Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Vėjo jėgainių atsparumo kibernetinėms atakoms tyrimas

Baigiamasis magistro projektas

Lukas Eidukevičius

Projekto autorius

Doc. Mindaugas Ažubalis

Vadovas

Kaunas, 2023

Kauno technologijos universitetas
Elektros ir elektronikos fakultetas

Vėjo jėgainių atsparumo kibernetinėms atakoms tyrimas

Baigiamasis magistro projektas
Energijos technologijos ir ekonomika (6211EX073)

Lukas Eidukevičius
Projekto autorius

Doc. Mindaugas Ažubalis
Vadovas

Lekt. Ramūnas Deltuva
Recenzentas

Kaunas, 2023

Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Lukas Eidukevičius

Vėjo jėgainių atsparumo kibernetinėms atakoms tyrimas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama(s) kitų asmenų autoriaus ar kitų teisių, laikydamasi(s) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;

2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąraše;

3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjęs (-usi);

4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta(s) iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Lukas Eidukevičius

Patvirtinta elektroniniu būdu

Eidukevičius, Lukas. Vėjo jėgainių atsparumo kibernetinėms atakoms tyrimas. Magistro baigiamasis projektas / vadovas doc. dr. Mindaugas Ažubalis; Kauno technologijos universitetas, Elektros ir elektronikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): studijų kryptis – energijos inžinerija, studijų krypčių grupė – inžinerijos mokslai.

Reikšminiai žodžiai: vėjo jėgainės, kibernetinis saugumas, kibernetinis atsparumas, kibernetinės atakos, įtaka tinklo dinaminiam stabilumui.

Kaunas, 2023. 69 p.

Santrauka

Didėjant grėsmei ir aktyvėjant Rusijos kibernetiniams sukčiams, kurie atjungė 5800 ir 2000 vėjo jėgainių parkus Vokietijoje ir Austrijoje, taip pat Rusijos laivams atliekant sabotažus prieš Šiaurės jūroje esančių vėjo jėgainių parkų infrastruktūrą, ypatingai svarbu imtis kibernetinio saugumo priemonių, siekiant užtikrinti tokių parkų efektyvų ir saugų veikimą. Tai tampa ypač aktualu, jog Baltijos jūroje iki 2028 metų turėtų atsidaryti du 700 MW vėjo jėgainių parkai, kurių bendras galingumas 1400 MW. Siekiant padidinti vėjo jėgainių kibernetinį atsparumą, šiame magistriniame darbe nagrinėjamas vėjo jėgainių kibernetinis atsparumas ir jo vertinimo metodikos. Darbe apžvelgtos vėjo jėgainių kibernetinio saugumo valdymo, saugumo praktikų, kibernetinių atakų taikinių ir pasekmių temos. Šiame darbe pateikiamas tyrimas, kuriame naudojama vėjo jėgainių kibernetinio atsparumo vertinimo ir reikiamų investicijų į kibernetinį saugumą apskaičiavimo metodikos. Kibernetinio atsparumo vertinimo metodikoje, naudojantis Bajeso atakų grafiku, sudarytas kibernetinės atakos modelis. Naudotas programinės įrangos ir sistemų pažeidžiamumo įvertinimo įrankis CVSS. Naudojantis gautu CVSS įvertinimų, apskaičiuotas vidutinis laikas iki sutrikimo ir vidutinis remonto laikas. Tuomet pagal „Sandia National Laboratories“ tyrėjų pateiktą, vėjo elektrinėms pritaikyta Gordono-Loebo modelį, įvertintos reikalingos investicijos į vėjo jėgainių kibernetinį saugumą. Teorinėje dalyje atskleidus vėjo jėgainių galimą poveikį elektros tinklo stabilumui, nuspręsta ištirti kibernetinėmis ir fizinėmis atakomis paveiktų Lietuvoje planuojamų vėjo jėgainių parkų įtaką Lietuvos elektros tinklo stabilumui. Šis tyrimas aktualus atsižvelgiant į didėjančius kibernetinių incidentų skaičius ir Lietuvoje planuojamus 700 MW jūrinius vėjo jėgainių parkus. Tyrimui buvo naudota PSS/E programa.

Eidukevičius, Lukas. Research of Wind Turbines Resilience to Cyberattacks. Master's Final Degree Project / supervisor assoc. prof. dr. Mindaugas Ažubalis; Faculty of Electrical and Electronics Engineering, Kaunas University of Technology.

Study field and area (study field group): study field – power engineering, study field group – engineering science.

Keywords: wind turbines, cybersecurity, cyber resilience, cyberattacks, influence on network dynamic stability.

Kaunas, 2023. 69.

Summary

With the increasing threat and the growing activity of Russian cyber fraudsters, who disconnected parks with 5,800 and 2,000 wind turbines in Germany and Austria, as well as Russian ships sabotaging the infrastructure of offshore wind parks in the North Sea, it is crucial to take cybersecurity measures to ensure the effective and secure operation of such parks. It becomes especially relevant that in the Baltic Sea, by 2028, two 700 MW offshore wind parks are expected to open, with a total capacity of 1400 MW. To enhance the cybersecurity resilience of wind turbines, this master's thesis examines the cyber resilience of wind turbines and its evaluation methodologies. The thesis reviews topics such as cyber security management of wind turbines, security practices, targets and consequences of cyber attacks. The research presented in this thesis applies a methodology for evaluating the cyber resilience of wind turbines, which was combined with an necessary investment methodology for cyber security. The cyber attack model was developed using Bayesian attack graphs, and the Common Vulnerability Scoring System (CVSS) was used for software and system vulnerability scoring. The average time to disruption and average repair time were then calculated by using CVSS score. In the theoretical part, after revealing the potential impact of wind turbines on the stability of the power grid, it was decided to investigate the influence of wind parks affected by cyber and physical attacks on the stability of Lithuania's power grid.. The PSS/E program was chosen to examine the influence of planned disconnections and short-circuits of 700 MW wind parks in Lithuania on the stability of the Lithuanian power grid.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų sąrašas

Santrumpos:

VJ – Vėjo jėgainė

VJP – Vėjo jėgainių parkas

CVS – Centrinė valdymo stotis

EAP – Elektroninis apsaugos perimetras

EPKSS – Elektroninė praėjimo kontrolės arba stebėjimo sistema

BESIVS – Bendra elektros sistema įrenginiai ir valdymo sistemos

INP – Interaktyvi nuotolinė prieiga

Įvadas

Kibernetinis atsparumas – sistemos gebėjimas palaikyti svarbias operacijas, kai vyksta priešiški veiksmai. Pastarąjį dešimtmetį kibernetinės atakos tapo viena iš didžiausių grėsmių, su kuria susiduria energijos technologijos. Vėjo jėgainės, kaip svarbus ir sparčiai augantis atsinaujinančios energijos šaltinis, nėra išimtis. Vėjo jėgainių sektoriuje pradėjus diegti daiktų internetą (IoT) sistema tapo tarpusavyje sujungtų įrenginių ekosistemos dalimi. Išmanieji jutikliai, valdikliai ir ryšių sistemos įgalino duomenų rinkimą, analizę ir valdymą realiuoju laiku, padidindami veiklos efektyvumą ir įgalindami nuspėjamą priežiūrą. Šios pažangos išplėtė potencialių kibernetinių grėsmių atakos paviršių.

2022 metais įvyko dvejos kibernetinės atakos kurios sustabdė tūkstančius vėjo jėgainių turinčius parkus, šios atakos atskleidė didelę vėjo jėgainių kibernetinio saugumo problemą. Šios atakos rodo, kad būtina imtis priemonių siekiant ištirti galimus vėjo jėgainių atakų taikinius ir suprasti galimą potencialią įtaką elektros tinklui, vėjo jėgainių įrangai, taip pat ir energetikos sektoriui apskritai. Išanalizavus galimus atakos vektorius, tampa aišku kurių sistemos taškų saugumą reikia stiprinti.

Plečiantis vėjo jėgainių parkams ir didėjant vėjo jėgainių įtakai pasaulyje yra svarbu plėsti sektoriaus kibernetinio saugumo žinias, kad būtų galima atskleisti galimas pažeidžiamas vietas ir parengti veiksmingas gynybos strategijas. Tyrimai padės atskleisti, kaip geriausiai apsaugoti vėjo jėgainių sistemą nuo kibernetinių grėsmių ir padidinti vėjo energetikos sistemos saugumą ir patikimumą.

Projekte bus taikomi tokie tyrimo metodai ir modeliai, kaip literatūros analizė, eksperimentinės tyrimų metodikos. Projekte formuluojama hipotezė apie galimą reikšmingą vėjo jėgainių kibernetinių atakų įtaką elektros tinklo stabilumui. Projekte bus apžvelgiami galimi vėjo jėgainių kibernetinių atakų būdai ir galimos atakų pasekmės. Projekto rezultatai galės pabrėžti vėjo jėgainių kibernetinio saugumo didinimo ir reagavimo į kibernetinius incidentus planų paruošimo svarbą.

Darbo tikslas –

atlikti teorinį ir praktinį vėjo jėgainių atsparumo kibernetinėms atakoms tyrimą.

Tiriamasis objektas –

Vėjo jėgainių kibernetinis atsparumas

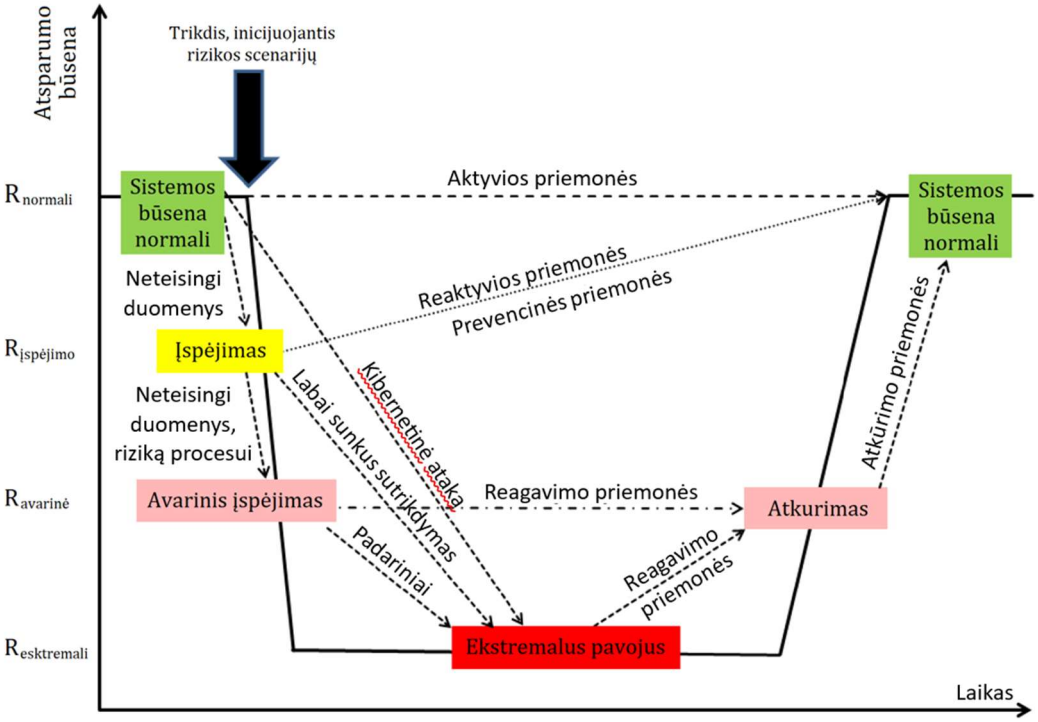
Darbo uždaviniai:

1. Atlikti vėjo jėgainių atsparumo tyrimų apžvalgą, vertinant įvairaus sudėtingumo vėjo jėgainių ir elektros tinklo pažeidžiamumus.
2. Pateikti pasirinktos kibernetinės atakos bei vėjo jėgainių modelius bei vėjo jėgainių atsparumo tyrimo metodiką.
3. Atlikti skaičiavimus su pasirinkta elektros tinklo schema ir pagal pasirinktą metodiką įvertinti vėjo jėgainių atsparumą.
4. Atlikti ekonominį investicijų į vėjo jėgainių kibernetinį saugumą vertinimą.

1. Vėjo jėgainių atsparumas kibernetinėms atakoms

1.1. Atsparumo sąvoka

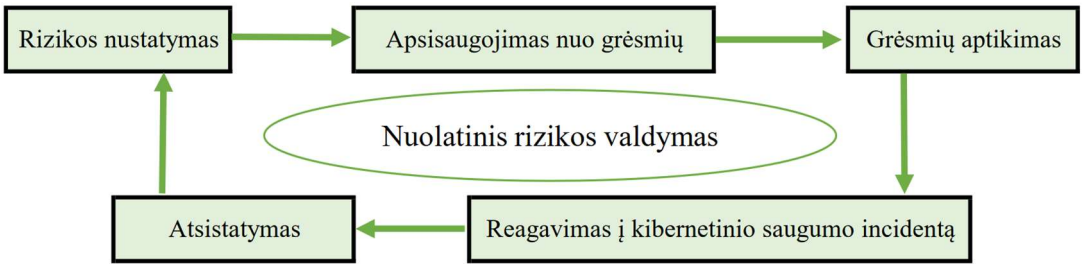
Atsparumo sąvoka reiškia techninių sistemų ar turto gebėjimą laiku ir veiksmingai atsilaikyti, prisitaikyti ir atsistatyti nuo pavojų poveikio, įskaitant esminių jų struktūrų ir funkcijų išsaugojimą ir atkūrimą [61]. Vėjo jėgainių kibernetinis atsparumas reiškia jų gebėjimą apsisaugoti nuo kibernetinių grėsmių ir išlaikyti stabilų bei saugų veikimą. Vėjo jėgainės gali veikti penkiomis veikimo būsenomis: normaliąja, įspėjamąja, avarine, ekstremaliąja (žlugimo) ir atkuriamąja, šios būsenos lygiagrečiai atspindi skirtingus sistemos atsparumo lygius (žr. 1 pav.) [3]. Kibernetiniam atsparumui palaikyti reikalingos aktyvios ir reaktyvios priemonės. Aktyvios priemonės yra saugumo protokolų tobulinimas, reagavimo į kibernetinius incidentus planų kūrimas, kitų išankstinių saugumo priemonių įgyvendinimas. Reaktyviąsias priemones, tokias kaip incidentų tyrimai, žalos kontrolė ir sistemos atkūrimo procedūros [1]. Aktyvių ir reaktyvių priemonių derinys valdymo sistemai atlieka gyvybiškai svarbų vaidmenį, palaikant sistemos atsparumą ir sprendžiant galimas saugumo rizikas bei gedimus.



1 pav. Konceptuali atsparumo kreivė [3]

1.2. Vėjo jėgainių parkų kibernetinio saugumo valdymas

Siekiant patobulinti vėjo jėgainių kibernetinį saugumą yra efektyviai kuriami kibernetinio saugumo modeliai, galintys valdyti rizikas ir padėti apsisaugoti nuo kibernetinių grėsmių. Didėjant kibernetinėms grėsmėms, vėjo jėgainėms gresia įsibrovėlių, darbuotojų, organizuotų grupių, priešiškų valstybių ar teroristų išpuoliai [30]. Siekdama pagerinti kibernetinį saugumą vėjo jėgainėse, „Siemens Gamesa“ sukūrė kibernetinio saugumo rizikos valdymo ir apsaugos modelį (žr. 2 pav.) [37].

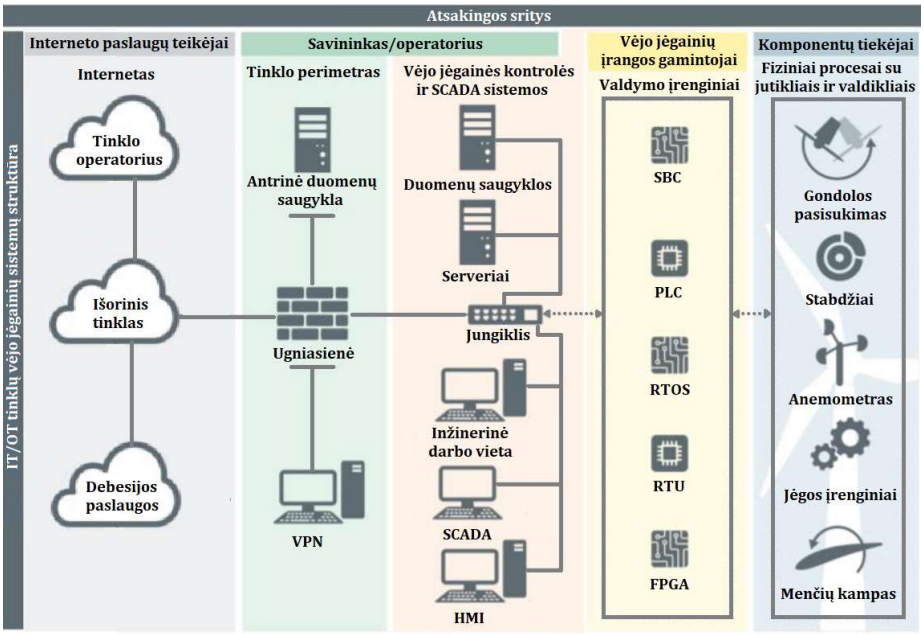


2 pav. „Siemens Gamesa“ Atsilaikymo prieš kibernetinę ataką struktūra, remiantis [37]

Kibernetinės rizikos vertinimas apima žinomų atakų metodų modeliavimą, sistemos ir naudojamų protokolų pažeidžiamumų analizę, ir darbuotojų paskyrų saugumo vertinimus. Apsisaugojimas nuo grėsmių vėjo jėgainėse apima daugybę būdų, įskaitant duomenų šifravimą, ugniasienių diegimą, tinklo segmentavimo priemones ir kitus saugumo sprendimus. Aptikimas apima sistemos būsenų įvertinimą, naudojant pažangius aptikimo algoritmus, tokius kaip: Markovo modelis, Kalmano filtro metodas ir kt. Atsižvelgiant į atakos padarinius, siekiant sumažinti pavojų, reikia turėti paruoštus planus ir žinoti kaip reaguoti į kibernetinio saugumo incidentus [26].

Kita vėjo jėgainių kibernetinį atsparumą didinanti struktūra, yra „Sandia National Laboratories“ (SNL) struktūra, kuri yra pranašesnė už „Siemens“ atvejo struktūrą. SNL siūlomas papildomas apsisaugojimo žingsnis - dalijimasis kibernetinės atakos metu surinkta informacija su kitomis vėjo jėgainių organizacijomis.

Kibernetinis saugumas vėjo jėgainių kontekste priklauso nuo kolektyvinių grupių ir organizacijų pastangų, kurios reikalauja bendradarbiavimo, dalijimosi informacija ir koordinuotų veiksmų sprendžiant kylančias kibernetinio saugumo probledmas. Už sklandų ir saugų vėjo jėgainių eksploatavimą atsakingi subjektai yra: interneto paslaugų teikėjai, savininkai/operatoriai, vėjo jėgainių įrangos gamintojai, komponentų tiekėjai. (žr. 3 pav.) [2].

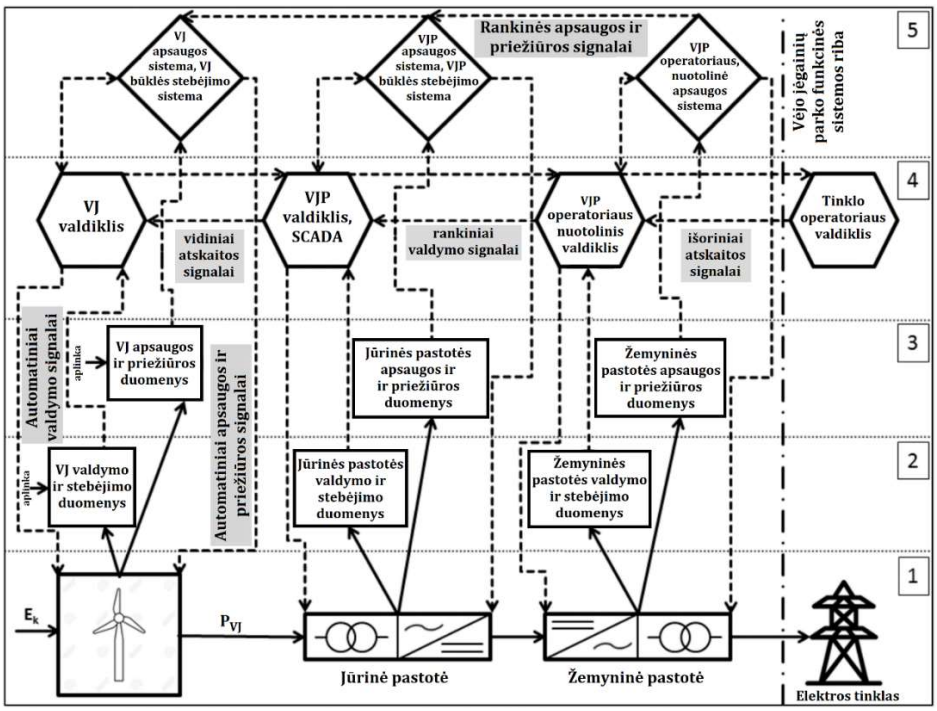


3 pav. Scheminis IT/OT infrastruktūros vaizdas vėjo jėgainėje [2]

„Siemens Gamesa“, „Vestas“, „GE“, „Enercon“ ir „Nordex“ yra pirmaujančios vėjo jėgainių gamintojos, kurios tai pat aktyviai deda pastangas siekdamos pagerinti vėjo jėgainių kibernetinį saugumą. Kibernetinės grėsmės gali sukelti didelę žalą jų reputacijai ir turtui, todėl šios įmonės diegia naujausias kibernetinio saugumo priemones, investuoja į pažangias technologijas ir sprendimus, kurie leidžia užtikrinti aukštą apsaugos lygį nuo potencialių kibernetinių atakų. Vėjo jėgainių savininkai ir operatoriai turėtų aktyviai sekti šių įmonių internetinius puslapius ir stebėti pateikiamą kibernetinio saugumo informaciją bei patarimus. Šios įmonės dažnai skelbia gerosios praktikos vadovėlius, rekomendacijas ir saugumo patarimus, kurie gali padėti stiprinti vėjo jėgainių kibernetinį saugumą.

1.3. Vėjo jėgainių parko funkcinis modelis

Funkcinis modelis parodo techninę sistemos elgseną, jos veikimo struktūrą ir funkcionalumą (žr. 4 pav.). VJP funkcinis veikimo modelis susideda iš penkių sluoksnių. Pirmasis yra energijos konvertavimo sluoksnis, kuriame vėjo energiją konvertuojama į elektros energija tuomet ji perduodama į pastotes, o iš pastočių į elektros tinklą. Antrasis yra duomenų gavimo sluoksnis, šiame sluoksnyje renkami reikalingi duomenys VJP valdymui ir stebėjimui. Trečiasis apsaugos ir priežiūros duomenų gavimo sluoksnis, kuris renka duomenis saugumo ir priežiūros tikslais. Ketvirtasis valdymo ir stebėjimo sluoksnis, kontroliuoja energijos konversiją ir stebi sistemos veikimą. Penktasis apsaugos ir priežiūros sluoksnis, užtikrina VJP saugumą ir struktūrinį vientisumą trikdžių metu [3].



4 pav. Bendrojo OVJP funkcinis modelis. VJ – vėjo jėgainė, VJP – Vėjo jėgainių parkas ištisinės rodyklės yra energijos/materijos srautai, punktyrinės linijos signalų/duomenų srautai [3]

VJP funkcinio modelio supratimas yra svarbus žingsnis siekiant įvertinti vėjo jėgainių kibernetinį atsparumą. Tai reiškia, kad kibernetinio saugumo grėsmės ir atsparumo priemonės turi būti įvertintos kiekviename VJP modelio sluoksnyje, o kibernetinio saugumo kontrolė turi būti koordinuojama visoje VJP sistemoje.

1.4. Saugumo praktikos ir rekomendacijos

Vėjo jėgainių technologijų srityje labai svarbus nuolatinis kibernetinio saugumo metodų tobulinimas ir dalinimasis informacija tarp vėjo jėgainių organizacijų. Bendradarbiavimo ir dalijimosi žiniomis tarp organizacijų skatinimas tampa itin svarbus siekiant sustiprinti bendrą sektoriaus apsaugą nuo besivystančių grėsmių. Šis iniciatyvus požiūris užtikrina nuolatinį vėjo jėgainių saugumą ir atsparumą, leidžiantį joms veiksmingai prisitaikyti prie būsimų iššūkių nuolat kintančioje kibernetinio saugumo aplinkoje. JAV Energetikos departamentas pateikia geriausios saugumo praktikos rekomendacijas kurios pateiktos pirmoje lentelėje [32].

1 lentelė. Rekomenduojamos vėjo jėgainių kibernetinio saugumo praktikos [32]

Vėjo kibernetinės kultūros plėtojimas	Nustatymas ir apsisaugojimas	Aptikimas	Reagavimas ir atsistaymas
Skatinti ir teikti išteklius kibernetinės saugos tyrimams.	Atlikti kibernetinės saugos vertinimus.	Išlaikyti pilną situacijos supratimą apie OT aplinką.	Mokytis geriau atpažinti ir greičiau pranešti apie galimus kibernetinius incidentus ar kenkėjišką veiklą.
Organizuoti suinteresuotų šalių kibernetinio saugumo darbo grupes ir kibernetinio saugumo vertinimus	Organizuoti kibernetinės higienos mokymus personalui.		Nustatyti kibernetinio saugumo vaidmenis ir atsakomybes.
Skatinti tiekėjus organizuoti klientų apklausas apie kibernetinio saugumo funkcijas. Dalyvauti informacijos bendrinimo programose.	Naudoti efektyvius tinklo segmentavimo metodus.	Naudoti įsibrovimo aptikimo metodus.	Paruošti reagavimo į kibernetinius incidentus planus.
Visos suinteresuotosios šalys turi dalyvauti atkūrimo procese reaguojant į pokibernetinius incidentus.	Tvarkyti kibernetinio turto sąrašus, juos nuolatos atnaujinti.		Savininkams ir operatoriams įsteigti reagavimo į kibernetinius incidentus komandas, kurios daugiausia dėmesio skiria vėjo energijai ir ekspertinėms žinioms.
	Naudoti įrenginių autentifikavimo lygius.	Nuolatos stebėti ir analizuoti tinklo duomenis dėl anomalios veiklos ir grėsmių.	
	Taikyti tinkamą fizinę pastatų ir įrangos saugumo kontrolę.		Įgyvendinti reagavimo į kibernetinius incidentus planus.
	Pardavėjams kurti kibernetiškai atsparias vėjo energijos technologijas.		Paslaugų teikėjams laiku pateikti atnaujinimus ir įrangos pataisymus.

VJ sektoriui reikalinga skaitmeninė ekosistema, kurios tikslas yra skatinti bendradarbiavimą ir bendras inovacijas, suteikiant centrinę platformą, kurioje suinteresuotos šalys galėtų keistis informacija ir įžvalgomis, susijusiomis su vėjo jėgainių sektoriumi [4].

Siekiant pagerinti VJ atsparumą kibernetinėms grėsmėms, yra svarbu, kad į kuriama ekosistemos platformą būtų įtrauktos VJ kibernetinio saugumo tema. Tai leistų skleisti žinias apie VJ kibernetinio saugumo rizikas, pažeidžiamumus, atsakomąsias priemones, geriausias praktikas ir sprendimus būdingas vėjo jėgainių sistemoms. Skatinant bendradarbiavimą ir keitimąsi informacija, ekosistema organizacijoms padėtų sukurti kibernetinio atsparumo kultūrą.

1.4.1. Kibernetinio saugumo technologijų efektyvumas vėjo energijos sektoriuje

Tam, kad būtų užtikrintas vėjo jėgainių tinklų kibernetinis saugumas, būtina tirti ir stebėti sistemos atsparumą kibernetinėms atakoms. Tyrimo grupė sukūrė bandymų prietaisų skydelį, kuriame buvo integruoti įspėjimai, tendencijos ir metrika kuri padeda stebėti sistemos kibernetinį atsparumą [4]. Šiame tyrime modeliuoti du atakų scenarijai. Pirmoji ataka buvo vykdoma nuotoliniu būdu, pasisavinus prisijungimo duomenis ir pasinaudojant VPN kanalais. Antroji ataka vykdyta vietinėje aplinkoje, užpuolikui sugadinus VJ durų užraktą ir prisijungus prie vietinio tinklo. Abiejų atakų atveju pagrindinis tikslas buvo pakeisti jėgainės nustatymus. Tyrėjai imitavo kibernetines atakas virtualioje aplinkoje ir įvertino skirtingų saugumo priemonių poveikį kibernetiniam ir fiziniam saugumui (žr. 2 lent.).

2 lentelė. Kibernetinio-fizinio atsparumo įvertinimas priklausomai nuo skirtingų saugumo įrankių. SIEM – saugos informacijos ir įvykių valdymas. Informacijos teikimas kibernetinės saugos komandoms; HIDS – pagrindinio kompiuterio įsibrovimų aptikimo sistema; NIDS - tinklo pagrindu veikianti įsilaužimo aptikimo sistema; SOAR - Saugumo organizavimas, automatizavimas ir reagavimas, tai metodai, apibrėžiantys kaip sustabdyti kibernetinę ataką ir atsigauti nuo neigiamo poveikio [6].

