Projekto Nr. 2020-1-LT01-KA203-078070

IO1 A2: Rezultatai „Kibernetinio saugumo mokymo programų analizė“

ATASKAITA

2021

Partneriai

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/

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Turinys

Lentelių sąrašas

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project №.: 2020-1-LT01-KA203-078070)

Santrumpų sąrašas

CCS	Kipro kompiuterininkų sąjunga (angl. Cyprus Computer Society)
CERT.LV	Latvijos kompiuterinių incidentų tyrimo grupė
CSSS	Kibernetinio saugumo įgūdžių trūkumas (angl. Cybersecurity Skills Shortage)
ESCO	Europos kibernetinio saugumo organizacija (angl. European Cybersecurity Organisation)
ENISA	Europos Sąjungos kibernetinio saugumo agentūra (angl. European Union Agency for Cybersecurity)
ES	Europos Sąjunga
HITSA	Informacinių technologijų švietimo fondas (angl. Information Technology Foundation for Education)
ISACA	Informacinių sistemų audito ir kontrolės asociacija (angl. Information Systems Audit and Control Association)
ISC2	Tarptautinis informacinių sistemų saugumo sertifikavimo konsorciumas (International Information System Security Certification Consortium)
NKSC	Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (Lietuvos Respublika)
NKSS	Nacionalinės kibernetinio saugumo strategijos
OCECPR	Elektroninių ryšių ir pašto reguliavimo komisaro biuras (Kipro Respublika)
RIA	Informacinių sistemų tarnyba (Estijos Respublika) (angl. Information System Authority)
MVI	Mažos ir vidutinės įmonės

Funded by the Erasmus+ Programme of the European Union

1. ĮVADAS

1.1. Kibernetinio saugumo gebėjimų trūkumas ir to priežastys

Remiantis kasmetine įmonių strategijos grupės (angl. „Enterprise Strategy Group“) ir informacinių sistemų saugumo asociacijos (angl. Information Systems Security Association) tyrimu,[1] atliktu 2019 metais, kibernetinio saugumo gebėjimų trūkumą jautė 74 % organizacijų visame pasaulyje. Pagrindinės šio trūkumo pasekmės yra padidintas esamo personalo apkrovimas, negalėjimas išnaudoti kai kurių saugumo technologijų, jaunesniojo ar mažiau patyrusio personalo samdymas vietoj patyrusių specialistų. Labiausiai gebėjimų trūkumą jaučiančios sritys yra saugūs skaičiavimai debesyse (33%), aplikacijų saugumas (32%), ir saugumo analizė ir tyrimai (30%).

Be to remiantis tyrimo, atlikto informacinių sistemų audito ir valdymo asociacijos (angl. Information Systems Audit and Control Association (ISACA)) [2] 2019 metais, rezultatais, 57% organizacijų turi laisvų darbo vietų kibernetinio saugumo srityje. Nurodoma, kad vidutinis laikas, siekiant rasti specialistus tokioms pozicijoms užpildyti, yra trys mėnesiai. Tai pažymėjo daugiau nei 60 % tyrime dalyvavusių organizacijų atstovų. Tikimasi, kad darbo vietų skaičius techninio kibernetinio saugumo srityje didės artimiausiais metais. Priešingai kitų darbo vietų skaičius išliks stabilus arba didės nežymiai.

Kaip pažymėjo respondentai, viena iš pagrindinių priežasčių kodėl darbo vietos lieka neužimtos, yra kvalifikuotų darbuotojų trūkumas. Beveik trečdalis organizacijų pažymėjo, kad apie 75% kandidatų neturi reikiamos kvalifikacijos tokiam darbui atlikti. Respondentų pastebėjimu labiausiai trūksta šių kompetencijų: programavimo įgūdžių stoka, IT sistemų architektūros žinios, nepakankamas verslo procesų supratimas, techniniai įgūdžiai ir praktinė patirtis kibernetinio saugumo srityje.

ENISA[3] duomenimis konsultuojantis su ES šalimis-narėmis buvo identifikuota, kad neatitikimas tarp gyventojų realių įgūdžių ir kibernetinio saugumo grėsmių, yra viena iš didžiausių kliūčių kuriant saugią kibernetinę erdvę.

„Nepaisant to, kad kibernetinio saugumo programas visoje Europoje siūlo beveik 600 akademinių institucijų ir mokymo centrų, kibernetinio saugumo įgūdžių trūkumas visuose sektoriuose tebėra didelė problema.“ (ENISA, 2019, p. 10).

Vertinama, kad 2020 metais kibernetinio saugumo specialistų trūkumas siekė apie 3.12 milijonų asmenų[4]. Manoma, kad vien tik Europoje kibernetinio saugumo specialistų deficitas 2022 metais sieks 350 000 darbuotojų. Šis skaičius bus dvigubai didesni nei 2018 metais[5].

Kibernetinio saugumo įgūdžių trūkumo priežastys

ENISA savo „Cybersecurity skills development in the EU“ ataskaitoje pažymėjo, kad yra keturios pagrindinės priežastys sąlygojančios kibernetinio saugumo įgūdžių trūkumą. Dvi iš jų yra susijusios su darbo vietos problematika, o kitos dvi susijusios su švietimo ir apmokymo reikalais. Tiksliau:

1. *Kibernetinio saugumo darbų rinka yra santykinai nauja ir dinamiška*. To pasėkoje reikalavimai darbo vietai labai priklauso nuo organizacijos dydžio veiklos sektoriaus. Pvz. Mažos ir

[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 (žiūrėta 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 (žiūrėta 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 (žiūrėta 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 (žiūrėta 09/03/2021)

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

Funded by the Erasmus+ Programme of the European Union

vidutinės įmonės (MVĮ), kurios nesispecializuoja kibernetinio saugumo srityje stengiasi įsidarbinti universalios kvalifikacijos IT specialistus, turinčius ir IT žinių. Priešingai didelės įmonės ir tos, kurios specializuojasi kibernetinio saugumo srityje, įdarbina darbuotojus besispecializuojančius konkrečiose kibernetinio saugumo srityse.

2. *Darbdaviai nepasiūlo tinkamo lygio apmokymo*. Tai neužtikrina tvaraus tinkamos kvalifikacijos darbuotojų parengimo bei esamų darbuotojų tinkamo kvalifikacijos kėlimo. Tai taip pat sukelia problemas kibernetinio saugumo specialistų, turinčių universalesnės prigimties pasirengimą toliau tobulėti pasirinktoje specializacijoje.
3. *Akademinės institucijos neparengia absolventų, turinčių reikiamas žinias ir įgūdžius.* Studentams trūksta realios praktinės patirties, kas sąlygoja gebėjimų neatitikimą tarp to, ko reikia verslui ir tų gebėjimų, kuriuos turi studentai.
4. *Kibernetinio saugumo mokymo turinys prastai adaptuojamas į pokyčius šioje srityje.* Dėl biurokratinių trukdžių kibernetinio mokymo programų turinys iki šiol prastai adaptuojamas į naujas ir kylančias saugumo grėsmes ir naujų gebėjimų poreikių tenkinimą.

1.2. Skaitmeninio ir kibernetinio saugumo edukacinė politika

2013 metais Europos Komisija paskelbė pirmąją kibernetinio saugumo strategiją, kurioje pabrėžtas problemos suvokimo stiprinimas ir gebėjimų vystymas kaip esminiai strateginiai tikslai.

“2017 metais Europos Komisija ir atstovas sąjungos užsienio reikalams ir saugumo politikai (angl. High Representative of the Union for Foreign Affairs and Security Policy) dar kartą pabrėžė, kad kibernetinis saugumas turi svarbų švietimo aspektą ir, kad veiksmingas kibernetinis saugumas labai priklauso nuo atitinkamų žmonių įgūdžių. Jie rekomendavo ES kartu su valstybėmis narėmis stiprinti kibernetinio saugumo švietimą ir įgūdžius, remiantis Skaitmeninių įgūdžių ir darbo vietų koalicijos darbu ir steigiant Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir nacionalinių kibernetinio saugumo koordinavimo centrų tinklą.” (ENISA, 2019, p.23)

2019 metais keturi Horizon 2020 programos projektai CONCORDIA, ECHO, SPARTA ir CyberSec4Europe[6] buvo pradėti vykdyti, siekiant sukurti bendrą Europos kibernetinio saugumo kompetencijų tinklą ir Europos kibernetinio saugumo tyrimų ir inovacijų planą.

2020 metais Europos Komisija pasiūlė Skaitmeninės Europos Programą,[7] ES programą, kuria siekiama paspartinti skaitmeninę Europos transformaciją. Numatoma, kad pagal šią programą bus skirta 580 mln. eurų pažangiems skaitmeniniams įgūdžiams ugdyti, remiant specializuotų programų ir stažuočių, skirtų būsimiems pagrindinių gebėjimų sričių, pavyzdžiui, dirbtinio intelekto, kibernetinio saugumo, kvantinės technologijos ir kt. specialistams, kūrimą ir įgyvendinimą. ir t.t.

2021 m. kovo mėn. Europos Taryba patvirtino naujas išvadas apie ES Kibernetinio saugumo strategiją[8]. Išvadose pripažįstamas skaitmeninių ir kibernetinio saugumo įgūdžių trūkumas ir pabrėžiama, kad reikia patenkinti rinkos paklausą toliau plėtojant švietimo ir mokymo programas.

[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 (žiūrėta 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 (žiūrėta 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 (žiūrėta 24/03/2021)

Funded by the Erasmus+ Programme of the European Union

1.3. Nacionalinės kibernetinio saugumo strategijos (NKSS)

Nuo 2017 metų visos ES šalys narės sukūrė ir paskelbė savo nacionalines kibernetinio saugumo strategijas (NKSS).

Kipras

Kipro Respublika supranta kibernetinio švietimo svarbą, siekiant užtikrinti nacionalinę kibernetinės erdvės apsaugą. Vienas iš pagrindinių esamos kibernetinio saugumo strategijos tikslų – skatinti kibernetinį saugumą ir didinti visuomenės (piliečių, darbo jėgos ir jaunimo) sąmoningumą bei kurti bendradarbiavimo atmosferą strategijai įgyvendinti.

