ЗАПИТ НА НАДАННЯ ВИСЛОВЛЕНЬ ЗАЦІКАВЛЕНОСТІ
(REoI № MF-IC-15)
(консультаційні послуги, індивідуальний консультант)

УКРАЇНА
ПРОЕКТ ЗМІЦНЕННЯ УПРАВЛІННЯ ДЕРЖАВНИМИ РЕСУРСАМИ ЧАСТИНИ В «ПІДТРИМКА ВПРОВАДЖЕННЯ СТРАТЕГІЇ УПРАВЛІННЯ ДЕРЖАВНИМИ ФІНАНСАМИ» (ПОРЯДКОВИЙ НОМЕР ПРОЕКТУ P161586)

Грант № TF0A5324

Назва завдання: Консультант з інформаційної кібербезпеки із створення хмарної системи управління державними фінансами

№ завдання (за Планом закупівель): MF-IC-15

Уряд України отримав фінансування з боку Міжнародного банку реконструкції та розвитку (далі – Світовий банк), який виступає адміністратором коштів гранту, наданого Європейською комісією від імені Європейського Союзу в рамках Програми партнерства ЄС та Світового банку в Європі та Центральній Азії та Програмного траст фонду за участю одного донора (Програма ЄС з реформування державного управління та фінансів (EURoPAF)) для реалізації Проекту зміцнення управління державними ресурсами.

Міністерство фінансів України (далі – МФУ) відповідає за реалізацію Частини В Проекту і, з метою посилення своєї спроможності щодо впровадження Проекту, залучає на умовах конкурсного відбору індивідуального консультанта – Консультанта з інформаційної кібербезпеки із створення хмарної системи управління державними фінансами (далі – Консультант) для реалізації організаційно-технічних заходів з розробки та впровадження комплексної системи захисту інформації в інформаційно-телекомунікаційній системі МФУ.

Консультаційні послуги (надалі - Послуги) передбачають надання МФУ допомоги в рамках етапів процесу розробки та створення комплексної системи захисту інформації (далі – КСЗІ) інформаційно-телекомунікаційної системи МФУ (далі - ІТС МФУ), з:

1) Проведення передпроектних досліджень середовищ функціонування ІТС МФУ, Державної митної служби, Державної податкової служби, Державної казначейської служби на предмет включення ресурсів зазначених органів до загальної хмари (територіально розподіленого центра обробки даних) Міністерства фінансів, ДМСУ, ДПСУ та ДКСУ (далі – загальна хмара СУДФ);.
2) Розробка політики безпеки інформації в ІТС для технологічних процесів обробки даних в загальній хмарі СУДФ;
3) Здійснення проектування КСЗІ ІТС загальної хмари СУДФ та підготовка КСЗІ до введення в експлуатацію.

В ході оцінки повинні бути виявлені основні прогалини в інформаційній безпеці, пов'язані з ними ризики і заходи щодо виправлення становища.

Очікується, що при оцінці стану справ будуть використовувати як стандарти ISO 27001, так і відповідні стандарти ДСТУ як еталон і використовувати СММ (модель зрілості можливостей) для оцінки рівня зрілості в кожній з оцінюваних областей.

Послуги надаватимуться в місці проживання Консультанта.

Очікується що Консультант буде працювати впродовж періоду з листопада 2020 року до березня 2021 року. Очікувані трудовитрати загалом не повинні перевищувати 120 робочих днів.

Консультант працюватиме в межах затвердженого Технічного завдання, яке додається.

МФУ запрошує правомочних фізичних осіб з – місцевих індивідуальних консультантів (надалі - Кандидати) висловити свою зацікавленість щодо надання Послуг у формі резюме (українською чи англійською мовами). Зацікавлені кандидати мають надати інформацію щодо відповідності своєї кваліфікації та досвіду для виконання Послуг.

Кандидати мають надати підтвердження у формі посилання на публічно підтверджену та доступну інформацію чи надання копій відповідних документів що засвідчують відповідний статус чи стан.

Кандидати можуть додавати будь-які інші додаткові матеріали, які можуть підтверджувати наявність заявленого кандидатом досвіду та кваліфікації.

Вимоги до кваліфікації зацікавлених кандидатів наступні.

Обов'язкові кваліфікаційні вимоги:

- вища технічна освіта;
- досвід роботи у сфері захисту інформації не менше п’яти років, з яких не менше 2 років впродовж останніх 5 років;
- наявність свідоцтва про підвищення кваліфікації у сфері технічного та криптографічного захисту інформації не менше одного за кожним напрямком;
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ впродовж останніх 5 років не менше 3 реалізованих договорів/проектів;
- Знання та наявність навичок практичного застосування основних сервісів Microsoft, мережевих сервісів (DNS, DHCP, VLAN, VPN);
- досвід роботи із засобами мережевої безпеки;
- вільне володіння письмовою та усною українською мовою.

