Projekta Nr.: 2020-1-LT01-KA203-078070

O1-A2: Rezultāti “Esošo kiberdrošības apmācības programmu analīze”

ZIŅOJUMS

2021

Partnerība

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

Eiropas Komisijas atbalsts šīs publikācijas izstrādei nav uzskatāms par tās satura apstiprinājumu, publikācijas saturs ir vienīgi tās autoru viedokļa atspoguļojums un Komisija neuzņemas atbildību par jebkādu publikācijā iekļautās informācijas izmantošanu. (Projekta Nr .: 2020-1-LT01-KA203-078070)

Satura rādītājs

Tabulu rādītājs

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

Eiropas Komisijas atbalsts šīs publikācijas izstrādei nav uzskatāms par tās satura apstiprinājumu, publikācijas saturs ir vienīgi tās autoru viedokļa atspoguļojums un Komisija neuzņemas atbildību par jebkādu publikācijā iekļautās informācijas izmantošanu. (Projekta Nr .: 2020-1-LT01-KA203-078070)

Saīsinājumu saraksts

CCS	Kipras Datorzinātņu asociācija
CERT.LV	Latvijas Datorapdraudējumu reaģēšanas vienība
CSSS	Kiberdrošības prasmju trūkums
ESKO	Eiropas Kiberdrošības organizācija
ENISA	Eiropas Savienības Kiberdrošības aģentūra
ES	Eiropas Savienība
HITSA	Informācijas tehnoloģiju fonds izglītībai
ISACA	Informācijas sistēmu audita un kontroles asociācija (ISACA)
ISC2	Starptautiskais informācijas sistēmu drošības sertifikācijas konsorcijs
NCSC	Valsts Aizsardzības ministrijas Nacionālais kiberdrošības centrs (Lietuvas Republika)
NCSS	Nacionālās kiberdrošības stratēģijas
OCECPR	Elektroniskās komunikācijas un pasta regulēšanas komisāra birojs (Kipras Republika)
RIA	Informācijas sistēmu pārvalde (Igaunijas Republika)
MVU	Mazie un vidējie uzņēmumi

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

1. IEVADS

1.1. Kiberdrošības prasmju trūkums (CSSS) un tā iemesli

Pamatojoties uz Enterprise Strategy Group un Informācijas sistēmu drošības asociācijas ikgadējo globālo pētījumu[1], kas tika veikts 2019. gadā, kiberdrošības prasmju trūkums ir ietekmējis 74% organizāciju visā pasaulē. Šī trūkuma galvenās sekas, kā norādīts ziņojumā, ir palielināta esošā personāla slodze, nespēja izmantot dažas drošības tehnoloģijas, kā arī jaunākā personāla pieņemšana darbā un apmācība, tā vietā, lai noalgotu pieredzējušākus profesionāļus. Viskritiskākais prasmju trūkums ir mākoņdatošanas drošība (33%), lietojumprogrammu drošība (32%), drošības analīze un izmeklēšana (30%).

Turklāt saskaņā ar Informācijas sistēmu audita un kontroles asociācijas (ISACA) veikto pētījumu[2] 2019. gadā 57% organizāciju bija neaizpildītas kiberdrošības vakances. Šo amatu aizpildīšanai nepieciešamais laiks parasti bija trīs mēneši, kā norāda vairāk nekā 60% respondentu, kuri piedalījās pētījumā. Lielākā daļa neaizpildīto amatu ir individuālā līdzstrādnieka (gan tehniskā, gan netehniskā kiberdrošība) un kiberdrošības vadītāja pozīcijās. Paredzams, ka nākamajos gados pieaugs pieprasījums pēc darba vietām individuālā līdzstrādnieka amatā tehniskās kiberdrošības jomā. Paredzams, ka pieprasījums pēc citām darbavietām saglabāsies nemainīgs vai nedaudz palielināsies.

Viens no galvenajiem respondentu norādītajiem iemesliem, kāpēc amati paliek neaizpildīti, ir kvalificētu pretendentu trūkums. Gandrīz trešdaļa organizāciju apgalvoja, ka aptuveni 75% kandidātu nav atbilstošas kvalifikācijas šim darbam. Respondentu norādītās būtiskākās prasmju nepilnības bija nepietiekamu prasmju, IT zināšanu trūkums, nepietiekams ieskats uzņēmējdarbībā, kiberdrošības tehniskās pieredzes un praktiskās pieredzes trūkums.

Saskaņā ar ENISA[3], konsultācijās ar dalībvalstīm kiberdrošības izpratnes un prasmju trūkums iedzīvotājos tika identificēts kā viens no galvenajiem šķēršļiem drošas kibertelpas veidošanā. *"Neskatoties uz gandrīz 600 akadēmisko iestāžu un mācību centru pieejamību, kas piedāvā kiberdrošības programmas visā Eiropā, kiberdrošības prasmju trūkums visās nozarēs joprojām ir būtisks izaicinājums"* (ENISA, 2019, 10. lpp.) .

2020. gadā kiberdrošības darbaspēka trūkums tika novērtēts kā aptuveni 3,12 miljoni profesionāļu[4]. Turpretī Eiropā vien kiberdrošības darbaspēka trūkums līdz 2022. gadam sasniedza 350 000 strādājošo. To skaits ir divkāršojies, salīdzinot ar 2018. gadā aprēķināto[5] .

Kiberdrošības prasmju trūkums (CSSS) un tā iemesli

ENISA savā ziņojumā "Kiberdrošības prasmju attīstīšana ES" ir norādījusi četrus galvenos cēloņus, kas varētu veicināt kiberdrošības prasmju trūkumu. Divi no tiem attiecas uz darba vietas jautājumiem, bet pārējie divi ir saistīti ar izglītības un apmācības sistēmas jautājumiem . Precīzāk:

1. *Kiberdrošības darba tirgus ir salīdzinoši nenobriedis un dinamisks*, kā rezultātā darba specifikācijas ir ļoti atkarīgas no organizācijas lieluma un nozares. Piemēram, MVU, kas nav specializējušies kiberdrošības nozarē, parasti pieņem darbā vispārīgus IT darbiniekus, kuriem ir ierobežotas zināšanas par kiberdrošību. Turpretī lielākos MVU un tajos, kas

[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 (skatīts 09/03/2021)

[2] ISACA (2020): Kiberdrošības stāvoklis 2020. gadā, 1. daļa: Jaunākā globālā informācija par darbaspēku un resursiem, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf (skatīts 09/03/2021)

[3] ENISA (2019): Kiberdrošības prasmju attīstīšana ES, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf (skatīts

[4] (ISC)² (2019): (ISC)² pētījums atklāj, ka kiberdrošības darbaspēks visā pasaulē ir pieaudzis līdz 3,5 miljoniem profesionāļu, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study- Atklāj-kiberdrošības-darbaspēks-globāli ir pieaudzis (skatīts 09.03.2021.)

[5] (ISC)² (2019): Kiberdrošības darbaspēka pētījums, URL https://www.isc2.org/Research/Workforce-Study (skatīts 03.03.2021.)

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

specializējas kiberdrošības jomā, darbinieki koncentrējas uz noteiktām kiberdrošības jomām.

2. *Darba devēji nepiedāvā pareizo apmācības līmeni*, kas kavē gan ilgstoša darbaspēka izveidi, gan pašreizējo darbinieku profesionālo attīstību. Tas rada šķēršļus kiberdrošības profesionāļiem ar vispārīgāku zināšanu pamatu turpināt attīstīt nepieciešamās profesionālās prasmes.
3. *Akadēmiskās programmas nespēj sagatavot kandidātus ar atbilstošām zināšanām un prasmēm*. Studentiem trūkst arī praktiskas pieredzes, kā rezultātā rodas neatbilstības starp nozares vajadzībām un studentiem piemītošajām prasmēm.
4. *Kiberdrošības mācību programmas reaģē lēni, salīdzinot ar nozares attīstību*. Birokrātijas dēļ līdz šim kiberdrošības mācību programmas ir cīnījušās, lai tiktu galā ar jaunajiem draudiem un jaunākajām prasmēm, kas nepieciešamas šo draudu novēršanai.

1.2. Digitālās un kiberdrošības izglītības politika ES

Eiropas Komisija 2013. gadā publicēja savu pirmo kiberdrošības stratēģiju, uzsverot izpratni un prasmju attīstību kā galvenos stratēģiskos mērķus.

"2017. gadā Eiropas Komisija un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos vēlreiz paziņoja, ka kiberdrošībai piemīt spēcīga izglītības dimensija un ka efektīva kiberdrošība lielā mērā ir atkarīga no attiecīgo cilvēku prasmēm. Tika rekomendēts, ka Dalībvalstīm kopā ar ES nepieciešams uzlabot kiberdrošības izglītību un prasmes, balstoties uz Digitālo prasmju un darbavietu koalīcijas darbu un izveidojot Eiropas kiberdrošības rūpniecības, tehnoloģiju un pētniecības kompetenču centru un nacionālo kiberdrošības koordinācijas centru tīklu". (ENISA, 2019. gads, 23. lpp.)

2019. gadā tika uzsākti četri projekti - CONCORDIA, ECHO, SPARTA un CyberSec4Europe[6] - saskaņā ar programmu "Horizon 2020", kuras mērķis ir izstrādāt kopēju Eiropas kiberdrošības kompetences tīklu un Eiropas kiberdrošības pētniecības un inovācijas plānu.

2020. gadā Eiropas Komisija ierosināja programmu Digitālā Eiropa[7] , ES programmu ar mērķi paātrināt Eiropas digitālo transformāciju. Paredzams, ka programmai tiks piešķirti 580 miljoni eiro progresīvu digitālo prasmju attīstīšanai, atbalstot specializētu programmu un stažēšanās plānošanu un nodrošināšanu topošajiem ekspertiem tādās galvenajās kapacitātes jomās kā AI, kiberdrošība, kvantu tehnoloģijas u.c.

2021. gada martā Eiropas Padome pieņēma jaunus secinājumus par ES kiberdrošības stratēģiju[8]. Secinājumos tiek atzīts, ka darbaspēkā trūkst digitālo un kiberdrošības prasmju, un uzsvērta nepieciešamība apmierināt tirgus pieprasījumu, turpmāk attīstot izglītības un apmācības programmas.

1.3. Nacionālās kiberdrošības stratēģijas (NCSS)

Kopš 2017. gada visas ES dalībvalstis ir izstrādājušas un publicējušas savas nacionālās kiberdrošības stratēģijas (NCSS).

