RĪGAS TEHNISKĀ UNIVERSITĀTE

Vladislavs Minkevičs

UZ LIELO DATU PARADIGMU BALSTĪTI RISINĀJUMI INFORMĀCIJAS SISTĒMU DROŠĪBAS PĀRVALDĪBAS UZLABOŠANAI

Promocijas darba kopsavilkums

RTU Izdevniecība
Rīga 2026

RĪGAS TEHNISKĀ UNIVERSITĀTE
Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte
Informācijas tehnoloģijas institūts

Vladislavs Minkevičs

Doktora studiju programmas "Informācijas tehnoloģija" doktorants

UZ LIELO DATU PARADIGMU BALSTĪTI RISINĀJUMI INFORMĀCIJAS SISTĒMU DROŠĪBAS PĀRVALDĪBAS UZLABOŠANAI

Promocijas darba kopsavilkums

Zinātniskais vadītājs
asociētais profesors
Dr. sc. ing. JĀNIS KAMPARS

RTU Izdevniecība
Rīga 2026

Minkevičs V. Uz lielo datu paradigmu balstīti risinājumi informācijas sistēmu drošības pārvaldības uzlabošanai. Promocijas darba kopsavilkums. – Rīga: RTU Izdevniecība, 2026. – 46 lpp.

Iespiests saskaņā ar promocijas padomes "RTU P-07" 2026. gada 23. janvāra lēmumu, protokols Nr. 04030-9.7/1.

Vāka attēls – MI ģenerēts no *www.freepik.com*.

https://doi.org/10.7250/9789934372902

ISBN 978-9934-37-290-2 (pdf)

PROMOCIJAS DARBS IZVIRZĪTS ZINĀTNES DOKTORA GRĀDA IEGŪŠANAI RĪGAS TEHNISKAJĀ UNIVERSITĀTĒ

Promocijas darbs zinātnes doktora (*Ph. D.*) grāda iegūšanai tiek publiski aizstāvēts 2026. gada 11. maijā plkst. 14.30 Rīgas Tehniskās universitātes Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultātē, Zundas krastmalā 10, 206. auditorijā.

OFICIĀLIE RECENZENTI

Asociētais profesors *Dr. sc. ing.* Dmitrijs Bļizņuks,
Rīgas Tehniskā universitāte

Profesors *Dr. sc. ing.* Gatis Vītols,
Latvijas Biozinātņu un tehnoloģiju universitāte, Latvija

Profesors *Dr. sc.* Linas Bukauskas,
Viļņas Unversitāte, Lietuva

APSTIPRINĀJUMS

Apstiprinu, ka esmu izstrādājis šo promocijas darbu, kas iesniegts izskatīšanai Rīgas Tehniskajā universitātē zinātnes doktora (*Ph. D.*) grāda iegūšanai. Promocijas darbs zinātniskā grāda iegūšanai nav iesniegts nevienā citā universitātē.

Vladislavs Minkevičs ……. (paraksts)

Datums: ……

Promocijas darbs ir uzrakstīts latviešu valodā, tajā ir ievads, četras nodaļas, secinājumi, literatūras saraksts, 49 attēli, 32 tabulas, viens pielikums, kopā 171 lappuse, ieskaitot pielikumus. Literatūras sarakstā ir 140 nosaukumu.

ANOTĀCIJA

Darbs veltīts aktuālas mūsdienu problēmas risināšanai, kas saistīta ar informācijas sistēmu drošības risku mazināšanu organizācijā. Darba rezultātā tika izstrādāts adaptīvais drošības pārvaldības modelis, kā arī tehnoloģiskā platforma drošības risku mazināšanai, kas, reaģējot uz incidentiem, veic atbilstošas adaptācijas. Izstrādātā tehnoloģiskā platforma un piedāvātais moduļu komplekts apvieno daudzus informācijas avotus un balstās lielo datu paradigmā, nodrošinot adekvātu informācijas sistēmu drošību, tai skaitā izpildot gan Eiropas, gan Latvijas likumdošanas prasības kiberaizsardzības jomā. Izstrādātais risinājums tika aprobēts Rīgas Tehniskajā universitātē (RTU) un ir apliecinājis savu efektivitāti, uzlabojot spēju reaģēt uz identificētiem incidentiem un samazinot Latvijas informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (*CERT.LV*) paziņojumus par inficētām iekārtām RTU tīklā par 99,98 %, kā arī palielinot spēju nekavējoties reaģēt uz drošības incidentiem. Automatizēta un operatīva potenciāli inficētas ierīces lietotāja iesaiste incidenta risināšanā, izmantojot piedāvāto tehnoloģisko platformu, nodrošināja drošības risku mazināšanu, laikus ieviešot preventīvas vai korektīvas darbības. Darbā piedāvātā tehnoloģiskā platforma ir mērogojama un balstīta atvērtajās tehnoloģijās un lielajos datos. Platformu var lietot jebkurā organizācijā vai iestādē, kas var nodrošināt piekļuvi auditācijas pierakstiem un savai tīkla datu plūsmai, jo platformas darbības pamatā ir datu analīze no dažādiem avotiem, tai skaitā ielaušanās noteikšanas, novēršanas sistēmām, ugunsmūriem, tīkla datiem, kā arī jebkuriem citiem citiem datu avotiem, kas ir spējīgi veidot auditācijas pierakstus. Platforma nodrošina iesūtīto datu agregāciju un analīzi, kā arī pielieto uz mašīnmācīšanās algoritmiem balstītas pieejas iepriekš neidentificētu apdraudējumu detektēšanai, analizējot gan domēnu pieprasījumus, gan tīkla plūsmas datus. Piedāvātā platforma būtiski atvieglo drošības risku pārvaldību organizācijā, laikus atklājot un dažādos veidos automātiski reaģējot uz identificētajiem drošības riskiem. Darba rezultāti tika aprobēti ne tikai RTU, bet arī Iepirkumu uzraudzības birojā un Centrālajā finanšu un līgumu aģentūrā.

SATURS

SAĪSINĀJUMU SARAKSTS 6
DARBA VISPĀRĒJS RAKSTUROJUMS 7
Tēmas aktualitāte 7
Darba mērķis un uzdevumi 11
Pētījuma metodika 12
Darba zinātniskie jaunieguvumi 13
Darba praktiskā nozīme 14
Darba apjoms un struktūra 17
1. LITERATŪRAS APSKATS UN IESPĒJAMIE PROBLĒMAS RISINĀJUMI 19
2. SPĒJORIENTĒTĀ DROŠĪBAS PĀRVALDĪBA 21
3. SPĒJORIENTĒTA DROŠĪBAS PĀRVALDĪBAS MODEĻA IEVIEŠANA RTU 25
4. IS DROŠĪBAS PĀRVALDĪBAS PLATFORMAS NOVĒRTĒJUMS 31
REZULTĀTI UN SECINĀJUMI 36
LITERATŪRAS SARAKSTS 37

SAĪSINĀJUMU SARAKSTS

EDR – (*Endpoint Detection and Response* – Galaierīču atklāšana un reaģēšana) tiek izmantots, lai noteiktu, vai galaierīcē ir uzinstalēta ļaunprātīga programmatūra, un atrastu veidus, kā reaģēt uz šāda veida draudiem.

SIEM – (*Security Information and Event Management* – Drošības informācijas un notikumu pārvaldība) tiek izmantots, lai nodrošinātu vienotu centrālo vietu datu glabāšanai un analīzei no dažādiem žurnālu avotiem.

SOC – (*Security operations centre* - Drošības operāciju centrs) ir vieta, kur tiek monitorēta tīkla, serveru un citu sistēmu drošība, izmantojot dažādus rīkus un tehnoloģijas, lai identificētu un novērstu drošības apdraudējumus.

ISMS – (*Information security management system* – Informācijas drošības pārvaldības sistēma) darbā piedāvātā adaptējamā drošības operāciju centra platforma, kuras pamatā ir spējās izstrādes metodika.

IDS – (*Intrusion detection system* – Ielaušanās noteikšanas sistēma) ielaušanās noteikšanas sistēma, kuras mērķis ir reālā laikā identificēt apdraudējumus tīkla datos.

NetFlow – *CISCO* ieviests risinājums tīkla metadatu vākšanai un analīzei.

CERT.LV – kiberincidentu novēršanas institūcija, kuras mērķis ir veicināt informācijas tehnoloģiju drošību Latvijā.

CDD – (*Capability driven developement* – Spējā izstrāde) spējās izstrādes metodika adaptīvu risinājumu specificēšanai un implementēšanai.

DGA – (*Domain generation algorithm* – Domēnu ģenerēšanas algoritms) algoritmiski ģenerēti domēni, ko izmanto robotu tīkli, lai sazinātos un nodotu nepieciešamās instrukcijas.

SVC – (*Support Vector Classification* - Atbalsta vektoru klasifikācija) uzraudzītas mašīnmācīšanās klasifikators atbalsta vektoru klasifikācija.

NNC – (*Neural Network Classifier* – Neironu tīkla klasifikators) uzraudzītas mašīnmācīšanās klasifikatora neironu tīkli, kas atdarina bioloģiskos procesus dzīvo organismu smadzenēs.

DTC – (*Decision Tree Classifier* - Lēmumu koka klasifikators) uzraudzītās mašīnmācīšanās klasifikatora lēmumu koki, kas tiek plaši izmantoti lēmumu vizualizācijai.

RFC – (*Random Forest Classifier* – Lēmumu mežu klasifikators) uzraudzītās mašīnmācīšanās klasifikatora lēmumu meži, kas ir lēmumu koku apvienojums.

MAC – (*Media Access Control address* – MAC adrese) ierīces unikālā adrese, ko tai piešķir ierīces ražotājs ražošanas procesā. Adrese ietver gan ražotāja kodu, gan arī unikālu ierīces identifikatoru.

DARBA VISPĀRĒJS RAKSTUROJUMS

Tēmas aktualitāte

Mūsdienu pasaulē ir grūti iedomāties jomu, kas var pastāvēt bez informācijas tehnoloģiju klātbūtnes. Gan valsts, gan privātais sektors ir atkarīgi no informācijas tehnoloģijām, un, ņemot vērā arvien pieaugošos digitalizācijas procesus pasaulē, šī atkarība arvien pieaug un pieaugs arī nākotnē [1]. Informācijas komunikāciju tehnoloģijas galvenokārt tiek lietotas, lai atvieglotu cilvēku dzīvi, veicot attālinātas un drošas darbības ar finansēm, saziņai ar valsts institūcijām un citiem mērķiem. Pieaugot atkarībai no informācijas un komunikāciju tehnoloģijām, pieaug arī varbūtība, ka ar to palīdzību ir iespējams nodarīt būtisku kaitējumu publiskās pārvaldes informācijas sistēmām un elektronisko sakaru tīkliem, neitralizēt valsts politisko, ekonomisko, militāro lēmumu pieņemšanas centrus, dezinformēt sabiedrību un izraisīt tehnogēnas avārijas. Tas rada pieaugošu nemilitāru draudu iespējamību ar smagām sekām. Valsts funkciju nodrošināšanā iesaistītajām iestādēm valsts informācijas sistēmu drošības jautājumi ir īpaši nozīmīgi un aktuāli.

Gan valstis atsevišķi, gan Eiropas Savienība kopumā ir pieņēmusi likumus, direktīvas un regulas, kas reglamentē informācijas tehnoloģiju drošību, viena no pēdējām iniciatīvām Eiropas savienībā ir NIS2 direktīvas pieņemšana [2]. Šajos normatīvajos aktos ir definētas minimālās prasības datu aizsardzībai konfidencialitātes, integritātes un pieejamības jomā, kas kopumā uzlabo kiberdrošību. Kiberdrošību var definēt vairākos veidos. Saskaņā ar [3] kiberdrošība ir spēja aizsargāt tīklus, ierīces un datus no neatļautas piekļuves vai noziedzīgas izmantošanas, kā arī spēja nodrošināt informācijas konfidencialitāti, integritāti un pieejamību. Kiberdrošība var tikt iedalīta tīkla drošībā, informācijas drošībā un citās kategorijās.

Saskaņā ar drošības kompāniju MITRE Corporation kiberdrošības risku mazināšanu nepieciešams plānot, ieviest un uzraudzīt tās progresu.

Risku mazināšana iekļauj:

- pieņemšanu – atzīt konkrēta riska esamību un apzināti lemt par tā pieņemšanu, neveicot darbības tā kontrolēšanai; šajā gadījumā nepieciešama sistēmas īpašnieku piekrišana;
- samazināšanu – pielāgot prasības vai ierobežojumus, lai novērstu vai samazinātu risku; šie pielāgojumi tiek veikti, mainot finansējumu, izpildes grafikus vai tehniskās prasības;
- kontroli – īstenot darbības, lai samazinātu riska ietekmi vai tā iestāšanās varbūtību;
- nodošanu – nodot atbildību un pilnvaras citai ieinteresētajai personai, kura vēlas uzņemties risku par samaksu, piemēram, apdrošināšanas kompānijai;

- uzraudzību – novērot vidi, lai identificētu izmaiņas, kas ietekmē riska iestāšanās varbūtību un/vai ietekmi.

Tomēr arvien vairāk ir dzirdēts par dažādiem kiberdrošības incidentiem, kas dažkārt skar pat visu pasauli, piemēram, *SolarWinds* [4], *Colonial Pipeline* [5] un pieejas atteices uzbrukumi Latvijas valsts iestādēm [6]. Šādu incidentu organizatori parasti ir labi finansētas noziedzīgās organizācijas, dažādi noziedzīgi grupējumi un pat valstis.

Robotu tīkli mūsdienās ir kļuvuši par vienu no lielākajiem kiberdrošības draudiem. Saskaņā ar *ENISA* pārskatu par 2019.–2020.gadu tika identificēti vairāk nekā 17 tūkstoši funkcionējoši robotu tīklu serveri [7].

Ņemot vērā iepriekš minēto, jebkurai iestādei, organizācijai vai privātuzņēmumam nepieciešams pievērst pienācīgu uzmanību informācijas sistēmu drošības pārvaldībai. Valsts un pašvaldību iestāžu darbību nosaka ārējie normatīvie akti, piemēram, Nacionālās kiberdrošības likums [8], pakārtotie MK noteikumi u. c. normatīvie akti. Uz privātuzņēmumu, ja tas apstrādā personu datus, attiecas Vispārīgā datu aizsardzības regula [9], kuras 5. panta f) apakšpunkts nosaka, ka, apstrādājot personu datus, nepieciešams tos aizsargāt, izmantojot atbilstošus tehniskos un organizatoriskos pasākumus. Bieži vien tikai notikušie incidenti liek privātuzņēmumiem veikt darbības, lai ieviestu atbilstošus drošības pasākumus. Diemžēl presē atrodama informācija par incidentiem, kas skar personu datus, piemēram, *Marriott* viesnīcu tīkla datu incidents [10], kura rezultātā viesu vārdi, uzvārdi, lojalitātes informācija un citi personu dati nonākuši neautorizētu personu rīcībā. Jāatzīmē, ka *Marriott* viesnīcu tīkla incidents ir jau otrs šāda veida incidents divu gadu laikā un viesnīcu tīkls par pārkāpumiem jau ir saņēmis sodu 18,4 milj. britu mārciņu apmērā [11]. Līdzīgs gadījums ir noticis arī Lietuvā, kur "*City Bee*" lietotāju dati tika nozagti un tirgoti internetā [12]. Latvijā viens no ievērojamākaiem incidentiem, kas skāris personu datus, bija "*Civinity*" nekustamo īpašumu pārvaldības uzņēmumu grupas klientu datu zādzība [13]. Šie gadījumi pastāvīgi atgādina par kiberuzbrukumu radīto risku, ko nedrīkst novērtēt par zemu.

Vēl pagājušā gadsimta 80. gados neviens nevarēja iedomājies par ielaušanās noteikšanas sistēmu nepieciešamību datortīklu aizsardzībai. Ielaušanās noteikšanas sistēmu (*IDS*) pirmsākumi ir meklējami ASV gaisa spēkos, kur *James P. Anderson* bija izstrādājis datortīkla draudu uzraudzības sistēmu [14], kas bija spējīga nepārtraukti skenēt un salīdzināt tīkla datus ar zināmu draudu sarakstu. Pagājušā gadsimta 90. gados *IDS* tehnoloģijas tika attīstītas un jau bija spējīgas atklāt tīkla uzbrukumus, kas arvien pieauga gan skaita, gan sarežģītības ziņā [15].