Кваліфікаційні вимоги, які відповідають специфіці завдання та будуть прийматись як перевага:

- наявність сертифікату СПБІС (CISSP) (Сертифікований професіонал з безпеки інформаційних систем) або САІС (CISA) (Сертифікований аудитор інформаційних систем) або СМІС (CISM) (Сертифікований менеджер інформаційних систем);
- наявність сертифікату про успішне проходження тренінгу/навчального курсу з питань впровадження та використання вимог ISO / IEC 27001:2013 «Інформаційні

технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» за напрямками Впроваджувач та/чи Аудитор;

- досвід впровадження комплексних системи захисту інформації різних типів (АС1, АС2, АС3);
- наявність наукового ступеню за технічними науками;
- наявність авторських патентів на розробки в галузі ТЗІ та КЗІ;
- наявність ліцензії Державної служби спеціального зв'язку та захисту інформації України на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації;
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ для організацій державного сектору економіки;
- володіння англійською мовою на рівні опрацювання технічної документації в сфері ІТ без словника.

Зацікавлені Кандидати мають звернути увагу на Розділ III, параграфи , 3.14,3.16, та 3.17, «Керівництва МБРР із закупівель для Позичальників інвестиційних проектів» (липень 2016 року, переглянуте в листопаді 2017 та серпні 2018 року) (далі – Керівництво із закупівель) що визначає політику Світового банку щодо конфлікту інтересів.

Відбір Консультанта здійснюватиметься за процедурою відбору індивідуальних консультантів (ІС), за правилами встановленими у вищевказаному Керівництві.

Зацікавлені Кандидати можуть отримати додаткову інформацію за зазначеною нижче контактною інформацією з 10:00 до 18:00 окрім вихідних днів:

Контактна особа: Володимир Воротюк
Телефон: +38 044 206 5773, 380 50 4100340
Ел.пошта: vorotyuk@outlook.com

Висловлення зацікавленості слід направляти електронною поштою за наведеною нижче адресою до 17:00 (за місцевим часом) 4 листопада 2020 року.

Міністерство фінансів України
До уваги: Ігоря Шевлякова, Керівника експертної групи з європейської інтеграції Директорату стратегічного планування та європейської інтеграції.
Тема листа – "Висловлення зацікавленості - MF-IC-15, Консультант з інформаційної кібербезпеки із створення хмарної системи управління державними фінансами"
Ел.пошта: shevliakov@minfin.gov.ua, обов'язкова копія vorotyuk@outlook.com.

Додаток до REoI №MF-IC-15

ТЕХНІЧНЕ ЗАВДАННЯ

на надання консультаційних послуг:

Консультант з інформаційної кібербезпеки із створення хмарної системи управління державними фінансами

(Індивідуальний консультант)

Номер закупівлі №: MF-IC-15

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

Уряд України отримав фінансування з боку Міжнародного банку реконструкції та розвитку (далі – Світовий банк), який виступає адміністратором коштів гранту, наданого Європейською комісією від імені Європейського Союзу (далі – Донор) в рамках Програми партнерства ЄС та Світового банку в Європі та Центральній Азії та Програмного траст фонду за участю одного донора (Програма ЄС з реформування державного управління та фінансів (EURoPAF)) у розмірі 3 030 661 євро (далі – Грант) для реалізації Проекту зміцнення управління державними ресурсами (далі – Проект). Цей Проект складається з двох частин: Частини А «Зміцнення управління людськими ресурсами на державній службі» та Частини В «Підтримка впровадження Стратегії управління державними фінансами».

Частина В Проекту, обсягом 1 110 618 євро, передбачає підтримку заходів для реалізації Стратегії реформування системи управління державними фінансами на 2017-2020 роки та визначення майбутніх потреб в інвестиціях в ІКТ системи в сфері управління державними фінансами шляхом проведення ІКТ аудиту; модернізації існуючого ІКТ обладнання для підтримки безперервної роботи МФУ; посилення спроможності ІКТ систем та ін.

Для досягнення мети одним із головних завдань Стратегії реформи управління державними фінансами є широке запровадження надійних ІТ-рішень та автоматизація існуючих процесів у сфері управління державними фінансами, з метою мінімізації людського впливу та пов’язаних із цим корупційних викликів.

Міністерство фінансів України (далі – МФУ) відповідає за реалізацію Частини В Проекту і, з метою посилення своєї спроможності щодо впровадження Проекту, залучає на умовах конкурсного відбору індивідуального консультанта – Консультанта з інформаційної кібербезпеки із створення хмарної системи управління державними фінансами (далі – Консультант) для реалізації організаційно-технічних заходів з розробки та впровадження комплексної системи захисту інформації в інформаційно-телекомунікаційній системі МФУ.

