VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Tomas PLĖTA

KIBERNETINIO SAUGUMO VALDYMO MODELIS VALSTYBIŲ KRITINĖS ENERGETINĖS INFRASTRUKTŪROS SAUGAI TOBULINTI

DAKTARO DISERTACIJA

SOCIALINIAI MOKSLAI,
VADYBA (S 003)

Vilnius, 2024

Disertacija rengta 2019–2024 metais Vilniaus Gedimino technikos universitete.

Vadovas

prof. dr. Manuela TVARONAVIČIENĖ (Vilniaus Gedimino technikos universitetas, vadyba – S 003).

Vilniaus Gedimino technikos universiteto vadybos mokslo krypties disertacijos gynimo taryba:

Pirmininkas

prof. dr. Ilona SKAČKAUSKIENĖ (Vilniaus Gedimino technikos universitetas, vadyba – S 003).

Nariai:

doc. dr. Aurelija BURINSKIENĖ (Vilniaus Gedimino technikos universitetas, vadyba – S 003),

prof. dr. Nikolaj GORANIN (Vilniaus Gedimino technikos universitetas, informatikos inžinerija – T 007),

habil. dr. Jarosław KORPYSA (Ščecino universitetas, Lenkija, vadyba – S 003),

dr. Marius LAURINAITIS (Mykolo Romerio universitetas, teisė – S 001).

Disertacija bus ginama viešame vadybos mokslo krypties disertacijos gynimo tarybos posėdyje **2024 m. gegužės 6 d. 10 val.** Vilniaus Gedimino technikos universiteto SRA-I posėdžių salėje.

Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.
Tel.: (8 5) 274 4956; faksas (8 5) 270 0112; el. paštas doktor@vilniustech.lt

Pranešimai apie numatomą ginti disertaciją išsiųsti 2024 m. balandžio 5 d.

Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto talpykloje https://etalpykla.vilniustech.lt ir Vilniaus Gedimino technikos universiteto bibliotekoje (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva).

Vilniaus Gedimino technikos universiteto 2024-009-M mokslo literatūros knyga

https://doi.org/10.20334/2024-009-M

© Vilniaus Gedimino technikos universitetas, 2024
© Tomas Plėta, 2024
tomas.pleta@vilniustech.lt

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Tomas PLĖTA

CYBER SECURITY MANAGEMENT MODEL FOR IMPROVING THE SECURITY OF CRITICAL ENERGY INFRASTRUCTURE OF STATES

DOCTORAL DISSERTATION

SOCIAL SCIENCES,
MANAGEMENT (S 003)

Vilnius, 2024

The doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2019–2024.

Supervisor

Prof. Dr Manuela TVARONAVIČIENĖ (Vilnius Gediminas Technical University, Management – S 003).

The Dissertation Defense Council of the Scientific Field of Management of Vilnius Gediminas Technical University:

Chairperson

Prof. Dr Ilona SKAČKAUSKIENĖ (Vilnius Gediminas Technical University, Management – S 003).

Members:

Assoc. Prof. Dr Aurelija BURINSKIENĖ (Vilnius Gediminas Technical University, Management – S 003),

Prof. Dr Nikolaj GORANIN (Vilnius Gediminas Technical University, Informatics Engineering – T 007),

Habil. Dr Jarosław KORPYSA (University of Szczecin, Poland, Management – S 003),

Dr Marius LAURINAITIS (Mykolas Romeris University, Law – S 001).

The dissertation will be defended at the public meeting of the Dissertation Defense Council of the Scientific Field of Management in the SRA-I Hall of Vilnius Gediminas Technical University at **10 a. m. on 6 May 2024**.

Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4956; fax +370 5 270 0112; e-mail: doktor@vilniustech.lt

A notification on the intended defence of the dissertation was sent on 5 April 2024. A copy of the doctoral dissertation is available for review at the Vilnius Gediminas Technical University repository https://etalpykla.vilniustech.lt and the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania).

Reziumė

Disertacijoje nagrinėjama kibernetinio saugumo valdymo problema kritinės energetikos infrastruktūroje. Tyrimų objektas – valstybių kritinės energetikos infrastuktūros kibernetinio saugumo valdymas. Darbo tikslas – sukurti valstybių kritinės energetikos infrastruktūros kibernetinio saugumo valdymo modelį, integruojantį veiksnius, būtinus efektyviai užtikrinti saugumo valdymą ir stiprinti kibernetinį saugumą.

Disertaciją sudaro įvadas, trys skyriai, bendrosios išvados, naudotos literatūros ir autoriaus publikacijų sąrašai, penki priedai.

Analizuojant egzistuojančias kibernetinio saugumo sampratas, buvo pastebėta, kad kol kas nėra bendros kritinės infrastruktūros sąvokos. Įvairių valstybių požiūris į kritinę infrastruktūrą priklauso nuo jų poreikių, tačiau visos valstybės taiko tuos pačius pagrindinius principus – apsaugoti kibernetinę aplinką nuo išpuolių ir užtikrinti konfidencialumą, vientisumą ir prieinamumą. Tyrimo duomenys parodė, kad pagrindinis kibernetinio saugumo pažeidimų veiksnys išlieka žmogus.

Įvertinus kritinės energetinės infrastruktūros kibernetinio saugumo valdymo ypatumus bei atsižvelgiant į jo esamą standartą, paaiškėjo, kad pagrindinė kibernetinio saugumo problema yra kibernetinių grėsmių nustatymas, prevencinių priemonių taikymas, strategijų, kaip reaguoti į kibernetinius išpuolius ir netikėtus scenarijus, trūkumas bei nepakankamas pažeidžiamumo įvertinimas. Esami kibernetinio saugumo valdymo modeliai neužtikrina tinkamos apsaugos.

Išanalizavus kritinės energetinės infrastruktūros silpnąsias vietas, įvertinus užsienio valstybėse taikomas gerąsias praktikas, nustatyta, kad kritinės infrastruktūros saugumo lygis yra nepakankamas. Todėl buvo sukurtas ir ekspertų įvertintas valstybių kritinės energetikos infrastruktūros kibernetinio saugumo valdymo modelis.

Naują valdymo modelį galima tobulinti ir toliau. Siekiant padidinti valstybių kritinės energetikos infrastruktūros kibernetinį saugumą, tikslinga sukurti specialų saugumo operacijų centrą (angl. *Security Operation Centre* (SOC)), integruojantį visus modelio komponentus ir galintį žymiai pagerinti kibernetinės saugos vadybą kritinėje energetinėje infrastruktūroje valstybės mastu.

Disertacijos tema paskelbtos aštuonios publikacijos recenzuojamuose mokslo leidiniuose. Dvi iš jų įtrauktos į *Scopus* duomenų bazę. Disertacijoje atliktų tyrimų rezultatai pristatyti keturiose mokslinėse konferencijose Lietuvoje ir užsienyje.

Abstract

The dissertation examines the problem of cyber security management in critical energy infrastructure. The research object is the cyber security management of critical energy infrastructure in states. The dissertation aims to develop a model for the cyber security management of states' critical energy infrastructure, integrating factors necessary to ensure effective security management and enhance cyber security.

The dissertation consists of an introduction, three chapters, general conclusions, lists of references and the author's publications, and five annexes.

The analysis of the existing cyber security concepts revealed the lack of a common concept of critical infrastructure. Although countries approach critical infrastructure depending on their needs, the fundamental principles remain the same: to protect the cyber environment from attacks and achieve confidentiality, integrity and availability. Research data has shown that humans are the main factor contributing to cyber security breaches.

Having evaluated the cyber security management in critical energy infrastructure and considering existing standards, it became apparent that the main cyber security problems are identifying cyber threats, applying preventive measures, the lack of strategies for responding to cyber-attacks and unexpected scenarios, and a weak vulnerability assessment. Existing cyber security management models do not ensure adequate protection.

Having analysed the weaknesses of critical energy infrastructure and evaluated best practices applied in foreign countries, it was determined that the security level of critical infrastructure is insufficient. Therefore, a model for the cyber security management of states' critical energy infrastructure was developed and assessed by experts.

The new management model can be further improved to enhance the effectiveness of the cyber security model for states' critical energy infrastructure. It is possible to create a dedicated Security Operation Centre (SOC), integrating all model components, aiming to significantly improve cyber security management on a national scale in critical energy infrastructure.

The research results of the dissertation have been published in eight peer-reviewed scientific publications, two of which are included in the *Scopus* database. The research results were presented at four scientific conferences in Lithuania and abroad.

Žymėjimai

Simboliai

m – ekspertų skaičius (angl. *number of experts*);

n – kriterijų skaičius (angl. *number of criteria*);

$\widetilde{r_{ij}}$ – *i*-tojo rodiklio normalizuota reikšmė *j*-ajam objektui (angl. *normalised value of the i-th indicator for j-th object*);

r_i – kriterijų rangas (angl. *criteria rank*);

r_{ij} – *i*-tojo rodiklio reikšmė *j*-ajam objektui (angl. *value of the i-th indicator for j-th object*);

S – kiekvieno *i*-tojo kriterijaus rangų sumos (angl. *rank sums for each i-th criterion*);

t_j – vienodų rangų skaičius kiekviename veiksnyje (angl. *number of equal ranks in each factor*);

x_{ij} – *i*-tojo eksperto *j*-ojo kriterijaus rangas (angl. *rank of the i-th expert in the j-th criterion*);

ω_i – *i*-tojo rodiklio svoris (angl. *weight the i indicator*).

Santrumpos

AHP – analitinės hierarchijos procesas (angl. *Analytic Hierarchy Process*);

AMI – pažangi matavimo infrastruktūra (angl. *Advanced Measurement Infrastructure*);

ATP – išplėstinė nuolatinė grėsmė (angl. *Advanced Persistent Threat*);

CAW – svertinio vidurkio metodas (angl. *Cumulative Average Weighing*);

CEI – kritinė energetinė infrastruktūra (angl. *Critical Energy Infrastructure*);

CERT-LT – Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (angl. *Computer Emergency Response Teams*);

CIS – ryšių ir informacinė sistema (angl. *Communication and Information System*);

CISA – kibernetinio saugumo ir infrastruktūros saugumo agentūra (angl. *Cybersecurity and Infrastructure Security Agency*);

DCS – paskirstyto valdymo sistemos (angl. *Distributed Control Systems*);

DMZ – demilitarizuota zona (angl. *Demilitarised Zone*);

DoS – informacijos sugadinimas, paslaugų trikdymas (angl. *Denial-of-Service Attack*);

EACMS – elektroninės prieigos kontrolės stebėjimo sistema (angl. *Electronic Access Control Monitoring System*);

ELECTRE – daugiakriterių alternatyvų reitingavimo metodas (pranc. *Elimination et choix Trduisant la realite*);

GCI – pasaulinis kibernetinio saugumo indeksas (angl. *Global Cybersecurity Index*);

HMI – žmogaus ir mašinos sąsaja (angl. *Human-machine Interface*);

ICS – pramonės valdymo sistema (angl. *Industrial Control System*);

IoT – daiktų internetas (angl. *Internet of Things*);

ITU – Tarptautinė telekomunikacijų sąjunga (angl. *International Telecommunication Union*);

JAV – Jungtinės Amerikos Valstijos (angl. *United States of America*);

NCCIC – Nacionalinės energetikos reguliavimo tarnyba (angl. *National Cybersecurity and Communications Integration Centre*);

NCISS – nacionalinė kibernetinių incidentų taškų vertinimo sistema (angl. *National Cyber Incident Scoring System*);

NCSS – nacionalinė kibernetinio saugumo strategija (angl. *National Cybersecurity strategy*);

NERC – Šiaurės Amerikos ne pelno siekianti tarptautinė elektros patikimumo korporacija (angl. *North American Electric Reliability Corporation*);

NIPP – Nacionalinis infrastruktūros apsaugos planas (angl. *National Infrastructure Protection Plan*);

NIST – Nacionalinis standartų ir technologijos institutas (angl. *National Institute of Standards and Technology*);

NKSC – Nacionalinis kibernetinio saugumo centras (angl. National Cyber Security Centre)

NOC – tinklo valdymo centras (angl. *Network Operational Centre*);

PLC – programuojamas loginis valdiklis (angl. *Programmable Logic Controller*);

RTU – nuotolinis telemetrijos įrenginys (angl. *Remote Terminal Unit*);

SAW – paprastasis adityvaus svorio metodas (angl. *Simple Additive Weighting Method*);

SCADA – stebėjimo ir valdymo sistema (angl. *Supervisory Control and Data Acquisition*);

SDLC – saugumo programinėje įrangoje gyvavimo ciklas (angl. *System Development Life Cycle*);

SOC – saugumo operacijų centras (angl. *Security Operation Centre*);

THIRA – grėsmių nustatymo ir rizikos vertinimo sistema (angl. *Threat Identification and Risk Assessment System*);

TOPSIS – užsakymo pirmenybės pagal panašumą į idealų sprendimą metodas (angl. *Technique for Order Preference by Similarity to Ideal Solution*);

UPS – nepertraukiamo maitinimo šaltinis (angl. *Uninterruptible Power Supplies*);

VPN – virtualus privatus tinklas (angl. *Virtual Private Network*).

Turinys

Contents

Įvadas

Problemos formulavimas

Kibernetinių grėsmių iššūkių vis daugėja, o tai rodo augantį įsilaužėlių profesionalumą ir jų skaičiaus didėjimą. Todėl kibernetinis saugumas yra vienas iš svarbesnių veiksnių, kuris turi būti sprendžiamas valstybės lygmeniu.

Patikima ir saugi kritinė infrastruktūra yra gyvybiškai svarbi ekonomikos klestėjimui, nes ji ne tik palaiko efektyvų verslo ir paslaugų veikimą, bet ir skatina ilgalaikį pasitikėjimą, planavimą ir investicijų pritraukimą. Tačiau informacinių technologijų vystymas, skaitmenizavimas, automatizavimas ir optimizavimas sukuria naujas galimybes kibernetinio saugumo grėsmėms plisti, o tai rodo, kad reikalingi pokyčiai ne tik kibernetinėje gynyboje, bet ir valdymo srityje.

Atsižvelgiant į energetikos sektoriaus pobūdį, specifiškumą ir struktūros ypatumus, siekiant stiprinti bei gerinti jo kibernetinį saugumą, būtina ieškoti naujų priemonių ir įrankių, taikant šiuolaikinius vadybos metodus ir priemones, sprendžiant kokybės vadybos problemą.

Besikeičianti aplinka skatina naują požiūrį į kritinės energetinės infrastruktūros kibernetinės saugumo valdymo aspektus. Todėl būtina sukurti efektyvų ir universalų valdymo modelį, kuris padėtų spręsti kibernetinio saugumo problematiką, nustatant ir valdant tarpusavyje sąveikaujančius procesus.

Darbo aktualumas

Pastaraisiais metais vis daugiau dėmesio yra skiriama kibernetiniam ir energetiniam saugumui. Valstybių strategijose kibernetinis bei energetinis saugumas išskiriami kaip vieni iš pirmaeilių nacionalinių saugumo interesų, kurių neginant, laikui bėgant, būtų pažeidžiami gyvybiniai valstybės interesai (Nacionalinio saugumo strategija, 2012). Galima teigti, jog kibernetinis saugumas ir energetikos sektorius glaudžiai susiję − kibernetinės grėsmės kritinei energetinei infrastruktūrai įgauna vis didesnį mastą (Smaliukas, 2015).

Sparti informacinių technologijų plėtra pamažu keičia pasaulį. Atvira ir laisva elektroninė erdvė padidina žmonių laisvę ir galimybes bei praturtina visuomenę. Tačiau tuo pat metu šiuolaikinio skaitmeninio pasaulio pranašumai ir informacinių technologijų plėtra sukuria naujas grėsmes nacionaliniam ir tarptautiniam saugumui (Šišulák, 2017). Todėl kuriant modelį taikoma besimokančios organizacijos koncepcija, o pats modelis laikomas besimokančia organizacija, susidedančia iš tarpusavyje susijusių elementų, kurie nuolat sąveikauja su aplinka ir prie jos prisitaiko.

Tyrimų objektas

Tyrimų objektas – valstybių kritinės energetikos infrastuktūros kibernetinio saugumo valdymas.

Darbo tikslas

Šio darbo tikslas – sukurti valstybių kritinės energetikos infrastruktūros kibernetinio saugumo valdymo modelį, integruojantį veiksnius, efektyviai užtikrinančius kibernetinio saugumo valdymą.

Darbo uždaviniai

Darbo tikslui pasiekti iškelti šie uždaviniai:

1. Išanalizuoti energetikos sektoriaus kibernetinį saugumą, kritinės energetinės infrastruktūros valdymą, iššūkius ir atskleisti jų problematiką, nagrinėjant atitinkamus dokumentus ir literatūros šaltinius.
2. Išnagrinėti ir įvertinti valstybių taikomas gerąsias praktikas ir silpnąsias vietas, numatant efektyviausius kibernetinių incidentų valdymo būdus.

3. Sukurti kibernetinio saugumo valdymo modelį užtikrinančius efektyvų kibernetinio saugumo valdymą, sistemų veiklos vientisumą ir efektyvumą.
4. Pateikti kritinės energetinės infrastruktūros kibernetinio saugumo valdymo modelio praktinio taikymo rekomendacijas.

Tyrimų metodika

Disertacijoje buvo taikyta lyginamoji analizė. Tyrime analizuojamos ypatingos svarbos energetikos infrastruktūros kibernetinės apsaugos strategijos, daugiausia dėmesio skiriant gairėms, valstybės strategijoms, teisės aktams, veikėjų strategijoms, tarptautiniams reglamentams, strateginiams dokumentams ir įvairių šalių gerajai praktikai, siekiant efektyvių sprendimų.

Ekspertiniai interviu su kritinės energetinės infrastruktūros ekspertais, tiesioginiais kritinės infrastruktūros operatoriais, Nacionalinio kibernetinio saugumo centro atstovais leido išskirti esmines kritinės energetikos infrastuktūros kibernetinio saugumo problemas bei nustatyti komponentų reikšmingumą. O paprastojo adityvaus svorių (angl. *Simple Additive Weighting Method* – SAW) metodo taikymas leido nustatyti komponentus, kuriuos labiau reikia tobulinti, siekiant pagerinti kritinės infrastruktūros saugumo lygį, ir surūšiuoti kibernetinio saugumo modelio komponentus pagal jų įgyvendinimo prioritetus.

Kuriant kritinės energetinės infrastruktūros kibernetinio saugumo modelį, vertinamos kritinės energetinės infrastruktūros kibernetinio saugumo modelio taikymo valstybėje galimybės, iššūkiai, spręstinos problemos. Atsižvelgiant į atliktą vertinimą, pasiūlyti modelio įgyvendinimo žingsniai.

Darbo mokslinis naujumas

Rengiant disertaciją buvo gauti šie nauji rezultatai, praplečiantys šiuolaikines vadybos teorijas, būtent besimokančios organizacijos koncepciją:

1. Atlikus dokumentų analizę bei ekspertinius interviu, įvertinus užsienio valstybėse taikomas gerąsias praktikas, sukurtas kibernetinio saugumo valdymo modelis, skirtas kokybės valdymui gerinti, taip išplečiant besimokančios organizacijos koncepcijos taikymą.
2. Išanalizavus egzistuojančias kritinės energetinės infrastruktūros kibernetinio saugumo strategijas, valstybių kibernetinį saugumą reglamentuojančius teisės aktus, atlikus ekspertų apklausą, sukurta metodika, kurioje taikomi pagrindiniai besimokančios organizacijos principai, siekiant

užtikrinti efektyvų kibernetinio saugumo valdymą, suformuoti bendrą plėtros strategiją ir efektyvų planavimą.

3. Saugumo problemoms ir rizikai spręsti pasiūlyta kibernetinio saugumo kokybės valdymo priemonė, užtikrinanti efektyvų kibernetinio saugumo sistemos vientisumą ir efektyvumą.

Darbo rezultatų praktinė reikšmė

1. Kibernetinio saugumo valdymo modelis, sudarytas iš organizacijos valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros organizacijoje, technologinio kibernetinio saugumo, rizikos valdymo, kibernetinių incidentų valdymo ir strateginio valdymo komponentų, padeda bet kuriai valstybei pasiekti efektyvų valdymą.
2. Kibernetinio saugumo valdymo modelio taikymas sudaro sąlygas pagerinti ir tobulinti kritinės energetinės infrastruktūros kibernetinį saugumą, sąveikaujant valdymo komponentams ir techninio valdymo sistemos įgyvendinimo galimybėms.
3. Sukurta kibernetinio saugumo valdymo modelio naudojimo metodika, susidedanti iš nuoseklių veiksmų, yra pagalbinė modelio priemonė, kuri kartu su pačiu modeliu sudaro sąlygas užtikrinanti efektyvų valstybių kritinės energetikos infrastruktūros kibernetinį saugumą.

Ginamieji teiginiai

1. Kibernetinio saugumo šešių komponentų (teisinis reguliavimas; organizacijos valdymas; rizikos valdymas; kibernetinio saugumo kultūra; technologijų valdymas; kibernetinių incidentų valdymas) valdymo modelio nepakanka kritinės energetinės infrastruktūros kibernetinio saugumo efektyviam valdymui, todėl jį reikia papildyti strateginio valdymo komponentu.
2. Sukurtas kibernetinio saugumo valdymo modelis, sudarytas iš organizacijos valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio kibernetinio saugumo, rizikos valdymo, kibernetinių incidentų valdymo ir strateginio valdymo komponentų, yra universalus bet kuriai kritinei energetinei infrastruktūrai.

3. Sukurta kibernetinio saugumo valdymo modelio taikymo metodika tinkama praktiniam naudojimui bet kurioje kritinėje energetinėje infrastruktūroje, gerinant ir tobulinant kibernetinį saugumą.

Darbo rezultatų aprobavimas

Disertacijos tema yra paskelbti du moksliniai straipsniai, įtraukti į *Clarivate Analytics Web of Science* ir *Scopus* duomenų bazes, bei šeši – į kitų tarptautinių duomenų bazių leidinius bei recenzuojamus mokslo žurnalus (Limba et al., 2017; Plėta, Karasov & Jakštas, 2019; Plėta, Tvaronavičienė & Della Casa, 2020; Plėta, Tvaronavičienė, Della Casa & Agafonov, 2020; Tvaronaviciene, Plėta, Semaskaitė, Paulauskienė & Vaiciutė, 2020; Tvaronavičienė, Plėta, Della Casa & Latvys, 2020; Tvaronavičienė, Plėta & Della Casa, 2021; Tvaronavičienė, Plėta, Beretas & Lelešienė, 2022).

Disertacijoje atliktų tyrimų rezultatai buvo paskelbti tarptautinėse mokslinėse konferencijose ir seminaruose Lietuvoje ir užsienyje:

- Tarptautinėje mokslinėje konferencijoje Contemporary Issues on Business, Management and Economics Engineering 2021 m. Vilniuje, Lietuva.
- Tarptautinėje mokslinėje konferencijoje „Komunikacijos ir informacijos mokslai tinklaveikos visuomenėje: patirtys ir įžvalga IV“ 2018 m. Vilniuje, Lietuva.
- XII tarptautinėje mokslinėje konferencijoje Transport Problems (TP`2020) 2020 m. Katovicuose, Lenkijoje.
- Moksliniame seminare 2022 m. Daugpilyje, Latvijoje.

Disertacijoje atliktų tyrimų rezultatai buvo aprobuoti, dalyvaujant 2022 m. NATO projekte „Informacijos saugumo operacijų centrų (SOC) steigimo įmonėse, turinčiose kritinę energetikos infrastruktūrą, preliminari techninė analizė“ (angl. *Preliminary Technical Analysis of the Establishment of Information Security Operations Centres* (SOC) *in Companies with Critical Energy Infrastructure*) ir paskelbti *NATO Energy Security Centre of Excellence* publikacijoje.

Disertacijos struktūra

Disertaciją sudaro: įvadas, trys skyriai, bendrosios išvados, literatūros šaltinių sąrašas ir priedai. Darbo apimtis – 130 puslapiai be literatūros šaltinių, santraukos anglų kalba, priedų ir autoriaus publikacijų sąrašo. Darbe pateikta 39 paveikslai ir 23 lentelės, panaudoti 180 literatūros šaltinių.

1

Kritinės energetikos infrastruktūros kibernetinio saugumo valdymo nagrinėjimas

Šiame skyriuje analizuojami kibernetinio saugumo ir kritinės infrastruktūros apibrėžimai, jų valdymo aspektai, spragos ir aktualumas kritinei energetinei infrastruktūrai. Nagrinėjamos naujos informacinės technologijos ir problemos, susijusios su kibernetiniu saugumu.

Skyriaus tematika paskelbtos dvi publikacijos (Limba et al., 2017; Plėta et al., 2019).

1.1. Kritinės energetikos infrastruktūros kibernetinio saugumo samprata ir aktualumas

Šiuolaikinis pasaulis aktyviai naudoja informacines technologijas ir virtualią erdvę, kurioje viskas realu, įskaitant nusikalstamumą. Elektroniniai nusikaltimai kelia grėsmę ne tik nacionaliniu, bet ir pasauliniu mastu. Šiuolaikiniai įsilaužėliai – tai didelės organizuotos nusikalstamumo grupės, dirbančios su aukštos kvalifikacijos programuotojais, kurie nuolat kuria naujas grėsmes. Didžiulis kiekis svarbių duomenų,

kuriuos galima pavogti arba sunaikinti, tapo viena iš priežasčių, dėl kurios kibernetinis saugumas tapo būtinas ne tik valstybei, bet ir privačiam sektoriui.

Pastaraisiais metais sąvoka „kibernetinis saugumas“ plačiai vartojama praktikoje ir politikoje, tačiau ši sąvoka suprantama skirtingai ir supratimas skiriasi priklausomai nuo konteksto. Norint geriau suprasti kibernetinio saugumo apimtį, kontekstą ir jų svarbą, nagrinėjant literatūros šaltinius, gaires ir strategijas bei įvairių kibernetinio saugumo organizacijų pateiktas koncepcijas, reikia nustatyti pagrindinės sąvokos „kibernetinis saugumas“ apibrėžimus (1.1 lentelė) ir kategorijas priklausomai nuo saugomos srities (1.2 lentelė).

1.1 lentelė. Kibernetinio saugumo sąvokos (sudaryta autoriaus)
Table 1.1. Concepts of cyber security (created by the author)

Aprašymas	Šaltinis
Veiksmai, kurių imamasi norint apsaugoti kibernetinę aplinką ir užtikrinti informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą.	(Lietuvos Respublikos Vidaus reikalų ministerija. Rizikos analizės vadovas, 2005)
Požiūris ir veikla, susijusi su saugumo rizikos valdymo procesais, kurių laikosi organizacijos ir vyriausybės, siekdamos apsaugoti elektroninėje erdvėje naudojamų duomenų ir turto konfidencialumą, vientisumą ir prieinamumą. Vizija apima gaires, politiką ir apsaugos priemonių, technologijų, įrankių ir mokymų rinkinius, kad būtų galima geriausiai apsaugoti kibernetinės aplinkos būklę ir jos vartotojus.	Schatz et al., 2017
Menas, skirtas apsaugoti tinklus, įrenginius ir duomenis nuo neteisėtos prieigos arba nusikalstamo naudojimo, ir praktika užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą.	(Cybersecurity & infrastructure security agency, 2021)
Kompiuterių saugumas, dar vadinamas kibernetiniu saugumu, kompiuterinių sistemų ir informacijos apsauga nuo žalos, vagystės ir neteisėto naudojimo.	*Computer security	Definition & Facts	Britannica* (2022), www.britannica.com
Teisinių, organizacinių ir techninių informacinių sklaidos priemonių, skirtų aptikti, analizuoti ir reaguoti į kibernetinius incidentus, pastariesiems išvengti, o įvykus – atkurti įprastinę elektroninių ryšių tinklų, informacinių ar pramoninių procesų valdymo sistemų veiklą, visuma.	Visuotinė Lietuvos enciklopedija, 2022
Įrankių, politikos, saugumo koncepcijų, saugos priemonių, gairių, rizikos valdymo metodų, veiksmų, mokymų, geriausios praktikos, technologijų, kurios gali būti naudojamos kibernetinei aplinkai, organizacijai ir turtui apsaugoti, rinkinys.	Integrated Country Strategy. South Africa. For Public Release, 2022)

1.2 lentelė. Kibernetinio saugumo kategorijos (sudaryta autoriaus)
Table 1.2. Cyber security categories (created by the author)

Kategorijų pavadinimas	Aprašymas	Šaltinis
Tinklo saugumas	kompiuterių tinklo apsauga nuo įsibrovėlių, nesvarbu, ar tai būtų užpuolikai, ar kenkėjiškos programos;	Securing Networks, 2023
Programinės įrangos saugumas	skirta programinės įrangos ir įrenginių apsaugai nuo grėsmių. Pažeista programinė įranga gali suteikti prieigą prie duomenų, kuriems ji skirta apsaugoti. Sėkmingas saugumas prasideda projektavimo metu, prieš diegiant programą ar įrangą;	Secure Software..., 2024
Informacijos saugumas	saugomas duomenų vientisumas ir konfidencialumas perdavimo bei saugojimo metu;	Cybersecurity Framework, 2023
Operacinis saugumas	procesų ir sprendimų, susijusių su informaciniais ištekliais ir jų saugumu, visuma (vartotojai, turintys prieigą prie tinklo, teisės ir procedūros, nustatančios, kaip ir kur galima saugoti ar bendrinti duomenis);	Operations security (OPSEC), 2023
Atsarginių kopijų kūrimas ir veiklos tęstinumas	ši funkcija nustato, kaip organizacija reaguoja į kibernetinį išpuolį ar bet kokį kitą įvykį, dėl kurio prarandami duomenys. Atsarginių kopijų atkūrimo politika apibrėžia, kaip organizacija atgauna savo operacijas ir informaciją, grįždama į tą patį pajėgumą, kuris buvo prieš incidentą. Verslo tęstinumas yra planas, kurio imasi organizacija, bandydama veikti be tam tikrų išteklių arba bandydama juos atkurti;	CRR Supplemental Resource Guide, 2022
Vartotojų mokymas	skirtas labiausiai nenuspėjamam kibernetinio saugumo faktoriui: žmogiškajam resursui. Kiekvienas asmuo gali netyčia įrašyti virusą į saugomą sistemą, nesilaikydamas tinkamų saugumo taisyklių. Kaip ištrinti įtartinus el. pašto priedus, vengti prijungti neatpažintas USB laikmenas ir įvairios kitos reikšmingos pamokos yra gyvybiškai svarbios bet kurios organizacijos saugumui	Wilson & Hash, 2003

Išanalizavus egzistuojančias kibernetinio saugumo sąvokas, sampratas ir kategorijas, galima pastebėti, kad pagrindiniai jų principai yra vienodi – apsaugoti kibernetinę aplinką nuo išpuolių, kurie tapo „nauju, moderniu pavojingu ginklu,

galinčiu paralyžiuoti ne tik atskirų įstaigų, gamybos, prekybos, transporto, ryšių, elektros, vandens tiekimo įmonių, bet net ir valstybių veiklą“ (Telksnys, 2016).

Apibendrinant kibernetinio saugumo sąvokas, jį galima apibūdinti kaip saugumo priemonių, strategijų, saugumo koncepcijų, rizikos valdymo metodų, veiksmų, mokymų, geriausiosios praktikos ir technologijų visumą, kurią galima naudoti siekiant apsaugoti kibernetinę aplinką.

Kibernetinis saugumas yra pasaulinė problema, kelianti grėsmę ne tik asmens saugumui, bet ir didelėms tarptautinėms įmonėms bei valstybei. Valdžios įstaigos, bankų sektorius, viešosios ir privačios tarnybos, atominės elektrinės, elektros tinklų operatoriai, vandens tiekėjai ar nuotekų valymo įmonės kasdien naudojasi ryšių ir informacinėmis technologijomis bei sistemomis, todėl yra visiškai priklausomi nuo kibernetinio saugumo. Kasmet viešasis ir privatusis sektorius išleidžia milijonus eurų technologijoms, programinei ir aparatinei įrangai, kad pagerintų kibernetinį saugumą, tačiau kibernetinis saugumas vis dar yra pažeidžiamas.

Pagrindinė problema yra ta, kad kibernetinis saugumas yra vertinamas tik iš techninės pusės. Šį požiūrį reikia keisti, nes kibernetinis saugumas yra ne technologija, o sudėtingas ir sisteminis organizmas, susidedantis iš fizinių, virtualių sistemų bei priemonių, turinčių įtakos visoms gyvenimo sritims, ypač kritinei infrastruktūrai.

Kritinė infrastruktūra plačiai aprašyta mokslinėje literatūroje. Lenkijoje kritinė infrastruktūra apibrėžta kaip valstybių ir jų piliečių saugumui būtinos sistemos, tarpusavyje susiję objektai, įranga, įrenginiai ir paslaugos, užtikrinančios efektyvų viešojo administravimo, įstaigų ir įmonių funkcionavimą (Wiśniewski, 2020). Sonesson et al. (2021) straipsnyje apie kritinės infrastruktūros valdymą rašo, kad kritinė infrastruktūra – tai transporto, energetikos ir telekomunikacijos sistemos, skirtos paslaugoms teikti ir reikalingos visuomenės funkcionavimui palaikyti (Sonesson et al., 2021).

Europos Sąjungos direktyvoje 2008/114/EC nuo 2008 m. gruodžio 8 d. parašyta, kad Europos ypač svarbi infrastruktūra yra kritinė infrastruktūra, kuri yra ES narių valstybių teritorijoje, ir jos sutrikdymas ar sunaikinimas turėtų didelį poveikį bent dvejoms ES valstybėms. Šio poveikio reikšmingumas turi būti vertinamas atsižvelgiant į kompleksinius kriterijus, kurie apima įvairių sektorių priklausomybes nuo kitų sektorių. Europos kritinei infrastruktūrai priklauso elektros energija, nafta ir dujos. NATO Energetinio saugumo kompetencijos centras pristatyme apie grėsmes energetiniam saugumui pateikė Europos Sąjungos, Vokietijos, Norvegijos, Jungtinės Karalystės bei Šveicarijos kritinės infrastruktūros apibrėžimus, atsižvelgiant į šalių nacionalinius dokumentus (Tarybos direktyva 2008/114/EC, 2008).

Vokietijos nacionalinės kritinės infrastruktūros apsaugos strategijoje teigiama, kad kritinė infrastruktūra – tai organizaciniai ir fiziniai statiniai bei įrenginiai, kurie yra gyvybiškai svarbūs visuomenei ir ekonomikai, nes įvykusi avarija

ar sutrikimas lemtų ilgalaikius energijos tiekimo trūkumus, reikšmingus apribojimus visuomenės saugumui ar sukeltų kitų dramatiškų pasekmių.

Norvegijos kritinės infrastruktūros objektai yra tie statiniai ir sistemos, kurios yra būtinos, siekiant išlaikyti visuomenės kritines funkcijas, kurios privalo būti laiku apsaugotos siekiant patenkinti visuomenės pagrindinius poreikius ir sukurti saugumo jausmą plačiajai visuomenei.

Jungtinės Karalystės Vyriausybė apibrėžia nacionalinę infrastruktūrą kaip „įrenginių, sistemų, svetainių bei kompiterinių tinklų, reikalingų valstybės funkcionavimui ir esminių paslaugų teikimui, nuo kurių priklauso Jungtinės Karalystės kasdieninis gyvenimas“. Šios šalies nacionalinę infrastruktūrą sudaro devyni sektoriai, tarp kurių yra ir energetika.

Šveicarijoje kritinės infrastruktūros objektai yra infrastruktūra, kurios sutrikdymas, sugadinimas arba sunaikinimas turėtų rimtą poveikį visuomenės funkcionavimui, ekonomikai ar valstybei. Šioje šalyje kritinę infrastruktūrą sudaro trys lygmenys:

- sektorius: energetikos, finansinių paslaugų, visuomenės sveikatos;
- subsektoriai: elektros energijos, naftos ir gamtinių dujų tiekimo;
- individualūs objektai / elementai: siurbliai, vamzdynai, užtvankos, aukštosios įtampos linijos, kontrolės sistemos (Smaliukas, 2015).

Lietuvos Respublikos Vyriausybė savo nutarime dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo kritinę infrastruktūrą apibrėžė taip: „ypatingos svarbos infrastruktūros objektas (toliau – YSI objektas) – institucija ar jos struktūrinis padalinys, įmonė, įrenginys ar įrenginio dalis, nepaisant to, ar jo valdytojas yra privatus ar viešojo administravimo subjektas, teikiantis ypatingos svarbos paslaugas, kurio neveikimas ar veiklos sutrikdymas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams“ (Lietuvos respublikos vyriausybė nutarimas ... Nr. 742, 2016).

Galima pastebėti, kad įvairių valstybių požiūris į kritinę infrastruktūrą priklauso nuo skirtingų poreikių ir sąlygų, nacionalinio konteksto. Vienintelis bendras dalykas, kuris būdingas skirtingų valstybių požiūriui į kritinę infrastruktūrą, yra poveikis, kuris gali būti padarytas dėl kritinės infrastruktūros sunaikinimo arba sutrikdymo, nacionaliniam saugumui, valstybės ekonomikai ir visuomenei.

Analizuojant įvairių valstybių požiūrį į kritinę infrastruktūrą, galima pastebėti, kad energetikos sektorius yra neatsiejama kritinės infrastruktūros dalis.

Galima pastebėti, kad energetikos sektorius yra vienas iš sudedamųjų dalykų, nuo kurių priklauso ne tik valstybės ekonomika, bet ir saugumas. Bet koks šio elemento sutrikdymas arba sunaikinimas, ir nesvarbu, ar fizinis, ar kenkėjiškų programų užpuolimas, turėtų didelę įtaką bet kurios valstybės saugumui.

Nacionalinis kibernetinio saugumo centras (NKSC) kiekvienais metais kibernetinio saugumo ataskaitoje pateikia statistinius duomenis apie išpuolius Lietuvoje. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) 2017 m. ištyrė 54 414 incidentų, gautų iš skirtingų paslaugų tiekėjų, interneto naudotojų ir užsienio saugumo incidentų tyrimo tarnybų, atliekančių tarptautinius incidentų tyrimus (Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT), 2017 metų veiklos ataskaita). 1.3 lentelėje pateikti duomenys apie kibernetinius išpuolius, suskirstytus pagal tipus bei pateikiamas incidentų kiekis už kiekvieną ketvirtį.

1.3 lentelė. CERT-LT 2017 Incidentų ataskaitą (sudaryta autoriaus remiantis CERT-LT 2017 m. ataskaita)
Table 1.3. CERT-LT 2017 incidents report, (created by the author based on CERT-LT report, 2017)

Apdorotų pranešimų tipai	2017 m.				
	I ketv.	II ketv.	III ketv.	IV ketv.	Iš viso
Apie kenkimo programinę įrangą	2580	2755	2898	2606	10 839
Apie informacinių sistemų užvaldymą	2962	2775	2704	2510	10 951
Apie el. paslaugos trikdymo atakas	12	7	11	20	50
Apie el. duomenų klastojimą	340	376	257	264	1237
Apie vientisumo pažeidimus	2	7	4	2	15
Apie įrenginių saugumo spragas	5848	5938	6464	6362	24 612
Įvairaus pobūdžio	2899	1672	943	1196	6710

Statistinių duomenų analizė parodė, kad Lietuvoje didžiausios kibernetinės problemos – kenkėjiška programinė įranga ir nesaugios informacinės sistemos, kurios papildo viena kitą bei padidina išpuolių riziką. Šiais atvejais toks nesaugumas leidžia platinti kenkėjišką programinę įrangą, skenuojant ir atakuojant informacines sistemas, renkant informaciją, valdant įrenginius ir t. t. Kiekvienais metais, kaip parodė statistika, kibernetinių išpuolių skaičius tik didėja. 2019 m., pagal Nacionalinio kibernetinio saugumo centro duomenis, ryšių ir informacinių sistemų kibernetinių grėsmių buvo užfiksuota 199 828, o išpuolių, naudojant kenkimo programinę įrangą, – 68 562. Daugiausiai incidentų buvo užfiksuota „ypatingos svarbos paslaugas teikiančių kibernetinio saugumo subjektų“ (Nacionalinis kibernetinio saugumo centras, 2020) (1.1 pav.).

1.1 pav. Informacija apie kibernetinius incidentus pagal ypatingos svarbos paslaugų sektorius (sudaryta autoriaus remiantis 2018 metų Nacionalinio kibernetinio saugumo būklės ataskaita, 2019)
Fig. 1.1. Information on the cyber incidents according to critical service sectors (compiled by the author based on the 2018 State of Cyber Security Report, 2019)

Kaip jau buvo minėta, yra daug sąvokų, apibūdinančių kritinę infrastruktūrą. Kritinės infrastruktūros terminas vartojamas apibūdinant visuomenei ir ekonomikai reikalingą turtą – infrastruktūrą, kurią dažniausiai sudaro šildymas, žemės ūkis, maisto gamyba, vandens tiekimas, visuomenės sveikata, transporto sistemos, apsaugos tarnybos, elektros gamyba, perdavimas ir paskirstymas, atsinaujinančiųjų išteklių energija (saulės šviesa, vėjas, lietus, potvyniai, bangos ir geoterminė šiluma), telekomunikacijos, ekonomikos sektorius, prekės ir finansinės bei kitokios paslaugos. 1996 m. Jungtinės Amerikos Valstijos prezidentas išleido įsakymą, kuriame išvardyti septyni kritinės Jungtinės Amerikos Valstijos (JAV) infrastruktūros objektai (Johnson, 2015): elektros tinklai, dujotiekiai, naftotiekiai, vandens tiekimo sistemos, transportas ir telekomunikacijos. Vieno ar kelių iš jų sutrikdymas turėtų pražūtingų padarinių kitiems, likusiems gyvybiškai svarbiems infrastruktūros objektams.

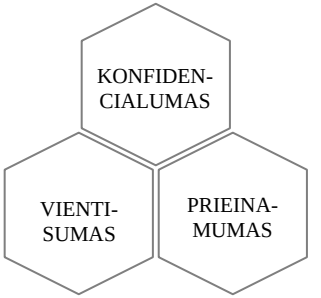
Reikia pabrėžti, kad šiandien kibernetinis saugumas nėra tik techninė sfera. Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinis saugumas apibrėžiamas kaip teisinės, informacinės, organizacinės ir techninės apsaugos priemonės, reikalingos aptikti, išanalizuoti ir reaguoti į kibernetinius incidentus, kurie apibūdinami kaip įvykis ar veikla, leidžianti:

- suteikti nesankcionuotą prieigą prie ryšių ir informacijos sistemų, elektroninių ryšių tinklų ar pramoninių procesų valdymo sistemų;
- sutrikdyti ar pakeisti informacines sistemas, įskaitant valdymo operacijų perėmimą;

- įdiegti elektroninių ryšių tinklų ar pramoninio proceso valdymo operacijas, skirtas sunaikinti, sugadinti, ištrinti ar modifikuoti elektroninę informaciją, panaikinti ar apriboti prieigą prie elektroninės informacijos, taip pat sudaryti galimybes neįgaliotiems asmenims įsisavinti ar kitaip naudoti neviešą informaciją elektroniniu formatu (Lietuvos respublikos kibernetinio saugumo įstatymas Nr. XII-1428, 2014; Limba et al., 2017).

Remiantis patvirtintomis kibernetinio saugumo ir kibernetinių incidentų sąvokomis, galima nustatyti pagrindinius kibernetinio saugumo tikslus, kurie užtikrina saugumą (1.2 pav.).

Išvardinti tikslai yra pagrindiniai informacijos saugumo principai, skirti užtikrinti, kad organizacija galėtų apsaugoti savo duomenis, sistemas ir resursus nuo neleistino naudojimo ar prieigos.



1.2 pav. Pagrindiniai kibernetinio saugumo tikslai (sudaryta autoriaus remiantis NKSC duomenimis, 2020)
Fig. 1.2. Key Cybersecurity Goals (created by the author based on the data of NCDC, 2020)

Teisiniai aspektai aiškiai parodo, kad kibernetinis saugumas ir valdymas yra glaudžiai susiję ir labai svarbūs kiekvienai organizacijai. Norint užtikrinti kritinės infrastruktūros saugumą, reikia pripažinti, kad kibernetinis saugumas yra toks pat svarbus, kaip ir fizinis (Ten et al., 2010).

Kiekvienais metais komercinės kompanijos ir tyrėjai analizuoja kibernetinio saugumo priemones, teikia ataskaitas savo svetainėse, publikuoja tyrimo rezultatus žurnaluose arba pristato juos konferencijose. Pagal *Cybercrime magazine* žurnalo duomenis, iki 2020 m. įsilaužėlių skaičius išaugo iki 6 milijonų. Nuo 1982 iki 2018 m. užregistruoti 268 incidentai, iš kurių 147 išpuoliai ir 121 saugumo incidentas (Ahmadian et al., 2020).

Vytautas Butrimas, Lietuvos nacionalinio saugumo ministerijos vyriausiasis kibernetinio saugumo administratorius, ir Audrius Brūzga, Lietuvos užsienio reikalų ministerijos energetinio saugumo centro direktorius, savo straipsnyje bandė atsakyti į pagrindinius klausimus apie kibernetinio saugumo valdymo aspektus

kritinėje infrastruktūroje, analizuojant tarptautinių ekspertų išvadas apie tirtas valdymo sistemas Lietuvos sektoriuje (elektros tinklo operatoriai LITGRID ir LESTO, nacionalinis gamtinių dujų operatorius „Lietuvos dujos“ ir Technologijų ir inovacijų centras) (Butrimas, 2012). Toks tyrimas atskleidė kibernetinės saugos valdymo nebuvimą kritinėje infrastruktūroje.

Kibernetinio saugumo rinkoje atsirado priemonių ir techninių standartų, skirtų kibernetiniam saugumui sustiprinti. Per pastaruosius du dešimtmečius labai domėtasi universaliomis, hibridinėmis saugumo priemonėmis, siekiant apsaugoti kritinę infrastruktūrą.

Kbernetinio saugumo svarba auga dėl greitai plintančių komunikacijos ir informacinių technologijų, patogesnio ir efektyvesnio paslaugų teikimo grėsmių (Limba et al., 2017). Todėl kritinės infrastruktūros pažeidžiamumas atsiranda greitai, ir šis procesas daro įtaką nacionalinei bei pasaulinei sistemai.

Pagrindinė didėjančio pažeidžiamumo problema susijusi su sistemos ir integracijos proceso sudėtingumu. Mažų sistemos elementų arba mažų sistemų integravimas į didesnius vienetus padidina sistemos vientisumą ir kartu sukuria pažeidžiamumą. „<...> išaugo kibernetinių incidentų sudėtingumas, atakos tampa vis labiau rafinuotos, o jų ištirti automatizuotomis priemonėmis neįmanoma. Didžiausios kibernetinio saugumo grėsmės kyla dėl didelio skaičiaus prie interneto prijungtų nesaugių įrenginių, pažeidžiamų interneto svetainių ir piktavališkų socialinės inžinerijos metodų naudojimo“ (Žintelis, 2018).

Kiekviena šalis, kaip ir dauguma kibernetinio saugumo tyrėjų, sutinka, kad integruoto ir hibridinio kibernetinio saugumo valdymo modelis reikalingas tam, kad būtų apsaugoti kritinės infrastruktūros sektoriai / objektai (pavyzdžiui, interneto balsavimo ar bankų sistemos).

Pasauliniu mastu pripažįstama, kad reikia kruopščiai valdyti ir saugoti savo kritinius išteklius. Užfiksuotų ir užblokuotų kompiuterinių išpuolių statistika, kuri pateikta 1.4 lentelėje, rodo, kad kiekvienais metais didėja ne tik išpuolių skaičiai, bet ir jų sudėtingumo lygis.

1.4 lentelė. Išpuolių suskirstymas pagal rizikos lygį (sudaryta autoriaus remiantis 2022 metų Nacionalinė kibernetinio saugumo būklės ataskaita, 2023)
Table 1.4. Distribution of published vulnerabilities by risk level (created by the author based on (2022 metų Nacionalinė kibernetinio saugumo būklės ataskaita, 2023)

Metai	Išpuolių skaičius			
	9–10 (kritinis lygis)	7–8,9 (aukštas lygis)	4–6,9 (vidutinis lygis)	Iš viso
2019	–	–	–	3241
2020	1	67	4262	4330
2021	0	93	3995	4088
2022	0	33	4047	4080

NKSC duomenimis, 2020 m. kibernetinių incidentų, lyginant su ankstesniais metais, padaugėjo 25 proc., o incidentų, susijusių su kenkimo programine įranga, – 49 proc. 2021 m. buvo užfiksuoti 4088 kibernetiniai incidentai ir tai 5 proc. mažiau negu 2020 m., bet šių incidentų sudėtingumo lygis padidėjo. O tai reiškia, kad kibernetinių nusikaltėlių profesionalumas auga, keičiasi jų interesai, trūksta kibernetinio saugumo kultūros, nepakankamai dėmesio skiriama organizacijų bei valstybės kibernetiniam saugumui. Analizuojant kibernetinių incidentų duomenis galima pastebėti tokias tendencijas:

- padidėjęs išpuolių, padarančių didelę žalą, skaičius;
- daugiapakopių atakų sudėtingumo didinimas, taikant specialius apsaugos nuo galimo atsakomojo poveikio metodus;
- poveikis beveik visiems elektroniniams (skaitmeniniams) įrenginiams;
- vis daugiau išpuolių prieš dideles įmones, svarbiausius pramonės objektus ir net vyriausybinių institucijų kritines energetines infrastruktūras;
- kompiuterinių technologijų naudojimas kibernetinėms atakoms prieš kitas valstybes.

Tinkamo ryšių ir informacinių sistemų funkcionavimo užtikrinimas yra neatsiejama ypatingos svarbos informacinės infrastruktūros (YSII) valdytojų ir valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų darbo dalis (2020 metų veiklos ataskaita, 2021). Bet ne visada darbas atliekamas gerai, todėl kibernetinio saugumo reikalavimų įgyvendinimas vis dar lėtas procesas. Tai lemia ne tik aplaidus YSII valdytojų požiūris į reikalavimų įgyvendinimą, kompetentingų kibernetinio saugumo, informacinių technologijų specialistų ir (ar) reikalingos kompetencijos trūkumas, bet ir pačių informacinių sistemų bei registrų sudėtingumas, kurį, savo ruožtu, lemia nuolatinė IRT plėtra (Krašto apsaugos ministerija, 2020).

Vyriausybės ir organizacijos supranta, kad kritinės infrastruktūros saugumas reikalauja didelių pastangų, nes tai yra vienintelis būdas užtikrinti šalies ir jos gyventojų, naudojančių kritinės energetikos infrastruktūrą, gerovę (Lankauskienė & Tvaronavičienė, 2012). 2000 m. Jungtinės Amerikos Valstijos pabrėžė, kad kibernetinis saugumas turėtų būti valdomas holistiškai, o ne atskiroje valstybės informacinėje sistemoje (JAV GAO, 2007; Europos valstybė, 2008; NATO, 2010; Lietuvos nacionalinė saugumo strategija, 2012; Johnson, 2015).

Kibernetinio saugumo tyrimuose daugiausia dėmesio buvo skiriama techniniams sprendimams, kuriuos galima įgyvendinti naudojant pramonės sektoriaus stebėjimo ir duomenų kaupimo bei energijos tiekimo infrastruktūros stebėjimo ir valdymo sistemas (angl. *Supervisory control and data acquisition* (SCADA)). Stebėjimo ir valdymo sistemos saugumą sudaro keturi pagrindiniai elementai: stebėjimas realiuoju laiku, anomalijų nustatymas, poveikio analizė ir švelninimo strategijos (Ten et al., 2012). Dažniausiai kibernetinis saugumas analizuojamas technologiniu požiūriu, tačiau šiandien reikia platesnio ir išsamesnio požiūrio į kibernetinio saugumo modelį.

Bet kuriai valstybei kibernetinis saugumas yra rimtas iššūkis gynybai. Analizuojant 2007 m. Estijos incidentą, kai įsilaužėliai užpuolė privačią ir valstybinę elektroninę infrastruktūrą, Europos Sąjungos valstybės pradėjo galvoti apie kibernetinio saugumo strategijas ir bendradarbiavimą. O tai reiškia, kad, kuriant šalies kritinės infrastruktūros kibernetinio saugumo modelį, reikia dalyvauti ne tik valstybinėms įstaigoms, nacionalinėms reguliavimo institucijoms, bet ir privačiajam sektoriui (JAV energetikos departamentas ir JAV vidaus saugumo departamentas, 2006; Europos saugumo ir bendradarbiavimo organizacija, 2014). Taip yra todėl, kad pasaulinių tiekimo grandinių sutrikimas atneša milžiniškus finansinius nuostolius tiek verslui, tiek valstybei, sukeldamas pavojų žmonių sveikatai ar net gyvybei. Patikima ir saugi kritinė infrastruktūra yra gyvybiškai svarbi ekonomikos klestėjimui, nes ji ne tik palaiko efektyvų verslo ir paslaugų veikimą, bet ir skatina ilgalaikį pasitikėjimą, planavimą ir investicijų pritraukimą.

1.2. Kritinės energetinės infrastruktūros kibernetinio saugumo valdymo iššūkiai

Didėjanti informacinės visuomenės priklausomybė nuo informacinių ir ryšių sistemų ir kritinės infrastruktūros sistemų pažeidžiamumas sukuria silpnąsias vietas, kurias galima sąmoningai panaudoti siekiant nusilpninti ar net sunaikinti kritinę infrastruktūrą ar jos dalį. Kibernetinis incidentas prieš vyriausybę ar viešąsias sistemas tam tikromis aplinkybėmis gali turėti tokias pačias pasekmes, kaip ir išpuolis prieš kritinę energetinę infrastruktūrą.

Per pastaruosius dvidešimt metų pažanga informacinių technologijų srityje lėmė, kad mūsų gyvenime atsirado daug naujų išmaniųjų prietaisų, žinomų kaip daiktų internetas (angl. *Internet of Things* (IoT)), kurio apimtis svyruoja nuo išmaniųjų laikrodžių iki didelės infrastruktūros, tokios kaip vandens, elektros energijos, informacijos tiekimo, sveikatos, transporto, finansų paslaugos ir pan. IoT įrenginiai yra sujungti vienas su kitu, kad teiktų paslaugas, naudojant valdymo sistemas internetu, iš dalies atskiriant pagrindinių įrenginių valdymą nuo periferinių įrenginių valdymo. Tikimasi, kad 75 milijardai įrenginių bus prijungti prie daiktų interneto (Das & Gündüz, 2020), tačiau skaitmeninių valdymo sistemų integracija pramonėje bus vis labiau pažeidžiama kibernetinių atakų. Vien 2017–2018 m. „išorinių išpuolių“ skaičius padidėjo 9 procentais (Accenture Security, 2019), tad bet kuri sistema gali tapti kritine, pažeidžiamumas gali tapti grėsme, sukeliančia įvairius griaunamus padarinius socialinėms sistemoms, energetikai, saugumui, sveikatai ir kitoms visuomenės dalims.

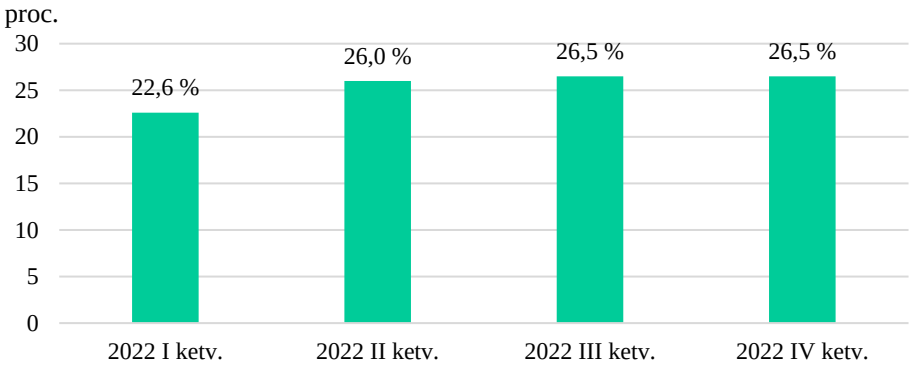
Daiktų interneto galimybės užtikrina saugų ir efektyvų duomenų perdavimą, sprendimų palaikymą ir bendrą komfortą, o tai yra patrauklu daugeliui įmonių. Prieš atsirandant naujai koncepcijai, technologinė kontrolė buvo padalinta į dvi

technologijas: informacinę (IT) ir operacinę (OT). Iš esmės IT yra naudojama informacijai saugoti, apdoroti ir perduoti, o OT – fizinei įrangai, pavyzdžiui, minėtoms stebėjimo ir valdymo sistemoms ir įterptosioms kompiuterinėms technologijoms (Inductive Automation, 2020). Tačiau, atsiradus daiktų internetui, pramonės organizacijos ir sistemų kūrėjai pateikė naują koncepciją – pramoninį daiktų internetą, kuriame OT ir IT sąveikauja toje pačioje aplinkoje. Šių technologijų sąveika vienoje aplinkoje padidina tikimybę tapti kibernetinių išpuolių taikiniu, nes strategijų, skirtų reaguoti į kibernetinius išpuolius prieš pramonines sistemas, parengimas vyksta lėčiau nei OT ir IT technologijų plėtra.

Pramonės valdymo sistema (angl. *Industrial Control System* (ICS)) – tai bendra sąvoka, apimanti paskirstytos valdymo, stebėjimo ir valdymo, pramonės automatines, pramonės automatikos ir valdymo sistemas bei kitas valdymo sistemas, tokias kaip programuojami loginiai valdikliai (angl. *programmable logic controller* (PLC)). Paskirstytos valdymo sistemos naudojamos duomenims apdoroti ir generuoti, o SCADA sistemos valdo paskirstymą. Dažniausiai pramonės valdymo sistemos būna naudojamos pramonės sektoriaus kritinėje infrastruktūroje, pavyzdžiui, atominėse ir šiluminėse elektrinėse, vandens valdymo įrenginiuose, energijos gamyboje ir energijos paskirstymo sistemose. Nors PVS ilgą laiką buvo izoliuota nuo interneto, technologijų plėtra ir verslo pažanga lėmė pramonės valdymo sistemų, interneto, informacinių technologijų ir debesų aplinkos konvergavimą. Toks sistemų ir technologijų derinys tapo didelių išpuolių taikiniu, jų pažeidimas gali padaryti fizinę žalą ir sukelti pavojų žmonių gyvybėms.

Pramonės valdymo sistema yra belaidžio tinklo ir valdymo komponentų (pvz., elektrinių, mechaninių, hidraulinių, pneumatinių) derinys, reikalingas įvairiems pramonėms tikslams pasiekti (pvz., gamybai, medžiagų ar energijos transportavimui). Paprastą ICS sudaro daugybė valdymo kontūrų, žmogaus ir mašinų sąsajų, nuotolinės diagnostikos bei priežiūros įrankių, naudojančių daug tinklo protokolų. Siekiant padidinti atsparumą išorinėms grėsmėms, tokioms kaip kenksmingas kodas, vadinamieji „oro“ tinklai yra fiziškai izoliuoti nuo neapsaugotų tinklų, tačiau bet kuris tinklo terminalas gali būti užkrėstas įterpiant USB atmintinę su kenkėjišku kodu, kuris paveiks visą sistemą (1.3 pav.).

Pramonės valdymo sistemų priklausomybės nuo daiktų interneto plėtojimas kelia didelę potencialią riziką, ypač kritinei infrastruktūrai. Taigi nuo 2017 iki 2018 m. kibernetinių išpuolių skaičius padidėjo 11 %, o nuo 2013 m. – 67 % (Accenture Security, 2019). Vis daugėja kibernetinių išpuolių tokiose operacijų technologijų srityse, kaip vandens sistemos, elektrinės, transporto, ryšių, gamybos ir kitos kritinės infrastruktūros. Dėl šios priežasties kritinės infrastruktūros apsauga pasaulinėje pramonės aplinkoje tampa vis svarbesnė (1.4 pav.). Kibernetiniai išpuoliai prieš ICS gali turėti poveikį gyventojų sveikatai ar gyvybei.

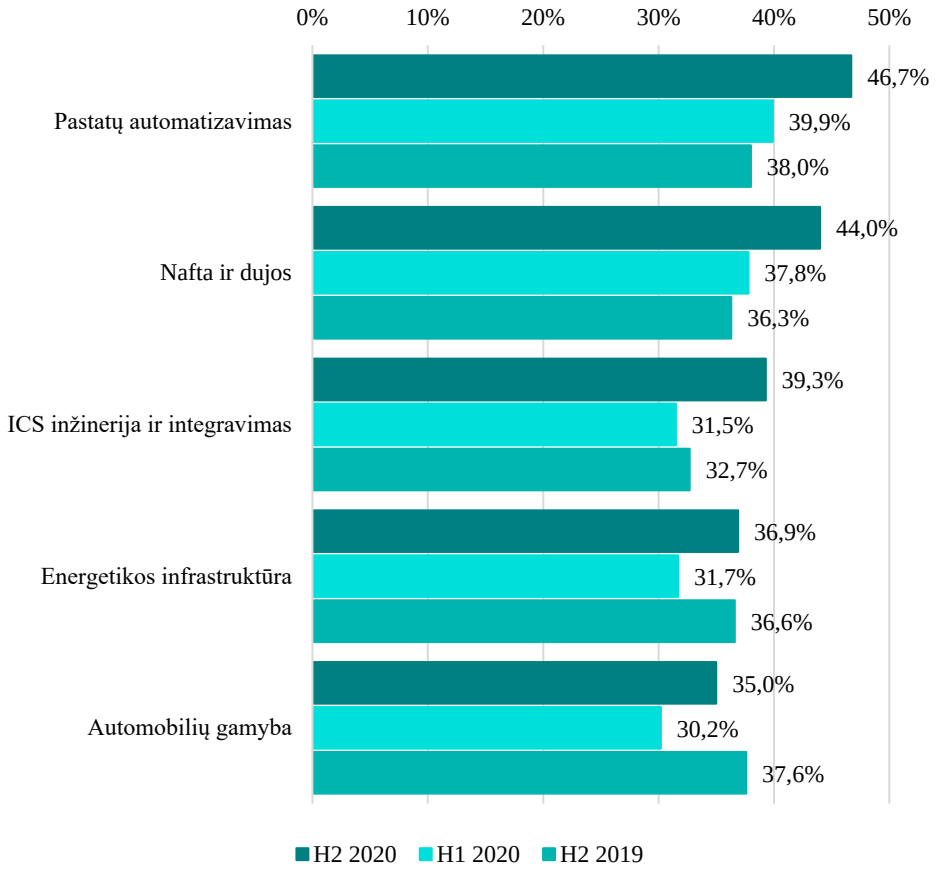


1.3 pav. Nustatytų išpuolių skaičius įvairiuose ICS komponentuose už 2022 m. (sudaryta remiantis Grėsmių aplinkos pramoninių automatizavimo sistemų atžvilgiu, 2023 duomenimis)
Fig. 1.3. Number of identified attacks in various ICS components for 2022 (based on the Threat landscape for industrial automation systems, 2023 data)

ICS yra vienos iš svarbiausių, kontroliuojant kritinę energetinę infrastruktūrą. Todėl labai svarbu stebėti ir analizuoti išpuolius prieš tokias sistemas, kad būtų išvengta būsimų išpuolių ir nustatytos grėsmės saugumui. Įvairi grėsmių ir atakų klasifikacija leidžia nustatyti jų šaltinį ir parametrus, kad būtų galima efektyviau apskaičiuoti naudingus rodiklius, tokius kaip rizikos.

Butrimas (2019) savo straipsnyje apie kylančias naujas kibernetines grėsmes ypatingos svarbos energetikos infrastruktūros objektams rašė, kad pramoninių valdymo ir saugos sistemų paskirtis – užtikrinti, kad fiziniai procesai pramonės įmonėse, elektros energijos gamybos objektuose ir kituose ypatingos svarbos infrastruktūros segmentuose, vyktų nustatytuose komponentuose, užkertant kelią brangios įrangos gedimams bei neigiamam poveikiui aplinkai ir žmonėms. Šių sistemų gedimai, nepriklausomai nuo to, ar gedimai buvo tyčiniai, ar ne, kelia didžiulę grėsmę ir gali ne tik sugadinti nuosavybę, bet ir atimti žmonių gyvybes (Butrimas, 2019).

Pagal Nacionalinio kibernetinio saugumo centro 2018 m. ataskaitos išvadas ir rekomendacijas, kurias pateikė profesorius Gintautas Žintelis, Lietuvos mokslų akademijos Technikos mokslų skyriaus pirmininkas, žurnale „Apžvalga“ 2019 m., „ypatingos svarbos informacinė infrastruktūra yra aktyvios kibernetinės veiklos objektas. 2018 m. daugiausiai kenkimo PĮ aptikta valstybės valdymo (iš viso 39 proc.), energetikos (20 proc.) ir užsienio reikalų ir saugumo politikos (19 proc.) sektoriuose. 2019 m. 18 proc. išaugo elektroninių ryšių tinklų žvalgymo (skenavimo) veikla, kuomet ypač buvo domimasi energetikos, valstybės valdymo ir krašto apsaugos sektoriais“ (Žintelis, 2019).



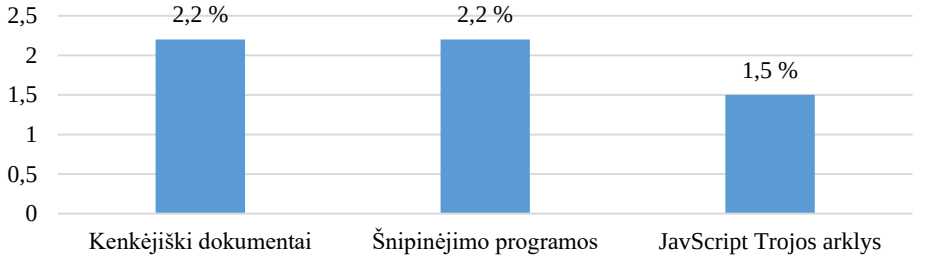
1.4 pav. ICS kompiuterių, kuriuose buvo užblokuota kenkėjiškų programų, procentai (sudaryta remiantis Grėsmių aplinkos pramoninių automatizavimo sistemų atžvilgiu, 2023 duomenimis)

Fig. 1.4. Percentage of ICS computers on which malware was blocked by industry (based on the Threat landscape for industrial automation systems, 2023 data)

Kibernetinių išpuolių atveju saugumą užtikrina teisingas reagavimo procesas, kurį galima suskirstyti į tris etapus: prieš išpuolį, jo metu ir po jo. Kiekviename etape pagrindinis tikslas yra užtikrinti saugią aplinką keitimuisi konfidencialiais duomenimis ir galimybę atkurti sistemą, jei dėl išorinių ar vidinių veiksnių ji buvo pažeista. Norint sukurti veiksmingą kibernetinio saugumo pažeidimų prevencijos metodą, būtina kiekviename įrenginyje įdiegti šiuolaikines užkardas ir antivirusi-

nes programas, nes senos sistemos yra labiausiai pažeidžiamos (Ryder, 2019). Kitas veiksmingas elementas, kuriuo įmonė turi pasikliauti kibernetinių išpuolių atveju, yra atsarginės kopijos: daugelis įmonių neturi standartizuotos kibernetinio saugumo rizikos vertinimo metrikos; taigi įmonės neturi žinių apie kibernetinio saugumo rizikos vertinimo metrikos įprastą elgesį (ISACA, 2019). Daugumoje valdymo strategijų taikomas tas pats požiūris, išskyrus kai kuriuos ypatumus: paprastai skiriamas modelis „didelė įmonė prieš mažą“.

Kibernetinius išpuolius galima suskirstyti į penkias grupes pagal užpuoliko tikslus: informacijos sugadinimas, paslaugų trikdymas (angl. *Denial – of – service attack* (DoS)), informacijos atskleidimas, išteklių vagystės ir fizinis sunaikinimas (Limba et al., 2017). Tačiau dažniausi kibernetiniai užpuolimai yra socialinės inžinerijos sukčiavimo forma, t. y. siunčiami elektroniniai laiškai, kuriuose prašoma konfidencialios informacijos, ir programos, reikalaujančios išpirkos už pavogtų konfidencialių duomenų atkūrimą, ar kenkėjiško kodo programa, suteikianti valdymo teises įsilaužėliams (1.5 pav.). Kitas pavyzdys yra robotų tinklų diegimas arba tiekimo grandinės sutrikimas dėl tiesioginės atakos prieš įrangą (CESG, 2016).



1.5 pav. Užblokuotų užpuolimų, siunčiamų elektroniniu paštu, procentinė dalis Europos kritinėje energetinėje infrastruktūroje už I ketvirtį 2020 m. (sudaryta remiantis Securelist.com duomenimis)

Fig. 1.5. Blocked attacks sent by email, the percentage of European critical energy infrastructure for the first quarter of 2020 (based on securelist.com data)

Analizuojant kritinės energetinės infrastruktūros saugumą, reikia atsižvelgti į išteklių tipą, ar tai iškastinis kuras, ar elektros gamybos tinklas, kurį sudaro branduolinė, geoterminė, hidroenergijos elektrinės, vėjo turbinos ir tiesioginiai saulės spinduliai (Blume, 2007). Elektros sistemų pažeidžiamumas priklauso nuo jų dinaminių infrastruktūrinių sistemų, kurios paprastai yra daugiasluoksnės (Amin, 2010). Dėl kibernetinių išpuolių energetinėje infrastruktūroje reikia skubesnės reakcijos skirtingais lygmenimis, nes vienos sistemos dalies gedimo pasekmės kelia

potencialią riziką žmogaus gyvybei, aplinkai ir verslui. Pastaraisiais metais pastebima centralizuoto elektros sistemų valdymo perėmimo ir sugadinimo tendencija. Keletas išpuolių, įvykdytų elektros tinkluose, rodo, kaip įsilaužėliams tapo lengva valdyti sąsajas ir siųsti užklausas mechaniniams komponentams, tokiems kaip jungikliai ir jungtys, sustabdyti elektros srautą gamykloje, sukeliant elektros tiekimo sutrikimus ar sprogimus (Kshetri, 2017).

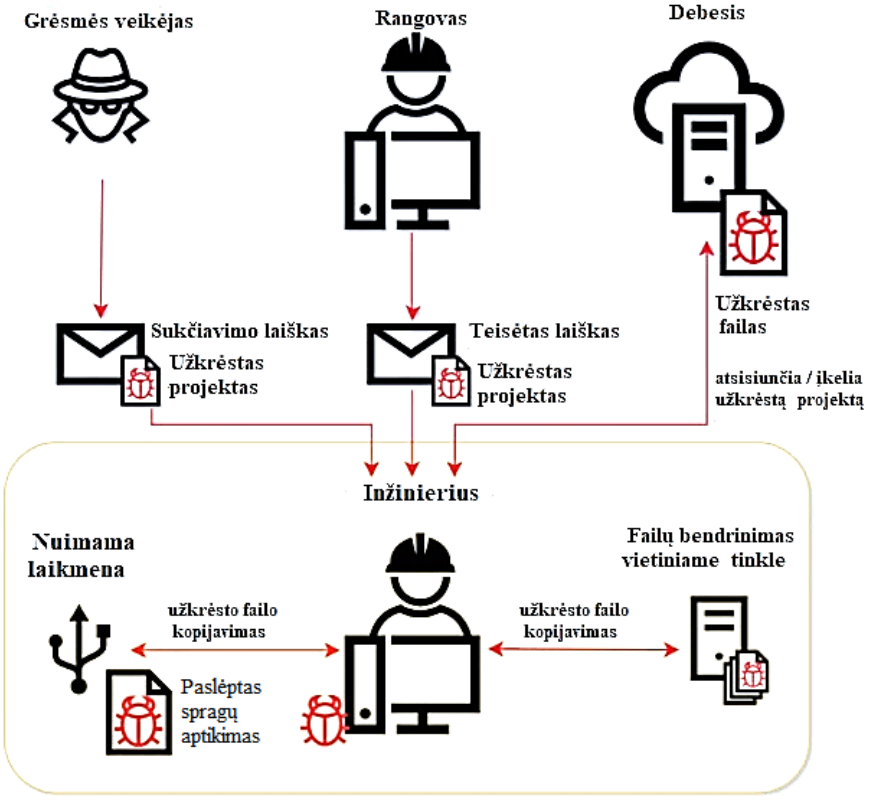
Elektros tinklo saugumas yra kiekvienos valstybės prioritetas. Kuriant ir užtikrinant elektros energijos tiekimo patikimumą, svarbus žingsnis buvo pažangiųjų tinklų, skaitmeninių tinklų, teikiančių abipusį ryšį tarp komunalinių paslaugų teikėjų ir vartotojų, plėtra. Tačiau tinklų skaitmeninimas padidino kibernetinių išpuolių tikimybę, nes sunaikino ribas tarp operacinių, informacinių ir ryšių technologijų (Oracle, 2012). Europos tinklų ir informacijos saugumo agentūra (ENISA) apibrėžia ICS sistemų dalis, kurios palaiko išmaniuosius tinklus ir gali būti pažeidžiamos kibernetinių išpuolių: *operacinės sistemos, klasikinės IT sistemos, ryšiai, tinklai, protokolai ir galiniai taškai* (Egozcue, 2012). Tokių sistemų skaitmeninimas padidina veiklos efektyvumą ir pagerina klientų aptarnavimą (Amin, 2010).

