхронізуватись в реальному часі з серверами та іншим обладнанням, що працюють в режимі «гарячого» резерву.

Виникнення позаштатної ситуації в ході роботи будь-якої підсистеми не повинне зупиняти роботу інших підсистем. Подовження роботи підсистем повинне відбуватись з набором даних, який був актуальний перед збоєм. Після відновлення працездатності підсистеми, що виходила зі строю, та її з'єднання з іншими підсистемами, дані, що задіяні з резерву для відновлення роботи підсистеми, актуалізуються для усіх підсистем.

Відновлення працездатності будь-якої підсистеми після виникнення позаштатної ситуації повинне відбуватись не більше, ніж за 24 години.

Претендент повинен представити рішення щодо забезпечення вимог до безпеки та сталої працездатності наступних елементів Системи:

1) вузлів мережі (серверів, робочих станцій на базі ПК, ноутбуків, планшетів, смартфонів (софтфонів) і т.і.), операційних систем і додатків, сховищ баз даних;
2) мережевих пристроїв і обладнання (маршрутизаторів, комутаторів, міжмережевих екранів, канального обладнання і т.і.);

передачі даних між підсистемами реєстру та/або з зовнішньої мережі.

Рішення з безпеки доступу до підсистем реєстру повинні бути побудовані на основі PKI (Public Key Infrastructure).

Адміністратор здійснюватиме автоматизовану перевірку параметрів та елементів Системи та залишає за собою право не розголошувати кількість та місця розташування спеціальних моніторингових програм (моніторів), які на основі визначених алгоритмів здійснюватимуть перевірку доступності, працездатності мережевих сервісів та служб. Претендент і надалі Оператор

реєстру зобов’язані інсталювати і встановлювати такі монітори, їх параметри і налаштування на вимогу Адміністратора у тих елементах підсистем, обладнанні, ОС які будуть визначені Адміністратором на основі даних, що подаватимуться у заяві.

2.1. Вимоги до параметрів Системи і до телекомунікаційної мережі.

Претендент повинен представити:

1) схему реалізації Системи з вказуванням технічних параметрів серверів, їх статусу і функціональних завдань, місць розташування;
2) схему роботи Системи у випадках позаштатних ситуацій з вказуванням технічних параметрів серверів, їх статусу і функціональних завдань, місць розташування, що є іншими;
3) схему реалізації телекомунікаційної мережі з вказуванням функціональних та технічних параметрів вузлів мережі, їх статусу і місць розташування.

Доступ до кожного мережевого вузлу повинен забезпечуватись через щонайменше через двох операторів/провайдерів телекомунікацій (Інтернет) за умови відсутності попереднього фільтрування мережевих пакетів і сервісів.

Претендент повинен представити своє рішення і проектні параметри зокрема для наступних характеристик Системи:

1) **транзакційність** – забезпечення цілісності даних та запобігання конфліктам невідповідності під час роботи кількох користувачів через програмні додатки з одним й тим самим набором (масивом) даних та одночасної обробки цих даних усередині системи;
2) **маштабованість** – можливість збільшити продуктивність системи за рахунок збільшення кількості серверних компонент або збільшення обчислювальної потужності окремих компонент. Процес такого збільшення продуктивності не повинен призводити до зростання простою системи для її вдосконалення;
3) **багатократне резервування вузлів і компонентів системи** – виключення можливості втрати або спотворення даних та мінімізація часу на відновлення повної працездатності підсистем у випадках виходу зі строю обладнання та виникнення інших непередбачуваних обставин;
4) **наявність інструментів самодіагностики і зовнішньої діагностики ключових компонентів системи** – придатність системи самостійно визначати проблеми з яким-небудь компонентом шляхом виклику та обробки спеціального набору тестових завдань, що виконуються щодо кожної з підсистем;
5) **відповідність протоколів і схем взаємодії міжнародним стандартам та стандартам Інтернет**;
6) **захищеність від зовнішніх несанкціонованих утручань** – реалізація системою політик безпеки, що надають максимальний захист від атак, утручань, несанкціонованого доступу до даних тощо.

Безпека обладнання, що використовуватиметься Претендентом в системі і телекомунікаційній мережі повинна бути підтверджена належними сертифікатами відповідності.

2.2. Підсистема реєстрацій.

2.2.1. Принципи роботи підсистеми реєстрацій та її доступність.