2. ОПИС ПРОБЛЕМИ

На сьогодні в Україні, кожний державний орган та підприємство повинні забезпечувати максимальну автоматизацію процесів своєї життєдіяльності, оперативну взаємодію та обмін інформацією в процесі прийняття управлінських рішень.

Залежність організації від інформаційних систем, які забезпечують її життєдіяльність, стає причиною серйозних ризиків щодо забезпечення захисту інформаційних ресурсів, які обробляються їхніми засобами. Відмова в роботі такої інформаційної системи або несанкціоноване втручання в її роботу може мати катастрофічні наслідки як для організації, так і для країни в цілому. Тому одночасно з впровадженням інформаційних систем (далі – ІС) велика увага приділяється їх безпеці, відмовостійкості та захисту інформації, яка циркулює в системах.

Інформаційно-телекомунікаційна система МФУ (далі – ІТС) представляє собою сервісно-орієнтовану програмно-апаратну платформу впровадження та виконання типізованих прикладних інформаційних сервісів, які реалізуються на єдиній програмно-апаратній платформі, підтримують єдину технологію обробки інформації та забезпечують механізми реалізації положень єдиної політики безпеки затвердженої МФУ.

Програмно-апаратна платформа ІТС реалізує стратегію єдиної інтеграційної системи, що об'єднує в собі технології та програмні засоби, які дозволяють забезпечувати функціонально замкнуту та самодостатню систему обробки даних в рамках створюваних (впроваджуємих) прикладних сервісів (автоматизованих систем) з підтримкою визначених фіксованих (для усіх систем ІТС) типів об'єктів захисту, суб'єктів доступу (груп і ролей користувачів) та базовими умовами експлуатації.

Відповідно до ст. 6 Закону України «Про доступ до публічної інформації» та ст. 21 Закону України «Про інформацію» до інформації, яка обробляється засобами інформаційних систем органів державної влади та яка зберігається в державних реєстрах, висуваються вимоги щодо забезпечення її конфіденційності, цілісності та доступності в процесі її обробки.

При цьому відповідно до Розпорядження КМУ від 10.07.2019 №594-р «Про схвалення Концепції з ІТ-централізації в системі управління державними фінансами» передбачено створення єдиного ландшафту ІТ-систем з високим рівнем інтеграції та взаємодії, що в свою чергу передбачає використання єдиного сховища даних з актуальною інформацією.

Реалізацію використання єдиного сховища даних можливо забезпечити шляхом створення загальної хмари (територіально розподіленого центра обробки даних) Міністерства фінансів, ДМСУ, ДПСУ та ДКСУ – далі загальна хмара СУДФ.

Використання хмарних послуг не тільки зручне, а й безпечне, оскільки, навіть якщо з технікою, на якій зберігається певна інформація, щось трапиться, дані не зникнуть, адже суть хмарних технологій полягає в перенесенні обробки даних із комп'ютерів на сервери всесвітньої мережі.

В Україні дане питання не врегульовано на законодавчому рівні належним чином, тому виникла необхідність у прийнятті документа, який би врегулював дані відносини, а також відносини, пов'язані з обробкою та захистом даних при наданні хмарних послуг, а також забезпечив та врегулював порядок використання хмарних послуг органами державної влади.

Таким чином, 16 червня 2020 р. Верховна Рада України в першому читанні прийняла Проект Закону «Про хмарні послуги» №2655 від 20.12.2019 р.

При цьому, з метою забезпечення політики безпеки ІТС у відповідності до вимог чинного законодавства України та виключення або мінімізації збитку, спричиненому

несанкціонованим доступом до інформаційних ресурсів на рішення (в тому числі з використанням хмарних технологій) повинна бути створена комплексна система захисту інформації (далі – КСЗІ) з підтвердженою відповідністю відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

КСЗІ ІТС розробляється згідно типового порядку створення КСЗІ в АС (НД ТЗІ 3.7-003-05), з урахуванням інтегрованого підходу щодо реалізації складових її архітектури.

Метою створення комплексної системи захисту інформації ІТС є забезпечення захисту інформації, яка обробляється засобами ІТС, шляхом запобігання та протидії несанкціонованому доступу, розголошенню, спотворенню та втратам при її обробці і передачі. Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування компонентів ІТС. Комплексна система захисту інформації є невід'ємною складовою частиною ІТС.