Attīstoties *IDS* sistēmām, daudzas drošības kompānijas sāka piedāvāt mākoņrisinājumus, kur, lai iegūtu ielaušanās noteikšanas funkcionalitāti, vienīgais nosacījums ir nepieciešamo datu nogādāšana mākonī. Lai arī kā, bet šādi pakalpojumi nav pārāk populāri viena iemesla dēļ – dati, kas tiek sūtīti uz mākoni, var ietvert personu datus un sensitīvu uzņēmuma komercinformāciju. Vēl viena aktuāla problēma mūsdienās ir attiecīgo speciālistu, kuri varētu interpretēt iegūtos rezultātus un pieņemt lēmumus drošības uzlabošanai, trūkums [16]. Satraukums par arvien pieaugošiem kiberdraudiem ir vērojams arī dažādos aktuālos pētījumos, piemēram, *PricewaterhouseCoopers* uzņēmumu vadītāju pētījumā [17] par 2021. gadu, 47 % vadītāju atzīst, ka viņus satrauc kiberdraudi, salīdzinot ar 2020. gadu, tie bija tikai 33 %.

Viena no mūsdienu organizāciju un iestāžu kļūdām ir dzīvošana maldīgā drošības sajūtā, uzskatot, ka, ja par mums neviens neko sliktu neraksta presē, tad visam jābūt kārtībā. Diemžēl šāda pieeja nav tālredzīga. Organizācijām nepieciešams lietot preventīvu pasākumu kopumu, lai pasargātu gan komercnoslēpumu, gan organizācijas darbinieku privātos datus no to nonākšanas nepilnvarotu personu rīcībā. Kā vienu no pirmajiem pasākumiem autors piedāvā norīkot par drošības pārvaldību atbildīgo personu.

Par drošības pārvaldību atbildīgajai personai ir nepieciešams plašs rīku klāsts drošības nodrošināšanai, kā arī atbilstošas zināšanas, kā šos rīkus lietot. Ir nepieciešams veikt gan tīkla, gan galaiekārtu uzraudzību, kā arī saprast ugunsmūra konfigurāciju un novērtēt iespējamos apdraudējumu avotus, tai skaitā noteikt ievainojamības ierīcēs un nepārtraukti sekot līdzi aktuālai informācijai informācijas un komunikāciju tehnoloģiju jomā. Rīku klāsts ir ļoti plašs un katram rīkam ir savas priekšrocības un savi trūkumi, tāpēc nepieciešams risinājums, kas apvieno pieejamo rīku priekšrocības, samazina to trūkumus, kā arī apstrādā un reaģē uz incidentiem, izmantojot daudzdimensionālu pieeju.

Yakencheck Jason, kurš pārstāv *securityintelligence.com* [18], uzskata, ka mūsdienās drošības pārvaldības īstenošanai ar manuālām darbībām vairs nepietiek. Speciālistam kiberdrošības jomā jābūt spējīgam izstrādāt un ieviest automatizācijas līdzekļus drošības uzraudzībai, kā arī jābūt padziļinātām zināšanām par datortīklu, ierīču arhitektūru, ievainojamībām, kiberaizardzības līdzekļiem un to efektivitāti. Lai arī drošības pārvaldības īstenošanai nepieciešamo tehnisko pusi ir iespējams īstenot, izmantojot maksas un bieži vien ērti izmantojamus, dažādu ar kiberdrošību saistītu uzņēmumu risinājumus [19], plašā klāstā ir pieejami arī bezmaksas atvērtā koda risinājumi un rīki.

Drošības pārvaldības problēmas risināšanai ir nepieciešams ņemt vērā kontekstu, ko veido ārējie datu avoti, dažādi informācijas sistēmu lokālie mērījumi un uzņēmuma definētie mērķi. Pilnvērtīgai konteksta informācijas apstrādei ir nepieciešams izmantot vairākus rīkus, jo gatavie risinājumi nespēj aptvert visu problēmapgabalu. Izaicinājums ir lielapjoma datu integrācija, lietojumprogrammu integrācija, kas papildināta ar mākslīgā intelekta moduļiem. Spējorientētā izstrādes metodoloģija palīdz veidot sistēmas, kas ir informētas gan par kontekstu, gan uzņēmuma mērķiem, tādēļ šī pieeja ir piemērota IS drošības pārvaldības modeļa izstrādei.

Katrs uzņēmums un iestāde vēlas justies droši mūsdienu digitālajā laikmetā, bet līdzekļi, ko šie uzņēmumi un iestādes atvēl informācijas sistēmu drošībai, joprojām tiek uzskaitīti izdevumu, nevis investīciju pozīcijās. Bieži vien par kiberdrošību tiek domāts maz vai netiek domāts vispār, līdz iestājas drošības incidents, vai arī kiberdrošība tiek noadresēta kādai trešai pusei, kurai nav izpratnes par organizācijas darbības mērķiem, un tiek nodrošināta minimālā aizsardzība, aizmirstot, ka kiberdrošība ir nevis stāvoklis, bet process. Saskaņā ar [20] kiberdrošība ietver piecas fāzes: identificēšana (izpratnes veicināšana par iespējamiem kiberriskiem), aizsardzība (risku mazinošo pasākumu īstenošana kritisko resursu aizsardzībai), draudu noteikšana (līdzekļu lietošana kiberdrošības incidenta noteikšanai), aktīva rīcība draudu gadījumā (darbību veikšana, lai mazinātu kiberdrošības incidenta ietekmi), kā arī atkopšanās pēc incidenta (pasākumu kopums, lai nodrošinātu servisu darbību pēc incidenta).

Ņemot vērā autora ilggadējo pieredzi par IS drošību atbildīgās personas amatā, kā arī pieredzi, kas gūta, piedaloties informācijas sistēmu un personu datu aizsardzības auditos, var secināt, ka galvenais izaicinājums uzņēmumos un iestādēs ir draudu noteikšanas un aktīvas rīcības fāzes (**Error! Reference source not found.**. tab.).

1. tabula

Kiberdrošības fāzes un risinājumi to nodrošināšanai

Kiberdrošības fāzes	Risinājumi
Identificēšana	*CERT.LV* [21] (informēšana)
Aizsardzība	2025. gada 25. jūlija Ministru kabineta noteikumi Nr. 397 [22] (Minimālās kiberdrošības prasības), *NIS2* direktīva [2]
Draudu noteikšana	*SOC* sistēmas [23], [24], [25], [26], [27], [28] (*SOC* ārpakalpojuma sniedzēji)

	1. tabulas turpinājums
Aktīva rīcība draudu gadījumā	Par IS drošību atbildīgās personas izpratnes un zināšanu līmenis (izglītība, sertifikācija, praktiskās iemaņas)
Atkopšanās pēc incidenta	2025. gada 25. jūlija Ministru kabineta noteikumi Nr. 397 [22] (Nepārtrauktās darbības plānošana), *NIS2* direktīva [2]

Ar līdzīgām problēmām bija saskārusies ikkatra organizācija, kurā autors ir vērtējis drošības pārvaldības atbilstību labajai praksei, it īpaši problēma ir aktuāla augstākās izglītības iestādēs, jo parasti drošības pārvaldības mērķim tiek atvēlēti ļoti nelieli līdzekļi un, īstenojot studiju procesu, vairāk tiek domāts par datortīklu ātruma un skaitļošanas jaudu palielinājumu. Lai īstenotu šīs fāzes, nepieciešama pilnvērtīga un nepārtraukta iekšējā tīkla, galaiekārtu un lietotāju darbību tīklā uzraudzība, kā arī jāsaprot, kā identificējams kiberdrošības incidents iekšējā tīklā.

Darba mērķis un uzdevumi

Promocijas darba mērķis ir izstrādāt no konteksta atkarīgu, adaptīvu drošības pārvaldības modeli un šī modeļa tehnisko realizāciju drošības pārvaldības platformā, kas ietver atbilstošus tehniskos risinājumus kiberdrošības vides uzlabošanai.

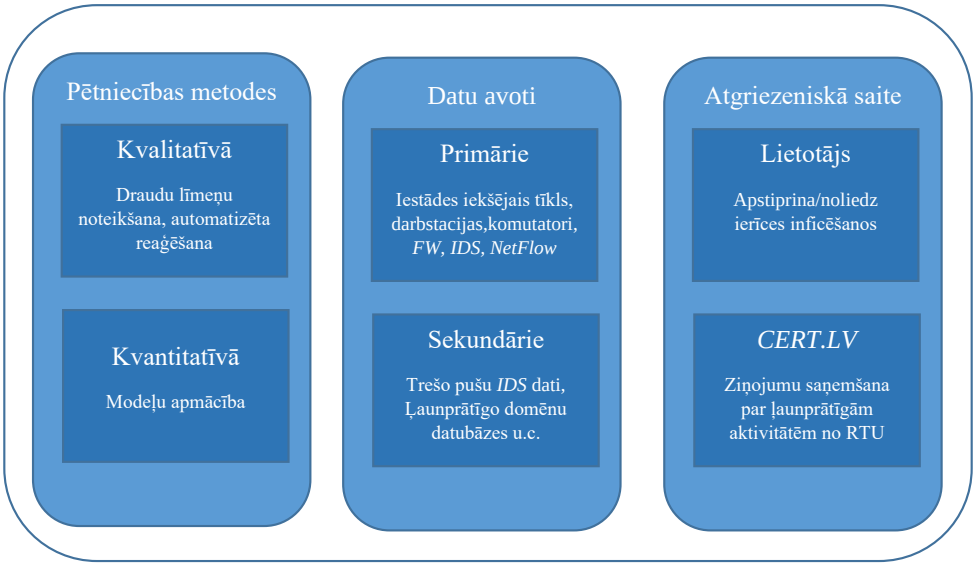
Definēto mērķi pamato pieņēmums, ka liela daļa organizāciju un iestāžu nav spējīgas pilnvērtīgi īstenot visas piecas kiberdrošības fāzes saskaņā ar [20].

Promocijas darba mērķa sasniegšanai definēti vairāki uzdevumi.

1. Novērtēt esošo situāciju IS drošības pārvaldības jomā, veicot literatūras analīzi un notikušo kiberdrošības incidentu iemeslu izpēti.
2. Apzināt esošos pētījumus IS drošības pārvaldības jomā, kuros tiek izmantoti gan tradicionālie draudu identificēšanas līdzekļi, gan mākslīgais intelekts nezināmo draudu identificēšanai, un pamatot tehnoloģiskās platformas būvēšanas nepieciešamību.
3. Sintezēt prasības no konteksta atkarīgam adaptīvam drošības pārvaldības modelim un tā tehniskajiem risinājumiem.
4. Izstrādāt no konteksta atkarīgu adaptīvu drošības pārvaldības modeli.
5. Aprobēt definēto modeli, izstrādājot atbilstoša tehniskā risinājuma (platformas) implementāciju augstākās izglītības iestādē.
6. Novērtēt izstrādātā modeļa un platformas efektivitāti.

Pētījuma metodika

Darba pamatā ir informācijas sistēmu drošības pārvaldības problēmu identificēšana un šo problēmu risinājumu piedāvāšana. Lai risinātu iepriekš minētās problēmas, darbā tika lietotas gan kvalitatīvās, gan kvantitatīvās pētniecības metodes (**Error! Reference source not found.**. att.). Draudu līmeņu noteikšana, balstoties dažādos avotos, un reaģēšana uz tiem, kā arī atgriezeniskās saites ar lietotājiem izmantošana pētījumā ir definētas kā kvalitatīvās pētniecības metodes. Savukārt ļaunprātīgas aktivitātes moduļu un to identificēšanas algoritmu apmācība pētījumā ir definēta kā kvantitatīvā pētniecības metode. Par primārajiem datu avotiem uzskatāmi dati, kas tika ievākti no iestādes iekšējā tīkla informācijas, lietotāju darbstacijām, komunikatoru datiem, ugunsmūra datiem, ielaušanās noteikšanas sistēmas datiem, *NetFlow* datiem, veiksmīgas/neveiksmīgas autentifickācijas, kā arī citiem auditācijas pierakstu failiem un citiem datu avotiem. Sekundārie dati [29], [30] tika izmantoti, lai apmācītu mašīnmācīšanās moduļus, klasificējot tos kā leģitīmus vai ļaunprātīgus domēnus. Papildu ļaunprātīgie domēnu vārdi (sekundārie dati) tika iegūti no iestādes izmantojamā ugunsmūra ar ielaušanās novēršanas funkcionalitāti, kā arī veikta izpēte domēna vārdu pieprasījumu datos un aizdomīgu domēna vārdu pieprasījumu manuāla klasifikācija un salīdzināšana ar ļaunprātīgo domēnu datubāzēm.



1. att. Pētījuma metodika.

Atgriezneniskās saites nodibināšanai ar informācijas sistēmu lietotājiem tika izmantotas *Microsoft Office Forms* izstrādātas formas, kurās potenciāli inficētās ierīces lietotājam tika uzdoti jautājumi par to, vai lietotājs ir noskenējis ierīci ar rekomendētajiem antivīrusiem un vai ierīcē tika atklāts ļaunprātīgais kods. Papildus tika ņemti vērā arī *CERT.LV* paziņojumi par

ļaunprātīgām aktivitātēm no iestādes. Šādā veidā (aizpildītas formas un *CERT.LV* ziņojumi) tika panākta lielāka apmācīto mašīnmācīšanās modeļu precizitāte, pārapmācot tos.

Adaptīvas IS drošības pārvaldības pamatā esošais informācijas drošības pārvaldības spējas konceptuālais modelis tika izstrādāts, izmantojot *CDD* [31] pieeju, jo tā ir piemērota adaptīvu risinājumu specificēšanai un implementēšanai. Darbā izstrādātā vispārīgā drošības pārvaldības spēju modeļa, kā arī specifiskā RTU pielāgotā spēju modeļa pamatā ir drošības riskus identificējošie moduļi, kā arī dažādi citi elementi drošības pārvaldības īstenošanai.

Darbā tika pētīti mašīnmācīšanās metodēs balstīti modeļi, kas identificē ļaunprātīgus domēnus (*DGA*). Tika veikti eksperimenti ar *DGA* domēnu atlases kritērijiem, kā arī pazīmju kopu veidošanu. *DGA* identificēšanai tika izvēlēti dažādi klasifikatori – atbalsta vektoru mašīna (*Support Vector Machine*; *SVC*), neironu tīkli (*NNC*), lēmumu koki (*DTC*) un lēmumu meži (*RFC*). Lai novērtētu klasifikatoru veikumu, katram no tiem tika mērīta ticamība (*Accuracy*), pārklājums (*Recall)*, F1 mērs (*F1 Score*), lietojot šķērsvalidāciju (*Cross validati*on). Eksperimetu rezultātā tika salīdzināti apmācīto klasifikatoru sniegtie rezultāti ar RTU izmantotā ugunsmūra ar *IPS* funkcionalitāti datiem. Turklāt tika veikti arī eksperimenti ar mašīnmācīšanās metodēs balstītu *NFAI* moduli, kura mērķis ir ļaunprātīgas darbības identificēšana tīkla datos.

DGA identificēšanas moduļa rezultāti tika salīdzināti ar RTU izmantotā ugunsmūra datiem. Rezultāti liecina, ka, lietojot mašīmācīšanās modeļus, *ISMS* efektivitāte uzlabojas, jo tie ļauj identificēt apdraudējumus dažādos līmeņos, agregējot datus. *ISMS* moduļi var iekļaut arī organizācijas mākoņpakalpojumos esošos datus, kas ugunsmūrim nav pieejami, tādējādi vēl papildus uzlabojot kiberdrošības apdraudējumu identicēšanu.

Pētījuma rezultātā tika definēts no konteksta atkarīgs, adaptīvs drošības pārvaldības modelis un izstrādāta tam atbilstoša, lielajos datos bāzēta, mērogojama drošības pārvaldības sistēmas platforma (*ISMS*), kurā iespējams integrēt neatkarīgus draudu noteikšanas un novēršanas moduļus atbilstoši organizācijas vajadzībām. *ISMS* platforma patlaban tiek aktīvi lietota RTU, Centrālajā finanšu un līgumu aģentūrā un Iepirkumu uzraudzības birojā lai novērstu kiberdrošības apdraudējumus.