Підсистема реєстрацій доменних імен та здійснення належних операцій з доменними іменами повинна забезпечувати взаємодію з технологічними автоматизованими комплексами Реєстраторів за протоколом EPP (Extensible Provisioning Protocol).

Кількість Front-end серверів підсистеми реєстрацій повинне бути не менше 3 (трьох). Ці сервери повинні бути розташовані щонайменше у 2 (двох) незалежних датацентрах. Мінімум 2 (два) сервери повинні знаходитись в режимі Stand-by.

Претендент повинен запропонувати та обґрунтувати оптимальний на його думку методо, що використовуватиметься до передачі даних і транспортний мережевий протокол.

Підсистема реєстрацій повинна:

1) ґрунтуватися на вже перевірених на практиці Претендентом процесах управління реєстраціями (транзакціями);
2) забезпечувати автоматичну обробку усіх транзакцій;
3) забезпечувати авторизацію Реєстраторів та автентифікацію операцій, що здійснюються в системі.

Претендент повинен представити рішення відносно автоматичної обробки усіх транзакцій.

Підсистема реєстрацій повинна забезпечувати і підтримувати увесь життєвий цикл доменного імені (домену), що визначатимуться в (проекті) Правилах реєстрацій і користування доменними іменами в домені .УКР та відповідному Технічному регламенті.

Доступність служби EPP – здатність сукупності EPP-серверів домену .УКР виконувати вдалу обробку запитів через коректні EPP-команди від акредитованих Реєстраторів, які мають належні облікові записи для доступу до EPP-серверів реєстру. Відповідь повинна включати належні відомості з Системи у відповідності до опису роботи EPP-команд. Дія стосовно очікування відповіді на запит EPP, під час якої значення показника параметру сервісу в п’ять разів перевищує відповідне необхідне значення, вважається такою, що завершилася невдало. Якщо в 51% або більше під час перевірки моніторами такі дії були невдалими, така служба EPP вважається недоступною впродовж певного часу.

Мінімальні значення параметрів, що мають бути забезпечені у підсистемі реєстрацій:

Параметр	**SLR (щомісячно)**
Доступність служби EPP	=< час простою 864 хв. (не менше 98%)

RTT команди керування сесією	=< 4000 мс принаймні для 90% команд
RTT команди на отримання інформації	=< 2000 мс принаймні для 90% команд
RTT команди на зміну інформації	=< 4000 мс принаймні для 90% команд

2.2.2. Безпека у підсистемі реєстрацій.

Окрім вимог щодо розробки і наступного впровадження комплексної системи захисту інформацій відповідно до вимог законодавства і що згадані в пункті 1.4 цих Вимог, зокрема основні сервери підсистеми реєстрацій Претендента, що матимуть статус Master, повинні надавати усім підлеглим серверам можливість актуалізації, обробки та зберігання даних про поточні реєстрації, але при цьому не повинні бути доступними ззовні і мати статус Hidden Back-End.

Підсистема реєстрацій повинна забезпечувати захищену обробку усіх транзакцій. Претендент повинен представити рішення стосовно захищеної обробки усіх транзакцій.

Підсистема реєстрацій повинна забезпечувати безвідмовну (безперебійну) роботу та здатність відновлення актуальних даних у випадку виникнення позаштатних і непередбачуваних ситуацій. Претендент повинен представити рішення стосовно забезпечення безвідмовної (безперебійної) роботи та здатності відновлення актуальних даних у випадку виникнення позаштатних і непередбачуваних ситуацій.

2.2.3. Набір інструментів з розробки програмного забезпечення EPP.

На момент подання заяви Претендент повинен мати документ «Опис API EPP», яким визначатимуться можливості з розробки і інструкції з вбудовування програмного забезпечення та його елементів у програмні комплекси Реєстраторів, для забезпечення автоматизованого процесу взаємодії програмних комплексів Реєстраторів з реєстром домену .УКР.

2.2.4. Інші вимоги до EPP.

Реалізація протоколу EPP, що пропонуватиметься Претендентом, повинна забезпечити на рівні «клієнт-сервер» таку можливість управління даними і об’єктами, що зберігаються у репозитарії (реєстрі), яка підтримуватиме обробку інформації з кодуванням як UTF-8 так і PUNYCODE.

2.3. Підсистема DNS.

