# Грант на поліпшення кібербезпеки (ГПКБ)
# Оголошення програми

## Читати англійською
## Читати українською

| | |
|---|---|
| Ціль: | Підвищити рівень інформаційної безпеки та кібербезпеки державних установ та державних підприємств критичної інфраструктури в Україні |
| Старт конкурсу: | **1 березня 2019 р.** |
| Кінцевий термін подачі заявки : | **1 квітня 2019 р.** (Програми переглядаються на постійній основі ) |
| Право на обрання: | Заявники – державні установи та державні підприємства – у сферах критичної інфраструктури в Україні як єдині постачальники послуг в Україні (наприклад, електроенергія або природний газ, тощо) |
| Як подати заявку: | Електронною поштою на адресу cysig@crdfglobal.org |
| Загальна сфера: | Кібербезпека |
| Сума премії: | До 25 000 доларів США |
| Термін премії: | Один рік |
| Оголошення та заявки: | http://www.crdfglobal.org/ (див. "Current Funding Opportunities") |

**Загальний огляд**

- ГПКБ є грантами, що фінансуються CRDF Global для підвищення рівня інформаційної безпеки та кібербезпеки державних установ та державних підприємств, які відповідають критеріям прийнятності.
- ГПКБ є одноразовим, однорічним грантом в розмірі до 25 000 доларів США кожна
- Грантова підтримка реалізується через CRDF Global.

**Право на обрання**

*Заявники ГПКБ повинні **відповідати наступним вимогам, щоб мати право на участь у цьому конкурсі *:**

ГПКБ відкритий для заявників – українських державних установ та державних підприємств – які відповідають усім зазначеним критеріям:

- Web-інтерфейс для взаємодії із споживачами послуг, які надають українські державні установи та державні підприємства;
- Наявна IT-інфраструктура, придатна для впровадження рішень із покращення рівня інформаційної безпеки та кібербезпеки державних установ та державних підприємств;
- Географічно розгалуджена мережа (яка охоплює Київ, Київську область та принаймні три інші області України)
- Природна монополія на постачання послуг в Україні (наприклад, в галузі електроенергії або природного газу)

Кожна пропозиція оцінюється незалежно і тому не повинна бути частиною інших пропозицій, поданих до цієї програми,та не залежати від її успішності.

Кожному заявнику – державним установам та державним підприємствам критичної інфраструктури в Україні - дозволено подати **лише одну заявку** на цей грантовий конкурс.

**CRDF Global залишає за собою право обмежувати участь будь-якої особи або установи в його програмах.**
**CRDF Global дотримується всіх законів і правил США, що стосуються експортного контролю та участі іноземних громадян або установ у його діяльності. Політикою CRDF Global є те, що він не повинен здійснювати будь-які операції з організаціями США, які попали під обмеження, без відповідного дозволу уряду США.**

**Необхідні матеріали заявки**

- **Заповнена заявка на ГПКБ (***обов'язково***)**
- **Заповнена бюджетна форма ГПКБ*** (*обов'язково*)
- **Біографія (CV)** кожного члена проектної групи з боку заявника – 3 сторінки максимум, у форматі Word або PDF – із зазначенням контактного номера телефону або електронної адреси Начальника відділу інформаційної безпеки (НВІБ) від установи-заявника (*обов'язково*)
- **Оцінка внутрішньої або зовнішньої вразливості** (у формі звіту або внутрішньої доповіді) (*обов'язково*)

Усі матеріали заявки повинні подаватися у вигляді додатків у файлах Word, PDF або RTF, надані CRDF Global.

* ГПКБ призначений для придбання **обладнання (та пов'язаних з ним оплат за встановлення), матеріалів та засобів,** що покращують інформаційну безпеку та кібербезпеку. **Витрати на оплату праці членів проектної групи з боку заявника не допускаються за рахунок цього грантового фінансування.**

**Допустимі витрати**
Максимальний загальний розмір гранту – до 25 000 доларів США від CRDF Global, що надається безпосередньо установі, в якій працевлаштована проектна група з боку заявника. * У випадку отримання гранту, бюджети, які вимагають фінансування CRDF Global, можуть бути переглянуті.

**Допустимі витрати** включають:

- Обладнання, Засоби та Послуги (ОЗП),
- Інші прямі витрати (інші витрати, які можуть виникнути у зв'язку з встановленням та обслуговуванням ОЗП)

**Критерії оцінювання пропозиції**
Усі пропозиції будуть оцінюватися на основі наступних критеріїв:

**Актуальність і вплив кібер-безпеки:**

- Якими є запропоновані поліпшення безпеки і як вони поліпшать безпеку в державній установі/державному підприємстві заявника?
- Як часто заявник спостерігав прецеденти спроб кібер-атаки, спрямованої на його інформаційні ресурси?
- Якими є максимально можливі наслідки в разі успішної кібер-атаки на ключові інформаційні ресурси?

**Стійкість та зобов'язання:**

- Чи має заявник змогу надалі надавати фінансову, матеріально-технічну та/або кадрову підтримку для проекту після закінчення грантового фінансування?