[6]Eiropas Komisija (2019): Četri ES pilotprojekti, kas sākti, lai sagatavotu Eiropas kiberdrošības kompetences tīklu, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network (skatīts 10.03.2021.)

[7]Eiropas Komisija (2020): Digitālās Eiropas programma: Piedāvātais finansējums 7,5 miljardu euro apmērā 2021. – 2027. gadam, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027 (skatīts 10.03.2021.)

[8] Eiropas Savienības Padome (2021. gads): Padomes secinājumu projekts par ES kiberdrošības stratēģiju digitālajai desmitgadei, 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 (skatīts 24.03.2021.)

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

Kipra

Kipras Republika apzinās kiberizglītības nozīmi, lai garantētu nacionālās kibertelpas aizsardzību. Viens no esošās kiberdrošības stratēģijas galvenajiem mērķiem ir kiberdrošības veicināšana un izpratnes veicināšana tās sabiedrībā (iedzīvotāji, darbaspēks un jaunieši) un sadarbības atmosfēras izveide stratēģijas īstenošanai.

Kipras Republikas kiberdrošības stratēģija tika ieviesta 2012. gadā[9] . Kipras nacionālās stratēģijas mērķis ir attīstīt tehnisko apmācību kibertelpas drošības jomā un mācīt, kā pasargāt sevi un rīkoties steidzamās situācijās. Viens no mērķiem ir izveidot specializētu darbaspēku, kas spēj tikt galā ar reālu kiberuzbrukumu. Šim nolūkam bija jārīko mācības, lai novērotu darbaspēka reaģēšanas ātrumu imitētā reālistiskā krīzē. Stratēģijas ieviešanas rezultātā būtu jāpiemēro kiberspecializēti amatu apraksti un sertifikācijas.

Stratēģija sastāv no 17 īpašām darbībām. Šīs darbības ietver pieejamo atbilstošo personāla apmācības programmu un sertifikāciju identificēšanu kiberdrošības un digitālās drošības jomā.

Kipras Republika ir apņēmusies arī nodibināt valsts un privātā sektora partnerības, lai atbalstītu augstākās izglītības iestādes, iekļaujot kiberdrošības priekšmetus un stiprinot profesionāļu un akadēmiķu apmācību kiberdrošības jomā.

Valsts kiberdrošības dokumenta jaunākā versija tika izstrādāta 2020. gadā. Stratēģija pašlaik tiek pārskatīta, un tai nepieciešams Komunikācijas ministrijas un Ministru padomes galīgais apstiprinājums.

Digitālās drošības iestāde (DSA)[10] ir neatkarīga valdības aģentūra, kuru pārrauga Elektronisko sakaru un pasta regulēšanas komisārs. Tā ir atbildīga par Eiropas TID (Tīklu un informācijas drošība) direktīvas ieviešanu, galveno uzmanību pievēršot augsta līmeņa kiberdrošības modernizēšanai un uzturēšanai visiem būtisko pakalpojumu un kritiskās informācijas infrastruktūras operatoriem Kiprā. Aģentūras mērķis ir arī paaugstināt sabiedrības izpratni par kiberdrošību un palielināt Kipras starptautisko konkurētspēju kopumā.

Vēl viena svarīga organizācija ir Kipras Datorzinātņu asociācija (CCS)[11], neatkarīga bezpeļņas organizācija, kas dibināta 1984. gadā, lai attīstītu, uzlabotu un popularizētu Kipras IT nozari. CCS cenšas noteikt augstus standartus nozares profesionāļiem, atzīstot informācijas un komunikācijas tehnoloģiju (IKT) ietekmi uz nodarbinātību, uzņēmējdarbību, sabiedrību un iedzīvotāju dzīves kvalitāti. Viens no CCS ikgadējiem rīkotajiem pasākumiem ir Kiberdrošības izaicinājums[12] . Pasākuma mērķis ir atklāt kibertalantus un motivēt jauniešus turpināt karjeru kiberdrošības jomā.

[9] OCECPR (2012): Kipras Republikas kiberdrošības stratēģija, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus (skatīts 11.03.2021.)
[10] Digitālās drošības pārvalde (DSA), URL https://dsa.cy/en/
[11] Kipras Datorzinātņu asociācija (CCS), URL https://ccs.org.cy/en/
[12] Kipras kiberdrošības izaicinājums, URL https://ccsc.org.cy/#home

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

Igaunija

Igaunija bija viena no kiberdrošības stratēģiju publicēšanas pionierēm, un pašlaik tā izstrādājusi trešo nacionālās kiberdrošības dokumenta versiju[13] . Stratēģija ir sadalīta četrās jomās: 1. Ilgtspējīga digitālā sabiedrība; 2. Kiberdrošības nozare, pētniecība un attīstība; 3. Vadošā starptautiskā līdzdalība; 4. Kiberbrīva sabiedrība.

Igaunijas stratēģija aktīvi tiecas uzlabot kiberizglītību, un tās piemērojamība ir aprakstīta plāna otrajā mērķī. Kopš 2014. gada valsts iegulda līdzekļus izglītībā un sadarbojas ar universitātēm, lai veicinātu kiberpētījumus, finansētu projektus un atbalstītu stipendijas. Mērķis ir garantēt, ka digitālās tehnoloģijas un kiberdrošības kompetences tiek iekļautas apmācībās, lai sagatavotu sabiedrību un panāktu izpratni par kiberdrošības jautājumiem.

Izglītības un pētniecības ministrija pārrauga šos izglītības projektus un ievēro kiberdrošības stratēģijas noteiktās prioritātes, lai izpildītu mūžizglītības plānu un atbalstītu kiberizglītības pamata izglītības attīstību visu līmeņu absolventiem.

Saskaņā ar stratēģiju stratēģisko mērķu sasniegšanu atbalsta Informācijas tehnoloģiju fonds izglītībai (HITSA), kas sniedz ieguldījumu nozares speciālistu apmācībā, koordinējot gan *Targalt Internetis* ("Rīkojies gudri tiešsaistē"), gan IT Akadēmijas programmas.

Vēl viena svarīga organizācija ir Informācijas sistēmas pārvalde (RIA)[14], kas koordinē informācijas sistēmu izstrādi un administrēšanu, organizē darbības, kas saistītas ar informācijas drošību, un rīkojas drošības incidentu gadījumā. RIA ir arī galvenā loma kiberhigiēnā, profilakses pasākumos un sabiedrības informētības palielināšanā.

"Tiks uzsāktas plaša mēroga profilakses un informatīvās kampaņas, lai izplatītu informāciju par kiberdraudiem dažādām mērķa grupām, tostarp uzņēmumiem. Lai paaugstinātu kiberhigiēnas līmeni valdības iestādēs, valsts iestādēm un pašvaldību darbiniekiem būs obligāti jānokārto kiberdrošības pārbaudes. Tiks turpināti apmācības kursi un imērķa grupu informatīvās kampaņas." (Igaunijas Republika, Ekonomikas un komunikācijas ministrija, 2019. g., 64. lpp.).

Latvija

Latvijā rūpes par nacionālo drošību ir saistītas arī ar pašreizējo tehnoloģiju attīstību. Pirmā Latvijas kiberdrošības stratēģija stājās spēkā 2014. gadā, plānu apstiprinot no 2014. gada līdz 2018. gadam. 2019. gadā tika apstiprināta jauna kiberdrošības stratēģija 2019. – 2022. gadam. Atjaunināts stratēģijas mērķis ir stiprināt un uzlabot Latvijas kiberdrošības iespējas, veicinot sabiedrības informētību un noturību pret kiberuzbrukumiem. Lai sasniegtu šos mērķus, stratēģijā ir ierosinātas darbības sešās jomās[15] :

1. uzlabota kiberdrošība un pārvaldāmi digitālās drošības riski;
2. IKT sistēmu izturība;
3. labāka vispārēja piekļuve stratēģiskām IKT sistēmām un pakalpojumiem;
4. sabiedrības informētība, izglītība un pētniecība;
5. starptautiskā sadarbība;
6. tiesiskums kibertelpā un kibernoziegumu novēršanā.

Attiecībā uz jomu "Sabiedrības informēšana, izglītība un pētniecība", stratēģijā ir norādīti pieci galvenie uzdevumi[16] :

- sniegt atbalstu izpētes attīstībai kiberdrošības jomā;

[13] Igaunijas Republika, Ekonomikas un komunikācijas ministrija (2019): Kiberdrošības stratēģija, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf (skatīts 03.03.2021.)
[14] Informācijas sistēmas pārvalde (RIA), URL https://www.ria.ee/lv.html
[15] Latvijas Aizsardzības ministrija (2019): Latvija apstiprina jauno kiberdrošības stratēģiju 2019.-2022. gadam, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022 (skatīts 11.03.2021.)
[16] Latvijas Aizsardzības ministrija (2019): Latvijas kiberdrošības stratēģija 2019. - 2022. gadam, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf (skatīts 11.03.2021.)

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

- palielināt izglītojamo un pasniedzēju informētību par informācijas drošību, privātuma aizsardzību un uzticamu e-pakalpojumu izmantošanu;
- stiprināt sabiedrības izpratni par drošu interneta lietošanu (izstrādāt izglītojošus un informatīvus materiālus dažādām vecuma grupām ar drošības ieteikumiem, aktivitātēm, izmantojot internetu, organizēt sociālās kampaņas). Izstrādāt un īstenot ikgadēju starpinstitūciju darba un rīcības plānu uzņēmumu informētības un izpratnes veidošanai par kiberdrošības jautājumiem;
- veicināt vietējo un valsts iestāžu darbinieku informētību par drošu IKT izmantošanu;
- veicināt izglītojošas aktivitātes un konkursus kiberdrošības jomā.

Stratēģija arī uzsver nepieciešamību pēc lielākas valsts un privāto dalībnieku iesaistes, lai stiprinātu kiberdrošības sistēmu noturību un nodrošinātu ieguldījumus IKT drošībā un darbinieku apmācībā.

Latvijas Datorapdraudējumu reaģēšanas vienība (CERT.LV) ir atbildīga par kiberdrošības incidentu uzraudzību un risināšanu. CERT.LV organizē arī izglītojošus pasākumus un apmācības kursus plašākai sabiedrībai. Paredzams, ka saskaņā ar jauno stratēģiju CERT.LV kopā ar publisko un privāto sektoru izstrādās resursus, lai apkopotu izlūkdatus par incidentiem analīzei un novērtēšanai[17] .