Darba zinātniskie jaunieguvumi

1. Izstrādāts no konteksta atkarīgs, adaptīvs IS drošības pārvaldības modelis un tā tehniskā realizācija.
2. Sagatavotas apmācību datu kopas ļaunprātīga *DNS* identificēšanai, kā arī ļaunprātīga koda darbības identificēšanai tīkla datos.

3. Izstrādāta unikāla pazīmju kopa ļaunprātīga *DNS* pieprasījuma identificēšanai un ļaunprātīga koda darbības identificēšanai tīkla datos.
4. Izstrādāts multidimensionālu draudu agregācijas algoritms, kas tika intergēts *ISMS* platformā, nodrošinot reakciju, balstoties identificētā drauda kritiskumā.
5. Radīta pieeja automatizēti iesaistīt galalietotāju kiberincidentu risināšanā, tai skaitā nodrošinot galalietotājam atgriezenisko saiti.

Darba praktiskā nozīme

Izstrādāts IS drošības pārvaldības modelis un tā tehniskā realizācija, sniedzot atbalstu izpildīt *NIST* definēto [20] draudu noteikšanas un aktīvas rīcības fāzes ieviešanu. Platformas implementācija ir veikta, galvenokārt izmantojot atvērtā koda risinājumus.

Veikta izstrādātās platformas aprobācija RTU, Centrālajā finanšu un līgumu aģentūrā un Iepirkumu uzraudzības birojā. Lietota lielo datu paradigmā balstīta daudzdimensionāla datu analīze un agregācija, nodrošinot platformas mērogojamamību. Platforma ir paplašināma ar apakšmoduļiem atbilstoši organizācijas vajadzībām. Mašīnmācīšanās metodēs balstīts robottīkla domēna identifikācijas modulis (*DGA*) ir aprobēts gan RTU, gan arī citās iestādēs, pierādot savu efektivitāti.

Novērtēta platformas efektivitāte informācijas sistēmu drošības nodrošināšanā.

Promocijas darbā aizstāvamās tēzes

1. tēze. Lai nodrošinātu efektīvu daudzdimesionālu datu analīzi drošības apdraudējumu identificēšanai, nepieciešams lietot lielo datu tehnoloģijas un mašīnmācīšanās metodes.

2. tēze. Informācijas sistēmu drošības pārvaldības efektivitāte ir atkarīga no spējas identificēt draudus un reakcijas laika pēc drauda identificēšanas.

3. tēze. Lai nodrošinātu adekvātu drošības pārvaldību, nepieciešams izmantot automatizētas sistēmas, kas reaģē uz drošības draudiem.

Promocijas darbā aizstāvamā **hipotēze**. Apvienojot vairākus datu avotus, specializētus draudu identificēšanas modeļus un platformas, tiek iegūta pilnvērtīgāka drošības incidentu identificēšana, salīdzinot ar individuālu šim mērķim paredzētu risinājumu izmantošanu.

Promocijas darba rezultātu aprobācija

Pētījumu rezultāti tika prezentēti 12 konferencēs.

1. Rīgas Tehniskās universitātes 45. zinātniskā konference, Rīga (Latvija), 2004. gada 14.–16. oktobrī. Referāts "Efektīva risku menedžmenta meklējumi".
2. 19. Eiropas konference modelēšanā un simulācijā, Rīga (Latvija), 2005. gada 1.–4. jūnijā. Referāts "Riska menedžmenta modelēšana unificētām draudu apstrādes sistēmām".
3. Rīgas Tehniskās universitātes 46. zinātniskā konference, Rīga (Latvija), 2005. gada 13.–15. oktobrī. Referātu "Riska menedžmenta modelēšana, izmantojot neironu tīklus".
4. Rīgas Tehniskās universitātes 47. zinātniskā konference, Rīga (Latvija), 2006. gada 12.–14. oktobrī. Referāts "Reāla laika riska menedžmenta izmantošana organizācijā".
5. 6. *Eurosim* kongress "*Eurosim 2007*", Ļubļana (Slovēnija), 2007. gada 9.–13. septembrī. Referāts "Reāla laika riska menedžmenta sistēmas modelēšana".
6. Rīgas Tehniskās universitātes 48. zinātniskā konference, Rīga (Latvija), 2007. gada 11.–13. oktobrī. Referāts "Reāla laika riska menedžmenta izmantošana organizācijā".
7. Rīgas Tehniskās universitātes 48. zinātniskā konference, Rīga (Latvija), 2008. gada 13.–15. oktobrī. Referāts "Reāla laika riska menedžmenta modelis".
8. *Modelling IT Security Risk Management in Academic Environment. IEEE Workshop on advances in information, electronic and electrical engineering* (*AIEEE'2017*), Rīga, 2017. gada 24. novembrī, Rīgā.
9. *IS Security Governance Capability Design for Higher Education Organization. 59th International Scientific Conference on Information Technology and Management Science of Riga-Technical-University* (*ITMS*), Rīga, 2018. gada 12.–14. novembrī.
10. *ICEIS 2020 – 22nd International Conference on Enterprise Information Systems*. Referāts "*Methods, models and techniques to improve information system's security in large organizations*", Prāga, Čehija (attālināti), 2020. gada 5.–7. maijā.
11. *Artificial intelligence and big data driven IS security management solution with applications in higher education organizations. 17th International Conference on Network and Service Management*, Izmira, Turcija, 2021. gada 25.–29. oktobrī.
12. *Managing Information System Security in Higher Education Organizations, IEEE Workshop on Advances in Information, Electronic and Electrical Engineering* (*AIEEE*), Viļņa, Lietuva, 2023. gada 27.–29. aprīlī.
13. Praktiskā pieredze *SOC* izveidē, izmantojot atvērtā koda risinājumus, *CERT.LV*, 2023. gada 12. decembrī, tiešsaistē: https://cert.lv/lv/2023/11/it-drosibas-seminars-esi-dross-decembri.

Promocijas darbā veikto pētījumu rezultāti atspoguļoti 13 publikācijās.

1. Minkevics V., Slihte J., Vulfs G. “Search for effective risk management”. RTU zinātnisko rakstu krājums “Datorzinātne. Datorvadības tehnoloģijas”, 5. sēr., 20. sēj., Rīga, RTU, 2004, 174.–180. lpp. (ISSN 1407-7493).
2. Minkevics V., Slihte J., Vulfs G. “Modelling risk management for unified threat management systems” 19th European Conference on Modelling and Simulation Riga 2005, 144.–150. lpp. (ISBN 1-84233-112-4).
3. Minkevics V., Slihte J., Vulfs G. “Modelling risk management system using neural networks”. RTU zinātnisko rakstu krājums “Datorzinātne. Datorvadības tehnoloģijas”, 5. sēr., 23. sēj., Rīga, RTU, 2005, 66.–72. lpp. (ISSN 1407-7493).
4. Minkevics V., Slihte J., Vulfs G. “Use of real – time risk management in organisation”. RTU zinātnisko rakstu krājums “Datorzinātne. Datorvadības tehnoloģijas”, 5. sēr., 28. sēj., Rīga, RTU, 2006, 23.–29. lpp. (ISSN 1407-7493).
5. Minkevics V., Slihte J., Vulfs G. “Modelling real – time risk management system”. Proceedings of the 6th EUROSIM Congress on Modelling and Simulation, vol. 1. (ISBN-13:978-3-901608-32-2), 414. lpp.
6. Minkevics V., Slihte J., Vulfs G. “Modelling real – time risk management system using associative approach”. RTU zinātnisko rakstu krājums “Datorzinātne. Datorvadības tehnoloģijas”, 5. sēr., 31. sēj., Rīga, RTU, 2007, 34.–40. lpp. (ISSN 1407-7493).
7. Minkevics V., Vulfs G. “Real-time risk management model”. RTU zinātnisko rakstu krājums “Datorzinātne. Datorvadības tehnoloģijas”, 36. sēj., Rīga, RTU, 2008, 49.–55. lpp. (ISSN 1407-7493).
8. Minkevičs, V., Šlihte, J. Modelling IT Security Risk Management in Academic Environment. No: 2017 5th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE 2017): Proceedings, Latvija, Riga, 24.–25. novembris, 2017. Piscataway: IEEE, 2017, 5.–8. lpp. ISBN 978-1-5386-4138-5. e-ISBN 978-1-5386-4137-8. Pieejams: doi:10.1109/AIEEE.2017.8270562.
9. Minkevičs V., Kampars J. IS Security Governance Capability Design for Higher Education Organization. No: 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS 2018): Proceedings, Latvija, Rīga, 29.–29. novembris, 2018. Piscataway: IEEE, 2018, 66.–70. lpp. ISBN 978-1-7281-0099-9. e-ISBN 978-1-7281-0098-2. Pieejams: doi:10.1109/ITMS.2018.8552975.

10. Minkevičs V., Kampars J. Methods, models and techniques to improve information system's security in large organizations: included in registration In Proceedings of the 22nd International Conference on Enterprise Information Systems – vol. 1, 2020: ICEIS, 632–639, 2020, ISBN: 978-989-758-423-7.
11. Minkevičs V., Kampars J. Artificial intelligence and big data driven IS security management solution with applications in higher education organizations, 17th International Conference on Network and Service Management, 2021, Izmir, Turkey, doi:10.23919/CNSM52442.2021.9615575,
12. Minkevičs V., Kampars J., Grabis J. Managing Information System Security in Higher Education Organizations, IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). 2023. gada 27.–29. aprīlis, Viļņa, Lietuva, doi:10.1109/AIEEE58915.2023.10134911.
13. Minkevičs V., Grabis J. A capability-driven automated cybersecurity monitoring and response system, Frontiers in Computer Science Journal, vol. 7, 2025, doi:10.3389/fcomp.2025.1692263.

Dalība ar promocijas darba tēmu saistītajos RTU projektos:

1) Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem (VPP-ARTSS: ARTSS, īstenots no 2020. gada 1. jūlija līdz 2020. gada 31. decembrim https://artss.rtu.lv/);
2) Lielo datu vadīta informācijas un komunikācijas tehnoloģiju drošības pārvaldības risinājuma izstrāde. Projekta realizācijas laiks no 2021. gada 1. janvāra līdz 2023. gada 30. jūnijam (BICTSEMS, http://iti.rtu.lv/vitk/lv/petnieciba/projekti/lielo-datu-vadita-informacijas-un-komunikacijas-tehnologiju-drosibas).

Darba apjoms un struktūra

Promocijas darbā ir piecas nodaļas, rezultāti un secinājumi, literatūras avotu saraksts un divi pielikumi.

Pirmajā nodaļā iekļauti promocijas darbā izmantotie pamatjēdzieni, literatūras apskats, pamatojoties uz *Kofod-Petersen* dizaina zinātnes metodoloģiju [32], esošās situācijas apraksts, kā arī iespējamie problēmas risinājumi.

Otrajā nodaļā aprakstīts izstrādātais problēmas risinājums, definējot pamatprasības izstrādājamajai platformai, tai skaitā sniegta tehniskā risinājuma augsta līmeņa arhitektūra. Šajā nodaļā izstrādājamā platforma ir prezentēta, izmantojot spējās izstrādes metodoloģiju [31].

Trešajā nodaļā prezentēta informācijas sistēmu drošības pārvaldības platformas ieviešana RTU, aprakstītas platformas sastāvdaļas, kā arī sniegts ieskats platformas darbības specifikā, tai skaitā piedāvāta arhitektūras detalizācija RTU lietošanas gadījumiem.

Ceturtajā nodaļā novērtēti dažādi platformā iekļautie moduļi, tādi kā *DGA* modulis, kas nosaka, vai izsauktās mājaslapas nosaukums (domēns) ir tipisks vai mākslīgi ģenerēts. Mākslīgi ģenerētie domēni tiek izmantoti robotu tīklu dalībnieku savstarpējai saziņai. Turklāt ir novērtēts arī draudu agregācijas modulis, kura pamatā ir dažādu moduļu rezultātu apvienošana ar mērķi identificēt inficētu ierīci un samazināt viltus pozitīvo ziņojumu skaitu. Darbā novērtēts *NFAI NetFlow* tīkla datu analīzes modulis, kas izmanto apmācītu mašīnmācīšanās algoritmu un, balstoties apmācības datos, nosaka, vai konkrētā komunikācija var tikt uzskatīta par ļaunprātīgu, vai nē.

Piektajā nodaļā vairākos posmos, izmantojot dažādas pieejas, ir novērtēta *ISMS* platforma, piemēram, salīdzinot platformu ar tirgū pieejamiem risinājumiem, veicot lietotāju reaģēšanas ātruma mērījumus, kā arī novērtējot atsevišķus platformas moduļus.

Rezultātu un secinājumu nodaļā sniegts darba rezultātu, iegūto secinājumu un turpmāko pētījumu izklāsts.

PROMOCIJAS DARBA NODAĻU IZKLĀSTS

1. LITERATŪRAS APSKATS UN IESPĒJAMIE PROBLĒMAS RISINĀJUMI

Promocijas darba pirmajā nodaļā aprakstīts veiktais literatūras apskats saskaņā ar [32] definētajiem strukturēta literatūras apskata veikšanas principiem. Tas ir iedalīts trīs posmos – literatūras apskata plānošanā, veikšanā un analīzē. Literatūras apskatā ietvertie izpētes jautājumi apkopoti **Error! Reference source not found.**. tabulā.

2. tabula

Literatūrā apskatīto jautājumu pārskats

Izpētes jautājums	Jautājuma mērķis	Sagaidāmais rezultāts
Kādi ir tipiskie informācijas sistēmu drošības pārvaldībā īstenojamie procesi?	Identificēt procesus, kas veido IS drošības pārvaldību	IS drošības pārvaldības procesu raksturojums
Kādi datu avoti mūsdienās tiek lietoti informācijas sistēmu (IS) drošības nodrošināšanai?	Identificēt datu avotus, kas tiek lietoti drošības analīzei, kā arī identificēt metodes, kas tiek lietotas šo datu apstrādei	Datu avotu, kas ir piemēroti sistēmas drošības analīzei, saraksts, kā arī datu avotu apstrādes metožu pārskats
Kādas automatizētas metodes un rīki tiek lietoti IS drošības pārvaldības nodrošināšanai?	Identificēt, kādas automatizēšanas metodes un rīki mūsdienās tiek lietoti IS drošības pārvaldības nodrošināšanai	Automatizācijas metožu un to lietojumu pārskats
Kādas mašīnmācīšanās metodes tiek lietotas IS drošības pārvaldības nodrošināšanai?	Identificēt, kādas mašīnmācīšanās metodes un rīki tiek lietoti, lai identificētu vēl nezināmus draudus	Dažādu mašīnmācīšanās metožu un rīku, kas tiek lietoti nezināmu draudu identificēšanai, pārskats
Kādi ir iespējamie risinājumi, lai nodrošinātu automatizētu ļaunprātīgas aktivitātes apturēšanu tīklā?	Identificēt iespējamos risinājumus, lai nodrošinātu automatizētu ļaunprātīgas aktivitātes apturēšanu tīklā	Risinājumu, kurus izmantojot, ir iespējams īsā laikā apturēt ļaunprātīgu aktivitāti tīklā, apraksts

Veicot literatūras analīzi, var secināt, ka pilnvērtīgas drošības analīzes nodrošināšanai ir nepieciešami:

1) *NetFlow* dati, ko iespējams iegūt, izmantojot dažādus atvērtā koda rīkus. Šie dati ļauj identificēt tīkla komunikācju, kas atšķiras no "normālas" uzvedības tīklā, šādi identificējot, piemēram, ļaunprātīgā koda darbību;

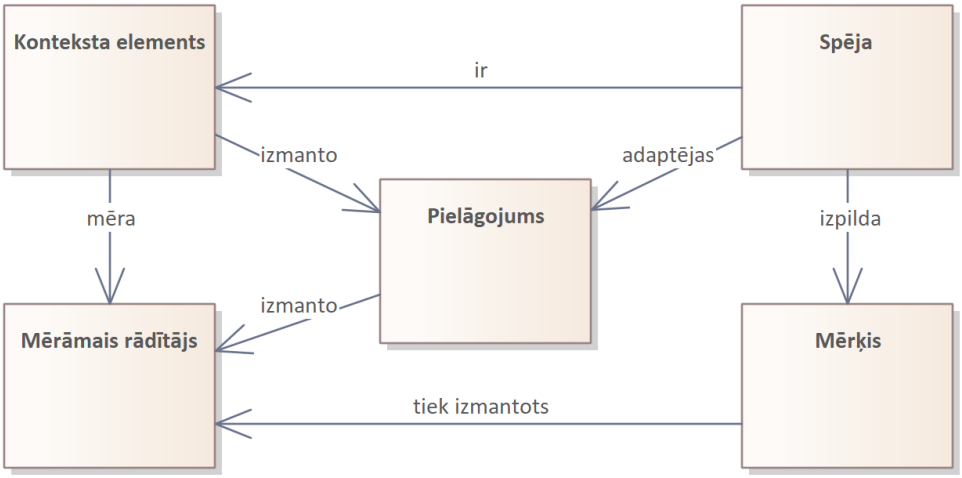
2) sistēmu auditācijas pieraksti, ko izmantojot, ir iespējams identificēt netipisku ierīces uzvedību, identificējot ļaunprātīgu darbību;
3) "meduspoda" funkcionalitāte, kas, pievilinot uzbrucējus, ļauj saprast uzbrukuma metodes un iespējamos rīkus, kā arī sniedz papildu laiku reālo informācijas sistēmu aizsardzībai gadījumos, kad uzbrucējs jau ir iekļuvis iekšējā datortīklā;
4) ugunsmūra dati (auditācijas pieraksti), kuros tiek uzkrāta informācija par ieejošajām un izejošajām datu plūsmām. Šī informācija var tikt izmantota, lai identificētu, vai ugunsmūra likumi strādā pareizi un vai nav identificēta ļaunprātīga aktivitāte tīklā;
5) *DNS* dati, kas satur informāciju par avota un galamērķa IP adresi un portu, kā arī informāciju par pieprasīto *DNS* vārdu. Domēna vārdu sintaksi var analizēt, lai identificētu algoritmiski ģenerētus domēna vārdu pieprasījumus, kas savukārt var liecināt par ierīces atrašanos robotu tīklā.

