Kiberdrošības izglītības viedtīklu jomā Zināšanu kopuma izstrādes un ieviešanas ceļvedis (Izpildpārskats)

Autori:

Rūta Pirta-Dreimane, Jana Bikovska, Andrejs Romānovs, Maria Valliou, Bahaa Eltahawy, Jānis Pekša

Kiberdrošības mācību programmu ieteikumi viedtīkliem (CC-RSG)

Erasmus+ stratēģiskās partnerības projekts

Intellectual Output 4

Rīgas Tehniskā universitāte, Vāsas Universitāte, Atēnu Nacionālā tehniskā universitāte, Oldenburgas Universitāte

Šis projekts ir saņēmis Eiropas Savienības Erasmus+ programmas finansējumu dotāciju līguma № 2020-1-FI01-KA203-066624 ietvaros.

Saturs

Saīsinājumi 3

1. Ievads 4

2. Izglītības mācību programmas modelis 4

2.1 Izglītības mācību programmas satura modelis 5

2.2 Izglītības programmas izveides metodoloģija 7

2.3 Metožu un instrumentu banka 9

3. Izglītības mācību programmas ieteikumi 9

3.1 Apmācāmo profili 9

3.2. Darba lomas un uzdevumi 10

3.3. Zināšanu jomas un zināšanu bloki 10

3.4. Metožu un instrumentu banka 10

Atsauces 12

Saīsinājumi

ACM Association for Computing Machinery (Datortehnikas asociācija)
NICE Nacionālā kiberdrošības izglītības iniciatīva
CC-RSG Cybersecurity Curricula Recommendations for Smart Grids (Kiberdrošības mācību programmu ieteikumi viedtīkliem)
CPES Center for Power Electronics Systems (Enerģijas elektronikas sistēmu centrs)
ENISA European Network and Information Security Agency (Eiropas Tīklu un informācijas drošības aģentūra)
ES Eiropas Savienība
JTF Joint Task Force (Apvienotā darba grupa)
IT Informāciju tehnoloģijas
IO Intellectual Output (Intelektuālais rezultāts)
MOOC Massive online open courses (Plaši atvērtie tiešsaistes kursi)
NIST National Institute of Standards and Technology (Nacionālais standartu un tehnoloģiju institūts)
PMU Phasor Measurement Unit (Fāzes mērvienība)
OT Operational Technology (Darbību tehnoloģija)
SCADA Supervisory control and data acquisition (Uzraudzības kontrole un datu iegūšana)
SMEs Small and medium-sized enterprises (Mazie un vidējie uzņēmumi)
VET Vocational education and training (Profesionālā izglītība un apmācība)
WP Work Package (Darba kopa)

1. Ievads

Kiberdrošība ir definēta kā viena no Eiropas stratēģiskajām iespējām, un ir atzīts, ka ES ir būtiski jāuzlabo savas digitālās iespējas kiberdrošības jomā [1]. Tas ietver digitālo tehnoloģiju ieviešanu, kā arī nepieciešamās digitālās prasmes visam ES darbaspēkam. Kiberdrošība ir starpdisciplinārs priekšmets [2]- [3], lai nodrošinātu visas kritiskās kompetences, izglītības programmās ir jāintegrē vairākas dimensijas un disciplīnas, piemēram, datorzinātnes, inženierzinātnes, psiholoģija, socioloģija un tiesību zinātne. Kiberdrošības speciālistiem jābūt ar padziļinātām tehniskām zināšanām, tomēr būtiskas ir arī vispārējās prasmes, īpaši krīzes situācijās.

Viedtīklu vide ir saistīta ar papildu sarežģītību kiberdrošības jomā. Viedtīkls integrē dažādus sensorus, vadības sistēmas un sakaru tīklus, kas palielina kiberuzbrukumu virsmu. Kiberdrošības speciālistiem, kuri strādā viedtīkla vidē, ir jābūt plašām kompetencēm, lai aizsargātu infrastruktūru, līdzsvarojot kiberdrošības un elektrotehnikas kompetences, kā arī programmatūras prasmēm.

Šis dokuments pārstāv projekta “Kiberdrošības mācību programmu ieteikumi viedtīkliem (CC-RSG)” WP4 rezultātus. Šīs darba aktivitātes mērķis ir konceptualizēt projektā iegūtās zināšanas un sniegt ieteikumus kiberdrošības mācību programmu izstrādei saistībā ar viedtīkliem.