КСЗІ є комплексом програмних і технічних засобів та організаційних заходів спрямованих на забезпечення встановленого рівня захисту інформації відповідно до умов середовищ експлуатації ІТС та вимог забезпечення основних характеристик безпеки, визначених політикою безпеки Системи та організації-розпорядника. КСЗІ ІТС призначена для реалізації положень політики безпеки інформації в частині:

- ідентифікації та автентифікації користувачів Системи під час доступу та використання об’єктів захисту;
- керування авторизованими користувачами та розподілу повноважень щодо використання інформаційних та програмних ресурсів ІТС;
- забезпечення конфіденційності та цілісності інформації, яка циркулює в ІТС та/або передається між її компонентами;
- забезпечення ідентифікації та автентифікації вузлів ІТС під час сеансу взаємодії;
- забезпечення конфіденційності та цілісності інформації, яка надається зовнішнім користувачам/системам;
- забезпечення ідентифікації та автентифікації вузлів зовнішніх систем під час сеансу взаємодії;
- забезпечення конфіденційності, цілісності та доступності технологічної інформації щодо функціонування системи;
- забезпечення доступності інформації, яка циркулює в ІТС, для авторизованих користувачів та процесів;
- реєстрації та обробки всіх подій в ІТС, які мають відношення до безпеки інформації;
- реалізації моніторингу актуального стану безпеки та працездатності компонентів ІТС;
- управління всіма механізмами безпеки через відповідний інтерфейс адміністрування, який повинен бути доступним тільки уповноваженому персоналу.

3. МЕТА І ЗАВДАННЯ

Метою завдання є надання в рамках етапів процесу розробки та створення комплексної системи захисту інформації ІТС МФУ послуг з:

- Проведення передпроектних досліджень середовищ функціонування ІТС МФУ, Державної митної служби, Державної податкової служби, Державної казначейської служби на предмет включення ресурсів зазначених органів до загальної хмари СУДФ;.
- Розробка політики безпеки інформації в ІТС для технологічних процесів обробки даних в загальній хмарі СУДФ;
- Здійснення проектування КСЗІ ІТС загальної хмари СУДФ та підготовка КСЗІ до введення в експлуатацію.

В ході оцінки повинні бути виявлені основні прогалини в інформаційній безпеці, пов'язані з ними ризики і заходи щодо виправлення становища.

Очікується, що при оцінці стану справ будуть використовувати як стандарти ISO 27001, так і відповідні стандарти ДСТУ як еталон і використовувати CMM (модель зрілості можливостей) для оцінки рівня зрілості в кожній з оцінюваних областей.

Ключові технічні аспекти, на яких буде зосереджена оцінка, серед іншого, будуть включати:

1) Документування системи (наявність інструкцій щодо розгортання, встановлення, оновлення тощо), політика безпеки та процедура безпеки);

2) Системи і методологія контролю доступу: для оцінки наявності засобів контролю доступу для запобігання отримання, використання або зміни інформації неавторизованими користувачами.

3) Ідентифікація та аутентифікація

4) Мережева безпека: щоб оцінити, чи працюють в мережі, зокрема, адекватні міжмережеві екрани, шифрування даних, служби аутентифікації і протоколи безпеки.

5) інфраструктура безпеки, включаючи міжмережеві екрани, системи запобігання вторгнень (IPS), інформацію про безпеку і управління подіями (SIEM), систему моніторингу підприємства (EMS);

6) організаційні заходи щодо реєстрації та обслуговування розподілених користувачів; і

7) заходи безпеки з боку адміністраторів користувачів і кінцевих користувачів і надання рекомендацій по мірі необхідності.

4. ОБСЯГ ЗАВДАННЯ ТА ОЧІКУВАНІ РЕЗУЛЬТАТИ

Консультант має виконувати наступні завдання відповідно до наступних етапів:

4.1 На етапі передпроектних досліджень середовищ функціонування ІТС МФУ, Державної митної служби, Державної податкової служби, Державної казначейської служби (на предмет включення ресурсів зазначених органів до загальної хмари СУДФ) консультант повинен:

4.1.1 Розробити та подати на затвердження Замовнику обґрунтовані концептуальні рішення щодо рівнів представлення архітектури ІТС загальної хмари СУДФ, ескізний проект та сценарій побудови КСЗІ в ІТС. Провести аналіз щодо можливості та необхідності реалізації ОТР.

4.1.2 За результатом наданих даних щодо аналізу ймовірності та наслідків потенційних загроз інформації відповідно до визначених ресурсів ІТС, технологічних процесів системи та вразливостей програмно-апаратного забезпечення компонентів ІТС на підставі затверджених концептуальних рішень щодо рівнів представлення архітектури ІТС всіх органів (МФУ, Державної митної служби, Державної податкової служби, Державної казначейської служби), сформувати завдання створення та впровадження КСЗІ ІТС загальної хмари СУДФ:

- визначити завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту (відповідно до ДСТУ 3396.1), основні напрями забезпечення захисту;

- здійснити аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, та ін.) і визначити перелік суттєвих загроз;

- визначити загальну структуру та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту, інші обмеження щодо середовищ функціонування ІТС, обмеження щодо використання ресурсів ІТС для реалізації задач захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

4.1.3 Підготувати документи за результатами аналізу , як визначено в п.п.1 Розділу 5 цього Завдання.