Technologija / Bandymas	Kibernetinė ataka	Šifravimas	Prieigos kontrolė	SIEM	HIDS	NIDS	SOAR	Kibernetinis atsparumas	Fizinis atsparumas
1	Nuotolinė	Bazinė						38,5%	46,6%
	Vietinė							61,5%	17,2%
2	Nuotolinė	X	X					46,2%	100%
	Vietinė							69,2%	100%
3	Nuotolinė			X		X		84,6%	100%
	Vietinė							92,3%	100%
4	Nuotolinė	X		X	X			53,8%	100%
	Vietinė							84,6%	100%
5	Nuotolinė			X	X	X	X	84,6%	100%
	Vietinė							92,3%	100%

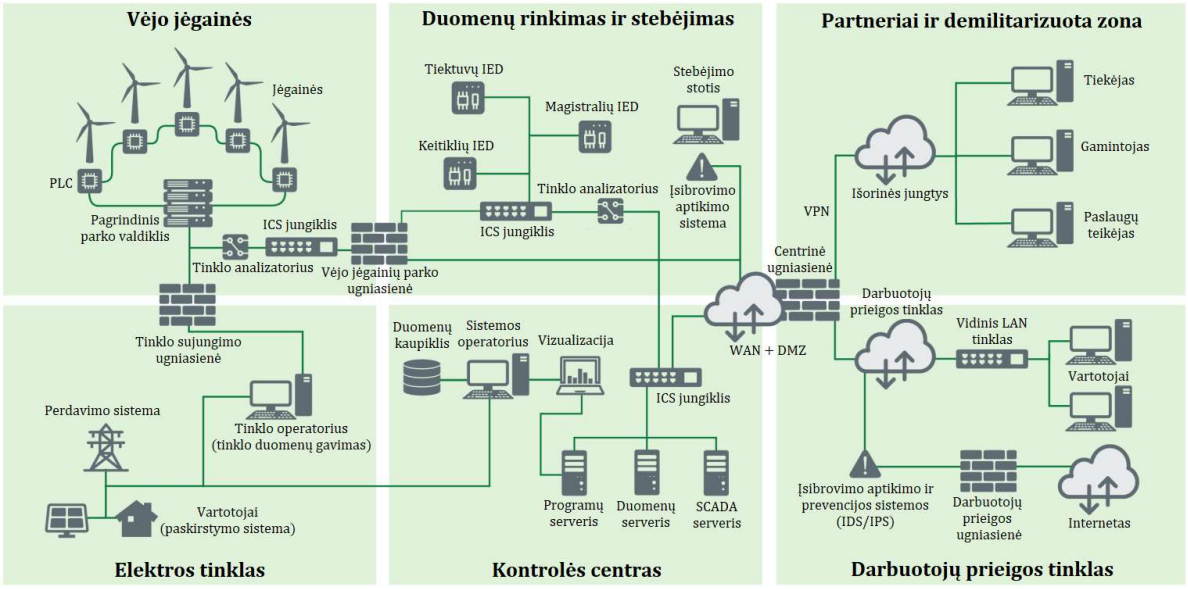
Šio tyrimo trečiasis ir penktasis bandymai atskleidė, kad kai sistemoje yra įdiegtos SIEM ir NIDS technologijos, papildomos investicijos į HIDS ir SOAR saugumo priemonės, visiškai nereikalingos, nes papildomai įdiegus šias technologijas nei fizinis, nei kibernetinis atsparumas nepakito. Atakų aptikimo technikas išmaniajame tinkle galima suskirstyti į penkias kategorijas taip kaip pavaizduota trečioje lentelėje [5].

3 lentelė. Kibernetinių atakų aptikimo technikų privalumai ir trūkumai [5].

Aptikimo technika	Funkcija	Privalumai	Trūkumai
Lokalizavimu pagrįsti metodai	Kibernetinių atakų šaltinio ar vietos nustatymas	Mažiau sudėtingas. Nebūtina žinoti tikslią kenkėjiško vartotojo ar užpuoliko vietą	Ilgas sinchronizavimo ir apdorojimo laikas.
Dirbtinis intelektas	Mašininio mokymosi algoritmais pagrįstos didelių duomenų analizės	Paprastai didelis aptikimo diapazonas ir maža klaidingo aliarmo tikimybė.	Mokymosi procesui ir testavimui reikalingas tinkamas duomenų rinkinys.
Prognozavimo modeliai	Naudoja statistinius metodus ir laiko eilučių duomenis būsimų tendencijų ir elgsenos prognozei	Dabartinių ir istorinių duomenų analizė. Tendencijų supratimas. Nustato galimą riziką ir naudingas ateities galimybes.	Neišsami ir prasta duomenų kokybė, lemia netikslius rezultatus.
Filtravimu pagrįstas metodas	Pagal nustatytas vertes stebi tinklo srautą, nustato anomalijas ir įsibrovimus	Lengvas įgyvendinimas. Patikimas.	Paprastai iš anksto nustatomos kriterijų vertės. Skaičiavimo sudėtingumas.
Įsibrovimo aptikimo sistema	Sistemos kurios nuolat stebi tinklo srautą, tikrina saugumo informaciją ir aptinka	Nereikia centralizuoti.	Didė klaidos tikimybė. Naudoja daug atminties išteklių.

1.5. Vėjo jėgainių kibernetinių atakų taikiniai

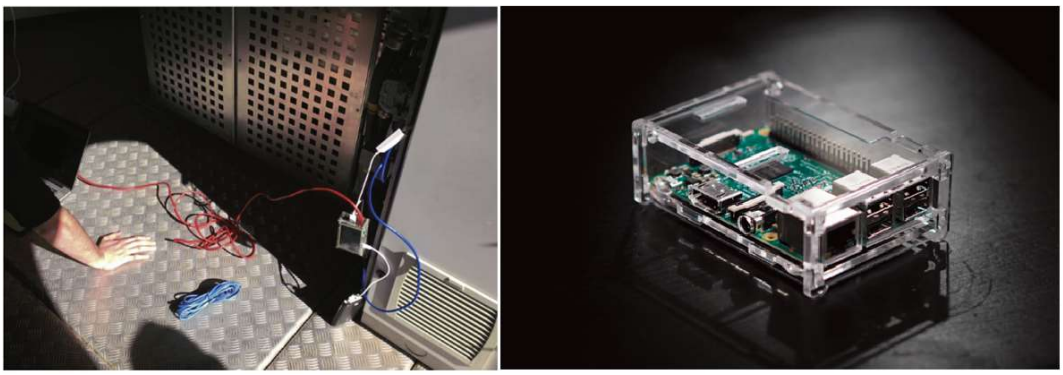
Vėjo elektrinių parko valdymo sistema yra sudėtinga sistema, apimanti įvairius įrenginius ir komponentus, skirtus valdyti ir stebėti vėjo jėgainių veikimą, gauti duomenis ir integruotis į elektros tinklą. Vėjo elektrinių parko valdymo sistemą sudaro šešios esminės sritys: vėjo jėgainių, duomenų rinkimo ir stebėjimo, partnerių ir demilitarizuotos zonos, elektros tinklo integravimo, kontrolės centro ir darbuotojų prieigos tinklo sritys kurios su joms priklausančiais įrenginiais pavaizduotos penktame paveiksle.



5 pav. Vėjo jėgainių parko valdymo sistemų architektūra [32]

Vėjo jėgainės, kurios buvo įdiegtos vienos pirmųjų vėjo jėgainių sektoriuje, jos buvo projektuotos netaikant kibernetinio saugumo reikalavimų, senos technologijos nėra pritaikytos moderniems saugumo reikalavimams [39]. Todėl vėjo jėgainių įrangą reikia keisti iš esmės, senų technologijų naudojimas kelia grėsmę kibernetiniam saugumui, nes sena įranga negali palaikyti naujausių programinių įrangų. Vėjo jėgainių saugumo problemos kilo dėl praeityje neapibrėžtų atsakomybės ribų, saugumo reikalavimų stokos, taip pat dėl pigių SCADA ir saugos kamerų sistemų, kurias diegiant praeityje nebuvo atsižvelgiama į kibernetinį saugumą [40]. Atnaujinant senas ir diegiant naujas kibernetinio saugumo technologijas vėjo jėgainėse, „Europos vėjo energijos asociacija“ rekomenduoja naudoti IEC62443 standartą [34].

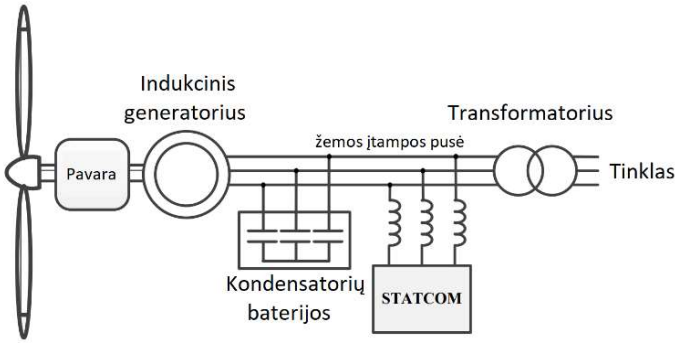
„University of Tulsa“ tyrime „Vėjo jėgainių parko saugumas: atakos paviršius, taikiniai, scenarijai ir švelninimas“ teigia, kad sugadinti vėjo jėgainės įėjimo durų spyną ir patekti į vėjo jėgainę užteko mažiau nei minutės [14]. Patekus į vėjo jėgainę tyrėjai „Ethernet“ kabeliu sujungė „Raspberry Pi“ mini kompiuterį ir PLC vėjo jėgainės valdiklį (žr. 6 pav.). Taip įgavo ne tik atakuojamos vėjo jėgainės stebėjimo ir kontrolės teisę, bet ir pasiekė kitų tame pačiame tinkle sujungtų jėgainių valdymo įrenginių IP adresus. Tinklo dizainas, kuomet tarp vėjo jėgainių valdymo sistemų nėra saugumo mechanizmų, leidžia užpuolikui nusitaikyti į kitas vėjo jėgaines [14].



6 pav. „Raspberry Pi“ įrenginio prijungimas prie vėjo jėgainės kairėje, „Raspberry Pi“ įrenginys dešinėje [14,64]

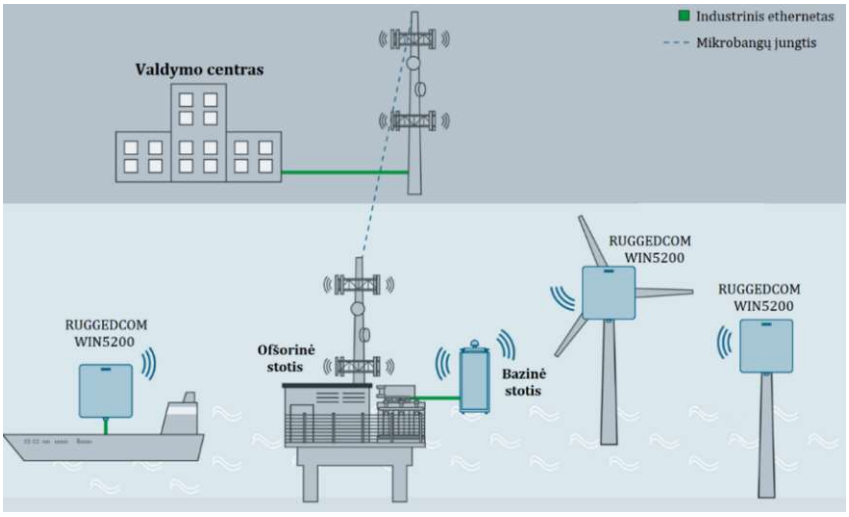
Norint sumažinti fizinių atakų riziką, svarbu įgyvendinti tokias priemones kaip anomalijų aptikimo sistemos, USB prievado saugumas, fizinės prieigos kontrolė, tinklo segmentavimas, prieigos kontrolės ir autentifikavimo mechanizmai, turi būti rengiami reguliarūs saugumo vertinimai ir mokymai, skirti darbuotojus informuoti apie kibernetinį saugumą. Įgyvendindami šias priemones VJ operatoriai gali sustiprinti savo valdymo sistemų saugumą ir sumažinti galimas rizikas [14].

STATCOM (STATic synchronous COMpensator) tai įrenginys pagerinantis galios koeficientą ir reguliuoja sistemos įtampą (žr. 7 pav.). Šis įrenginys skirtas reaguoti į įtampos pokyčius ir prireikus tiekti reaktyviosios galios palaikymą vėjo jėgainių sistemai. Klaidingų duomenų įvedimo ataka gali paveikti generatoriaus valdymo sistemos kintamosios srovės įtampos jutiklį, ir pateikti sistemai klaidingas AC įtampos vertes, kurios gali priversti „STATCOM“ kompensuoti įtampos kritimą ir į jėgainės sistemą tiekti perteklinę reaktyviąją galią [12]. Dėl to gali prasidėti sistemos kondensatorių baterijų perteklinės reaktyviosios galios absorbcija, ir įtampos vertės gali pasiekti maksimalią vertę [12]. Tai gali sukelti apsauginės generatoriaus įtampos kontrolės relės suveikimą ir generatoriaus atsijungimą nuo tinklo [16].



7 pav. STATCOM statinis sinchroninis kompensatorius [23]

Siemens paskelbė vėjo jėgainėse naudojamų pramoninių ryšio produktų, naudojamų DHCP (angl. Dynamic Host Configuration Protocol) pažeidžiamumą, tokiuose kaip „RUGGEDCOM WIN5200“ (žr. 8 pav.). Tai pramoninis belaidžio ryšio maršrutizatorius, naudojantis Wi-Fi, LTE, 4G, 3G ryšius. Dėl šio pažeidžiamumo užpuolikas gali sukelti sistemos įrenginio perpildymą duomenimis (angl. buffer overflow) [41]. CVSS įvertinimas šiam pažeidžiamumui įvertintas 9,8 iš 10, tai reiškia pažeidžiamumas gali būti nesunkiai išnaudojamas ir gali pridaryti kritinės žalos valdymo sistemai.



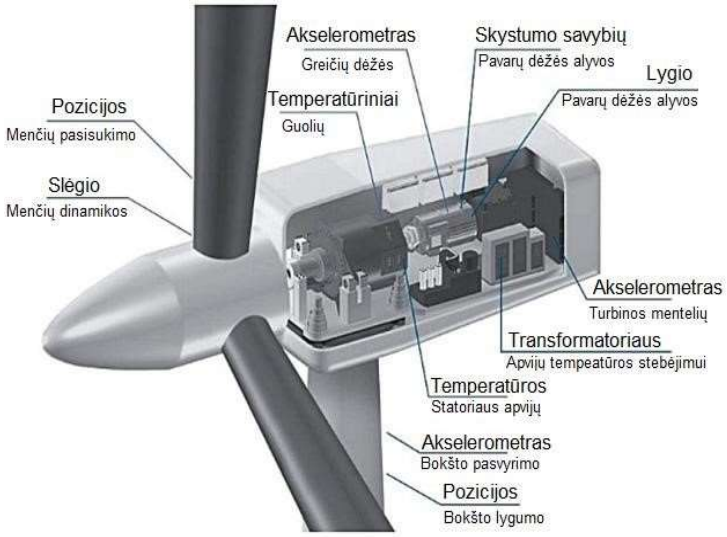
8 pav. „Siemens“ „RUGGEDCOM WIN5200“ panaudojimo schema [47]

DHCP priskiria įrenginiams IP adresus ir nustatymus. Užpuolikas gali atakuoti sistemą, jei sužino unikalius IP adresus. Jei saugumo funkcijos yra apeinamos, užpuolikas gali sukelia duomenų perpildymą per specialų DHCP paketą, leidžiantį įvykdyti kenkėjiško kodo įvedimą į sistemą. Tai gali lemti vėjo jėgainės(-ių) išjungimą ir jos įrenginių sugadinimą [41].

Plečiantys vėjo jėgainių parkams ir didėjant jų įtakai energetikos sektoriuje, valstybės institucijos turi imtis veiksmų, kurie užtikrintų vėjo jėgainių kibernetinį saugumą atsakingų šalių, tinkamą funkcijų atlikimą. Turi būti priskirtos kompetentingos institucijos, kurios būtų atsakingos už reguliarius kibernetinio saugumo auditus. Auditų metu turėtų būti tikrinama ar yra vėjo jėgainėse yra laikomasi kibernetinio saugumo funkcijų, ar programinė įranga yra laiku atnaujinama, ar yra vėjo jėgainėse yra taikomos tinkamos fizinio saugumo priemonėmis. Tokie auditai padidintų kibernetinio saugumo lygį vėjo jėgainių sektoriuje.

1.5.1. Vėjo jėgainių jutiklių saugumo aspektai ir autentifikavimo metodai

Vėjo jėgainių jutiklius pagal jų svarbą galima suskirstyti į dvi kategorijas. Pirmajai kategorijai priklauso vėjo jutikliai, kurie yra gyvybiškai svarbūs vėjo jėgainių veikimui ir tiesiogiai veikia elektros energijos gamybą. Tai apima vėjo krypties, greičio jutiklius, menčių padėties, gondolos pasisukimo padėties, rotoriaus greičio jutiklius ir t.t. Antroji kategorija apima jutiklius atsakingus už įrenginių techninę būklę, kurie naudojami stebėjimo ir priežiūros tikslais ir nėra tiesiogiai susiję su elektros gamyba. Šie jutikliai apima vibracijos ir temperatūros jutiklius, poslinkio jutiklius, tepalo, alyvos lygio jutiklius, alyvos tepimo jutiklius, slėgio jutiklius ir t.t. (žr. 9 pav.)

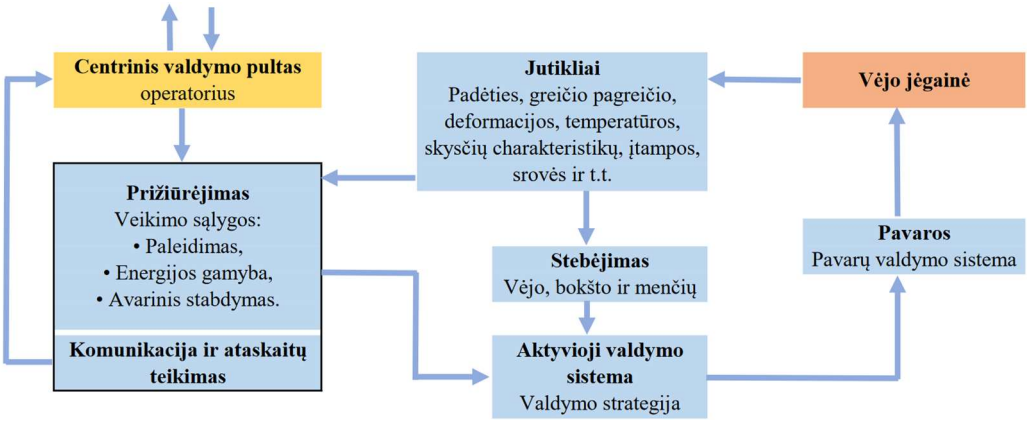


9 pav. Vėjo jėgainės jutikliai [49]

Informacijos perdavimas iš jutiklių turi būti anonimiškas, apsaugotas nuo atakų ir greitas. Kriptografinio raktų generavimo pagrįstas autentifikavimo metodas yra efektyvus apsaugos lygis, kuris naudoja vienkryptę maišos funkciją ir raktų grandinę. Jutiklis siunčia užklausą centrinei stebėjimo sistemai, nurodydamas būseną ir sugeneruotą grandinės raktą. Sistema naudoja raktą, kad patvirtintų pranešimo autentiškumą, palygina jį su ankstesniuoju raktu, ir procesas kartojamas, kol jutiklis praeina visus nustatytus grandinės taškus [13].

1.6. SCADA vaidmuo vėjo jėgainėse ir SCADA sistemos saugumo iššukiai

SCADA tai Priežiūros kontrolės ir duomenų gavimo sistema. SCADA yra būtina vėjo jėgainių priemonėje. SCADA yra pagrindinė sąsaja tarp vėjo jėgainės operatoriaus ir vėjo jėgainių parko įrangos. SCADA sistema renka vėjo jėgainės įrenginių, jutiklių, pavarų, valdiklių duomenis, bei juos vizualizuoja operatoriaus valdymo pulto ekrane (žr. 10 pav).



10 pav. Vėjo jėgainių valdymo sistemos architektūra [25]

Pagrindiniai įvesties duomenys į SCADA sistemą apima vėjo greitį, rotoriaus greitį, menčių žingsnį, elektros energiją ir temperatūrą kritinėje srityje. Tačiau kai kurios sistemos apima įtempimus, įtempius (bokšto, menčių), greitį, padėtį (posūkį, pavaras, rotoriaus posvyrį, svyravimo kampą, skysčio savybes ir lygius, elektros sistemą (sroves, įtampą, komunalinio tinklo charakteristikas), apledėjimo sąlygas, apšvietimas, drėgmė) [25].

Elektros energijos paskirstymas ir transformacija vykdoma elektros pastotėse, kurios yra vienos svarbiausių elektros tinklų komponentų. Pastotės darbo sutrikdymas gali sukelti didelių tinklo sutrikimų. Kadangi pastočių įrenginiai vis labiau skaitmeninami, automatizuojami ir susiejami su išoriniais tinklais, todėl pastotės tampa pažeidžiamos kibernetinių atakų.

2016 m. Ukrainos energijos skirstymo operatorius „Ukrenergo“ patyrė kenkėjiškos programos „Crashoverride“ ataką, užpuolikai įsilaužę į SCADA tinklą ir naudodamiesi „Siemens“ kompanijos RTU valdiklio pažeidžiamumu, atidarė elektros pertraukiklių grandines, taip 225 000 žmonių šešioms valandoms neteko elektros energijos [31].

2015 metais „Sandworm Team“ įvykdė kibernetinę ataką prieš Ukrainos energijos skirstymo operatoriaus SCADA sistemas, atjungdama nuo elektros tinklo 30 pastočių ir be elektros palikdama daugiau nei 200 000 klientų, pavogdama VPN kredencialus, naudodama nuotolinės prieigos priemones ir paleisdama „DDoS“ atakas ir operatoriaus sistemose įdiegdama modifikuota standžiojo disko valymo programinė įranga „Killdisk“, todėl buvo ištrinti duomenys iš valdymo sistemų, įskaitant UPS sistemas [7].

Siekiant užkirsti kelią vėjo jėgainių kibernetinėms atakoms ateityje, būtina sustiprinti tinklo saugumo stebėjimo galimybes, apriboti prieigos taškus ir įdiegti tokias priemones kaip: dviejų veiksnių autentifikavimas, blokų grandinės technologija, ir įsibrovimo aptikimo sistemas [15]. Ukrainos energijos skirstymo operatoriaus patirtis rodo, kad reikia tobulinti ypatingos svarbos infrastruktūros objektų kibernetinio saugumo protokolus. Vyriausybės ir privačios organizacijos turėtų investuoti į

savo darbuotojų mokymą ir naujausių saugumo technologijų taikymą, kad apsisaugotų nuo kibernetinių atakų.

Vėjo jėgainių ir valdymo sistemoms apsaugoti yra taikomos prevencinės priemonės. Saugumo priemonės yra bendras terminas, apimantis skirtingas priemones ir technologijas, kurios skirtos užtikrinti, kad informacijos ir IT sistemos būtų apsaugotos. Išskiriamos pagrindinės vėjo jėgainių saugumo priemonių kategorijos pavaizduotos ketvirtoje lentelėje [5].

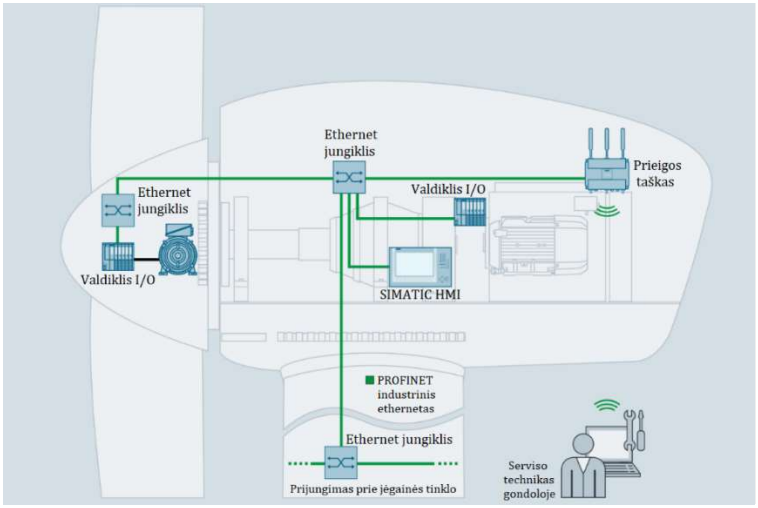
4 lentelė. Saugumo priemonių privalumai ir trūkumai [5].

Saugumo priemonė	**Privalumai**	**Trūkumai**
Saugūs protokolai ir standartai	Lankstumas. Paprasta valdyti ir prižiūrėti.	Nėra labai saugių protokolų išmaniame tinkle. Mažas ryšių pasirinkimas.
Kriptografija ir autentifikavimas	Kriptografinių algoritmų nauda. Konfidencialumas.	Įgyvendinimo sudėtingumas. Ne visada efektyvus.
Įsibrovimų aptikimo prevencija	Aukštas apsaugos lygis.	Reikia įgyvendinti su kitais atsakomųjų priemonių metodais.
Sklaidos spektro metodai (ryšio signalų keitimas)	Aukštas apsaugos lygis.	Sudėtingas įdiegimas. Neefektyvus pralaidumas.
Darbuotojų mokymas	Paprastumas. Suteikia saugumo žinių darbuotojams.	Nepakanka apsaugoti ir užkirsti kelią nuo atakų.
Prieigos kontrolė ir kibernetinio saugumo politika	Didelis mastelio keitimas. Paprasta naudoti.	Neužtikrina apsaugos nuo atakų. Tinka mažiems tinklams.

JAV kibernetinio saugumo ir infrastruktūros saugumo agentūra išleido bendrą kibernetinio saugumo patarimą, įspėjantį, apie kibernetinius sukčius kurie turi galimybę gauti visą sistemos prieigą prie kelių pramoninės valdymo sistemos (ICS) / priežiūros valdymo ir duomenų gavimo (SCADA) įrenginių: „Schneider Electric PLC“, „OMRON Sysmac NEX PLC“ ir „OPC UA“ serverių, gavę prieigą sukčiai gali nuskaityti, pažeisti ir valdyti paveiktus įrenginius [42].

Norint apsaugoti sistemų nuotolinės prieigos prie ICS (angl. Indsutrial Control System) ir jos įrenginiai turi būti apsaugoti kelių veiksnių autentifikavimu, slaptažodžiai turi būti reguliariai keičiami. Svarbu kad visų įrenginių ir sistemų numatyti gamykliniai slaptažodžiai būtų pakeisti į naujus ir unikalius slaptažodžius. ICS/SCADA sistemų apsaugojimui naudoti stebėjimo sistemas, kurios yra sukurtos nuolatiniam ir automatiniam operacinių technologijų (OT) tinklo stebėjimui [42].

2022 m. Siemens paskelbė vėjo jėgainėse naudojamų „SIMATIC SCADA“ HMI (žr. 11 pav.) kuris bendru pažeidžiamumų vertinimo balų (CVSS) vertinamas 9,9 balams iš 10. Tai reiškia, kad pažeidžiamumas yra priskiriamas labiausiai pažeidžiamam, kritiniam saugos lygiui ir į jį būtina greitai reaguoti ir imtis veiksmų. Atrasti pažeidžiamumai gali leisti užpuolikams išplėsti privilegijas, stebėti, redaguoti arba ištrinti svarbias duomenų rinkmenas sistemoje [43]. Ataka inicijuojama užpuolikui sugeneravus duomenų rinkmeną su specialiu pavadinimu, kuriame yra specialieji ženklai: kabutės ir pasvirieji brūkšniai, tuomet į pavadinimą įšvirkščiamas nulinis baitas ir siunčiamas sistemai, sistema į gaunamą duomenų rinkinį, sureaguoja kaip į užduotą komandą ir pradeda vykdyti užpuoliko komandą [42].

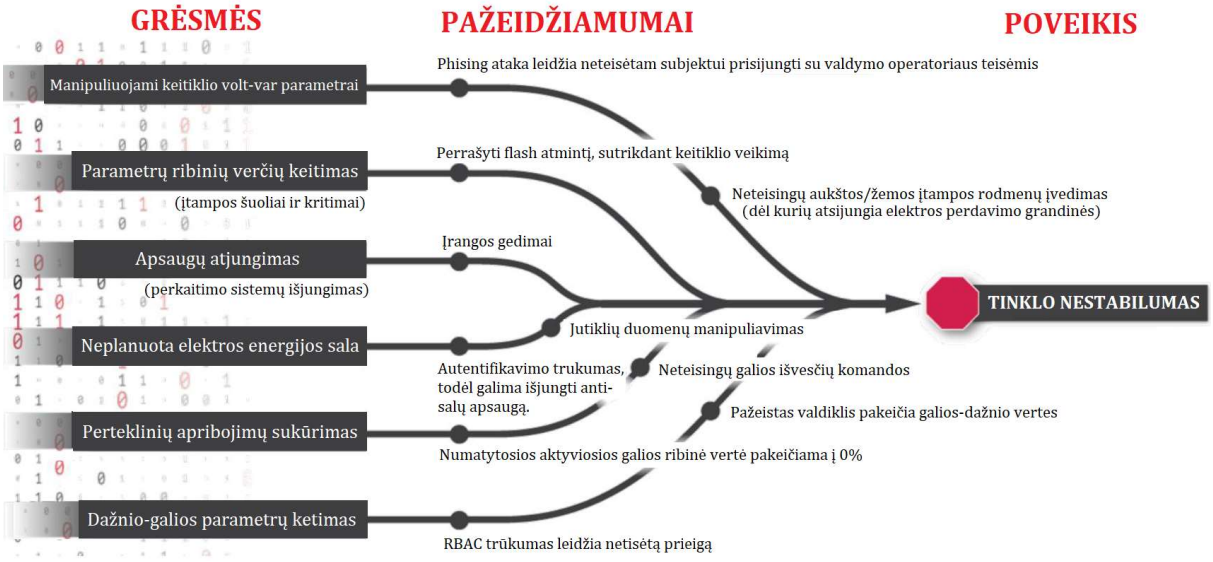


11 pav. SIMATIC HMI įrenginys [47]

Norint apsaugoti vėjo jėgainių sistemas nuo atakų, atsakingi asmenys už vėjo jėgainių saugumą turėtų nuolat stebėti naujausius kibernetinius pažeidžiamumus ir jų ištaisymo būdus, taip pat rinkti informaciją apie naujus išpuolių būdus, kad būtų galima apsaugoti savo sistemas nuo naujų grėsmių.