2.3.1. Принципи роботи підсистеми DNS та її доступність

Доступність служби DNS - здатність групи серверів доменних імен, що визначені як повноважні сервери DNS для домену .УКР, відповідати на запити (здебільшого це запити типу nslookup) інших серверів і клієнтів DNS або запити від спеціальних моніторів щодо адресації та іншої службової

інформації доменних імен. Для того, щоб служба DNS вважалася доступною в конкретний момент часу, принаймні для двох повноважних серверів доменних імен, мають бути отримані успішні результати DNS-перевірок. Якщо у 51% або більше випадків DNS-перевірок служба недоступна впродовж певного часу, така служба DNS вважається недоступною.

Доступність сервера імен DNS - здатність окремого DNS сервера відповідати на запити інших DNS-серверів і клієнтів у формі визначеній Інтернет-стандартами.

Всі зареєстровані у вповноваженій службі DNS вищого рівня IP-адреси всіх серверів доменних імен, що контролюються, повинні проходить перевірку в індивідуальному порядку. Якщо у 51% або більше випадків DNS перевірок для певних серверів впродовж заданого часу отримуються відповіді типу «undefined/unanswered» (не визначено/без відповіді), такий сервер імен вважається недоступним.

Мінімальні значення параметрів, що мають бути забезпечені у підсистемі DNS:

Параметр	**SLR (щомісячно)**
Доступність служби DNS	Час простою 0 хв. = 100% доступність
Доступність сервера імен DNS	=< Час простою 432 хв. (не менше 99%)
RTT для DNS/TCP	=< 1500 мс принаймні для 95% запитів
RTT для DNS/UDP	=< 1500 мс принаймні для 95% запитів
Час оновлення DNS	=< 60 хв. принаймні для 95% тих, хто звертається за інформацією

2.3.2. Надійність роботи груп серверів у підсистемі DNS.

Надійність роботи груп серверів у підсистемі DNS повинна бути 100%.

Претендент повинен передбачити у рішеннях, що ним представляються, можливість захисту даних від модифікації, спотворення та дискредитації їх в процесі передавання цих даних від DNS-серверів до клієнтів. Також, повинні бути представлені засоби запобігання створенню хибних DNS-серверів, які надаватимуть недостовірні дані (відповіді).

2.3.3. Обслуговування файлу зони.

Програмне забезпечення у Системі, що представлятиметься Претендентом, повинне забезпечувати динамічне поновлення файлу зони.

Претендент повинен представити у належному рішенні технічні параметри, що необхідні для поточного обслуговування, архівування і депонування файлу зони домену .УКР/xn--j1amh.

Збереження дампу (архіву) файлу зони повинне проводитись щоденно на окремі з'ємні носії інформації, включаючи такі, які не перезаписуються.

При виникненні позаштатної (непередбачуваної) ситуації щодо працездатності Системи, відновлення бази даних і файлу зони повинне здійснюватися з окремих з'ємних носіїв інформації на дискові масиви серверів, що задіяні у забезпеченні роботи Системи і що є резервними і знаходяться у стані «гарячої заміни» («гарячого резерву»).

2.3.4. Вимоги до DNS-серверів.

Підсистема DNS-серверів у складі рішення Претендента повинна складатись щонайменше 13 серверів, що розташовані мінімум у 5 (п'яти) різних датацентрах. Як мінімум 5 (пять) серверів повинні знаходитись у стані «гарячої заміни» («гарячого резерву»), з яких мінімум 3 (три) повинні бути у стані Stand-by.

Мінімальна конфігурація серверів: Quad Core CPU, 16GB DDR3 ECC, 2-4 HDD (SAS/SATA/SSD), Raid controller, 64-bit Unix operating system, IPMI, дубльоване живлення, 100% готовності «гарячої заміни».

2.4. Служба WHOIS

2.4.1. Принципи роботи служби WHOIS та її доступність.

Підсистема WHOIS повинна підтримувати UTF-8 (Unicode) з можливістю отримання і надання відповідей запитів українською та російською мовами, а також в ASCII.

Доступність служби WHOIS - здатність всіх служб WHOIS домену .УКР надавати у відповідь на запити користувачів Інтернету відповідні дані з реєстру. Якщо в 51% або у більш випадках перевірка WHOIS спеціальними моніторами показує, що яка-небудь із служб WHOIS недоступна впродовж певного часу, така служба WHOIS вважається недоступною.

Мінімальні значення параметрів, що мають бути забезпечені службою WHOIS:

Параметр	**SLR (щомісячно)**
Доступність WHOIS	=< час простою 864 хв. (не менше 98%)
RTT WHOIS -запиту	=< 2000 мс принаймні для 95% запитів
Час оновлення WHOIS	=< 60 хв.

