Tehnikas līmenis, tendences un prasmju trūkums viedo energotīklu kiberdrošībā (izpildes ziņojums)

Autori:

Džirapa Kamsamrons (*Jirapa Kamsamrong*), Bjerns Zīmerss (*Bjoern Siemers*), Šadi Atara (*Shadi Attarha*),
Sebastians Lēnhofs (Sebastian Lehnhoff), Marija Vajū (*Maria Valliou*), Andrejs Romānovs,
Jana Bikovska, Jānis Pekša, Rūta Pirta-Dreimane,
Jānis Grabis, Nadežda Kuņicina, Jūlija Strebko,
Tero Vartiainens (*Tero Vartiainen*), Bahā Eltavijs (*Bahaa Eltahawy*), Mike Mekanens (*Mike Mekkanen*)

Kiberdrošības mācību programmu ieteikumi viedajiem energotīkliem (*CC-RSG*)

Erasmus+ Stratēģiskās partnerības projekts

Intelektuālais ieguldījums 1

2022. gada aprīlis

Recenzents: Fivs Palaiojannis (*Foivos Palaiogiannis*)

Koordinators: Vāsas Universitāte
Partneri: Oldenburgas Universitāte, Rīgas Tehniskā universitāte, Atēnu Nacionālā tehniskā universitāte

Šis projekts ir saņēmis finansējumu no Eiropas Savienības *Erasmus+* programmas saskaņā ar dotācijas nolīgumu № 2020-1-FI01-KA203-066624.

Eiropas Komisijas sniegtais atbalsts šī izdevuma publicēšanai nenorāda uz to, ka tā atbalsta izdevuma saturu, kas atspoguļo tikai autoru viedokļus, un Komisiju nevar uzskatīt par atbildīgu attiecībā uz jebkādu izdevumā ietvertās informācijas iespējamo lietojumu.

Vaasan yliopisto
UNIVERSITY OF VAASA

National Technical University of Athens

1862
RIGA TECHNICAL UNIVERSITY

CARL VON OSSIETZKY universität OLDENBURG

Saturs

List of Tables 4
List of Figures 4
Abbreviations 5
1. Introduction 6
1.1 Objectives 6
1.2 Structure of the document 6
2. Research Methodology 7
3. Cybersecurity Policy in European Union 7
3.1 EU Policies and Strategic Directions 7
3.2 Organization related to cybersecurity 8
3.3 Industry Studies and Recommendations 8
3.4 Industry Studies and Recommendations 8
4. State of the art and trends in cybersecurity in smart grids 9
4.1 Categorization 9
4.2 Technology and Education Development 10
4.3 Gaps analysis 11
5. State of the art in education in smart grids and cyber security 12
5.1 Higher education study programs 12
5.2 Continuing education programs 13
5.3 Massive open online courses (MOOC) 13
6. Identification of skill gaps in cyber security in smart grids 13
7. Identification of useful tools for education in cyber security in smart grid 14
7.1 Basic tools for active learning about cybersecurity 14
7.2 Advanced tools for vulnerabilities experiments 14
8. Conclusion and recommendations 15
9. Bibliography 16

Tabulu saraksts

Table 1 Cyberattacks classification considering CIA..... 10
Table 2 Gap analysis for existing CPES laboratory/testbed..... 11
Table 3 Cybersecurity Risks in the CPES..... 12
Table 4 Recommendation from the stakeholder workshop [70] 13
Table 5 Educational Approaches in Smart Grids and Cyber Security 14
Table 6 Cybersecurity tools for smart grids 15

Attēlu saraksts

Figure 1 Research methodology of WP1 7
Figure 2 Cybersecurity education curriculum thought model 8
Figure 3 Categorization of skill gaps based on the literature review 9

Saīsinājumi

ACM Skaitļošanas tehnikas asociācija (*Association for Computing Machinery*)
AES Uzlabots šifrēšanas standarts (*Advanced Encryption Standard)*
CIA Konfidencialitāte, integritāte un pieejamība (*Confidentiality, Integrity, and Availability*)
CPES Kiberfizikālās enerģijas sistēma (*Cyber Physical Energy System*)
DdoS Izkliedētais pakalpojuma atteikums (*Distributed Denial of Service*)
DMZ Demilitarizētas zonas
DoS Pakalpojuma atteikums (*Denial of Service*)
ENISA Eiropas Savienības Tīklu un informācijas drošības aģentūra (*European Network and Information Security Agency*)
ES Eiropas Savienība
HPC Aparatūras snieguma rādītāji (*Hardware performance counters*)
ICS Ražošanas vadības sistēmas (*Industrial Control Systems*)
IKT Informācijas un komunikācijas tehnoloģijas
IAS Ielaušanās atklāšanas sistēma
IEC Starptautiskā Elektrotehnikas komisija (*International Electrotechnical Commission*)
IoT Lietu internets (*Internet of Things*)
IP Interneta protokols
KU Zināšanu vienības (*Knowledge Units*)
MOOC Masveida atvērtie interneta kursi (*Massive online open courses*)
PIA Profesionālā izglītība un apmācības
WP Darba grupa (*Work Package*)

1. Ievads

Pēdējos gados enerģētikā ir ievērojami palielinājusies digitalizācijas pakāpe, modernizētā un uzlabotā elektrotīklā ieviešot dažādu digitālo skaitļošanu, komunikācijas, kā arī ražošanas vadības sistēmas un tehnoloģijas. Turklāt Eiropā mērķis ir veikt pilnīgu ieviešanu, vienkāršojot pārrobežu reāllaika tirgus datu apmaiņu. Milzīga datu apjoma un *IoT* plašā izmantojuma dēļ enerģētikas nozare ir kļuvusi pievilcīgāka hakeriem. Tam nepieciešams plašs klāsts vairākdisciplīnu zināšanu, tostarp par energosistēmām, datortīklu veidošanu, programmatūru, integrētām sistēmām, svarīgu infrastruktūras drošību un drošības pārvaldību.