1.7. Vėjo jėgainių kibernetinių atakų pasekmės

Vėjo jėgainių kibernetinės atakos gali turėti rimtų ekonominiu, aplinkosaugos ir geros reputacijos praradimo padarinių [34]. Kalbant apie kibernetinės atakos metu patirtus nuostolius juos gali atlyginti draudimo kompanijos, bet draudimo įmokos po patirtos kibernetinės atakos didėtų ženkliai, kadangi nuostoliai gali siekti milijonus ar net milijardus eurų [33]. Įsilaužėliai vėjo jėgainių sistemoje gali paveikti valdymo sistemas, vėjo jėgainės jutiklius ir kitus įrenginius. Ataka į elektros valdymo sistemos valdymo signalus, taip pat gali turėti neigiamų pasekmių. Išjungiant generatoriaus ir įtampos keitiklio šilumos ar vibracijos apsaugos funkcijas, gali atsirasti trumpalaikiai srovės svyravimai ir viršįtampiai, kurie gali sugadinti galios elektroniką ar net sukelti gaisrą [3]. Tokios atakos gali priversti vėjo jėgaines veikti viršijant nustatytas saugumo ribas, o tai gali privesti prie tokių procesų kaip vėjo jėgainės įrangos pažeidimas ar poveikis energijos tinklo stabilumui (žr. 12 pav.) [18].



12 pav. Vėjo jėgainių grėsmes ir pažeidžiamumai vedantys prie tinklo nestabilumo poveikio [18]

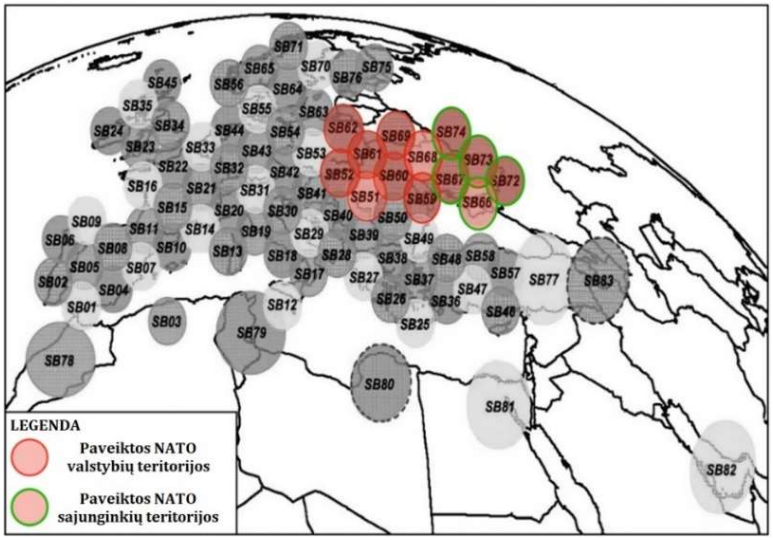
1.7.1. Vėjo jėgainių kibernetinės atakos galinčios pakenkti elektros tinklo stabilumui

Elektros tiekimo sistema turi būti sureguliuota taip, kad elektros gamyba visada atitiktų elektros vartojimo poreikius. Kai elektros gamyba viršija elektros vartojimo poreikius, tai gali sukelti perpildymą ir gali sutrikdyti elektros tiekimo sistemą. Priešingai, kai elektros gamyba yra mažesnė nei elektros vartojimo poreikiai, tai gali sukelti elektros tiekimo trūkumą ar netgi elektros tiekimo sutrikimus [30].

2022 m. atakų prieš JAV elektros tinklus skaičius išaugo 77 % ir pasiekė rekordinį lygį [66]. Kibernetinė ataka išjungianti vieną vėjo jėgainių parką, neturėtų didelės įtakos tinklo balansui ir nekeltų realaus pavojaus aplinkai ar žmonėms, tačiau vienu metu atjungus kelis jėgainių parkus, tokia ataka gali turėti reikšmingą įtaką tinklo balansui [30]. Energetikos sistemų dinamiškumas ir patikimumas vis labiau priklauso nuo vėjo jėgainių veikimo [8]. Didėjant vėjo jėgainių skaičiui pasaulyje, vėjo energija tampa vis svarbesne energijos gamybos dalimi, todėl ateityje turės labai didelę įtaką elektros tinklo dinamikai ir patikimumui [16].

1.7.2. Kibernetinės atakos sutrikdė vėjo jėgainių parkų darbą

2022-02-24, tapačia dieną, kai rusų kariuomenė įsiveržė į Ukrainą, rusų kibernetiniai sukčiai įsilaužė į „Viasat“ bendrovės „KA-SAT“ palydovinio interneto paslaugų teikėjo palydovo palydovinį ryšį. Ši kibernetinė ataka sutrikdė dalį rytų ir vidurio Europos palydovinio ryšio, todėl „Enercon“ prarado nuotolinę prieigą prie 5800 vėjo jėgainių, kurių bendras galingumas siekia 11 GW (žr. 13 pav.) [9].



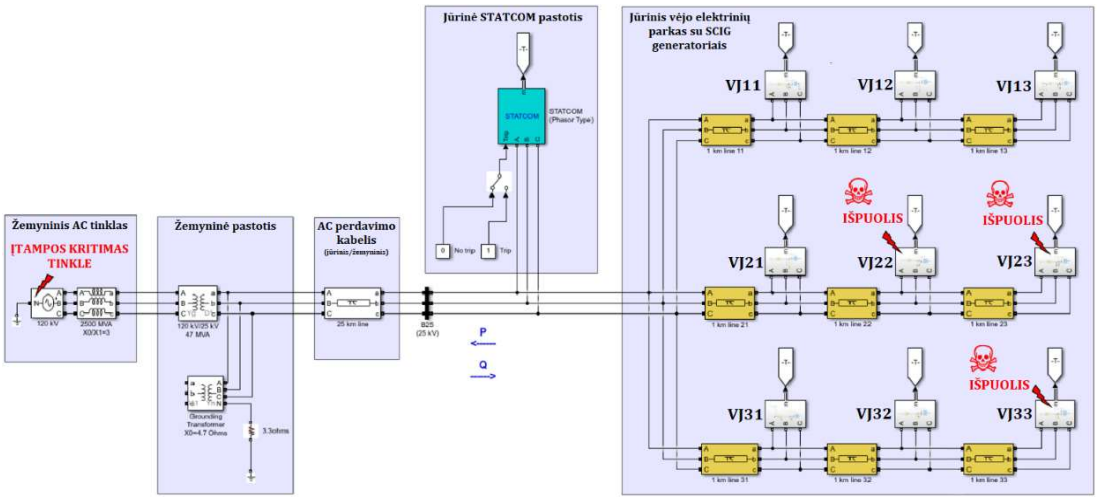
13 pav. „ViaSat“ palydovinių antenų veikimo ribos [9]

Užpuolikas naudojantis interneto prieigą per neatnaujintą VPN, pasiekė operatoriaus „Skylogic“, serverių tinklą. Tuomet užpuolikas galėjo įrašyti programinės aparatinės įrangos atnaujinimą, kartu su ja įdiegdamas programinę įrangą pavadintą „AcidRain“, kuri ištrynė visus duomenis iš modemų operatyviosios atminties [9]. Atakos metu vėjo jėgainių nuotolinis stebėjimas ir valdymas tapo nebeįmanomas, vėjo jėgainės persijungė į automatinio valdymo režimą ir išsijungė. Operatorius ryšį su jėgainėmis atkūrė per alternatyvųjį LTE/mobilųjį radijo tinklą. Vėjo jėgainės parkas buvo vėl paleistas po dviejų dienų [9]. Atlikti programinės įrangos atnaujinamai ar naujausių saugos pataisymų įdiegimas būtų apsaugoję nuo tokio masto atakos.

Vokietijos vėjo jėgainių parko operatorę „Deutsche Windtechnik“ 2022 m. balandžio mėnesį, užpuolė išpirkos reikalaujantys „Black Basta“ kibernetiniai sukčiai, kurie darbuotojams išsiuntė apgaulingus elektroninius laiškus, su apgaulingomis nuorodomis, kurias paspaudus į darbuotojų kompiuterį buvo įdiegiama kenksminga programa. Programa sukūrė paslėptą prieigos tašką sistemoje, taip užpuolikai įgavo nuotolinę prieigą prie sistemos. Užpuolikai paveikė operatoriaus vėjo jėgainių nuotolinių duomenų stebėjimą. Praradus duomenų stebėjimą saugumo sumetimais buvo išjungta 2000 vėjo jėgainių. Vėjo jėgainių darbas pilnai buvo atnaujintas po dviejų dienų [45].

1.7.3. Jūrinių vėjo jėgainių parkų jungimo topologijos ir saugumo aspektai

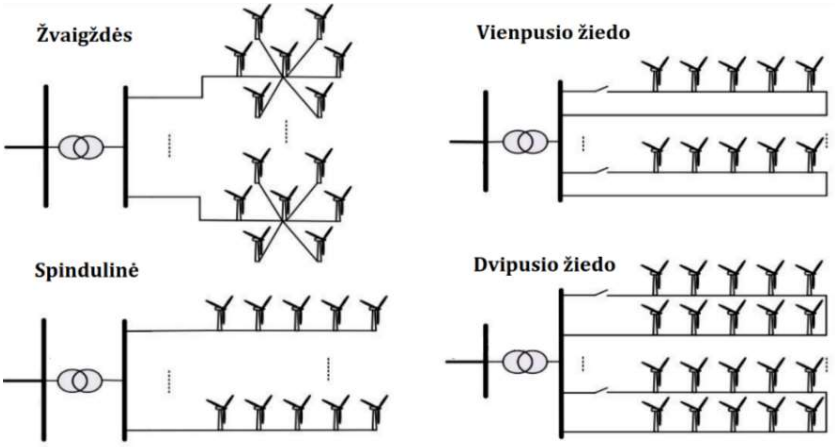
Autorius aprašo, kad išjungus apsaugos sistemas, elektrą gaminančiai vėjo jėgainei nustatomas nulinis menčių žingsnio kampas. Pirmojo atakos scenarijaus metu kai atakuojama viena vėjo jėgainė (žr. 14 pav.) generuojamos galios vertės sumažėjimas pastebimas tik manipuliuojamos elektrinės ribose. Antrajame ir trečiajame scenarijuose (žr. 14 pav.) vienu metu manipuliuojamos dviejų VJ valdymo ir apsaugos sistemoms. Šiais atvejais nenormalios elektrinės vertės išplinta į kitas parko elektrines. Dėl nepakankamos AC įtampos, suveikia aplinkinių, jėgainių SCIG apsaugos sistemos į jos nutraukia elektros gamyba. Taigi sukimo momento pertrūkis gali sukelti įtampos kritimą, dėl kurio gali suveikti kitų vėjo jėgainių apsaugos [10].



14 pav. Vėjo jėgainių parko schema, pirmajame atakos scenarijuje atakuojama „VJ23“, antrajame atakos scenarijuje atakuojama „VJ22“ ir „VJ23, trečiajame atakos scenarijuje atakuojama „VJ23“ ir „VJ33“ [10]

Trifazis trumpojo jungimo scenarijus jūriniame VJP, kuris įvyksta jėgainės žemos įtampos (690 V) gnybtuose, gali lemti viso VJP išsijungimą [10]. Šaltinio autorius kaip trumpojo jungimo priežastį pasirenka laivą, kuris užkliudo VJ pamatą, ir taip sujudina bokštą, todėl jėgainės gnybtyne įvyksta trumpasis jungimas. Remiantis autoriumi VJP buvo sujungtas spindulinės topologijos schema, todėl trumpasis jungimas įtakojo toje pačioje schemoje sujungtų VJ atsijungimą.

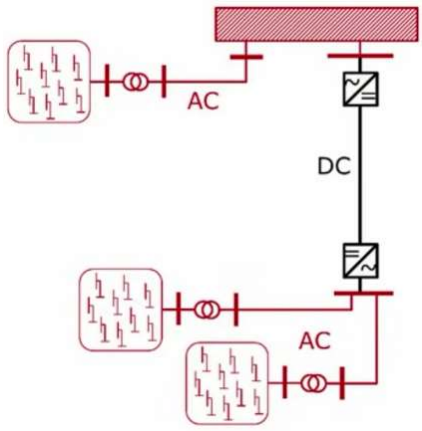
Spindulinė topologija (žr. 15 pav.), yra pigiausiai ir technologiškai lengviausiai įgyvendinama, tačiau pati nepatikimiausia. Ištyrus spindulinės topologijos schema sujungtų VJ ryšių priklausomybę nuo viena kitos, gauta išvada. Jeigu vienoje iš VJ bus pažeistas komunikacijos ar jėgos kabelis, įvyks domino efektas – jėgainės kurios sujungtos spindulinės topologijos schema tai pat gali prarasti komunikacijos ar elektros perdavimo galimybę [19].



15 pav. Vėjo jėgainių parkų topologijos [19]

Žvaigždinės topologijos jungimo VJP jėgos kabelis skirtas tik jos vienos generuojamai galiai perduoti, todėl parenkamas kabelis yra mažesnės vardinės galios, nei kitose jungimo topologijose, o tai reiškia kabelis yra pigesnis. Nors bendras viso VJP kabelių ilgis ir montavimo išlaidos didesnės, nei kitų jungimo topologijų. Remiantis atliktu tyrimu, patikimiausia VJ jungimo topologija yra žvaigždės. Žvaigždės topologijoje įvykus trumpajam jungimui, ar komunikacijos kabelių pažeidimui, tai neturės įtakos kitų tame pačiame parke esančių jėgainių darbui [19].

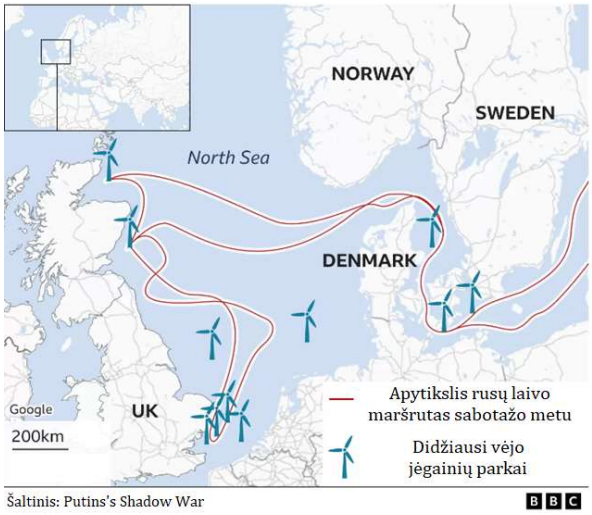
Jūros vėjo jėgainių parke pagaminta elektros energija povandeniniu kabeliu siunčiama į krante esančią pastotę. Iš pastotės elektros energija paskirstoma į elektros tinklą. Naudojant kintamos srovės (AC) įtampą, perduodant elektros energiją linijomis kurios viršija 100km, išvengti didelių elektros energijos perdavimo nuostolių ir įtampos kritimų, be kompensacinės įrangos yra neįmanoma [11]. Todėl jūroje tolimojo susisiekimo transmisijai virš 100 km, naudojama aukštos įtampos nuolatinės srovės (HVDC) perdavimo sistema (žr. 16 pav.) kuri gali perduoti elektros energijos kelis šimtus kilometrų [48].



16 pav. Jūrinių vėjo jėgainių parkų jungimo būdai [48]

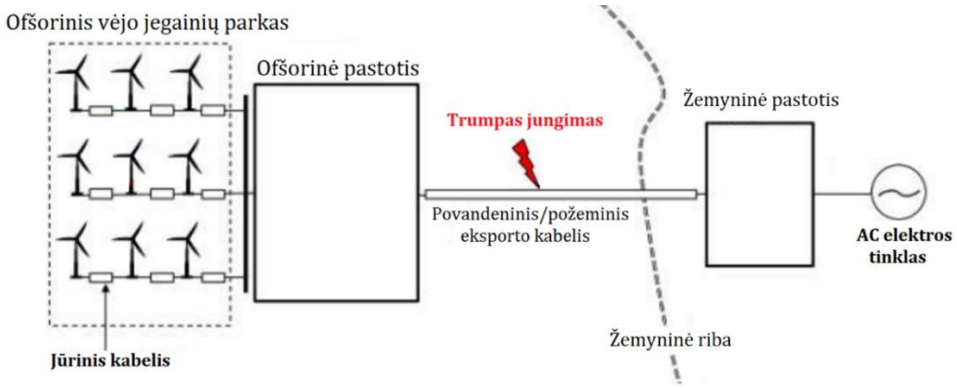
Povandeniniai jūriniai kabeliai neturi tokios apsaugos, kuri užtikrintų jų fizinę apsaugą. Todėl verta sunerimti dėl jų saugumo. Kadangi „BBC News“ ir kitos naujienų agentūros praneša apie 2022 metais lapkričio mėnesį pirmą kartą pastebėta Rusų laivą kuris šnipinėjo vėjo elektrinės prie Škotijos krantų. Antrą kartą laivas buvo pastebėtas 2023 vasario mėnesį prie Danijos krantų esančių vėjo elektrinių. 2023 metų balandžio 19 dieną „BBC News“ ir kitos naujienų tarnybos pranešė, kad remiantis naujais

kaltinimais, Rusija vykdo vėjo jėgainių ir ryšių kabelių sabotavimo programą Šiaurės jūroje (žr. 17 pav.). Straipsnio autorius teigia, kad detalės gautos iš bendro Danijos, Norvegijos, Švedijos ir Suomijos visuomeninių transliuotojų tyrimo [65].



17 pav. Laivo keliančio grėsmę VJP Šiaurės Jūroje maršrutas [64]

Rusijos vykdomą vėjo jėgainių ir ryšių kabelių sabotavimo programą Šiaurės jūroje, kelia grėsmę energijos tiekimui, ypač turint omenyje, kad 2022 metais buvo susprogdintas „Nord Stream 2“ dujotiekis. Galima teigti, kad ataka prieš vėjo jėgainių kabelių tinklą būtų vykdoma siekiant padaryti kuo didesnę žalą. Remiantis 2022 metų gruodžio mėnesio ir 2023 vasario ir balandžio mėnesių publicistiniais straipsniais, galima teigti, kad praeitame skyriuje autoriaus nagrinėtas atakos scenarijus, kuomet yra pažeidžiamas jėgos kabelis jungiantis vėjo jėgaines tarpusavyje, nėra pats aktualiausias tyrimas, kuris atspindint šių dienų aktualijas. Susiklosčius pavojingai energetinei situacijai Europoje, kuomet Rusija vykdo sabotavo programą prieš vėjo jėgainių kabelių infrastruktūrą reikia modeliuoti drastiškesnius ir pavojingesnius atakos vektorius. Pavyzdžiui kokią įtaką elektros tinklui gali padaryti didžiausio jūrinio vėjo jėgainių parko įvadinio jėgos kabelio jungiančio su žemyniniu tinklu, pažeidimas (žr. 18 pav.).



18 pav. Trumpojo jungimo scenarijus jūriniame vėjo jėgainių parke [10]

Povandeninių jūrinių VJP kabelių tinklo pažeidimas turėtų ilgalaikę įtaką energijos tiekimui regione ir sukeltų ekonominių nuostolių. Todėl būtina imtis atsargumo priemonių ir užtikrinti vėjo jėgainių saugumą, kad būtų išvengta tokių incidentų. Tai pat svarbu turėti atsarginius planus, žinoti, kaip

reaguoti nutikus avarijoms. Tam išsiaiškinti, gali būti naudojami elektros sistemos stabilumo modeliavimai, tiriant visus galimus vėjo elektrinių avarijų scenarijus.

1.8. Skyriaus išvados ir apibendrinimai

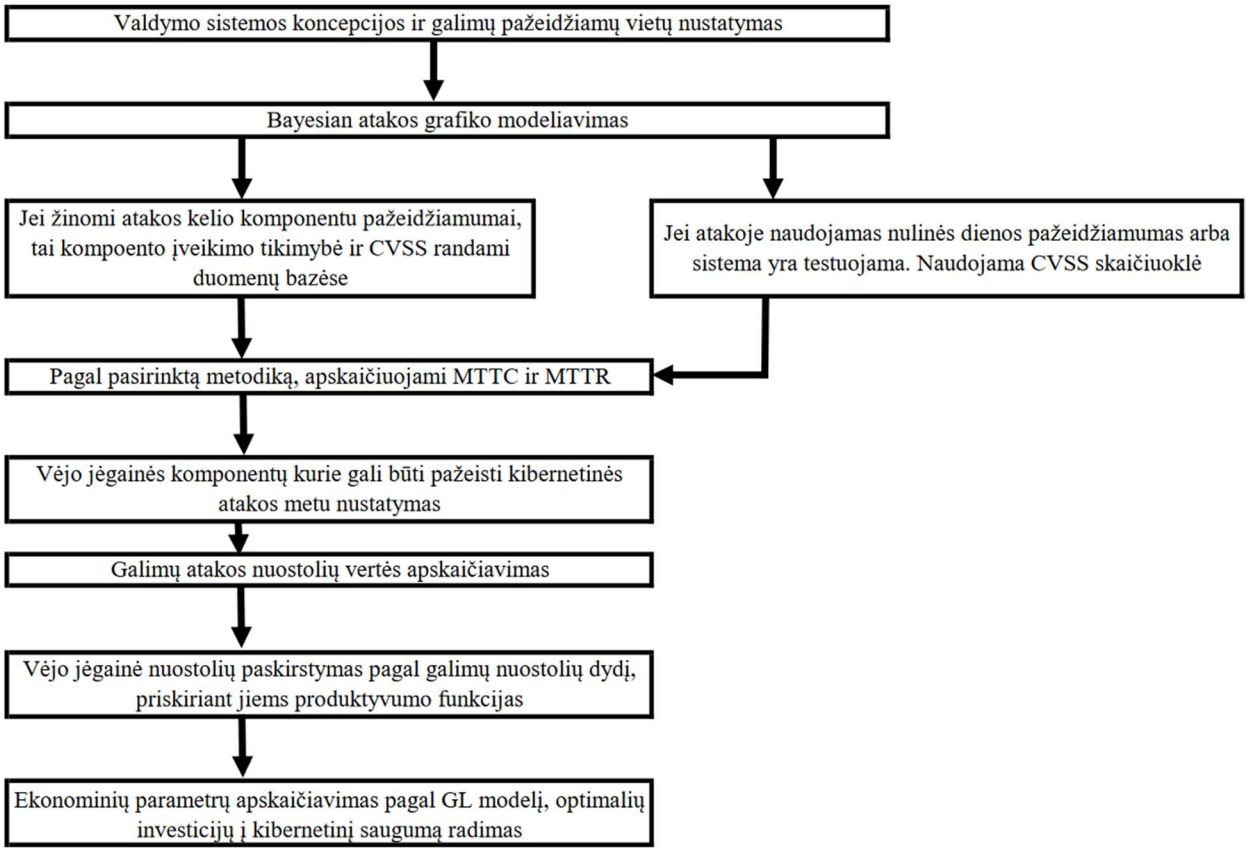
Atlikus vėjo jėgainių atsparumo tyrimų apžvalgą nustatyta, kad kibernetinėmis atakomis labiausiai pažeidžiami vėjo jėgainių komponentai yra: kontrolės sistemos, valdikliai, duomenų perdavimo maršrutizatoriai ir jutikliai. Dažniausiai prieš šiuos komponentus naudojami atakų tipai yra: sukčiavimo apsimetant atakos, kenkėjiškų programų atakos ir klaidingų duomenų įvedimo atakos. Pagrindinės priežastys dėl kurių nutinka kibernetinės atakos yra neatnaujinta programinė įranga, fizinės prieigos saugos ir darbuotojų kibernetinės saugos mokymų trūkumas. Siekiant padidinti vėjo jėgainių kibernetinį atsparumą reikia įdiegti įsibrovimo aptikimo priemones, reguliariai atnaujinti sistemas, vykdyti darbuotojų mokymus ir valdymo sistemai pritaikyti IEC62443 standartą, kuris yra tinkamiausias vėjo jėgainėms.

2. Vėjo jėgainių kibernetinio atsparumo ir investicijų į kibernetinę saugą įvertinimo metodika

Tiriamojoje dalyje pateikta metodika, kuri įvertina vėjo jėgainės atsparumą kibernetinėms atakoms ir optimalias investicijas į kibernetinę saugą (žr. 19 pav.). Metodika susideda iš kelių dalų, pradedant valdymo sistemos koncepcijų ir galimų pažeidžiamų vietų nustatymu. Taip pat bus taikomas Bajeso tinklo atakos modeliavimas, kuris padės nustatyti galimų atakų kelius ir jų poveikį sistemai. Jei žinomi atakos kelio komponentų pažeidžiamumai, komponento įveikimo tikimybė ir CVSS (Common Vulnerability Scoring System) reikšmes, randamos duomenų bazėse. Jei atakoje naudojamas nulinės dienos pažeidžiamumas arba sistema yra testuojama, reikia naudoti CVSS skaičiuoklė.

Toliau, pagal pasirinktą metodiką, apskaičiuojamas vidutinis laikas iki sutrikimo - MTTC (angl. Mean Time to Compromise) ir vidutinis laikas iki atsigavimo MTTR (angl. Mean Time to Recover), kad būtų galima numatyti atakos poveikį vėjo jėgainės veikimui. Taip pat nustatomi vėjo jėgainės komponentai, kurie gali būti pažeisti kibernetinės atakos metu, ir bus apskaičiuota galimų atakos nuostolių vertė.

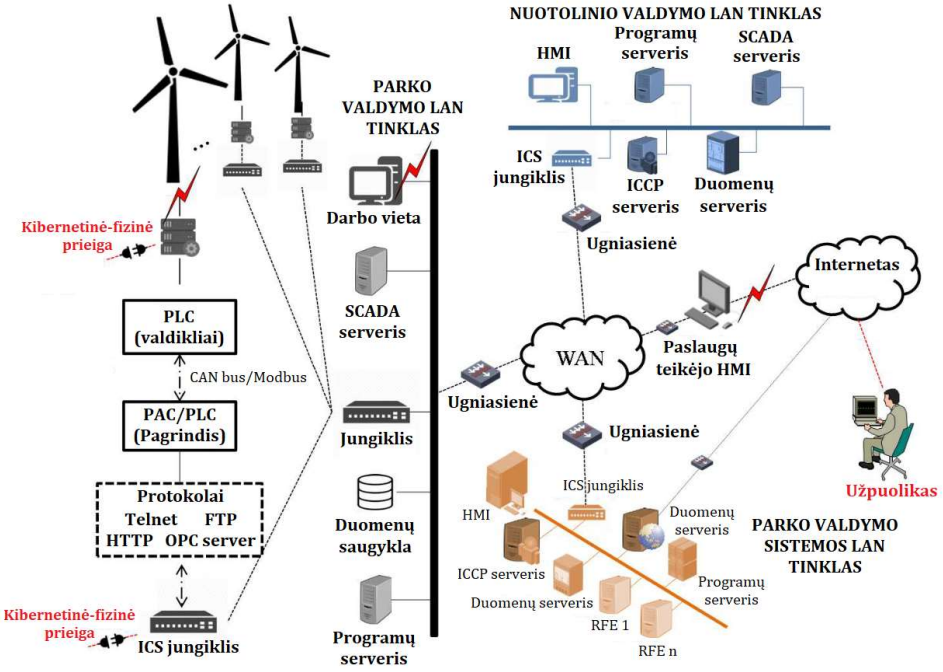
Toliau, vėjo jėgainės nuostoliai paskirstomi pagal galimų nuostolių dydį, priskiriant jiems produktyvumo funkcijas. Galiausiai, taikant Gordono-Loebo (GL) modelį, apskaičiuojami ekonominiai parametrai ir apskaičiuojamos optimalios investicijos į kibernetinį saugumą.



19 pav. Vėjo jėgainių kibernetinio atsparumo vertinimo ir investicijų į kibernetinę saugą įvertinimo metodikos struktūra [20,21,27,]

2.1. Vėjo jėgainių kibernetinio atsparumo vertinimo metodika

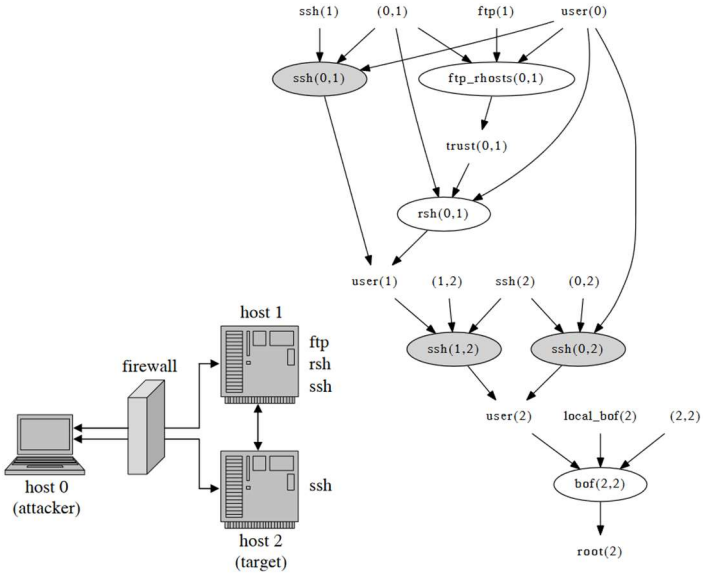
Šiame tyrime analizuotas vėjo jėgainių kibernetinis atsparumas kibernetinėms atakoms ir vertinami galimi saugumo trūkumai, siekiant padidinti jėgainių kibernetinį saugumą. Bajeso tinklo grafikas šiame tyrime naudotas atvaizduoti sistemos įrenginių priklausomybes ir ryšius. Sistemos komponentų pažeidžiamumo tikimybių apskaičiavimui naudojama CVSS vertinimo skaičiuoklė. Valdymo sistemos koncepcija ir galimų pažeidžiamų vietų nustatymas yra vieni svarbiausių veiksmų kibernetinės atakos modeliavimo procese. Tai leidžia suprasti, kurias sistemos vietas ir kaip kibernetinės atakos gali paveikti valdymo sistemą. Vėjo jėgainių valdymo struktūra pavaizduota 20 paveiksle.



