Конкурс Грантових Заявок

Назва Конкурсу:

‘Гранти на поліпшення кібербезпеки для державних інституцій України’

Номер: DE-02-2023

Оновлено: 12 грудня2023 р.

Початок Конкурсу	3 листопада 2023
Кінцевий термін подачі заявок	15 грудня 2023
Сесія запитань та відповідей	14 листопада 2023
Дата оголошення результатів Конкурсу	На регулярній основі
Сума гранту	До 42 000 доларів США
Тривалість проєкту за грантом	До 7 місяців
Допустимі заявники	Центральні органи влади України / Державні підприємства критичної інфраструктури України
Допустимі країни	Україна
Допустима тематика проєктів	Покращення в галузі кібербезпеки та розвиток спроможності заявників

ЗМІСТ

ЗАГАЛЬНА ІНФОРМАЦІЯ

CRDF Global приймає грантові заявки від Центральних органів влади України / Державних підприємств критичної інфраструктури України на грантовий Конкурс - «Гранти на поліпшення кібербезпеки для державних інституцій України» (надалі «Конкурс»). Цей конкурс організовує та адмініструє CRDF Global за підтримки Державного департаменту США.

Гранти на поліпшення кібербезпеки для державних інституцій України (CySIG) призначені для забезпечення рішень, а також для задоволення поточних і нових потреб у кібербезпеці з метою підвищення рівня кібербезпеки та стійкості систем кібербезпеки в цих установах, шляхом призначення експерта(-ів) з кібербезпеки для забезпечення високого рівня захисту важливих інформаційних ресурсів та мереж цих інституцій, сприяючи зміцненню кіберзахисту України.

CRDF Global (Фонд цивільних досліджень та розвитку США) є незалежною некомерційною організацією, яка впроваджує безпеку та стабільність в межах міжнародні місії розвитку та глобальної допомоги. CRDF Global є надійним партнером України вже понад 25 років, надаючи технічну допомогу, логістичну підтримку, навчальні програми та програми стратегічного розвитку у галузях кібербезпеки, нерозповсюдження та захисту від хімічних, біологічних, радіологічних та ядерних речовин, глобальної охорони здоров'я, стратегічного управління торгівлею, вищої освіти, міжнародних професійних обмінів тощо. Штаб-квартира організації знаходиться в Арлінгтоні, штат Вірджинія, США. Регіональні центри розташовані в Аммані, Йорданії, Манілі та Києві.

Щоб дізнатися більше, будь ласка, перейдіть за посиланням: http://www.crdfglobal.org.

Цілі та завдання

Реалізації грантових угод в рамках цього Конкурсу Грантових Заявок має на меті наступні завдання:

(1) Проведення аналізу поточних систем безпеки Центральних органів влади України / Державних підприємств критичної інфраструктури України.
(2) Визначення потенційних загроз та подальша розробка інноваційних рішень із кібербезпеки для захисту Центральних органів влади України / Державних підприємств критичної інфраструктури України від таких загроз.
(3) Підвищення кібербезпеки та стійкості систем кібербезпеки Центральних органів влади України / Державних підприємств критичної інфраструктури України.

ПРЕДМЕТ ТА ОБСЯГ КОНКУРСУ

Опис проблематики

У контексті повномасштабної війни з боку Росії, Центральні органи влади України / Державні підприємства критичної інфраструктури України постають перед серйозними викликами, зокрема, кібератаками, дезінформаційними кампаніями, які загрожують їхній безпеці та стабільності роботи. Ці виклики створюють нагальну потребу в Україні посилити заходи з кібербезпеки та стійкості, протистояти дезінформаційним кампаніям та захищати критичну інфраструктуру, забезпечуючи неперервне функціонування та безпеку державних установ і життєво важливих

секторів під час воєнних дій. Для досягнення цих цілей потрібен комплексний та координований підхід до забезпечення національної безпеки українських державних установ та державних підприємств критичної інфраструктури. Цей підхід передбачає захист конфіденційної інформації, проведення ретельного аналізу потенційних загроз та впровадження надійних заходів безпеки для захисту від кібератак та інших загроз.

