Riikliku küberturvalisuse uudiskiri

2021-11

Majandus- ja kommunikatsiooniministeerium

Võrgu- ja infosüsteemide turbe direktiiv (NIS2) jõudis EL Nõukogusse

Majandus- ja kommunikatsiooniministeerium

Eesti seisukohad EL ühise küberüksuse (Joint Cyber Unit) osas

TalTech

8.12 toimub veebikonverents ja uue õppematerjali tuvustus teemal “Naised küberturbes – eeskujud tüdrukutele”

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja kommunikatsiooniministeerium

Elektroonilise side seaduse vastu võtmine avab tee sidevõrkude turvalisuse tagamiseks 3

Võrgu- ja infosüsteemide turbe direktiiv (NIS2) jõudis EL Nõukogusse 3

Eesti seisukohad EL ühise küberüksuse (Joint Cyber Unit) osas 4

Kõrgemad Küberkaitse ja Digiriigi kursused 5

Küberturvalisuse seaduse muudatusi käsitlev infotund ETO-dele 5

TalTech

TalTechi küberkriminalistika ja küberjulgeoleku keskusel täitus seitsmes tegutsemisaasta 6

8.12 toimub veebikonverents ja uue õppematerjali tuvustus teemal “Naised küberturbes — eeskujud tüdrukutele” 6

8.12 toimub suurim Eesti noorte algajate kübervõistlus KüberPuuring 6

Cybernetica

Cybernetica ja TalTech asuvad koostöös uurima tuleviku digiallkirju 7

Tartu Ülikool

Teine CHAISE uudiskiri annab ülevaate plokiahela tehnoloogia tööturu hetkeseisust Euroopas 7

Elektroonilise side seaduse vastu võtmine avab tee sidevõrkude turvalisuse tagamiseks

Riigikogu võttis 2021. a 24. novembril 73 poolthääle, kahe vastuhääle ning ühe erapooletu häälega vastu elektroonilise side seaduse, ehitusseadustiku ja riigilõivuseaduse muutmise seaduse (437 SE). 6. detsembril kuulutas President Alar Karis seadusemuudatuse välja.

Seadusega võetakse üle Euroopa elektroonilise side seadustik (Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1972) ning täpsustakse nõudeid sidevõrkude riist- ja tarkvara kasutamisele, et nende kasutamine ei ohustaks riigi julgeolekut. Muudatuse tulemusena on võimalik vastu võtta Vabariigi Valitsuse määrusi muutev määrus, millega mh täpsustatakse sideettevõtjatele sidevõrgus kasutatavast riist- ja tarkvarast teavitamiskohustuse, kasutusloa kohustuse ja auditeerimiskohustuse sisu ja korda. Seaduste ja määruste muudatused on kavandatud jõustuma 2022. a 1. veebruaril.

Võrgu- ja infosüsteemide turbe direktiiv (NIS2) jõudis EL Nõukogusse

23. novembril jõudis EL alaliste esindajate komitee COREPER (liikmesriikide alalistest esindajatest, reeglina suursaadikutest või nende asetäitjatest koosnevad komiteed) kokkuleppele NIS2 (võrgu- ja infosüsteemide turbe direktiiv) ühise lähenemise suhtes ning eelnõu saadeti kinnitamisele ka EL Nõukogusse.

Edasi algavad arutelud juba Euroopa Parlamendis. Ettepanekud varasema õigusakti (NIS1) muutmiseks esitas Euroopa Komisjon juba möödunud aasta detsembris. NIS2 direktiivi eesmärk on tõsta üldist küberturvalisuse taset EL riikides ja ühtlustada ka seonduvaid seadusi. Kuna küberturvalisuse tase on riigiti väga erinev, samuti nägemused olukorra parandamiseks, möödusid läbirääkimised üsna pingelises õhustikus ning kompromissini jõudmine võttis aega.

Suurimad takistused edasiminekul olid direktiivi ulatusala (nt ei soovinud mitmed liikmesriigid hõlmata avalikku sektorit), kriteeriumid (nn suuruse reegel, mille kohaselt haaratakse ulatusalasse ettevõtted 50 või enama töötajaga), erinevate EL õigusaktide jurisdiktsiooni ühtlustamine, intsidentidest teavitamine (välja jäeti nt kohustuslike ohuteadete edastamine), jne. Kuigi Eesti pooldas kohati ambitsioonikamat lähenemist, võib tulemust pidada üsna heas tasakaalus liikmesriikide kompromissiks, mis aitab kindlasti kaasa ka küberturvalisuse baastaseme tagamisele Eestis. Edasised läbirääkimised Euroopa Parlamendis jõuavad eeldatavasti lõpule Prantsusmaa eesistumise ajal.

