Կիբերանվտանգության բարելավման դրամաշնորհ (CySIG)

ԱՆԳԼԵՐԵՆ

Նպատակը՝	**Արդիականացնել տեղեկատվության և կիբերանվտանգության մակարդակը Վրաստանի և Հայաստանի ակադեմիական և հետազոտական հաստատություններում:** Դրամաշնորհները նախատեսված են ընդլայնելու ակադեմիական և հետազոտական հաստատությունների հնարավորությունները, պաշտպանելու և արձագանքելու չարագործ կառույցների կողմից իրականացվող կիբերհարձակումներին, որոնք համակարգչային համակարգերի անթույլատրելի մատչման միջոցով նպատակ են հետապնդում գողանալ գաղտնի հետազոտական
Մրցույթի մեկնարկ՝	**Վրաստան՝ հունիսի 9, 2022 թ.** **Հայաստան՝ սեպտեմբերի 29, 2022 թ.** **Թուրքիա, Ադրբեջան, Բուլղարիա՝ սեպտեմբերի 23, 2022 թ.**
Հայտերի վերջնաժամկետ՝	**Վրաստան՝ հուլիսի 22, 2022 թ.** **Հայաստան, Թուրքիա, Ադրբեջան, Բուլղարիա՝ նոյեմբերի 7, 2022 թ.**
Իրավասություն՝	Հայտատուներ՝ ակադեմիական և հետազոտական հաստատություններ, որոնք արդիական հետազոտություններ են իրականացնում հետևյալ ոլորտներին առնչվող թեմաների շուրջ՝ • Գիտություն և տեխնոլոգիա • Ճարտարագիտություն (բոլոր տեսակի) • Հասարակական գիտություններ • Բժշկական • Համակարգչային գիտություն • Նավիգացիա և օդագնացային էլեկտրոնիկա • Շարժիչ համակարգեր • Հեռահաղորդակցություն և տեղեկատվական անվտանգություն • Էլեկտրոնիկա Իրավասու երկրներն են՝ Վրաստան, Հայաստան, Թուրքիա, Ադրբեջան, Բուլղարիա
Ինչպես դիմել՝	Էլ.փոստով՝ cysig@crdfglobal.org
Ընդհանուր ոլորտ՝	Կիբերանվտանգություն
Դրամաշնորհի կողմից	Մինչև $30,000
Դրամաշնորհի	Մեկ տարի
Հայտարարություն և հայտադիմում՝	http://www.crdfglobal.org/ (տես «Ընթացիկ ֆինանսավորման հնարավորություններ»)

Համառոտ նկարագրություն

Աշխատաժողովի միջոցով առաջատար կիբերանվտանգության ծրագրի համար գիտելիքների, հմտությունների և գործիքների ձեռքբերումը պետք է ամրապնդվի կարողությունների հզորացմամբ, որպեսզի ինչպես հարկն է իրականացվեն առաջարկվող հսկողությունն ու պաշտպանությունը: CRDF Global-ը դրամաշնորհներ կտրամադրի հետազոտական և կրթական հաստատություններին, որոնց ներկայացուցիչները մասնակցել են աշխատաժողովներից առնվազն մեկին՝ տեղեկատվությունը և կիբերանվտանգությունը բարելավող սարքավորումների ձեռքբերման, դրանց առնչվող տեղադրման վճարների, նյութերի և պարագաների վերաբերյալ:

- Կիբերանվտանգության բարելավման դրամաշնորհները CRDF Global-ի կողմից ֆինանսավորվող դրամաշնորհներ են՝ արդիականացնելու տեղեկատվության և կիբերանվտանգության մակարդակն ակադեմիական և հետազոտական հաստատություններում, որոնք համապատասխանում են սահմանված չափանիշներին:
- CySIG-երը յուրաքանչյուրին $30,000-ի չափով մեկանգամյա, մեկ տարով շնորհվող դրամաշնորհներ են
- Դրամաշնորհներն իրականացվում են CRDF Global-ի միջոցով:

Իրավասություն

Դրամաշնորհին կարող է դիմել կիբերգողությունների թեմայով աշխատաժողովներից մեկին մասնակցելու նպատակով ներկայացուցիչ ուղարկած ցանկացած հետազոտական ընկերություն կամ բարձրագույն կրթական հաստատություն: Հայտատուները կարող են դիմել որպես առանձին հաստատություն կամ որպես կոնսորցիում: Կարիք չկա, որ հետազոտական թիմի գլխավոր ուսումնասիրողը և դրամաշնորհի հետազոտական մյուս անդամները մասնակցեն աշխատաժողովին: Տվյալ մրցույթին հայտերի մասնակցության համար պահանջվում է ինստիտուցիոնալ հաստատում:

CySIG-երը բաց են հայտատուների (հանրային և մասնավոր սեկտորի ակադեմիական և հետազոտական հաստատությունների ձեռնարկությունները ներկայացնող անձինք) համար, որոնք համապատասխանում են սահմանված չափանիշներին.

- Ակտիվ հետազոտություն՝ վերը նշված թեմաների վերաբերյալ: Պատշաճ հիմնավորման դեպքում՝ կարող են դիմել այլ հետազոտական թեմաների ուսումնասիրությամբ զբաղվող թեկնածուները:
- Առկա SS ենթակառուցվածք, որը համապատասխանում է անվտանգության արդի բարելավումներին
- Ֆիզիկական ներկայություն իրավասու երկրներից որևէ մեկում
- Հաստատում ինստիտուցիոնալ մակարդակով

Յուրաքանչյուր առաջարկ գնահատվում է առանձին և ուստի չպետք է հանդիսանա այս ծրագրին ներկայացված մեկ այլ առաջարկի մաս, կամ էլ կախված լինի դրանցից որևէ մեկի հաջողությունից:

Յուրաքանչյուր հայտատու (հաստատություն) սույն դրամաշնորհի մրցույթին կարող է ներկայացնել միայն մեկ հետազոտական բաժնին առնչվող հայտ:

CRDF Global-ն իրեն իրավունք է վերապահում սահմանափակել ցանկացած անհատի կամ հաստատության մասնակցությունն այս ծրագրերին: CRDF Global-ը համապատասխանում է ԱՄՆ-ի բոլոր օրենքներին և կանոնակարգերին, որոնք առնչվում են վերահսկողության միջոցների արտահանմանը և օտարերկրացիների կամ օտարերկրյա հաստատությունների մասնակցությանն իր կողմից կազմակերպված գործունեության ոլորտներում: CRDF Global-ի քաղաքականությունն է չիրականացնել որևէ գործարք ԱՄՆ-ի կողմից սահմանափակված կառույցների հետ՝ առանց ԱՄՆ-ի կողմից համապատասխան թույլտվության: Կառավարություն:

Հայտի ներկայացման համար պահանջվող նյութեր

Բոլոր հայտատուները պետք է ներառեն տվյալները և կից փաստաթղթերը CRDF Global-ի՝ *ակադեմիական շրջանակներում կիբերգողությունների դեմ պայքարի վերաբերյալ դրամաշնորհին դիմելու ստուգաթերթում,* որը կարելի է ներբեռնել որպես Microsoft Word-ի փաստաթղթի ձևանմուշ: Հայտադիմումի փաստաթղթերը և հետազոտական նյութերը կարող են ներկայացվել անգլերենով կամ տվյալ երկրի պետական լեզվով: Հայտադիմումի և մյուս նյութերի ծավալը պետք է սահմանափակվի մեկ բացատ ունեցող հինգ էջով: Լրացուցիչ օժանդակ փաստաթղթերը և աղյուսակները կարող են կցվել այս նյութերին կամ ուղարկվել որպես առանձին փաստաթղթեր:

CySIG-ի լրացված հայտադիմումի ձևաթուղթը և օժանդակ փաստաթղթերը ներառում են.