Vēl viena svarīga organizācija ir Latvijas Drošāka interneta centrs. Tās galvenie uzdevumi ir izglītot, informēt un palielināt sabiedrības informētību par drošāku interneta lietošanu, nodrošināt platformu, lai tiešsaistē ziņotu par nelegālu saturu un drošības pārkāpumiem, izmantojot uzticības dienestu, kā arī piedāvāt profesionālas psihologa konsultācijas, izmantojot tās palīdzības tālruni.[18] .

Lietuva

2018. gadā valdība apstiprināja atjaunināto Lietuvas Nacionālo Lietuvas Republikas kiberdrošības stratēģiju[19] .

„Stratēģijas galvenais mērķis ir nodrošināt Lietuvas sabiedrībai iespēju izmantot informācijas un komunikācijas tehnoloģiju (IKT) potenciālu, efektīvi identificējot kiberincidentus, novēršot to rašanos un izplatīšanos, kā arī pārvaldot kiberincidentu radītās sekas. Rezolūcija par valsts kiberdrošības stratēģijas apstiprināšanu, 2018. gada 13. augusts, Nr. 818

Mērķa sasniegšanai stratēģijā ir ierosināti pieci mērķi:

1. stiprināt valsts kiberdrošību un kiberaizsardzības spēju attīstību;
2. nodrošināt noziedzīgu nodarījumu novēršanu un izmeklēšanu kibertelpā;
3. veicināt kiberdrošības kultūru un inovāciju attīstību;
4. stiprināt ciešu sadarbību starp privāto un publisko sektoru;
5. uzlabot starptautisko sadarbību un nodrošināt starptautisko saistību izpildi kiberdrošības jomā.

Kiberdrošības kultūras un inovāciju veicināšana ir valsts stratēģijas galvenais mērķis. Stratēģijā ir ierosinātas šādas darbības, lai sasniegtu šo konkrēto mērķi[20] :

- nepārtraukti un regulāri atjaunināti apmācības kursi privātā un publiskā sektora darbiniekiem, kuru mērķis ir palielināt darbinieku informētību un veidot vispārēju kiberdrošības kultūru;

[17] Cyber Wiser (2021): Izglītība un apmācība valsts kiberdrošības stratēģijā, URL https://www.cyberwiser.eu/latvia-lv (skatīts 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] Lietuvas Republikas valdība (2018): Rezolūcija par valsts kiberdrošības stratēģijas apstiprināšanu, URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29 .pdf
[20] Cyber Wiser (2021): Izglītība un apmācība valsts kiberdrošības stratēģijā, URL [20]https://www.cyberwiser.eu/latvia-lv (skatīts 11.03.2021.)

- nepārtraukta informācijas izplatīšana par jaunākajiem kiberincidentiem;
- IKT izglītības padarīšana par izglītības procesa daļu jau no mazotnes, sākot no bērnudārza līdz vidusskolai;
- nepārtraukta skolotāju kvalifikācijas celšana un apmācība, ar mērķi uzlabot viņu kvalifikāciju kiberdrošības jomā.

Stratēģija uzsver nepieciešamību attīstīt kiberdrošības prasmes un kompetences, lai nepārtraukti apmierinātu tirgus vajadzības. Lai sasniegtu šo mērķi, stratēģija ierosina "*izveidot kiberdrošības kompetences modeli un standartus, attīstīt apmācības sistēmas, akreditāciju un sertifikāciju, kas orientēta uz darba tirgus vajadzībām, nodrošināt apmācību un testēšanas vidi kiberdrošībai, piedāvāt apmācību IKT darbiniekiem utt.*". Rezolūcija par valsts kiberdrošības stratēģijas apstiprināšanu, 2018. gada 13. augusts, Nr. 818

Stratēģija arī uzsver nepieciešamību attīstīt inovācijas kiberdrošības jomā. Lai sasniegtu šo mērķi, ļoti svarīga ir sadarbība starp galvenajiem valsts un privātajiem dalībniekiem un akadēmisko aprindu pārstāvjiem.

Valsts aizsardzības ministrijas Nacionālais kiberdrošības centrs (NCSC)[21] ir centrālā Lietuvas kiberdrošības iestāde, kas atbild par kiberincidentu apstrādi, kiberdrošības prasību īstenošanas uzraudzību un informācijas resursu akreditāciju. NCSC strādā arī pie kiberdrošības izpratnes veicināšanas sabiedrībā.

Malta

Nacionālā Maltas digitālā stratēģija, kas pazīstama arī kā Digitālā Malta,[22] tika īstenota 2016. gadā. Stratēģija aptver trīs galveno valsts ieinteresēto pušu - valsts sektora, privātā sektora un pilsoniskās sabiedrības - vajadzības un cerības nodrošināt kiberdrošību. Stratēģijas pamatā ir piecas dimensijas - politika, likumdošana, riska vadība, kultūra/izpratne un izglītība.

Stratēģija piedāvā četrus galvenos mērķus:

1. apkarot kibernoziedzību, nosakot trūkumus un stiprinot tiesībaizsardzības aģentūru spēju izmeklēt kibernoziegumus;
2. stiprināt valsts kiberaizsardzību, vadot un palīdzot publiskām un privātām struktūrām uzlabot to kiberaizsardzības iespējas;
3. nodrošināt kibertelpā lielāku uzticības līmeni, īstenojot izpratnes veidošanas programmas un nodrošinot uzticamus, uz IKT balstītus pakalpojumus;
4. uzlabot kapacitāti (izpratni par kiberdrošību un izglītību), identificējot un attīstot nepieciešamās prasmes un izglītības tvērumus.

Pēdējais galvenais mērķis (Izpratne un izglītība) attiecas uz akadēmisko vidi, publisko un privāto sektoru un pilsoņiem kā līdzekli, lai uzlabotu informētību, zināšanas, kā arī iespējas un specializāciju kiberdrošības jomā, izmantojot nepārtrauktas izglītības un izpratnes kampaņu, kā arī stingrus un nepārtrauktus izglītības un apmācības vingrinājumus, kas vērsti gan uz pašreizējo darbaspēku, gan uz jaunāko studentu paaudzi. Tādējādi šis pasākums galvenokārt ietver šādus aspektus[23]:

- Turpmāka kiberdrošības prasmju un kompetenču nepieciešamības atzīšana;
- Akadēmiskās un apmācības programmas, kas paredzētas kiberdrošības specializēto zināšanu nostiprināšanai;

[21] Nacionālais kiberdrošības centrs, URL https://www.nksc.lt/en/
[22] Maltas informācijas tehnoloģiju aģentūra (2016): Kipras Republikas kiberdrošības stratēģija, URL [22]https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus (skatīts 12.03.2021.)
[23] Cyber Wiser (2021): Izglītība un apmācība valsts kiberdrošības stratēģijā (MT), URL https://www.cyberwiser.eu/malta-mt (accessed 12/03/2021)

- Pārskatīt esošās mācību programmas, kas koncentrējas uz kiberdrošību, kā arī IKT un plašsaziņas līdzekļu kompetencēm.

Stratēģijas mērķis ir arī dot iespēju jauniešiem, izmantojot viņu atbalsta tīklu, proti, vecākus, aprūpētājus, pedagogus un jaunatnes darbiniekus. Paredzēts, ka *"Digitālā pilsonība"* kļūs par daļu no Nacionālās izglītības programmas, lai bērniem un jauniešiem sniegtu iemaņas, kas nepieciešamas interneta lietošanai, vienlaikus radot radošu tiešsaistes saturu.

Digitālā Malta pauž valdības apņemšanos ar izglītības iestāžu un nozares starpniecību atbalstīt specializētas izglītības virzienu izveidi, apmierināt darba tirgus prasības, izstrādāt mācību programmu un nodrošināt tehniskos materiālus. Būtu jāturpina veicināt ar kiberdrošību saistītas apmācības un sertifikācijas programmas kā iespēja efektīvi paaugstināt organizāciju drošības līmeni un ilgtermiņā saglabāt šādu paaugstinātu drošības līmeni.

Kiberdrošība Maltā[24] ir daļa no Maltas Nacionālās kiberdrošības stratēģijas, kuras mērķis ir izveidot pārvaldības sistēmu, apkarot kibernoziedzību, stiprināt nacionālo kiberaizsardzību un nodrošināt izpratni par kiberdrošību un izglītību. Viens no galvenajiem Nacionālās kiberdrošības stratēģijas mērķiem ir valsts mēroga kiberdrošības izpratnes un izglītības kampaņa.

Vēl viena svarīga organizācija ir Maltas nacionālā datoru drošības incidentu reaģēšanas grupa (CSIRT). CSIRT Malta atbalsta Maltas kritiskās infrastruktūras organizācijas, aizsargājot tās un to datus no kiberdraudiem un starpgadījumiem[25].

1.4. Projekts "Aizsardzība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā"

Kiberdrošība kļūst par vienu no lielākajiem izaicinājumiem[26] digitālajā laikmetā, jo informācija kļūst par dārgu aktīvu, kas saistīts ar milzīgiem datu apjomiem, uzlabojot saziņu ar digitālo vidi. Digitālās ierīces un informācijas sistēmas kļūst arvien pievilcīgāki mērķi kiberuzbrukumiem.

Pikšķerēšana ir viena no lielākajām problēmām, jo kibernoziedznieki pikšķerēšanas kampaņu veikšanai izmanto arvien ātrākus un novatoriskākus tehnoloģiskos rīkus. Tāpēc nepieciešams izstrādāt un padarīt plaši pieejamu cilvēka vadītu pikšķerēšanas aizsardzības sistēmu, kas izmanto cilvēka dabisko instinktu atklāt lietas un tehnoloģijas, lai mērogotu atbildes reakciju. Lai radītu cilvēku vadītu pikšķerēšanas aizsardzību, lietotājam ir nepieciešama izglītība, lai pareizi identificētu pikšķerēšanas uzbrukumus un reaģētu uz tiem.

Viļņas Universitātes Kauņas fakultātes un partneru aizsāktais starptautiskais projekts "Aizsardzība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā" ("CyberPhish") sākās 2020. gada novembra sākumā un ilgs divus gadus.

Projekta mērķis ir izglītot augstskolu studentus, pedagogus, universitāšu darbiniekus (kopienas locekļus), izglītības centrus, uzņēmējdarbības nozari (darba devējus un darbiniekus), kā arī veicināt mērķa grupas kritisko domāšanu kiberdrošības jomā .

Projekta partneri izstrādās mācību programmu, e-mācību materiālus, jaukta tipa mācību vidi, zināšanu un prasmju pašnovērtēšanas un zināšanu novērtēšanas sistēmas simulācijas studentiem un citiem lietotājiem, lai novērstu pikšķerēšanas uzbrukumus, paaugstinātu kompetences, kas palīdzēs vērst uzmanību uz draudiem un veikt atbilstošus profilakses pasākumus.