Kipro Respublikos kibernetinio saugumo strategija buvo parengta 2012 metais[9]. Kipro nacionaline strategija siekiama plėtoti techninį mokymą kibernetinio saugumo srityje ir mokyti, kaip apsisaugoti ir spręsti neatidėliotinas situacijas. Vienas iš tikslų – turėti specializuotų darbuotojų, galinčių susidoroti su tikromis kibernetinėmis atakomis. Tuo tikslu turėjo būti surengtos pratybos, kuriose būtų stebima, kaip darbuotojai susidoroja su imituota realia krize. Įgyvendinant strategiją turėtų būti įtvirtinti kibernetinės specializacijos pareigybių aprašymai ir sertifikatai.

Strategija apima 17 specifinių veiklų. Šios veiklos apima esamo tinkamo personalo reikiamų apmokymo programų identifikavimą, specialistų sertifikavimą kibernetinio ir skaitmeninio saugumo srityje. Kipro Respublika taip pat siekia užmegzti viešojo ir privačiojo sektorių partnerystę ir remti aukštojo mokslo institucijas, įtraukiant kibernetinio saugumo dalykus ir stiprinant kibernetinio saugumo srities specialistų ir mokslininkų rengimą.

Naujausia nacionalinės kibernetinio saugumo strategijos dokumento versija parengta 2020 metais. Šiuo metu ji peržiūrima ir laukia galutinio patvirtinimo iš Susisiekimo ministerijos ir Ministrų tarybos.

Skaitmeninio saugumo tarnyba (angl. Digital Security Authority, DSA)[10] yra nepriklausoma vyriausybinė agentūra prižiūrima elektroninių ryšių ir pašto reguliavimo komisijos. Ji atsakinga už Europos tinklų ir informacijos saugumo (angl. Network and Information Security, NIS) direktyvos įgyvendinimą, sutelkiant dėmesį į visų esminių paslaugų ir kritinės informacinės infrastruktūros operatorių Kipre kibernetinio saugumo kompetencijų gerinimą ir jų aukšto lygio palaikymą. Agentūra taip pat siekia pagerinti kibernetinio saugumo svarbos suvokimą visuomenėje ir padidinti bendrą Kipro tarptautinį konkurencingumą.

Kita svarbi organizacija yra Kipro kompiuterininkų sąjunga (Cyprus computer society, CCC)[11], nepriklausoma nepelno siekianti organizacija įkurta 1984 metais. Organizacija vysto, tobulina ir populiarina Kipro IT sektorių. KKS siekia nustatyti aukštus standartus IT sektoriaus profesionalams, įvertinant tai, kokią svarbą informacinės ir ryšių technologijos turi užimtumui, verslui, visuomenei ir piliečių gyvenimo kokybei. Vienas iš kasmetinių KKS renginių yra Kibernetinio saugumo iššūkis[12]. Šiuo renginiu siekiama atrasti informatikos talentus ir motyvuoti jaunimą siekti karjeros kibernetinio saugumo srityje.

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

Funded by the Erasmus+ Programme of the European Union

Estija

Estija buvo viena iš kibernetinio saugumo strategijų skelbimo pradininkių ir šiuo metu turi jau trečią nacionalinio kibernetinio saugumo dokumento versiją[13]. Strategija suskirstyta į keturias sritis: 1. Darni skaitmeninė visuomenė; 2. Kibernetinio saugumo pramonė, moksliniai tyrimai ir plėtra; 3. Pirmaujantis tarptautinis pagalbininkas; 4. Kibernetinio saugumo visuomenė.

Estijos strategijoje siekiama stiprinti kibernetinį švietimą, o jo pritaikomumas aprašytas antrajame plano tiksle. Nuo 2014 m. šalis investuoja į švietimą ir sudarinėja sandorius su universitetais, siekdama skatinti kibernetines studijas, finansuoja projektus ir remia stipendijas. Siekiama užtikrinti, kad skaitmeninių technologijų ir kibernetinio saugumo kompetencijos būtų įtrauktos į kontaktinius mokymus ir paruošti visuomenę kibernetinio saugumo supratimui.

Švietimo ir mokslo ministerija prižiūri šiuos švietimo projektus ir laikosi Kibernetinio saugumo strategijoje nustatytų prioritetų, kad būtų vykdomas mokymosi visą gyvenimą planas ir remiamas bazinio kibernetinio išsilavinimo plėtojimas visų lygių absolventams.

Pagal strategiją strateginių tikslų įgyvendinimą remia Informacinių technologijų švietimo fondas (HITSA), kuris prisideda prie šios srities specialistų rengimo koordinuodamas programas „Targalt Internetis“ (angl. „Staying Smart Online“) ir „IT akademija“.

Kita svarbi organizacija yra Informacinių sistemų tarnyba (angl. Information System Authority, RIA),[14] kuri koordinuoja informacinių sistemų kūrimą ir administravimą, organizuoja su informacijos saugumu susijusią veiklą ir nagrinėja saugumo incidentus. RIA taip pat atlieka pagrindinį vaidmenį kibernetinės higienos, prevencinės veiklos ir visuomenės sąmoningumo didinimo srityje.

„Siekiant skleisti informaciją apie kibernetines grėsmes įvairioms tikslinėms grupėms, įskaitant įmones, bus pradėtos plataus masto prevencijos ir sąmoningumo didinimo kampanijos. Siekiant pakelti kibernetinės higienos lygį valstybės institucijose, valstybės institucijų ir vietos valdžios institucijų darbuotojams taps privaloma išlaikyti kibernetinio saugumo žinių testus. Bus tęsiami tikslinėms grupėms skirti mokymo kursai ir informacinė sklaida“ (Estijos Respublika, Ekonomikos ir komunikacijų ministerija, 2019, p. 64).

[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 (žiūrėta 10/03/2021)
[14] Information System Authority (RIA), URL https://www.ria.ee/en.html

Funded by the Erasmus+ Programme of the European Union

Latvija

Latvijoje susirūpinimas nacionalinius saugumu glaudžiai siejamas su šiuolaikinių technologinių vystymusi. Pirma Latvijos kibernetinio saugumo strategija buvo patvirtinta 2014 metais su detalizuotais planais 2014-2018 metams. 2019 metais buvo patvirtinta nauja kibernetinio saugumo strategija 2019-2022 metams. Atnaujinta strategija siekiama stiprinti ir tobulinti Latvijos kibernetinio saugumo pajėgumus didinant visuomenės sąmoningumą ir atsparumą kibernetinėms atakoms. Šiems tikslams pasiekti strategijoje siūlomi veiksmai šešiose srityse[15]:

1. Sustiprintas kibernetinis saugumas ir valdomos skaitmeninio saugumo rizikos;
2. Informacinių ir ryšių technologijų sistemų atsparumas;
3. Geresnė visuotinė prieiga prie strateginių IRT sistemų ir paslaugų;
4. Visuomenės informavimas, švietimas ir moksliniai tyrimai;
5. Tarptautinis bendradarbiavimas;
6. Teisinės valstybės principų kibernetinėje erdvėje ir elektroninių nusikaltimų prevencijos.

Kalbant apie „Visuomenės informavimas, švietimas ir moksliniai tyrimai“ sritį, strategija išskiria penkis pagrindinius uždavinius[16]:

- teikti paramą mokslinių tyrimų plėtrai kibernetinio saugumo srityje;
- didinti besimokančiųjų ir pedagogų sąmoningumą informacijos saugumo, privatumo apsaugos ir patikimų e. paslaugų naudojimo klausimais;
- stiprinti visuomenės sąmoningumą apie saugų naudojimąsi internetu (rengti mokomąją ir informacinę medžiagą įvairioms amžiaus grupėms su saugumo rekomendacijomis, užsiėmimus naudojantis internetu, organizuoti socialines kampanijas). Parengti ir įgyvendinti metinį tarpinstitucinį darbo ir veiksmų planą, skirtą įmonių informavimui ir sąmoningumo didinimui kibernetinio saugumo klausimais;
- skatinti vietos ir valstybės institucijų darbuotojų sąmoningumą apie saugų IRT naudojimą;
- skatinti švietėjišką veiklą ir konkursus kibernetinio saugumo srityje.

Strategijoje taip pat pabrėžiama, kad reikia aktyvesnio viešųjų ir privačiųjų subjektų dalyvavimo stiprinant kibernetinio saugumo sistemų atsparumą ir numatant investicijas į IRT saugumą ir darbuotojų mokymą.

Už kibernetinio saugumo incidentų stebėseną ir jų nagrinėjimą atsakinga Latvijos kompiuterinių incidentų tyrimo grupė (CERT.LV). CERT.LV taip pat organizuoja šviečiamuosius renginius ir mokymo kursus plačiajai visuomenei. Pagal naująją strategiją tikimasi, kad CERT.LV kartu su viešuoju ir privačiuoju sektoriais plėtos išteklius, skirtus rinkti žvalgybinę informaciją apie incidentus, kad juos būtų galima analizuoti ir vertinti[17].

Kita svarbi organizacija yra Latvijos saugesnio interneto centras. Pagrindiniai jo uždaviniai – šviesti, informuoti ir didinti visuomenės sąmoningumą apie saugesnį naudojimąsi internetu, teikti platformą, kurioje karštąja linija galima pranešti apie neteisėtą turinį ir saugumo pažeidimus internete, taip pat teikti profesionalias psichologo konsultacijas per pagalbos liniją[18].

[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 (žiūrėta 11/03/2021)

[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 (žiūrėta 11/03/2021)

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

Funded by the Erasmus+ Programme of the European Union

Lietuva

2018 metais Vyriausybė patvirtino atnaujintą Lietuvos Respublikos nacionalinę kibernetinio saugumo strategiją[19].

„Pagrindinis strategijos tikslas – suteikti Lietuvos visuomenei galimybę išnaudoti informacinių ir ryšių technologijų (IRT) potencialą, efektyviai identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui bei valdant kibernetinių incidentų sukeltas pasekmes.“ Nutarimas dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo, 2018 m. rugpjūčio 13 d. Nr. 818.