Ettevõtlus- ja infotehnoloogiaminister Andres Sutt osales 3. detsembril Euroopa Liidu telekommunikatsiooniministrite kohtumisel Brüsselis

„NIS2 puhul on tegu EL kõige olulisema küberturvalisust puudutava õigusaktiga, mis on aluseks kõikide liikmesriikide küberturvalisuse

seadustele. Selle fookus on kriitilise taristu küberturvalisuse tõstmine ning liikmesriikide vaheline koostöö küberturbe valdkonnas. Meie IT-süsteemide ja -teenuste terviklikkus ja toimimine sõltub suuresti kehtivast seadusandlusest. Kuigi ka olemasolev NIS-direktiiv oli küberjulgeoleku vallas ülemaailmne teerajaja, on küberohupildi muutus ning pandeemia toonud esile vajaduse seda ajakohastada," selgitas Sutt. Eesti on kehtiva NIS-direktiivi üle võtnud küberturvalisuse seadusega, mida tuleb uuendatud direktiivi jõustumisel täiendada.

Eesti toetab EL-is üldise lähenemisviisi vastuvõtmist. NIS direktiiv aitab parandada kriitilise taristu ning teiste oluliste teenuste toimepidevust ja loob EL-is ühtsemad tingimused turvanõuete ja intsidenditest teavitamise jaoks. Samuti parandab see piiriülest koostööd — läbi intsidentidele reageerimise, kerksuse parandamise ning järelevalve tõhustamise ettevõtete ja pädevate asutuste vahel. Kehtiva direktiiviga võrreldes on eelnõu kohaldamisalas mitmed uued sektorid, mille kriitilisus või olulisus ühiskonna jaoks ilmnes peamiselt pandeemia kontekstis.

Eesti seisukohad EL ühise küberüksuse (Joint Cyber Unit) osas

Vabariigi Valitsus kiitis 18.11.2021 istungil heaks EE seisukohad komisjoni soovitused EL ühise küberüksuse loomise osas:

1. Eesti toetab ühise küberüksuse algatuse eesmärki arendada Euroopa Liidu kriisihalduse raamistikku. Oluline on tagada liikmesriikide ja asjaomaste liidu asutuste olukorrateadlikkus ning koordineeritud vastus suuremahuliste küberintsidentide ja -kriiside korral ning neist taastumine.

2. Leiame, et enne ühise küberüksuse loomisega edasi liikumist tuleb tuvastada Euroopa Liidu kriisihalduse võimelüngad, sealhulgas probleemid küberkriiside halduses. Peame oluliseks, et küberkriiside haldamisel kasutataks maksimaalselt ära juba olemasolevaid liidu teabevahetus ja operatiivkoostöö platvorme, vältimaks asjatut dubleerimist.

3. Toetame Euroopa Komisjoni plaani luua ühise küberüksuse raames liikmesriikide ekspertidest koosnevad Euroopa Liidu küberturvalisuse kiirreageerimisrühmad, mida oleks võimalik kriisi korral abi vajavasse liikmesriiki saata. Nimetatud kiirreageerimisüksuste täpsemad funktsioonid ning mandaat peaksid samas olema õiguslikult reguleeritud. Arvestada tuleb olemasolevate koostöövormidega nagu alalise struktureeritud koostöö formaadis loodud küberkiirreageerimise tiim.

4. Toetame kavatsust laiendada ühise küberüksuse raames tehtavat koostööd ka

erasektori huvirühmadele, sh küberturvalisuse lahenduste ja teenuste kasutajatele ja pakkujatele. Peame seejuures oluliseks koostöö ja kaasamise põhimõtete selgemat kindlaksmääramist.