- **CySIG-ի բյուջեի լրացված ձևաթուղթ*** (*պարտադիր*)
- Նախագծին մասնակցող թիմի հայտատուի կողմից ներկայացված յուրաքանչյուր անդամի **ինքնակենսագրությունը (CV)** (յուրաքանչյուրն առավելագույնը 3 էջի սահմաններում, Word կամ PDF ձևաչափով), որտեղ նշված է դիմող հաստատության Տեղեկատվության անվտանգության հարցերով գլխավոր պատասխանատուի (CISO) կոնտակտային հեռախոսահամարը և էլ.փոստի հասցեն (*պարտադիր*)
- **Կիբերանվտանգության ներքին և արտաքին խոցելիության գնահատում**՝ հաշվետվության կամ ներքին տեղեկագրի տեսքով (*պարտադիր*)
- **Ինստիտուցիոնալ երաշխավորագիր նամակ** (*պարտադիր)*պահանջներին համապատասխանելու մասին. ձեր հաստատության ղեկավարության կողմից տրված փաստաթուղթը պետք է նշի, որ դուք ունեք ձեր հաստատության աջակցությունը՝ այս ղրամաշնորհին դիմելու և այն իրականացնելու համար: Ձևաթուղթը* **պետք է** *ստորագրվի ղեկավարության կողմից:*
- **Հղումների ցանկը** պետք է տրամադրվի անկախ անհատների կողմից, ովքեր ծանոթ են Գլխավոր հետազոտողի կամ նախագծի թիմի աշխատանքի հետ

Հայտի բոլոր նյութերը պետք է ներկայացվեն որպես կից փաստաթղթեր Word կամ PDF ֆայլերով՝ օգտագործելով CRDF Global-ի կողմից տրամադրված ձևաթղթերը:

Դրամաշնորհի ֆինանսավորման ծածկույթը

CySIG-երը նախատեսված են **սարքավորումների (և դրանց առնչվող տեղադրման վճարների), նյութերի և պարագաների համար**, որոնց օգնությամբ կբարելավվեն տեղեկատվության անվտանգությունը և կիբերանվտանգությունը: **Այս դրամաշնորհի ֆինանսավորման շրջանակներում հայտատուներին չի թույլատրվում ներառել նախագծի թիմի աշխատուժի ծախսերը:**

Տրամադրվող միջոցներ

Դրամաշնորհի ընդհանուր գումարը կազմում է $30,000: CRDF Global-ի կողմից տրամադրվող ԱՄՆ դոլարով գումարն անմիջապես շնորհվում է այն հաստատությանը, որտեղ աշխատում է հիմնական կոնտակտային անձը: *Դրամաշնորհը տրամադրվելու դեպքում՝ CRDF Global-ի կողմից ֆինանսավորվող նախագծերի բյուջեները կարող են ենթարկվել վերանայումների:

Թույլատրելի ծախսեր

- Սարքավորումներ, պարագաներ և ծառայություններ (ESS),
- Այլ ուղղակի ծախսեր (ESS-ի տեղադրման և տեխնիկական սպասարկման հետ կապված այլ կողմնակի ծախսեր)

Առաջարկի գնահատման չափանիշներ

Բոլոր առաջարկները պետք է գնահատվեն՝ ելնելով հետևյալ չափանիշներից.

1. **Կիբերանվտանգության համապատասխանությունը և ազդեցությունը.**
   - Որո՞նք են առաջարկվող անվտանգության արդիականացումները և ինչպես դրանք կբարելավեն հաստատության անվտանգությունը:
   - Որքա՞ն հաճախ է հայտատուն ականատես լինում իր տեղեկատվական ռեսուրսներին ուղղված կիբերհարձակումների փորձերի:
   - Որո՞նք են առավելագույն հնարավոր հետևանքները՝ տեղեկատվության հիմնական ռեսուրսների

2. **Կայունություն և հանձնառություն.**

- Արդյո՞ք հայտատուի կազմակերպությունը հանձնառություն է ցուցաբերում նախագծի նկատմամբ՝ առաջարկելով ֆինանսական, լոգիստիկ և/կամ անձնակազմի լրացուցիչ աջակցություն:
- Արդյո՞ք հայտատուն ունի հստակ մշտադիտարկման/գնահատման ռազմավարություն կամ պլան: Ինչպե՞ս կարող է հայտատուն պարզել՝ արդյոք պահանջվող արդիականացումը ունեցել է նախատեսված ազդեցությունը, թե ոչ:
- Արդյո՞ք հայտատուի կողմից ներկայացվող հաստատությունն առաջարկում է երկարաժամկետ ֆինանսական աջակցություն կամ տեխնիկական սպասարկման մանրակրկիտ պլան:

3. Հստակություն, իրագործելիություն և մանրակրկտություն.

