Projekti number: 2020-1-LT01-KA203-078070

O1-A2: Tulemused "Olemasolevate küberturvalisuse koolitusprogrammide analüüs"

RAPORT

2021

Partnerid

Vilnius University, Lithuania

Website: http://www.vu.lt

University of Tartu

Website: https://www.ut.ee/et

MECB - Macdac Engineering Consultancy Bureau LTD , Malta

Website: http://www.mecb.com.mt/eu

Altacom SIA, Latvia

Website: https://www.altacom.eu/

DOREA Educational Institute, Cyprus

Website: https://dorea.org/

ECDL- Information Technologies Institute, Lithuania

Website: http://www.ecdl.lt/

Co-funded by the Erasmus+ Programme of the European Union

Sisukord

Tabelite loend

Co-funded by the Erasmus+ Programme of the European Union

Lühendite loend

CCS	Cyprus computer society
CERT.LV	Latvian Computer Emergency Response Team
CSSS	Cybersecurity skills shortage
ESCO	European Cybersecurity Organisation
ENISA	European Union Agency for Cybersecurity
EU	European union
HITSA	Information Technology Foundation for Education
ISACA	Information Systems Audit and Control Association (ISACA)
ISC2	International Information System Security Certification Consortium
NCSC	National Cybersecurity Centre at the Ministry of National Defence (the Republic of Lithuania)
NCSS	National cybersecurity strategies
OCECPR	Office of Commissioner of Electronic Communication & Postal Regulation (the Republic of Cyprus)
RIA	Information System Authority (the Republic of Estonia)
SMEs	Small and medium enterprises

Co-funded by the Erasmus+ Programme of the European Union

1. SISSEJUHATUS

1.1. Küberturvalisuse oskuste puudus ja puudujäägi põhjused

Enterprise Strategy Group and the Information Systems Security Association[1] turbeühingu 2019. aastal läbi viidud iga-aastase ülemaailmse uuringu põhjal on küberturvalisuse oskuste puudus mõjutanud 74% organisatsioonidest kogu maailmas. Aruandes nimetatud puudujäägi peamisteks tagajärgedeks on suurenenud töökoormus olemasoleval personalil, suutmatus mõnda turvatehnoloogiat kasutada ning nooremate töötajate värbamine ja koolitamine kogenumate spetsialistide palkamise asemel. Kõige kriitilisemad oskuste puudujäägid on pilvandmetöötluse turvalisus (33%), rakenduste turvalisus (32%) ning turvalisuse analüüs ja uurimine (30%).

Lisaks sellele oli Information Systems Audit and Control Association (ISACA)[2] poolt 2019. aastal läbi viidud uuringute kohaselt 57% organisatsioonidest täitmata küberturvalisuse ametikohti. Nende ametikohtade täitmiseks kulus tavaliselt kolm kuud, millele vastas rohkem kui 60% uuringus osalenutest. Suurem osa täitmata töökohtadest on individuaalsete kaastöötajate (nii tehnilise kui ka mittetehnilise küberturvalisuse) ja küberturvalisuse juhi ametikohad. Eeldatavasti kasvab lähiaastatel nõudlus veelgi individuaalse kaastöötajate (tehnilise küberjulgeoleku) valdkonna spetsialistide järele. Seevastu ennustatakse, et üldine töökohtade arv jääb samaks või suureneb ainult veidi.

Üheks peamiseks põhjuseks, mille vastajad on välja toonud, miks ametikohad jäävad täitmata, on kvalifitseeritud kandidaatide puudumine. Ligi kolmandik organisatsioonidest väitis, et umbes 75% kandidaatidest ei oma selleks ametiks vajalikku kvalifikatsiooni. Kõige olulisemad oskuste puudujäägid, millele vastajad viitasid, olid sotsiaalsete oskuste, IT-teadmiste puudumine, ebapiisav ülevaade ettevõtlusest, küberturvalisuse tehnilise kogemuse ja praktiliste oskuste puudus.

ENISA[3] tuvastas konsultatsioonide kõigus, et küberturvalisuse alase teadlikkuse ja oskuste puudujääk elanikkonnas on turvalisuse küberruumi rajamise peamiste takistuste hulgas. "Hoolimata ligi 600 akadeemilise asutuse ja koolituskeskuse olemasolust, mis pakuvad küberturvalisuse programme kogu Euroopas, on küberturvalisuse oskuste lõhe kõigis sektorites endiselt märkimisväärne väljakutse" (ENISA, 2019, lk 10).

Aastal 2020 oli küberjulgeoleku tööjõu hinnanguline ülemaailmne puudus umbes 3,12 miljonit spetsialisti[4]. Seevastu ainuüksi Euroopas on küberjulgeoleku tööjõu puudus aastaks 2022 hinnanguliselt 350 000 töötajat. 2018 aastaga võrreldes on puudujäägi hinnang kahekordistunud[5].

Küberturvalisuse oskuste puudujäägi (CSSS) põhjused

ENISA on oma aruandes "Küberjulgeoleku oskuste arendamine ELis" toonud välja neli peamist põhjust, mis võivad aidata kaasa küberturvalisuse oskuste puudusele. Kaks neist on keskendunud töökoha probleemidele, ülejäänud kaks on seotud hariduse ja koolituse probleemidega. Täpsemalt:

1. *Küberjulgeoleku tööturg on suhteliselt ebaküps ja dünaamiline* - mille tulemusena sõltuvad töö spetsifikatsioonid suuresti organisatsiooni suurusest ja sektorist. Näiteks kipuvad VKEd, kes ei ole spetsialiseerunud küberturvalisusele, palkama üldisi IT-töötajaid, kellel on üldised

[1] Jon Oltsik (2019): The Life and Times of Cybersecurity Professionals 2018, URL https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/surveys/esg-issa-2018-survey-results.pdf (külastatud 09/03/2021)

[2] ISACA (2020): State of Cybersecurity 2020 Part 1: Global Update on Workforce Efforts and Resources, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf (külastatud 09/03/2021)

[3] ENISA (2019): Cybersecurity skills development in the EU, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf (külastatud 09/03/2021)

[4] (ISC)² (2019): (ISC)² Study Reveals the Cybersecurity Workforce Has Grown to 3.5 Million Professionals Globally, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study-Reveals-the-Cybersecurity-Workforce-Has-Grown-Globally (külastatud 09/03/2021)

[5] (ISC)² (2019): Cybersecurity workforce study, URL https://www.isc2.org/Research/Workforce-Study (külastatud 09/03/2021)

Co-funded by the Erasmus+ Programme of the European Union

küberturvalisuse alased teadmised. Seevastu suuremates ja küberturvalisusele spetsialiseerunud VKE-des on töötajad keskendunud konkreetsetele küberturvalisuse teemadele.

2. *Tööandjad ei paku õiget koolitustaset* - mis takistab karjäärimudeli tekkimist kui ka praeguste töötajate professionaalset arengut. See loob üldisema taustaga küberturvalisuse spetsialistidele takistusi vajalike eriala oskuste edasiarendamiseks.
3. *Akadeemilised asutused ei suuda pakkuda vajalike teadmiste ja oskustega kandidaate.* - Tihti puudub õpilastel praktiline erialane kogemus, mille tulemuseks on oskuste mittevastavus tööstuse vajaduste ja õpilaste koolist saadud oskuste vahel.
4. *Küberturvalisuse õppekavad reageerivad valdkonna arengutega aeglaselt.* - Bürokraatia tõttu on küberturvalisuse õppekavad seni olnud hädas uute ohtude õpetamisel ja nende ohtudega toimetulemiseks vajalike praktiliste oskuste lisamisega õppekavadesse.

1.2. Informaatika ja küberturvalisuse hariduspoliitika ELis

2013. aastal avaldas Euroopa Komisjon oma esimese küberturvalisuse strateegia, tuues strateegiliste põhieesmärkidena esile teadlikkuse tõstmise ja oskuste arendamise.

*"*2017. aastal teatasid Euroopa Komisjon ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja taas, et küberturvalisusel on tugev hariduslik mõõde ja tõhus küberturvalisus sõltub suuresti valdkonna inimeste oskustest. Nad soovitasid ELil koos liikmesriikidega parandada küberturvalisuse alast haridust ja oskusi, tuginedes digitaalsete oskuste ja töökohtade koalitsiooni tööle ning asutades Euroopa küberturvalisuse tööstus-, tehnoloogia- ja teadustöö kompetentsikeskuse ning riiklike küberturvalisuse koordineerimiskeskuste võrgustiku" (ENISA, 2019, p.23)

2019 aastal loodi 4 projekti Horizon 2020 programmi raames — CONCORDIA, ECHO, SPARTA ja CyberSec4Europe[6] — mille eesmärk oli välja töötada ühine Euroopa küberturvalisuse kompetentsivõrgustik ning Euroopa küberturvalisuse teadusuuringute ja innovatsiooni tegevuskava.

2020. aastal tegi Euroopa Komisjon ettepaneku Digital Europe Programme[7], mis on ELi programm Euroopa digitaalse ümberkujundamise kiirendamiseks. Eeldatavasti eraldatakse programmist 580 miljonit eurot kõrgemate digitaalsete oskuste arendamiseks, toetades tulevaste ekspertide jaoks spetsiaalsete õppekavade, praktikakohtade väljatöötamist ja läbiviimist olulisemates uutes valdkondades nagu tehisintellekt, küberturvalisus, kvantarvutused jne.

2021. aasta märtsis võttis Euroopa Ülemkogu vastu uued järeldused ELi küberturvalisuse strateegia kohta[8]. Järeldustes tunnistatakse digitaalsete ja küberturvalisuse oskuste nappust tööjõus ning rõhutatakse vajadust rahuldada turunõudlust haridus- ja koolitusprogrammide edasiarendamise kaudu.