Kartais periodiški sistemos saugos atnaujinamai, reikalingi saugumui palaikyti, nėra diegiami galutiniams vartotojams arba diegiami, bet neaktyvuojami, nes gali pakenkti programinės įrangos veikimui (Amin, 2010). Vienas iš svarbiausių išmaniųjų tinklų komponentų yra pažangi matavimo infrastruktūra (angl. *Advanced measurement infrastructure* (AMI)), matuojanti ir kaupianti informaciją apie namų energijos suvartojimą. AMI paprastai sudaro milijardai nebrangių įrenginių, kurie yra marginalizuojami, atsižvelgiant į tinklo dydį (McLaughlin et al., 2010). Jei kibernetinis išpuolis pažeidžia išmanųjį skaitiklį (angl. *Smart meter*), įsilaužėlis stebi namų maitinimą ir naudoja išmaniuosius skaitiklius kaip įėjimo tašką tolesnėms atakoms prieš sistemos tinklą (Mahmud, 2015).

Kita problema yra tinklo pažeidžiamumas dėl kenkėjiškų išpuolių. Įsilaužėliai jau retai naudoja vadinamuosius nulinės dienos pažeidžiamumus, tai yra sistemos trūkumus, kurių programuotojai nepastebėjo diegdami programinę įrangą. Tačiau viskas priklauso nuo sistemos apsaugos lygio, pavyzdžiui, gali tekti pasirašyti tvarkyklės privačiu raktu nežinomiems išorės veikėjams (Falliere, 2011). Yra daug problemų, susijusių su kritinės energetikos infrastruktūra, nes daugelis įmonių neturi tinkamo reagavimo plano į kibernetinį išpuolį, o darbuotojai nėra apmokyti.

Požiūris į kibernetines grėsmes skiriasi kiekvienoje šalyje, o didėjantis pražūtingų epizodų skaičius paskatina didžiules investicijas į kibernetinio saugumo strategijas ir technologijas. Tačiau pagrindinis kibernetinio saugumo pažeidimų veiksnys išlieka žmogus, kuris atsakingas už 95 % visų saugumo problemų dėl netyčinių klaidų ar netinkamų veiksmų (Ahola, 2019).

Statistinis pavyzdys, įsilaužėliai užkrėstą USB atmintinę palieka įmonės automobilių stovėjimo aikštelėje arba šalia jos įrenginių, saugos personalas ją suranda ir, norėdamas pasidomėti, prisijungia prie kompiuterio, kad pamatytų, kas yra viduje. Antroji galimybė yra mokėti darbuotojui (esamam arba buvusiam) tam tikrą atlygį siekiant USB jungtimi įdiegti kenkėjišką programinį kodą. Tokie atvejai kelia personalo patikimumo klausimus. Yra pavojus, kad darbuotojas gali pavogti arba nukopijuoti parašą už atlygį (1.6 pav.).



1.6 pav. Galima užkrėtimo schema (Insider Threat Mitigation, 2022)
Fig. 1.6. Possible infection scheme (Insider Threat Mitigation, 2022)

Ne taip seniai kritinės infrastruktūros kibernetinės grėsmės buvo žinomos tik kaip valstybių veiksmai, nes tik valstybės turėjo įvairių įgūdžių ir išteklių, reikalingų tokioms grėsmėms sukurti. Paprastai ištekliai rėmėsi analoginėmis operacinėmis technologijomis ir buvo izoliuoti nuo interneto. Norint gauti prieigą prie tokių išteklių, reikėjo specializuotų bei žvalgybos įrankių, analoginių operacinių

technologijų ir net fizinės prieigos prie objekto, bet sparti informacinių technologijų plėtra pamažu keičia pasaulį. Atvira ir laisva elektroninė erdvė padidina žmonių laisvę ir galimybes.

Šiuolaikinė kritinė energetinė infrastruktūra yra pats sudėtingiausias techninis įrenginys, unikalus savo mastu ir reikšme, užtikrinantis žmogaus gyvybę ir jo gerovę. Dėl fizinių savybių ir veikimo principų tokių objektų valdymas ir eksploatavimas yra sudėtingas techninis ir organizacinis iššūkis. Šiandien automatizuotos apsaugos ir valdymo sistemos yra sudėtingas informacinis kompleksas, apimantis visus energetinės infrastruktūros objektų eksploatavimo aspektus, ir yra neatsiejama kritinės energetinės infrastruktūros dalis.

Sparti kompiuterinių ir ryšių technologijų, naudojamų visose technologijų srityse, įskaitant kritinės energetinės infrastruktūros įrangos automatizavimą, plėtra pakeitė ne tik saugos sistemų technines priemones, skirtas sistemos komponentams valdyti, bet ir projektavimo principus, atsižvelgiant į naujas valdymo ir stebėjimo galimybes.

2019 m. sausio mėnesį Šiaurės Amerikos ne pelno siekianti tarptautinė elektros patikimumo korporacija (angl. *North American Electric Reliability Corporation* (NERC)) pristatė kibernetinio saugumo pranešimą apie elektros tinklo incidentus, t. y. tiekimo, reagavimo ir planavimo sistemą, vadinamą CIP-008-6 patikimumo standartu, kuriame pateikiamos rekomendacijos, kaip pranešti ir reaguoti į kibernetinius incidentus, klasifikuojamus pagal OT ir Karka standartus (NERC, 2019). Kibernetinių incidentų tipai skirstomi pagal spalvų kodą, kuris svyruoja nuo „nėra pranešimų“ iki „skubūs pranešimai“. „Žalia“ reiškia „nėra pranešimų, įvykių ar operacijų arba jų nebuvo galima nustatyti“, „Geltona“ reiškia „nedeklaruojamas kibernetinio saugumo incidentas“, „Oranžinė“ reiškia „ataskaitų teikimas, bandymas įsilaužti į taikomą sistemą“ ir „Raudona“ reiškia „kibernetinio saugumo incidentas“ (angl. *North American Electric Reliability Corporation* (NERC)).

Taigi atsakymas „privaloma pranešti / nepranešta“ į užfiksuotą kibernetinį incidentą reiškia, kad energetikos įmonėje naudojama klasifikavimo sistema gali būti labai naudinga nustatant tinkamą reakciją į įvairius kibernetinius įvykius, kadangi reaguojant į kylančias kibernetines grėsmes reikalingi skirtingi vaidmenys.

Pateikta sistema yra kibernetinių incidentų klasifikavimo pavyzdys, taikant Nacionalinės energetikos reguliavimo tarnybos (angl. *The National Cybersecurity and Communications Integration Centre* (NCCIC)) kibernetinių incidentų taškų vertinimo sistemą (angl. *The National Cyber Incident Scoring System* (NCISS)), pagrįstą Nacionalinio standartų ir technologijos instituto (angl. *National Institute of Standards and Technology* (NIST)) specialiosios publikacijos 800-61 2 versija, ir kompiuterių saugumo incidentų valdymo vadovą (angl. *Cybersecurity and infrastructure security agency* (CISA)) (CISA, 2021). Struktūroje aprašyta infrastruktūra padalinta į įmonių ir SCADA zonas:

- Įmonės zoną sudaro nuolatiniai korporatyviniai padėjėjai ir yra išorinė infrastruktūros dalis, saugoma elektroninio saugumo perimetro ir elektroninės prieigos kontrolės stebėjimo sistemos (angl. *Electronic Access Control Monitoring System* (EACMS)).
- SCADA zona yra pramoninės kontrolės sistemos branduolys, saugomas kitų EACM ir įmonių ugniasienės, apsaugančios turtą nuo interneto įsilaužimų (NERC, 2019).

Įvedus kibernetinę klasifikaciją, rizikos įvertinimo metodu pagrįsti incidentai galėtų tapti tinkama technine priemone kuriant bendrą modelį. Tačiau, jei modelis turėtų apimti visų tipų kritinę energetinę infrastruktūrą (angl. *Critical Energy Infrastructure* (CEI)), reikėtų atsižvelgti į bendresnius elektroninės infrastruktūros elementus, nes tie elementai gali skirtis. Ekspertų skyrimas atsižvelgiant į incidentų sunkumą taip pat yra geras būdas reaguoti į kibernetinius incidentus ir turėtų būti įtrauktas į bendrąsias CEI gaires. Šioje sistemoje atsižvelgiama į rizikos įvertinimo metodą, kibernetinių incidentų klasifikavimą ir „išmoktų pamokų“ metodą, tačiau žalą, kurią padaro CEI kibernetiniai išpuoliai, galima įvertinti ne tik finansiniu, bet ir gyventojams padarytos žalos požiūriu. Dėl šios priežasties „išmoktų pamokų“ metodas nerekomenduojamas.

Kibernetines grėsmes yra labai sunku numatyti ir laiku imtis prevencinių priemonių (Fleisher & Bensoussan, 2003; Craig & Valeriano, 2016), dėl to padidėja sėkmingos kibernetinės atakos rizika, ypač kai klaidos daromos dėl nežinojimo ar neveiklumo. Toliau pateikiamas dažniausiai organizacijų daromų klaidų sąrašas:

1. Įsitikinimas, kad bet kurią infrastruktūrą galima apsaugoti nuo bet kokio pažeidžiamumo.
2. Geriausių specialistų samdymas apsaugai nuo kibernetinių grėsmių, tikintis, kad vienas specialistas nuveiks visą darbą už visą organizaciją.
3. Netinkamai pasirinktos apsaugos technologijos ir įrankiai, naudojami kibernetiniam saugumui užtikrinti.
4. Į kibernetinį saugumą žiūrima tik kaip į efektyvų stebėjimą.
5. Saugumo priemonės, naudojamos siekiant apsaugoti organizaciją nuo kibernetinių grėsmių, yra veiksmingesnės nei darbuotojų mokymas.

Analizuojant išvardintas klaidas, kiekviena organizacija turi suprasti, kad kibernetinis saugumas yra visos organizacijos požiūris (WISAC, 2015) ir kiekvieno organizacijos nario tikslas, kurio reikia siekti. Pažeidžiamiausių sričių supratimas, veiksmai, padedantys išvengti grėsmių, nenormalių infrastruktūros veiksmų nustatymo mechanizmai ir aiškus planas, apibūdinantis, kaip sumažinti nuostolius ir atkurti infrastruktūrą, yra svarbus saugumo aspektas (WISAC, 2015). Tačiau kritinių situacijų aptikimas ir reagavimas į jas, žymiai sumažinant žalą, susijusią su kibernetinio saugumo pažeidimais, yra viena iš pagrindinių organizacijos saugumo koncepcijų (Techrepublic, 2004), turinčių įtakos efektyvumui ir saugumui.

Šiuolaikiniame pasaulyje naudojamos technologijos ir įranga gali padėti, tačiau tai yra tik technologija ir ji negali užtikrinti visiško kibernetinio saugumo (Techrepublic, 2004; Wei et al., 2010). Todėl investuojant į įrangą, vadovai turi prisiimti atsakomybę, domėtis kibernetinio saugumo sritimi ir apmokyti kiekvieną darbuotoją, kad darbuotojas suprastų kibernetinių išpuolių grėsmę ir pasekmes.

Kalbant apie kibernetinį saugumą, verta ne tik stebėti, bet ir atlikti korekcijas remiantis stebėjimų rezultatais. Nes suprasdami išorinius kibernetinio saugumo pokyčius ir tendencijas, galime sukurti tinkamą politiką bei strategijas sėkmingai kovojant su kibernetiniais nusikaltimais. Organizacijos turi suprasti, kaip grėsmės vystosi ir kokios galimybės yra pasiruošti gresiantiems pavojams. Toks požiūris yra ekonomiškesnis (finansinių ir žmogiškųjų išteklių atveju), nes turi tam tikro pranašumo, lyginant su trumpalaikiu saugumo pagerinimu. Kiekviena organizacija turi užtikrinti dalijimąsi informacija apie saugos spragas, nes tik keitimasis informacija gali suteikti bendrą tikrojo kibernetinio saugumo vaizdą nacionaliniu ar pasaulio mastu (Govindarasu & Hahn, 2017).

Norint pasiekti savo tikslus, reikia užtikrinti efektyvų kibernetinį saugumą ir stengtis išvengti kibernetinių atakų. Kibernetinio saugumo politika turėtų teikti pirmenybę investicijoms į ypatingos svarbos infrastruktūrą ir išteklius, o ne į naujausias technologijas ar sistemas (WISAC, 2015). Būtina suprasti, kas ir kodėl gali dominti organizacijos veikloje, suprasti organizacijos IT turto vertę, mokėti įvertinti ir prisiimti tam tikrą riziką, nes neišmatuojamą vertę turinčios technologijos nesuteikia visiško saugumo.

Pagrindinis kibernetinio saugumo aspektas yra tas, kad kibernetinis saugumas turėtų būti kertinis akmuo kuriant naujus IT sprendimus ir sistemas. Metodai ir procedūros, naudojamos prieš IT sistemas, dabar kelia pavojų ir operacinių technologijų sistemoms (angl. *Operation technology* (OT)), todėl reikalingas naujas požiūris į kibernetinį saugumą, kuris sujungs IT ir OT saugumą. Naujos grėsmės kritinei infrastruktūrai rodo, kad reikalingi pokyčiai ne tik kibernetinėje gynyboje, bet ir valdymo srityje, nes esami kibernetinio saugumo valdymo modeliai nesuteikia tinkamos apsaugos reaguojant į kibernetines atakas, netikėtus scenarijus ir pažeidžiamumus. Todėl itin svarbu kibernetinio saugumo problemas spręsti kritinėse situacijose, siekiant apsaugoti pagrindinius valstybės interesus.

1.3. Kritinės energetikos infrastruktūros kibernetinio saugumo valdymo aspektai

Hatch ir Cunliffe (2013) knygoje apie šiuolaikinę, simbolinę ir postmodernios organizacijos teoriją rašo, kad veiksminga organizacinė struktūra yra tokia, kuri leidžia optimizuoti organizacijos veiklą, užtikrindama nustatytų tikslų įgyvendinimą, ir naudoti tinkamiausius išteklius tikslams pasiekti (pinigus, medžiagą,

žmones). Organizacinė struktūra nėra vien efektyviausio darbo ir veiklos struktūrinimas ir koordinavimas. Ji padeda planuoti, priimti sprendimus ir sumažinti problemas, susijusias su darbine veikla.

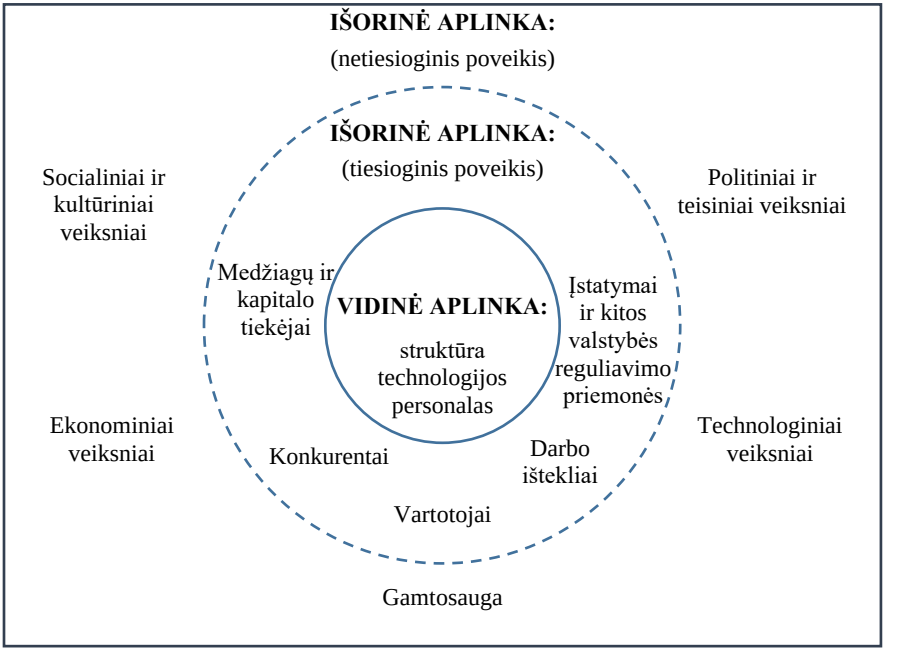
Klasikinės vadybos teorijos tyrimais siekiama surasti vieną iš geriausių būdų sukurti organizacinę struktūrą (pavyzdžiui, Weber biurokratija). Nenumatytų atvejų teoretikai teigia, kad nėra vienos bendros organizacinės struktūros, todėl organizacijos vadovai turi suprasti, kuri organizacinė struktūra yra tinkamiausia, atsižvelgdami į organizacijos tikslus, technologijas, produkto ar paslaugos rūšį, aplinkosaugos reikalavimus ir kitus nenumatytus atvejus. Norint tai padaryti, reikia mokėti analizuoti organizaciją ir jos aplinką, nustatyti tinkamiausią struktūrą, nuolat stebėti ir peržiūrėti ją, taip užtikrinant efektyvumą. Norint suvokti kibernetinio saugumo valdymo struktūrą, efektyvumą ir technologijas, reikia jį nagrinėti vadybos teorijos kontekste.

Nagrinėjant kibernetinio saugumo valdymą vadybos teorijos kontekste, būtina taikyti įvairias vadybos teorijas, siekiant suprasti, kaip sukurti ir valdyti struktūrą, taikant efektyvesnius metodus.

Kritinę infrastruktūrą galima apibūdinti kaip didelę, sudėtingą, dinaminę, atvirą, tikslingą ir valdomą sistemą, susidedančią iš skirtingų elementų ir posistemių, susijusių informaciniu, tiesioginiu ir grįžtamuoju ryšiu. Kibernetinės infrastruktūros vidinė aplinka (struktūra, technologijos, personalas) sąveikauja su išorine aplinka, kurią sudaro specialioji (vartotojai, medžiagų ir kapitalo tiekėjai, konkurentai, darbo ištekliai) ir bendroji (politiniai, teisiniai, technologiniai, ekonominiai, socialiniai ir kultūriniai veiksniai, gamtosauga) aplinka (1.7 pav.).

Analizuojant kritinę infrastruktūrą vadybos teorijos kontekste, galima pasakyti, kad tai biurokratinio tipo organizacija, turinti formalius principus, taip pat naudojanti administracines funkcijas (pavyzdžiui, kibernetinio saugumo strategijos, planų, teisės aktų kūrimas, pareigų ir funkcijų organizavimas ir kontrolė). Išorinės aplinkos analizė, struktūros vidinių komponentų priklausomybė nuo išorinės aplinkos ypatybių padeda geriau suprasti, kokiais metodais galima pasiekti tikslus tam tikroje situacijoje, ypač sprendžiant kibernetinio saugumo problemas. Lyginamoji analizė gali būti naudojama analizuojant panašias situacijas, jas lyginant ir taikant sprendimus, kurie jau buvo naudojami ir išbandyti panašiu atveju, pavyzdžiui, išpuolių kritinės infrastruktūros atveju.

Analizuojant tyrimo problemą, būtina pritaikyti strateginį planavimą, nes tokio pobūdžio sistemos negali egzistuoti ir funkcionuoti be jo. Optimalus mikroklimatas darbo grupėje, optimalus darbo režimas, geras darbo užmokestis, optimalus darbo pasidalijimas ir organizavimas – dar keli aspektai, be kurių efektyvus valdymas yra neįmanomas.



1.7 pav. Organizacijos išorinės ir vidinės aplinkos veiksniai (Bivainis, 2011)
Fig. 1.7. Factors of the organisation's external and internal environment (Bivainis, 2011)

Kritinė infrastruktūra − tai biurokratinio tipo hierarchinė organizacija, sudaryta iš kelių lygmenų, griežtai reglamentuota teisės aktais su formaliais principais ir atliekanti administracines funkcijas. Pavyzdžiui, stabilizuojantys, reglamentuojantys ir nurodantys metodai gali būti rašytinės arba virtualios formos, o, pavyzdžiui, nukreipiantys metodai gali būti rašytinės, žodinės ir virtualios formos. Kalbant apie virtualią pateikimo formą, naudotini dokumentai su elektroniniu parašu, paskelbti specialiuose portaluose.

Kritinės infrastruktūros saugumo valdymas yra tiesiogiai susijęs su kritinės infrastruktūros struktūra ir valdymu, o tai turi įtakos jos įgyvendinimui. Todėl kibernetinio saugumo valdymas turi būti vertinamas valdymo kontekste.

Kuriant kritinės infrastruktūros saugumo modelį, reikia išanalizuoti ir suprojektuoti įvairias situacijas, kurios gali kilti išpuolių atveju. Norint tai įgyvendinti programiškai, būtina taikyti įvairius kiekybinius metodus. Pavyzdžiui, taikant matematinę statistiką galima susisteminti duomenis, patikrinti hipotezes, nustatyti priklausomybes, o analizei galima naudoti ne visus statistinius duomenis, o tik jų dalį. Matematinė statistika suteikia galimybę rinkti duomenis (imtis) įvairiais būdais, pavyzdžiui, sudaryti ekspertinę arba sisteminę imtį, panaudoti įvairių būdų derinį.

Taikant tikimybių teoriją galima apskaičiuoti puolimo įvykio arba kitų aktualių besikartojančių įvykių tikimybes. Scenarijų metodas akivaizdžiai parodo įvairių veiksnių poveikius. Pagal šį metodą tinkamiausias scenarijus yra analitinis, kuris pagrįstas ekspertiniais vertinimais ir susijusių veiksnių analize. Taikant šį metodą, galima, pavyzdžiui, aprašyti serverio „griuvimą“ po programišiaus puolimo. Atsižvelgiant į ekspertų vertinimus, reikia sudaryti scenarijų rengimo užduotį, nustatyti įtakos veiksnius ir komponentus. Parengti pirminių galimų veiksnių scenarijus, įvertinti juos, atrinkti tinkamus ir patobulinti juos.

Jeigu situacijos tyrimą reikia atlikti skubiai arba nepakanka duomenų priimti tinkamą sprendimą, galima atkartoti situaciją. Pavyzdžiui, dar nebuvo kažkokio tipo užpuolimo arba buvo, bet užpuolimų skaičius labai mažas ir neužtenka išanalizuoti situaciją bei padaryti tinkamas išvadas.

Nagrinėjant kibernetinio saugumo valdymą organizacijos valdymo kontekste, reikia išanalizuoti tiriamą problemą, atsižvelgiant į rizikas, kylančias iš bet kokios veiklos valdymo. Todėl kibernetinio saugumo valdymas, kaip ir kiekvienas priimtas sprendimas, yra susijęs su rizika, nesvarbu, ar tai būtų veiklos, saugumo, investicinis ar finansinis sprendimas.

Rizikos valdymas – tai organizacijos finansinės, teisinės, strateginės ir saugumo rizikos nustatymo, įvertinimo ir kontrolės procesas (Tucci, 2023). Grėsmės ar rizikos gali kilti iš įvairių šaltinių, įskaitant finansinį netikrumą, teisinius įsipareigojimus, technologijų problemas, strateginio valdymo klaidas, avarijas ir stichines nelaimes. Efektyvus rizikos valdymas – tai bandymas kiek įmanoma labiau kontroliuoti būsimus rezultatus, sumažinant tiek rizikos atsiradimo tikimybę, tiek galimą jos poveikį. Nenumatytų įvykių pasekmės gali būti nedidelės arba sukelti katastrofą ir rimtas pasekmes. Todėl, siekiant sumažinti riziką, būtina panaudoti išteklius neigiamų įvykių poveikiui sumažinti, stebėti ir kontroliuoti. Nuoseklus, sistemingas ir integruotas požiūris į rizikos valdymą gali padėti nustatyti, valdyti ir sumažinti reikšmingą riziką. Rizikos valdymas turbūt niekada nebuvo toks svarbus, kaip dabar. Rizika, su kuria susiduria šiuolaikinės organizacijos, tapo sudėtingesnė dėl spartaus globalizacijos tempo. Nuolat atsiranda naujų pavojų, dažnai susijusių su skaitmeninių technologijų naudojimu (Tucci, 2023).

Rizikos ekspertas Greg Witte, (angl. *Huntington Ingalls Industries)* vyresnysis saugumo inžinierius ir Nacionalinio standartų ir technologijų instituto kibernetinio saugumo fondų architektas, sakė: „Norėdami suprasti, kas gali būti ne taip, turite pradėti nuo to, ką reikia padaryti teisingai“ (Tucci, 2023). Anot autoriaus, apibrėžiant rizikas svarbu suprasti, kad rizika gali būti tik tuomet, jei ji turi įtakos. Pavyzdžiui, vadovaujantis Nacionalinio standartų ir technologijų instituto rekomendacijomis, nustatant kibernetinio saugumo rizikas, reikia atkreipti dėmesį į šiuos keturis veiksnius:

- vertingas turtas ar ištekliai, kurie gali būti paveikti;
- grėsmės šaltiniai, kurie veiks prieš šį turtą;

- jau esamas pažeidžiamumas, kuris leistų tam grėsmės šaltiniui veikti;
- bet kokia kenkėjiška veikla, kuri išnaudoja šį pažeidžiamumą.

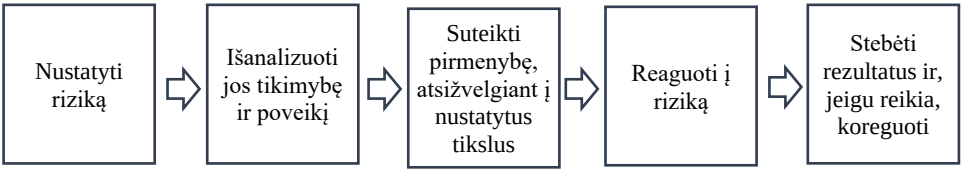
Rizikos gali būti klasifikuojamos pagal veiksnius, turinčius didelę įtaką sistemai, mūsų atveju – kritinei infrastruktūrai. Veiksnius, turinčius įtakos kritinei infrastruktūrai, galima suskirstyti į dvi grupes: priklausomus (vidinius) ir nepriklausomus (išorinius) (1.7 pav.). *Treadway* komisijos remiančių organizacijų komiteto teigimu, didžiausią įtaką turi keturi rizikos tipai:

- strateginė rizika (pvz., reputacija, santykiai su klientais, techninės naujovės);
- finansinė ir atskaitomybės rizika (pvz., rinkos, mokesčių, kredito rizika);
- atitikties ir valdymo rizika (pvz., etinė, reguliavimo rizika, tarptautinės prekybos, privatumas);
- veiklos rizika (pvz., IT saugumas ir privatumas, tiekimo grandinė, darbo problemos, stichinės nelaimės).

Norint valdyti riziką, reikia žinoti ir suprasti, ką reikia padaryti. Apie tai parašyta daug dokumentų, kuriuose aiškiai aprašomas kiekvienas veiksmas, reikalingas norint valdyti riziką. Vienas iš žinomiausių šaltinių yra ISO 31000 (2018) „Rizikos valdymas. Vadovas“ standartas, kurį sukūrė Tarptautinė standartizacijos organizacija. Šiame dokumente aprašomi penki pagrindiniai rizikos valdymo žingsniai, kurie gali būti taikomi bet kokio tipo organizacijoje (1.8 pav.):

1. nustatyti riziką;
2. išanalizuoti jos tikimybę ir poveikį;
3. suteikti pirmenybę, atsižvelgiant į nustatytus tikslus;
4. reaguoti į riziką;
5. stebėti rezultatus ir, jei reikia, koreguoti.

Rizikos analizė yra gana sudėtingas procesas, kurio metu naudojama daug informacijos, tačiau tai svarbi planavimo priemonė, galinti sutaupyti ne tik laiko ir pinigų, bet ir išsaugoti reputaciją. Dėl šios priežasties kibernetinio saugumo valdymas padeda spręsti ne tik saugumo problemas, bet ir rizikos valdymą, analizuojant išorinius ir vidinius veiksnius, turinčius įtaką kibernetiniam saugumui.



1.8 pav. Penki rizikos valdymo žingsniai, sudaryta remiantis (Tucci, 2023)
Fig. 1.8. Five steps to risk management (based on Tucci, 2023)

Strateginis valdymas dažniau yra nagrinėjamas vadybos arba kituose moksluose, kurie susiję su organizacijų valdymu ir planavimu, bet kibernetiniam saugumui jį galima pritaikyti, planuojant ir realizuojant pagrindinius saugumo aspektus, ypač kritinėje energetinėje infrastruktūroje.

Mokslinėje literatūroje strateginio valdymo samprata yra kompleksiška, o skirtingi autoriai pabrėžia šią sąvoką iš skirtingų perspektyvų. Mintzberg (2011) apibūdina strateginį valdymą kaip dinamišką procesą. Hamel (2002) pabrėžia strateginio valdymo svarbą diegiant naujoves ir skatinant organizacijų inovacijas. Lafley et al. (2014) apibūdina strateginį valdymą kaip procesą, kuriame svarbu aiškinti tikslus, įgyvendinti taktiką ir nuolat tobulinti strategiją.

Įvairių autorių požiūriai leidžia suvokti strateginio valdymo sąvoką kaip kompleksišką procesą, kuriame svarbu organizacijos gebėjimas prisitaikyti prie aplinkos pokyčių, nuolat kurti ir įgyvendinti strateginius planus, integruojant technologijas ir įtraukiant žmones.

Mokslinėje literatūroje nebuvo aprašytas strateginio valdymo apibrėžimas kibernetiniam saugumui. Tačiau autoriai įžvelgia svarba kibernetinio saugumo valdymui per strateginio valdymo aspektus. Rattray (2001) strategiškai vertina kibernetinio saugumo svarbą ilgalaikiams tikslams siekti, akcentuodamas strategijų kūrimo reikšmę organizacijų atsparumui kibernetinėms grėsmėms. Wall (2014) išryškina strateginio valdymo reikšmę kibernetinėje saugumo srityje, pabrėždamas nuolatinio organizacijos konteksto suvokimo ir lankstaus veiksmų pritaikymo esmę siekiant ilgalaikės ir efektyvios kibernetinio saugumo strategijos. Nye (2014) analizuoja strateginio valdymo aspektus kibernetinėje erdvėje, akcentuodamas aktualijas ir iššūkius, su kuriais organizacijos susiduria šioje sparčiai kintančioje srityje. Jo tyrinėjimai pabrėžia tikslų aiškinimą, taktikos įgyvendinimą ir nuolatinį strategijos tobulinimą kibernetinio saugumo kontekste. Luckyardi et al. (2023) pabrėžia, jog strateginio valdymo samprata evoliucionuoja vystantis informacinėms technologijoms, tačiau ši tema vis dar reikalauja papildomų tyrimų.

Šie požiūriai leidžia suprasti, kaip skirtingi autoriai strateginį valdymą vertina kibernetiniame saugume ir kaip tai gali paveikti organizacijų atsparumą kibernetinėms grėsmėms.

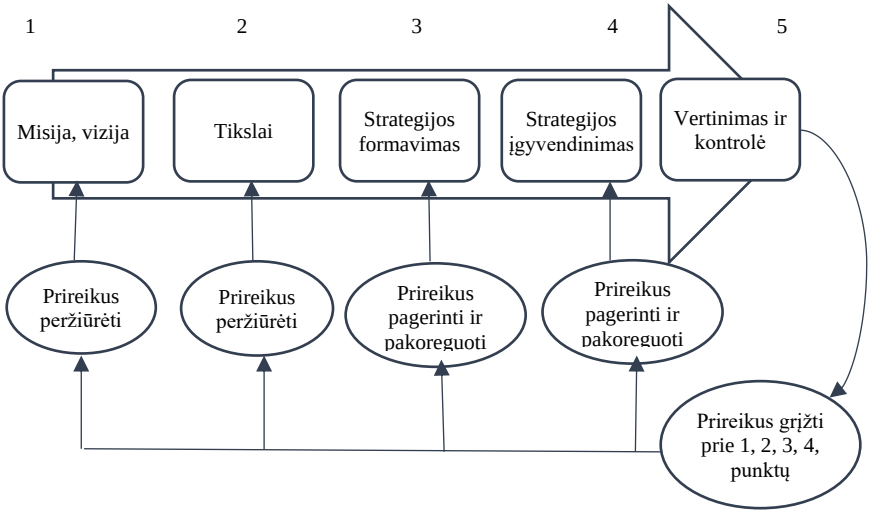
Galima apibrėžti, kad strateginis kibernetinio saugumo valdymas yra kompleksiškas procesas orientuotas į nuoseklų, dinamišką ir kryptingą veiksmų planavimą ir įgyvendinimą, siekiant efektyviai apsisaugoti nuo kibernetinių grėsmių. Nuolatinis prisitaikymas prie kintančios kibernetinės aplinkos, inovacijų ir technologijų skatinimas kartu įtraukiant žmones yra veiksmingos ilgalaikės ir efektyvios kibernetinio saugumo strategijos formavimo ir įgyvendinimo pagrindas.

Strateginio valdymo ir jo pritaikymo kibernetinio saugumo modelio kontekste reikia suprasti, kas yra strategija. Strategija yra veiksmų visuma, kuri leidžia nustatyti problemų prioritetus ir išteklius tam, kad būtų pasiekti pagrindiniai tikslai ir viena judėjimo kryptis. Taikant kibernetinio saugumo modelį kritinėje

energetinėje infrastruktūroje, pagrindinis tikslas ir jo įgyvendinimo kryptis – užtikrinti kibernetinį saugumą.

Strateginis valdymas orientuotas į trumpalaikius ir ilgalaikius planus, kurie leidžia vertinti, valdyti ir koreguoti organizacijos tikslus, atsižvelgiant į aplinkos pokyčius. Strateginio valdymo procesas yra dinamiškas strategijų kūrimas, įgyvendinimas, peržiūra ir stebėjimas, siekiant nustatyti organizacijos, šiuo atveju kritinės energetinės infrastruktūros, strateginius ketinimus.

Atsižvelgiant į išorinės ir vidinės aplinkos pokyčius, strateginio valdymo procesas turi grįžtamąjį ryšį, iš kurio gaunama informacija gali būti panaudota koreguoti proceso veiksmus. Todėl strateginio valdymo procesas turėtų atrodyti taip (1.9 pav.).

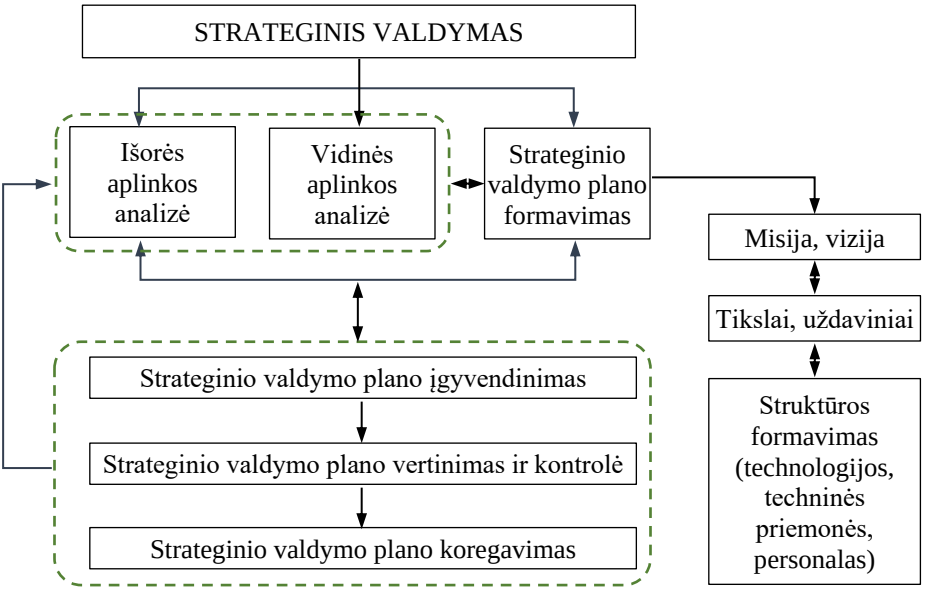


1.9 pav. Pagrindinės strateginio valdymo proceso dalys (sudaryta autoriaus)
Fig. 1.9. Main parts of the strategic management process (created by the author)

Strateginis valdymas yra gana sudėtingas procesas, kuris prasideda suformavus misiją ir viziją, tikslus ir uždavinius, biudžetą ir planus. Tai apima ir strateginį planavimą, kuris yra vienas iš svarbių strateginio valdymo komponentų, leidžiančių kritiškai analizuoti esamą situaciją, nustatyti, kas geriausia organizacijai, ir suprasti, ką reikia padaryti, kad būtų pasiektas galutinis tikslas. Taip pat strateginis valdymas padeda nustatyti, ar strategija teisingai įgyvendinta ir veikia, planuoti žinomus ir nežinomus nenumatytus atvejus, įgyvendinti strategiją, kuri sujungs žmones, procesus ir technologijas, siekiant visuotinio *tikslo:* sumažinti riziką ir didinti kibernetinio saugumo brandos lygį.

Tinkamam strateginio valdymo ir kaštų kontrolės strategijos kūrimui reikalingas detalus planavimas, kuris padės suprasti strateginio valdymo sampratą ir

esančius procesus, kuriuos galima pritaikyti atliekant nedidelius pakeitimus (1.10 pav.).



1.10 pav. Strateginio valdymo procesai (sudaryta autoriaus)
Fig. 1.10. Strategic management processes (created by the author)

Šiuolaikinė vadybos teorija, lyginant su kitomis, yra gana nauja sąvoka, kurios raidą stipriai veikia naujos ir sparčiai besivystančios informacinės technologijos. Reaguodamos į aplink vykstančius pokyčius, šiuolaikinės organizacijos turi tobulėti, diegdamos modernias technologijas ir naujus valdymo būdus, darbui naudoti kompiuterines technologijas, dirbti virtualiose komandose, perduoti žinias ir patirtį elektroninei nuosavybei. Taip pat turi nuolat tobulinti žinias ir įgūdžius, analizuoti esamus pavyzdžius ir įgytą patirtį, siekdamos gerinti savo galimybes ir konkurenciją. Visa tai reikalauja profesionalios apsaugos. O kadangi technologijos nestovi vietoje ir vystosi neįtikėtinai sparčiai, virtualioje erdvėje vis daugėja profesionalių įsilaužėlių, todėl kibernetinio saugumo sistema laikui bėgant turi keistis ir tobulėti. Todėl kibernetinio saugumo modelis, taikydamas besivystančios organizacijos koncepciją, nuolat analizuodamas surinktus duomenis ir skirtingų praktikų patirtį, įgyja naujų žinių ir naujos patirties kibernetinių atakų prevencijai.

Besimokančios organizacijos koncepcija, kaip ir šiuolaikinė vadybos teorija, yra gana nauja sąvoka, susiformavusi 1990 m. Senge savo darbuose besimokančią organizaciją apibūdina ne kaip „geriausios praktikos modulį“, o kaip poreikį siekti

idealių organizacijos savybių, dalijimąsi patirtimi, pagalbą kitiems ir atsakomybės didinimą. Jo nuomone, visos organizacijos turėtų siekti tobulumo. Garvin (1993), ne visiškai sutikdamas su Senge (Garvin, 1993), manydamas, kad jo besimokančios organizacijos samprata yra abstrakti, apibūdino besimokančią organizaciją kaip nuolat besikeičiančią.

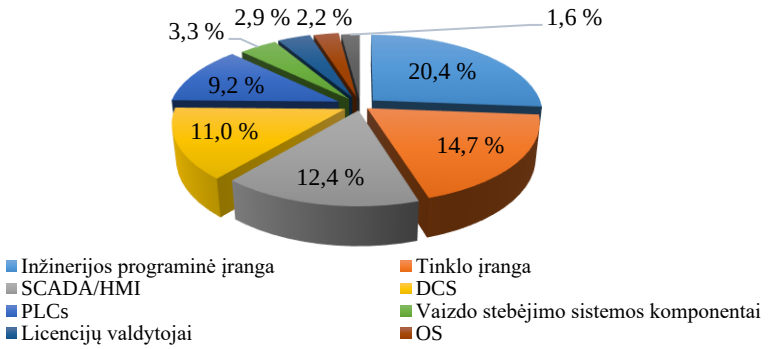
Egzistuoja daugybė besimokančios organizacijos apibrėžimų, tačiau juos visus sieja vienas principas – noras prisitaikyti prie pokyčių, įgyjant naujų žinių ir įgūdžių. O tai yra nuolatinis organizacijos tobulėjimo procesas.

Tobulėjant moksliniam ir technologiniam procesui, itin spartėja profesinių žinių ir gebėjimų senėjimas. Organizacijos gebėjimas kurti, valdyti ir palaikyti žinias prisideda prie naujovių, galinčių padidinti efektyvumą, kūrimo ir diegimo. Darbuotojų žinių lygio kėlimas, taip pat atitinkamų sąlygų kūrimas yra vieni iš inovacijų veiksnių. Įmonės, turinčios geresnes žinių valdymo sistemas, mokosi greičiau, o tai padidina jų galimybes mažinti išlaidas, greitai reaguoti į pokyčius, kurti kūrybines idėjas ir naujoves.

Nagrinėjant kibernetinio saugumo modelį šiuolaikinės vadybos teorijos kontekste, galima daryti prielaidą, kad besimokančių organizacijų koncepciją galima pritaikyti kibernetinio saugumo modeliui. Visi šio modulio komponentai atspindi pagrindinius besimokančios organizacijos principus: formuoja bendrą plėtros strategiją ir efektyvų planavimą, skatina inovatyvias idėjas ir naujas technologijas, gerai suvokia situaciją ir prisitaiko prie išorinių bei vidinių pokyčių, nuolat vystosi ir tobulėja. Reaguodama į nuolatinius pokyčius, sistema prisitaiko, įgyvendindama įvairias strategijas, įvertindama darbuotojų perspektyvas, vidines galimybes ir kompetencijas, plėtodama strateginius veiksmus, siekiant nustatyto tikslo – efektyvumo ir saugumo.

1.4. Kritinės energetinės infrastruktūros kibernetinio saugumo pažeidimo rizikų apžvalga ir aktualumas

Kritinės energetinės infrastruktūros kibernetinio saugumo svarba kiekvienais metais tik didėja. O kibernetiniai išpuoliai taip pat tampa vis sudėtingesni ir išskirtiniai. Kibernetiniai nusikaltėliai, siekdami finansinės ar politinės naudos, daug dėmesio skiria kritinei infrastruktūrai. Didžiausias pažeidžiamumas šioje srityje yra dėl to, kad sistemose naudojami komerciniai produktai. O turėdamas tam tikrų techninių žinių, užpuolikas gali pasinaudoti šių produktų, telekomunikacijos metodų ir bendros operacinės sistemos pažeidžiamumu (Roadmap to Secure Control Systems in the energy Sector, 2006) (1.11 pav.). Be to, sistemų pažeidžiamumų sąrašai yra visiems viešai prieinami.



1.11 pav. Visų išpuolių, nustatytų įvairiuose ICS komponentuose, procentinė dalis (sudaryta remiantis Securelist.com duomenimis, 2019)
Fig. 1.11. Distribution of vulnerabilities identified by ICS components (based on Securelist.com data, 2019)

Tokia situacija lemia didelį pasitikėjimą ryšių ir informacinėmis sistemomis (angl. *Communication and information system* (CIS)) bei technologijomis. Kibernetinis išpuolis prieš kritinę infrastruktūrą paveikia ne tik vyriausybę, bet ir privatųjį sektorių. Pavyzdžiui, 2015 m. gruodžio mėn. nuo Ukrainos elektros tiekimo sistemos buvo atjungta 225 000 vartotojų. JAV vidaus saugumo departamentas pranešė apie kibernetinį išpuolį naudojant kenkėjišką programinę įrangą. Tikriausiai tai pirmas žinomas sėkmingo elektros energijos tiekimo nutraukimo atvejis kibernetinio užpuolimo būdu. Buvo daug bandymų surasti kibernetinių išpuolių kaltininkus, tačiau visada susiduriama su problema – surasti įvykio kaltininkus labai sunku (Volz, 2016). Norint išvengti kibernetinių incidentų, būtina gerinti kibernetinį saugumą. Tačiau svarbu nepamiršti, kad kibernetines grėsmes sunku numatyti ir laiku imtis prevencinių priemonių gali būti sudėtinga. Todėl didėja rizika, kad kibernetiniai išpuoliai bus sėkmingi ir jų vis daugės, bus „pagerinama“ sėkmingų išpuolių skaičių statistika.

Kibernetinės saugos valdyme, neįvertindamos egzistuojančių kibernetinių grėsmių, dar nesukūrė strategijų, kaip reaguoti į kibernetinius išpuolius ir netikėtus scenarijus. Itin svarbu ir aktualu tirti kibernetinio saugumo aspektus kritinės infrastruktūros kontekste, siekiant užtikrinti gyvybiškai svarbių nacionalinių interesų saugumą. Kaip jau buvo minėta, vien technologiniai sprendimai neišsprendžia visų problemų, o kritinės infrastruktūros kibernetinio saugumo valdymo modelis turi būti tobulinamas kartu su sparčiai besivystančiomis technologijomis, teisiniais aspektais ir kitais kibernetiniam saugumui įtakos turinčiais dalykais (Limba et al., 2017).

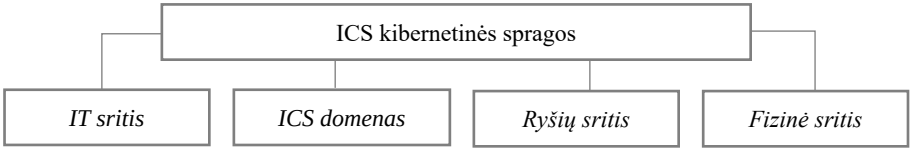
Vyriausybinės organizacijos (JAV energetikos departamentas, JAV vidaus saugumo departamentas) ir tyrėjai (Tranchita et al., 2010) atkreipia dėmesį į pagrindinius išpuolių tipus prieš kritinę infrastruktūrą arba pramonės valdymo sistemas. Išpuolius galima skirstyti į penkias pagrindines grupes, priklausomai nuo užpuoliko siekiamų tikslų (1.5 lentelė).

1.5 lentelė. Išpuolių grupės (sudaryta autoriaus remiantis Cybersecurity Framework, 2023)
Table 1.5. Attack groups (created by the author based on Cybersecurity Framework, 2023)

Išpuolis	Rezultatas
Informacijos sugadinimas	duomenų keitimas neteisingais duomenimis sistemoje ar ryšio kanale
Paslaugos blokavimas (DoS)	kai įgaliotiesiems vartotojams neleidžiama prisijungti prie sistemos
Informacijos atskleidimas	slapta informacija atskleidžiama pašaliniams asmenims ar sistemoms
Išteklių vagystė	sistemos išteklius naudoja pašaliniai asmenys
Fizinis sunaikinimas	fizinis sugadinimas ar sunaikinimas atliekamas naudojant ICS

Kritinės infrastruktūros saugumas priklauso nuo technologijų plėtros ir kintančių rinkos tendencijų. O tai lemia sistemų valdymo pokyčius ir kritinės infrastruktūros atsparumą kibernetinėms spragoms.

Kibernetinio saugumo tyrinėtojai nustatė, kad ICS kibernetinių spragų atsiranda ten, kur yra didžiausias prisijungimų skaičius, o prieigos kontrolė yra silpniausia, bei išskiria 4 kibernetinių spragų sritis (kiekviena sritis turi savo atakų vektorius, kuriuos naudoja kibernetiniai nusikaltėliai, siekdami savo tikslų) (1.12 pav.) (Barnes et al., 2004).



1.12 pav. Kibernetinių spragų sritis (Barnes et al., 2004)
Fig. 1.12. Area of Cyber Vulnerabilities (Barnes et al., 2004)

Šiuo metu sparti technologijų plėtra neleidžia atskirti ICS domeno nuo IT srities, nes jų komponentai yra tarpusavyje susiję, ypač kritinėje energetinėje infrastruktūroje.

JAV Vyriausybės atskaitomybės tarnyba skirsto kibernetines atakas pagal siekiamus tikslus:

1. „Bot“ tinklo operatoriai,
2. nusikalstamos grupuotės,
3. užsienio žvalgybos tarnybos,
4. įsilaužėliai,
5. vidiniai darbuotojai
6. sukčiai,
7. brukalo siuntėjai,
8. šnipinėjimo ir kenkėjiškų programų autoriai,
9. teroristai.

Visų išvardintų grupių tikslai yra skirtingi, bet jų veiksmai nukreipti į kritinę infrastruktūrą ar kitus informacinių technologijų išteklius. Aišku, kad visos grupės yra pavojingos, tačiau, priklausomai nuo pasekmių, bet kuri grupė gali būti identifikuota kaip nekenksminga.

Kiekvienas užpuolikas bando išnaudoti sistemos spragas, naudodamasis keletu išpuolių krypčių, tokiu būdu valdydamas sistemą, kurią bando sugadinti ar išnaudoti. Daugeliu atvejų užpuolikai išnaudoja spragas, kad pasiektų savo tikslus (Stouffer et al., 2013). Kibernetinis išpuolis dažnai vyksta penkiais etapais (1.13 pav.):

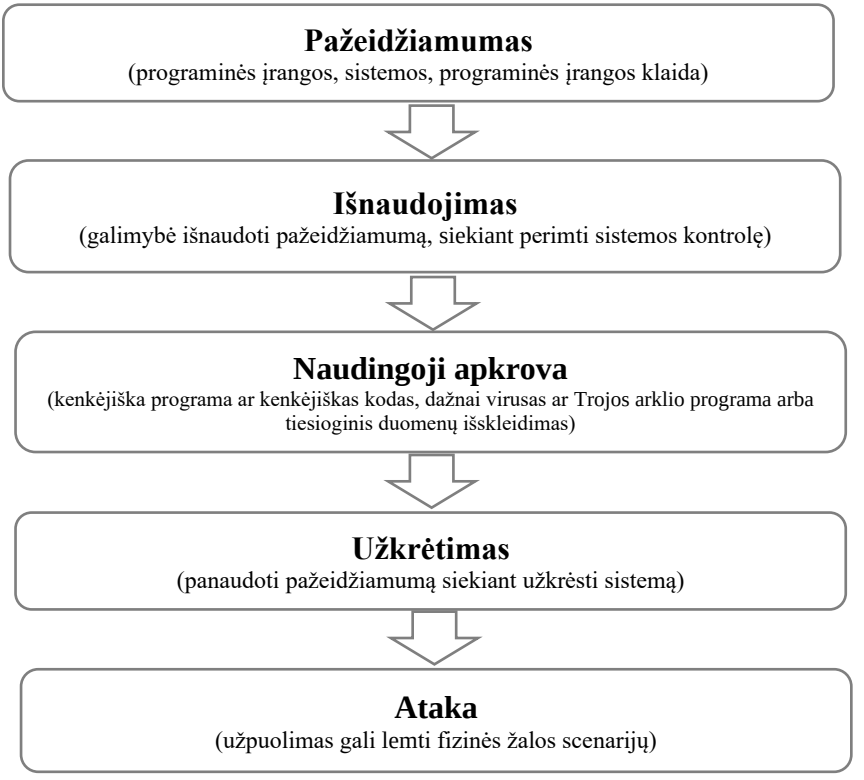
- rasti sistemos pažeidžiamumą,
- perimti sistemos ar jos dalies kontrolę,
- įterpti kenkėjišką programinę įrangą
- užkrėsti kitus sistemos komponentus,
- užpulti visą sistemą ar specialią jos dalį.

Kibernetinio saugumo spragos kelia iššūkį kiekvienam sistemos savininkui ar operatoriui, tačiau gali būti, kad jos nebus suvokiamos kaip kritinės infrastruktūros sistemų spragos, nes jų puolimo poveikis būtų beveik nepastebimas.

Sistemos puolimas gali turėti įvairių pasekmių. Išskiriami dažniausiai pasitaikantys atakų tipai:

- Kai kuriais išpuoliais prieš infrastruktūrą siekiama sukelti gyventojų paniką ir sutrikdyti įprastą gyvenimą. Pavyzdžiai, 2006 m. Los Andželo šviesoforo ataka (GAO, 2007), 2007 m. Volgodonsko ir Šv. Sankt Peterburgo 2008 m. atominės elektrinės išpuoliai (Butrimas & Bruzga, 2012) ir kt.
- Šnipinėjimo išpuoliai, tokie kaip 2006/2013 m. JAV energetikos objektų išpuoliai (Umbach, 2013), raudonasis spalis 2012 m. (securelist.com, 2013), „Gauss 2012“, „Careto“ (kaukė) 2014 m. (Kaspersky Lab’s, 2014) ir kt.

- Atakos, kurių pagrindinis tikslas yra sunaikinti ar sutrikdyti įprastą sistemos įrangos darbą. 1982 m. SSRS SCADA išpuolis (Radziwill, 2015).
- Australijos nuotekų išsiliejimas (Crawford, 2006). Ko gero, labiausiai žinoma atominės elektrinės ataka – „STUXNET 2010“ (Karnouskos, 2011; Langner, 2013) ir kt.



1.13 pav. Kibernetinių atakų vykdymo etapai (sudaryta remiantis IMIA darbo grupės, 2016)
Fig. 1.13. Cyber-attack development stages (based on IMIA Working Group, 2016)

Reikia suprasti, kad tai nėra baigtinis sąrašas, užpuolikai gali siekti ir kitų tikslų, atakuodami ne tik kritinę infrastruktūrą.

Šiandien neįmanoma įsivaizduoti kritinės infrastruktūros be ICS valdymo. Toks valdymas neįmanomas be šiuolaikinių technologijų, kurios supaprastina ir sumažina eksploatacines išlaidas. Tačiau tuo pat metu sukuriamos saugumo spragos, kurios išnaudojamos kibernetiniams pažeidžiamumams. Technologijų

įmonės bando paspartinti kritinės energetinės infrastruktūros plėtrą ir pašalinti kibernetines grėsmes, sukurdamos centralizuotą valdymo sistemą, skirtą kritinei infrastruktūrai apsaugoti nuo kibernetinių grėsmių. Tačiau kartais naujos technologijos užpuolikams tiesiog atveria naujas galimybes (Wei et al., 2010).

Atsižvelgiant į temos aktualumą, atliktuose tyrimuose bandyta ieškoti būdų užtikrinti kritinės infrastruktūros kibernetinį saugumą. Pažymėtina, kad šiai sričiai itin daug dėmesio teikia Estijos mokslo tyrėjai. Šie tyrėjai pagrindžia sisteminio požiūrio į kibernetinį saugumą svarbą. Jų manymu, užtikrinant kritinės energetinės infrastruktūros kibernetinį saugumą, itin svarbus bendradarbiavimas – tiek valstybės, tiek tarptautiniu lygmeniu (Bulakh et al., 2016). Savo ruožtu, Estijos tyrėjai siūlo šias gerąsias praktikas: aiškiai apibrėžti informacinio saugumo standartai, Nacionalinio saugumo strategija vystyta įtraukiant privataus sektoriaus atstovus, įsteigtas kritinės infrastruktūros apsaugos komitetas (Bulakh et al., 2016).

Siekiant mažinti kibernetinių pažeidimų rizikas, imamasi svarbių iniciatyvų ir tarptautiniu lygmeniu. Europos Komisija organizavo viešojo ir privačiojo sektoriaus bendradarbiavimo stiprinimą – sukurtas kritinės infrastruktūros apsaugos informacijos sklaidos tinklas (Europos Komisija, 2015). Šis tinklas sudaro galimybes valstybės institucijoms, privataus sektoriaus atstovams, kitiems ekspertams keistis informacija, dalintis gerosiomis praktikomis. Visgi, pažymima, kad privačiame sektoriuje yra kur kas mažiau iniciatyvos dalintis informacija apie specifines atakas (Europos Komisija, 2012), nors tokia informacija galėtų labai prisidėti prie kibernetinio saugumo stiprinimo. Manytina, kad privataus sektoriaus atstovai dalintis tokia informacija nėra linkę dėl galimų neigiamų pasekmių, parodančių jų pažeidžiamumą ar kvestionuojančių jų patikimumą, jei būtų dalinamasi informacija apie įvykusias atakas. Sunkumai užtikrinti patikimą, efektyvų bendradarbiavimą, diegti bendrą kritinės infrastruktūros modelį pabrėžiami ir 2016 m. liepos 6 dieną Europos Parlamento patvirtintoje direktyvoje, numatančioje naujas kibernetinio saugumo taisykles (Europos parlamento ir tarybos direktyva. Nr. 5581/1/16 REV 1, 2016). Siekiant spręsti kibernetinio saugumo problemas, ši direktyva kritinę infrastruktūrą, taip pat ir energetikos, valdančius operatorius įpareigoja užtikrinti saugią ir patikimą skaitmeninę aplinką (Europos Parlamento ir Tarybos direktyva, 2016). Visgi, konkretūs būdai nėra numatyti.

Kuriant kritinės energetinės infrastruktūros modelį, sprendžiant minėtas problemas, rekomenduotinas platus valstybės institucijų, nacionalinio lygmens reguliuotojų, kitų viešųjų institucijų įsitraukimas, taip pat tarpvalstybinis bendradarbiavimas, bandant ieškoti efektyviausio reguliavimo, atsižvelgimas į tarptautinių institucijų normas, rekomendacijas (Organisation for Security and Cooperation in Europe, 2013). Šį aspektą taip pat pabrėžia JAV vidaus saugumo, energetikos departamentai – teigiama, jog efektyviam kritinės energetikos infrastruktūros modeliui pasiekti itin svarbus pramonės atstovų bei valstybės institucijų bendradarbiavimas (Roadmap to Secure Control Systems in the energy Sector, 2006).

Kibernetinio saugumo tyrėjai bandė rasti veiksmingą kibernetinio saugumo modelį. Jų nuomone, bendradarbiavimas užtikrinant kritinės infrastruktūros kibernetinį saugumą yra nepaprastai svarbus tiek nacionaliniu, tiek tarptautiniu mastu. Pažymima, kad kritinės infrastruktūros elementai yra labai glaudžiai susiję, kibernetinis išpuolis gali plačiai plisti ir pakenkti kitoms sistemoms, nes pažeidimas vienoje srityje gali lengvai plisti į kitą (Bulakh, 2016). Būtina stiprinti viešojo ir privačiojo sektorių partnerystę teikiant kritinės infrastruktūros išteklius. Viešasis sektorius yra tam tikros kritinės infrastruktūros ar ryšių sistemų, kurias paprastai valdo privatūs operatoriai, dalies savininkas.

Reikėtų pažymėti, kad viena iš Europos Komisijos iniciatyvų – organizuoti viešojo ir privačiojo sektorių partnerystę, kuriant informacijos apie kritinės infrastruktūros objektų apsaugą sklaidos tinklą. Šis tinklas leidžia valdžios institucijoms, privačiajam sektoriui ir ekspertams keistis informacija ir geriausia praktika.

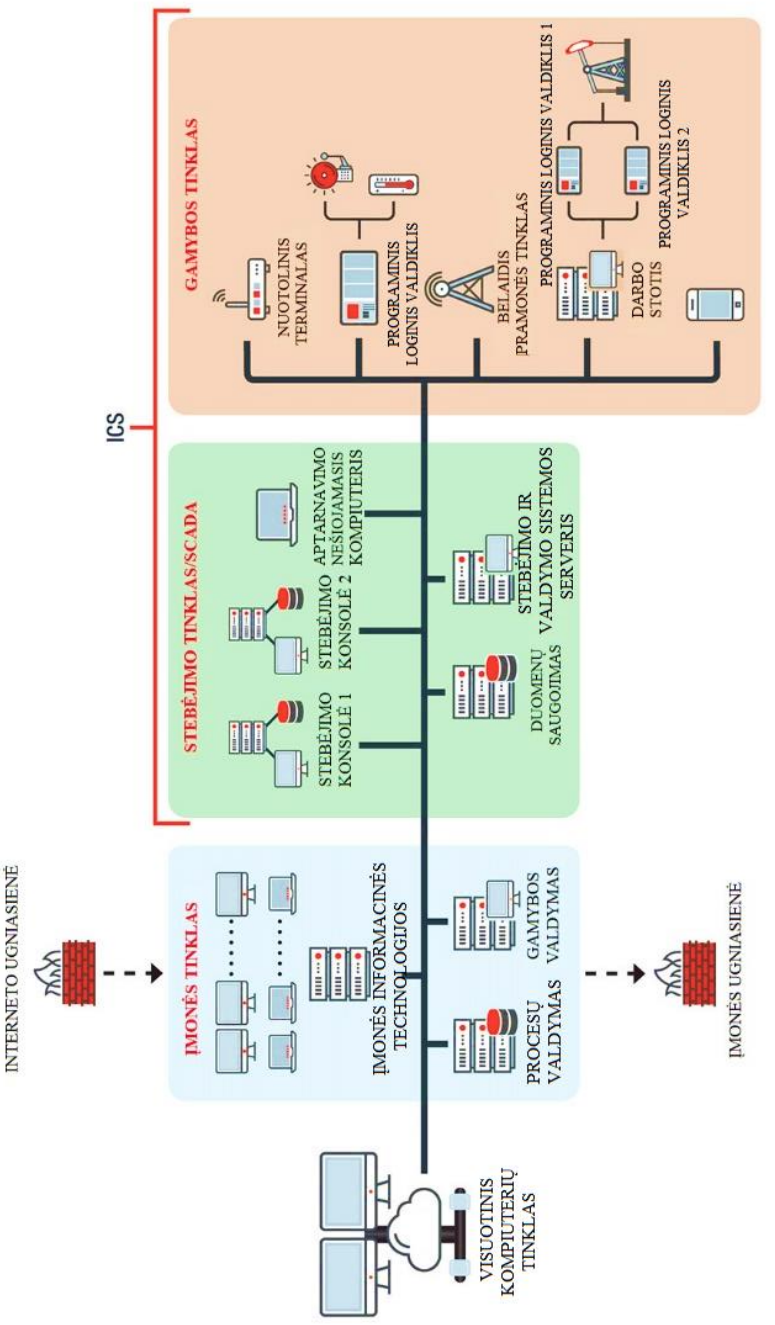
Tačiau privatusis sektorius daug rečiau dalijasi informacija apie konkrečius išpuolius, nors tokia informacija gali reikšmingai prisidėti gerinant kibernetinį saugumą. Vargu ar privatusis sektorius galės dalintis informacija apie savo kibernetinio saugumo išpuolius ir infrastruktūros pažeidžiamumus, nes ši informacija gali pakenkti sektoriaus reputacijai, tapusi vieša gali verslo partnerį padaryti patrauklesnį naujoviškam bendradarbiavimui (Europos Komisija, 2016; Rosner, 2013).

Masera (2010) pažymi, kad šiuolaikinė infrastruktūra, ypač energetinė infrastruktūra, integruoja pramonės valdymo sistemą su programinės įrangos komponentais, tai yra pagrindinis argumentas šiuo atveju – technologinė plėtra ir progresas.

Pramonės valdymo sistemos sąvoka vartojama apibūdinti aparatinės (angl. *Operation technology*) ir programinės (angl. *Information technology*) įrangos integravimą į bendrą tinklą, palaikantį kritinę infrastruktūrą. Priklausomai nuo pramonės veiklos, kiekviena pramonės valdymo sistema veikia skirtingai ir skirta efektyviai atlikti užduotis elektroniniu būdu. Šiandien pramonės valdymo sistemos protokolai ir prietaisai naudojami praktiškai visuose pramonės sektoriuose net ir tokiose kritinėse infrastruktūrose, kaip gamybos, transporto, energetiko, vandens valymo infrastruktūros.

Egzistuoja keli ICS tipai, iš kurių labiausiai paplitęs yra stebėjimo ir valdymo (angl. *Supervisory control and data acquisition*) bei automatinio valdymo sistemos (AVS). Vietines operacijas kontroliuoja vadinamieji lauko įrenginiai, kurie priima valdymo komandas iš nutolusių stočių (1.14 pav.).

Įranga ir valdymo moduliai sąveikauja naudodami įvairius ryšio protokolus, skirtus konkretiems tikslams, pavyzdžiui, procesams automatizuoti, elektros sistemoms automatizuoti ir kt. Protokolai buvo sukurti siekiant užtikrinti suderinamumą tarp skirtingų gamintojų. Tačiau yra keletas protokolų, kurie veikia tik tuo atveju, jei protokolus ir aparatinę įrangą teikia tas pats gamintojas.



1.14 pav. ICS sistemos pavyzdys (sudaryta remiantis Trendmicro.com)
Fig. 1.14. Example of an ICS system (based on Trendmicro.com)

Šiuolaikinis pasaulis susiduria su vis didėjančia naujų technologijų plėtra. Vienas pavyzdžių yra daiktų internetas, kuris, užtikrindamas saugų ir efektyvų duomenų perdavimą, sprendimų palaikymą ir bendrą komfortą, yra patrauklus daugeliui įmonių. IoT leidžia objektus stebėti naudojant esamą tinklo infrastruktūrą, įskaitant internetą, padidinant efektyvumą, tikslumą ir kainą.

Technologijų valdymą sudaro informacinės technologijos, naudojamos duomenims saugoti, apdoroti ir perduoti, ir operacijų technologijos, skirtos gamybos įrangai, pavyzdžiui, SCADA sistema, skaičiavimo technologija *Indukcinė automatika* (Inductive Automation, 2020). Pripažindamos daiktų interneto naudą, pramonės organizacijos ir sistemų kūrėjai pateikė naują koncepciją – pramoninį daiktų internetą, kuriame OT ir IT sąveikauja. Turėdama prieigą prie duomenų, įmonė gali dažniau priimti geresnius sprendimus.

Pavyzdžiui, bet kuriame naftos įrenginyje gali būti daugiau nei 16 000 kilometrų vamzdynų, tūkstančiai programuojamų loginių valdiklių, prietaisų bei laidų. Įprastoje stebėjimo ir saugumo sistemoje naudojami tik kritiniai darbo duomenys, iš kurių 80 % duomenų neatvaizduojami. Pramoninis daiktų internetas (angl. *Industrial internet of things* (IoT) gali perduoti visus šiuos duomenis ir dar daugiau. Papildoma informacija apie tinklo įrenginių būseną padeda priimti sprendimus, pavyzdžiui, ar automobilį siųsti remontui, ar išspręsti problemą vietoje.

Siekiant pagerinti sistemos funkcionalumą ir našumą, kiekviename ICS nuolat diegiamos naujos technologijos ir programinė įranga. Sujungus IT ir OT atsiranda didesnė pažeidžiamumo rizika. Vienas iš dažniausių OT infrastruktūros saugumo trūkumų yra jų nesugebėjimas apsaugoti senas valdymo sistemas, tokias kaip SCADA. Be to, organizacijos susiduria su didėjančiais saugumo iššūkiais, susijusiais su naujomis technologijomis.

Svarbu tai, kad kibernetines grėsmes labai sunku numatyti, prognozuoti ir laiku imtis prevencinių priemonių (Craig & Valerino, 2016), todėl didėja rizika, kad kibernetiniai išpuoliai bus sėkmingai įgyvendinti. Todėl svarbu stebėti ir atlikti išsamų kibernetinių incidentų vertinimą, siekiant išvengti būsimų išpuolių ir nustatyti saugumo grėsmes. Įvairi grėsmių ir atakų klasifikacija leidžia nustatyti jų šaltinį ir parametrus, kad būtų galima efektyviau apskaičiuoti naudingus rodiklius, tokius kaip rizikos rodikliai.

Mokslininkai savo darbuose siūlo naudoti taksonominę struktūrą su būtinomis charakteristikomis, analizuojant saugumo incidentus ir nagrinėjant jų pagrindines savybes. Siekiant gerinti situaciją buvo daug kartų siūlyta incidentų klasifikavimo taksonomija. Taip 1998 m. Howard ir Longstaff (1998) pasiūlė suskirstyti incidentus į tris grupes: atvejis, ataka ir incidentas. Kituose šaltiniuose, pavyzdžiui, ISA/IES-62443 (ISA-99 arba ANSI/ISA-99) (2009) aprašytos keturios incidentų grupės: aktyvios atakos, pasyvios atakos, vidaus ir išorės atakos. Ruf et al. (2008) pasiūlė „trijų stačiakampių klasifikacijų modelį“, pagal kurį grėsmės klasifikuojamos pagal matmenis ir vadinamos „motyvacija“, „lokalizavimu“ ir „agentu“. Sandro et al. pasiūlė hibridinį modelį, vadinamą „informacinės sistemos

saugumo grėsmių kubine klasifikacija“ arba C3 modeliu. Pagrindinė šio modelio idėja yra naudoti būtinus ir naudingus klasifikavimo kriterijus, kurie yra: grėsmių dažnis, mastas ir šaltinis (Ahmadian et al., 2020). Orgie (2017) savo darbuose analizavo 242 kritinės infrastruktūros saugumo incidentus, kurie buvo užregistruoti nuo 1982 iki 2014 m. duomenų bazėje RISI, naudojant tik keturis incidentų kriterijus: aktyvios atakos, pasyvios atakos, vidaus ir išorės atakos.

Kritinė energetinė infrastruktūra patiria daug saugumo incidentų, todėl svarbu visus juos nustatyti, siekiant sumažinti riziką. Tačiau anksčiau nagrinėta klasifikavimo taksonomija neapima visų būtinų charakteristikų. Nagrinėjamuose mokslinio tyrimo darbuose buvo ištirta saugumo incidentų taksonomija, taikant analitinį hierarchinį procesą, vieną iš daugiakriterių sprendimų metodų.

Hierarchinė taksonominė struktūra apima ankstesnių ir naujų saugumo incidentų taksonomijos savybes, todėl metodas tampa lankstus ir jį galima pritaikyti bet kurioje situacijoje. Kibernetinio saugumo tyrėjai siūlė tokias šio metodo pagrindines savybes (1.6 lentelė).

Tiriant kibernetinės saugos įvykių seką, nuo 1982 iki 2018 m. užregistruoti 268 kritinės energetinės infrastruktūros saugumo incidentai. Taikant hierarchinį taksonominį metodą, 147 iš 268 incidentų buvo nustatyti kaip išpuoliai, o 121 – saugumo incidentai.