Eiropas Komisija (ES) ir izveidojusi ES Kiberdrošības stratēģiju, lai uzlabotu Eiropas kolektīvo noturību pret kiberdraudiem un nodrošinātu, ka visi pilsoņi un uzņēmumi var pilnībā izmantot drošus un uzticamus digitālos rīkus. Šī stratēģija attiecas uz būtisko pakalpojumu drošību, tostarp energotīkliem un aizvien lielāku apjomu savienoto priekšmetu pilsoņu mājās un birojos vai rūpnīcās. Stratēģija nosaka, ka esošās ES kiberdrošības spējas nav pietiekamas. Lai uzlabotu kiberdrošības spējas, gan ES Kiberdrošības stratēģija, gan Digitālās Eiropas programma izceļ nepieciešamību palielināt sabiedrības kiberdrošības informētību un uzlabot jauno speciālistu kiberdrošības prasmes.

1.1 Mērķi

WP1 ziņojuma mērķi ir norādīti tālāk.

- Analizēt esošās tendences un tehnikas līmeni akadēmiskajā vidē.
- Analizēt ES augstākās izglītības esošās un nākotnes mācību programmas.
- Analizēt nozarē nepieciešamās prasmes.
- Identificēt prasmju trūkumu attiecībā uz augstāko izglītību un nozares vajadzībām, pamatojoties uz iepriekš minēto analīzi.

1.2 Dokumenta struktūra

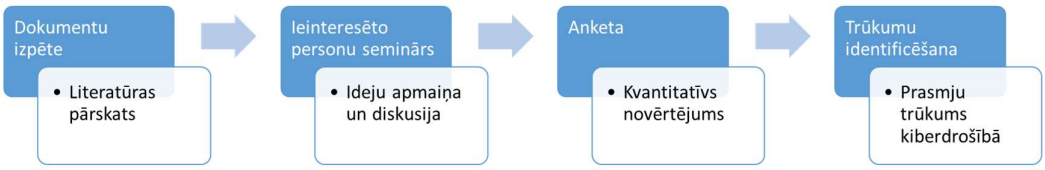
Dokuments ir strukturēts tālāk minētajā veidā.

- 2. sadaļā izklāstīta pētniecības metodoloģija, kas šajā pētījumā izmantota, lai apkopotu datus un analizētu rezultātus, kā arī pētījuma joma.
- 3. sadaļā izskaidrota ES politika attiecībā uz kiberdrošību viedajā energotīklā.
- 4. sadaļā sniegta akadēmiskās vides perspektīva, izmantojot literatūras pārskatu. Literatūras pārskata mērķis ir arī noskaidrot tehnikas līmeni un izglītības tendences kombinētajā viedo energotīklu un kiberdrošības jomā.
- 5. sadaļā apkopota informācija par esošajām kiberdrošības izglītības programmām, tostarp par augstāko izglītību, tālākizglītību un *MOOC*.
- 6. sadaļā identificēta nozare un attiecīgās prasmes, kas nepieciešamas darbiniekiem tajā. Vajadzīgo prasmju noteikšana tiek veikta, izmantojot ieinteresēto personu semināru un īpašu aptauju.
- 7. sadaļā izklāstīti noderīgi rīki attiecībā uz kiberdrošības izglītību, kas tiek analizēti, balstoties uz literatūras pārskatu un ieinteresēto personu aptauju.
- 8. sadaļa ietver secinājumus un sākotnējās prasības un ieteikumus attiecībā kiberdrošību viedo energotīklu izglītībā.

Šī dokumenta nobeigumā ir secinājumi un bibliogrāfija.

2. Pētniecības metodoloģija

Lai gūtu ieskatu un uzzinātu viedo energotīklu kiberdrošības tehnikas līmeni, pirmais solis ir literatūras pārskats, lai apkopotu pētniecības tendences un jaunumus, kā arī izglītības metodes un esošās piedāvātās mācību programmas. *WP1* pētniecības metodoloģija tiek parādīta 1. attēls. .



1. attēls. *WP1* pētniecības metodoloģija.

Dokumentu izpēte atkarībā no pētniecības konteksta un mērķa nodrošina tikai uz konkrētiem tematiem un nozarēm balstītu informāciju. Lai iegūtu plašāku skatu uz prasmju trūkumu kiberdrošības ziņā, it īpaši no nozares perspektīvas, ieinteresēto personu seminārs ir būtisks ideju un viedokļu apmaiņai starp akadēmisko vidi un nozari.

3. Kiberdrošības politika Eiropas Savienībā

3.1 ES politika un stratēģiskā vadība

Kiberdrošības politika var palīdzēt valstij risināt būtiskus aspektus, kas ir nepieciešami, lai novērstu kiberievainojamības radīto negatīvo ietekmi. Eiropas Komisija un Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos ir izveidojuši jaunu 5 gadu ES kiberdrošības stratēģiju (2020–2025), lai nostiprinātu un aizsargātu digitālo sistēmas pārveidi no kiberdraudiem. Šī stratēģija arī uzsver to, cik svarīgs ir ES darbaspēks ar kiberprasmēm. Gatavība kiberdrošības ziņā un izpratne par to uzņēmumu un cilvēku starpā joprojām ir maza, un pastāv ievērojams kiberdrošības darbaspēka trūkums.