4.1.4 Підготувати та подати відповідний звіт з проведення передпроектного обстеження і вносити до нього зміни, у разі необхідності.

4.2 На етапі розробки політики безпеки інформації в ІТС зальної хмари СУДФ для технологічних процесів обробки даних та розробки Технічного завдання на створення КСЗІ в ІТС загальної хмари СУДФ консультант повинен:

4.2.1 Розробити та подати на затвердження Замовнику структуру та концепцію технічного завдання та створення КСЗІ в ІТС загальної хмари СУДФ, яка, виходячи із визначених основних рівнів архітектури ІТС, повинна включати у вигляді окремих документів та/або розділів:

- Технічне завдання на КСЗІ Програмно-технічного комплексу центрального сегменту інформаційно-телекомунікаційної системи загальної хмари СУДФ
- Технічні вимоги щодо Організаційно-технічних рішень (далі – ОТР) впровадження заходів та технологій захисту для типових інтерфейсів доступу користувачів до інформаційних ресурсів ІТС.

- Технічне завдання на КСЗІ Програмно-технічного комплексу центрального сегменту інформаційно-телекомунікаційної системи Міністерства фінансів України, до складу якого входять:
  - Центр обробки даних (далі – ЦОД);
  - Система оперативно-технічного управління та адміністрування (далі – СОТУ).
- Технічне завдання на КСЗІ Підсистеми прикладних сервісів ІТС (далі – ППС), яка реалізується прикладним та функціональним програмним забезпеченням, розгорнутим на базі обчислювальних ресурсів ЦОД.
- Технічні вимоги щодо Організаційно-технічних рішень (далі – ОТР) впровадження заходів та технологій захисту для типових інтерфейсів доступу до ресурсів ЦОД та ППС, які реалізують доступ користувачів до інформаційних ресурсів ІТС.
-

4.2.2 Визначити цілі безпеки щодо інформації та обчислювальних ресурсів відповідно до кожного рівня архітектури ІТС, з урахуванням запропонованих в моделі загроз заходів зменшення рівня ризиків реалізації загроз, характеристик середовищ експлуатації та технологій обробки інформації.

4.2.3 Визначити типи інформаційних об’єктів, які містять інформаційні та обчислювальні ресурси ІТС, описують/представляють суб’єктів доступу та підлягають захисту в рамках обробки інформації.

4.2.4 Надати опис політики безпеки. Всі суб'єкти, об'єкти, операції, атрибути безпеки, і інші терміни, які використовуються в ІТС (в її складі), повинні бути визначені в рамках наданої політики безпеки. Виклад положень політики безпеки в ТЗ повинен ідентифікувати усі вимоги та заходи захисту, відповідно до технологічних процесів обробки інформації, архітектури системи та визначених сценаріїв і ризиків реалізації загроз.

4.2.5 Визначити рівень гарантій та вимоги, які можуть бути забезпечені Розробником в процесі розробки і впровадження КСЗІ. Рівень гарантій, не повинен бути нижчим за Г2, специфікація вимог якого визначена НД ТЗІ 2.5-04-99.

4.2.6 Підготувати документи за результатами аналізу, як визначено в п.п.2 Розділу 5 цього Завдання.

4.2.7 Підготувати та подати відповідний звіт з розробки політики безпеки інформації в ІТС і вносити до нього зміни, якщо необхідно.

4.3 На етапі здійснення проектування КСЗІ ІТС загальної хмари СУДФ та підготовки КСЗІ до введення в експлуатацію, консультант повинен:

4.3.1 Виконати розробку загальних проектних рішень, необхідних для реалізації вимог ТЗ відповідно до сценаріїв реалізації загроз, рішень щодо структури КСЗІ ІТС, алгоритмів функціонування та умов використання засобів захисту.

4.3.2 Розробити проект архітектури комплексу засобів захисту інформації в ІТС, з урахуванням затверджених рівнів та інтегрованих компонентів системи.

4.3.3 Сформувати завдання на робоче проектування компонентів та підсистем комплексів засобів захисту та комплексу криптографічного захисту інформації в ІТС.

4.3.4 Розробити проект організаційної структури управління інформаційною безпекою ІТС відповідно до затвердженої архітектури КСЗІ ІТС та з урахуванням міжнародних та регіональних стандартів, який включає:

- проектні рішення щодо основних процесів забезпечення управління інформаційною безпекою в ІТС, відносно затвердженої архітектури КСЗІ та правил її експлуатації;
- штатну структуру та режими роботи персоналу обслуговування КЗЗ та СУІБ;
- вимоги щодо кваліфікаційних рівнів персоналу, програми навчання.