Siekiant šio tikslo, strategijoje siūlomi penki uždaviniai:

1. Stiprinti šalies kibernetinį saugumą ir plėtoti kibernetinės gynybos pajėgumus;
2. Užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir tyrimą;
3. Skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą;
4. Stiprinti glaudų privataus ir viešojo sektorių bendradarbiavimą;
5. Stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.

Kibernetinio saugumo kultūros ir inovacijų skatinimas yra pagrindinis nacionalinės strategijos tikslas. Strategijoje siūlomi šie veiksmai šiam konkrečiam tikslui pasiekti [20]:

- Nuolatiniai ir reguliariai atnaujinami mokymo kursai privataus ir viešojo sektoriaus darbuotojams, kuriais siekiama didinti darbuotojų sąmoningumą ir formuoti bendrą kibernetinio saugumo kultūrą;
- Nuolatinis informacijos apie naujausius kibernetinius incidentus skleidimas;
- IRT mokymą įtraukti į ugdymo procesą nuo ankstyvojo amžiaus, pradedant darželinukais ir baigiant vidurine mokykla;
- Nuolatinis mokytojų kvalifikacijos kėlimas ir mokymas, siekiant pagerinti jų kvalifikaciją kibernetinio saugumo srityje.

Strategijoje pabrėžiama būtinybė nuolat tobulinti kibernetinio saugumo įgūdžius ir kompetencijas, kad būtų patenkinti rinkos poreikiai. Šiam tikslui pasiekti strategijoje siūloma „sukurti kibernetinio saugumo kompetencijų modelį ir standartus, kurti mokymo sistemas, akreditaciją ir sertifikavimą, orientuotą į darbo rinkos poreikius, sukurti kibernetinio saugumo mokymo ir testavimo aplinką, siūlyti mokymus IRT darbuotojams ir kt.“ Nutarimas dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo, 2018 m. rugpjūčio 13 d. Nr. 818.

Strategijoje taip pat pabrėžiamas poreikis plėtoti inovacijas kibernetinio saugumo srityje. Šiam tikslui pasiekti labai svarbus pagrindinių viešųjų ir privačiųjų subjektų bei akademinės bendruomenės bendradarbiavimas.

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC)[21] yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už kibernetinių incidentų nagrinėjimą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir informacinių išteklių akreditavimą. NKSC taip pat dirba skatindamas visuomenės sąmoningumą kibernetinio saugumo srityje.

[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

[20] Cyber Wiser (2021): Education and training in national cybersecurity strategy (LT), URL https://www.cyberwiser.eu/lithuania-lt (žiūrėta 11/03/2021)

[21] National Cyber Security Centre, URL https://www.nksc.lt/en/

Funded by the Erasmus+ Programme of the European Union

Malta

Maltos nacionalinė skaitmeninė strategija, dar vadinama Digital Malta[22] buvo paskelbta 2016 metais. Strategija apima trijų pagrindinių nacionalinių suinteresuotųjų subjektų – viešojo sektoriaus, privačiojo sektoriaus ir pilietinės visuomenės – poreikį ir lūkesčius užtikrinti kibernetinį saugumą. Strategijoje išdėstyti penki aspektai, kuriais grindžiama strategija: politika, teisės aktai, rizikos valdymas, kultūra / sąmoningumas ir švietimas.

Strategijoje siūlomi keturi pagrindiniai tikslai:

1. Kovoti su kibernetiniais nusikaltimais nustatant spragas ir stiprinant teisėsaugos institucijų gebėjimus tirti kibernetinius nusikaltimus;
2. Stiprinti nacionalinę kibernetinę gynybą vadovaujant ir padedant viešiesiems ir privatiems subjektams gerinti jų kibernetinės gynybos pajėgumus;
3. Užtikrinti aukštesnį pasitikėjimo kibernetine erdve lygį įgyvendinant sąmoningumo didinimo programas ir teikiant patikimas, IRT paremtas paslaugas;
4. Ugdyti gebėjimus (kibernetinio saugumo supratimą ir švietimą) nustatant ir plėtojant reikalingus įgūdžius ir švietimo sistemas.

Paskutinis pagrindinis tikslas (sąmoningumo didinimas ir švietimas) skirtas akademinei bendruomenei, viešajam ir privačiajam sektoriui bei piliečiams, kad būtų didinamas sąmoningumas, būtų gerinamos žinios, gebėjimai ir kompetencija kibernetinio saugumo srityje vykdant nuolatinę švietimo ir sąmoningumo didinimo kampaniją, taip pat griežtas ir nuolatines švietimo ir mokymo pratybas, skirtas dabartiniams darbuotojams ir jaunajai studentų kartai. Taigi ši priemonė visų pirma apima[23]:

- tolesnį kibernetinio saugumo įgūdžių ir kompetencijų poreikio pripažinimą;
- akademinės ir mokymo programos, skirtos kibernetinio saugumo kompetencijai įtvirtinti;
- esamų mokymo programų, kuriose kibernetiniam saugumui skiriamas dėmesys kartu su IRT ir žiniasklaidos kompetencijomis, peržiūra.

Strategija taip pat siekiama suteikti jaunimui daugiau galių pasitelkiant jų paramos tinklą, t. y. tėvus, globėjus, pedagogus ir su jaunimu dirbančius asmenis. Numatoma, kad „Skaitmeninis pilietiškumas“ taps nacionalinės švietimo programos dalimi, kad vaikai ir jaunimas įgytų įgūdžių, reikalingų saugiai naudotis internetu ir kurti kūrybišką interneto turinį.

Skaitmeninės Maltos strategijoje teigiama, kad vyriausybė įsipareigoja per švietimo įstaigas ir pramonės įmones remti specializuotų švietimo krypčių kūrimą, atsižvelgti į darbo rinkos reikalavimus, rengti mokymo programą ir teikti techninę medžiagą. Reikėtų toliau skatinti su kibernetiniu saugumu susijusias mokymo ir sertifikavimo programas, nes tai yra galimybė veiksmingai padidinti organizacijų saugumo lygį ir tokį padidintą saugumo lygį išlaikyti ilguoju laikotarpiu.

Kibernetinis saugumas Maltoje[24] yra Maltos nacionalinės kibernetinio saugumo strategijos, kuria siekiama sukurti valdymo sistemą, kovoti su kibernetiniais nusikaltimais, stiprinti nacionalinę kibernetinę gynybą ir užtikrinti sąmoningumą bei švietimą kibernetinio saugumo srityje, dalis. Vienas iš pagrindinių Nacionalinės kibernetinio saugumo strategijos tikslų – visoje šalyje vykdoma kibernetinio saugumo sąmoningumo ugdymo ir švietimo kampanija.

[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 (žiūrėta 12/03/2021)

[23] Cyber Wiser (2021): Education and training in national cybersecurity strategy (MT), URL https://www.cyberwiser.eu/malta-mt (žiūrėta 12/03/2021)

[24] Cyber Security Malta, URL https://cybersecurity.gov.mt/

Funded by the Erasmus+ Programme of the European Union

Kita svarbi organizacija yra Maltos nacionalinė reagavimo į kompiuterių saugumo incidentus grupė (CSIRT). CSIRT Malta padeda Maltos ypatingos svarbos infrastruktūros organizacijoms apsaugoti save ir savo duomenis nuo kibernetinių grėsmių ir incidentų[25].

1.4. Projektas „Prevencinės priemonės kovai su fišingu 4-sios pramonės revoliucijos amžiuje“

Kibernetnis saugumas tampa vienu iš didžiausių iššūkių skaitmeniniame amžiuje[26], nes informacija tampa brangiu turtu, susijusiu su didžiuliais duomenų kiekiais, gerėjančiu ryšiu su skaitmenine aplinka. Skaitmeniniai įrenginiai ir informacinės sistemos vis labiau tampa patrauklūs kibernetinėms atakoms.

Viena didžiausių problemų yra sukčiavimas (angl. phishing), nes kibernetiniai nusikaltėliai sukčiavimo kampanijoms vykdyti naudoja greitesnes ir naujoviškas technologines priemones. Todėl turėtų būti sukurta ir plačiai auditorijai laisvai prieinama žmogaus valdomos apsaugos nuo sukčiavimo (angl. phishing) sistema, kurioje aptikimui naudojamas žmogaus instinktas, o atsako masto didinimui – technologijos. Norint sukurti žmogaus valdomą apsaugos nuo sukčiavimo sistemą, reikia šviesti naudotojus, kad jie galėtų atpažinti sukčiavimo atakas ir tinkamai į jas reaguoti.

Vilniaus universiteto Kauno fakulteto ir partnerių inicijuotas tarptautinis projektas „Prevencinės priemonės kovai su fišingu 4-sios pramonės revoliucijos amžiuje“ (CyberPhish) prasidėjo 2020 m. lapkričio pradžioje ir truks dvejus metus.

Projekto tikslas – šviesti aukštųjų mokyklų studentus, dėstytojus, universitetų darbuotojus (bendruomenės narius), švietimo centrus, verslo sektorių (darbdavius ir darbuotojus) ir skatinti tikslinės grupės kritinį mąstymą kibernetinio saugumo srityje.

Projekto partneriai sukurs mokymo programą, el. mokymosi medžiagą, mišrią mokymosi aplinką, žinių ir įgūdžių įsivertinimo bei patikrinimo testus studentams ir kitiems naudotojams, siekiant apsisaugoti nuo fišingo atakų, įgyti kompetencijų, kurios padės atkreipti dėmesį į grėsmes ir imtis reikiamų prevencijos priemonių.

Projekto konsorciumą sudaro šios organizacijos:

1. Vilniaus universitetas, Lietuva (Koordinatorius)
2. Informacinių Technologijų Institutas, Lietuva
3. DOREA Edukacinis Institutas, Kipras
4. Tartu universitetas, Estija
5. Altacom SIA, Latvija
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

Daugiau informacijos apie projektą ir projekto veiklas pateikiama projekto puslapyje: https://cyberphish.eu/.

Naujienos apie projektą ir apie kibernetinį saugumą publikuojamos Facebook puslapyje: https://www.facebook.com/eucyberphish.