Система WHOIS-серверів Претендента повинна складатись щонайменше з 6 (шести) серверів, що розташовані у 3 (трьох) різних датацентрах. 3 (три) сервера повинні знаходитися у стані «гарячої заміни» («гарячого резерву»).

2.4.2. Формат інформації у службі WHOIS

Набір даних в службі WHOIS повинен відображати інформацію на оригінальній мові реєстрації доменного імені з автоматичною

транслітерацією в ASCII або із можливістю автентичного перекладу англійською мовою в ASCII шляхом редагування відповідних полів.

2.4.3. Набір даних WHOIS

Послідовність даних, що мають бути надані у відповідь на запит, наведені у нижче приведеної таблиці

Поле	**Значення**
Domain Name (PUNYCODE):	Ім’я домену в кодуванні PUNYCODE
Domain Name (UTF8):	Ім’я домену в кодуванні UTF8
Registry Domain ID:	Ідентифікатор реєстрації доменного імені
Registrar WHOIS Server:	WHOIS-сервер Реєстратора
Updated Date:	Дата проведення модифікації домену
Creation Date:	Дата реєстрації доменного імені
Expiration Date:	Дата закінчення дії реєстрації доменного імені
Registry Status:	Поточний статус, в якому знаходиться домен
Registrar:	Назва Реєстратора
Registrar URL:	Адреса сайту Реєстратора
Registrar ID:	Ідентифікатор Реєстратора
Registrar Abuse Contact Email:	Адреса електронної пошти Реєстратора, на яку слід відправляти скарги відносно використання домену
Registrar Abuse Contact Phone:	Телефон Реєстратора, на яку слід дзвонити у випадку виникнення скарг відносно використання домену
Registry Registrant ID:	Ідентифікатор Реєстранта
Registrant Name:	Ім’я (Назва) Реєстранта
Registrant Organization:	Назва організації Реєстранта
Registrant Street:	Вулиця, номер дому з адреси Реєстранта
Registrant City:	Місто з адреси Реєстранта
Registrant Postal Code:	Поштовий код з адреси Реєстранта

Registrant Country:	Країна з адреси Реєстранта
Registrant Phone:	Телефонний номер Реєстранта
Registrant Phone Ext:	Додатковий номер офісної АТС до телефонного номеру Реєстранта
Registrant Fax:	Номер факсу Реєстранта
Registrant Fax Ext:	Додатковий номер офісної АТС до факсу Реєстранта
Registrant Email:	Адреса електронної пошти Реєстранта
Registry Admin ID:	Ідентифікатор адміністратора домену
Admin Name:	Ім’я адміністратора
Admin Organization:	Назва організації адміністратора
Admin Street:	Вулиця, номер дому з адреси адміністратора
Admin City:	Місто з адреси адміністратора
Admin Postal Code:	Поштовий код з адреси адміністратора
Admin Country:	Країна з адреси адміністратора
Admin Phone:	Телефонний номер адміністратора
Admin Phone Ext:	Додатковий номер офісної АТС до телефонного номеру адміністратора
Admin Fax:	Номер факсу адміністратора
Admin Fax Ext:	Додатковий номер офісної АТС до факсу адміністратора
Admin Email:	Адреса електронної пошти адміністратора
Registry Tech ID:	Ідентифікатор технічного контакту домену
Tech Name:	Ім’я технічного контакту
Tech Organization:	Назва організації технічного контакту
Tech Street:	Вулиця, номер дому з адреси технічного контакту
Tech City:	Місто з адреси технічного контакту

Tech Postal Code:	Поштовий код з адреси технічного контакту
Tech Country:	Країна з адреси технічного контакту
Tech Phone:	Телефонний номер технічного контакту
Tech Phone Ext:	Додатковий номер офісної АТС до телефонного номеру технічного контакту
Tech Fax:	Номер факсу технічного контакту
Tech Fax Ext:	Додатковий номер офісної АТС до факсу технічного контакту
Tech Email:	Адреса електронної пошти технічного контакту
Registry Bill ID:	Ідентифікатор фінансового контакту домену
Bill Name:	Ім’я фінансового контакту
Bill Organization:	Назва організації фінансового контакту
Bill Street:	Вулиця, номер дому з адреси фінансового контакту
Bill City:	Місто з адреси фінансового контакту
Bill Postal Code:	Поштовий код з адреси фінансового контакту
Bill Country:	Країна з адреси фінансового контакту
Bill Phone:	Телефонний номер фінансового контакту
Bill Phone Ext:	Додатковий номер офісної АТС до телефонного номеру фінансового контакту
Bill Fax:	Номер факсу фінансового контакту
Bill Fax Ext:	Додатковий номер офісної АТС до факсу фінансового контакту
Bill Email:	Адреса електронної пошти фінансового контакту
NS servers (Domain servers in listed order):	Перелік серверів імен, які обслуговують домен

2.5. Вимоги до мережі.