[6] European Commission (2019): Four EU pilot projects launched to prepare the European Cybersecurity Competence Network, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network (külastatud 10/03/2021)

[7] European Commission (2020): Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027 (külastatud 10/03/2021)

[8] Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy (külastatud 24/03/2021)

Co-funded by the Erasmus+ Programme of the European Union

1.3. Riiklikud küberturvalisuse strateegiad (NCSS)

Alates 2017. aastast on kõik ELi liikmesriigid välja töötanud ja avaldanud oma riiklikud küberturvalisuse strateegiad (NCSS).

Küpros

Küprose Vabariik on teadlik küberhariduse tähtsusest riikliku küberruumi kaitse tagamisel. Üks praeguse küberturvalisuse strateegia põhieesmärke on edendada küberturvalisust ja tõsta avalikkuse (kodanike, tööjõu ja noorte) teadlikkust valdkonnast ning luua strateegia elluviimiseks koostöö õhkkond.

Küprose Vabariigi küberturvalisuse strateegia võeti kasutusele 2012. aastal[9]. Küprose riikliku strateegia eesmärk on arendada küberruumi turvapiirkonnas tehnilist koolitust ning õpetada, kuidas ennast kaitsta ja kiireloomulistes olukordades toime tulla. Üks eesmärkidest on ehitada spetsialiseeritud tööjõud, mis suudaks tegeleda tõelise küberrünnakuga. Selleks korraldati õppused jälgimaks tööjõu toimetulekut simuleeritud realistlikus kriisis. Strateegia elluviimise tulemuseks peaks olema küberteenustega seotud ametijuhendite ja tunnistuste jõustamine.

Strateegia koosneb 17 konkreetsest tegevusest. Need meetmed hõlmavad olemasolevate asjakohaste personali koolitusprogrammide ja sertifikaatide kindlakstegemist küber- ja digitaalse turvalisuse valdkonnas.

Küprose Vabariik on pühendunud ka avaliku ja erasektori partnerluste loomisele, et toetada kõrgharidusasutusi, lisades küberturvalisuse õppeaineid ning tugevdades küberjulgeoleku valdkonna spetsialistide ja akadeemilise personali koolitusi.

Riikliku küberturvalisuse dokumendi uusim versioon töötati välja 2020. aastal. Strateegia on praegu läbivaatamisel ja ootab kommunikatsiooniministeeriumi ja ministrite nõukogu lõplikku heakskiitu.

Digital Security Authority (DSA)[10] on sõltumatu valitsusasutus, mis allub elektroonilise side ja postiteenuste voliniku järelevalve alla. Ta vastutab Euroopa võrgu- ja infoturbe direktiivi rakendamise eest, keskendudes Küprose kõigi põhiteenuste ja esmatähtsate infoinfrastruktuuride operaatorite küberturvalisuse ajakohastamisele ja säilitamisele. Agentuuri eesmärk on ka suurendada küberturvalisuse alast teadlikkust ühiskonnas ja suurendada Küprose rahvusvahelist konkurentsivõimet üldiselt.

Teine oluline organisatsioon on Küprose arvutiselts (CCS)[11], iseseisev mittetulundusühing, mis asutati 1984. aastal Küprose IT-sektori arendamiseks, täiendamiseks ja edendamiseks. CCS püüab seada tööstuse spetsialistide seas kõrged standardid, tunnistades info- ja sidetehnoloogia (IKT) mõju tööhõivele, ettevõtlusele, ühiskonnale ja kodanike elukvaliteedile. Üks CCSi korraldatavatest iga-aastastest üritustest on küberturvalisuse väljakutse[12]. Ürituse eesmärk on avastada andekaid spetsialiste ja motiveerida noori tegema küberturvalisuses karjääri.

[9] OCECPR (2012): Cybersecurity Strategy of the Republic of Cyprus , URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus (külastatud 11/03/2021)

[10] Digital Security Authority (DSA), URL https://dsa.cy/en/

[11] Cyprus computer society (CCS), URL https://ccs.org.cy/en/

[12] [12] Cyprus cyber security challenge, URL https://ccsc.org.cy/#home

Co-funded by the Erasmus+ Programme of the European Union

Eesti

Eesti oli üks küberturvalisuse strateegiate avaldamise eestvedajatest ja praegu on riikliku küberturvalisuse dokumendi kolmas versioon[13]. Strateegia on jagatud neljaks valdkonnaks: 1. jätkusuutlik digitaalne ühiskond; 2. ettevõtlus ning teadus- ja arendustegevus; 3. rahvusvahelised suhted; 4. Küberoskuslik ühiskond.

Eesti strateegia toetab küberhariduse eelis-edendamist ja selle rakendatavust on kirjeldatud plaani teisel eesmärgil. Alates 2014. aastast on riik investeerinud haridusse ja tegeleb ülikoolidega, et edendada küberuuringuid, rahastada projekte ja toetada stipendiume. Eesmärk on tagada nii riigi kui avaliku sektori jaoks vajalik kübervaldkonna tööjõud, arendades selleks andekaid noori nii formaalhariduses kui koolivälise tegevuste kaudu ning koolitada tööturu nõudlustele vastavuses küberturvalisuse spetsialiste.

Haridus- ja Teadusministeerium arvestab küberturvalisuse strateegia eesmärkides kokku lepitud prioriteetidega elukestva õppe strateegia tegevuste planeerimises, toetades kõigi haridustasemete lõpetajatele baasteadmiste omandamist küberohtudega toimetulekuks. Haridus- ja Teadusministeeriumi haldusalas toetab küberturvalisuse strateegia eesmärkide täitmist Hariduse Infotehnoloogia Sihtasutus (HITSA), mis aitab kaasa valdkonna spetsialistide ettevalmistamisele nii Targalt Interentis programmi kui IT Akadeemia programmi koordineerimise kaudu.

Majandus- ja Kommunikatsiooniministeerium juhib ja koordineerib küberturvalisuse strateegia koostamist ja elluviimist osana infoühiskonna arengukava tervikpildist ning koostöös Riigi Infosüsteemi Ametiga (RIA)[14] omab keskset rolli tehnoloogilise vastupanuvõime, kriiside ja intsidentide halduse ning küberturbe sektori ettevõtluse arendamise ning teadus- ja arendustegevuse suunamisega seotud tegevustes. Sealjuures on Riigi Infosüsteemi Ameti ülesanded küberturvalisuse valdkonnas laiapindsed, hõlmates kõikide riigi toimimiseks oluliste võrgu- ja infosüsteemide turvalisuse tagamist seadusest tulenevate eranditega.

"Käivitatakse laiamahulised ennetus- ja teadlikkusekampaaniad küberohtude teadvustamiseks erinevatele sihtrühmadele, sealjuures ettevõtjatele. Luuaks formaat teadlikkuse kasvatamisega seonduvate tegevuste koordineerimiseks Eestis ning koondatakse ennetustegevusi puudutav info arusaadaval ja avalikkusele kättesaadaval kujul ühte kohta. Riigiasutuste küberhügieeni taseme tõstmiseks muudetakse kohustuslikuks riigiasutuste ja KOVide töötajatele küberturvalisust puudutavate testide läbiviimine. Jätkatakse sihtrühmade koolituste ning teavitustegevustega". (The Republic of Estonia, Ministry of Economic Affairs and Communication, 2019, p. 64).

Läti

Lätis on mure riikliku julgeoleku pärast seotud tehnoloogilise arenguga. Läti esimene küberturvalisuse strateegia jõustus 2014. aastal, kava kiideti heaks perioodiks 2014 – 2018. Aastal 2019 kinnitati uus küberturvalisuse strateegia aastateks 2019–2022. Uuendatud strateegia eesmärk on tugevdada ja parandada Läti küberturvalisuse võimekust, suurendades üldsuse teadlikkust ja vastupidavust küberrünnakute vastu. Nende eesmärkide saavutamiseks pakutakse strateegias meetmeid kuues valdkonnas[15]:

1. suurem küberturvalisus ja hallatavad digitaalsed turvariskid;
2. IKT-süsteemide vastupidavus;
3. parem üldine juurdepääs strateegilistele IKT-süsteemidele ja -teenustele;
4. ühiskonna teadlikkus, haridus ja teadusuuringud;
5. rahvusvaheline koostöö;

[13] Republic of Estonia, Ministry of Economic Affairs and Communication (2019): Cybersecurity Strategy, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf (külastatud 10/03/2021)

[14] Information System Authority (RIA), URL https://www.ria.ee/en.html

[15] Latvian Defence Ministry (2019): Latvia approves new Cyber Security Strategy 2019-2022, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022 (külastatud 11/03/2021)

Co-funded by the Erasmus+ Programme of the European Union

6. õigusriik küberruumis ja küberkuritegevuse ennetamine.

Ühiskonna teadlikkuse, hariduse ja teadusuuringute valdkonnas on strateegias välja toodud viis peamist eesmärki[16]:

- toetada küberturvalisuse alaseid teadusuuringuid;
- tõsta õppijate ja koolitajate teadlikkust infoturbest, privaatsuse kaitsest ja usaldusväärsete e-teenuste kasutamisest;
- tugevdada ühiskonna teadlikkust Interneti turvalisest kasutamisest (töötada välja eri vanuserühmadele mõeldud ohutusalaste soovituste, Interneti-alaste tegevuste, sotsiaalkampaaniate korraldamise haridus- ja informatiivsed materjalid). Töötada välja ja rakendada iga-aastane töö ja tegevuskava ettevõtete küberturvalisuse küsimustes teabe ja teadlikkuse suurendamiseks.;
- edendada kohalike ja riiklike institutsioonide töötajate teadlikkust IKT ohutust kasutamisest;
- edendada küberturvalisuse alaseid haridustegevusi ja võistlusi..