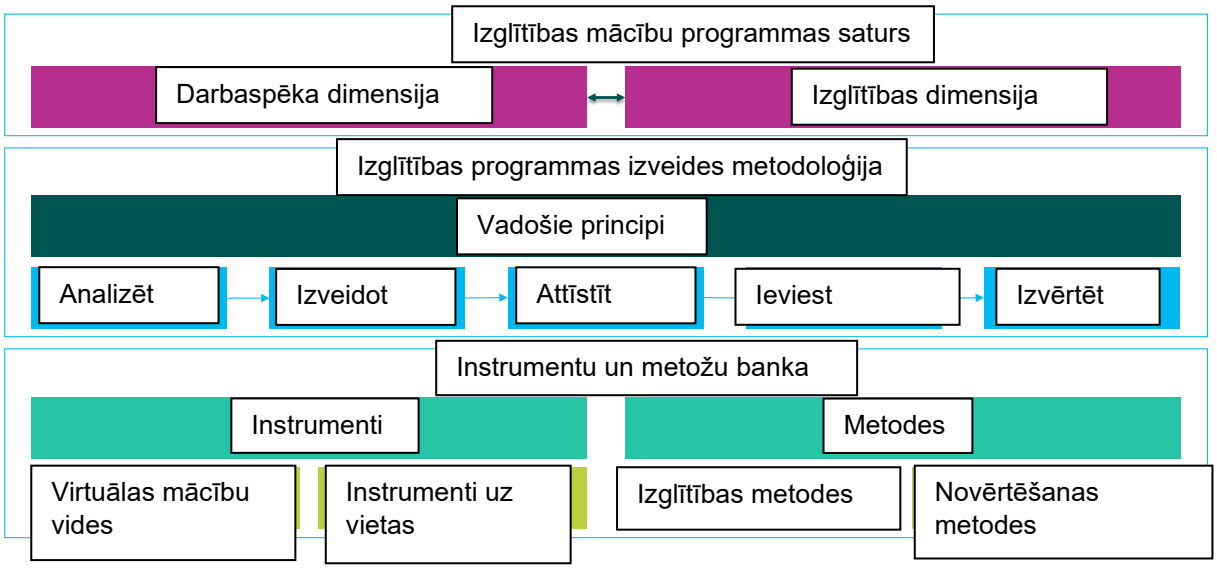
Dokumenta galvenais mērķis ir sniegt ieteikumus pedagogiem un citām ieinteresētajām pusēm izglītības programmu izstrādei, ņemot vērā nozares vajadzības, darbaspēka prasības, uz studentiem orientētas izglītības metodes un jaunus atbalsta instrumentus.

2. Izglītības mācību programmas modelis

Modeļa mērķis ir sniegt norādījumus uz kompetencēm balstītām kiberdrošības izglītības programmām viedtīklu izveidei, izpildei un novērtēšanai. Modelis izskaidro, kā zināšanu kopums (piemēram, šis dokuments) ir jāizmanto, lai nodrošinātu darbaspēka un izglītības dimensiju integrāciju.

Modelis ir balstīts uz [4] ieteikto metodoloģiju un sastāv no trīs pamata izveides blokiem (1. attēls):

1. **Izglītības mācību programmas saturs** nosaka lomas un uz uzdevumiem balstītas kompetences un saistītās zināšanu jomas, zināšanu blokus, mācību tematus un mācību rezultātus.
2. **Izglītības programmas dizaina metodoloģija** iesaka mācību programmu un kursu izveides, izpildes un novērtēšanas principus un procesu.
3. **Instrumentu un metožu banka** ietver metožu un rīku sarakstu un to lietošanas norādījumus (modeļus), ko var izmantot kiberdrošības izglītības programmās viedtīklu izveidei, izpildei un novērtēšanai.