У зв'язку з вищезазначеним, цей грантовий конкурс призначений для вирішення конкретних проблем, з якими стикаються Центральні органи влади України / Державні підприємства критичної інфраструктури України. Він націлений на надання підтримки в галузі кібербезпеки для грантоотримувачів з метою ідентифікації вразливих зон та захисту їхніх систем від можливих кіберінцидентів, шляхом підвищення загального рівня кібербезпеки та стійкості інформації в цих установах. Це можливо досягти, залучивши кваліфікованого спеціаліста в галузі кібербезпеки з метою забезпечення високого рівня захисту важливої інформації, ресурсів та мереж цих установ, сприяючи підвищенню рівня кіберзахисту України.

Допустима тематика проєктів

Для цілей цього Конкурсу, заявники мають запропонувати грантові проєкти в наступних сферах:

(1) Кібербезпека.
(2) Кібергігієна.
(3) Захист даних.
(4) Аналіз загроз.
(5) Посилення потенціалу грантоотримувачів у сферах, зазначених вище.

З огляду на вищезазначене, проєктні активності можуть включати, але не обмежуватися наступним:

(1) Проведення аналізу вразливих зон грантоотримувача, які можуть стати потенційними цілями для кібератак та інцидентів у сфері кібербезпеки.
(2) Розробка стратегічних / операційних рішень для запобігання та реагування на потенційні кібератаки та кіберінциденти.
(3) Оптимізація та вдосконалення процесів кібербезпеки для грантоотримувача у зазначених вище сферах.

Запропоновані проєктні активності / стратегія реалізації мають враховувати / включати наступне:

- Зазначити кількість експертів з кібербезпеки.
- Зазначити загальний обсяг робіт для кожного експерта із кібербезпеки та сферу вразливості, яку має державна установа.
- Подати резюме (CV) Відповідального виконавця (координатора проєкту).
- Вказати потенційні вразливості у сфері кібербезпеки, які грантоотримувач має намір опрацювати терміном до семи (7) місяців.

ВИМОГИ ДО ЗАЯВНИКІВ ТА ГРАНТОВИХ ПРОЄКТІВ

Усі заявники та грантові проєкти мають відповідати **кожній** вимозі нижче:

(1) Заявки приймаються від Центральних органів влади України / Державних підприємств критичної інфраструктури України, які піддаються потенційним кіберзагрозам або іншим кіберінцидентам.
(2) Заявники надали чітке формулювання проблеми та визначили ключові вимоги до експерта (-ів) з кібербезпеки, якого(-их) пізніше буде залучено до проєкту.
(3) Заявники подали повний пакет необхідних документів.

ВАЖЛИВО:	CRDF Global залишає за собою право відмовити у розгляді та оцінці заявок, які не відповідають вимогам до заявників та грантових проєктів, що наведені вище.

РОЗГЛЯД ГРАНТОВИХ ЗАЯВОК

Процедура розгляду заявок

Усі грантові заявки та інформація, що міститься в них, залишатимуться конфіденційними до моменту підписання грантової угоди. Після отримання грантових заявок представники CRDF Global перевірять відповідність таких заявок вимогам до заявників та грантових проєктів, а також наявність повної необхідної інформації у таких заявках. Усі заявки, що відповідатимуть вимогам до заявників та грантових проєктів, будуть оцінені за відповідними критеріями. CRDF Global буде керуватися критеріями оцінки, що наведені нижче, для оцінювання кожної заявки з точки зору їх якості та відповідно прийматиме рішення про надання гранту за результатами такого оцінювання. CRDF Global обере фіналістів конкурсу з урахуванням результатів оцінювання і прийнятих рішень.

CRDF Global розглядатиме заявки, що відповідають вимогам до заявників та грантових проєктів, відповідно до місцевого законодавства та внутрішніх політик організації. За результатами такого розгляду, CRDF Global визначить заявників, з якими буде укладено грантові угоди, та повідомить про це електронним листом відповідальним виконавцям та / або контактним особам.

ВАЖЛИВО:	Будь-яке рішення про надання гранту (укладення грантової угоди) залежить від фактичної наявності фінансування від донорів / спонсорів програми. Усі рішення CRDF Global про надання / ненадання гранту (укладення грантової угоди) є остаточними.