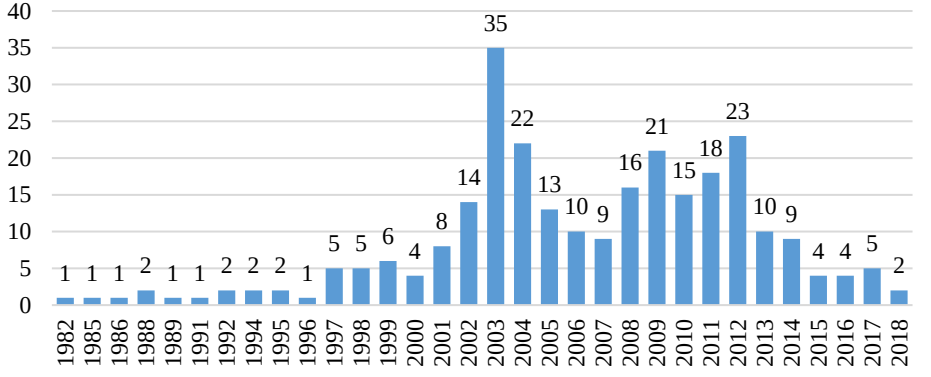
1.6 lentelė. Taksonominio metodo savybės (sudaryta autoriaus remiantis Operations security (OPSEC), 2023)
Table 1.6. Taxonomy method properties (created by the author based on Operations security (OPSEC), 2023)

Įvykis	Apibūdinimas
1	2
Incidento šaltinis (angl. *Source*)	jį sudaro šaltinio tipas ir pradinis taškas. Incidentas gali būti vidinis (angl. *internal*), išorinis (angl. *external*) ir hibridinis (ir vidinis, ir išorinis)
Sritys (angl. *Target industry*)	šis parametras nustato, kuriai sričiai (pramonės, cheminei, atominei ir pan.) priklauso incidento objektas
Objekto tipas (angl. *Target Type*)	apibūdina objekto rūšį (komercinė, vyriausybinė, švietimo ir pan.)
Poveikis (angl. *Direct impacts*)	gali būti tiesioginis poveikis (paslaugų sutrikimas, fizinis sunaikinimas, informacijos ar duomenų sunaikinimas / atskleidimas, mirtis ar sunkus sužalojimas) arba netiesioginis poveikis (reputacijos, pasitikėjimo ar verslo praradimas, politinis poveikis)
Sunkumas (angl. *Severity*)	aukštas, vidutinis, mažas

1.6 lentelės pabaiga

1	2
Pažeidimas (angl. *Violation of the CIA*)	šiuo atveju kalbama apie bet kurį informacijos konfidencialumo pažeidimą, iškraipymą ar sunaikinimą, paslaugų sutrikdymą ar fizinį sunaikinimą
Tyčinis įvykis (angl. *Agent intention*)	pavyzdžiui, kibernetinis fizinis nusikaltimas arba informacijos sugadinimas
Neeilinis įvykis (angl. *Means*)	apibūdinama, kaip įvyko incidentas ir kokie metodai buvo taikomi
Užpuolimas (angl. *Attack*)	sisteminga kibernetinių atakų klasifikacija pagal jų savybes, metodus, tikslus ar uždavinius. Atakų klasifikacija keičiasi, kai atsiranda naujų atakų metodų.
Režimas (angl. *Mode*)	režimas gali būti pasyvus arba aktyvus

Duomenims apie saugumo incidentus rinkti geroji praktika yra įvykių analizė. Nuo 2015 m. RISI internetinė duomenų bazė nebuvo atnaujinta, todėl analizuojant duomenis būtina rinkti informaciją iš kitų šaltinių. Moksliniuose tyrimuose pažymėta, kad dėl šios priežasties nuo 2015 m. incidentų skaičius yra mažesnis. Ši tendencija aiškiai matyti diagramoje (1.15 pav.). Nuo 2003 m. užregistruotų incidentų skaičius mažėja ir mažėja. Išanalizavus duomenis, galima pastebėti, kad nuo 2005 iki 2012 m. incidentų buvo daug tik todėl, kad buvo pakankamai surinktos informacijos iš teisinių duomenų bazių ir interneto, kur šie incidentai buvo paviešinti.



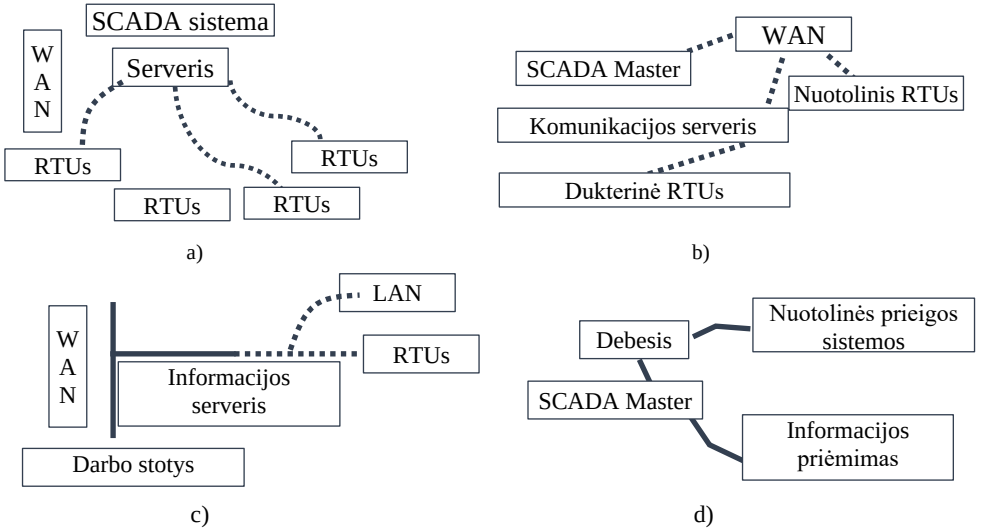
1.15 pav. Užfiksuotų incidentų skaičius 1982–2018 metais (Ahmadian et al., 2020)
Fig. 1.15. Number of recorded incidents by 1982–2018 year (Ahmadian et al., 2020)

Hierarchinėje taksonominėje struktūroje yra sąvoka, vadinama neeiliniu įvykiu. Norint suprasti, kam ji skirta, reikia išanalizuoti jau žinomus pažeidimus ir būdus.

Incidentus galima suskirstyti į tyčinius ir netyčinius. Netyčiniai incidentai daugiausiai buvo dėl nekompetentingų ir neapgalvotų žmonių sprendimų. Tokių sprendimų pavyzdžiai Černobylio atominė elektrinė (1986 m.), eksperimentas „Aurora“ Aidaho nacionalinėje laboratorijoje (2007 m.), 2009 m. hidroelektrinė Sibire ir pan. Šių incidentų poveikis buvo katastrofiškas: nuo žmonių mirties iki aplinkos užteršimo.

Ne taip seniai pasaulis sužinojo apie naują grėsmę – kibernetinę, kylančią dėl gerai apgalvotų veiksmų. Kiekvienais metais šių pavojų skaičius auga. Grėsmės tampa sudėtingesnės ir sunkiai atpažįstamos sistemoje.

Šiai problemai skirta daugybė straipsnių ir tyrimų, kuriuose buvo nagrinėjami gyvybiškai svarbių objektų kibernetinių išpuolių ypatumai. SCADA priežiūros ir kontrolės sistema yra naudojama dabartiniams procesams ir duomenims kritinėje infrastruktūroje stebėti ir valdyti. Tyrėjai tikisi, kad iki 2020 m. SCADA sistema kainuos iki 300 milijonų eurų, todėl reikės sudėtingesnės stebėjimo ir kontrolės sistemos, kad būtų galima išspręsti nenumatytas ir neapibrėžtas situacijas (Tariq et al., 2019). Norint taikyti šią sistemą šiuolaikiniame pasaulyje, ji turi prisitaikyti prie besivystančių technologijų ir procesų, o tai reiškia, kad SCADA sistema turi atitikti aukštus standartus. SCADA sistemos plėtrą (1.16 pav.) galima suskirstyti į keturis etapus:



1.16 pav. SCADA sistemos plėtra (Tariq et al., 2019)
Fig. 1.16. SCADA system development (Tariq et al., 2019)

a) pirmos kartos – monolitinė su nuotoliniu terminalu;
b) antros kartos – paskirstyta SCADA sistema;
c) trečios kartos – tinkle sujungta SCADA sistema;
d) ketvirtos kartos – *IoT Cloud* pagrįsta sistema.

Analizuojama hierarchinė taksonominė sistema, leidžianti klasifikuoti išpuolius, ir ją galima pritaikyti bet kokiems organizacijos reikalavimams. Šios sistemos tyrinėtojai tvirtina, kad sistemos parametrus galima keisti, išplėsti ar sureguliuoti. Remiantis šiuo metodu, galima atlikti statistinį ir analitinį tyrimą, žinant kibernetinių išpuolių tendencijas. Aišku, turėtų būti pasaulinė duomenų bazė, kurioje visi išpuoliai būtų užfiksuoti ne tik prieš valstybines įstaigas, bet ir prieš privatųjį sektorių. Toks analizės metodas labiau tiktų ekspertams ir analitikams, kurie galėtų rengti statistiką, teikti pasiūlymus ir problemų sprendimus, tirdami incidentus ir jų padarinius.

Kibernetinio saugumo valdymas turi būti visapusiškas. Tai nėra tik techninis klausimas.

1.5. Pirmojo skyriaus išvados

1. Nagrinėjant egzistuojančias kibernetinio saugumo sampratas, galima matyti, kad nėra bendros kritinės infrastruktūros sąvokos. Įvairių valstybių požiūriai į kritinę infrastruktūrą priklauso nuo skirtingų poreikių ir sąlygų. Nepriklausomai nuo skirtingų požiūrių į kritinę infrastruktūrą, galima rasti bendrą dalyką, su kuriuo sutinka visos valstybės, tai poveikis, kuris gali būti padarytas dėl kritinės infrastruktūros sunaikinimo arba sutrikdymo, saugumui, valstybės ekonomikai ir visuomenei. Analizuojant kibernetinio saugumo sampratas buvo išskirti pagrindiniai jų principai – apsaugoti kibernetinę aplinką nuo išpuolių ir užtikrinti konfidencialumą, vientisumą ir prieinamumą. Kibernetinis saugumas yra vienas iš svarbiausių šiuolaikinio gyvenimo aspektų. Siūloma analizuoti kibernetinį saugumą ne tik iš techninės pusės, bet ir organizacinės / strateginės, nes bet kurios sistemos, ypač kritinės infrastruktūros, pažeidžiamumas atsiranda greitai, ir šis procesas daro įtaką nacionalinei bei pasaulinei sistemai.
2. Apibendrinus tyrimo duomenis, galima teigti, kad požiūris į kibernetines grėsmes skiriasi kiekvienoje šalyje, o didėjantis pražūtingų epizodų skaičius skatina didžiules investicijas į kibernetinio saugumo strategijas bei technologijas. Pagal statistinius duomenis Lietuvoje didžiausios kibernetinės problemos – kenkėjiška programinė įranga ir nesaugios informacinės sistemos, kurios papildo viena kitą bei padidina išpuolių riziką. Tačiau pagrindinis kibernetinio saugumo pažeidimų veiksnys išlieka

žmogus, kurio dėka 95 % saugumo problemų kyla dėl netyčinių klaidų ar netinkamų veiksmų.

3. Analizuojant įvairių valstybių požiūrį į kritinę infrastruktūrą, galima pastebėti, kad energetikos sektorius yra neatsiejama kritinės infrastruktūros dalis. Visos valstybės suprato, kad energetikos sektorius yra viena iš sudedamųjų dalių, nuo kurių priklauso ne tik valstybės ekonomika, bet ir saugumas. Bet koks šio elemento sutrikdymas arba sunaikinimas, ir nesvarbu, ar fizinis, ar nuo kenkėjiškų programų arba užpuolimų, turėtų didelę įtaką bet kurios valstybės saugumui.
4. Įvertinus kibernetinio saugumo valdymą kritinėje energetinėje infrastruktūroje, atsižvelgiant į esamą standartą, kuriame pateikiamos rekomendacijos, kaip pranešti ir reaguoti į kibernetinius incidentus, nustatyta, kad kibernetines grėsmes labai sunku nustatyti ir laiku imtis prevencinių priemonių. Esami kibernetinio saugumo valdymo modeliai nesuteikia tinkamos apsaugos reaguojant į kibernetines atakas, netikėtus scenarijus ir pažeidžiamumus, todėl itin svarbu kibernetinio saugumo problemas spręsti kritinėse situacijose, siekiant apsaugoti pagrindinius valstybės interesus. Galima padaryti išvadą, kad reikia platesnio ir išsamesnio požiūrio į kibernetinio saugumo valdymo modelį.
5. Kritinė infrastruktūra turi daug skirtingų pramonės sektorių tarpusavio priklausomybių bei santykių tarp partnerių. Taigi galima teigti, kad, atsižvelgiant į fizines ar kitas ryšių technologijas, ICS veikia kaip tarpusavyje susijusi sistema. Norint padidinti atsparumą rizikai, reikia įgyvendinti stiprią įrangos tiekimo grandinę, kad galima būtų valdyti kibernetinį saugumą ir įvairius susijusius aspektus. Veikla, skirta atsparumui ir efektyvumui pagerinti, apima bendrosios komunikacijos protokolų kūrimą, pranešimą apie pažeidžiamumą pardavėjui ir atsakomybės už reagavimą į kibernetinio saugumo incidentus priskyrimą. Be to, įvairių apribojimų įgyvendinimas, glaudus bendradarbiavimas su pagrindiniais tiekėjais, jų įtraukimas į tobulinimo procesus leidžia tinkamai valdyti tiekimo grandinę ir pagerinti savo infrastruktūros kibernetinį saugumą.
6. Daugelis šalių neturi strategijų, kaip reaguoti į kibernetinius incidentus ir netikėtus scenarijus, bei neįvertina savo pažeidžiamumo. Atliktuose moksliniuose tyrimuose bandyta ieškoti būdo, kaip užtikrinti kritinės infrastruktūros kibernetinį saugumą. Vien technologiniai sprendimai neišsprendžia visų problemų, todėl reikia aiškiai apibrėžti visus standartus, sukurti Kibernetinę nacionalinio saugumo strategiją ir būtinai bendradarbiauti – valstybės, tarptautiniu ir privačiojo sektoriaus lygmeniu. Siekiant mažinti kibernetinius išpuolius, siūloma sukurti priemonę, kuri padės užtikrinti kibernetinio saugumo valdymą ir kuri gali būti naudojama bet kuriai kritinei infrastruktūrai.

2

Kritinės energetinės infrastruktūros kibernetinio saugumo valdymo praktikos kitose valstybėse

Šiame skyriuje nagrinėjamos skirtingų šalių gerosios praktikos, turinčios įtaką kritinės energetinės infrastruktūros kibernetiniam saugumui, ir kibernetinio saugumo valdymo modelio pritaikymas. Taip pat analizuojamos kritinės energetinės infrastruktūros silpnosios vietos, naudojant pasiūlytą kibernetinio saugumo valdymo modelį.

Skyriaus tematika paskelbti trys autoriaus straipsniai (Plėta et al., 2020; Plėta et al., 2020; Tvaronavičienė et al., 2020; Tvarovavičienė et al., 2020).

2.1. Kibernetinio saugumo aspektai, didinantys ir gerinantys kibernetinį atsparumą

Atsižvelgiant į tikrovę, kurioje gyvenama, būtina reglamentuoti kritinės infrastruktūros objektų apsaugą tam, kad būtų užtikrintas aukštesnis apsaugos lygis nuo visų rūšių galimų grėsmių. Sudėtinga atsakyti į klausimą, ar infrastruktūros ob-

jektų sauga yra pakankama, nes nėra pakankamos informacijos apie techniką, kurią naudoja kibernetiniai nusikaltėliai. Todėl negalima 100 % garantuoti, kad kritinė infrastruktūra yra saugi (Aradau, 2010).

Vadovaudamiesi kritinės infrastruktūros apibrėžimu pagal JAV ar ES įstatymus, galime nustatyti, kas daro infrastruktūrą kritinę. Ji apibrėžiama kaip turinti daug skirtingų pramonės sektorių, tarpusavio priklausomybes ir santykius tarp jų. Taigi, galima teigti, kad, atsižvelgiant į fizines ar kitas ryšių technologijas, ICS veikia kaip tarpusavyje susijusi sistema, o bet koks įvykis gali tiesiogiai ar netiesiogiai paveikti kitas infrastruktūros dalis (Newbill, 2019).

ICS veikia kaip neatskiriama kritinės infrastruktūros dalis ir naudojama palengvinti operacijas gyvybiškai svarbiose pramonės šakose, tokiose kaip elektros, naftos ir dujų, vandens tiekimo, transporto, gamybos ar chemijos. ICS naudojama ne tik pramoninės automatikos sistemose, atsakingose už duomenų rinkimą, vizualizavimą ir pramoninių procesų kontrolę, bet yra ir kibernetinių-fizinių sistemų dalis, naudojama kritinei infrastruktūrai valdyti. Šiuolaikinės pramoninės valdymo sistemos yra sudėtingos socialinės ir techninės sistemos, apimančios aparatinę įrangą, pavyzdžiui, programuojamus loginius valdiklius ir nuotolinius telemetrijos įrenginius (angl. *Remote terminal unit* (RTU)) bei programinę įrangą, skirtą tokios aparatūros, sąveikaujančios su fiziniu procesu, valdymo logikai įgyvendinti. Pastarąjį dešimtmetį susirūpinimas dėl galimų kibernetinių atakų kritinėse infrastruktūrose labai išaugo. Šiems kibernetiniams incidentams kritinės infrastruktūros sektoriuose būtų galima iš dalies užkirsti kelią užtikrinant visišką tinklo ir sistemų matomumą naudojant saugos valdymo sistemą. Garsiausias pavyzdys yra kibernetinis išpuolis prieš Ukrainos elektros tinklą 2015 m. Ekspertų teigimu, tokiame išpuolyje buvo pasinaudota programinės ir techninės įrangos, tinklo architektūros, taip pat žmogiškųjų ir organizacinių aspektų pažeidžiamumu ir sukelta papildoma rizika (Burge, 2023).

2015 m. išpuolis prieš tris energijos skirstymo bendroves Ukrainoje (*Kievoblenergo, Prykarpatyoblenergo* ir *Chernovtsyoblenergo*) sukėlė neplanuotą elektros energijos tiekimo nutraukimą, kuris truko kelias valandas ir paveikė apie 225 000 vartotojų. Nelaimingų atsitikimų tyrimas paskatino bendradarbiauti įvairias žvalgybos grupes, kurios pranešė, kad būtent kibernetinis išpuolis sutrikdė energijos valdymo sistemą. Tokie patvirtinimai yra labai svarbūs, nes incidentas buvo pirmasis sėkmingas kibernetinis bandymas sutrikdyti elektros energijos tiekimą ir sutrikdė visą elektros tinklą. Todėl šios bylos svarstymas turi didelę reikšmę tolesniems apmąstymams, kurie paprastai apima kibernetinio saugumo aspektus.

Tokių išpuolių negalima likviduoti taikant tradicinius saugumo sprendimus. Norint valdyti riziką (taikyti rizikos valdymo būdus), reikia įgyvendinti stiprią įrangos tiekimo grandinę, kad galima būtų valdyti kibernetinį saugumą ir įvairius susijusius aspektus (Park & Walstrom, 2017).

Įvairiuose elektros infrastruktūros objektuose naudojamos pramoninės valdymo sistemos, susijusios su gamybos veikla, tokia kaip šilumos reguliavimas, mechaninis valdymas, avarinis išjungimas ir kt. OT sistema kontroliuoja ir prižiūri tokią infrastruktūrą kaip gamyba, komunalinės paslaugos bei gynyba ir sukuria infrastruktūrą, kuri valdo konkrečius įrenginius ir procesus. Kritinė energetinė infrastruktūra yra vienas iš sektorių, kuriame galima rasti operacinių technologijų sistemas. Paprastai kritinės energetinės infrastruktūros aplinkoje neįmanoma valdyti sistemų ir užtikrinti operacijų saugumo. Paradoksalu, tačiau kritinėse infrastruktūrose naudojamos OT sistemos dažnai veikia su pasenusia programine įranga ir pasenusia aparatūra, todėl jas sunku pataisyti ir jos labai pažeidžiamos kibernetiniu aspektu. Anksčiau kibernetinis saugumas nebuvo būtinybė dėl nepakankamo sistemų ir interneto sąveikavimo. Tokios aplinkybės sukūrė uždarą tinklą, kuris nėra veikiamas išorinių grėsmių. Tačiau, plečiantis skaitmeninėms inovacijoms ir IT, ir OT konvergencijai, tai tampa sudėtingu tinklu, kuriame skirtingi saugumo sprendimai negali keistis informacija ir suteikti visišką matomumą sprendžiant konkrečias problemas (Hahn, 2016).

Kritinės infrastruktūros saugumo valdymo kontekste IT ir OT tinklai yra atskirti. Sukuriami du tinklo saugumo planai, kurių kiekvienas yra atsakingas už savo tinklo dalies apsaugą. Todėl pašalinamas saugumo strategijų skaidrumas ir dubliavimas, susijęs su skirtingomis OT ir IT techninėmis charakteristikomis. Tai apsunkina įrangos, prijungtos prie kritinės infrastruktūros tinklo, identifikavimą ir rizikos bei saugumo spragų paiešką. Egzistuoja keli alternatyvūs būdai įvertinti OT sistemą, įskaitant pasyvų tinklo pažeidžiamumo izoliavimą arba pasyvią tinklo analizę naudojant jutiklius, prijungtus prie tinklo įrangos. OT tinklus sunku efektyviai valdyti, kadangi tinklai turi kritinių kibernetinio saugumo spragų. Kiekvienas kibernetinio saugumo aspektas yra būtinas norint sumažinti riziką kritinės energetinės infrastruktūros aplinkoje, ypač atsižvelgiant į OT tinklą, kurį bent iš dalies galima pagerinti įgyvendinant saugos valdymą. Pramonės kibernetinio saugumo rinka, apimanti kritinės infrastruktūros sistemų saugumą, ICS aplinką ar kitus IT ir OT tinklo komponentus, yra labai konkurencinga ir greitai auganti sritis. Remiantis pranešimais, šis sektorius iki 2023 m. pasieks daugiau nei 24 mlrd. dolerių. Todėl didesnis dėmesys kibernetinio saugumo aspektams kritinėje infrastruktūroje paprastai rodo patikimo tiekimo grandinės valdymo poreikį, kuris padidintų atsparumą įvairioms rizikoms. Pagrindinis uždavinys yra apibrėžti saugumo schemą, kuri galėtų efektyviai sumažinti riziką OT tinkluose. Kritinės energetinės infrastruktūros, jos įrangos tiekėjų, visos CEI tiekimo grandinės, saugumo įvertinimas leidžia nustatyti, ar OT struktūros pasiekia geriausią savo tinklų apsaugos praktiką, ir nurodyti jų galimybę sumažinti sistemos saugumo riziką (IT vs OT Security..., 2023).

Naujausias leidinys „Pagrindinės kibernetinės tiekimo grandinės rizikos valdymo praktikos: pramonės pastebėjimai“ apie kibernetinių tiekimo grandinių valdymą ir saugumą, kurį pateikė Nacionalinis standartų ir technologijų institutas (angl. *National institute of standards and technology* (NIST)), yra pagrindas toms organizacijoms, kurios turi pradėti spręsti kibernetinių tiekimo grandinių valdymo problemą (Information security..., 2012). Jame aprašytas geriųjų praktikų ir įrankių rinkinys, pagrįstas pramonės tyrimais, atliktais 2023 m. NSTI gairėse pateikiami apmąstymai apie kibernetinio tiekimo grandinių valdymo integraciją visoje organizacijoje, kuriant aiškius bendrus kibernetinio tiekimo grandinės, kibernetinio produkto ir fizinio saugumo vaidmenis bei struktūras. Tai apibrėžia tiekimo grandinės ir kibernetinio saugumo ryšio svarbą (NIST, 2023).

Labai svarbu įtraukti į nenumatytų atvejų planavimą, reagavimą ir atkūrimą pardavėjus, produktus bei turtą ar objektus. Veikla, skirta atsparumui ir efektyvumui pagerinti, apima bendrosios komunikacijos protokolų kūrimą, pranešimą apie pažeidžiamumą pardavėjui ir atsakomybės už reagavimą į kibernetinio saugumo incidentus pasiekiamumą. NSTI leidiniuose apie „Geriausią kibernetinių tiekimo grandinių rizikos valdymo praktiką“ taip pat nagrinėjami įvairūs kibernetinio saugumo aspektai, įskaitant kibernetinės tiekimo grandinės valdymą. Atsižvelgiant į padėtį Ukrainoje, svarbiausios rekomendacijos yra susijusios su stebėjimo programomis, stebinčiomis visus infrastruktūros komponentus ir sistemas. Nors šis aspektas daugiausia apima įrangos kilmės nustatymą, tai taip pat suteikia galimybę bendrai stebėti IT ir OT sistemas (Information security..., 2012).

SANS (angl. *Escal institute of advanced technology*) institutas yra mokslinių tyrimų, tirianti kibernetinių tiekimo grandinių rizikos valdymą ir siūlanti būdus, kaip sušvelninti (pvz., Ukrainoje) įvykusių išpuolių pasekmes. Norint išvengti tokių kenkėjiškų programų, dažnai rekomenduojamas baltasis programų sąrašas, kuris gali būti efektyvus ICS aplinkose, jei ICS pardavėjas sutinka jį naudoti. Be to, įvairių apribojimų įgyvendinimas, glaudus bendradarbiavimas su pagrindiniais tiekėjais, jų įtraukimas į tobulinimus leidžia tinkamai valdyti tiekimo grandinę ir pagerinti savo infrastruktūros kibernetinį saugumą (SANS Information..., 2023).

2.2. Kritinės infrastruktūros kibernetinio saugumo valdymo spragų nustatymas ir vertinimas

Šiandieną susiduriama su daugybe iššūkių nacionaliniam saugumui, pavyzdžiui, kibernetinėmis atakomis, kurios tampa vis labiau apčiuopiamos ir galingesnės. Todėl strateginis prioritetas yra kritinė energetinė infrastruktūra, kuri gali susidurti su daugybe naujų grėsmių. Norint kritinę energetinę infrastruktūrą apsaugoti reikia parengti veiklos tęstinumo planą, kuriame bus pasiūlytos galimų grėsmių prevencijos ir apsaugos priemonės fizinės saugos, ryšių ir technologijų saugumo

srityje. Gyvybiškai svarbių paslaugų teikimo užtikrinimas, susidūrus su naujomis grėsmėmis, yra ne tik valstybės, bet ir privačių įmonių pareiga (Lightman, 2022).

Kritinės energetinės infrastruktūros atakos tampa vis dažnesnės. Šiuolaikinių kibernetinių atakų ypatumas yra jų tikslingumas ir orientacija į konkrečią veiklos sritį ar atskirą įmonę. Dažniausiai kibernetinė ataka atrodo visai įprastai: blogiausiu atveju vartotojo ekrane pasirodo pranešimas, kad jo kompiuteris užšifruotas ir reikalaujama sumokėti išpirką. Kai kuriais atvejais nevyksta nieko – daugelis kenkėjiškų programų stengiasi būti kuo tylesnės ir nepastebimos, kad pavogtų kuo daugiau vertingos informacijos, kol jos yra nepastebėtos (2022 metų Nacionalinė kibernetinio saugumo būklės ataskaita, 2023).

Šiuo metu nėra sukurtas kibernetinio saugumo valdymo modelis, kuris leistų reaguoti į kibernetines atakas, netikėtus scenarijus ir pažeidžiamumą, todėl labai svarbu kibernetinio saugumo klausimus spręsti kritinės infrastruktūros kontekste, siekiant apsaugoti pagrindinius valstybės interesus (Limba et al., 2017), aptariant ne tik teisinius aspektus, bet ir išanalizuojant praktinius, kurie kartu su normomis, taisyklėmis ir nuostatomis padės apsaugoti kritinę energetinę infrastruktūrą nuo išpuolių.

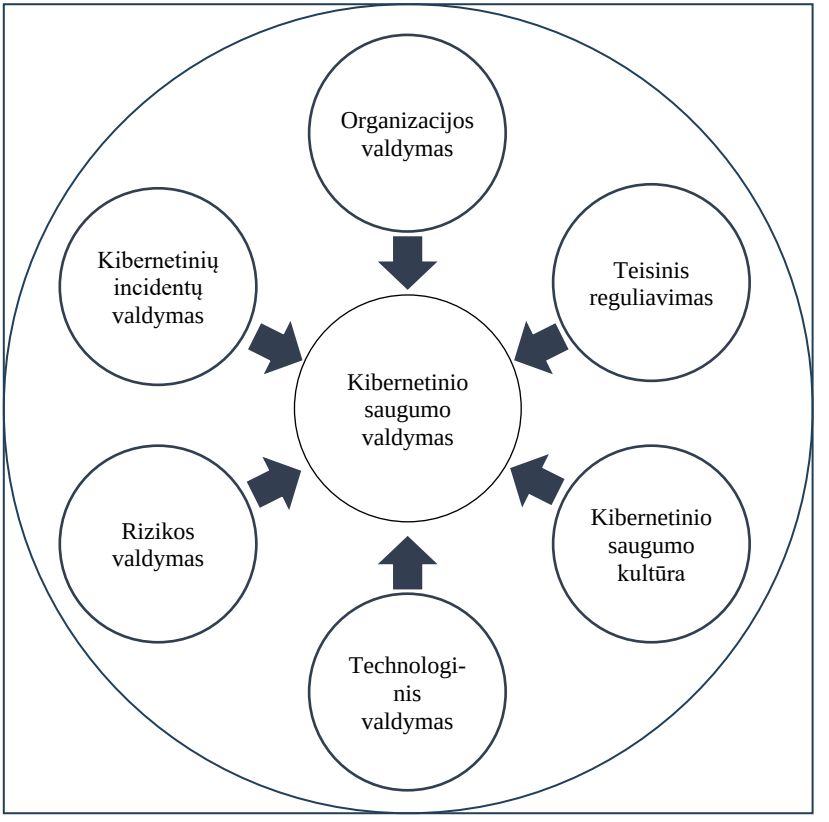
Dažniausias kritinėje energetinėje infrastruktūroje pasitaikančias klaidas galima palyginti ir įvertinti pagal tam tikrus kriterijus, kurie sudaro teorinį kibernetinio saugumo valdymo modelį, naudojamą bet kuriai kritinei infrastruktūrai (2.1 pav.).

Iš pradžių kibernetinio saugumo valdymo modelis buvo siejamas su pramoninių valdymo sistemų apsauga nuo kibernetinių atakų. Siūlomas modelis suteikia supratimą apie informacinių technologijų vystymąsi saugumo požiūriu, atsižvelgiant ne tik į operacines technologijas, bet ir į operacinių ir informacinių technologijų susijungimą dėl pramoninių technologijų skaitmenizavimo. Problema, kurią pabrėžia Limba et al. (2017), yra ta, kad būtina sukurti saugumo modelį, kuris galėtų atsižvelgti į OT ir IT technologijas, taip pat apimtų valdymo sistemą, galinčią palaikyti kibernetinio saugumo aspektus (Limba et al., 2017). Be to, Limbos (2017) ir kitų autorių, tarp jų ir šios disertacijos autoriaus, pasiūlytame modelyje ypatingas dėmesys skiriamas kibernetinio saugumo technologijų valdymo aspektams. Šio komponento naudojimas padeda suprasti ir klasifikuoti kiekvieną įmonės komponentą ir iš jo kylančius pažeidžiamumus.

Modelis susideda iš šešių pagrindinių komponentų, kurie yra vienodai svabūs ir turi būti tobulinami kartu, kad padarytų didelę įtaką organizacijos saugumui. Kiekvienas komponentas turi būti identifikuotas, įvertintas, suprojektuotas ir organizacija turi parengti planą, kaip spręsti kiekvienoje kibernetinio saugumo valdymo modelio srityje kylančias problemas.

Teisinis reguliavimas susijęs su teisiniais procesais ir teisinių aktų reikalavimais, tokiais kaip saugumo instrukcijos, atsakingų už informacijos saugumą pareigybių aprašymai ir kt. (Limba et al., 2017) Organizacijos valdymas suteikia

supratimą apie gaires, kurios turėtų būti naudojamos tiesiogiai reaguojant į kibernetines atakas. Rizikos valdymas suteikia supratimą apie būtinybę sumažinti kibernetinių incidentų poveikį ir analizuoti augančias rizikas. Kibernetinio saugumo kultūra yra svarbi kiekvienai organizacijai, nes kiekvienas organizacijos darbuotojas turi suprasti, kas yra saugumas (Limba et al., 2017). Penktas modelio kriterijus – technologinis kibernetinis saugumas – yra susijęs su kiekvieno IT valdomo komponento žiniomis, o šeštas – kibernetinių incidentų valdymas – daugiau su specialiųjų planų, taikomų įvykus incidentui, parengimu.



2.1 pav. Kibernetinio saugumo valdymo modelis (Limba et al., 2017)
Fig. 2.1. Cyber Security Management Model (Limba et al., 2017)

Komponentai yra suskirstyti į lygmenis, atsakingus už konkrečius veiksmus, būtinus kibernetiniam saugumui užtikrinti. Pavyzdžiui, *pradiniu lygmeniu* organizacija nustato problemas, kurias reikia išspręsti, naudodama kibernetinio sau-

gumo modelį, analizuoja teisines problemas, turinčias įtakos kibernetiniam saugumui, apibrėžia organizacijos politiką, peržiūri valdymo sistemą ir nustato, kuris skyrius ar asmuo dalyvauja sprendimų priėmimo procese. Taip pat organizacija analizuoja vidines ir išorines rizikas, turinčias įtakos organizacijos veiklai, bei darbe naudojamas technologijas, mokosi suprasti, kad bet kuri organizacija gali nukentėti dėl technologinių ar socialinių aspektų, o tai yra pagrindas tobulinti organizacijos kibernetinį saugumą (Katina et al., 2023).

Vidutiniu lygmeniu aiškiai apibrėžti teisiniai aspektai ir darbo instrukcijos, organizacinė struktūra su aiškiomis atsakomybėmis, detalūs kibernetinių incidentų planai (kas ir kada atsakingas už kokius veiksnius, kaip vykdoma komunikacija ir pan.), žmogiškųjų išteklių valdymo planai ir įgūdžiai, kuriuos privalo turėti kiekvienas organizacijos narys, aiški informacija apie organizacijos naudojamą programinę įrangą ir technologijas, įskaitant naudotą (seną) įrangą. Kiekvienas padalinys ar organizacijos narys turėtų žinoti sistemos atkūrimo planą sėkmingos kibernetinės atakos atveju. Taip pat turėtų būti laiku atliktas kibernetinio saugumo modelio auditas ir atnaujinti planai (Limba et al., 2017).

Aukščiausiu lygmeniu kibernetinio saugumo valdymo modelį naudojančią organizaciją galima palyginti su misiją vykdančia kariuomene, nes kiekvienas kibernetinio saugumo modelio komponentas yra neatsiejama jo dalis ir suteikia galimybę išmokti valdyti incidentus bei sumažinti jų poveikį organizacijai ir jos dalyviams. Kartu gerinama organizacijos reputacija, nes jei jai rūpi kibernetinis saugumas, ji yra patrauklesnė vartotojams (Limba et al., 2017).

Modelis sukurtas taip, kad pradinį ir vidutinį lygmenis sudarantys veiksmai gali būti įgyvendinami atskirai, nejungiant tikslų ir parengtų tobulinimo planų. Kiekvienas modelio komponentas sąveikauja tarpusavyje ir kiekvienas organizacijos narys atlieka tam tikrą vaidmenį (Limba et al., 2017). Ir visa tai kartu gerina kibernetinį saugumą, leidžiantį organizacijai pasiekti aukščiausią lygmenį. Pasiekus šį lygmenį galima teigti, kad organizacija atlaiko kibernetines atakas ir supranta, kad pasaulis keičiasi labai greitai, o naujos technologijos gali pasenti per vieną naktį.

Integruodama šį modelį, organizacija gali susidurti su sunkumais dėl technologijų ir vadybos nesupratimo, nes technikos specialistai ir valdybos specialistai dažnai nesupranta vieni kitų. Organizacija turi keistis, kad geriau suprastų kibernetinių nusikaltimų pasaulį ir kibernetinio saugumo tendencijas, laikyti kibernetinį saugumą kaip valdymo rūpestį ir laiku išbandyti bei atnaujinti modelio komponentus.

Nors pastebimos bei pateikiamos tam tikros rizikas, bei galime kalbėti apie nedidelį kibernetinių atakų prieš kritinę infrastruktūrą skaičių. Vis dėlto situacija kitokia: žinome šimtus dokumentuotų tokių išpuolių atvejų visame pasaulyje. Atakos prieš tokius tinklus vyksta dešimtmečius. Tačiau yra kibernetinių atakų, kurios patraukia dėmesį dėl savo masto ar sudėtingumo. Analizuodamas

pastarojo dešimtmečio kibernetines atakas, noriu atkreipti dėmesį į garsiausius kibernetinius išpuolius prieš kritinę energetinę infrastruktūrą, atrinktus dėl nustatytų atakuojamų tinklų organizavimo ir saugumo trūkumų.

Prieš pradedant analizuoti žinomas kibernetines atakas prieš kritinę energetinę infrastruktūrą, norisi priminti kai kuriuos įvykdytus išpuolius, kurie padarė nemenką žalą tiek finansiškai, tiek fiziškai.

1992 m. atleistas *Chevron* naftos kompanijos darbuotojas įsilaužė į kompiuterius, atsakingus už viešojo informavimo sistemas Niujorko ir San Chosės biuruose, perkonfigūruodamas jas taip, kad paleidus sukeltų avariją. Apie tai nebuvo žinoma tol, kol Redmonde, Kalifornijoje, įvyko toksinis išsiliejimas, dėl kurio tūkstančiams žmonių kilo didelis pavojus (*Terrorism 2.0...*, 2011).

1994 m. rugpjūčio mėnesį Lane Jarret Davis sugebėjo įsilaužti į *Salt River Project* tinklą ir gauti prieigą prie informacijos, ištrynęs failus, atsakingus už vandens ir elektros energijos stebėjimą bei teikimą. Įsilaužėlis gavo prieigą prie klientų ir įmonės darbuotojų asmeninių ir finansinių duomenų (Turk, 2005).

1997 m. kovo 10 d. buvo užfiksuotas įsilaužimas į Vusterio oro uosto valdymo sistemą (JAV, Masačusetsas), kuris sukėlė sistemos gedimą, dėl kurio šešioms valandoms buvo nutrauktas telefono ryšys. Kontrolės bokštas, oro uosto priešgaisrinė gelbėjimo tarnyba ir kitos kompanijos, įsikūrusios oro uosto teritorijoje, liko be telefono ryšio.

Buvęs Maručio vandens sistemos (Australija) darbuotojas gavo dviejų metų laisvės atėmimo bausmę už tai, kad 2000 m. įsilaužė į vandens valdymo sistemą, dėl kurios milijonai litrų nuotekų pateko į netoliese esančią upę, užtvindant ir vietinį viešbutį (Cohen, 2021).

2001 m. buvo užpulta Amerikos kompanijos pastatyta dujų perdirbimo gamykla. Šešis mėnesius trukęs tyrimas parodė, kad ataką įvykdė vienas iš tiekėjų, kuris, siekdamas nuslėpti savo klaidą, nusprendė nukreipti dėmesį įsilaužęs į tris įmonės kompiuterius ir išjungdamas dujų tiekimą vienoje Europos šalyje (Stergiopoulos et al., 2020).

2002 m. gruodžio mėnesį Venesuelos naftos kompanija PDVSA buvo užpulta. Dėl įsilaužimo naftos gamyba sumažėjo nuo 3 milijonų iki 370 tūkstančių barelių per dieną. 2008 m. 14-metis studentas įsilaužė į Lenkijos miesto Lodžės tramvajų tinklą. Keturi tramvajai nuvažiavo nuo bėgių, dvylika žmonių buvo sužeista (Electronic Sabatoge of Venezuela Oil Operations, 2002).

Išpuolių istorija rodo, kad įsilaužimas į kritinę infrastruktūrą prasidėjo dar tada, kai internetas ir informacinės technologijos mūsų gyvenime nebuvo taip plačiai paplitę. Apibendrinant pateiktą informaciją galima matyti, kad būtent kritinės infrastruktūros objektai tampa kibernetinių atakų taikiniais.

Tolesnei analizei buvo pasirinkti garsiausi kibernetinių atakų įvykiai prieš kritinę energetinę infrastruktūrą. Pirmas nagrinėjamas atvejis yra *Stuxnet* byla. Tai viena iš pirmųjų užfiksuotų kibernetinių atakų, nukreiptų į atominę elektrinę, kaip

vieną iš svarbiausių kritinės energetinės infrastruktūros objektų. Praėjus beveik dešimtmečiui kaltininkas vis dar nenustatytas ir vis dar nėra galiojančio sprendimo dėl kenkėjiškos programinės įrangos poveikio (Stuxnet, 2023).

Antrasis atvejis – *Shamoon* kenkėjiška programa yra įdomi tuo, kad *Saudi Aramco* kompanija buvo kelis kartus užpulta naudojant tą pačią kenkėjišką programinę įrangą – 2012 ir 2017 m. Šiame darbe ypatingas dėmesys skiriamas 2012 m. atakai, nes tai pirmoji ataka, kuri sudaro galimybę išnagrinėti organizacijos veiksmus į kibernetinį išpuolį (Dehlawi & Abokhodair, 2013).

Trečias atvejis – šalis, kuri ne kartą buvo kibernetinių atakų ir kitų hibridinio karo priemonių taikiniu, – Ukraina. Kalbant apie Ukrainos atvejį, būtų netikslinga analizuoti kibernetines atakas, neatsižvelgiant į ten per pastarąjį dešimtmetį vykusius įvykius. 2015 m. kibernetinis išpuolis prieš elektros energijos tinklus yra Ukrainos piliečiams padarytos fizinės žalos pavyzdys (Power grid cyberattack in Ukraine, 2015).

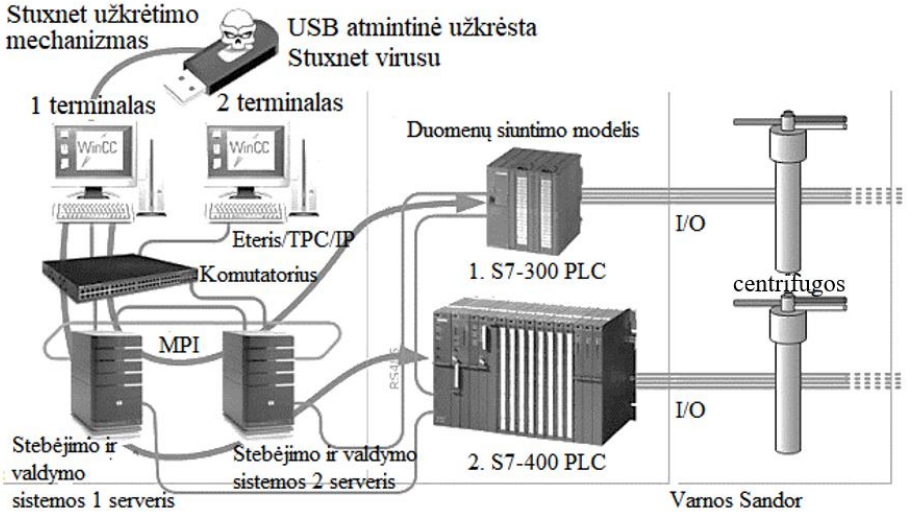
Kiekvienas išpuolių atvejis yra kaip energetinės infrastruktūros kibernetinio saugumo iššūkis, kurį reikia analizuoti ne tik atsižvelgiant į pasekmes, bet ir į tai, kad nėra tinkamo reagavimo plano bei apsaugos. Bet kokia kenkėjiška programa, patekusi į infrastruktūrą, sukelia fizinius sutrikimus, kurie tiesiogiai gali paveikti valstybę ir piliečius. Nepaisant technologijų gausybės, ne visada pavyksta rasti kaltininką ir teisingą sprendimą, kaip išvengti kibernetinių išpuolių. Apžvelgiant žymiausius kritinės energetinės infrastruktūros kibernetinius išpuolius galima matyti, su kokiais iššūkiais susiduria valstybės ir jų kibernetinės saugos specialistai.

Pirmoji analizuojama ataka yra 2010 m. aptiktas kirminas *Stuxnet*, kurio pagrindinis tikslas buvo sutrikdyti Irano branduolinių objektų veiklą. Ataka prieš Irano atominę elektrinę ir urano sodrinimo gamyklą Natanze įvyko tuo metu, kai tarp JAV ir Irano kilo įtampa (Beazner & Patrice, 2017). Nors oficialūs vykdytojai dar nerasti, o virusas sugebėjo išplisti ir užkrėsti apie 100 000 kompiuterių (Falliere, 2011), jame buvo kai kurių elementų, dėl kurių Iranas tapo puolimo taikiniu. Kenkėjiška programa buvo užprogramuota užkrėsti SCADA sistemas, ypač PLC, kurios buvo sugrupuotos į grupes po 164 objektus, ir panaudota Natanzo gamykloje su 164 centrifugomis. Išpuolis buvo sėkmingas, nes gamybai buvo naudojama programinė įranga, pritaikyta kompiuteriniams tinklams, neturintiems sąsajų su internetu (Beazner & Patrice, 2017).

Įvedus kenksmingą kodą, išpuolio procesas gali skirtis nuo konfidencialios informacijos gavimo iki tiekimo grandinės keitimo, kartu apgaunant gamyklos operatorius, imituojant tinkamą veikimą, lyg procesas veikia kaip įprasta (Ayral, 2016). Tačiau norint efektyviai valdyti PLC, būtina suprasti jo struktūrą ir veikimą. *Stuxnet* kirminų atvejis yra pavyzdys, kad penkių–dešimties programuotojų komandai prireikė mažiausiai šešių mėnesių, kad sukurtų programą, skirtą Irano atominės elektrinės ir urano sodrinimo įrenginių PLC (Beazner & Patrice, 2017). Išnaudodami keturis nulinės dienos pažeidžiamumus, įsilaužėliai sugebėjo perimti

sistemos kontrolę ir išplatinti kenkėjišką kirminą daugiau nei 10 000 kompiuterių (Falliere, 2011).

Išpuolis tapo įmanomas įvedant išorinius kenkėjiškus kodus, kurie sutrikdė sistemą (2.2 pav.). Analizuojant padarytas klaidas, galima pasakyti, kad pagrindiniai trūkumai šiuo atveju – tai testavimo ir komunikavimo nebuvimas. Virusas išplito naudojant netinkamai patikrintas technines ir organizacines saugumo priemones, būtinas sisteminiams trūkumams nustatyti, modeliuojant ir įvertinant nulinės dienos pažeidžiamumą *Microsoft Windows* operacinėje sistemoje. Komunikacijos trūkumas susijęs su organizacijos elgesiu išpuolio metu ir po jo. Kadangi pati ataka greičiausiai buvo politiškai motyvuota, nes buvo nukreipta į Irano urano sodrinimo objektus, Iranas ne iš karto viešai pranešė apie atakų pasekmes. Iranui oficialiai nepripažinus, kad kai kurie asmeniniai kompiuteriai buvo užkrėsti virusu, be jokio paaiškinimo staiga buvo sustabdyta sodrinto urano gamyba (Beazner, 2017). Komunikacijos trūkumas yra dažna atakuojamų organizacijų klaida, nes pripažinimas, kad jos tapo kibernetinės atakos auka, gali pakenkti jų viešajam įvaizdžiui. Todėl tendencija neatskleisti jokių detalių apsunkina virusų šalinimo ir sistemos atkūrimo procesą. *Stuxnet* atveju programuojamu loginiu valdikliu valdomos centrifugos buvo fiziškai pažeistos. Iš 6000–9000 centrifugų, naudojamų Natanzo gamykloje, turėjo būti pakeistos 1000 (De Falco, 2012).



2.2 pav. *Stuxnet* išplėtimas, sudaryta remiantis (Varnos Sandor, 2017)
Fig. 2.2. Stuxnet extension (Varnos Sandor, 2017)

Rekomenduojamos geriausiosios praktikos tokio tipo atakoms yra sutelkti dėmesį į kibernetinių incidentų valdymo strategiją, nes ataką įvykdė užpuolikai, turintys skaitmeninius sertifikatus, leidžiančius nepastebėtai prisijungti prie sistemos (Beazner & Patrice, 2017). Kuriant efektyvią apsaugos sistemą pirmiausia reikia apsvarstyti darbo grupių sukūrimą, jos turėtų tikrinti protokolus ir bendrą SCADA sistemų saugumą. Labai svarbu kiekvienam prie sistemos prijungtam įrenginiui nustatyti šifravimą ir abipusį autentifikavimą (De Falco, 2012). Taip pat labai svarbu laikytis griežtų skaitmeninių sertifikatų valdymo taisyklių, tokių kaip privataus rakto saugojimas ir sertifikatų kokybė.

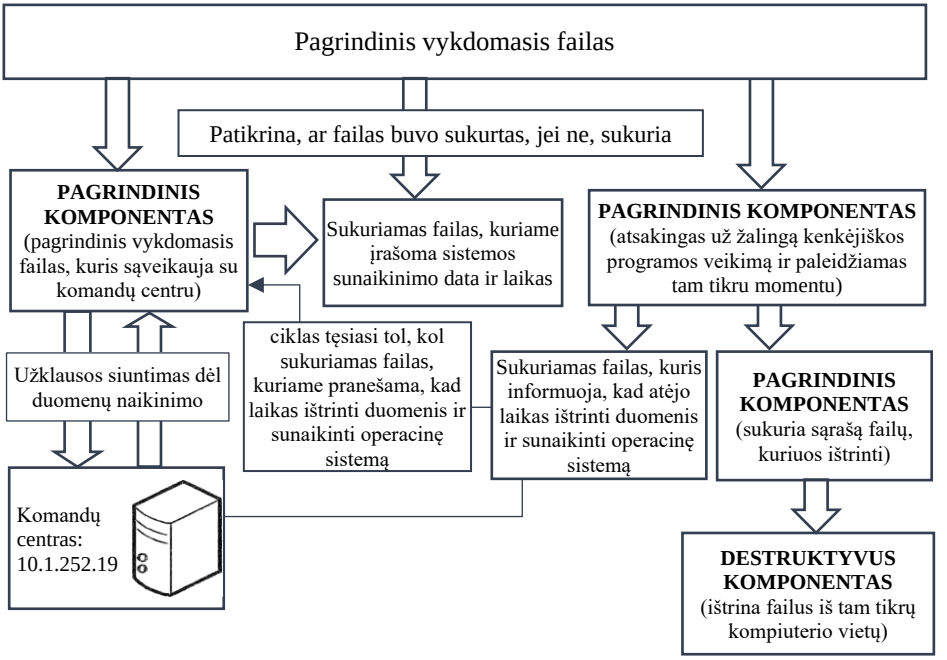
Išanalizavus šį išpuolį, galima daryti išvadą, kad pagrindinės vadovybės klaidos buvo susijusios su komunikacija ir viešinimu, sistemos testavimo trūkumu. Nacionalinėms institucijoms netolygus ir neaiškus bendravimas turėtų būti kaip nepriimtinas elgesys kritinėje energetinėje infrastruktūroje: skaidrumas ir bendradarbiavimas yra esminiai dalykai, užtikrinantys pasirengimą tinkamai reaguoti. Sistemos trūkumai, ypač nulinės dienos pažeidžiamumas, leido įsilaužėliams įterpti kenkėjiškas programas ir paveikti PLC veikimą. Nuolatinis sistemų testavimas yra būtinas norint aptikti galimus sistemos trūkumus ir juos pašalinti, nekeliant pavojaus visai infrastruktūrai.

Antrojo tipo išpuolis, kuris bus analizuojamas, yra 2012 m. *Shamoon* kenkėjiška programa, kuri buvo nukreipta prieš didžiausią pasaulyje naftos kompaniją *Saudi Aramco*, įsikūrusią Saudo Arabijoje. Kenkėjiška programa, dar žinoma kaip *W32.Disttrack*, susideda iš trijų komponentų – kontaktas, ištrynimas (valymas) ir siuntimas (angl. *dropper, wiper, reporter*) ir paveikė maždaug apie 30 000 kompiuterių *Saudo Aramco* gamykloje (Wuuest, 2014). Kontaktas *Dropper* yra pagrindinis komponentas, kuris kopijuoja kitus komponentus į užkrėstą kompiuterį, taip pat kiekvieną kartą nukopijuoja ir paleidžia *save* atidarius *Windows* operacinę sistemą. Valymas *Wiper,* antrasis komponentas, yra destruktyvus modulis, kuris ištrina failus iš tam tikrų kompiuterio vietų. Išsiuntęs informaciją užpuolikui, modulis perrašo failus sugadintais JPEG failais. Paskutinis komponentas yra siuntėjas *reporter,* kuris siunčia informaciją atgal į užpuoliko centrinį kompiuterį (Mackenzie, 2012) (2.3 pav).

Tikėtina, kad ataką organizavo nenustatytas asmuo, gavęs prieigą prie vartotojų kredencialų ir domeno valdiklio (Wuuest, 2014). Nors asmuo ir buvo palyginamas su *Stuxnet* kenkėjiška programa, nusikaltėliai buvo apibūdinti kaip „patyrę mėgėjai“ dėl savo žemesnių kompetencijų ir programavimo įgūdžių (Onyeji et al., 2014). Nagrinėjamas išpuolio tipas yra išplėstinė nuolatinė grėsmė (angl. *Advanced Persistent Threat* (ATP)), kuri reiškia, kad užpuolikai rado administratorių slaptažodžius ir gavo prieigą prie aukštesnių sistemos lygių (Alshathry, 2017).

Klausimai, kurie buvo svarstomi šiuo atveju, buvo susiję su organizacijos reagavimu į kibernetinį išpuolį ir realiu išpuolio poveikiu organizacijos sistemai. Po kibernetinio išpuolio bendrovė pranešė, kad sumažino savo elektroninių sistemų

kiekį išorėje, kad išvengtų tolesnių išpuolių. *Saudi Aramco* (2015) pareiškė, kad, nepaisant duomenų sunaikinimo iš serverio, fizinis pažeidimas nebuvo užfiksuotas ir įmonės atkūrimas buvo baigtas (Rashid, 2015; Alshathry, 2017). Tačiau, net ir paskelbus apie visišką atsigavimą, buvo užfiksuotas organizacijos svetainės neveikimas (Onyeji et al., 2014).



2.3 pav. *Shamoon* kenkėjiškos programos veikimo principas (sudaryta remiantis Securelist.com, 2012)
Fig. 2.3. Shamoon operating principle of the malicious program (based on Securelist.com, 2012)

Kaip ir pirmuoju atveju, pagrindinė šio puolimo problema yra komunikacijos trūkumas, t. y. organizacijos elgesys atakos metu ir po jos. Informacija apie išpuolį buvo dalinė, virusas išplito už organizacijos ribų, prarandant gręžimo ir gamybos duomenis. Gręžimo procedūros generuoja didžiulį duomenų kiekį, kuris siunčiamas į *Saudi Aramco* duomenų bazę. Po to duomenys apdorojami, filtruojami ir rankiniu būdu siunčiami du kartus per dieną. Tikėtina, kad dėl šventės Ramadanas nebuvo atsarginių gręžimo ir gamybos duomenų kopijų, o filtruoti duomenys buvo prarasti (Onyeji et al., 2014).

Bendrovė paskelbė apie visišką atsigavimą beveik iš karto po atakos, siekdama patikinti kitus tiekėjus ir klientus, kad žala nedidelė. Tai nebuvo teisingas

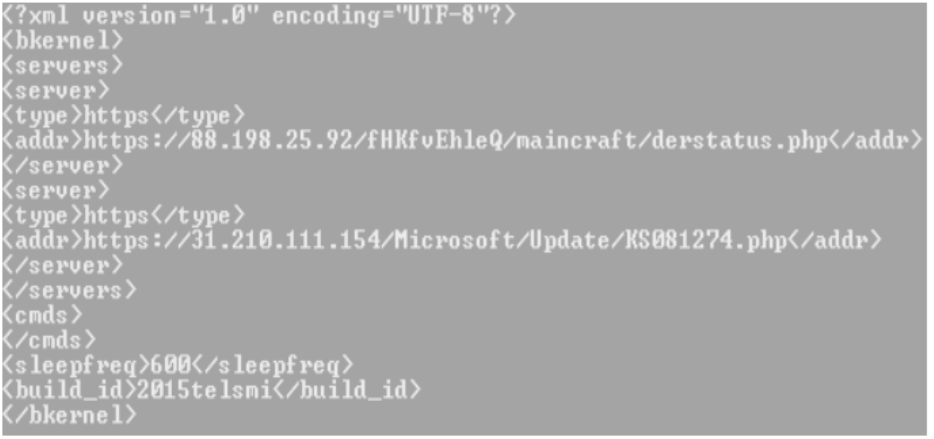
sprendimas reaguojant į kibernetines atakas, ypač kritinėje energetinėje infrastruktūroje.

Pagrindinė kibernetinio incidento valdymo problema, nustatyta šiame scenarijuje, yra saugumo ir komunikacijos trūkumas. Dėl atsarginių kopijų nebuvimo sistemose buvo sunaikintos interneto svetainės ir duomenys. Valdant kibernetinius incidentus, siūlomi problemos sprendimo būdai turėtų būti įgyvendinti jau pasirengimo etape. Efektyviausias būdas šiuo atveju – atsarginės kopijos turėjimas (angl. *redundancy*), alternatyvi reakcija į nesėkmingą būklę. Esant kritinei energetinei infrastruktūrai, sistemos gedimas gali sukelti fizinę žalą, todėl labai svarbu užtikrinti homogenišką procesą. *Redundancy* yra atsarginės sistemos kopijos turėjimas, kuris nuolat atnaujinamas, kad „atspindėtų“ naudojamus komponentus ir gedimo atveju perimtų valdymą (ICS Engineering Inc., 2017). Atsarginės kopijos turėtų būti privalomos kritinėse energetinėse infrastruktūrose, nes pagreitina atsigavimo procesą po išpuolio.

Paskutinis, trečiasis, analizuojamas kibernetinis puolimas įvyko 2015–2016 m. Ukrainoje ir buvo nukreiptas prieš Ukrainos energetikos sistemą. Išpuolis įvyko įsilaužus į įmonės kompiuterį ir SCADA sistemą (E-ISAC, 2016). 2015 m. gruodžio 23 d. trims valandoms buvo išjungta maždaug 30 elektros pastočių, dėl to nutrūko elektros energijos tiekimas trijose regioninėse skirstomųjų tinklų įmonėse – *Kievoblenergo*, *Prykarpatyeoblenergo* ir *Chernivtsyoblenergo*, nuo maitinimo šaltinio atjungus daugiau nei 200 000 vartotojų (FireEye, 2016).

Užpuolikai, turintys aukštą kvalifikaciją ir naudodami daugybę techninių komponentų, pasitelkę sukčiavimo agentą (angl. *phishing*) gavo prieigą prie tinklo. Kitas žingsnis buvo įdiegti *BlackEnergey 3* kenkėjišką programinę įrangą, kad pavogtų kredencialus iš įmonių tinklų, įskaitant virtualius privačius tinklus (angl. *Virtual private network* (VPN)), jog būtų galima prisijungti prie ICS tinklo. Gavę prieigą, užpuolikai naudojo esamus nuotolinės prieigos įrankius komandoms duoti iš nuotolinės stoties ir modifikuotą *KillDisk* standžiojo disko šalinimo programą, kad ištrintų organizacijos užpultas sistemas. Elektros tiekimo sutrikimą sukėlė veikiantys nepertraukiamo maitinimo šaltiniai (angl. *Uninterruptible power supplies* (UPS)), kurie paprastai teikia avarinį maitinimą nutrūkus elektrai, tačiau dėl viruso veikiantys maitinimo šaltiniai padidino apkrovą ir sukėlė gedimą. Paskutinis išpuolio etapas buvo DDoS (angl. *Denial-od-service attack*) ataka prieš pagalbos centrą, kad klientai nepraneštų apie iškilusią problemą (Anatomy of a SCADA..., 2022).

Analizuojant klaidas, lėmusias ataką, valdymo požiūriu, galima teigti, kad jų buvo daug tiek pasirengimo, tiek išpuolių metu. Įsilaužėliai panaudojo įvairias galimybes – nuo viešai prieinamos informacijos apie naudojamos ICS sistemos tipą iki abipusio VPN autentifikavimo trūkumo. Be to, žiniasklaidoje atsirado informacija, kad šie objektai neturi tinklo saugumo stebėjimo sistemų ir niekas negali rankiniu būdu kontroliuoti ICS tinklo (E-ISAC, 2016).



2.4 pav. 2015 m. *BlackEnergy* konfigūracijos pavyzdys (sudarytas remiantis Securelist.com, 2015)
Fig. 2.4. BlackEnergy configuration example (based on Securelist.com, 2015)

Apibendrinant galima teigti, kad pirmiausiai reikia stiprinti tinklo saugumo stebėjimo galimybes, nes užpuolikai sugebėjo valdyti sistemą, kuri nekontroliavo savo prieigos taškų (FireEye, 2016). Antra, įgyvendinti atsakomybės apimties apribojimą, užtikrinant, kad tik vienas operatorius galėtų valdyti kai kuriuos sistemos komponentus, o tai gali apriboti įsilaužėlių galimybes valdyti žmogaus ir mašinos sąsają (angl. *Human-machine interface* (HMI)). Galiausiai, abipusių autentifikavimo, blokų grandinės technologijos arba taikomųjų programinių įrangų įtraukimo į baltąjį sąrašą įgyvendinimas gali pagerinti saugią sistemos prieigos kontrolę.

Informacinių ir operacijų technologijų konvergencija lėmė naują internetinių sistemų koncepciją ir daugybę naujovių kritinės infrastruktūros valdymo srityje (Kumar et al., 2023). Kartu su naujovėmis atsiranda ir nauja kibernetinio saugumo koncepcija – dirbtinio intelekto panaudojimas, kuris tampa efektyviu įrankiu tiek IT, tiek OT požiūriu. Pasaulinė tendencija rodo, kad kritinė energetinė infrastruktūra turėtų tapti vienu pagrindinių kibernetinių atakų taikinių, todėl prioritetas – gerinti jos apsaugą ir informuoti apie bendrą nepasirengimą kuriant efektyvią kritinės energetinės infrastruktūros kibernetinio saugumo strategiją. Įvairių kibernetinių išpuolių prieš kritinę energetinę infrastruktūrą analizė atskleidė organizacijų reakcijas ir valdymo klaidas rengiantis kibernetiniams išpuoliams ir reaguojant į juos.

Kaip jau buvo minėta, kibernetinio saugumo srityje svarbų vaidmenį atlieka žmogiškasis faktorius: tai viena iš pagrindinių kibernetinių atakų priežasčių dėl žinių trūkumo, neatidumo ir netinkamo elgesio. Kibernetinių atakų analizė parodė, kad visais kibernetinių užpuolimų atvejais informacija nebuvo atskleista dėl

politinio konflikto pobūdžio. Tokio tipo klaidos kartu su saugumo problemomis yra pavojingiausios kritinėms energetinėms infrastruktūroms, nes jos ne tik pažeidžia atakuojamos organizacijos vientisumą, bet ir neleidžia tirti taikomų metodų ar technologijų, tai sudaro galimybę leisti įsilaužėliams veikti kitur. Tinkamas reagavimas į kibernetinius incidentus reikalauja aiškios komunikacijos ir bendradarbiavimo nacionaliniu ir tarptautiniu lygiu.

Nagrinėjant žinomas kibernetines atakas prieš kritines infrastruktūras, siekiant visapusiškai įvertinti jų saugumą, būtina išanalizuoti duomenis naudojant anksčiau aprašyto kibernetinio saugumo modelio komponentus, kurie padės suprasti ir klasifikuoti kiekvieną įmonės komponentą ir iš jo kylančius pažeidžiamumus (Choraś et al., 2016). Atsižvelgiant į šią aplinkybę, šio modelio naudojimas kibernetinio saugumo efektyvumo požiūriu gali būti naudingas analizuojant kibernetines atakas šioje dalyje, o kitame skyriuje kai kurių šalių gerąsias praktikas. Šio modelio pritaikymo praktikoje rezultatai pateikti 2.1 lentelėje, kurioje atakų atvejų analizės metu nustatyti trūkumai pažymėti X.

2.1 lentelė. Nustatytos kibernetinio saugumo spragos (sudaryta remiantis (Limba et al., 2017)
Table 2.1. Cybersecurity gaps identified (based on Limba et al., 2017)

	Organizacijos valdymas	Teisinis reguliavimas	Kibernetinio saugumo kultūra	Rizikos valdymas	Technologinis kibernetinis	Kibernetinių incidentų valdymas
1 atvejis (*Stuxnet*)	×			×		
2 atvejis (*Shamoon*)		×	×			×
3 atvejis (Ukraina 2015 m.)	×		×			

Analizuojant 2.1 lentelėje pateiktus duomenis, galima matyti, kad kiekvienu aprašytu atveju yra spragų, kurias reikia spręsti. *Stuxnet*, pirmoji analizuota kibernetinė ataka, yra įdomus organizacijos saugumo modelio pažeidimo atvejis. Organizacija susidūrė su komunikavimo ir saugumo problemomis, tačiau šį atvejį galima pritaikyti prie 2.1 lentelėje pateiktos analizės. 2.1 lentelė gerai atsispindi, kad *Stuxnet* atvejis (1 atvejis) parodo organizacijos ir rizikos valdymo spragas. Tinkamas valdymas yra labai svarbus patikimam kibernetiniam saugumui. Bet kokia organizacijoje planuojama veikla turi būti įvertinta saugumo požiūriu. *Stuxnet* atvejis parodė Natanzo elektrinės sistemos pažeidžiamumą, o organizacija, atrodo, neteikė prioriteto galimoms kibernetinėms spragoms. Tokio pat tipo pažeidžiamumas užfiksuotas ir 3 atveju (2015 m. ataka Ukrainoje), nes šiuo atveju

kibernetinė ataka buvo įvykdyta naudojant sukčiavimo el. laiškus, o tai reiškia, kad sistema nebuvo pakankamai apsaugota. Kalbant apie rizikos valdymo spragą, užfiksuotą *Stuxnet* atveju, saugumo ir testavimo trūkumas lėmė daug nulinės dienos pažeidžiamumų, kuriuos vėliau panaudojo įsilaužėliai, norėdami į sistemą įvesti kenkėjiškus kodus (Falliere, 2011).

Nagrinėjant antro atvejo rezultatus, galima matyti komunikacijos, teisinio reguliavimo, kibernetinio saugumo kultūros ir incidentų valdymo spragas. Kenkėjiška programa pažeidė *Saudi Aramco* naftos gamyklos sistemą ir iš daugelio kompiuterių ištrynė duomenis, tačiau gręžimo ir gamybos duomenų atsarginių kopijų stoka padidino žalą. Integruotos (nerankinės) atsarginės kopijos sistemos nebuvimas ir tai, kad darbuotojai netikrino filtruotų duomenų, lėmė kibernetinio saugumo kultūros spragas. Ukrainos atvejis (3 atvejis) taip pat parodė kibernetinio saugumo kultūros spragas, dėl kurių objektų tinklų kontrolė buvo gauta naudojant sukčiavimo programas. Kalbant apie incidentų valdymą, *Shamoon* kenkėjiška programa buvo blogai valdoma bendraujant su valdžios institucijomis, nes organizacija perdavė tik dalį informacijos (Onyeji et al., 2014).

Apibendrinant galima teigti, kad tiek organizacijos kibernetinis valdymas, tiek kibernetinio saugumo kultūra yra tikslingiausi kibernetinio saugumo spragų matavimai, nes ir kibernetinis valdymas ir kibernetinio saugumo kultūra turėjo lemiamą vaidmenį dviejuose iš trijų analizuotų atvejų. Svarbu pažymėti, kad net šešių kategorijų kibernetinio saugumo valdymo modulio vis dar nepakanka, kad apimtų visus svarbiausios kritinės energetikos infrastruktūros aspektus. Kol kas nėra skaičiavimų, kuriais remiantis būtų pasiūlyti tinkami rodikliai kibernetinio saugumo poveikiui matuoti. Ši analizė gali būti vienas iš daugelio elementų, į kuriuos reikia atsižvelgti, pavyzdžių.

2.3. Kritinės infrastruktūros kibernetinio saugumo valdymo geruųjų praktikų pavyzdžiai

Kadangi kibernetiniai išpuoliai laikomi augančiu reiškiniu, ypač išsivysčiusiose šalyse, daugelis valstybių nusprendė įgyvendinti naujas strategijas, kuriose atsižvelgiama į kibernetinį saugumą tiek privačioje, tiek viešojoje srityje. Tarptautinės telekomunikacijų sąjungos (angl. *International telecommunication union* (ITU)) duomenimis, 2018 m. pabaigoje internetu naudojosi 3,9 milijardo žmonių (ITU, 2019), o tai rodo, kad virtuali erdvė kasmet vis labiau auga ir ją reikia saugoti. Pasaulio šalys paskelbė Nacionalines kibernetinio saugumo strategijas (angl. *National cybersecurity strategy* (NCSS)), kurios padės apsaugoti kibernetinę erdvę nuo kibernetinių išpuolių.

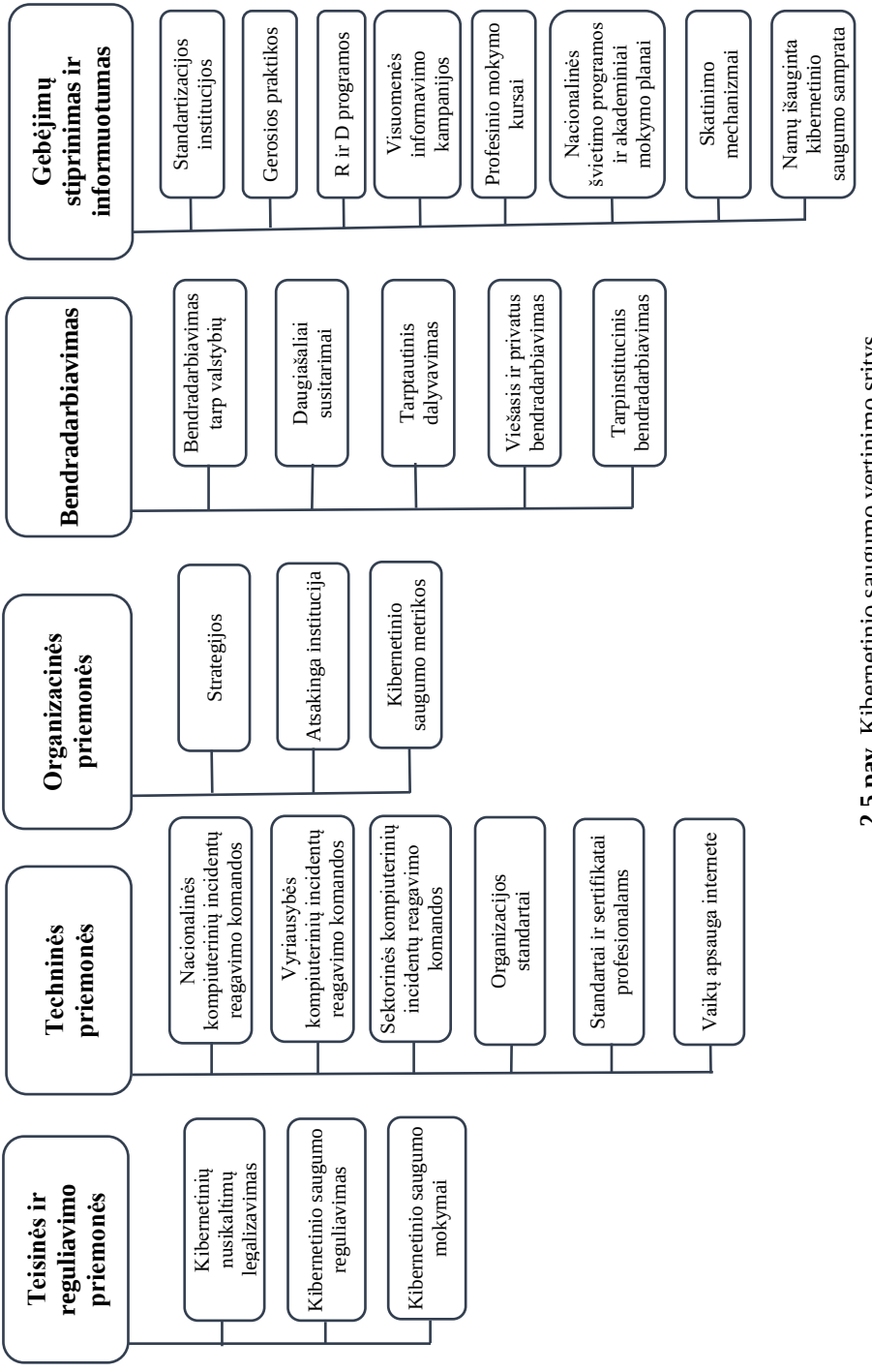
„Kritinės infrastruktūros“ apibrėžimas įvairiose šalyse gali skirtis, tačiau galima surasti bendrų juos vienijančių reikšmių, pavyzdžiui, „visuomenės naudojamos paslaugos, objektai ir įrenginiai, kurių gedimas ar netinkamas veikimas gali sukelti neigiamų pasekmių visuomenei“ (Izycki & Colli, 2019). Nors ankstesni išpuoliai daugiausia buvo nukreipti į informacinės technologijos aplinką, dabartinė tendencija rodo, kad kibernetinė rizika šiuo metu yra didesnė operacinių technologijų aplinkoje. Nors kibernetinių puolimų rizika egzistuoja ir didėja, daugelis šalių neįgyvendina konkrečių kibernetinio saugumo planų, apimančių kritinės infrastruktūros objektų apsaugą, ir nepripažįsta, kad reikalinga tinkama tiekimo grandinės struktūra ir pagalba kibernetinės atakos metu ir po jos.