4.3.5 Підготувати документи за результатами проектування, як визначено в п.п.3 Розділу 5 цього Завдання.

4.3.6 Підготувати документи за результатами розробки політик безпеки та проведення попереднього тестування КСЗІ ІТС, як визначено в п.п.3 Розділу 5 цього Завдання;

4.3.7 Підготувати та подати відповідний звіт зі створення проектної документації КСЗІ і вносити до нього зміни, якщо необхідно.

Передбачається, що консультант буде виконувати більшу частину своєї роботи на центральному майданчику в Міністерстві фінансів України, де розміщується інфраструктура майбутньої загальної хмари СУДФ.

Додатково, консультант повинен відвідати ДМСУ, ДПСУ, ДКСУ для збору інформації безпосередньої в місцях обробки та накопичення первинної інформації.

Консультант застосує свою методологію для виконання роботи.

Очікується, що консультант буде використовувати різні інструменти та технологічні компоненти для проведення тестів (в тому числі і свої власні).

5. РЕЗУЛЬТАТИ ДІЯЛЬНОСТІ КОНСУЛЬТАНТА ТА ГРАФІК НАДАННЯ МАТЕРІАЛІВ

Консультант має підготувати та надати МФУ наступні результати[1]:

No.	Результат	Строк надання *(з дати укладання договору з консультантом)*
1	Звіт з проведення передпроектного обстеження середовищ функціонування ІТС МФУ, ІТС МФУ, Державної митної служби, Державної податкової служби, Державної казначейської служби (на предмет включення ресурсів зазначених органів до загальної хмари СУДФ), який включає в себе: • звіт за результатом аналізу ризиків; • ескізний проект КСЗІ в ІТС (в якому враховані описи моделі загроз, моделі порушника, акту	Впродовж 80 робочих днів

1 Наповнення результатів та строк виконання завдання може бути уточнено під час контрактних переговорів з консультантом, відповідно до запропонованої методології надання послуг.

	обстеження, розробку яких здійснює інший індивідуальний консультант); • план захисту інформації.	
2	Звіт з розробки політики безпеки ІТС загальної хмари СУДФ та технічного завдання на КСЗІ ІТС загальної хмари СУДФ, який включає в себе: • Пояснювальна записка щодо розробки Технічного завдання на КСЗІ ІТС. • Технічне завдання на КСЗІ Програмно-технічного комплексу центрального сегменту інформаційно-телекомунікаційної системи загальної хмари СУДФ. • Технічні вимоги щодо Організаційно-технічних рішень (далі – ОТР) впровадження заходів та технологій захисту для типових інтерфейсів доступу користувачів до інформаційних ресурсів ІТС.	Впродовж 90 робочих днів
3	Звіт з підготовки технічного проекту КСЗІ ІТС загальної хмари СУДФ та підготовка КСЗІ до введення в експлуатацію, який включає в себе: а) Проектну документацію технороботочого проекту КСЗІ загальної хмари СУДФ: • Відомість технічного проекту • Пояснювальна записка до технічного проекту. • Опис організаційної структури адміністрування та експлуатації ІТС б) Документацію за результатами проведеного тестування КСЗІ • Протоколи встановлення основних параметрів політики безпеки; в) Допоміжна документація КСЗІ • Форми реєстраційних журналів	Впродовж 120 робочих днів

6. КООРДИНАЦІЯ, ПІДЗВІТНІСТЬ ТА ЗВІТУВАННЯ

Консультант працює під керівництвом Координатора Проекту від МФУ та є йому підзвітним. Всі документи, які готуються Консультантом, в подальшому можуть бути включенні до пакету документів, який буде затверджений на рівні нормативно-правового акту МФУ.

Консультант має координувати свою роботу з координатором МФУ з ІТ-питань в частині розробки узгоджених рішень для відпрацювання та побудови концептуальної моделі, закладеної в проекті Стратегії розвитку інформаційних технологій Міністерства фінансів

України на 2020-2022 роки та надання вихідної інформації щодо виконання завдань представникам МФУ.

Консультант в рамках оперативної взаємодії погоджує свою роботу з Провідним консультантом з інформаційної кібербезпеки (Індивідуальний консультант) та співпрацює з профільним підрозділом МФУ, відповідальним за впровадження функцій з захисту інформації.

Провідний консультант з інформаційної кібербезпеки (Індивідуальний консультант) уповноважений щодо Консультанта:

- контролює дотримання строків та якості підготовки всіх звітних документів Консультанта;
- надає коментарі (у разі їх наявності) до документації, що додається до звітності Консультанта, та перевіряє врахування таких коментарів.