Strateegias rõhutatakse ka avaliku ja erasektori osalejate parema kaasamise vajadust küberturvalisuse süsteemide vastupidavuse tugevdamiseks ning investeeringute tegemiseks IKT turvalisusse ja töötajate koolitusse.

Küberturvalisuse juhtumite jälgimise ja käitlemise eest vastutab Läti arvuti hädaolukorra lahendamise meeskond (CERT.LV). CERT.LV korraldab ka avalikkusele harivaid üritusi ja koolituskursusi. Uue strateegia kohaselt peaks CERT.LV arendama koos avaliku- ja erasektoriga vahendid küberintsidentide kohta teabe kogumiseks analüüsimiseks ja hindamiseks[17].

Teine oluline organisatsioon on Läti turvalisema Interneti keskus. Selle põhiülesanded on harida, teavitada ja suurendada üldsuse teadlikkust Interneti turvalisemast kasutamisest, luua platvorm ebaseadusliku sisu ja turvarikkumistest teavitamiseks veebist vihjeliinile ning pakkuda oma abitelefoni kaudu professionaalseid psühholoogide konsultatsioone[18].

Leedu

2018. aastal kiitis valitsus heaks Leedu Leedu Vabariigi riikliku küberturvalisuse strateegia [19].

"Strateegia peamine eesmärk on anda Leedu ühiskonnale võimalus kasutada ära info- ja kommunikatsioonitehnoloogia (IKT) potentsiaali, tuvastades küberintsidente tõhusalt, ennetades nende toimumist ja levikut ning haldades küberintsidentidest tulenevaid tagajärgi." Resolutsioon riikliku küberturvalisuse strateegia heakskiitmise kohta, 13 August 2018 No. 818

Eesmärgi saavutamiseks pakutakse strateegias välja viis eesmärki:

1. tugevdada riigi küberturvalisust ja küberkaitsevõime arendamist;
2. tagada küberruumis kuritegude ennetamine ja uurimine;
3. edendada küberturvalisuse kultuuri ja innovatsiooni arendamist;
4. tugevdada tihedat koostööd era- ja avaliku sektori vahel;
5. tõhustada rahvusvahelist koostööd ja tagada rahvusvaheliste kohustuste täitmine küberjulgeoleku valdkonnas.

[16] Latvian Defence Ministry (2019): Latvia's cyber security strategy for 2019 – 2022, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf (külastatud 11/03/2021)

[17] Cyber Wiser (2021): Education and training in national cybersecurity strategy, URL https://www.cyberwiser.eu/latvia-lv (külastatud 11/03/2021)

[18] ENISA, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Latvia

[19] Government of the Republic Of Lithuania (2018): Resolution on the approval of the national cyber security strategy, URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf

Co-funded by the Erasmus+ Programme of the European Union

Küberturvalisuse kultuuri ja innovatsiooni edendamine on riikliku strateegia põhieesmärk. Strateegias pakutakse välja järgmised tegevused eesmärkide saavutamiseks [20]:

- pidevad ja regulaarselt ajakohastatud koolitused era- ja avaliku sektori töötajatele, mille eesmärk on suurendada töötajate teadlikkust ja kujundada üldist küberturvalisuse kultuuri;
- viimaste küberintsidentide kohta järjepidev teabe levitamine;
- muuta IKT-haridus varakult haridusprotsesside osaks, alates lasteaiast kuni keskkoolini;
- õpetajate pidev täiendus ja koolitus küberturvalisuse alase kvalifikatsiooni tõstmiseks.

Strateegias rõhutatakse vajadust arendada küberturvalisuse oskusi ja pädevusi, et turu vajadusi pidevalt rahuldada. Selle eesmärgi saavutamiseks tehakse strateegias ettepanek „luua küberturvalisuse kompetentsimudel ja standardid, töötada välja tööturu vajadustele orienteeritud koolitussüsteemid, akrediteerimine ja sertifitseerimine, pakkuda küberturvalisuse koolitus- ja testimiskeskkondi, pakkuda IKT töötajatele koolitust jne". Resolutsioon riikliku küberturvalisuse strateegia heakskiitmise kohta, 13 August 2018 No. 818

Strateegias rõhutatakse ka vajadust arendada innovatsiooni küberturvalisuse valdkonnas. Selle eesmärgi saavutamiseks on ülioluline koostöö peamiste avaliku ja erasektori osalejate ning akadeemiliste ringkondade vahel.

Riigikaitseministeeriumi riiklik küberturvalisuse keskus (NCSC)[21] on Leedu keskne küberturvalisuse asutus, mis vastutab küberintsidentide käsitlemise, küberturvalisuse nõuete rakendamise jälgimise ja teabeallikate akrediteerimise eest. NCSC töötab ka küberturvalisuse alase teadlikkuse edendamisel ühiskonnas.

Malta

Malta riiklik digitaalne strateegia, tuntud ka kui digitaalne Malta[22], viidi ellu 2016. aastal. Strateegia hõlmab kolme peamise riikliku sidusrühma - avaliku sektori, erasektori ja kodanikuühiskonna vajadust ja ootusi küberturvalisuse tagamiseks. Strateegia aluseks olevas strateegias on välja toodud viis mõõdet - poliitika, seadusandlus, riskijuhtimine, kultuur / teadlikkus ja haridus.

Strateegias pakutakse välja neli peamist eesmärki:

1. võidelda küberkuritegevusega, tehes kindlaks lüngad ja tugevdades õiguskaitseasutuste võimet küberkuritegevuse uurimiseks;
2. tugevdada riiklikku küberkaitset, suunates ja abistades avalikke ja eraõiguslikke üksusi nende küberkaitsevõime parandamisel;
3. kindlustada küberruumis suurem usalduse tase teadlikkuse tõstmise programmide ja usaldusväärsete, IKT-toega teenuste pakkumise kaudu;
4. arendada suutlikkust (küberturvalisuse alane teadlikkus ja haridus), määratledes ja arendades vajalikke oskusi ja haridusraamistikke.

Viimane põhieesmärk (teadlikkus ja haridus) on suunatud akadeemilisele ringkonnale, avalikule ja erasektorile ning kodanikele kui vahendile küberjulgeoleku alase teadlikkuse, teadmiste, samuti võimete ja asjatundlikkuse suurendamiseks käimasoleva haridus- ja teadlikkuse tõstmise kampaania, samuti range ja pideva haridustee kaudu. Viiakse läbi koolitusharjutusi, mis on suunatud nii praegusele tööjõule kui ka nooremale õpilastele. See meede tähendab seega peamiselt[23]:

[20] Cyber Wiser (2021): Education and training in national cybersecurity strategy (LT), URL https://www.cyberwiser.eu/lithuania-lt (külastatud 11/03/2021)
[21] National Cyber Security Centre, URL https://www.nksc.lt/en/
[22] The Malta Information Technology Agency (2016): Malta Cyber Security strategy 2016, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Malta (külastatud 12/03/2021)
[23] Cyber Wiser (2021): Education and training in national cybersecurity strategy (MT), URL https://www.cyberwiser.eu/malta-mt (külastatud 12/03/2021)

Co-funded by the Erasmus+ Programme of the European Union

- Küberturvalisuse oskuste ja pädevuste vajaduse edasine tunnustamine;
- küberjulgeoleku alaste teadmiste tugevdamiseks kavandatud akadeemilised ja koolitusprogrammid;
- Olemasolevate õppekavade ülevaade, mis keskenduvad küberturvalisusele koos IKT ja meediapädevustega.

Strateegia eesmärk on ka noorte toetamine nende tugivõrgustiku kaudu (vanemad, hooldajad, koolitajad ja noorsootöötajad). Eeldatakse, et digitaalsest kodakondsusest saab osa riiklikust hariduse õppekavast, et varustada lapsi ja noori interneti kasutamiseks vajalike oskustega, luues samal ajal loomingulist veebisisu ohutult.
Digital Malta kinnitab valitsuse pühendumust haridusasutuste ja tööstuse kaudu toetada erihariduse omandamise võimalusi, käsitleda tööturu nõudeid, arendada õppekava ja pakkuda tehnilisi materjale. Küberturvalisusega seotud koolitus- ja sertifitseerimisprogramme tuleks veelgi julgustada kui võimalust organisatsioonide turvalisuse taset tõhusalt tõsta ja säilitada selline kõrgendatud turvalisuse tase pikas perspektiivis.
Küberturvaline Malta[24] on osa Malta riiklikust küberturvalisuse strateegiast, mille eesmärk on luua juhtimisraamistik, võidelda küberkuritegevusega, tugevdada riiklikku küberkaitset ning pakkuda küberturvalisuse alast teadlikkust ja haridust. Riikliku küberturvalisuse strateegia üks põhieesmärke on üleriigiline küberturvalisuse alane teadlikkuse tõstmise ja hariduse kampaania.
Teine oluline organisatsioon on Malta riiklik arvutiturbeintsidentidele reageerimise meeskond (CSIRT). CSIRT Malta toetab Malta esmatähtsate infrastruktuuride organisatsioone oma andmete kaitsmisel küberohtude ja -intsidentide eest[25].

1.4. Projekt "Andmepüügi vastu võitlemine 4. tööstusrevolutsiooni ajastul"

Küberturvalisusest saab digiajastu üks suurimaid väljakutseid[26], sest informatsioonist saab kallis vara, mis tegeleb tohutute andmemahtudega, parandades suhtlust digitaalse keskkonnaga. Digitaalsed seadmed ja infosüsteemid muutuvad küberrünnakute jaoks üha atraktiivsemaks.

Andmepüük on üks suurimaid probleeme, kuna küberkurjategijad kasutavad andmepüügi kampaaniate läbiviimiseks kiiremaid ja uuenduslikke tehnoloogilisi vahendeid. Seetõttu tuleks välja töötada laiale publikule vabalt kättesaadav inimpõhine andmepüügi kaitsesüsteem, mis kasutab inimese avastamisinstinkti ja tehnoloogiat üheskoos. Inimesest juhitud andmepüügikaitse loomiseks on vaja haridust, et kasutaja saaks õngitsemisrünnakud õigesti tuvastada ja neile reageerida.