[25] Cyber Security Intelligence, URL https://www.cybersecurityintelligence.com/csirt-malta-2727.html (žiūrėta 12/03/2021)

[26] European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020

Funded by the Erasmus+ Programme of the European Union

1. TYRIMO ANALIZĖ

2.1. Duomenų rinkimo metodika

Prieš atliekant esamų studijų programų ir mokymų programų kibernetinio saugumo ir sukčiavimo (angl. *phishing*) srityje tyrimą, šiam tyrimui vadovaujanti organizacija (DOREA Educational Institute) parengė šabloną. Šiame dokumente pateikiama informacija, kurią partneriai turėjo pateikti teikdami aprašymus apie jų šalyse esamus mokymus, susijusius su kibernetiniu saugumu.

Lentelė 1: Programų kibernetinio saugumo ir sukčiavimo srityje analizės šablonas

Programos ar kurso pavadinimas	
Programos tipas	
Studijų sritis	
Laipsnis	
Organizuojanti institucija	
Instrukcijos kalba	
Trukmė (valandomis arba ECTS)	
Tikslinė grupė	
Pagrindinis dėmesys: temos ar moduliai	
Mokymosi rezultatai	
Metodika (jei taikoma)	
Nuoroda / URL	

Partneriams buvo rekomenduojama naudoti kibernetinio saugumo aukštojo mokslo duomenų bazę[27] ir atlikti tyrimus savo šalyje, kadangi kai kurios studijų programos dar nėra įkeltos į esamą duomenų bazę.

Projekto partnerių taip pat buvo paprašyta atlikti trumpus nacionalinės kibernetinio saugumo švietimo politikos / strategijos tyrimus. Tyrimas buvo atliktas visose šalyse partnerėse – Kipre, Estijoje, Latvijoje, Lietuvoje ir Maltoje. Tyrimo analizės rezultatai buvo perkelti į Nacionalinę išvadų lentelę (suskirstyta pagal šalis – Kipras, Estija, Latvija, Lietuva ir Malta).

Surinkti duomenys bus naudojami siekiant nustatyti įgūdžių spragas ir parengti rekomendacijas dėl naujos mokymų programos, siekiant sustiprinti interneto vartotojų įgūdžius, švietimą ir sąmoningumo didinimą apie naujausias iškilusias kibernetinio saugumo problemas ir grėsmes, visų pirma – sukčiavimą (angl. *phishing*).

Remdamasis esamų kibernetinio saugumo studijų programų ir apklausos rezultatais, partnerių konsorciumas parengs mokymų medžiagą, žinių įsivertinimo ir žinių vertinimo testus bei simuliacijos scenarijus.

[27] Kibernetionio saugumo ir aukštojo mokslo duomenų bazė (CyberHEAD) yra didžiausia patvirtinta kibernetinio saugumo aukštojo mokslo duomenų bazė ES ir ELPA šalyse. URL https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/education-courses

Funded by the Erasmus+ Programme of the European Union

2.2. Kipras

Visi žymiausi Kipro universitetai siūlo bakalauro ir magistro studijas informatikos ar kibernetinio saugumo srityse. Kipro universitetų bakalauro laipsnis yra 240 ECTS kreditų ir magistro laipsnis nuo 90 iki 120 ECTS kreditų. Studijų programos dėstomos graikų arba anglų kalbomis.

Lentelė 2. Aukštųjų mokyklų kibernetinio saugumo studijų programų pavyzdžiai Kipre

Programos pavadinimas	**Informatika**	**Kompiuterių ir tinklo sauga**	**Kibernetinis karas (angl. *Cyber Warfare*)**	**Ryšiai ir tinklo sauga**
Programos tipas	Studijų programa	Studijų programa	Studijų programa	Studijų programa
Studijų sritis	Informatikos magistras	Informatikos magistras	Kibernetinio saugumo magistras	Kibernetinio saugumo magistras
Laipsnis	Magistro laipsnis	Magistro laipsnis	Magistro laipsnis	Magistro laipsnis
Organizuojanti institucija	Nikosijos universitetas	Kipro atvirasis universitetas	Centrinio Lankašyro universitetas (UCLAN)	Kipro Europos universitetas
Kalba	Anglų	Anglų	Anglų	Anglų
Trukmė	90 ECTS	90 ECTS	10 ECTS	7 ECTS
Tikslinė grupė	Bakalauro ar jam prilyginto laipsnio studentai	Bakalauro ar jam prilyginto laipsnio studentai	Bakalauro ar jam prilyginto laipsnio studentai	Bakalauro ar jam prilyginto laipsnio studentai
Temos ar moduliai	• Kibernetinės-fizinės sistemos ir daiktų internetas; • Kriptografija ir tinklo sauga; • Paskirstyta sistema; • **Kibernetinis karas (angl. *Cyberwarfare*);** • Etiškas įsilaužimas; • Kibernetinio saugumo projektas; • Tinklo gynyba ir atsakomosios priemonės.	• Ryšių tinklai; • Kompiuterinė ir tinklo kriminalistika; • Kompiuterių ir tinklo sauga; • Kriptografija; • **Informacinių ir ryšių sistemų saugumo rizikos valdymas;** • Tyrimo metodai.	• Kibernetinio karo (angl. *Cyberwarfare*) pagrindai; • Teisinis kibernetinio karo statusas ir etika; • Kibernetinės erdvės mūšio laukas – ginklavimasis kenkėjiškomis programomis (įskaitant psichologinius ginklus: **socialinę inžineriją**, SE taktikos metodus ir procedūras bei kt.); • Internetinės erdvės iššūkiai ir kibernetinio karo ateitis.	• Pagrindinių tinklo principų ir įrenginių atnaujinimas; • Tinklas kaip kibernetinių atakų maršrutas, kaip galima apsaugoti tinklą, pažeidžiamumas, grėsmės; • Tinklo atakos, įskaitant **sukčiavimą** (angl. *phishing*); • Bendra apsauga, prevencija ir aptikimas.

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

Nė vienoje Kipro aukštųjų mokyklų studijų programoje kaip atskiras modulis nėra dėstoma sukčiavimas ar socialinė inžinerija. Vietoj to, šie dalykai yra įtraukti į kai kuriuos kursų modulius, pvz., *„Kibernetinis karas (angl. cyberwarfare)“, „Komunikacijos ir tinklo saugumas“, „Saugumo rizikos valdymas“, „Kibernetinio saugumo rizikos analizė ir valdymas“* ir kt.

Nors kai kuriose bakalauro studijų programose taip pat yra modulių, orientuotų į „minkštuosius įgūdžius“ (angl. *soft skills*) (pvz., viešasis kalbėjimas, psichologija), daugumoje magistro studijų daugiausia dėmesio skiriama studentų „kietųjų įgūdžių“ (angl. *hard skills*) lavinimui, apeinant „minkštuosius įgūdžius“.

Lentelė 3. Mokymo kursų kibernetinio saugumo srityje pavyzdžiai Kipre

Programos pavadinimas	**Kibernetinio saugumo supratimas**	**Sertifikuotas saugus kompiuterio vartotojas (CSCU)**	**„CompTIA Security +“ sertifikatas (SY0-601)**	**Kibernetinio saugumo taikymas**
Programos tipas	Mokymų kursas	Mokymų kursas	Mokymų kursas	Mokymų kursas
Studijų sritis	Kibernetinė sauga	Kibernetinė sauga	Kibernetinė sauga	Kibernetinė sauga
Laipsnis	Pažymėjimas	Pažymėjimas	Pažymėjimas	Pažymėjimas
Organizatorius	Nikosijos universitetas ir pasauliniai mokymai	AKTINA	„New Horizons“ kompiuterių mokymosi centras	Viešojo, kibernetinio ir nacionalinio saugumo institutas
Kalba	Anglų	Anglų	Anglų	Anglų
Trukmė	2 val.	14 val.	5 dienos	12 savaičių (apie 120 val.)
Tikslinė grupė	Verslininkai, vadybininkai, IT darbuotojai, studentai ir kt.	Kompiuterių vartotojai	IT specialistai ir studentai	IT ir kibernetinio saugumo specialistai ir konsultantai
Temos ar moduliai	Kibernetinė sauga; **Socialinė inžinerija / sukčiavimas**; Socialinės žiniasklaidos išpuoliai, netikri įspėjimai; Sukčiavimo el. laiškai; Kenkėjiški el. pašto priedai; Kenkėjiška programinė įranga; „Wi-Fi“ atakos; Slaptažodžiai; Demonstracija.	Operacinių sistemų apsauga; Kenkėjiškos programos ir antivirusinės programos; Interneto apsauga; Saugumas socialinių tinklų svetainėse; El. pašto, mobiliųjų įrenginių, debesų ir tinklo ryšių saugumas; Duomenų atsarginės kopijos ir atkūrimas po nelaimių.	**Grėsmės, išpuoliai ir pažeidžiamumas;** Architektūra ir dizainas; Įgyvendinimas; Operacijos ir reagavimas į incidentus.	Kibernetinis saugumas ir kibernetinė rizika; Kibernetinės rizikos tendencijos, praktinė patirtis; NIST kibernetinio saugumo sistema; Kibernetinių grėsmių nustatymo priemonės ir metodai; Įmonės grėsmės rizikos vertinimų, atitikties ataskaitų ir mažinimo planų kūrimas.

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

Daugelis valstybinių ir privačių organizacijų siūlo kibernetinio saugumo mokymo kursus IT specialistams, studentams, darbuotojams ir plačiajai visuomenei. Kurso trukmė svyruoja nuo poros valandų iki kelių mėnesių. Kai kuriuose mokymų kursuose dalyvis turi laikyti egzaminą, kad gautų pažymėjimą.

Daugumoje ilgesnės trukmės mokymų kursų sukčiavimas ir socialinė inžinerija yra dėstomi kaip atskiri dalykai. Trumpieji mokymų kursai (vienos dienos) daugiausia skirti tik sukčiavimui ir socialinei inžinerijai.