2.5.1. Управління мережею.

Управління мережею повинне відбуватись з одного центру у штатному режимі роботи.

Управління мережею повинне передбачати можливість віддаленого доступу до вузлів підсистеми управління реєстром (Системою) у випадках виникнення позаштатних ситуацій.

Управління мережею повинне відбуватись у режимі 7x24x365.

2.5.2. Безпека мережі.

Базовими вимогами по забезпеченню безпеки мережі для Претендента є наступне:

1) **ідентифікація** – яка здійснюється з метою попередження загроз знеособленого і несанкціонованого доступу до ресурсів і даним підсистем реєстру (Системи). У вимогах визначається, що дії щодо ідентифікації обов'язково і завжди містять авторизацію;
2) **цілісність**, яка забезпечує захист від підслуховування, сканування та маніпулювання даними, підтримуючи конфіденційність та незмінність інформації, що передається мережею;
3) **активна перевірка**, яка означає перевірку правильності застосування приписів політик безпеки і допомагає виявляти несанкціоноване проникнення в мережу і атаки типу DDoS. Активна перевірка повинна відбуватись в режимі on-line.

З метою забезпечення підтримки (забезпечення) безпеки мережеве обладнання на кожному вузлі повинне здійснювати аудит мережі і аналіз мережевих інцидентів в режимі on-line.

Фільтрування IP-адрес певних мереж допускається виключно у випадках виникнення атак з цих мереж типу DDoS і т.п. на вузли Системи.

Реєстратори проходитимуть процедуру акредитації. Претендент повинен представити своє рішення щодо принципів технічної вимоги у процедурі акредитації Реєстраторів з точки зору взаємодії автоматизованих систем Реєстраторів і безпеки мережі.

З'єднання автоматизованих систем Реєстраторів з підсистемою реєстрацій у складі реєстру (Системи) повинне відбуватися виключно з використанням протоколів захисту мережевих з'єднань. Кожному акредитованому Реєстраторові повинен бути у Системі присвоєний ID та пароль (або токен). Доступ з автоматизованих систем Реєстраторів до підсистеми реєстрацій повинен бути дозволений від заздалегідь визначених IP-адрес. Претендент повинен представити своє рішення щодо застосування ним захищеного доступу (у тому числі мережевого) та ідентифікації.

2.6. Вимоги до забезпечення безперервності бізнес-процесів

2.6.1. План дій щодо забезпечення безперервності бізнес-процесів.

Претендент повинен представити документи «План по відновленню працездатності Системи та/або підсистем у разі виникнення позаштатних ситуацій (катастроф, аварій тощо) та відповідні посадові інструкції» та «План

дій щодо забезпечення технічної підтримки безперервності бізнес-процесів», які повинні серед іншого описувати наступне:

1) Відмовостійкість.
2) Подолання надзвичайних ситуацій .
3) Резервне копіювання і відновлення.
4) Підтримка критично важливих бізнес-процесів.

Плани дій повинні містити розробку сценаріїв Претендента (Оператора реєстру) зокрема в умовах:

1) перебоїв з електроживленням (включаючи довготривалі);
2) збоїв в роботі обладнання ІТ-системи;
3) збоїв в роботі програмного забезпечення (як ОС, так і прикладного і додатків);
4) збоїв в роботі мережевого обладнання;
5) недостатня кваліфікація технічного персоналу та його помилки;
6) помилок в програмних комплексах, що обслуговують реєстр (Систему).

2.6.2. Вимоги до організації служби підтримки Оператора реєстру

Управління мережею повинне здійснюватися безперервно впродовж трьох робочих змін. Штатний розклад однієї робочої зміни повинен передбачати не менше 2 (двох) системних адміністраторів у денний час, що задіяні виключно у цій роботі, і одного у нічний час, що також задіяний виключно у цій роботі, та не менш ніж 2 (двох) працівників персоналу технічної підтримки у денний час і одного у нічний час. Претендент повинен представити відповідні посадові інструкції чергового персоналу змін щодо усіх позицій.