Literatūras apskats ļauj secināt, ka IS drošības pārvaldības nodrošināšanai jāietver daudzdimensionālu datu analīzi no plaša avotu klāsta. Eksistē arī liels skaits potenciāli izmantojamo draudu noteikšanas metožu, ko būtu nepieciešams implementēt kā neatkarīgus draudu identifikācijas servisus. Visu pieejamo datu avotu un draudu noteikšanas moduļu efektīva izmantošana vienotā drošības pārvaldības risinājumā, kas būtu pielāgojams organizācijas kontekstam, ir problēma, kas zinātniskajā literatūrā nav pietiekami pētīta un kam autors pievērš īpašu uzmanību, izstrādājot no konteksta atkarīgu, adaptīvu drošības pārvaldības modeli, kas balstās spējā metodoloģijā un tās tehniskajā realizācijā – *ISMS* platformā.

2. SPĒJORIENTĒTĀ DROŠĪBAS PĀRVALDĪBA

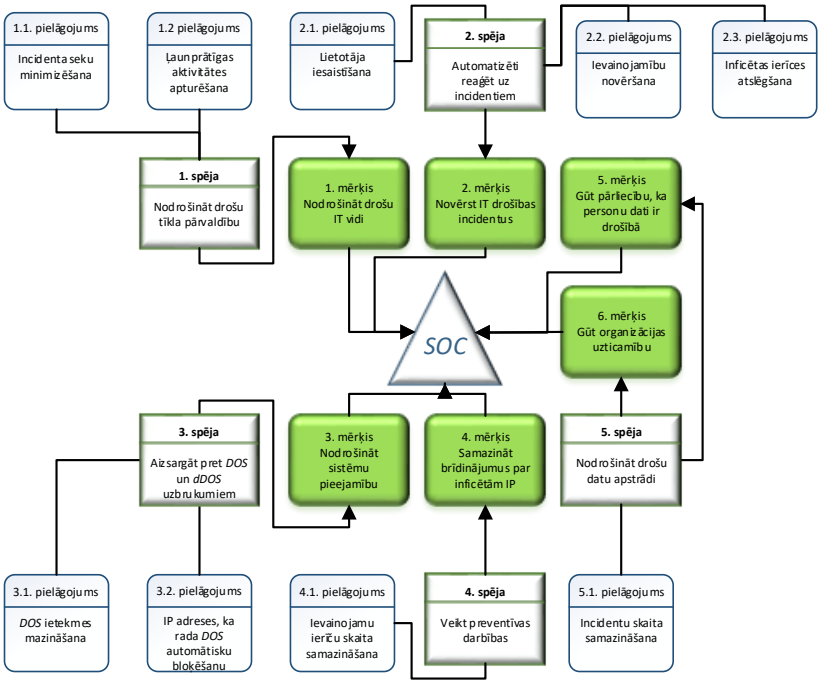
Promocijas darba otrajā nodaļā apskatīta spējorientētā drošības pārvaldība, tās galvenie koncepti ir spējas, konteksta elementi un mērāmie rādītāji. Darbā izstrādātais spējorientētais drošības pārvaldības modelis ir balstīts spējā izstrādē (*CDD*) [31]. Tas spēj ņemt vērā pilnu konteksta informāciju, kā arī veikt automātiskas adaptīvas darbības drošības līmeņa atjaunošanai draudu gadījumā.

Darbā ir definēts drošības pārvalības modeļa spējas metamodelis (**Error! Reference source not found.**. att.). Drošības pārvaldības modelis tiek raksturots ar mērķi, kura izpildei tiek noteikti mērāmie rādītāji, ar konteksta elementiem, kas tiek mērīti, izmantojot mērāmos rādītājus, un ar spēju, kas pielāgojas un izmanto gan konteksta elementus, gan mērāmos rādītājus.



2. att. Drošības pārvalības modeļa spējas metamodelis.

Izmantojot iepriekš minēto pieeju, ir iespējams aprakstīt drošības pārvaldības sistēmas konteksta elementus, mērāmos rādītājus un spējas, tādā veidā skaidri definējot tās darbības principus.



3. att. Vispārīgais informācijas drošības pārvaldības modelis.

Informācijas drošības pārvaldības spēja (**Error! Reference source not found.**. att.) tiek īstenota, lai sasniegtu dažādus definētos mērķus drošības pārvaldības uzlabošanai. Šī spēja izpilda galveno mērķi (1. mērķis) – nodrošināt drošu IT vidi, ko atbalsta pieci papildu mērķi: 2. mērķis – novērst IT drošības incidentus; 3. mērķis – nodrošināt sistēmu pieejamību; 4. mērķis – samazināt brīdinājumus par inficētām IP adresēm; 5. mērkis – gūt pārliecību, ka personu dati ir drošībā; 6. mērķis – gūt organizācijas uzticamību. Katram mērķim ir atbilstoša spēja un pielāgojums.

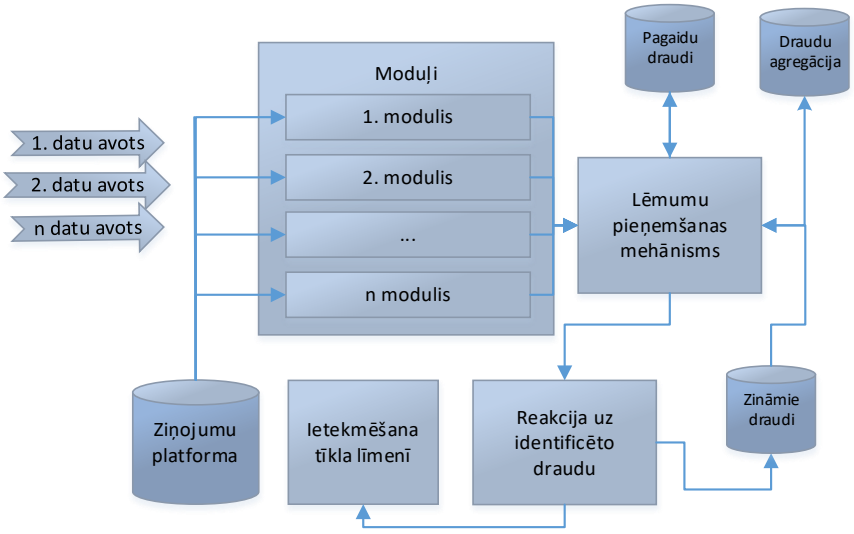
Papildus otrajā nodaļā ir apkopotas prasības tehniskajam risinājumam (*ISMS* platformai), kas nodrošina IS drošības pārvaldību atbilstoši iepriekš definētajam spēju modelim (**Error! Reference source not found.**. tab.), iekļaujot trīs pamatkomonentes: 1) datu avoti; 2) datu analīze; 3) darbība jeb reaģēšana. Prasības ir definētas atbilstoši literatūrā apskatītajam un ir attiecināmas uz jebkuru organizāciju, kas izvēlas ieviest spējorientētu IS drošības pārvaldību. Darbā katrai prasībai ir norādīts ieviešanas sagaidāmais rezultāts.

3. tabula

Prasību definēšana *ISMS* platformai

Nr. p. k.	Prasība
1.	Izmantot atvērtā koda tehnoloģijas un augsta līmeņa programmēšanas valodu
2.	Identificēt ierīci, kā arī tās pieslēguma vietu, arī gadījumos, kad tiek izmantotas dinamiskās IP adreses
3.	Identificēt lietotāju un iesaistīt viņu drošības pārvaldības procesā
4.	Izmantot mērogojamu risinājumu, lai gadījumā, kad nepieciešams apstrādāt lielāku datu apjomu, to varētu izdarīt bez platformas pārbūves
5.	Izmantot atvērtā kodā bāzētu ielaušanās noteikšanas sistēmu ar signatūru papildināšanas iespēju
6.	Izmantot auditācijas pierakstu analīzi ļaunprātīgas darbības identificēšanai
7.	Izmantot atvērtā kodā bāzētu tīkla datu analīzes mehānismu
8.	Izmantot atvērtā kodā bāzētu tīkla metadatu analīzes mehānismu
9.	Izmantot "meduspoda" funkcionalitāti, lai gūtu iespēju padziļināti pētīt ļauprātīgā koda vai cilvēka darbību
10.	Identificēt lietotāja autentifikācijas datu zādzību
11.	Identificēt ļaunprātīgu darbību tīklā, izmantojot tīkla metadatus un atvērtā kodā bāzētas sistēmas, kā arī izmantot mašīnmācīšanos
12.	Identificēt portu skanēšanu un paroļu minēšanu iekšējā tīklā
13.	Identificēt un uz noteiktu laiku bloķēt ārējas IP adreses, kas nav iesaistītas nevienā komunikācijā, bet tikai veic portu skanēšanu
14.	Izmantot adaptīvu pieeju dažādu draudu gadījumā. Piemēram, specifiska draudu gadījumā reaģēt ātrāk nekā cita drauda gadījumā
15.	Izmantot automatizētu ievainojamību identificēšanu un automātisku ziņošanu atbildīgajai personai
16.	Identificēt agoritmiski ģenerētus domēnus *DNS* informācijā, izmantojot statiskos sarakstus un mašīnmācīšanos
17.	Atslēgt ierīces, kas rada apdraudējumu iekšējā tīklā
18.	Parādīt atklātos incidentus un nosūtītos paziņojumus par drošību atbildīgajai personai, izmantojot grafisko saskarni

Galvenās drošības pārvaldības platformas komponentes redzamas **Error! Reference source not found.**. attēlā. Platformas komponentes ir implementētas, izmantojot atvērtā pirmkoda industrijā plaši abrobētas tehnoloģijas, t. sk. *Python3*, *Influx DB*, *Apache Kafka*, *Grafana*.



4. att. Galvenās drošības pārvaldības platformas komponentes.

Izmantojamo tehnoloģiju ietvars tiek paplašināts atbilstoši iegūtajai informācijas organizācijas IS drošības pārvaldības spējai modelēšanas laikā. Darbā *Apache Kafka* un *Influx DB* ļauj nodrošināt lielapjoma statisku un reāllaika datu integrāciju, savukārt *Apache Spark* nodrošina lielo datu apstrādi, identificējot ļaunprātīgu darbību tīkla datos.

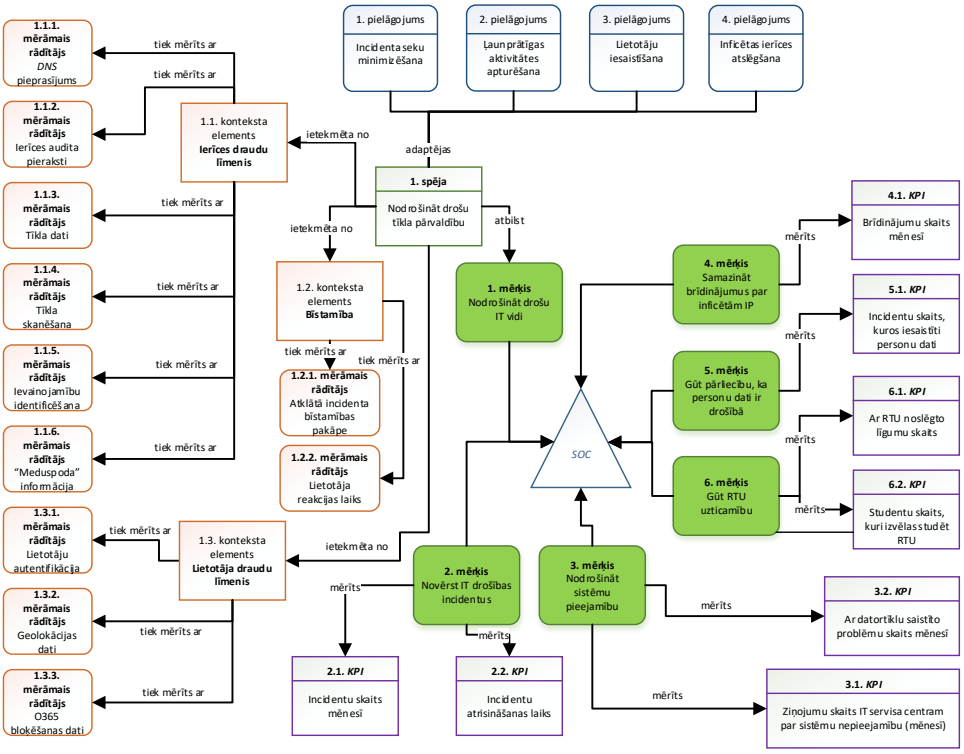
Galvenie ieguvumi piedāvātajā *ISMS* platformā ir:

- galiekārtu kontroles nodrošināšana;
- dinamiska tīkla datu analīze;
- procesu automatizācija;
- adaptīva reaģēšana;
- moduļu pievienoša gadījumos, kad mainās uzbrukumu vektori;
- atgriezeniskās saites nodrošināšana, automatizēta reaģēšana un ātra izmaiņu ieviešana sistēmā.

3. SPĒJORIENTĒTA DROŠĪBAS PĀRVALDĪBAS MODEĻA IEVIEŠANA RTU

Trešajā nodaļā aprakstīts izveidotā modeļa ieviešanas plāns Rīgas Tehniskajā universitātē, pielāgojot vispārīgo modeli (**Error! Reference source not found.**. att.), kā arī nosakot specifiskus organziācijas mērķus un to mērāmos rādītājus. Lai ieviestu iepriekšējā nodaļā minētās prasības, organizācijai nepieciešams nodrošināt:

1) iespēju saņemt datus no dažādiem datu avotiem, kā arī saprast tīkla protokolus;
2) *Python* vai citas augsta līmeņa skriptošanas valodas pārzināšanu, lai spētu adaptēt automatizācijas procesus;
3) mācēt izmantot atvērtā koda programmatūru, tai skaitā lielajos datos bāzētu programmatūru;
4) izmantot statiskas IP adreses iekšējā tīklā vai, izmantojot *DHCP*, spēt identificēt dinamiski piešķirtās IP adreses;
5) mācēt identificēt galalietotāju pēc IP adreses, lai spētu viņu iesaistīt drošības incidenta seku mazināšanā;
6) mācēt izmantot atvērtā koda vai maksas risinājumus, lai identificētu ievainojamības;
7) mācēt lietot atvērtā koda ielaušanās noteikšanas sistēmas;
8) mācēt uzkrāt un lietot *Netflow* datus;
9) mācēt izmantot atvērtā koda vai maksas "meduspoda" risinājumus;
10) mācēt strādāt ar *M365* datiem, tai skaitā *GraphAPI*;
11) saprast *API* darbību un mācēt to lietot – gan veicot ierīces atslēgšanu no tīkla, gan saņemot un nosūtot datus no/uz dažādām informācijas sistēmām;
12) mācēt izmantot ugunsmūra datus;
13) spēt novērtēt, kuros drošības incidenta gadījumos reaģēt ir nepieciešams ātrāk un kuri gadījumi var gaidīt;
14) saprast, kā notiek *DNS* izsaukums un mācēt tos analizēt;
15) mācēt koriģēt drošības pārvaldības sistēmas grafisko saskarni.