20 pav. Vėjo jėgainių valdymo struktūra [24]

2.2. Kibernetinės atakos modeliavimas: Bajeso atakų grafikas

Bajeso atakų grafikas yra skirtas atvaizduoti sistemos priklausomybes ir ryšius (žr. 21 pav.). Kibernetinių sukčių, kurie atakuoja vėjo jėgaines, pagrindinis tikslas yra įgauti valdymo teisę sistemoje. Tam reikia įveikti apsaugos komponentus, kad būtų įgauta šakninė valdymo teisė (angl. root) [20]. Bajeso atakos grafikas yra abstraktus būdas vizualizuoti komponentų ir ryšių priklausomybes. Jis pateikia grafinį vaizdą, kuriame komponentai yra mazgai, o tarp jų esantys ryšiai žymimi linijomis. Kiekvienam komponentui galima priskirti savybes, teises ar pažeidžiamumus, kurie gali būti simboliais arba rašmenimis. Pavyzdžiui, "SSH" gali reikšti SSH prieigą su tam tikra identifikacija arba teisėmis, o "ftp_rhost" gali rodyti FTP ryšį su konkrečiu prieigos tašku [20].



21 pav. Principinė sistemos valdymo schema kairėje, Bajeso atakos grafikas dešinėje [20]

Pažeidžiamumas yra sistemos, tinklo ar programinės įrangos savybė, dėl kurios jos gali būti prieinamos arba pažeistos. Tai yra tam tikri trūkumai arba spragos, kurios leidžia potencialiems užpuolikams įsibrauti, patekti arba paveikti sistemą, pažeidžiant jos saugumą arba neleidžiant jai veikti kaip numatyta. Pažeidžiamumas gali būti techninės, dizaino, programinės įrangos arba žmogiškosios klaidos rezultatas. Norint įveikti sistemą saugančius komponentus, reikia išnaudoti jų pažeidžiamumus, todėl užpuolikai ieško ir naudoja spragas ar silpnąsias vietas, kurios leidžia prasibrauti pro saugumo komponentus ir gauti neleistiną prieigą ar kontrolę. Yra du pagrindiniai tipai galimų pažeidžiamumų. Pirmas tipas yra žinomi pažeidžiamumai, kurių duomenys yra viešai prieinami. Antrasis tipas yra nulinės dienos pažeidžiamumai, tai tokie pažeidžiamumai kurie yra nauji, ir apie juos duomenų bazėse informacijos nėra.

Jeigu modeliuojamoje atakoje yra naudojama nulinės dienos pažeidžiamumo ataka, kuri nėra viešai žinoma ir kurios pažeidžiamumo balai nėra viešai paskelbti, tai pavienio mazgo pažeidžiamumo tikimybė apskaičiuojama pagal (1) formulę [17].

$$p(E) = \frac{CVSS}{10}. \quad (1)$$

Modeliuojant ataką, kurioje naudojami žinomi pažeidžiamumai, tai valdymo sistemos komponentų pažeidžiamumai vertinami naudojantis pažeidžiamumų duomenų bazėmis, tokiomis kaip:

- NVD (angl. National Vulnerability Database) nuo 2005 m., veikianti JAV vyriausybės finansuojama duomenų bazė, kurioje pateikiama informacija apie įvairių programinės įrangos produktų pažeidžiamumus. NVD duomenų bazę valdo „Nacionalinis standartų ir technologijų institutas“ - NIST (angl. National Institute of Standards and Technology) [50].
- CVE (angl. Common Vulnerabilities and Exposures) tai duomenų bazė kuri nuo 1999 metų viešai dalinasi informacija apie bendrus programinių įrangų ir sistemų pažeidžiamumus ir poveikį jiems. CVE valdo „Sertifikuotas informacinių sistemų auditorius“ - CISA (angl. Certified Information Systems Auditor CISA) [51].

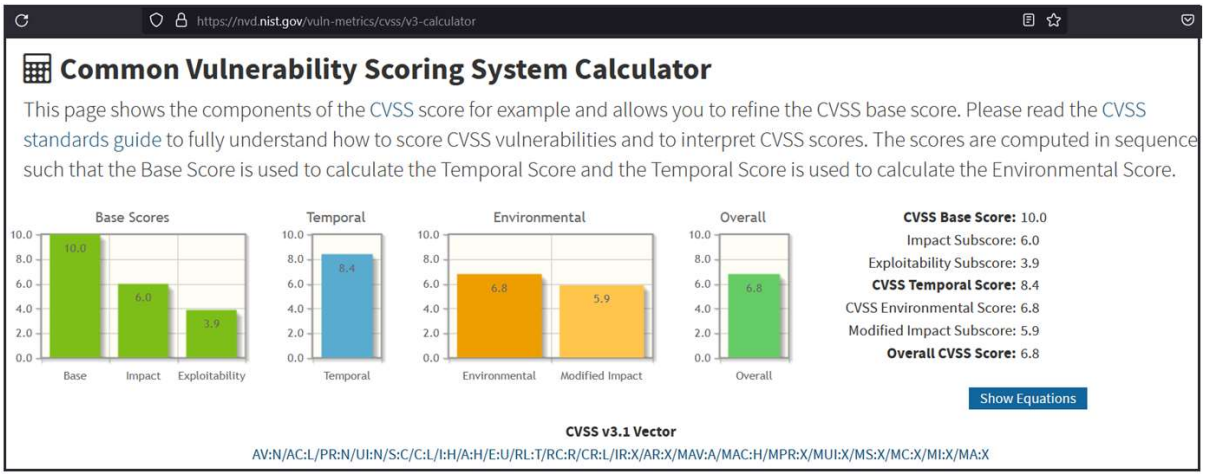
Penktoje lentelėje pateikiami CVE duomenų bazėje pateiktų komponentų pažeidžiamumų identifikavimo kodai, pažeidžiamumo balai ir pažeidžiamumo išnaudojimo tikimybių duomenys:

5 lentelė. CVE pažeidžiamumų lentelė [17].

Komponentas / Duomenys	Ugniasienė	Jungiklis	Duomenų serveris	Programų serveris
CVE ID	CVE 2020-5148	CVE 2020-12523	CVE-2017-7907	CVE 2020-25188
CVSS įvertinimas	8,2	9,1	6,6	7,8
Tikimybė įveikti komponentą, p(E)	0,82	0,91	0,66	0,78

2.3. CVSS: Programinės įrangos ir sistemų pažeidžiamumo balo vertinimo įrankis

CVSS (angl. Common Vulnerability Scoring System) tai standartizuota kompiuterinių sistemų ir programinės įrangos vertinimo sistema, naudojama galimo pažeidžiamumo poveikio nustatymui. CVSS balo apskaičiavimas yra metodas, kuris leidžia organizacijoms įvertinti pažeidžiamumų rimtumą ir nustatyti tinkamas saugumo priemones bei veiksmus. CVSS yra skirta įvertinti programinės, aparatinės įrangos ir programinės įrangos spragų technines charakteristikas [52].



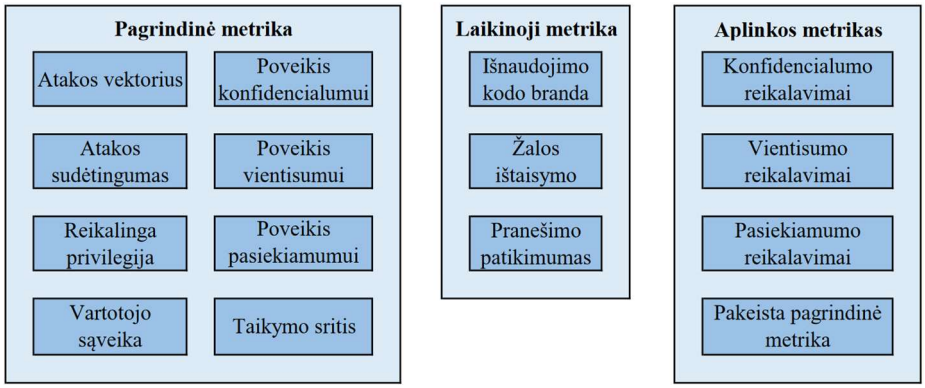
22 pav. NIST CVSS skaičiuoklės rezultatų vaizdas [53]

CVSS pagrindinio įvertinimo matavimo ribos yra nuo 0 iki 10, aukštesnis įvertinimas rodo didesnę sistemos komponento įveikimo tikimybę ir pažeidimo įtaką atakuojamam komponentui ar sistemai (žr. 6 lent.). CVSS balą galima apskaičiuoti Jungtinių Valstijų „Nacionalinio Standartų ir Technologijų Instituto“ (NIST) pateikiamą naujausios (3.1 versijos) CVSS balų skaičiuoklė (žr. 22 pav.) [53].

6 lentelė. CVSS pagrindinio pažeidžiamumo balo vertinimo skirstymas [53].

Pažeidimo poveikio sunkumo ir išnaudojimo galimybės vertinimas	**CVSS įvertinimas**
Nėra	0
Žemas	0,1-3,9
Vidutinis	4,0-6,9
Aukštas	7,0-8,9
Kritinis	9,0-10,0

CVSS skaičiuoklėje apskaičiuojamos trys metrikos grupės: pagrindinė, laikinoji ir aplinkos (žr. 23 pav.). Pagrindinė vaizduoja vidinius pažeidžiamumo atributus, kurie laikui bėgant išlieka pastovūs, pavyzdžiui, tai gali apimti sistemos autentifikacijos arba duomenų saugumo aspektus. Laikinoji grupė apibūdina pažeidžiamumo požymius, kurie laikui bėgant keičiasi, pavyzdžiui, tai gali būti sistemos atnaujinimai, programinės įrangos versijų arba atliktų įrenginių pakeitimų padariniai. Aplinkosaugos grupė nurodo pažeidžiamumo savybes, kurios yra unikalios vartotojo aplinkai [53].



23 pav. CVSS metrikos ir jų balą sudarantys subjektai [52]

Kiekvienas CVSS skaičiuoklėje padarytas pasirinkimas padaro įtaką galutiniam įvertinimui (žr. 24 pav.).

Metrika	Metrinė vertė	Skaitinė vertė
Atakos vektorius, angl. Attack Vector(AV)	Tinklas	0,85
	Gretimas	0,62
	Vietinis	0,55
	Fizinis	0,2
Atakos sudėtingumas, angl. AttackComplexity(AC)	Žemas	0,77
	Aukštas	0,44
Reikalinga privilegija, angl. Privileges Required (PR)	Nėra	0,85
	Žemas	0,62 (arba 0,68 jei taikymo sritis pakeista)
	Aukštas	0,27 (arba 0,5 jei taikymo sritis pakeista)
Vartotojo sąsaja, angl. User Interaction (UI)	Nėra	0,85
	Reikalingas	0,62
Konfidencialumas, angl. Confidentiality (C) (reikšmės ir modifikuotiems)	Aukštas	0,56
	Žemas	0,22
	Nėra	0
Vientisumas, angl. Integrity (I) (reikšmės ir modifikuotiems)	Aukštas	0,56
	Žemas	0,22
	Nėra	0
Pasiekiamumas, angl. Availability (A) (reikšmės ir modifikuotiems)	Aukštas	0,56
	Žemas	0,22
	Nėra	0

Metrika	Metrinė vertė	Skaitinė vertė
Pasiekiamumas, angl. Availability (A) (reikšmės ir modifikuotiems)	Aukštas	0,56
	Žemas	0,22
	Nėra	0
Kodo išnaudojimo metrika, angl. Exploit Code Maturity(E)	Neapibrėžta	1
	Aukštas	1
	Funkcinis	0,97
	Koncepcijos įrodymas	0,94
	Nejrodyta	0,91
Ištaisymo lygis, angl. RemediationnLevel (RL)	Neapibrėžta	1
	Nepasiekiamas	1
	Sprendimo būdas	0,97
	Laikinas pataisymas	0,96
	Oficialus pataisymas	0,95
Pranešimo patikimumas, angl. Report Confidence (RC)	Neapibrėžtas	1
	Patvirtinti	1
	Pagrįstas	0,96
	Nežinoma	0,92
Konfidencialumo reikalavimas / vientisumo reikalavimas / prieinamumo reikalavimas	Neapibrėžtas	1
	Aukštas	1,5
	Žemas	1
	Nėra	0,5

24 pav. CVSS metrikų verčių skaitinės vertės [52]

2.4. Vidutinis laikas iki sutrikimo ir vidutinis remonto laikas

Vidutinis laikas iki sutrikimo - MTTC yra vienetas, kuris plačiai naudojamas kiekybiškai įvertinti kibernetinių atakų dažnumą ir jų poveikį (žr. 25 pav.) [24]. MTTC parametro laiko ribos prasideda nuo laiko momento, kuomet užpuolikas pradeda atakos paruošiamuosius veiksmus iki laiko kuomet prasideda aktyvi kibernetinės atakos fazė ir sistema pajunta pirmuosius atakos veiksmus. Pavyzdžiui

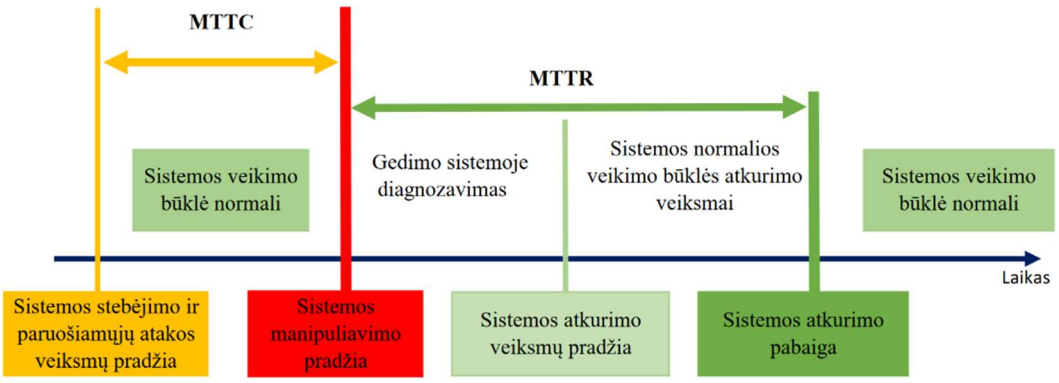
tai gali būti laikas nuo užkrėstų laiškų išsiuntimo darbuotojams iki vėjo jėgainių valdymo sistemų išjungimo.

Yra daugybė kibernetinio saugumo įrankių ir paslaugų, kurios gali padėti apskaičiuoti MTTC vertę specifinei sistemai. Kibernetinio saugumo metrikos skaičiavimas ir jų naudojimo metodika gali skirtis priklausomai nuo to, kokia sistema yra vertinama ir kokie yra naudojami vertinimo kriterijai. Dėl to neegzistuoja universali MTTC skaičiavimo metodika ar įrankis, kuris būtų tinkamas visiems atvejams. Dažnai tyrimuose naudojama MTTC apskaičiuojamas pagal (2) formulę [20].

$$MTTC = \left(dien.pažeid.išn. + \frac{10}{cvss(e)}\right) + \left(dien..pažeid.išn. + 5{,}8 * \frac{10}{(cvss(e)}\right) * e^{\frac{-xk}{m}} \quad (2)$$

čia: x - atakos kelio komponentų skaičius pro kuriuos užpuolikui reikia prasibrauti norint pasiekti kibernetinės atakos tikslą; k - bendras pažeidžiamumų, skaičius; m – bendras programinės įrangos subjektų skaičius; $cvss\,(e)$ - CVSS vertinimo sistemos pažeidžiamumo (angl. exploitability) įvertinimas; 5,8 - „McQueen“ iškelta hipotezė gama duomenų patikslinimas, kurio vidurkis yra 5,8 dienos [20].

Vidutinis remonto laikas - MTTR, yra bendras laikas reikalingas normaliam sistemos darbo atstatymui. MTTR laiką sudaro: gedimo identifikavimo trukmė, gedimo pašalinimas, laikas reikalingas įrangos gavimui, įrangos įdiegimui, bei galutiniam sistemos darbo patikrinimui (žr. 26 pav.) [23, 54]. MTTR yra naudingas elektros generavimo netiekimo skaičiavimuose, ypač jei vėjo jėgainės patiria prastovas dėl vėjo jėgainių gedimų ar remonto darbų.



25 pav. MTTC ir MTTR veikimo ribos

2.5. NERC kibernetinių incidentų vertinimo sistema

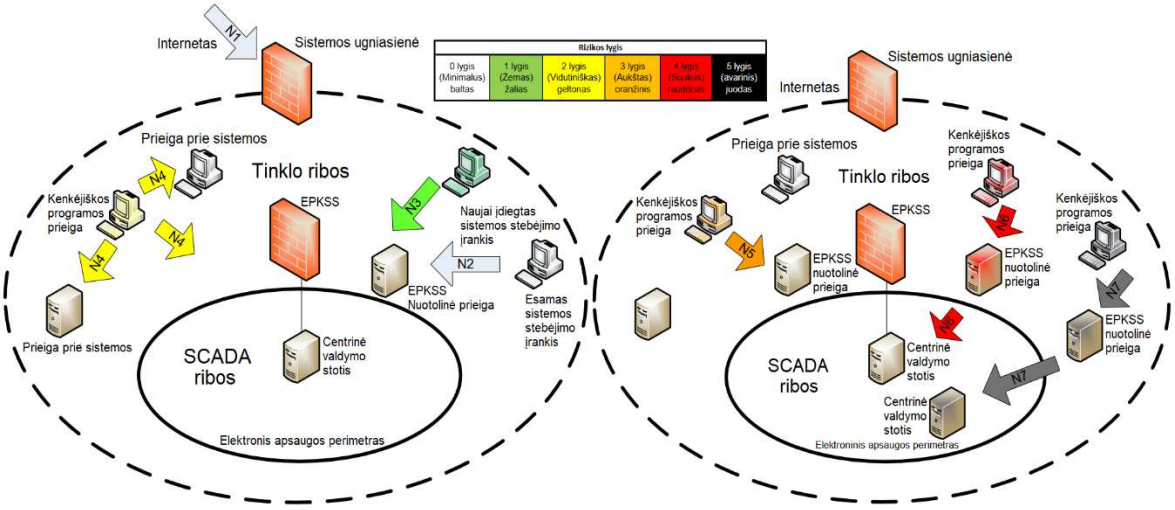
Kibernetinis incidentas – įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims [55].

7 lentelė. Kibernetinių atakų klasifikacijos schema [38]

Rizikos lygis	Bendras apibūdinimas	Pasekmės
5 lygis (avarinis) juodas	Kibernetinis incidentas, pažeidžia, sutrikdo CVS, atsakingą už funkcinio subjekto ypatingos svarbos užduočių atlikimą.	Kibernetinio saugumo incidentas, keliantis grėsmę sistemos saugai ir BESIVS patikimumui. Incidentus kurie sutrikdo CVS sistemą, atsakingą už funkcinių užduočių atlikimą reikia pranešti atsakingoms institucijoms.
4 lygis (Sunkus) raudonas	Kibernetinis incidentas, susijęs su EPKSS arba EAP sistemos pažeidimu ar sutrikdymu, arba bandymu pažeisti CVS.	Kibernetinio saugumo incidentas keliantis grėsmę sistemos saugai ir BESIVS patikimumui, reikia nedelsiant reaguoti, apie juos pranešt, įskaitant EPKSS ar EAP sistemų pažeidimus ar sutrikimus arba bandymus pakenkti CVS.
3 lygis (Aukštas) oranžinis	Kibernetinis incidentas, kuriuo buvo bandoma pakenkti EPKSS arba EAP sistemai arba ją sutrikdyti.	Bandymas pakenkti EPKSS, nekelia grėsmės sistemos saugumui ar BESIVS patikimumui, tačiau vis tiek reikia imtis veiksmų. Kibernetinio saugumo incidentas, apie kurį būtina pranešti kaip apie bandymą pakenkti EPKSS.
2 lygis (Vidutiniškas) geltonas	Kibernetinis incidentas, kuris nebuvo konkrečiai nukreiptas į taikomą sistemą ar perimetrą.	Incidentas, kuris yra kenkėjiškas ar įtartinas, tačiau nekelia grėsmės saugumui ar BESIVS patikimumui. Reikia imtis veiksmų, kad būtų išvengta tolesnės žalos sistemai.
1 lygis (Žemas) žalias	Kibernetinis incidentas, kuris tyrimo metu, nebuvo pripažintas kenkėjiškas ar įtartinas.	Kibernetinis incidentas, nekeliantis grėsmės saugumui.
0 lygis (Minimalus) baltas	Nereikšmingi kibernetiniai įvykiai.	Kibernetiniai įvykiai, kurių nereikia tirti ir kurie nėra kibernetiniai incidentai. Tai nekelia grėsmės saugumui.

NERC (angl. North American Electric Reliability Corporation) kibernetinių incidentų vertinimo sistema [38]. Naudojantis šia sistema galima klasifikuoti potencialius incidentus pagal jų sunkumą ir riziką, pagal tai parenkant reagavimo veiksmus. Kibernetinės atakos pagal prasiskverbimo į valdymo sistemą gilumą yra skirstomos į 5 lygius (žr. 7 lentelę.)

Vidinio tinklo nuskaitymas iš nežinomo šaltinio, po kurio sėkmingai prisijungta prie EACMS INP ir tada sekęs bandymas prisijungti prie pagrindinio valdiklio (žr. 26 pav. raudonas vektorius) pagal NERC „KIVS“ kaip raudono rizikos lygio ataka. Vidinio tinklo nuskaitymas iš nežinomo šaltinio, po kurio sėkmingai prisijungta prie EACMS INP ir pagrindinio valdiklio (žr. 26 pav. juodas vektorius) šis rizikos lygis vertinamas juodu rizikos lygiu – pačiu pavojingiausiu. (žr. 26 pav. N1, N2, N3, N4, N5) atakoms nepavyko prasibrauti pro sistemos apsaugas. Pagal NERC standartą kibernetiniai incidentai, dėl kurio reikia atlikti tyrimus pateikti (26 pav., N3, N4, N5, N6, N7).



26 pav. Galimi valdymo tinklo kibernetinės atakos vektoriai

Užkardos yra svarbus tinklo saugumo komponentas, naudojamas srautui tarp skirtingų tinklo segmentų arba tarp tinklo ir interneto stebėti ir valdyti. Užkardos sugeneruotuose žurnaluose yra išsami informacija apie srautą, kuris praėjo per užkardą, įskaitant srauto šaltinį ir paskirties vietą, naudojamo protokolo tipą ir visus užkardos veiksmus [38]. Peržiūrėję žurnalus, tinklo administratoriai ir saugos darbuotojai gali gauti vertingų įžvalgų apie tinklo veiklą ir nustatyti galimas saugumo grėsmes ar pažeidžiamumus .

2.6. Vėjo jėgainės investicijų į kibernetinį saugumą nustatymo metodika

SNL Jungtinių Valstijų Energetikos departamentui pateiktoje „Vėjo energijos sistemų grūdinimo nuo Kibernetinių grėsmių ataskaitoje“, tyrėjai GL modelį, pritaiko vėjo jėgainių sektoriui, šis modelis padeda nustatyti vėjo jėgainių investicijų į kibernetinį saugumą dydį ir parodo kaip investicijos gali sumažinti galimus nuostolius.

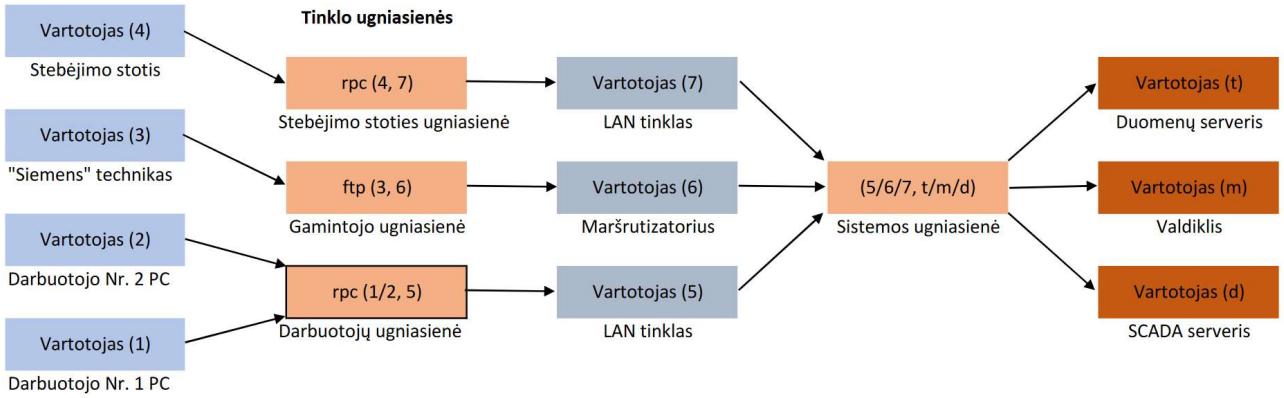
Vėjo jėgainės investicijų į kibernetinį saugumą nustatymo modelį sudaro trys dedamosios. Pirmoji dedamoji yra kibernetinės atakos metu patirtų, numatomų nuostolių rinkinių sudarymas, pagal svarbumą. Antroji modelio dedamoji yra kiekvieno rinkinio pažeidžiamumo įvertinimas remiantis žalos dydžiu. Tai reiškia, kad reikia įvertinti kiekvienos informacijos rinkinio ar turto pažeidimo tikimybę. Trečioji dedamoji yra investicijų produktyvumo funkcijos nustatymas ir priskyrimas kiekvienam informacijos ar turto rinkiniui. Produktyvumo funkcija parodo kaip investicijos į kibernetinį saugumą gali sumažinti numatomus nuostolius [1].

3. Vėjo jėgainių kibernetinio atsparumo tyrimas

3.1. Vėjo jėgainių kibernetinio atsparumo vertinimas

Nulinės dienos pažeidžiamumo išnaudojimas yra kibernetinė ataka, kurios metu pasinaudojama programinės įrangos, aparatinės įrangos ar programinės įrangos saugumo trūkumu, kuris dar nėra viešai žinomas ir nėra aprašytas pažeidžiamumų duomenų bazėse. Terminas „nulinė diena“ vartojamas, nes tarp pirmą kartą aptikto sistemos pažeidžiamumo ir to sistemos pažeidžiamumo išnaudojimo, nėra jokių tarpinių dienų, t.y. ataka yra viešai žinoma nulį dienų. Dėl šios savybės nulinės dienos išnaudojimai ypač pavojingi, nes dažniausiai naujiems pažeidžiamumams nėra jokių įmanomų pataisų ar priemonių, apsaugančių nuo atakos [1,20].

Žinant vėjo jėgainės valdymo struktūrą, kibernetinės atakos tipą galima sudaryti atakos modelį. Priimama, kad užpuolikas panaudojęs sukčiavimo užkrėstais elektroniniais laiškais ataką (angl. phishing), gauna nuotolinę prieigą prie darbuotojų tinklo kompiuterio. Užpuolikas turintis nuotolinę prieigą prie darbuotojo kompiuterio, išnaudojęs nulinės dienos pažeidžiamumą prasibrauna pro darbuotojų prieigos ugniasienę (žr. 28 pav.). Naudojantis tuo pačiu nulinės dienos pažeidžiamumu prasibrauna pro sistemos ugniasienę ir pasiekia norimą atakos tikslą – SCADA serverius, bei įgauna sistemos valdymo teisę, bei galimybę išjungti apsaugos sistemas ir vėjo jėgaines (žr. 28 pav.).



27 pav. Sumodeliuotas atakos modelis

Kadangi MTTC radimo formulėje (3) naudojamas CVSS išnaudojimo įvertinimas, pagal CVSS metodikoje pateikiamą išnaudojimo įvertinimo radimo formulę (3), matome, kad išnaudojimo įvertinimą lemia: koeficientas, atakos vektoriaus, atakos sudėtingumo, reikalingų teisių ir vartotojo sąsajos parametrai [52].

Išnaudojimo įvertinimas = 8,22 × Atakos vektorius × Atakos sudėtingumas × Reikalingos teisės × Vartotojo sąsaja. (3)

Pagal priimta atakos modelį parametrai parenkami taip:

Atakos vektorius (angl. attack vector): tinklas, nes ataka prasideda nuotoliniu būdu per internetinį tinklą, naudojant sukčiavimo (phishing) užkrėstus elektroninius laiškus. Šis aspektas yra atitinkamas, nes ataka vyksta per tinklą.

Atakos sudėtingumas (angl. attack complexity): maža, nes tai reiškia, kad ataka gali būti įgyvendinta su minimaliu sunkumu ir išteklių panaudojimu. Šis aspektas yra atitinkamas, nes ataka įgyvendinama naudojant sukčiavimo elektroninį laišką.