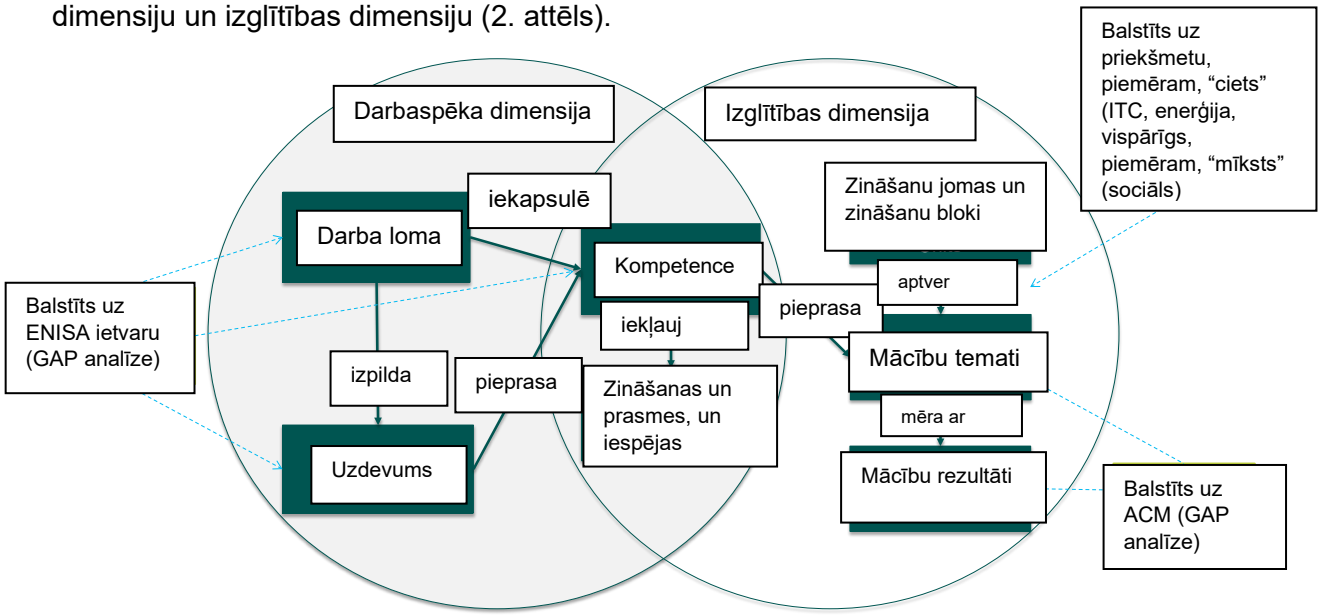


1. attēls. Izglītības mācību programmas modeļa pārskats

2.1 Izglītības mācību programmas satura modelis

Izglītības programmas ir jāizstrādā, pamatojoties uz darbaspēka prasībām, lai nodrošinātu, ka kiberdrošības speciālistu kompetences atbilst nozares pieprasījumam, tostarp prasmēm, kas jāiemāca, un kompetences jomām, kas jāaptver [2].

Ieteiktais izglītības programmu modelis ietver divas dimensijas – darbaspēka dimensiju un izglītības dimensiju (2. attēls).



2. attēls. Izglītības mācību programmas modeļa pārskats

Darbaspēka dimensija ietver šādas galvenās koncepcijas [5]:

- **Darba lomas** ir visdetalizētākie ar kiberdrošību saistītie darba grupējumi, tostarp atribūtu saraksts, t.i., zināšanas, prasmes un iemaņas, kas nepieciešamas ar šo lomu saistīto uzdevumu veikšanai.
- **Uzdevumi** ir konkrētas noteiktas darba daļas, kas apvienojumā ar citiem identificētiem uzdevumiem veido darba apjomu specialitātes jomā vai darba lomā.
- **Kompetences** raksturo spējas pielietot vai izmantot zināšanas, prasmes, iemaņas, uzvedību un personiskās īpašības, lai veiksmīgi veiktu kritiskus darba uzdevumus, noteiktas funkcijas vai darbotos noteiktā lomā vai amatā. Ir svarīgi atšķirt tematam specifiskās (piem., "cietās prasmes") un vispārīgās ("mīkstās prasmes") spējas. Cietās prasmes ietver tehnisko vai administratīvo kompetenci. Mīkstās prasmes ir produktīvu personības iezīmju kopums, kas raksturo cilvēka attiecības sociālajā vidē. Šīs prasmes var ietvert sociālo žēlastību, komunikācijas spējas, valodas prasmes, personīgos ieradumus, kognitīvo vai emocionālo empātiju, laika pārvaldību, komandas darbu un līderības iezīmes.