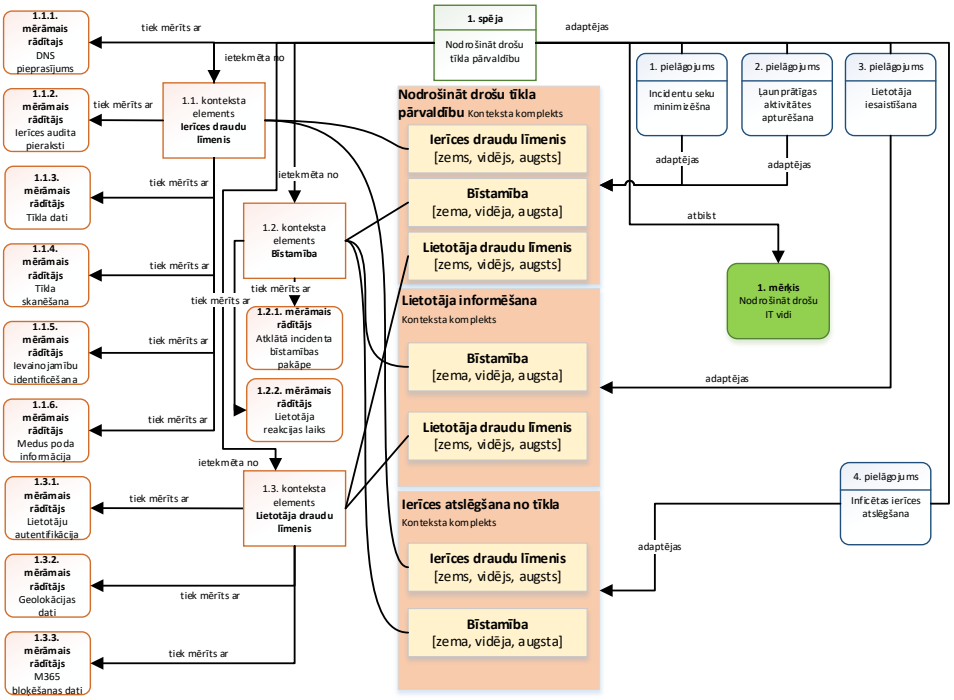
5. att. Pielāgotais *CDD* mērķa modelis.

Šajā modelī (**Error! Reference source not found.**. att.) drošības pārvaldības spēja tiek īstenota, lai nodrošinātu drošu augstākās izglītības iestādes darbību. Šī spēja izpilda galveno mērķi (1. mērķis) – nodrošināt drošu IT vidi, kas tiek atbalstīts ar pieciem papildu mērķiem: 2. mērķis – novērst drošības incidentus; 3. mērķis – nodrošināt sistēmu pieejamību; 4. mērķis – samazināt brīdinājumus par inficētām IP; 5. mērķis – gūt pārliecību, ka personu dati ir drošībā; 6. mērķis – iegūt RTU uzticamību. Katru apakšmērķi mēra ar atšķirīgu mērāmo rādītāju (*KPI*), lai novērtētu šī mērķa izpildi. 2. mērķis tiek mērīts ar 2.1. *KPI* – incidentu skaits mēnesī un 2.2. *KPI* – incidentu atrisināšanas laiks. 3. mērķis tiek mērīts ar 3.1. *KPI* – ziņojumu skaits IT servisa centram par sistēmu nepieejamību (mēnesī) un ar 3.2. *KPI* – ar datortīklu saistīto problēmu skaits mēnesī. 4. mērķis tiek mērīts ar 4.1. *KPI* – brīdinājumu skaits mēnesī. 5. mērķis tiek mērīts ar 5.1. *KPI* – incidentu skaits, kuros iesaistīti personu dati. Savukārt 6.

mērķis tiek mērīts ar 6.1. *KPI* un 6.2. *KPI* – noslēgto līgumu skaits ar RTU un studentu skaits, kuri izvēlas studēt augstskolā.

Spēju ietekmē attiecīgie konteksta elementi: 1.1. konteksta elements – ierīces draudu līmenis, lai identificētu, vai ar tīklu savienota ierīce ir iespējami inficēta un apdraud pārējās tīklā esošās ierīces; 1.2. konteksta elements – bīstamība, lai identificētu reaģēšanas laiku uz incidentu; 1.3. konteksta elements – lietotāja draudu līmenis, lai saprastu, vai lietotājs, piemēram, ir nozaudējis savus autentifikācijas datus. Visi konteksta elementi tiek novērtēti, izmantojot vairākus mērāmos rādītājus. Ierīces draudu līmeni mēra pēc 1.1.1. mērāmā rādītāja – *DNS* pieprasījuma, kurā saprot, vai ierīce nav kompromitēta un nepieprasa robottīkla komandcentra domēnu komandu saņemšanai, 1.1.2. mērāmā rādītāja – ierīces audita pierakstiem jeb žurnālfailu datiem, ja tādi pieejami, 1.1.3. mērāmā rādītāja – tīkla plūsmas datiem, kuros tiek identificēta ierīces netipiska uzvedība, 1.1.4. mērāmā rādītāja – tīkla portu skenēšanas identificēšanas un 1.1.5. mērāmā rādītāja – ievainojamību identificēšanas, kur ierīce tiek pārbaudīta attiecībā uz zināmām ievainojamībām. Draudu līmenis jeb 1.2. konteksta elements – bīstamība palielinās, ja identificētais incidents ir definēts, kā augstas prioritātes (*Critical*) (1.2.1. mērāmais rādītājs), kā arī ja 1.2.2. mērāmais rādītājs – lietotāja reakcijas laiks uz incidentu ir novēlots. 1.3. mērāmā rādītāja – lietotāja draudu līmenis ir atkarīgs no žurnālfailos reģistrētās lietotāja autentifikācijas informācijas (1.3.1. mērāmais rādītājs – lietotāju autentifikācija), 1.3.2. mērāmā rādītāja – ģeolokācijas datiem, izmantojot kurus, tiek identificēta lietotāja atrašanās vieta autentifikācijas laikā, kā arī 1.3.3. mērāmā rādītāja – *M365* automatizētās bloķēšanas informācija, kad lietotājs tiek bloķēts, ja tiek identificēta mēstuļu sūtīšana. Lietotāja reakcijas līmenis tiek novērtēts pēc 1.2.2. mērāmā rādītāja – lietotāja reakcijas laika. 1. spēja tiek īstenota, izmantojot četrus primāros pakalpojumus – ļaunprātīgas darbības identifikācijas pakalpojumu, kas izmanto vairākas metodes, lai identificētu inficētās ierīces tīklā, incidentu izmeklēšanu, kas nodrošina precīzu incidenta noteikšanu, kā arī nosaka tā bīstamības pakāpi, lietotāju informēšanas pakalpojuma, kas izmanto dažādus līdzekļus, lai informētu lietotājus par darbībām, kas nepieciešamas incidenta novēršanai, kā arī inficētās ierīces atslēgšanas pakalpojuma, kas izmanto ugunsmūri un citas ierīces, lai atslēgtu inficēto ierīci no datortīkla. Spēju modeļa elementu apraksts ir dots promocijas darbā un autora publikācijā [33].

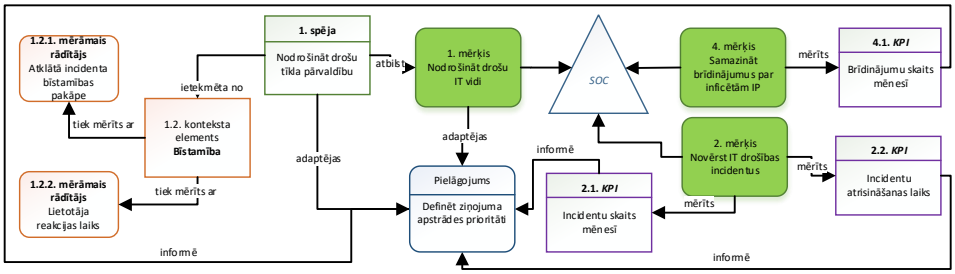
Konteksta un pielāgošanas modelis redzams **Error! Reference source not found.**. attēlā.



6. att. Konteksta un pielāgošanas modelis.

Pielāgošanas modeļa aprakstā, piemēram, pielāgojums "Pārliecināties, ka ziņojums nav viltus pozitīvs", nosaka spēju identificēt viltus pozitīvos ziņojumus. Spēja tiek nodrošināta, izmantojot eksperta izstrādātu datubāzi ar kritērijiem patiesi pozitīvo noteikšanai. Katram no šiem kritērijiem ir izstrādāta lietotājam nosūtāmā informācija ar nepieciešamo rīcību un pamācību drauda novēršanai.

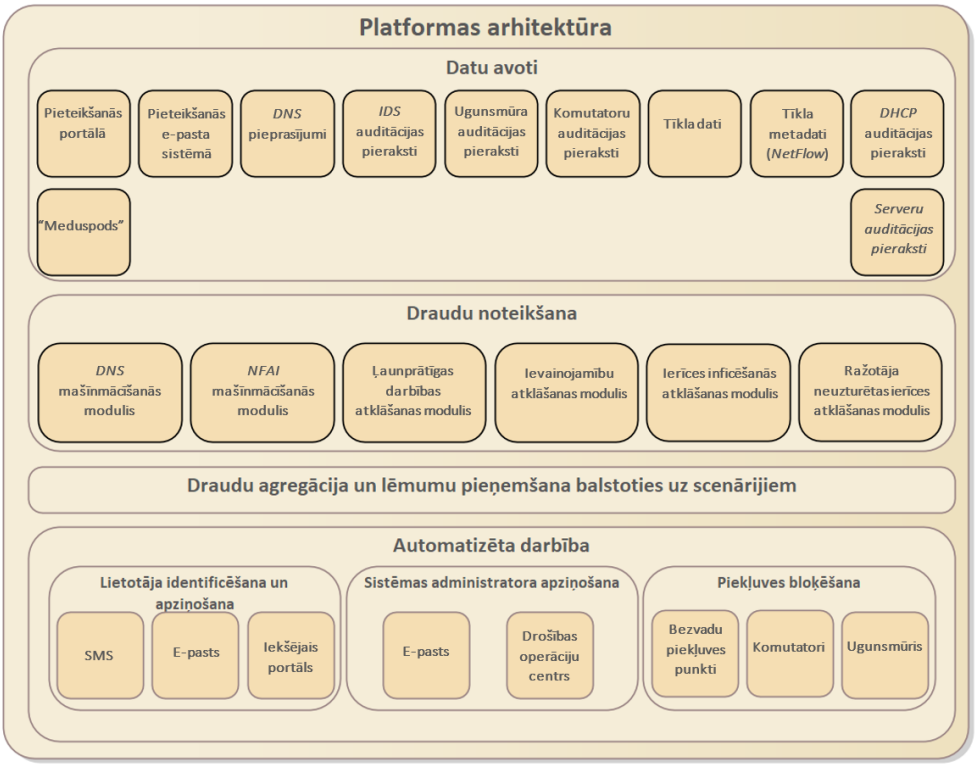
Reaģēšanas spējas adaptācija prioritāru ziņojumu gadījumā redzama **Error! Reference source not found.**. attēlā. Atkarībā no ziņojumu skaita par inficētām IP un incidentu skaita mēnesī tiek papildus pielāgota reaģēšana uz šiem incidentiem. Ja ziņojumu skaits pārsniedz noteiktu līmeni, ziņojumu pritoritāte tiek paaugstināta un notiek iepriekš izmantotā apziņošanas mehānisma maiņa no e-pasta uz *SMS* jeb prioritātes korekcija.



7. att. Prioritātes korekcija.

ISMS platforma ietver (**Error! Reference source not found.**. att.):

1) lietotāja identificēšanas un apziņošanas moduli, ar kura palīdzību tiek identificēts lietotājs, kura ierīcei ir piešķirta IP adrese. Šajā modulī tiek izmantots *Apache Kafka* [34] un *Python* skripti. Modulis ietver trīs apakšmoduļus:
    a) lietotāja apziņošana, izmantojot *SMS*;
    b) lietotāja apziņošana, izmantojot e-pastu;
    c) lietotāja apziņošana, izmantojot iekšējo portālu;
2) administratora apziņošana tiek nodrošināta, izmantojot e-pastu un operācijas centra grafisko saskarni, kuras pamatā ir *Influx* datubāze [35] un *Grafana* grafiskās saskarne [36];
3) piekļuves bloķēšanas modulis iekļauj bezvadu tīkla bloķēšanu, izmantojot *Aruba Clearpass* [37]. Piekļuve komutatoriem var tikt bloķēta automātiski, izmantojot mikroservisus, kas nododod informāciju ugunsmūrim par bloķējamajām IP adresēm.



8. att. *ISMS* platformas arhitektūra.

4. IS DROŠĪBAS PĀRVALDĪBAS PLATFORMAS NOVĒRTĒJUMS

Ceturtajā nodaļa aprakstīts ieviestā modeļa novērtējums dažādos laika periodos, sākot no 2021. gada janvāra, veicot dažādus mērījumus. No 2021. gada janvāra līdz 2024. gada janvārim *ISMS* platforma ir ģenerējusi vairāk nekā 88 tūkstošus ziņojumus. Lielākā daļa no tiem bija ieteikumi noskenēt iekārtu un veikt uzlabojumus drošībā, piemēram, atjaunināt novecojušu programmatūru.

Ir novērtēts *DGA* modulis, kura nolūks ir noskaidrot, vai *DNS* pieprasījums var tikt klasificēts kā *DGA*, tādējādi var tikt uzskatīts par ļaunprātīgu pieprasījumu. Pazīmju kopa *DNS* klasifikatoru apmācībai tika izveidota, par pamatu ņemot *Selvi et al.* [38] pētījumu, izmantojot 10 pazīmju kopu. *DGA* modulis, kas izmantoja *RFC* mašīnmācīšanās algoritmu, tika apmācīts ar 8856 "sliktajiem" un 8856 "labajiem" domēniem un salīdzināts ar "*Palo Alto"* ugunsmūri.

Error! Reference source not found.. tabulā dots *ML* modeļu salīdzinājums, kas parāda, ka labāko rezultātu deva *RFC*.

4. tabula

Klasifikatoru vērtības

Klasifikators	Precizitāte	Pārklājums	F1 mērs	Ticamība
RFC	0,934	0,948	0,941	0,940
DTC	0,916	0,928	0,922	0,921
NNC	0,869	0,854	0,862	0,852
SVM	0,858	0,860	0,859	0,859

RFC modelis tika pilnveidots, atlasot piemērotākās pazīmes (**Error! Reference source not found.**. tab.).

5. tabula

RFC modeļa pilnveidošana

–	Precizitāte	Pārklājums	F1 mērs	Ticamība
1. kopa	0,934	0,947	0,940	0,940
2. kopa	0,933	0,946	0,939	0,939
3. kopa	0,933	0,946	0,939	0,939

4. kopa	0,930	0,946	0,938	0,938
5. kopa	0,934	0,948	0,941	0,940

Error! Reference source not found.. tabulā redzams, ka labākos rezultātus uzrādīja 5. pazīmju kopa. Vairāk par pazīmju kopu atlasi – promocijas darbā.

Tika salīdzināta "*Palo Alto*" ugunsmūra *DGA* funkcionalitāte ar *DGA* moduli (6. tab.). Neraugoties uz to, ka *DGA* modulis var radīt augstāku viltus pozitīvo rezultātu īpatsvaru, tas identificēja septiņus papildu *DNS* pieprasījumus, kurus arī neatkarīga trešā puse klasificē kā DGA, salīdzinājumā ar "Palo Alto" ugunsmūri.