Vilniuse Ülikooli Kaunase teaduskonna ja partnerite algatatud rahvusvaheline Projekt „Andmepüügi vastu võitlemine 4. tööstusrevolutsiooni ajastul“ („*CyberPhish*“) algas 2020. aasta novembri alguses ja kestab kaks aastat.

Projekti eesmärk on harida kõrgkoolide üliõpilasi, õppejõude, ülikoolide töötajaid (kogukonna liikmeid), hariduskeskusi, ärisektorit (tööandjaid ja töötajaid) ning julgustada osaliste kriitilist mõtlemist küberturvalisuse vallas.

Projekti partnerlus koosneb kuuest organisatsioonist viiest Euroopa riigist:
1. Vilniuse Ülikool, Leedu (koordinaator)
2. Infotehnoloogia instituut, Leedu
3. DOREA haridusinstituut, Küpros
4. Tartu Ülikool, Eesti
5. Altacom SIA, Läti
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

[24] Cyber Security Malta, URL https://cybersecurity.gov.mt/
[25] Cyber Security Intelligence, URL https://www.cybersecurityintelligence.com/csirt-malta-2727.html (Külastatud 12/03/2021)
[26] European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020

Co-funded by the Erasmus+ Programme of the European Union

Lisateavet projekti ja projekti tegevuste kohta leiate projekti veebisaidilt: https://cyberphish.eu/ . Projekti ja küberturvalisuse uuendusi võib jälgida ka projekti Facebooki lehel: https://www.facebook.com/eucyberphish .

Co-funded by the Erasmus+ Programme of the European Union

2. UURINGU ANALÜÜS

2.1. Andmete kogumise metoodika

Küberturvalisuse ja andmepüügi valdkonnas eksisteerivate õppeprogrammide ja koolitusprogrammide uurimiseks on juhtiv organisatsioon IO1 (DOREA Haridusinstituut) koostanud malli. Mall hõlmab põhiteavet, nagu akrediteerimine ja akadeemiline nimetus, programmi struktuur ja teave kursuste kohta.

Tabel 1: Küberjulgeoleku ja andmepüügi valdkonnas olemasolevate programmide analüüsi mall

Programmi või kursuse pealkiri	
Programmi tüüp	
Õppevaldkond	
Kraad	
Korraldav asutus	
Õppekeel	
Kestus (tundi või ECTS)	
Sihtrühm	
Põhirõhk: teemade või moodulite sisu	
Õpitulemused	
Metoodika (kui on teada)	
Viide link / URL	

Kõiki partnereid julgustati kasutama küberjulgeoleku kõrghariduse andmebaasi[27] ja tegema kohalikke riiklikke uuringuid, kuna osasid õppeprogrammi pole veel olemasolevasse andmebaasi sisestatud.

Samuti paluti projektipartneritel teha lühiuuringuid küberjulgeoleku hariduse riiklike poliitikate ja strateegiate kohta. Uuring viidi läbi kõigis partnerriikides - Küprosel, Eestis, Lätis, Leedus ja Maltal. Uuringu analüüsi tulemused kanti riiklikele tulemuste tabelitele (struktureeritud riigiti - Küpros, Eesti, Läti, Leedu ja Malta).

Kogutud andmeid kasutatakse oskuste puudujääkide väljaselgitamiseks ja uue õppekava kohta soovituste ettevalmistamiseks, et tugevdada Interneti-kasutajate oskusi, haridust ja teadlikkust uusimatest esilekerkivatest küberturvalisuse probleemidest ja ohtudest, eelkõige andmepüügist valdkonnas.

Tuginedes olemasoleva küberturvalisuse õppekavade analüüsi tulemustele ja küsitluse tulemustele, töötab partnerite konsortsium välja koolitusmaterjali, teadmiste enesekontrolli ja teadmiste hindamise testid ning simulatsioonistsenaariumid koolituse jaoks.

[27] The Cybersecurity Higher Education Database (CyberHEAD) is the largest validated cybersecurity higher education database in the EU and EFTA countries. URL https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/education-courses

Co-funded by the Erasmus+ Programme of the European Union

2.2. Küpros

Kõik Küprose peamised ülikoolid pakuvad bakalaureuse- ja magistriõppe õppekavasid informaatikas või küberturvalisuses. Bakalaureusekraad Küprose ülikoolides on 240 ECTS ainepunkti ja magistrikraad 90-120 ECTS ainepunkti. Õppekavasid õpetatakse kas kreeka või inglise keeles.

Tabel 2. Küberjulgeoleku valdkonna kõrgkoolide õppeprogrammide ülevaade Küprosel

Õppekava nimetus	**Informaatika**	**Arvuti ja võrgu turvalisus**	**Kübersõda**	**Side ja võrgu turvalisus**
Programmi tüüp	Õppekava	Õppekava	Õppemoodul	Õppemoodul
Valdkond	Informaatika magister	Informaatika magister	Küberturvalisuse magister	Küberturvalisuse magister
Kraad	Magistrikraad	Magistrikraad	Magistrikraad	Magistrikraad
Korraldav asutus	University of Nicosia	Open University of Cyprus	University of Central Lancashire (UCLAN)	European University of Cyprus
Keel	Inglise	Kreeka	Inglise	Inglise
Maht	90 ECTS	90 ECTS	10 ECTS	7 ECTS
Sihtrühm	Bakalaureusekraad või samaväärne kraadiõppur	Bakalaureusekraad või samaväärne kraadiõppur	Bakalaureusekraad või samaväärne kraadiõppur	Bakalaureusekraad või samaväärne kraadiõppur
Teemad ja moodulid	• küberfüüsikalised süsteemid ja asjade internet; • krüptograafia ja võrgu turvalisus; • hajussüsteem; • **kübersõda**; • eetiline häkkimine; • küberturvalisuse projekt; • võrgu kaitse ja vastumeetmed.	• sidevõrgud • arvuti- ja võrgueksperti isid • arvuti ja võrgu turvalisus • krüptograafia • **info- ja sidesüsteemide turvariskide juhtimine** • uurimismeetodid	• kübersõja alused; • kübersõda ja eetika õiguslikust aspektist; • küberruumi lahinguväli - pahavara relvastus (sh psühholoogilised relvad: **sotsiaalse ründed, sotsiaalsed taktika võtted ja protseduurid**; • küberruumi eripärad ja kübersõja tulevik.	• ülevaade peamistest võrgutehnoloogia alusteadmistest ja -seadmetest • võrk kui küberrünnakute kanal, kuidas võrku kaitsta, haavatavused, ohud. • võrgurünnakud, sealhulgas **andmepüük**. • üldine kaitse, ennetamine ja avastamine

Ükski Küprose kõrgharidusõppe õppeprogrammidest ei õpeta eraldi moodulina andmepüüki ega sotsiaalseid ründeid. Selle asemel on need õppeained integreeritud kursusemoodulitesse, nagu kübervõitlus, side- ja võrguturvalisus, turberiski juhtimine, küberturvalisuse riskianalüüs ja -juhtimine jne.

Co-funded by the Erasmus+ Programme of the European Union

Kuigi mõned bakalaureuseõppekava moodulid hõlmavad ka pehmeid oskusi (nt avalik esinemine, psühholoogia), keskendub enamik magistriõpinguid üliõpilaste tehniliste oskuste arendamisele, jättes pehmed oskused tahaplaanile.

Tabel 3. Küprose küberturvalisuse valdkonna koolituste ülevaade

Õppekava nimetus	**Küberturvalisuse teadlikkus**	**Sertifitseeritud turvaline arvutikasutaja (CSCU)**	**CompTIA Security+ Sertifikaat (SY0-601)**	**Rakenduslik küberturvalisus**
Programmi tüüp	Koolitus	Koolitus	Koolitus	Koolitus
Valdkond	Küberturvalisus	Küberturvalisus	Küberturvalisus	Küberturvalisus
Kraad	Tunnistus	Tunnistus	Tunnistus	Tunnistus
Korraldav asutus	The University of Nicosia and Global training	AKTINA	New Horizons Computer Learning centre	Institute of Public, Cyber and National Security
Keel	Inglise keeles	Inglise keeles	Inglise keeles	Inglise keeles
Maht	2 tundi	14 tundi	5 päeva	12 nädalat (u. 120 tundi)
Sihtrühm	Ettevõtjad, juhid, IT-töötajad, üliõpilased jne	Arvutikasutajad üldiselt	(IT) spetsialistid ja üliõpilased	IT ja küberturvalisuse spetsialistid ja konsultandid
Teemad ja moodulid	Küberturvalisus; **sotsiaal-tehnika / andmepüük;** sotsiaal-meedia rünnakud, võltsteated; andmepüügi meilid; pahatahtlikud e-posti manused; pahatahtlik tarkvara; WiFi-rünnakud; paroolid; demonstratsioon.	Operatsioonisüsteemide turvamine; pahavara ja viirusetõrje; interneti turvalisus; turvalisus suhtlusvõrgustikes; e-posti, mobiilseadmete, pilve- ja võrguühenduste turvamine; andmete varundamine ja katastroofide taastamine.	**Ähvardused, rünnakud ja haavatavused**; arhitektuur ja disain; rakendamine; operatsioonid ja intsidentidele reageerimine.	Küberturvalisus ja küberrisk; küberriski arengusuunad, praktiline kogemus; NIST küberturvalisuse raamistik; tööriistad ja tehnikad **küberohtude avastamiseks**; ettevõtte ohuriski hindamise, vastavusaruannete ja leevendamiskavad.