Kai kurias mokymo kursų išlaidas iš dalies subsidijuoja Kipro žmogiškųjų išteklių ir plėtros institucija (HRDA)[28] vykdydama kibernetinio saugumo ir skaitmeninių įgūdžių strategijų veiksmus ir iniciatyvas.

[28] Kipro žmogiškųjų išteklių ir plėtros institucija (HRDA), UR http://www.hrdauth.org.cy/

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

2.3. Estija

Pagrindinės aukštosios mokyklos, siūlančios informatikos ar kibernetinio saugumo studijų programas, yra Talino technologijos universitetas ir Tartu universitetas. Estijos universitetų bakalauro laipsnis yra nuo 180 iki 240 ECTS kreditų ir magistro laipsnis nuo 60 iki 120 ECTS kreditų. Studijų programos dėstomos estų ir anglų kalbomis.

Lentelė 4. Kibernetinio saugumo studijų programų pavyzdžiai Estijoje

Programos pavadinimas	**Kibernetinio saugumo inžinerija**	**Kibernetinis saugumas**	**Kriptografija, SECCLO Erasmus+ specializacija**
Programos tipas	Studijų programa	Studijų programa	Studijų programa
Studijų sritis	Inžinerijos mokslo bakalauras	Inžinerijos mokslo magistras	Inžinerijos mokslo magistras
Laipsnis	Bakalauro laipsnis	Magistro laipsnis	Magistro laipsnis
Organizuojanti institucija	Talino technologijos universitetas (TalTech)	Talino technologijos universitetas (TalTech) ir Tartu universitetas	Tartu universitetas
Kalba	Anglų	Anglų	Anglų
Trukmė	180 ECTS	120 ECTS	120 ECTS
Tikslinė grupė	Vidurinių mokyklų absolventai	Bakalauro ar jam prilyginto laipsnio studentai	Bakalauro ar jam prilyginto laipsnio studentai
Temos ar moduliai	Socialiniai, profesiniai ir etiniai IT aspektai; Elektronika IT srityje; Logika ir diskreti matematika; Bendravimo įgūdžiai; IT infrastruktūros paslaugos; „Linux“ ir „Windows“ administravimas; Tinklų kūrimo pagrindai; Informatikos ir kompiuterių įvadas; **Įvadas į kibernetinį saugumą**; Programavimo pagrindai; Interneto technologijos; Kibernetinio saugumo valdymas; Duomenų bazių pagrindai; Kompiuterių tinklo apsauga; **Socialinė inžinerija**; Registravimas ir stebėjimas; Saugus programavimas.	Kompiuterinis programavimas; Sistemos administravimas; Tinklo technologija; Estų kalba ir kultūra; Verslumas ir verslo planavimas; **Žmogiškieji kibernetinio saugumo aspektai**; Teisiniai kibernetinio saugumo aspektai; Kibernetinio saugumo valdymas; Kibernetinio saugumo technologijos; Kriptografija; Kibernetinių incidentų tvarkymas; Saugus programinės įrangos dizainas; Komandinio darbo projektas; Kompiuterių tinklo apsauga; Informacinių sistemų atakos ir gynyba; Kibernetinis saugumas I ir II; Specialios kriptografijos temos; Mobiliųjų telefonų kriminalistika; Strateginė komunikacija ir kibernetinis saugumas; Duomenų gavyba; Kenkėjiškos programos; Kibernetinės gynybos stebėjimo sprendimai; Privatumą saugančios technologijos; Belaidės technologijos ir saugumas; „Blockchain“; Kriptologija.	Kriptografiniai protokolai; Matematiniai kompiuterijos pagrindai; Tyrimų seminaras kriptografijos srityje; Kriptologija II, kvantinė kriptografija; Tipo teorija; Įvadas į kodavimo teoriją; Mobiliųjų programų kūrimas – projektai, metodai TCS; Speciali užduotis kriptografijoje; Teorinės informatikos projektas; Estų kalba pradedantiesiems I; Magistro lygio seminaras.

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

Analizuotose Estijos aukštųjų mokyklų studijų programose sukčiavimas „phishing“ nėra dėstomas kaip atskiras modulis. Tačiau sukčiavimo dalis gali būti įtraukta į kitus kurso modulius, tokius kaip *„Įvadas į kibernetinį saugumą“, „Kompiuterių tinklo saugumas“* ir kt.

Tačiau Talino technologijos universiteto siūlomoje kibernetinio saugumo inžinerijos studijų programoje socialinė inžinerija yra atskiras modulis. Modulio tikslas yra suteikti studentams pagrindinių žinių apie socialinės manipuliacijos pobūdį (daugiausia atsižvelgiant į IRT) ir pagrindines jos formas, technikas bei metodus (įskaitant hibridines atakas su technologiniu komponentu) ir apsaugą nuo jų. Modulio trukmė yra 3 ECTS kreditai

Talino technologijos universiteto ir Tartu universiteto siūlomoje kibernetinio saugumo studijų programoje yra *žmogiškųjų kibernetinio saugumo aspektų*. Modulio tikslas – apžvelgti kibernetinio saugumo žmogiškuosius aspektus, ypač socialinės manipuliacijos elementus ir apsaugos nuo jų mechanizmus. Modulio trukmė yra 6 ECTS kreditai.

Studijų programose yra daugybė specializuotų studijų modulių, siūlančių gerą įgytų teorinių žinių ir praktinių studijų santykį. Jos taip pat turi „minkštųjų įgūdžių“ kursų modulius, tokius kaip bendravimo įgūdžiai, verslumas, psichologija ir kt.

Lentelė 5. Mokymų kursų kibernetinio saugumo srityje pavyzdžiai Estijoje

Programos pavadinimas	**Žiniatinklio programų sauga**	**Tinklo saugumo administratorius**
Programos tipas	Mokymų kursai	Mokymų kursai
Studijų sritis	Etiškas įsilaužimas	Tinklo sauga
Laipsnis	Pažymėjimas	Pažymėjimas
Organizatorius	Clarified Security	NobleProg
Kalba	Anglų	Anglų
Trukmė	4 dienos	5 dienos
Tikslinė grupė	WebApp programuotojai, prižiūrėtojai, interneto serverių ar prieglobos paslaugų teikėjai / administratoriai, informacijos saugumo specialistai ir kt.	Sistemos administratoriai ir tinklo administratoriai, visi, kurie domisi gynybinėmis tinklo saugumo technologijomis.

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

Temos ar moduliai	Kliento pusės atakos: sauga, informacijos šaltiniai, kliento ir serverio ryšys, HTTP ir HTTPS, HTTP užklausų metodai, „JavaScript“ ir „JavaScript“ injekcijos, URL ir manipuliavimas URL, manipuliavimas slapukais, seansų užgrobimas, seanso taisymas, užklausos dėl klastojimo atakų (CSRF ir OSRF), vartotojo sąsajos atkūrimo išpuoliai, trečiosios šalies turinio naudojimas, kombinuotos kliento atakos). Serverio pusės atakos: autentifikavimas, slaptažodžiai, autorizacijos pažeidžiamumai, verslo logikos problemos, „Google“ įsilaužimai, tinklo serverio konfigūracija ir failų sistema, komandų įvedimas, failų tvarkymas, failų įtraukimo atakos, failų įkėlimas, XXE (XML eXternal Entity) atakos, SQL injekcija.	Įvadas į tinklo saugumą, tinklo protokolus, saugumo politiką, fizinį saugumą, tinklo užpuolimus (dabartinė statistika, terminų apibrėžimas: grėsmės, užpuolimas ir išnaudojimas, įsilaužėlių ir atakų klasifikavimas, šnipinėjimas; šlamštas; **sukčiavimas**; „war dialing“; slaptažodžių nulaužimas, tinklalapio šmeižtas; SQL injekcija; „wire tapping“; „buffer overflow“, „war driving“; „war chalking“), įsilaužimo aptikimo sistema, ugniasienės, paketų filtravimas ir tarpiniai serveriai, „Bastion Host“ ir „Honeypots“, maršrutizatorių stiprinimas, operacinių sistemų saugumo stiprinimas, pataisų valdymas, programų sauga, interneto sauga, el. pašto sauga; šifravimas, virtualūs privatūs tinklai, WLAN, gedimų tolerancijos sukūrimas, reagavimas į incidentus, atkūrimas po nelaimių ir planavimas, tinklo pažeidžiamumo vertinimas.

Yra keletas privačių organizacijų („Clarified Security“, „NoblePro“, „Cyberexer“, „Rangeforce“, „CTF Pärnu“ ir kt.), kurios siūlo mokymų kursus įvairiomis temomis, pvz., e-mokymas, skirtas kibernetinei higienai ir duomenų apsaugai, pažeidžiamumo vizualizavimas, rizikos vertinimas, kibernetinis saugumas, sukčiavimas ir kt. Kursai daugiausia skirti IT specialistams, įmonėms ir plačiajai visuomenei, besidominčiai šia tema. Atsižvelgiant į pateiktą atestaciją, norint gauti sertifikatą, dalyviams gali tekti laikyti egzaminą.

Siekdama padėti vietos verslui kovoti su kibernetinio saugumo grėsmėmis, Estijos informacinės sistemos tarnyba taip pat pradėjo informacinę kampaniją, skirtą mažoms ir vidutinėms įmonėms. Kampanijos metu daugiausia dėmesio skiriama kibernetinių incidentų tipams, kurie pastaraisiais metais įmonėms padarė didžiausią finansinę žalą[29].

[29] Kibernetinio saugumo kampanija, URL https://itvaatlik.ee/

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

2.4. Latvija

Pagrindinės aukštosios mokyklos, siūlančios informatikos ar kibernetinio saugumo studijų programas, yra Turiba universitetas, Rygos technikos universitetas, Vidžemės taikomojo mokslo universitetas, BA verslo ir finansų mokykla. Latvijos universitetų bakalauro laipsnis yra nuo 160 iki 240 ECTS kreditų, o magistro laipsnis - 120 ECTS kreditų. Studijų programos dėstomos latvių ir anglų kalbomis.