Reikalingos privilegijos (angl. privileges required): nėra, nes atakai įgyvendinti nereikia jokių privilegijų, tai reiškia, kad ji gali būti vykdoma neturint specialių prieigos teisių. Šis aspektas yra atitinkamas, nes užpuolikui nereikia turėti specialių prieigos teisių, jis gali prieiti darbuotojų tinklo kompiuterį nuotoliniu būdu.

Vartotojo sąveika (angl. user interaction): nėra, nes laiškas gali atrodyto kaip tikras ir patikimas, darbiniams reikalams skirtas laiškas. Žmonės gali būti lengvai apgauti ir nesuprasti, kad jie susiduria su kenksmingu laišku.

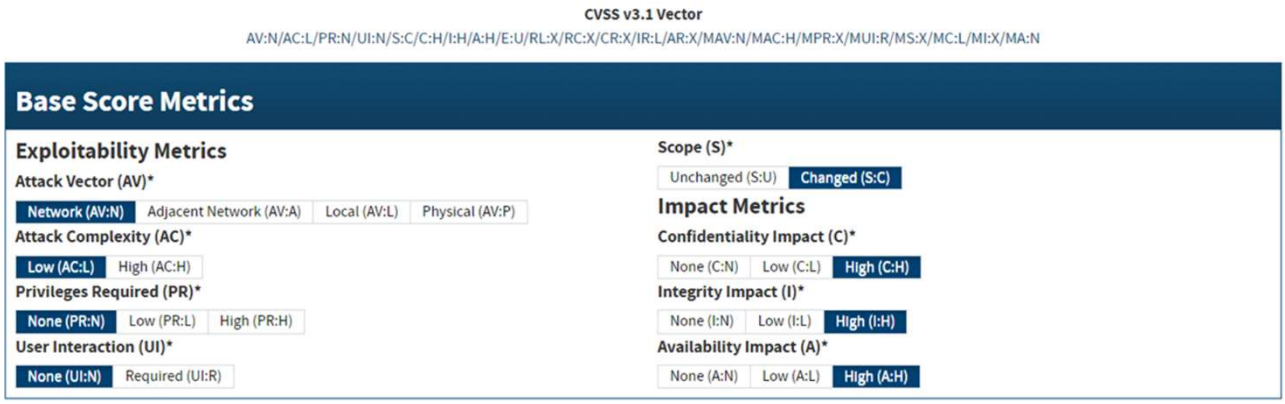
Tai pat įvedami poveikio parametrai naudojami poveikio ir pagrindiniam įvertinimui apskaičiuoti:

Konfidencialumo poveikis (angl. confidentiality impact): aukštas, gali padaryti žalos vejo jėgainės sistemos konfidencialumui. Tai reiškia, kad užpuolikas gali gauti nepageidaujamą prieigą prie konfidencialios informacijos, pvz., verslo planų, finansinių duomenų ar kitos jautrios informacijos, kuri gali būti naudojama įvairiems tikslams, įskaitant ekonominę žalą ar reputacijos praradimą.

Vientisumo poveikis (angl. impact metrics): aukštas vientisumo poveikis reiškia, kad ataka gali turėti didelę neigiamą įtaką vejo jėgainės sistemos duomenų vientisumui. Užpuolikui gavus šaknines privilegijas ir įveikus dvi ugniasienes, jis gali keisti ar trinti duomenis, įdiegti kenksmingą programinę įrangą arba vykdyti kitus veiksmus, kurie paveiks sistemos duomenų vientisumą. Tai gali lemti duomenų praradimą, klaidingus arba netikslus veikimą bei sudaryti sąlygas tolimesnei žalai ir trukdžiams vejo jėgainės veikloje.

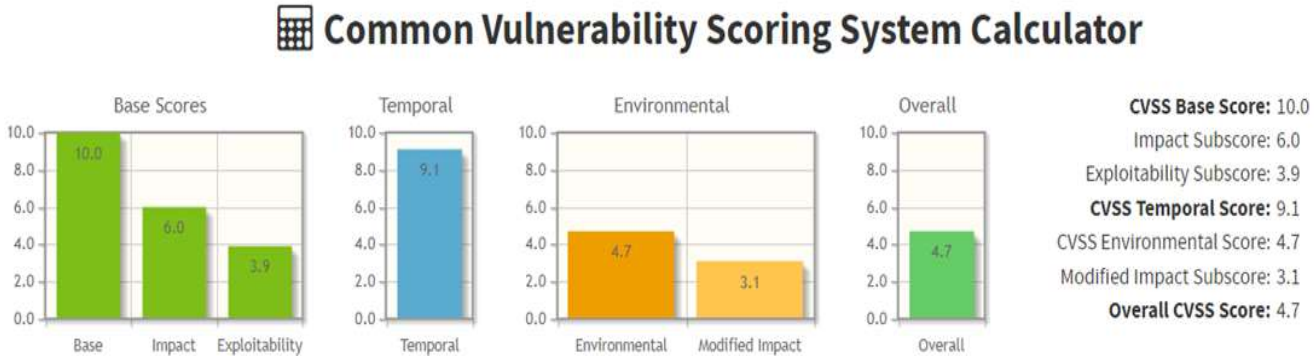
Prieinamumo poveikis (angl. availability impact): aukštas prieinamumo poveikis rodo, kad ataka gali turėti didelę įtaką vejo jėgainės sistemos prieinamumui. Užpuolikui gavus šaknines privilegijas ir įveikus dvi ugniasienes, jis gali trukdyti tinklo veikimui, išjungti arba sugadinti svarbius komponentus, kuriuos priklauso vejo jėgainei. Tai gali lemti sistemos darbo sutrikimus, praradimus arba net iš viso nutraukti veiklą. Prieinamumo pažeidimai gali turėti finansinių nuostolių, veiklos sutrikimų ar vartotojų nepasitenkinimo pasekmes.

Po parametrų nustatymo, parametrai įvedami į CVSS skaičiuoklę (žr. 28 pav).



28 pav. Modeliuojamos atakos duomenys įvesti į NIST CVSS balo skaičiuoklę

Sumodeliavus atakos parametrus, CVSS 3.1 versijos NIST bendro pažeidžiamumo įvertinimo skaičiuoklė, sugeneravo didžiausią įmanomą išnaudojimo (angl. exploitability) balą – 3,9 kuris bus naudojamas tolimesniuose skaičiavimuose. Bendras modeliuojamos nulinės atakos išnaudojimo metrikos įvertinimas – 10 (žr. 29 pav.).



29 pav. CVSS 3.1 skaičiuoklės sugeneruoti pažeidžiamumo balai

Apskaičiavus CVSS įvertinimą galima atlikti tolimesnius veiksmus. Norint įvertinti MTTC reikia žinoti, kiek dienų reikia nulinės dienos pažeidžiamumui išnaudoti. Vidutinis laikas nulinės dienos pažeidžiamumui išnaudoti ir prasibrauti pro sistemą yra 65 dienos [20]. Šiame tyrime priimta, užpuolikas išorinę ugniasienę įveiks per 24 dienas, o vidinės sistemos ugniasienei įveikti per 41 dieną. Antrosios ugniasienės pažeidimo laikas pasirinktas ilgesnis kadangi vėjo jėgainių užpuolikas norintis padaryti kuo didesnę žalą sistemos stabilumui ataką turėtų pradėti kuomet vėjo greitis ir sistemos apkrovimas didžiausi. Analizuojant sistemos saugumo matavimo indekso (4) formulę, aišku, kad norint padaryti žalos ne tik vėjo jėgainei, bet ir elektros tinklo stabilumui, užpuolikui reiktų kibernetinę ataką pradėti tuo momentu, kuomet apkrovimas elektros tinkle yra didžiausias ir vėjo jėgainės generuojama galia yra didžiausią [22].

$$V_a(t) = P_{generacija}(t) - P_{apkrova}(t) - \Delta P_{atakos}\ (\text{t}), \qquad (4)$$

čia: V_a (t) - sistemos saugumo matavimo indeksas; $P_{generacija}(t)$ – visų atakuojamų jėgainių gamybos pajėgumas, laiko momentu t; $P_{apkrova}(t)$ – bendra apkrovimo paklausa laiku t; $\Delta P_{atakos}(t)$ – vėjo jėgainių gaminama energija, kurią užpuolikas gali paveikti.

Nustačius reikalingas dienas pažeidžiamumui išnaudoti, galimi tolimesni MTTC radimo veiksmai. Kadangi modeliuojama ataka susideda iš dviejų ugniasienių, tai atakos kelio komponentų skaičius yra – 2. Bendras nulinės dienos pažeidžiamumų skaičius yra 441 [20]. Bendras programinės įrangos subjektų skaičius yra 7083 [20]. Subjektų skaičius sistemoje yra priklausomas nuo tiriamosios sistemos struktūros. Apskaičiuotas CVSS išnaudojimo įvertinimas yra 3,9. Žinant visus duomenis, į (2) formulę įsistačius reikšmes, (5) formulėje apskaičiuojamas MTTC laikas.

$$\text{MTTC} = \left(24 + \frac{10}{3{,}9}\right) + \left(41 + 5{,}8 \times \frac{10}{3{,}9}\right) \times e^{\frac{-2\times 441}{7083}} = 27\ dienos. \qquad (5)$$

Toliau apskaičiuojama atakos kelio įveikimo tikimybė. Bendrą ugniasienių įveikimo tikimybę, galima apskaičiuoti naudojantis Bajeso tinklu, kuris apibrėžia bendra atakos kelio įveikimo tikimybės (6) formule [20].

$$P(E_i \text{ ir } E_j) = P(E_i) \times P(E_j|E_i), \qquad (6)$$

čia E_i ir E_j yra atskirų ugniasienių tikimybės, o $P(E_i|E_j)$ yra tikimybė, kad antra ugniasienė bus išnaudota, žinant, kad jau buvo išnaudota pirmoji.

Apskaičiuojama pirmosios ugniasienės įveikimo tikimybė [20]:

$$\mathrm{p}_1 = 1 - e^{\frac{-\mathrm{xk}}{\mathrm{m}}} = \ 1 - e^{-2*\frac{441}{7083}} = \ 0{,}117. \tag{7}$$

Apskaičiuojama antrosios ugniasienės įveikimo tikimybė [20]:

$$\mathrm{p}_2 = \ 1 - e^{\frac{-\mathrm{xk}}{\mathrm{m}}} = \ e^{-2*\frac{491}{7083}} = \ 0{,}8829. \tag{8}$$

Apskaičiuojama bendro atakos kelio tikimybė:

$$p_{bendras} = 0{,}117 * 0{,}8829 = 0{,}10. \tag{9}$$

Apskaičiavus bendro atakos kelio įveikimo tikimybę, galima apskaičiuoti vidutinį sistemos atstatymo laiką - MTTR. Turint reikiamus duomenis, vidutinis sistemos atstatymo laikas apskaičiuojamas naudojantis (10) formule [21].

$$p_{bendras} = \frac{MTTR}{MTTR+MTTC} = \frac{3}{3+27} = 0{,}1 \tag{10}$$

Vidutinis laikas, reikalingas vėjo jėgainių gedimui ar gedimams sutaisyti, atstatyti vėjo jėgainių parko normalų darbą, yra 3 dienos. Žinant MTTR galima apskaičiuoti nuostolius kuriuos patirs vėjo jėgainės savininkas kuomet vėjo jėgainių parkas patirs prastovas.

3.2. Skyriaus išvados ir apibendrinimai

Šiame skyriuje buvo sudaryta Bajeso tinklo modelis, kuriame yra pavaizduoti valdymo sistemos ryšiai ir galimi atakos scenarijai. Remiantis Bajeso metodu, buvo apskaičiuota bendra atakos kelio įveikimo tikimybė, kuri lygi 0,10, ir parodo, kaip tikėtina, kad užpuolikas sugebės įveikti saugumo priemones ir patekti į sistemą. Taip pat naudojant priimant atakos modelį ir CVSS skaičiuoklę, buvo įvestos jėgainės valdymo sistemos saugumo funkcijos ir atakos kelio braižas. Gautas aukščiausias galimas išnaudojimo balo įvertinimą 3,9.

Aukštesnis CVSS įvertinimas gali reikšti didesnį pažeidžiamumo sunkumą ir greitesnį išnaudojimo laiką, kas savo ruožtu gali padidinti MTTR ir sumažinti MTTC laikus. Iš to kyla išvada, kad organizacijos turi teikti pirmenybę pažeidžiamumo šalinimui su aukštesniais CVSS išnaudojimo įvertinimais, taip veiksmingai sumažinant sėkmingų atakų riziką. Tyrime apskaičiuota vidutinė laiko trukmė, reikalinga pažeidžiamumui išnaudoti, yra 27 dienos, o vidutinis sistemos atstatymo laikas yra 3 dienos.

Nustatyta, kad kuo daugiau valdymo sistema turi komponentų, tuo didesnė kibernetinės atakos įveikimo tikimybė. Nulinės dienos pažeidžiamumo išnaudojimas yra pavojingiausias, nes gali nebūti jokių įmanomų pataisų ar priemonių, apsaugančių nuo atakos ir saugos darbuotojams sunku nustatyti galimus atakos scenarijus ar galimus padarinius.

4. Investicijų į kibernetinį saugumą nustatymas

GL modelis siūlo numatant galimus nuostolius suskirstyti juos į turto ir informacijos šaltinių rinkinius, kuriuos praradus organizacija patirtų atitinkamus nuostolius [27]. Kadangi visi vėjo jėgainės įrenginiai yra reikalingi sklandžiam vėjo jėgainės veikimui, nuostolių rinkinys negali būti suskirstytas pagal svarbą, nes nėra kriterijų kurie išskirtų vėjo jėgainių įrenginius pagal svarbumą. Todėl šiame tyrime nuostolių rinkiniai sudaromi naudojantis SNL tyrėjų pritaikytu GL modelių, kuomet jėgainės nuostolių rinkiniai sudaromi pagal galimų nuostolių dydžius.

Šiame tyrime galimų nuostolių dydžio nustatymo proceso žingsniai:
1. Tiriamos vėjo jėgainės tipo nustatymas. Šiame tyrime, pasirenkamos jėgainių tipas kurios bus naudojamos Lietuvoje planuojamuose 700 MW vėjo jėgainių parkuose.
2. VJ įrenginių kurie gali būti pažeisti nustatymas. Įrenginiai bus pasirinkti pagal literatūros apžvalgos dalyje išnagrinėtų vėjo jėgainės įrenginių kurie gali būti pažeisti kibernetinėmis atakomis.
3. Pažeidžiamų vėjo jėgainės įrenginių kainos nustatymas.
4. Pagal pasirinktą vėjo jėgainės tipą ar modelį sudedamųjų dalių kainos išreikštos procentine dalimi apskaičiavimas, pagal aštuntą lentelę.
5 Nuostolių rinkiniai nustatomi remiantis pagal Lietuvos Respublikos vyriausybės nutarime „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (2018), nustatytais kriterijais, kuriais vadovaujantis kibernetiniai incidentai skirstomi į kibernetinių incidentų kategorijas.
6. Naudojantis GL modelyje pateiktomis produktyvumo funkcijomis, jos priskiriamos prie nusistatytų nuostolių rinkinių.
7. Apskaičiuojami grynųjų naudų ir pažeidimo tikimybių sumažėjimo duomenų lentelės ir nubraižomas investavimo į kibernetinį saugumą naudos grafikas.

Pagal Litgrid 2023m., paskelbtas „Išankstinės prisijungimo sąlygos vėjo elektrinių jūrinėje teritorijoje prijungimui prie elektros perdavimo tinklo“. Nustatyta, kad Baltijos jūroje 700 MW vėjo jėgainių parkuose bus naudojamos 10 MW galingumo, fiksuoto pamato tipo, vėjo jėgainės [56]. Pagal vėjo jėgainių kainų apžvalgos duomenis, nustatoma fiksuoto pamato jūrinės vėjo jėgainės kainą [36]. Nustačius, kad jūros vėjo jėgainių parke bus diegiamos 10 MW galingumo fiksuoto pamato tipo vėjo jėgainės, pagal (Offshore Wind Marker Report: 2022 Edition (Musial et al. 2022)) nurodoma, kad 1 kW vėjo jėgainės su visais reikiamais įrenginiais darbui, neįskaičiuojant darbo ir kitų išlaidų kainuoja 1,301 $ tai, reiškia 10 MW elektrinė kainuos 13 010 000 $ [36]. Pagal 2023-05-03 „Nasdaq“ (EUR/USD) kursą [67], doleriai konvertuoti į eurus: 11 716 800 €.

Pagal pateiktus vėjo jėgainės investicinių sąnaudų paskirstymo duomenis apskaičiuojami galimi vėjo jėgainės nuostoliai (žr. 8 lentelę) [28]. Šiame tyrime kabinos, veleno, menčių, stebulės, bokšto, bei grafų „kiti“ įrenginiai nėra įtraukiami tarp kibernetinių atakų taikinių, kadangi teorinėje dalyje apžvelgtuose literatūriniuose šaltiniuose nebuvo pateikta informacijos apie kibernetinių atakų įtaką šioms dalims ir įrenginiams. Priimta, kad galimi kibernetinių atakų taikiniai yra įrenginiai, kurie buvo paminėti teorinėje dalyje apžvelgtuose šaltiniuose: galios keitiklis, generatorius, kontrolės valdymo sistema, menčių pasisukimo žingsnių valdymo sistema. Galimų vėjo jėgainės nuostolių dalis nuo visos vėjo jėgainė kainos apskaičiuojama taip:

$10{,}61\%_{\text{galios keitiklis}} + 15{,}15\%_{\text{generatorius}} + 3{,}79\%_{\text{kontrolės valdymo sistema}} + 1{,}52\%_{\text{žingsnių sistema}} = 31{,}07\%.$

Atakos metu gali būti paveikta 31,07% visos vėjo jėgainės vertės tai yra: 3 640 409,76 €.

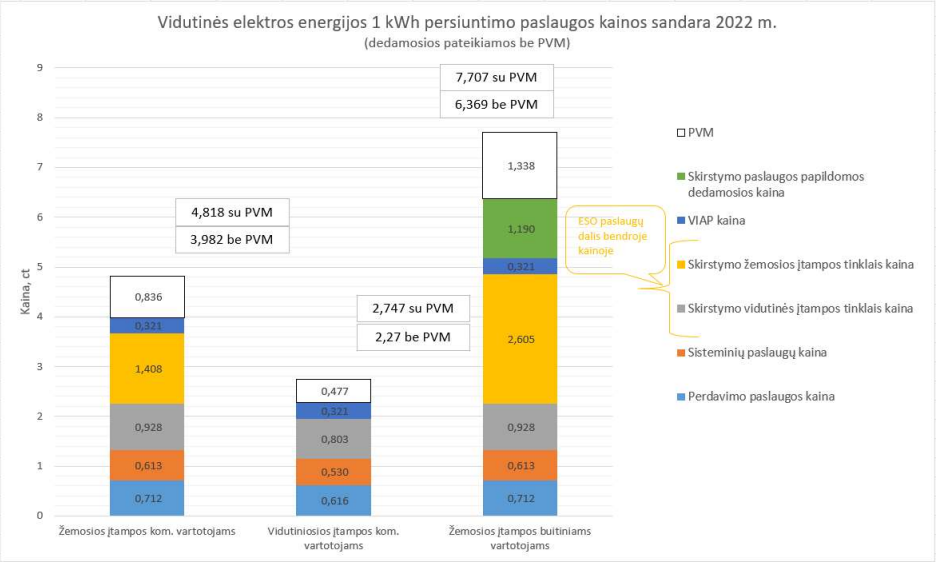
8 lentelė. 10 MW jūros vėjo jėgainės sudedamųjų kainos dalių išreiškimas procentine dalimi [28].

Įrenginio pavadinimas	Komponento kainos dalis visos vėjo elektrinės vertės kontekste
Kabina:	60,61 %
Guoliavietė ir velenas	6,06 %
Vėjaračio guoliai	3,03 %
Pavarų dėžė	10,61 %
Generatorius	15,15 %
Galios keitiklis	10,61 %
Valdymo sistema	3,79 %
Kiti	11,06 %
Rotorius:	28,79 %
Vėjaračio mentės	19,70 %
Vėjaračio stebulė	2,27 %
Menčių sukinėjimo sistema	1,52 %
Kiti	5,15 %
Bokštas	10,61%

Kadangi vėjo jėgainių parke stovinčios vėjo jėgainės yra 10 MW galingumo, o apskaičiuotas MTTR laikas yra 3 dienos arba 72h. Bendras nepagamintos ir neparduotos elektros energijos kiekis per laiką kuomet vėjo jėgainė dėl kibernetinės atakos padarinių patirs prastovas yra 720 MW.

Tyrime priimta, kad elektrinių savininkas yra Lietuvos valstybė, už prastovų metu nepagamintą ir neparduotą elektros energiją, į Lietuvos valstybės biudžetą nebus sumokėtas PVM. Nesumokėtas PVM apskaičiuojamas atliekant nepagamintos elektros energijos kiekio sandaugą su 2022 metų duomenų, vidutinės elektros energijos persiuntimo paslaugos kainos PVM dalimi – 0,0133 € / 1 kWh (žr. 30 pav.). Prarastos valstybės pajamos už vartotojų nesumokėtus PVM mokesčius apskaičiuojamos taip:

$$720\,000\ \text{kW} \times 0{,}01338\ € \text{ (PVM dedamoji)} = 9633{,}6\ €. \qquad (11)$$



30 pav. 2022 metų Lietuvos elektros kainos dedamųjų vidutinės vertės [58]

Remiantis „Kaspersky“ tyrimų numatomos kibernetinės atakos padarytos žalos remonto darbų vidutinės išlaidos organizacijai yra apie 600 000 € [46]. Žinant kad Baltijos jūroje planuojamo vėjo elektrinių parko galia yra 700 MW, o vienos vėjo jėgainės galingumas 10 MW, tai vienos vėjo jėgainės vidutinės remonto išlaidos randamos yra 8572 € [1].

Maksimalūs piniginiai nuostoliai nustatomi sudedant pažeidžiamos įrangos vertę, numatomas remonto išlaidas, prarastas pajamos už nepagamintą ir neparduotą elektros energiją:

$$L = 3\,640\,409{,}76\ € + 8572\ € + 9633{,}6\ € = 3\,658\,615{,}2\ €. \quad (12)$$

Pagal SNL pritaikytą GL modelį jėgainės pažeidžiamumas priimamas su 0,5 tikimybe. Tai reiškia kad užpuolikas gali sugadinti 50 % pažeidžiamos vėjo jėgainių įrangos vertės. Tikėtini nuostoliai dėl kibernetinės atakos pažeidimo, įvertinus pažeidžiamumo tikimybę, apskaičiuojami taip [1]:

$$vL = 0{,}5 \times 3\,658\,615{,}2\ € = 1829307{,}6\ €, \quad (13)$$

čia: L – atakos nuostoliai; v – pažeidžiamumas.
Tyrime, naudojamos GL modelyje pateiktos produktyvumo funkcijos [27]. Šiame tyrime nuspręsta produktyvumo funkcijas priskirti pavojingumo kategorijoms pagal nuostolių dydžius, nustatytus Lietuvos Respublikos vyriausybės nutarime „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (2018). Nutarime nustatyti kriterijai, kuriais vadovaujantis kibernetiniai incidentai skirstomi į keturias kibernetinių incidentų kategorijas [55,62]:
- pavojingi kibernetiniai incidentai;
- didelio poveikio kibernetiniai incidentai;
- vidutinio poveikio kibernetiniai incidentai;
- nereikšmingo poveikio kibernetiniai incidentai.

Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami pavojingumo kategorijai aprašyti devintoje lentelėje. Įvertinus galimų nuostolių dydį, naudojantis pateiktais kriterijais kibernetinė ataka priskiriama pavojingumo kategorijai.

9 lentelė. Kriterijų, kuriais vadovaujantis kibernetiniai incidentai priskiriami kibernetinių incidentų kategorijoms, sąrašas [55,62].

Nereikšmingas (N) (bent vienas iš kriterijų)				**Vidutinis (V)** (du ar daugiau kriterijų)					**Didelis (D)** (du ar daugiau kriterijų)					**Pavojingas (P)** (bent vienas iš kriterijų)		
RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše

Produktyvumo funkcija yra matematinis modelis, kuris įvertina, kaip investicijos į kibernetinę saugą turi įtakos kibernetiniam atsparumui [27]. Pagal NERC vertinimo sistemą (žr. 7 lent.) šiame tyrime modeliuojama ataka atitinka pačios pavojingiausios 5 lygio rizikos grupės, aprašymą, nes atakos metu užpuolikas įgyja sistemos valdymo teisę. Remiantis, kad investicijos paprastai yra produktyvesnės ten, kur pažeidžiamumas yra didžiausias produktyvumo funkcijos paskirstomos taip [27]:

- Produktyvumo funkcija: $s(z,v)=v/(1+z)$ naudojama esant nereikšmingam poveikiui, kuomet nuostoliai mažiau nei 250 000 €.
- Produktyvumo funkcija: $s(z,v)=v/(1+z)^2$ naudojama esant vidutiniam poveikiui, kuomet nuostoliai daugiau nei 250 000 €, bet mažiau nei 500 000 €.
- Produktyvumo funkcija: $s(z,v)=v/(1+z)^3$ naudojama esant didelio arba pavojingo poveikio incidentui, kuomet nuostoliai daugiau nei 500 000 €.

Produktyvumo funkcijos parinkimas pagal devintos lentelės nuostolių ribas:

$$1829307{,}6\ € > 500\ 000\ €. \tag{14}$$

Kadangi galimi nuostoliai yra daugiau, nei 500 000 € tai, pasirenkama produktyviausia funkcija:

$$s(z, v) = v / (1 + z)^3. \tag{15}$$

Pirmiausia apskaičiuojamas pažeidimo tikimybės sumažėjimas, priklausomai nuo investicijų pagal (15) formulę. Gauti rezultatai pateikti dešimtoje lentelėje.

10 lentelė. Pažeidimo tikimybės sumažėjimas, priklausomai nuo investicijų

Investicijos į kibernetinę saugą, €	0	100 000	200 000	285 000	286 000	287 000	300 000	400 000	500 000
Pažeidimo tikimybės sumažėjimas	0	0,124	0,211	0,264	0,265	0,265	0,272	0,318	0,352
Investicijos į kibernetinę saugą, €	530 000	531 000	532 000	600 000	700 000	800 000	900 000	1 000 000	1 100 000
Pažeidimo tikimybės sumažėjimas	0,360	0,361	0,361	0,378	0,398	0,414	0,427	0,438	0,446
Investicijos į kibernetinę saugą, €	1 200 000	1 300 000	1 400 000	1 500 000	1 600 000	1 700 000	1 800 000	1 900 000	2 000 000
Pažeidimo tikimybės sumažėjimas	0,453	0,459	0,464	0,468	0,472	0,475	0,477	0,479	0,481

Pagal (16) formulę, naudojantis: pradinių nuostolių dydžiu, investicijų dydžiu, pradine nuostolių tikimybę ir pagal dešimtoje lentelėje gautomis tikimybėmis, apskaičiuotos skirtingų investicijų į kibernetinį saugumą grynosios naudos (EBNC) pateiktos vienuoliktoje lentelėje [1]:

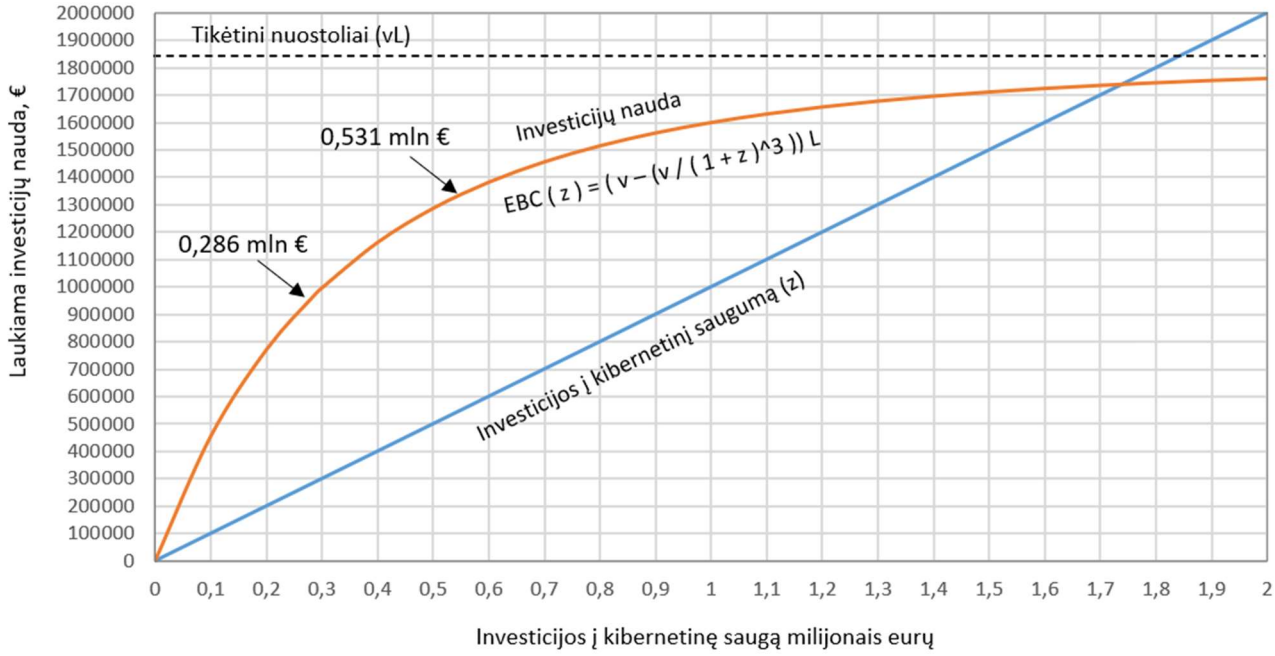
$$EBNC(z) = [v - s(z, v)] L - z, \tag{16}$$

čia: z - investicijos į kibernetinį saugumą; s(z, v) - produktyvumo funkcija, kai investicijos į kibernetinio saugumo technologijas sumažina sistemos pažeidžiamumą sumažindamos pažeidimo tikimybę.