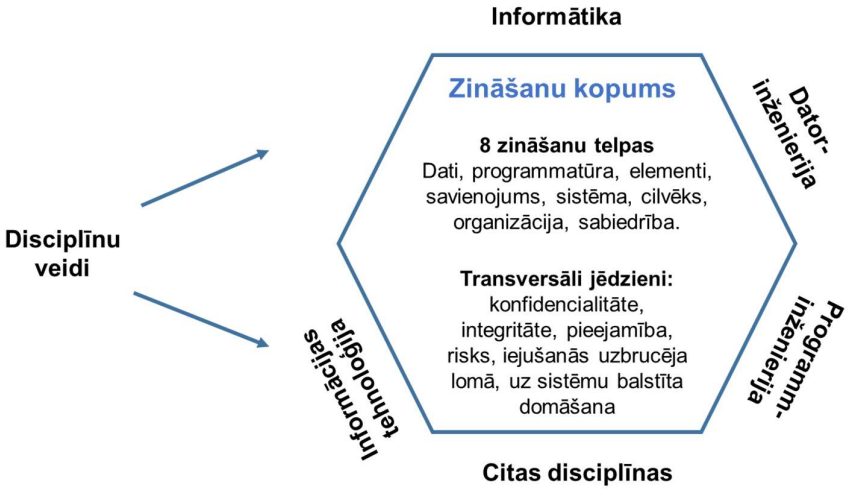
ES kiberdrošības stratēģija atbilst ES Pārskatītajam Digitālās izglītības rīcības plānam [1], kura mērķis ir uzlabot izpratni par kiberdrošību cilvēku vidū, it sevišķi bērnu un jauniešu vidū, un organizācijās, it īpaši MVU. Plānā paredzētas divas prioritātes [1]: veicināt augstas veiktspējas digitālās izglītības ekosistēmu un [2] uzlabot digitālās prasmes un kompetences digitālajai pārveidei. Izpildīt aizvien lielākās prasības pēc IKT darbaspēka IKT drošības ekspertiem ar praktiskām zināšanām par enerģijas jomu ir kļuvis sarežģītāk, un, lai to panāktu, var nākties uzlabot inženierijas un IKT mācību programmas. Turklāt izglītības rīcības plānā ir ieteikta ieinteresēto personu izglītošana un apmācības visā viedo energotīklu jauno drošības risinājumu dzīves ciklā. Tajā noteikts, ka izglītības un apmācību programmām jāmotivē ieinteresētās personas domāt citādos, novatoriskos veidos, kā arī pieredzēt jaunas pieejas. Izglītības un mācību programmām jāpievērš vairāk uzmanības informētības palielināšanai (un uzlabošanai), ieskatu sniegšanai un īstu gadījumu scenāriju aplūkošanai, kā arī jaunu (kiberdrošības) koncepciju izstrādei, eksperimentēšanai un pieredzēšanai.

3.2 Ar kiberdrošību saistīta organizācija

ES kiberdrošības aģentūra (*ENISA*) saskaņā ar Kiberdrošības aktu ir atbildīga par kiberdrošību ES [2]. Kiberdrošības akts uzlabo *ENISA* struktūru, piešķirot pastāvīgas pilnvaras ar konkrētiem resursiem un uzdevumiem, lai palielinātu pielietojuma darbības ES līmenī. *ENISA* ir pilnvarota ES dalībvalstīm sniegt atbalstu attiecībā uz kiberdrošības ieviešanu, izveidojot Eiropas kiberdrošības sertifikāciju [3]. ES uzņēmumu precēm un pakalpojumiem saskaņā ar direktīvu jāatbilst noteiktām prasībām.

3.3 Nozares pētījumi un ieteikumi

Nozares asociācijas un interešu grupas ir izpētījušas esošās kiberdrošības izglītības tehnikas līmeni un sagatavojušas ieteikumus kiberdrošības mācību programmām. Tomēr ieteikumi viedo energotīklu kiberdrošības izglītības ziņā joprojām ir ierobežoti. Kopīgo kiberdrošības izglītības darba grupu veido vairākas asociācijas, kas ir sagatavojušas dokumentu "*Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*" (Pēcvidusskolas kiberdrošības grāda programmu mācību programmu pamatnostādnes) [4]. Kopīgā darba grupa uzskata, ka pasaulē pastāv un palielinās kvalificētu praktizējošu kiberdrošības profesionāļu darbaspēka trūkums. Piedāvātās kiberdrošības izglītības programmas ir parādītas 2. attēls. .



2. attēls. Domu modelis par kiberdrošības izglītības mācību programmām [4].

3.4 Nozares pētījumi un ieteikumi

Enerģētikas nozarē pēdējā laikā ir uzsākts digitālās pārveides process ar viedo energotīklu ieviešanu, kas izraisa nepieciešamību no jauna izglītot novecojošo darbaspēku un apmācīt topošo darbaspēku. Aktīvo mācību veicinošai izglītības platformai būtu jāietver tālāk minētie temati [5].