Lentelė 6. Aukštųjų mokyklų kibernetinio saugumo studijų programų pavyzdžiai Latvijoje

Programos pavadinimas	**Kompiuterių sistemos**	**Kibernetinio saugumo inžinerija**	**Informacinės technologijos**
Programos tipas	Studijų programa	Studijų programa	Studijų programa
Studijų sritis	Kompiuterių sistemų bakalauras	Kibernetinio saugumo inžinerijos magistras	Informacinių technologijų magistras
Laipsnis	Bakalauro laipsnis	Magistro laipsnis	Magistro laipsnis
Organizuojanti institucija	Turiba universitetas	Rygos technikos universitetas	Vidžemės taikomojo mokslo universitetas
Kalba	Latvių ir anglų	Anglų	Anglų
Trukmė	240 ECTS	120 ECTS	120 ECTS
Tikslinė grupė	Vidurinių mokyklų absolventai	Bakalauro ar jam prilyginto laipsnio studentai	Bakalauro ar jam prilyginto laipsnio studentai
Temos ir moduliai	Anglų ir latvių kalbos; Civilinė ir aplinkos apsauga; Kompiuterių architektūra, Kompiuterių inžinerija ir sistemos; Matematika; Programinės įrangos kūrimo pagrindai; Projektinis mąstymas; Ekonomika ir verslumas; Programinės įrangos testavimas ir kokybė; Kodavimas ir kriptografija; **IT saugumas ir rizikos valdymas**; Mašinų mokymasis ir intelektualioji analizė; Programinės įrangos projektų valdymas; Duomenų analizė ir palyginimas; Žaliosios / IT sistemos ir metodai; Operacijų tyrimų įvadas; Finansai ir apskaita; IT įstatymai ir autorių teisės; Robotika.	**Kibernetinė sauga**; Informacinių sistemų patikimumas; Įmonės informacinių technologijų architektūra; Kritinių infrastruktūrų valdymo pagrindai; Pramonės sauga; **Tinklo saugumas**; Programinės įrangos saugumas; Kriptografija ir duomenų saugumo technologijos; Adaptyvių sistemų projektavimas; Inžinerinių sistemų saugumas; Sociotechninių sistemų modeliavimas; Duomenų gavyba ir žinių atradimas; Projektų valdymas; Saugios elektroninės prekybos technologijos; Duomenų integravimo technologijos; Socialinė atsakomybė ir verslas.	Etiškas įsilaužimas; Atvirkštinės inžinerijos; Tinklo, mobiliojo ir debesų sauga; Skaitmeninė kriminalistika; Saugus programinės įrangos projektavimas; Incidentų valdymas ir reagavimas; Sistemos saugumo inžinerija; Projektų valdymas; Strateginis IRT valdymas; Duomenų gavyba; Bendravimas; Kritinis mąstymas; Socialinės žiniasklaidos analizės seminaras; **Interneto psichologija**; Veikėjų teisės, pareigos ir atsakomybė internete; Duomenų saugumo ir tyrimo įstatymas; Kibernetinio saugumo politika; Informacinių sistemų auditas ir patikimumas; **Informacijos saugumo rizikos valdymas**; Saugumo kultūra; Kriptografija; Inovacijos ir kūrybiškas problemų sprendimas.

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

Analizuojamose aukštųjų mokyklų studijų programose Latvijoje nemokoma sukčiavimo ar socialinės inžinerijos kaip atskirų modulių. Tačiau informacija šiomis temomis gali būti įtraukta į kitus kursų modulius, tokius kaip *„IT saugumas ir rizikos valdymas“, „Tinklo saugumas“, „Kibernetinio saugumo ir informacijos saugumo rizikos valdymas“, „Interneto psichologija“* ir kt.

Kaip ir Estijoje, atrodo, kad siūlomos studijų programos yra plačios ir praktiškai orientuotos, kurso moduliai apima „minkštuosius įgūdžius“, tokius kaip bendravimo įgūdžiai, verslumas, kūrybinis problemų sprendimas ir kt.

Lentelė 7. Mokymų kursų kibernetinio saugumo srityje pavyzdžiai Latvijoje

Programos pavadinimas	**ESET nuotolinės kibernetinio saugumo žinios**	**IT saugumo mokymai vartotojams**	**Kibernetinis saugumas**
Programos tipas	Mokymų kursai	Mokymų kursai	Mokymų kursai
Studijų sritis	Tinklo sauga	Kibernetinio saugumo akademija	Kibernetinė sauga
Laipsnis	Pažymėjimas	Pažymėjimas	Pažymėjimas
Organizatorius	ESET Latvija	Kibernetinio saugumo akademija	„Dialogs AB“ mokymų centras
Kalba	Latvių ir anglų	Latvių, anglų, rusų	Latvių
Trukmė	2 val.	4 val.	1 savaitė (42 val.)
Tikslinė grupė	Įmonės ir jų darbuotojai.	Verslo vadybininkai, IT saugumo vadybininkai, įmonės ir plačioji visuomenė.	Verslo lyderiai, informacinių technologijų kūrėjai, plačioji visuomenė.
Temos ar moduliai	Grėsmių apžvalga (kenkėjiškų programų tipai, sukčiavimo principai ir **socialinė inžinerija**); Slaptažodžių teorija; Darbas nuotoliniu būdu; Saugumas visur; **Apsauga nuo sukčiavimo**; El. Pašto saugumas (šlamštas, **sukčiavimas** ir paprasti sukčiai); Programų valdymas.	Kodėl svarbu žinoti apie IT saugumo grėsmes; Pažinti savo priešą; Fizinis saugumas; Slaptažodžio saugumas; Socialinė inžinerija; **Sukčiavimas**; **SMSishing**; **Vishing**; Asmens duomenų apsauga.	Informacinių technologijų veikimas ir vaidmuo; Informacijos šaltiniai ir jų vaidmuo; **Informacijos saugumo grėsmės**, jų rūšys ir poveikis; Informacijos saugumo valdymo įrankiai ir metodai; Kibernetinio saugumo dokumentų svarba.

Remiantis atliktais tyrimais, kelios organizacijos siūlo kibernetinio saugumo mokymus įmonėms, IT specialistams ir plačiajai visuomenei. Trumpesnės trukmės mokymo kursuose daugiausia dėmesio skiriama tik įvairių rūšių grėsmėms, įskaitant sukčiavimą, socialinę inžineriją ir apsisaugojimo būdus, tačiau ilgesnės trukmės mokymo kursai suteikia platesnę kibernetinio saugumo perspektyvą.

Mokymų teikėjai pirmiausia orientuoti į verslo vadovus, darbuotojus, IT specialistus ir suinteresuotą plačiąją visuomenę.

Nuo 2018 m. Latvijos Respublikos informacinių technologijų saugumo incidentų reagavimo įstaiga (CERT.LV) vykdo akciją „Kibernetinio saugumo pajėgumų gerinimas Latvijoje“.

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

Kampanijos metu CERT.LV sukūrė informacinį vadovą ir vaizdo įrašus, surengė kibernetinio saugumo konferenciją bei sukūrė svetainę[30], kurioje yra kibernetinio saugumo šaltiniai, skirti darbo vietai.

Latvijos saugesnio interneto centras[31] studentams taip pat siūlo nemokamus internetinius seminarus apie saugumą internete. O Latvijos vietinės valdžios mokymo centras siūlo kursus suaugusiems apie saugų interneto ir socialinės žiniasklaidos naudojimą.

[30] Kibernetionio saugumo kampanija, URL https://www.esidross.lv/
[31] Latvijos saugesnio interneto centras, URL https://drossinternets.lv/lv/nodarbibas

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

2.5. Lietuva

Lietuvos universitetai ir kolegijos siūlo informatikos ar kibernetinio saugumo srities bakalauro ir magistro studijas. Lietuvos aukštojo mokslo bakalauro laipsnis yra nuo 180 iki 240 ECTS kreditų, o magistro laipsnis – nuo 90 iki 120 ECTS kreditų. Studijų programos dėstomos lietuvių ir anglų kalbomis.

Lentelė 8. Aukštųjų mokyklų kibernetinio saugumo studijų programų pavyzdžiai Lietuvoje

Programos pavadinimas	**Informacinės sistemos ir kibernetinis saugumas**	**Informacijos ir informacinių technologijų saugumas**	**Kibernetinio saugumo valdymas**
Programos tipas	Studijų programa	Studijų programa	Studijų programa
Studijų sritis	Kompiuterijos bakalauras	Kibernetinio saugumo inžinerijos magistras	Verslo vadybos magistras
Laipsnis	Bakalauro laipsnis	Magistro laipsnis	Magistro laipsnis
Organizuojanti institucija	Vilniaus universitetas	Vilniaus Gedimino technikos universitetas	Mykolo Riomerio universitetas
Kalba	Lietuvių ir anglų	Anglų	Lietuvių ir anglų
Trukmė	210 ECTS	120 ECTS	90 ECTS
Tikslinė grupė	Vidurinių mokyklų absolventai	Bakalauro ar jam prilyginto laipsnio studentai	Bakalauro ar jam prilyginto laipsnio studentai
Temos ar moduliai	Algoritmo teorija ir duomenų struktūros; Matematika; Kibernetinio saugumo teisiniai reglamentai; Programavimo įvadas; Informacinės sistemos ir duomenų bazės; Skaitmeninė kriminalistika; Operacinės sistemos ir jų apsauga; Programavimo kalbos; WWW kūrimo technologijos; Informacinių sistemų kūrimas; E. operacijos ir jų saugumas; Etiniai įsilaužimai; **Informacijos saugumas ir rizikos valdymas; Kompiuteriniai tinklai ir jų apsauga**; Duomenų saugumas ir kriptografija; Kompiuterių infrastruktūros projektavimas; Virtualios sistemos; Duomenų gavyba; Informacinių sistemų testavimas ir kokybės užtikrinimas; Kriminalistinė skaitmeninio turinio analizė ir kenkėjiškų programų analizė.	Informacinių technologijų saugumo metodai; Duomenų bazės ir elektroninių dokumentų apsauga; Kriptografinės sistemos; Mokslinių tyrimų ir inovacijų pagrindai; Kompiuterių tinklai ir operacinės sistemos sauga; Virtuali infrastruktūra ir debesų kompiuterijos sauga; Etinės įsilaužimo technikos; Kibernetinė kriminalistika; **Informacijos saugumo valdymas**; Saugus programavimas**.**	Studijos apima sistemos ir tinklo saugumo metodus, kriptografiją, etines įsilaužimo technologijas, elektroninių nusikaltimų tyrimą, informacijos saugumo valdymą ir kitus specifinius kurso padalinius. Privalomi kursai: E. valdymo ir elektroninės demokratijos sprendimai; Teisinė kibernetinio saugumo aplinka; **Kibernetinio saugumo valdymas**; Viešųjų ryšių strategija; Privatumas ir duomenų apsauga; Saugumo ekonomika; Intelektinė nuosavybė; IT projektų valdymas; Elektroninės informacijos saugumo modeliavimas.