Komisjoni president Ursula von der Leyen avalikustas ühise küberüksuse idee oma poliitilistes suunistes juba 2019. aasta juulis ning see on olulisel kohal ka 2020. aasta digistrateegias ja 2020. aasta detsembris avaldatud EL küberturvalisuse strateegias, kus üksust kirjeldatakse Euroopa tulevase küberturvalisuse kriisireguleerimise raamistiku olulise komponendina. Soovitusel on ühisosa ka Eesti Digiühiskond 2030 arengukavaga, mis hõlmab ka küberturvalisuse suunda. Üksus on mõeldud toimima ühise platvormina, tagamaks liikmesriikide kooskõlastatud reageerimine ulatuslikele küberinitsidentidele, mis mõjutavad avalikke teenuseid, samuti ettevõtteid ja kodanike elu kogu Euroopa Liidus. Hetkel on liikmesriikidel ja ka Euroopa Liidu käsutuses palju analoogseid üksusi, mis on seotud eri valdkondade ja sektoritega. Viimasest koorub välja ka liikmesriikide peamine kriitika ettepaneku osas — loodava küberüksuse ülesannete dubleerimine teiste EL agentuuride juba tehtava tööga. Kuna arvamusi on palju, on läbirääkimised hetkel veel üsna algusjärgus.

Kõrgemad Küberkaitse ja Digiriigi kursused

24.-26. novembril leidsid aset peale 2-aastast pausi järjekorras neljandad Kõrgemad Küberkaitse ja Digiriigi kursused (KÜDI).

Pildid Kõrgematelt Küberjulgeoleku ja Digiriigi kursustelt. Fotograaf: Aron Urb.

Sündmus leidis aset Roosta puhkekeskuses ja tõi kokku 30 osalejat riigisektorist, akadeemiast, ajakirjandusest ja erasektorist. Kolmepäevasel intensiivsel kursusel pidasid loenguid ja juhtisid arutelusid oma ala absoluutsed tipud, teemadel mis ulatusid küberkuritegevusest e-ID tulevikuni, globaalsetest küberohtudest privaatsuse kontseptsiooni arenguteni õiguses.

Kursuse avas ettevõtlus- ja infotehnoloogiaminister Andres Sutt ning sellel võtsid sõna teiste hulgas õiguskantsler Ülle Madise, Cybernetica juht Oliver Väärtnõu, CERT-EE juht Tõnu Tammer, Ericsson Eesti juht Andrus Durejko ja paljud teised.

KÜDI korraldas Majandus- ja kommunikatsiooniministeerium koostöös Rahvusvahelise kaitseuuringute keskusega, üritus toimus Euroopa Liidu struktuuritoetuse toetusskeemist "Infoühiskonna teadlikkuse tõstmine", mida viib ellu Riigi Infosüsteemi Amet ja rahastab Euroopa Regionaalarengu Fond. Üritust aitas korraldada Publicon OÜ.

Küberturvalisuse seaduse muudatusi käsitlev infotund ETO-dele

15. detsembril leiab aset virtuaalne infotund elutähtsate teenuste osutajatele ning teistele küberturvalisuse seaduses määratud teenuse osutajatele, et tutvustada planeeritavaid muudatusi seadusesse. Fookuses on Eesti infoturbestandardi (E-ITS) kehtestamine ning sellega seonduvad küsimused. Infotunni korraldab Majandus- ja kommunikatsiooniministeerium koostöös Riigi infosüsteemi ametiga. Uue infoturbestandardiga saab tutvuda veebis aadressil eits.ria.ee.

TalTechi küberkriminalistika ja küberjulgeoleku keskusel täitus seitsmes tegutsemisaasta

12. novembril tähistas TalTechi küberkriminalistika ja küberjulgeoleku keskus seitsmendat sünnipäeva.

Keskus asutati konverentsil CyberCrime 2014 eesmärgiga tõsta Eesti küberjulgeoleku kompetentsi ja võimekust läbi haridus-, teadus- ja arendustegevuse. Asutajateks olid Tallinna Tehnikaülikool, Siseministeerium, Justiitsministeerium, Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium, Politsei- ja Piirivalveamet, Eesti Kohtuekspertiisi Instituut ja Riigi Infosüsteemi Amet.

Täna kuulub keskuse multidistsiplinaarsesse ja rahvusvahelisse meeskonda 23 teadlast, doktoranti, eksperti ja spetsialisti, nende hulgas kuus professorit ja kaasatud professorit. Lisaks on keskusega seotud üheksa tööstusdoktoranti. Keskus kuulub tehnikaülikooli tarkvarateaduse instituudi koosseisu ning koordineerib TalTechi ja Tartu Ülikooli ühist küberkaitse magistriõppekava.

Käimas on mitmeid mahukaid projekte, nende hulgas koostöö Euroopa küberkaitse keskuste võrgustiku ning innovatsiooni ja operatsioonide kompetentsikeskuse (ECHO) ja merenduse küberjulgeoleku keskuse loomisel (MariCybERA). Lisaks toimub palju tegevusi õppuste läbiviimisel ning küberkaitse teadlikkuse tõstmise, hariduse ja järelkasvu vallas.