Vairāki ietvari nosaka ar kiberdrošību saistītās lomas, saistītos uzdevumus un nepieciešamās kompetences, piemēram, Nacionālās kiberdrošības izglītības iniciatīvas (NICE) darbaspēka ietvars (NIST NICE ietvars) [5] un Eiropas Savienības Kiberdrošības aģentūras (ENISA) prasmju ietvars (ENISA ietvars) [6].

Kiberdrošības izglītībai viedtīklos kā izglītības programmu izstrādes pamatu iesaka izmantot ENISA kompetences modeli, jo tam ir vienkāršāka darba lomu struktūra, salīdzinot ar NIST. NIST lomas galvenokārt ir paredzētas lieliem uzņēmumiem, tādēļ tās atspoguļo kiberdrošības iespējas, kas sadalītas starp organizācijām. Empīriskie novērojumi liecina, ka uzņēmumi parasti apvieno līdzīgas lomas un nodrošina "T veida" kompetences un daudzfunkcionālas komandas.

Esošie kiberdrošības kompetenču modeļi ir vērsti uz kiberdrošības pārvaldību un IT specifiskiem kiberdrošības aspektiem, taču tie neattiecas uz viedtīklu kiberdrošības lomām, uzdevumiem un kompetencēm. Tādēļ viedtīklu kiberdrošības uzdevumi ir iekļauti ENISA modelī (3.2. sadaļa). Uzdevumus un kompetences ierosina projekta ekspertu komanda (3. sadaļa). Tādēļ šajā dokumentā ir definēts viedtīkla kiberdrošības lomu un uzdevumu atsauces modelis, kas ir pamats attiecīgo izglītības programmu izstrādei.

Darbaspēka dimensija iejaucas izglītības dimensijā, izmantojot kompetences, kas ietver prasmes, iemaņas un zināšanas. Izglītības dimensija ietver šādas galvenās koncepcijas [7]:

- **Zināšanu jomas** un **zināšanu bloki** ir tematiski grupējumi, kas iekļauj vairākus saistītus **mācību tematus**.
- **Mācību rezultāti** atspoguļo detalizētākus rezultātus nekā kompetences, un tos var uzskatīt par kursa vai mācību stundu apguves rezultātiem. Mācību rezultāti uzsver, ko studenti var darīt, nevis tikai to, ko studenti zina.

Vairāki kiberdrošības mācību programmu ieteikumi iesaka galvenās zināšanu jomas, zināšanu blokus, mācību tematus un mācību rezultātus. Piemēram, Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020), ko sagatavoja Datortehnikas asociācijas skaitļošanas izglītības komiteja kopienas koledžās [7] un CSEC2017 Joint Task Force on Cybersecurity Education (JTF) globālās kiberdrošības mācību programmas ieteikumi [3].

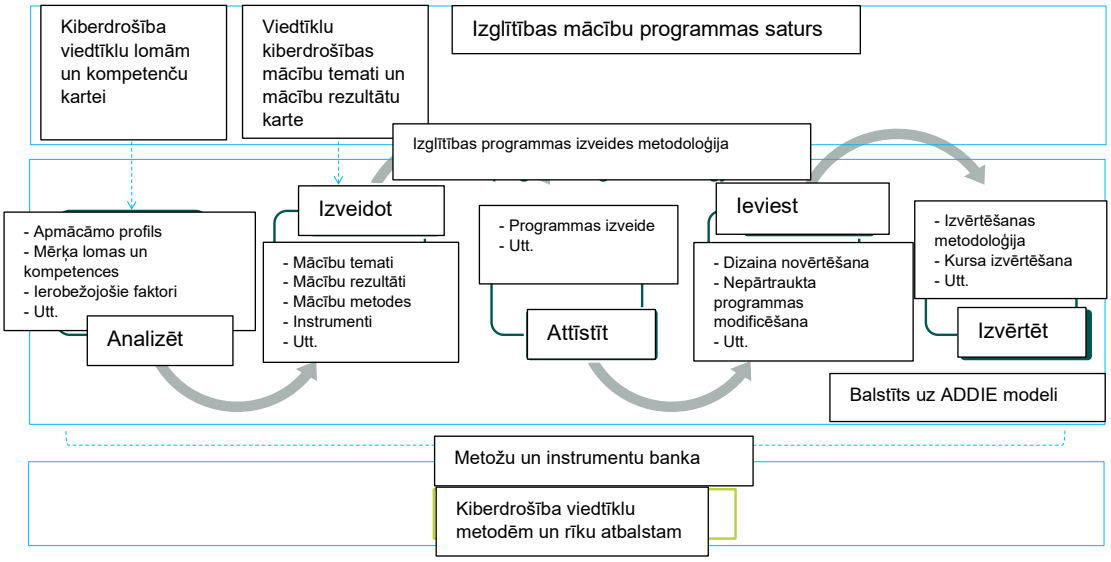
Viedtīklu kiberdrošības izglītībai ir ieteicams piemērot Cyber2yr2020 vadlīnijas IT specifiskām kiberdrošības zināšanu vienībām, zināšanu jomām, tēmām un mācību rezultātu noteikšanai. Viedtīkliem specifiskā kiberdrošības izglītība esošajos ietvaros ir ierobežota, tāpēc viedtīklu kiberdrošības specifiskās kompetences, mācību tēmas un mācību rezultāti ir iekļauti Cyber2yr2020 modelī. Viedtīklu specifiskās kiberdrošības kompetences, mācību tēmas un mācību rezultātus iesaka projekta ekspertu komanda (3.3. sadaļa).