Paljud avaliku ja erasektori organisatsioonid pakuvad küberturvalisuse koolitusi IT-spetsialistidele, üliõpilastele, töötajatele ja laiemale avalikkusele. Kursuse kestus varieerub paarist tunnist mitme kuuni. Sõltuvalt pakutavast tunnistusest peab osaleja mõnel koolituskursusel tunnistuse saamiseks sooritama eksami. Enamik pikema kestusega koolituskursusi sisaldab eraldi objektidena õngitsemist ja sotsiaaltehnikat. Seevastu lühiajalised (umbes ühe päeva pikkused) koolituskursused keskenduvad peamiselt ainult andmepüügile ja sotsiaalsetele rünnetele. Küberturvalisuse ja digitaalsete oskuste strateegiate meetmete ja algatuste raames toetab Küprose inimressursside ja arendusasutus (HRDA[28]) osaliselt koolituskursuste kulusid.

[28] Human Resource and Development authority in Cyprus (HRDA), UR http://www.hrdauth.org.cy/

Co-funded by the Erasmus+ Programme of the European Union

2.3. Eesti

Peamised arvutiteaduse või küberturvalisuse õppeprogramme pakkuvad kõrgkoolid on Tallinna Tehnikaülikool ja Tartu Ülikool. Eesti ülikoolide bakalaureusekraad on vahemikus 180 kuni 240 EAP, magistrikraadi puhul 60 kuni 120 EAP. Õppekavasid õpetatakse eesti ja inglise keeles.

Tabel 4. Küberjulgeoleku valdkonna kõrgkoolide õppeprogrammide ülevaade Eestis

Õppekava nimetus	**Küberturbe tehnoloogiad**	**Cybersecurity**	**Cryptography, specialisation of SECCLO Erasmus+**
Programmi tüüp	Õppekava	Õppekava	Õppekava
Valdkond	Tehnikateaduste bakalaureus	Tehnikateaduste magister	Tehnikateaduste magister
Kraad	Bakalaureuse kraad	Bakalaureuse kraad	Bakalaureuse kraad
Korraldav asutus	Tallinna Tehnikaülikool (TalTech)	Tallinna Tehnikaülikool (TalTech) ja Tartu Ülikool	Tartu Ülikool
Keel	Inglise	Inglise	Inglise
Maht	180 ECTS	120 ECTS	120 ECTS
Sihtrühm	Keskkooli lõpetanud	Bakalaureusekraad või samaväärne kraadiõppur	Bakalaureusekraad või samaväärne
Teemad ja moodulid	IT sotsiaalsed, ametialased ja eetilised aspektid; elektroonika IT-s; loogika ja diskreetne matemaatika; suhtlemisoskused; IT-infrastruktuuri teenused; Linuxi ja Windowsi haldus; võrgutehnooloogia alused; informaatika ja arvutite tutvustus; **sissejuhatus küberturvalisusse**; programmeerimise alused; veebitehnoloogiad; küberturvalisuse juhtimine ja haldus; andmebaasi põhitõed; arvutivõrgu turvalisus; sotsiaaltehnika; logimine ja jälgimine; turvaline programmeerimine.	Arvuti programeerimine; süsteemihaldus; võrgutehnoloogia; Eesti keel ja kultuur; ettevõtlus ja äriplaan; **küberjulgeoleku inimlikud aspektid**; küberjulgeoleku õiguslikud aspektid; küberjulgeoleku juhtimine; küberturvalisuse tehnoloogiad; krüptograafia; küberintsidentide käitlemine; T´turvaline tarkvara kujundamine; meeskonnatöö projekt; arvutivõrgu turvalisus; infosüsteemide rünnakud ja kaitse; I ja II küberturvalisus; krüptograafia eriteemad; mobiiltelefonide kohtueksperiisid; strateegiline kommunikatsioon ja küberturvalisus; andmete kaevandamine; pahavara; küberkaitse seirelahendused; privaatsust säilitavad tehnoloogiad; traadita tehnoloogiad ja turvalisus;	Krüptograafilised protokollid; arvutiteaduse matemaatilised alused; teadusseminar krüptograafias; krüptoloogia II, kvantkrüptograafia; sissejuhatus kodeerimisteooriasse; mobiilirakenduste arendamine - projektid, meetodid TCS-is; krüptograafia erikursus; teoreetilise informaatika projekt; Eesti keel algajatele I; Magistriseminar.

Co-funded by the Erasmus+ Programme of the European Union

Analüüsitud kõrgkoolide õppeprogrammid Eestis ei näi õpetavat õngitsemist eraldi moodulina. Andmepüügiinfot võib lisada ka teistesse kursustesse nagu näiteks küberturvalisuse tutvustus, arvutivõrgu turvalisus jt.

Tallinna tehnikaülikooli pakutav küberturvalisuse spetsialisti õppeprogramm sisaldab aga eraldi moodulina sotsiaaltehnikat. Mooduli eesmärk on anda õpilastele põhiteadmised sotsiaalse manipuleerimise olemusest (peamiselt IKT kontekstis) ning selle põhivormidest, tehnikatest ja tehnikatest (sealhulgas hübriidrünnakud koos tehnoloogilise komponendiga) ja kaitsest selle eest. Mooduli kestus on 3 EAP.

Tallinna Tehnikaülikooli ja Tartu Ülikooli pakutav küberturvalisuse õppeprogramm sisaldab küberturvalisuse inimaspekte. Mooduli eesmärk on anda ülevaade küberturvalisuse inimlikest aspektidest, täpsemalt sotsiaalse manipuleerimise elementidest ja nende vastu suunatud kaitsemehhanismidest. Mooduli kestus on 6 EAP.

Õppekavad hõlmavad laia valikut spetsialiseeritud õppemooduleid, pakkudes head suhet omandatud teoreetiliste teadmiste ja praktilise õppe vahel. Neil on ka pehmete oskuste kursusemoodulid nagu suhtlemisoskus, ettevõtlikkus, psühholoogia jms.

Tabel 5. Küberjulgeoleku valdkonna koolitused Eestis

Õppekava nimetus	**Veebirakenduste turvalisus**	**Võrgutehnoloogia turvalisuse administraator**
Programmi tüüp	Koolitus	Koolitus
Valdkond	Eetiline häkkimine / läbitungimise testimine	Network's security
Kraad	Tunnistus	Tunnistus
Korraldav asutus	Clarified Security	NobleProg
Keel	Inglise keeles	Inglise keeles
Maht	4 päeva	5 päeva
Sihtrühm	Veebirakenduste arendajad, hooldajad, veebiserveri majutuse pakkujad / administraatorid, infoturbespetsialistid jne	Süsteemiadministraatorid ja võrguadministraatorid, kõik võrguturbe tehnoloogiate huvilised.

Co-funded by the Erasmus+ Programme of the European Union

Teemad ja moodulid	Kliendipoolsed rünnakud: (turvalisus, teabeallikad, klient-server suhtlus, HTTP vs HTTPS, HTTP päringud, JavaScripti ja JavaScripti süstimine, URL-i ja URL-i manipuleerimine, küpsiste ja küpsiste manipuleerimine, seansi ja seansi kaaperdamine, seansi fikseerimine, võltsimisrünnakute taotlemine (CSRF ja OSRF), kasutajaliidese parandusrünnakud, kolmanda osapoole sisu kasutamine, kombineeritud kliendipoolsed rünnakud) Serveripoolsed rünnakud: (autentimine, paroolid ja räsid, autoriseerimisnõrkused, äriloogika probleemid, Google'i häkkimine, veebiserveri seadistamine ja failisüsteem, käskude sisestamine, failide käitlemine, failide kaasamise rünnakud, failide üleslaadimine, XXE (XML eXternal Entity) rünnakud , SQL-i süstimine)	Võrguturbe, võrguprotokollide, turvapoliitika, füüsilise turvalisuse, võrgurünnakute tutuvustamine (praegune statistika, terminite määratlemine: ohud, rünnak ja ärakasutamine, häkkerite ja rünnakute klassifikatsioon, võltsimine; rämpspost; pealtkuulamine; andmepüük; paroolide murdmine, veebilehe väljanägemise rikkumine; SQLi süstimine; traadi pealtkuulamine; puhvri ületäitumine, WarDriving; ja hajutatud DOS), sissetungi tuvastamise süsteem, tulemüürid, pakettide filtreerimine ja puhverserverid, Bastion host ja honeypot, turvamine, ruuterid, operatsioonisüsteemide turvalisusesuurendamine, Patch Management, rakenduste turvalisus, veebiturve, e-posti turvalisus; krüptimine, virtuaalsed eravõrgud, WLAN, tõrketaluvuse loomine, intsidentidele reageerimine, katastroofide taastamine ja planeerimine, võrgu haavatavuse hindamine.

Mitmeid eraõiguslikud organisatsioonid (Clarified Security, NoblePro, Cyberexer, Rangeforce, CTF Pärnu jt) pakuvad koolituskursusi erinevatel teemadel, näiteks küberhügieeni ja andmekaitse e-õpe, haavatavuse visualiseerimine, riskihindamine, küberturvalisus, andmepüük. Kursused on peamiselt suunatud IT-spetsialistidele, ettevõtetele ja laiemale avalikkusele, kes on teemast huvitatud. Sõltuvalt pakutavast tunnistusest võivad osalejad sertifikaadi saamiseks sooritada eksami.

Et aidata kohalikel ettevõtetel küberturvalisuse ohtudele vastu seista, on Eesti Infosüsteemide Amet käivitanud ka väikestele ja keskmise suurusega ettevõtetele suunatud teavituskampaania. Kampaania keskendub küberintsidentide tüüpidele, mis on ettevõtetele viimastel aastatel kõige rohkem rahalist kahju tekitanud[29].

