Безвъзмездни средства за подобряване на киберсигурността (CySIG)

БЪЛГАРСКИ ЕЗИК

Цел:	**Повишаване на нивото на информационна и киберсигурност в академичните и изследователските институции.** Безвъзмездните средства са предназначени за повишаване на капацитета на академичните и научноизследователските институции за защита и реагиране на киберзаплахите, породени от злонамерени лица, които се опитват да откраднат чувствителни данни от научни изследвания и проекти чрез
Откриване на конкурса:	**Грузия: 9 юни 2022 г.** **Армения: 29 септември 2022 г.** **Турция, Азербайджан, България: 23 септември 2022 г.**
Краен срок за кандидатстване:	**Грузия: 22 юли 2022 г.** **Армения, Турция, Азербайджан, България: 7 ноември 2022 г.**
Допустимост:	Кандидати - академични и изследователски институции - с научни изследвания по теми, като: • Наука и технологии • Инженеринг (всички видове) • Социални науки • Медицински • Изчисления • Навигация и авиационна техника • Задвижващи системи • Телекомуникации и информационна сигурност • Електроника Допустими държави - Грузия, Армения, Турция, Азербайджан, България
Как да	По имейл доcysig@crdfglobal.org
Обща област:	Киберсигурност
Размер на отпуснатите	До 30 000 USD
Продължителност на	Една година
Обявяване и кандидатстване:	http://www.crdfglobal.org/ (вижте “Текущи възможности за финансиране”)

Преглед

Придобиването на знания, умения и инструменти за успешна програма за киберсигурност чрез семинар трябва да бъде допълнено с изграждане на капацитет за прилагане на препоръчаните мерки за контрол и защита. CRDF Global ще отпусне безвъзмездни средства на изследователски институции и университети, които са изпратили свои представители на един от семинарите за оборудване и свързаните с него такси за инсталиране, материали и консумативи с цел подобряване на информационната и киберсигурността.

- Безвъзмездните средства за подобряване на киберсигурността са безвъзмездни средства, спонсорирани от CRDF Global, за повишаване на нивото на информационна и киберсигурност в академични и изследователски институции, които отговарят на критериите за допустимост.
- CySIG се отпускат еднократно за срок от една година, като размерът на всяка от тях е до 30 000 USD.
- Средствата се предоставят чрез CRDF Global.

Допустимост

Право да кандидатства има всяка научноизследователска институция или висше учебно заведение, което е изпратило свой представител на един от семинарите по програмата, посветени на киберкражбите. Кандидатите могат да кандидатстват като отделна организация или като консорциум. Не се изисква главният изследовател и другите членове на екипа за отпускане на безвъзмездни средства за научни изследвания да са присъствали на семинара. За разглеждане на кандидатурите в този конкурс е необходимо одобрение от страна на институцията.

CySIG са отворени за кандидати - публични и частни академични и изследователски институции и предприятия - които отговарят на всички от изброените критерии:

- Активни научноизследователски дейности по изброените по-горе теми. Кандидатите от други изследователски области могат да кандидатстват с надлежна обосновка.
- Съществуваща ИТ инфраструктура, пригодена за подобряване на сигурността.
- Физическо присъствие в някоя от допустимите държави
- Институционално одобрение

Всяко предложение се разглежда самостоятелно и следователно не трябва да бъде част от други предложения, подадени в рамките на тази програма, нито да бъде зависимо от техния успех.

Всеки кандидат - институция - може да подаде само едно заявление за този конкурс за безвъзмездни средства за всеки изследователски отдел.

CRDF Global си запазва право да наложи ограничения на участието на което и да е лице или институция в своите програми. CRDF Global спазва всички закони и нормативни актове на САЩ, свързани с контрола на износа и участието на чуждестранни граждани или институции в нейните дейности. Политика на CRDF Global е да не извършва никакви транзакции с юридически лица с ограничен достъп в САЩ без съответното разрешение от правителството на САЩ.

