Конкурс Грантових Заявок

Назва Конкурсу:

‘Гранти на поліпшення кібербезпеки державних установ та об’єктів критичної інфраструктури України’

Номер: DE-03-2023

Початок Конкурсу	27 грудня 2023
Кінцевий термін подачі заявок	4 лютого 2024
Сесія запитань та відповідей	17 січня 2024
Дата оголошення результатів Конкурсу	На регулярній основі
Тривалість проєкту за грантом	До 30 серпня 2024
Допустимі заявники	Державні установи / Об’єкти критичної інфраструктури України
Допустимі країни	Україна
Допустима тематика проєктів	Покращення рівня кібербезпеки та інформаційної безпеки в Державних установах та об’єктах критичної інфраструктури України

ЗМІСТ

Зміст 2
загальна інформація 3
Цілі та завдання 3
предмет та обсяг конкурсу 4
Допустима тематика проєктів 4
вимоги до заявників та грантових проєктів 6
розгляд грантових заявок 6
Процедура розгляду заявок 6
підготовка та подача грантової заявки 7
Допустимі витрати та бюджет проєкту 9
Перелік заборонених предметів 9
Політики та умови CRDF Global 9
Загальні умови та правила 9

ЗАГАЛЬНА ІНФОРМАЦІЯ

CRDF Global приймає грантові заявки від Державних установ та об'єктів критичної інфраструктури України (далі – потенційні заявники) на грантовий Конкурс - «Гранти на поліпшення кібербезпеки державних установ та об'єктів критичної інфраструктури України» (надалі «Конкурс»). Цей конкурс організовує та адмініструє CRDF Global за підтримки Державного департаменту США.

Гранти на поліпшення кіберзахисту в державних установах та об'єктах критичної інфраструктури України (CySIG) призначені для вирішення актуальних та нових викликів у сфері кібербезпеки. Їх мета полягає в удосконаленні заходів із кіберзахисту, стійкості кібербезпекових систем у цих установах, забезпечення надійності, конфіденційності та доступності інформації, а також зменшення ризиків кібератак та інших кіберзагроз. Ці гранти націлені на зміцнення кібербезпеки у державних інституціях через впровадження новітніх технологій, надання послуг із підтримки потенційним заявникам виявляти та запобігати потенційним кіберзагрозам, забезпечуючи впевненість у стійкості їх інформаційних систем та мереж перед можливими кібератаками, а також сприяти покращенню інфраструктури та методів захисту, створення або покращення існуючих систем захисту інформації, а також надання фахівцям, що працюють у сфері кібербезпеки цих установ, можливості отримати навички та знання для ведення комунікації із представниками міжнародних спільнот та ключовими донорами, обміну кращими практиками та вивчення міжнародних стандартів, що дозволить ефективніше співпрацювати та впроваджувати передові підходи в роботі з цими партнерами. Такий компонент розширить навички використання доступних міжнародних ресурсів, що сприятиме підвищенню рівня кібербезпеки в державних установах та об'єктах критичної інфраструктури 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) Підвищити рівень кібербезпеки та стійкості систем кібербезпеки Державних установ та об'єктів критичної інфраструктури України.
(2) Сприяти розбудові та / або покращенню існуючої інформаційної та кібер інфраструктури зазначених установ шляхом забезпечення необхідними ресурсами (послугами, обладнанням, апаратним та програмним забезпеченням).

(3) Вдосконалити навички та рівень знань фахівців, які дотичні до сфери кібербезпеки зазначених установ, з метою уможливлення вивчення міжнародних стандартів у сфері кібербезпеки та кібероборони та використання доступних міжнародних професійно-інформаційних ресурсів.

ПРЕДМЕТ ТА ОБСЯГ КОНКУРСУ

Опис проблематики

У зв'язку із повномасштабною війною з боку росії, Державні установи та об’єкти критичної інфраструктури України постають перед серйозними загрозами, такими як кібератаки та дезінформаційні кампанії, які ставлять під загрозу їхню безпеку та стабільність функціонування. Ці виклики вимагають негайних заходів з посилення кібербезпеки та стійкості, здатності протистояти дезінформації та захисту критичної інфраструктури для забезпечення безперебійної роботи та безпеки державних установ України та життєво важливих секторів під час воєнних дій.

У контексті цього Конкурсу, слід зазначити, що існує значна нестача технічного обладнання та програмного забезпечення в українських державних установах, яка суттєво ускладнює процес захисту цих установ від кіберзагроз та інших кібератак. Відсутність адекватних інструментів та програм може порушити стійкість та ефективність захисту даних та інфраструктури, що в свою чергу підвищить рівень вразливості перед сучасними кіберзагрозами.

Варто зазначити, що така критична потреба існує не лише у покращенні систем кібербезпеки, але й у розвитку комунікаційних навичок у фахівців, які працюють у державних установах та критичних підприємствах. Нестача цих ключових навичок обмежує їхню здатність ефективно спілкуватися з міжнародними представниками та адаптуватися до сучасних вимог кіберзахисту, що може ускладнити успішний захист критично важливих систем у сучасних умовах загроз. Для вирішення вищезазначених проблематик, необхідний комплексний та узгоджений підхід до забезпечення національної безпеки українських державних установ та державних підприємств критичної інфраструктури. Такий підхід допоможе не лише розвивати технічні аспекти кіберзахисту, а й забезпечить ефективну комунікацію та співпрацю з міжнародними експертами, що є критичним для успішної захисту критичної інфраструктури в умовах сучасних кіберзагроз.