Консультант готує та надає МФУ наступні звіти:

- Звіт з проведення передпроектного обстеження середовищ функціонування ІТС МФУ, ІТС МФУ, Державної митної служби, Державної податкової служби, Державної казначейської служби (на предмет включення ресурсів зазначених органів до загальної хмари СУДФ);

- Звіт з розробки політики безпеки ІТС загальної хмари СУДФ та технічного завдання на КСЗІ ІТС загальної хмари СУДФ;

- Звіт з підготовки технічного проекту КСЗІ ІТС загальної хмари СУДФ та підготовка КСЗІ до введення в експлуатацію;

1. Консультант надає МФУ Звіт з проведення передпроектного обстеження середовищ функціонування ІТС МФУ, Державної митної служби, Державної податкової служби, Державної казначейської служби (на предмет включення ресурсів зазначених органів до загальної хмари СУДФ) не пізніше терміну встановленого для результату № 1 в розділі 5 цього Технічного завдання. Звіт готується за результатами виконання завдань та повинен включати наступну інформацію:
    - інформація про перший етап виконання робіт згідно з переліком документів визначених в п.1 розділу 5 цього Технічного завдання;
    - проблемні питання, які Консультант вбачає як перешкоди вчасного та якісного надання послуг та пропоновані заходи щодо їх усунення;
    - загальна інформація про готовність всього комплекту документів зазначених в п.1 розділу 5 цього Технічного завдання;
    - інша інформація на розсуд Консультанта.

До Звіту додається підготовлена Консультантом документація, визначена для результату № 1 в п. 5 цього Технічного завдання.

2. Консультант надає МФУ Звіт з розробки політики безпеки ІТС загальної хмари СУДФ та технічного завдання КСЗІ ІТС загальної хмари СУДФ не пізніше терміну встановленого для результату № 2 в розділі 5 цього Технічного завдання. Звіт готується за результатами виконання завдань та повинен включати наступну інформацію:
    - загальна інформація про другий етап виконання робіт

- проектну документацію техноробочого проекту КСЗІ відповідно до переліку документів визначених в п.п. 2 розділу 5 цього Технічного завдання;
- проблемні питання, які Консультант вбачає як перешкоди вчасного та якісного надання послуг та пропоновані заходи щодо їх усунення;
- загальну інформація про готовність всього комплекту документів зазначених в п 2 розділу 5 цього Технічного завдання;
- інша інформація на розсуд Консультанта.

До Звіту додається підготовлена Консультантом документація, визначена для результату № 2 в розділі 5 цього Технічного завдання.

3. Консультант надає МФУ Звіт за результатами підготовки технічного проекту КСЗІ ІТС загальної хмари СУДФ та підготовка КСЗІ до введення в експлуатацію не пізніше терміну встановленого для результату № 3 розділу 5 цього Технічного завдання. Звіт готується за результатами виконання завдань та повинен включати наступну інформацію:

    - інформація про готовність комплекту документів зазначених в розділі 5 цього Технічного завдання результат № 3.
    - проектну документацію техноробочого проекту КСЗІ відповідно до переліку документів визначених в результаті. №3 розділу 5 цього Технічного завдання;
    - проблемні питання, які Консультант вбачає як перешкоди вчасного та якісного надання послуг та пропоновані заходи щодо їх усунення;
    - інша інформація на розсуд Консультанта.

До Звіту додається підготовлена Консультантом документація, визначена для результату № 3 в розділі 5 цього Технічного завдання.

1. Вимоги до звітів

Всі звіти готуються українською мовою. Будь-які додаткові документи до них подаються мовою оригіналу.

Всю звітність Консультант подає наступним чином:

- Консультант подає звітні документи в електронному вигляді для розгляду та надання коментарів МФУ на адресу _____ (звіти мають бути підписані, відскановані в форматі pdf файлу та відправлений з електронної адреси Консультанта зазначеної в п. 5 нижче). Супроводжуюча документація повинна бути у форматі MS Word, MS Excel або MS PowerPoint, чи іншому форматі прийнятному для МФУ, залежно від типу документу.
- у випадку погодження МФУ наданих Консультантом документів в електронній формі, Консультант має подати відповідні документи в паперовій формі в 2-х екземплярах підписаних Консультантом. Паперові версії направляються поштою за наступною адресою: *04071, м. Київ, вул. Межигірська, буд. 11, до уваги Ігоря Шевлякова*.

У випадку, якщо звіт Консультанта посилається на раніше підготовлену інформацію або документи, такі документи повинні бути додані до звіту. Структура та форма звітних

документів, зазначених у Розділі 5 цього Технічного завдання, визначається вимогами нормативних документів системи технічного захисту інформації.

