



RTU ATTĪSTĪBAS FONDS

Nodibinājums «Rīgas Tehniskās universitātes Attīstības fonds», Reģ. Nr. 40008067097, Kaļķu iela 1, Rīga, LV-1658, Latvija

Tālr. 67089429, e-pasts: fonds@rtu.lv, www.fonds.rtu.lv

Kārtība whiteCryption SIA pētniecības darbu stipendiju piešķiršanai Nr. 1-2021/RTUAF-2021/15

whiteCryption SIA sadarbībā ar nodibinājumu „Rīgas Tehniskās universitātes Attīstības fonds” izsludina stipendiju piešķiršanas kārtību pētniecības darbu stipendijām ar mērķi paaugstināt studentu pētniecības darbu kvalitāti un praktisko pielietojamību. Piesakoties konkursā, studenti ne tikai iegūst iespēju saņemt whiteCryption SIA speciālistu atbalstu pētniecības darbu izstrādes procesā, bet arī pretendēt uz stipendiju.

1. Vispārīgie noteikumi.

- 1.1. Stipendiju konkursā var pieteikties informācijas tehnoloģiju, datortehnikas, datorvadības un datorzinātnes jomas bakalaura un maģistra līmeņa studenti no Latvijā akreditētas augstākas izglītības iestādes, kas 2021./2022. studiju gada pavasara semestrī izstrādās pētniecības darbus kādā no pielikumā Nr.1 piedāvātajām vai tām pietuvinātām tēmām.
- 1.2. Konkursa kārtībā tiks piešķirtas 3 stipendijas **1000 EUR** apmērā pētniecības darba izstrādei par kādu no whiteCryption SIA piedāvātajām pētniecības darbu tēmām (skatīt pielikumu Nr.1).
- 1.3. Stipendija studentam tiks izmaksāta divās daļās:
 - 1.3.1.pirmā daļa jeb 200,00 EUR tiks izmaksāta pēc pētniecības darba izstrādes starpatskaites saņemšanas saskaņā ar 5.3. punktu;
 - 1.3.2.otra daļa jeb 800,00 EUR tiks izmaksāta pēc darba nodošanas un aizstāvēšanas saskaņā ar 5.4. punktu.
- 1.4. Stipendiju konkurss notiek divās kārtās.

2. Stipendiju konkursā pretendentiem:

- 2.1. Jāiesniedz līdz 1-2 A4 formāta lapām (burtu lielums „12”, fonts „Times New Roman”) garu konkursa pieteikuma darba kopsavilkumu brīvā formā, izvēloties darba saturisko daļu par kādu no tēmām (skatīt pielikumu Nr.1).
- 2.2. Pieteikuma darba kopsavilkums jāaugšupielādē un konkursa elektroniskā anketa jāaizpilda nodibinājuma „Rīgas Tehniskās universitātes Attīstības fonds” mājaslapā www.fonds.rtu.lv sadaļā „Aktuālie konkursi” pie „whiteCryption SIA pētniecības darbu stipendija” līdz 2021. gada **1. novembrim (ieskaitot)**.

3. Pretendentu atlase.

- 3.1. Pretendenti tiek izvērtēti pēc iesniegtās informācijas un var tikt aicināti uz individuālajām intervijām (intervijas vieta un laiks konkursa gaitā tiek saskaņoti ar pretendentu individuāli), prezentējot savu izvēlēto tēmas pētnieciskā darba kopsavilkumu, kā arī atbildot uz komisijas jautājumiem.
- 3.2. Stipendiju konkursa izvērtēšanas komisija vērtē pretendentes un izvēlas pētniecības darbu autorus, kas saņems stipendiju, balstoties uz 4. punktā minēto kritēriju vērtējumu.

4. Kritēriji pretendentu vērtēšanai pirmajā kārtā:

- 4.1. Studenta motivācija izvēlēto pētniecības darba pētīšanā (kritērija vērtība 0,3);
- 4.2. Studenta iesniegtā pieteikuma darba kopsavilkuma kvalitāte (kritērija vērtība 0,7).