[29] Cyber security campaign, URL https://itvaatlik.ee/

Co-funded by the Erasmus+ Programme of the European Union

2.4. Läti

Peamised arvutiteaduse või küberturvalisuse õppeprogramme pakkuvad kõrgkoolid on Turiba Ülikool, Riia Tehnikaülikool, Vidzeme rakenduskõrgkool, BA äri- ja rahanduskool. Läti ülikoolides on bakalaureusekraad vahemikus 160 kuni 240 ECTS ja magistrikraad 120 ECTS. Õppekavasid õpetatakse läti ja inglise keeles.

Tabel 6. Küberjulgeoleku valdkonna kõrgkoolide õppeprogrammide ülevaade Lätis

Õppekava nimetus	**Informaatika**	**Küberturvalisus**	**Infotehnoloogia**
Programmi tüüp	Õppekava	Õppekava	Õppekava
Valdkond	Tehnikateaduste bakalaureus	Tehnikateaduste magister	Tehnikateaduste magister
Kraad	Bakalaureuse kraad	Magistri kraad	Magistri kraad
Korraldav asutus	Turiba University	Riga Technical University	Vidzeme University of applied science
Keel	Läti ja inglise keel	Inglise keeles	Inglise keeles
Maht	240 ECTS	120 ECTS	120 ECTS
Sihtrühm	Keskkooli lõpetanud	Bakalaureusekraad või samaväärne kraadiõppur	Bakalaureusekraad või samaväärne kraadiõppur
Teemad ja moodulid	Inglise ja läti keel; tsiviil- ja keskkonnakaitse; arvutiarhitektuur, arvutitehnika ja süsteemid; matemaatika; tarkvaraarenduse alused; disainmõtlemine; majandus ja ettevõtlus; tarkvara testimine ja kvaliteet; kodeerimine ja krüptograafia**; IT-turvalisus ja riskijuhtimine**; masinõpe ja intelligentne analüüs; tarkvara projektijuhtimine; andmete analüüs ja võrdlusuuringud; rohelised IT süsteemid ja meetodid; sissejuhatus operatsiooni-uuringutesse; rahandus ja raamatupidamine; IT-seadused ja autoriõigused; robootika.	Küberturvalisus; infosüsteemide töökindlus; ettevõtte infotehnoloogia arhitektuur; esmatähtsate infrastruktuuride juhtimise alused; tööstuslik ohutus; **võrgu turvalisus**; tarkvara turvalisus; krüptograafia ja andmeturbe tehnoloogiad; kohanduvate süsteemide projekteerimine; insenerisüsteemide turvalisus; sotsiotehniliste süsteemide modelleerimine; andmekaevandamine ja teadmiste avastamine; projektijuhtimine; turvalised e-kaubanduse tehnoloogiad; andmete integreerimise tehnoloogiad; Sotsiaalne vastutus ja ettevõtlus.	Eetiline häkkimine; pöördkonstrueerimine; võrgu-, mobiili- ja pilveturve; digitaalne kohtueksperтiis; turvaline tarkvara kujundus; intsidentide käsitlemine ja reageerimine; süsteemi turvalisuse projekteerimine; projektijuhtimine; strateegiline IKT juhtimine; andmete kaevandamine; suhtlemine; kriitiline mõtlemine; sotsiaalmeedia analüüsi töötuba; **interneti-psühholoogia**; internetis osalejate õigused, kohustused ja vastutus; andmeturbe ja uurimise seadus; küberturvalisuse poliitika; infosüsteemi auditid ja kinnitused; **infoturbega seotud riskide juhtimine;** turvakultuur; krüptograafia; innovatsioon ja loominguline probleemide lahendamine.

Co-funded by the Erasmus+ Programme of the European Union

Lätis analüüsitud kõrgkoolide õppeprogrammid ei õpeta andmepüüki ega sotsiaalseid ründeid eraldi moodulitena. Teavet nende teemade kohta võib siiski leida muudest kursusemoodulitest nagu IT-turvalisus ja riskijuhtimine, võrguturvalisus, küberturvalisuse, infoturbe riskijuhtimine ja interneti-psühholoogia jne.

Nagu ka Eestis, näivad pakutavad õppeprogrammid olevat laiapõhjalised ja tehnilistele oskustele orienteeritud, samas hõlmates kursuse mooduleid pehmete oskuste osas nagu suhtlemisoskus, ettevõtlikkus, loominguline probleemilahendus jne.

Tabel 7. Küberjulgeoleku valdkonna koolitused Lätis

Õppekava nimetus	**ESET Kaugteadmised küberturvalisusest**	**IT security training for users**	**"Kiberdrošība"**
Programmi tüüp	Koolitus	Koolitus	Koolitus
Valdkond	Võrguturvalisus	Küberturvalisus	Küberturvalisus
Kraad	Tunnistus	Tunnistus	Tunnistus
Korraldav asutus	ESET Läti	Küberturvalisuse akadeemia	"Dialogs AB" koolituskeskus
Keel	Läti ja inglise keeles	Läti, Inglise, Vene keeles	Läti keeles
Maht	2 tundi	4 tundi	1 nädal (42 tundi)
Sihtrühm	Ettevõtted ja nende töötajad	Ärijuhid, IT-turbejuhid, ettevõtted ja laiem avalikkus	Ärijuhid, IT-turbejuhid, ettevõtted ja laiem avalikkus
Teemad ja moodulid	Ülevaade ohtudest (pahavara tüübid, pettuse põhimõtted ja sotsiaalsed ründed); paroolid; kaugtöö; turvalisus kõikjal; **andmepüügi vältimine**; e-posti turvalisus (rämpspost, **andmepüük** ja lihtsad pettused); tarkvara haldamine.	Miks on oluline olla teadlik IT-turvaohtudest; oma vaenlase tundmine; füüsiline turvalisus; turvaline parool; **sotsiaalsed ründed; andmepüük; SMS-i saamine; *Vishing***; isikuandmete turvalisus	Infotehnoloogia toimimine ja roll; teabeallikad ja nende roll**; infoturbeohud, nende tüübid ja mõju**; infoturbe haldamise tööriistad ja meetodid; küberjulgeoleku dokumentide tähtsus.

Tehtud uuringute põhjal pakuvad mitmed organisatsioonid küberturvalisuse alaseid koolitusi ettevõtetele, IT-spetsialistidele ja laiemale avalikkusele. Kui lühema kestusega koolituskursused keskenduvad tavaliselt ainult erinevat tüüpi ohtudele, sealhulgas andmepüük, sotsiaalne insener ja enesekaitse viisid, pakuvad pikemaajalised koolituskursused küberturvalisusele laiemat vaatenurka. Koolituse pakkujad on suunatud peamiselt ärijuhtidele, üldtöötajatele, IT-spetsialistidele ja huvitatud laiemale üldsusele.

Co-funded by the Erasmus+ Programme of the European Union

Alates 2018. aastast on Läti Vabariigi infotehnoloogia turvaintsidentidele reageerimise asutus (CERT.LV) rakendanud tegevust nimega "Küberjulgeoleku võimekuse parandamine Lätis". Kampaania ajal on CERT.LV välja töötanud informatiivse juhendi ja videod, korraldanud küberturvalisuse konverentsi ja käivitanud töökoha küberturvalisuse ressurse sisaldava veebisaidi[30].

Läti Turvalisema Interneti keskus[31] pakub õpilastele ka tasuta veebiseminare Interneti-ohutuse kohta. Seevastu Läti kohalike omavalitsuste koolituskeskus pakub täiskasvanutele kursusi Interneti ja sotsiaalmeedia ohutu kasutamise kohta.

[30] Cyber Security campaign, URL https://www.esidross.lv/

[31] Latvian Safer Internet Centre, URL https://drossinternets.lv/lv/nodarbibas

Co-funded by the Erasmus+ Programme of the European Union

2.5. Leedu

Enamik Leedu ülikoole ja kolledžeid pakuvad bakalaureuse- ja magistriõppekavasid arvutiteaduses või küberturvalisuses. Leedu kõrghariduse bakalaureusekraad on vahemikus 180 kuni 240 ECTS ja magistrikraad 90 kuni 120 ECTS. Õppekavasid õpetatakse leedu ja inglise keeles..

Tabel 8. Küberjulgeoleku valdkonna kõrgkoolide õppeprogrammide ülevaade Leedus

Õppekava nimetus	**Informaatika ja küberturvalisus**	**Information and Information Technologies Security**	**Cybersecurity Management**
Programmi tüüp	Õppekava	Õppekava	Õppekava
Valdkond	Bakalaureus arvutiteadustes	Magister küberturvalisuses	Magister küberturvalisuse halduses
Kraad	Bakalaureuse kraad	Magistri kraad	Magistri kraad
Korraldav asutus	Vilnius Ülikool	Vilnius Gediminas Tehnikaülikool	Mykolas Romeris Ülikool
Keel	Leedu ja inglise keeles	Inglise keeles	Leedu ja inglise keeles
Maht	210 ECTS	120 ECTS	90 ECTS
Sihtrühm	Keskkooli lõpetanud	Bakalaureusekraad või samaväärne kraadiõppur	Bakalaureusekraad või samaväärne kraadiõppur
Teemad ja moodulid	Algoritmiteooria ja andmestruktuurid; matemaatika; küberjulgeoleku õiguslikud eeskirjad; sissejuhatus programmeerimisse; infosüsteemid ja andmebaasid; digitaalne kohtueksperiis; operatsioonisüsteemid ja nende turvalisus; programmeerimiskeeled; WWW arendustehnoloogiad; infosüsteemide loomine; e-tehingud ja nende turvalisus; eetiline häkkimine; **infoturve ja riskijuhtimine; arvutivõrgud ja nende turvalisus**; andmete turvalisus ja krüptograafia; arvutitaristude kujundamine; virtuaalsüsteemid; andmete kaevandamine; infosüsteemide testimine ja kvaliteedi tagamine; digitaalse sisu kohtueksperiisi analüüs ja pahavara analüüs.	Infotehnoloogia turvameetodid; andmebaasid ja elektrooniliste dokumentide turvalisus; krüptograafilised süsteemid; teadusuuringute ja innovatsiooni alused; arvutivõrgud ja operatsioonisüsteemi turvalisus; virtuaalne infrastruktuur ja pilvandmetöötluse turvalisus; eetilised häkkimistehnikad; küberkriminalistika; **infoturbehaldus**; turvaline programmeerimine.	Uuringud hõlmavad süsteemi ja võrgu turvameetodeid, krüptograafiat, eetilisi sissetungitehnoloogiaid, küberkuritegevuse uurimist, infoturbehaldust ja muid spetsiifilisi kursuste üksusi. Kohustuslikud kursused: E-valitsemise ja e-demokraatia otsused; küberjulgeoleku õiguslik keskkond; küberturvalisuse haldamine; avalike suhete strateegia; **privaatsus ja andmekaitse**; turvaökonoomika; intellektuaalne omand; IT-projekti juhtimine; elektroonilise infoturbe modelleerimine.