Norint įvertinti kritinės energetinės infrastruktūros problemą kaip nacionalinės kibernetinės saugumo strategijos spragą, būtina išanalizuoti ir palyginti nacionalinės kibernetinės saugumo strategijos sprendimus ir pokyčius penkiose skirtingose šalyse. Šalys parenkamos pagal 2019 m. paskelbtą pasaulinį kibernetinio saugumo indeksą (angl. *Global cybersecurity index* (GCI)). Sąrašas sudarytas įvertinus šalies įsipareigojimus ir plėtrą kibernetinio saugumo sprendimams.

PKSI yra patikimas etalonas, įvertinantis šalių įsipareigojimą kibernetiniam saugumui pasauliniu lygiu, siekiant geriau suvokti problemos svarbą ir įvairius jos aspektus. Kadangi kibernetinis saugumas yra platus, apimantis skirtingų sektorių, kiekvienos šalies išsivystymo lygį arba šalių įsitraukimas vertinamas penkiose pagrindinėse srityse (2.5 pav.), turinčiose vienodą reikšmę skaičiuojant galutinį rezultatą (ITU, 2019), tai taikomos:

1. Teisinės ir reguliavimo priemonės – su kibernetiniu saugumu susijusių teisinių institucijų ir struktūrų buvimas.
2. Kibernetinio saugumo valdymas ir standartai (techninės priemonės) – su kibernetiniu saugumu susijusių techninių institucijų ir struktūrų buvimas.
3. Organizacinės priemonės – koordinuojančios institucijos politikos buvimas.
4. Gebėjimų stiprinimas ir informuotumas – mokslinių tyrimų ir plėtros programos prieinamumas, švietimas ir mokymai.
5. Bendradarbiavimas – partnerystės ir bendradarbiavimo sistemos buvimas.

PKSI rezultatai (2.2 lentelė) rodo bendrą visų penkių kibernetinio saugumo sričių pagerėjimą ir stiprėjimą, išlaikant regionines kibernetinio saugumo spragas. Todėl, atsižvelgus į PKSI skaičiavimo rezultatus, susumavus kiekvienoje kibernetinio saugumo srityje gautus balus ir surūšiavus šalis mažėjimo tvarka (2.2 lentelė), tolimesnei analizei ir kibernetinio saugumo valdymo modelio testavimui (aprobavimui) buvo atrinktos pirmosios penkios daugiausiai balų surinkusios šalys. Anot ITU (2019), šios šalys, palyginti su kitomis, žymiai pagerino ir sustiprino kibernetinį saugumą pasauliniu mastu, įgyvendindamos geriausią įmanomą praktiką.



2.5 pav. Kibernetinio saugumo vertinimo sritys
Fig. 2.5. Areas of cyber security assessment

Pirmąsias penkias pasaulio reitingo sąrašo vietas iš eilės užima šios šalys: Jungtinė Karalystė, Jungtinės Amerikos Valstijos, Prancūzija, Lietuva ir Estija (ITU, 2019) (2.2 lentelė).

2.2 lentelė. 2019 m. GCI indeksas, sudarytas iš dešimties labiausiai įsipareigojusių pasaulio šalių, sudaryta remiantis ITU, 2019)
Table 2.2. GCI index of the ten most committed countries in the world in 2019 (based on ITU, 2019)

		Vertinami balais					
Vieta	Valstybė	GCI balai	Teisinis	Techninis	Organizacinis	Gebėjimų stiprinimas	Bendradarbiavimas
1	Jungtinė Karalystė (JK)	0,931	0,200	0,191	0,200	0,189	0,151
2	Jungtinės Amerikos Valstijos (JAV)	0,926	0,200	0,184	0,200	0,191	0,151
3	Prancūzija	0,918	0,200	0,193	0,200	0,186	0,139
4	Estija	0,908	0,200	0,168	0,200	0,185	0,155
5	Lietuva	0,905	0,200	0,195	0,186	0,170	0,153
6	Singapūras	0,898	0,200	0,186	0,192	0,195	0,125
7	Ispanija	0,896	0,200	0,180	0,200	0,168	0,148
8	Malaizija	0,893	0,179	0,196	0,200	0,198	0,120
9	Norvegija	0,892	0,191	0,196	0,177	,0185	0,143
9	Kanada	0,892	0,195	0,189	0,200	0,172	0,137
10	Australija	0,890	0,200	0,174	0,200	0,176	0,139

Kibernetinio saugumo valdymo modelis, kuriuo remiantis buvo analizuojamos pasirinktų šalių kibernetinio saugumo strategijos spragos, susideda iš šešių komponentų, kurių kiekvienas įvertina konkrečią funkciją, reikalingą tinkamai kibernetinio saugumo valdymo modelio struktūrai. Teisinis reguliavimas įvertina organizacijos supratimą apie kibernetinį saugumą, jo tikslus ir reikalingą planavimą; rizikos valdymas įvertina organizacijos gebėjimą identifikuoti augančią riziką ir parengti adekvatų atsaką (rizikos valdymo būdus). Kiti, ne mažiau svarbūs,

komponentai yra kibernetinio saugumo kultūra, kuri įvertina kiekvieno organizacijos nario kibernetinio saugumo supratimo lygį; technologinis valdymas susijęs su visų organizacijos elementų ir jų pažeidžiamumų žiniomis; incidentų valdymas susietas su incidentų valdymo planu.

Įvertinus pirmas penkias atrinktas šalis pagal GCI, sudarytas reitingas, pagal kurį galima nustatyti geriausią ir blogiausią strategiją turinčias šalis. Kibernetinio saugumo pasirengimo lygiui nustatyti paimti dokumentai iš oficialų šaltinių, jeigu konkrečių dokumentų nėra, naudojamos nacionalinės kibernetinės saugumo strategijos.

Kadangi šios analizės tikslas – nustatyti esamas nacionalinių kritinės infrastruktūros objektų strategijų spragas, šiam tikslui buvo atrinktos šalys, kurios įgyvendino geriausią įmanomą praktiką pagal Pasaulinį kibernetinio saugumo indeksą. Toliau pateikta pasirinktų šalių kibernetinio saugumo strategijų trumpa analizė.

Jungtinė Karalystė. Pagal pasaulinį kibernetinio saugumo indeksą (GCI) JK sąraše užima pirmąją vietą (ITU, 2019). Toks pasirinkimas atspindi rimtą šalies įsipareigojimą investuoti į kibernetinį saugumą. 2015 m. Vyriausybė paskelbė Nacionalinio saugumo strategiją bei gynybos ir saugumo strateginę apžvalgą (HM Government, 2016), kurioje yra skyrius „Kritinė nacionalinė infrastruktūra (CNI) ir energetinis saugumas“. Strategijoje aprašyti veiksmai, kuriuos atliekant CNI galima padaryti atsparią būsimoms grėsmėms, tokioms kaip elektros energijos tiekimo nutraukimas ir panašiai (HM Government, 2015). Be to, Vyriausybė įsteigė Nacionalinį infrastruktūros apsaugos centrą, kurio tikslas sumažinti nacionalinės infrastruktūros pažeidžiamumą (National Cyber Security Centre, 2020).

Analizuojant JK požiūrį į kritinės infrastruktūros apsaugos valdymo aspektus, paaiškėjo, kad pagrindiniai dokumentai yra antrasis ir trečiasis jungtinio nacionalinio saugumo komiteto, kibernetinio saugumo įgūdžių strategijų ir JK svarbios nacionalinės infrastruktūros pranešimas (Joint Committee on the National Security Strategy, 2018). Dokumentai patvirtina, kad Vyriausybė 2016 m. paskelbė Nacionalinę kibernetinio saugumo strategiją 2016–2021 m., skyriuje „plėtra“ nurodomi „sisteminiai kibernetinių įgūdžių deficito klausimai“ (Joint Committee on the National Security Strategy, 2018). Užfiksuotos problemos yra susijusios su išsilavinimo ir kompetencijų kibernetinio saugumo tema stoka (Joint Committee on the National Security Strategy, 2018). Nėra pakankamai JK piliečių, turinčių reikiamų įgūdžių ir gebėjimų dirbti kritiniame nacionalinės infrastruktūros sektoriuje (Joint Committee on the National Security Strategy, 2018). Trečiojoje ataskaitoje taip pat teigiama, kad Vyriausybės kritinės nacionalinės infrastruktūros apibrėžimas yra per platus ir nepadeda nustatyti labiausiai saugotinų infrastruktūros objektų / sektorių (Joint Committee on the National Security Strategy, 2018).

Taikant kibernetinio saugumo valdymo modelio komponentus JK nacionalinio kibernetinio saugumo strategijos analizei, galima pasakyti, kad oficialios institucijos pripažįsta kritinės infrastruktūros objektų saugą. Dokumente „Kibernetinio saugumo strategija“ vienas iš tikslų yra „apsaugoti mūsų kritinę nacionalinę infrastruktūrą ir kitus prioritetinius sektorius“ (Tvaronavičienė et al., 2020). JK Vyriausybė skelbia, kad reikalinga reguliavimo sistema, bet nepateikia papildomos informacijos. Analizuojant rizikos valdymą, pateikta šiek tiek bendrų gero valdymo elementų (Tvaronavičienė et al., 2020). Dokumente (The UK Cyber ..., 2011) pateikiami procedūros ir planavimo procesai, avarinių operacijų kontroliniai sąrašai ir atsakomybė. Tačiau dėl kritinių situacijų įvairovės pateikta informacija yra per bendra, kad būtų pasirinktos tinkamos procedūros. Kalbant apie saugumo kultūrą, galima matyti, kad dokumentuose yra bendri paaiškinimai apie skirtingų kibernetinių išpuolių tipus, kuriuos gali patirti bet kokia organizacija (Cyber Security Toolkit..., 2020). Tačiau procedūrų, aprašytų dokumentuose, galėtų laikytis tik kitos organizacijos. Analizuojant technologinį ir incidentų valdymą, reikia pažymėti, kad nėra jokių sprendimų ar konkrečių dokumentų, susijusių su kritine infrastruktūra.

Jungtinės Amerikos Valstijos. Antroji šalis pasaulyje pagal kibernetinį saugumą yra Jungtinės Amerikos Valstijos. JAV Vyriausybė kibernetiniam saugumui skyrė Vidaus saugumo departamentą, Kibernetinio saugumo ir infrastruktūros saugumo agentūrą (angl. *Cybersecurity and infrastructure security agency* (CISA), turinčią Nacionalinį infrastruktūros apsaugos planą (angl. *National infrastructure protection plan* (NIPP)) (CISA, 2021), kad suformuotų konkrečią ir išsamią CIP strategiją. Yra daug dokumentų, skirtų kritinei infrastruktūrai: svetainė siūlo plačią prieigą prie pagrindinių paslaugų ir galimybių (Cyber Incident Reporting ..., 2022). Jungtinių Amerikos Valstijų nacionalinio saugumo departamentas teikia pirmenybę infrastruktūros vertinimams atlikti, kad padėtų organizacijoms priimti sprendimus, teikti ir dalytis informacija tarp viešojo ir privačiojo sektorių. Kitas svarbus aspektas yra mokymai ir bendradarbiavimo tarp valstybių pratybos vietiniu ir nacionaliniu lygmeniu, taip pat rengiant ypatingos svarbos infrastruktūros saugumo mokymus (CISA, 2021).

Svarbiausias dokumentas yra NIPP 2013 (CISA, 2020), „Partnerystė siekiant užtikrinti infrastruktūros objektų saugumą ir atsparumą“ (NIPP, 2013), kuriame aprašoma, kaip Vyriausybė ir privatusis sektorius turi elgtis, kad pasiektų CIP. Šis dokumentas yra ankstesnės NIPP versijos, paskelbtos 2006 m., raida ir joje pateikiamos gairės, kaip pasiekti integruotą ir bendradarbiaujantį požiūrį į saugią ir efektyvią ypatingos svarbos infrastruktūrą. Dokumentas suskirstytas į penkis skyrius: vizija, misija ir tikslai, kuriuose nagrinėjami pagrindiniai kritinės infrastruktūros principai, ypatingos svarbos infrastruktūros aplinka, kurią sudaro politika, rizika ir partnerystės struktūra, reikalinga tikslams pasiekti, pagrindiniai principai,

aprašantys NIPP principus, bendradarbiavimas rizikos valdymo srityje, apibūdinant rizikos valdymo veiklos pagrindą, ir galiausiai raginimas veikti visai kritinės infrastruktūros bendruomenei (NIPP..., 2020).

Teisinio reguliavimo komponentas pagal kibernetinio saugumo modelį vertinamas atsižvelgiant į saugos instrukcijas darbuotojams, informacijos pateikimą saugumo pareigūnams bei tinklo administratoriams, standartus (Limba et al., 2017). JAV dokumentuose siūlomas platus standartų pasirinkimas, tačiau svarbiausias yra „Kritinės infrastruktūros kibernetinio saugumo gerinimo sistema“ (Boyens et al., 2021), kurį naudodama kiekviena organizacija gali pagerinti savo kibernetinio saugumo lygį ir įvertinti standartų pasirinkimo efektyvumą. Dar vienas svarbus dokumentas, kuriame pateikiamas visų subjektų, dalyvaujančių keitimosi informacija procese, sąrašas ir kontaktai, yra „Kritinės infrastruktūros grėsmių informacijos mainų sistema“ (Critical Infrastructure Threat ..., 2016; NIPP..., 2020). Papildomai pateikta informacija apie federalinius resursus, kuriuos gali naudoti partneriai kritinės infrastruktūros pažeidžiamumams nustatyti ir įvertinti.

Saugumo planavimas vertinamas, atsižvelgiant į dokumentą „Partnerystė, siekiant užtikrinti kritinės infrastruktūros saugumą ir atsparumą“ (NIPP..., 2020). Jame paaiškinta kritinės infrastruktūros saugos politika ir aplinka. Dokumentuose aprašytos partnerystės ir nacionalinės partnerystės struktūra, infrastruktūros partnerių bei suinteresuotųjų šalių vaidmuo, kuriant efektyvų bendradarbiavimą.

Rizikos valdymo aspektu, kuriuo vertinamas nenumatytų atvejų plano egzistavimas ir kuris yra viena iš pagrindinių analizės krypčių, tinkamiausiu laikomas dokumentas „Papildomas įrankis: kritinės infrastruktūros rizikos valdymo metodo įgyvendinimas“, kuriame aprašoma kritinės infrastruktūros objektų rizikos valdymo sistema, taikoma visų rūšių grėsmėms ir pavojams, ir palaikoma grėsmių nustatymo bei rizikos vertinimo sistema (angl. *Threat indentification and risk assesment system* (THIRA)). Be to, Energetikos kibernetinio saugumo pagrindų įgyvendinimo gairėse (JAV energetikos departamentas, 2015 m.) siūlomi kritinės energetikos infrastruktūros saugumo rizikos valdymo metodai, galimų metodų sąrašai, kuriuos gali įgyvendinti bet kuri organizacija.

Kalbant apie saugumo kultūrą, reikia atsižvelgti į dokumentą „Kritinės infrastruktūros grėsmių komunikacijos sistema“, kuriame pateiktos gairės kritinės infrastruktūros savininkams bei operatoriams ir bendros kritinių įvykių pranešimo rekomendacijos, atspindinčios incidentų valdymą (Limba et al., 2017). Analizuojant technologijų valdymą – žinias apie organizacijas, jų komponentus ir veikimo principus, pagrindinis dokumentas yra „Partnerystė, siekiant užtikrinti kritinės infrastruktūros saugumą ir atsparumą“, kuriame prioritetas teikiamas kritinės infrastruktūros identifikavimui.

Prancūzija. Pagal 2016 m. Prancūzijos nacionalinę skaitmeninio saugumo strategiją (Government of France, 2015), vienas iš strateginių Prancūzijos kibernetinio saugumo tikslų yra „pagrindinių viešųjų informacinių sistemų ir kritinės infrastruktūros objektų interesų, gynybos ir saugumo, didelių kibernetinio saugumo krizių“ pasiekimas (Government of France, 2015). Pagal kibernetinio saugumo indeksą (ITU, 2019) trečiojoje vietoje esanti Prancūzija kibernetinio saugumo srityje evoliucionavo. Dokumente ji paaiškino, kad Vyriausybė nusprendė Europos lygiu bendradarbiauti su Europos *Enisa* agentūra (Europos Sąjungos tinklų ir informacijos saugumo agentūra) ir pasikliauti ES ir NCCIR sertifikatu Šiaurės Atlanto sutarties organizacijoje (NATO) (Government of France, 2015). Taigi prancūzų požiūris yra gana savitas, nes remiasi ne nacionaliniu, o tarptautiniu lygmeniu. Kalbant apie nacionalines organizacijas, Prancūzija 2013 m. sukūrė kritinės infrastruktūros objektų informacijos apsaugos (KIPP) reguliavimo sistemą (angl. *Ange national de la securite des systemes d'information* (ANSSI, 2020)) – „CIPP įstatymas“. Bendradarbiaujant su Krašto apsaugos ir saugumo generaliniu sekretoriatu, apibrėžta 12 sektorių ir 200 operatorių, nustatytų kaip „operatoriai, kurių nebuvimas gali smarkiai pakenkti tautos ekonominiam ar kariniam potencialui, saugumui ar tvarumui“ (ANSSI, 2020). CI apsauga laikoma prioritetu, o Nacionalinė kibernetinio saugumo agentūra (ANSSI) kartu su Vyriausybe paskiria operatorius kiekvienam CI, kurie turėtų parengti tiek Operatoriaus saugumo planą (OSP), tiek konkrečius apsaugos planus (Krašto apsaugos ir saugumo generalinis sekretoriatas, 2017).

Apibendrinant, galima teigti, kad teisinis reguliavimas yra, nes Vyriausybė žino apie kritinės infrastruktūros objektų problemą ir todėl sukuria sprendimą, paversdama jų apsaugą vienu iš pagrindinių savo strategijos tikslų (Government of France, 2015). Kalbant apie gerą saugumo valdymą, saugumo planavimas nėra tinkamas, nes vienintelės saugumo taisyklės yra bendros kiekvienos rūšies CI, o procesai priklauso nuo skirtingų operatorių, o apie veiksmingą bendrą ir visapusišką sistemą nėra užsimenama (ANSSI, 2020; Limba et al., 2017). Yra keletas nenumatytų atvejų priemonių, pagal kurias ANSSI gauna informaciją iš organizacijos ir teikia pagalbą, tačiau apie planus ar veiksmingus reglamentus neminima: incidentų valdymas gali būti vertinamas kaip žemas, bet vis dar veikiantis (ANSSI, 2020; Limba et al., 2017).

Estija. Estijos Respublika investuoja į kibernetinį saugumą, tačiau savo 2019–2022 m. strategijoje pažymi, kad viena iš problemų yra „nepakankamas kibernetinių grėsmių, incidentų ir infrastruktūros tarpusavio priklausomybės poveikio supratimas“ (Republic of Estonia, 2018). 2018 m. buvo priimtas kibernetinio saugumo įstatymas, kuriame buvo nustatyti įmonių ir institucijų reikalavimai pasirengti kibernetinei grėsmei (Republic of Estonia, 2018). Be to, 2018 m. įmonių ir informacinių technologijų ministras priėmė Kibernetinio saugumo įstatymą, kuris nustato

tinklo ir informacinių sistemų rizikos analizės ir saugumo priemonių aprašo reikalavimus (Republic of Estonia, 2018). Po 2007 m. Taline įvykusių kibernetinių atakų, kurios kelias dienas sukėlė viešąją netvarką, 2009 m. Vyriausybė priėmė Ekstremalių situacijų įstatymą, kuris suteikia teisinį pagrindą planuoti ir valdyti krizes (Estijos Vyriausybė, 2009). Įstatyme pateiktos planavimo ir rizikos vertinimo gairės gyvybiškai svarbių paslaugų, t. y. kritinės infrastruktūros objektų, teikėjams. Taip pat Estijoje veikia NATO bendradarbiavimo kibernetinės gynybos kompetencijos centras, kuris užsiima kibernetinio saugumo tyrimais ir atsakingas už saugumo incidentų valdymą kompiuterių tinkluose (Cyber Defence 2020; NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2012).

Analizė rodo geresnį Estijos pasirengimą ypatingos svarbos infrastruktūros apsaugai nei Prancūzijos, kuri vis dėlto yra aukščiau už Estiją. Visuose minėtuose dokumentuose minima būtinybė plėtoti veiksmingą kibernetinį saugumą kritinės infrastruktūros objektams, tačiau visų pirma kibernetinio saugumo įstatyme pabrėžiamas poreikis išlaikyti „tinklo ir informacinių sistemų, būtinų visuomenės funkcionavimui, veikimą ir priežiūrą“ (Republic of Estonia, 2018). Kibernetinio saugumo įstatymas gali būti svarstomas kartu su tinklų ir informacinių sistemų rizikos analizės ir saugumo priemonių aprašymo reglamentavimu, kaip gero valdymo reikalavimų rinkinys, nes jame siūlomas saugumo planavimas, lyginant su kritinės infrastruktūros objektų rizikos analize (Republic of Estonia, 2018). Kalbant apie rizikos valdymą, Estijos Vyriausybė siūlo apžvalgą Nepaprastųjų situacijų įstatyme, kuriame išdėstyti svarbiausių paslaugų teikėjų teisiniai įsipareigojimai įgyvendinti rizikos vertinimo planą ir nuolatinį operacinės rizikos vertinimą (Governance – Estonia, 2023). Tame pačiame dokumente pateikiamos operatorių gairės, kurių reikia laikytis įvykus kritinių paslaugų incidentams ir sutrikimams (Limba et al., 2017; Governance – Estonia, 2023). Vis dėlto strategija neįvertino kibernetinės saugos kultūros ir technologinio valdymo.

Lietuva. Paskutinė šalis yra Lietuva, užimanti penktą vietą (ITU, 2019). Kibernetinio saugumo problemos sprendimas aptartas 2018 m. Nacionalinėje kibernetinio saugumo strategijoje (Government of the Republic of Lithuania, 2018). Be to, 2016 m. Lietuva įkūrė Nacionalinį kibernetinio saugumo centrą (NKSC), kuris perėmė informacijos saugumo incidentų tyrimus. Kalbant apie kibernetinės erdvės apsaugą, šiuo metu Lietuvoje veikia Kompiuterių avarinės pagalbos komanda (CERT-LT), padedanti organizacijoms ir įmonėms (Government of the Republic of Lithuania, 2018). Tačiau strategijoje minima, kad nacionaliniu lygmeniu saugumo rizikos ir kibernetinio saugumo rizikos vertinimo kultūra vis dar yra susiskaidžiusi. Trūksta kibernetinių grėsmių ir saugumo spragų analizės bei visiškos integracijos į veiklos rizikos vertinimo procesus (Government of the Republic of Lithuania, 2018). Akcentuojama ypatingos svarbos informacinės infrastruktūros apsauga, tačiau nėra jokių ženklų, kad būtų diegiama CI apsaugos sistema. Taip pat verta paminėti, kad Vilniuje veikiantis NATO energetinio saugumo kompetencijos centras

(ENSEC COE) dirba su Vyriausybe taikant naujus ypatingos svarbos infrastruktūros apsaugos problemos sprendimus (Butrimas, 2017). Kitas svarbus dokumentas, į kurį reikia atsižvelgti, yra Nacionalinis kibernetinių incidentų valdymo planas, parengtas ir įgyvendintas 2018 m. (Government of the Republic of Lithuania, 2018).

Taikant analizei kibernetinio saugumo valdymo modelį (Tvaronavičienė et al., 2020), Lietuvos Respublikos požiūris į kritines infrastruktūros objektų saugos problemas yra nepakankamas, nes aptariami dokumentai nebuvo sukurti kritinei infrastruktūrai. Nacionaliniame kibernetinių incidentų valdymo plane pateikiama tam tikra įžvalga apie bendras rizikos ir incidentų valdymo procedūras (Government of the Republic of Lithuania, 2018; Limba et al., 2017). Yra bendrų nuorodų į tai, kad kritinių informacinių infrastruktūrų kibernetinio saugumo didinimas gali būti laikomas pradiniu teisinio reguliavimo etapu (Limba et al., 2017).

Išanalizavus penkių geriausių šalių kibernetinio saugumo lygį (ITU, 2019), naudojant šešis kibernetinio saugumo valdymo modelio komponentus (Tvaronavičienė et al., 2020), kurių kiekvienas buvo įvertintas penkių balų skalėje (nuo nulio iki penkių), gauti rezultatai pateikti 2.3 lentelėje. Nulinė komponento reikšmė reiškia, kad analizuojamuose dokumentuose trūksta informacijos apie komponentą ir net nėra alternatyvos bendram požiūriui į kibernetinį saugumą. Kuo didesnė vertė (balas), tuo tinkamesnės ir išsamesnės dabartinės taisyklės.

2.3 lentelė. Penkių šalių kibernetinio saugumo vertinimas (Tvaronavičienė et al., 2018)
Table 2.3. Cybersecurity analysis of five countries (Tvaronavičienė et al., 2018)

	Teisinis reguliavimas (balai)	Organizacijos valdymas (balai)	Rizikos valdymas (balai)	Kibernetinės saugos kultūra (balai)	Technologinis valdymas (balai)	Incidentų valdymas (balai)	Iš viso balų
JK	4	3	3	4	0	0	14
JAV	5	5	4	4	4	4	26
Prancūzija	3	2	0	0	0	2	7
Estija	4	4	3	0	0	3	14
Lietuva	2	0	1	0	0	2	5

Penkių šalių analizės rezultatai rodo, kad kritinės infrastruktūros objektų apsauga, nors ir yra gyvybiškai svarbi šalies kibernetiniam saugumui, dar nėra pakankamai išvystyta net ir kibernetinio saugumo požiūriu pažangiausiose šalyse. Jungtinės Amerikos Valstijos modelis šiuo metu yra pati išsamiausia ir tinkamiausia kritinės infrastruktūros objektų apsaugos sistema, nes analizėje ji surinko aukščiausią balą. Įdomu pastabėti, kad pagal pasaulinį kibernetinio saugumo indeksą Jungtinė Karalystė užima pirmąją vietą, nors 2.3 lentelėje aiškiai matyti sritys, kuriose

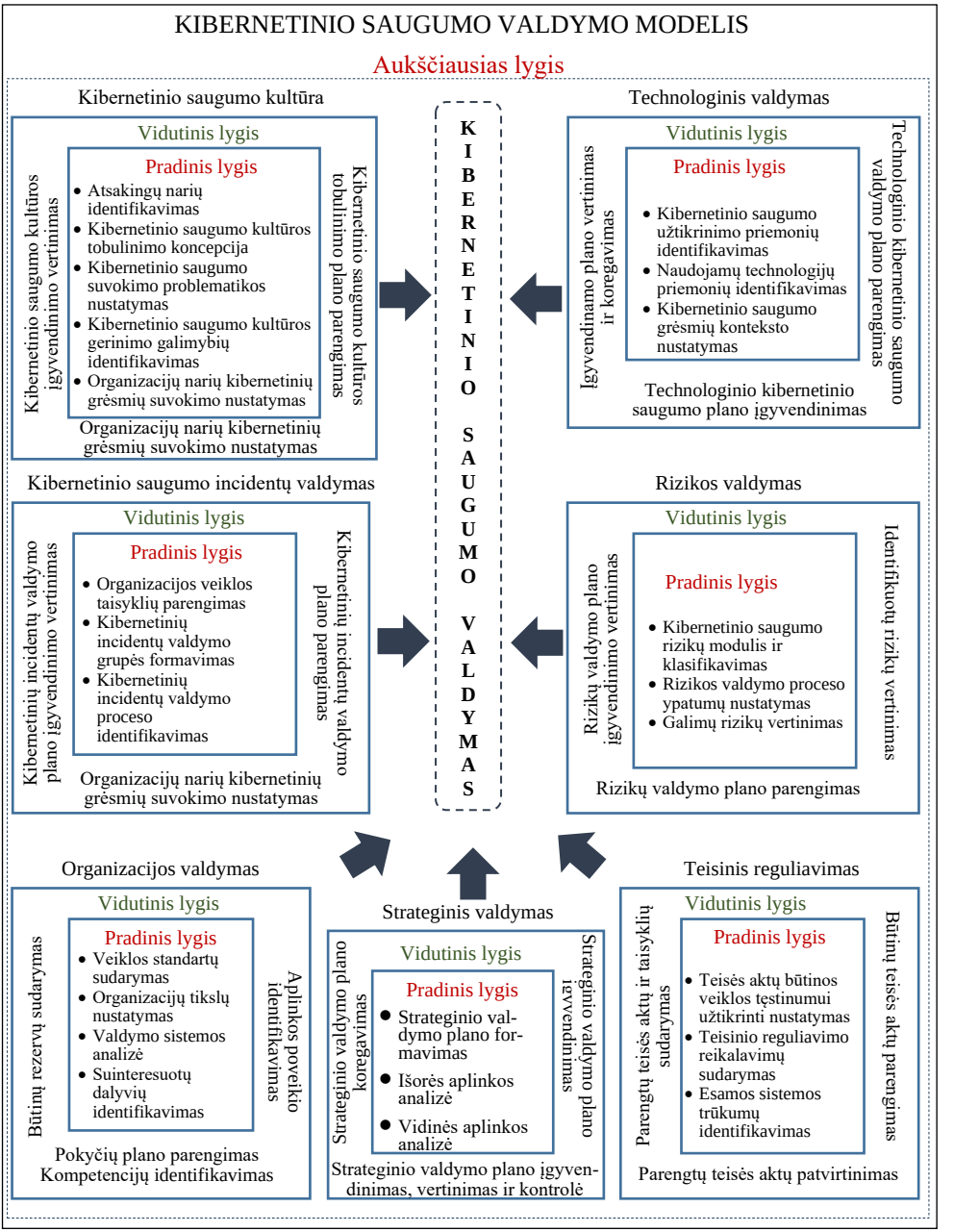
šalys turi spragų. Prasčiausiai sekasi Lietuvai, kuri pagal GCI yra penktoje vietoje, ir stebėtina, kad aukščiau Estijos yra Prancūzija, nors analizių duomenys rodo ką kita. Daugiausia balų surinkusios sritys yra teisinis reguliavimas ir organizacijos valdymas, o daugiau spragų turi kibernetinės saugos kultūra ir technologijų valdymas. Tai rodo, kad didžiausia silpnoji vieta įgyvendinant kritinės infrastruktūros objektų apsaugą yra darbuotojų informuotumas ir mokymas, o tai yra esminis dalykas kuriant naujus sprendimus. Be to, Jungtinė Karalystė visai neturi žinių apie įvairius kritinės infrastruktūros objektų komponentus, jų dalis ir jų veikimą.

Analizė atskleidė kritinės infrastruktūros saugumo spragas ir nepakankamą saugumo lygį, išskyrus Jungtines Amerikos Valstijas. Analizėje naudojamas kibernetinio saugumo valdymo modelis ne tik rodo, kad šalims trūksta tinkamos sistemos, bet ir tai, kad bendras požiūris į kibernetinį saugumą gali būti patenkinamas, jei remiasi Tarptautinės telekomunikacijų sąjungos kriterijais, kuriant Pasaulinį kibernetinio saugumo indeksą, tačiau kibernetinio saugumo indeksas gali būti klaidinantis, kai vertinamas tik praktinis kibernetinio saugumo principų taikymas.

2.4. Valstybių kritinės energetinės infrastruktūros kibernetinio saugumo valdymo modelio formavimas

Aprobuotas kibernetinio saugumo valdymo modelis yra gana tinkamas kritinės infrastruktūros kibernetiniam saugumui užtikrinti, tačiau jame trūksta komponentų, kuriuos taikant būtų atsižvelgta į tai, kad šalies vystymuisi reikia daugiau elementų. Taip pat reikėtų atsižvelgti į hierarchinį kritinės infrastruktūros objektų klasifikavimo metodą, sudarant sąrašą, kuriame įvairūs kritinės infrastruktūros objektai šalyje būtų suskirstyti pagal jų svarbą atakos ar ekstremalios situacijos atveju. Toks požiūris galėtų padėti šalims, kurių valstybės biudžetas žemas, teikti pirmenybę investicijoms į kritinės infrastruktūros objektų apsaugą. Kitas dalykas, į kurį reikia atsižvelgti kuriant naują modelį, yra planavimas. Nes retai būna aišku, ką tiksliai reikia apsaugoti kritinės infrastruktūros objektuose, ir tai patvirtino technologijų valdymo analizė.

Išanalizavus galimas su kibernetiniu saugumu susijusias problemas ir išbandžius kibernetinio saugumo valdymo modelį, prieita prie išvados, kad būtina taikyti informacinių technologijų standartą ISO/ES 27002 (Technical Committee ISO/IEC JTC 1, 2013), kuris pateikia geriausią praktiką įgyvendinant veiksmingą kritinės infrastruktūros objektų saugumo modelį. Svarbu nepamiršti, kad modelio struktūra ir pagrindiniai principai bus taikomi visų tipų kritinei energetikos infrastruktūrai, siekiant sustiprinti kibernetinį saugumą ir skatinti naujas technologijas, kaip neatsiejamą modelio dalį. Suvokę pagrindinius tinkamo kibernetinio saugumo lygio pasiekimo aspektus, galime pasiūlyti naują kibernetinio saugumo valdymo modelį, kurį sudaro septyni komponentai (2.6 pav.).



2.6 pav. Valstybių kritinių energetikos infrastruktūros kibernetinio saugumo modelis (sudaryta autoriaus)

Fig. 2.6. Cyber security model of states' critical energy infrastructure (created by the author)

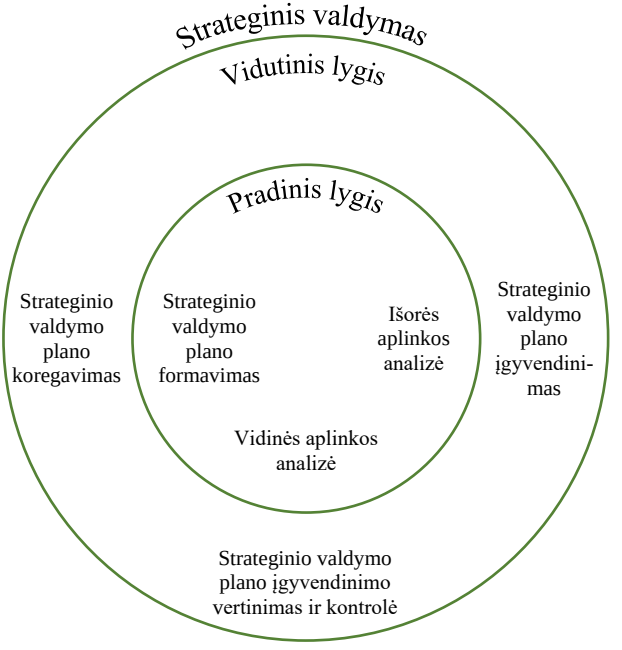
Kaip minėta anksčiau, kibernetinio saugumo valdymo modelio įgyvendinimas yra gana sudėtingas ir daug laiko reikalaujantis procesas, kurį geriausia atlikti etapais. Todėl kiekvienas modelio komponentas suskirstytas į lygmenis, kuriuos galima įgyvendinti nepriklausomai vienas nuo kito. Tačiau norint tai padaryti, reikia suprasti, už ką atsakingas kiekvienas komponentas ir ką reikia padaryti, kad pasiektų aukščiausią lygį ir atliktų pagrindinę užduotį – užtikrintų svarbiausios valstybių energetinės infrastruktūros kibernetinį saugumą.

1. *Organizacijos valdymas*. Pradiniame lygmenyje, išanalizavus organizacijos valdymo sistemą ir identifikuojant, kas dalyvauja sprendimų priėmimo procesuose, galima suprasti, kas dalyvauja kibernetinio saugumo valdymo procese ir kokią įtaką kibernetinio saugumo valdymas turi organizacijai. Pereidama į kitą lygmenį, organizacija turi aiškiai išmanyti pavaldumo grandinę, reguliuoti sprendimų priėmimo procesus ir nustatyti organizacijos narių atsakomybės ribas.
2. *Teisinis reguliavimas*. Šiame lygmenyje atliekama išorinė ir vidinė teisinės sistemos analizė bei visų teisinių aspektų reikalavimai ir nustatomi esami trūkumai, galintys turėti įtakos organizacijos saugumo politikai. Visi teisiniai aspektai, veiklos instrukcijos ir taisyklės turi būti aiškiai apibrėžti, parengti ir pristatyti kiekvienam organizacijos nariui. Periodiškai taip pat turėtų būti atliekamas teisinio reguliavimo sistemos auditas.
3. *Kibernetinio saugumo kultūra*. Pradiniame lygmenyje organizacija nustato ir aiškiai supranta taikomas kibernetinio saugumo priemones, kurios gali pagerinti kibernetinį saugumą. O tada kitame lygmenyje nustatomi būtini personalo įgūdžiai ir planuojami organizacijos narių mokymai, nes visi organizacijos nariai yra atsakingi už kibernetinį saugumą.
4. *Technologijų valdymas*. Šiame lygmenyje apibrėžiamos visos technologijos, kurios naudojamos organizuojant kasdienius darbo procesus. Toks požiūris padeda nustatyti, kokios kibernetinės atakos gali būti vykdomos, kokia kryptimi ir kokių priemonių galima imtis siekiant joms užkirsti kelią ar sumažinti jų padarinius. Vidutiniame lygmenyje techninės ir programinės įrangos, įskaitant techninės įrangos gyvavimo ciklą, identifikavimas prisideda prie sėkmingo technologijų valdymo plano įgyvendinimo, nes technologijų sistemose slypi saugumo spragų. Nuolatinis auditas leis teisingai planuoti finansinius išteklius, reikalingus technologinėms sistemoms atnaujinti ir prižiūrėti.
5. *Rizikos valdymas*. Pradiniame lygmenyje aprašomi visi galimi vidiniai ir išoriniai rizikos veiksniai bei kiti veiksniai, galintys turėti įtakos organizacijos veiklai. Toliau kitame lygmenyje rizikos veiksniai identifikuojami ir sudaromas jų valdymo planas.

6. *Kibernetinių incidentų valdymas*. Šiame lygmenyje susiformuoja supratimas, kad bet kuri organizacija yra pažeidžiama ir tai susiję ne tik su techninе ar programine įranga, bet ir su personalu. Suvokimas apie kibernetinio saugumo incidentus ir jų veikimo būdą yra esminis žingsnis gerinant kibernetinį saugumą organizacijoje. Šiame lygmenyje tikrinamas organizacijos pasirengimas kibernetinio saugumo incidentams ir organizacijos narių žinios apie valdymo ir atkūrimo planus bei veiksmus, kurių reikia imtis kibernetinės atakos metu ar po jos.

Trumpai apibūdinus šešis kibernetinio saugumo valdymo modelio komponentus, būtina išsamiau panagrinėti septintąjį modelio komponentą – *strateginį valdymą*, kuris šioje disertacijoje yra nagrinėjamas vadybos kontekste.

Modelis veikia taip, kad kiekvieno komponento veiksmai įgyvendinami palaipsniui, užtikrinant parengiamųjų ir pagrindinių procesų vykdymo seką. Ne išimtis ir strateginio valdymo komponentas, kuris, kaip ir kiti modelio komponentai, susideda iš dviejų lygių: pradinio ir vidutinio. 2.7 paveiksle pateikta strateginio valdymo komponento struktūra.



2.7 pav. Strateginio valdymo komponento struktūra (sudaryta autoriaus)
Fig. 2.7. Structure of the strategic management component (created by the author)

Kad būtų įvykdyta pagrindinė užduotis – užtikrinti valstybių kritinės energetinės infrastruktūros kibernetinį saugumą, kiekviename lygmenyje būtina įgyvendinti tam tikras priemones, kurios pateiktos 2.4 lentelėje.

2.4 lentelė. Strateginio valdymo komponento priemonės (sudaryta autoriaus)
Table 2.4. Tools of the strategic management component (made by the author)

<table>
<tr><td colspan="3">Strateginio valdymo komponentas</td></tr>
<tr><td>Pradinis lygis</td><td>Vidutinis lygis</td><td></td></tr>
<tr><td>Išorinės aplinkos analizė</td><td rowspan="4">Strateginio valdymo plano įgyvendinimas</td><td rowspan="4">Strateginis valdymas yra sudedamasis kibernetinio saugumo valdymo modelio susiejimas ir sujungimas su kitais kibernetinio saugumo modelio komponentais</td></tr>
<tr><td>Vidinės aplinkos analizė</td></tr>
<tr><td>Strateginio valdymo plano formavimas
Misijos ir vizijos nustatymas
Tikslų ir uždavinių nustatymas
Struktūros formavimas (technologijos (procesai), techninės priemonės, personalas)</td></tr>
<tr><td></td><td>Strateginio valdymo plano vertinimas ir kontrolė</td></tr>
<tr><td></td><td>Strateginio valdymo plano koregavimas</td><td></td></tr>
</table>

Pradiniu lygiu, norint įgyvendinti strateginio valdymo komponentą, reikia imtis šių priemonių:

- *Išorinės aplinkos analizė*. Organizacija egzistuoja besikeičiančioje aplinkoje, kuri turi įtakos ne tik jos produktyvumui, bet ir kibernetiniam saugumui. Todėl organizacija turi reaguoti į tokius pokyčius, o tam reikalinga išorinė aplinkos analizė: politika, ekonomikos tendencijos, demografija, teisinės problemos, bendruomenės problemos, konkuren-

cija ir naudos gavėjų poreikiai. Įgyvendinant komponentą kritinės infrastruktūros kontekste, būtina išsami išorinių veiksnių, turinčių įtakos kibernetiniam saugumui, analizė, kadangi išorinės aplinkos pokyčiai ir nesugebėjimas prie jų prisitaikyti gali lemti tai, kad organizacija nebus pasiruošusi laiku ir teisingai reaguoti į galimą ataką ar spragą. Todėl, norint apsisaugoti nuo kibernetinių atakų, būtina išanalizuoti teisines problemas, galimas rizikas, naujų technologijų diegimą ir pan.

- *Vidinės aplinkos analizė.* Kita priemonė, kurią reikia įgyvendinti siekiant geriau reaguoti į būtinus pokyčius – įvertinti ir suprasti vidinę organizacijos situaciją. Todėl, vertinant vidinę aplinką, būtina išanalizuoti organizaciją ir visą jos veiklą. Priklausomai nuo organizacijos tipo, gali tekti peržiūrėti finansus, valdymą, personalą, rinkodarą, paslaugas, programinę įrangą ir kasdienėje veikloje naudojamas technologijas. Remiantis kibernetinio saugumo modeliu ir jo taikymu bet kuriai kritinei energetinei infrastruktūrai, galima panaudoti kibernetinio saugumo valdymo modulio organizacinio valdymo, kibernetinio saugumo kultūros, kibernetinio saugumo technologijos ir kibernetinių incidentų valdymo komponentus. Taip pat būtina suprojektuoti sistemos gyvavimo ciklą, nes ji turi tam tikrą tarnavimo laiką, o aplinka, kurioje strateginio valdymo planas bus įgyvendinamas, nuolat kinta.
- *Strateginio valdymo plano formavimas.* Kaip jau minėta, kibernetinio saugumo valdymo modelis yra nagrinėjamas vadybos kontekste, todėl strateginio valdymo plano formavimas bus grindžiamas strateginiu planavimu kaip valdymo įrankiu, kuris šiame darbe naudojamas kibernetiniam saugumui gerinti. Strateginio valdymo plano kūrimas yra daug darbo reikalaujantis procesas, atimantis daug laiko ir resursų. Todėl strateginio valdymo plano sudarymas yra suskirstytas į kelis etapus, reikalingus jam įgyvendinti.
  1. Tam, kad suprastų, ką reikia daryti ir ko ji siekia, organizacija turi nustatyti kryptį, kuria ji vystysis, trumpai ir aiškiai apibūdindama savo misiją ir viziją.
  2. Įvertinus išorinę ir vidinę aplinką, išanalizavus gautus duomenis ir remiantis misija, išsikelti tikslus ir uždavinius, kuriuos būtina įgyvendinti.
  3. Nustačius tikslus ir uždavinius, įvertinus organizacijos techninę ir programinę bazę, reikia apgalvoti ir suprasti, kaip bus pasiekti užsibrėžti tikslai ir uždaviniai. Įgyvendinimui galima panaudoti paprastą struktūrą, susidedančią iš trijų tarpusavyje susijusių elementų: technologijos (procesų), techninių priemonių ir personalo:
  - *Technologijos (procesai).* Strateginio valdymo planui įgyvendinti naudojama gana daug procesų ir procedūrų, todėl norint suprasti, kokias

funkcijas naudoti, būtina atlikti analizę, orientuotis į pagrindinius uždavinius bei procesus, kurie užtikrins strateginio valdymo plano įgyvendinimą. Pavyzdžiui, informacijos saugumo ir IT duomenys turi būti renkami, saugomi ir tvarkomi taip, kad vartotojai galėtų pranešti apie įtartiną veiklą ir tirti incidentus bei reaguoti į juos. Todėl pačioje strateginio valdymo plano įgyvendinimo pradžioje geriau taikyti mažiau funkcijų negu daugiau. Tik supratus, ką reikia automatizuoti, galima pereiti prie kito etapo – techninių priemonių pasirinkimo. Išskyrus tradicines sistemas, reikės daug papildomų įrankių, dažnai nebrangių ar nemokomų, tačiau iš personalo reikalaujančių tam tikrų žinių. Dėl to galima nustatyti „kokybinius ir kiekybinius“ reikalavimus personalui.

- *Techninės priemonės*. Atsižvelgiant į funkcionalumą ir vykstančius procesus, technines priemones galima suskirstyti į tris blokus, kurių veiksmai bus įgyvendinami naudojant šiuolaikinę įrangą ir technologijas:

1. Pirmasis blokas valdo, analizuoja ir filtruoja išorinius ryšius, sukuria aktyvius spąstus ir netikrus išteklius bei imituoja nuolatinį realių vartotojų, programinės ir techninės įrangos veikimą.
2. Antrasis blokas automatizuoja aptikimo užduotis ir incidentų apdorojimą, renkant, koreliuojant ir analizuojant informacijos saugos įvykius ir įrankius, analizuojant srautą, didinant reagavimo į incidentus greitį ir šifruojant duomenis arba leidžiant prieiti iš vidinio tinklo. Be to, antrasis blokas gali atlikti papildomas užduotis: IT infrastruktūros inventorizaciją ir kontrolę, pažeidžiamumo valdymą, pažeidžiamumo prioritetų nustatymą pagal informacinių išteklių kritiškumo lygį, automatinį atsakingų asmenų paskyrimo ir pašalinimo terminus.
3. Trečiasis blokas susijęs su tinklo srauto stebėjimu, apskaita, valdymu ir vartotojų prieiga prie išorinių išteklių, failų ir programų tvarkymu, laiškų filtravimu ir apsauga nuo šiukšlių, apkrovos balansavimo ir perkrovos. Trečiasis blokas taip pat palaiko išsamų paketų ir jų priklausymo esamam ryšiui patikrinimą, aptinka kenkėjiškas programas ir atakas bei apsaugo nuo įsibrovimų.

- *Personalas*. Paskutinis strateginio valdymo plano formavimo etapas siejamas su kvalifikuoto personalo, kuris valdys įrangą ir atliks numatytas funkcijas, atranka. Samdant žmones strateginio valdymo planui įgyvendinti, rekomenduojama vadovautis principu „kokybė prieš kiekybę“, nes tokiu atveju pagrindinė užduotis yra užtikrinti, kad pagrindines pareigas užimtų aukšto lygio specialistai. Stipri komanda yra labai svarbi bet kokios strategijos įgyvendinimui. Nes ji pirmoji tiria daugumą saugumo incidentų ir į juos reaguoja. Tokių komandų nariams reikia įvairių techninių ir netechninių įgūdžių, kad galėtų efektyviai dirbti. Todėl, siekiant

nustatyti ir išnaudoti esamas galimybes sumažinti išlaidas ir išvengti pertekliaus, reikia atlikti išsamų patikrinimą.

Pradiniu lygiu išorinę ir vidinę aplinkos analizę bei strateginio valdymo plano formavimą galima vadinti parengiamaisiais procesais, būtinais strateginiam planui įgyvendinti. Prieš pradedant įgyvendinti, strateginis valdymo planas turi būti dokumentuotas ir patvirtintas. Paskui galite pereiti prie kito lygio:

- *Strateginio valdymo plano įgyvendinimas*. Strateginiame plane numatyta kryptis, laikas ir turinys. Tačiau šiam tikslui pasiekti būtina sukurti įrankį, kuris padėtų įgyvendinti strateginį valdymo planą, taptų incidentų valdymo proceso pagrindu. Duomenų apsaugos poreikis nuolat auga, kaip ir nenutrūkstamas informacijos srautas, todėl į naudojamą įrankį turi būti įtraukta saugumo ekspertų komanda, turinti patirties ir technologijų, leidžiančių aptikti, analizuoti ir užkirsti kelią kibernetinėms grėsmėms. Įgyvendinant strateginio valdymo planą, įvykių ir informacijos saugumo kontrolės priemonės turėtų būti peržiūrėtos, siekiant nustatyti incidentus. Tai turi būti daroma ne tik realiuoju laiku, bet ir per tam tikrą laikotarpį, siekiant nustatyti praleistus incidentus. Tam, kad incidentas nepasikartotų, svarbu išanalizuoti reagavimo rezultatus. Metrikų reikšmių stebėjimas leidžia laiku nustatyti ir pašalinti problemas, kurių gali kilti tiek organizuojant procesą, tiek jį įgyvendinant. Būtina suprasti, kodėl įvyko incidentas ir kokių veiksmingų priemonių buvo imtasi jam išspręsti. Todėl naudojant strateginio valdymo plano įgyvendinimo įrankį, organizacinė sistema gali būti skirstoma į zonas, o zonos – į lygius. Taip pat kiekviena zona yra padalinta į tinklo segmentus, apimančius viešąsias paslaugas ir atskiriančius jas nuo privačių. Tai suteikia papildomą vietinio tinklo saugumo lygį, kad atakos atveju būtų sumažinta žala.
- *Strateginio valdymo plano vertinimas ir kontrolė.* Strateginio valdymo plano įgyvendinimas yra nuolatinis procesas, kurį reikia stebėti ir vertinti, nes tik taip galima nustatyti, kaip priemonės įgyvendinamos ir kaip jos funkcionuoja. Todėl planas turi būti nuolat vertinamas ir stebimas, siekiant užtikrinti, kad kibernetinio saugumo veikla būtų savalaikė, efektyvi, aktuali ir reikalinga.
- *Strateginio valdymo plano koregavimas.* Įvertinus plano įgyvendinimą ir išanalizavus rezultatus, gali tekti koreguoti jo įgyvendinimą ir gautus rezultatus tobulinti. Koregavimas yra neišvengiamas ir ne visada dėl neigiamų veiksnių. Svarbiausia nepraleisti momento, kai reikia atlikti reikiamus pakeitimus.

Kibernetinio saugumo valdymo modelio strateginio valdymo komponento pirmųjų dviejų lygių įgyvendinimas siejamas su komponento integravimu į patį modelį, kaip neatskiriamą jo dalį, ir sujungia jį su kitais modelio komponentais

(Tvaronavičienė et al., 2021). Strateginio valdymo plano įgyvendinimo priemonės ir jų panaudojimas detaliai aprašytos 3.3 poskyryje „Valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio praktinio taikymo rekomendacijos“.

Apibendrinant galima pasakyti, kad tikslus strateginio valdymo komponento taikymas kartu su tinkamu darbuotojų mokymu, teisinga tinklo ir įrenginių konfigūracija bei fizine sauga leis išvengti rizikos arba ją žymiai sumažinti iki toleruotino lygio. Pažeidžiamumų nustatymas, kibernetinio saugumo politikos įgyvendinimas, mokymas, sistemų atnaujinimas ir netgi būtinų sistemų, kurios neatitinka dabartinių saugumo ir veiklos poreikių, pašalinimas yra svertas, padedantis užkirsti kelią kibernetiniams pavojams ateityje.

2.5. Antrojo skyriaus išvados

1. Kibernetinį saugumą užtikrina teisingas reagavimo procesas, kurį galima suskirstyti į tris etapus: prieš išpuolį, jo metu ir po jo. Kiekviename etape pagrindinis tikslas yra užtikrinti saugią aplinką keitimuisi konfidencialiais duomenimis ir galimybę atkurti sistemą, jei dėl išorinių ar vidinių veiksnių ji buvo pažeista. Daugumą kibernetinių atakų sukelia žmogaus veiksniai ir kenkėjiško kodo įvedimas į sistemą. Yra daug problemų, susijusių su kritine energetine infrastruktūra, nes daugelis įmonių neturi tinkamo reagavimo į kibernetinį išpuolį plano, taip pat darbuotojai nėra apmokyti.
2. Apibendrinant garsiausių kibernetinio saugumo išpuolių analizės rezultatus prieš kritinę energetinę infrastruktūrą, naudojant organizacijos kibernetinio valdymo modelio komponentus, galima teigti, kad tiek organizacijos kibernetinis valdymas, tiek kibernetinio saugumo kultūra yra tiksliniai kibernetinio saugumo spragų matavimo komponentai. Taip pat svarbu paminėti, kad pateiktame kibernetiniame saugumo valdymo modelyje šešių komponentų vis tiek nepakanka, kad būtų apimti visi aspektai, būdingi kritinei energetinei infrastruktūrai. Vis dar nėra skaičiavimų, kurie pasiūlytų kibernetinio saugumo kriterijus, kad tinkamai būtų įvertinta kritinė energetinė infrastruktūra. Tačiau tokią analizę galima taikyti įvertinant organizacijos kibernetinio saugumo lygį.
3. Išanalizavus kritinės energetinės infrastruktūros silpnąsias vietas, įvertinus užsienio valstybėse taikomas gerąsias praktikas galima konstatuoti, kad kritinės infrastruktūros saugumo lygis yra nepakankamas. Kibernetinio saugumo modelis, sudarytas iš šešių komponentų, yra tinkamas kibernetinio saugumo vertinimui, tačiau jį galima patobulinti, atsižvelgiant į hierarchinį požiūrį, klasifikuojant kritinę infrastruktūrą, panaudojant

tarptautinius kriterijus, atsižvelgiant į šalies vystymuisi reikalingus elementus, taip pat atsižvelgiant į planavimą, nes nėra aišku, ką tiksliai reikia saugoti kritinėje infrastruktūroje, o analizė patvirtino technologijų valdymo trūkumus.

4. Sukurtas naujas kibernetinio saugumo valdymo modelis, sudarytas iš septynių komponentų, vienas iš kurių – strateginis valdymas. Tikslus strateginio valdymo komponento taikymas kartu su tinkamu darbuotojų mokymu, teisinga tinklo ir įrenginių konfigūracija bei fizine sauga leis išvengti rizikos arba ją žymiai sumažinti iki toleruotino lygio. Pažeidžiamumų nustatymas, kibernetinio saugumo politikos įgyvendinimas, mokymas, sistemų atnaujinimas ir netgi būtinų sistemų, kurios neatitinka dabartinių saugumo ir veiklos poreikių, pašalinimas yra svertas, padedantis užkirsti kelią kibernetiniams pavojams ateityje.

3

Kritinės energetinės infrastruktūros kibernetinio saugumo valdymo modelio empirinio tyrimo metodika

Šiame skyriuje pateikiama kibernetinio saugumo kritinės energetinės infrastruktūros empirinio tyri mo metodika, pagrįsta pateiktu modeliu, jo komponentais, tyrimo planu ir kiekviename įgyvendinimo etape naudojamais metodais. Nagrinėjami etapai: pasirengimas ekspertiniam vertinimui, kriterijų reikšmingumo nustatymas bei ekspertinių nuomonių suderinamumo skaičiavimas, vykdomas empirinis tyrimas ir rezultatų apibendrinimas bei išvadų kibernetinio saugumo valdymui rekomendacijų parengimas. Pasirengimo etape sudaryti veiksnių ir vertinimo kriterijų rinkiniai bei ekspertų grupė, pasirinktas apklausos tipas. Kriterijų reikšmingumai nustatyti pagal ekspertinį vertinimą ir apskaičiuoti ekspertų nuomonių suderinamumo ir kompetentingumo koeficientai. Empiriniame tyrime dalyvavo penki ekspertai, turintys ne mažiau negu 3 metų darbo patirtį kritinės infrastruktūros kibernetinės saugos, konsultavimo ir priežiūros srityje. Taikant ekspertų apklausos būdą, ekspertai vertino balais kiekvieno veiksnio rinkinį pagal svarbą. Rezultatų apdorojimo etape, taikant paprastąjį adityvų svorių metodą (SAW), apskaičiuojami gautų rezultatų kiekvieno kritinio valdymo modelio kom-

ponento įvertis ir nustatyti jų rangai. Pagal įverčių rangus nustatytas kritinės energetinės infrastruktūros kibernetinio saugumo valdymo modelio komponentų paskirstymas. Taip pat nustatytas komponentas, kurį reikia būtinai tobulinti, kad būtų teisingai organizuotas kritinės energetinės infrastruktūros saugumo procesas. Šio skyriaus pabaigoje pateiktos rekomendacijos strateginiam valdymui taikyti. Šio skyriaus tematika paskelbta publikacija (Pleta, 2022).

3.1. Valstybės kritinės energetinės infrastruktūros kibernetinio saugumo valdymo modelio empirinio tyrimo metodai ir jų taikymas

Kibernetinio saugumo kritinės energetinės infrastruktūros valdymo modelio praktiniam taikymui sudaryta metodika susideda iš trijų etapų: pasirengimo, tyrimo vykdymo ir rezultatų apibendrinimo (3.1 lentelė).

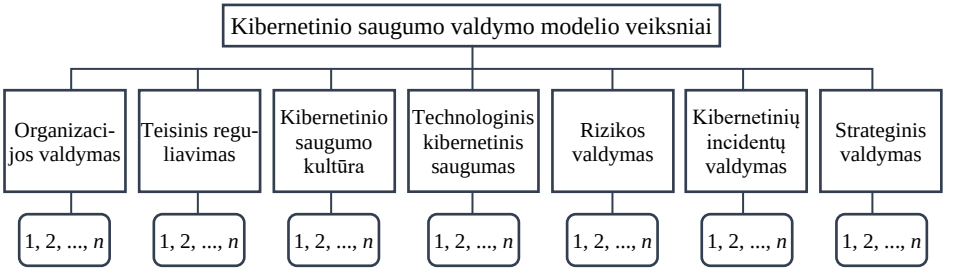
3.1 lentelė. Metodologijos įgyvendinimo planas
Table 3.1. Methodology implementation plan

Etapai		Metodikos (tyrimo) etapų detalizavimas
1	2	2
Pasirengimas	Veiksnių rinkinio sudarymas	Vertinimo klausimai (veiksniai) sujungiami į grupes pagal kibernetinio saugumo valdymo modelio komponentų skaičių, kad kiekviename būtų ne mažiau nei penki klausimai (veiksniai).
	Kriterijų, skirtų veiksniams vertinti, sudarymas	Klausimams (veiksniams) vertinti siūlomi kriterijai: organizacijos valdymas, teisinis reguliavimas, kibernetinio saugumo kultūra, technologinis kibernetinis saugumas, rizikos valdymas, kibernetinių incidentų valdymas, strategijos valdymas.
	Ekspertų grupės sudarymas	Ekspertų kriterijų parinkimas: ne mažesnė negu 3 metų valdymo patirtis.
	Pasirengimas ekspertiniam vertinimui	Apklausos tipo parinkimas: siūloma individuali apklausa el. paštu.

3.1 lentelės pabaiga

1	2	3
		Tyrimo instrumento sudarymas. Instrukcijos parengimas anketoms pildyti
	Kriterijų reikšmingumo nustatymas	Kriterijų reikšmingumui nustatyti taikomas subjektyvusis vertinimas ir matematinės statistikos metodai.
	Ekspertinių nuomonių suderinamumo skaičiavimas	Ekspertų nuomonių suderinamumas skaičiuojamas taikant daugiakriterį vertinimo metodą.
Tyrimo vykdymas	Empirinis tyrimas	Individuali ekspertų apklausa pagal parengtą anketą (A priedas).
Rezultatų apibendrinimas	Rezultatų apdorojimas	Duomenų normalizavimas.
		Veiksnių įverčių skaičiavimas ir rangavimas.
		Galutinių veiksnių įverčių kiekvienam komponentui skaičiavimas.
		Modulio pritaikomumo nustatymas.

Veiksnių rinkinio sudarymas. Kritinės energetinės infrastruktūros kibernetinis saugumas yra sudėtinga sistema, vertinant ją, reikia atsižvelgti į skirtingus komponentus, kurie sudaro kibernetinį saugumą. Dėl šios priežasties, siekiant suformuoti veiksnių rinkinį, veiksnius būtina sujungti į septynias grupes pagal modelio komponentų skaičių, kur kiekvienoje turi būti ne mažiau nei penki veiksniai (3.1 pav.).



3.1 pav. Veiksnių rinkinio sudarymas
Fig. 3.1. Compilation of a set of factors

Sudarant veiksnių sąrašą, reikia parinkti kriterijus, pagal kuriuos ekspertai galės įvertinti kritinės energetinės infrastruktūros kibernetinio saugumo modelį.

Kriterijų, skirtų veiksniams vertinti, sudarymas. Bet kokia svarbi infrastruktūra turi užtikrinti atsparumą, vientisumą ir reguliarumą, o tai turėtų padėti sukurti sėkmingą saugumo strategiją. Europos Sąjunga yra suinteresuota susietų ypatingos svarbos infrastruktūrų saugumu. Kritinė infrastruktūra yra svarbus šalies ekonomikos elementas, kuris tapo labiau pažeidžiamas dėl išpuolių, galinčių sutrikdyti šalies ekonomiką.

Vertinant kritinės energetikos infrastruktūros saugumą, būtina atsižvelgti į poreikius, įrangą, veikimo metodus, saugą ir nustatyti aiškias eksploatavimo ir situacijos valdymo taisykles. Reikia atitinkamai pritaikyti saugumo priemones atliekant reguliarų rizikos vertinimą. Naudojant rizikos vertinimo veiksnius, turi būti įmanoma įvertinti infrastruktūrą, užfiksuoti esamas problemas ir valdymo būdus.

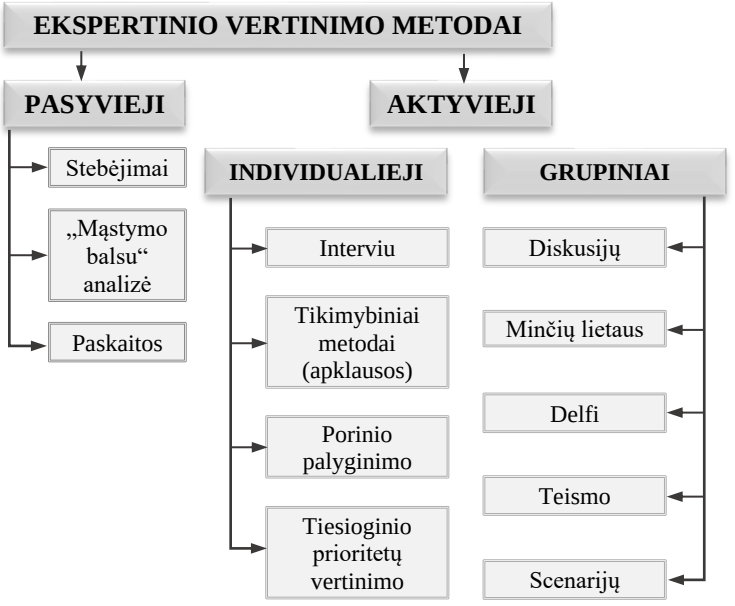
Forcepoint (2020) teigimu, kibernetinio saugumo samprata remiasi trimis pagrindiniais tikslais, kurie taikomi norint užtikrinti bet kurios kritinės energetinės infrastruktūros kibernetinį saugumą:

1. konfidencialumas – slaptos informacijos apsauga nuo neteisėtos prieigos;
2. vientisumas – duomenų apsauga nuo neteisėtos prieigos;
3. prieinamumas – sistemų mechanizmų prieinamumas kritiniais atvejais.

Naujų energijos tiekimo sistemų vystymas kritinėje energetinėje infrastruktūroje (CEI) reikalauja pasirinkti tokius kriterijus, kuriuos būtų galima pritaikyti kiekvienam CEI tipui ir kurie galėtų suteikti kibernetinį saugumą skirtingoms sistemoms (Onyeji et al., 2014). Pagrindinis dėmesys turėtų būti skiriamas kritinės infrastruktūros kibernetiniam saugumui ir apsaugos užtikrinimui. Bet kuri organizacija turi žinoti ne tik elementus, sudarančius fizinę sistemą, bet ir saugumo sistemų pažeidžiamumus, silpnąsias vietas. Reagavimas į išpuolius, atakų prevencija, elgesys po kibernetinių atakų, operatyvinis saugumas yra dar vieni kriterijai, kuriuos reikia įvertinti, norint apsaugoti kritinę infrastruktūrą. Kibernetinį saugumą sudaro ne tik fizinė infrastruktūra, bet ir programinė, telekomunikacinė ir tinklo įranga, kuri priklauso nuo kibernetinio saugumo metodų, taikomų atsižvelgiant į jos tipą.

Vertinant bet kurios sistemos kibernetinį saugumą, svarbu nepamiršti tokio informacinio aspekto kaip „žmogus“, kuris taip pat yra sistemos dalis, o sistemos saugumas priklauso nuo jo sąmoningumo. Todėl vertinant kritinės infrastruktūros saugumą, tikslinga būtų pasirinkti tokius kriterijus: organizacijos valdymas, teisinis reguliavimas, kibernetinio saugumo kultūra, technologinis kibernetinis saugumas, rizikos valdymas, kibernetinių incidentų valdymas, strategijos valdymas.

Kriterijų reikšmingumo nustatymas. Norint sužinoti, kaip kriterijai daro įtaką rezultatams, reikia nustatyti kriterijų reikšmingumą. Dažniausiai praktikoje taikomas subjektyvusis vertinimas, kai kriterijų reikšmingumą nustato atitinkamos srities ekspertai, o skaičiavimui taikomi matematinės statistikos metodai. Prieš atliekant ekspertinį vertinimą reikia nustatyti ne tik, kiek ekspertų dalyvaus tyrime, kaip įvertinti jų kompetencijas ir gautus rezultatus, bet ir koks vertinimo metodas taikomas. Augustinaitis teigė, kad ekspertinio vertinimo metodai skirstomi į kelis būdus: į *aktyviuosius* ir *pasyviuosius,* o šie du dar į dvi grupes (individualiuosius ir grupinius), o šios grupės skirstomos dar smulkiau (3.2 pav.) (Augustinaitis et al., 2009).

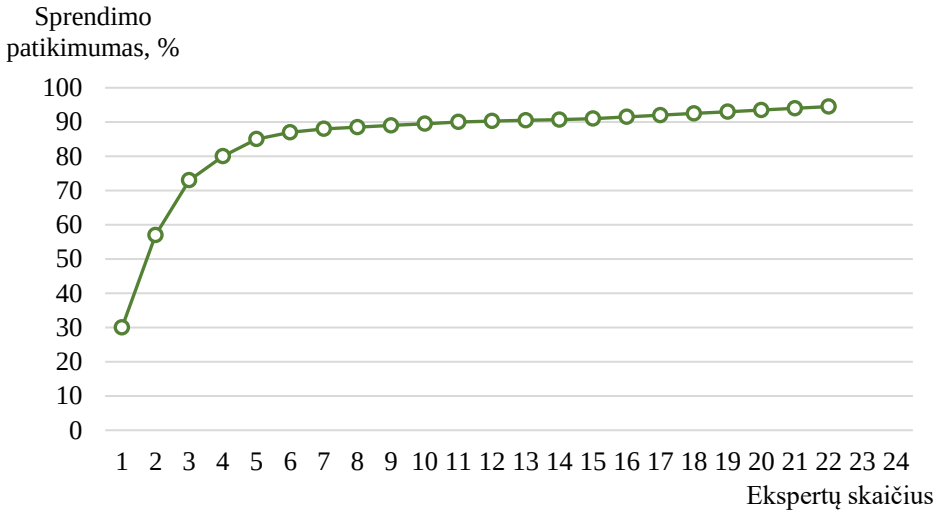


3.2 pav. Ekspertinių vertinimo metodų klasifikavimas pagal žinių šaltinį (Augustinaitis et al., 2009)
Fig. 3.2. Classification of peer-review methods by sources of knowledge (Augustinaitis et al., 2009)

Nagrinėjant ekspertinių vertinimo metodų klasifikavimą, galima teigti, kad teikiamaisiais būdais ekspertams vertinti nagrinėjamus veiksnius yra aktyvus individualusis vertinimo būdas – tikimybinis.

Dažniausiai pageidaujamos ekspertų savybės vertinamos kokybiškai (Glassner & Morenno, 1989; Maxwell, 1996). Prie tokių savybių priskiriama

kompetencija, kūrybiškumas, požiūris į ekspertizę, mąstymo lankstumas, patikimumas, savikritiškumas, mokėjimas dirbti kolektyve. Viena iš svarbiausių savybių – kompetencija – dažniausiai vertinama paties eksperto (savęs vertinimas) arba remiamasi kitų ekspertų nuomonėmis. Nustatant priimtiną ekspertų kiekį reikia vadovautis metodologinėmis prielaidomis, suformuluotomis klasikinėje testų teorijoje (Brock & Hommes, 1997). Teorija teigia, kad agreguotų sprendimų patikimumą ir priimančiųjų sprendimus (šiuo atveju ekspertų) skaičių sieja greitai slopstantis netiesinis ryšys (3.3 pav.) (Augustinaitis et al., 2009).



3.3 pav. Ekspertų skaičiaus įtaka vertinimo patikimumui
(sudaryta remiantis Augustinaitis et al. (2009)
Fig. 3.3. Influence of the number of experts on the reliability of the assessment
(based on Augustinaitis et al. (2009)

3.3 paveiksle matyti, kad, pradedant nuo 9 vertinimo, patikimumas beveik nesikeičia, todėl galima teigti, kad tyrime gali dalyvauti ne mažiau kaip 5 ir ne daugiau kaip 10 ekspertų. Kaip sako Augustinaitis (2009) savo darbe „tikslinga ne didinti ekspertų grupę, o kelti ekspertų kompetenciją“. Papildomai kiekvienam ekspertui reikia matematiškai apskaičiuoti kompetencijos koeficientą, kad būtų nustatytas ekspertų suderinamumo lygis. Jeigu tyrime dalyvauja tik du ekspertai, jų suderinamumas tikrinamas taikant koreliacijos koeficientą. Kai ekspertų daugiau, skaičiuojamas konkordancijos koeficientas, kurio skaičiavimo eiga pateikta 3.2 lentelėje.

3.2 lentelė. Konkordacijos koeficiento skaičiavimo eiga
Table 3.2 Procedure for calculating the concordance coefficient

Veiksniai	Skaičiavimo formulė
Rangų sumos apskaičiavimas	$e_i = \sum_{j=1}^{m} e_{ij}$
Nuokrypio nuo bendro vidurkio kvadratų sumos skaičiavimas	$S = \sum_{i=1}^{m} (e_i - \bar{e})^2$
Bendro vidurkio apskaičiavimas	$\bar{e} = \frac{\sum_{i=1}^{n} e_i}{n} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} e_{ij}}{n}$, čia m – veiksnių skaičius.
Konkordancijos koeficiento skaičiavimas	$W = \frac{12S}{r^2 m(m^2-1)}$, čia S – kiekvieno i-tojo kriterijaus rangų sumos, m – veiksnių skaičius, r – ekspertų skaičius.
Konkordancijos koeficiento skaičiavimas, kai yra vienodi rangai	$W = \frac{12S}{r^2((m^3-m)-r*\sum_{j=1}^{m}(t_j^3-t_j))}$, čia t_j – vienodų rangų skaičius kiekviename veiksnyje.