6. tabula

"*Palo Alto*" ugunsmūra *DGA* funkcionalitātes un izstrādātā *DGA* moduļa salīdzinājums

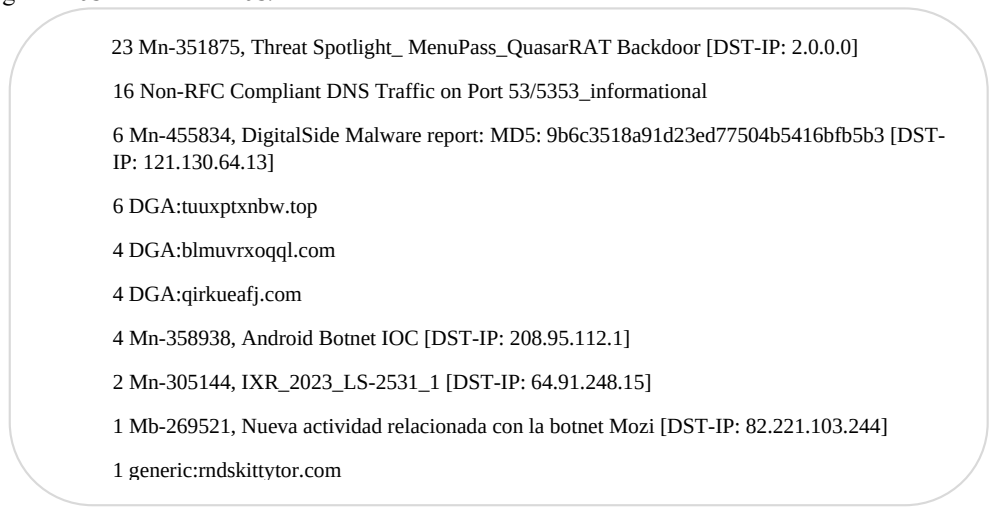
Nr. p. k.		Ugunsmūris identificējis *DGA* (kopā – 87)	Modulis identificējis *DGA* (kopā – 167)
1.	Ugunsmūris identificēja *DGA*	87	25
2.	Modulis identificēja *DGA*	79	167
3.	Trešā puse identificēja *DGA*	31	18
4.	Trešā puse identificēja *DGA*, modulis identificēja *DGA*, bet ugunsmūris neidentificēja *DGA*	–	7

Bez *DGA* moduļa tika novērtēts arī *NFAI* modulis, kura mērķis ir ļaunprātīgas darbības identificēšana tīkla datos. Diemžēl *NFAI* neuzrādīja ļoti labus rezultātus, bet joprojām to var lietot kā papildelementu ļaunprātīgas darbības identificēšanai tīklā.

Šajā nodaļā tika novērtēts arī draudu agregācijas modulis, kura pamatā ir dažādu moduļu rezultātu apvienošana ar mērķi identificēt inficētu ierīci. Šim mērķim galvenokārt tika izmantota *Influx DB* datubāze. Lai veiktu draudu agregāciju, tika izstrādāti scenāriji, kas īstenojoties ģenerē noteiktas prioritātes ziņojumu. Atkarībā no ziņojuma prioritātes ierīces lietotājs par to tiek informēts vai arī tiek liegta ierīces piekļuve tīklam. Ņemot vērā dinamisko IP adrešu izsniegšanu, lai draudu agregācijas modulis spētu pilnvērtīgi darboties, nepieciešama IP adreses sasaiste ar ierīces *MAC* adresi. Kad šāda sasaiste tika veikta, ierīces *MAC* adrese tika uzskatīta par unikālu vērtību un draudu agregācija notika pēc drauda kritiskuma, piemēram, nosakot, ka noteikts skaits ar vidējas prioritātes ziņojumiem tiek uzskatīts par draudu. Tāpat

draudus iespējams agregēt pēc draudu kategorijas, piemēram, ja tiek identificēts *DGA* un vēl citi vidējas prioritātes ziņojumi noteiktā laika intervālā, tas tiek uzskatīts par draudu.

Draudu agregācija (**Error! Reference source not found.**. att.) tika veikta, izmantojot dažādas draudu avotu kopas, piemēram *IDS* auditācijas pierakstus, ugunsmūra datus, kā arī aloritmiski ģenerētus domēnu vārdus.



9. att. Datu agregācija, izmantojot dažādas draudu avotu kopas.

Draudu agregācijas moduļa galvenais uzdevums ir samazināt viltus pozitīvo ziņojumu skaitu. Dažkārt mērķētu reklāmu atskaņošanai tiek izmantoti algoritmiski ģenerēti domēni, tāpēc tūlītēji uzskatīt šāda domēna izsaukšanu par draudu būtu nepareizi. Arī dažādu "melno" sarakstu IP adreses ne vienmēr būtu uzskatāmas par tiešu drauda norādi, jo bieži vien drošības kompānijas nepārliecinās, vai "melnajā" sarakstā nonākusī IP adrese nav dinamiski piešķirta, un, ja tas tā ir, tad nākamais klients, kurš saņēmis šo dinamisko IP adresi, tiks uzskatīts par apdraudējumu. Draudu agregācijas moduļa ģenerētais ziņojums tiek uzskatīts par tipisku ziņojumu par identificētiem draudiem, nosūtot ierīces lietotājam ziņojumu e-pastā. Šāda draudu agregācija var tikt īstenota arī uz platformas ģenerētiem ziņojumiem, padarot šo ziņojumu apkopojumu par augstākas prioritātes draudu.

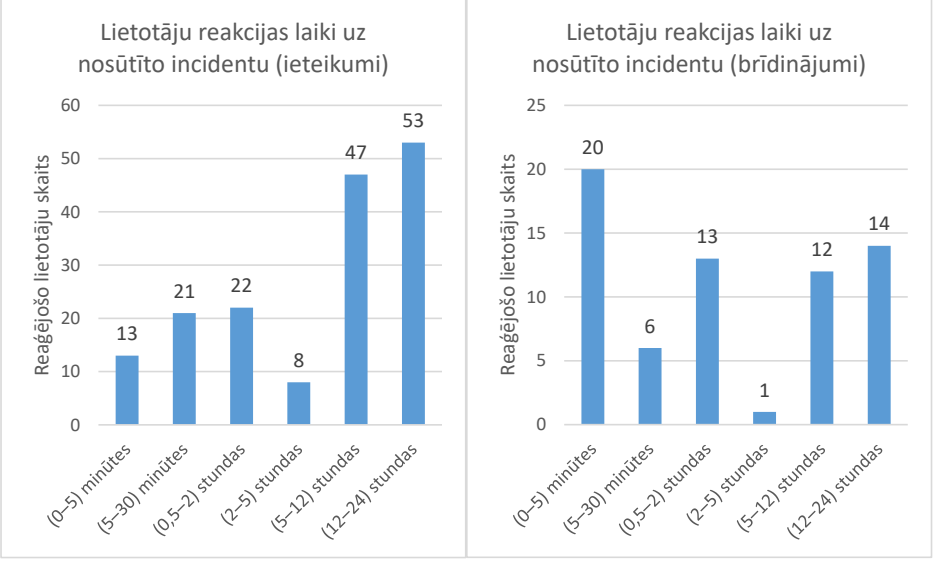
Darbā tika novērtēta *ISMS* platforma, un tas tika darīts vairākos posmos, izmantojot dažādas pieejas. *ISMS* platforma tika novērtēta, gan salīdzinot platformu ar tirgū pieejamiem risinājumiem, gan veicot lietotāju reaģēšanas ātruma mērījumus, kā arī novērtējot atsevišķus platformas moduļus (7. tab.).

7. tabula

ISMS platformas salīdzinājums ar tirgū pieejamiem risinājumiem

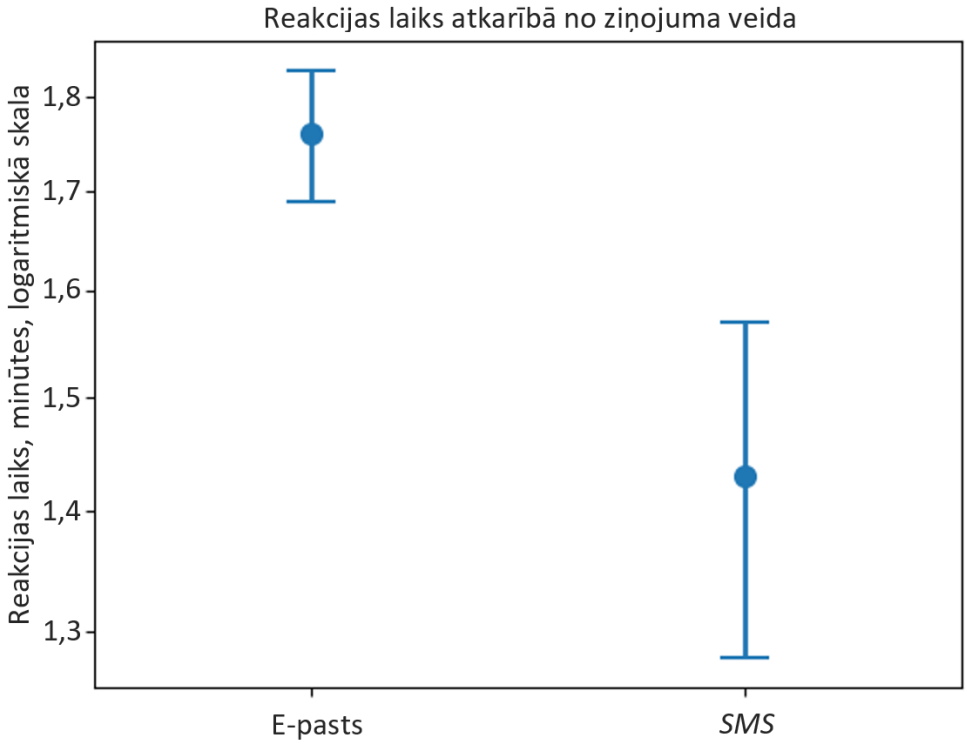
Novērtējuma struktūra	
Nr. p. k.	Platformas novērtējuma apraksts
1.	RTU IP adrešu un portu skanētāju identificēšanas moduļa novērtējums
2.	Platformas salīdzināšana ar "*Palo Alto"* ugunsmūra iebūvēto *IDS* funkcionalitāti
3.	Lietotāju reakcijas laiks, saņemot automātisku ziņojumu no platformas
4.	Platformas darbības efektivitātes novērtējums, balstoties lietotāju atgriezeniskajā saitē
5.	Platformas efektivitātes novērtējums, balstoties trešo pušu ziņojumos par inficētām ierīcēm RTU tīklā
6.	*Gartner Magic quadrant* TOP līderu salīdzinājums ar *ISMS* platformu

Lietotāju reakcijas laiks uz ieteikumiem, kur informācijas tika sūtīta tikai e-pastā un iekļauta portālā, ir aptuveni 5–10 stundas kopš ziņojuma saņemšanas, savukārt brīdinājumi, kuros tika nosūtīta informācija, tai skaitā *SMS* veidā, tiek apskatīti jau piecu minūšu laikā (**Error! Reference source not found.**. att.).



10. att. Reakcijas laiks uz brīdinājumiem un ieteikumiem.

Apstiprinājums tam, ka lielākā daļa lietotāju atbildēja uz *SMS* paziņojumu piecu minūšu laikā, ir parādīts intervāla diagrammā (11. att.), kur attēlots vidējais atbildes laiks atbilstoši saziņas veidam.



11. att. Reakcijas laiks atkarībā no ziņojuma veida.

Pārējo aspektu novērtēšanas rezultāti ir doti promocijas darbā.

REZULTĀTI UN SECINĀJUMI

Promocijas darba galvenais mērķis bija izstrādāt spējā metodoloģijā balstītu, no konteksta atkarīgu adaptīvu drošības pārvaldības modeli un atbilstošus tehniskos risinājumus kiberdrošības vides uzlabošanai, samazinot kiberdrošības incidentu skaitu un uzlabojot reaģēšanas ātrumu kiberincidenta gadījumā. Papildus galvenajam mērķim tika izveidota un aprobēta *ISMS* platforma, kā arī novērtēti tās darbības rezultāti. Mērķa sasniegšanai iegūti šādi rezultāti:

1) veikta analīze un novērtēta esošā situācija IS drošības pārvaldības jomā;
2) apzināti esošie pētījumi un izpētītas esošo drošības pārvaldības rīku iespējas, kā arī izpētīti pakalpojumi, kas nodrošina drošības pārvaldību;
3) identificētas nepieciešamās kontroles, ko var automatizēt, lai nodrošinātu IS drošības pārvaldību uzņēmumā;
4) izstrādāta vispārējā drošības pārvaldības spēja un augsta līmeņa tehniskā arhitektūra *ISMS* platformai;
5) izstrādāts *ISMS* platformas spēju modelis un identificēti nepieciešamie moduļi *ISMS* platformas darbībai;
6) definēta *ISMS* platformas implementācija;
7) adaptēts *ISMS* platformas spēju modelis RTU prasībām;
8) novērtēta *ISMS* platformas *ISMS* darbības efektivitāte;
9) sniegti secinājumi un priekšlikumi IS drošības pārvaldības uzlabošanai.

Izstrādātā *ISMS* platforma Rīgas Tehniskajā universitātē tika ieviesta kopš 2016. gada, papildinot to ar dažādiem moduļiem. Pirmsākumā tā bija tikai *IDS* sistēma ar automatizētu iespēju paziņot lietotājam par identificēto inficēto ierīci. Sākotnēji tas palīdzēja nākamajā gadā pēc ieviešanas vairāk nekā uz pusi samazināt *CERT* paziņojumu skaitu par inficētām ierīcēm RTU tīklā. Pēc tehnoloģiskā risinājuma izveides (*ISMS*) situācija uzlabojās vēl vairāk. Tika ieviesta spēja automātiski bloķēt ierīci, kuras lietotājs nereaģē uz paziņojumiem. Pakāpeniski, ieviešot papildu *ISMS* platformas moduļus, samazinājās *CERT* ziņojumu skaits par ificētajām ierīcēm RTU tīklā. Ieviešot paroles zādzības identificēšanas moduli, tika konstatēts, ka visbiežāk paroļu zagļi mēģina izmantot leģitīmu lietotāju kontus, lai apietu e-pasta servera aizsardzības mehānismu pret mēstulēm, kā arī tika konstatēts, ka visbiežāk šie ļaundari izmanto Āfrikas kontinenta IP adrešu apgabalu. Ļaundari arvien uzlabo savas prasmes, un mūsdienās piķšķerēšanas e-pasts ir ļoti grūti atšķirams no leģitīma e-pasta, var tikt izmantoti arī *html* faili

kā e-pasta pielikums. Piemēram, viena no veiksmīgākajām autora novērotajām piķšķerēšanas kampaņām bija zagtas lietotāja paroles izmantošana, kā arī jau atsūtītas vēstules izmantošana, nosūtot atbildi uz to ar saiti, kurā it kā tiek kopīgots dokuments, lai to atvērtu, ir nepieciešams autentificēties viltus *M365* portālā.

Ieviešot *DGA* moduli *ISMS* platformā, tika atklātas robotu tīklā esošas ierīces, piemēram, stāvvietas vārtiņu atvēršanas kontrolieris, kas pēc tā uzstādīšanas netika uzturēts, un ierīce tika inficēta. Lai arī mūsdienās *DNS* ir iespējams slēpt, izmantojot gan *DNS over HTTP*, gan arī *DNS over TLS* metodes, tomēr ir novērots, ka ļaunprātīgu programmu veidotāji šādas metodes izmanto reti. *DNS* moduļa ieviešana palīdzēja būtiski samazināt *CERT* paziņojumu skaitu, jo daudzas robotu tīklā esošas iekārtas uzvedās ļoti piesardzīgi un tās varēja identificēt tikai pēc *DNS* pieprasījuma. Darbā tika salīdzināts *DGA* modulis ar vienu no labākajiem ugunsmūriem *Gartner* kvadranta ieskatā [39], kuram ražotājs bija paredzējis *DGA* identificēšanas funkcionalitāti. *DGA* modulis identificēja ļaunprātīgu pieprasījumu 92,4 % gadījumu, salīdzinot ar iepriekšminēto ugunsmūri. *DGA* modulis 8,5 % gadījumu ir atklājis ļaunatūru, ko ugunsmūris nav atklājis, bet to ir apstiprinājusi vismaz viena no trim trešām pusēm (*Cloudfare* [40], *Norton* [41] vai *Quad9* [42]).