5. Stipendiju konkursa otrajā kārtā:

- 5.1. Finālistam jāizstrādā pētniecības darbs iepriekš izvēlētajā tēmā noteiktajā apjomā, un:
 - 5.1.1.līdz 2022. gada 31. martam jāiesniedz starpatskaite par veikto pētījumu (vismaz 20% no darba kopējā apjoma) un turpmāk plānoto darba gaitu, elektroniski nosūtot uz fonds@rtu.lv (tiks nodots arī uzņēmumam);

- 5.1.2.līdz 2022. gada 15. maijam jāiesniedz pabeigts pētījums, elektroniski nosūtot uz fonds@rtu.lv (tiks nodots arī uzņēmumam).
- 5.2. Stipendiju konkursa izvērtēšanas komisija vērtē finālista izstrādātā pētniecības darba atbilstību tematam un praktisko pielietojamību.
- 5.3. Pirmā stipendijas daļa 200,00 EUR apmērā tiek izmaksāta gadījumā, ja pētniecības darba starpatskaites saturs atbilst apstiprinātajam tematam, ir vismaz 20% no kopējā darba apjoma un ir skaidrs turpmākā darba plāns.
- 5.4. Otra stipendijas daļa 800,00 EUR apmērā tiek izmaksāta gadījumā, ja pētniecības darbs atbilst apstiprinātajam tematam, ir praktiski pielietojams un darba uzdevums ir sasniegts.

6. Stipendiju konkursa izvērtēšanas komisija:

- | | |
|---|--------------------------------|
| 6.1. Komisijas priekšsēdētājs | whiteCrypton SIA pārstāvis |
| 6.2. Komisijas priekšsēdētāja vietnieks | whiteCrypton SIA pārstāvis |
| 6.3. Komisijas loceklis | RTU Attīstības fonda pārstāvis |

7. Citi noteikumi

- 7.1. Konkursa finālistam pētniecības darba izstrādes procesā tiek piedāvāts whiteCrypton SIA atbalsts pilnvērtīgai darba izstrādei, piedāvājot ekspertu un speciālistu konsultācijas, izmantojamās literatūras avotus un materiālus.
- 7.2. Ja vairāki pretendenti tiek novērtēti vienlīdzīgi, izvērtēšanas komisijai ir tiesības lemt par papildus stipendiju piešķiršanu.
- 7.3. Pētniecības darbu vada izglītības iestādes mācībspēks, ar kuru vienojas pats pētniecības darba autors. Pēc izvēles ir iespējams piesaistīt konsultantus no whiteCrypton SIA puses.
- 7.4. Galīgās pētniecības darbu tēmas var tikt precizētas pēc konkursa pirmās kārtas savstarpēji vienojoties whiteCrypton SIA ar studentu un darba vadītāju no izglītības iestādes puses.
- 7.5. Gadījumā, ja konkursa otrajā kārtā finālista izstrādātais pētniecības darbs neatbilst apstiprinātajam tematam, nav praktiski pielietojams vai nav sasniegts izvirzītais uzdevums, otra daļa stipendijas 800,00 EUR apmērā netiek izmaksāta, bet pirmā daļa 200,00 EUR apmērā nav jāatgriež.
- 7.6. Ar whiteCrypton SIA atbalstu izstrādātie studiju pētniecības darbi var tikt izmantoti whiteCrypton SIA darbības attīstībā, šim nolūkam vienojoties ar darba autoru par viņa iesaisti whiteCrypton SIA darbības attīstībā.
- 7.7. Kārtība stipendijas piešķiršanai izdota saskaņā ar nodibinājuma „Rīgas Tehniskās universitātes Attīstības fonds” nolikumu „Par sasniegumiem zinātnē un pētniecībā” Nr. RTUAF-2021/15.