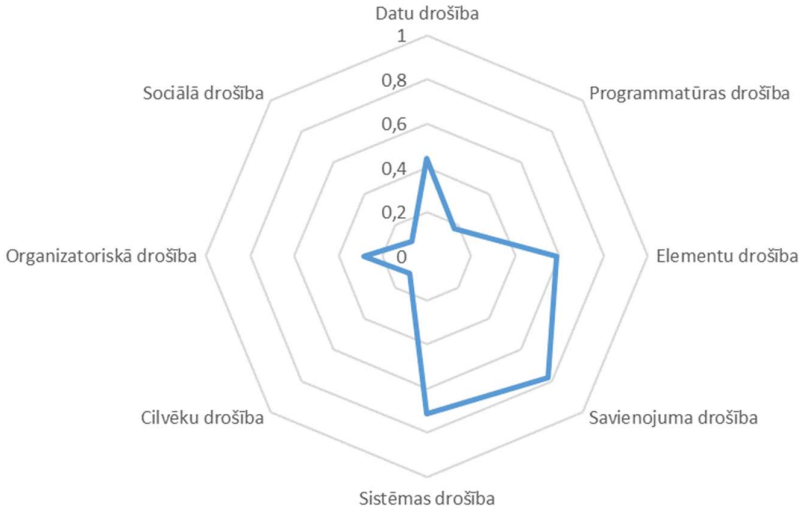
- Kiberinfrastruktūra elektrotīklā.
- Uzraudzība un situācijas apzināšanās.
- Uzlabotā mērīšanas infrastruktūra.
- Viedā energotīkla pamatnostādnes dokumenti.
- Enerģētikas nozares spēju brieduma modelis.

- Privātums viedajā energotīklā.
- Svarīgas infrastruktūras drošības piemēri un ietekme.
- Drošības perspektīva.
- Drošības izaicinājumi sadales automatizācijā.
- Iekļauts novērtējums.
- *SCADA* pamati un stabilas vadības sistēmas.

4. Tehnikas līmenis un tendences viedo energotīklu kiberdrošībā

4.1. Kategorizēšana

Ar *Google Scholar* un *Microsoft Academic* tiek apkopoti atbilstoši 2017.–2020. gada pētījumi, izmantojot atslēgvārdus "kiberdrošība" un "viedais energotīkls". Rezultāti ir norādīti pētījumu nosaukumos un arī saturā, kopumā aplūkoti apmēram 164 dokumenti. Visi šie pētījumi ir augstā līmenī pārskatīti, lai atlasītu atbilstošos pētījumus, kas ir saistīti ar kiberdrošību un viedo energotīklu. Pēc tam atlasītie pētījumi tiek kategorizēti, izmantojot *ACM* kiberdrošības sistēmu, kas parādīta 3. attēls. . Katrs atlasītais pētījums tiek rūpīgi pārskatīts, lai identificētu pētījuma mērķi, metodi un rezultātu. Jo augstāks ir skaitlis, jo vairāk pētījumu aplūkoja attiecīgo jomu, Jānorāda, ka viens pētījums var aplūkot vairākus aspektus.



3. attēls. Prasmju trūkuma kategorizēšana, pamatojoties uz literatūras pārskatu.

Ir skaidrs, ka organizācijai, cilvēku un sociālajai drošībai pievērsts mazāk uzmanības, salīdzinot ar sistēmas drošību, savienojuma drošību un elementu drošību. Tehniskās, sistēmas un elementu drošības izpēte tiek veikta, izmantojot konkrētas testēšanas vides un/vai kiberfizikālās enerģijas sistēmas (*cyber physical energy system — CPES*) laboratorijas eksperimentu veikšanai un/vai studentu mācīšanai.

4.2. Tehnoloģijas un izglītības attīstība

4.2.1. Kiberdrošības apdraudējumi viedajā energotīklā

CPES ietver vairākas inženierijas jomas un komunikācijas disciplīnas, kurām nepieciešamas atbilstošas mācību programmas un būtiski rīki, lai identificētu ievainojamību. Lai novērstu iepriekšējos un gaidāmos kiberuzbrukumu notikumus, ļoti nepieciešami pasīvi un aktīvi pretpasākumi. Sistēmas operatoriem un praktizējošiem darbiniekiem nepieciešama reālistiska testēšanas vide, lai pārbaudītu reālās dzīves scenārijus un pretpasākumus. Kiberuzbrukumi ietver tīklierosas ierīces, kuru programmatūra tiek inficēta ar ļaunprogrammatūru. Pēdējos gados pret viedo energotīklu sistēmām veikti vairāki kiberuzbrukumi. Šie kiberuzbrukumi var tikt veikti apzināti vai neapzināti un ietekmē konfidencialitāti, integritāti un pieejamību (*confidentiality, integrity, and availability — CIA*). Kiberuzbrukuma klasificēšana, ņemot vērā *CIA* aspektu, ir veikta 1. tabula. .

1. tabula. Kiberuzbrukumu klasificēšana, ņemot vērā *CIA*.

Kiberuzbrukuma veids	Īss apraksts	Piemērs
Konfidencialitāte	Datu aizsargāšana, nepieļaujot neatļautu informācijas atklāšanu.	Pārtvērējuzbrukums, *Stuxnet*, pikšķerēšanas kampaņa, *SQL* iespraudzbrukums, sānu kanāla uzbrukums, tiesību piesavināšanās, *AES* kešatmiņas uzbrukums
Integritāte	Pārtverts un izmainīts ziņojums.	Nepatiesu datu ievadīšana, slodzes maiņas uzbrukums, pikšķerēšanas kampaņa, manipulācija
Pieejamība	Ziņojuma/plūsmas bloķēšana vai aizkavēšana	*DoS*/*DDoS*, izspiedējprogrammatūra, bloķēšanas uzbrukums, tiesību piesavināšanās, *AES* kešatmiņas uzbrukums, bufera pārpilde

4.2.2. Pretpasākumi

Nav viena pretpasākuma visiem uzbrukumiem. Katram uzbrukumam nepieciešami pretpasākumi atkarībā no uzbrukuma konteksta. Vairāki pētījumi par kiberdrošību viedajā energotīklā iesaka izmantot plaši pazīstamus pretpasākumus, piemēram, ielaušanās atklāšanas sistēmu (IAS), demilitarizētas zonas (DMZ), aparatūras snieguma rādītājus (*hardware performance counters — HPC*), bloķētāju, žurnālu pārvaldību, daudzfaktoru autentifikāciju, aktīvu tīkla uzraudzību, IP adresi un lietotņu iekļaušanu baltajā sarakstā, tīkla segmentāciju un viedos slēdžus/maršrutētājus, kā arī apmācību informētībai par drošību.