11 lentelė. Grynoji nauda iš investicijų į kibernetinį saugumą (EBNC)

Investicijos į kibernetinę saugą, €	0	100 000	200 000	285 000	286 000	287 000	300 000	400 000	500 000
Investicijų į kibernetinį saugumą grynoji nauda, €	0	355 094	570 972	682 535	683 545	684 549	697 046	763 090	787 778
Investicijos į kibernetinę saugą, €	530 000	531 000	532 000	600 000	700 000	800 000	900 000	1 000 000	1 100 000
Investicijų į kibernetinį saugumą grynoji nauda, €	789 052	789 052	789 050	783 223	757 519	716 214	663 197	601 250	532 397
Investicijos į kibernetinę saugą, €	1 200 000	1 300 000	1 400 000	1 500 000	1 600 000	1 700 000	1 800 000	1 900 000	2 000 000
Investicijų į kibernetinį saugumą grynoji nauda, €	458 137	379 593	297 622	212 880	125 881	37 026	-53 364	-145 034	-237 778

Gordon-Loeb modelis teigia, kad optimalus investicijų lygis pasiekiamas tada, kai laukiama ribinė nauda yra lygi numatomoms ribinėms išlaidoms. Tai reiškia, kad organizacija pasieks optimalią investicijų lygį, kai papildomos investicijos į kibernetinį saugumą teikia naudą, kuri yra proporcinga investicijų išlaidoms. Todėl tiriamajame atvejyje optimalios investicijos yra 286 000 €. O investicijos su didžiausia grynąją nauda yra 531 000 €. Naudojantis vienuolikta lentele, nubraižomas investavimo į kibernetinį saugumą naudos grafikas grafikas (žr. 31 pav.).



31 pav. Investavimo į kibernetinį saugumą naudos grafikas

Gordonas ir Loebas parodė, kad organizacijos turėtų investuoti ne daugiau kaip 37 % tikėtinų nuostolių nuo kibernetinio saugumo pažeidimo. Numatomos investicijos turi atitikti (17) nelygybę:

$$z^*(v) \leq vL / e, \quad (17)$$

čia: z* - optimalus investicijų lygis; e - 2,7182 konstanta.

Gordon-Loeb modelis teigia, kad optimalus investicijų lygis pasiekiamas tada, kai laukiama ribinė nauda yra lygi numatomoms ribinėms išlaidoms. Tai reiškia, kad organizacija pasieks optimalią investicijų lygį, kai papildomos investicijos į kibernetinį saugumą teikia naudą, kuri yra proporcinga investicijų išlaidoms. Todėl tiriamajame atvejyje optimalios investicijos yra 286 000 €.

$$286\,000\ € \times (0{,}5) \leq 0{,}8606 \times 1\,829\,307{,}6\ € / 2{,}7182. \quad (18)$$

$$143\,000\ € \leq 579\,170{,}82\ €. \quad (19)$$

4.1. Skyriaus išvados ir apibendrinimai

Gordono-Loebo modelio rekomendacija neinvestuoti daugiau nei 37% nuo nuostolių yra pagrįsta ekonomine logika ir siekia maksimizuoti investicijų naudą ir riboti riziką. Kai investicijų į informacijos saugumą suma viršija 37% nuostolių, papildomos investicijos nebepridedа pakankamai naudos, kad būtų pagrįsta tokią didelę riziką ir sąnaudas. Tiriamajame atvejyje maksimalios investicijos atitinkančios 37 % rekomendaciją yra 579 170 eurų.

Skaičiuojant GL modelį, investicijos į kibernetinę apsaugą ne visiškai panaikina atakos tikimybę, bet ją tik sumažina. Tačiau investuoti pinigai į kibernetinę apsaugą gali sumažinti galimus atakos nuostolius. Tai reiškia, kad nors visiškas atakų išvengimas yra neįmanomas, investicijos į kibernetinę saugą padidina organizacijos gynybos lygį ir sumažina potencialius finansinius nuostolius.

Šiame skyriuje pagal pasirinktos vėjo jėgainės tipą, įvertinamos pažeidžiamų įrenginių kainos, apskaičiuojami potencialūs nuostoliai dėl patirtos kibernetinės atakos. Taip pat įvertinami kibernetinės atakos padarytos žalos remonto darbų išlaidos, negautas pajamos už nepagamintos ir neparduotos elektros energijos vidutinės išlaidas. Maksimalūs piniginiai nuostoliai apskaičiuojami sudedant objekto įrangos vertę, remonto išlaidas ir prarastas pajamas už neparduotą elektros energiją.

Pagal Gordono-Loebo modelį priimta kibernetinės atakos įrenginių sugadinimo tikimybė yra 0,5, galimi vėjo jėgainės kibernetinės atakos nuostoliai yra 1 830 000 €. Naudojantis galimų nuostolių dydžiais, buvo priskirtos produktyvumo funkcijos parodančios kaip investicijos į kibernetinės saugos priemonės didiną vėjo jėgainių kibernetinį atsparumą. Tyrimo metu nustatyta, kad investicijų nauda didžiausia, kuomet investavus 531 000 € į kibernetinio saugumo užtikrinimą, kibernetinės atakos tikimybė sumažėjo nuo 0,5 iki 0,1396. 531 000 eurai į kibernetinio atsparumo didinimą neviršijo 37% vėjo jėgainės nuostolių vertės.

Investuojant į kibernetinės saugos priemones 285 000 €, grynoji nauda siektų 682 535 €. Jei investuotume papildomą tūkstantį, t. y. 286 000 €, grynoji nauda padidėtų iki 683 545 €. Tai reiškia, kad papildomai investuotas tūkstantis eurų atneštų papildomos grynosios naudos už 1010 €. Tačiau, jei investicijos padidėtų iki 287 000 €, grynoji nauda padidėtų iki 684 549 €, bet papildomai investuotas tūkstantis eurų atneštų naudos už mažiau nei tūkstantį eurų t.y. 996 € (žr. 11 lentelę).

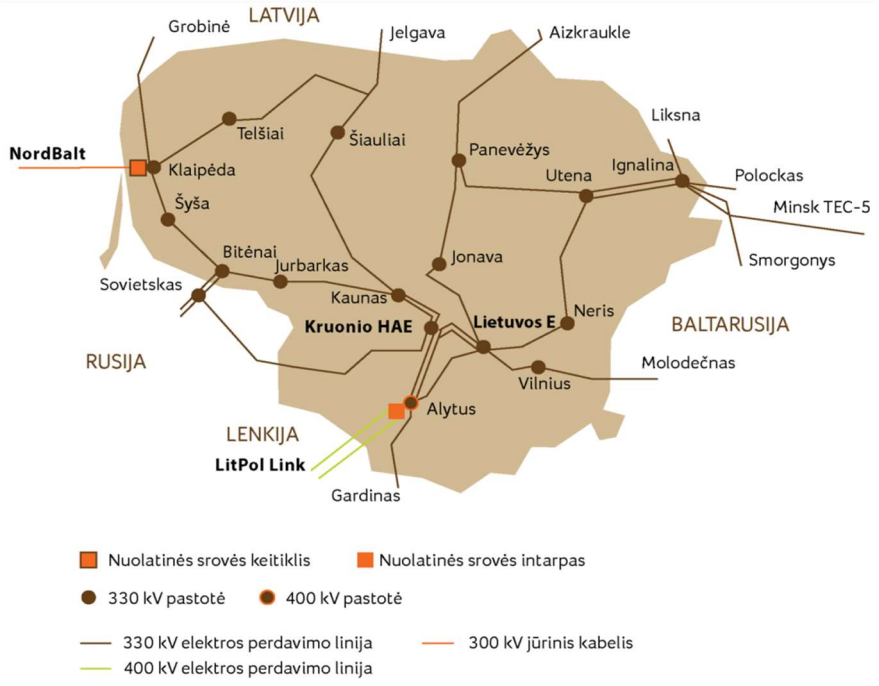
Gordon-Loeb modelis teigia, kad optimalus investicijų lygis pasiekiamas tada, kai laukiama ribinė nauda yra lygi numatomoms ribinėms išlaidoms. Tai reiškia, kad organizacija pasieks optimalią investicijų lygį, kai papildomos investicijos į kibernetinį saugumą teikia naudą, kuri yra proporcinga investicijų išlaidoms. Todėl tiriamajame atvejyje optimalios investicijos yra 286 000 €.

5. Vėjo jėgainių parko kibernetinės-fizinės atakos įtaka elektros tinklui tyrimas

Atsižvelgiant į aktyvėjančius rusų kibernetinius sukčius, kurie vykdo arba vykdė sabotažus prieš energetikos sistemas, įskaitant Ukrainą, Vokietiją ir Austriją taip pat matant jų veiklą Šiaurės jūros dugne, kur rusų laivai vykdo vėjo jėgainių parkų ir komunikacijos kabelių infrastruktūros stebėjimą, taip pat atsižvelgiant į Rusijos taikomas taktikas Ukrainos karo kontekste, galima manyti, jog Rusijos atakos tikslas yra ne tik padaryti žalą tiesiogiai atakuojamiems objektams, bet ir destabilizuoti elektros tinklą. Šiuo metu Baltijos jūroje yra planuojamas 700 MW Lietuvos vėjo jėgainių parko atidarymas iki 2028 metų pirmuoju etapu, kuris užtikrins iki ketvirtadalio Lietuvos elektros energijos poreikio. Antruoju šio projekto etapu planuojamas dar vienas 700 MW vėjo jėgainių parkas, taigi abiejų jėgainių bendras galingumas sieks 1400 MW [57]. Štai kodėl yra itin svarbu suprasti, kokios pasekmės gali kilti dėl potencialių kibernetinių ir fizinių atakų bei kokią įtaką tai gali turėti elektros tiekimui regione [59]. Tyrimas gali padėti įvertinti rizikos lygį ir parengti atitinkamas saugumo priemones, kurios padėtų apsisaugoti nuo potencialių atakų ir užtikrinti stabilų elektros tiekimą regione.

5.1. Esama energijos perdavimo infrastruktūra

Lietuvos elektros energetikos sistema turi tiesioginius sujungimus su su Švedijos, Lenkijos, Baltarusijos, Latvijos ir Rusijos elektros sistemomis (žr. 32 pav.). Švedijos elektros energetikos sistema (EES) yra sujungta su Lietuvos EES nuolatinės srovės jungtimi, kurios pralaidumas yra iki 700 MW. Lietuvos ir Lenkijos EES yra sujungtos dvigrande 400 kV elektros perdavimo liniją. Latvijos EES yra sujungta su Lietuvos EES per keturias 330 kV ir tris 110 kV linijas. Pjūvio pralaidumas siekia 1500 MW į Lietuvos EES ir 1200 MW iš Lietuvos EES. Baltarusijos EES yra sujungta su Lietuvos EES per penkias 330 kV ir septynias 110 kV linijas. Pjūvio pralaidumas siekia 1300 MW į Lietuvos EES ir 1350 MW iš Lietuvos EES. Rusijos (Kaliningrado) EES yra sujungta su Lietuvos EES per tris 330 kV ir tris 110 kV linijas [61].

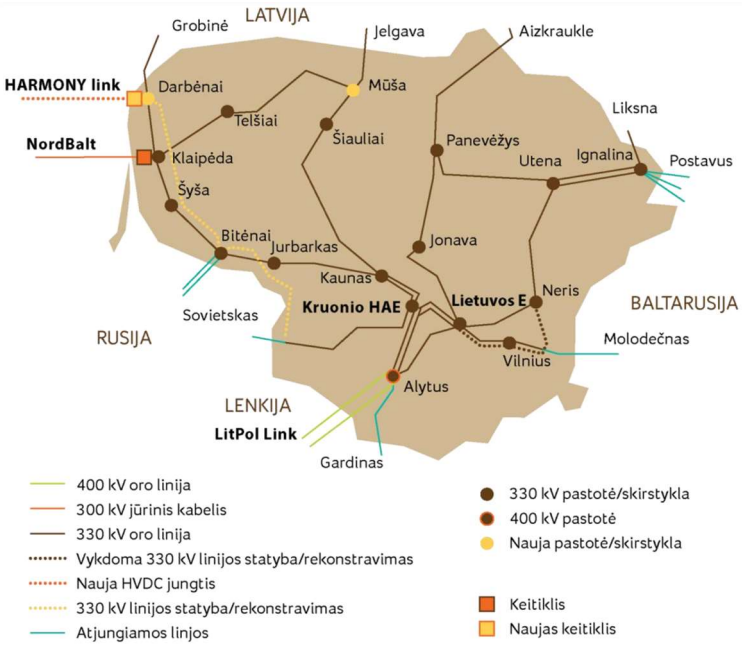


32 pav. Elektros perdavimo schema ir duomenys [61]

2022m. vėjo elektrinėse pagaminta elektra sudarė 13,52 proc. galutinio Lietuvos elektros energijos suvartojamo kiekio arba 2 proc. daugiau nei 2021 m. Energetikos ministerijos duomenimis, praeitais metais Lietuvoje išaugo instaliuota vėjo elektrinių galia. Per metus prisidėjo apie 370 MW ir metų pabaigoje šalyje iš viso buvo instaliuota 946 MW galios vėjo elektrinių (803 MW vėjo elektrinių perdavimo tinkle, 143 MW vėjo elektrinių skirstomajame tinkle). Jos sudaro 62,4 proc. šalies tinkle instaliuotų atsinaujinančių energijos išteklių [54].

5.2. Lietuvos 2028 m. 330-400 kV perdavimo tinklo sinchronizavimo ir integracijos prognozė

Lietuvos elektros energetikos tikslas yra iki 2028 m. sinchroniniu režimu sujungti Baltijos šalių (Lietuvos, Latvijos, Estijos) elektros energijos sistemas su Kontinentiniu Europos tinklu (KET) ir integruotis į Šiaurės šalių elektros rinką. Bet pirmiau Lietuvos, Latvijos ir Estijos elektros tinklai bus atjungti nuo Rusijos ir Baltarusijos elektros tinklų (žr. 33 pav.).



33 pav. 400–330 kV perdavimo tinklas [61]

Prisijungimui prie KET planuojama rekonstruoti esamą viengrandę 330 kV OL Lietuvos E-Vilnius į dvigrandę, optimizuoti Šiaurės rytų Lietuvos elektros perdavimo tinklą, atlikti darbus „LitPol Link“ išplėtimui, pastatyti naują 330 kV elektros perdavimo liniją (EPL) Vilnius-Neris. Įrengiant naują jūrinę jungtį su Lenkijos elektros energijos sistema, kuri reikalauja pastatyti 330 kV EPL Bitėnai – Kruonio HAE, EPL Darbėnai – Bitėnai, ir 330 kV skirstyklas „Darbėnai“ ir „Mūšą“ [61].

5.3. Elektros energetikos sistemos stabilumas

Elektros energetikos sistema yra elektrą gaminančių elektrinių, elektros vartotojų imtuvų ir aukštos ir žemos įtampos tinklų visuma, kuri yra sujungta bendru elektros gamybos, perdavimo ir vartojimo režimu. Lietuvoje už aukštų įtampų elektros perdavimo linijų ir įrenginių elektros perdavimą atsakingas perdavimo sistemos operatorius LITGRID AB. [60] Žemų ir vidutinių įtampų elektros skirstymo tinklų elektros energijos persiuntimą galutiniam vartotojui atsakingi skirstomųjų tinkų operatoriai [60].

Dinaminis elektros energetikos sistemos stabilumas – elektros energetikos sistemos savybė atkurti buvusį arba jam artimą savo darbo režimą po staigaus didelio trikdžio. Tokiais trikdžiais laikomi trumpieji jungimai, apkrautų elektros energetikos sistemos elementų atsijungimas ir panašiai [63].

Leidžiamieji įtampos nuokrypiai po nenumatytų atvejų 330 kV Europos tinkluose yra 10% [35]. Didžiausias galimas 330 kV tinklo dažnio nuokrypis Europos elektros tinkluose yra 0,8 Hz, t.y. mažiausias galimas dažnis yra 49,2 Hz [29]. Jei įtampa ir dažnis 330 kV tinkle neatitinka stabilumo reikalavimų, elektros tinklo operatorius gali imtis veiksmų sumažinti tinklo apkrovas atjungiant tam tikras elektros linijas, energijos tiekimo šaltinius arba vartotojus.

Elektros sistemos režimas yra visų procesų, vykstančių sistemoje, visuma, kuri apibūdina sistemos būseną tam tikru laiko momentu ar laiko intervale. Režimas yra apibrėžiamas sistemos parametrais - kiekybiniais rodikliais, kurie atspindi sistemos būseną, tokiais kaip galia, įtampa, srovė, kampas ir pan., ir kurie yra tarpusavyje susiję.

Elektros sistemos režimas gali būti suskirstytas į dvi pagrindines kategorijas: stacionariuosius (nusistovėjusius) ir pereinamuosius. Stacionarus režimas pasižymi tuo, kad elektros sistemos parametrai svyruoja aplink vidutinės reikšmės lygį, tačiau nepasiekia aukštesnių ar žemesnių ribų. Šio režimo metu elektros energija tiekiama stabiliai, o avarijų neįvyksta. Stacionarus režimas gali būti paprastas arba sudėtingas, priklausomai nuo elektros sistemos dydžio ir sudėtingumo.

Pereinamasis režimas įvyksta, kai elektros sistemos parametrai keičiasi nuo stacionaraus režimo į kitą arba iš vieno režimo į kitą. Šio režimo metu gali kilti laikini nestabilumai ir elektros energijos tiekimo šuoliai. Pereinamasis režimas gali būti planuojamas arba neatidėliotinas, priklausomai nuo situacijos.

Skirtingi elektros sistemos režimai yra suskirstyti į penkias kategorijas [68]:
1. Normalūs stacionarieji - tai elektros sistemos režimas, kai jos parametrai yra stabilūs, elektros energija tiekiama nuolat ir be avarijų.
2. Normalūs pereinamieji - tai elektros sistemos režimas, kai jos parametrai keičiasi planuotai arba nuolat, pavyzdžiui, perjungiant elektros linijas arba patiriant didelę elektros energijos apkrovą.
3. Avariniai pereinamieji - tai elektros sistemos režimas, kai jos parametrai keičiasi dėl elektros sistemos avarijos, bet vėliau grįžta į normalią būseną.
4. Avariniai stacionarieji - tai elektros sistemos režimas, kai jos parametrai yra stabilūs, tačiau elektros energija tiekiama alternatyviomis priemonėmis dėl elektros sistemos avarijos.
5. Po avariniai stacionarieji - tai elektros sistemos režimas, kai jos parametrai yra stabilūs, bet elektros energija tiekiama alternatyviomis priemonėmis po elektros sistemos avarijos, kol bus atkurti normalūs elektros sistemos parametrai.

Normalių ir avarinių režimų skaičiavimai atlikti naudojantis „Siemens“ „PSS/E 33“ programa. Lietuvos elektros sistema modeliuojama remiantis 2028 metų prognoze, kuomet Lietuvos elektros tinklas bus sujungtas su kontinentinės Europos elektros tinklais darbui sinchroniniu režimu [44]. Todėl šiame tyrime į tiriamąją Lietuvos elektros tinklo schema nėra įtraukti Baltarusijos ir Rusijos tinklai, modeliuojant modelį jie buvo atjungti. Lietuvos elektros tinklas schemoje sujungtas su Latvija, Lenkija ir Švedija.

Atliekant šį tyrimą nagrinėti normalių ir avarinių režimų scenarijai. Siekiant ištirti Lietuvos elektros tinklo dinaminio stabilumo reakciją į planuojamų vėjo jėgainių parkų atsijungimus, ir trumpuosius jungimus.

Šiame tyrime pagal 2016 metų duomenis nagrinėti žiemos maksimumo darbo dienų apkrovimai ir vasaros minimumo darbo dienų apkrovimai. Kelių Lietuvos tinklo didžiausių generatorių apkrovimai pateikti (žr. 12 ir 13 lentelę).

12 lentelė. Skaičiuojamųjų režimų vasaros minimumo duomenys.

Vasaros minimumas				
Pavadinimas	**Mazgo Nr.**	**Galia MW**	**Qmax MW**	**Qmin**
Šyša	5293	42	8,5285	-8,5285
KHAE G3, G4	5819, 5820	126	120	-40
LE8	5828	189	248	-120
LE9	5823	311,5	260	-134
VE3_B1	5877	113	181	-74,5
SANTAKA2	5881	32,9	20	-20
VE_BITĖNAI 20	6834	54,6	11,087	-11,087

13 lentelė. Skaičiuojamųjų režimų žiemos maksimumo duomenys.

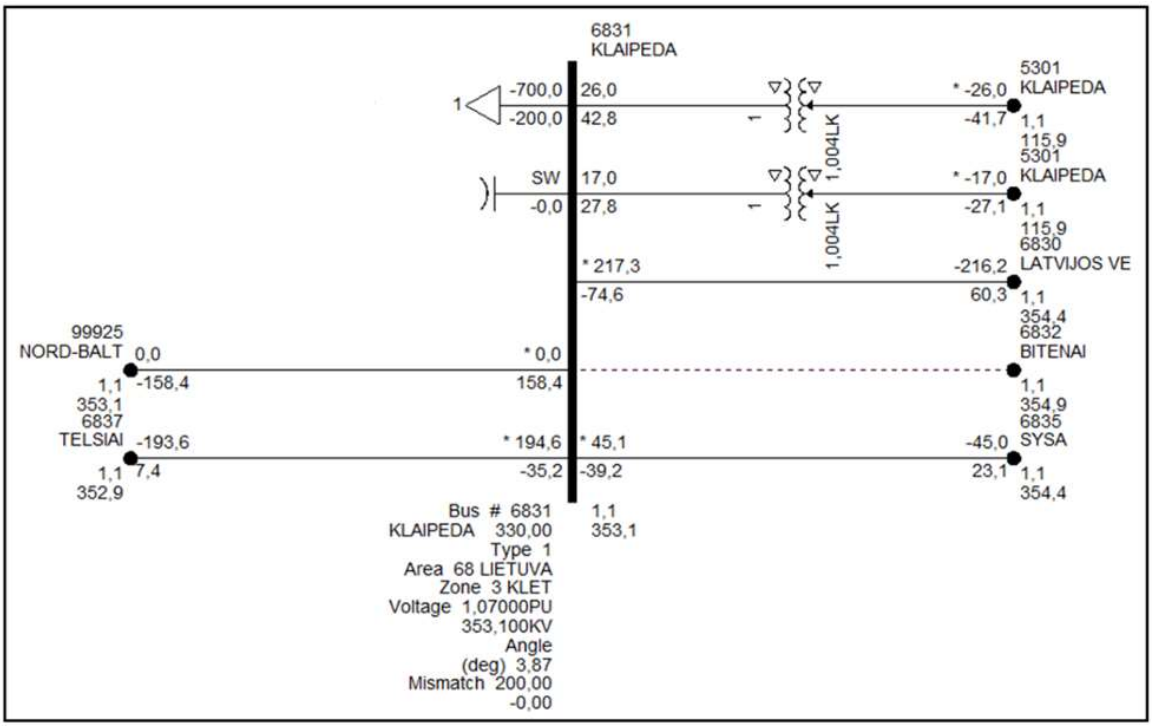
Žiemos maksimumas				
Pavadinimas	**Mazgo Nr.**	**Galia MW**	**Qmax MW**	**Qmin**
Šyša	5293	60	12,1835	-12,1835
KHAE G3, G4	5819, 5820	180	10	-8
LE8	5828	270	248	-120
LE9	5823	445	260	-134
VE3_B1	5877	162	181	-74,5
SANTAKA2	5881	47	20	-20
VE_BITĖNAI 20	6834	78	15,8386	-15,8386

Klaipėdos 330 kV mazge, nustatyti prijungtų vėjo jėgainių darbo apkrovimai, priklausomai nuo skaičiuojamo scenarijaus ir naudojamo režimo (žr. 14 lentelę).

14 lentelė. Nustatyti prijungtų vėjo jėgainių darbo apkrovimai priklausomai nuo režimo.

Pavadinimas	**Galia MW**	**Qmax MW**	**Qmin**
700 MW VJP vasaros min.	350	140	-140
700 MW VJP žiemos maks.	700	200	-200
1400 MW VJP vasaros min.	980	280	-280
1400 MW VJP žiemos maks.	1400	400	-400

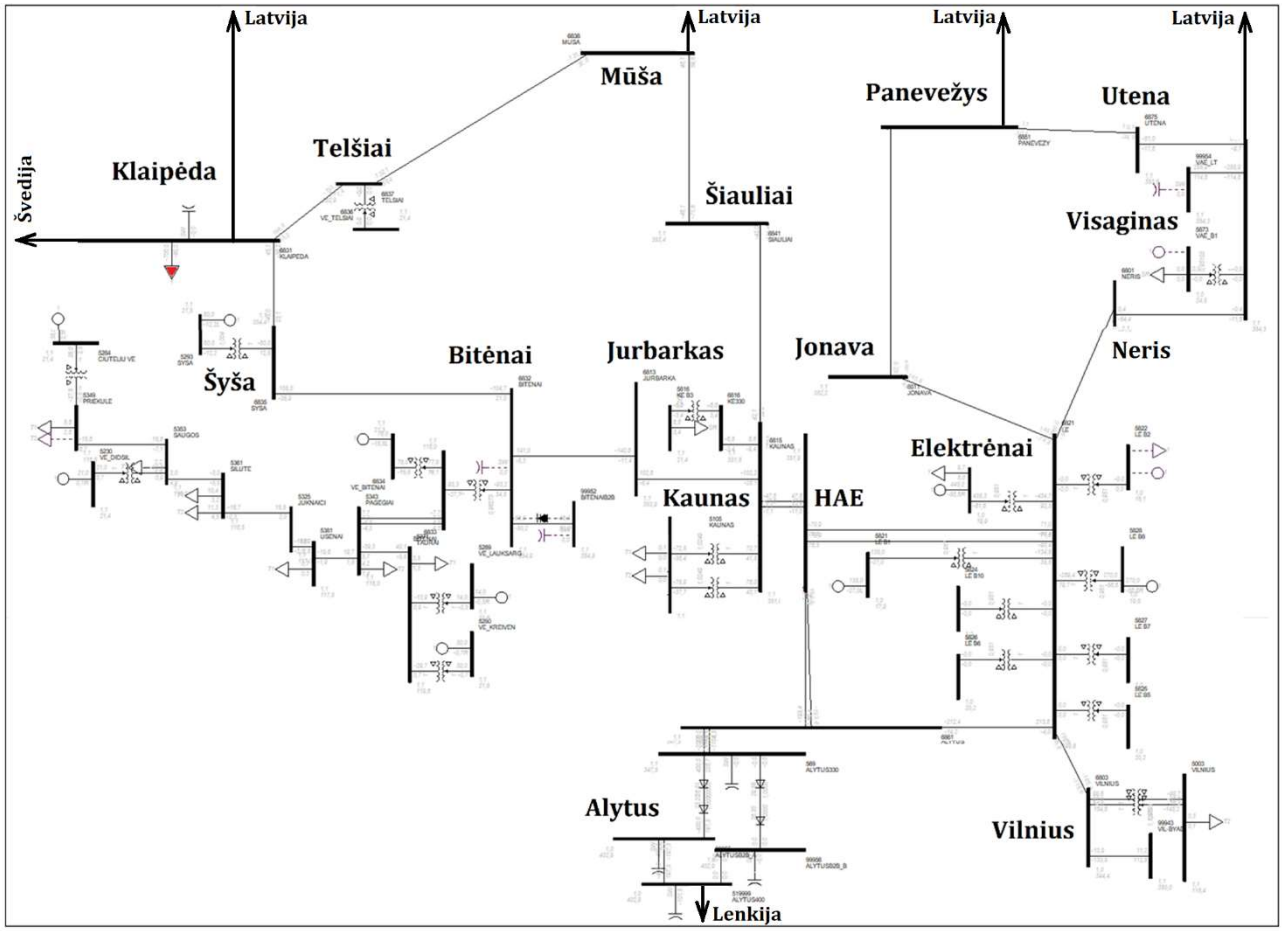
Vėjo jėgainių prijungimo prie elektros sistemos prijungimo vieta pavaizduota paveiksle (žr. 34 pav.)



34 pav. Vėjo jėgainių parko prijungimo prie elektros sistemos prijungimo vieta

PSS/E programoje pirmiausia nustatyta elektros tinklo schemą, remiantis 2028 metų 330-400 kV Lietuvos tinklo prognoze, buvo atjungti Rusijos ir Baltarusijos elektros tinklai. Tuomet nustatyti sistemos mazgų, generatorių, transformatorių ir apkrovų duomenys. Parinkti keturi ataskaitiniai mazgai: Klaipėdos 330 kV mazgas, Alytaus 330 kV mazgas, Kauno Hidro Akumuliacinės Elektrinės (KHAE) 330 kV mazgas ir Visagino Atominės Elektrinės (VAE) 330 kV mazgas. Šiuose mazguose bus analizuojamas įtampos ir dažnio stabilumas. Tuomet įvesti duomenys apie tiriamojo vėjo jėgainių parką. Pridėjus VJP prie elektros sistemos patikrinama, kaip šie įvesti duomenys veikia elektros sistemos tinklą. Patikrinama ar prie sistemos pridėjus neigiamą apkrovą (Vėjo jėgainių parką), išvengiama žadinimo reguliatorių peržengimo ribų, reikia suderinti režimus, taip, kad reaktyvioji balansinio mazgo galia būtų leistinose ribose, visais tirtais atvejais reaktyvioji balansinio mazgo galia buvo 0,00 MVA.