Keskuse kohta saab lähemalt lugeda kodulehel.

8.12 toimub veebikonverents ja uue õppematerjali tuvustus teemal “Naised küberturbes — eeskujud tüdrukutele”

Eestis on palju tublisid naisi, kes tegutsevad IT ja küberturbe valdkonnas. Konverentsil ja õppematerjalides saame nende naistega tuttavaks. Saame teada, milline on olnud nende teekond IT valdkonnas, kuidas neil on läinud ja millest nad unistavad, millised on nende arvates naiste tugevused IT valdkonnas.

“Naised küberturbes - eeskujud tüdrukutele” e-raamat on valminud vajadusest tuua esile tublid naised IT- ja küberturbesektorist, kuid pakkuda ka võimalusi mõista, millised on võimalused küberturbe ja IT-ga tegelema hakkamisel ning millised on karjäärivõimalused. Samas näidata ka asja inimlikumat poolt - jagada muresid ja kahtluseid ning oskust nendest üle saada. Õppematerjalid asuvad siin.

Projekti viib ellu TalTech. Toetavad Startup Estonia, Kredex, Kaitseministeerium ja Haridus- ja Noorteamet.

8.12 toimub suurim Eesti noorte algajate kübervõistlus KüberPuuring

KüberPuuring võistluse lõppvoorus osalevad tiimid 94 koolist. Iga kool võis esitada kuni 2 poiste ja 2 tüdrukute võistkonda, keda kokku tuli 205 tükki.

Projekti viib ellu TalTech. Peatoetaja on Kaitseministeerium ja Targalt Internetis projekt koos Euroopa Liiduga.

Võistluse ülesanded lõid ja viisid ellu Cyber Moon, Aegrelee ja Forwardspace, kelle taha peituvad KüberNaaskli võistluse talendid ja treenerid.

Cybernetica

Cybernetica ja TalTech asuvad koostöös uurima tuleviku digiallkirju

Cybernetica ning Tallinna Tehnikaülikool kaasjuhendavad tööstusdoktorantuuri õppekohta, mille tulemusena valmib teadustöö, mis uurib uusi turvalisi digiallkirjastamise viise. Teadustöö aitab arendada uusi tehnoloogiaid, mis on sarnased näiteks Smart-ID teenuses kasutusel olevale Cybernetica loodud SplitKey lahendusele. Samuti on töö osaks digiallkirjade vastupidavus kvantarvutitele tulevikus.

Cybernetica teadusdirektor Dan Bogdanov ütles, et kuigi tänane digiallkiri on krüptograafiliselt tugev, siis tasub tulevikku vaadata ning valmistuda näiteks kvantarvutitega kaasa tulevate muutuste tarbeks tulevikus. "Kvantarvutid täna veel ei ohusta seda krüptograafiat, mida kasutatakse Eesti digitaalse identiteedi tarbeks. Siiski meie põhimõte on alati olnud arendada tulevikku vaatavaid tehnoloogiad. Krüptograafilised võtmed on iga süsteemi turvalisuse eelduseks ja SplitKey stiilis võtmete kaitse krüptograafiliste lahendustega on kiiresti arenev valdkond," selgitas Bogdanov.

Professor Rain Ottis TalTechi küberkriminalistika ja küberjulgeoleku keskusest märkis, et tööstusdoktorantuuril on otsene positiivne mõju nii Eesti teadus-, kui ka ettevõtlusmaastikule. "Ühelt poolt saavad teadlased pead murda meie majanduse ja laiemalt ühiskonna probleemide kallal ning teiselt poolt kasvab Eestis teadusmahukat ja kõrget lisandväärtust pakkuvate ettevõtete võime ka globaalsel turul läbi lüüa," täpsustas Ottis.