Gautas konkordancijos koeficientas keičiasi intervale nuo 0 iki 1. Jeigu ekspertų nuomonės suderintos, konkordancijos koeficiento *W* reikšmė artėja prie vieneto. Jeigu skaičiavimai parodė, kad reikšmė artėja prie nulio, tai reiškia, kad suderinamumo tarp ekspertų nuomonių nėra. Ekspertų vertinimų suderinamumas laikomas pakankamu, jeigu konkordancijos koeficientas *W* yra intervale nuo 0,6 iki 0,7. Nustatant konkordancijos koeficientą, būtinai reikia pašalinti rezultatus, kuriuose ekspertų nuomonės yra nesuderinamos. Kendall (1975) įrodė, kad jeigu alternatyvų skaičius didesnis negu 7, tai konkordancijos koeficientas *W* skaičiuojamas, taikant χ^2 kriterijų (3.1):

$$\chi^2 = Wr(m-1) = \frac{12S}{rm(m+1)}. \quad (3.1)$$

Pagal pasirinktą reikšmingumo lygmenį α (paprastai α reikšmė imama 0,05 arba 0,01) iš χ^2 skirstinio lentelės su $y = m - 1$ laisvės laipsnių skaičiumi randama kritinė χ^2 reikšmė. Jeigu pagal (3.1) formulę suskaičiuota χ^2 reikšmė yra didesnė už χ^2_{kr}, tai reiškia, kad ekspertų vertinimai yra suderinti.

Apskaičiuotas konkordancijos koeficientas neparodo, kurių ekspertų nuomonė skiriasi ir kuriuos reikia pašalinti iš tyrimo. Todėl būtinai reikia įvertinti ir ekspertų kompetenciją. Naudojama keletas ekspertų kompetencijos koeficiento skaičiavimo algoritmų, vienas iš jų – iteracinis būdas, kuris ir bus naudojamas vertinant ekspertų kompetenciją (3.2). Ekspertai kompetentingi, jeigu kompetencijų įverčių suma lygi vienetui.

$$K_i^t = \frac{1}{\lambda} * \sum_{j=1}^{n} x_j^t * x_{ij}, \sum_{i=1}^{m} K_i^t = 1, \quad (3.2)$$

čia $x_j^t = \sum_{i=1}^{m} K_i^{t-1} * x_{ij}, j = 1,2, \dots n$ ir $\lambda = \sum_{j=1}^{n} \sum_{i=1}^{m} x_j x_{ij}$, m – ekspertų skaičius, n – kriterijų skaičius, x_{ij} – i-tojo eksperto j-ojo kriterijaus rangas.

Ekspertinių nuomonių suderinamumo skaičiavimas. Dažniau nepažįstami žmonės (šiuo atveju ekspertai) įvertina problemą ir siūlo variantus, kaip iškilusią problemą galima spręsti. Delfi metodas – vienas iš būdų priimti sudėtingus sprendimus, atliekant minčių lietų, interviu arba apklausą. Taikant šį metodą, galima gauti ekspertų nuomonę tam tikrais klausimais, nes manoma, kad žmonės, nepriklausantys vienas nuo kito, efektyviau sprendžia pavestas užduotis negu sudarytos komandos.

Delfi metodą sukūrė Helmer ir jo kolegos tam, kad moksliškai būtų pagrįstas ateities prognozavimas (Dalkey & Helmer, 1962). Šiandien Delfi metodas plačiai taikomas norint gauti sudėtingų problemų ir situacijų prognozes, kurioms apibūdinti nepakanka informacijos. Delfi metodas priklauso euristinių ir kiekybinių tyrimų ir prognozavimo metodų grupei, todėl jo taikymas prasideda nuo dalyvių grupių formavimo. Pirmąją grupę sudaro ekspertai, kurie išreiškia savo nuomonę apie sprendžiamą problemą. Antrąją grupę sudaro analitikai, kurie tiria ekspertų nuomones ir, remdamiesi jomis, nustato optimalų problemos sprendimą. Pats procesas susideda iš trijų etapų (3.4 pav.):

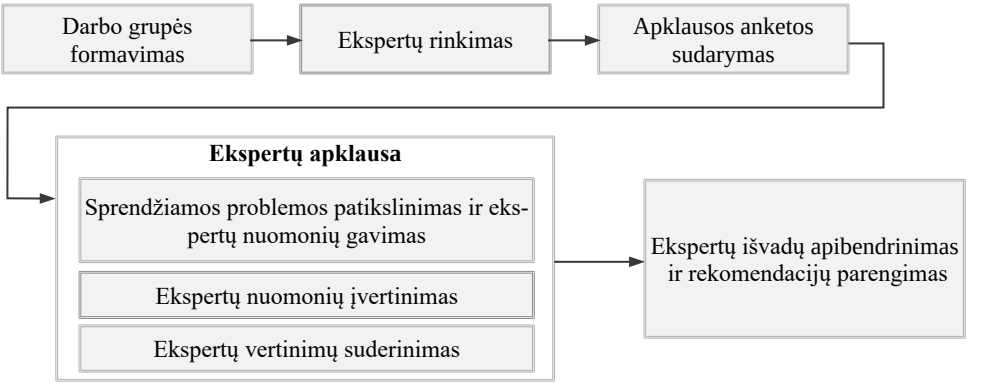
- *parengiamasis* – surinkti ekspertus, kurių skaičius yra neribojamas, tačiau rekomenduojama kviesti ne daugiau kaip 20 žmonių;
- *pagrindinis* – sprendžiama problema skirstoma į keletą mažesnių, analizuojama, grupuojama pagal svarbą (arba kitus kriterijus) ir formuojama anketa. Ekspertai analizuoja, tikrina, tiria anketą ir gali pasiūlyti pridėti papildomų duomenų. Analitikai gauna išsamius atsakymus (atsižvelgiant į ekspertų grupės dalyvių skaičių), analizuoja ir, jeigu reikia, rengia dar vieną anketą, kuri grįžta į ekspertų grupę, kurios tikslas pasiūlyti problemos sprendimo būdus, atsižvelgiant į daugelį veiksnių: išteklius, siūlomų idėjų aktualumą bei galimybes;
- *analitinis* – atlikus pagrindinį darbą, būtina įvertinti ekspertų nuomonių suderinamumą, ištirti ir išanalizuoti gautą informaciją ir sugalvoti geriausią problemos sprendimo būdą.

Šis metodas skiriasi nuo kitų tuo, kad atliekamas anonimiškai ir nedalyvaujant kitiems ekspertams. Anonimiškumas ir nedalyvavimas tyrime leidžia išvengti autoritetingų ekspertų nuomonių įtakos likusių narių nuomonei. Apklausa gali būti atliekama, naudojant specialias anketas, siunčiamas įprastu arba elektroniniu paštu. Ekspertai, kurie dalyvauja apklausoje, ne tik ranguoja klausimus, bet ir rašo paaiškinimus, kuriuos naudojant galima papildyti arba, atvirkščiai, panaikinti neaktualius ir nesvarbius klausimus. Taip pat paaiškinimai gali „nukreipti“ analitikus link teisingo problemų sprendimo būdo.

Taikant Delfi metodą šiame tyrime, labiausiai domina vidutinis ekspertų įvertinimas (3.3) ir ekspertų vertinimų suderinamumas, kuris buvo aprašytas anksčiau.

$$R = \frac{\sum_{i=1}^{N} r_i}{N}, \tag{3.3}$$

čia r_i – kriterijų rangas, N – kriterijų skaičius.



3.4 pav. Delfi metodo proceso eiga
Fig. 3.4. Delphi method process

Rezultatų apdorojimas. Nagrinėjant kritinės energetinės infrastruktūros kibernetinio saugumo reiškinius, būtina atlikti kokybinę arba kiekybinę analizę. Dažniausiai tokio tipo analizė yra daugiakriterė, nes vienu metu reikia vertinti kelis kriterijus, kurie gali būti prieštaringi. Kasdieniame gyvenime pasirinkimas remiantis keliais kriterijais dažniausiai daromas intuityviai, o jo pasekmės gali būti priimtinos sprendimus priimančiam asmeniui. Tačiau intuicija negali būti vieninte lė sprendimų priėmimo priemonė, ypač sprendžiant sudėtingas užduotis, turinčias daug kriterijų. Tokiu atveju būtina gauti kuo objektyvesnį alternatyvų įvertinimą. Norint gauti tokį įvertinimą, reikia kruopščiai išanalizuoti visus kriterijus, nustatyti jų priklausomybes ir prioritetus.

Egzistuoja daug daugiakriterių metodų, kuriais galima spręsti įvairias daugiakriteres problemas. Tačiau svarbu rasti tinkamiausią konkrečiai problemai spręsti. Nes daugiakriteriai metodai turi nemažai skirtumų tiek gautais rezultatais (rastų sprendimų skaičiumi, sprendinių pateikimu ir pan.), tiek jų taikymu (reikalingos informacijos kiekiu, informacijos rinkimo metodais ir pan.). Ne visi metodai gali būti taikomi sprendžiant konkrečią problemą.

Neįmanoma išsamiai apsvarstyti visų esamų metodų, todėl apsvarstysime keletą iš jų ir pasirinksime tinkamiausią.

Analitinės hierarchijos procesas (angl. *Analytic Hierarchy process* (AHP)) yra struktūrinta sudėtingų sprendimų priėmimo technika. Šis metodas neatsako į klausimą, kas teisinga, o kas neteisinga, bet leidžia sprendimus priimančiam asmeniui įvertinti, kuris iš variantų, jo nuomone, geriausiai atitinka jo poreikius ir problemos (užduoties) supratimą (Saaty, 2001).

Užsakymo pirmenybės pagal panašumą į idealų sprendimą metodas (angl. *Technique for order preference by similarity to ideal solution* (TOPSIS)) buvo sukurtas devintajame dešimtmetyje kaip daugiakriteris sprendimų priėmimo metodas. Metodo esmė – ieškoti alternatyvų, kurių įverčiai yra arčiausiai idealaus teigiamo sprendimo ir labiausiai nutolę nuo idealaus neigiamo sprendimo. Idealus teigiamas sprendimas yra alternatyvų svertinių įverčių matricos didžiausiųjų verčių vektorius. Kita vertus, idealus neigiamas sprendimas yra mažiausiųjų verčių vektorius (Sarraf et al., 2012).

Daugiakriterių alternatyvų reitingavimo metodas (pranc. *Elimination et choix Trduisant la realite* (ELECTRE)) – vienas iš daugelio sprendimų analizės metodų, atsiradusių Europoje septintojo dešimtmečio viduryje. Šis metodas skirtas spręsti problemas su jau pateiktomis daugiakriterėmis alternatyvomis. Šiuo metodu kiekvienos iš alternatyvų kokybės rodiklis nėra kiekybiškai įvertinamas. Nustatomas tik vienos alternatyvos pranašumas prieš kitą. Metodo trūkumas yra tas, kad tai tik pagalbinė priemonė, o ne būdas sukurti geresnį sprendimą (Roy, 1991).

Neaiškioji logika (angl. *Fuzzy logic*) – Zadeh sukūrė neaiškių rinkinių koncepciją, kuri yra susijusi su netikslumais ir neapibrėžtumu visais sprendimų priėmimo aspektais (Abdullah, 2013). Neaiškioji logika yra kintamųjų apdorojimo metodas, leidžiantis apdoroti kelias galimas tos paties kintamojo tiesos reikšmes. Taip pat yra taisyklių rinkinys, naudojamas išvadoms iš neaiškių duomenų rinkinių daryti. Neaiškioji logika kilo iš tikimybių teorijos ir labiau tinka bet kokiems realaus gyvenimo reiškiniams modeliuoti. Neaiškioji logika padeda išspręsti konkrečią problemą, įvertindama visus turimus duomenis ir priimdama tinkamą sprendimą. Šis metodas imituoja žmogaus sprendimų priėmimą, atsižvelgiant į visas galimybes.

Svertinio vidurkio metodas (angl. *Cumulative Average Weighing* (CAW) yra duomenų rinkinio, kuriame tam tikri skaičiai yra svarbesni už kitus, vidurkis. Statistinėje analizėje dažniausiai naudojami svertiniai vidurkiai. Skaičių tikslumą lemia konkretiems kintamiesiems priskiriamas svoris. Atliekant galutinius skaičiavimus, kiekvienas skaičius dauginamas iš nurodyto svorio, o tai pagerina duomenų tikslumą lyginant su paprastu vidurkiu (Ahsan et al., 2001).

Paprastasis adityvus svorių metodas (angl. *Simple Additive Weighting*, trumpai (SAW) yra vienas iš daugiakriterių problemų sprendimo būdų, paremtas sver-

tinio sumavimo koncepcija. Pagrindinis metodo principas yra rasti kiekvienos alternatyvos pagal visus kriterijus svertinį balą. Aukščiausias įvertinimas laikomas geriausia alternatyva (Podvezko, 2011).

Nagrinėjant kritinės energetinės infrastruktūros kibernetinio saugumo reiškinius, kurie yra tikslūs, apibrėžti ir dinamiški, o kiekvienas iš jų yra svarbus kibernetinio saugumo požiūriu, buvo nuspręsta taikyti vieną iš daugiakriterių vertinimo metodų, pasitelkiamų ieškant optimalaus sprendimo, kuris leistų įvertinti sprendžiamą problemą, atsižvelgiant į iškeltus tikslus, ir parinkti racionalią alternatyvą.

Dar nenustatyta, koks daugiakriterinis metodas yra tinkamiausias sprendžiant skirtingo pobūdžio uždavinius. Geriausias variantas pasirinkti patikimą, prieinamą, paprastą ir daug laiko nereikalaujantį metodą. Paprastasis adityvus svorių metodas SAW yra vienas iš plačiai taikomų metodų, kurių taisykles apibendrino MacCrimmon (1968).

Taikant SAW metodą sudaroma normalizuota sprendimų matrica, o kiekvienas normalizuotas narys dauginamas iš jo reikšmingumo ir sudedamas su kitais eilutės nariais. Į vieną dydį jungiamos rodyklių reikšmės ir jų svoriai. Visų veiksnių pasvertų normalizuotų reikšmių suma S_j kiekvienam *j*-ajam objektui skaičiuojama pagal (3.3) formulę:

$$S_j = \sum_{i=1}^{m} \omega_i \widetilde{r_{ij}}, \tag{3.3}$$

čia ω_i – *i*-tojo rodiklio svoris, $\widetilde{r_{ij}}$ – *i*-tojo rodiklio normalizuota reikšmė *j*-ajam objektui ($\sum_{i=1}^{m} \omega_i = 1$).

Vienas iš pradinių duomenų normalizavimo variantų (3.4):

$$\widetilde{r_{ij}} = \frac{r_{ij}}{\sum_{i=1}^{m} r_{ij}}, \tag{3.4}$$

čia r_{ij} – *i*-tojo rodiklio reikšmė *j*-ajam objektui.

Taikant SAW metodą tinkamiausia S_j kriterijaus reikšmė yra didžiausia. Rodikliai gali būti tiek maksimizuojantys, tiek minimizuojantys, skaičiavimo metodikoje galima įvesti skirtingą rodiklių skaičių ir kiekvieno rodiklio svorinį koeficientą. Minimizuojamus rodiklius galima pertvarkyti į maksimizuojamus pagal formules (3.5):

a) maksimizavimo atveju: $r_{ij}^{max} = \frac{r^{min_i}}{r_{ij}}$; (3.5)

b) minimizavimo atveju: $r_{ij}^{min} = \frac{r^{max_i}}{r_{ij}}$. (3.6)

Daugiakriterį uždavinį galima pavaizduoti kaip *a* aibę *n* galimų veiksnių a_j (j = 1, 2, 3, ..., *n*), kur *k* yra kriterijų aibė (i = 1, 2, 3, ..., *m*) svarbiam sprendimui priimti. Vertinant įvertinimas x_1 bus geresnis už įvertinimą x_2 (abu priklauso įver-

tinimų aibei *X*) pagal *i*-tąjį kriterijų, jei $x_{i1} > x_{i2}$. Daugiakriterio uždavinio sprendimas pavaizduotas 3.3 lentelėje. Turint *A* (veiksnių) ir *K* (kriterijų) aibes, kur yra *n* veiksnių ir *m* kriterijų, galima sudaryti *nm* matricą *X*, kurios elementas x_{iaj} (i = 1, 2, 3,..., *m* ir *j* = 1, 2, 3, ..., *n*) rodo *i*-tojo veiksnio įvertinimą pagal *j*-ąjį kriterijų. Jei i_1, i_2, i_3, ..., i_n yra veiksniai, o j_1, j_2, j_3, ..., j_m – kriterijai, tai x_{ij} yra sprendinio a_i įvertinimas pagal k_j kriterijų. Kriterijai dažniausiai yra skirtingi pagal savo svarbą ir turi skirtingus įverčius. Pažymėjus kriterijų įverčius η_1, η_2, η_3…..η_n kiekvienai lentelės eilutei skaičiuojamas dydis S_i pagal formulę (3.7):

$$S_i = x_{i1}\eta_1 + x_{i2}\eta_2 + x_{i3}\eta_3 + \cdots + x_{in}\eta_n. \qquad (3.7)$$

3.3 lentelė. Veiksnių įvertinimų matrica
Table 3.3 Matrix of factor ratings

Kriterijai	j_1		j_2		j_j		$\sum_{i=1}^{j} K_{ij}\eta_j$	Rangas
Veiksniai	Įvertis	$K_{ij}\eta_1$	Įvertis	$K_{ij}\eta_2$	Įvertis	$K_{ij}\eta_j$		
i_1	Veiksnio i_1 reikšmė pagal kriterijų j_1	Kriterijaus reikšmingumo ir įverčio sandauga	Veiksnio i_1 reikšmė pagal kriterijų j_1		Veiksnio i_1 reikšmė pagal kriterijų j_j		Veiksnio i_1 reikšmė	2
i_2	Veiksnio i_2 reikšmė pagal kriterijų j_1	Kriterijaus reikšmingumo ir įverčio sandauga	Veiksnio i_2 reikšmė pagal kriterijų j_2		Veiksnio i_2 reikšmė pagal kriterijų j_j		Veiksnio i_2 reikšmė	3
i_n	Veiksnio i_n reikšmė pagal kriterijų j_1	Kriterijaus reikšmingumo ir įverčio sandauga	Veiksnio i_n reikšmė pagal kriterijų j_2		Veiksnio i_n reikšmė pagal kriterijų j_j		Veiksnio i_n reikšmė	1

3.3 lentelėje išvardinami kiekybiniai vertinimo kriterijai, kurie matuojami intervalų ar santykių skalėje, o kokybiniai kriterijai išmatuojami nominalia ar paprasta skale. Toliau veiksniai rūšiuojami pagal svarbą vertinant juos balais. Tokiu

būdu sprendiniams surūšiuoti nereikia veiksnių reikšmingumo, pakanka kokybinės informacijos apie veiksnio svarbą. Sudaryta veiksnių įvertinimo matrica leidžia veiksnius surūšiuoti. Rūšiuojant svarbiausiam veiksniui suteikiamas rangas, lygus vienetui, ir atitinkamai pagal svarbumą surūšiuojami kiti veiksniai. Veiksniai ranguojami, siekiant numatyti, kuriems veiksniams skirti prioritetus ir būtent nuo šių veiksnių pradėti veiklos kibernetinio saugumo įgyvendinimo procesą.

3.2. Valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio empirinio tyrimo rezultatai

Pagal 3.1 poskyryje aprašytą metodiką (3.1 lentelė) reikia nustatyti pasirinktų komponentų reikšmingumą valstybių kritinės energetinės infrastruktūros kibernetiniam saugumui.

Ekspertinis vertinimas. Komponentų reikšmingumui nustatyti buvo parinkta 10 ekspertų iš skirtingų Lietuvos įmonių, atitinkančių tam tikrus kriterijus: išsilavinimas, įgyvendintų projektų skaičius, darbo patirtis, darbo stažas, mokslinis laipsnis ir gebėjimas spręsti konkrečias atitinkamos srities problemas. Taip pat pokalbių su vadovybe metu buvo nustatytas tyrimo laikas, ekspertų kompetencijos ir jų skaičius. Mokslininkų teigimu, norint gauti patikimus ir objektyvius rezultatus, rekomenduojama apklausti ne mažiau kaip 5 ekspertus. Didėjant ekspertų skaičiui vertinimo patikimumas didėja nežymiai, o didžiausias įverčių tikslumas yra esant 5–9 ekspertų grupės skaičiui (Augustinaitis et al., 2009). Todėl pagrindiniai ekspertų atrankos kriterijai buvo magistro kvalifikacinis laipsnis, vadovaujamos pareigos ir ne mažesnė kaip 3 metų darbo patirtis kibernetinio saugumo valdymo srityje energetikos sektoriuje. Detalesnė informacija apie ekspertus pateikta 3.7 lentelėje.

Dalyvaujantys ekspertinje apklausoje, turi pakankamą patirtį, kad būtų išnagrinėtos ir pateiktos iškylančios problemos – valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modulio komponentų sukūrimo ir sprendimo būdas. Tyrimo metu buvo taikytas individualios apklausos tyrimo metodas. Ekspertams buvo sudaryta anketa anglų kalba (A priedas) ir išsiųsta elektroniniu paštu 10 ekspertų. Tyrimo metu ekspertai turėjo įvertinti balais nuo 1 iki 5, kur 1 – labai svarbus, o 5 – nesvarbus, ne tik komponentus, bet ir klausimus.

Deja, buvo gauti tik 5 atsakymai, bet to užteko, kad būtų atliktas tyrimas ir gautas patikimas nagrinėjamos problemos vertinimas. Vertinimo rezultatai pateikti 3.4 lentelėje.

3.4 lentelė. Ekspertų vertinimo rezultatų reikšmingumas
Table 3.4. Significance of expert evaluation results

Ekspertai / Komponentai	E_1	E_2	E_3	E_4	E_5	Reikšmingumas	Rangas
Rizikos valdymas	0,2	0,21	0,14	0,14	0,09	0,16	4
Teisinis reguliavimas	0,1	0,07	0,21	0,14	0,18	0,14	3
Kibernetinio saugumo kultūra	0,1	0,14	0,21	0,21	0,09	0,16	4
Technologinis kibernetinis saugumas	0,2	0,29	0,14	0,14	0,18	0,19	5
Kibernetinių incidentų valdymas	0,1	0,14	0,07	0,14	0,18	0,13	2
Strateginis valdymas	0,1	0,07	0,07	0,07	0,18	0,10	1
Organizacijos valdymas	0,2	0,07	0,14	0,14	0,09	0,13	2

Apklausos duomenų analizė parodė, kad ekspertai aukščiausią rangą suteikė strateginiam valdymui (reikšmingumas – 0,10), o žemiausią – technologiniam kibernetiniam saugumui (reikšmingumas – 0,19). Įvertinus ekspertų vertinimo rezultatų reikšmingumą, papildomai būtina nustatyti ekspertų nuomonių suderinamumą (3.5 lentelė), naudojant aprašytą 3.2 lentelėje skaičiavimo eigą.

3.5 lentelėje pateikti skaičiavimo rezultatai rodo, kad konkordancijos koeficientas *W* artėja prie vieneto ir lygus 0,875, o tai reiškia, kad ekspertų vertinimo suderinamumas pakankamai geras ir gautus rezultatus galima naudoti tolesniems tyrimams. Kadangi ekspertų vertinimuose buvo vienodi rangai, konkordancijos koeficientas skaičiuojamas, taikant formulę (3.2 lentelė), kai yra vienodi rangai.

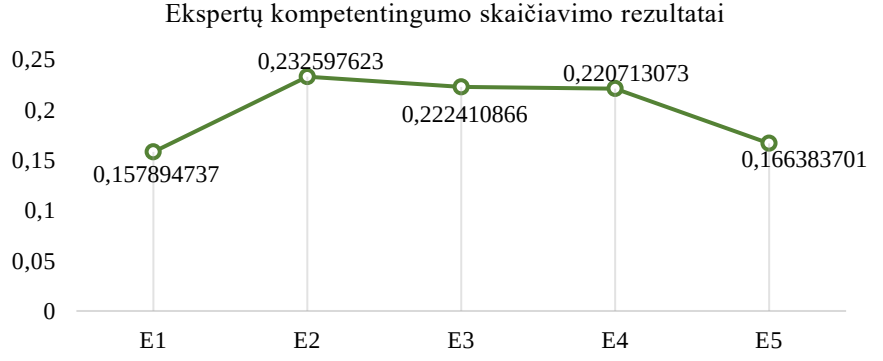
Apskaičiuojant konkordancijos koeficientą, būtinai reikėjo įvertinti ir ekspertų kompetenciją, kuri skaičiuojama pagal 3.2 formulę. Ekspertai kompetentingi, jeigu kompetencijų įverčių suma lygi vienetui. Skaičiavimo rezultatai pavaizduoti 3.7 diagramoje ir 3.6 lentelėje. Pagal 3.6 lentelėje pateiktus skaičiavimus matyti, kad įverčių suma lygi vienetui, o tai reiškia, kad ekspertai kompetentingi ir jų nuomonėmis galima tikėti ir naudoti jas tyrime.

3.5 lentelė. Ekspertų nuomonių suderinamumo rezultatai
Table 3.5. Results of concordance of expert opinions

	Rizikos valdymas	Teisinis reguliavimas	Kibernetinio saugumo kultūra	Technologinis kibernetinis saugumas	Kibernetinių incidentų valdymas	Strateginis valdymas	Organizacijos valdymas
Rangų suma	10	9	10	12	8	6	8
Rangų sumų vidurkis	9						
Nuokrypių kvadratas	1	81	100	144	64	36	64
Nuokrypių kvadratų suma	490						
Konkordancijos koeficientas *W*	0,875						

3.6 lentelė. Ekspertų kompetencijos skaičiavimo rezultatai
Table 3.6. Results of expert competence calculation

	E1	E2	E3	E4	E5	Įverčių suma
Ekspertų kompetencija	0,16	0,23	0,22	0,22	0,17	1



3.5 pav. Ekspertų kompetentingumo skaičiavimo rezultatai
Fig. 3.5. Results of expert competence calculation

Veiksnių rinkinio sudarymas. 3.1 poskyryje buvo aprašytas Delfi metodas, kurį taikant buvo atliekamas tyrimas (Günaydın, 2006). Pagal šį metodą spren-

džiama problema turi būti suskaidyta. Todėl valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modulis buvo suskaidytas į 7 komponentus. Siekiant gauti tikslų ir išsamų sprendžiamos problemos vertinimą, kiekvieną komponentą sudaro klausimai, kuriuos ekspertai ne tik ranguoja pagal svarbumą (1 – labai svarbus, 5 – neįdomu), bet ir turi parašyti savo nuomonę.

Organizacijos ir kibernetinių incidentų valdymo procesai sudaro po 2 veiksnius, teisinį reguliavimą, kibernetinio saugumo kultūrą – po 6 klausimus, technologinį kibernetinį saugumą ir rizikos valdymą – po 5 veiksnius, o strateginį valdymą – po 3 klausimus (3.6 pav.).

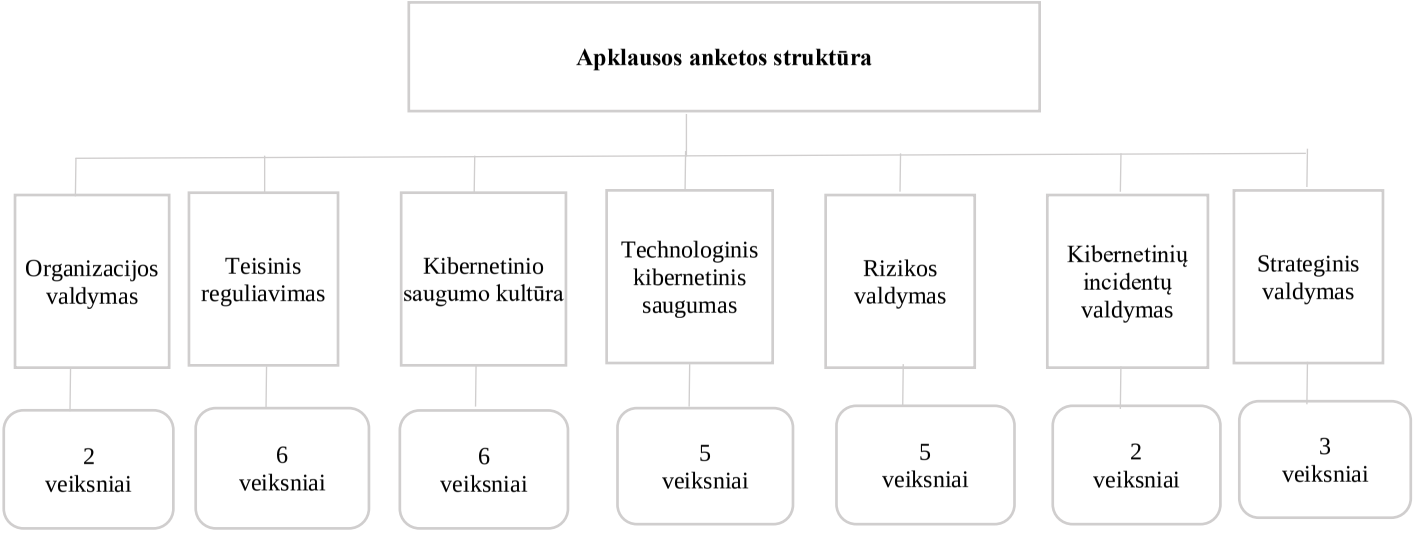
Sukurto kibernetinio saugumo modelio empirinis tyrimas buvo atliktas 2020 m. liepos–rugpjūčio mėn. Ekspertai, kurie dalyvavo tyrime, buvo pasirinkti pagal tokį kriterijų: ne mažesnė negu 3 metai valdymo patirtis kibernetinio saugumo srityje. Dalyvavimui apklausoje pagal nustatytus kriterijus buvo pasirinkti penki ekspertai, turintys daugiau negu 3 metų valdymo patirtį šioje srityje. Pasirinktų ekspertų duomenys pateikti 3.7 lentelėje.

3.7 lentelė. Ekspertų charakteristikos
Table 3.7. Experts characteristics

Ekspertai	Išsilavinimas	Darbo stažas	Pareigos	Įmonė, šalis
E1	Magistras	7	vadovas	INL, US
E2	Magistras	5	vadovas	AOTD, Lietuva
E3	Daktaras	5	vadovas	KAM, Lietuva
E4	Daktaras	10	vadovas	NKSC, Lietuva
E5	Magistras	10	ekspertas	IK-Institute, Prancūzija

Ekspertų charakteristikos. Anketavimas buvo anonimiškas, todėl tyrime vartojami sutartiniai žymėjimai – E (ekspertas) ir skaičius, kuris rodo eksperto numerį.

Apklausoje dalyvavo karjeros bei statutiniai valstybės tarnautojai, mokslininkai, dirbantys kibernetinio saugumo srityje energetikos sektoriuje. Pagal tyrimo reikalavimus ekspertas privalo būti Europos Sąjungos šalių narių pilietis (tik išskirtiniais atvejais gali būti daromos išimtys), turintis mažiausiai 3 metų darbo patirtį kibernetinio saugumo, konsultavimo ir priežiūros srityje. Privalo mokėti bent dvi oficialias ES kalbas (anglų ir prancūzų) ir turėti socialinių ar technologinių mokslų išsilavinimą.



3.6 pav. Apklausos anketos struktūra
Fig. 3.6. Survey structure according to the Delphi method

Tam, kad būtų patikrintas kibernetinio saugumo modelis, buvo sudaryta anketa (A priedas). Anketoje pateikti 29 klausimai, suskirstyti pagal 7 komponentus. Kiekvienam komponentui pateiktas išplėstinis paaiškinimas. Anketavimo tikslas buvo įvertinti kiekvieną komponentą, pateiktus klausimus ir išrikiuoti juos pagal svarbumą. Tyrimui atlikti buvo pasirinktas anoniminis, nedalyvaujamasis anketavimas. Kiekvienam ekspertui anketa su paaiškinimais buvo išsiųsta elektroniniu paštu. Ekspertams reikėjo įvertinti kiekvieną klausimą balais nuo 1 (labai svarbus) iki 5 (nesvarbu) pagal septynis komponentus: organizacijos valdymas, teisinis reguliavimas, kibernetinio saugumo kultūra, technologinis kibernetinis saugumas, rizikos valdymas, kibernetinių incidentų valdymas ir strateginis valdymas. Taip pat ekspertai prieš kiekvieną klausimą parašė savo nuomonę ir išrikiavo kibernetinio saugumo modulio komponentus pagal svarbumą.

Pagal gautus apklausos rezultatus, taikant paprastąjį adityvų svorių metodą SAW, sudaryta skaičiavimo matrica, duomenys normalizuoti ir apskaičiuoti įverčiai, nustatyti rangai (3.3 lentelė). 3.8 lentelėje parodyti penkių ekspertų, dalyvaujančiųjų tyrime, visų komponentų įverčiai ir rangai.

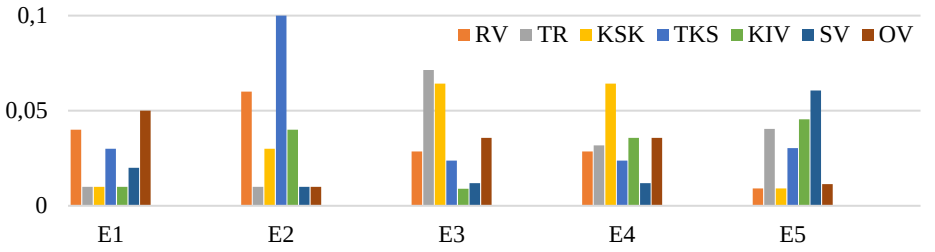
3.8 lentelė. Visų komponentų įverčiai ir rangai
Table 3.8. Estimates and ranks for all components

	E1		E2		E3		E4		E5		Rangų vidurkis	Galutinis rangas
	Įverčiai	Rangas	Įverčiai	Rangas	Įverčiai	Rangas	Įverčiai	Rangas	Įverčiai	Rangas		
RV	0,04	2	0,06	2	0,028571	4	0,028571	4	0,009091	6	3,2	3
TR	0,01	5	0,01	5	0,071429	1	0,031746	3	0,040404	3	3,4	4
KSK	0,01	5	0,03	4	0,064286	2	0,064286	1	0,009091	6	3,2	3
TKS	0,03	3	0,10	1	0,02381	5	0,02381	5	0,030303	4	3,2	3
KIV	0,01	5	0,04	3	0,008929	7	0,035714	2	0,045455	2	3	2
SV	0,02	4	0,01	5	0,011905	6	0,011905	6	0,060606	1	2,4	1
OV	0,05	1	0,01	5	0,035714	3	0,035714	2	0,011364	5	3,6	5

OV – organizacijos valdymas, TR – teisinis reguliavimas, KSK – kibernetinio saugumo kultūra, TKS – technologinis kibernetinis saugumas, RV – rizikos valdymas, KIV – kibernetinių incidentų valdymas, SV – strateginis valdymas.

Analizuojant rezultatus, pateiktus 3.8 lentelėje, galima pastebėti, kad svarbiausias valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modulio komponentas yra strateginis valdymas, antroje vietoje – kibernetinių incidentų valdymas, o trečioje – rizikos valdymas, kibernetinio saugumo kultūra ir

technologinis kibernetinis saugumas. Ketvirtoje ir penktoje vietoje – teisinis reguliavimas ir organizacijos valdymas.



OV – organizacijos valdymas, TR – teisinis reguliavimas, KSK – kibernetinio saugumo kultūra, TKS – technologinis kibernetinis saugumas, RV – rizikos valdymas, KIV – kibernetinių incidentų valdymas, SV – strateginis valdymas.

3.7 pav. Komponentų įverčių paskirstymas
Fig. 3.7. Distribution of component estimates

Daugiakriterio vertinimo metodo SAW taikymas leidžia susumuoti visų komponentų įverčius. Galutinis kiekvieno komponento įvertis skaičiuojamas sumuojant visus įverčius (3.9 lentelė).

3.9 lentelė. Visų komponentų įverčiai ir rangai
Table 3.9. Estimates and ranks for all components

	E1	E2	E3	E4	E5	E6	
	Įverčiai	Įverčiai	Įverčiai	Įverčiai	Įverčiai	Galutiniai įverčiai	Rangai
RV	0,04	0,06	0,028571	0,028571	0,009091	0,16623	5
TR	0,01	0,01	0,071429	0,031746	0,040404	0,16358	4
KSK	0,01	0,03	0,064286	0,064286	0,009091	0,17766	6
TKS	0,03	0,10	0,02381	0,02381	0,030303	0,20792	7
KIV	0,01	0,04	0,008929	0,035714	0,045455	0,1401	2
SV	0,02	0,01	0,011905	0,011905	0,060606	0,11442	1
OV	0,05	0,01	0,035714	0,035714	0,011364	0,14279	3

OV – organizacijos valdymas, TR – teisinis reguliavimas, KSK – kibernetinio saugumo kultūra, TKS – technologinis kibernetinis saugumas, RV – rizikos valdymas, KIV – kibernetinių incidentų valdymas, SV – strateginis valdymas.

Analizuojant rezultatus, pateiktus 3.9 lentelėje, galima teigti, kad skirtumas tarp komponentų įverčių nėra didelis. Kiekvienas ekspertas, dalyvaujantis tyrime, nagrinėjant valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio komponentus, išreiškė nuomonę, kad visi komponentai yra svarbūs. Tačiau yra tokių, kuriuos būtinai reikia tobulinti, pvz., strateginį valdymą. Kaip parašė vienas iš ekspertų: „Pirmiausia turime įsivaizduoti, kaip elgtis. Jei neturime trumpalaikės ar ilgalaikės strategijos, galime išvaistyti laiką ir išteklius ir niekada nepasiekti tinkamo rezultato ar nepriimti tinkamų sprendimų“.

3.3. Valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio praktinio taikymo rekomendacijos

Apibendrinant empirinio tyrimo rezultatus, galima pateikti valstybių kritinės energetinės infrastruktūros kibernetinio saugumo valdymo modelio praktinio taikymo rekomendacijas.

Antrajame skyriuje buvo aprašytas ir aprobuotas teorinis valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelis, kurį sudaro šeši komponentai: organizacijos valdymas, teisinis reguliavimas, kibernetinio saugumo kultūra, technologinis kibernetinis saugumas, rizikos valdymas ir kibernetinių incidentų valdymas (2.1 pav.). Išanalizavus galimas su kibernetiniu saugumu susijusias problemas ir kibernetinio saugumo valdymo modelio aprobavimo rezultatus, paaiškėjo, kad siekiant tobulinti ir stiprinti valstybių kritinės infrastruktūros kibernetinio saugumo valdymą, modelio įgyvendinimo procesas turi būti paremtas ISO/ES 27002 informacinių technologijų standartu (ISO/IES Techninio komiteto JTC1, 2013), kuriame pateikiama geroji praktika įgyvendinant veiksmingą kritinės infrastruktūros objektų saugumo modelį. Dėl to ir buvo patobulintas kibernetinio saugumo modelis ir pridėtas dar vienas komponentas – strateginis valdymas (2.7 pav.).

Patobulinus modelį, buvo atliktas kiekybinis empirinis tyrimas, siekiant ne tik išsiaiškinti ekspertų nuomonę apie valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio struktūrą, komponentų svarbą, bet ir išsiaiškinti, ar strateginis valdymas yra būtinas, kai kalba eina apie kibernetinį saugumą.

Autoriaus validuojamas valstybių kritinės infrastruktūros kibernetinio saugumo modelis buvo vertinamas penkių balų sistema pagal svarbiausius komponentus, kurie yra tokie: rizikos valdymas, teisinis reguliavimas, kibernetinio saugumo kultūra, technologinis kibernetinis saugumas, kibernetinių incidentų valdymas, organizacijos valdymas ir strateginis valdymas. Atsižvelgiant į ekspertų vertinimą ir pateiktą nuomonę, galima nustatyti, kokius komponentus reikia

tobulinti, pritaikant šį modelį bet kokiai kritinei infrastruktūrai, kad būtų pagerintas kibernetinis saugumas.

Analizuojant gautus duomenis, ekspertų nuomones ir skaičiavimo rezultatus, galima padaryti išvadą, kad kiekvienas valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio komponentas yra svarbus. Suprantama, kad norint apsaugoti bet kokią infrastruktūrą, šiuo atveju – valstybės kritinę energetinę infrastruktūrą, būtinai reikia plėtoti kiekvieną komponentą, ypač strateginį valdymą, nes kol kas tai yra nauja valstybių kritinės infrastruktūros kibernetinio saugumo modelio dalis.

Apskaičiuoti komponentų įverčiai, taikant paprastąjį adityvų svorių metodą (SAW), turi būti susumuojami ir būtinai išdėstyti, siekiant nustatyti komponentų prioritetus. Remiantis gautais rezultatais, galima spręsti, kuriuos komponentus pirmiausia reikia pagerinti, norint padidinti kibernetinio saugumo lygį.

Remiantis atlikto tyrimo rezultatais, galima teigti, kad šio darbo tikslas – sukurti naują kibernetinio saugumo valdymo modulį – pasiektas. Teoriškai darbe buvo analizuojamas valstybių kritinės energetinės infrastuktūros kibernetinio saugumo valdymas bei stiprinimas. Tačiau, kaip žinome, teorija turi būti paremta praktika. Todėl būtina parodyti, kaip galima pritaikyti šį modulį su visais jo komponentais, kurie sąveikauja tarpusavyje. Ir kaip techniškai įmanoma įgyvendinti kritinės energetikos infrastuktūros kibernetinio saugumo valdymą ir stiprinimą.

Tyrimo rezultatai parodė, kad strateginio valdymo komponentas turi būti tobulinamas, nes vien struktūrinimo nepakanka išsamiam jo panaudojimui. Būtina nustatyti veiksmus, kurių reikia imtis norint teisingai ir aiškiai įgyvendinti kibernetinį saugumą naudojant šį komponentą. Remiantis antroje darbo dalyje aprašyta strateginio valdymo komponento struktūra (2.6 pav.), turėtų būti aiškiai aprašyti pagrindiniai etapai ir įgyvendinti būtini veiksmai.

1. Išorinės aplinkos analizė

Kuriamas strateginis planas egzistuos ir veiks nuolat kintančioje aplinkoje, kuri veikia plano elementus ir jų funkcionalumą, o tai savo ruožtu veikia ir paties plano įgyvendinimą. Todėl reikalinga išorinė aplinkos analizė ir tam galima panaudoti kibernetinio saugumo valdymo modelio rizikos valdymo ir teisinio reguliavimo komponentus.

Užpuolikai puola kritinės infrastruktūros objektus, kurie atlieka pagrindinį vaidmenį valstybės ir ekonomikos struktūroje. Todėl sistemų pažeidžiamumų ir gedimų tikrinimas turi būti atliekamas atidžiai. Štai kodėl, norint nustatyti prioritetus, pirmiausia reikia atlikti rizikos vertinimą, kuris yra labai svarbus elementas nustatant saugumo problemas, susijusias su galima žala.

Rizikos analizė padeda nustatyti tikimybę ir galimus būdus, kaip riziką suvaldyti. Būtina įvertinti prioritetus, rizikas, bendrus pažeidžiamumus, saugumo spragas, įskaitant personalą. Taip pat įvertinti pavojų poveikio riziką, kuri padės

sukurti struktūrą, tinkamai paskirstyti išteklius, atsakomybę ir nustatyti specializuotas apsaugos priemones.

Kritinės infrastruktūros objektai turi atnaujinti informacinių sistemų ir tinklų, įskaitant pramoninę įrangą, saugumo tyrimus ir įvertinti poveikį infrastruktūros ištekliams. Taigi rizikos ir poreikių analizė yra du tarpusavyje susiję dalykai.

2. Vidinės aplinkos analizė

Suvokus išorinę aplinką, norint geriau reaguoti į būtinus pokyčius, svarbu suprasti ir teisingai įvertinti vidinę situaciją. Todėl, vertinant vidinę aplinką, būtina išanalizuoti organizaciją ir visą jos veiklą, naudojant kibernetinio saugumo valdymo modulio organizacijos valdymo, kibernetinio saugumo kultūros, kibernetinio saugumo technologijų ir kibernetinių incidentų valdymo komponentus.

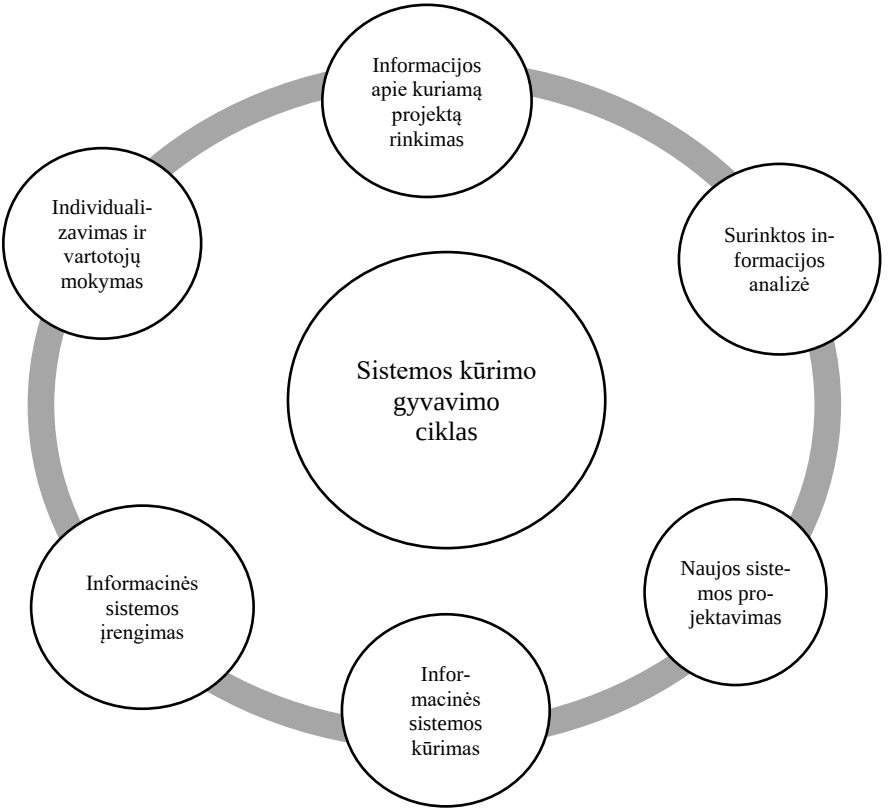
Šiame procese naudingas įrankis gali būti sistemos kūrimo gyvavimo ciklo projektavimo metodas. Tai vienas seniausių kompiuterinių informacinių sistemų kūrimo metodų, taikomas didelėse ir sudėtingose infrastruktūrose, tokiose kaip kritinės infrastruktūros. Manoma, kad informacinė sistema turi iš anksto nustatytą gyvavimo trukmę, todėl ji lyginama su žmogaus gyvavimo ciklu. O kadangi aplinka, kurioje planas bus įgyvendinamas, nuolat kinta, toks sistemos ciklas turi prasmę.

Sistemos kūrimo gyvavimo ciklo metodas susideda iš 6 etapų (3.8 pav.):

1. Informacijos apie kuriamą projektą rinkimas.
2. Surinktos informacijos analizė.
3. Naujos sistemos projektavimas, atsižvelgiant į būtinas sąlygas ir saugos reikalavimus.
4. Informacinės sistemos kūrimas.
5. Informacinės sistemos įrengimas infrastruktūroje.
6. Individualizavimas ir vartotojų mokymas.
7. Sistemos kūrimo gyvavimo ciklo metodas, kaip minėta anksčiau, yra plačiai taikomas kuriant informacines sistemas didelėms infrastruktūroms, įskaitant kritines infrastruktūras. Kritinėms infrastruktūroms reikia kruopščios saugumo reikalavimų ir specifikacijų analizės. Kuriant informacines sistemas būtina griežta technologinė kontrolė.

3. Strateginio valdymo plano formavimas

Atlikus rizikos analizę, būtina suformuluoti strategijos valdymo planą. Ir tam, visų pirma, reikia išsiaiškinti, iš kokių elementų strategijos valdymo planas bus sudarytas ir ką tiksliai reikia padaryti, norint tai įgyvendinti. Savo struktūra ir darbo specifika visos įmonės yra skirtingos, tačiau rengiant strateginio valdymo planą pagrindiniai elementai, kuriais bus naudojamasi, bus vienodi visiems (3.9 pav.). Verta prisiminti, kad visi darbai, įvertinimai ir reikalavimai, reikalingi strateginiam planui įgyvendinti, turi būti dokumentuoti.



3.8 pav. Sistemos kūrimo gyvavimo ciklas
Fig. 3.8. Software development life cycle

3.9 pav. Strateginio valdymo proceso seka
Fig. 3.9. Strategic management process sequence

Kiekvienas strateginio valdymo plano elementas turėtų būti išsamiai aprašytas, tačiau prieš tai reikia nuspręsti, kuriuos elementus įtraukti, o kurių ne. Formuojant misiją, nustatant tikslus ir uždavinius, būtina viską įvertinti atsižvelgiant į infrastruktūros ir duomenų saugumą, nes įgyvendinimo strategija yra atsakinga už visus aspektus: IT (vietinį ir nuotolinį), OT, debesų ir mobiliąsias technologijas.

Funkciniai reikalavimai. Kitas žingsnis, kurį reikia atlikti, norint sėkmingai įgyvendinti strateginio valdymo strategiją, yra funkcijų, kurios bus vykdomos, pasirinkimas. Iš tikrųjų yra daugiau nei 40 funkcijų – nuo duomenų apie incidentus rinkimo iki bendravimo su teisėsaugos institucijomis, nuo kenkėjiško kodo analizės iki darbuotojų informuotumo didinimo. Tačiau tai nereiškia, kad jomis visomis reikia naudotis. D priede parodytos visos funkcijos, kurias galima naudoti, atsižvelgiant į užduotis ir išteklius. Todėl pačioje strategijos įgyvendinimo pradžioje geriau taikyti mažiau funkcijų negu daugiau. Norint suprasti, kokias funkcijas naudoti, būtina atlikti analizę, orientuotis į pagrindinius uždavinius bei procesus, kurie užtikrins strategijos įgyvendinimą. Pavyzdžiui, informacijos saugumo ir IT duomenys turi būti renkami, saugomi ir tvarkomi taip, kad vartotojai galėtų pranešti apie įtartiną veiklą ir tirti incidentus bei reaguoti į juos.

Procesai ir procedūros gali būti pavaizduoti kaip seka, sugrupuoti pagal veiklos sritis (3.10 pav.).

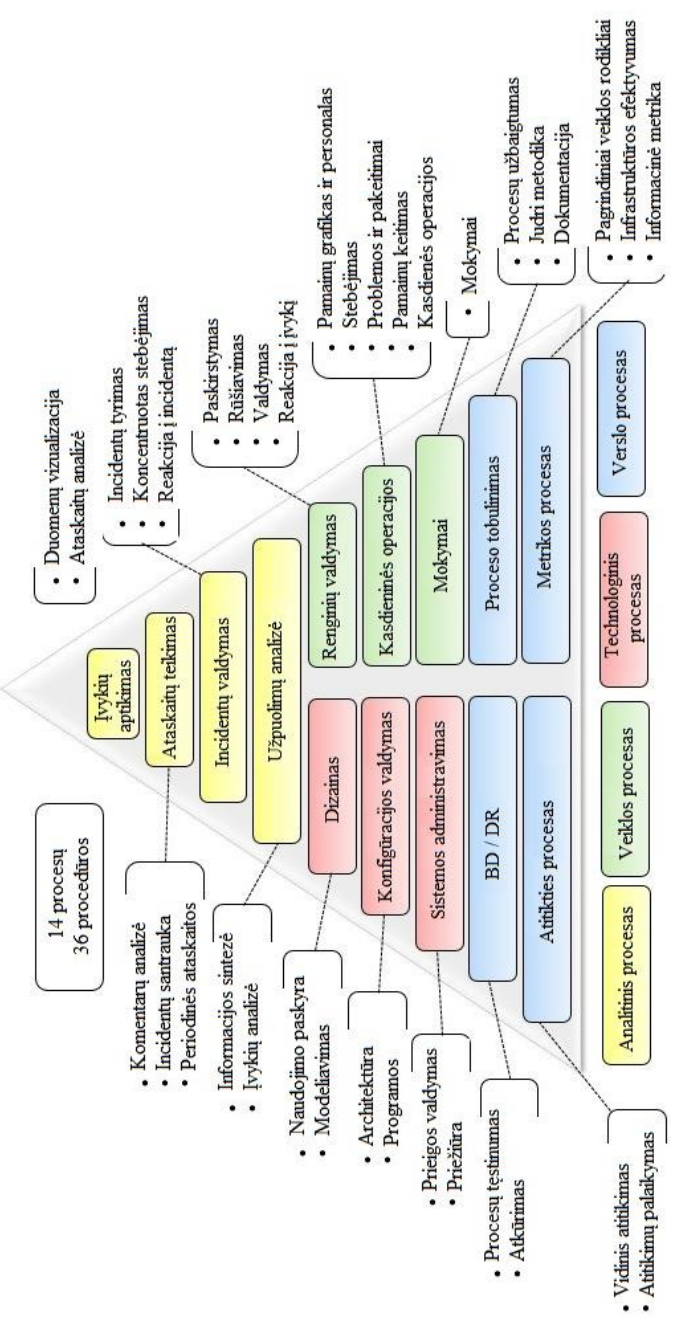
Nepaisant didžiulio funkcijų pasirinkimo, kiekviena organizacija orientuojasi į savo tikslus ir uždavinius, turimus darbuotojus ir biudžetą. Todėl, rengiant strategiją, verta atkreipti dėmesį į 10 pagrindinių funkcijų, kurias būtina atlikti (3.10 lentelė):

3.10 lentelė. 10 pagrindinių funkcijų sąrašas, sudaryta remiantis Trellix.com
Table 3.10. List of ten key features (based on Trellix.com)

	Funkcija	Aprašymas
1	2	3
1	Turimų resursų įvertinimas	Turimų resursų įvertinimas, skirstomas į du tipus: įvairūs įrenginiai, procesai ir programos, kuriuos reikia apsaugoti, ir turimi apsaugos įrankiai, padedantys užtikrinti šią apsaugą.
2	Paruošimas ir profilaktinė priežiūra	Netgi geriausiai įrengti ir lanksčiausi reagavimo procesai negali išvengti problemų. Norint išvengti užpuolimų, būtina įgyvendinti prevencines priemones, kurias galima suskirstyti į dvi pagrindines kategorijas: *Paruošimas* – komandos nariai turi žinoti naujausias saugumo naujoves, kibernetinių nusikaltimų tendencijas ir kylančias grėsmes. Šis tyrimas gali padėti sukurti saugumo planą, nurodantį įmonės kibernetinio saugumo kryptį, taip pat atkūrimo planą, kuris būtų naudojamas blogiausiu atveju. Profilaktinė priežiūra – šis žingsnis apima visus veiksmus, kurių imamasi siekiant apsunkinti sėkmingas atakas, įskaitant nuolatinę esamų sistemų priežiūrą ir atnaujinimą, ugniasienės politikos atnaujinimą, pažeidžiamumų taisymą ir įtraukimą į baltąjį sąrašą, įtraukimą į juodąjį sąrašą ir programų apsaugą.

3.10 lentelės pabaiga

1	2	3
3	Nuolatinis aktyvus stebėjimas	24 valandas per parą, 7 dienas per savaitę naudojami įrankiai nuskaito tinklą, kad užfiksuotų bet kokius nukrypimus arba įtartiną veiklą. Stebint tinklą 24/7 nedelsiant pranešama apie kylančias grėsmes, o tai suteikia daugiau galimybių užkirsti kelią žalai arba ją sumažinti.
4	Įspėjimų reitingavimas ir valdymas	Gavus įspėjimus, reikia atidžiai išanalizuoti kiekvieną iš jų, atmetant visus klaidingus, ir nustatyti, kiek pavojingos yra grėsmės ir į ką jos gali būti nukreiptos. Tai leidžia tinkamai rūšiuoti kylančias grėsmes, pirmiausia sprendžiant pačias aktualiausias problemas.
5	Reagavimas į grėsmes	Patvirtinus incidentą, atliekami šie veiksmai: galinių taškų išjungimas arba izoliavimas, kenkėjiškų procesų nutraukimas (arba jų paleidimo užkardymas), failų ištrynimas ir kt. Reakcija į incidentą turi būti tokia, kad kuo mažiau paveiktų procesų tęstinumą.
6	Atkūrimas ir taisymas	Sistemos ir visų prarastų ar pažeistų duomenų atkūrimas. Tai apima galinių taškų valymą ir paleidimą iš naujo, sistemų perkonfigūravimą arba patikimų atsarginių kopijų diegimą. Jei pavyks, šis veiksmas grąžins tinklo būseną, buvusią prieš incidentą.
7	Žurnalo valdymas	Informacija apie tinklo veiklą ir komunikavimą renkama, saugoma ir reguliariai peržiūrima. Šie duomenys padeda nustatyti „įprastos“ tinklo veiklos pradinę padėtį, nustatyti grėsmes ir gali būti naudojami taisymui bei analizei po incidento.
8	Pagrindinės priežasties tyrimas	Po incidento atliekant tyrimą naudojami žurnalo duomenys ir kita informacija, kad būtų galima atsekti problemos šaltinį, o tai gali padėti išvengti panašių problemų ateityje.
9	Saugumo tobulinimas ir gerinimas	Kibernetiniai nusikaltėliai nuolat tobulina savo įrankius ir taktiką, o, norint juos aplenkti, būtina nuolat tobulinti saugumo sistemą. Šiame etape saugumo gairėse išdėstyti planai įgyvendinami praktiškai.
10	Atitikties valdymas	Daugelį procesų reglamentuoja nusistovėjusios gerosios praktikos, tačiau kai kuriems taikomi atitikties reikalavimai. Veikimas pagal šias taisykles ne tik padeda apsaugoti įmonei patikėtus konfidencialius duomenis, bet ir gali apsaugoti organizaciją nuo žalos ir teisinių problemų, kylančių dėl pažeidimo.



3.10 pav. Procesai ir procedūros (sudaryta remiantis *Hewlett-Packard* plėtros duomenimis)
Fig. 3.10. Processes and procedures (based on Hewlett-Packard development company)

Naudojami procesai ir procedūros įgyvendinant strategiją turėtų būti dokumentuojami. Visos organizacijos turi skirtingas dokumentavimo procedūras, tačiau šiame etape reikėtų viską sutvarkyti, kad visi proceso dalyviai (o jų yra daug) žinotų pareigas ir bendrą tikslą. Tik supratus, ką reikia automatizuoti, galima pereiti prie kito etapo – techninių priemonių pasirinkimo. Išskyrus tradicines sistemas, reikės daug papildomų įrankių, dažnai nebrangių ar nemokamų, tačiau iš personalo reikalaujančių tam tikrų žinių. Dėl to galima nustatyti „kokybinius ir kiekybinius“ reikalavimus personalui (Davenport, 1993).

Techniniai reikalavimai. Atlikus vidinę analizę, naudojant kibernetinio saugumo valdymo modulio organizacijos valdymo, kibernetinio saugumo kultūros, kibernetinio saugumo technologijų ir kibernetinių incidentų valdymo komponentus bei apibendrinant gautus rezultatus, galima sukurti struktūrą, padedančią įgyvendinti strategiją.

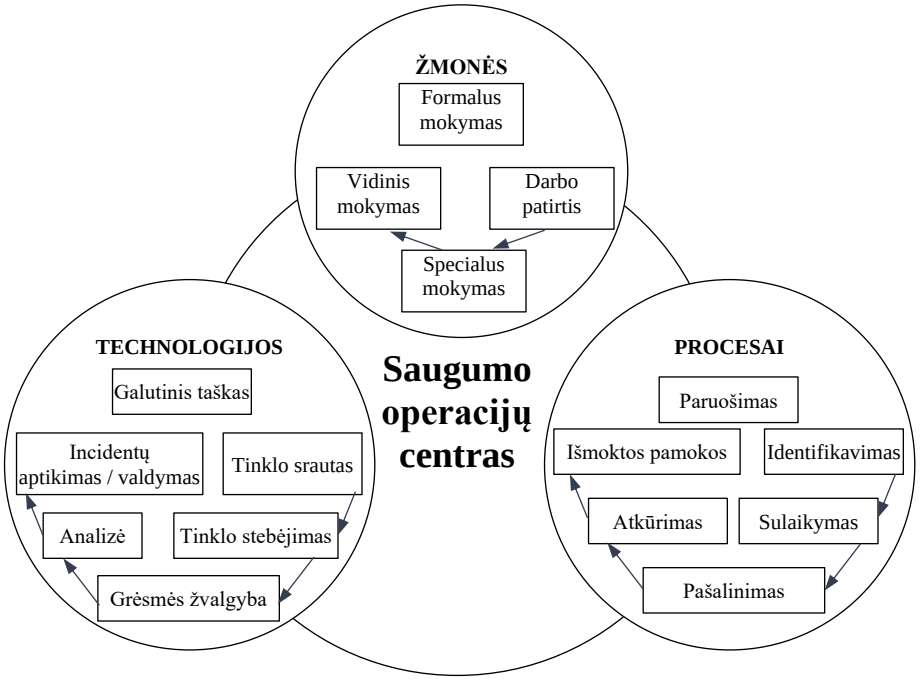
Kadangi duomenų apsaugos poreikis ir toliau auga, reikalingas specialus saugumo operacijų centras (angl. *Security Operation Centre* (SOC)), kuris būtų incidentų valdymo proceso pagrindas.

Visų pirma, SOC yra saugumo ekspertų komanda, turinti kompetencijas ir technologijas, skirtas kibernetinėms grėsmėms aptikti, analizuoti ir užkirsti joms kelią. SOC galima palyginti su ugniagesių ar paramedikų darbu. SOC specialistai, kaip ir gelbėtojai, padeda nelaimės atveju: greitai pasirodo reikiamoje vietoje, analizuoja grėsmes ir tinkamai reaguoja. Juos vienija noras užkirsti kelią tokiems incidentams.

SOC yra nenutrūkstami informacijos srautai, kuriuos apdoroja kompiuterinės sistemos ir ekspertai. Pasirinkus funkcijas, reikia pereiti prie struktūros, apibrėžiančios pagrindinius klasikinės triados „personalas – procesai – technologijos“ komponentus, kūrimo (3.11 pav.).

Nėra vienos SOC struktūros, nes kiekviena turi savo „privalomąjį“ SOC rinkinį, priklausomai nuo funkcijų ir sprendžiamų užduočių apimties. Siūloma struktūra yra savotiškas šablonas, kurį galima naudoti kuriant SOC, prireikus jį tobulinti. Todėl kūrimo metu reikia išspręsti keletą klausimų.

Pirma, kaip SOC užtikrins saugumą? Pavyzdžiui, ar funkcijas atliks nedidelė specializuota komanda, ar auditorija tokia didelė, kad prasminga SOC funkcijas paskirstyti kelioms komandoms? Kitas klausimas – personalo paskirstymas priklausomai nuo atliekamų funkcijų. Kitaip tariant, kaip funkcijos bus perkeltos į personalo vaidmenis ir organizacinę struktūrą. Kaip jau minėta, vienos SOC struktūros, tinkamos visoms organizacijoms, nėra, todėl jas galima derinti. E priede lentelės pavidalu pateikiamos pagrindinės SOC organizacijos struktūros ir su ja susijusios procedūros. Ši lentelė yra šablonas, kuris gali būti naudojamas organizuojant SOC sistemą.

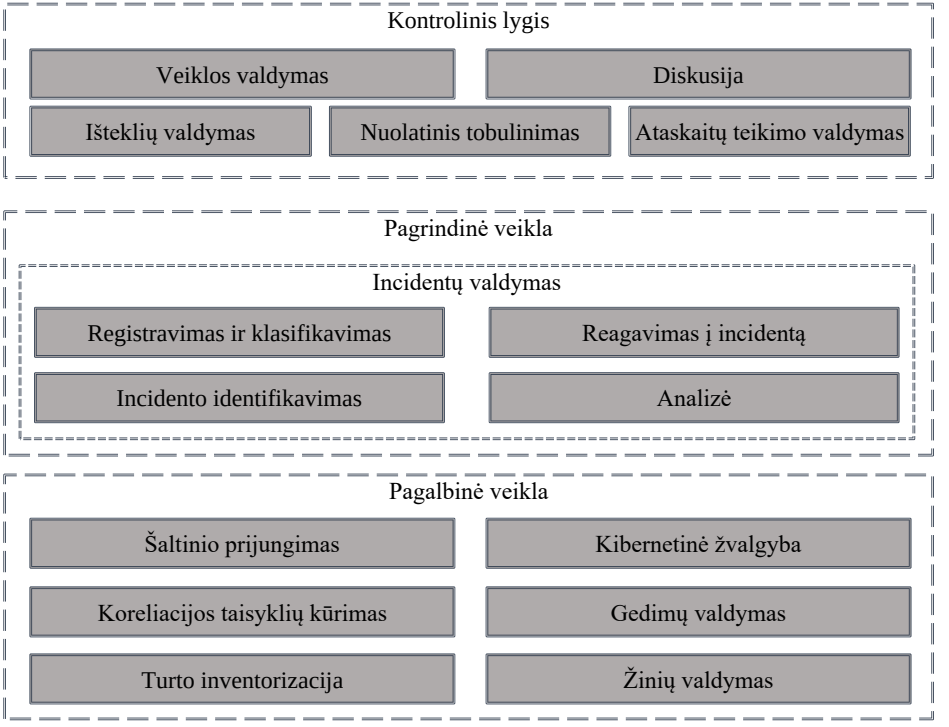


3.11 pav. Pagrindiniai elementai: žmonės, procesai ir technologijos (sudaryta remiantis Muniz (2021)
Fig. 3.11. People, process and Technology Core Elements (based on Muniz, 2021)

Dažna klaida kuriant SOC yra neteisingas procesų derinimas: dažnai standartinė dokumentacija nėra gyvybinga ir „paliekama stalčiuje“. Dėl to specialistai lieka be aiškaus supratimo apie užduotis, su kuriomis susiduria, ir be išsamių instrukcijų, kaip jas įgyvendinti. Tokiomis sąlygomis labai sunku organizuoti veiksmingą sąveiką SOC viduje ir su jais susijusiais padaliniais. Siekiant SOC efektyvumo, rekomenduojama modeliuoti valdymo ir veiklos lygmens procesus. Pirmieji padės užtikrinti pagrindinio funkcionalumo plėtrą ir kokybišką diegimą. Antrieji susiję su pagrindinių ir pagalbinių procesų kūrimu. Jie padeda nustatyti įvykių šaltinius, plėtoti koreliacijos logiką, spręsti trikdžių šalinimo užduotis, atnaujinti informacijos išteklių sąrašą ir duomenis apie juos (3.12 pav.).

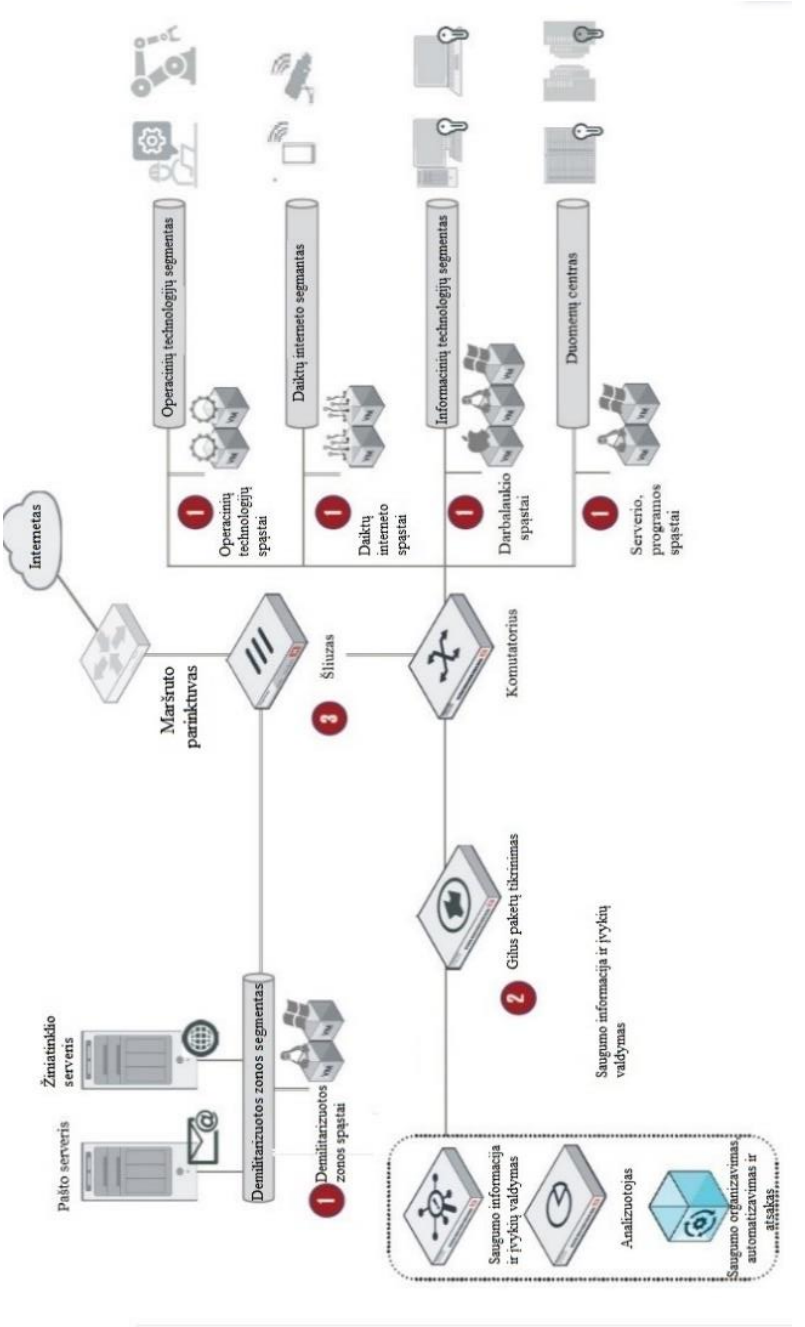
SOC turėtų išanalizuoti įvykius ir informacijos saugos kontrolę, kad nustatytų incidentus. Tai turi būti daroma ne tik realiuoju laiku, bet ir už tam tikrą laikotarpį, siekiant nustatyti praleistus incidentus. Tam, kad incidentas nepasikartotų, svarbu išanalizuoti reagavimo rezultatus. Būtina suprasti, kodėl įvyko incidentas ir kokių

veiksmingų priemonių buvo imtasi jam pašalinti. Metrikų reikšmių stebėjimas leidžia laiku nustatyti ir pašalinti problemas, kurių gali kilti tiek organizuojant procesą, tiek jį įgyvendinant.



3.12 pav. Bendra SOC procesų schema
Fig. 3.12. General diagram of SOC processes

Kaip jau buvo minėta, nėra vienos visiems tinkamos SOC struktūros. Bet, atsižvelgiant į funkcionalumą ir vykstančius procesus, techniškai SOC struktūrą galima suskirstyti į tris pagrindinius blokus, kuriuose vyks visi pagrindiniai procesai. Todėl veiksmų įgyvendinimas SOC sistemoje gali būti reprezentuojamas naudojant modernią įrangą ir technologijas (3.13 pav.).



3.13 pav. SOC veikimo eiga (sudaryta remiantis FortiNet duomenimis)
Fig. 3.13. Deception Workflow (based on FortiNet)

1. Pirmasis blokas valdo, analizuoja ir filtruoja išorinius ryšius, sukuria aktyvius spąstus ir netikrus resursus, imituoja nuolatinį tikrų vartotojų, programinės ir techninės įrangos darbą (Jena, 2023). Įsilaužėliai sėkmingai juos atakuoja, pasiekdami tariamus puolimo rezultatus, tai suteikia SOC komandai laiko atsakyti, taip pat kontroliuoja, draudžia.
2. Antrasis blokas – šis blokas susideda iš trijų sistemų: SIEM (angl. *Security information and event management*), SOAR (angl. *Security Orchestration, Autonation and Response*) ir analizatoriaus (angl. *Analyser*), kurios automatizuoja incidentų aptikimo ir apdorojimo užduotis renkant, koreliuojant ir analizuojant įvykius bei informacijos saugos įrankius, analizuoja srautą, padidina reagavimo į incidentus greitį ir koduoja duomenis arba leidžia prieigą iš vidinio tinklo, be to, šios sistemos gali atlikti papildomas užduotis: IT infrastruktūros inventorizaciją ir kontrolę, pažeidžiamumo valdymą, pažeidžiamumo prioritetų nustatymą pagal informacinio turto kritiškumo lygius, automatinį atsakingų asmenų paskyrimą ir pašalinimo terminus.
3. Trečiasis blokas yra tinklo srauto stebėjimas, apskaita, kontrolė ir vartotojų prieigos iš tinklo prie išorinių išteklių kontrolės, gilaus paketų tikrinimo palaikymas, tikrinant, ar vartotojai priklauso esamam ryšiui, kenkėjiškų programų ir atakų aptikimas, failų ir programų valdymas, el. laiškų filtravimas ir apsauga nuo šlamšto, įsibrovimų prevencija, apkrovos balansavimas, perkrovimas ir kt.