Изисквани материали за кандидатстване

Всички кандидатури трябва да включват информацията и придружаващите документи, посочени в *Контролния списък за кандидатстване за безвъзмездни средства за противодействие на киберкражбите в академичните среди на CRDF Global*, който може да бъде изтеглен като образец на документ в Microsoft Word. Материалите за кандидатстване и научноизследователските продукти могат да бъдат подадени на английски език или на стандартизиран национален език. Позициите в заявлението и описанието трябва да бъдат ограничени до пет страници с един интервал. Допълнителни съпътстващи документи и електронни таблици могат да бъдат приложени към това описание или изпратени като отделни документи.

Попълнен формуляр за кандидатстване на CySIG и придружаващи документи, включително:

- **Попълнен формуляр за бюджет на CySIG*** (*задължително*)
- **Автобиография (CV)** на всеки член на екипа по проекта от страна на кандидата — максимум 3 страници за всеки, във формат Word или PDF - с посочени телефон и електронна поща за връзка с ръководителя по сигурността на информацията (CISO) от кандидатстващата институция (*задължително)*
- **Вътрешна или външна оценка на уязвимостта на киберсигурността** — под формата на доклад или вътрешен доклад (*задължително)*
- **Потвърдително писмо от институцията***(задължително) *за да се класирате, документ от ръководството на вашата институция трябва да посочва, че имате необходимата подкрепа от вашата институция за кандидатстване и изпълнение на тази безвъзмездна помощ. Формулярът **трябва** да бъде подписан от ръководството.*
- Трябва да се представи **списък с препоръки** от независими лица, които са запознати с работата на Главния изследовател или екипа на проекта.

Всички материали за кандидатстване трябва да бъдат представени като прикачени файлове в Word или PDF, като се използват формулярите, предоставени от CRDF Global.

Приложно поле на безвъзмездната помощ

*CySIG са предназначени за финансиране на **оборудване и свързаните с него такси за инсталиране, материали и консумативи**, които подобряват информационната сигурност и киберсигурността. **Работните разходи на членовете на екипа на проекта от страна на кандидата не се допускат в рамките на това безвъзмездно финансиране.**

Допустими средства
Максималният общ размер на безвъзмездните средства е до 30 000 щатски долара от CRDF Global, които се отпускат директно на института, в който работи основното лице за контакт. **В случай на отпускане на средства, бюджетите, за които се иска финансиране от CRDF Global, могат да бъдат преразгледани.

Допустими разходи
- Оборудване, консумативи и услуги (ESS)
- Други преки разходи (други съпътстващи разходи, които могат да възникнат във връзка с инсталирането и поддръжката на ESS)

Критерии за оценка на предложенията
Всички предложения ще бъдат оценени на базата на следните критерии:

1. **Значение и въздействие на киберсигурността:**
   - Какви са предложените актуализации на сигурността и как ще подобрят сигурността в институцията?
   - Колко често кандидатът е наблюдавал прецеденти на опити за кибератаки, насочени към
2. **Устойчивост и ангажимент:**

- Организацията на кандидата демонстрира ли своята ангажираност към проекта, като предлага безплатна финансова, логистична и/или екипна подкрепа?
- Има ли кандидатът ясна стратегия или план за мониторинг/оценка? Как ще разбере кандидатът, че исканото подобрение е оказало предвиденото въздействие?
- Предлага ли кандидатстващата институция дългосрочна финансова подкрепа или подробен план за поддръжка?

3. **Яснота, целесъобразност и подробности:**
   - Има ли проектът ясен и разумен график и план за осъществяване?
   - Съобразен и обоснован ли е предложеният бюджет за дейностите?
   - Подходяща ли е настоящата информационно-комуникационна система на институцията за предложените подобрения?

4. **Предишни резултати:**
   - Има ли кандидатът опит във висококачествени проучвания по въпроси, свързани с отговорна научна и изследователска етика, почтеност, информационна сигурност, управление на данни, отговорни технологии, институционално съответствие, познаване на технологии с двойна употреба и контрол на износа?