Šajā dokumentā kompetences ir iedalītas četrās grupās:

- IT specifiskas kompetences nosaka zināšanas, spējas un prasmes, kas nepieciešamas IT specifisku kiberdrošības uzdevumu veikšanai. Šīs kompetences ir balstītas uz Cyber2yr2020 vadlīnijām (tikai pamatkompetences). Šīs kompetences nosaka "kas jāpaveic" aspektus [7].
- Viedtīkliem specifiskas kompetences nosaka zināšanas, spējas un prasmes, kas nepieciešamas viedtīklu specifisku kiberdrošības uzdevumu veikšanai. Šīs kompetences sagatavo projekta ekspertu komanda un apstiprina nozares eksperti. Šīs kompetences nosaka "kas jāpaveic" aspektus [7].
- Darbības kompetences apkopo vadības un darbības kompetences, kas definē "kā jāveic darbības" gan IT, gan viedtīklu jomās.
- Vispārējās kompetences nosaka sagaidāmās "mīkstās prasmes".

2.2 Izglītības programmas izveides metodoloģija

Izglītības programmu izveides metodoloģija definē vispārīgos principus, kas jāievēro, un galvenos soļus izglītības programmas definēšanā (2. attēls). Programmas definēšanā, izpildes un izvērtēšanas pedagogi var izmantot viedtīkla kiberdrošības kompetences modeli un mācību satura ieteikumus, kas norādīti šajā dokumentā. Tomēr precīzs saturs ir jāsaskaņo ar programmas audzēkņu profiliem un viņu vajadzībām (mērķa lomas utt.).



3. attēls. Izglītības programmas izveides metodoloģija

Izglītības programmas jāsagatavo, ievērojot vairākus pamatprincipus. Saskaņā ar dizaina domāšanas pieeju attiecībā uz izmantošanu izglītības dizainā [8], [9] dizaina

principi bieži tiek izmantoti, lai noteiktu galveno virzienu, kas jāievēro programmu izstrādē un izpildē [10]. Dizaina principi ir noteikti kā [9]: "...starpposms starp zinātniskiem atklājumiem, kam jābūt vispārināmiem un atkārtojamiem, un lokālo pieredzi vai piemēriem, kas rodas praksē. Tā kā dizaina principi ir jāinterpretē, tie nav tik viegli viltojami kā zinātniskie likumi. Principi tiek radīti induktīvi no iepriekšējiem panākumu piemēriem un laika gaitā tiek pilnveidoti, jo citi mēģina tos pielāgot savai pieredzei." Dizaina principi piesaista dizaina zināšanas no veiksmīgas mācību vides [10] un apkopo vislabākās prakses.