Управління мережею повинне здійснюватися персоналом в режимі 7x24x365. Час відклику і реагування на зовнішнє звернення не повинне перевищувати 120 секунд.

Кваліфікація персоналу повинна бути підтверджена Претендентом.

2.6.3. Охорона територій.

Пропуск на території офісних приміщень Оператора реєстру може бути вільним, але з дозволу персоналу. Усі робочі комп’ютери, з яких забезпечується доступ до Системи повинні не зберігати постійно паролі доступу у програмних додатках і в ОС, вводитись кожного разу у кожному сеансі доступу. Тривалість сеансів має бути короткою, комп’ютери не повинні залишатись без нагляду персоналу, щоб запобігти використанню цих комп’ютерів сторонніми особами, що зайшли до офісних приміщень. Має бути передбачена можливість екстреної або заздалегідь підготовленої передачі управління і доступу у ІТ-систему реєстру збоку керівного складу Оператора реєстру та Адміністратора через віддалений вузол з можливістю підняття привілей управління в Системі з метою відміни усіх можливих змін, що були зроблені з поточними привілеями управління у разі, якщо такий доступ скомпрометовано (отримано доступ сторонніми особами). Усі особи крім

керівного складу Оператора реєстру та Адміністратора щодо дій з підвищеними привілеями є сторонніми особами, яким такі дії забороняються та інформація про можливість таких дій (адреси, послідовність тощо) повинна бути недоступною.

Пропуск на територію виробничих приміщень Оператора реєстру повинне відбуватися виключно на підставі відповідного допуску.

Допуск до обладнання ІТ-систем та телекомунікаційного (мережевого) обладнання має дозволятися строго обмеженому колу осіб з персоналу Оператора реєстру або персоналу того датацентру, з яким у Оператора реєстру укладено договір. Відповідальність за безперервність і сталість роботи реєстру (Системи) покладається на Оператора реєстру.

Претендент повинен представити усі рішення та інструкції з зазначених питань у цьому розділі Вимог.

2.6.4. Система сповіщення.

Система сповіщення повинна забезпечувати негайне повідомлення про виникнення позаштатної ситуації черговій зміні (у відповідності до посадових інструкцій персоналу) та керівному складу Оператора реєстру, а також протоколювання таких повідомлень та їх вистежування.

Претендент повинен представити своє рішення з організації системи сповіщення.

2.6.5. Вимоги до звітності.

Звітність повинна представлятися в електронному та письмовому (друкованому) вигляді.

Звітність у вигляді Технічного звіту зміни повинна відкриватись як журнал на початку кожної зміни, вестись впродовж усієї зміни (до передачі іншій зміни, а не до завершенням зміни) і завершуватись відповідними записами і підписом відповідальної особи наприкінці зміни.

Технічний звіт зміни повинен містити повні відомості про кожну обставину або ситуацію, що є позаштатними (час виникнення, встановлені причини виникнення, дії персоналу, відповідального за ліквідування, час завершення (повернення у штатний стан), наслідки).

У разі, якщо позаштатні ситуації виникають з періодичністю повинен бути складений Технічний звіт про позаштатну ситуацію, у якому описується з вичерпною повнотою характер виникнення позаштатної ситуації, характерні ознаки, дії, що застосовувались, іншу інформацію, що може бути корисною. Технічний звіт про позаштатну ситуацію, що виникає періодично складається призначеною відповідальною особою або керівництвом Оператора реєстру..

Зберігання звітності здійснюється на електронних носіях. Відповідальність за збереження, цілісність, коректність і своєчасність надання звітності про технічний стан реєстру несе Оператор реєстру.

Термін зберігання звітності необмежений і визначається рішенням Адміністратора.

Претендент повинен представити своє рішення з організації звітності.

2.6.6. Статистика та інформація про стан працездатності.

Система повинна мати інтерфейс доступу до статистичних даних (кількість реєстрацій, подовжень реєстрацій, скасувань, певних станів доменних імен, стану працездатності підсистем, час безперервної роботи, кількість збоїв та їх тривалість тощо). Система статистики повинна мати можливість автоматизованого експорту частини даних, що визначатиметься Адміністратором, для обробки їх зовнішніми системами. Доступ до системи статистики та інформації про стан працездатності має бути обмеженим і визначатиметься Адміністратором.

Претендент повинен представити своє рішення з організації системи статистики та інформації про стан працездатності.