Pereinamųjų procesų skaičiavimų etape atliekti skaičiavimai ir analizė, susiję su pereinamaisiais procesais elektros sistemoje. Įtraukiamos skirtingos scenarijų analizės. Pirmasis scenarijus nuo Klaipėdos 330 kV pastotės atjungiant 700 MW vėjo jėgainių parką. Antrasis scenarijus nuo Klaipėdos 330 kV pastotės atjungiant 1400 MW vėjo jėgainių parką. Scenarijų atjungimams taikyti vasaros ir žiemos apkrovimų režimai. Vėjo jėgainių parkų prijungimas pavaizduotas (žr. 35 pav.).



35 pav. Lietuvos 330 kV elektros tinklas, (raudonai pažymėtas planuojama vėjo jėgainių parkas)

5.4. Elektros energetikos sistemos dinaminio stabilumo skaičiavimai

Reikalingų duomenų įvedimui, dinaminiams elektros sistemos proceso skaičiasu lvimams PSS/E programoje, naudojamas „Python“ kodas. Šis kodas leidžia pagreitinti dinaminių procesų skaičiavimus PSS/E programoje, nes nereikia rankiniu būdų, nuolatos įvedinėti dinaminių procesų parametrų. Kai pradedamas skaičiavimo procesas ir dinaminio elektros sistemos elemento parametrai yra įvedami, programa nuskaito paruoštą normalaus režimo bylą (žr. 15 lentelę). Po to ji atlieka pakeitimus skaičiuojama elektros tinkle, priklausomai nuo tiriamojo scenarijaus (žr. 16 ir 17 lenteles). Baigus pakeitimus, modelis įyra paleidžiamas iš naujo. Programai pabaigus skaičiavimus rezultatai yra automatiškai išsaugomi faile kuris vadinamas „.out“. Naudojantis rezultatų failu atliekama analizė, kurioje matomi elektros sistemos pokyčiai, vykstantys pereinamojo proceso metu. Šie rezultatai suteikia informaciją apie elektros sistemos elgesį, įvairius parametrus, srovės ir įtampos pokyčius, taip pat kitus svarbius duomenis, kurie gali padėti suprasti elektros sistemos veikimą ir identifikuoti potencialias problemas.

15 lentelė. Normalaus prieš avarinio režimo skaičiavimo tvarka.

Nr.	Komanda	Komandos aprašymas
1.	psspy_case	Ši komanda naudojama nurodyti PSS/E „sav“ bylos failą, kuriame yra elektros tinklo sistemos duomenys ir modeliavimo konfigūracija skirta galios srautų skaičiavimui.
2.	psspy.fdns	Ši komanda naudojama norint atlikti greit atsietą energijos sistemos apkrovos srauto analize.
3.	psspy.cong	Ši komanda naudojama generatorių valdymo režimams nurodyti. Generatoriaus valdymo režimas nustato, kaip sureguliuojama generatoriaus galia, kad būtų išlaikytas elektros energijos sistemos stabilumas.
4.	psspy.conl	Ši komanda naudojama apkrovų režimams nurodyti. Apkrovos valdymo režimai nustato, kaip apkrovos reaguoja į elektros energijos sistemos sąlygų pokyčius.
5.	psspy.ordr	Ši komanda naudojama norint nurodyti tvarką, kuria modeliavimo metu turi būti apdorojamos maitinimo sistemos magistralės
6.	Psspy.fact	Ši komanda naudojama energijos sistemos matricų pertvarkymui.
7.	psspy.tysl	Ši komanda naudojama pertvarkytų elektros energijos tinklo lygčių sistemą.
8.	psspy.dyre	Ši komanda naudojama elektros energijos sistemos lygtims išspręsti naudojant kartotinį sprendimo metodą.
9.	psspy.bsys:	Ši komanda naudojama bazinei modeliavimo sistemai nurodyti, apimantį sistemos dažnį, įtampą ir kitus parametrus. Bazinė sistema nurodo maitinimo sistemos įtampos, srovės ir galios atskaitos reikšmes ir yra naudojama visiems elektros energijos sistemos duomenims konvertuoti į bendrą vienetų rinkinį.
10.	psspy.chsb	Ši komanda paleidžia dinaminį modeliavimą
11.	psspy.run	Ši komanda paleidžia dinaminį modeliavimą ir pradeda rezultatų apskaičiavimą
12.	dynamics_solution_param2	Ši komanda nurodo dinaminio modeliavimo parametrus.

„Python“ komandos skirtos avariniam sistemos režimui skaičiuoti kuomet vėjo jėgainių parkas atjungiamas dėl fizinės atakos kuomet sabotažas prieš elektros maitinimo kabelius sukelią 330 kV magistralinio kabelio trifazį trumpąjį jungimą pavaizduotos 16 lentelėje.

16 lentelė. Trumpojo jungimo komandos.

Nr.	Komanda	Komandos aprašymas
1.	change_channel_out_file	Komanda naudojama pakeisti kanalo išvesties failą. Kanalo išvesties faile yra modeliavimo rezultatai.
2.	psspy.dist_bus_fault	Komanda naudojama tam tikros magistralės gedimui imituoti paskirstymo sistemoje. Ši komanda naudojama paskirstymo sistemos elgsenai tirti esant gedimo sąlygoms, pvz.: trumpiesiems jungimams įvesties duomenis, nurodytus naudojant kitas PSS/E komandas.
3.	psspy.dist_clear_fault	Komanda, naudojama paskirstymo sistemos gedimui pašalinti ir sistemos normaliam veikimui atkurti
4.	psspy.dist_branch_trip	Komanda, naudojama paskirstymo sistemos atšakos atjungimui imituoti. Ši komanda paprastai naudojama tiriant sistemos reakciją į gedimą ar kitą trikdymą, dėl kurio suveikia sistemos atšaka.
5.	psspy.run	Komanda naudojama modeliavimui pradėti ir rezultatams apskaičiuoti.

„Python“ komandos skirtos avariniam sistemos režimui skaičiuoti kuomet užpuolikai išjungią vėjo jėgainių parką pavaizduotos 17 lentelėje.

17 lentelė. Vėjo jėgainių parko atjungimo scenarijaus komandos.

Nr.	Komanda	Komandos aprašymas
1.	psspy.change_channel_out_file	Komanda naudojama pakeisti kanalo išvesties failą. Kanalo išvesties faile yra modeliavimo rezultatai.
2.	psspy. Run	Komanda naudojama modeliavimui pradėti ir rezultatams apskaičiuoti.
3.	Load_chang_4	Komanda naudojama keičiant magistralės apkrovimą.
4.	psspy.run	Komanda naudojama modeliavimui pradėti ir rezultatams apskaičiuoti.

5.5. Tinklo įtampų ir dažnio tyrimas

Įtampų ir dažnio tyrimas yra svarbus ir vertingas analizuojant vėjo jėgainių kibernetinių atakų poveikį valstybės tinklo stabilumui. Ši analizė padeda ištirti ir įvertinti, kaip kibernetinės atakos gali paveikti valstybės tinklo elektros įtampą ir dažnį. Tyrime naudoti scenarijai pateikti 18 lentelėje. Šioje lentelėje pateikiamos įvairios situacijos, kurios buvo nagrinėjamos ir modeliuojamos tyrimo metu. Pirmieji keturi scenarijai susiję su VJP atsijungimu nuo tinklo žiemos maksimalių ar vasaros minimalių apkrovų režimuose. Tai atspindi situacijas, kai VJP yra išjungtas dėl kibernetinės atakos. Kiti scenarijai yra susiję su VJP magistralės trifazio trumpojo jungimo režimu (toliau t.t.j.), kuomet vėjo jėgainės infrastruktūra yra atakuojama fizine ataka. Šie scenarijai yra suskirstyti į žiemos maksimalių apkrovų režimą ir vasaros minimalių apkrovų režimą, ir skiriasi trumpojo jungimo trukme.

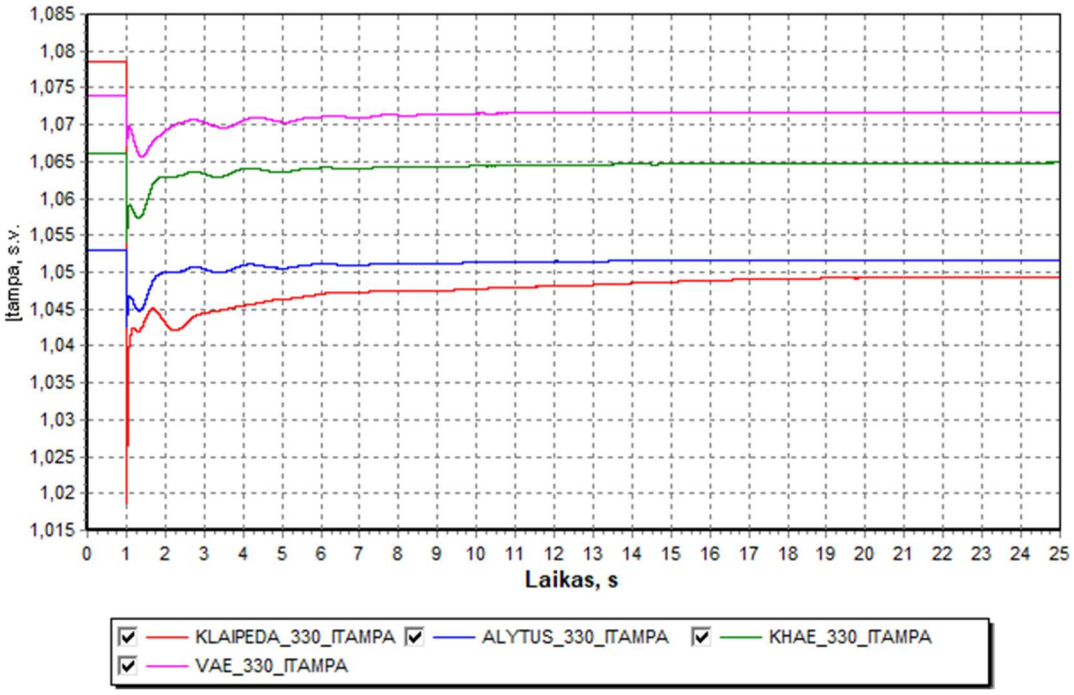
18 lentelė. Tyrime naudoti scenarijai.

Nr.	Tyrime naudoto scenarijaus pavadinimas
1.	700 MW VJP atsijungimas nuo tinklo žiemos maksimalių apkrovų režime.
2.	700 MW VJP atsijungimas nuo tinklo vasaros minimalių apkrovų režime.
3.	1400 MW VJP atsijungimas nuo tinklo žiemos maksimalių apkrovų režime.
4.	1400 MW VJP atsijungimas nuo tinklo vasaros minimalių apkrovų režime.
5.	700 MW VJP magistralės t.t.j., režimas (t = 0,15s) vasaros minimalių apkrovų režime.
6.	700 MW VJP magistralės t.t.j., režimas (t = 0,25s) vasaros minimalių apkrovų režime.
7.	700 MW VJP magistralės t.t.j., režimas (t = 0,15s) žiemos maksimalių apkrovų režime.
8.	700 MW VJP magistralės t.t.j., režimas (t = 0,25s) žiemos maksimalių apkrovų režime.
9.	1400 MW VJP magistralės t.t.j., režimas (t = 0,15s) vasaros minimalių apkrovų režime.
10.	1400 MW VJP magistralės t.t.j., režimas (t = 0,25s) vasaros minimalių apkrovų režime.
11.	1400 MW VJP magistralės t.t.j., režimas (t = 0,15s) žiemos maksimalių apkrovų režime.
12.	1400 MW VJP magistralės t.t.j., režimas (t = 0,25s) žiemos maksimalių apkrovų režime.

Atlikus 700 MW vėjo jėgainių parko (VJP) atsijungimo scenarijus žiemos maksimalių ir vasaros minimalių apkrovų režimuose (žr. 1 ir 2 priedą), nustatyta, kad žiemos maksimalių apkrovų režime dažnis pasiekia mažiausią vertę visuose keturiuose 330 kV tyrinėtuose mazguose praėjus 0,25 s po VJP atsijungimo. Klaipėdos, Alytaus ir KHAE 330 kV mazguose, atsijungus VJP, dažnis nukrenta

nuo 50 Hz iki 49,95 Hz. VAE 330 kV mazge dažnis nukrenta nuo 50 Hz iki 49,96 Hz. Visuose tyrinėtuose mazguose dažnis nusistovi per 24 s, pasiekdamas 49,97 Hz vertę.

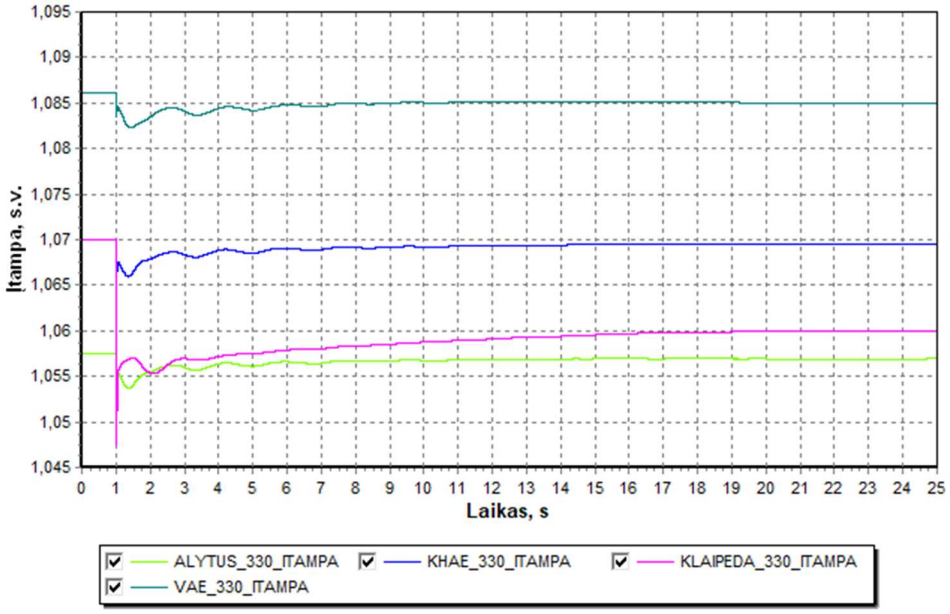
Atsijungus 700 MW VJP žiemos maksimalių apkrovų režime, įtampos vertės tyrinėtuose mazguose iš karto pasiekia mažiausią įtampos kritimo amplitudės vertę. Didžiausias įtampos pokytis pastebimas Klaipėdos 330 kV mazge, kur įtampa sumažėja 0,062 s.v., (žr. 36 pav.). Kituose tyrinėtuose taškuose, t. y. Alytaus, KHAE ir VAE 330 kV mazguose, įtampa sumažėja mažiau, atitinkamai: 0,0105 s.v., 0,011 s.v. ir 0,0095 s.v. Visuose tyrinėtuose mazguose įtampa nusistovi per 5 s. Alytaus, KHAE ir VAE mazguose įtampa sumažėjo 0,002 s.v. nuo pradinių verčių, o Klaipėdos mazge įtampa pakito labiausiai ir nusistovėjo 0,026 s.v. sumažėjusi nuo pradinės vertės.



36 pav. 700 MW VJP atsijungimo įtaka įtampai, žiemos maksimalių apkrovų režime

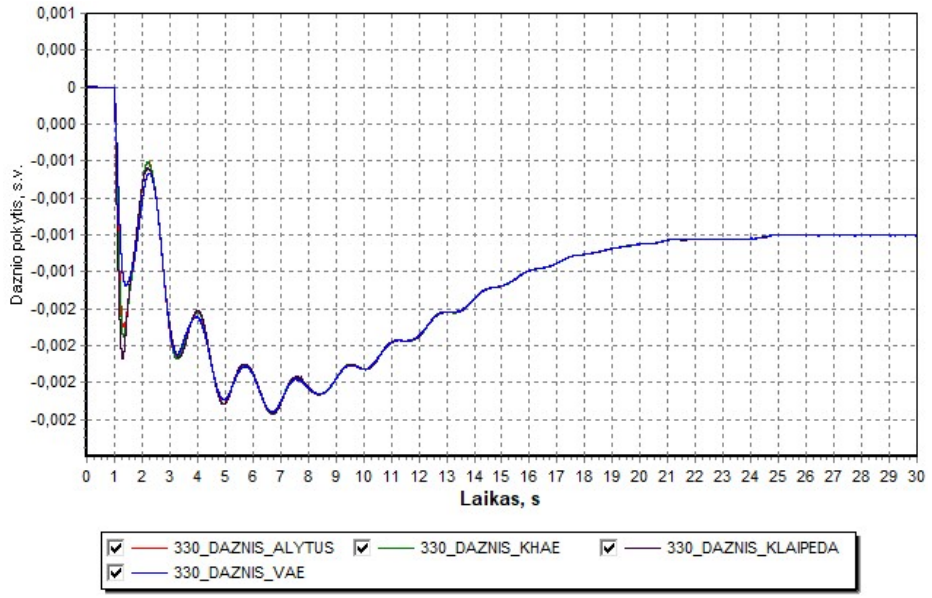
Atlikus 700 MW VJP atsijungimo scenarijų vasaros minimalių apkrovimų režime, nustatyta, kad dažnis pasiekia mažiausią vertę visuose keturiuose 330 kV tyrinėtuose mazguose praėjus 6,7 s po VJP atsijungimo. Visuose tyrinėtuose 330 kV mazguose, atsijungus VJP, dažnis nukrenta nuo 50 Hz iki 49,97 Hz, o per 24 s nusistovi ties 49,98 Hz. Vasaros minimalių apkrovimų režime atsijungus 700 MW VJP, įtampos vertės tyrinėtuose mazguose iš karto pasiekia mažiausią įtampos kritimo amplitudės vertę. Didžiausias įtampos pokytis pastebimas Klaipėdos 330 kV mazge, kur įtampa sumažėja 0,023 s.v., (žr. 37 pav.). Kituose tyrinėtuose taškuose, t. y. Alytaus, KHAE ir VAE 330 kV mazguose, įtampa sumažėja mažiau, atitinkamai: 0,004 s.v., 0,003 s.v. ir 0,004 s.v. Klaipėdos 330 kV mazge įtampa nusistovi per 14 s, sumažėjusi 0,01 s.v. Visuose kituose tyrinėtuose mazguose įtampa nusistovi per 5 s, Alytaus, KHAE ir VAE mazguose įtampa nuo pradinių verčių sumažėjo 0,001 s.v.

Taigi nors ir įtaka dažnio stabilumui abiem skaičiuotais režimai nėra didelė, bet atsijungus 700 MW VJP žiemos maksimalių apkrovų režime, padaroma didesnė įtaka dažnio ir įtampos stabilumui negu vasaros minimalių apkrovų režime. Ištyrus šiuos atvejus galima teigti, kad nei dažnio nei įtampos stabilumas nėra pažeidžiamas.



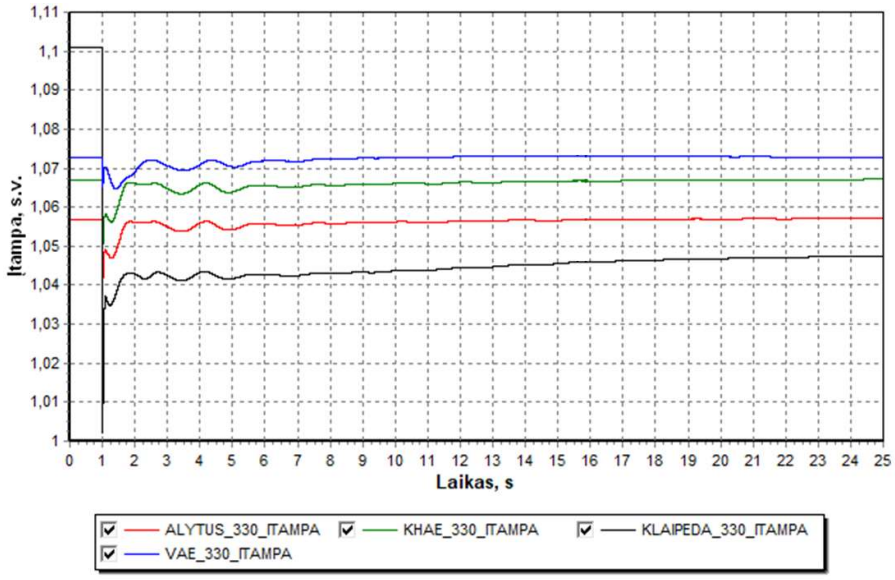
37 pav. 700 MW VJP atsijungimo įtaka įtampai, vasaros minimalių apkrovų režime

Atlikus 1400 MW Vėjo jėgainių parko (VJP) atsijungimo scenarijų žiemos maksimalių ir vasaros minimalių apkrovų režimuose (žr. 3 ir 4 priedą), nustatyta, kad žiemos maksimalių apkrovų režime dažnis Klaipėdos, Alytaus ir KHAE 330 kV mazguose pasiekia mažiausią dažnio kitimo amplitudės vertę po 0,25 s nuo VJP atsijungimo momento. VAE 330 kV mazge mažiausia dažnio kitimo amplitudė pastebima po 6,75 s. Didžiausias dažnio mažėjimas pastebimas Klaipėdos 330 kV mazge, kur dažnis nukrenta nuo 50 Hz iki 49,86 Hz (žr. 38 pav.). Alytaus ir KHAE mazguose dažnis nuo 50 Hz mažėja iki 49,87 Hz. Mažiausias dažnio pokytis pastebimas VAE 330 kV mazge, kur dažnis nukrenta nuo 50 Hz iki 49,90 Hz. Visuose tyrinėtuose mazguose dažnis stabilizuojasi per 20 s, pasiekdamas 49,93 Hz vertę.



38 pav. 1400 MW VJP atsijungimas žiemos maksimalių apkrovų režime

Atsijungus 1400 MW VJP žiemos maksimalių apkrovų režime, įtampos vertės tiriamuose mazguose iš karto pasiekia mažiausią įtampos kritimo amplitudės vertę. Didžiausias įtampos pokytis pastebimas Klaipėdos 330 kV mazge, kur įtampa sumažėja 0,098 s.v., (žr. 39 pav.). Kituose tiriamuose taškuose, t. y. Alytaus, KHAE ir VAE 330 kV mazguose, įtampa sumažėja žymiai mažiau, atitinkamai: 0,0105 s.v., 0,0175 s.v. ir 0,0005 s.v. Klaipėdos 330 kV mazge įtampa nusistovi per 19 s, sumažėjusi 0,0535 s.v. nuo pradinės vertės (žr. 1400 įtampos lentelę). Visuose kituose tyrinėtuose mazguose įtampa nusistovi per 5 s, išliekant toje pačioje vertėje kaip ir prieš VJP atsijungimą.



39 pav. 1400 MW VJP atsijungimas žiemos maksimumo režime.

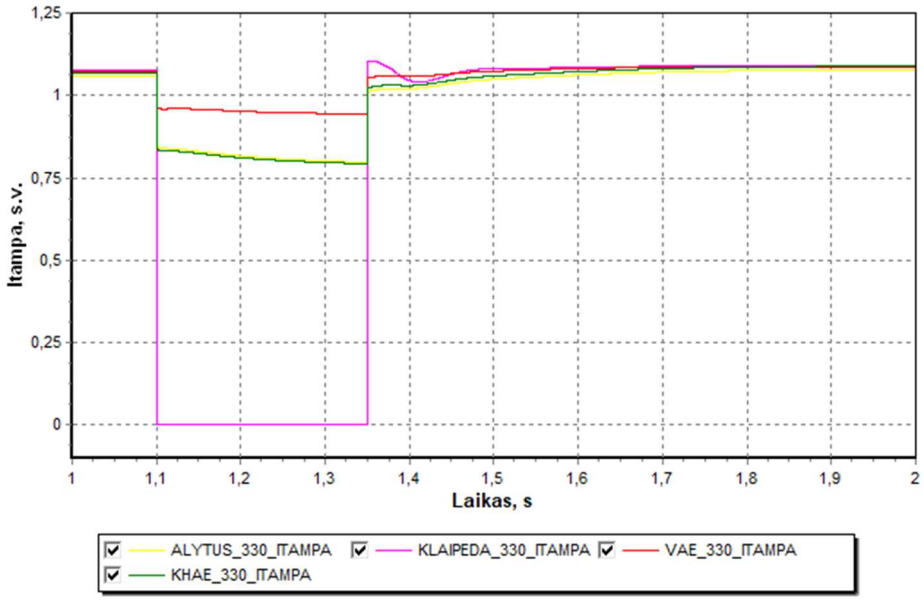
Naudojant vasaros minimalių apkrovų režimus, atlikus 1400 MW VJP atsijungimo scenarijus, nustatyta, kad dažnis pasiekia mažiausią vertę visuose keturiuose 330 kV tyrinėtuose mazguose po 6,75 s nuo VJP atsijungimo momento. Visuose tiriamuose mazguose dažnis mažėja nuo 50 Hz iki 49,92 Hz. Visų mazgų dažnis stabilizuojasi per 19 s, pasiekdamas 49,96 Hz vertę. Atsijungus 1400 MW VJP vasaros minimalių apkrovų režimuose, įtampos vertės tiriamuose mazguose iškart pasiekia mažiausią įtampos kritimo amplitudės vertę. Didžiausias įtampos pokytis pastebimas Klaipėdos 330 kV mazge, kur įtampa sumažėja 0,075 s.v. Kituose tiriamuose taškuose, t. y. Alytaus, KHAE ir VAE 330 kV mazguose, įtampa sumažėja žymiai mažiau, atitinkamai: 0,01 s.v., 0,0125 s.v. ir 0,005 s.v. Klaipėdos 330 kV mazge įtampa nusistovi per 14 s, sumažėjusi 0,04 s.v. nuo pradinės vertės. Visuose kituose tyrinėtuose mazguose įtampa nusistovi per 6 s, išliekant toje pačioje vertėje kaip ir prieš VJP atsijungimą.

Palyginus 700 MW ir 1400 MW VJP atsijungimus skirtingais apkrovų režimais, pastebima, kad nors abiem skaičiuotais scenarijais įtaka dažnio stabilumui nėra didelė, didesnė įtaka tinklo dažniui ir įtampos stabilumui pastebima Klaipėdos 330 kV mazge, kai atsijungia 1400 MW VJP žiemos maksimalių apkrovų režime. Klaipėdos 330 kV mazge įtampa sumažėja 0,098 s.v., kas sudaro 8,9 % įtampos sumažėjimą nuo pradinės įtampos vertės. Žinant, kad leidžiami įtampos nuokrypiai po nenumatytų atvejų 330 kV Europos tinkluose yra 10 %, galima teigti, kad įtampos stabilumas tinkle nėra pažeidžiamas.

Žiemos maksimalių apkrovų režime 700 MW VJP 0,15s trukmės trifazio trumpojo jungimo metu, Klaipėdos 330 kV mazge įtampos mažėjimo amplitudė yra 1,09 s.v. Alytaus ir KHAE 330 kV

mazguose įtampos mažėjimo amplitudės yra 0,025 s.v. Mažiausia įtampos kritimo amplitudė pastebima VAE 330 kV mazge, kur įtampa trifazio trumpojo jungimo metu sumažėja 0,11 s.v. Visuose tiriamuose mazguose šio scenarijaus metu įtampa po trumpojo jungimo nusistovi per 0,1s ir grįžta į pradinę, prieš avarinę, vertę.

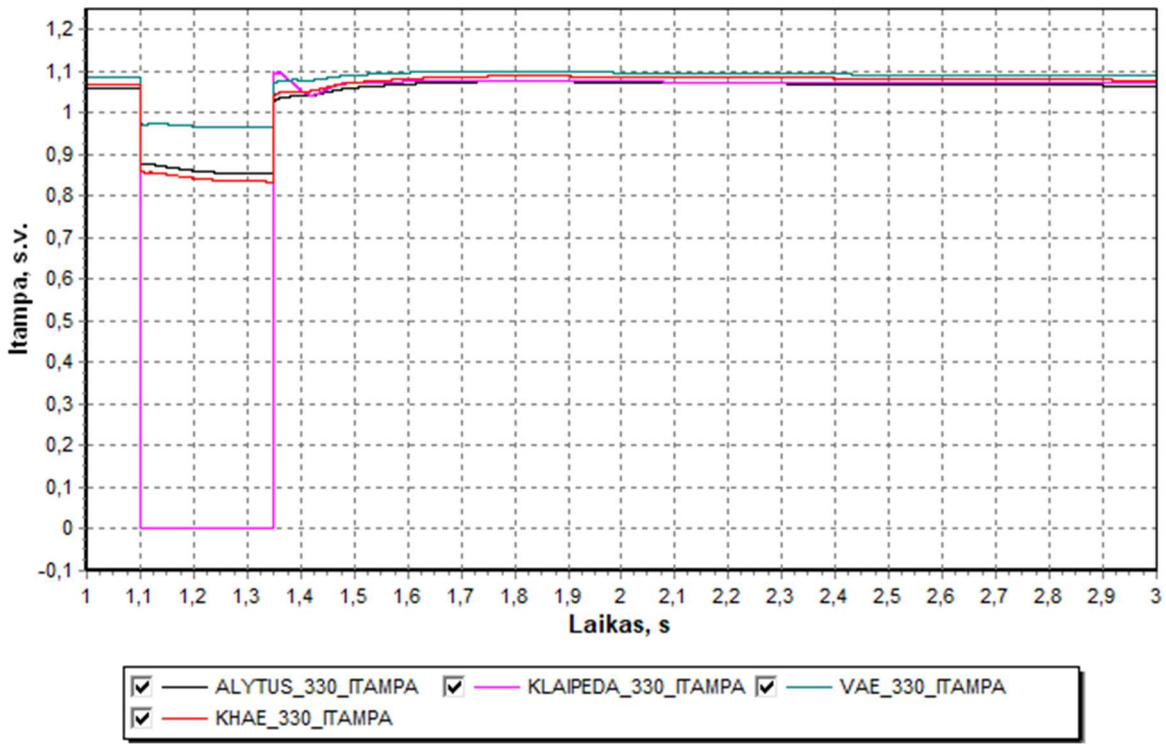
Antru atveju žiemos maksimalių apkrovų režime 700 MW VJP 0,25s trukmės trifazio trumpojo jungimo metu, Klaipėdos 330 kV mazge įtampos mažėjimo amplitudė yra 1,07 s.v. Alytaus ir KHAE 330 kV mazguose įtampos mažėjimo amplitudės yra 0,027 s.v. Mažiausia įtampos kritimo amplitudė pastebima VAE 330 kV mazge, kur įtampa trifazio trumpojo jungimo metu sumažėjo 0,13 s.v. Visuose tiriamuose mazguose šio scenarijaus metu įtampa po trumpojo jungimo nusistovi per 0,1 sekundės ir grįžta į pradinę, prieš avarinę, vertę (žr. 40 pav.).