Viedtīklu kiberdrošības izglītībā ieteicams ievērot šādus galvenos principus:

1) **Mērķa lomu un uzdevumu virzīts kompetenču dizains** – kompetences jānosaka, pamatojoties uz izglītojamo mērķa lomām, lai nodrošinātu darbaspēka un izglītības dimensiju integrāciju.
2) **Fokuss uz izglītojamo un personalizācija** – studiju programmām jākoncentrējas uz studentu vajadzībām un jānodrošina profilam specifiska kompetenču attīstība.
3) **Priekšmetam raksturīgo un vispārējo kompetenču sinerģija** – vispārējās kompetences ir jāintegrē katrā mācību tēmā kopā ar mācību priekšmeta kompetencēm.
4) **Reālās dzīves pieredzes integrācija** – studiju programmām un kursu saturam ir jāatspoguļo reālās dzīves izaicinājumi un laika gaitā ir jāpielāgojas.
5) **Vertikālā integrācija** – kiberdrošība ir daudznozaru priekšmets; programmās ir jāintegrē sociālās zinātnes (piemēram, psiholoģija), lai nodrošinātu vispārējo kompetenču attīstību.
6) **Uz atsauksmēm balstīta nepārtraukta uzlabošana** – nepārtraukta uzlabošana ir jāplāno, pamatojoties uz audzēkņu un darbaspēka atsauksmēm.

Ieteiktais izglītības programmas izstrādes process ir balstīts uz ADDIE modeli [11]. ADDIE modelis ir vispārīgs process, ko tradicionāli izmanto mācību programmu un apmācību izstrādātāji. Modelis ietver piecus posmus:

1. **Analīze** – apmācāmo profilu analīze (tostarp viņu īpašības, esošā kompetence, paredzamās mērķa lomas un apmācību vajadzības), mācību mērķi un mērķu noteikšana. Programma ir jāizstrādā tā, lai tajā būtu iekļautas kompetences, kas nepieciešamas izglītojamo mērķa lomām. Šajā dokumentā ir iekļautas tipiskas kiberdrošības lomas, kas ir papildinātas ar viedtīklam specifiskiem kiberdrošības uzdevumiem un kompetencēm (3.2. sadaļa). Šo dokumentu var izmantot kā atsauces modeli apmācāmā mērķa lomu kartēšanai. Lomas ir izstrādātas, pamatojoties uz identificētiem tipiskiem viedtīkla kiberdrošības apmācāmo profiliem (3.1. sadaļa), kas noteikti, pamatojoties uz projekta ekspertu pieredzi.
2. **Dizains –** studiju programmas mērķi, mācību tēmas, mācīšanās rezultāti un mācīšanas metožu noteikšana. Šis dokuments nosaka mācību tēmu un mācību rezultātu kopumu, kam jābūt definētajām lomām (3.3. sadaļa). Tēmas ir iekļautas zināšanu jomās un elementos. Darba lomu, uzdevumu, kompetenču un mācību tēmu karte ir pievienota 1. pielikumā. Tēmas ir jāizvēlas, pamatojoties uz noteiktajām apmācāmo mērķa lomām. Apmācāmajiem var būt individuāli plāni, pamatojoties uz viņu esošajām kompetencēm (piemēram, ja apmācāmajiem ir iepriekšēja izglītība IT specifiskā kiberdrošības jomā un viņš vēlas kļūt par drošības arhitektu enerģētikas iestādē, viņam jāapgūst viedtīkla specifiskās kiberdrošības

kompetences). Dokumentā ir iekļauta metožu banka (4. sadaļa) un instrumentu banka (5. sadaļa), ko var izmantot izglītības programmu izstrādes atbalstam.

3. **Attīstība** – studiju programmu materiālu izstrāde un ielāde e-studiju sistēmās (ja attiecināms).
4. **Ieviešana – faktiskās programmas un kursu piegāde.**
5. **Novērtēšana –** atsauksmes un datu vākšana uzlabošanas jomu noteikšanai. Dokumentā ir iekļauta metožu banka (4. sadaļa) un instrumentu banka (5. sadaļa), ko var izmantot izglītības programmu novērtēšanas atbalstam.

2.3 Metožu un instrumentu banka

Metožu banka un instrumentu banka (4. sadaļa) piedāvā metodes un instrumentu kopumu, ko studiju programmu izstrādātāji un pedagogi var izmantot visās izglītības attīstības procesa fāzēs (analīze, izstrāde, attīstība, ieviešana un novērtēšana). Metodes un instrumenti ir definēti atkārtoti lietojamu modeļu veidā, kas veido zināšanu bāzi kursu izstrādes un izpildes atbalstam. Metodes un instrumenti, kas saistīti ar izglītības izstrādes un izpildes procesa fāzēm, ir aprakstīti katras metodes/instrumenta kartē.