Kuriant SOC procesus dažniausiai pasitaikančių klaidų išvengimo strategijos:

- Į kūrimo procesą įtraukti visus susijusius padalinius.
- Nustatyti specialistų atsakomybės sritis ir patogiausius bendravimo kanalus.
- Atlikti pirminius bandymus remiantis rezultatais.
- Organizuoti ir įgyvendinti mokymus visiems, kurie bus įtraukti į procesų įgyvendinimą, atlikti realių atvejų analizę.
- Sukurti rodiklių rinkinį, kad būtų galima įvertinti teisingą proceso veikimą.

Saugumo specialistų darbas priklauso nuo organizacijos, jos tikslų ir poreikių. Todėl saugumo operacijų centre turi dirbti kvalifikuoti ir atestuoti darbuotojai. Kadangi problemos ir grėsmės nuolat kinta, reikalingi žmonės, kurie mokosi, lengvai prisitaiko ir gali mąstyti nestandartiškai, kai reikia greitai priimti sprendimus. Geriausias variantas įtraukti esamus IT specialistus, kurie gali spręsti šias užduotis:

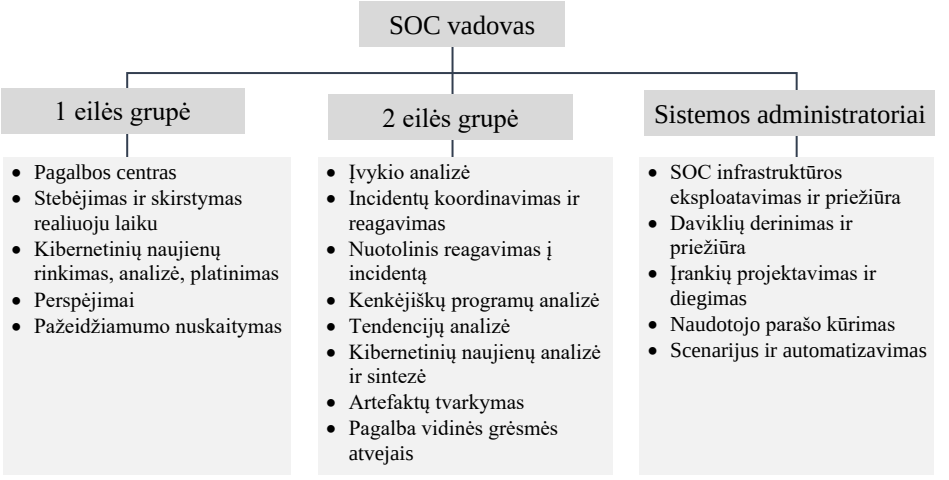
- informacijos saugumo įvykių stebėjimas;
- įtariamų informacijos saugumo incidentų registravimas ir kvalifikavimas;

- reikiamų duomenų rinkimas įtariamam informacijos saugumo incidentui analizuoti;
- įtariamų incidentų analizė, siekiant juos nustatyti;
- reagavimo koordinavimas į informacijos saugumo incidentus;
- SOC techninės įrangos administravimas;
- SOC infrastruktūros plėtra.

Pagrindinę komandą reikėtų suformuoti kuo anksčiau, kad ji dalyvautų diegiant sistemas ir derinimo procesus. Geras pagrindas SOC darbuotojams – IT sistemų ir tinklo infrastruktūros administravimo, informacijos saugumo diegimo ir administravimo patirtis bei sistemų testavimo įgūdžiai. Darbuotojai turi turėti ne tik darbo įgūdžius, bet ir atitinkamus pažymėjimus:

- Kibernetinės saugos vadovas (1-CISO CISSP, CISSM).
- SOC – vadovas (1-SoC viršininkas / grupės vadovas CISSP, ISACA IT rizika, GIAC).
- 3 lygis Grėsmių paieška (CEH, penkiasdešimtas, reversinė inžinerija).
- 3 lygis 2 Incidentų valdymas (CEH, GIAC: GCFA / GCIH).
- 6 lygis 1 Analitikas (GIAC: GSEC / GCIH /GCFE).

Išskyrus IT ir informacijos saugumo sistemų informacinius pranešimus, SOC turi greitai apdoroti vartotojų užklausas ir skambučius, pranešimus iš įvairių įmonės padalinių, informaciją iš išorinių šaltinių ir kt. 3.14 pav. pateiktas SOC vaidmenų pasiskirstymo pavyzdys.



3.14 pav. SOC vaidmenų pasiskirstymo pavyzdys
(sudaryta remiantis Zimmerman (2014)
Fig. 3.14. SOC role model example (Small SOC) **(**based on Zimmerman, 2014**)**

Norint apdoroti gaunamą informaciją, rekomenduojama sukurti pirmosios eilės grupę. Pirmosios eilės specialistai neatlieka išsamios incidentų analizės, jų pagrindinė užduotis – greitai apdoroti gaunamą informaciją, peržiūrint IDS ar SIEM įrankius. Visi incidentai, kurių kritiškumo lygis aukštas, yra eskaluojami. Todėl vėlavimas tarp pirmosios eilės duomenų gavimo ir eskalavimo neturėtų viršyti griežtai nustatyto laiko, pavyzdžiui, 20 minučių.

Antros eilės specialistai gali tirti incidentą nuo vienos minutės iki savaitės, rinkdami išsamius duomenis, pasikviesdami ekspertus, atkurdami veiksmų seką ir pateikdami rekomendacijas dėl incidento padarinių likvidavimo, įgyvendindami atsakomąsias priemones ir didindami informuotumą. Todėl incidentus tiriantys specialistai turi turėti daugiau žinių ir įgūdžių.

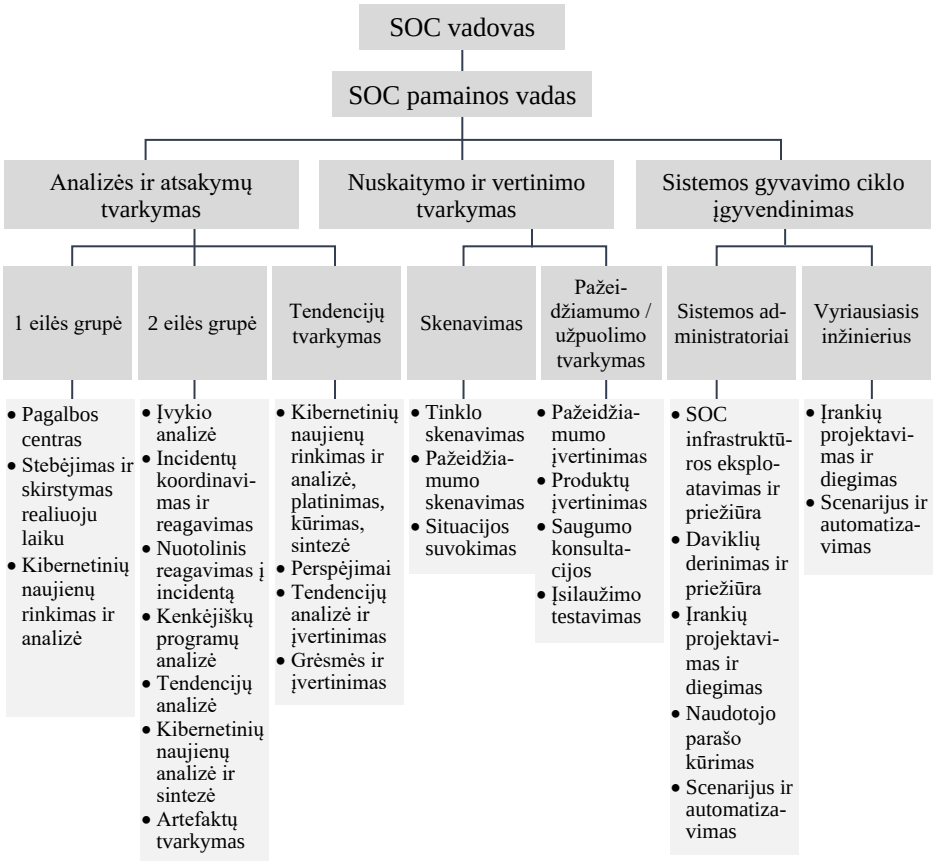
SOC viduje rekomenduojama atlikti laikiną darbuotojų rotaciją: antrosios eilės specialistai turėtų dirbti dalį laiko pirmoje eilėje, o pirmosios eilės specialistai turėtų dalyvauti tiriant kai kuriuos incidentus. Šiomis priemonėmis siekiama gerinti SOC darbo kokybę, kelti darbuotojų profesinį lygį ir didinti jų motyvaciją. Vykdydami šias rotacijas ar kitu laiku antros eilės specialistai (arba atskira ekspertų komanda) turėtų patobulinti pirmosios eilės specialistų naudojamus incidentų analizės ir eskalavimo rodiklius, taip pat analizuoti netipines ir anomalias veiklas.

Sistemos administratorius prižiūri SOC sistemą, dalyvauja kuriant ir diegiant naujas infrastruktūros funkcijas, konfigūruoja ir prižiūri jutiklius, kuria individualius parašus, scenarijus ir yra atsakingas už automatizavimą.

Kalbant apie didelę organizaciją, kuri turi kritinę infrastruktūrą, galima naudoti išplėstą funkcijų rinkinį ir visiškai atskirti vaidmenis bei atsakomybes. Galimas SOC vaidmenų pasiskirstymas pavaizduotas 3.15 pav.

Kaip ir mažoje SOC sistemoje, taip ir didelėje svarbu užtikrinti efektyvų kryžminį mokymą. Inžinieriai turi žinoti pagrindines darbo grupės problemas, taip pat mokėti greitai panaudoti 90 procentų sprendimų. Be to, jei valdymas susideda iš kelių lygių, vienos eilės operatoriai turėtų laisvai dirbti su bet kuria kita SOC dalimi.

Svarbus klausimas, dažnai sukeliantis daug ginčų, yra SOC sistemos darbo režimas. Idealus variantas – dirbti 24/7/365 visu pajėgumu, nes daugelis išpuolių, ypač tikslinių, vyksta naktį. Tai lemia tai, kad dirbant 8/5 režimu visavertė reakcija bus tik kitos darbo dienos pietų metu, kai analitikai išanalizuos nakties (ar savaitgalio) duomenis ir išspręs situacijas. Todėl personalas turi dirbti 3 pamainomis po 24 val. Priklausomai nuo SOC sistemos, darbuotojų skaičius gali būti skirtingas. Jeigu tai ne valstybės įmonė, tai pamainoje gali būti ne mažiau kaip 3 žmonės: 2 darbuotojai ir 1 vadovas. Jeigu valstybės įmonė, tada nuo 12 iki 15 žmonių (Pleta, 2023).



3.15 pav. SOC vaidmenų pasiskirstymo pavyzdys
(sudaryta remiantis Zimmerman 2014)
Fig. 3.15. Large SOC role model example (based on Zimmerman, 2014)

Reikalavimai personalui. Kibernetinio saugumo valdymo modelio strateginio valdymo plano įgyvendinimas neįmanomas be komandos, nes techninės priemonės yra tik įrankis, kurį valdytų kvalifikuotas personalas (Pleta, 2023). Kai strateginio valdymo planui įgyvendinti reikia samdyti darbuotojus, verta vadovautis principu „kokybė, o ne kiekybė“. Nes šiuo atveju pagrindinis uždavinys – užtikrinti, kad pagrindines pareigas užimtų aukšto lygio specialistai.

Stipri komanda yra labai svarbi bet kokios strategijos įgyvendinimui, nes darbuotojai tiria daugumą saugumo incidentų ir į juos reaguoja. Tikimasi, kad tokie darbuotojai visada teiks patikimas paslaugas, dažnai patiriant didelį spaudimą ir

apribojimus. Tokių komandų nariams reikia įvairių techninių ir netechninių įgūdžių, kad galėtų efektyviai dirbti. Todėl, siekiant nustatyti ir išnaudoti esamas galimybes sumažinti išlaidas ir išvengti pertekliaus, reikia atlikti išsamų patikrinimą.

Esamų darbuotojų reikalingų žinių spragų nustatymas turėtų būti kitas komandos formavimo žingsnis. Kiekvienam komandos nariui būtina suformuoti mokymo programą, pagrįstą žinių vertinimo rezultatais, o vėliau skirti lėšų mokymams (3.11 lentelė).

3.11 lentelė. Mokomosios programos pavyzdžiai
Table 3.11 Examples of curriculum

Komandos narys	Esami įgūdžiai	Reikalingi įgūdžiai
1	2	3
Tinklo palaikymo komandos narys 1	Ugniasienės administravimas Ugniasienės žurnalo analizė VPN (angl. *Virtual private network*) ir prieigos kontrolė Maršruto parinktuvų ir komutatorių veikimo supratimas TCP/IP suvokimas	Incident triage – Yr1 TCP/IP packet analysis (GCIA) – Yr2 Basic ethical hacking skills – Yr2 CISSP contents – Yr1 SIEM training – Yr1
Tinklo palaikymo komandos narys 2	IDS (angl. *Instrusion detection system*) administravimas IDS konfigūravimas ir derinimas TCP/IP (angl. *Transmission control protocol/internet protocol*) paketų analizė TCP/IP suvokimas	Incident Handling (GCIH) – Yr2 OS security concepts – Yr1 SIEM training – Yr1 Malware Analysis (GIAC Certified Reverse Engineering Malware – GREM) – Yr2
Operacinės sistemos palaikymo komandos narys 1	*Win Server* OS administravimas Antivirusinė programa, *Proxy & mail* šliuzas	SIEM training – Yr1 GCIH training – Yr 2 CISSP contents – Yr1 Incident triage – Yr1
Operacinės sistemos palaikymo komandos narys 2	*Linux Server* OS ir pašto serverio administravimas	TCP/IP packet analysis – Yr1 CISSP contents – Yr1 Incident triage – Yr1 Network security concepts – Yr1
SCADA palaikymo komandos narys 1	Įgūdžių rinkinys 1 Įgūdžių rinkinys 2 Įgūdžių rinkinys 3	Įgūdžių rinkinys 1 Įgūdžių rinkinys 2 Įgūdžių rinkinys 3

3.11 lentelės pabaiga

1	2	3
SCADA palaikymo komandos narys 2	Įgūdžių rinkinys 1 Įgūdžių rinkinys 2	Įgūdžių rinkinys 1 Įgūdžių rinkinys 2

Nors komandoje gali būti darbuotojų, galinčių atlikti kai kurias pareigas, vis tiek būtina investuoti į išorės talentus, siekiant sukurti geriausią komandą, susidedančią iš darbuotojų, reikalingų strategijai įgyvendinti, pvz.:

- *Vadovas*: vadovauja komandai ir atsiskaito vyriausiajam informacijos apsaugos pareigūnui.
- *Saugumo analitikas*: realiuoju laiku atlieka rizikos valdymą ir saugumo analizę.
- *SIEM inžinierius*: prižiūri SIEM (angl. *Security information and event management*) administravimą, atsaką į incidentus ir tiekėjų valdymą.
- *Tyrėjas*: analizuoja įvykių duomenis, įrodymus ir elgesį.
- *Reagavimo į incidentus specialistas*: atlieka pirminius tyrimus ir grėsmių vertinimus, naudodamas reagavimo į incidentus planus.
- *Auditorius*: užtikrina, kad procedūros atitiktų vyriausybės reglamentus ir pramonės standartus.

Surinkus komandą, būtina organizuoti ir pravesti mokymus, kurie apima ne tik techninius aspektus, bet ir procedūras, supažindinant su pareigomis, taisyklėmis ir metodais. Mokymai leis greitai orientuotis tarp sudėtingų produktų, tokių kaip SIEM ar saugos skaitytuvai. Informacijos apie naujas grėsmes ir saugumo tendencijas rinkimas ir platinimas komandoje turėtų būti nusistovėjęs tęstinis procesas, o ne vienkartinis įvykis. Keitimasis patirtimi ir žiniomis komandoje, taip pat ir vidinės rotacijos metu, yra svarbi mokymo dalis.

Remiantis darbuotojų žiniomis ir kvalifikacija, būtina nustatyti techninius reikalavimus įrangai, kuri bus naudojama strategijai įgyvendinti. Kai kurie įrankiai gali būti paprasti, pavyzdžiui, antivirusinė, ugniasienė ir įsibrovimo aptikimo sistema. Kiti yra sudėtingesni, pavyzdžiui, duomenų pažeidimų prevencija, programų saugos testavimas, duomenų bazės veiklos stebėjimas arba automatiniai pažeidžiamumo vertinimo įrankiai.

Kaip jau minėta, sistemoje gali būti naudojamos tiek pagrindinės, tiek pažangios saugumo technologijos. Tačiau kai kurie elementai išlieka nepakitę ir būtini, pavyzdžiui, žurnalų naudojimas, kurie turi būti centralizuoti ir perduoti visą reikiamą informaciją. 3.12 lentelėje pateiktas saugos technologijų valdymo priemonių pavyzdys, suskirstytas į tris kategorijas.

3.12 lentelė. Saugos technologijos valdymo priemonių kategorijos, sudaryta remiantis Srinivas (2014)
Table 3.12. Security technology control categories (based on Srinivas, 2014)

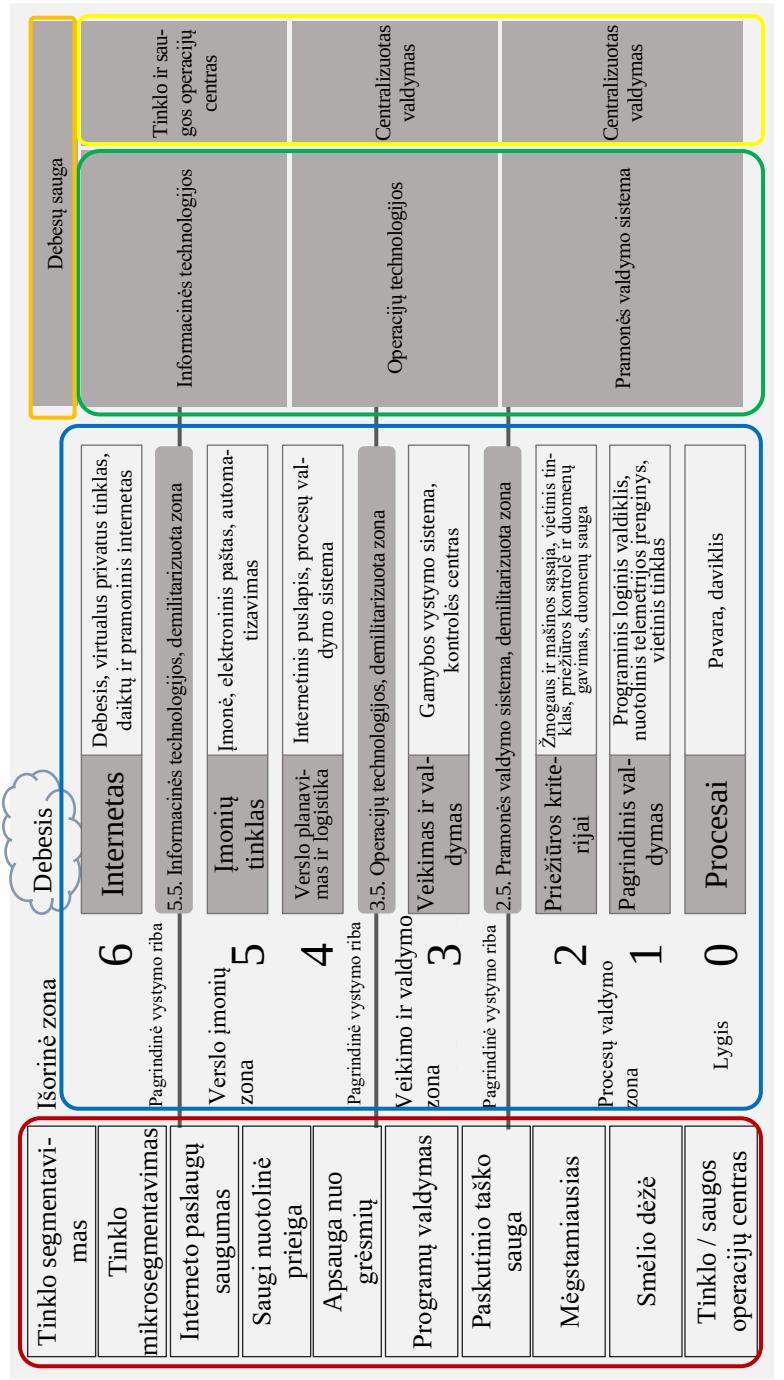
Lygis	Aprašymas
Pagrindinis lygis	*Endpoint Antivirus, Gateway Antivirus,* ugniasienė, įsibrovimų aptikimas, įsibrovimų į įmonės tinklus testai, stiprūs autentifikavimo valdikliai, sisteminių žurnalų serveriai
Pažangus lygis	Automatizuoti pažeidžiamumo skaitytuvai, duomenų bazių saugos stebėjimo valdikliai, įsibrovimo prevencijos sistemos, duomenų nutekėjimo prevencijos sistemos, duomenų diodai tarp SCADA ir įmonės tinklo, SIEM.
Specialus lygis	Žiniatinklio programų ugniasienės, failų vientisumo tikrinimo įrankiai, grėsmių duomenų tiekimas į SIEM, pažangi ekspertizė, leistinų programų įtraukimas į baltąjį sąrašą.
Geriausia prieinama praktika	Saugumo programinėje įrangoje gyvavimo ciklas (angl. *System development life cycle*, trumpai SDLC), įmonės saugos architektūra, informacijos mainų forumai, patikima kompiuterija.

Biudžetas. Saugumo kontrolės ir atsakomųjų priemonių įgyvendinimo sąnaudos turi įtakos saugumui ir reagavimui į kibernetines atakas. Dėl ribotų sistemų diegimo ir reagavimo į incidentus kaštų atsiranda sudėtingų arba neišsamių metodų. Reikėtų įvertinti saugumo politikos įgyvendinimo išlaidas, atsižvelgiant į infrastruktūros sistemų saugumą ir žalos bei remonto išlaidas.

4. Strateginio valdymo plano įgyvendinimas

Apibrėžus žmonių vaidmenį ir procesų, kuriuos atlieka SOC sistema, vaidmenis, būtina apibūdinti technologijas, naudojamas strateginio valdymo planui įgyvendinti. SOC sistemoje dauguma procesų turi būti automatizuoti, todėl SOC sistemoje naudojami įrankiai, leidžiantys tai atlikti. Kai kurie įrankiai gali būti standartiniai, pavyzdžiui, antivirusinė programa, ugniasienė ir įsilaužėlių aptikimo sistema. Kiti gali būti pažangesni, pavyzdžiui, duomenų nutekėjimo prevencijos priemonės, taikomųjų programų saugumo testavimas, duomenų bazės veiklos stebėjimas arba automatiniai pažeidžiamumo vertinimo įrankiai (Lacey, 2013).

Informacinių technologijų rinkos siūlo daugybę įvairių įrankių ir paruoštų sistemų, kurios gali padėti organizuoti SOC fiziniu lygmeniu. Viskas priklauso nuo sistemos dydžio ir investuoto biudžeto. Belieka tik suprasti technologiją ir nustatyti pagrindinius elementus, būtinus SOC sistemos funkcionavimui. 3.16 pav. pavaizduota SOC sistemos loginė schema (Zimmerman, 2014).



3.16 pav. SOC loginė schema (sudaryta remantis Zimmerman (2014)
Fig. 3.16. Modern SOC logical chart (based on Zimmerman, 2014)

SOC sistema suskirstyta į zonas, o zonos į lygius. Kiekviena demilitarizuota zona (angl. *Demilitarised zone* (DMZ)) yra padalinta į tinklo segmentus, apimančius viešąsias paslaugas ir atskiriančius jas nuo privačių. Tai suteikia papildomą vietinio tinklo saugumo lygį, kad atakos atveju būtų sumažinta žala. 3.16 pav. matyti, kokias technologijas ir priemones galima naudoti kiekvienoje zonoje. Pavyzdžiui, procesų valdymo zonose gali būti naudojami šie įrankiai: *Secure Switch,* VPN, EDR, *Fabric* API, *Application Controls*, *Threat Protection*, *Transparent* NGFW. Kiekvienas elementas fiziškai (angl. *Secure Switch*) arba programiškai (angl. *Threat Protection, Application Control, Fabric API*) aptinka grėsmes, užtikrina saugumą, pašalina saugumo spragas, užtikrinant efektyvesnį veikimą (Pleta, 2023).

Kritinės infrastruktūros objektai yra infrastruktūros, teikiančios paslaugas, sistemos ir posistemės, kurios yra būtinos ir yra gyvybiškai svarbios visuomenės funkcionavimui, sveikatai, fizinei apsaugai, piliečių saugumui, ekonominei ir socialinei gerovei. Kritinės infrastruktūros tiek fiziniu, tiek skaitmeniniu lygmeniu yra tarpusavyje sujungtos sudėtingais mechanizmais, kurie priklauso vienas nuo kito. Viena vertus, tai yra privalumas, kita vertus – trūkumas. Privalumas yra tas, kad visos operacijos yra automatizuotos ir viena sistema atpažįsta kitas. Tačiau problema ta, kad kibernetinės atakos atveju bet kuri visos sistemos dalis gali sukelti grandininę reakciją kitose tarpusavyje susijusiose pramonės šakose (Cyber attacks on critical infrastructure, 2016).

3.13 lentelė. Pagrindinės technologijos, naudojamos kuriant SOC sistemą (sudaryta autoriaus)
Table 3.13. Basic technologies are used to create a SOC system (compiled by the author)

Technologija	Aprašymas
1	2
Tinklo segmentavimas	yra viena iš efektyviausių architektūrinių koncepcijų, užtikrinančių OT aplinką. Idėja yra tokia, kad padalinti tinklą į kelis funkcinius segmentus arba „zonas“ (kuriose gali būti mikrosegmentai) ir padaryti kiekvieną zoną prieinamą tik įgaliotiems įrenginiams, programoms ir vartotojams. Ugniasienė apibrėžia ir užtikrina zonas bei kanalus, leidžiančius jautriems duomenims ir programoms perduoti iš vienos zonos į kitą. Architektūrinis zonų ir kanalų modelis žymiai sumažina įsilaužimo riziką. Vartotojai arba įrenginiai, kuriems leidžiama atlikti tam tikrus veiksmus tam tikroje zonoje, gali normaliai veikti tik toje zonoje (*Fortinet, The Security Approach to Protecting Converged IT and OT*).
Tinklo mikrosegmentavimas	tai smulkesnio lygmens pozonių kūrimo procesas, detaliai kontroliuojant atskirus arba logiškai sugrupuotus aktyvus. Toks suskirstymas aiškiai matomas SOC loginėje schemoje (3.22 pav.). Keturios zonos (procesų valdymo zona, operacijų ir valdymo zona, verslo ir įmonės zona

3.13 lentelės tęsinys

1	2
	bei išorinė zona) ir kiekviena zona suskirstyta į kelis lygmenis – pozonius (proceso, pagrindinės kontrolės, priežiūros kontrolės zona), kurie valdo tam tikrus procesus.
Interneto paslaugų saugumas	standartas, reikalingas saugiam ryšiui žiniatinklio tarnybose. Standartas aprašo tris pagrindines technologijas: autentifikavimą (kaip pritvirtinti saugos žetonus, kad būtų galima identifikuoti siuntėją), vientisumą (kaip pasirašyti SOAP pranešimus, siekiant užtikrinti vientisumą) ir konfidencialumą (kaip užšifruoti SOAP pranešimus, siekiant užtikrinti konfidencialumą).
Saugi nuotolinė prieiga	technologija, naudojama užtikrinti saugią nuotolinę prieigą prie sistemų ar programų. Pavyzdžiui, virtualus privatus tinklas, Endpoint Security, stipri slaptažodžių politika, kelių veiksnių autentifikavimas, saugumo ugdymas ir informavimas ir kt.
Apsauga nuo grėsmių	paslauga, aptinkanti ir tirianti atakas prieš tinklus ir padedanti efektyviai į jas reaguoti.
Programų valdymas	saugos technologija, kuri blokuoja arba riboja neleistinų programų vykdymą. Valdymo funkcijos priklauso nuo konkrečios programos tikslų, tačiau pagrindinis yra užtikrinti naudojamų ir tarp taikomųjų programų perduodamų duomenų konfidencialumą ir saugumą. Programos skirstomos į keturias grupes: saugios, pavojingos, labai apribotos ir šiek tiek ribojamos. Atsižvelgiant į tai, nustatomas įvestų apribojimų lygis. Kiekvienai programų grupei nustatomos taisyklės, kuriomis reguliuojama prieiga prie įvairių išteklių (failų, aplankų, registrų, tinklo adresų). Pavyzdžiui, jei programai reikia prieigos prie konkretaus ištekliaus, programų valdymo funkcija patikrina, ar ji turi tinkamas teises, ir atlieka operaciją pagal nurodytas taisykles. Programų paleidimai taip pat registruojami. Ši informacija naudojama tiriant incidentus ir atliekant įvairius patikrinimus. Funkcionalumas (galia ir patogumas naudoti) lemia, kaip efektyviai tinklo administratoriai gali įgyvendinti ir prižiūrėti įvairias saugos strategijas.
Galinio taško saugumas (*Endpoint Security*)	aptinka įvykius galutiniuose vartotojų ir serverių mazguose, taip pat gali būti naudojamas registruojant ir detaliai analizuojant, kas vyksta operacinės sistemos lygiu. Ši sistema gali būti SIEM sistemos įvykių šaltiniu.
Honeypot	įrankis, imituojantis kompiuterinę sistemą su programomis ir duomenimis, skirtas įvairių tipų grėsmėms aptikti. „Spąstų“ principas labai paprastas. Kibernetiniai nusikaltėliai tai priima kaip tiesą ir užpuola. Atakos metu gauti duomenys padeda suprasti užpuoliko strategiją, naudojamas priemones, taip prisidedant prie teisingo informacijos saugumo išteklių paskirstymo.

3.13 lentelės pabaiga

1	2
Smėlio dėžė (angl. *Sandbox*)	saugaus programų vykdymo mechanizmas naudojamas nepatvirtintam kodui iš nežinomų šaltinių paleisti ir virusams aptikti. Kodas paleidžiamas izoliuotoje stotyje, atidžiai prižiūrint. Tai aktualu, kai kenkėjiška programa sustoja savo veikimo pradžioje. Smėlio dėžė, naudodama elgsenos analizės technologijas, aptinka grėsmes failuose, kurie perduodami tinklu (el. pašto žinutės, failų atsisiuntimas iš interneto ir kt.). Šis mechanizmas padeda aptikti ir užkirsti kelią grėsmėms, kol jos neįsiskverbia į konkretų pagrindinį kompiuterį.
NOC/SOC	integruotas valdymo ir analizės sprendimas, turintis tinklo valdymo centro (angl. *Network Operational Centre,* trumpai NOC) ir saugos valdymo centro (angl. *Security Operation Centre*, SOC) funkcijas. Šis įrankis automatizuoja IT procesus ir atsaką į grėsmes, įvertina išmatuojamus saugos rodiklius, stebi SIEM elementų ir operacijų būseną bei sujungia *Analyser* ir SIEM galimybes.

Pažeidžiamumų nustatymas, saugumo politikos įgyvendinimas, mokymas, sistemų atnaujinimas ir netgi būtinų sistemų, kurios neatitinka dabartinių saugumo ir veiklos poreikių, pašalinimas yra svertas, padedantis užkirsti kelią kibernetiniams pavojams ateityje. Tikslus kibernetinio saugumo politikos taikymas kartu su tinkamu darbuotojų mokymu, teisinga tinklo ir įrenginių konfigūracija bei fizine sauga leis išvengti rizikos arba ją žymiai sumažinti iki toleruotino lygio.

5. Strateginio valdymo plano įgyvendinimo vertinimas ir kontrolė

Saugumo metodų valdymas ir įgyvendinimas kritinėse infrastruktūrose – tai verslo procesas, kurio tikslas – nustatyti saugumo spragas, įvertinti jų riziką ir priimti atitinkamus sprendimus. Veiksmai turi būti koordinuojami, o rezultatai iš naujo įvertinti, siekiant patikrinti jų veiksmingumą. Šis procesas turi būti vykdomas reguliariai, nes informacijos saugumo, tikslumo ir saugumo kontrolės priemonių reikalavimai nuolat didėja. Todėl būtina atlikti šiuos paruošiamuosius veiksmus:

1. Infrastruktūros ir valdymo personalo saugumo patikrinimas.
2. Sistemų tyrimo dydžio ir lygio nustatymas.
3. Saugumo spragų nustatymas ir rizikos vertinimo priemonės naudojimas.
4. Rezultatų ir saugos reikalavimų įvertinimas.
5. Saugumo spragų, kurios buvo nustatytos ir ištaisytos įgyvendinant saugumo politiką, tikrinimas.

Kiekvienai kritinei infrastruktūrai su įmonės tinklu ir susijusiu turtu reikalingas IT rizikos valdymas. Norint apdoroti didėjančius saugos duomenis, reikalingas SOC, kuris padidina saugumą nuolat tikrindamas, ar tinkle nėra pažeidžiamumų, ir šalindamas juos, kol pažeidimai netampa kritinėmis problemomis

ar incidentais. Taigi, SOC orientuojasi į kasdienį veiklos saugumą ir nėra susijęs su saugumo strategijų ar architektūros kūrimu. Be to, galima teigti, kad SOC yra saugumo veiklos koordinavimo ir pagrindinės informacijos bei politikos platinimo priemonė, kuri turi papildomų privalumų:

1. Išlaidų mažinimas – viena saugos komanda padeda sumažinti darbo įsipareigojimų dubliavimą.
2. Centralizuota veikla – sujungia IT saugos funkcijas įvairiose darbo grupėse ir vietose į vieną komandą, kad būtų pagerintas bendradarbiavimas, dalijamasi žiniomis ir patirtimi, siekiant optimizuoti rezultatus.

Aprašytas patobulintas kibernetinio saugumo valdymo modelis ir pateiktas techninis sprendimas buvo aprobuotas NATO projekte, kurio tikslas – pateikti išplėstinį kritinių infrastruktūrų kibernetinio / fizinio saugumo standartų, jų koreliacijų vertinimą bei analizę. Analizė parodė, kad SOC pagerina kibernetinio saugumo valdymą kritinėje energetinėje infrastruktūroje ir suteikia galimybę stebėti incidentus realiuoju laiku bei laiku į juos reaguoti, – priimant savalaikius sprendimus.

3.4. Trečiojo skyriaus išvados

1. Teorinį valstybės kritinės energetinės infrastruktūros kibernetinio saugumo valdymo modelį, papildytą komponentu – strateginiu valdymu – įvertino ekspertų grupė, dirbanti kibernetinio saugumo valdymo srityje ne trumpiau kaip 3 metus. Apskaičiuoti ekspertų nuomonių suderinamumo ir kompetentingumo koeficientai. Gauti rezultatai parodė, kad ekspertai, kurie dalyvavo apklausoje, yra kompetentingi kibernetinio saugumo srityje. Anoniminės apklausos metu ekspertai įvertino komponentus balais nuo 1 iki 5, kur 1 balas yra aukščiausias, pateikė savo nuomonę kiekvienam klausimui, kurie buvo pateikti anketoje. Paprastuoju adityvaus svorių metodu (SAW) buvo apskaičiuoti komponentų įverčiai ir nustatytas komponentų svarbumas valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelyje.
2. Apskaičiuojant gautus ekspertų įverčius, empirinio tyrimo rezultatai parodė, kad valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio komponentai pagal galutinį rangą paskirstomi taip (nuo aukščiausio iki žemiausio): organizacijos valdymas (5), teisinis reguliavimas (4), kibernetinio saugumo kultūra (3), technologinis kibernetinis saugumas (3), rizikos valdymas (3), kibernetinių incidentų valdymas (2) ir strateginis valdymas (1). O tai reiškia, kad būtina gerinti ir plėtoti valstybių kritinės infrastruktūros kibernetinio saugumo modelį, pradedant nuo strateginio valdymo.

3. Paprastasis adityvus svorių metodas (SAW) leidžia sujungti visų komponentų įverčius į vieną bendrą dydį, pagal kurį galima nustatyti kiekvieno valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio komponento svarbą. Bendri komponentų įverčiai nelabai skiriasi, išskyrus strateginį valdymą (0,11442). Darant išvadą pagal gautus rezultatus, galima konstatuoti, kad kiekvienas komponentas yra svarbus ir reikalingas. Strateginis valdymas yra naujas komponentas ir dar plačiai netaikomas kibernetinio saugumo srityje. Tačiau ekspertai beveik vienareikšmiškai nurodė, kad strateginis valdymas reikalingas tam, kad būtų teisingai organizuotas saugumo procesas. Toks šio strateginio valdymo komponento įvertinimas tik parodė plėtros šia kryptimi poreikį.
4. Pateikiamos patobulinto kibernetinio saugumo valdymo modelio praktinio taikymo rekomendacijos, apibūdinančios šio modelio naudojimą projektuojant saugumo sistemą ir saugumo operacijų centrą (SOC). Pateikta veiksmų seka ir loginė SOC sistemos schema. Aprašyta struktūra ir pagrindiniai komponentai.

Bendrosios išvados

1. Išstudijavus aktualius dokumentus ir literatūros šaltinius, išanalizavus energetikos sektoriaus kibernetinį saugumą, kritinės energetinės infrastruktūros valdymą ir identifikavus jo problemas, buvo nustatyta, kad:

1.1 nėra bendros kritinės infrastruktūros sampratos, tačiau yra bendra koncepcija, pagrįsta kibernetinės aplinkos apsauga nuo atakų ir konfidencialumo, vientisumo ir prieinamumo užtikrinimu;

1.2 valstybių požiūris į kritinę infrastruktūrą yra skirtingas, tačiau visur kaip ypatingos svarbos infrastruktūros komponentas yra energetikos sritis, kurios pažeidimas ar sunaikinimas turi rimtą poveikį bet kurios šalies saugumui;

1.3 dabartiniai kibernetinio saugumo valdymo modeliai neužtikrina tinkamos apsaugos. Daugeliui šalių trūksta strategijų, kaip reaguoti į kibernetines atakas ir netikėtus scenarijus, o daugelis jų neįvertina savo pažeidžiamumo;

1.4 kritinės energetinės infrastruktūros kibernetiniam saugumui įtakos turintiems veiksniams reikia skirti daugiau dėmesio įvairiais lygmenimis, nes vienos sistemos dalies gedimo pasekmės gali būti pavojingos žmonių gyvybei, aplinkai ir verslui.

2. Ištyrus ir įvertinus penkių šalių (Jungtinės Karalystės, Jungtinių Amerikos Valstijų, Prancūzijos, Estijos ir Lietuvos) kritinės energetinės infrastruktūros silpnąsias vietas bei taikomas gerąsias praktikas, nustatyta, kad kritinės energetinės infrastruktūros saugumo lygis yra nepakankamas (Tvaronavičienė et al., 2020).

Taip pat pagrįstos kibernetinio saugumo modelio panaudojimo galimybės siekiant veiksmingai užtikrinti kritinės energetinės infrastruktūros kibernetinį saugumą, atsižvelgiant į hierarchinį kritinės infrastruktūros klasifikavimo metodą, naudojant tarptautinius kriterijus, taip pat atsižvelgiant į planavimą, nes neaišku, ką tiksliai reikia apsaugoti kritinės infrastruktūros objektuose.

3. Įvertinus penkių šalių (Jungtinės Karalystės, Jungtinių Amerikos Valstijų, Prancūzijos, Estijos ir Lietuvos) kritinės energetinės infrastruktūros silpnąsias vietas bei taikomas gerąsias praktikas, galima konstatuoti, kad kritinės infrastruktūros saugumo lygis yra nepakankamas. Šešių komponentų kibernetinio saugumo modelis yra tinkamas kibernetiniam saugumui vertinti, tačiau jį galima patobulinti atsižvelgiant į hierarchinį kritinės infrastruktūros klasifikavimo metodą pagal tarptautinius kriterijus, pagal kuriuos atsižvelgiama į šalies plėtrai ir planavimui būtinus elementus. Analizė taip pat patvirtino technologijų valdymo trūkumus.

4. Sukurtas naujas kibernetinio saugumo valdymo modelis, susidedantis iš septynių lygiaverčių komponentų (organizacijos valdymas, teisinis reguliavimas, kibernetinio saugumo kultūra, technologinis kibernetinis saugumas, rizikos valdymas, kibernetinių incidentų valdymas ir strateginis valdymas), kurie visi kartu padės užtikrinti efektyvų kibernetinio saugumo valdymą.

5. Atlikus empirinį tyrimą ir įvertinus kibernetinio saugumo srities ekspertų apklausos rezultatus, tikslinga nustatyti valstybių kritinės energetinės infrastruktūros kibernetinio saugumo modelio komponentų reikšmingumą, naudojant paprastąjį adityvų svorių metodą (SAW), siekiant nustatyti, kurį komponentą reikia vystyti pirmiausia.

6. Empirinio tyrimo rezultatai rodo, kad kiekvienas modelio komponentas yra būtinas ir svarbus siekiant tinkamai organizuoti saugos procesą ir taip pat pagrindžia strateginio valdymo komponento panaudojimą kibernetinio saugumo modelyje ir tolesnį jo vystymą bei taikymą.

7. Valstybės kritinės energetinės infrastruktūros kibernetinio saugumo modelio efektyvumui gerinti reikalingas specialus saugumo operacijų centras (SOC), kuris integruoja visus modelio komponentus ir gali itin pagerinti kibernetinio saugumo valdymo efektyvumą kritinėje energetinėje infrastruktūroje valstybės mastu. Todėl pateikiamos rekomendacijos sukurto kibernetinio saugumo valdymo modelio praktiniam pritaikymui, veiksmų seka ir SOC sistemos veikimo loginė schema. Aprašyta struktūra ir pagrindiniai komponentai.

8. Sukurta kibernetinio saugumo valdymo priemonė (SOC) ir pasiūlyta kibernetinio saugumo problemų ir rizikų sprendimo metodika užtikrina efektyvų kibernetinio saugumo valdymą, sistemos vientisumą ir efektyvumą.

Literatūra ir šaltiniai

Abdullah, L. (2013). Fuzzy multi criteria decision making and its applications: A brief review of category. In *Procedia – Social and Behavioral Sciences*, *97*, 131–136. https://doi.org/10.1016/j.sbspro.2013.10.213

Accenture Security. (2019). *The Cost of Cybercrime. Ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection.* Traverse City, Michigan, Ponemon Institute LLC and jointly developed by Accenture. https://mma.prnewswire.com/media/882924/Accenture_Cybercrime_Costs_Canadian_Companies_more_than_US_9M_La.pdf?p=original

Ahmadian, M. M., Shajari, M., & Ali Shafiee, M. (2020). Industrial control system security taxonomic framework with application to a comprehensive incidents survey. *International Journal of Critical Infrastructure Protection*, *29*, 100356. https://doi.org/10.1016/j.ijcip.2020.100356

Ahola, M., Säteri, J., & Sariola, L. (2019). Revised Finnish classification of indoor climate 2018. *E3S Web Conferences. CLIMA 2019 Congress*, *111*. https://doi.org/10.1051/e3sconf/201911102017

Ahsan, M. Z., Khandkar, M. R., & Islam, M. S. (2001). Algorithm for Performance Appraisal using Cumulative Average Weighing Method. *BMJ*, *2*(1), 59–74. https://bsmrmu.edu.bd/public/files/econtents/63bd35fde8748bmj-02-01-05.pdf.

Ayral, T. (2016, July). Minimize industrial cyber security risk in plants in 12 steps. *Hydrocarbon Processing*. https://www.hydrocarbonprocessing.com/magazine/2016/july-

2016/process-control-and-instrumentation/minimize-industrial-cyber-security-risk-in-plants-in-12-steps

Alshathry. (2017, February). Cyber Attack on Saudi Aramco. *International Journal of Management of Information Technology, 11*(5), 3037. https://rajpub.com/index.php/ijmit/article/view/5613

Amin, S. M. (2010, March 29). *Securing the Electricity Grid*. National academy of engineering. https://www.nae.edu/18868/Securing-the-Electricity-Grid

Anatomy of a SCADA Malware, BlackEnergy 3 Attack on the Ukraine Grid. (2022). SCADA Hacking: https://www.hackers-arise.com/post/2018/10/10/scada-hacking-anatomy-of-a-scada-malware-blackenergy-3

ANSI/ISA-62443-1-1 (99.01.01)-2007. *Security for Industrial Automation and Control Systems. Quick Start Guide: An Overview of ISA/IEC 62443 Standards. Security of Industrial Automation and Control Systems* (2020, June). Global CyberSecurity Alliance. https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

ANSSI. (2020). *The French CIIP Framework*. https://cyber.gouv.fr/en/french-ciip-framework

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue, 41*(5), 491–514. https://doi.org/10.1177/0967010610382687

Augustinaitis, A., Dagytė, I., Petrauskas, R., & Rudzkienė, V. (2009). *Lietuvos e. valdžios gairės: ateities įžvalgių tyrimas.* Mykolo Romerio universiteto leidybos centras. https://cris.mruni.eu/server/api/core/bitstreams/bc4f77f7-ec3d-49fa-8a04-c148146534f9/content

Barnes, K., Johnson, B., & Nickelson, R. (2004). *Introduction to SCADA protection and vulnerabilities.* https://doi.org/10.2172/911209

Beazner, M., & Patrice, R. (2017). Hotspot Analysis: Stuxnet. In *CSS Cyber Defense Hotspot Analysis*, *0*(4). Center for Security Studies (CSS), ETH Zurich. https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/s/t/u/x/stuxnet

Bivainis, J. (2011). *Vadyba studentams.* Technika.

Blume, S. W. (2007). *Electric Power System Basics: For the Nonelectrical Professional.* Wiley & Sons, INC. https://www.amazon.com/Electric-System-Nonelectrical-Professional-Engineering-ebook/dp/B01N1IUI9O

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi J. (2021). *NISTIR 8276. Key practices in cyber supply chain risk management: Observations from industry*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8276

Brock, W., & Hommes, C. (1997). A Rational Route to Randomness. *Econometrica, 65*(5), 1059–1096. https://doi.org/10.2307/2171879

Bulakh, A., Tuohy, E., & Pernik, P. (2016). Estonia's Developing Level Playing Field for Critical Energy Infrastructure Protectors – a Model for Broader Scale Platforms? *Energy Security: Operational Highlights, 10,* 4–9.

Burge, S. (2023). What is industrial control systems security? *ISJ International security journal*. https://internationalsecurityjournal.com/industrial-control-systems/

Butrimas, V. (2012). The Cybersecurity Dimension of Critical Energy Infrastructure. *perConcordiam*. https://www.marshallcenter.org/sites/default/files/files/2020-10/pC_V3N4_en_Butrimas_Bruzga_1.pdf

Butrimas, V. (2019). Gyvenimas pavojuje: besikeičiančių kibernetinių grėsmių aplinkoje. *Kibernetinio saugumo apžvalga*, 34–40. https://www.mii.lt/files/doc/lt/skelbimai/ks_apzvalga_8.pdf

Butrimas, V. (2017, May 30). *NCRA of Lithuania ESReDA 52*. NATO ENSEC CoE. https://www.esreda.org/wp-content/uploads/2017/06/Round-Table-Discussion-1-V.-Butrimas.pdf

Butrimas, V., & Bruzga, A. (2012). The Cyber Security Dimension of Critical Energy Infrastructure, *PerConcordiam*. *Journal of European Security and Defense Issues*. https://www.marshallcenter.org/sites/default/files/files/2020-10/pC_V3N4_en_Butrimas_Bruzga_1.pdf

CESG. (2016). *Common cyber attacks: reducing the impact*. London, CESG. https://www.ncsc.gov.uk/static-assets/documents/common_cyber_attacks_ncsc.pdf

Choraś, M., Kozik, R., Flizikowski, A., Hołubowicz, W., & Renk, R. (2016). *Managing the Complexity of Critical Infrastructures.* doi:10.1007/978-3-319-51043-9_7

Cyber attacks on critical infrastructure. Expert risk article. (2016). Allianz: https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html

Cyber Defence. (2020, March 17). NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

Cyber Incident Reporting For Critical Infrastructure Act (CIRCIA). (2022). Nuskaityta iš Cybersecurity and infrastructure security agency: https://www.cisa.gov/

Cybersecurity and Infrastructure Security Agency [CISA]. (2021, July 20). *ICS Alert*. C*yber-Attack Against Ukrainian Critical Infrastructure*. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA. (2020, December 17). *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience. Washington DC: Homeland Security*. Homeland Security. Cybersecurity & infrastructure secyrity agency. https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

Coole, M., Corkill, J., & Woodward, A. (2012). *Defence-in-depth, protection in depth and security in-depth: A comparative analysis towards a common usage language.* Edith Cowan University. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1023&context=asi

CRR Supplemental Resource Guide. (2022). CERT, OCTAVE. https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-SC.pdf

Fleisher, C. S., & Bensoussan, B. (2003). *Strategic and competitive analysis: Methods and techniques for analyzing business competition* (1st ed.). Prentice Hall.

Cohen, G. (2021). *Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire*. Industrial Cyber Security Pulse: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire/

Craig, A., & Valeriano, B. (2016). Reacting to Cyber Threats: Protection and Security in the Digital Age. *Global Security and Intelligence Studies, 1*(2). http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/reacting_to_cyber_threats_gsis_craig_and_valeriano.pdf

Crawford, M. (2006). *Utility hack led to security overhaul*. Computerworld Australia. https://www.computerwoche.de/a/utility-hack-led-to-security-overhaul,572421

Critical Infrastructure Warning Information Network. (2024). European Commission: http://ec.europa.eu/dgs/home-affairs/what-wedo/

Critical Infrastructure Threat Information Sharing Framework. A Reference Guide for the Critical Infrastructure Community. (2016). Homeland Security: https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

Critical Infrastructure Warning Information Network. (2015, March 2). https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin_en

Dalkey, N., & Helmer, O. (1962, July). *Memorandum RM-727/1-ABRIDGED. An experimental application of the Delphi method to the use of experts.* Santa Monica California: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2009/RM727.1.pdf

Das, R., & Gündüz, M. (2020). Analysis of cyber-attacks in IoT-based critical infrastructures. Computer Science, Engineering, Environmental Science. *Journal of Environmental Science, Computer Science and Engineering & Technology, 8*(4), 122–133.

Davenport, T. (1993, February 24). *Process Innovation: Reengineering Work Through Information Technology*. Harvard Business Press.

De Falco, M. (2012). *Stuxnet facts report: A technical and strategic analysis.* NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Tallinn, Estonia. https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Dehlawi, Z., & Abokhodair, N. (2013, June). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. *2013 Conference: Intelligence and Security Informatics (ISI), June 4-7, 2013, Seattle, Washington, USA.* https://doi.org/10.1109/ISI.2013.6578789

Egozcue, E. (2012). Annex II. Security aspects of the smart grid. Teoksessa D. H. Egozcue, *Smart Grid Security: Recommendations for Europe and Member States. European Network and Information Security Agency (ENISA).* https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

Electronic Sabatoge of Venezuela Oil Operations. (2002). Risidata: https://www.risidata.com/Database/Detail/electronic-sabatoge-of-venezuela-oil-operations

European Commission. (2012, November). *Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection* (November 2012). Brussels, EC. https://energy.ec.europa.eu/document/download/86c1c6fe-816c-41dd-a22d-541fdeaa6091_en?filename=20121114_tnceip_eupolic

Europos Parlamento ir Tarybos direktyva. (2016, gegužės 17 d.). *Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti Nr. 5581/1/16 REV 1. Briuselis*. http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/lt/pdf

Europos saugumo ir bendradarbiavimo organizacija (ESBO). (2014, sausio 29 d.). https://www.lrs.lt/sip/portal.show?p_r=38895&p_k=1

Falliere, N. (2011). *W32.Stuxnet Dossier. Cupertino, CA: Symantec Security Response*. https://css.csail.mit.edu/6.858/2014/readings/stuxnet.pdf

FireEye. (2016). *Cyber Attacks on the Ukrainian Grid: What you should know*. Milpitas, CA, FireEye. https://www.almendron.com/tribuna/wp-content/uploads/2020/12/fe-cyber-attacks-ukrainian-grid.pdf

Forcepoint. (2020, November 2). *The CIA triad defined*. https://www.forcepoint.com/it/cyber-edu/cia-triad

Garvin, D. (1993). *Building a Learning Organization. Beyond high philosophy and grand themes lie the gritty details of practice.* Harvard Way Boston, Harvard Business Publishing.

Glassner, B., & Moreno, J. D. (1989). *The Qualitative-Quantitative Distinction in the Social Sciences.* Springer Book Archive. https://doi.org/10.1007/978-94-017-3444-8

Governance – Estonia. (2023). Nuskaityta iš European Commission: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/governance-estonia

Government Accountability Office (GAO). (2007). *Critical Infrastructure Protection – Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*. Government Accountability Office (GAO). United States. http://www.gao.gov/assets/270/268137.pdf

Government of France. (2015). *French National Digital Security Strategy*. Paris, Government of France. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy

Government of the Republic of Lithuania. (2018). *National Cyber Incident Management Plan*.
https://www.ird.lt/media/force_download/?url=/uploads/structure/docs/42166_cf30b855d9ac94e388b0d52cbf96ae86.pdf

Government of the Republic of Lithuania. (2018). *Resolution on the approval of the National Cyber Security Strategy*. Government of the Republic of Lithuania. Vilnius.

Govindarasu, M., & Hahn, A. (2017). *Cybersecurity of the Power Grid: A Growing Challenge*. https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge

Grinius, L. (2016). Kibernetinio saugumo situacijos Lietuvoje apžvalga ir tendencijos. *Kibernetinio saugumo apžvalga*, 16–18. https://site2.cmm.lt/cms/images/kibernetinis_saugumas.pdf

Hahn, A. (2016). Operational Technology and Information Technology in Industrial Control Systems. In E. J. M. Colbert, & A. Kott (Eds.), *Cyber-security of SCADA and other Industrial Control Systems. Advances in Information Security*. Springer, Cham. https://doi.org/10.1007/978-3-319-32125-7_4

Hamel, G. (2002). *Leading the Revolution: How to Thrive in Turbulent Times by Making Innovation a Way of Life* . Plume.

Hatch, M. J., & Cunliffe, A. L. (2013). *Organization Theory Modern, Symbolic and Postmodern Perspectives* (3rd ed.). Oxford University Press.

HM Government. (2016). *National Cyber Security Strategy 2016–2021*. London, HM Government: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

HM Government. (2015). *National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

Howard, J. D., & Longstaff, T. A. (1998). *A Common Language for Computer Security Incidents. Sandia Report.* http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf

Hunger, J. D., & Wheelen, T. L. (2005). *Essentials of Strategic Management.* Pearson. Prentice Hall.

Schmidl, A. (2016). Cyber Risks Engineering Insurers Perspective. *IMIA Annual Conference, 2016 – Doha, Qatar. 98(16).* IMIA Working Group Paper. Retrieved from https://www.imia.com/wp-content/uploads/2023/07/Presentation-of-WGP-9816-Cyber-Risks-in-Engineering_Doha_final.pdf

Inductive Automation. (2020, February 28). *IIoT: Combining the Best of OT and IT. 95\14.* Industrial Ethernet Book. USA, IEB Media GdR. https://iebmedia.com/index.php?id=11673&parentid=63&themeid=255&hft=95&showdetail=true&bb=1

Information security. Guide for Conducting Risk Assessments. (2012). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Insider Threat Mitigation. (2022). Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

Trendmicro.com. (2023). *Your security needs. Covered*. https://www.com/en_gb/forHome.html

ISA/IEC-62443-1-1. (2009). *Industrial communication networks, Network and system security. Technical specification Part 1-1: Terminology, concepts and models IEC/IS-62443-1-1*. https://www.isa.org/standards-and-publications/isa-standards

ISACA. (2019). *COBIT 2019 Framework*: *Governance and Management Objectives*. https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19igio

Claroty. (2023, June 13). *IT vs OT Security: Key Differences in Cybersecurity.* The Claroty Team. https://claroty.com/blog/it-and-ot-cybersecurity-key-differences

ITU. (2019). *Global Cybersecurity Index (GCI) 2018*. Geneva, ITU. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Izycki, E., & Colli, R. (2019). Protection of critical infrastructure in national cyber security strategies. In *18th European Conference on Cyber Warfare and Security (ECCWS 2019) 4–5 July 2019, Coimbra, Portugal.* Conference. Academic Conferences Ltd.

Johnson, T. (2015). *Cybersecurity. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* CRC Press.

Joint Committee on the National Security Strategy. (2018). *Cyber Security Skills and the UK's Critical National Infrastructure: Second Report of Session 2017–19.* London, House of Lords & House of Commons. https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf

Jucevičius, R. (1997). *Strateginis organizacijų vystymas: disertacija.* Vytauto Didžiojo universitetas.

Karnouskos, S. (2011). STUXNET Worm Impact on Industrial Cyber-Physical System Security. *37th Annual Conference of the IEEE Industrial Electronics Society.* https://doi.org/10.1109/IECON.2011.6120048

Kaspersky Lab's. (2014, February 10). *Kaspersky Lab Uncovers "The Mask": One of the Most Advanced Global Cyber-espionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers*. https://usa.kaspersky.com/about/press-releases/2014_kaspersky-lab-uncovers--the-mask--one-of-the-most-advanced-global-cyber-espionage-operations-to-date-due-to-the-complexity-of-the-toolset-used-by-the-attackers

Katina, J., Plėta, T., Petkevičius, R., & Lelešienė, L. (2023). Industrial Control Systems (ICS) cyber prediction model. *Insights into Regional Development, 5*(1), 86–96. https://doi.org/10.9770/IRD.2023.5.1(6)

Kendall, M. G. (1975). *Rank Correlation Methods, 4th edition.* London: Charles Griffin.

Korsakienė, R., & Grybaitė, V. (2012). *Strateginis organizacijų valdymas. Mokomoji knyga.* Technika.

Krašto apsaugos ministerija. (2020). https://kam.lt/

KAM 2020 metų veiklos ataskaita. (2021). Lietuvos Respublikos krašto apsaugos ministerija.

Kshetri, N. (2017). Hacking Power Grids: A Current Problem. In *IEEE Security & Privacy*, 91–95. https://doi.org/10.1109/MC.2017.4451203

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. *Journal of Computer Mechanical Management, 2*(3), 31–42.

Lafley, A. G., Martin, R. L., & Ganser, L. J. (2014). *Playing to Win: How Strategy Really Works Audio CD – CD.* Brilliance Audio.

Langer, R. (2013, November 2). *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Lankauskienė, T., & Tvaronavičienė, M. (2012). Security and sustainable development: approaches and dimensions in the globalization context. *Journal of Security and Sustainability Issues, 1*(4), 287–297. https://journals.lka.lt/journal/jssi/article/1740/info

Lightman, S. (2022). *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control*. Retrieved from NIST IR 8401: https://csrc.nist.gov/pubs/ir/8401/final

Lietuvos Respublikos kibernetinio saugumo įstatymas. (2014 m. gruodžio 11 d.). *Nr. XII-1428*. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee

Lietuvos Respublikos Vyriausybės nutarimas dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo Nr. 742. (2016 m. liepos 20 d.). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/77d6b4914f2611e68f45bcf65e0a17ee?jfwid=q8i88m9wc

Lietuvos Respublikos vidaus reikalų ministerija. (2005). *Rizikos analizės vadovas.* Vilnius, VAGA.

Lithuania National Security Strategy. (2012). https://www.e-tar.lt/portal/lt/legalAct/TAR.FD615B2F7F90

Mackenzie, H. (2012, October 25). *Shamoon Malware and SCADA Security – What are the Impacts?* Tofino Security: https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-–-what-are-impacts

Mahmud, R., Vallakati, R., Mukherjee, A., Ranganathan, P., & Nejadpak, A. (2015). A survey on smart grid metering infrastructures: Threats and solutions. In *2015 IEEE International Conference on Electro/Information Technology (EIT)* (pp. 386–391). https://doi.org/10.1109/EIT.2015.7293374

Masera, M. (2010). Governance: How to Deal with ICT Security in the Power Infrastructure? In Z. D. Lukszo, *Securing Electricity Supply in the Cyber Age. Topics in Safety, Risk, Reliability and Quality.* Springer.

Maxwell, J. (1996). *Qualitative research design: An interactive approach.* Sage Publications, Inc.

McLaughlin, S., Podkuiko, D., & McDaniel, P. (2010). Energy Theft in the Advanced Metering Infrastructure. In E. Rome, & R. Bloomfield (Eds), *Critical Information Infrastructures Security. CRITIS 2009. Lecture Notes in Computer Science, 6027*, 176–187. Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14379-3_15

Melnikas, B., & Chlivickas, E. (2016). *Viešasis valdymas: aktualijos ir sprendimai globalizacijos ir žinių visuomenės kūrimo sąlygomis.* Technika. https://doi.org/10.3846/2364-M

Melnikas, B., & Smaliukienė, R. (2007). *Strateginis valdymas.* Generolo Jono Žemaičio Lietuvos karo akademija.

Mintzberg, H. (2011). *Managing*. Berrett-Koehler Publishers.

Muniz, J. (2021). *The Modern Security Operations Center The People, Process, and Technology for Operating SOC Services.* Professional Addison Wesley.

Nacionalinė kibernetinio saugumo būklės ataskaita. 2022. (2023). Krašto apsaugos ministerija. https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf

2018 metų Nacionalinio kibernetinio saugumo būklės ataskaita. (2019). Vilnius: Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos. Retrieved from https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf

Nacionalinio saugumo strategija Nr. XI-2131. (2012 m. birželio 26 d.). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.428981

National Cyber Security Centre. (2020). *Cyber security incident analysis and reports.* https://www.nksc.lt/en/

NATO Energy Security Center of Excellence. (n.d.). *About Us. What is NATO COE?*. NATO Energy Security Center of Excellence. https://enseccoe.org/en/about/6

NERC. (2019). *Cyber Security –Incident Reporting and Response Planning Implementation Guidance for CIP-008-6*. NERC. https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/Implementation_Guidance_for_CIP-008-6_Final_Ballot_01152019.pdf

Newbill, C. (2019). Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies, 26*(2), 761–780. https://doi.org/10.2979/indjglolegstu.26.2.0761

NIST. (2023). *Risk Management Framework. Information Technology Laboratory. Computer security resource center. Projects nist risk management framework*. https://csrc.nist.gov/projects/risk-management/about-rmf

Ogie, R. (2017). Cyber security incidents on critical infrastructure and industrial networks. In *Proceedings of the 9th International Conference on Computer and Automation Engineering.*

Onyeji, I., Bazilian, M., & Bronk, Ch. (2014). *Cyber security and critical energy infrastructure.* Elsevier.

Operations security (OPSEC). (2023). NIST: https://csrc.nist.gov/glossary/term/operations_security

OSCE Organization for Security and Co-operation in Europe. (2013). *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from*

Terrorist Attacks Focusing on Threats Emanating from Cyberspace. https://www.osce.org/files/f/documents/7/5/103954.pdf

Park, D., & Walstrom, M. (2017, October 11). *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Peleckis, K. (2014). Efektyvios verslo derybų strategijos teorinės prielaidos. *Journal of Management, 2*(25), 15–26.

Podvezko, V. (2011). The Comparative Analysis of MCDA Methods SAW and COPRAS. *Engineering Economics, 22*(2), 134–146. https://inzeko.ktu.lt/index.php/EE/article/view/310

Power grid cyberattack in Ukraine. (2015). International Cyber Law: https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)

Radziwill, Y. (2015). *Cyber-Attacks and the Exploitable Imperfections of International Law*. Brill/Nijhoff.

Rashid, F. Y. (2015). *Inside The Aftermath Of The Saudi Aramco Breach*. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/inside-the-aftermath-of-the-saudi-aramco-breach

Raudeliūnienė, J., Davidavičienė, V., Tvaronavičienė, M., & Jonuška, L. (2018). Evaluation of Advertising Campaigns on Social Media Networks. *Sustainability, 10*(4), 973. https://doi.org/10.3390/su10040973

Securelist.com (2013). *Red October Diplomatic Cyber Attacks Investigation*. https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation

Republic of Estonia. (2018). *Cybersecurity Act*. https://www.riigiteataja.ee/en/eli/523052018003/consolide

Ryder, R. (2019). *Cyber Crisis Management.* New Delhi, Bloomsbury India.

Roadmap to Secure Control Systems in the energy Sector. (2006). US Department of energy, US Department of Homeland Security: https://www.energy.gov/ceser/articles/roadmap-secure-control-systems-energy-sector-january-2006

Roy, B. (1991). The outranking approach and the foundations of ELECTRE methods. *Theory and Decision, 31*, 49–73. https://doi.org/10.1007/BF00134132

Rosner, K. (2013, December). Is Information Sharing a Help or Hindrance to Critical Energy Infrastructure Protection? *Energy Security Forum.* https://www.enseccoe.org/wp-content/uploads/2024/01/2013-08-12.pdf

Ruf, L., Thorn, A., Christen, T., Gruber, B., Portmann, R., & Luzer, H. (2008). Threat Modeling in Security Architecture – The Nature of Threats. *ISSS Working Group on Security Architectures*.

Rumelt, R. P. (2012, August 1). Good Strategy/Bad Strategy: The Difference and Why It Matters. *Strategic Direction, 28*(8). https://doi.org/10.1108/sd.2012.05628haa.002

Saaty, T. L. (2001). *Fundamentals of the Analytical Hierarchy Process.* Pitsburg: RWS Publications.

SANS Information Security White Papers. (n.d.). *See what white papers are top of mind for the SANS community*. https://www.sans.org/white-papers/

Sarraf, A. Z., Mohaghar, A., Ų Bazargani, H. (2012). Developing TOPSIS method using statistical normalization for selecting Knowledge management strategies. *Journal of Industrial Engineering and Management, 6*(4), 860–875. http://dx.doi.org/10.3926/jiem.573

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law, 12*. https://doi.org/10.15394/jdfsl.2017.1476

Secure.com (n.d.). *Empowering Partners & Consumers*. https://secure.com/

Securelist by Kaspersky. (2021, November 8). *DDoS attacks in Q3 2021*. https://securelist.com/ddos-attacks-in-q3-2021/104796/

Secure Software Development Framework SSDF. (2024). National Institute of standards and Technology US Department of Commerce: https://csrc.nist.gov/projects/ssdf

Securing Networks. (2023). Nuskaityta iš CISA. Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/topics/cyber-threats-and-advisories/securing-networks

Senge, P. (1990). *The Fifth Discipline: The Art and Practice of the Learning Organization.* New York: Doubleday/Currency.

Cybersecurity Framework. (2023). NIST: https://www.nist.gov/cyberframework

Smaliukas, G. (2015). *Grėsmės energetiniam saugumui*. NATO Energetinio saugumo kompetencijos centras, Lietuvos šilumos tiekėjų asociacija. http://www.lsta.lt/files/seminarai/2015-01-29%20LMA_seminaras/02_Gresmes%20energetiniam%20saugumui.pdf

Sonesson, T. R., Johansson, J., & Cedergren, A. (2021). Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety Science, 142*, 105383. https://doi.org/10.1016/j.ssci.2021.105383

Srinivas, B. V. (2014). *Security operation center (SOC) in a utility organization.* SANS Institute. SANS GIAC certifications.

Stouffer, K., Falco, J., & Kent, K. (2013). *Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC).* https://doi.org/10.6028/NIST.SP.800-82r1

Svetikas, K. Ž., & Arimavičiūtė, M. (2012). *Strateginis valdymas.* Mykolo Romerio universistetas.

Stergiopoulos, G., Gritzalis, D. A., Limnaios, E. (2020). Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access, 8*, 128440-128475. doi:10.1109/ACCESS.2020.3007960

Šišulák, S. (2017). Userfocus – tool for criminality control of social networks at both the local and international level. *Entrepreneurship and Sustainability Issues, 5*(2), 297–314. https://doi.org/10.9770/jesi.2017.5.2(10)

Tariq, N., Asim, M., & Khan, F. A. (2019). Securing SCADA-based Critical Infrastructures: Challenges and Open. *Procedia Computer Science, 155*, 612–617. https://doi.org/10.1016/j.procs.2019.08.086

Tarybos direktyva 2008/114/EC Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. (2008 m. gruodžio 8 d.). Infolex. https://www.infolex.lt/teise/default.aspx?id=1929&crd=32008L0114R(01)#

Technical Committee ISO/IEC JTC 1. Information technology - Security techniques - Code if practice for information security controls. Switzerland: ISO/IEC. (2013). https://www.iso.org/standard/62726.html

Techrepublic. (2004). *Disaster Planning and Recovery Pack.* TechRepublic.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

Telksnys, L. (2016). Kibernetinis saugumas. *Kibernetinis saugumas. Gruodžio mėn. specialus priedas*, 3. https://site2.cmm.lt/cms/images/kibernetinis_saugumas.pdf

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. In *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 40*(4), 853–865. https://doi.org/10.1109/TSMCA.2010.2048028

Oil & Gas IQ. (2011, March 3). *Terrorism 2.0 - Is Coffee Still More Important Than IT Security?*. https://www.oilandgasiq.com/oil-and-gas-production-and-operations/articles/terrorism-2-0-is-coffee-still-more-important-than

Tranchita, C., Hadjsaid, N., Viziteu, M., Rozel, B., & Caire, R. (2010). ICT and Powers Systems: An Integrated Approach. *Securing Electricity Supply in the Cyber Age, Springer*, 71-109. https://doi.org/10.1007/978-90-481-3594-3_5

The UK Cyber Security Strategy . Protecting and promoting the UK in a digital world . (2011). The National Archives, Kew, London. https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf.

Threat landscape for industrial automation systems. Statistics for H1 2023. (2023). Securelist by Kaspersky: https://securelist.com/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023/110605/

Tucci, L. (2023, September). *What is risk management and why is it important?* Techtarget Security. https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important#:~:text=Risk%20management%20is%20the%20process,errors%2C%20accidents%20and%20natural%20disasters

Turk, R. (2005, October). *Cyber Incidents Involving Control Systems. The INL is a U.S.* https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1f8fa134eca5fe92143bd154ec9f6446b38b63ae

Umbach, F. (2013). *Cyber attacks on critical energy infrastructures are increasing globally*. https://www.getabstract.com/es/resumen/cyber-attacks-on-critical-energy-infrastructures-are-increasing-globally/19668?st=RELATED&si=21865https://www.gisreportsonline.com/cyber-attacks-on-critical-energy-infrastructures-are-increasing-globally,defense,818,report.html

United States Government Accountability Office (GAO). (2007, September). *Critical infrastructure protection: Multiple efforts to secure control systems are under way, but challenges remain*. http://www.gao.gov/assets/270/268137.pdf

US Government Accountability Office (US GAO). (2005, May). *Critical Infrastructure Protection*. http://www.gao.gov/new.items/d05434.pdf

bolyongó.hu. (2023). *Varnos Sandor*. https://bolyongo.hu/doku.php?id=passport:a_stuxnet_sztori

Vasiliauskas, A. (2015). *Strateginis valdymas: įmonių ir nacionalinės ekonomikos strategijų sintezė.* Vilniaus universiteto leidykla.