5. Розгляд та затвердження Звітів

МФУ розглядає подану звітність та затверджує або надає зауваження протягом 10 робочих днів з дати отримання відповідного звіту за результатами роботи. Зауваження до звітів викладаються письмово та направляються Консультанту засобами електронного зв'язку на електронну поштову скриньку _____ з повідомленням про доставку відповідного повідомлення. Консультант впродовж доби після отримання зауважень від МФУ, повідомляє про отримання відповідних зауважень та строк їх врахування. Поправки (зауваження) МФУ до відповідних звітів повинні бути враховані Консультантом та відповідний оновлений звіт має бути наданий МФУ не пізніше 5 робочих днів з дати їх надходження на вказану електронну скриньку Консультанта.

У випадку відсутності надання МФУ зауважень впродовж вказаного терміну, такі звіти вважаються прийнятими.

7. РЕСУРСИ ЗАМОВНИКА

МФУ забезпечує Консультанта:
i) всіма відповідними документами і даними, які не мають грифу обмеження доступу або не віднесені до конфіденційної інформації;
ii) доступом до приміщення МФУ;
iii) у випадку необхідності контакту з організаціями, що входять до структури державного управління фінансами, МФУ забезпечує здійснення такого контакту для Консультанта.

8. ОБМЕЖЕННЯ

В Договорі з Консультантом застосовується стандартне положення щодо Конфлікту інтересів. Крім цього, всі матеріали, створені під час надання послуг за договором, залишаються власністю МФУ і можуть використовуватись лише з офіційного письмового дозволу МФУ.
До початку надання послуг Консультант разом з МФУ готує заяву про конфіденційність, де бере на себе зобов'язання не розголошувати конфіденційну інформацію, яку може отримати під час виконання завдання. Положення заяви про конфіденційність повинні відповідати вимогам чинного законодавства України.

9. МІСЦЕ, ТРИВАЛІСТЬ, УМОВИ ПРАЦІ ТА ВИНАГОРОДА

Очікується що Консультант буде працювати впродовж періоду з листопада 2020 року до березня 2021 року. Очікувані трудовитрати загалом не повинні перевищувати 120 робочих днів. Завдання передбачає роботу Консультанта, як в місці його проживання.

Обсяг винагороди буде визначений в результаті переговорів з обраною особою та проводитиметься на основі наданих результатів робіт, що оформлюються відповідними звітами.

Консультант відповідальний за всі видатки, які він несе у зв'язку з наданням послуг, зокрема наступними, але не обмежуючись ними: проживання в місці надання послуг, переклади, витрати на зв'язок.

Відбір Консультанта буде проводитись відповідно до вимог «Керівництва МБРР із закупівель для Позичальників інвестиційних проектів» (липень 2016 року, переглянуте в листопаді 2017 та серпні 2018 року).

10. ВИМОГИ ДО ОСВІТИ ТА КВАЛІФІКАЦІЇ

. Консультант повинен відповідати наступним кваліфікаційним вимогам:

Обов'язкова кваліфікація Консультанта:

- вища технічна освіта;
- досвід роботи у сфері захисту інформації не менше п'яти років, з яких не менше 2 років впродовж останніх 5 років;
- наявність свідоцтва про підвищення кваліфікації у сфері технічного та криптографічного захисту інформації не менше одного за кожним напрямком;
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ впродовж останніх 5 років не менше 3 реалізованих договорів/проектів;
- Знання та наявність навичок практичного застосування основних сервісів Microsoft, мережевих сервісів (DNS, DHCP, VLAN, VPN);
- досвід роботи із засобами мережевої безпеки;
- вільне володіння письмовою та усною українською мовою.

Додаткові кваліфікаційні вимоги, які відповідають специфіці завдання та будуть прийматись як перевага

Відповідність Консультанта наступним кваліфікаційним вимогам буде розглядатись Замовником, як перевага:

- наявність сертифікату СПБІС (CISSP) (Сертифікований професіонал з безпеки інформаційних систем) або CAIC (CISA) (Сертифікований аудитор інформаційних систем) або CMIC (CISM) (Сертифікований менеджер інформаційних систем);
- наявність сертифікату про успішне проходження тренінгу/навчального курсу з питань впровадження та використання вимог ISO / IEC 27001:2013 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» за напрямками Впроваджувач та/чи Аудитор;
- досвід впровадження комплексних системи захисту інформації різних типів (АС1, АС2, АС3);
- наявність наукового ступеню за технічними науками;
- наявність авторських патентів на розробки в галузі ТЗІ та КЗІ;

- наявність ліцензії Державної служби спеціального зв’язку та захисту інформації України на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації;
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ для організацій державного сектору економіки;
- володіння англійською мовою на рівні опрацювання технічної документації в сфері ІТ без словника.

Кандидати мають надати підтвердження у формі посилання на публічно підтверджену та доступну інформацію чи надання копій відповідних документів що засвідчують відповідний статус чи стан.