3. Izglītības mācību programmas ieteikumi

Izglītības mācību programmas ieteikumi veido atsauces modeli darbaspēka un izglītības integrācijai. Tas ietver šādus galvenos aspektus:

- **Apmācāmo profili** – tipiski viedtīkla kiberdrošības apmācāmo profili nodrošina pamatojumu mērķa darba lomu noteikšanai;
- **Darba lomas un uzdevumi** ataino apmācāmo mērķa lomas, uzdevumus un nepieciešamās kompetences (tostarp IT specifiskās kiberdrošības kompetences, viedtīkla specifiskās kiberdrošības kompetences, darbības un vispārējās kompetences);
- **Zināšanu bloki un zināšanu jomas** nosaka **mācību tematus un mācību rezultātus,** kas nepieciešami, lai iegūtu kompetenci.

3.1 Apmācāmo profili

Studentu profila mērķis ir izcelt studentu grupas, kurām var piemērot mācību programmas modeli.

Šeit var izcelt divas absolventu grupas, kuras varētu būt ieinteresētas turpināt izglītību viedtīklu kiberdrošības jomā: skaitļošanas jomas absolventi un energosistēmu absolventi. Divas citas grupas ir IT un OT vai viedtīklu pārvaldības profesionāļi. Viņiem ir darba pieredze energosistēmu un viedtīklu jomā, taču viņiem ir vajadzīgas plašākas zināšanas viedtīklu kiberdrošībā.

Profilam tiek ņemti vērā šādi atribūti:

- pieredze attiecas uz apmācāmā izglītības sasniegumiem vai profesionālajām prasmēm;
- izglītības vajadzības ir plaisa starp apmācāmā pašreizējo zināšanu, prasmju un attieksmju līmeni un vēlamo līmeni, lai pielāgotos jaunai situācijai, ko var iegūt ar izglītību.
- Sagaidāmais raksturo zināšanas un prasmes, kas studentiem jāparāda līdz studiju beigām.

Enerģētikas nozarei ir vajadzīgs kiberdrošības jomā zinošs darbaspēks, un augstākajai izglītībai varētu būt vērtīga loma šīs nepilnības aizpildīšanā.

3.2. Darba lomas un uzdevumi

Viedtīklu kiberdrošības darba lomas ir balstītas uz ENISA ieteiktajām lomām: galvenais informācijas drošības speciālists (CISO), reaģētājs uz kiberincidentiem, kiberjomas juridiskais, politikas un atbilstības speciālists, kiberdrošības arhitekts, kiberdrošības revidents, kiberdrošības īstenotājs un kiberdrošības risku vadītājs. Lomas, uzdevumi un kompetences ir papildinātas atbilstoši viedtīklu specifikai.

Ņemot vērā viedtīklu specifiku, ENISA lomas tika papildinātas ar jaunām lomām – enerģētikas pilsonis, tīkla aktīvu pārvaldnieks un tīkla komunikāciju inženieris. Kopējie biznesa mērķi viedtīklu specifiskajām lomām ir [12]: uzturēt drošību, uzturēt energosistēmas uzticamību, uzturēt energosistēmas noturību un atbalstīt tīkla modernizāciju.

3.3. Zināšanu jomas un zināšanu bloki

Zināšanu jomas un bloki ir balstīti uz “ACM Cybersecurity Curricular Guidance for Associate-Degree Programs 2020 Cyber2yr2020”, ko izstrādāja datortehnikas asociācijas (ACM) Skaitļošanas izglītības komiteja kopienas koledžās (CCECC): datu drošība, programmatūras drošība, komponentu drošība, savienojumu drošība, sistēmu drošība, cilvēku drošība, organizācijas drošība, sabiedrības drošība. Tie ir papildināti ar viedtīklam specifiskām kompetencēm, kas nepieciešamas noteiktām darba lomām (3.2. sadaļa). Jauna zināšanu joma “Viedtīklu drošība” papildina ACM ietvaru.

3.4. Metožu un instrumentu banka

Metožu un instrumentu banka nosaka ieteicamās metodes un instrumentus, ko izmantot viedtīklu kiberdrošības izglītībā: simulācijas rīki, CPES laboratorijas un testēšanas platformas, spēļu izmantošana, uz problēmām un projektiem balstīta mācīšanās un apgrieztā mācīšanās. Ātrs veids, kā skolotājiem/instruktoriem, kuri vēlas noformulēt mācību programmu, apskatīt metodes pamatelementus un tās parastos lietošanas gadījumus saistībā ar kiberdrošības un/vai viedtīklu tēmu. Līdzās izglītības metodēm ir aprakstīts arī simulācijas testu rīks ar lietošanas gadījumiem.