Допустима тематика проєктів

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

(1) Кібербезпека та покращення матеріально-технічної бази для її забезпечення.
(2) Захист даних та аналіз загроз.
(3) Координація та поліпшення доступу до міжнародно-аналітичних ресурсів із обміну інформації.
(4) Законотворча робота та стандартизація у сфері кібербезпеки.

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

(1) Забезпечення необхідними ресурсами (обладнання, послуги, апаратне та програмне забезпечення.

(2) Оптимізація та вдосконалення процесів / систем кібербезпеки для грантоотримувача у зазначених вище сферах.
(3) Впровадження рекомендованих оновлень та/або захисту безпеки в державних установах та об'єктах критичної інфраструктури України.
(4) Підвищення кваліфікаційних навичок із напрямку кібербезпеки для працівників державних установ та об'єктів критичної інфраструктури України

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

- Надати детальний опис проблематики та можливі рішення, які допоможуть знизити ризик кіберінцидентів та удосконалити системи кібербезпеки.
- Визначити які критичні ресурси та/або конфіденційна інформація будуть захищені в результаті реалізації активностей за цим грантом та надати аргументацію необхідності захисту.
- Надати очікувані результати реалізації гранту.
- Надати деталізацію обладнання/послуг/програмного забезпечення/матеріалів/засобів, а саме: ключові характеристики та кількість кожного продукту із посиланнями на аналогічні моделі та марки обладнання.
- Зазначити деталізацію витрат, обґрунтовуючи доцільність саме цієї марки та моделі продукту (розрахунок цін у гривнях із зазначенням суми еквіваленту у доларах США, включаючи податок на додану вартість (ПДВ), витрати на доставку та витрати на встановлення).
- Подати резюме (CV) Відповідального виконавця (координатора проєкту).

*Якщо потенційні заявники потребують конкретну марку та модель обладнання, виходячи з досвіду розуміють, що тільки ця модель може покрити технічні потреби, вони повинні надати змістовне та детальне обґрунтування цієї потреби. Навести приклади технічної переваги цього обладнання саме для виконання тих завдань, які заплановані в проєкті заявника.

ВИМОГИ ДО ЗАЯВНИКІВ ТА ГРАНТОВИХ ПРОЄКТІВ

Усі заявники та грантові проєкти мають відповідати **кожній** з вимог нижче:

- Заявки приймаються від Державних установ та об'єктів критичної інфраструктури України, які піддаються потенційним кіберзагрозам або іншим кіберінцидентам.
- Заявники надали чітке формулювання проблеми та обґрунтували необхідність придбання обладнання / послуг / програмного забезпечення.
- Заявники надали чітку деталізацію необхідного обладнання / послуг / програмного забезпечення.
- 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**
• Актуальність і вплив на кібербезпеку: аргументація та деталізація того, як проєкт допоможе покращити системи кібербезпеки та інформаційну стійкість.	

2. Потреба у забезпеченні обладнання/ програмного забезпечення та/або наданні послуг	**30 балів**
• Зазначити чітке формулювання проблеми та обґрунтування необхідності придбання конкретного обладнання/ послуг/ програмного забезпечення для грантоотримувача. Як ця допомога буде інтегрована у вже існуючу систему кіберзахисту інституції.	

3. Ясність викладення, реалістичність виконання та достатній рівень деталізації проєктних активностей	**20 балів**
• Заявка має чітко визначену мету у забезпеченні наданні ресурсів (обладнання/ послуг/ програмного забезпечення/матеріалів). Як надана допомога буде впливати на сталість системи кіберзахисту інституції у майбутньому.	

4. Економічна доцільність	**20 балів**
• Деталізація витрат в наданому бюджеті проєкту та їх обґрунтування в описі бюджету.	

ЗАГАЛЬНА ОЦІНКА	**100 балів**

ПІДГОТОВКА ТА ПОДАЧА ГРАНТОВОЇ ЗАЯВКИ

Подача повної грантової заявки

Усі грантові заявки мають бути подані не пізніше **26 січня 2024 року.**

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

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

"DE-03-2023_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,

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: nonpro-grants@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: 17 січня, 2024 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/qXe7uPF3Vd

ДОПУСТИМІ ВИТРАТИ ТА БЮДЖЕТ ПРОЄКТУ

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 національними та міжнародними постачальниками послуг.

Закупівля обладнання та матеріалів: задля побудови та/або зміцнення існуючої інформаційної та кібер інфраструктури.

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. Кожний заявник – Державних установ України – може подати **лише одну грантову заявку** за цим Конкурсом.

2. Після оголошення результатів Конкурсу кожний обраний заявник буде проінформований про це електронним листом від CRDF Global.
3. Кожний обраний грантоотримувач має надати Фінальний програмний звіт протягом 1 місяця після отримання грантової допомоги.
4. Кожний обраний грантоотримувач має надати підписаний Акт прийому - передачі по отриманому обладнанню.