4.2.3. Kiberfizikālās enerģijas sistēmas (*Cyber Physical Energy System — CPES*) laboratorija

Mūsdienās universitātes, valdība un nozares pārstāvji ir izveidojuši testēšanas vides, lai veiktu eksperimentus attiecībā uz kiberdrošības izpēti un attīstību. Kiberdrošības temati ir sarežģīti un ietver zināšanas par vairākām jomām, piemēram, datorinženieriju, elektrotehniku, rūpniecības celtniecību. Jomu starpsavienojums ļauj praktizējošiem darbiniekiem izprast un gūt vispārēju priekšstatu par to, kā dažādas jomas ir savienotas. Daudzfunkcionālai un vairāku jomu testēšanas videi ir vairāk priekšrocību nekā videi ar vienu funkciju un jomu. Vienkārša un lēta testēšanas vide ļauj bakalaura līmeņa studentiem atveidot un izpētīt kiberdrošības pamatprincipu. Sarežģīta testēšanas vide ir dārga, un nozares pārstāvju sadarbība ar universitāti var paātrināt modernu novatorisko izpēti.

4.2.4. Komunikācijas protokoli

Kiberdrošības izpēte un izglītība pievērš uzmanību arī komunikācijas protokoliem, kas pastāv starp ierīcēm un/vai sistēmām. Protokoli tiek pārbaudīti laboratorijā un konkrētā testēšanas vidē. Jebkādai datu pārraidei tīkla ietvaros nepieciešami standarta protokoli, kas definē noteiktus komunikācijas noteikumus. Pastāv vairāki komunikācijas protokoli, kas atkarībā no latentuma, uzticamības, datu pārraides ātruma, mērogojamības un drošības ir tikuši izmantoti viedajos energotīklos. *IEC* 61850 ļauj nodrošināt dažādu ražotāju dažādu elementu un funkciju sadarbspēju.

Tā kā *IEC* 61850 vieglas savienošanas ar *ethernet* un standartizētu ziņojumu struktūru dēļ kļūst aizvien populārāks elektroenerģijas automatizācijas sistēmās, tikušas atklātas ievainojamības attiecībā uz pieeju konfidenciāliem datiem un pakalpojuma traucējumu, kas saistītas ar datu apmaiņas integritāti. Lai uzlabotu kiberdrošību elektroenerģijas komunikācijas ziņā, *IEC* 62351 var nodrošināt gala–gala informācijas drošību energosistēmu vadības darbībām. Tas definē dažādas prasības drošai datu komunikācijai un apstrādei energosistēmās. *IEC* 62351 standarts pievērš vairāk uzmanības *IEC TC* 57 protokolu drošībai, kas var sniegt atbalstu autentifikācijai un šifrēšanai. *IEC* 62351 var nodrošināt *IEC* 61850 ziņojumus, piemēram, kā *GOOSE*, *SV*, *R-GOOSE*, *R-SV*.

4.3. Trūkumu analīze

Energosistēma ir sarežģīta un ietver dažādas ierīces un protokolus. Universitātes izstrādātā testēšanas vide galvenokārt ir nepilnīga attiecībā uz nozarē pastāvošo īstās pasaules praksi. Lai izglītotu studentus un praktizējošos darbiniekus, testēšanas vide jāuzstāda un jāaprīko ar iestrādātiem elementiem un reālistisku vidi, kurā veikt vairāku jomu holistisko eksperimentu. Esošo *CPES* laboratoriju un/vai testēšanas vižu trūkumu analīzes apkopojums ir parādīts 2. tabula..

2. tabula. Esošo *CPES* laboratoriju / testēšanas vižu trūkumu analīze.

Aspekts	Prasmju trūkuma analīze
Mērķis	Ierobežota tikai vienas jomas analīze — vai nu energosistēmai, vai komunikācijas tīklam.
Uzticamība	Tīras simulācijas testēšanas vide. Trūkst padziļinātu zināšanu par *ICS* elementu, fizikālo procesu un praktisko īstenošanu.
Pieejamība	Tikai fiziska pieejamība. Trūkst saskarnes platformas atbalsta.
Elastība	Nav iespēju izvēlēties starp simulāciju vai fizikālajiem procesiem. Pašizstrādāta protokola dēļ nav iespējams konfigurēt īsto elementu. Trūkst spēju ieviest dažādus simulatorus.
Mērogojamība	Ierobežotu resursu dēļ trūkst spējas palielināt eksperimenta mērogu.
Lietojuma ērtība	Vairāki programmēšanas rīki. Trūkst grafiskās lietotājsaskarnes.
Rentabilitāte	Augstas ieguldījumu izmaksas īstai/fizikālai ierīcei un elementiem.
Atkārtojamība	Testēšanas vides arhitektūras dizaina zemā granularitāte atkārtojamībai un uzticamībai. Mērījuma nenoteiktība. Nav atkārtojams pašizstrādāta reālās dzīves rūpnieciskā procesa dēļ.
Standarts un protokols	Vairākiem aparatūras un komunikācijas protokoliem trūkst atbalsta. Nepieciešama jauna *ICS* testēšanas vide, kas apvieno vecos un jaunos protokolus.

Aspekts	Prasmju trūkuma analīze
	Trūkst *IoT* vārtejas un īstu ierīču.
Zināšanas	Starpdisciplināru zināšanu trūkums, kas ietver tikai datorinženieriju vai elektrotehniku.