Projekta partnerību veido sešas organizācijas no piecām Eiropas valstīm:

1. Viļņas universitāte, Lietuva (koordinators)
2. Informācijas tehnoloģiju institūts, Lietuva
3. DOREA izglītības institūts, Kipra
4. Tartu universitāte, Igaunija

[24] Kiberdrošība Maltā, URL https://cybersecurity.gov.mt/
[25] Kiberdrošības izlūkošana, URL https://www.cybersecurityintelligence.com/csirt-malta-2727.html (skatīts 12.03.2021.)
[26] Eiropas Savienības Kiberdrošības aģentūra (2020): ENISA drošības apdraudējumu aina 2019. – 2020.

5. Altacom SIA, Latvija
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

Lai iegūtu papildinformāciju par projektu un projekta aktivitātēm, lūdzu, apmeklējiet projekta vietni: https://cyberphish.eu/

Jaunumus par projektu kopumā un, jo īpaši, kiberdrošību var iegūt, sekojot arī projekta Facebook lapai: https://www.facebook.com/eucyberphish.

2. PĒTĪJUMA ANALĪZE

2.1. Datu vākšanas metodika

Lai izpētītu esošās studiju programmas un apmācības programmas kiberdrošības un pikšķerēšanas jomā, IO1 vadošā organizācija (DOREA Izglītības institūts) ir sagatavojusi paraugu. Paraugs ietvēra galveno informāciju, piemēram, par akreditāciju un akadēmisko nosaukumu, programmas struktūru un informāciju par kursiem.

1. tabula: Veidne esošo programmu analīzei kiberdrošības un pikšķerēšanas jomā

Programmas vai kursa nosaukums	
Programmas veids	
Studiju joma	
Izglītības līmenis	
Organizējošā institūcija	
Mācību valoda	
Ilgums (stundas vai ECTS)	
Mērķa grupa	
Galvenais mērķis: tēmas vai moduļi	
Mācību rezultāti	
Metodika (ja piemērojams)	
Atsauces saite / URL	

Visi partneri tika mudināti izmantot Kiberdrošības augstākās izglītības datu bāzi[27] un veikt izpēti savā valstī, jo dažas studiju programmas vēl nav augšupielādētas esošajā datu bāzē.

Projekta partneriem tika lūgts arī veikt īsus pētījumus par nacionālo kiberdrošības izglītības politiku / stratēģiju. Pētījums tika veikts visās partnervalstīs - Kiprā, Igaunijā, Latvijā, Lietuvā un Maltā. Pētījuma analīzes rezultāti tika pārnesti uz Nacionālo rezultātu tabulu (strukturēti pa valstīm - Kipra, Igaunija, Latvija, Lietuva un Malta)

Apkopotie dati tiks izmantoti, lai identificētu prasmju trūkumus un sagatavotu ieteikumus jaunai mācību programmai, lai stiprinātu interneta lietotāju prasmes, izglītību un informētību par jaunākajiem jaunajiem kiberdrošības jautājumiem un draudiem, jo īpaši - pikšķerēšanu.

Kopumā, pamatojoties uz datorizētu pētījumu par esošo kiberdrošības studiju programmu un aptaujas rezultātiem, partneru konsorcijs izstrādās mācību materiālu, zināšanu pašnovērtēšanas un zināšanu novērtēšanas testus un simulācijas scenārijus apmācībai.

[27] Kiberdrošības augstākās izglītības datu bāze (CyberHEAD) ir lielākā apstiprinātā kiberdrošības augstākās izglītības datu bāze ES un EBTA valstīs. 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.Kipra

Visas ievērojamākās Kipras universitātes piedāvā bakalaura un maģistra studijas datorzinātnēs vai kiberdrošības jomā. Kipras universitātēs bakalaura programma ietver 240 ECTS un maģistra programma ietver no 90 līdz 120 ECTS kredītpunktiem. Studiju programmas tiek pasniegtas vai nu grieķu, vai angļu valodā.

2. tabula Augstākās izglītības studiju programmu paraugs kiberdrošības jomā Kiprā

Programmas nosaukums	**Datorzinātne**	**Datoru un tīkla drošība**	**Kiberkarš**	**Sakari un tīkla drošība**
Programmas veids	Studiju programma	Studiju programma	Studiju modulis	Studiju modulis
Studiju joma	Maģistra grāds datorzinātnēs	Maģistra grāds datorzinātnēs	Maģistra grāds kiberdrošībā	Maģistra grāds kiberdrošībā
Izglītības līmenis	Maģistra grāds	Maģistra grāds	Maģistra grāds	Maģistra grāds
Organizējošā institūcija	Nikosijas universitāte	Kipras Atklātā universitāte	Centrālā Lankašīras Universitāte (UCLAN)	Kipras Eiropas universitāte
Valoda	Angļu	Grieķu	Angļu	Angļu
Ilgums	90 ECTS	90 ECTS	10 ECTS	7 ECTS
Mērķa grupa	Bakalaura vai līdzvērtīga līmeņa studenti	Bakalaura vai līdzvērtīga līmeņa studenti	Bakalaura vai līdzvērtīga līmeņa studenti	Bakalaura vai līdzvērtīga līmeņa studenti
Tēmas vai moduļi	• Kiberfiziskās sistēmas un lietu internets; • Kriptogrāfija un tīkla drošība; • Izkliedētā sistēma; • **Kiberkarš;** • Ētiska uzlaušana; • Kiberdrošības projekts; • Tīkla aizsardzība un pretpasākumi.	• Sakaru tīkli • Datoru un tīkla kriminālistika • Datoru un tīkla drošība • Kriptogrāfija • **Informācijas un komunikācijas sistēmu drošības risku pārvaldība** • Pētījuma metodes	• Kiberkara pamati; • Kiberkara juridiskais statuss un ētika; • Kibertelpas kaujas lauks - ļaunprogrammatūra kā ierocis (tostarp Psiholoģiskie ieroči: **sociālā inženierija**, SI taktikas tehnikas un procedūras u.t.t.); • Kibertelpas izaicinājumi un kiberkara nākotne.	• Atkārtojums par tīkla principiem un ierīču pamatiem • Tīkls kā kiberuzbrukumu ceļš, kā tīklu var aizsargāt, ievainojamības, draudi. • Uzbrukumi tīklam, tostarp pikšķerēšana. • Vispārēja aizsardzība, novēršana un noteikšana

Nevienā no AII studiju programmām Kiprā netiek mācīta pikšķerēšana vai sociālā inženierija kā atsevišķs modulis. Tā vietā šie priekšmeti ir iekļauti dažos kursu moduļos, piemēram, *Kiberkarš, Sakari un tīkla drošība, Drošības risku vadība, Kiberdrošības riska analīze un vadība utt.*

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

Kaut arī dažās bakalaura studiju programmās ir iekļauti arī moduļi, kas vērsti uz vispārīgajām prasmēm (piemēram, publiskā uzstāšanās, psiholoģija), lielākā daļa maģistra studiju ir vērsta uz studentu speciālo prasmju attīstīšanu, ignorējot vispārīgās prasmes.

3. tabula Apmācību kursu paraugs kiberdrošības jomā Kiprā

Programmas nosaukums	**Kiberdrošības izpratne**	**Sertificēts drošs darbs ar datoru (CSCU)**	**CompTIA Security+ sertifikāts (SY0-601)**	**Lietišķā kiberdrošība**
Programmas veids	Apmācības kurss	Apmācības kurss	Apmācības kurss	Apmācības kurss
Studiju joma	Kiberdrošība	Kiberdrošība	Kiberdrošība	Kiberdrošība
Izglītības līmenis	Sertifikācija	Sertifikācija	Sertifikācija	Sertifikācija
Organizators	Nikosijas universitāte un Global Training	AKTINA	New Horizons Datorzinību centrs	Sabiedrības, kiberdrošības un nacionālās drošības institūts
Valoda	Angļu	Angļu	Angļu	Angļu
Ilgums	2 stundas	14 stundas	5 dienas	12 nedēļas (aptuveni 120
Mērķa grupa	Uzņēmēji, vadītāji, IT personāls, studenti utt.	Vispārīgi datorlietotāji	(IT) profesionāļi un studenti	IT un kiberdrošības profesionāļi un konsultanti
Tēmas vai moduļi	Kiberdrošība; **Sociālā inženierija / pikšķerēšana**; Sociālo mediju uzbrukumi, Viltus brīdinājumi; Pikšķerēšanas e-pasts; Ļaunprātīgi e-pasta pielikumi; Ļaunprogrammatūra; Wi-Fi uzbrukumi; Paroles; Demonstrācija.	Operētājsistēmu drošība; Ļaunprogrammatūra un antivīruss; Interneta drošība; Drošība sociālo tīklu vietnēs; E-pasta sakaru, mobilo ierīču, mākoņa un tīkla savienojumu drošība; Datu dublēšana un katastrofu seku novēršana.	**Draudi, uzbrukumi un ievainojamība**; Arhitektūra un dizains; Ieviešana; Operācijas un reaģēšana uz incidentiem.	Kiberdrošība un kiberrisks; Kiberriska tendences, praktiska pieredze; NIST kiberdrošības sistēma; Instrumenti un metodes, atklājot **kibernoziegumu draudus;** Uzņēmuma apdraudējuma riska novērtējumu, atbilstības

Daudzas valsts un privātās organizācijas piedāvā kiberdrošības apmācības kursus IT profesionāļiem, studentiem, darbiniekiem un plašākai sabiedrībai. Kursu ilgums svārstās no pāris stundām līdz vairākiem mēnešiem. Atkarībā no rezultātā izsniegtās sertifikācijas dalībniekam jākārto eksāmens, lai saņemtu sertifikātu dažos apmācības kursos.

Lielākajā daļā ilgāka laika apmācības kursu pikšķerēšana un sociālā inženierija ir atsevišķas tēmas. Turpretī īstermiņa apmācības kursi (apmēram vienu dienu ilgi) galvenokārt koncentrējas tikai uz pikšķerēšanu un sociālo inženieriju.

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

Eiropas Komisijas atbalsts šīs publikācijas izstrādei nav uzskatāms par tās satura apstiprinājumu, publikācijas saturs ir vienīgi tās autoru viedokļa atspoguļojums un Komisija neuzņemas atbildību par jebkādu publikācijā iekļautās informācijas izmantošanu. (Projekta Nr .: 2020-1-LT01-KA203-078070)

Dažu apmācības kursu izmaksas daļēji subsidē Kipras Cilvēkresursu un attīstības iestāde (HRDA)[28] kiberdrošības un digitālo prasmju stratēģiju aktivitāšu un iniciatīvu ietvaros.