Volz, D. (2016). *U. S. government concludes cyber attack caused Ukraine power outage*. Reuters. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K

Wei, D., Lu, Y., Jafari, M., Skare, P., & Rohde, K. (2010). *An integrated security system of protecting Smart Grid against cyber attacks* (pp. 1–7). In *2010 Innovative Smart Grid Technologies (ISGT)*, Gaithersburg, MD, USA. https://doi.org/10.1109/ISGT.2010.5434767

World International Studies Committee. (2015). *WISAC - Wales International Study Centre (WISC)*. https://www.wiscnetwork.net/

Wilson, M., & Hash, J. (2003). *Computer security. Building an Information Technology Security Awareness and Training Program.* Washington: U.S. Government printing office. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication80

Wiśniewski, M. (2020). Methodology of situational management of critical infrastructure security. *Foundations of Management*, *12*(1), 43–60. https://doi.org/10.2478/fman-2020-0004

Wuuest, C. (2014, January 13). *Targeted Attacks Against the Energy Sector*. Security Response. https://docs.broadcom.com/doc/targeted-attacks-against-engery-sector-14-en

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operation Center.* The MITRE Corporations 2014. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Žintelis, G. (2018). NKSC 2018 metų ataskaitos išvados ir rekomendacijos. *Kibernetinio saugumo apžvalga*, 4–6. https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf

Autoriaus mokslinių publikacijų disertacijos tema sąrašas

Straipsniai recenzuojamuose mokslo žurnaluose

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and sustainability issues*, *4*(4), 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)

Plėta, T., Karasov, S., & Jakštas, T. (2019). The means to secure critical energy infrastructure in the context of hybrid warfare: the case of Ukraine. *Journal of security and sustainability issues.* https://doi.org/10.9770/jssi.2018.7.3(16)

Plėta, T., Tvaronavičienė, M., & Casa, S. D. (2020). Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development*, *2*(2), 538–548. https://doi.org/10.9770/IRD.2020.2.2(3)

Plėta, T., Tvaronavičienė, M., Casa, S. D., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. *Insights into Regional Development*, *2*(3), 703–715. https://doi.org/10.9770/IRD.2020.2.3(7)

Tvaronaviciene, M., Pleta, T., Semaskaite, V., Paulauskiene, T., & Vaiciute, K. (2020). Cold energy economy and cybersecurity of floating storage and regasification units: emerging trends, challenges, and opportunities. *Journal of Security and Sustainability Issues, 10*(1): 249–262. https://www.researchgate.net/publication/344339480_Cold_en-

ergy_economy_and_cybersecurity_of_floating_storage_and_regasification_units_emerging_trends_challenges_and_opportunitiesTvaronavičienė, M., Plėta, T., Casa, S. D., & Latvys. J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, *2*(4), 802–813. https://doi.org/10.9770/IRD.2020.2.4(6)

Tvaronavičienė, M., Plėta. T., Beretas, Ch. P., & Lelešienė, L. (2022). Analysis of the critical infrastructure cyber security policy. *Insights into Regional Development*, *4*(1), 26–39. https://doi.org/10.9770/IRD.2021.4.1(2)

Straipsniai kituose leidiniuose

Tvaronavičienė; M., Plėta, T., & Casa, S. D. (2021). Cyber security management model for critical infrastructure protection. *Scientific Conference „Contemporary Issues in Business, Management and Economics Engineering". 13–14 May 2021, Vilnius, Lithuania Vilnius Gediminas Technical University* (pp. 133–139). https://doi.org/10.3846/cibmee.2021.611

Plėta, T. (2023). Preliminary Technical Analysis of the Establishment of Information Security Operations Centers in Companies with Critical Energy Infrastructure. Vilnius: NATO Energy security Centre of excellence. Prieiga per internetą: https://www.enseccoe.org/publications/preliminary-technical-analysis-of-the-establishment-of-information-security-operations-centers-in-companies-with-critical-energy-infrastructure/

Summary in English

Introduction

Problem Formulation

Cyber threat challenges are constantly increasing, indicating a growing level of expertise among hackers and an expansion in their number. Therefore, cybersecurity is one of the crucial factors that needs to be addressed at the state level.

A reliable and secure critical infrastructure is vital for economic prosperity as it supports the efficient operation of businesses and services and fosters long-term trust, planning, and investment attraction. However, new opportunities for cyber threats arise with the development of information technology, digitisation, automation, and optimisation. This highlights the necessity for changes in cybersecurity defence and management.

Considering the energy sector's nature, specificity, and structural characteristics, it is essential to explore new measures and tools to strengthen and improve its cybersecurity. This involves employing modern management methods and tools to address the issue of quality management.

The changing environment encourages a new approach to managing the cybersecurity of critical energy infrastructure. Therefore, it is crucial to develop an effective and universal management model that addresses cybersecurity issues by identifying and managing interrelated processes.

Relevance of the Dissertation

In recent years, increasing attention has been devoted to cybersecurity and energy security. National strategies highlight cybersecurity and energy security as primary national security interests that, if neglected, could compromise vital state interests over time (National Security Strategy, 2012). Cybersecurity and the energy sector are closely intertwined, and cyber threats to critical energy infrastructure are gaining greater prominence (Smaliukas, 2015).

The rapid information technology development is gradually changing the world. An open and free electronic space increases people's freedom and opportunities, enriching society. However, at the same time, the modern digital world's advantages and the expansion of information technology pose new threats to national and international security (Šišulák, 2017). Therefore, the model was created using the concept of a learning organisation, and the module itself is considered a learning organisation consisting of interconnected elements that constantly interact with the environment and adapt to it.

Research Object

The research object is the cyber security management of the critical energy infrastructure in states.

Aim of the Dissertation

This dissertation aims to create a cyber security management model for the critical energy infrastructure of states, integrating factors that effectively ensure cyber security management.

Tasks of the Dissertation

The following tasks are implemented to achieve the dissertation's aim:

1. Analyse the cybersecurity of the energy sector, management of critical energy infrastructure, and challenges, and reveal their issues by examining relevant documents and literature sources.
2. Examine and evaluate the best practices and weaknesses applied by the states, foreseeing the most effective ways of managing cyber incidents.
3. Develop a cyber security management model ensuring effective cybersecurity management, the integrity of system operations, and efficiency.
4. Provide practical application recommendations for the cyber security management model of critical energy infrastructure.

Research Methodology

The dissertation employed a comparative analysis. The study analyses cybersecurity strategies for critical energy infrastructure, primarily focusing on guidelines, state strategies, legislation, actors' strategies, international regulations, strategic documents, and best practices of various countries. The goal is to identify effective solutions in the field of cybersecurity.

Interviews with critical energy infrastructure experts, direct operators of critical infrastructure, and representatives from the National Cyber Security Centre allowed for identifying key cybersecurity issues in critical energy infrastructure and determining the significance of components. The Simple Additive Weighting Method (SAW) enabled the identification of components that require more improvement to enhance the security level of critical infrastructure. It also facilitated ranking cybersecurity model components based on their implementation priorities.

In creating the cybersecurity model for critical energy infrastructure, the assessment includes evaluating the possibilities, challenges, and addressable issues related to applying the cybersecurity model for critical energy infrastructure in the country. Proposed steps for implementing the model are provided.

Scientific Novelty of the Dissertation

In preparing the dissertation, the following new results were obtained, expanding contemporary management theories, specifically the concept of a learning organisation:

1. Through document analysis and expert interviews and by evaluating best practices applied in foreign countries, a cyber security management model has been developed to enhance quality management, thereby expanding the application of the concept of a learning organisation.
2. A methodology has been created after analysing existing cybersecurity strategies for critical energy infrastructure, legal acts regulating cybersecurity in states, and conducting an expert survey. This methodology incorporates key principles of a learning organisation to ensure effective cybersecurity management, formulate a common development strategy, and facilitate efficient planning.
3. To address security issues and risks, a cybersecurity quality management measure has been proposed, ensuring the effective integrity and efficiency of the cybersecurity system.

Practical Value of the Research Findings

4. The cybersecurity management model, comprised of organisation management processes, legal regulation, cyber security culture within the organisation, technological cyber security, risk management, cyber incident management, and strategic management components, helps a state achieve effective management.
5. The application of the cyber security management model enables the improvement and enhancement of the cyber security of critical energy infrastructure by interacting with management components and ensuring the feasibility of technical management systems.
6. A methodology for the use of the cyber security management model, consisting of sequential actions, serves as a supportive tool for the model. Together with the model itself, it creates conditions for ensuring effective cyber security of critical energy infrastructure in states.

Defended Statements

7. The cybersecurity management model of six components (legal regulation, organisational management, risk management, cyber security culture, technology management, and cyber incident management) is insufficient for effective management of cyber security in critical energy infrastructure. Therefore, it needs to be supplemented with the strategic management component.
8. The developed cyber security management model, consisting of organisational management, legal regulation, cyber security culture, technology management, risk management, cyber incident management, and strategic management components, is universal for any critical energy infrastructure.
9. The created methodology for applying the cyber security management model is suitable for practical use in any critical energy infrastructure, enhancing and improving cyber security.

Approval of the Research Findings

The topic of the dissertation is covered in two scientific articles published in the *Clarivate Analytics Web of Science* and *Scopus* databases, and six other international databases and peer-reviewed scientific journals (Limba, Plėta, Agafonov & Damkus, 2017; Plėta, Karasov & Jakštas, 2019; Plėta, Tvaronavičienė & Della Casa, 2020; Plėta, Tvaronavičienė, Della Casa & Agafonov, 2020; Tvaronaviciene, Plėta, Semaskaitė, Paulauskienė & Vaiciutė, 2020; Tvaronavičienė, Plėta, Della Casa & Latvys, 2020; Tvaronavičienė, Plėta & Della Casa, 2021; Tvaronavičienė, Plėta, Beretas & Lelešienė, 2022). The research results of the dissertation were presented at international scientific conferences and seminars in Lithuania and abroad:

1. International scientific conference "*Contemporary Issues on Business, Management and Economics Engineering"*, 2021, Vilnius, Lithuania;
2. International scientific conference "*Communication and Information Sciences in the Network Society: Experiences and Insights IV*", 2018, Vilnius, Lithuania;
3. 12th international scientific conference "*Transport Problems (TP'2020)*", 2020, Katowice, Poland;
4. Scientific seminar, 2020, Daugpils, Latvia.

The research results of the dissertation were approved through participation in the 2022 NATO project "Preliminary Technical Analysis of the Establishment of Information Security Operations Centres (SOC) in Companies with Critical Energy Infrastructure" and published in the NATO ENERGY SECURITY CENTRE OF EXCELLENCE publication.

Structure of the Dissertation

The dissertation consists of an introduction, three chapters, general conclusions, a list of literature sources, and appendices. The scope of the work is 130 pages, excluding literature sources, the summary in English, appendices, and the list of author's publications. The dissertation includes 39 figures, 23 tables, and references to 180 literature sources.

1. Analysis of Cybersecurity Management in Critical Energy Infrastructure

Cybersecurity is crucial in the modern digital world, as electronic crimes pose a global threat. Large organised crime groups and skilled programmers constantly create new threats, making it essential for states and the private sector to protect crucial data from theft or destruction. The fundamental cybersecurity principle is to protect the cyber environment from modern, dangerous attacks (Telksnys, 2016).

Summarising the concepts of cybersecurity, it can be described as a set of security measures, strategies, security concepts, risk management methods, actions, training, best practices, and technologies that can be used to protect the cyber environment. It establishes the key cybersecurity objectives: confidentiality, integrity, and availability (Wiśniewski, 2020).

Cybersecurity is a complex, systemic issue that affects critical infrastructure, including electricity, oil, and gas, which could be significantly impacted by disruption or destruction (Johnson, 2015).

The increasing vulnerability, primarily stemming from the complexity of the system and integration process, poses a major challenge. Ensuring the proper functioning of communication and information systems is integral to the responsibilities of managers overseeing special importance information infrastructure and state information resource managers. However, the sluggish implementation of cybersecurity requirements persists due to lax attitudes among SII managers, a shortage of competent cybersecurity and information technology professionals, and the continual expansion of information and communication technology (Lankauskienė & Tvaronavičienė, 2012).

The Internet of Things (IoT) has introduced various smart devices, from smartwatches to large-scale infrastructure. The growing reliance of industrial control systems on the IoT poses a substantial potential risk, especially for critical infrastructure. Cyberattacks are increasing in operational technology sectors like water systems, power grids, transportation, communication, manufacturing, and other critical infrastructure. Industrial Control Systems (ICS) are crucial in managing critical energy infrastructure, emphasising the need to monitor and analyse attacks to prevent future breaches and identify security threats (Das & Gündüz, 2020).

A new cybersecurity approach is necessary to integrate IT and OT security. Existing cybersecurity management models fail to adequately protect against cyber-attacks, unexpected scenarios, and vulnerabilities. Addressing cybersecurity issues in critical situations is crucial to safeguard key national interests, necessitating an integrated and hybrid cybersecurity management model (Limba et al., 2017).

Cybersecurity is crucial for critical energy infrastructure, as cybercriminals target commercial products for financial or political gains. Despite challenges in predicting threats and implementing timely preventive measures, the risk of successful attacks is increasing (Plėta et al., 2019).

Many countries lack strategies to respond to cyber-attacks and unforeseen scenarios. Critical infrastructure security is influenced by technological developments and changing market trends, impacting system management and resilience to cyber vulnerabilities. Cybersecurity gaps present challenges for system owners or operators but might not be recognised as vulnerabilities in critical infrastructure systems (Limba et al., 2017).

Estonian researchers stress the significance of a systemic cybersecurity approach, which necessitates substantial national and international collaboration. Best practices involve clearly defining information security standards, formulating a National Security Strategy with private sector involvement, and establishing a committee for protecting critical infrastructure (Bulakh et al., 2016).

Predicting, forecasting, and implementing timely preventive measures against cyber threats remain difficult, heightening the risk of successful cyber-attacks. Monitoring and conducting comprehensive assessments of cyber incidents are crucial to prevent future attacks and identify security threats.

2. Cybersecurity Management Practices for Critical Energy Infrastructure in Other Countries

Critical infrastructure objects require robust security management, particularly in outdated operational technology systems. The industrial cybersecurity market demands robust supply chain management, communication protocols, vulnerability reporting, and accountability. A continuity of operations plan is necessary for protecting critical energy infrastructure. Researchers have proposed a management model that focuses on industrial control systems security, considering operational and information technologies convergence due to digitisation and information technology development (Limba et al., 2017). This model includes a management system capable of supporting aspects of cybersecurity, focusing on cybersecurity technologies and their management (Fig. S2.1).

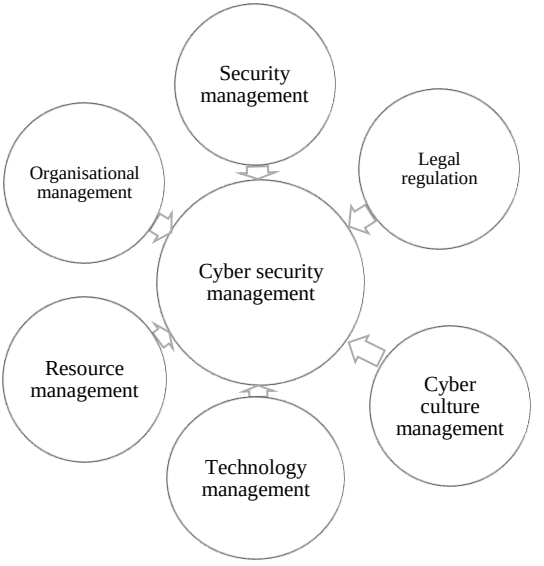


Fig. S2.1. Cyber Security Management Model (based on Limba et al., 2017)

The cybersecurity management model consists of six components, each addressing specific actions for an organisation's security. It allows for individual implementation of actions at different levels, enhancing cybersecurity and enabling organisations to adapt to

rapid technological changes. Cyberattacks on critical infrastructure, such as energy infrastructure, have been occurring since before the Internet and information technology. Identifying perpetrators and finding optimal solutions to prevent cyber-attacks is not always feasible (Limba et al., 2017).

The most common errors in critical energy infrastructure can be compared and evaluated according to certain criteria that make up the cybersecurity management model: security management, legal regulation, cyberculture management, technology management, organisation management, and resource management.

Table S2.1. Cybersecurity gaps identified (based on Limba et al., 2017)

	Organisational management	Legal management	Cyberculture management	Resource management	Technology management	Security management
Case 1 (Stuxnet)	×			×		
Case 2 (Shamoon)		×	×			×
Case 3 (Ukraine, 2015)	×		×			

Table S2.1 highlights cybersecurity gaps in various cases. Stuxnet exposed vulnerabilities in the Natanz nuclear plant, the Ukraine 2015 attack revealed insufficient system protection, and Shamoon malware demonstrated communication issues, leading to breaches in law, information security, cyber hygiene, and incident management. Saudi Aramco oil plant faced disruption (Falliere, 2011).

Organisational and cyberculture management are key cybersecurity gap indicators in two out of three cases. A six-category cybersecurity management module is insufficient for critical energy infrastructure, and no suitable method exists for measuring impact (Onyeji et al., 2014).

To assess the problem of critical energy infrastructure as a gap in the national cybersecurity strategy, it is necessary to analyse and compare the decisions and changes in the national cybersecurity strategy in five different countries. The countries are selected following the 2019 published Global Cybersecurity Index (GCI). The list was compiled after assessing the country's commitments and developing cybersecurity solutions.

The assessment is done by scoring five main elements that have the same value when calculating the final score (ITU, 2019):

1. Legal and regulatory measures – the existence of legal institutions and structures related to cybersecurity;
2. Cyber security management and standards (technical measures) – existence of technical institutions and structures related to cyber security;
3. Organisational measures – the presence of an institution coordinating policy;
4. Capacity building and awareness – access to research and development programmes, education and training;
5. Cooperation – the existence of a system of partnership and cooperation.

Table S2.2. Cybersecurity analysis of five countries (based on Tvaronavičienė et al., 2019)

	Legal management	Organisational management	Resource management	Cyberculture management	Technology management	Security management	Total
UK	4	3	3	4	0	0	12
USA	5	5	4	4	4	4	26
France	3	2	0	0	0	2	7
Estonia	4	4	3	0	0	3	12
Lithuania	2	0	1	0	0	2	5

The analysis of five countries reveals inadequacy in critical infrastructure protection, with the US model being the most comprehensive, and suggests a comprehensive cybersecurity approach.

The approved cybersecurity management model is reasonably suitable for ensuring cybersecurity in critical infrastructure, but it lacks components that consider the need for more elements in the country's development (Plėta et al., 2020).

The cybersecurity management model comprises six components, including strategic management, implemented gradually to ensure critical energy infrastructure cybersecurity. A new model with seven components aims to address key aspects (Plėta et al., 2021).

The cybersecurity management model is a complex and time-consuming process best implemented in stages, with each component divided into levels for independent implementation. Understanding each component's responsibilities is crucial for achieving high cybersecurity levels (Plėta et al., 2021).

- **Organisational Management Processes.** At the initial level, by analysing the organisation's management system and identifying those involved in decision-making processes, it is possible to understand who participates in the cybersecurity management process and what impact cybersecurity management has on the organisation. Moving to the next level, the organisation must have a clear understanding of the chain of command, regulate decision-making processes, and establish the limits of responsibility for organisation members.
- **Legal Regulation.** At this level, an external and internal analysis of the legal system is conducted, along with the requirements and existing shortcomings of all legal aspects that could influence the organisation's security policy. All legal aspects, operational instructions, and rules must be clearly defined, prepared, and presented to each organisation member. Periodic audits of the legal regulatory system should also be conducted.
- **Cybersecurity Culture**. At the initial level, the organisation identifies and clearly understands the cybersecurity measures in place that can enhance cybersecurity. Then, at the next level, necessary skills for personnel are identified, and training plans for organisation members are planned since all organisation members are responsible for cybersecurity.

- **Technology Management.** At this level, the definition of daily work processes technologies helps identify potential cyber-attacks and their direction. The identification of hardware and software life cycles contributes to successful technology management, while continuous audits plan financial resources for system updates and maintenance.
- **Risk Management.** At the initial level, all possible internal and external risk factors and other factors that could impact the organisation's activities are described. Further, at the next level, they are identified, and a risk management plan is developed.
- **Incident Management**. Organisations are vulnerable to technical and personnel issues, and awareness of cybersecurity incidents is crucial for improving security. This level checks preparedness, management, and recovery plans and examines actions during or after cyberattacks.

In summary, briefly describing the six components of the cybersecurity management model, it is necessary to examine the seventh component – strategic management – more thoroughly, which is discussed in the context of management in this dissertation.

The model gradually implements components, including the strategic management component, which consists of initial and intermediate levels, as illustrated in Figure S2.2.

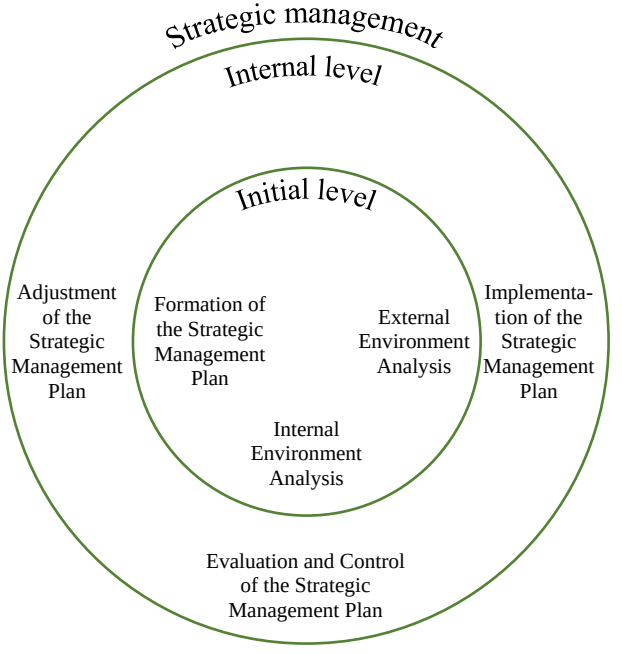


Fig. S2.2. Structure of the strategic management component

To accomplish the main task of ensuring the cybersecurity of the critical energy infrastructure of the states, it is necessary to implement specific measures at each level, as outlined in Table S2.3.

Table S2.3. Tools of the strategic management component (made by the author)

<table>
<tr><td colspan="3">The Strategic Management Component</td></tr>
<tr><td>Initial Level</td><td>Intermediate Level</td><td></td></tr>
<tr><td>External Environment Analysis</td><td rowspan="3">Implementation of the Strategic Management Plan</td><td rowspan="4">Strategic management is the integration and connection of the cybersecurity management model, linking it with other components of the cybersecurity model.</td></tr>
<tr><td>Internal Environment Analysis</td></tr>
<tr><td>Formation of the Strategic Management Plan
Establishment of Mission and Vision Setting Objectives and Tasks
Formation of Structure (Technology (Processes), Technical Means, Personnel)</td></tr>
<tr><td></td><td>Evaluation and Control of the Strategic Management Plan</td></tr>
<tr><td></td><td>Adjustment of the Strategic Management Plan</td><td></td></tr>
</table>

At the initial level, conducting an external and internal environmental analysis and forming the strategic management plan can be referred to as preparatory processes necessary for implementing the strategic plan. However, before starting the implementation of the strategic management plan, it must be documented and approved.

The strategic management component of the cybersecurity management model integrates with other components, with measures for implementation and utilisation detailed in sub-chapter 3.3, “Recommendations for the Practical Application of the Cybersecurity Model for Critical Energy Infrastructure of States”.

In summary, the effective application of the strategic management component, along with proper employee training, correct network and device configuration, and physical security, will help avoid risks or significantly reduce them to a tolerable level. Identifying vulnerabilities, implementing cybersecurity policies, training, system updates, and even removing necessary systems that do not meet current security and operational needs are levers to prevent future cybersecurity threats.

3. Methodology for Empirical Research on the Management Model of Cybersecurity for Critical Energy Infrastructure

In the second chapter, a theoretical model for the cybersecurity of the critical energy infrastructure of states was described and approved (Fig. S2.1). The study suggests that implementing a cybersecurity management model for critical infrastructure should adhere to

the ISO/IEC 27002 information technology standard, which offers best practices for effective security. Consequently, the cybersecurity model was refined, and an additional component – strategic management – was added (Fig. S2.7).

Having refined the model, a quantitative empirical study was conducted to understand expert opinions on the structure and importance of cybersecurity model components for states' critical energy infrastructure and determine whether strategic management is essential.

The study reveals that each component of the cybersecurity model for critical energy infrastructure is crucial, particularly strategic management, as it is a new part of the model.

The research results show that the strategic management component needs improvement, as mere structuring is insufficient for its full utilisation. Actions required to correctly implement cybersecurity using this component must be identified. The key stages and essential steps to implement them should be clearly described (Bivainis, 2011).

Step 1: External Environment Analysis

Based on the core processes of strategic management, the development of a strategy framework must begin with an analysis of the external environment, which can use the risk management and legal regulation components of the cybersecurity management model.

Step 2: Internal Environment Analysis

Understanding the external environment is crucial for better responsiveness to necessary changes, but it is equally important to comprehend and accurately assess the internal situation (Bivainis, 2011). Therefore, when evaluating the internal environment, it is essential to analyse the organisation and its entire operations, utilising the components of the cybersecurity management module: organisational management, cybersecurity culture, cybersecurity technologies, and cybersecurity incident management. In this process, a useful tool can be the System Development Life Cycle design method.

The System Development Life Cycle method consists of six stages:

1. ***Collecting information about the project***, *i.e.*, gathering data about the planned project and identifying needs and objectives.
2. ***Analysing collection information***, i.e., examining and processing the gathered information to better understand the project and its requirements.
3. ***Designing a new system***, i.e., considering necessary conditions and security requirements: the development stage where a new system is designed, considering all relevant aspects, including security requirements.
4. ***Creating the information system***, i.e., the physical stage of creating the new system, involves developing and testing software.
5. ***Installing the information system in the infrastructure***, i.e., installing the developed information system into the organisation's infrastructure.
6. ***Customising and user training***, i.e., adapting to specific organisational needs and training users on how to use the new system.

Step 3: Formation of the Strategic Management Plan

After conducting a risk analysis, it is essential to formulate a strategy management plan. First, it is necessary to clarify its composing elements and implementation actions to be taken. While the structure and specifics of work may vary across companies, the key elements used in preparing a strategic management plan are generally the same for all

(Fig. S3.1). It is worth noting that all activities, assessments, and requirements needed for implementing the strategic plan must be documented (Tucci, 2023).

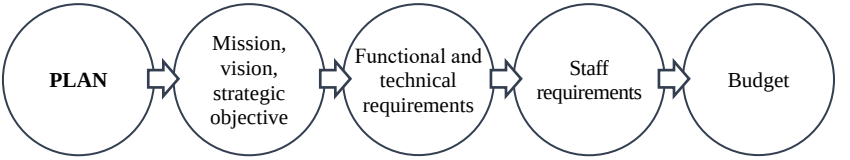


Fig. S3.1. Strategic management process sequence

Each element of the strategic management plan should be thoroughly described. When formulating the mission and setting goals and objectives, it is crucial to carefully assess all aspects related to infrastructure and data security, as the implementation strategy is responsible for all aspects, including IT (local and remote), OT, cloud, and mobile technologies.

Functional requirements. To implement a management strategy, select the right functions from over 40 available functions (based on Trellix.com). Less is better than more at the beginning. Analyse key tasks and processes, such as information security and IT data management, to ensure successful implementation. This will enable users to report suspicious activity, investigate incidents, and respond appropriately.

The processes and procedures used in implementing the strategy should be documented. All organisations have different documentation procedures, but at this stage, it is important to organise everything so that all participants in the process (and there are many) are aware of their responsibilities and the common goal. Moving to the next stage – the selection of technical tools – is conditional on understanding what needs to be automated. In addition to traditional systems, many additional tools will be needed, often inexpensive or easy to use but requiring certain knowledge from the staff. Therefore, it is possible to establish "qualitative and quantitative" requirements for personnel.

Technical requirements. After conducting an internal analysis using the management module of cybersecurity, encompassing organisational management, cybersecurity culture, cybersecurity technologies, and components of cybersecurity incident management, and summarising the obtained results, a structure can be developed to facilitate the implementation of the strategy.

As the need for data protection continues to grow, a specialised Security Operations Centre (SOC) is required, which serves as the foundation for the incident management process.

First and foremost, SOC is a team of security experts with the competencies and technologies to detect, analyse, and prevent cyber threats. SOC can be likened to the work of firefighters or paramedics. SOC specialists, like rescuers, assist in case of emergencies: they quickly appear at the necessary location, analyse threats, and respond appropriately. Their goal is to prevent such incidents.

SOC deals with continuous streams of information processed by computer systems and experts. After selecting functions, it is necessary to move on to the structure that defines the main components of the classic triad "personnel–processes–technologies" development (Fig. S3.2).

No one-size-fits-all SOC structure exists because each has its "mandatory" set of SOC components, depending on the scope of functions and tasks addressed. However, considering functionality and ongoing processes, technically, the SOC structure can be divided into three main blocks, where all key processes will take place. Therefore, the implementation of actions in the SOC system can be represented using modern equipment and technologies.

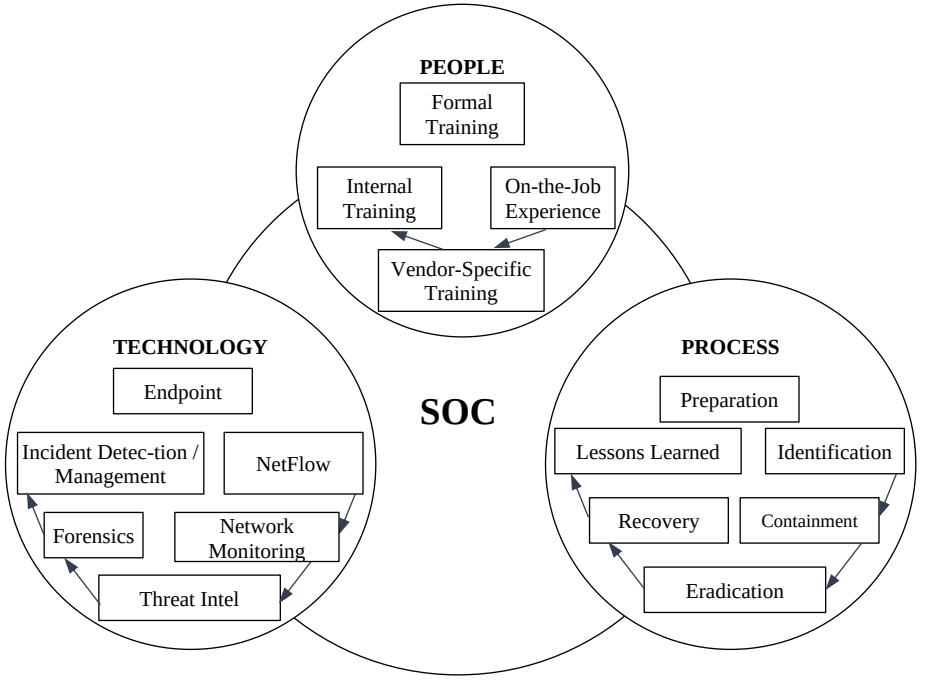


Fig. S3.2. People, process and Technology Core Elements (based on Muniz, 2021)

1. The first block manages analyses, and filters external communications, creates active traps and fake resources, and simulates the continuous work of legitimate users, software, and technical equipment (Jena, 2023). Attackers successfully target these, achieving presumed attack results and providing the SOC team with time to respond. It also monitors and prohibits.
2. The second block consists of three systems: SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and Analyser, which automate tasks of incident detection and processing by collecting, correlating, and analysing events and information security tools. It anal-

yses the flow, increases incident response speed, encodes messages, or allows access from the internal network. Additionally, these systems can perform additional tasks such as IT infrastructure inventory and control, vulnerability management, prioritising vulnerabilities based on criticality levels of information assets, automatic assignment of responsible individuals, and removal deadlines.

3. The third block is network traffic monitoring, accounting, control, and control of user access from the network to external resources. It supports deep packet inspection to verify if they belong to existing communication, detects malware and attacks, manages files and programs, filters and protects against spam emails, intrusion prevention, load balancing, reloading, etc.

SOC should analyse events and information security controls to detect incidents. This should be done not only in real-time but also over a certain period to identify missed incidents. To prevent the recurrence of incidents, it is crucial to analyse the results of the response. It is necessary to understand why the incident occurred and what effective measures were taken to eliminate it. Monitoring the values of metrics allows the timely identification and resolution of issues that may arise both in organising the process and in its implementation (Zimmerman, 2014).

A crucial question often causing much debate is the operational mode of the SOC system. The ideal scenario is to operate 24/7/365 at full capacity since many attacks, especially targeted ones, occur during the night. Working in an 8/5 mode would result in a full response only during the next business day's lunchtime when analysts analyse the night (or weekend) data and resolve situations. Therefore, the staff must work in three shifts of 24 hours each. Depending on the SOC system, the number of employees may vary. If it is not a state enterprise, then there should be no fewer than three people per shift: two employees and one supervisor. If it is a state enterprise, then the number may range from 12 to 15 people (Zimmerman, 2014).

Staff requirements. The strategic management plan for cybersecurity requires a team with qualified personnel to control technical measures. Hiring high-level specialists is crucial for successful implementation. A strong team with diverse technical and non-technical skills is essential for effective response to security incidents. A comprehensive examination is necessary to identify opportunities and reduce costs. Each team member should develop a training program based on knowledge assessment results.

While there may be employees within the team capable of performing certain roles, it is still essential to invest in external talent to create the best team, comprised of individuals necessary for implementing the strategy, such as:

- **Manager**, who leads the team and reports to the chief information security officer
- **Security Analyst**, who conducts real-time risk management and security analysis.
- **SIEM Engineer**, who manages Security Information and Event Management (SIEM), incident response, and supplier management.
- **Investigator**, who analyses event data, evidence, and behaviour.
- **Incident Responder**, who conducts initial investigations and threat assessments using incident response plans.

- **Auditor**, who ensures that procedures comply with government regulations and industry standards.

To ensure effective cybersecurity, it is crucial to organise and conduct training sessions for a team, covering technical aspects and procedures, continuously collect and disseminate information about new threats and security trends, and determine technical requirements for equipment, including antivirus, firewall, intrusion detection systems, and more complex tools, and budget for security controls and response measures, considering infrastructure security and repair costs.

Step 4: Implementation of the Strategic Management Plan

A Security Control Centre (SOC) system automates processes using tools like antivirus, firewall, and hacker detection systems. The system is divided into zones, each with its layer of security to minimise damage in case of an attack. Tools like Secure Switch, VPN, EDR, Fabric API, Application Controls, Threat Protection, and Transparent NGFW are used in process control areas. Critical infrastructure objects, interconnected with complex mechanisms, can trigger a chain reaction in case of a cyber-attack (Fig. S3.3). To prevent future threats, identifying vulnerabilities, implementing security policies, training, system updates, and removing unnecessary systems are crucial. Proper employee training, network and device configuration, and physical security can significantly reduce risk.

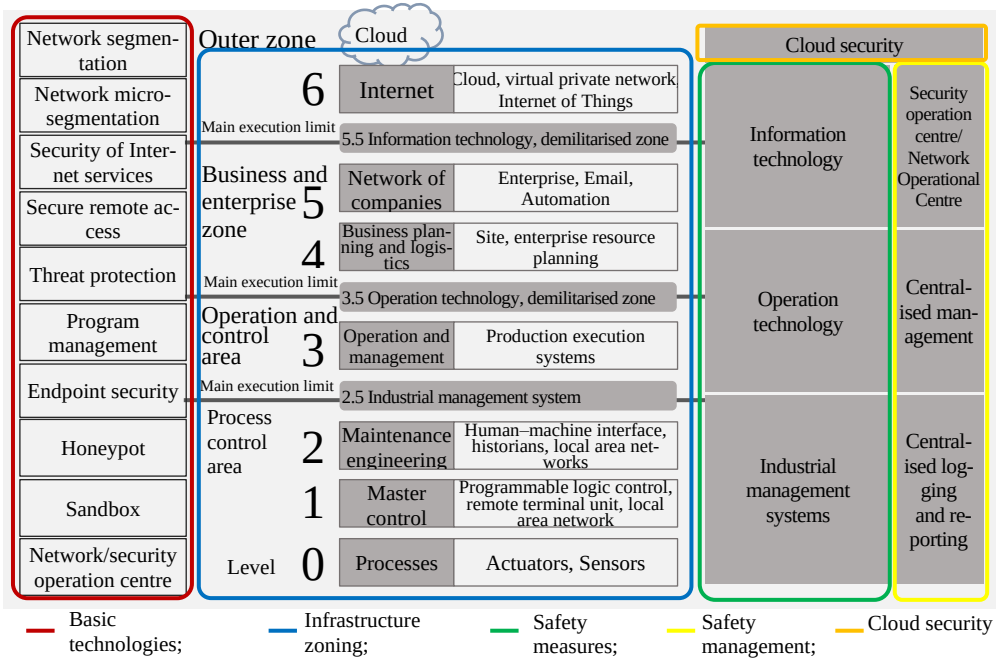


Fig. S3.3. Modern SOC logical chart (based on Zimmerman, 2014)

Step 5: Evaluation and Control of the Implementation of the Strategic Management Plan

The management and implementation of security methods in critical infrastructure involves identifying vulnerabilities, assessing risks, and making appropriate decisions. Regularly conducting security audits, and system investigations, identifying vulnerabilities, evaluating results, and verifying vulnerabilities are essential. A Security Operations Centre (SOC) is required to process increasing security data and enhance security by continuously checking for network vulnerabilities. SOCs can reduce costs and centralise operations, improving collaboration and knowledge sharing. A NATO project approved an enhanced model of cybersecurity management, demonstrating that SOC improves cybersecurity management in critical energy infrastructure, enabling real-time incident monitoring and timely responses.

General Conclusions

1. The following conclusions were determined having studied relevant documents and literature sources, analysed the cybersecurity of the energy sector and management of critical energy infrastructure, and identified its issues:

1.1 There is no common concept of critical infrastructure, but a shared understanding is based on safeguarding the cyber environment against attacks and ensuring confidentiality, integrity, and availability.

1.2 The approach of states towards critical infrastructure varies; however, universally, the energy sector is considered a component of paramount importance. The compromise or destruction of this sector has a profound impact on the security of any country.

1.3 Current cybersecurity management models fail to provide adequate protection. Many countries lack strategies for responding to cyber-attacks and unforeseen scenarios, with many failing to assess their vulnerabilities.

1.4 Factors influencing the cybersecurity of critical energy infrastructure require increased attention at various levels. The consequences of a failure in one system component can be hazardous to human life, the environment, and business.

2. After examining and evaluating the weaknesses in the critical energy infrastructure of five countries and reviewing best practices, it was identified that the level of security in critical energy infrastructure is insufficient. Furthermore, the potential application of a cybersecurity model to effectively ensure the cybersecurity of critical energy infrastructure was justified. This consideration considers the hierarchical classification method of critical infrastructure, utilising international criteria, and emphasises the importance of planning since it is unclear what specifically needs protection in critical infrastructure objects.

3. After evaluating the weaknesses and best practices in the critical energy infrastructure of five countries (the United Kingdom, the United States, France, Estonia, and Lithuania), it can be concluded that the level of security in critical infrastructure is insufficient. The six-component cybersecurity model is suitable for assessing cybersecurity, but it can be enhanced by considering the hierarchical classification method of critical infrastructure based on international criteria, which considers elements essential for the country's development and planning. The analysis also confirmed deficiencies in technology management.

4. A new cybersecurity management model has been developed, consisting of seven equivalent components (organisational management processes, legal regulation, cybersecurity culture, technological cybersecurity, risk management, cybersecurity incident management, and strategic management). Each component, individually and all together, will help ensure effective cybersecurity management.

5. After conducting an empirical study and evaluating the results of the expert survey in the field of cybersecurity, it is pertinent to determine the significance of the components of the cybersecurity model for the critical energy infrastructure of states. This can be achieved using the Simple Additive Weighting (SAW) method to identify which component needs to be developed first.

6. The results of the empirical study indicate that each component of the model is necessary and crucial for organising the security process properly. They also provide a rationale for the utilisation of the strategic management component in the cybersecurity model and its further development and application.

7. To improve the efficiency of the state's critical energy infrastructure cybersecurity model, a dedicated Security Operations Centre (SOC) is required. This centre integrates all components of the model and can significantly enhance the effectiveness of cybersecurity management in critical energy infrastructure at the national level. Therefore, recommendations are provided for the practical implementation of the developed cybersecurity management model, the sequence of actions, and the logical scheme of SOC system operation. The structure and key components are described.

8. The established Security Operations Centre (SOC) and proposed methodology for addressing cybersecurity issues and risks ensure effective cybersecurity management, system integrity, and efficiency.

Priedai

A priedas. Apklausos anketa, naudota empiriniame tyrime
B priedas. Ekspertų vertinimo rezultatai
C priedas. Daugiakriterio vertinimo rezultatai
D priedas. Saugumo operacijų centro procedūros ir funkcijos
E priedas. Saugumo operacijų centro struktūra

A priedas. Apklausos anketa, naudota empiriniame tyrime

Kartu su prof. dr. Manuela Tvaronavičienė atliekame tyrimą siekdami įvertinti kibernetinio saugumo valdymo modelį kritinės infrastruktūros saugumo kontekste, atsižvelgdami į kategorijų ir struktūros pasirinkimą. Tuo tikslu reikėjo nustatyti, kaip ekspertai aktualizuoja kibernetinio valdymo modelio komponentų svarbumą. Dėkoju už bendradarbiavimą ir skirtą laiką.

Tomas Plėta
Vadybos katedra
Verslo vadybos fakultetas
Vilniaus Gedimino technikos universitetas

Eksperto eilės Nr.: Apklausos data: Apklausos laikas:

Parengiamoji dalis ekspertams:

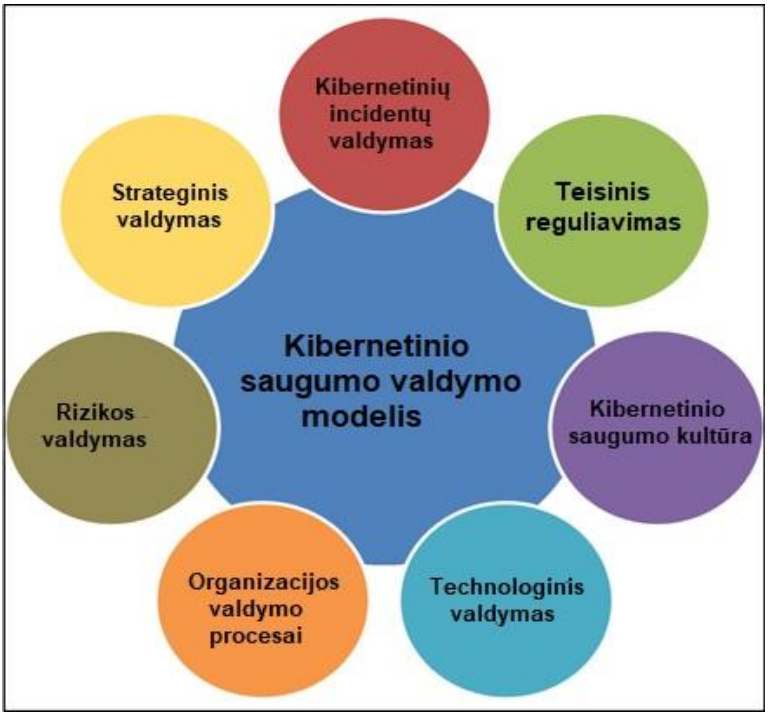
P1 pav. parodyta kritinės infrastruktūros objektų kibernetinio saugumo valdymo modelio konceptuali schema, apimanti septynias kibernetinio saugumo valdymo komponentus. Jei modelis būtų taikomas, teoriškai galėtų padėti užtikrinti visų tipų kritinės infrastruktūros objektų kibernetinį saugumą.

Norint visapusiškai pasiekti kibernetinį saugumą, reikia atsižvelgti į tai, kad modelis buvo sukurtas taikyti visų tipų kritinėms infrastruktūroms, o tai reiškia, kad modelio suskirstymas ir pagrindinės problemos yra bendros visų tipų kritinėms infrastruktūroms. Dėl šios priežasties pateiktas modelis gali būti integruotas su jau esamais valdymo planais, būdingais kritinės infrastruktūros tipui.

Autorius puikiai suvokia, kad realiai pasiekti visišką kibernetinį saugumą neįmanoma, tačiau, norint pasiekti kuo geresnių rezultatų, taip pat būtina atsižvelgti į modelį kaip taikytiną visuose trijuose kibernetinio saugumo valdymo kūrimo etapuose: pasirengimo, taikymo ir atkūrimo fazėse. Modelis neturi pradinio vaidmens kuriant kibernetinio saugumo valdymą, tačiau būtina jį nuolat atnaujinti ir naudoti stebėjimo bei tobulinimo tikslais. Tačiau skirtingus komponentus galima įgyvendinti ir savarankiškai, nors tai tikriausiai reikštų, kad galutinis modelio veikimas būtų ne toks išsamus.

Apibendrinant kibernetinio saugumo valdymo modelio kūrimo prielaidas, manoma, kad visų konceptualaus kibernetinio saugumo valdymo modelio komponentų pirmasis (pradinis) lygis yra susijęs su organizacijos gebėjimu aiškiai identifikuoti, kokie kibernetinio saugumo iššūkiai ir problemos egzistuoja organizacijoje. Antrasis kibernetinio saugumo valdymo modelio lygis orientuotas į

konkrečių veiksmų planų, skirtų organizaciniams pokyčiams, įgyvendinimą, planai leidžia organizacijai pagerinti kibernetinį saugumą kiekviename komponente. Trečiasis skirtas kibernetinio saugumo valdymo modeliui harmonizuoti ir visiems komponentams integruoti, siekiant užtikrinti visapusišką kibernetinį saugumą ir jo valdymą organizacijoje.



A1 pav. Kibernetinio saugumo valdymo modelis
Fig. A1 . Cyber security management model

Modelio autorių pateikta anketa turi tikslą apibrėžti visapusį projekto vertinimą, o pagrindinis tyrimo klausimas (PK) gali būti toks:

PK: ***Kaip vertinate valdymo modelį kritinės infrastruktūros objektų saugumo kontekste, atsižvelgiant į kategoriją ir struktūros pasirinkimą?***

Atsižvelgdami į tai, kad toks klausimas atveria platų galimų atsakymų spektrą, autoriai manė, kad tinkamiau parengti keletą klausimų, susijusių su kiekvieno komponento vertinimu, kad gautų išsamesnį atsakymą nustatant galimą komponentų „reitingą“. Tokiu būdu modelio modifikavimo procesas, pagrįstas grįžtamuoju ryšiu, būtų greitesnis ir tiesiogiškesnis.

Literatūra:

Autoriaus atliktoje analizėje buvo atsižvelgta į pateiktą modelį ir ypač buvo įvertintas jų veikimas kritinės infrastruktūros objektų saugumo požiūriu. Siekdamas sukurti efektyvų modelį, analizės metu autorius svarstė galimus kitų modelių elementus, kurie galėtų būti integruoti su naujai sukurtu modeliu. Analizė atskleidė keletą tokių elementų, kuriuos reikia integruoti į modelį:

1. *Procesai,* kuriuos galima apibūdinti kaip visumą praktikų ir veiklų, kurios iš viso užtikrina visišką kibernetinį saugumą. Bendras apibrėžimas paimtas iš COBIT 2019 protokole vartojamo apibrėžimo, kuriame kiekvienam procesui skiriama viena ar daugiau veiklos rūšių (ISACA, 2018).
2. *Vaidmenys ir pareigos*: šis elementas yra labai naudingas organizaciniams valdymo aspektams, nes jo tikslas yra apibrėžti ir klasifikuoti vaidmenis įmonėje, įskaitant trumpą vaidmens prioritetų aprašymą. Kuriant tokį elementą taip pat reikėtų vadovautis COBIT 2019 sistemos siūlomomis direktyvomis, nors būtų naudinga sukurti specifinį, visą laiką aktyvų vaidmenį, kuris reikalingas informuoti apie kibernetinį incidentą ir į kurį organizacijos nariai galėtų kreiptis poreikio metu. Panašiai kaip E-ISAC/NCCIC ataskaitų teikimo koordinavimo vaidmuo, minimas NERC sistemoje (NERC, 2019).
3. *Technologijų valdymas* apima labiau techninius valdymo aspektus. Atsižvelgiant į tai, kad modelis yra skirtas įvairių tipų CEI, šis elementas bus konkrečiau skirtas techninių komponentų, naudojamų įmonės saugumui ir klasifikavimui.
4. *Politika* yra vienas iš novatyviausių valdymo modeliavimo aspektų. Kaip jau minėta, šis modelis taikomas bet kokiam CEI tipui, o kad veiktų, konkretesni saugumo valdymo aspektai kiekvienam CEI nėra paminėti.
5. *Pažeidžiamumas* užbaigia organizacinio valdymo aspektus. Kartu su įmonėje naudojamais procesais ir technikomis, svarbu įvertinti ir galimas sistemos silpnąsias vietas, testuojant ir klasifikuojant sistemos pažeidžiamumą.

KLAUSIMYNAS

Iš anksto dėkojame už pagalbą ir laiką.

1. Nurodykite savo vadovavimo patirtį šioje (arba ankstesnėje) įmonėje:

a) Iki 3 metų
b) Nuo 3 iki 5 metų
c) Nuo 6 iki 10 metų
d) Daugiau negu 10 metų

2. Ar sutinkate, kad technologinės plėtros strateginio valdymo įrankiai turi didelę įtaką energijos vartojimo efektyvumui ir kibernetiniam (informaciniam) saugumui:

a) Taip
b) Ne
c) Nežinau

3. Suskirstykite pagal svarbą nuo 1 iki 5 (kur 1 yra svarbus, o 5 – nesvarbu) kibernetinių incidentų valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio valdymo, organizacijos valdymo, rizikos valdymo ir strategijos valdymo komponentus.

Rizikos valdymas *Rizikos valdymo komponentas apibūdina sistemą, kuriai taikomas modelis.*	**Vertinimas**	**Ką reikia tobulinti?**
Koks yra kibernetinio saugumo valdymo fenomeno poveikis rizikos valdymo komponentui?		
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir panaudojimas organizacijoje, jos valdymo sistemoje ir tarp organizacijos narių turi įtakos pačios organizacijos kibernetinio saugumo užtikrinimo procesui?		
Kokia kibernetinio saugumo komponento reikšmė organizacijos (naujai įgyvendinamuose) projektuose ir kaip galima pagerinti kibernetinio saugumo komponento integravimą į organizacijos veiklą?		
Ar norint užtikrinti kibernetinio saugumo įgyvendinimą organizacijoje, būtina peržiūrėti ir koreguoti organizacijos valdymo procesus?		
Ar nurodyti veiksmai gali patobulinti rizikos valdymo procesus kibernetinio saugumo kontekste: • organizacijos siekiamų tikslų nustatymas; • organizacijos saugumo sistemos sudedamųjų elementų nustatymas; • organizacijos aplinkos ypatybių nustatymas; • kibernetinio saugumo fenomeno integravimas į organizacijos verslo procesus; • tolesni žingsniai.		

Teisinis reguliavimas *Teisinis valdymas, be jokios abejonės, yra įdomus modelio papildymas, nes suteikia galimybę į modelį įtraukti jau egzistuojančią sistemą. Kadangi modelis tinkamas taikyti kiekvienam CI tipui, tokia kategorija reikalinga, kad kiekvienam modeliui būtų pridėtos konkretesnės savybės ir rekomendacijos.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar yra procesai, kurie apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje? Įvertinkite jų svarbumą. Kokie veiksniai, Jūsų nuomone, apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje?		
Kaip Jūs vertinate teisinio reguliavimo svarbumą kibernetinio saugumo srityje saugumo tikslams pasiekti?		
Kaip Jūs vertinate reguliavimo procesų įtaką organizacijos kibernetiniam saugumui? Dėl kokių priežasčių reikia nagrinėti valdymo sritį organizacijoje kibernetinio saugumo kontekste? Ar reguliavimo procesai gali turėti įtakos organizacijos kibernetiniam saugumui?		
Kaip Jūs vertinate vidinės ir išorinės aplinkos teisinio valdymo įtaką organizacijos kibernetinio saugumo valdymo įgyvendinimui? Kuri organizacinė aplinka (išorinė ar vidinė) yra svarbesnė jas svarstant kibernetinio saugumo reguliavimo kontekste?		
Ar svarbūs teisinio reguliavimo aspektai organizacijos saugumo tikslams pasiekti? Kuo teisinio reguliavimo aspektas naudingas organizacijos saugumo tikslais?		
Ar nurodyti veiksmai gali padėti patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste? Kokių veiksmų organizacija turi imtis, kad patobulintų teisinio valdymo aspektus kibernetinio saugumo reiškinio kontekste: • esamos teisinės bazės reikalavimų ir trūkumų nustatymas; • organizacijai reikalingų teisinių ypatumų nustatymas; • modelyje siūlomų korekcinių priemonių įgyvendinimas; • papildomų, konkrečių procedūrų, susijusių su organizacijos saugumo poreikiais, nustatymas; • pastarųjų integravimas į esamą modelį;		

• organizacijos įgyvendintų priemonių ir veiklos auditas; • teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • tolesni žingsniai.		

Kibernetinio saugumo kultūra *Kibernetinio saugumo kultūros komponente nagrinėjami informaciniai kibernetinio saugumo aspektai, taip pat „žmogiškoji“ sistemos dalis. Šios kategorijos prioritetas yra nustatyti darbuotojų saugą, didinti sąmoningumą ir mokyti darbuotojus suprasti kibernetinio saugumo valdymo pagrindus.*	**Vertinimas**	**Ką reikia tobulinti?**
Įvertinkite kibernetinio saugumo kultūros svarbumą? Kaip galima apibūdinti „kibernetinio saugumo kultūrą“? (Ką reiškia „kibernetinio saugumo kultūra“?)		
Ar kibernetinio saugumo kultūros kūrimas yra svarbus? Įvertinkite. Kam kurti kibernetinio saugumo kultūrą, o ne, tarkime, didinti žmogaus informatyvumą (sąmoningumą)?		
Ar svarbu skaidyti kibernetinio saugumo kultūrą į elementus? Kokie elementai sudaro kibernetinio saugumo kultūrą?		
Ar kibernetinio saugumo kultūros mokymai yra svarbūs? Kokie kibernetinio saugumo kultūros mokymo būdai ir metodai, jūsų nuomone, yra efektyviausi?		
Ar organizacijos kibernetinio saugumo kultūros aspektai turėtų būti taikomi ir organizacijos partneriams bei paslaugų teikėjams?		
Ar nurodytų veiksmų galima imtis organizacijoje, kad būtų pašalintas žmogiškojo faktoriaus ir kibernetinio saugumo kultūros fenomeno poveikis organizacijoje. Kokių veiksmų reikia imtis? • nustatyti kibernetinio saugumo suvokimo problemas; • pateikti kibernetinio saugumo supratimo gerinimo metodus ir būdus; • stebėti kibernetinio saugumo kultūros pokyčius; • tolesni žingsniai.		

Technologijų valdymas *Technologijų valdymas yra dar vienas svarbus modelio komponentas, kuris lemia programinės įrangos, telekomunikacijų ir tinklo kibernetinį saugumą. Organizacijos valdymo komponente buvo nagrinėjamas fizinis infrastruktūros saugumas, o šiuo atveju dėmesys skiriamas naudojamos IT aplinkos kokybei, diegiant įvairius kibernetinio saugumo metodus, kurie skirsis priklausomai nuo programinės įrangos ir modelio infrastruktūros tipo.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios? Įvertinkite. Kokios technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje?		
Ar įmanoma užtikrinti visišką kibernetinį saugumą naudojant techninę ir programinę įrangą?		
Ar svarbu vertinti technologinius kibernetinio saugumo trūkumus? Kokie galėtų būti technologinio kibernetinio saugumo trūkumai?		
Ar technologijų valdymo priemonės turi būti technologiškai neutralios?		
Ar nurodyti veiksmai užtikrintų tinkamą technologinio kibernetinio saugumo įgyvendinimą? Kokių veiksmų turi imtis organizacija? • naudojamų technologinių priemonių nustatymas; • technologinių priemonių parinkimas ir diegimas; • technologinių priemonių naudojimo poveikio kibernetiniam saugumui įvertinimas; • tolesni žingsniai.		

Kibernetinių incidentų valdymas *Kibernetinių incidentų valdymas yra orientuotas į efektyvų valdymo planų, kurie būtų taikomi kritinėje situacijoje ir apimantys visus įvykio aspektus, nuo pasiruošimo iki identifikavimo ir tvarkymo, kūrimą. Komponente taip pat pateikta informaciją apie kitus su kibernetiniais nesusijusius padarinius, tokius kaip fiziniai incidentai ir saugos valdymas ir planavimas.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar saugos valdymo procesas yra aktualus organizacijai kibernetinio saugumo kontekste?		

Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti saugumo valdymo procesus? Kokių veiksmų turi imtis organizacija? • nustatyti saugumo valdymo procesus organizacijoje; • klasifikuoti galimas rizikas ir atlikti jos vertinimą; • parengti saugumo valdymo planus ir taisykles; • tolesni žingsniai.		

Strateginis valdymas *Strategijos valdymas daugiausia susijęs su metodais, tokiais kaip skaičiavimas, taip pat su kitų esamų kritinės energetinės infrastruktūros CEI aptikimu ir susiję su modeliu.*	**Vertinimas**	**Ką reikia tobulinti?**
Kaip strategijos valdymas yra susijęs su kibernetinio saugumo valdymo sprendimais?	3	
Kiek svarbu sukurti modelį, apskaičiuojantį didžiausio nacionalinio poveikio laipsnį gedimo ar atakos atveju?	3	
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti organizacijos valdymo procesus? Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus? • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.		

Organizacijos valdymas *Organizacinio valdymo komponentas suteikia supratimą apie gaires, kurios turėtų būti naudojamos tiesiogiai reaguojant į kibernetines atakas. Šiame komponente daugiausia dėmesio skiriama atakos pasekmėms, būtent avarinio atkūrimo planavimui, kuris apima bendrą instrukciją, kaip elgtis pagal įvairius scenarijus po kibernetinės atakos. Be to, jame taip pat atkreipiamas dėmesys į operatyvinį saugumą, paaiškinant įvairius metodus, taikomus kibernetinių atakų prevencijai ir reagavimui į juos.*	**Vertinimas**	**Ką reikia tobulinti?**

Ar organizacijos valdymas yra naudingas kibernetinio saugumo valdymo požiūriu?		
Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus: • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius organizacinius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.		

4. Įvertinkite modelio komponentus nuo 1 iki 5, kur 1 – blogai, reikia tobulinti, 5 – nieko daryti nereikia.

Modelio komponentai	**Vertinimas**
Rizikos valdymas	
Teisinis reguliavimas	
Kibernetinio saugumo kultūra	
Technologijų valdymas	
Kibernetinių incidentų valdymas	
Strateginis valdymas	
Organizacijos valdymas	

Papildomos ekspertų pastabos arba nuomonė:

B priedas. Ekspertų vertinimo rezultatai

KLAUSIMYNAS (E1)

Iš anksto dėkojame už pagalbą ir laiką.

4. Nurodykite savo vadovavimo patirtį šioje (arba ankstesnėje) įmonėje:
   a) Iki 3 metų
   b) Nuo 3 iki 5 metų
   c) Nuo 6 iki 10 metų
   d) Daugiau negu 10 metų
5. Ar sutinkate, kad technologinės plėtros strateginio valdymo įrankiai turi didelę įtaką energijos vartojimo efektyvumui ir kibernetiniam (informaciniam) saugumui:
   a) Taip
   b) Ne
   c) Nežinau
6. Suskirstykite pagal svarbą nuo 1 iki 5 (kur 1 yra svarbus, o 5 – nesvarbu) kibernetinių incidentų valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio valdymo, organizacijos valdymo, rizikos valdymo ir strategijos valdymo komponentus.

Rizikos valdymas *Rizikos valdymo komponentas apibūdina sistemą, kuriai taikomas modelis.*	**Vertinimas**	**Ką reikia tobulinti?**
Koks yra kibernetinio saugumo valdymo fenomeno poveikis rizikos valdymo komponentui?	1	Žinodami savo išteklius, supraskite, ką su jais galite padaryti arba kaip juos apsaugoti.
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir panaudojimas organizacijoje, jos valdymo sistemoje ir tarp organizacijos narių turi įtakos pačios organizacijos kibernetinio saugumo užtikrinimo procesui?	1	Taip
Kokia kibernetinio saugumo komponento reikšmė organizacijos (naujai įgyvendinamuose) projektuose ir kaip galima pagerinti kibernetinio saugumo	1	Padarykite taip, kad CS suprastų pagrindinę projekto dalį, o ne paskutinį projekto įgyvendinimo žingsnį.

Ar norint užtikrinti kibernetinio saugumo įgyvendinimą organizacijoje, būtina peržiūrėti ir koreguoti organizacijos valdymo procesus?	1	Taip. Manau, kad pagrindinė užduotis yra padaryti organizaciją saugesnę.
Ar nurodyti veiksmai gali patobulinti rizikos valdymo procesus kibernetinio saugumo kontekste: • organizacijos siekiamų tikslų nustatymas; • organizacijos saugumo sistemos sudedamųjų elementų nustatymas; • organizacijos aplinkos ypatybių nustatymas; • kibernetinio saugumo fenomeno integravimas į organizacijos verslo procesus; • tolesni žingsniai.	1	Visi etapai plius dar vienas: organizacijos valdymo sistemos pritaikymas siekiant suprasti organizacijos kibernetinį saugumą

Teisinis reguliavimas *Teisinis valdymas, be jokios abejonės, yra įdomus modelio papildymas, nes suteikia galimybę į modelį įtraukti jau egzistuojančią sistemą. Kadangi modelis tinkamas taikyti kiekvienam CI tipui, tokia kategorija reikalinga, kad kiekvienam modeliui būtų pridėtos konkretesnės savybės ir rekomendacijos.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar yra procesai, kurie apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje? Įvertinkite jų svarbumą. Kokie veiksniai, Jūsų nuomone, apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje?	2	Tarptautinė teisė ne visada pereina į valstybės teisę.
Kaip Jūs vertinate teisinio reguliavimo svarbumą kibernetinio saugumo srityje saugumo tikslams pasiekti? Ar toks komponentas reikalingas?	1	Taip, reikalingas
Kaip Jūs vertinate reguliavimo procesų įtaką organizacijos kibernetiniam saugumui? Dėl kokių priežasčių reikia nagrinėti valdymo sritį	2	Turite laikytis standartų ir įstatymų. Norint įteisinti visus organizacijos teisės

organizacijoje kibernetinio saugumo kontekste? Ar reguliavimo procesai gali turėti įtakos organizacijos kibernetiniam saugumui?		aktus, turi būti taikomas reguliavimo procesas.
Kaip Jūs vertinate vidinės ir išorinės aplinkos teisinio valdymo įtaką organizacijos kibernetinio saugumo valdymo įgyvendinimui? Kuri organizacinė aplinka (išorinė ar vidinė) yra svarbesnė jas svarstant kibernetinio saugumo reguliavimo kontekste?	2	Abu yra svarbūs ir į juos reikia atsižvelgti tobulinant organizacijos kibernetinį saugumą. Sunku vienareikšmiškai pasakyti, kuris iš jų yra svarbesnis.
Ar svarbūs teisinio reguliavimo aspektai organizacijos saugumo tikslams pasiekti? Kuo teisinio reguliavimo aspektas naudingas organizacijos saugumo tikslais?	2	Aiškūs teisės aktai leidžia suprasti visus vaidmenis ir atsakomybę.
Ar nurodyti veiksmai gali patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste? Kokių veiksmų organizacija turi imtis, kad patobulintų teisinio valdymo aspektus kibernetinio saugumo reiškinio kontekste: • esamos teisinės bazės reikalavimų ir trūkumų nustatymas; • organizacijai reikalingų teisinių ypatumų nustatymas; • modelyje siūlomų korekcinių priemonių įgyvendinimas; • papildomų, konkrečių procedūrų, susijusių su organizacijos saugumo poreikiais, nustatymas; • minėtų veiksnių integravimas į esamą modelį; • organizacijos įgyvendintų priemonių ir veiklos auditas; • teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • tolesni žingsniai.	1	Pateikti žingsniai yra darbo modelis. Tiesiog reikia įvertinti pažangą.

Kibernetinio saugumo kultūra *Kibernetinio saugumo kultūros komponente nagrinėjami informaciniai kibernetinio saugumo aspektai, taip pat „žmogiškoji“ sistemos dalis. Šios kategorijos prioritetas yra nustatyti darbuotojų saugą, didinti sąmoningumą ir mokyti darbuotojus suprasti kibernetinio saugumo valdymo pagrindus.*	**Vertinimas**	**Ką reikia tobulinti?**
Įvertinkite kibernetinio saugumo kultūros svarbumą? Kaip galima apibūdinti „kibernetinio saugumo kultūrą“? (Ką reiškia „kibernetinio saugumo kultūra“?)	1	Žmogiškasis faktorius yra bene pavojingiausias kibernetiniam saugumui
Ar kibernetinio saugumo kultūros kūrimas yra svarbus? Įvertinkite. Kam kurti kibernetinio saugumo kultūrą, o ne, tarkime, didinti žmogaus informatyvumą (sąmoningumą)?	1	Manau, kad tai tas pats. Informuokite savo darbuotojus apie kibernetinį saugumą ir jūs žengsite pirmuosius žingsnius kibernetinio saugumo kultūros didinimo link.
Ar svarbu skaidyti kibernetinio saugumo kultūrą į elementus? Kokie elementai sudaro kibernetinio saugumo kultūrą?	2	Taip. Mokymai, testavimas, seminarai, informacijos sklaida organizacijos nariams.
Ar kibernetinio saugumo kultūros mokymai yra svarbūs? Kokie kibernetinio saugumo kultūros mokymo būdai ir metodai, jūsų nuomone, yra efektyviausi?	1	Informacijos skleidimas tarp darbuotojų ir kibernetinių atakų imitavimas
Ar organizacijos kibernetinio saugumo kultūros aspektai turėtų būti taikomi ir organizacijos partneriams bei paslaugų teikėjams?	1	Taip. Dėl tikrumo. Pasakyk man, kas tavo draugai, ir aš pasakysiu, kas tu.
Ar nurodytų veiksmų galima imtis organizacijoje, siekiant pašalinti žmogiškojo faktoriaus ir kibernetinio saugumo kultūros fenomeno poveikį organizacijoje. Kokių veiksmų reikia imtis? • nustatyti kibernetinio saugumo suvokimo problemas;	2	Patikrinkite savo narius ir įvertinkite pakeitimus, kurie parodys, ar kažkas negerai.

• pateikti kibernetinio saugumo supratimo gerinimo metodus ir būdus; • stebėti kibernetinio saugumo kultūros pokyčius; • tolesni žingsniai.		

Technologijų valdymas *Technologijų valdymas yra dar vienas svarbus modelio komponentas, kuris lemia programinės įrangos, telekomunikacijų ir tinklo kibernetinį saugumą. Organizacijos valdymo komponente buvo nagrinėjamas fizinis infrastruktūros saugumas, o šiuo atveju dėmesys skiriamas naudojamos IT aplinkos kokybei, diegiant įvairius kibernetinio saugumo metodus, kurie skirsis priklausomai nuo programinės įrangos ir modelio infrastruktūros tipo.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios? Įvertinkite. Kokios technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje?	2	Stenkitės galvoti apie koncepciją, o ne apie dabartinius produktus. Pabandykite įsivaizduoti, kaip viskas turėtų veikti, tada pabandykite rasti tinkamą aplinką.
Ar įmanoma užtikrinti visišką kibernetinį saugumą naudojant techninę ir programinę įrangą?	2	Ne. Jei tiesiog įdiegsite programinę ar aparatinę įrangą nežinodami, kaip ji veiks, tai bus tik pinigų švaistymas.
Ar svarbu vertinti technologinius kibernetinio saugumo trūkumus? Kokie galėtų būti technologinio kibernetinio saugumo trūkumai?	2	Dvi skirtingos programos atlieka tą patį darbą. Galite išleisti daug pinigų, bet niekada nepasieksite rezultato.
Ar technologijų valdymo priemonės turi būti technologiškai neutralios?	1	Dėl tikrumo. Rasite tą, kuris atitiks jūsų poreikius.

Ar nurodyti veiksmai užtikrintų tinkamą technologinio kibernetinio saugumo įgyvendinimą? Kokių veiksmų turi imtis organizacija? • naudojamų technologinių priemonių nustatymas; • technologinių priemonių parinkimas ir diegimas; • technologinių priemonių naudojimo poveikio kibernetiniam saugumui įvertinimas; • tolesni žingsniai.	2	Procesų vertinimas ir stebėjimas.

Kibernetinių incidentų valdymas *Kibernetinių incidentų valdymas yra orientuotas į efektyvų valdymo planų, kurie būtų taikomi kritinėje situacijoje ir apimantys visus įvykio aspektus, nuo pasiruošimo iki identifikavimo ir tvarkymo, kūrimą. Komponente taip pat pateikta informaciją apie kitus su kibernetiniais padariniais nesusijusius padarinius, tokius kaip fiziniai incidentai ir saugos valdymas ir planavimas.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar saugos valdymo procesas yra aktualus organizacijai kibernetinio saugumo kontekste?	1	Dėl tikrumo. Tai gali išgelbėti jus nuo didelių nuostolių.
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti saugumo valdymo procesus? Kokių veiksmų turi imtis organizacija? • nustatyti saugumo valdymo procesus organizacijoje; • klasifikuoti galimas rizikas ir atlikti jų vertinimą; • parengti saugumo valdymo planus ir taisykles; • tolesni žingsniai.	1	Prieš kurdami planus suraskite arba pabandykite numatyti kibernetinio saugumo spragas. Planai turi būti parengti žinomoms kibernetinio saugumo spragoms, planai reikalingi ir papildomoms situacijoms. Taip pat išmatuokite efektyvumą.

Strateginis valdymas *Strategijos valdymas daugiausia susijęs su metodais, tokiais kaip skaičiavimas, taip pat su kitų esamų kritinės energetinės infrastruktūros CEI aptikimu ir susiję su modeliu.*	**Vertinimas**	**Ką reikia tobulinti?**
Kaip strategijos valdymas yra susijęs su kibernetinio saugumo valdymo sprendimais?	1	Pirmiausia turite įsivaizduoti, kaip elgsitės, o tada pabandykite veikti. Jei neturite trumpalaikės ar ilgalaikės strategijos, galite gaišti laiką ir pinigus ir niekada nerasti teisingo kelio ar nepriimti teisingų sprendimų.
Kiek svarbu sukurti modelį, apskaičiuojantį didžiausio nacionalinio poveikio laipsnį gedimo ar atakos atveju?	1	Jei naudositės šiuo modeliu, galėsite numatyti blogas situacijas.
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti organizacijos valdymo procesus? Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus? • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	2	Pažangos įvertinimas ir aiškus pasiektų etapų supratimas.

Organizacijos valdymas *Organizacinio valdymo komponentas suteikia supratimą apie gaires, kurios turėtų būti naudojamos tiesiogiai reaguojant į kibernetines atakas. Šiame komponente daugiausia dėmesio skiriama atakos pasekmėms, būtent avarinio atkūrimo planavimui,*	**Vertinimas**	**Ką reikia tobulinti?**

kuris apima bendrą instrukciją, kaip elgtis įvairiuose scenarijuose po kibernetinės atakos. Be to, jame taip pat atkreipiamas dėmesys į operatyvinį saugumą, kuriame paaiškinami įvairūs metodai, taikomi kibernetinių atakų prevencijai ir reagavimui į jas.		
Ar organizacijos valdymas yra naudingas kibernetinio saugumo valdymo požiūriu?	1	Taip. Aiškios instrukcijos pašalina PANIKOS veiksnį.
Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus: • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius organizacinius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	2	Apibūdinkite „mūšio ritmą“ kritinių situacijų metu, kol bus nustatytas normalus veikimas.

4. Įvertinkite modelio komponentus nuo 1 iki 5, kur 1 – blogai, reikia tobulinti, 5 – nieko daryti nereikia.