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

Analizuojamose aukštojo mokslo studijų programose Lietuvoje nėra mokoma sukčiavimo ar socialinės inžinerijos kaip atskirų modulių. Tačiau informacija šiomis temomis gali būti įtraukta į kitus kursų modulius, tokius kaip *„Kibernetinis saugumas“, „Informacijos saugumas ir rizikos valdymas“, „Kompiuteriniai tinklai ir jų apsauga“, „Privatumas ir duomenų apsauga“* ir kt.

Priešingai nei siūlomos studijų programos Latvijoje ir Estijoje, tiek bakalauro, tiek magistro studijos Lietuvoje yra orientuotos daugiausia į studentų „sunkiųjų įgūdžių“ ugdymą, mažiau akcentuojant „minkštųjų įgūdžių“ svarbą.

Lentelė 9. Mokymo kursų kibernetinio saugumo srityje pavyzdžiai Lietuvoje

Programos pavadinimas	**ESET nuotolinis kibernetinio saugumo žinių mokymas**	**IT saugumo supratimo mokymai**	**Kibernetinio saugumo vartotojams pagrindai**
Programos tipas	Mokymų kursai	Mokymų kursai	Mokymų kursai
Studijų sritis	Kibernetinė sauga	Kibernetinė sauga	Kibernetinė sauga
Laipsnis	Pažymėjimas	Pažymėjimas	Pažymėjimas
Organizatorius	ESET	UAB „Hermitage sprendimai“	Vilniaus universitetas
Kalba	Lietuvių	Lietuvių	Lietuvių
Trukmė	2 val.	6 val.	8 val.
Tikslinė grupė	Įmonės ir darbuotojai.	Verslo vadybininkai, IT saugumo vadybininkai, įmonės, darbuotojai ir plačioji visuomenė.	Plačioji visuomenė.
Temos ar moduliai	**Sukčiavimas,** nuotolinis darbas; Prisijungimas prie įmonės tinklo; Prevencinės priemonės; Grėsmių apžvalga; Slaptažodžių politika; Interneto apsauga; Daiktų internetas; El. elektroninio pašto apsauga; Praktiniai patarimai.	Kodėl IT saugumo raštingumas yra svarbus visiems; Grėsmės pripažinimas; Fizinė duomenų apsauga; Slaptažodžiai**; Socialinė inžinerija; Sukčiavimas**; Mobilioji duomenų apsauga; Asmens duomenų apsauga.	Asmens duomenų saugumo principai; stiprūs slaptažodžiai; socialinių tinklų veikla; „Wi-Fi“ naudojimo principai; **Socialinė inžinerija** (populiariausios socialinės inžinerijos atakos; kaip atpažinti socialinės inžinerijos išpuolius; saugumo priemonės).

Kelios valstybinės ir privačios organizacijos siūlo kibernetinio saugumo mokymų kursus IT specialistams, įmonėms, darbuotojams ir plačiajai visuomenei. Taip pat yra keletas organizacijų, organizuojančių individualiai pritaikytus kursus, skirtus įmonėms ir jų darbuotojams, kibernetinio saugumo srityje. Kursai apima sukčiavimo ir socialinės inžinerijos temas, jų trukmė svyruoja nuo poros valandų iki kelių dienų.

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

2020 m. „Versli Lietuva“ komanda, bendradarbiaudama su Krašto apsaugos ministerija ir Nacionaliniu kibernetinio saugumo centru, atliko tyrimus ir išleido vadovą „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas[32]“.

Vadove aptariama kibernetinio saugumo svarba, pateikiami praktiniai patarimai vertinant grėsmių riziką ir rekomendacijos, kaip valdyti galimus kibernetinius incidentus ir kt.

[32] Versli Lietuva (2020): „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas“, URL https://www.enterpriselithuania.com/naujienos/isleistas-leidinys-kibernetinis-saugumas-ir-verslas-ka-turetu-zinoti-kiekvienas-imones-vadovas/ (žiūrėta 17/03/2021)

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

2.6. Malta

Pagrindinės aukštosios mokyklos, siūlančios informatikos ar kibernetinio saugumo studijų programas, yra Maltos universitetas (UoM) ir Maltos menų, mokslo ir technologijos kolegija (MCAST). Maltos universitetų bakalauro laipsnis yra nuo 180 iki 240 ECTS kreditų ir magistro laipsnis nuo 60 iki 120 ECTS kreditų. Studijų programos dėstomos anglų kalba

Lentelė 10. Aukštojo mokslo studijų programų kibernetinio saugumo srityje pavyzdžiai Maltoje

Programos pavadinimas	**Informacinių technologijų mokslas**	**Informacijos ir informacinių technologijų saugumas**	**Informacinės technologijos ir sistemos**
Programos tipas	Studijų programa	Studijų programa	Studijų programa
Studijų sritis	Kibernetinio saugumo bakalauras	Kibernetinio saugumo inžinerijos magistras	Informacinių technologijų ir sistemų magistras
Laipsnis	Bakalauro laipsnis	Magistro laipsnis	Magistro laipsnis
Organizuojanti institucija	STC aukštasis mokslas	Amerikos Maltos universitetas	Maltos menų, mokslo ir technologijų kolegija
Kalba	Anglų	Anglų	Anglų
Trukmė	180 ECTS	96 ECTS	90 ECTS
Tikslinė grupė	Vidurinių mokyklų absolventai	Bakalauro ar jam prilyginto laipsnio studentai	Bakalauro ar jam prilyginto laipsnio studentai
Temos ar moduliai	Skaičiavimo įgūdžiai; Kompiuterių sistemos; Kompiuterių tinklai; Duomenų bazės; Svetainės kūrimas; Programinės įrangos kūrimo būdai; Objektinių programų kūrimas; Biuro sprendimų kūrimas; **Kibernetinio saugumo architektūra ir operacijos**; Kompiuterių tinklai; Tinklo saugumas; Etinis įsilaužimas; Objektinis projektavimas ir programavimas; Duomenų gavyba; Pažangūs tinklai; Skaitmeninės teismo medicinos ir **kibernetinio saugumo valdymas**; Sistemų architektūra ir daiktų internetas; Projektas ir profesionalumas naudojant kibernetinio saugumo artefaktą; Kibernetinė žvalgyba.	Informacinių technologijų saugumo metodai; Duomenų bazės ir elektroninių dokumentų apsauga; Kriptografinės sistemos; Mokslinių tyrimų ir inovacijų pagrindai; Kompiuterių tinklai ir operacinės sistemos sauga; Virtuali infrastruktūra ir debesų kompiuterijos sauga; Etinės įsilaužimo technikos; Kibernetinė kriminalistika; **Informacijos saugumo valdymas**; Saugus programavimas.	Informacinės sistemos ir valdymas; Operacinės sistemos ir debesų kompiuterija; Tinklo protokolai ir tinklo automatika; Duomenų mokslas ir nuspėjamoji analizė; **Kibernetinio saugumo pagrindai**; Žiniatinklio technologijos ir saugi elektroninė komercija; Mobilieji kompiuteriai ir 5G tinklai; Daiktų internetas; Finansų skaičiavimas ir kriptovaliutos; **Verslumas ir inovacijų valdymas.**

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

Kaip ir kitose analizuojamose šalyse (išskyrus Estiją), Maltos aukštojo mokslo studijų programos neteikia sukčiavimo ar socialinės inžinerijos kaip atskiro modulio. Tačiau informacija šiomis temomis gali būti įtraukta į kitus kurso modulius, tokius kaip *„Kibernetinio saugumo valdymas“, „Kibernetinio saugumo architektūra ir operacijos“, „Informacijos saugumo valdymas“, „Kibernetinio saugumo pagrindai“, „Saugumas ir informacijos užtikrinimas“* ir kt.

Dauguma studijų programų yra orientuotos į „kietųjų įgūdžių“ ugdymą. Iš visų analizuotų programų tik Maltos menų, mokslo ir technologijų kolegija ir Maltos universitetas siūlo studijų modulius, kuriuose pagrindinis dėmesys skiriamas „minkštiesiems įgūdžiams“, tokiems kaip *verslumas ir inovacijų valdymas, verslumas*: *pradėkite savo novatorišką verslą, projektų valdymas* ir kt.

Lentelė 11. Mokymų kursų kibernetinio saugumo srityje pavyzdžiai Maltoje

Programos pavadinimas	**Etinio įsilaužimo kursai**	**Sertifikuotas informacinių sistemų saugos specialistas (CISSP)**	**Informacijos ir kibernetinio saugumo praktikas**
Programos tipas	Mokymų kursai	Mokymų kursai	Mokymų kursai
Studijų sritis	Kibernetinė sauga	Informacinės sistemos	Kibernetinė sauga
Laipsnis	Pažymėjimas	Pažymėjimas	Pažymėjimas
Organizatorius	ICE Malta	Cybersecurity Malta	Lead training
Kalba	Anglų	Anglų	Anglų
Trukmė	24 val.	5 dienos	12 dienų / 6 ECTS kreditai
Tikslinė grupė	Studentai ir plačioji visuomenė	Su IT saugumu susiję specialistai, auditoriai, konsultantai, tyrėjai ar instruktoriai.	Vadybininkai, informacijos saugumo ir IT specialistai, atitikties pareigūnai, buhalteriai ir kt.
Temos ar moduliai	Įvadas į etinį įsilaužimą; Tinklų pagrindai; Duomenų rinkimas (angl. *footprinting and reconnaissance*); Skenavimas; Slaptažodžiai; Paketų perėmimas (angl. *sniffing*); **Socialinė inžinerija**; Kriptografija; Įsilaužimas į belaides sistemas.	Saugumas ir rizikos valdymas; Turto saugumas; Apsaugos inžinerija; Ryšiai ir tinklo sauga; Tapatybės ir prieigos valdymas; **Saugumo incidentai** – pasirengimas, reagavimas ir atkūrimas; Saugumo vertinimas ir testavimas; Apsaugos operacijos; Programinės įrangos kūrimo saugumas.	Informacijos saugumo pagrindai, **kibernetinis vertinimas ir reagavimas į incidentus**, informacinių sistemų auditas ir valdymas.