[28] Cilvēkresursu un attīstības pārvalde Kiprā (HRDA), UR http://www.hrdauth.org.cy/

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

2.3.Igaunija

Galvenās augstākās izglītības iestādes, kas piedāvā datorzinātņu vai kiberdrošības studiju programmas, ir Tallinas Tehnoloģiskā universitāte un Tartu Universitāte. Igaunijas universitātēs bakalaura programma ietver no 180 līdz 240 ECTS kredītpunktiem un maģistra programma no 60 līdz 120 ECTS kredītpunktiem. Studiju programmas tiek pasniegtas igauņu un angļu valodās.

4. tabula Augstākās izglītības studiju programmu paraugs kiberdrošības jomā Igaunijā

Programmas nosaukums	**Kiberdrošības inženierija**	**Kiberdrošība**	**Kriptogrāfija, SECCLO Erasmus+ specializācija**
Programmas veids	Studiju programma	Studiju programma	Studiju programma
Studiju joma	Bakalaura grāds inženierzinātnē	Bakalaura grāds inženierzinātnē	Bakalaura grāds inženierzinātnē
Izglītības līmenis	Bakalaura grāds	Maģistra grāds	Maģistra grāds
Organizējošā institūcija	Tallinas Tehniskā universitāte (TalTech)	Tallinas Tehniskā universitāte (TalTech) un Tartu Universitāte	Tartu Universitāte
Valoda	Angļu	Angļu	Angļu
Ilgums	180 ECTS	120 ECTS	120 ECTS
Mērķa grupa	Vidusskolas absolventi	Bakalaura vai līdzvērtīga līmeņa studenti	Bakalaura vai līdzvērtīga līmeņa studenti
Tēmas vai moduļi	IT sociālie, profesionālie un ētiskie aspekti; Elektronika IT jomā; Loģika un diskrētā matemātika; Komunikācijas prasmes; IT infrastruktūras pakalpojumi; Linux un Windows administrēšana; Tīklošanas pamati; Ievads informātikā un datoros; **Ievads kiberdrošībā**; Programmēšanas pamati; Tīmekļa tehnoloģijas; Kiberdrošības pārvaldība un vadība; Datu bāžu pamati; Datoru tīkla drošība; **Sociālā inženierija;** Žurnalēšana un uzraudzība; Droša programmēšana.	Datoru programmēšana; Sistēmas administrēšana; Tīkla tehnoloģija; Igauņu valoda un kultūra; Uzņēmējdarbība un biznesa plānošana; **Kiberdrošības cilvēka aspekti**; Kiberdrošības juridiskie aspekti; Kiberdrošības vadība; Kiberdrošības tehnoloģijas; Kriptogrāfija; Kibernoziegumu apstrāde; Drošas programmatūras projektēšana; Komandas darba projekts; Datoru tīkla drošība; Informācijas sistēmu uzbrukumi un aizsardzība; Kiberdrošība I un II; Īpašas kriptogrāfijas tēmas; Mobilo tālruņu kriminālistika; Stratēģiskā komunikācija un kiberdrošība; Datu ieguve; Ļaunprogrammatūra; Kiberaizsardzības uzraudzības risinājumi; Privātumu saglabājošas tehnoloģijas; Bezvadu tehnoloģijas un drošība; Blokķēdes; Kriptoloģija.	Kriptogrāfijas protokoli; Datorzinātnes matemātiskie pamati; Pētniecības seminārs kriptogrāfijā; Kriptoloģija II, Kvantu kriptogrāfija; Tipa teorija; Ievads kodēšanas teorijā; Mobilās lietojumprogrammas izstrāde - projekti, TCS metodes; Īpašs uzdevums kriptogrāfijā; Teorētiskās informātikas projekts; Igauņu valoda iesācējiem I; Maģistra līmeņa seminārs.

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

Šķiet, ka analizētās Igaunijas augstskolu studiju programmas pikšķerēšanu nemāca kā atsevišķu moduli. Tomēr informācija par pikšķerēšanu var būt iekļauta citos kursu moduļos, piemēram, *Ievads kiberdrošībā, Datoru tīkla drošība* un citos.

Tomēr Tallinas Tehniskās universitātes piedāvātajā kiberdrošības inženierijas studiju programmā kā atsevišķs modulis ir iekļauta sociālā inženierija. Moduļa mērķis ir sniegt studentiem pamatzināšanas par sociālās manipulācijas būtību (galvenokārt IKT kontekstā) un tās pamatformām, paņēmieniem un metodēm (ieskaitot hibrīdus uzbrukumus ar tehnoloģisko komponentu) un aizsardzību pret to. Moduļa ilgums ir 3 ECTS kredītpunkti.

Tallinas Tehniskās universitātes un Tartu Universitātes piedāvātā kiberdrošības studiju programma ietver *Kiberdrošības cilvēciskos aspektus*. Moduļa mērķis ir sniegt pārskatu par kiberdrošības cilvēciskajiem aspektiem, īpaši sociālās manipulācijas elementiem un aizsardzības mehānismiem pret tiem. Moduļa ilgums ir 6 ECTS kredītpunkti.

Studiju programmas ietver plašu specializēto studiju moduļu klāstu, piedāvājot labu attiecību starp iegūtajām teorētiskajām zināšanām un praktiskajām studijām. Tāpat tiek piedāvāti vispārīgo prasmju moduļi, piemēram, komunikācijas prasmes, uzņēmējdarbība, psiholoģija u.t.t.

5. tabula Apmācību kursu paraugs kiberdrošības jomā Igaunijā

Programmas nosaukums	**Tīmekļa lietojumprogrammu drošība**	**Tīkla drošības administrators**
Programmas veids	Apmācības kurss	Apmācības kurss
Studiju joma	Ētiska uzlaušana/ ielaušanās testēšana	Tīkla drošība
Izglītības līmenis	Sertifikācija	Sertifikācija
Organizators	Clarified Security	NobleProg
Valoda	Angļu	Angļu
Ilgums	4 dienas	5 dienas
Mērķa grupa	Tīmekļa lietojumprogrammu izstrādātāji, uzturētāji, tīmekļa serveru vai mitināšanas pakalpojumu sniedzēji/ administratori, informācijas drošības speciālisti u.t.t.	Sistēmas administratori un tīkla administratori, ikviens, kuru interesē aizsardzības tīkla drošības tehnoloģijas.

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

Eiropas Komisijas atbalsts šīs publikācijas izstrādei nav uzskatāms par tās satura apstiprinājumu, publikācijas saturs ir vienīgi tās autoru viedokļa atspoguļojums un Komisija neuzņemas atbildību par jebkādu publikācijā iekļautās informācijas izmantošanu. (Projekta Nr .: 2020-1-LT01-KA203-078070)

Tēmas vai moduļi	Klienta puses uzbrukumi: (Drošība, Informācijas avoti, Klienta-servera saziņa, HTTP pret HTTPS, HTTP pieprasījumu metodes, JavaScript un JavaScript injicēšana, URL un URL manipulēšana, Sīkfaili un sīkfailu manipulēšana, Sesijas un sesijas nolaupīšana, Sesijas fiksēšana, Pieprasījuma viltojumu uzbrukumi (CSRF & OSRF), Lietotāja saskarnes labošanas uzbrukumi, Trešās puses satura izmantošana, Kombinēti klienta puses uzbrukumi Servera puses uzbrukumi: (Autentifikācija, paroles un jaukšana, Autorizācijas ievainojamības, Biznesa loģikas problēmas, Google uzlaušana, Tīmekļa servera konfigurācija un failu sistēma, Komandu ievadīšana, Failu apstrāde, Failu iekļaušanas uzbrukumi, Failu augšupielāde, XXE (XML eXternal Entity) uzbrukumi, SQL ievadīšana)	Ievads tīkla drošībā, Tīkla protokoli, Drošības politika, Fiziskā drošība, Tīkla uzbrukumi (Pašreizējā statistika, Terminu Draudi, uzbrukums un izmantošana definīcijas, Hakeru un uzbrukumu klasifikācija, Mānīšana; Surogātpasts; Ošņātājuzbrukums; **Pikšķerēšana;** Automātiskā zvanīšana; Paroles uzlaušana, Tīmekļa lapu sabojāšana; SQL ievadīšana; Pieslēgpārtveršana; Bufera pārpilde; Piekļuves punktu kartēšana, izmantojot atvērtu WiFi tīklu (WarDriving, War Chalking, War Flying); Pakalpojumatteices (DOS) uzbrukumi un izkliedēti DOS); Ielaušanās atklašanas sistēma, Ugunsmūri, Pakešu filtrēšana un starpniekserveri, Bastiona resursdatori un urķuslazdi, Maršrutētāju rūdīšana, Operētājsistēmu drošības rūdīšana, Ielāpu vadība, Lietojumprogrammu drošība, Tīmekļa drošība, E-pasta drošība, Šifrēšana, Virtuālie privātie tīkli, WLAN, Kļūdu tolerances radīšana, Reaģēšana uz negadījumiem, Atkopšana un plānošana pēc negadījumiem, Tīkla ievainojamības novērtēšana

Ir vairākas privātas organizācijas (Clarified Security, NoblePro, Cyberexer, Rangeforce, CTF Pärnu u.c.), kas piedāvā apmācības kursus par dažādām tēmām, piemēram, e-apmācība par tādām tēmām kā kiberhigiēna un datu aizsardzība, ievainojamības vizualizācija, riska novērtēšana, kiberdrošība, pikšķerēšana utt. Kursi galvenokārt paredzēti IT profesionāļiem, uzņēmumiem un plašākai sabiedrībai, kas interesējas par šo tēmu. Atkarībā no rezultātā izsniegtās sertifikācijas dalībniekam jākārto eksāmens, lai saņemtu sertifikātu.

Lai palīdzētu vietējiem uzņēmumiem pārvarēt kiberdrošības draudus, Igaunijas Informācijas sistēmu pārvalde ir uzsākusi arī informācijas kampaņu, kuras mērķauditorija ir mazie un vidējie uzņēmumi. Kampaņas uzmanības centrā ir kiberincidentu veidi, kas pēdējos gados ir nodarījuši uzņēmumiem lielāko finansiālo kaitējumu[29] .