Spriežot no kibernotikumiem, kuri pasaulē ir pieredzēti līdz šim, apdraudētāju tehniskās spējas ir ievērojami attīstījušās. Tāpēc svarīgām infrastruktūrām viedajā energotīklā jāspēj noteikt kiberuzbrukumu un atlabt pēc tā. 3. tabula. saskaņā ar *CPES* pielietojumu identificē *CPES* kiberdrošības trūkumus.

3. tabula. *CPES* kiberdrošības riski.

Zona/pielietojums	Kiberdrošības risks
Robežu aizsardzība	- Nekonstatēta neatļauta darbība svarīgajās sistēmās. - Vājākas robežas starp *ICS* un uzņēmumu tīkliem.
Resursu sadale	- Nav rezerves vai cits personāls aizvietošanai gadījumā, ja galvenais personāls nevar strādāt. - Zaudētas svarīgas zināšanas par vadības sistēmām.
Konta pārvaldība	- Apdraudēta, nedroša komunikācija par paroli. - Apdraudēta parole var pieļaut uzticamu neatļautu piekļuvi sistēmām.
Identifikācija un autentifikācija	- Trūkst atbildības par lietotāja darbībām un to izsekojamība, ja konts ir apdraudēts. - Aizvien lielākas grūtības attiecībā uz kontu drošību, ja darbinieki atstāj organizāciju, it īpaši attiecas uz lietotājiem ar administratora pieeju.

Fiziskas piekļuves kontrole	- Neatļauta fiziska piekļuve aprīkojumam un atrašanās vietām rada lielāku iespēju veikt tālāk minētās darbības.
	  o Ļaunprātīgi pārveidot, dzēst vai kopēt ierīces programmas un aparātprogrammatūru.
	  o Piekļūt *ICS* tīklam.
	  o Nozagt vai sabojāt kiberaktīvus.
	- Pievienot ierīces ar ļaunprogrammatūru, lai ierakstītu un pārsūtītu tīkla datplūsmu.

Vismazākā funkcionalitāte	- Lielāki vektori, kas ļauj ļaunprātīgām pusēm piekļūt svarīgām sistēmām. - Izveidota neatļauta un ļaunprātīga iekšējā piekļuve.

5. Tehnikas līmenis viedo energotīklu un kiberdrošības izglītībā

5.1. Augstākās izglītības mācību programmas

Kopā tika izpētītas 84 universitātes, kas informācijas tehnoloģiju mācību programmās piedāvā ar drošību saistītu informāciju. 14 no 84 universitātēm neatbilda vispārējiem kritērijiem. Pastāv konkrēti mācību programmu kritēriji saistībā ar kiberdrošību, tomēr informācijas tehnoloģijas, informātikas vai datorsistēmu mācību programmas nenodrošina padziļinātas zināšanas par kiberdrošību. Kiberdrošības izglītības tehniskā attīstība notiek ātri, bet kopumā mācību programmu pielāgošana universitātē notiek lēni. Vienmēr ir sarežģīti mazināt atšķirības starp nozares vajadzībām un izglītības rezultātiem topošo pētnieku un inženieru ziņā. Viena no galvenajām darbībām, lai to paveiktu, ir regulāri uzlabot jaunāko kontekstu un mācību metodes.

5.2. Tālākizglītības programmas

Pastāv profesionālas apmācības kursi [6], kas cenšas sagatavot studentus un profesionāļus karjerai jaunajā viedo energotīklu kiberdrošības jomā. Vairāki specializēti sertifikācijas kursi ļauj palielināt speciālistu kompetenci, spējas un prasmes un piedāvā konkrētu zināšanu klāstu. Pētījumā [7] ir atklāts, ka daudzās valstīs mācībās tiek piedāvāts vairāk zināšanu vienību. Piemēram, saskaņā ar stingrākajiem aptvēruma mērījumiem Spānijā, Francijā, Vācijā un Itālijā obligātajos kursos tiek mācīti 75 % zināšanas vienību (KU). Tomēr valsts lielums nav noteicošais faktors [7]. Var novērot vairāku profesionālo prakšu pieejamību un veicināšanu, kas ļauj palielināt zināšanas un nostiprināt specifisko tehnisko pieredzi, kas kopumā nepieciešama nozarē.

5.3. Masveida atvērtie interneta kursi (*Massive open online courses — MOOC*)

Tiešsaistes kursi kļūst aizvien populārāki, jo kļūst plašāk pieejami. Izmantojot *edX*, ir pieejami ar kiberdrošību saistīti tiešsaistes kursi. Tomēr pieejamie kiberdrošības izglītības kursi tiek organizēti, balstoties uz tematu, nevis uz izmantotajiem rīkiem, tādējādi studentiem apgrūtinot konkrēto kiberdrošības zināšanu praktizēšanu. Masveida atvērtie interneta kursi (*Massive open online course — MOOC*) vēl var attīstīties kiberdrošības un viedo energotīklu apmācību ziņā, to var izdarīt, sniedzot praktiskus piemērus, kuros studentiem ir iespējas gūt pieredzes reālās dzīves laboratorijās, t. i., reāllaika simulācijās.