Leedus analüüsitud kõrgkoolide õppeprogrammid ei õpeta andmepüüki ega sotsiaalseid ründeid eraldi moodulitena. Teavet nende teemade kohta võib siiski lisada muudesse kursustesse nagu küberturvalisus, infoturve ja riskijuhtimine; arvutivõrgud ja nende turvalisus; privaatsus ja andmekaitse jne.

Co-funded by the Erasmus+ Programme of the European Union

Vastupidiselt Lätis ja Eestis pakutavatele õppeprogrammidele näivad nii bakalaureuse- kui ka magistriõpe Leedus keskenduvat peamiselt üliõpilaste tehniliste oskuste arendamisele, pöörates vähem rõhku pehmete oskuste olulisusele.

Tabel 9. Küberjulgeoleku valdkonna koolitused Leedus

Õppekava nimetus	**ESET Kaugteadmised küberturvalisusest**	**IT-turvateadlikkuse koolitus**	**Tarbijate küberturvalisuse alused**
Programmi tüüp	Koolitus	Koolitus	Koolitus
Valdkond	Küberturvalisus	Küberturvalisus	Küberturvalisus
Kraad	Tunnistus	Tunnistus	Tunnistus
Korraldav asutus	ESET	UAB "Hermitage Solutions"	Vilniuse Ülikool
Keel	Leedu keeles	Leedu keeles	Leedu keeles
Maht	2 tundi	6 tundi	8 tundi
Sihtrühm	Ettevõtted ja töötajad	Ärijuhid, IT-turbejuhid, ettevõtted, töötajad ja laiem avalikkus	Laiem avalikkus
Teemad ja moodulid	**Andmepüük**; kaugtöö; ühendamine ettevõtte võrguga; ennetavad meetmed; ohtude ülevaade; paroolipoliitika; interneti turvalisus; asjade internet; Elektroonilise e-posti kaitse; praktilised nõuanded	Miks on IT-turvalisuse alane kirjaoskus kõigile oluline? Ohu äratundmine; Füüsiline andmekaitse; Paroolid; **Sotsiaalsed ründed**; a**ndmepüük**; mobiilne andmekaitse; isikuandmete kaitse.	Isikuandmete turvalisuse põhimõtted; tugevad paroolid; suhtlusvõrgustike tegevus; Wi-Fi kasutamise põhimõtted; **sotsiaalsed ründed** (kõige populaarsemad sotsiaalsed rünnakud; kuidas sotsiaalseid rünnakuid ära tunda; turvameetmed).

Mitmed avaliku ja erasektori organisatsioonid pakuvad küberturvalisuse koolituskursusi IT-spetsialistidele, ettevõtetele, töötajatele ja laiemale avalikkusele. Küberjulgeoleku valdkonnas korraldavad mitmed organisatsioonid ka spetsiaalselt ettevõtetele ja nende töötajatele suunatud kursusi. Kursused hõlmavad andmepüügi ja sotsiaaltehnoloogia teemasid ning nende kestus varieerub paarist tunnist mitme päevani.

2020. aastal viis "Loo Leedu" meeskond koostöös riigikaitse ministeeriumi ja riikliku küberturvalisuse keskusega läbi uuringud ja andis välja juhendi "Küberjulgeolek ja ettevõtlus. Mida peaks teadma iga ettevõtte juht"[32]. Juhendis käsitletakse küberturvalisuse olulisust ja antakse praktilisi nõuandeid ohtude riskide hindamiseks ning soovitusi võimalike küberintsidentide haldamiseks.

[32] Create Lithuania (2020): “Cyber Security and Business. What every company manager should know”, UR https://www.enterpriselithuania.com/naujienos/isleistas-leidinys-kibernetinis-saugumas-ir-verslas-ka-turetu-zinoti-kiekvienas-imones-vadovas/ (külastatud 17/03/2021)

Co-funded by the Erasmus+ Programme of the European Union

2.6. Malta

Peamised arvutiteaduse või küberturvalisuse õppeprogramme pakkuvad kõrgkoolid on Malta ülikool (UoM) ja Malta kunsti-, teadus- ja tehnoloogiakolledž (MCAST). Malta ülikoolide bakalaureusekraad on vahemikus 180–240 ECTS ja magistrikraad 60–120 ECTS-i. Õppekavasid õpetatakse inglise keeles.

Tabel 10. Küberjulgeoleku valdkonna kõrgkoolide õppeprogrammide ülevaade Malta

Õppekava nimetus	**Infotehnoloogia**	**Info- ja küberturvalisus**	**Infotehnoloogia süsteemid**
Programmi tüüp	Õppekava	Õppekava	Õppekava
Valdkond	Bakalaureus küberturvalisuses	Magister Küberturvalisuses	Magister küberturvalisuses
Kraad	Bakalaureuse kraad	Magistrikraad	Magistrikraad
Korraldav asutus	STC Higher Education	American University of Malta	Malta kunsti-, teadus- ja tehnoloogiakolledž (MCAST)
Keel	Inglise keel	Inglise keel	Inglise keel
Maht	180 ECTS	96 ECTS	90 ECTS
Sihtrühm	Keskkooli lõpetanud	Bakalaureusekraad või samaväärne kraadiõppur	Bakalaureusekraad või samaväärne kraadiõppur
Teemad ja moodulid	Arvutioskused; arvutisüsteemid; arvutivõrgud; andmebaasid; veebilehe kujundamine ja arendamine; tarkvaraarenduse tehnikad; objektorienteeritud programmeerimine; kontorilahenduste arendamine; **küber-turvalisuse arhitektuur ja operatsioonid**; arvutivõrgud; võrgu turvalisus; eetiline häkkimine; objektorienteeritud disain ja programmeerimine; andmete kaevandamine; täiustatud võrgud; digitaalne kohtueksperti**isi riskide ja küberturvalisuse juhtimine**; süsteemiarhitektuur ja asjade internet; küberturvalisuse projekt; küberluure.	Infotehnoloogia turvameetodid; andmebaasid ja elektrooniliste dokumentide turvalisus; krüptograafilised süsteemid; teadusuuringute ja innovatsiooni alused; arvutivõrgud ja operatsioonisüsteemi turvalisus; virtuaalne infrastruktuur ja pilvandmetöötluse turvalisus; eetilised häkkimistehnikad; küberkriminalistika; **infoturbehaldus**; turvaline programmeerimine.	Infosüsteemid ja juhtimine; pperatsioonisüsteemid ja pilvandmetöötlus; võrguprotokollid ja võrgu automatiseerimine; andmeteadus ja ennustav analüüs; küberjulgeoleku alused; veebitehnoloogiad ja turvaline e-kaubandus; mobiilarvutid ja 5G võrgud; asjade Internet (IoT); finantsarvutus ja krüptorahad; **ettevõtlus ja innovatsiooni juhtimine**

Nagu teisteski analüüsitud riikides (välja arvatud Eesti), ei paku Malta kõrgharidusõppe õppeprogrammid eraldi moodulina andmepüüki ega sotsiaaltehnikat. Teavet nende teemade kohta võib siiski leida muudest kursusemoodulitest nagu küberturvalisuse juhtimine, küberturvalisuse arhitektuur ja operatsioonid, infoturbehaldus, küberturvalisuse alused, turvalisus ja teabekindlus jne.

Co-funded by the Erasmus+ Programme of the European Union

Enamik õppeprogramme on suunatud tehniliste oskuste arendamisele. Kõigist analüüsitud programmidest pakuvad ainult Malta kunsti-, teaduse ja tehnoloogia kolledž ning Malta Ülikool pehmetele oskustele keskenduvaid õppemooduleid, nagu ettevõtlus ja innovatsiooni juhtimine, ettevõtlus: alustage oma innovaatilist äri, projektijuhtimist jne.