Modelio komponentai	Vertinimas
Rizikos valdymas	2
Teisinis reguliavimas	1
Kibernetinio saugumo kultūra	1
Technologijų valdymas	2
Kibernetinių incidentų valdymas	1
Strateginis valdymas	1
Organizacijos valdymas	2

Papildomos ekspertų pastabos arba nuomonė:
Kibernetinis saugumas yra daugiau nei technologija, teisė, kultūra ar bet kas kita. Tai reiškinys, sujungiantis technologijas, socialinius aspektus, komunikacijos ir valdymo problemas. Būtent tai sujungia visus mokslus ir suteikia mums saugumo bei pasitikėjimo naudojamomis technologijomis.

KLAUSIMYNAS (E2)

Iš anksto dėkojame už pagalbą ir laiką.

1. Nurodykite savo vadovavimo patirtį šioje (arba ankstesnėje) įmonėje:
   a) Iki 3 metų
   b) Nuo 3 iki 5 metų
   c) Nuo 6 iki 10 metų
   d) Daugiau negu 10 metų
2. Ar sutinkate, kad technologinės plėtros strateginio valdymo įrankiai turi didelę įtaką energijos vartojimo efektyvumui ir kibernetiniam (informaciniam) saugumui:
   a) Taip
   b) Ne
   c) Nežinau
3. Suskirstykite pagal svarbą nuo 1 iki 5 (kur 1 yra svarbus, o 5 – nesvarbu) kibernetinių incidentų valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio valdymo, organizacijos valdymo, rizikos valdymo ir strategijos valdymo komponentus.

Rizikos valdymas *Rizikos valdymo komponentas apibūdina sistemą, kuriai taikomas modelis.*	**Vertinimas**	**Ką reikia tobulinti?**
Koks yra kibernetinio saugumo valdymo fenomeno poveikis rizikos valdymo komponentui?	1	Neįmanoma užtikrinti kibernetinio saugumo be tinkamo resursų valdymo (žmonių, laiko, pinigų).
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir panaudojimas organizacijoje, jos valdymo sistemoje ir tarp organizacijos narių turi įtakos pačios organizacijos kibernetinio saugumo užtikrinimo procesui?	3	Suvokimas yra susijęs su organizacijos kultūros elementu, nors reikia atsižvelgti į visus verslo modelio elementus, įskaitant santykius, siekiant užtikrinti informacijos saugumą (organizaciją, procesus, žmones ir technologijas).
Kokia kibernetinio saugumo komponento reikšmė organizacijos (naujai įgyvendinamuose) projektuose ir kaip galima pagerinti kibernetinio saugumo komponento integravimą į organizacijos veiklą?	2	Tai padės visapusiškai užtikrinti organizacijų kibernetinį saugumą ir rizikos valdymą. Jį būtų galima patobulinti nustatant pokyčių valdymo procedūras, kurias būtų galima išmatuoti ir

		kontroliuoti pagal verslo poreikius.
Ar norint užtikrinti kibernetinio saugumo įgyvendinimą organizacijoje, būtina peržiūrėti ir koreguoti organizacijos valdymo procesus?	4	Kibernetinis saugumas turi palaikyti organizacijos valdymo procesus ir verslo poreikius.
Ar nurodyti veiksmai gali padėti patobulinti rizikos valdymo procesus kibernetinio saugumo kontekste: • organizacijos siekiamų tikslų nustatymas; • organizacijos saugumo sistemos sudedamųjų elementų nustatymas; • organizacijos aplinkos ypatybių nustatymas; • kibernetinio saugumo fenomeno integravimas į organizacijos verslo procesus; • tolesni žingsniai.	1	Rizikos valdymas turėtų būti organizuojamas kaip kibernetinio saugumo strategijos įgyvendinimo programos dalis: ✓ Tikslai ✓ CSF, KPI ✓ Laikas ✓ Žmonės ✓ Pinigai

Teisinis reguliavimas *Teisinis valdymas, be jokios abejonės, yra įdomus modelio papildymas, nes suteikia galimybę į modelį įtraukti jau egzistuojančią sistemą. Kadangi modelis tinkamas taikyti kiekvienam CI tipui, tokia kategorija reikalinga, kad kiekvienam modeliui būtų pridėtos konkretesnės savybės ir rekomendacijos.*	**Vertinimas**	**Ką reikia patobulinti?**
Ar yra procesai, kurie apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje? Įvertinkite jų svarbumą. Kokie veiksniai, Jūsų nuomone, apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje?	4	Kenkėjiškos veiklos priskyrimas.
Kaip Jūs vertinate teisinio reguliavimo svarbumą kibernetinio saugumo srityje saugumo tikslams pasiekti? Ar toks komponentas reikalingas?	3	Organizaciniu lygmeniu – taip, tarptautiniu lygmeniu;

		– tai turėtų būti kitos atgrasymo priemonės ir struktūriniai elementai.
Kaip Jūs vertinate reguliavimo procesų įtaką organizacijos kibernetiniam saugumui? Dėl kokių priežasčių reikia nagrinėti valdymo sritį organizacijoje kibernetinio saugumo kontekste? Ar reguliavimo procesai gali turėti įtakos organizacijos kibernetiniam saugumui?	3	Išoriniai reglamentai turėtų būti vertinami rizikos valdymo požiūriu. Pagrindinis organizacijos valdymo struktūros tyrimo tikslas – suprasti tikruosius verslo poreikius.
Kaip Jūs vertinate vidinės ir išorinės aplinkos teisinio valdymo įtaką organizacijos kibernetinio saugumo valdymo įgyvendinimui? Kuri organizacinė aplinka (išorinė ar vidinė) yra svarbesnė jas svarstant kibernetinio saugumo reguliavimo kontekste?	3	Vidinis reguliavimas turėtų būti rizikingas, pagrįstas išoriniais veiksniais. Išorinių taisyklių laikymasis neturėtų viršyti organizacijos verslo poreikių.
Ar svarbūs teisinio reguliavimo aspektai organizacijos saugumo tikslams pasiekti? Kuo teisinio reguliavimo aspektas naudingas organizacijos saugumo tikslais?	3	Teisinė pagalba vadovybei atitikties klausimais ir galimomis nuobaudomis (pavyzdžiui, GDPR)
Ar nurodyti veiksmai gali patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste? Kokių veiksmų organizacija turi imtis, kad patobulintų teisinio valdymo aspektus kibernetinio saugumo reiškinio kontekste: • esamos teisinės bazės reikalavimų ir trūkumų nustatymas; • organizacijai reikalingų teisinių ypatumų nustatymas; • modelyje siūlomų korekcinių priemonių įgyvendinimas; • papildomų, konkrečių procedūrų, susijusių su organizacijos saugumo poreikiais, nustatymas; • minėtų veiksnių integravimas į esamą modelį; • organizacijos įgyvendintų priemonių ir veiklos auditas;	2	Pirmiausia reikia atlikti spragų analizę, tada rizikos analizę, o tada – mažinimo priemones.

• teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • tolesni žingsniai.		

Kibernetinio saugumo kultūra *Kibernetinio saugumo kultūros komponente nagrinėjami informaciniai kibernetinio saugumo aspektai, taip pat „žmogiškoji“ sistemos dalis. Šios kategorijos prioritetas yra nustatyti darbuotojų saugą, didinti sąmoningumą ir mokyti darbuotojus suprasti kibernetinio saugumo valdymo pagrindus.*	**Vertinimas**	**Ką reikia tobulinti?**
Įvertinkite kibernetinio saugumo kultūros svarbumą? Kaip galima apibūdinti „kibernetinio saugumo kultūrą“? (Ką reiškia „kibernetinio saugumo kultūra“?)	3	Tai žmonių ir organizacijos elementų santykis BMIS – bendri įsitikinimai ir elgesio supratimas, kuriuo siekiama organizacijos ar asmeninių tikslų.
Ar kibernetinio saugumo kultūros kūrimas yra svarbus? Įvertinkite. Kam kurti kibernetinio saugumo kultūrą, o ne, tarkime, didinti žmogaus informatyvumą (sąmoningumą)?	2	Kultūra suteikia galimybę keisti elgesį, kai informacijos turinys suteikia supratimą apie galimas grėsmes.
Ar svarbu skaidyti kibernetinio saugumo kultūrą į elementus? Kokie elementai sudaro kibernetinio saugumo kultūrą?	3	Žmonės, vadovavimas, normos.
Ar kibernetinio saugumo kultūros mokymai yra svarbus? Kokie kibernetinio saugumo kultūros mokymo būdai ir metodai, jūsų nuomone, yra efektyviausi?	2	Pavyzdys per lyderystę, kryptingą mokymąsi, atskaitomybę.
Ar organizacijos kibernetinio saugumo kultūros aspektai turėtų būti taikomi ir organizacijos partneriams bei paslaugų teikėjams?	4	Tam tikru mastu tai galima pasiekti naudojant SLA, nors bus sunku bendrauti.

Ar nurodytų veiksmų galima imtis organizacijoje, kad būtų pašalintas žmogiškojo faktoriaus ir kibernetinio saugumo kultūros fenomeno poveikis organizacijoje. Kokių veiksmų reikia imtis?: • nustatyti kibernetinio saugumo suvokimo problemas; • pateikti kibernetinio saugumo supratimo gerinimo metodus ir būdus; • stebėti kibernetinio saugumo kultūros pokyčius; • tolesni žingsniai.	2	Atranka, mokymas, vaidmenimis pagrįsta prieiga prie informacijos / sistemų.

Technologijų valdymas *Technologijų valdymas yra dar vienas svarbus modelio komponentas, kuris lemia programinės įrangos, telekomunikacijų ir tinklo kibernetinį saugumą. Organizacijos valdymo komponente buvo nagrinėjamas fizinis infrastruktūros saugumas, o šiuo atveju dėmesys skiriamas naudojamos IT aplinkos kokybei, diegiant įvairius kibernetinio saugumo metodus, kurie skirsis priklausomai nuo programinės įrangos ir modelio infrastruktūros tipo.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios? Įvertinkite. Kokios technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje?	1	Tokių priemonių, kurios labai sumažina žmogiškųjų klaidų faktorių.
Ar įmanoma užtikrinti visišką kibernetinį saugumą naudojant techninę ir programinę įrangą?	5	Ne, nes techninės priemonės turi būti įgyvendinamos kartu su administracinėmis ir fizinėmis.
Ar svarbu vertinti technologinius kibernetinio saugumo trūkumus? Kokie galėtų būti technologinio kibernetinio saugumo trūkumai?	3	Klaidinga nuomonė, kad technologija gali

		išspręsti visas problemas
Ar technologijų valdymo priemonės turi būti technologiškai neutralios?	3	Ne, nors reikėtų atsižvelgti į suderinamumo problemas.
Ar nurodyti veiksmai užtikrintų tinkamą technologinio kibernetinio saugumo įgyvendinimą? Kokių veiksmų turi imtis organizacija? • naudojamų technologinių priemonių nustatymas**;** • technologinių priemonių parinkimas ir diegimas; • technologinių priemonių naudojimo poveikio kibernetiniam saugumui įvertinimas; • tolesni žingsniai.	1	Rizikos valdymas

Kibernetinių incidentų valdymas *Kibernetinių incidentų valdymas yra orientuotas į efektyvų valdymo planų, kurie būtų taikomi kritinėje situacijoje ir apimantys visus įvykio aspektus, nuo pasiruošimo iki identifikavimo ir tvarkymo, kūrimą. Komponente taip pat pateikta informacija apie kitus su kibernetiniais padariniais nesusijusius padarinius, tokius kaip fiziniai incidentai ir saugos valdymas ir planavimas.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar saugos valdymo procesas yra aktualus organizacijai kibernetinio saugumo kontekste?	1	Taip
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti saugumo valdymo procesus? Kokių veiksmų turi imtis organizacija? • nustatyti saugumo valdymo procesus organizacijoje; • klasifikuoti galimas rizikas ir atlikti jos vertinimą; • parengti saugumo valdymo planus ir taisykles; • tolesni žingsniai.	1	Atlikti BIA, parengti incidentų valdymo planą, PKP planus, DRP.

Strateginis valdymas *Strategijos valdymas daugiausia susijęs su metodais, tokiais kaip skaičiavimas, taip pat su kitų*	**Vertinimas**	**Ką reikia tobulinti?**

esamų kritinės energetinės infrastruktūros CEI aptikimu ir susiję su modeliu.		
Kaip strategijos valdymas yra susijęs su kibernetinio saugumo valdymo sprendimais?	1	Kibernetinio saugumo valdymas turėtų užtikrinti strategijos valdymą.
Kiek svarbu sukurti modelį, apskaičiuojantį didžiausio nacionalinio poveikio laipsnį gedimo ar atakos atveju?	1	
Ar nurodyti veiksmai padės organizacijai inkamai įgyvendinti organizacijos valdymo procesus? Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus? • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	2	

Organizacijos valdymas *Organizacinio valdymo komponentas suteikia supratimą apie gaires, kurios turėtų būti naudojamos tiesiogiai reaguojant į kibernetines atakas. Šiame komponente daugiausia dėmesio skiriama atakos pasekmėms, būtent avarinio atkūrimo planavimui, kuris apima bendrą instrukciją, kaip elgtis pagal įvairius scenarijus po kibernetinės atakos. Be to, jame taip pat atkreipiamas dėmesys į operatyvinį saugumą, paaiškinami įvairūs metodai, taikomi kibernetinių atakų prevencijai ir reagavimui į jas.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar organizacijos valdymas yra naudingas kibernetinio saugumo valdymo požiūriu?	1	Taip.
Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus: • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius organizacinius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles;	1	Taip

• tolesni žingsniai.		

4. Įvertinkite modelio komponentus nuo 1 iki 5, kur 1 – blogai, reikia tobulinti, 5 – nieko daryti nereikia.

Modelio komponentai	**Vertinimas**
Rizikos valdymas	3
Teisinis reguliavimas	1
Kibernetinio saugumo kultūra	2
Technologijų valdymas	4
Kibernetinių incidentų valdymas	2
Strateginis valdymas	1
Organizacijos valdymas	1

Papildomos ekspertų pastabos arba nuomonė:

KLAUSIMYNAS (E3)

Iš anksto dėkojame už pagalbą ir laiką.

1. Nurodykite savo vadovavimo patirtį šioje (arba ankstesnėje) įmonėje:
   a) Iki 3 metų
   b) Nuo 3 iki 5 metų
   c) Nuo 6 iki 10 metų
   d) Daugiau negu 10 metų
2. Ar sutinkate, kad technologinės plėtros strateginio valdymo įrankiai turi didelę įtaką energijos vartojimo efektyvumui ir kibernetiniam (informaciniam) saugumui:
   a) Taip
   b) Ne
   c) Nežinau
3. Suskirstykite pagal svarbą nuo 1 iki 5 (kur 1 yra svarbu, o 5 – nesvarbu) kibernetinių incidentų valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio valdymo, organizacijos valdymo, rizikos valdymo ir strategijos valdymo komponentus.

Rizikos valdymas *Rizikos valdymo komponentas apibūdina sistemą, kuriai taikomas modelis.*	**Vertinimas**	**Ką reikia tobulinti?**
Koks yra kibernetinio saugumo valdymo fenomeno poveikis rizikos valdymo komponentui?	1	Strateginius tikslus.
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir panaudojimas organizacijoje, jos valdymo sistemoje ir tarp organizacijos narių turi įtakos pačios organizacijos kibernetinio saugumo užtikrinimo procesui?	2	Visi elementai vienodai svarbūs.
Kokia kibernetinio saugumo komponento reikšmė organizacijos (naujai įgyvendinamuose) projektuose ir kaip galima pagerinti kibernetinio saugumo komponento integravimą į organizacijos veiklą?	1	Taikyti pokyčių stebėseną ir turi būti atliekamas savalaikis valdymas
Ar norint užtikrinti kibernetinio saugumo įgyvendinimą organizacijoje, būtina peržiūrėti ir koreguoti organizacijos valdymo procesus?	3	Kibernetinis saugumas turi užtikrinti organizacijos veiklos tęstinumą.
Ar nurodyti veiksmai gali patobulinti rizikos valdymo procesus kibernetinio saugumo kontekste:	2	Rizikų valdymas yra būtinas.

• organizacijos siekiamų tikslų nustatymas; • organizacijos saugumo sistemos sudedamųjų elementų nustatymas; • organizacijos aplinkos ypatybių nustatymas; • kibernetinio saugumo fenomeno integravimas į organizacijos verslo procesus; • tolesni žingsniai.		

Teisinis reguliavimas *Teisinis valdymas, be jokios abejonės, yra įdomus modelio papildymas, nes suteikia galimybę į modelį įtraukti jau egzistuojančią sistemą. Kadangi pastarasis tinkamas taikyti kiekvienam CI tipui, tokia kategorija reikalinga, kad kiekvienam modeliui būtų pridėtos konkretesnės savybės ir rekomendacijos.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar yra procesai, kurie apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje? Įvertinkite jų svarbumą. Kokie veiksniai, Jūsų nuomone, apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje?	1	Kritinės infrastruktūros techninių reikalavimų nebuvimas.
Kaip Jūs vertinate teisinio reguliavimo svarbumą kibernetinio saugumo srityje saugumo tikslams pasiekti? Ar toks komponentas reikalingas?	3	Operacinis lygmuo, neturintis teisinio pagrindo įgyvendinti geriausias praktikas.
Kaip Jūs vertinate reguliavimo procesų įtaką organizacijos kibernetiniam saugumui? Dėl kokių priežasčių reikia nagrinėti valdymo sritį organizacijoje kibernetinio saugumo kontekste? Ar reguliavimo procesai gali turėti įtakos organizacijos kibernetiniam saugumui?	4	Procesų supratimas yra reikalingas, jis efektyvina kibernetinės saugos valdymą.
Kaip Jūs vertinate vidinės ir išorinės aplinkos teisinio valdymo įtaką organizacijos kibernetinio saugumo valdymo įgyvendinimui? Kuri organizacinė aplinka (išorinė ar vidinė) yra svarbesnė jas svarstant kibernetinio saugumo reguliavimo kontekste?	3	Vidinis reguliavimas turėtų būti ne mažesnis nei išorinis reguliavimas ir papildantis jį.

Ar svarbūs teisinio reguliavimo aspektai organizacijos saugumo tikslams pasiekti? Kuo teisinio reguliavimo aspektas naudingas organizacijos saugumo tikslais?	2	Teisinis reguliavimas padeda valstybei susidaryti pirminį paveikslą.
Ar nurodyti veiksmai gali patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste? Kokių veiksmų organizacija turi imtis, kad patobulintų teisinio valdymo aspektus kibernetinio saugumo reiškinio kontekste: • esamos teisinės bazės reikalavimų ir trūkumų nustatymas; • organizacijai reikalingų teisinių ypatumų nustatymas; • modelyje siūlomų korekcinių priemonių įgyvendinimas; • papildomų, konkrečių procedūrų, susijusių su organizacijos saugumo poreikiais, nustatymas; • minėtų veiksmų integravimas į esamą modelį; • organizacijos įgyvendintų priemonių ir veiklos auditas; • teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • tolesni žingsniai.	2	Kiekvienas atvejis unikalus. Gerosios praktikos taikymas konkrečioje srityje.

Kibernetinio saugumo kultūra *Kibernetinio saugumo kultūros komponente nagrinėjami informaciniai kibernetinio saugumo aspektai, taip pat „žmogiškoji“ sistemos dalis. Šios kategorijos prioritetas yra nustatyti darbuotojų saugą, didinti sąmoningumą ir mokyti darbuotojus suprasti kibernetinio saugumo valdymo pagrindus.*	**Vertinimas**	**Ką reikia tobulinti?**
Įvertinkite kibernetinio saugumo kultūros svarbumą? Kaip galima apibūdinti „kibernetinio saugumo kultūrą“? (Ką reiškia „kibernetinio saugumo kultūra“?)	3	Svarbi sritis, kuri veikia bendrus tikslus. Siekiant efektyvinti kiberne-

		tinės saugos valdymą, būtina nuolat tobulinti ją.
Ar kibernetinio saugumo kultūros kūrimas yra svarbus? Įvertinkite. Kam kurti kibernetinio saugumo kultūrą, o ne, tarkime, didinti žmogaus informatyvumą (sąmoningumą)?	2	Svarbūs elgesio kaitos aspektai, kuriais galima būtų siekti geresnių rezultatų kibernetinės saugos valdymo srityje.
Ar svarbu skaidyti kibernetinio saugumo kultūrą į elementus? Kokie elementai sudaro kibernetinio saugumo kultūrą?	3	Priemonės, žmonės.
Ar kibernetinio saugumo kultūros mokymai yra svarbūs? Kokie kibernetinio saugumo kultūros mokymo būdai ir metodai, jūsų nuomone, yra efektyviausi?	2	Mokymasis iš geriausių praktikų. Automatizuoti būdai.
Ar organizacijos kibernetinio saugumo kultūros aspektai turėtų būti taikomi ir organizacijos partneriams bei paslaugų teikėjams?	2	Taip. Tiek žmogiškųjų išteklių, tiek infrastruktūrinių sprendinių nuomos aspektu.
Ar nurodytų veiksmų galima imtis organizacijoje, kad būtų pašalintas žmogiškojo faktoriaus ir kibernetinio saugumo kultūros fenomeno poveikis organizacijoje? Kokių veiksmų reikia imtis? • nustatyti kibernetinio saugumo suvokimo problemas; • pateikti kibernetinio saugumo supratimo gerinimo metodus ir būdus; • stebėti kibernetinio saugumo kultūros pokyčius; • tolesni žingsniai.	2	Analizė, geroji praktika, vertinimas, diegimas.

Technologijų valdymas *Technologijų valdymas yra dar vienas svarbus modelio komponentas, kuris lemia programinės įrangos, telekomunikacijų ir tinklo kibernetinį saugumą. Organizacijos*	**Vertinimas**	**Ką reikia tobulinti?**

valdymo komponente buvo nagrinėjamas fizinis infrastruktūros saugumas, o šiuo atveju dėmesys skiriamas naudojamos IT aplinkos kokybei, diegiant įvairius kibernetinio saugumo metodus, kurie skirsis priklausomai nuo programinės įrangos ir modelio infrastruktūros tipo.		
Ar technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios? Įvertinkite. Kokios technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje?	1	Informacijos apdorojimo aspektu.
Ar įmanoma užtikrinti visišką kibernetinį saugumą naudojant techninę ir programinę įrangą?	5	Ne, žmogiškasis veiksnys visada yra.
Ar svarbu vertinti technologinius kibernetinio saugumo trūkumus? Kokie galėtų būti technologinio kibernetinio saugumo trūkumai?	3	Svarbu. Žmogiškasis veiksnys.
Ar technologijų valdymo priemonės turi būti technologiškai neutralios?	2	Ne, saugumo ir suderinamumo klausimai.
Ar nurodyti veiksmai užtikrintų tinkamą technologinio kibernetinio saugumo įgyvendinimą? Kokių veiksmų turi imtis organizacija? • naudojamų technologinių priemonių nustatymas; • technologinių priemonių parinkimas ir diegimas; • technologinių priemonių naudojimo poveikio kibernetiniam saugumui įvertinimas; • tolesni žingsniai.	1	Rizikos valdymas.

Kibernetinių incidentų valdymas *Kibernetinių incidentų valdymas yra orientuotas į efektyvų valdymo planų, kurie būtų taikomi kritinėje situacijoje ir apimtų visus įvykio aspektus, nuo pasiruošimo iki identifikavimo ir tvarkymo, kūrimą. Komponente taip pat*	**Vertinimas**	**Ką reikia tobulinti?**

pateikta informaciją apie kitus su kibernetiniais padariniais nesusijusius padarinius, tokius kaip fiziniai incidentai ir saugos valdymas ir planavimas.		
Ar saugos valdymo procesas yra aktualus organizacijai kibernetinio saugumo kontekste?	1	Taip.
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti saugumo valdymo procesus? Kokių veiksmų turi imtis organizacija? • nustatyti saugumo valdymo procesus organizacijoje; • klasifikuoti galimas rizikas ir atlikti jų vertinimą; • parengti saugumo valdymo planus ir taisykles; • tolesni žingsniai.	1	Būtina.

Strateginis valdymas *Strategijos valdymas daugiausia susijęs su metodais, tokiais kaip skaičiavimas, taip pat su kitų esamų kritinės energetinės infrastruktūros CEI aptikimu ir susiję su modeliu.*	**Vertinimas**	**Ką reikia tobulinti?**
Kaip strategijos valdymas yra susijęs su kibernetinio saugumo valdymo sprendimais?	1	Strateginis valdymas reikalingas kaip atspirties taškas.
Kiek svarbu sukurti modelį, apskaičiuojantį didžiausio nacionalinio poveikio laipsnį gedimo ar atakos atveju?	1	
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti organizacijos valdymo procesus? Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus? • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	1	

Organizacijos valdymas *Organizacinio valdymo komponentas suteikia supratimą apie gaires, kurios turėtų būti naudojamos tiesiogiai reaguojant į kibernetines atakas. Šiame komponente daugiausia dėmesio skiriama atakos pasekmėms, būtent avarinio atkūrimo planavimui, kuris apima bendrą instrukciją, kaip elgtis pagal įvairius scenarijus po kibernetinės atakos. Be to, jame taip pat atkreipiamas dėmesys į operatyvinį saugumą, paaiškinant įvairius metodus, taikomus kibernetinių atakų prevencijai ir reagavimui į juos.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar organizacijos valdymas yra naudingas kibernetinio saugumo valdymo požiūriu?	1	Taip.
Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus: • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius organizacinius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	1	Taip.

4. Įvertinkite modelio komponentus nuo 1 iki 5, kur 1 – blogai, reikia tobulinti, 5 – nieko daryti nereikia.

Modelio komponentai	**Vertinimas**
Rizikos valdymas	3
Teisinis reguliavimas	1
Kibernetinio saugumo kultūra	2
Technologijų valdymas	1
Kibernetinių incidentų valdymas	2
Strateginis valdymas	1
Organizacijos valdymas	1

Papildomos ekspertų pastabos arba nuomonė:

KLAUSIMYNAS (E4)

Iš anksto dėkojame už pagalbą ir laiką.

- Nurodykite savo vadovavimo patirtį šioje (arba ankstesnėje) įmonėje:
  a) Iki 3 metų
  b) Nuo 3 iki 5 metų
  c) Nuo 6 iki 10 metų
  d) Daugiau negu 10 metų
- Ar sutinkate, kad technologinės plėtros strateginio valdymo įrankiai turi didelę įtaką energijos vartojimo efektyvumui ir kibernetiniam (informaciniam) saugumui:
  a) Taip
  b) Ne
  c) Nežinau
- Suskirstykite pagal svarbą nuo 1 iki 5 (kur 1 yra svarbu, o 5 – nesvarbu) kibernetinių incidentų valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio valdymo, organizacijos valdymo, rizikos valdymo ir strategijos valdymo komponentus.

Rizikos valdymas *Rizikos valdymo komponentas apibūdina sistemą, kuriai taikomas modelis.*	**Vertinimas**	**Ką reikia tobulinti?**
Koks yra kibernetinio saugumo valdymo fenomeno poveikis rizikos valdymo komponentui?	2	Strategijos nebuvimas.
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir panaudojimas organizacijoje, jos valdymo sistemoje ir tarp organizacijos narių turi įtakos pačios organizacijos kibernetinio saugumo užtikrinimo procesui?	2	Suvokiant kibernetinio valdymo aspektus galima išvengti kibernetinių incidentų ar žmogiškųjų klaidų.
Kokia kibernetinio saugumo komponento reikšmė organizacijos (naujai įgyvendinamuose) projektuose ir kaip galima pagerinti kibernetinio saugumo komponento integravimą į organizacijos veiklą?	1	Trečiųjų šalių ir vidinio personalo grėsmė.
Ar norint užtikrinti kibernetinio saugumo įgyvendinimą organizacijoje būtina peržiūrėti ir koreguoti organizacijos valdymo procesus?	1	Būtina.

Ar nurodyti veiksmai gali patobulinti rizikos valdymo procesus kibernetinio saugumo kontekste? • organizacijos siekiamų tikslų nustatymas; • organizacijos saugumo sistemos sudedamųjų elementų nustatymas; • organizacijos aplinkos ypatybių nustatymas; • kibernetinio saugumo fenomeno integravimas į organizacijos verslo procesus; • tolesni žingsniai.	1	Taip.

Teisinis reguliavimas *Teisinis valdymas, be jokios abejonės, yra įdomus modelio papildymas, nes suteikia galimybę į modelį įtraukti jau egzistuojančią sistemą. Kadangi teisinis valdymas tinkamas taikyti kiekvienam CI tipui, tokia kategorija reikalinga, kad kiekvienam modeliui būtų pridėtos konkretesnės savybės ir rekomendacijos.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar yra procesai, kurie apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje? Įvertinkite jų svarbumą. Kokie veiksniai, Jūsų nuomone, apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje?	2	Standartizacijos nebuvimas.
Kaip Jūs vertinate teisinio reguliavimo svarbumą kibernetinio saugumo srityje saugumo tikslams pasiekti? Ar toks komponentas reikalingas?	1	Taip, reikalingas.
Kaip Jūs vertinate reguliavimo procesų įtaką organizacijos kibernetiniam saugumui? Dėl kokių priežasčių reikia nagrinėti valdymo sritį organizacijoje kibernetinio saugumo kontekste? Ar reguliavimo procesai gali turėti įtakos organizacijos kibernetiniam saugumui?	2	Teisinis reguliavimas turi būti griežtas.
Kaip Jūs vertinate vidinės ir išorinės aplinkos teisinio valdymo įtaką organizacijos kibernetinio saugumo valdymo įgyvendinimui? Kuri organizacinė aplinka (išorinė ar vidinė) yra svarbesnė jas	1	Išorinis reguliavimas turi būti suvokiamas kaip

svarstant kibernetinio saugumo reguliavimo kontekste?		minimalus reikalavimas, o vidinis gali būti ir griežtesnis.
Ar svarbūs teisinio reguliavimo aspektai organizacijos saugumo tikslams pasiekti? Kuo teisinio reguliavimo aspektas naudingas organizacijos saugumo tikslais?	1	Teisinė atsakomybė įpareigoja sprendimo priėmėjus laikytis įstatymų ar reglamentų.
Ar nurodyti veiksmai gali patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste? Kokių veiksmų organizacija turi imtis, kad patobulintų teisinio valdymo aspektus kibernetinio saugumo reiškinio kontekste? • esamos teisinės bazės reikalavimų ir trūkumų nustatymas; • organizacijai reikalingų teisinių ypatumų nustatymas; • modelyje siūlomų korekcinių priemonių įgyvendinimas; • papildomų, konkrečių procedūrų, susijusių su organizacijos saugumo poreikiais, nustatymas; • minėtų veiksmų integravimas į esamą modelį; • organizacijos įgyvendintų priemonių ir veiklos auditas; • teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • tolesni žingsniai.	1	Taip, gali.

Kibernetinio saugumo kultūra *Kibernetinio saugumo kultūros komponente nagrinėjami informaciniai kibernetinio saugumo aspektai, taip pat „žmogiškoji“ sistemos dalis. Šios kategorijos prioritetas yra nustatyti darbuotojų saugą, didinti sąmoningumą ir mokyti darbuotojus suprasti kibernetinio saugumo valdymo pagrindus.*	**Vertinimas**	**Ką reikia tobulinti?**

Įvertinkite kibernetinio saugumo kultūros svarbumą. Kaip galima apibūdinti „kibernetinio saugumo kultūrą“? (Ką reiškia „kibernetinio saugumo kultūra“?)	2	Svarbi sritis. Elgsenos ypatumai gali efektyviai padėti valdyti kibernetinę saugą.
Ar kibernetinio saugumo kultūros kūrimas yra svarbus? Įvertinkite. Kam kurti kibernetinio saugumo kultūrą, o ne, tarkime, didinti žmogaus informatyvumą (sąmoningumą)?	3	Informacijos sklaida palaipsniui formuoja kultūros ypatumus.
Ar svarbu skaidyti kibernetinio saugumo kultūrą į elementus? Kokie elementai sudaro kibernetinio saugumo kultūrą?	3	Paprasti vartotojai ir privilegijuoti. Jiems turi būti diegiama atskira kultūra.
Ar kibernetinio saugumo kultūros mokymai yra svarbus? Kokie kibernetinio saugumo kultūros mokymo būdai ir metodai, jūsų nuomone, yra efektyviausi?	1	Mokymai yra labai svarbūs.
Ar organizacijos kibernetinio saugumo kultūros aspektai turėtų būti taikomi ir organizacijos partneriams bei paslaugų teikėjams?	2	Jei reikalinga perteikti konkrečios organizacijos kibernetinės valdymo saugos aspektus.
Ar nurodytų veiksmų galima imtis organizacijoje, kad būtų pašalintas žmogiškojo faktoriaus ir kibernetinio saugumo kultūros fenomeno poveikis organizacijoje. Kokių veiksmų reikia imtis? • nustatyti kibernetinio saugumo suvokimo problemas; • pateikti kibernetinio saugumo supratimo gerinimo metodus ir būdus; • stebėti kibernetinio saugumo kultūros pokyčius; • tolesni žingsniai.	2	Taip, galima analizuoti juos ir gerinti.

Technologijų valdymas *Technologijų valdymas yra dar vienas svarbus modelio komponentas, kuris lemia programinės įrangos, telekomunikacijų ir tinklo kibernetinį saugumą. Organizacijos valdymo komponente buvo nagrinėjamas fizinis infrastruktūros saugumas, o šiuo atveju dėmesys skiriamas naudojamos IT aplinkos kokybei, diegiant įvairius kibernetinio saugumo metodus, kurie skirsis priklausomai nuo programinės įrangos ir modelio infrastruktūros tipo.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios? Įvertinkite. Kokios technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje?	1	IPS IDS XDR.
Ar įmanoma užtikrinti visišką kibernetinį saugumą naudojant techninę ir programinę įrangą?	3	Neįmanoma.
Ar svarbu vertinti technologinius kibernetinio saugumo trūkumus? Kokie galėtų būti technologinio kibernetinio saugumo trūkumai?	3	Programinio kodo klaidos.
Ar technologijų valdymo priemonės turi būti technologiškai neutralios?	2	Neįmanoma to pasiekti.
Ar nurodyti veiksmai užtikrintų tinkamą technologinio kibernetinio saugumo įgyvendinimą? Kokių veiksmų turi imtis organizacija? • naudojamų technologinių priemonių nustatymas; • technologinių priemonių parinkimas ir diegimas; • technologinių priemonių naudojimo poveikio kibernetiniam saugumui įvertinimas; • tolesni žingsniai.	3	Iš dalies. Reiktų atsižvelgti į technologijų kūrėjų kilmę, kai kalbama apie kritinę infrastruktūrą.

Kibernetinių incidentų valdymas *Kibernetinių incidentų valdymas yra orientuotas į efektyvų valdymo planų, kurie būtų taikomi kritinėje situacijoje ir apimtų visus įvykio aspektus, nuo pasiruošimo iki identifikavimo ir tvarkymo, kūrimą. Komponente taip pat pateikta*	**Vertinimas**	**Ką reikia tobulinti?**

informacija apie kitus su kibernetiniais padariniais nesusijusius padarinius, tokius kaip fiziniai incidentai ir saugos valdymas ir planavimas.		
Ar saugos valdymo procesas yra aktualus organizacijai kibernetinio saugumo kontekste?	1	Taip.
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti saugumo valdymo procesus? Kokių veiksmų turi imtis organizacija? • nustatyti saugumo valdymo procesus organizacijoje; • klasifikuoti galimas rizikas ir atlikti jų vertinimą; • parengti saugumo valdymo planus ir taisykles; • tolesni žingsniai.	2	Taip.

Strateginis valdymas *Strategijos valdymas daugiausia susijęs su metodais, tokiais kaip skaičiavimas, taip pat su kitų esamų kritinės energetinės infrastruktūros CEI aptikimu ir susiję su modeliu.*	**Vertinimas**	**Ką reikia tobulinti?**
Kaip strategijos valdymas yra susijęs su kibernetinio saugumo valdymo sprendimais?	1	Strateginis valdymas labai aktualus gynybiniu aspektu.
Kiek svarbu sukurti modelį, apskaičiuojantį didžiausio nacionalinio poveikio laipsnį gedimo ar atakos atveju?	1	Labai svarbu.
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti organizacijos valdymo procesus? Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus? • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	1	Taip, padės.

Organizacijos valdymas *Organizacinio valdymo komponentas suteikia supratimą apie gaires, kurios turėtų būti naudojamos*	**Vertinimas**	**Ką reikia tobulinti?**

tiesiogiai reaguojant į kibernetines atakas. Šiame komponente daugiausia dėmesio skiriama atakos pasekmėms, būtent avarinio atkūrimo planavimui, kuris apima bendrą instrukciją, kaip elgtis pagal įvairius scenarijus po kibernetinės atakos. Be to, jame taip pat atkreipiamas dėmesys į operatyvinį saugumą, paaiškinant įvairius metodus, taikomus kibernetinių atakų prevencijai ir reagavimui į juos.		
Ar organizacijos valdymas yra naudingas kibernetinio saugumo valdymo požiūriu?	2	Naudojant organizacines priemones didėja informuotumas ir atsakomybė.
Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus: • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius organizacinius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	3	Turto valdymas. Saugos reikalavimai technologiniams sprendimams (patikimas gamintojas ir t. t.).

4. Įvertinkite modelio komponentus nuo 1 iki 5, kur 1 – blogai, reikia tobulinti, 5 – nieko daryti nereikia.

Modelio komponentai	**Vertinimas**
Rizikos valdymas	2
Teisinis reguliavimas	2
Kibernetinio saugumo kultūra	3
Technologijų valdymas	1
Kibernetinių incidentų valdymas	2
Strateginis valdymas	1
Organizacijos valdymas	2

Papildomos ekspertų pastabos arba nuomonė:

KLAUSIMYNAS (E5)

Iš anksto dėkojame už pagalbą ir laiką.

- Nurodykite savo vadovavimo patirtį šioje (arba ankstesnėje) įmonėje:

a) Iki 3 metų
b) Nuo 3 iki 5 metų
c) Nuo 6 iki 10 metų
d) Daugiau negu 10 metų

- Ar sutinkate, kad technologinės plėtros strateginio valdymo įrankiai turi didelę įtaką energijos vartojimo efektyvumui ir kibernetiniam (informaciniam) saugumui:

a) Taip
b) Ne
c) Nežinau

3 Suskirstykite pagal svarbą nuo 1 iki 5 (kur 1 yra svarbu, o 5 – nesvarbu) kibernetinių incidentų valdymo, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio valdymo, organizacijos valdymo, rizikos valdymo ir strategijos valdymo komponentus.

Rizikos valdymas *Rizikos valdymo komponentas apibūdina sistemą, kuriai taikomas modelis.*	**Vertinimas**	**Ką reikia tobulinti?**
Koks yra kibernetinio saugumo valdymo fenomeno poveikis rizikos valdymo komponentui?	3	Iš dalies.
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir panaudojimas organizacijoje, jos valdymo sistemoje ir tarp organizacijos narių turi įtakos pačios organizacijos kibernetinio saugumo užtikrinimo procesui?	2	Iš dalies.
Kokia kibernetinio saugumo komponento reikšmė organizacijos (naujai įgyvendinamuose) projektuose ir kaip galima pagerinti kibernetinio saugumo komponento integravimą į organizacijos veiklą?	2	Kompetencijos.
Ar norint užtikrinti kibernetinio saugumo įgyvendinimą organizacijoje būtina peržiūrėti ir koreguoti organizacijos valdymo procesus?	1	Taip, būtina.
Ar nurodyti veiksmai gali patobulintų rizikos valdymo procesus kibernetinio saugumo kontekste: • organizacijos siekiamų tikslų nustatymas; • organizacijos saugumo sistemos sudedamųjų elementų nustatymas;	2	Iš dalies

• organizacijos aplinkos ypatybių nustatymas; • kibernetinio saugumo fenomeno integravimas į organizacijos verslo procesus; • tolesni žingsniai.		

Teisinis reguliavimas *Teisinis valdymas, be jokios abejonės, yra įdomus modelio papildymas, nes suteikia galimybę į modelį įtraukti jau egzistuojančią sistemą. Kadangi teisinis valdymas tinkamas taikyti kiekvienam CI tipui, tokia kategorija reikalinga, kad kiekvienam modeliui būtų pridėtos konkretesnės savybės ir rekomendacijos.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar yra procesai, kurie apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje? Įvertinkite jų svarbumą. Kokie veiksniai, Jūsų nuomone, apsunkina tarptautinės teisės taikymą kibernetinio saugumo srityje?	2	Informacijos apsikeitimas.
Kaip Jūs vertinate teisinio reguliavimo svarbumą kibernetinio saugumo srityje saugumo tikslams pasiekti? Ar toks komponentas reikalingas?	2	Reikalingas.
Kaip Jūs vertinate reguliavimo procesų įtaką organizacijos kibernetiniam saugumui? Dėl kokių priežasčių reikia nagrinėti valdymo sritį organizacijoje kibernetinio saugumo kontekste? Ar reguliavimo procesai gali turėti įtakos organizacijos kibernetiniam saugumui?	2	Didėjant kibernetinių incidentų mastui nėra pasaulinio teisinio reguliavimo (pvz., Azijos šalys), nėra atsakomybių ir pan.
Kaip Jūs vertinate vidinės ir išorinės aplinkos teisinio valdymo įtaką organizacijos kibernetinio saugumo valdymo įgyvendinimui? Kuri organizacinė aplinka (išorinė ar vidinė) yra svarbesnė jas svarstant kibernetinio saugumo reguliavimo kontekste?	1	Išorinis teisinis reguliavimas turi būti griežtesnis ir eiti koja kojon su besikeičiančia aplinka.
Ar svarbūs teisinio reguliavimo aspektai organizacijos saugumo tikslams pasiekti? Kuo teisinio reguliavimo aspektas naudingas organizacijos saugumo tikslais?	2	Drausmina vadovus, kurie privalo jo laikytis.

Ar nurodyti veiksmai gali patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste? Kokių veiksmų organizacija turi imtis, kad patobulintų teisinio valdymo aspektus kibernetinio saugumo reiškinio kontekste: • esamos teisinės bazės reikalavimų ir trūkumų nustatymas; • organizacijai reikalingų teisinių ypatumų nustatymas; • modelyje siūlomų korekcinių priemonių įgyvendinimas; • papildomų, konkrečių procedūrų, susijusių su organizacijos saugumo poreikiais, nustatymas; • minėtų veiksnių integravimas į esamą modelį; • organizacijos įgyvendintų priemonių ir veiklos auditas; • teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • tolesni žingsniai.	3	Iš dalies teisinis reguliavimas atsilieka nuo dabartinių kibernetinių geruųjų praktikų.

Kibernetinio saugumo kultūra *Kibernetinio saugumo kultūros komponente nagrinėjami informaciniai kibernetinio saugumo aspektai, taip pat „žmogiškoji“ sistemos dalis. Šios kategorijos prioritetas yra nustatyti darbuotojų saugą, didinti sąmoningumą ir mokyti darbuotojus suprasti kibernetinio saugumo valdymo pagrindus.*	**Vertinimas**	**Ką reikia tobulinti?**
Įvertinkite kibernetinio saugumo kultūros svarbumą? Kaip galima apibūdinti „kibernetinio saugumo kultūrą“? (Ką reiškia „kibernetinio saugumo kultūra“?)	2	Svarbu, nes kibernetinę saugą ne visada pavyksta pasiekti technologinėmis priemonėmis.
Ar kibernetinio saugumo kultūros kūrimas yra svarbus? Įvertinkite.	3	Svarbus iš dalies, nes dalį to galima įgyvendinti technologiškai.

Kam kurti kibernetinio saugumo kultūrą, o ne, tarkime, didinti žmogaus informatyvumą (sąmoningumą)?		
Ar svarbu skaidyti kibernetinio saugumo kultūrą į elementus? Kokie elementai sudaro kibernetinio saugumo kultūrą?	2	Vartotojai, administratoriai.
Ar kibernetinio saugumo kultūros mokymai yra svarbūs? Kokie kibernetinio saugumo kultūros mokymo būdai ir metodai, jūsų nuomone, yra efektyviausi?	1	Labai svarbūs.
Ar organizacijos kibernetinio saugumo kultūros aspektai turėtų būti taikomi ir organizacijos partneriams bei paslaugų teikėjams?	2	Gali būti taikomi, jei yra įvardintos tokios rizikos.
Ar nurodytų veiksmų galima imtis organizacijoje, kad būtų pašalintas žmogiškojo faktoriaus ir kibernetinio saugumo kultūros fenomeno poveikis organizacijoje. Kokių veiksmų reikia imtis? • nustatyti kibernetinio saugumo suvokimo problemas; • pateikti kibernetinio saugumo supratimo gerinimo metodus ir būdus; • stebėti kibernetinio saugumo kultūros pokyčius; • tolesni žingsniai.	1	Taip, galima.

Technologijų valdymas *Technologijų valdymas yra dar vienas svarbus modelio komponentas, kuris lemia programinės įrangos, telekomunikacijų ir tinklo kibernetinį saugumą. Organizacijos valdymo komponente buvo nagrinėjamas fizinis infrastruktūros saugumas, o šiuo atveju dėmesys skiriamas naudojamos IT aplinkos kokybei, diegiant įvairius kibernetinio saugumo metodus, kurie skirsis priklausomai nuo programinės įrangos ir modelio infrastruktūros tipo.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios? Įvertinkite.	1	Labai svarbios.

Kokios technologinės kibernetinio saugumo įgyvendinimo priemonės yra svarbios siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje?		
Ar įmanoma užtikrinti visišką kibernetinį saugumą naudojant techninę ir programinę įrangą?	3	Neįmanoma.
Ar svarbu vertinti technologinius kibernetinio saugumo trūkumus? Kokie galėtų būti technologinio kibernetinio saugumo trūkumai?	1	Svarbu. Programinio kodo spragos, kompetencijos stoka.
Ar technologijų valdymo priemonės turi būti technologiškai neutralios?	1	Saugumo aspektu turi būti įvertintos ir analizuotinos. Nenaudotinos saugumo aspektu priemonės turi būti nenaudojamos.
Ar nurodyti veiksmai užtikrintų tinkamą technologinio kibernetinio saugumo įgyvendinimą? Kokių veiksmų turi imtis organizacija? • naudojamų technologinių priemonių nustatymas; • technologinių priemonių parinkimas ir diegimas; • technologinių priemonių naudojimo poveikio kibernetiniam saugumui įvertinimas; • tolesni žingsniai.	2	Taip.

Kibernetinių incidentų valdymas *Kibernetinių incidentų valdymas yra orientuotas į efektyvų valdymo planų, kurie būtų taikomi kritinėje situacijoje ir apimtų visus įvykio aspektus, nuo pasiruošimo iki identifikavimo ir tvarkymo, kūrimą. Komponente taip pat pateikta informacija apie kitus su kibernetiniais padariniais nesusijusius padarinius, tokius kaip fiziniai incidentai ir saugos valdymas ir planavimas.*	**Vertinimas**	**Ką reikia tobulinti?**
Ar saugos valdymo procesas yra aktualus organizacijai kibernetinio saugumo kontekste?	2	Taip.

Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti saugumo valdymo procesus? Kokių veiksmų turi imtis organizacija? • nustatyti saugumo valdymo procesus organizacijoje; • klasifikuoti galimas rizikas ir atlikti jos vertinimą; • parengti saugumo valdymo planus ir taisykles; • tolesni žingsniai.	2	Padės.

Strateginis valdymas *Strateginis valdymas daugiausia susijęs su metodais, tokiais kaip skaičiavimas, taip pat su kitų esamų CEI aptikimu ir susiję su modeliu.*	**Vertinimas**	**Ką reikia tobulinti?**
Kaip strategijos valdymas yra susijęs su kibernetinio saugumo valdymo sprendimais?	2	Visame sistemos gyvavimo cikle.
Kiek svarbu sukurti modelį, apskaičiuojantį didžiausio nacionalinio poveikio laipsnį gedimo ar atakos atveju?	1	Svarbu.
Ar nurodyti veiksmai padės organizacijai tinkamai įgyvendinti organizacijos valdymo procesus? Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus? • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	2	Taip.

Organizacijos valdymas *Organizacinio valdymo komponentas suteikia supratimą apie gaires, kurios turėtų būti naudojamos tiesiogiai reaguojant į kibernetines atakas. Šiame komponente daugiausia dėmesio skiriama atakos pasekmėms, būtent avarinio atkūrimo planavimui, kuris apima bendrą instrukciją, kaip elgtis pagal įvairius scenarijus po kibernetinės atakos. Be to, jame taip pat atkreipiamas dėmesys į operatyvinį saugumą, paaiškinant įvairius metodus, taikomus kibernetinių atakų prevencijai ir reagavimui į juos.*	**Vertinimas**	**Ką reikia tobulinti?**

Ar organizacijos valdymas yra naudingas kibernetinio saugumo valdymo požiūriu?	1	Naudingas.
Kokių veiksmų turi imtis organizacija, kad tinkamai įgyvendintų organizacijos valdymo procesus? • nustatyti organizacijos rizikas ir pažeidžiamumą; • suorganizuoti tikslius organizacinius atkūrimo ir įvertinimo planus po kibernetinių atakų; • įgyvendinti organizacijos valdymo planus ir taisykles; • tolesni žingsniai.	2	

4. Įvertinkite modelio komponentus nuo 1 iki 5, kur 1 – blogai, reikia tobulinti, 5 – nieko daryti nereikia.

Modelio komponentai	**Vertinimas**
Rizikos valdymas	1
Teisinis reguliavimas	1
Kibernetinio saugumo kultūra	1
Technologijų valdymas	2
Kibernetinių incidentų valdymas	2
Strateginis valdymas	1
Organizacijos valdymas	1

Papildomos ekspertų pastabos arba nuomonė:

C priedas. Daugiakriterio vertinimo metodai

Daugiakriterio vertinimo metodus sudaro šie žingsniai:

1. Vertinimo suderinamumo, reikšmingumo ir ekspertų kompetencijos skaičiavimas.
2. Normalizuotos sprendimų matricos sudarymas.
3. Įverčių ir rangų skaičiavimas.

C1 lentelė. Ekspertų vertinimo rezultatai
Table C1. Results of expert evaluation

Modelio komponentas	Ekspertų vertinimas				
	E1	E2	E3	E4	E5
Rizikos valdymas	2	3	2	2	1
Teisinis reguliavimas	1	1	3	2	2
Kibernetinio saugumo kultūra	1	2	3	3	1
Technologijų valdymas	2	4	2	2	2
Kibernetinių incidentų valdymas	1	2	1	2	2
Strateginis valdymas	1	1	1	1	2
Organizacijos valdymas	2	1	2	2	1

1. Vertinimo suderinamumo, reikšmingumo ir ekspertų kompetencijos skaičiavimas.

Nustatomas ekspertų suderinamumo lygis, skaičiuojant konkordancijos koeficientą. Skaičiavimo eiga pateikta C1 lentelėje.

C2. lentelė. Konkordacijos koeficiento skaičiavimo eiga
Table C2. The procedure for calculating the concordance coefficient

Veiksniai	Skaičiavimo formulė
Rangų sumos apskaičiavimas	$e_i = \sum_{j=1}^{m} e_{ij}$
Nuokrypio nuo bendro vidurkio kvadratų sumos skaičiavimas	$S = \sum_{i=1}^{m} (e_i - \bar{e})^2$
Bendro vidurkio apskaičiavimas	$\bar{e} = \frac{\sum_{i=1}^{n} e_i}{n} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} e_{ij}}{n}$, čia m – veiksnių skaičius.

Konkordancijos koeficiento skaičiavimas	$W = \frac{12S}{r^2 m(m^2-1)}$, čia S – kiekvieno i-tojo kriterijaus rangų sumos, m – veiksnių skaičius, r – ekspertų skaičius.
Konkordancijos koeficiento skaičiavimas, kai yra vienodi rangai	$W = \frac{12S}{r^2((m^3-m)-r*\sum_{j=1}^{m}(t_j^3-t_j))}$, čia t_j – vienodų rangų skaičius kiekviename veiksnyje.

C3 lentelė. Ekspertų nuomonių suderinamumo rezultatai
Table C3. Results of concordance of expert opinions

	Rizikos valdymas	Teisinis reguliavimas	Kibernetinio saugumo kultūra	Technologinis kibernetinis saugumas	Kibernetinių incidentų valdymas	Strateginis valdymas	Organizacijos valdymas
Rangų suma	10	9	10	12	8	6	8
Rangų sumų vidurkis	9						
Nuokrypių kvadratas	1	81	100	144	64	36	64
Nuokrypių kvadratų suma	490						
Konkordacijos koeficientas W	0,875						

Atliekant skaičiavimus, buvo pastebėta, kad yra vienodi rangai, todėl konkordacijos koeficientas skaičiuojamas pagal tokią formulę

$$W = \frac{12S}{r^2((m^3-m)-r*\sum_{j=1}^{m}(t_j^3-t_j))}, \qquad \text{(C priedas. 1)}$$

čia t_j – vienodų rangų skaičius kiekviename veiksnyje.

C4 lentelė. Vienodų rangų skaičiai
Table C4. Results of expert evaluation

	Ekspertų vertinimas				
	E1	**E2**	**E3**	**E4**	**E5**
Vienodų rangų grupių skaičius	2	2	3	1	2
Vienodų rangų elementų skaičius	4	2	3	5	3
	3	2	2		4
			2		

$t_j^3 - t_j$	60	6	24	120	24
	24	6	6		60
			6		
T_j (koregavimo suma)	84	12	36	120	84

Konkordancijos koeficientas W lygus 0,875 ir artėja prie vieneto, tai reiškia, kad ekspertų vertinimo suderinamumas pakankamai geras ir gautus rezultatus galima naudoti tolesniems tyrimams.

Toliau vertinama ekspertų kompetencija, kuri skaičiuojama pagal C priedo 2 formulę. Ekspertai kompetentingi, jeigu kompetencijų įverčių suma lygi vienetui.

$$K_i^t = \frac{1}{\lambda} * \sum_{j=1}^{n} x_j^t * x_{ij}, \sum_{i=1}^{m} K_i^t = 1, \qquad \text{(C priedas. 2)}$$

čia $x_j^t = \sum_{i=1}^{m} K_i^{t-1} * x_{ij}, j = 1,2, \dots n$ ir $\lambda = \sum_{j=1}^{n} \sum_{i=1}^{m} x_j x_{ij}$, m – ekspertų skaičius, n – kriterijų skaičius, x_{ij} – i-tojo eksperto j-ojo kriterijaus rangas.

C5 lentelė. Ekspertų kompetentingumo skaičiavimo rezultatai
Table C5. Results of the calculation of experts' competence

	E1	**E2**	**E3**	**E4**	**E5**	Įverčių suma
Ekspertų kompetencija	0,16	0,23	0,22	0,22	0,17	**1**

C6 lentelė. Ekspertų vertinimo rezultatų reikšmingumas
Table C6. Significance of expert evaluation results

Ekspertai / Komponentai	E_1	E_2	E_3	E_4	E_5	Reikšmingumas	Rangas
Rizikos valdymas	0,2	0,21	0,14	0,14	0,09	0,16	4
Teisinis reguliavimas	0,1	0,07	0,21	0,14	0,18	0,14	3
Kibernetinio saugumo kultūra	0,1	0,14	0,21	0,21	0,09	0,16	4
Technologinis kibernetinis saugumas	0,2	0,29	0,14	0,14	0,18	0,19	5
Kibernetinių incidentų valdymas	0,1	0,14	0,07	0,14	0,18	0,13	2
Strateginis valdymas	0,1	0,07	0,07	0,07	0,18	0,10	1
Organizacijos valdymas	0,2	0,07	0,14	0,14	0,09	0,13	2
	1	**1**	**1**	**1**	**1**	**1**	

2. Normalizuotos sprendimų matricos sudarymas.

C7 lentelė. Pradinė duomenų matrica
Table C7. The original data matrix

Modelio komponentas	Ekspertų vertinimas					Suma	Vidurkis
	E1	**E2**	**E3**	**E4**	**E5**		
Rizikos valdymas	2	3	2	2	1	***10***	***2***
Teisinis reguliavimas	1	1	3	2	2	***9***	***1,8***
Kibernetinio saugumo kultūra	1	2	3	3	1	***10***	***2***
Technologijų valdymas	2	4	2	2	2	***12***	***2,4***
Kibernetinių incidentų valdymas	1	2	1	2	2	***8***	***1,6***
Strateginis valdymas	1	1	1	1	2	***6***	***1,2***
Organizacijos valdymas	2	1	2	2	1	***8***	***1,6***
	10	***14***	***14***	***14***	***11***	***63***	***12,6***

Skaičiuojama normalizavimo matrica

$$\widetilde{r_{ij}} = \frac{r_{ij}}{\sum_{i=1}^{m} r_{ij}}, \qquad \text{(C priedas. 3)}$$

čia r_{ij} – *i*-tojo rodiklio reikšmė *j*-tajam objektui.

Toliau skaičiuojamas kiekvieno komponento svoris:

$$\omega_i = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}}, \text{ čia } \left(\sum_{i=1}^{m} \omega_i = 1\right). \qquad \text{(C priedas. 4)}$$

C8 lentelė. Normalizuota sprendimų matrica
Table C8. Normalized decision matrix

Modelio komponentas	E1		E2		E3		E4		E5	
		Svoris		Svoris		Svoris		Svoris		Svoris
Rizikos valdymas	0,2	0,2	0,3	0,21	0,2	0,143	0,2	0,143	0,1	0,09
Teisinis reguliavimas	0,11	0,1	0,11	0,07	0,33	0,214	0,22	0,143	0,22	0,18
Kibernetinio saugumo kultūra	0,1	0,1	0,2	0,14	0,3	0,214	0,3	0,214	0,1	0,09
Technologijų valdymas	0,17	0,2	0,33	0,29	0,167	0,143	0,167	0,143	0,167	0,18
Kibernetinių incidentų valdymas	0,13	0,1	0,25	0,14	0,125	0,07	0,25	0,143	0,25	0,18
Strateginis valdymas	0,17	0,1	0,17	0,07	0,167	0,07	0,167	0,07	0,33	0,18
Organizacijos valdymas	0,25	0,2	0,13	0,07	0,25	0,143	0,25	0,143	0,125	0,09
		1		***1***		***1***		***1***		***1***

3. Kiekvieno komponento įverčių ir rangų skaičiavimas.

Taikant paprastąjį adityvų svorių metodą (SAW) sudaroma normalizuota sprendimų matrica (C7 lentelė) ir skaičiuojamas kiekvieno komponento įvertis:

$$n_{ij} = \omega_i \widetilde{r_{ij}}. \qquad \text{(C priedas. 5)}$$

Visų veiksnių pasvertų normalizuotų reikšmių suma S_j kiekvienam *j*-ajam objektui skaičiuojama pagal formulę (C priedas. 6):

$$S_j = \sum_{i=1}^{m} \omega_i \widetilde{r_{ij}}, \qquad \text{(C priedas. 6)}$$

čia ω_i – *i*-tojo rodiklio svoris, $\widetilde{r_{ij}}$ – *i*-tojo rodiklio normalizuota reikšmė *j*-ajam objektui ($\sum_{i=1}^{m} \omega_i = 1$).

C9 lentelė. Visų komponentų įverčiai ir rangai
Table C9. Estimates and ranks for all components

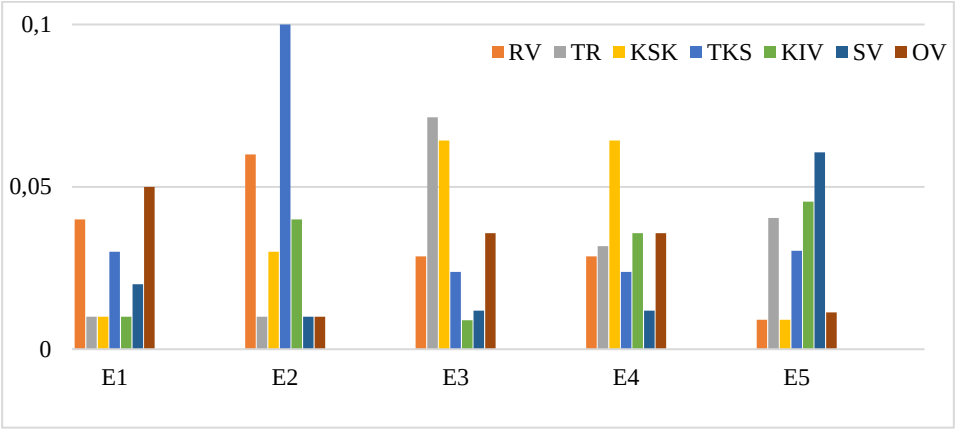
	E1		E2		E3		E4		E5		Rangų vidurkis	Galutinis rangas
	Įverčiai	Rangas	Įverčiai	Rangas	Įverčiai	Rangas	Įverčiai	Rangas	Įverčiai	Rangas		
RV	0,04	2	0,06	2	0,028571	4	0,028571	4	0,009091	6	3,2	3
TR	0,01	5	0,01	5	0,071429	1	0,031746	3	0,040404	3	3,4	4
KSK	0,01	5	0,03	4	0,064286	2	0,064286	1	0,009091	6	3,2	3
TKS	0,03	3	0,10	1	0,02381	5	0,02381	5	0,030303	4	3,2	3
KIV	0,01	5	0,04	3	0,008929	7	0,035714	2	0,045455	2	3	2
SV	0,02	4	0,01	5	0,011905	6	0,011905	6	0,060606	1	2,4	1
OV	0,05	1	0,01	5	0,035714	3	0,035714	2	0,011364	5	3,6	5

OV – organizacijos valdymas, TR – teisinis reguliavimas, KSK – kibernetinio saugumo kultūra, TKS – technologinis kibernetinis saugumas, RV – rizikos valdymas, KIV – kibernetinių incidentų valdymas, SV – strateginis valdymas.

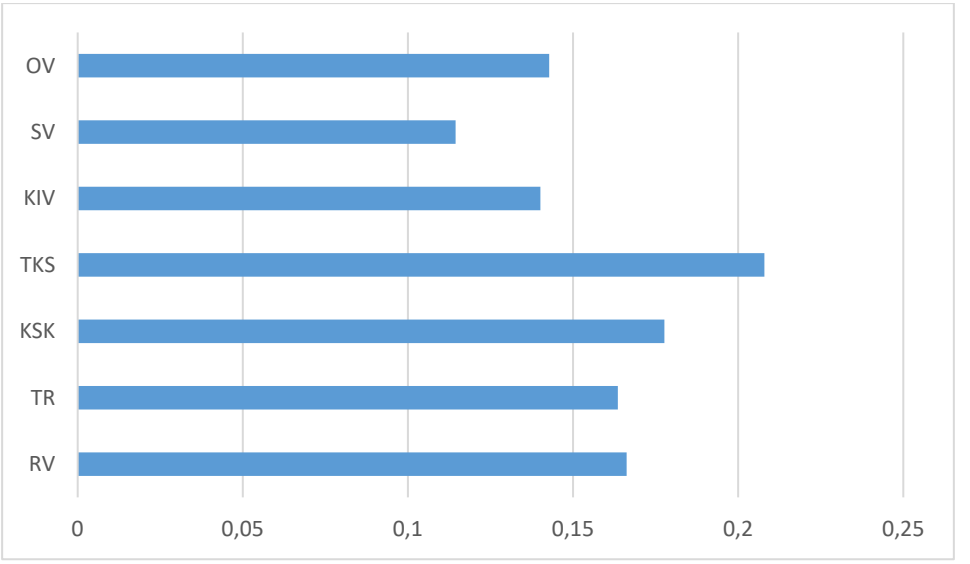
C10 lentelė. Visų komponentų įverčiai ir rangai
Table C10. Estimates and ranks for all components

	E1	E2	E3	E4	E5	E6	
	Įverčiai	Įverčiai	Įverčiai	Įverčiai	Įverčiai	Galutiniai įverčiai	Rangai
RV	0,04	0,06	0,028571	0,028571	0,009091	0,16623	5
TR	0,01	0,01	0,071429	0,031746	0,040404	0,16358	4
KSK	0,01	0,03	0,064286	0,064286	0,009091	0,17766	6
TKS	0,03	0,10	0,02381	0,02381	0,030303	0,20792	7
KIV	0,01	0,04	0,008929	0,035714	0,045455	0,1401	2
SV	0,02	0,01	0,011905	0,011905	0,060606	0,11442	1
OV	0,05	0,01	0,035714	0,035714	0,011364	0,14279	3

OV – organizacijos valdymas, TR – teisinis reguliavimas, KSK – kibernetinio saugumo kultūra, TKS – technologinis kibernetinis saugumas, RV – rizikos valdymas, KIV – kibernetinių incidentų valdymas, SV – strateginis valdymas.

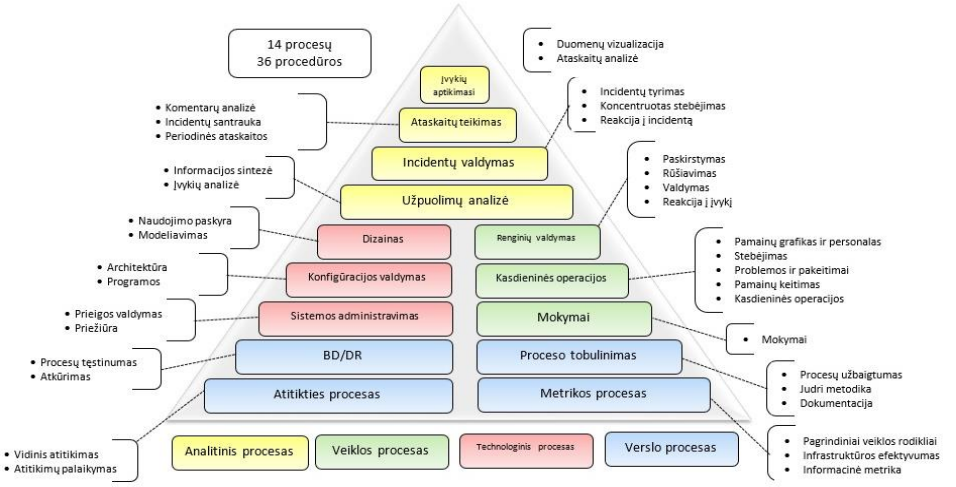


C1 pav. Komponentų įverčių paskirstymas
Fig. C1. Distribution of component estimates



C2 pav. Kibernetinio saugumo komponentų galutiniai įverčiai
Fig. C2. Final estimates for cyber security components

D priedas. Saugos operacijų centro procedūros ir funkcijos



D1 pav. Procesai ir procedūros, sudaryta remiantis Hewlett-Packard development company duomenimis

Fig. D1. Processes and procedures (based on Hewlett-Packard development company)

E priedas. Saugos operacijų cento struktūra

E1 lentelė. SOC galimybių šablonai, sudaryta remiantis Knerler et al. (2022)
Table E.1. Capability Template, based on Knerler et al. (2022)

	Saugumas kaip papildoma atsakomybė	Platinami SOC, maži / jauni, centralizuoti ir federaciniai SOC	Didelis / išvystytas centralizuotas ir federacinis SOC	Hierarchiniai SOC	Koordinavimas ir nacionaliniai SOC
Incidentų rūšiavimas, analizė ir atsakas					
Įspėjimų stebėjimas ir rūšiavimas realiuoju laiku	B	B	A	A	N
Pranešimų apie incidentus priėmimas	B	B	A	A	A
Įvykių analizė ir tyrimas	B	B	A	A	A
Apribojimas, naikinimas ir atkūrimas	B	B	A	A	A
Incidentų koordinavimas	B	B	A	A	A
Artefaktų analizė	N	O	B	A	A
Kenkėjiškų programų analizė	N	O	A	A	A
Reagavimas į „skrydžio“ incidentus	O	O	B	A	A
Kibernetinių grėsmių analizė, paieška ir analizė					
Informacijos apie kibernetines grėsmes rinkimas, apdorojimas ir konsolidavimas	O	B	A	A	O
Informacijos apie kibernetines grėsmes analizė ir rengimas	N	O	B	A	A
Keitimasis informacija apie kibernetines grėsmes ir jos platinimas	N	O	B	A	A
Grėsmių paieška	O	O	A	A	O
Jutiklių nustatymas ir analizė	B	B	A	A	O
Vartotojų analizės ir aptikimo kūrimas	O	O	A	A	O

Duomenų mokslas ir mašinų mokymasis	N	O	B	A	O
Išplėstas SOC veikimas					
Atakų modeliavimas ir įvertinimas	N	O	B	A	A
Apgaulė	N	N	O	O	O
Vidinė grėsmė	N	N	O	B	O
Pažeidžiamumo valdymas (jei yra SOC)					
Ištekliaus atvaizdavimas ir sudėtinės inventorizacijos	B	B	A	A	O
Pažeidžiamumo nuskaitymas	B	B	A	O	O
Pažeidžiamumo vertinimas	N	O	B	A	B
Ataskaitų apie pažeidžiamumų gavimas ir	B	B	B	A	A
Pažeidžiamumo tyrimas, atradimas ir atskleidimas	N	N	O	B	A
Pažeidžiamumų taisymas ir šalinimas	B	O	O	N	N
SOC įrankiai, architektūra ir dizainas					
Anklavinė jutiklių ir SOC architektūra	O	B	A	A	O
Tinklo saugumo galimybių kūrimas ir valdymas	O	B	A	O	O
Endpoint Security kūrimas ir valdymas	B	B	A	O	N
Debesų saugumo galimybių kūrimas ir valdymas	O	B	A	A	N
Mobiliojo ryšio saugumo galimybių kūrimas ir valdymas	O	O	B	O	N
Eksploatacija, technologijos, sauga, projektavimas ir valdymas	O	O	O	O	N
Analitinės platformos kūrimas ir valdymas	O	B	A	A	A
SOC anklavo inžinerija ir valdymas	O	B	A	A	A
Vartotojų patirties plėtra	N	O	B	A	A
Situacijos suvokimas, bendravimas ir mokymasis					
Situacijos suvokimas ir bendravimas	B	B	A	A	A
Vidinis mokymas ir švietimas	O	B	A	A	A
Išorinis mokymas ir švietimas	O	O	O	O	A

Pratimai	O	O	B	A	A
Vadovavimas ir valdymas					
SOC operacijų valdymas	B	B	A	A	A
Strategijos, planavimo ir procesų tobulinimas	O	B	A	A	A
Operacijų tęstinumas	O	B	B	A	A
Metrika	O	B	A	A	A

- **Pagrindinis (B**): šios kategorijos SOC paprastai siūlo šią galimybę / paslaugą pagrindiniu našumo lygmeniu SOC viduje.
- **Išplėstinė (A):** šios kategorijos SOC siūlo šią galimybę / paslaugą pažangesniu, brandesniu našumo lygmeniu SOC viduje.
- **Neprivaloma (O):** šios kategorijos SOC gali pasiūlyti šią galimybę ar funkciją arba jų neteikti. Jų pasirinkimas tai daryti dažniausiai labiau susijęs su jų branda, ištekliais, dėmesiu ir išoriniais reikalavimais, bet nebūtinai su jų organizaciniu modeliu.
- **Nerekomenduojama (N):** mažai tikėtina, kad šios kategorijos SOC pasiūlys šią funkciją ar funkciją namuose. Paprastai taip yra dėl to, kad nėra pagrindinių galimybių ir kompetencijos, riboti ištekliai arba dėmesys sutelkiamas į tai, kas labiausiai tinka organizacijos modelio tipui.

Tomas PLĖTA

KIBERNETINIO SAUGUMO VALDYMO MODELIS VALSTYBIŲ KRITINĖS ENERGETINĖS INFRASTRUKTŪROS SAUGAI TOBULINTI

Daktaro disertacija

Socialiniai mokslai,
Vadyba (S 003)

CYBER SECURITY MANAGEMENT MODEL FOR IMPROVING THE SECURITY OF CRITICAL ENERGY INFRASTRUCTURE OF STATES

Doctoral Dissertation

Social sciences,
management (S 003)

Lietuvių kalbos redaktorė Dalia Markevičiūtė
Anglų kalbos redaktorė Jūratė Griškėnaitė

2024 04 05. 19,8 sp. l. Tiražas 20 egz.
Leidinio el. versija *https://doi.org/10.20334/2024-009-M*
Vilniaus Gedimino technikos universitetas
Saulėtekio al. 11, 10223 Vilnius
Spausdino UAB „Ciklonas“,
Žirmūnų g. 68, 09124 Vilnius