5. **Бюджет:**
   - Съпоставил ли е кандидатът дейностите и задачите в предложението с бюджета на проекта?
   - Достатъчен ли е бюджетът на проекта за осъществяване на задачите в предложението през посочения период на изпълнение?
   - Бюджетните позиции представляват ли разумни и обичайни разходи и подходящ баланс между преките и непреките разходи?

Имайте предвид, че CySIG са безвъзмездни средства на конкурсен принцип и повторното финансиране на едни и същи лица или институции е ограничено.

Допълнителна информация

- За подробна информация относно конкурса на CySIG посетете: https://www.crdfglobal.org/docs/default-document-library/cysig-faq.docx
- За подробна информация относно общите правила за отпускане на безвъзмездни средства на CRDF Global, посетете: http://www .crdfglobal .org/grants -and-grantees/faqs+
- За допълнителни въпроси относно конкурса на CySIG, моля, свържете се с CRDF Global на cysig@crdfglobal.org

Как да кандидатствате

- Изпратете попълненото заявление, бюджета и необходимите документи на **cysig@crdfglobal.org**.

Глобални политики на CRDF

Защита от плагиатство: CRDF Global няма да предостави финансиране на заявление, в което има плагиатство. Всички заявления за финансиране, подадени до CRDF Global, ще бъдат проверени внимателно за плагиатство спрямо голям брой източници, включително публикувани научни статии, книги, резюмета на конференции и уебсайтове. Когато бъде открито плагиатство, програмата в рамките на CRDF Global, която контролира възможността за финансиране, ще определи конкретните действия, които трябва да бъдат предприети. Предприетите действия могат да включват, но не се ограничават до: а) уведомяване на кандидата, че е открито плагиатство; б) изключване на кандидата от възможността за финансиране; в) уведомяване на институцията на кандидата; г) уведомяване на рецензентите; д) уведомяване на организациите, които си сътрудничат с CRDF Global по отношение на възможността за финансиране; е) забрана на кандидата да участва в бъдещи възможности за финансиране.

ПРИМЕРНИ ПРОЕКТИ НА CYSIG

***Моля, имайте предвид, че CySIGs няма да финансира обучения или семинари. CySIG ще финансира само обучения, свързани с използването на поръчаното оборудване за киберсигурност или с разбирането на процедурите за киберсигурност.**

Примерите за оборудване, което се използва за осигуряване на киберсигурността на информационните и телекомуникационните системи (ИТС) и за физическата сигурност на обектите на информационна дейност (ОИД), включват:

1. Системи за контрол на достъпа до обектите на информационна дейност (ОИД) и/или сървърни помещения (напр. камери, електронни цифрови ключалки)
2. Екран за защита на уеб приложенията (WAF)
3. Защитна стена (мрежова защитна стена)
4. Системи за предотвратяване на проникване (IPS)
5. Системи за управление на информацията и събитията в сигурността (SIEM) (например McAfeeEnterprise Security Manager)
6. Антивирусен софтуер

***Моля, обърнете внимание, че горепосоченият списък не е изчерпателен списък на отговарящи на изискванията проекти. CRDF Global препоръчва на кандидатите да се свържат сcysig@crdfglobal.org ако имат някакви въпроси или притеснения относно допустимостта на потенциална тема.**

Примери за дейности и процедури за създаване или повишаване на киберсигурността:

1. Одит и разработване на процеси за управление на ИТ (например въз основа на методологията COBIT 5)
2. Одит на информационната сигурност и разработване на препоръки въз основа на него (например въз основа на пакета от стандарти ISO 270XX)
3. Разработване и внедряване на процедури за управление на инциденти, свързани с информационната сигурност (политики)
4. Разработване и внедряване на процедури (политики) за управление на промените в информационните системи
5. Разработване и внедряване на процедури (политики) за контрол на достъпа до информационни ресурси
6. Обучение и сертифициране на служителите на отдела за информационна сигурност в съответствие с международните изисквания (например сертифициране по някоя от програмите на ISACA).