Lai arī *NFAI* modulis ne vienmēr darbojās labi, tomēr tika identificētas inficētas ierīces tīklā pat tādos gadījumos, kad tika lietota *DNS* pieprasījumu šifrēšana, kā arī visas datu plūsmas šifrēšana. Atbilstoši sniegtajām lietotāju atsaucēm kopumā tika identificēti seši ļaunatūras varianti, kas vēl nebija zināmi ugunsmūrim un *IDS* sistēmai. Arī "meduspoda" modulis ir devis pozitīvus rezultātus, identificējot inficētas ierīces laikā, kad tās iesāk tīkla ierīču skanēšanu un meklē jaunus potenciālos upurus.

Apvienojot *ISMS* platformā dažādus moduļus, tika samazināti viltus trauksmes ziņojumi.

Iesaistot galalietotājus incidenta novēršanas procesā, kā arī spējot atslēgt ierīci, tika samazināta iespējamība, ka inficētā ierīce inficēs citas tīklā esošas ierīces. Īpaši tas ir aktuāli gadījumos, kad inficētā ierīce nav RTU pārvaldībā (piemēram, studentu ierīces).

Papildus RTU *ISMS* ir ieviests arī divās Latvijas valsts iestādēs – Centrālajā finanšu un līgumu aģentūrā (CFLA) un Iepirkumu uzraudzības birojā (IUB). 8. tabulā apkopoti galvenie novērojumi par *ISMS* izmantošanu minētajās organizācijās. CFLA aizstāja *Splunk* drošības informācijas un notikumu pārvaldības (*SIEM*) sistēmu ar *ISMS*, kas licenču maksās ļāva ietaupīt aptuveni 50 000 EUR gadā. Šie ietaupījumi galvenokārt tika panākti, atceļot *Splunk* licenču maksas un samazinot maksājumus ārējiem pakalpojuma sniedzējiem, kas bija atbildīgi par

Splunk notikumu konfigurēšanu un uzraudzību. Daudzas trešo pušu lietojumprogrammas, piemēram, dokumentu pārvaldības sistēma IUB, ģenerē žurnālu failus, kas iepriekš tika analizēti atsevišķi šajās lietojumprogrammās. IUB dokumentu pārvaldības sistēmas žurnālu failu analīze tika integrēta *ISMS*, samazinot izmaksas, kas tika maksātas trešo pušu lietojumprogrammu izstrādātājiem.

Šo funkciju vērtību ir apstiprinājusi abu organizāciju vadība. *ISMS* tika prezentēta arī Latvijas informācijas tehnoloģiju drošības kopienai *CERT.LV* seminārā "*Be Secure*" 2023. gadā, kā arī IT drošības pasākumā "*Cyber Commando*", kas 2024. gadā notika Rīgā.

8. tabula

Izmantotās *ISMS* iespējas CFLA un IUB

Iespējas	**CFLA**	**IUB**
Izmaksas	Licenču izmaksu samazināšana	Izmaksu samazināšna, nepērkot dokumetu vadības sistēmas auditācijas moduli
Datu avoti	Tiek izmantoti tie paši datu avoti kā RTU gadījumā	Papildu datu avoti, piemēram, tiek pievienoti žurnāli no ārējām uzņēmuma sistēmām, nepalielinot licenču maksu
Organizācijai specifiski moduļi	Tīkla datplūsmas analīzes modulis iekšējā audita vajadzībām, lai pārbaudītu atbilstību	Modulis trešo pušu lietojumprogrammu žurnālu failu analīzei, izmantojot *ISMS*
Automatizēta lietotāju iesaiste	Lietoti iestādes specifiskie komunikācijas kanāli ziņojuma nodošanai	Lietotājiem tiek nosūtītas instrukcijas problēmas novēršanai, īpašos gadījumos tiek iesaistīti sistēmas administratori
Drošības incidentu pārvaldība	Paziņojumu veidi un automatizācijas moduļi ir pielāgoti organizācijas vajadzībām	Paziņojumu veidi un automatizācijas moduļi ir pielāgoti organizācijas vajadzībām

Nobeigumā autors secina, ka *ISMS* platforma ir līdzvērtīgs risinājums komerciāliem produktiem drošības pārvaldības jomā. Platforma nodrošina organizācijai nepieciešamo kiberdrošības risku identificēšanu un mazināšanu, kā arī apstiprina autora izvirzīto hipotēzi, ka, apvienojot vairākus datu avotus, specializētus draudu identificēšanas modeļus un platformas, tiek iegūta pilnvērtīgāka drošības incidentu identificēšana, salīdzinot ar individuālu šim mērķim paredzētu risinājumu izmantošanu.

LITERATŪRAS SARAKSTS

[1] M. o. D. o. Latvia, “Latvian Cybersecurity strategy 2019–2022”, 2019. [Tiešsaiste]. Available: http://tap.mk.gov.lv/doc/2018_11/AiMpamn_221118_PLKS.1220.docx. [Piekļūts 08.06.2020].

[2] “An official website of the European Union”, 14 12 2022. [Tiešsaiste]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555. [Piekļūts 06.09.2023].

[3] CISA, “What is Cybersecurity?”, Cybersecurity & Infrastructure Security agency, 2009. [Tiešsaiste]. Available: https://us-cert.cisa.gov/ncas/tips/ST04-001. [Piekļūts 30.04.2021].

[4] “SolarWinds hack was 'largest and most sophisticated attack' ever”, Reuters, 21 02 2021. [Tiešsaiste]. Available: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R. [Piekļūts 26.04.2021].

[5] “Colonial Pipeline CEO admits to authorizing $4.4 million ransomware payment”, CNN, 19.05.2021. [Tiešsaiste]. Available: https://edition.cnn.com/2021/05/19/politics/colonial-pipeline-ransom/index.html. [Piekļūts 10.06.2021].

[6] “Nedēļas nogalē atvairīti kiberuzbrukumi 70 valsts iestāžu tīmekļa vietnēm”, DIENA. [Tiešsaiste]. Available: https://www.diena.lv/raksts/latvija/zinas/nedelas-nogale-atvairiti-kiberuzbrukumi-70-valsts-iestazu-timekla-vietnem-14280778. [Piekļūts 24.05.2022].

[7] ENISA, “ENISA Threat Landscape 2020 – Botnet”. ENISA, 20.10.2020. [Tiešsaiste]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-botnet. [Piekļūts 30.04.2021].

[8] Saeima, “Nacionālās kiberdrošības likums”, Saeima, 20 06 2024. [Tiešsaiste]. Available: https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums. [Piekļūts 13.01.2025].

[9] E. P. U. PADOME, *EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula),* Eiropas Savienības Oficiālais Vēstnesis, 2016.

[10] “Marriott reveals its second customer data breach in two years”, CBSnews, 31.03.2020. [Tiešsaiste]. Available: https://www.cbsnews.com/news/marriott-data-breach-2020-5-million/. [Piekļūts 27.04.2021].

[11] “ICO fines Marriott International Inc”, Information Commisioner's office, 30.10.2020. [Tiešsaiste]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/. [Piekļūts 27.04.2021].

[12] “City Bee” pēc Lietuvas klientu datu noplūdes apgalvo, ka lietotāju dati Latvijā ir drošībā», Apollo ziņas, 17.02.2021. [Tiešsaiste]. Available: https://www.apollo.lv/7182586/city-bee-pec-lietuvas-klientu-datu-nopludes-apgalvo-ka-lietotaju-dati-latvija-ir-drosiba. [Piekļūts 27.04.2021].

[13] “Latvijā, iespējams, notikusi nekustamo īpašumu apsaimniekošanas uzņēmumu klientu datu noplūde”, Ziņu aģentūra LETA, 05.02.2021. [Tiešsaiste]. Available: https://nra.lv/latvija/338501-latvija-iespejams-notikusi-nekustamo-ipasumu-apsaimniekosanas-uznemumu-klientu-datu-noplude.htm. [Piekļūts 27.04.2021].

[14] J. P. Anderson, Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., 1980.

[15] P. Scwab, “The History of Intrusion Detection Systems (IDS) – Part 1”, 09.09.2015. [Tiešsaiste]. Available: https://www.threatstack.com/blog/the-history-of-intrusion-detection-systems-ids-part-1. [Piekļūts 08.06.2020].

[16] ISACA, “State of Cybersecurity 2020”, ISACA, 2020. [Tiešsaiste]. Available: https://www.isaca.org/go/state-of-cybersecurity-2020. [Piekļūts 26.04.2021].

[17] PWC, “24th Annual Global CEO Survey”, PricewaterhouseCoopers, 2021. [Tiešsaiste]. Available: https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2021.html. [Piekļūts 26.04.2021].

[18] J. Yakencheck, “Increase Automation to Overcome Cyber Resilience Challenges”, [Tiešsaiste]. Available: https://securityintelligence.com/posts/increase-automation-to-overcome-cyber-resilience-challenges/. [Piekļūts 26.03.2020].

[19] e. planet, “Top Cybersecurity Companies”, eSecurity planet, 05 01 2021. [Tiešsaiste]. Available: https://www.esecurityplanet.com/products/top-cybersecurity-companies/. [Piekļūts 27.04.2021].

[20] N. I. o. S. a. Technology, “Framework for Improving Critical Infrastructure Cybersecurity”, 18.04.2018. [Tiešsaiste]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Piekļūts 08.06.2020].

[21] “CERT.LV”, [Tiešsaiste]. Available: https://cert.lv/lv. [Piekļūts 08.06.2021].

[22] Saeima, “Minimālās kiberdrošības prasības”, Saeima, 25.06.2025. [Tiešsaiste]. Available: https://likumi.lv/ta/id/361481-minimalas-kiberdrosibas-prasibas. [Piekļūts 30.11.2025].

[23] “SOC-as-a-Service”, Deltarisk, 2021. [Tiešsaiste]. Available: https://deltarisk.com/soc-as-a-service/. [Piekļūts 04.05.2021].

[24] R. Cybersecurity, “SOC as a Service”, Radar Cybersecurity, 2021. [Tiešsaiste]. Available: https://www.radarcs.com/service-technology/managed-security-services/. [Piekļūts 04.05.2021].

[25] At&T, “SOC as a service”, At&T, 2021. [Tiešsaiste]. Available: https://cybersecurity.att.com/solutions/security-operations-center/soc-as-a-service. [Piekļūts 04.05.2021].

[26] Profico, “SOC-as-a-Service”, Profico, 2021. [Tiešsaiste]. Available: https://www.proficio.com/soc-as-a-service/. [Piekļūts 04.05.2021].

[27] Netsurion, “Security Operations Center (SOC)”, Netsurion, 2021. [Tiešsaiste]. Available: https://www.netsurion.com/managed-threat-protection/security-operations-center. [Piekļūts 04.05.2021].

[28] “SOC Report Cost”, TrustNet, 2021. [Tiešsaiste]. Available: https://www.trustnetinc.com/pricing/soc-ssae18-report-cost/. [Piekļūts 05.05.2021].

[29] “Alexa Top million domains”, Alexa, [Tiešsaiste]. Available: http://s3.amazonaws.com/alexa-static/top-1m.csv.zip. [Piekļūts 11.08.2021].

[30] “Alexa Top Sites”, Amazon, 2021. [Tiešsaiste]. Available: https://aws.amazon.com/alexa-top-sites/. [Piekļūts 07.05.2021].

[31] K. Sandkuhl un J. Stirna, Capability Management in Digital Enterprises, Springer International Publishing, 2018, p. 396.

[32] A. Kofod-Petersen, “How to do a Structured Literature Review in computer science”, ResearchGate, 2015.

[33] K. J. G. J. Minkevičs V., “Managing Information System Security in Higher Education Organizations”, %1 *IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Vilnius, Lithuania, 2023.

[34] “Apache Kafka”, Apache, 2021. [Tiešsaiste]. Available: https://kafka.apache.org/. [Piekļūts 06.05.2021].

[35] “Build on InfluxDB”, InfluxData, 2021. [Tiešsaiste]. Available: https://www.influxdata.com/. [Piekļūts 06.05.2021].

[36] “Your observability wherever you need it”, GrafanaLabs, 2021. [Tiešsaiste]. Available: https://grafana.com/. [Piekļūts 06.05.2021].

[37] “Secure Network Access Control for Modern IT”, Aruba, 2021. [Tiešsaiste]. Available: Secure Network Access Control for Modern IT. [Piekļūts 06.05.2021].

[38] E.-O. Jose Selvi, Ricardo J.Rodríguez, “Detection of algorithmically generated malicious domain names using masked N-grams”, *Elsevier*, sēj. 124, pp. 156–163, 2019.

[39] “Gartner Magic Quadrant”, Gartner, [Tiešsaiste]. Available: https://www.gartner.com/en/research/methodologies/magic-quadrants-research. [Piekļūts 04.06.2021].

[40] “Introducing 1.1.1.1 for Families”, Cloudfare, [Tiešsaiste]. Available: https://blog.cloudflare.com/introducing-1-1-1-1-for-families/. [Piekļūts 07.06.2021].

[41] “Norton ConnectSafe”, Norton, [Tiešsaiste]. Available: https://en.wikipedia.org/wiki/Norton_ConnectSafe. [Piekļūts 07.06.2021].

[42] “An open DNS recursive service for free security and high privacy”, Quad9, 2021. [Tiešsaiste]. Available: https://quad9.com/. [Piekļūts 07.05.2021].

[43] “Suricata Open Source IDS / IPS / NSM engine”, The Open Information Security Foundation., [Tiešsaiste]. Available: https://suricata-ids.org/. [Piekļūts 20.08.2019].

[44] ISO, “Information security management (ISO/IEC 27001)”, ISO, 2013. [Tiešsaiste]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Piekļūts 27.04.2021].

[45] CISA, “Cybersecurity Framework”, CISA, 2021. [Tiešsaiste]. Available: https://us-cert.cisa.gov/resources/cybersecurity-framework. [Piekļūts 27.04.2021].

[46] J. Y. P. L. a. R. F. E. C. Zhong, “Learning From Experts’ Experience: Toward Automated Cyber Security Data Triage”, *IEEE Systems Journal*, sēj. 13, pp. 603–614, 2019.

[47] Z. Chkirbene, S. Eltanbouly, M. Bashendy, N. Alnaimi un A. Erbad, “Hybrid Machine Learning for Network Anomaly Intrusion Detection”, *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, pp. 163–170, 2020.

[48] C. I. f. Cybersecurity, “Publiski pieejams datu avots NSL-KDD”, 2009. [Tiešsaiste]. Available: https://www.unb.ca/cic/datasets/nsl.html. [Piekļūts 30.04.2021].

[49] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed un M. Xu, “A Survey on Machine Learning Techniques for Cyber Security in the Last Decade”, *IEEE Access*, sēj. 8, pp. 222310–222354, 2020.

[50] R. M. Elbasiony, E. A. Sallam, T. E. Eltobely un M. M. Fahmy, “A hybrid network intrusion detection framework based on random forests and weighted k-means”, *Ain Shams Engineering Journal*, sēj. 4, pp. 753–762, 2013.

[51] MITRE, “Risk Mitigation Planning, Implementation, and Progress Monitoring”, MITRE Corporation, 2018. [Tiešsaiste]. Available: https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring. [Piekļūts 03.05.2021].

[52] A. Ahluwalia, I. Traore, K. Ganame un N. Agarwal, "Detecting Broad Length Algorithmically Generated Domains", *Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, pp. 19–34, 2017.

[53] F. F. Daniel Plohmann, U. o. B. Khaled Yakdan, D. Michael Klatt, J. Bader un F. F. Elmar Gerhards-Padilla, "A Comprehensive Measurement Study of Domain Generating Malware", %1 *25th USENIX Security Symposium*, Austin, TX, 2016.

[54] D.-T. Truong un G. Cheng, "Detecting domain-flux botnet based on DNS traffic features in managed network", *Security and Communication Networks*, sēj. 9, nr. 14, pp. 2338–2347, 2016.

[55] "Firefox DNS-over-HTTPS", Firefox, [Tiešsaiste]. Available: https://support.mozilla.org/en-US/kb/firefox-dns-over-https. [Piekļūts 03.05.2021].