6. Prasmju trūkuma identificēšana viedo energotīklu kiberdrošībā

Lai labāk izprastu reālās dzīves situāciju nozarē un akadēmiskajā vidē, mēs organizējām virtuālo semināru, lai izklāstītu literatūras pārskata rezultātus un sniegtu kontekstu enerģijas jomas kiberdrošības temata nepieciešamo rīku un prasmju pārrunāšanai. 4. tabula. parāda ieinteresēto personu semināra rezultātu. Seminārā apkopotie ieteikumi parāda, ka akadēmiskajā vidē ir nepieciešamas pamatzināšanas par kiberdrošību dažādās jomās (piemēram, komunikācijas tīklos, svarīgā infrastruktūrā), vairāk praktiskas pieredzes un dažādu kiberdrošības rīku izmantošana. Ir svarīgi pieminēt, ka studentiem, kuri nākotnē vēlas iegūt darbu šajā nozarē, kiberdrošības mācību programmās nepietiek ar teorijas mācīšanu un izklāstīšanu.

4. tabula. Ieteikumi no ieinteresēto personu semināra [8].

Joma	Aspekti, kurus jāsāk ietvert	Aspekti, kurus jāturpina ietvert	Aspekti, kas jāietver biežāk	Aspekti, kas jāietver retāk
Akadēmiskā vide	• Savienot energosistēmu un komunikācijas infrastruktūru zināšanas. • Proaktīvi izstrādāt, attīstīt un uzraudzīt kiberdrošības pasākumu un politiku. • Atvēlēt vairāk budžeta pētniecībai.	• Testbud. • Būtiski izstrādes un testēšanas rīki. • Zināšanas par kiberdrošību vairākās jomās (piemēram, svarīga infrastruktūra, komunikācijas sistēma, energosistēma). • Praktiska pieredze.	• Zināšanas par elementu energosistēmā (RTU, *IED*, *PMU*). • Starptautiskas izpētes veikšana kiberdrošībā. • Profesionāla apmācība. • Sertifikāti (piemēram, *CISM*/*CISSP*/*CISA*/*CEH*).	• Tikai teorija.

Nozare	• Padziļināta izpratne par dažādu veidu drošības apdraudējumiem.	• Pašmācība. • Vairāku jomu izpratne (piemēram, energosistēma, komunikācijas tīkls). • Nulles uzticēšanās.	• Pašmācība. • Zināšanas par energosistēmas un komunikācijas tīkla ievainojamībām. • Funkcionālas vispārīgās prasmes. • Jaunu tehnoloģiju apguve. • Zināšanas par populārākajām *SCADA* platformām. • Praktiskas lietošanas piemēri. • Apdraudējuma analīzes pamatrīki.	-

7. Noderīgu rīku identificēšana viedo energotīklu kiberdrošībā

7.1. Pamatrīki aktīvām mācībām par kiberdrošību

Ir vairākas zināšanu izplatīšanas pieejas, kuras var izmantot vispārēji kiberdrošības un konkrēti viedo energotīklu jomās. 5. tabula. parāda izglītības pieejas viedajā energotīklā un kiberdrošībā, lai veidotu padziļinātas zināšanas un izpratni par galvenajiem jēdzieniem, kas saistīti ar nozari, kā arī nodrošinātu analītiskas prasmes, kas nepieciešamas turpmākai attīstībai.

5. tabula. Izglītības pieejas viedajā energotīklā un kiberdrošībā.

Pieeja	Mērķis	Rīku piemēri
Attālinātas un virtuālas laboratorijas	pašmācība un reālajiem apstākļiem pietuvinātas saskarsmes veidošana klasē	*Labview*, *OMWeb*, *NI ELVIS*, *Labster*, *LabAlive*
Paplašinātā realitāte	interaktīva mācīšanās	*Worklink*, *CoSpaces*, *Merge Cube*
Datu vizualizācija	vizualizācija un analītika	*Tableau*, *Microsoft Power Bi*, *IBM Congos Analytics*
Mākoņdatošana	moderni algoritmi un funkcijas, piemēram, datizrace un mašīnu dziļā mācīšanās	*Google Classroom*, *Microsoft Education Center*, *Amazon Web Services*
Apgrieztā mācīšana	aktīvas inženierijas mācības	Masveida atvērtie interneta kursi (*Massive Open Online Courses — MOOC*)
Spēliskošana un spēļu teorija	varbūtības un kiberdrošības scenāriju analīze	*Kahoot*, *Gimkit*
Simulācija	dažādu gadījumu izmēģināšana un testēšana	*MATLAB*, *Simulink*

7.2. Uzlaboti ievainojamību eksperimentu rīki

Viedā energotīkla sistēma ir kompleksa un ietver elektrotīklu un komunikāciju tīklus. Pēdējos gados viedo energotīklu sistēmās ir notikuši vairāki kiberuzbrukumi, kuri ir izraisījuši ievērojamas sekas. Traucējumi būtībā ir kompleksi, un tiem var būt plašs klāsts avotu, tostarp dabas parādības un cilvēku izraisīti notikumi. 6. tabula. parāda uzlabotus rīkus, kas kategorizēti pēc to funkcijām, ievainojamību novēršanai un eksperimentiem.

6. tabula. Viedo energotīklu kiberdrošības rīki.