Datums skatāms laika zīmogā

Nodibinājuma

„Rīgas Tehniskās universitātes
Attīstības fonds” izpilddirektore

Anita Straujuma

**DOKUMENTS PARAKSTĪTS AR DROŠU ELEKTRONISKO PARAKSTU UN SATUR
LAIKA ZĪMOGU**



**RTU
ATTĪSTĪBAS FONDS**

Nodibinājums «Rīgas Tehniskās universitātes Attīstības fonds», Reģ. Nr. 40008067097, Kalķu iela 1, Rīga, LV-1658, Latvija

Tālr. 67089429, e-pasts: fonds@rtu.lv, www.fonds.rtu.lv

Pielikums Nr.1
pie kārtības Nr. 1-2021/RTUAF-2021/15
whiteCryption SIA pētniecības darbu stipendiju piešķiršanai

whiteCryption SIA pētniecības darba stipendiju konkursa pieteikuma darba tēmas

Nr.p.k.	Temats
1.	ARM TrustZone izmantošana datorprogrammu pretkopēšanas aizsardzībai https://www.arm.com/products/security-on-arm/trustzone
2.	Datu un ar tiem veicamo operāciju maskēšana (aizsardzība pret novērošanu un analīzi) pilnīgi atklātā programmas izpildīšanās vidē (white-box environment) http://www.whiteboxcrypto.com/
3.	Pilnībā homomorfiskas šifrēšanas implementācija ar piemēriem https://en.wikipedia.org/wiki/Homomorphic_encryption https://crypto.stanford.edu/craig/easy-fhe.pdf https://crypto.stanford.edu/craig/craig-thesis.pdf https://eprint.iacr.org/2015/1192.pdf https://tfhe.github.io/tfhe/ https://github.com/google/fully-homomorphic-encryption
4.	Pētījums par specializēto Intel procesora instrukciju izmantošanu kriptogrāfisko algoritmu paātrināšanai https://en.wikipedia.org/wiki/CLMUL_instruction_set http://www.intel.co.kr/content/dam/www/public/us/en/documents/whitepapers/polynomial-multiplication-instructions-paper.pdf https://eprint.iacr.org/2011/589.pdf
5.	Pētījums par uz režģiem balstītām kriptosistēmām https://en.wikipedia.org/wiki/Lattice-based_cryptography
6.	Pētījums par jaunākajiem bloku algoritmu šifrēšanas režīmiem uz diska glabātu datu aizsardzībai https://en.wikipedia.org/wiki/Disk_encryption_theory
7.	Uz TPM (Trusted Platform Module) balstīta platformas apstiprināšana un droša sāknēšana http://www.trustedcomputinggroup.org/trusted-platform-module-tpmsummary/
8.	Koda integritātes nodrošināšana JavaScript programmās
9.	Koda integritātes pārbaude, kas pieļauj Intel PIN rīku lietošanu
10.	Pārskats par pieejamo aparatūras atbalstu drošai skaitļošanai (ARM TrustZone, TPM, Rambus CryptoManager, Intel TXT/SGX/AMT u.c.) https://www.arm.com/products/security-on-arm/trustzone http://www.trustedcomputinggroup.org/trusted-platform-module-tpmsummary https://www.rambus.com/security/cryptomanager-platform https://software.intel.com/en-us/articles/intel-trusted-execution-technology-aprimer https://en.wikipedia.org/wiki/Intel_Active_Management_Technology
11.	Cita konkrēta, ar SIA „whiteCryption” saskaņota pētniecības tēma, kas iekļaujas kādā no zemāk minētajiem tematiem: 1. Klasiskā kriptogrāfija (simetriskās un publiskās atslēgas algoritmi, kopīgas atslēgas izveidošanas protokoli, digitālie paraksti, utml.);

- | | |
|--|---|
| | <ol style="list-style-type: none">2. "Baltās kastes" (white-box) kriptogrāfija;3. Programmas koda un datu integritātes pārbaude un nodrošināšana;4. Programmas koda obfuskācija (obfuscation);5. Pretkopēšanas aizsardzība;6. Nodevēju izsekošana (traitor tracing);7. Digitālā satura tiesību pārvaldība (digital rights management);8. Būla ķēžu obfuskācija;9. Cita ar datu vai programmatūras drošību saistīta tēma. |
|--|---|