[29] Kiberdrošības kampaņa, URL https://itvaatlik.ee/

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

2.4. Latvija

Galvenās augstākās izglītības iestādes, kas piedāvā datorzinātņu vai kiberdrošības studiju programmas, ir Turība, Rīgas Tehniskā universitāte, Vidzemes augstskola un Banku augstskola. Latvijas universitātēs bakalaura programma ietver 160 līdz 240 ECTS un maģistra programma ietver 120 ECTS kredītpunktus. Studiju programmas tiek pasniegtas latviešu un angļu valodās.

6. tabula Augstākās izglītības studiju programmu paraugs kiberdrošības jomā Latvijā

Programmas nosaukums	**Datorsistēmas**	**Kiberdrošības inženierija**	**Informācijas tehnoloģijas**
Programmas veids	Studiju programma	Studiju programma	Studiju programma
Studiju joma	Bakalaura grāds datorsistēmās	Maģistra grāds kiberdrošības inženierijā	Maģistra grāds informācijas tehnoloģijās
Izglītības līmenis	Bakalaura grāds	Maģistra grāds	Maģistra grāds
Organizējošā institūcija	Turība	Rīgas Tehniskā universitāte	Vidzemes augstskola
Valoda	Latviešu un angļu	Angļu	Angļu
Ilgums	240 ECTS	120 ECTS	120 ECTS
Mērķa grupa	Vidusskolas absolventi	Bakalaura vai līdzvērtīga līmeņa studenti	Bakalaura vai līdzvērtīga līmeņa studenti
Tēmas vai moduļi	Angļu un latviešu valoda; Civilā un vides aizsardzība; Datoru arhitektūra, Datortehnika un sistēmas; Matemātika; Programmatūras izstrādes pamati; Dizaina domāšana; Ekonomika un uzņēmējdarbība; Programmatūras testēšana un kvalitāte; Kodēšana un kriptogrāfija; **IT drošība un risku vadība**; Mašīnmācīšanās un inteliģentā analītika; Programmatūras projektu vadība; Datu analīze un salīdzinošā novērtēšana; Zaļās / IT sistēmas un metodes; Ievads operāciju izpētē; Finanses un grāmatvedība; IT likumi un autortiesības; Robotika.	**Kiberdrošība**; Informācijas sistēmu uzticamība; Uzņēmuma informācijas tehnoloģiju arhitektūra; Kritisko infrastruktūru vadības pamati; Rūpnieciskā drošība; **Tīkla drošība**; Programmatūras drošība; Kriptogrāfijas un datu drošības tehnoloģijas; Adaptīvo sistēmu projektēšana; Inženiertehnisko sistēmu drošība; Sociotehnisko sistēmu modelēšana; Datu ieguve un zināšanu atklāšana; Projektu vadība; Drošas e-komercijas tehnoloģijas; Datu integrācijas tehnoloģijas; Sociālā atbildība un bizness.	Ētiska uzlaušana; Reversā inženierija; Tīkla, mobilā un mākoņdrošība; Digitālā kriminālistika; Droša programmatūras projektēšana; Incidentu risināšana un reaģēšana; Sistēmas drošības inženierija; Projektu vadība; Stratēģiskā IKT vadība; Datu ieguve; Komunikācija; Kritiskā domāšana; Sociālo mediju analīzes seminārs; **Interneta psiholoģija**; Dalībnieku tiesības, pienākumi un atbildība internetā; Datu drošības un izmeklēšanas likums; Kiberdrošības politika; Informācijas sistēmu auditi un verifikācija; **Informācijas drošības risku vadība**; Drošības kultūra; Kriptogrāfija; Inovācijas un radoša problēmu risināšana.

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

Nevienā no analizētajām AII studiju programmām Latvijā netiek mācīta pikšķerēšana vai sociālā inženierija kā atsevišķs modulis. Tomēr informācija par šīm tēmām varētu būt iekļauta citos kursu moduļos, piemēram, *IT drošība un riska pārvaldība, Tīkla drošība, Kiberdrošība un Informācijas drošības risku vadība, Interneta psiholoģija u.t.t.*

Tāpat kā Igaunijā, šķiet, ka piedāvātās studiju programmas ir plaša mēroga un praktiski orientētas, kursu moduļus iekļauj vispārīgās prasmes, piemēram, komunikācijas prasmes, uzņēmējdarbību, radošu problēmu risināšanu u.t.t.

7. tabula Apmācību kursu paraugs kiberdrošības jomā Latvijā

Programmas nosaukums	**ESET Remote Cyber Drošības zināšanas**	**IT drošības apmācība lietotājiem**	**"Kiberdrošība"**
Programmas veids	Apmācības kurss	Apmācības kurss	Apmācības kurss
Studiju joma	Tīkla drošība	Kiberdrošības akadēmija	Kiberdrošība
Izglītības līmenis	Sertifikācija	Sertifikācija	Sertifikācija
Organizators	ESET Latvija	Kiberdrošības akadēmija	Mācību centrs "Dialogs AB"
Valoda	Latviešu un angļu	Latviešu, angļu, krievu	Latviešu
Ilgums	2 stundas	4 stundas	1 nedēļa (42 stundas)
Mērķa grupa	Uzņēmumi un to darbinieki	Uzņēmumu vadītāji, IT drošības vadītāji, uzņēmumi un sabiedrība kopumā	Uzņēmumu vadītāji, informācijas tehnoloģiju izstrādātāji, sabiedrība kopumā
Tēmas vai moduļi	Draudu pārskats (ļaunprogrammatūras veidi, krāpšanas principi un **sociālā inženierija**); Paroļu teorija; Darbs attālināti; Drošība visur; **Pikšķerēšanas novēršana**; E-pasta drošība (surogātpasts, **pikšķerēšana** un vienkārši krāpnieki); Lietojumprogrammu pārvaldība.	Kāpēc ir svarīgi apzināties IT drošības draudus; Pazīsti savu ienaidnieku; Fiziskā drošība; Paroļu drošība; **Sociālā inženierija; Pikšķerēšana**; **SMSishing; Vishing**; Personas datu drošība	Informācijas tehnoloģiju darbība un loma; Informācijas resursi un to loma; **informācijas drošības draudi**, to veidi un ietekme; Informācijas drošības pārvaldības rīki un metodes; Kiberdrošības dokumentācijas nozīme.

Pamatojoties uz veikto izpēti, vairākas organizācijas piedāvā kiberdrošības apmācības uzņēmumiem, IT speciālistiem un plašākai sabiedrībai. Lai gan īsāki apmācības kursi parasti koncentrējas tikai uz dažāda veida draudiem, tostarp pikšķerēšanu, sociālo inženieriju un veidiem, kā sevi pasargāt, ilgāki apmācības kursi sniedz plašāku skatījumu uz kiberdrošību. Apmācību nodrošinātāji galvenokārt orientējas uz uzņēmumu vadītājiem, darbiniekiem, IT profesionāļiem un plašāku sabiedrību.

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

Kopš 2018. gada Latvijas Republikas Datorapdraudējumu reaģēšanas vienība (CERT.LV) īsteno aktivitāti ar nosaukumu "Kiberdrošības spēju uzlabošana Latvijā". Kampaņas laikā CERT.LV ir izstrādājis informatīvu ceļvedi un video, organizējis kiberdrošības konferenci un izveidojis vietni[30], kas satur kiberdrošības resursus darba vietā.

Latvijas Drošāka interneta centrs[31] piedāvā arī bezmaksas tiešsaistes seminārus studentiem par drošību internetā. Turpretī Latvijas Pašvaldību mācību centrs pieaugušajiem piedāvā kursus par drošu interneta un sociālo mediju lietošanu.

[30] Kiberdrošības kampaņa, URL https://www.esidross.lv/
[31] Latvijas Drošāka interneta centrs, URL https://drossinternets.lv/lv/nodarbibas

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

2.5. Lietuva

Lielākā daļa Lietuvas universitāšu un koledžu piedāvā bakalaura un maģistra studijas datorzinātnēs vai kiberdrošības jomā. Lietuvas augstskolu bakalaura grāds ir no 180 līdz 240 ECTS kredītpunktiem un maģistra grāds ir no 90 līdz 120 ECTS kredītpunktiem. Studiju programmas tiek pasniegtas lietuviešu un angļu valodās.

8. tabula Augstākās izglītības studiju programmu paraugs kiberdrošības jomā Lietuvā

Programmas nosaukums	**Informācijas sistēmas un kiberdrošība**	**Informācija un informācijas tehnoloģiju drošība**	**Kiberdrošības pārvaldība**
Programmas veids	Studiju programma	Studiju programma	Studiju programma
Studiju joma	Bakalaura grāds skaitļošanā	Maģistra grāds kiberdrošības inženierijā	Maģistra grāds biznesa vadībā
Izglītības līmenis	Bakalaura grāds	Maģistra grāds	Maģistra grāds
Organizējošā institūcija	Viļņas Universitāte	Viļņas Ģedimina tehniskā universitāte	Mykolas Romeris universitāte
Valoda	Latviešu un angļu	Angļu	Latviešu un angļu
Ilgums	210 ECTS	120 ECTS	90 ECTS
Mērķa grupa	Vidusskolas absolventi	Bakalaura vai līdzvērtīga līmeņa studenti	Bakalaura vai līdzvērtīga līmeņa studenti
Tēmas vai moduļi	Algoritmu teorija un datu struktūras; Matemātika; Kiberdrošības juridiskie noteikumi; Ievads programmēšanā; Informācijas sistēmas un datu bāzes; Digitālā kriminālistika; Operētājsistēmas un to drošība; Programmēšanas valodas; WWW izstrādes tehnoloģijas; Informācijas sistēmu izveide; E-darījumi un to drošība; Ētiskā uzlaušana; **Informācijas drošība un risku vadība**; **Datoru tīkli un to drošība**; Datu drošība un kriptogrāfija; Datoru infrastruktūras projektēšana; Virtuālās sistēmas; Datu ieguve; Informācijas sistēmu testēšana un kvalitātes nodrošināšana; Digitālā satura kriminālistikas analīze un ļaunprogrammatūras analīze.	Informācijas tehnoloģiju drošības metodes; Datu bāzes un elektronisko dokumentu drošība; Kriptogrāfijas sistēmas; Zinātniskās izpētes un inovāciju pamati; Datoru tīkli un operētājsistēmu drošība; Virtuālā infrastruktūra un mākoņdatošanas drošība; Ētiskās uzlaušanas metodes; Kibernoziegumu kriminālistika; **Informācijas drošības vadība** ; Droša programmēšana **.**	Studijas ietver sistēmu un tīkla drošības metodes, kriptogrāfiju, ētiskas ielaušanās tehnoloģijas, kibernoziegumu izmeklēšanu, informācijas drošības pārvaldību un citus specifiskus kursus. Obligātie kursi: E-pārvaldības un e-demokrātijas lēmumi; Kiberdrošības tiesiskā vide; Kiberdrošības pārvaldība; Sabiedrisko attiecību stratēģija; **Privātums un datu aizsardzība**; Drošības ekonomika; Intelektuālais īpašums; IT projektu vadība; Elektroniskās informācijas drošības modelēšana.