[56] M. Vale, "Google Public DNS now supports DNS-over-TLS", Google, 2019. [Tiešsaiste]. Available: https://security.googleblog.com/2019/01/google-public-dns-now-supports-dns-over.html. [Piekļūts 03.05.2021].

[57] Cloudfare, "DNS over TLS", Cloudfare, 2021. [Tiešsaiste]. Available: https://developers.cloudflare.com/1.1.1.1/dns-over-tls. [Piekļūts 03.05.2021].

[58] Zonefiles, "Compromised domain lis", Zonefiles, 05 2021. [Tiešsaiste]. Available: https://zonefiles.io/compromised-domain-list/. [Piekļūts 03.05.2021].

[59] S. H. Mousavi, M. Khansari un R. Rahmani, "A fully scalable big data framework for Botnet detection based on network traffic analysis", *Information Sciences*, nr. 512, pp. 629–640, 2020.

[60] B. B. Gupta, Machine Learning for Computer and Cyber Security Principles, Algorithms, and Practices, New York: CRC Press Taylor & Francis Group, 2018.

[61] Mcafee, "10 key functions performed by the SOC", Mcafee, 2021. [Tiešsaiste]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html#definition. [Piekļūts 03.05.2021].

[62] M. R. Long, "A Small Business Guide to the Security Operations Center", Montley Fool, 18.11.2020. [Tiešsaiste]. Available: https://www.fool.com/the-blueprint/soc/. [Piekļūts 04.05.2021].

[63] Y. Korff, "How much does it cost to build a 24x7 SOC?", 28.02.2018. [Tiešsaiste]. Available: https://expel.io/blog/how-much-does-it-cost-to-build-a-24x7-soc/. [Piekļūts 05.05.2021].

[64] "Intelligent Management Software", Hewlett Packard Enterprise, 2021. [Tiešsaiste]. Available: https://buy.hpe.com/us/en/software/intelligent-management-software/c/c001014. [Piekļūts 05.05.2021].

[65] "The Nessus Family", Tenable, 2021. [Tiešsaiste]. Available: https://www.tenable.com/products/nessus. [Piekļūts 05.05.2021].

[66] "Downloading Nmap", Nmap.org, 2021. [Tiešsaiste]. Available: https://nmap.org/download.html. [Piekļūts 05.05.20201].

[67] R. Alguliyev un Y. Imamverdiyev, "Big Data: Big Promises for Information Security", %1 *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT)*, 2014.

[68] "Apache Spark™ is a unified analytics engine for large-scale data processing", Apache, 2021. [Tiešsaiste]. Available: https://spark.apache.org/. [Piekļūts 06.05.2021].

[69] K. R. S. Barbosa, E. Souto, E. Feitosa un K. El-Khatib, "Identifying and Classifying Suspicious Network Behavior Using Passive DNS Analysis", *2015 IEEE International Conference on Computer and*

Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 160–167, 2015.

[70] H. S. A. A. A. D. G. Jonathan Woodbridge, *Predicting Domain Generation Algorithms with Long Short-Term Memory Networks*, Arlington,VA 22201: Endgame, Inc, 2016, p. 13.

[71] M. Mowbray un J. Hagen, "Finding Domain-Generation Algorithms by Looking at Length Distribution", %1 *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, 2014.

[72] J. Peck, C. Nie, R. Sivaguru, C. Grumer, F. Olumofin, B. Yu, A. Nascimento un M. D. Cock, "CharBot: A Simple and Effective Method for Evading DGA Classifiers", *IEEE Access*, pp. 91759–91771, 2019.

[73] P. H. Z. Hu, L. Zhu, J. Heidemann, A. Mankin,D. Wessels, *Specification for DNS over Transport Layer Security (TLS)*, IETF Tools, 2016, p. 18.

[74] Mozilla.org, "About DNS-over-HTTPS", Mozilla.org, 07 01 2020. [Tiešsaiste]. Available: https://support.mozilla.org/en-US/kb/firefox-dns-over-https#w_about-dns-over-https. [Piekļūts 07.01.2020].

[75] "Analyze suspicious files and URLs to detect types of malware", VirusTotal, 2021. [Tiešsaiste]. Available: https://www.virustotal.com/gui/home/url. [Piekļūts 07.05.2021].

[76] "ICANN root zone", ICANN, 2021. [Tiešsaiste]. Available: http://stats.research.icann.org/dns/tld_report/archive/index.html. [Piekļūts 07.05.2021].

[77] M. Sheng, Machine Learning for Computer and Cyber Security Principles, Algorithms, and Practices, New York: CRC Press Taylor & Francis Group, 2019.

[78] "fprobe", SourceForge, 2016. [Tiešsaiste]. Available: https://sourceforge.net/p/fprobe/wiki/Home/. [Piekļūts 13.05.2021].

[79] "nfdump", GitHub, 2021. [Tiešsaiste]. Available: https://github.com/phaag/nfdump. [Piekļūts 13.05.2021].

[80] K. Singh, S. C. Guntuku, A. Thakur un C. Hota, *Big Data Analytics framework for Peer-to-Peer Botnet detection using Random Forests*, Information Sciences, 2014.

[81] K. P. Shung, "Accuracy, Precision, Recall or F1?", 15 05 2015. [Tiešsaiste]. Available: https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9. [Piekļūts 25.03.2021].

[82] F. Pacheco, E. Exposito, M. Gineste, C. Baudoin un J. Aguilar, "Towards the Deployment of Machine Learning Solutions in Network Traffic Classification: A Systematic Survey", 2019.

[83] "BlackBerry Protect", BlackBerry, [Tiešsaiste]. Available: https://www.blackberry.com/us/en/products/unified-endpoint-security/blackberry-protect. [Piekļūts 10.06.2021].

[84] "McAfee Endpoint Security", McAfee, [Tiešsaiste]. Available: https://www.mcafee.com/enterprise/en-us/products/endpoint-security.html. [Piekļūts 10.06.2021].

[85] "Prevent endpoint breaches", Broadcom, [Tiešsaiste]. Available: https://www.broadcom.com/products/cyber-security/endpoint/end-user. [Piekļūts 10.06.2021].

[86] D.-b. X. Lin Li, "Research on the network security management based on data mining", %1 *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Chengdu, China, 2010.

[87] “Blacklist Check List”, [Tiešsaiste]. Available: https://whatismyipaddress.com/blacklist-check. [Piekļūts 16.06.2021].

[88] “Blacklists”, [Tiešsaiste]. Available: https://mxtoolbox.com/blacklists.aspx. [Piekļūts 16.06.2021].

[89] “IPv4 – Packet Structure”, TutorialsPoint, [Tiešsaiste]. Available: https://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm. [Piekļūts 16.06.2021].

[90] “Suricata User Guide”, Suricata, [Tiešsaiste]. Available: https://suricata.readthedocs.io/en/suricata-6.0.2/. [Piekļūts 16.06.2021].

[91] S. C. M. M. a. D. C. A. Shah, “Building Multiclass Classification Baselines for Anomaly-based Network Intrusion Detection Systems”, %1 *2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA)*, 759–760.

[92] Z. K. J. B. a. R. I. A. Sharma, “Analysis of security data from a large computing organization”, %1 *IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*, 506–517, 2011.

[93] N. F. A. G. E. M. a. M. P. I. Rose, “Something Is Better Than Everything: A Distributed Approach to Audit Log Anomaly Detection”, %1 *IEEE Cybersecurity Development (SecDev)*, 2017.

[94] W. Z. a. W. Xinyu, “NetFlow Based Intrusion Detection System”, %1 *2008 International Conference on MultiMedia and Information Technology*, 2008.

[95] R. Gerhards, *The Syslog Protocol.*

[96] R. D. C. A. P. Marcello Cinque, “Contextual filtering and prioritization of computer application logs for security situational awareness”, *Future Generation Computer Systems*, sēj. 111, nr. ISSN 0167-739X, pp. 668–680, 2020.

[97] “The World’s First Truly Open Threat Intelligence Community”, Aleanvault, [Tiešsaiste]. Available: https://otx.alienvault.com/. [Piekļūts 18.06.2021].

[98] “IBM Security QRadar”, IBM, [Tiešsaiste]. Available: https://www.ibm.com/security/security-intelligence/qradar. [Piekļūts 18.06.2021].

[99] «Security Information and Event Management (SIEM)”, Logrhythm, [Tiešsaiste]. Available: https://logrhythm.com/solutions/security/siem/. [Piekļūts 18 06 2021].

[100] “Splunk Enterprise Security”, Splunk, [Tiešsaiste]. Available: https://www.splunk.com/en_us/software/enterprise-security.html. [Piekļūts 18.06.2021].

[101] “The Significance and Role of Firewall logs”, Exabeam, [Tiešsaiste]. Available: https://www.exabeam.com/siem-guide/siem-concepts/firewall-logs/. [Piekļūts 09.08.2021].

[102] S. K. Hajar Esmaeil As-Suhbani, “Classification of Firewall Logs Using Supervised Machine Learning Algorithms”, %1 *International Journal of Computer Sciences and Engineering Vol. 7, Issue 8*, 2019.

[103] D. W. V. a. J. P. Sharma, “Optimized Classification of Firewall Log Data using Heterogeneous Ensemble Techniques”, %1 *2021 International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2021*, 2021.

[104] “Intrusion detection system”, Wikipedia, [Tiešsaiste]. Available: https://en.wikipedia.org/wiki/Intrusion_detection_system. [Piekļūts 10.08.2021].

[105] M. A. F. B. S. OUIAZZANE, “A Multi-Agent Model for Network Intrusion Detection”, %1 *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, 2019.

[106] G. F. T. H. S. N. W.-S. Y. Jared Lee Lewis, “IP Reputation Analysis of Public Databases and Machine Learning Techniques”, %1 *International Conference on Computing, Networking and Communications, ICNC 2020. IEEE*, 2020.

[107] “AbuseIPDB”, [Tiešsaiste]. Available: https://www.abuseipdb.com/. [Piekļūts 11.08.2021].

[108] F. a. M. J. P. Magalhaes, “Adopting machine learning to support the detection of malicious domain names”, *7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020*, 2020.

[109] “DGA Collection”, [Tiešsaiste]. Available: https://github.com/pchaigno/dga-collection. [Piekļūts 11.08.2021].

[110] abuse.ch, [Tiešsaiste]. Available: https://urlhaus.abuse.ch/downloads/text/. [Piekļūts 11.08.2021].

[111] “English Dictionary”, Cambridge, [Tiešsaiste]. Available: https://dictionary.cambridge.org/dictionary/english/. [Piekļūts 11.08.2021].

[112] “Vulnerabilities, Exploits, and Threats at a Glance”, Rapid7, [Tiešsaiste]. Available: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/. [Piekļūts 11.08.2021].

[113] “The OWASP Testing Project”, OWASP, [Tiešsaiste]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/2-Introduction/README. [Piekļūts 11.08.2021].

[114] “CVE details”, MITRE Corporation, [Tiešsaiste]. Available: https://www.cvedetails.com/index.php. [Piekļūts 11.08.2021].

[115] “OpenVas by Greenbone”, Greenbone, [Tiešsaiste]. Available: https://openvas.org. [Piekļūts 11.08.2021].

[116] “One platform one agent one view”, Qualys, [Tiešsaiste]. Available: https://www.qualys.com. [Piekļūts 11.08.2021].

[117] “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”, likumi.lv, [Tiešsaiste]. Available: https://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam. [Piekļūts 12.08.2021].

[118] API Explorer, “API Explorer”, Aruba, [Tiešsaiste]. Available: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Guest/Content/AdministrationTasks1/API_Explorer.htm. [Piekļūts 12.08.2021].

[119] “clearpass-api-python”, Aruba, [Tiešsaiste]. Available: https://github.com/aruba/clearpass-api-python. [Piekļūts 12.08.2021].

[120] “Getting started with the REST API”, Hewlett Packard, [Tiešsaiste]. Available: https://developers.hp.com/hp-proactive-management/getting-started-rest-api. [Piekļūts 12.08.2021].

[121] “REST API Guide”, Juinper, [Tiešsaiste]. Available: https://www.juniper.net/documentation/us/en/software/junos/rest-api/index.html. [Piekļūts 12.08.2021].

[122] “PAN-OS REST API”, Palo Alto, [Tiešsaiste]. Available: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-rest-api/pan-os-rest-api.html. [Piekļūts 12.08.2021].

[123] M. D. H. Garg, “Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware”, %1 *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019.

[124] Y. S. Y. H. Y. L. J. L. Wei Wang, "BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors", *Information Sciences*, sēj. 511, pp. 284–296, 2020.

[125] H. B. S. Nõmm, "Unsupervised Anomaly Based Botnet Detection in IoT Networks", %1 *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2018.

[126] Z. T. R. Z. L. L. J. Liu, "A Distance-Based Method for Building an Encrypted Malware Traffic Identification Framework", %1 *IEEE Access*.

[127] E. S. I. K. I. S. A. Privalov, "Graph-based evaluation of probability of disclosing the network structure by targeted attacks", %1 *NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium*, 2020.

[128] J. Y. Z. W. H. L. X. Sun, "HGDom: Heterogeneous Graph Convolutional Networks for Malicious Domain Detection", %1 *NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium*, 2020.

[129] "dumpcap – Dump network traffic", Wireshark, [Tiešsaiste]. Available: https://www.wireshark.org/docs/man-pages/dumpcap.html. [Piekļūts 27.08.2021].

[130] "tshark – Dump and analyze network traffic", Wireshark, [Tiešsaiste]. Available: https://www.wireshark.org/docs/man-pages/tshark.html. [Piekļūts 27.08.2021].

[131] "Perl", Perl.org, [Tiešsaiste]. Available: https://www.perl.org. [Piekļūts 27.08.2021].

[132] R. D. Muhammet Baykara, "A novel honeypot based security approach for real-time intrusion detection and prevention systems", *Journal of Information Security and Applications*, sēj. 41, pp. 103–116, 2018.

[133] S. S. Sivatha Sindhu, S. Geetha un A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach", *Expert Systems with Applications*, sēj. 39, nr. 1, pp. 129–141, 2012.

[134] "Umbrella Popularity List", Cisco, 09 2021. [Tiešsaiste]. Available: http://s3-us-west-1.amazonaws.com/umbrella-static/index.html. [Piekļūts 21.09.2021].

[135] CERT.LV, "Latvija kopā ar sabiedrotajiem veikusi IKT sistēmu draudu meklēšanas operāciju", CERT, 30.11.2022. [Tiešsaiste]. Available: ka ir ārkārtīgi svarīgi nodrošināt tīkla inventarizāciju un redzamību, operētājsistēmu un izmantotās programmatūras savlaicīgus atjauninājumus, sistēmas drošības notikumu apkopošanu un uzraudzību, kā arī reaģēšanu uz incidentiem. [Piekļūts 07.12.2022].

[136] "SOAR defined", Microsoft, [Tiešsaiste]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-soar. [Piekļūts 23.09.2023].

[137] S. Shea, "SOAR (security orchestration, automation and response)", TechTarget, [Tiešsaiste]. Available: https://www.techtarget.com/searchsecurity/definition/SOAR. [Piekļūts 26.09.2023].

[138] "CIS Critical Security Controls", Cisecurity, [Tiešsaiste]. Available: https://www.cisecurity.org/controls. [Piekļūts 27.12.2023].

[139] "SOC for Cybersecurity", Aicpa&Cima, [Tiešsaiste]. Available: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity. [Piekļūts 27.12.2023].

[140] "Cyber Essentials", National Cyber Security Cetre, UK, [Tiešsaiste]. Available: https://www.ncsc.gov.uk/cyberessentials/overview. [Piekļūts 27.12.2023].

[141] S. Cass, "The Top Programming Languages 2023", IEEE, [Tiešsaiste]. Available: https://spectrum.ieee.org/the-top-programming-languages-2023. [Piekļūts 04.01.2024].

Vladislavs Minkevičs was born in 1978 in Daugavpils, Latvia. He earned a Bachelor's degree and a Master's degree (2003) in Information Technology from Riga Technical University. He is currently the Head of Information Security at the Central Finance and Contracting Agency. His research interests include cybersecurity, the automation of security operations centres, and the application of artificial intelligence in cybersecurity.