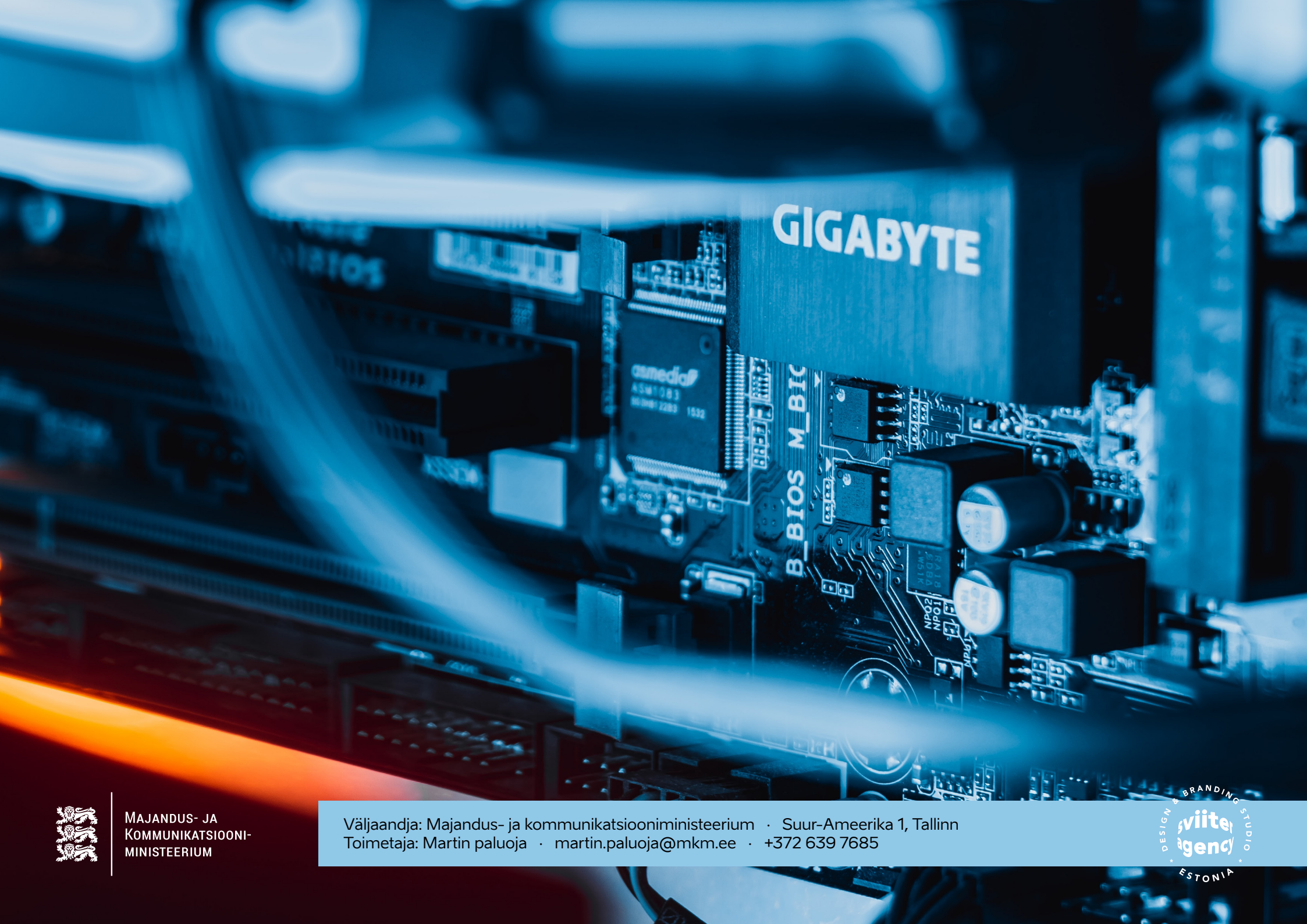
Doktoritöö juhendajateks on Tallinna Tehnikaülikooli professor Ahto Buldas ning Cybernetica vanemteadur Jan Willemson.

Tartu Ülikool

Teine CHAISE uudiskiri annab ülevaate plokiahela tehnoloogia tööturu hetkeseisust Euroopas

Erasmus+ kaudu rahastatud valdkondlike oskuste ühendus CHAISE on välja andnud oma teise uudiskirja, kust saab ülevaate kui paljud inimesed valdavad Euroopa tööturul plokiahela tehnoloogiatega töötamiseks vajalikke oskusi ja milliste tehnoloogiate tundmist hindavad nüüdisajal tööandjad.

CHAISE peamine ülesanne on välja töötada Euroopa plokiahela tehnoloogia oskuste arendamise strateegia ja pakkuda tulevikku suunatud koolitusi, mis parandavad plokiahel tehnoloogiaga seotud oskusi, et kindlustada Euroopale selle valdkonna spetsialistide olemasolu praegu ja tulevikus.



Majandus- ja Kommunikatsiooni-
ministeerium

Väljaandja: Majandus- ja kommunikatsiooniministeerium · Suur-Ameerika 1, Tallinn
Toimetaja: Martin paluoja · martin.paluoja@mkm.ee · +372 639 7685

Design & Branding Studio Estonia