Критерії оцінки заявок

Наступні критерії оцінки будуть застосовуватися під час розгляду і оцінки кожної грантової заявки:

1. Актуальність заявки та її потенційний вплив	**30 балів**

- Технічні переваги. Чи описує проєкт необхідні сфери вдосконалення у галузі кібербезпеки та наскільки елементи технічного завдання (обсягу роботи) відповідають загальній меті проєкту. Оцінка доцільності завершення проєкту терміном виконання до 7 місяців.
- Актуальність і вплив на кібербезпеку: ймовірність того, що проєкт допоможе проаналізувати та покращити системи кібербезпеки та інформаційну стійкість грантоотримувачів.
- Перевага надається Центральним органам влади / Державним підприємствам критичної інфраструктури України, чия заявка містить чіткий і обґрунтований графік, мотивацію, та визначені напрями для можливих покращень системи кібербезбеки.

2. Потреба в експерті з кібербезпеки та обсяг робіт (опис завдання для виконання)	**30 балів**

- Обґрунтувати необхідність залучення експерта(-ів) з кібербезпеки для Центральних органів влади України / Державних підприємств критичної інфраструктури України.
- Зазначити поточні проблеми у сфері кібербезпеки, які потребують аналізу, вирішення та покращення терміном виконання до 7 місяців.
- Технічне завдання (Обсяг Робіт) для експерта з кібербезпеки є детальним та містить перелік задач для вирішення та подальшого уникнення проблем у сфері кібербезпеки грантоотримувача.

3. Ясність викладення, реалістичність виконання та достатній рівень деталізації проєктних активностей	**15 балів**

- Заявка має чітко визначену мету, а також обґрунтування потреби в експерті(-ах) з кібербезпеки.
- План проєкту. Технічне обґрунтування доцільності запропонованого обсягу робіт, виконання запропонованого робочого плану та його відповідність потребам, які підлягають аналізу та удосконаленню експертом(-ами) з кібербезпеки.

4. Економічна доцільність	**10 балів**

- Деталізація витрат в наданому бюджеті проєкту та їх обґрунтування в описі бюджету.

5. Сталість запропонованого підходу / проєктних активностей	**15 балів**

- Зазначити як запропонована діяльність може сприяти посиленню систем кібербезпеки Грантоотримувачів?
- Зазначити очікуваний результат кожного етапу плану робіт.

ЗАГАЛЬНА ОЦІНКА	**100 балів**

ПІДГОТОВКА ТА ПОДАЧА ГРАНТОВОЇ ЗАЯВКИ

Подача повної грантової заявки

Усі грантові заявки мають бути подані не пізніше 15 грудня 2023 року.

Усі грантові заявки мають бути подані в електронному форматі та з використанням шаблону грантової заявки CRDF Global на наступну електронну адресу: vsheliekhova@crdfglobal.org

У темі листа потрібно обов'язково зазначити номер конкурсу та назву заявника в форматі, який наведено у прикладі нижче:

"DE-02-2023_ГО «Промінь»".

Після електронної подачі документів, заявники отримають лист-відповідь, в якому буде підтвердження отримання заявки з боку CRDF Global.

Грантова заявка, що надається CRDF Global, має бути підготовлена англійською або українською мовами з використанням шаблону грантової заявки. Допустимі формати файлів: Майкрософт Ексель (.exsm) та pdf, коли прямо зазначається інструкціями в шаблоні грантової заявки.

Шаблон грантової заявки включає наступні розділи (вкладки):

Обов'язкові:

(1) Інформація про організацію,
(2) Опис проєктної заявки,
(3) Обсяг роботи (опис завдань для виконання),
(4) Робочий план проєкту,
(5) Бюджет,
(6) Опис бюджету,
(7) Графік платежів та звітності за проєктом.

Додаткові документи, наведені нижче:

(I) Резюме Відповідального виконавця (який виконує функції координатора проєкту та відповідає за його реалізацію).

У разі виникнення питань щодо процесу подання грантових заявок, будь ласка, зверніться до CRDF Global за наступною електронною адресою: vsheliekhova@crdfglobal.org.

Сесія запитань та відповідей

CRDF Global організує онлайн сесію запитань та відповідей (Q&A) з метою надання інформації щодо Конкурсу та положень цього документу, включаючи інформацію щодо вимог до заявників та грантових проєктів, подачі та оцінки грантових заявок та інших пов'язаних з Конкурсом питань.