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

Nevienā no analizētajām AII studiju programmām Lietuvā netiek mācīta pikšķerēšana vai sociālā inženierija kā atsevišķs modulis. Tomēr informācija par šīm tēmām varētu būt iekļauta citos kursu moduļos, piemēram, *Kiberdrošība; Informācijas drošība un riska vadība; Datortīkli un to drošība; Privātums un datu aizsardzība u.t.t.*

Pretēji Latvijā un Igaunijā piedāvātajām studiju programmām gan bakalaura, gan maģistra studijas Lietuvā, šķiet, ir vērstas galvenokārt uz studentu speciālo prasmju attīstīšanu, mazāk uzsverot vispārīgo prasmju nozīmi .

9. tabula Apmācību kursu paraugs kiberdrošības jomā Lietuvā

Programmas nosaukums	**ESET attālinātā kiberdrošības zināšanu apmācība**	**IT drošības izpratnes apmācība**	**Kiberdrošības pamati patērētājiem**
Programmas veids	Apmācības kurss	Apmācības kurss	Apmācības kurss
Studiju joma	Kiberdrošība	Kiberdrošība	Kiberdrošība
Izglītības līmenis	Sertifikācija	Sertifikācija	Sertifikācija
Organizators	ESET	UAB "Hermitage Solutions"	Viļņas Universitāte
Valoda	Lietuviešu	Lietuviešu	Lietuviešu
Ilgums	2 stundas	6 stundas	8 stundas
Mērķa grupa	Uzņēmumi un darbinieki	Uzņēmumu vadītāji, IT drošības vadītāji, uzņēmumi, darbinieki un sabiedrība	Sabiedrība kopumā
Tēmas vai moduļi	**Pikšķerēšana;** Attālināts darbs; Savienojuma izveide ar korporatīvo tīklu; Profilakses pasākumi; Draudu pārskats; Paroļu politika; Interneta drošība; Lietu internets; E-pasta aizsardzība; Praktiski padomi	Kāpēc IT drošības prasme ir svarīga ikvienam? Draudu atpazīšana; Fiziskā datu aizsardzība; Paroles; **Sociālā inženierija; Pikšķerēšana** ; Mobilā datu aizsardzība; Personas datu aizsardzība.	Personas datu drošības principi; spēcīgas paroles; darbības sociālajos tīklos; Wi-Fi izmantošanas principi; **Sociālā inženierija** (populārākie sociālās inženierijas uzbrukumi; kā atpazīt sociālās inženierijas uzbrukumus; drošības pasākumi).

Vairākas valsts un privātās organizācijas piedāvā kiberdrošības apmācības kursus IT profesionāļiem, uzņēmumiem, darbiniekiem un plašākai sabiedrībai. Ir arī vairākas organizācijas, kas kiberdrošības jomā organizē individuāli pielāgotus kursus, kuru mērķauditorija ir uzņēmumi un to darbinieki. Kursi ietver pikšķerēšanas un sociālās inženierijas tēmas, un to ilgums svārstās no pāris stundām līdz vairākām dienām.

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

Eiropas Komisijas atbalsts šīs publikācijas izstrādei nav uzskatāms par tās satura apstiprinājumu, publikācijas saturs ir vienīgi tās autoru viedokļa atspoguļojums un Komisija neuzņemas atbildību par jebkādu publikācijā iekļautās informācijas izmantošanu. (Projekta Nr .: 2020-1-LT01-KA203-078070)

2020. gadā “Radi Lietuvu” komanda sadarbībā ar Valsts aizsardzības ministriju un Nacionālo Kiberdrošības centru veica pētījumu un izdeva ceļvedi“Kiberdrošība un bizness. Kas jāzina katram uzņēmuma vadītājam[32]”. Ceļvedī ir apspriesta kiberdrošības nozīme un sniegti praktiski padomi apdraudējuma risku novērtēšanai un ieteikumi potenciālo kiberincidentu pārvaldībai utt.

[32] Radi Lietuvu (2020): “Kiberdrošība un bizness. Kas jāzina katram uzņēmuma vadītājam ”, UR https://www.enterpriselithuania.com/naujienos/isleistas-leidinys-kibernetinis-saugumas-ir-verslas-ka-turetu-zinoti-kiekvienas-imones-vadovas/ (skatīts 17.03.2021.)

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

2.6. Malta

Galvenās augstākās izglītības iestādes, kas piedāvā datorzinātņu vai kiberdrošības studiju programmas, ir Maltas Universitāte (UoM) un Maltas Mākslas, zinātnes un tehnoloģijas koledža (MCAST). Maltas universitātēs bakalaura programma ietver no 180 līdz 240 ECTS kredītpunktiem un maģistra programma no 60 līdz 120 ECTS kredītpunktiem. Studiju programmas tiek pasniegtas angļu valodā.

10. tabula Augstākās izglītības studiju programmu paraugs kiberdrošības jomā Maltā

Programmas nosaukums	**Zinātne informācijas tehnoloģijās**	**Informācija un informācijas tehnoloģiju drošība**	**Informācijas tehnoloģija un sistēmas**
Programmas veids	Studiju programma	Studiju programma	Studiju programma
Studiju joma	Maģistra grāds kiberdrošībā	Maģistra grāds kiberdrošības inženierijā	Maģistra grāds informācijas tehnoloģijā un sistēmās
Izglītības līmenis	Bakalaura grāds	Maģistra grāds	Maģistra grāds
Organizējošā institūcija	STC Higher Education	Amerikas Maltas universitāte	Maltas Mākslas, zinātnes un tehnoloģijas koledža
Valoda	Angļu	Angļu	Angļu
Ilgums	180 ECTS	96 ECTS	90 ECTS
Mērķa grupa	Vidusskolas absolventi	Bakalaura vai līdzvērtīga līmeņa studenti	Bakalaura vai līdzvērtīga līmeņa studenti
Tēmas vai moduļi	Skaitļošanas prasmes; Datoru sistēmas; Datoru tīkli; Datu bāzes; Tīmekļa vietnes projektēšana un izstrāde; Programmatūras izstrādes paņēmieni; Uz objektu orientētu programmu dizains un izstrāde; Biroja risinājumu izstrāde; **Kiberdrošības arhitektūra un operācijas**; Datoru tīklošana; Tīkla drošība; Ētiskā uzlaušana; Uz objektu orientēta projektēšana un programmēšana; Datu ieguve; Uzlabotie tīkli; Digitālā kriminālistikas risku un **kiberdrošības pārvaldība**; Sistēmu arhitektūra un lietu internets; Projekts un profesionalitāte ar kiberdrošības artefaktu; Kiberizlūkošana.	Informācijas tehnoloģiju drošības metodes; Datu bāzes un elektronisko dokumentu drošība; Kriptogrāfijas sistēmas; Zinātniskās izpētes un inovāciju pamati; Datoru tīkli un operētājsistēmu drošība; Virtuālā infrastruktūra un mākoņdatošanas drošība; Ētiskās uzlaušanas metodes; Kibernoziegumu kriminālistika; **Informācijas drošības vadība** ; Droša programmēšana **.**	Informācijas sistēmas un vadība; Operētājsistēmas un mākoņdatošana; Tīkla protokoli un tīkla automatizācija; Datu zinātne un predikatīvā analīze; **Kiberdrošības pamati**; Tīmekļa tehnoloģijas un droša e-komercija; Mobilā skaitļošana un 5G tīklošana; Lietu internets (IoT); Finanšu skaitļošana un kriptovalūta; **Uzņēmējdarbības un inovāciju vadība.**

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

Tāpat kā citās analizētajās valstīs (izņemot Igauniju), arī Maltas augstākās izglītības studiju programmas pikšķerēšanu vai sociālo inženieriju nepiedāvā kā atsevišķu moduli. Tomēr informācija par šīm tēmām var būt iekļauta citu kursu moduļos, piemēram, *Kiberdrošības vadība, Kiberdrošības arhitektūra un operācijas, Informācijas drošības vadība, Kiberdrošības pamati, Drošība un informācijas nodrošināšana* u.t.t.

Lielākā daļa studiju programmu ir vērstas uz prasmju pilnveidošanu. No visām analizētajām studiju programmām, tikai Maltas Mākslas, zinātnes un tehnoloģijas koledža un Maltas Universitāte piedāvā studiju moduļus, kas koncentrējas uz vispārīgajām prasmēm, piemēram, *Uzņēmējdarbība un inovāciju vadība; Uzņēmējdarbība: Sāciet savu novatorisko biznesu, Projektu vadību utt.*

11. tabula Apmācību kursu paraugs kiberdrošības jomā Maltā

Programmas nosaukums	**Ētiskas uzlaušanas kurss**	**Sertificēts informācijas sistēmu drošības profesionālis (CISSP)**	**Informācijas un kiberdrošības speciālists**
Programmas veids	Apmācības kurss	Apmācības kurss	Apmācības kurss
Studiju joma	Kiberdrošība	Informācijas sistēmas	Kiberdrošība
Izglītības līmenis	Sertifikācija	Sertifikācija	Sertifikācija
Organizators	ICE Malta	Cybersecurity Malta	Lead training
Valoda	Angļu	Angļu	Angļu
Ilgums	24 stundas	5 dienas	12 dienas / 6 ECTS kredītpunkti
Mērķa grupa	Studenti un vispārēja sabiedrība	Ar IT drošību saistīti speciālisti, revidenti, konsultanti, izmeklētāji vai instruktori.	Vadītāji, informācijas drošības un IT speciālisti, atbilstības amatpersonas, grāmatveži utt.
Tēmas vai moduļi	Ievads ētiskajā uzlaušanā; Tīklu veidošanas pamati; Digitālā pēda un informācijas iegūšana; Skenēšana; Paroles; Tīkla noklausīšanās; **Sociālā inženierija**; Kriptogrāfija; Bezvadu sistēmu uzlaušana	Drošība un risku vadība; Aktīvu drošība; Drošības inženierija; Komunikācija un tīkla drošība; Identitātes un piekļuves pārvaldība; **Drošības incidenti** - sagatavošanās, reaģēšana un atkopšana; Drošības novērtēšana un testēšana; Drošības operācijas; Programmatūras izstrādes drošība.	Informācijas drošības, **kibervērtējumu un reaģēšanas uz incidentiem**, informācijas sistēmu revīzijas un pārvaldības pamati

Vairākas valsts un privātās organizācijas piedāvā kiberdrošības apmācības kursus IT profesionāļiem, ar drošību saistītiem speciālistiem, uzņēmumiem, darbiniekiem, studentiem un plašākai sabiedrībai. Ir arī vairākas privātas organizācijas, kas piedāvā individuālus kursus kiberdrošības un ielaušanās un sociālās inženierijas testēšanas pakalpojumu jomā. Lielākā daļa pārbaudīto apmācības kursu sniedz plašāku skatījumu uz kiberdrošību, nevis koncentrējas tikai uz pikšķerēšanas vai sociālās inženierijas tēmām.