Testa platformas izmanto, lai dažādās pakāpēs simulētu reālās dzīves sistēmas. Dažās testēšanas platformās sistēmas daļām tiek izmantota programmatūras simulācija, bet citās tiek izmantoti tikai aparatūras komponenti. Turklāt ir testēšanas platformas, kas simulē tikai sistēmas komponentu, un citas, kas simulē visu sistēmu. Reāllaika simulatora izmantošana apvienojumā ar reālu aparatūru (piemēram, invertoriem un PMU), lai simulētu visu mikrotīklu, ir visreālākais un pilnīgākais veids, kā izpētīt elektrisko tīklu uzvedību kiberuzbrukuma laikā.

Spēļu izmantošana ir mācību metode, kurā tiek izmantoti spēļu izstrādes elementi un mehānismi, lai palielinātu studentu iesaisti [13]. Šie elementi un mehānismi var būt, piemēram, stāstījums, ierobežots laiks uzdevuma veikšanai, punkti, nozīmītes un līmeņa pārspēšana.

Uz problēmām balstītajā apmācībā (PBL) studentu grupa pēta atvērtu reālās pasaules problēmu un mēģina izdomāt vispiemērotāko risinājumu, ko pēc tam grupa prezentē citiem studentiem. Uz projektu balstītā apmācība ir balstīta uz to pašu ideju, taču kopumā tai ir ilgāks ilgums un konkrēts rezultāts, nevis teorētisks risinājums.

Apgrieztās mācīšanās galvenā iezīme ir tā, ka studenti apgūst materiālu, ko parasti apgūst mācību stundās savās mājās. Tādā veidā, atrodoties stundā, viņiem ir iespēja pārdomāt apgūto materiālu un ir laiks eksperimentiem.

Atsauces

[1] Eiropas Komisija, “The EU’s Cybersecurity Strategy for the Digital Decade,” 2020. [Tiešsaistē]. Pieejams: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta un R. De Nicola, “Framework, Tools and Good Practices for Cybersecurity Curricula,” *IEEE piekļuve*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3093952.

[3] Joint Task Force on Cybersecurity Education, *Curricula 2017 Cybersecurity Curriculum - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*, vol. versija 1., no. Decembris, 2017.

[4] R. Pirta-Dreimane, A. Brilingaite, E. Roponena un K. Parish, “Multi-dimensional Cybersecurity Education Design: A Case Study,” in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, IEEE, Sept. 2022, 1–8. lpp., doi: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927931.

[5] D. S. M. C. S. K. A. W. un G. W. R. Petersen, “Workforce Framework for Cybersecurity (NICE Framework),” 2020.

[6] E. European Union Agency for Cybersecurity, “European cybersecurity skills framework,” *https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles*, 2022.

[7] Cyber2yr2020 Task Group, *Cybersecurity Curricular Guidance for Associate-Degree Programs*. 2020. doi: 10.1145/3381686.

[8] I. Wrogemann, L. Sarp, N. Susser un J. Falk, “D-Learning – Design Thinking as a means to innovative product development in adult learning,” *https://cesie.org/media/ d-learning-manual-en.pdf,* 2021.

[9] S. Panke, “Design Thinking in Education: Perspectives, Opportunities and Challenges,” *Open Education Studies*, vol. 1, Nr. 1. 2019. doi: 10.1515/edu-2019-0022.

[10] Y. Kali, R. Levin-Peled un Y. Dori, “The role of design-principles in designing courses that promote collaborative learning in higher-education. Computers in Human Behavior,” *Comput Human Behav*, vol. 25, 2009.

[11] G. Morrison un S. Ross, *Designing Effective Instruction, 7th Edition*. 2013.

[12] J. Marron, A. Gopstein, N. Bartol un V. Feldman, “Cybersecurity framework smart grid profile,” Gaithersburg, MD, jūl. 2019. doi: 10.6028/NIST.TN.2051.

[13] S. Deterding, K. O’Hara, M. Sicart, D. Dixon un L. Nacke, “Gamification: Using game design elements in non-gaming contexts,” in *Conference on Human Factors in Computing Systems - Proceedings*, 2011. doi: 10.1145/1979742,1979575.