ВАЖЛИВО:

CRDF Global не має наміру розглядати, оцінювати або радити стосовно конкретних грантових заявок, або у будь-який інший спосіб допомагати заявникам з розробкою конкретних проєктних активностей або загальної ідеї гранту. Метою такої сесії є, насамперед, надання роз'яснень та відповідей на питання стосовно цього Конкурсу, що, в свою чергу, має підвищити загальну якість заявок, що будуть подані.

Сесія запитань та відповідей буде записана на відео та розміщена на сайті CRDF Global.

Нижче наведено інформацію про дату і час проведення сесії питань і відповідей.

Дата: 14 листопада, 2023 року
Час: 12:00 за Київським часом
Платформа / засіб комунікації: Zoom.

Учасники сесії запитань та відповідей мають завчасно зареєструватися для участі. Будь ласка, скористайтеся посиланням, що наведено нижче, для реєстрації Вашої участі. Заявники заздалегідь отримають листа із запрошенням в Zoom.

Посилання для реєстрації у сесії питань і відповідей: https://forms.office.com/r/5K8AaBmyr5.

ДОПУСТИМІ ВИТРАТИ ТА БЮДЖЕТ ПРОЄКТУ

Максимальна сума грантової угоди. Максимальна сума гранту складає до **42 000 доларів США**, яка надається протягом строку імплементації гранту.

У разі отримання гранту, бюджет проєкту може підлягати перегляду співробітниками CRDF Global.

CRDF Global розподілятиме грантові кошти за допомогою механізму грантів у натуральній формі (in-kind grant).

Відповідно до умов і політик CRDF Global для цього Конкурсу дозволені такі витрати:

Послуги: що включає надання інформаційних та консультаційних послуг грантоотримувачам місцевими постачальниками послуг, які є експертами з питань кібербезпеки. Такі експерти повинні відповідати вимогам, які зазначені заявниками.

Перелік заборонених предметів

Предмети (товари), що наведені в переліку нижче не можуть бути включені до бюджету заявників за цим Конкурсом:

1. Зброя та вибухові речовини;
2. Алкогольні напої;
3. Незаконні та / або обмежені речовини, такі як наркотики;
4. Обладнання для спостереження;
5. Предмети розкоші та ювелірні вироби;
6. Обладнання для азартних ігор;

7. Спортивний інвентар.

ПОЛІТИКИ ТА УМОВИ CRDF GLOBAL

Загальні умови та правила

Загальні умови та правила CRDF Global включені в цей документ шляхом посилання на них та публікації разом з цим Конкурсом на сайті CRDF Global. Будь ласка, обов'язкового ознайомтеся з цими умовами і правилами (викладено англійською мовою).

Заявники мають ознайомитися із зазначеними умовами і правилами до подачі їх заявок в рамках цього Конкурсу.

Спеціальні умови і правила

1. Усі завдання та процеси, які можуть бути виконані експертом (-ами) з кібербезпеки в рамках майбутніх Грантових угод, наданих CRDF Global, повинні бути обмежені та не включати жодних дій, спрямованих на зміну коду, технічних можливостей або характеристик систем кіберзахисту грантоотримувачів. Це включає в себе будь-які дії, спрямовані на втручання в систему кібербезпеки за допомогою кодування, створення скриптів та інших засобів програмного забезпечення, які можуть вплинути на роботу систем кіберзахисту грантоотримувачів. Невиконання цих умов з боку грантоотримувачів та / або експерта (-ів) з кібербезпеки призведе до одностороннього розірвання грантової угоди CRDF Global.
2. Кожний заявник – Центральний орган влади України / Державне підприємство критичної інфраструктури України – може подати **лише одну грантову заявку** за цим Конкурсом.
3. Після оголошення результатів Конкурсу кожний обраний заявник буде проінформаваний про це електронним листом від CRDF Global. Заявники матимуть **не більше 10 календарних днів** для підписання наданої грантової угоди. Якщо заявник не підпише грантову угоду протягом зазначеного терміну, CRDF Global залишає за собою право відмовити в наданні гранту в односторонньому порядку.
4. Кожний обраний грантоотримувач має надати Фінальний програмний звіт після завершення грантової угоди відповідно до строків, зазначених у цій угоді.