- Чи має заявник чітку стратегію або план моніторингу/оцінки результативності впроваджених рішень та/або встановленого обладнання? Яким чином заявник зможе проаналізувати, чи досягнуто очікуваного впливу завдяки впровадженим рішенням?
- Чи пропонує установа-заявник довгострокову фінансову підтримку або детальний план технічного обслуговування?

**Чіткість, доцільність і деталізація:**
- Чи має проект чіткий і обґрунтований термін і план реалізації?
- Чи є запропонований бюджет обґрунтованим та доцільним для даної діяльності?
- Чи будуть перерви в роботі з веб-інтерфейсом або інформаційним ресурсом (мережею) безпосередньо впливати на послуги, що надаються державними установами та державними підприємствами?
- Чи є поточна інформаційна та телекомунікаційна система установи відповідною для запропонованих оновлень?

*Будь ласка, зверніть увагу, що ГПКБ є цільовими грантами, і повторне фінансування тих самих установ або підприємств обмежене.*

**Додаткова інформація**
- Для отримання детальної інформації щодо конкурсу ГПКБ відвідайте: https://www.crdfglobal.org/funding-opportunities/CyberUkraine
- Для отримання детальної інформації щодо загальної політики CRDF Global щодо наданя грантів відвідайте: http://www.crdfglobal.org/grants-and-grantees/faqs
- За додатковими питаннями щодо конкурсу ГПКБ звертайтеся до CRDF Global за адресою cybsig@crdfglobal.org

**Як подати заявку**
- Подайте заповнену заявку, бюджет та необхідні документи за наступною адресою: **cysig@crdfglobal.org**.

## Політики CRDF Global

**Анти-плагіат:** CRDF Global не надаватиме фінансування для заявки, в якій існує плагіат. Всі заявки на фінансування, подані до CRDF Global, будуть ретельно перевірені на плагіат стосовно великої кількості джерел, включаючи опубліковані наукові статті, книги, реферати конференцій та веб-сайти. Коли виявлено плагіат, програма в рамках CRDF Global, яка контролює можливість фінансування, визначить конкретні заходи, які необхідно вжити. Вжиті заходи можуть включати, але не обмежуються: a) інформування заявника про виявлення плагіату; b) виключення заявника з можливості фінансування; в) інформування установи заявника; d) інформування рецензентів; e) інформування організацій, які співпрацюють з CRDF Global щодо можливості фінансування; f) заборона заявнику брати участь в майбутніх можливостях фінансування.

**Конфіденційність пропозицій та інформації про заявника:** CRDF Global гарантує конфіденційність матеріалів усіх заявок і вимагатиме від усіх учасників та рецензентів дотримання конфіденційності заявок. Проте автори заявок повинні знати, що успішні заявки/пропозиції будуть розглядатися як публічна інформація. Отже, на власний розсуд, якщо в заявці є конкретна інформація, що є конфіденційною для бізнесу та не призначена для публічного розповсюдження, вона повинна бути чітко позначена як така. Такі частини заявки будуть утримані від публічного поширення, якщо заявка/пропозиція буде успішною.

**Приклади проектів для участі в конкурсі грантів на поліпшення кібербезпеки (ГПКБ):**

*** Будь ласка, зверніть увагу, що ГПКБ не фінансує навчання чи семінари. ГПКБ надаватиме фінансування лише на тренінги, пов'язані з використанням закупленого обладнання для кібербезпеки або розуміння процедур кібербезпеки.**

**До прикладів обладнання для забезпечення кібербезпеки інформаційно-телекомунікаційних систем (ІТС) та для фізичної безпеки об'єктів інформаційної діяльності (ОІА) належать:**

1. Системи контролю доступу до об'єктів інформаційної діяльності (ОІА) та/або серверних приміщень (наприклад, камери, електронні цифрові замки)
2. Екран захисту веб-додатків (WAF)
3. Брандмауер (мережевий брандмауер)
4. Системи запобігання вторгнень (IPS)
5. Системи управління інформацією та безпекою (SIEM) (наприклад, McAfee Enterprise Security Manager)
6. Антивірусне програмне забезпечення
7. Обладнання для забезпечення фізичної безпеки та безперервності роботи серверних кімнат і центрів обробки даних (резервне енергопостачання, пожежна сигналізація, система пожежогасіння, клімат-система)

*** Будь ласка, зверніть увагу, що вище зазначена інформація не є вичерпним переліком проектів, які можуть бути подані для розгляду в рамках цього грантового конкурсу. CRDF Global заохочує заявників звертатися до cysig@crdfglobal.org, якщо у них є якісь питання або сумніви щодо прийнятності потенційної теми.**

Приклади діяльності та процедури встановлення або зміцнення кібербезпеки:

1. Аудит та розвиток процесів управління ІТ (наприклад, на основі методології COBIT 5)
2. Аудит інформаційної безпеки та розробка рекомендацій на його основі (наприклад, на основі пакета стандартів ISO 270XX)
3. Розробка та впровадження процедур (політик) управління інцидентами інформаційної безпеки
4. Розробка та впровадження процедур (політик) управління змінами в інформаційних системах
5. Розробка та впровадження процедур (політик) управління доступом до інформаційних ресурсів
6. Навчання та атестація персоналу відділу інформаційної безпеки відповідно до міжнародних вимог (наприклад, сертифікація однією з програм ISACA)