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

2018. gadā Maltā tika uzsākta Nacionālā kiberdrošības izpratnes un izglītības kampaņa. Kampaņas mērķis bija palielināt izpratni par to, kā uzlabot digitālo drošību, uzsverot nepieciešamību pēc garākām parolēm, paroļu īpašībām un nepieciešamību tās regulāri mainīt, palielinot piesardzību attiecībā uz personas datu sniegšanu un iegādi. Kampaņas mērķis bija arī izglītot cilvēkus par surogātpasta ziņojumu identificēšanu, sociālo mediju atbildīgu izmantošanu un pikšķerēšanas fenomenu.

Turklāt sadarbībā ar Finanšu pakalpojumu un digitālās ekonomikas un inovāciju parlamentāro sekretāru tajā pašā gadā Maltas Informācijas tehnoloģiju aģentūra ir uzsākusi jaunu shēmu, lai veicinātu un stiprinātu gatavību kiberdrošībai privātajā sektorā. Shēma palīdz privātajam sektoram novērtēt digitālo aktīvu noturību pret kiberdrošības draudiem un nodrošina darbiniekiem apmācību[33] .

Maltas BeSmartOnline![34] projekta mērķis ir palielināt izpratni un izglītot bērnus, jauniešus un viņu atbalsta tīklu, piemēram, aprūpētājus, vecākus un pedagogus, par drošu interneta lietošanu, izveidojot, uzturot un veicinot ziņošanas iespējas par ļaunprātīgu izturēšanos internetā.

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

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

3. KOPSAVILKUMS UN GALVENIE ATZINUMI

- Kiberdrošības prasmju trūkums ir ietekmējis 74% organizāciju visā pasaulē. 2019. gadā 57% organizāciju bija neaizpildītas kiberdrošības vakances. Šo amatu aizpildīšanai nepieciešamais laiks parasti bija trīs mēneši.

- Viskritiskākais prasmju trūkums ir mākoņdatošanas drošība (33%), lietojumprogrammu drošība (32%), drošības analīze un izmeklēšana (30%).

- Viens no galvenajiem respondentu norādītajiem iemesliem, kāpēc amati paliek neaizpildīti, ir kvalificētu pretendentu trūkums. Gandrīz trešdaļa organizāciju apgalvoja, ka gandrīz 75% kandidātu nav atbilstošas kvalifikācijas šim darbam. Respondentu norādītās būtiskākās prasmju nepilnības bija nepietiekamu prasmju, IT zināšanu trūkums, nepietiekams ieskats uzņēmējdarbībā, kiberdrošības tehniskās pieredzes un praktiskās pieredzes trūkums. Respondentu norādītās būtiskākās prasmju nepilnības bija nepietiekamu prasmju, IT zināšanu trūkums, nepietiekams ieskats uzņēmējdarbībā, kiberdrošības tehniskās pieredzes un praktiskās pieredzes trūkums.

- 2020. gadā kiberdrošības darbaspēka trūkums tika novērtēts kā aptuveni 3,12 miljoni profesionāļu. Turpretī Eiropā vien kiberdrošības darbaspēka trūkums līdz 2022. gadam sasniedza 350 000 strādājošo. To skaits ir divkāršojies, salīdzinot ar 2018. gadā aprēķināto.

- ENISA savā ziņojumā "Kiberdrošības prasmju attīstīšana ES" ir identificējusi četrus galvenos cēloņus, kas varētu veicināt kiberdrošības prasmju trūkumu. Divi no tiem attiecas uz darba vietas jautājumiem, bet pārējie divi ir saistīti ar izglītības un apmācības sistēmas jautājumiem.

- Eiropas Komisija 2013. gadā publicēja savu pirmo kiberdrošības stratēģiju, uzsverot izpratni un prasmju attīstību kā galvenos stratēģiskos mērķus. Kopš 2017. gada visas ES dalībvalstis ir izstrādājušas un publicējušas savas nacionālās kiberdrošības stratēģijas (NCSS).

- Viens no visu projekta partnervalstu nacionālo drošības stratēģiju galvenajiem mērķiem ir kiberizglītības un informētības veicināšana, koncentrējoties uz akadēmiskajām aprindām, sabiedrisko un privāto sektoru un plašāku sabiedrību.

- Visu projekta partnervalstu nacionālās drošības stratēģijās tiek uzsvērta arī publiskā, privātā un akadēmiskā partnerība, lai stiprinātu kiberdrošības sistēmu noturību, ieguldījumi IKT drošībā, personāla apmācībā un studentu kiberdrošības prasmju attīstībā, lai apmierinātu tirgus vajadzības.

- Visu augstākās izglītības iestāžu studiju programmu analīze liecina, ka visās projekta partnervalstīs, izņemot Igauniju, kā pikšķerēšana un sociālās inženierijas tēmas netiek iekļautas kā atsevišķi mācību moduļi. Tomēr informāciju par šīm tēmām var iekļaut citos kursu moduļos. 2 augstskolu studiju programmās Igaunijā ir iekļauti studiju moduļi, kas vērsti uz sociālo inženieriju. Šādu moduļu vidējais ilgums ir 4,5 ECTS.

- Analizētajās augstskolu studiju programmās Igaunijā, Latvijā un Maltā ir iekļauti maģistra līmeņa kursu moduļi vispārīgo prasmju apguvei,, piemēram, komunikācijas prasmes, uzņēmējdarbība, psiholoģija utt. Turpretī AII studiju programmas Kiprā un Lietuvā galvenokārt ir vērstas uz specializētajām prasmēm, mazāk uzsverot vispārīgo prasmju nozīmi.

- Visās partnervalstīs ir vairākas publiskas un privātas organizācijas, kas piedāvā kiberdrošības apmācības kursus, kuru mērķauditorija ir kiberdrošības un IT speciālisti, uzņēmumi, darbinieki un plašāka sabiedrība. Lai gan īsāki apmācības kursi parasti koncentrējas tikai uz dažāda veida draudiem, tostarp pikšķerēšanu, sociālo inženieriju un veidiem, kā sevi pasargāt, ilgāki apmācības kursi sniedz plašāku skatījumu uz kiberdrošību. Ir arī vairākas organizācijas, kas piedāvā ielaušanās un sociālās inženierijas testus uzņēmumiem un to darbiniekiem.

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

Eiropas Komisijas atbalsts šīs publikācijas izstrādei nav uzskatāms par tās satura apstiprinājumu, publikācijas saturs ir vienīgi tās autoru viedokļa atspoguļojums un Komisija neuzņemas atbildību par jebkādu publikācijā iekļautās informācijas izmantošanu. (Projekta Nr .: 2020-1-LT01-KA203-078070)

4. BIBLIOGRĀFIJA:

1. (ISC)2 (2019): (ISC)² pētījums atklāj, ka kiberdrošības darbaspēks visā pasaulē ir pieaudzis līdz 3,5 miljoniem profesionāļu, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study- Atklāj-kiberdrošības-darbaspēks-globāli ir pieaudzis
2. (ISC)2 (2019): Kiberdrošības darbaspēka pētījums, URL https://www.isc2.org/Research/Workforce-Study
3. Cyber Wiser (2021): Izglītība un apmācība valsts kiberdrošības stratēģijā, URL https://www.cyberwiser.eu/latvia-lv
4. Cyber Wiser (2021): Izglītība un apmācība valsts kiberdrošības stratēģijā (MT), URL https://www.cyberwiser.eu/malta-mt
5. Cyber Wiser (2021): Izglītība un apmācība valsts kiberdrošības stratēģijā (LV), URL https://www.cyberwiser.eu/latvia-lv
6. Eiropas Savienības Padome (2021. gads): Padomes secinājumu projekts par ES kiberdrošības stratēģiju digitālajai desmitgadei, 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. Eiropas Komisija (2013): Eiropas Savienības kiberdrošības stratēģija, URL https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
9. Eiropas Komisija (2019): Četri ES pilotprojekti, kas sākti, lai sagatavotu Eiropas kiberdrošības kompetences tīklu, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network
10. Eiropas Komisija (2020): Digitālās Eiropas programma: Piedāvātais finansējums 7,5 miljardu euro apmērā 2021. – 2027. gadam, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027
11. Eiropas Savienības Kiberdrošības aģentūra (2019): Kiberdrošības prasmju attīstīšana ES
12. Eiropas Savienības Kiberdrošības aģentūra (2020): ENISA drošības apdraudējumu aina 2019. – 2020.
13. Lietuvas Republikas valdība (2018): Rezolūcija par valsts kiberdrošības stratēģijas apstiprināšanu, 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): Kiberdrošības stāvoklis 2020. gadā, 1. daļa: Jaunākā globālā informācija par darbaspēku un resursiem, 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. Latvijas Aizsardzības ministrija (2019): Latvija apstiprina jauno kiberdrošības stratēģiju 2019.-2022. gadam, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
17. Latvijas Aizsardzības ministrija (2019): Latvijas kiberdrošības stratēģija 2019. - 2022. gadam, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
18. OCECPR (2012): Kipras Republikas kiberdrošības stratēģija, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus
19. Igaunijas Republika, Ekonomikas un komunikācijas ministrija (2019): Kiberdrošības stratēģija, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
20. Maltas informācijas tehnoloģiju aģentūra (2016): Kipras Republikas kiberdrošības stratēģija, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus

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

Eiropas Komisijas atbalsts šīs publikācijas izstrādei nav uzskatāms par tās satura apstiprinājumu, publikācijas saturs ir vienīgi tās autoru viedokļa atspoguļojums un Komisija neuzņemas atbildību par jebkādu publikācijā iekļautās informācijas izmantošanu. (Projekta Nr .: 2020-1-LT01-KA203-078070)