Rīks	Funkcija
Drošības platforma	Vienota drošības pārvaldība, lai nodrošinātu centralizētu vadību un darbības pret apdraudējumiem, kas ietekmē organizācijas infrastruktūru.
Tīkla uzraudzība	Uzraudzīt tīkla kvalitāti, lai novērstu atteici vai traucējumus, tādējādi nodrošinot nepārtrauktību un veiktspējas līmeni.
Ievainojamības skenēšana	Skenēt dažādas sistēmas un programmatūras elementus izmēģinājumos, lai identificētu trūkumus un vājības, kuras var izmantot.
Ielaušanās testēšana	Novērtēt sistēmas drošību, izmantojot atrastās ievainojamības.
Pakešu okšķeri un porta skeneri	Uzraudzīt tīkla datplūsmu, identificēt aktīvos pakalpojumus un novērtēt drošības politiku.
Šifrēšana	Saglabāt konfidencialitātes un informācijas nepretrunīgumu, tādējādi pasargājot datus no neatļautas piekļuves.
Pretvīruss	Noteikt un rīkoties pret ļaunprogrammatūru un citu nelikumīgu programmatūru, piemēram, izspiedējprogrammatūru, tārpiem, Trojas zirgu utt.
Ugunsmūris	Nodrošināt aizsardzību pret uzbrukumiem, novēršot ļaunprātīgas datplūsmas iekļūšanu noteiktā tīklā vai viedierīcē.
Bezvadu drošība	Novērst neatļautu piekļuvi bezvadu tīklam, kā arī aizsargāt nosūtītu datplūsmu, nodrošinot augsta līmeņa datu šifrēšanu.
Paroļu pārvaldība	Droši kontrolēt kontus.

Esošie uzlabotie rīki galvenokārt ir paredzēti ar tehniku saistītām problēmām, kas attiecas uz kiberfizikālām sistēmām. Uzlabotajiem rīkiem būtu jābūt piemērotiem arī nepareiziem un nepareizi identificētiem apdraudējumiem, kā arī ilgākam noteikšanas un reaģēšanas laikam. Tas palīdzētu studentiem iegūt praktisku pieredzi, izmantojot aktīvās mācības.

8. Secinājumi un ieteikumi

ES ir identificējusi kiberdrošības izglītību kā vienu no stratēģiskajām digitālajām prasmēm, kas jāuzlabo, nodrošinot formālu un ikdienēju mācīšanos (tostarp PIA, tālākizglītību) un praktisku tematu pielietojumu (praktizēšanu) organizāciju pētniecības un izstrādes projektos. Kiberdrošība ir ietverta dažādās izglītības formās, piemēram, augstākajā izglītībā, tālākizglītībā un *MOOC*. Viedo energotīklu attīstības kiberdrošības mācību programmu uzlabošanas galvenās prasības ir minētas tālāk.

- Izglītībai jābūt pieejamai dažādām ES pilsoņu grupām (tostarp uzņēmumiem, C līmeņa vadītājiem, pieaugušajiem, kas vēlas paaugstināt savu kvalifikāciju un pārkvalificēties, un jaunajiem speciālistiem).
- Ieteicams piedāvāt kiberdrošības attālinātās mācīšanās, tiešsaistes un kombinēto mācību iespējas, lai padarītu kvalifikācijas paaugstināšanu un pārkvalifikāciju pieejamāku pieaugušajiem.
- Izglītībā jāaplūko vispārēji drošības apsvērumi un ar nozari saistīti temati (piemēram, enerģijas piegādes ķēdes kiberdrošība un rīki/metodes, kā arī pasākumi to uzraudzībai un kontrolei).
- Jānodrošina teorētiskas lekcijas un praktiska apmācība, piemēram, kiberdrošības pārvaldības rīku un virtuālo laboratoriju izmantošana, un jāveic simulācijas un eksperimenti, izmantojot digitālos dvīņus un līdzīgas vides. Viedo energotīklu

kiberdrošības izglītībā ir svarīgi konkrēti ar viedo energotīklu saistītie drošības rīki, piemēram, enerģētikas jomas pārziņu uzraudzības rīki.

- Izglītības un apmācības programmas jāizstrādā sadarbībā ar atbilstošiem partneriem (piemēram, universitātēm un nozares pārstāvjiem).
- Viedo energotīklu kiberdrošības programmās uzmanība jāpievērš visām šīm jomām [9]: konfidencialitāte, integritāte un pieejamība (tostarp sniegums un savlaicīgums), kā arī datu privātums (organizācijas, integritātes un konfidencialitātes kombinācija) un nenoliedzamība (piemēram, elektroniskie līgumi). Tātad tvērums ir lielāks par tikai datu drošību, jo datu drošība ir tikai viens (un svarīgs) no drošības aspektiem, ieviešot viedos energotīklus Eiropā.
- Kiberdrošības temati jāietver kā obligāta enerģētikas mācību programmu daļa.
- Lai kiberdrošības izglītība būtu interaktīvāka un studentiem pievilcīgāka, ieteicams ieviest spēliskošanas elementus, piemēram, apdraudējumu spēles, kiberpoligonus un kiberdrošības izbēgšanas spēles.
- Studentiem jānodrošina reāllaika simulācijas infrastruktūras un praktiskie scenāriji, kā arī pamata un uzlaboto rīku pieejamība aktīvo mācību nolūkiem.
- Atbilstošas augstākās kiberdrošības izglītības kontekstā studentu mobilitāte jāuztver par programmu daļu.

9. Bibliogrāfija

[1] The European Commission, The Revised Digital Education Action Plan. The European Commission, 2020.

[2] The European Parliament, “Cybersecurity act,” 2019.

[3] The European Commission, The EU cybersecurity certification framework.

[4] J. T. F. on Cybersecurity Education, Curriculum Guidelines for Post- Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, 2017.

[5] Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) https://tcipg.org/.

[6] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, “Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application,” in 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, 2014.

[7] N. Dragoni, A. Lluch Lafuente, F. Massacci and A. Schlichtkrull, "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]," in IEEE Security & Privacy, 19. sēj,, Nr. 1, 81-88 lpp., Jan.-Feb. 2021, doi: 10.1109/MSEC.2020.3037446

[8] B. Siemers et al., "Modern Trends and Skill Gaps of Cyber Security in Smart Grid: Invited Paper," IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, 2021, 565-570 lpp., doi: 10.1109/EUROCON52738.2021.9535632.

[9] The European Commission, European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids. European Commission, 2019.