Kelios valstybinės ir privačios organizacijos siūlo kibernetinio saugumo mokymo kursus IT specialistams, su saugumu susijusiems specialistams, įmonėms, darbuotojams, studentams ir plačiajai visuomenei. Taip pat yra keletas privačių organizacijų, siūlančių individualius kibernetinio saugumo ir įsiskverbimo bei socialinės inžinerijos testavimo paslaugų kursus. Dauguma nagrinėtų mokymų kursų pateikia platesnę kibernetinio saugumo perspektyvą, užuot susitelkę tik į sukčiavimo ar socialinės inžinerijos temas.

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

2018 m. Maltoje buvo pradėta nacionalinė kibernetinio saugumo ir švietimo kampanija. Kampanija buvo siekiama padidinti supratimą, kaip galima pagerinti skaitmeninį saugumą, pabrėžiant ilgesnių slaptažodžių, charakteristikų poreikį ir bei jų reguliarų keitimą, didinant atsargumą teikiant asmens duomenis ir perkant.

Be to, bendradarbiaudama su finansinių paslaugų, skaitmeninės ekonomikos ir inovacijų parlamentiniu sekretoriumi, tais pačiais metais Maltos informacinių technologijų agentūra pradėjo naują sistemą, skirtą skatinti ir stiprinti pasirengimą kibernetiniam saugumui privačiame sektoriuje. Ši schema padeda privačiajam sektoriui įvertinti savo skaitmeninio turto atsparumą prieš kibernetinio saugumo grėsmes ir teikia darbuotojams mokymus.[33]

Maltos „BeSmartOnline!“[34] projektu siekiama didinti vaikų, jaunimo ir jų palaikymo tinklo, pvz., globėjų, tėvų ir pedagogų sąmoningumą ir šviesti apie saugų interneto naudojimą, sukuriant, valdant ir skatinant pranešimo apie piktnaudžiavimą internetu priemones.

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

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

2. SANTRAUKA IR PAGRINDINĖS IŠVADOS

- Kibernetinio saugumo įgūdžių trūkumas paveikė 74% organizacijų visame pasaulyje. 2019 m. 57% organizacijų turėjo laisvų kibernetinio saugumo darbo vietų. Šių pareigybių užpildymui dažniausiai reikėjo trijų mėnesių..

- Labiausiai trūksta šių įgūdžių: debesų kompiuterijos saugumo (33 %), taikomųjų programų saugumo (32 %), saugumo analizės ir tyrimų (30 %).

- Viena iš pagrindinių apklaustųjų nurodytų priežasčių, kodėl pozicijos lieka laisvos, yra kvalifikuotų pretendentų trūkumas. Beveik trečdalis organizacijų teigė, kad beveik 75% kandidatų neturi tinkamos kvalifikacijos šiam darbui. Svarbiausios respondentų nurodytos įgūdžių spragos buvo „minkštųjų įgūdžių“, IT žinių trūkumas, nepakankamo verslo supratimo, kibernetinio saugumo techninės patirties ir praktinės patirties trūkumas.

- Apskaičiuota, kad 2020 m. pasaulyje trūks apie 3,12 mln. kibernetinio saugumo specialistų. Tuo tarpu vien tik Europoje iki 2022 m. kibernetinio saugumo darbo jėgos trūkumas turėtų siekti 350 000 darbuotojų. Šis skaičius padvigubėjo, palyginti su tuo, kas buvo apskaičiuota 2018 m.

- ENISA savo pranešime „Kibernetinio saugumo įgūdžių ugdymas ES“ nustatė keturias pagrindines priežastis, kurios gali būti siejamos su kibernetinio saugumo įgūdžių trūkumu. Dvi iš jų yra orientuotos į darbo vietos problemas, o likusios dvi yra susijusios su švietimo ir mokymo sistemos klausimais.

- 2013 m. Europos Komisija paskelbė savo pirmąją kibernetinio saugumo strategiją, kurioje išskiriami pagrindiniai strateginiai tikslai, tokie kaip sąmoningumo ugdymas ir įgūdžių ugdymas. Nuo 2017 m. visos ES valstybės narės sukūrė ir paskelbė savo nacionalines kibernetinio saugumo strategijas (NCSS).

- Vienas pagrindinių visų projekto šalių partnerių nacionalinių saugumo strategijų tikslų yra akademinės bendruomenės, viešojo ir privataus sektorių bei plačiosios visuomenės kibernetinio švietimo ir sąmoningumo didinimas.

- Visų projekto šalių partnerių nacionalinėse saugumo strategijose taip pat pabrėžiama viešojo, privataus ir akademinio sektoriaus partnerystė siekiant stiprinti kibernetinio saugumo sistemų atsparumą, investicijos į IRT saugumą, personalo mokymą ir studentų kibernetinio saugumo įgūdžių ugdymą, kad jie atitiktų rinkos poreikius.

- Visose projekto šalyse partnerėse, išskyrus Estiją, aukštojo mokslo studijų programų analizė neapima sukčiavimo ir socialinės inžinerijos temų kaip atskirų modulių. Tačiau informacija šiomis temomis gali būti įtraukta į kitus kurso modulius. Dvi Estijos aukštojo mokslo studijų programos apima studijų modulius, orientuotus į socialinę inžineriją. Vidutinė tokių modulių trukmė yra 4,5 ECT.

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

- Analizuojamos aukštojo mokslo studijų programos Estijoje, Latvijoje ir Maltoje apima „minkštųjų įgūdžių“ kursus, tokius kaip bendravimo įgūdžiai, verslumas, psichologija ir kt. Priešingai, Kipro ir Lietuvos aukštojo mokslo studijų programos daugiausia orientuotos į „kietuosius įgūdžius“, mažiau akcentuojant „minkštųjų įgūdžių“ svarbą.

- Visose šalyse partnerėse yra keletas viešųjų ir privačių organizacijų, siūlančių kibernetinio saugumo mokymo kursus, skirtus kibernetinio saugumo ir IT specialistams, įmonėms, darbuotojams ir plačiajai visuomenei. Trumpesnės trukmės mokymų kursuose daugiausia dėmesio skiriama tik įvairių rūšių grėsmėms, įskaitant sukčiavimą, socialinę inžineriją ir apsisaugojimo būdus, tačiau ilgesnės trukmės mokymų kursai suteikia platesnę kibernetinio saugumo perspektyvą. Taip pat yra keletas organizacijų, siūlančių įsiskverbimo (angl. penetration) ir socialinės inžinerijos testus, skirtus įmonėms ir jų darbuotojams.

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

3. BIBLIOGAFIJA

1. (ISC)2 (2019): (ISC)² Tyrimas atskleidžia, kad kibernetinio saugumo darbo jėga išaugo iki 3,5 milijono profesionalų visame pasaulyje, 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): Kibernetinio saugumo darbo jėgos tyrimas, URL https://www.isc2.org/Research/Workforce-Study
3. Cyber Wiser (2021): Švietimas ir mokymas nacionalinės kibernetinio saugumo strategijos srityje (LT), URL https://www.cyberwiser.eu/lithuania-lt
4. Cyber Wiser (2021): Švietimas ir mokymas nacionalinės kibernetinio saugumo strategijos srityj (MT), URL https://www.cyberwiser.eu/malta-mt
5. Cyber Wiser (2021): Švietimas ir mokymas nacionalinės kibernetinio saugumo strategijos srityj (LV), URL https://www.cyberwiser.eu/latvia-lv
6. Council of the European Union (2021): Tarybos išvadų dėl ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos projektas, 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. Europos Komisija (2013): Europos Sąjungos kibernetinio saugumo strategija, URL https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
9. Europos Komisija (2019): Pradėti keturi ES bandomieji projektai, skirti parengti Europos kibernetinio saugumo kompetencijos tinklą, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network
10. Europos Komisija (2020): Skaitmeninės Europos programa: siūlomas 7,5 mlrd. EUR finansavimas 2021–2027 m., URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027
11. Europos Sąjungos kibernetinio saugumo agentūra (2019): Kibernetinio saugumo įgūdžių ugdymas ES
12. Europos Sąjungos kibernetinio saugumo agentūra (2020): ENISA grėsmės kraštovaizdis 2019-2020
13. Lietuvos Respublikos Vyriausybė (2018): Rezoliucija dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo, 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): Kibernetinio saugumo būklė 2020 m. 1 dalis. Visuotinis darbo jėgos pastangų ir išteklių atnaujinimas, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf
15. Jon Oltsik (2019): Kibernetinio saugumo specialistų gyvenimas ir laikai 2018, URL https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/surveys/esg-issa-2018-survey-results.pdf
16. Latvijos gynybos ministerija (2019 m.): Latvija patvirtina naują 2019–2022 m. kibernetinio saugumo strategiją 2019-2022, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
17. Latvijos gynybos ministerija (2019): Latvijos kibernetinio saugumo strategija 2019 - 2022 m, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
18. OCECPR (2012): Kipro Respublikos kibernetinio saugumo strategija, 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

19. Estijos Respublika, Ekonomikos reikalų ir komunikacijos ministerija (2019): kibernetinio saugumo strategija, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
20. Maltos informacinių technologijų agentūra (2016 m.): 2016 m. Maltos kibernetinio saugumo strategija, 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