- Արդյո՞ք նախագիծն ունի հստակ և խելամիտ ժամանակացույց և իրականացման պլան:
- Արդյո՞ք առաջարկվող բյուջեն համապատասխան է և ողջամիտ տվյալ գործունեության համար:
- Արդյո՞ք հաստատության ներկայիս տեղեկատվության և հեռահաղորդակցության համակարգը համապատասխանում է առաջարկվող արդիականացումներին:

4. Նախկինում գրանցված արդյունքները.

- Արդյո՞ք հայտատուն ունի բարձր որակի հետազոտական փորձ՝ պատասխանատու գիտական և հետազոտական էթիկայի, հավաստիության, տեղեկատվության անվտանգության, տվյալների կառավարման, պատասխանատու տեխնոլոգիայի, ինստիտուցիոնալ համապատասխանության, երկակի օգտագործման տեխնոլոգիաների և արտահանման վերահսկողության գիտելիքների թեմաների շուրջ:

5. Բյուջե.

- Արդյո՞ք հայտատուն կազմել է առաջարկի գործողությունները և առաջադրանքները նախագծի բյուջեին համապատասխան:
- Արդյո՞ք նախագծի բյուջեն բավարար է նշված ժամանակահատվածի ընթացքում առաջարկում նշված գործողություններն իրականացնելու համար:
- Արդյոք բյուջեի բաժնում նշված կետերը ներկայացնում են խելամիտ ու համապատասխան ծախսեր, ինչպես նաև ուղղակի և անուղղակի ծախսերի հավասարակշռություն:

Խնդրում ենք նկատի ունենալ, որ CySIG-երը մրցունակ դրամաշնորհներ են, և նույն անհատներին կամ հաստատություններին տրամադրվող կրկնվող ֆինանսավորումը սահմանափակ է:

Լրացուցիչ տեղեկություն

- CRDF Global-ի կողմից կազմակերպած մրցույթի վերաբերյալ մանրամասն տվյալների համար այցելեք՝ https://www.crdfglobal.org/docs/default- document-library/cysig-faq.docx
- CRDF Global-ի դրամաշնորհային քաղաքականության վերաբերյալ մանրամասն տվյալների համար այցելեք՝ http://www .crdfglobal .org/grants -and- grantees/faqs+
- CySIG-ի մրցույթի վերաբերյալ լրացուցիչ հարցերի դեպքում խնդրում ենք կապ հաստատել CRDF Global-ի հետ հետևյալ էլ.հասցեով՝ cysig@crdfglobal.org

Ինչպես դիմել

- Ուղարկեք լրացված հայտադիմումը, բյուջեն և պահանջվող փաստաթղթերը հետևյալ էլ.հասցեով՝ **cysig@crdfglobal.org**:

CRDF GLOBAL-Ի ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆՆԵՐԸ

Հակագրագողություն. CRDF Global-ը չի տրամադրի ֆինանսավորում այն հայցադիմումների համար, որոնցում առկա է գրագողություն: CRDF Global-ին ֆինանսավորման նպատակով ներկայացված բոլոր հայտադիմումներում ներկայացված նյութերը մանրամասնորեն կուսումնասիրվեն գրագողությունը բացառելու համար՝ ներգրավվելով մեծ քանակությամբ աղբյուրներ՝ ներառյալ հրապարակված հետազոտական աշխատանքներ, գրքեր, համաժողովում ներկայացված քաղվածքներ և կայքեր: Գրագողության բացահայտման դեպքում՝ CRDF Global ծրագիրը, որը վերահսկում է ֆինանսավորման հնարավորությունը, կսահմանի ձեռնարկման ենթակա հատուկ գործողություններ: Ձեռնարկվելիք գործողությունները կարող են ներառել, սակայն չսահմանափակվել հետևյալով՝ ա) տեղեկացնել հայտատուին, որ հայտնաբերվել է գրագողություն, բ) բացառել հայտատուին ֆինանսավորման հնարավորությունից, գ) տեղեկացնել հաստատությանը, որտեղ գրանցված է հայտատուն դ) տեղեկացնել տեսաբաններին, ե) տեղեկացնել CRDF Global-ի հետ ֆինանսավորման հնարավորության հարցում համագործակցող կազմակերպություններին, զ) արգելել հայտատուին մասնակցել ֆինանսավորման հետագա հնարավորություններին:

CySIG ՆԱԽԱԳԾԻ ՕՐԻՆԱԿՆԵՐ

***Խնդրում ենք նկատի ունենալ, որ CySIG-երը չեն ֆինանսավորում դասընթացներ կամ աշխատաժողովներ: CySIG-երը միայն կֆինանսավորեն այն դասընթացները, որոնք առնչվում են գնված կիբերանվտանգության սարքավորումների օգտագործմանը կամ կիբերանվտանգության ընթացակարգերի ըմբռնմանը:**

Տեղեկատվության և հեռահաղորդակցության համակարգի (ITS) անվտանգության և տեղեկատվության գործունեությունն ապահովող իրերի (OIA) ֆիզիկական անվտանգությունն ապահովող սարքավորումների օրինակները ներառում են՝

1. Տեղեկատվության գործունեությունն ապահովող իրերի (OIA) նկատմամբ մուտքի վերահսկողության համակարգեր և/կամ սերվերների սենյակներ (օրինակ՝ տեսախցիկներ, էլեկտրոնային թվային փականներ)
2. Վեբ հավելվածի պաշտպանության էկրան (WAF)
3. Հրապատ (ցանցային հրապատ)
4. Ներխուժման կանխարգելման համակարգեր (IPS)
5. Անվտանգության տվյալների և միջոցառումների կառավարման (SIEM) համակարգեր (օրինակ՝ McAfeeEnterprise Security Manager)
6. Հակավիրուսային ծրագրակազմ

***Խնդրում ենք նկատի ունենալ, որ վերը նշվածը իրավասու նախագծերի սպառիչ ցանկ չէ: CRDF Global-ը հայտատուներին խրախուսում է կապ հաստատել cysig@crdfglobal.org էլ.փոստի միջոցով՝ հավանական թեմայի իրավասության առնչությամբ հարցեր կամ մտահոգություններ ունենալու դեպքում:**

Կիբերանվտանգության հաստատման կամ հզորացման գործողությունների և ընթացակարգերի օրինակներ են՝

1. Աուդիտ և SS կառավարման գործընթացների մշակում (օրինակ՝ COBIT 5 մեթոդաբանության հիման վրա)
2. Ըստ դրա՝ տեղեկատվության անվտանգության աուդիտ և առաջարկությունների մշակում (օրինակ՝ ըստ ISO 270XX ստանդարտների փաթեթի)
3. Տվյալների անվտանգության հետ առնչվող պատահարների կառավարմանն ուղղված ընթացակարգերի մշակում և իրականացում (քաղաքականություններ)
4. Տեղեկատվական համակարգերի կառավարման մեջ փոփոխություններ իրականացնելու նպատակով ընթացակարգերի (քաղաքականությունների) մշակում և իրականացում
5. Տեղեկատվական աղբյուրների նկատմամբ մուտքի վերահսկման ընթացակարգերի (քաղաքականությունների) մշակում և իրականացում
6. Տեղեկատվության անվտանգության բաժնի անձնակազմի՝ միջազգային պահանջներին համապատասխան վերապատրաստում և վկայագրում (օրինակ՝ ISACA ծրագրերից մեկի կողմից վկայագրում)