Tabel 11. Küberjulgeoleku valdkonna koolitused Malta

Õppekava nimetus	**Eetilise häkkimise kursus**	**The Certified Information Systems Security Professional (CISSP**	**Information & Cybersecurity Practitioner**
Programmi tüüp	Koolitus	Koolitus	Koolitus
Valdkond	Küberturvalisus	Informaatika	Küberturvalisus
Kraad	Tunnistus	Tunnistus	Tunnistus
Korraldav asutus	ICE Malta	Cybersecurity Malta	Lead training
Keel	Inglise keel	Inglise keel	Inglise keel
Maht	24 tundi	5 päeva	12 päeva/ 6 ECTS
Sihtrühm	Õpilased ja laiem avalikkus	IT-turvalisusega seotud praktikud, audiitorid, konsultandid, uurijad või instruktorid	Juhid, infoturbe- ja IT-spetsialistid, nõuetele vastavuse eest vastutavad ametnikud, raamatupidajad jne
Teemad ja moodulid	Sissejuhatus eetilisse häkkimisse; võrgutehnoloogia alused; jälgede ajamine ja tutvumine; skaneerimine; paroolid; nuusutamine; **sotsiaaltehnika**; krüptograafia; juhtmeta süsteemide häkkimine	Turvalisus ja riskijuhtimine; vara turvalisus; turvatehnika; side ja võrgu turvalisus; identiteedi ja juurdepääsu haldamine; **turvaintsidendid** - ettevalmistamine, reageerimine ja taastamine; turvalisuse hindamine ja testimine; turvaoperatsioonid; tarkvaraarenduse turvalisus.	Infoturbe, **küberhindamise ja juhtumitele reageerimise**, infosüsteemide auditeerimise ja haldamise alused

Mitmed avaliku ja erasektori organisatsioonid pakuvad küberturvalisuse koolituskursusi IT-spetsialistidele, turvalisusega seotud spetsialistidele, ettevõtetele, töötajatele, üliõpilastele ja laiemale avalikkusele. Samuti pakuvad mitmed eraõiguslikud organisatsioonid küberturvalisuse ja turvatestimise ning sotsiaalse rünnaku spetsiifilisi kursusi. Enamik uuritud koolitustest pakub küberturvalisusele laiemat vaatenurka, selle asemel et keskenduda ainult andmepüügi või sotsiaalse inseneri teemadele.

2018. aastal käivitati Maltal riiklik küberturvalisuse teadlikkuse ja hariduse kampaania. Kampaania eesmärk oli tõsta teadlikkust selle kohta, kuidas digitaalset turvalisust saab parandada, rõhutades pikemate paroolide, omaduste vajadust ja neid regulaarselt muutes, suurendades

Co-funded by the Erasmus+ Programme of the European Union

ettevaatlikkust isikuandmete edastamisel ja internetist kaupade ostmisel. Kampaania eesmärk oli ka harida inimesi rämpspostide tuvastamisel, sotsiaalmeedia vastutustundlikul kasutamisel ja andmepüügi äratundmisel.

Lisaks käivitas Malta Infotehnoloogia Agentuur koostöös finantsteenuste ning digitaalse majanduse ja innovatsiooni parlamendisekretäriga samal aastal uue kava küberturvalisuse edendamiseks ja tugevdamiseks erasektoris. Kava aitab erasektoril hinnata nende digitaalse vara olukorda küberturvalisuse ohtude vastu ja pakub töötajatele koolitust[33].

Malta BeSmartOnline![34] Projekti eesmärk on tõsta teadlikkust ja harida lapsi, noori ja nende tugivõrgustikke, näiteks hooldajaid, lapsevanemaid ja koolitajaid, Interneti ohutu kasutamise kohta, luues, haldades ja edendades Interneti-kuritarvitamisest teatamise võimalusi.

[33] B-SECURE Scheme, URL https://cybersecurity.gov.mt/bsecure/#1569427288152-9f8f5200-6588
[34] BeSmartOnline! project, URL https://www.besmartonline.org.mt/

Co-funded by the Erasmus+ Programme of the European Union

3. KOKKUVÕTE JA PEAMISED TULEMUSED

- Küberturvalisuse oskuste puudus on mõjutanud 74% organisatsioonidest kogu maailmas. 57% organisatsioonidest oli 2019. aastal täitmata küberturvalisuse töökohti. Nende ametikohtade täitmiseks kulus tavaliselt kolm kuud.

- Kõige kriitilisemate oskuste puudujääkide hulka kuuluvad pilvandmetöötluse turvalisus (33%), rakenduste turvalisus (32%) ning turvalisuse analüüs ja uurimine (30%).

- Üks peamistest põhjustest, miks vastavad ametikohad jäävad täitmata, on kvalifitseeritud taotlejate puudumine. Ligi kolmandik organisatsioonidest väitis, et peaaegu 75% kandidaatidest ei oma selleks ametiks vajalikku kvalifikatsiooni. Kõige olulisemad oskuste puudujäägid, millele vastajad viitasid, olid pehmete oskuste, IT-teadmiste puudumine, ebapiisav ülevaade ettevõtlusest, küberturvalisuse tehniline kogemus ja praktiline kogemus.

- 2020. aastal oli küberjulgeoleku valdkonna töötajate arv hinnanguliselt üle 3,12 miljoni spetsialisti. Seevastu ainuüksi Euroopas on küberjulgeoleku tööjõu puudujääk aastaks 2022 hinnanguliselt 350 000 töötajat. See arv on 2018. aastast hinnanguliselt kahekordistunud.

- ENISA on oma aruandes "Küberjulgeoleku oskuste arendamine ELis" välja toonud neli peamist põhjust, mis võivad olla seotud küberturvalisuse oskuste nappusega. Kaks neist on keskendunud töökoha probleemidele, ülejäänud kaks on seotud haridus- ja koolitussüsteemi probleemidega.

- 2013. aastal avaldas Euroopa Komisjon oma esimese küberturvalisuse strateegia, rõhutades teadlikkuse tõstmist ja oskuste arendamist kui peamisi strateegilisi eesmärke. Alates 2017. aastast on kõik ELi liikmesriigid välja töötanud ja avaldanud oma riiklikud küberturvalisuse strateegiad (NCSS).

- Kõigi projekti partnerriikide riiklike julgeolekustrateegiate põhieesmärk on küberhariduse ja teadlikkuse suurendamine ühiskonnas keskendudes akadeemilisele ringkonnale, avalikule ja erasektorile ning üldsusele.

- Kõigi projekti partnerriikide riiklikud julgeolekustrateegiad rõhutavad ka avaliku, erasektori ja akadeemilist partnerlust, et tugevdada küberturbe süsteemide vastupidavust, investeeringuid IKT turvalisusse, personali koolitamist ja õpilaste küberturvalisuse oskuste arendamist turu vajaduste rahuldamiseks.

- Kõigi projekti partnerriikide, välja arvatud Eesti, kõrgharidusasutuse õppeprogrammide analüüs ei sisalda andmepüügi- ja sotsiaaltehnika teemasid eraldi moodulitena. Teavet nende teemade kohta võib siiski lisada ka teistesse kursusemoodulitesse. Kaks Eesti kõrgharidusõppe õppeprogrammi sisaldavad sotsiaalmehaanikale keskendunud õppemooduleid. Selliste kursuste keskmine kestus on 4,5 EAP.

Co-funded by the Erasmus+ Programme of the European Union

- Analüüsitud kõrgharidusasutuste õppeprogrammid Eestis, Lätis ja Maltal sisaldavad pehmete oskuste kursuste mooduleid, nagu suhtlemisoskus, ettevõtlus, psühholoogia jms. Vastupidiselt on Küprose ja Leedu kõrgkoolide õppeprogrammid keskendunud peamiselt tehnilistele oskustele, pannes vähem rõhku sotsiaalsete oskustele.

- Kõigis partnerriikides on arvukalt avaliku ja erasektori organisatsioone, kes pakuvad küberturvalisuse alaseid koolitusi, mis on suunatud küberturvalisuse ja IT-spetsialistidele, ettevõtetele, töötajatele ja laiemale avalikkusele. Kui lühema kestusega koolituskursused keskenduvad tavaliselt ainult erinevat tüüpi ohtudele, sealhulgas andmepüük, sotsiaalsed ründed ja enesekaitse viisid tutvustamisele, pakuvad pikemaajalised koolituskursused küberturvalisusele laiemat vaatenurka. Samuti on mitmeid organisatsioone, mis pakuvad enesekontrolli ja sotsiaalse ründe teste, mis on suunatud ettevõtetele ja nende töötajatele.

Co-funded by the Erasmus+ Programme of the European Union

4. KASUTATUD KIRJANDUS

1. (ISC)2 (2019): (ISC)² Study Reveals the Cybersecurity Workforce Has Grown to 3.5 Million Professionals Globally, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study-Reveals-the-Cybersecurity-Workforce-Has-Grown-Globally
2. (ISC)2 (2019): Cybersecurity workforce study, URL https://www.isc2.org/Research/Workforce-Study
3. Cyber Wiser (2021): Education and training in national cybersecurity strategy (LT), URL https://www.cyberwiser.eu/lithuania-lt
4. Cyber Wiser (2021): Education and training in national cybersecurity strategy (MT), URL https://www.cyberwiser.eu/malta-mt
5. Cyber Wiser (2021): Education and training in national cybersecurity strategy (LV), URL https://www.cyberwiser.eu/latvia-lv
6. Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy
7. ENISA, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Latvia
8. European Commission (2013): Cybersecurity Strategy of the European Union, URL https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
9. European Commission (2019): Four EU pilot projects launched to prepare the European Cybersecurity Competence Network, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network
10. European Commission (2020): Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027
11. European Union Agency for Cybersecurity (2019): Cybersecurity skills development in the EU
12. European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
13. Government of the Republic Of Lithuania (2018): Resolution on the approval of the national cybersecurity strategy, URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf
14. ISACA (2020): State of Cybersecurity 2020 Part 1: Global Update on Workforce Efforts and Resources, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf
15. Jon Oltsik (2019): The Life and Times of Cybersecurity Professionals 2018, URL https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/surveys/esg-issa-2018-survey-results.pdf
16. Latvian Defence Ministry (2019): Latvia approves new Cyber Security Strategy 2019-2022, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
17. Latvian Defence Ministry (2019): Latvia's cybersecurity strategy for 2019 – 2022, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
18. OCECPR (2012): Cybersecurity Strategy of the Republic of Cyprus, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus
19. The Republic of Estonia, Ministry of Economic Affairs and Communication (2019): Cybersecurity Strategy, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
20. The Malta Information Technology Agency (2016): Malta Cyber Security strategy 2016, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Malta

Co-funded by the Erasmus+ Programme of the European Union