40 pav. 700 MW VJP 0,25s trukmės trifazis trumpasis jungimas, žiemos maksimalių apkrovų režime

Vasaros minimalių apkrovų režime 700 MW VJP 0,15s trukmės trifazio trumpojo jungimo metu Klaipėdos 330 kV mazge įtampos mažėjimo amplitudė yra 1,06 s.v. Alytaus, KHAE ir VAE 330 kV mazguose įtampos mažėjimo amplitudės atitinkamai yra 0,11 s.v., 0,12 s.v. ir 0,07 s.v. Taigi, mažiausia įtampos kritimo amplitudė pastebima VAE 330 kV mazge. Visuose tiriamuose mazguose šio scenarijaus metu įtampa po trumpojo jungimo nusistovi per 0,15 sekundės ir grįžta į pradinę, prieš avarinę, vertę.

Kitu atveju vasaros minimalių apkrovų režime, skaičiuojant 0,25 s trukmės 700 MW VJP trifazį trumpąjį jungimą, Klaipėdos 330 kV mazge trumpojo jungimo metu įtampos mažėjimo amplitudė yra didžiausia, 1,06 s.v. Alytaus, KHAE ir VAE 330 kV mazguose įtampos mažėjimo amplitudės atitinkamai yra 0,019 s.v., 0,25 s.v. ir 0,1075 s.v. Mažiausia įtampos kritimo amplitudė pastebima VAE 330 kV mazge. Visuose tiriamuose mazguose šio scenarijaus metu įtampa po trumpojo jungimo nusistovi per 0,25 sekundės ir sumažėja iki 1 kV vertės nuo pradinės prieš avarinės mazgų įtampos reikšmės (žr. 41 pav.).

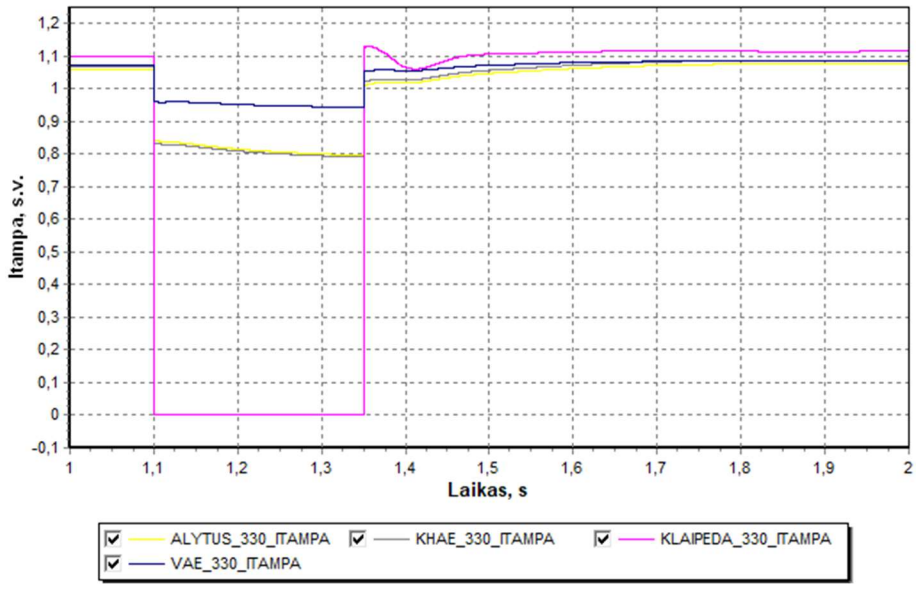


41 pav. 700 MW VJP 0,25s trukmės trifazis trumpasis jungimas, vasaros minimalių apkrovų režime

Palyginus 700 MW trumpųjų jungimų scenarijus (žr. 6 ir 7 priedus), taikant skirtingus apkrovų režimus ir skirtingą trumpųjų jungimų trukmės laiką, didžiausia įtaka 330 kV tiriamiems mazgams pastebima žiemos maksimalių apkrovų režime. Visuose tiriamuose mazguose, visais nagrinėtais scenarijais, trumpojo jungimo metu įtampos sumažėjimas nuo pradinės įtampos vertės buvo didesnis nei 10%. Žinant, kad leidžiamieji įtampos nuokrypiai po nenumatytų atvejų 330 kV Europos tinkluose yra 10%, tai įtampos stabilumas Lietuvos tinkle yra pažeidžiamas.

Žiemos maksimalių apkrovų režime 1400 MW VJP 0,15s trukmės trifazio trumpojo jungimo metu Klaipėdos 330 kV mazge įtampos mažėjimo amplitudė yra 1,1 s.v (žr. 11 priedą). Alytaus ir KHAE 330 kV mazguose įtampos sumažėjimo amplitudės atitinkamai yra 0,27 s.v. ir 0,28 s.v. Mažiausia įtampos kritimo amplitudė yra VAE 330 kV mazge, kur įtampa trifazio trumpojo jungimo metu sumažėja 0,15 s.v. Visuose tirtuose šio scenarijaus mazguose įtampa pasibaigus trumpajam jungimui nusistovi per 0,15 s ir sugrįžta į pradinę prieš avarinę vertę.

Antru atveju, žiemos maksimalių apkrovų režime 1400 MW VJP 0,25 s sekundės trukmės trifazio trumpojo jungimų metu Klaipėdos 330 kV mazge įtampos mažėjimo amplitudė yra 1,1 s.v. Trumpojo jungimo metu Alytaus ir KHAE 330 kV mazguose įtampos sumažėjimo amplitudės yra atitinkamai 0,28 s.v. ir 0,29 s.v. Mažiausia įtampos kritimo amplitudė pastebima VAE 330 kV mazge, kur įtampa trifazio trumpojo jungimo metu sumažėja 0,018 s.v. Visuose tirtuose šio scenarijaus mazguose įtampa pasibaigus trumpajam jungimui nusistovi per 0,25 s ir sugrįžta į pradinę prieš avarinę vertę (žr. 42 pav.).



42 pav. 1400 MW VJP 0,25s trukmės trifazis trumpasis jungimas, žiemos maksimalių apkrovų režime

Vasaros minimalių apkrovų režime 1400 MW VJP 0,15 s sekundės trukmės trifazio trumpojo jungimo metu Klaipėdos 330 kV mazge įtampos mažėjimo amplitudė yra 1,1 s.v. Alytaus ir KHAE 330 kV mazguose įtampos mažėjimo amplitudės yra atitinkamai 0,23 s.v. ir 0,25 s.v. Mažiausia įtampos kritimo amplitudė yra VAE 330 kV mazge, kur įtampa trifazio trumpojo jungimo metu sumažėja 0,11 s.v. Visuose tirtuose šio scenarijaus mazguose įtampa pasibaigus trumpajam jungimui nusistovi per 0,15 s ir sugrįžta į pradinę prieš avarinę vertę.

Antru atveju, vasaros minimalių apkrovų režime 1400 MW VJP 0,25 s sekundės trukmės trifazio trumpojo jungimo metu Klaipėdos 330 kV mazge įtampos mažėjimo amplitudė yra 1,1 s.v. Trumpojo jungimo metu Alytaus ir KHAE 330 kV mazguose įtampos mažėjimo amplitudės yra atitinkamai 0,24 s.v. ir 0,26 s.v. Mažiausia įtampos kritimo amplitudė pastebima VAE 330 kV mazge, kur įtampa trifazio trumpojo jungimo metu sumažėjo 0,012 s.v. Visuose tirtuose šio scenarijaus mazguose įtampa pasibaigus trumpajam jungimui nusistovi per 0,25 s ir sugrįžta į pradinę prieš avarinę vertę.

Atlikus 700 MW ir 1400 MW VJP magistralių trifazio trumpojo jungimo skaičiavimus, pastebėta, kad dažnis žymiai nepakito nei vasaros minimalių apkrovų režimuose, nei žiemos maksimalių apkrovų režimuose. Visuose tiriamuose trifazio trumpojo jungimo scenarijuose Klaipėdos, Alytaus, KHAE ir VAE mazguose dažnis nepasiekė vertės žemesnės už 49,92 Hz. Tai reiškia, kad visi trumpųjų jungimų scenarijai turėjo mažesnę įtaką nei 1400 MW VJP atsijungimas žiemos maksimalių apkrovų režime, kai Klaipėdos 330 kV mazgo dažnis sumažėjo nuo 50 Hz iki 49,86 Hz. Atsižvelgiant į šį faktą, tolimesnių trumpojo jungimo įtakų dažnio stabilumui nagrinėjimas šiame darbe nebuvo įtrauktas, nes jos buvo mažesnės nei minėtas atvejis ir tokie dažnio svyravimai nedaro reikšmingos įtakos tinklo stabilumui. Duomenys apie atvejus, kurie nebuvo nagrinėti, pateikti prieduose (žr. 5, 8, 10, 12 priedus).

5.6. Skyriaus išvados ir apibendrinimai

Tyrimo rezultatai rodo, kad dažnis nei viename Lietuvos mazge nenukrenta žemiau 49,2 Hz, tai reiškia dažnio stabilumas tinkle nėra pažeidžiamas. Didžiausias dažnio pakitimas iš visų skaičiuotų scenarijų buvo skaičiuojant žiemos maksimumo režimo 0,25s trukmės trifazį trumpąjį jungimą 1400

MW vėjo jėgainių magistralėje. Klaipėdos, Alytaus, KHAE 330 kV mazguose, nukrito iki 49,86 Hz. Po 21 sekundės visų tiriamų ataskaitinių mazgų dažnis nusistovėjo ties 49,92 Hz.

Atsijungus vėjo jėgainių 700 MW VJP didžiausias įtampos kritimas pastebimas žiemos maksimalių apkrovų režime Klaipėdos 330 kV mazge, įtampos svyravimai santykiniais vienetais siekia 0,06 vertės t.y. įtampa nukrenta 19,8 kV. po 16 sekundžių, įtampa nusistovi sumažėjusi 9,5 kV nuo pradinės prieš avarinės įtampos vertės. Kituose tiriamuosiuose mazguose įtampa nusistovi per 8-9 s. sumažėjusi 0,0025-0,003 s.v. Atsijungus 1400 MW VJP žiemos maksimalių apkrovų režime Klaipėda 330 kV 0,098 s.v. ir per 0,25s įtampa nusistovi 0,05 s.v.sumažėjusi nuo pradinės įtampos vertės. Taigi nei vienu tirtu vėjo jėgainių staigaus atsijungimo atveju leidžiamos įtampos nuokrypiai 330 kV mazguose neviršija 10% leistinų įtampos nuokrypių.

Tyrimo metu VAE 330 kV mazge trumpųjų jungimų metu įtampa nenukrito žemiau 0,1 s.v. Visais kitais tirtais atvejais visuose mazguose įtampa nukrito daugiau nei 0,1 s.v. Vykstant trumpajam jungimui 1400 MW VJP žiemos maksimumo apkrovų režime buvo pastebėtas didžiausia įtampos mažėjimo amplitudė Alytaus ir KHAE 330 kV mazguose, kur įtampos kritimai siekė nuo 0,3 s.v. iki 0,45 s.v. Praėjus 4,5s po trumpojo jungimo visų mazgų įtampos reikšmės sugrįžo į pradines, stabilias, vertes buvusias prieš trumpąjį jungimą. Taigi trifazių trumpųjų jungimų metu išskyrus VAE 330 kV mazgą visuose tirtuose Lietuvos tinklo mazguose leidžiami įtampos nuokrypiai viršijo 10% leistinus įtampos nuokrypius, tai reiškia įtampos stabilumas Lietuvos elektros tinkle yra pažeidžiamas.

Išvados

1. Atlikus vėjo jėgainių atsparumo kibernetinėms atakoms tyrimų apžvalgą nustatyta, kad kibernetinėms atakomis labiausiai pažeidžiami elementai yra šie: vėjo jėgainių kontrolės sistemos, valdikliai, duomenų perdavimo maršrutizatoriai, ir jutikliai. Dažniausiai jie paveikiami kenkėjiškų programų atakomis arba klaidingų duomenų įvedimo atakomis. Tyrimo metu nustatytos kibernetinių atakų sąlygos ir priežastys, tai neatnaujinta programinė įranga, fizinės prieigos saugos pažeidimai ir darbuotojų kibernetinės saugos mokymų trūkumas.

2. Sudaryta vėjo jėgainių kibernetinio atsparumo vertinimo ir investicijų į kibernetinę saugą įvertinimo metodikos struktūra. Sumodeliavus Bajeso atakos grafiką apskaičiuota bendra abiejų ugniasienių įveikimo tikimybė, kuri lygi 0,10. Atlikus sistemos išnaudojimo įvertinimą, gautas aukščiausias sistemos pažeidžiamumo įvertinimas 3,9. Apskaičiuota vidutinė laiko trukmė, reikalinga pažeidžiamumui išnaudoti, yra 27 dienos, o vidutinis sistemos atstatymo laikas yra 3 dienos.

3. Pagal Gordono-Loebo modelį nusistačius įrenginių sugadinimo tikimybę 0,5 galimi vėjo jėgainės kibernetinės atakos metu patirti nuostoliai yra 1 830 000 EUR. Tyrimo metu nustatyta, kad investicijų nauda didžiausia, kuomet investavus 531 000 EUR į kibernetinio saugumo užtikrinimą, kibernetinės atakos tikimybė sumažėjo nuo 0,5 iki 0,1396. Reikia pabrėžti, kad ši suma neviršija 37% vėjo jėgainės kibernetinės atakos metu patiriamų nuostolių vertės ir gali būti laikoma tikslinga investicija į kibernetinį saugumą.

4. Tyrimo rezultatai rodo, kad visais tirtais atvejais dažnis nei viename Lietuvos mazge nenukrenta žemiau 49,8 Hz ir galima teigti, kad dažnio stabilumas tinkle nėra pažeidžiamas. Visais staigaus vėjo jėgainių parko atsijungimo atvejais leidžiamos įtampos nuokrypiai 330 kV mazguose neviršijo 10% leistinų įtampos nuokrypių, tačiau trifazių trumpųjų jungimų metu visuose tirtuose Lietuvos tinklo mazguose, išskyrus Visagino Atominės Elektrinės 330 kV mazgą, leidžiami įtampos nuokrypiai viršijo 10% leistinus įtampos nuokrypius, todėl galime teigti, kad kibernetinės atakos poveikis elektros perdavimo tinklo dažnio ir įtampos stabilumui yra mažesnis nei trifazio trumpojo jungimo sukeltas poveikis.

Literatūros sąrašas

1. Jay Johnson, Craig G Rieger, Rafer Cooley, Jake Paul Gentle (2023). Hardening Wind Energy Systems from Cyber Threats-Final Project Report. [Žiūrėta 2023-04-10]. Prieiga per interneta: https://www.researchgate.net/publication/368599508_Hardening_Wind_Energy_Systems_from_Cyber_Threats-Final_Project_Report

2. Jay Johnson (2017). Roadmap for Photovoltaic Cyber Security [Žiūrėta 2022-06-05]. Prieiga per internetą: https://www.researchgate.net/publication/322568290_Roadmap_for_Photovoltaic_Cyber_Security

3. Nikolai Kulev, Oliver Eichorn, Eveling Engler, Carl Wrede (2019). Non-resilient behavior of offshore wind farms due to cyber-physical attacks. [Žiūrėta 2022-03-05]. Prieiga per internetą: https://www.researchgate.net/publication/337338720_Non-resilient_behavior_of_offshore_wind_farms_due_to_cyber-physical_attacks

4. Sarah Barber, Luiz Andre Moyses Lim, Yoshiaki Sakagami, Julian Quick, Effi Latiffianti, Yichao Liu, Riccardo Ferrari, Simon Letzgus, Xujie Zhang, Florian Hammer (2022). Enabling Co-Innovation for a Successful Digital Transformation in Wind Energy Using a New Digital Ecosystem and a Fault Detection Case Study. [Žiūrėta 2022-10-01]. Prieiga per internetą: https://www.researchgate.net/publication/362452732_Enabling_Co-Innovation_for_a_Successful_Digital_Transformation_in_Wind_Energy_Using_a_New_Digital_Ecosystem_and_a_Fault_Detection_Case_Study

5. Tala Talaei Khoei, Hadjar Ould Slimane, Naima Kaabouch (2022). A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions. [Žiūrėta 2022-09-15]. Prieiga per internetą: https://www.researchgate.net/publication/362090495_A_Comprehensive_Survey_on_the_Cyber-Security_of_Smart_Grids_Cyber-Attacks_Detection_Countermeasure_Techniques_and_Future_Directions

6. Jay Johnson, Craig G Rieger, Rafer Cooley, Jake Paul Gentle (2023). Cyber Resilience for Wind Installations: A Cyber Resilient Reference Architecture. [Žiūrėta 2023-04-24]. Prieiga per internetą: https://www.researchgate.net/publication/367074443_Cyber_Resilience_for_Wind_Installations_A_Cyber_Resilient_Reference_Architecture

7. Tomas Plėta, Manuela Tvaronavičienė, Silvia Della Casa, Konstantin Agafonov (2020). Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. [Žiūrėta 2022-03-04]. Prieiga per internetą: https://www.researchgate.net/publication/345716538_Cyber-attacks_to_critical_energy_infrastructure_and_management_issues_overview_of_selected_cases

8. Tim Krause, Raphael Ernst, Benedikt Klaer, Immanuel Hacker (2021). Cybersecurity in Power Grids: Challenges and Opportunities. [Žiūrėta 2022-10-17]. Prieiga per internetą: https://www.researchgate.net/publication/351298708_Cybersecurity_in_Power_Grids_Challenges_and_Opportunities

9. Nicolò Boschetti, Nathaniel Gordon, Gregoy Falco (2022). Space Cybersecurity Lessons Learned from The ViaSat Cyberattack. [Žiūrėta 2023-01-17]. Prieiga per internetą: https://www.researchgate.net/publication/363558808_Space_Cybersecurity_Lessons_Learned_from_The_ViaSat_Cyberattack

10. Nikolai Kulev, Frank Sill Torres (2022). Investigation of high-impact low-probability disturbances in offshore wind farms. [Žiūrėta 2023-03-01]. Prieiga per internetą: https://www.researchgate.net/publication/365318668_Investigation_of_high-impact_low-probability_disturbances_in_offshore_wind_farms

11. Zhengxuan Li, Qiang Song, Feng an, Biao Zhao (2021). Review on DC transmission systems for integrating large-scale offshore wind farms. [Žiūrėta 2022-03-01]. Prieiga per internetą: https://www.researchgate.net/publication/349591096_Review_on_DC_transmission_systems_for_integrating_large-scale_offshore_wind_farms

12. Nazha Cherkaoui, Touria Haidi, Belfqih Aziz, Elmariami Faissal (2018). A Comparison Study of Reactive Power Control Strategies in Wind Farms with SVC and STATCOM. [Žiūrėta 2022-07-01]. Prieiga per internetą: https://www.researchgate.net/publication/330653088_A_Comparison_Study_of_Reactive_Power_Control_Strategies_in_Wind_Farms_with_SVC_and_STATCOM

13. Yingli Shu, Quande Yuan, Wende Ke, Lei Kou (2022). Security Access Control Method for Wind-Power-Monitoring System Based on Agile Authentication Mechanism. [Žiūrėta 2022-11-24]. Prieiga per internetą: https://www.researchgate.net/publication/365830255_Security_Access_Control_Method_for_Wind-Power-Monitoring_System_Based_on_Agile_Authentication_Mechanism

14. Jason Staggs, David Ferlemann, Sujeet Shenoi (2017). Wind farm security: attack surface, targets, scenarios and mitigation. [Žiūrėta 2022-05-08]. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S1874548217300434?via%3Dihub

15. Wenhui Zhang, Yizheng Jiao, Dazhong Wu, Srivatsa Srinivasa, Asmit De, Swaroop Ghosh, Peng Liu (2020). Armor PLC: A Platform for Cyber Security Threats Assessments for PLCs. [Žiūrėta 2022-03-02]. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S2351978920304017

16. Nikolai Kulev, Frank Sill Torres (2022). Simulation of the impact of parameter manipulations due to cyber-attacks and severe electrical faults on Offshore Wind Farms.[Žiūrėta 2023-01-05]. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S0029801822012720

17. Amir Rostami, Mohammad Mohammadi, Hadis Karimipour (2023). Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities. [Žiūrėta 2023-05-05]. Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S0142061522008882?fbclid=IwAR3EdSynBi3ofosHOrttw2QJyZ2NQlKBA-z7zH5lvuqHhb8jYuG6HX5vw9I&via%3Dihub

18. Megan J. Culler, Sean Morash, Brian Smith, Frances Clevland, Jake Gentle (2021). A Cyber-Resilience Risk Management Architecture for Distributed Wind. [Žiūrėta 2022-10-01]. Prieiga per internetą: https://ieeexplore.ieee.org/document/9611786

19. K Givaki, D Chen, O. Anaya-Lara (2016). Stability studies of different AC collection network topologies in wind farms connected to weak grids. [Žiūrėta 2022-09-07]. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/8123827

20. William Nzoukou, Lingyu Wang, Sushil Jajodia, Anoop Singhal (2013). A Unified Framework for Measuring a Network's Mean Time-to-Compromise. [Žiūrėta 2022-09-07]. Prieiga per internetą: https://ieeexplore.ieee.org/document/6656277

21. Sirui Tang, Zhaoxi Liu, Lingfend Wang (2020). Power System Reliability Analysis Considering External and Insider Attacks on the SCADA System. [Žiūrėta 2022-06-05]. Prieiga per internetą: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9299922

22. Yichi Zhang, Yingmeng Xiang, Lingfeng Wang (2017). Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems. [Žiūrėta 2022-06-05]. Prieiga per internetą: https://ieeexplore.ieee.org/document/7406763

23. Andres Felipe Obando-Montano, Camilo Carrillo, Jose Cidras, Eloy Diaz-Dorado (2014). A STATCOM with Supercapacitors for Low-Voltage Ride-Through in Fixed-Speed Wind Turbines .[Žiūrėta 2022-08-15]. Prieiga per internetą: https://www.mdpi.com/1996-1073/7/9/5922

24. Honghao Wu, Junyong Liu, Jichun Liu, Mingjian Cui, Xuan Liu, Hongjun Gao (2019). Power Grid Reliability Evaluation Considering Wind Farm Cyber Security and Ramping Events. [Žiūrėta 2022-10-05]. Prieiga per internetą: https://www.mdpi.com/2076-3417/9/15/3003

25. Khairy Sayed, Ahmed G. Abo-Khalil, and Ali M. Eltamaly (2021). Wind Power Plants Control Systems Based on SCADA System. [Žiūrėta 2022-10-09]. Prieiga per internetą: https://faculty.ksu.edu.sa/sites/default/files/wind_power_plants_control_systems_based_on_scada_system.pdf

26. Ihor Furson, Klym Yamkovyi, Oleksandr Shmatko (2022). Mart grid and wind generators: an overview of cyber threats and vulnerabilities of power supply networks. [Žiūrėta 2023-02-05]. Prieiga per internetą: http://195.88.72.95:57772/csp/nauchportal/Arhiv/REKS/2022/REKS422/4Fursov.pdf

27. Lawrence A. Gordon, Martin P. Loeb, Lei Zhou Robert H. Smith School of Business, University of Maryland, College Park (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. [Žiūrėta 2022-02-02]. Prieiga per internetą: https://www.scirp.org/journal/paperinformation.aspx?paperid=64892

28. Thi Quynh Mai Pham, Sungwoo Im, Joonmo Choung (2021). Prospects and Economics of Offshore Wind Turbine Systems. [Žiūrėta 2022-02-02]. Prieiga per internetą: https://www.joet.org/upload/pdf/KSOE-2021-061.pdf

29. Europos Elektros tinklo operatorių asociacijos (ENTSO-E) įsakymas (2009). P1 – Policy 1: Load-Frequency Control and Performance [C] [Žiūrėta 2023-05-08]. Prieiga per internetą: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/entsoe/Operation_Handbook/Policy_1_final.pdf

30. Gabrielle Desarnaud (2017). Cyber attacks and energy infrastructures. [Žiūrėta 2022-11-09]. Prieiga per internetą: https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf

31. U.S. Departamento of Energy (2022). CyOTE case study: crashoverride/industroyer. [Žiūrėta 2023-11-07]. Prieiga per internetą: https://cyote.inl.gov/cyote/wp-content/uploads/2022/11/CRASHOVERRIDE-CyOTE-Case-Study_508_FINAL.pdf

32. U.S. Department of Energy, Office energy efficiency & renewable energy (2020). Roadmap for Wind Cybersecurity. [Žiūrėta 2022-06-05]. Prieiga per internetą: https://www.energy.gov/sites/prod/files/2020/07/f76/wind-energy-cybersecurity-roadmap-2020v2.pdf

33. U.S. Office of Energy Efficiency & Renewable Energy, Wind Energy Technologies Office (2023). WETO-Funded Research Focuses on Reducing Cybersecurity Threats to Nation's Wind Fleet . [Žiūrėta 2023-03-05]. Prieiga per internetą: https://www.energy.gov/eere/wind/articles/weto-funded-research-focuses-reducing-cybersecurity-threats-nations-wind-fleet

34. Wind Europe (2021). A cybersecurity framework fit for wind energy. [Žiūrėta 2022-09-05]. Prieiga per internetą: https://windeurope.org/wp-content/uploads/files/policy/position-papers/20220103-WindEurope-position-paper-cybersecurity-framework-fit-for-wind-energy.pdf

35. Electricity Coordinating Center Ltd (2021). Technical Assistance for the Connection Network Codes Implementation in the Energy Community [Žiūrėta 2023-05-07]. Prieiga per interneta: https://www.energy-community.org/dam/jcr:29ecd404-8c39-4568-862b-b81d0fef5054/ECC_CNC_GE_062021.pdf

36. Tyler Stehly and Patrick Duffy National Renewable Energy Laboratory (2022). 2021 Cost of Wind Energy Review. [Žiūrėta 2022-12-05]. Prieiga per internetą: https://www.nrel.gov/docs/fy23osti/84774.pdf

37. Cyber security policy of Siemens Gamesa Renewable Energy S.A (2021). [Žiūrėta 2022-02-05]. Prieiga per internetą: https://www.siemensgamesa.com/en-int/-/media/siemensgamesa/downloads/en/investors-and-shareholders/corporate-governance/corporate-policies/20210916-cybersecurity-policy-def.pdf?la=en-bz&hash=CD6C4F287B326E5632A4755804F3D6F6567B52E0

38. North American electric reliability corporation (2019). Cyber Security –Incident Reporting and Response Planning. [Žiūrėta 2022-07-05]. Prieiga per internetą: https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/Implementation_Guidance_for_CIP-008-6_Final_Ballot_01152019.pdf

39. Wolf K., Freudenberg, DNV (2019). Why windfarms need to step up cyber security. [Žiūrėta 2022-06-27]. Prieiga per internetą: https://www.dnv.com/cybersecurity/cyber-insights/why-windfarms-need-to-step-up-cyber-security.html

40. Ellie Biddulph, Greensolver (2019). The growing threat of cyber security in the renewable energy sector. [Žiūrėta 2022-06-24]. Prieiga per internetą: https://greensolver.net/the-growing-threat-of-cyber-security-in-the-renewable-energy-sector/

41. America's cyber defence agency (2022). Siemens VxWorks-based Industrial Products (Update C). [Žiūrėta 2022-11-27]. Prieiga per internetą: https://www.cisa.gov/news-events/ics-advisories/icsa-21-194-12

42. The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) (2022). APT Cyber Tools Targeting ICS/SCADA Devices [Žiūrėta 2022-11-05]. Prieiga per internetą: https://www.cisa.gov/sites/default/files/publications/AA22-103A_APT_Cyber_Tools_Targeting_ICS_SCADA_Devices.pdf

43. America's cyber defence agency (2022). Siemens SIMATIC WinCC (Update E). [Žiūrėta 2022-10-11]. Prieiga per internetą: https://www.cisa.gov/news-events/ics-advisories/icsa-21-315-03

44. Lietuvos Respublikos elektros energetikos sistemos sujungimo su kontinentinės Europos elektros tinklais darbui sinchroniniu režimu įstatymo Nr. XI-2052 papildymo 13-1 straipsniu įstatymas. [Žiūrėta 2023-03-05]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/20643bc2badd11ea9a12d0dada3ca61b

45. Kasperspky (2022). H1 2022 – a brief overview of the main incidents in industrial cybersecurity. [Žiūrėta 2023-02-05\3]. Prieiga per internetą: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-H1-2022-A-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-En.pdf

46. Kasperspky Lab (2022). Damage control: the cost of security breaches IT security risks special report series. [Žiūrėta 2023-03-02]. Prieiga per internetą: https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

47. SIEMENS. [Žiūrėta 2023-05-01]. Prieiga per internetą: https://www.siemens.com/global/en.html

48. Nexans (2020). Integrated cable solutions for offshore wind development. [Žiūrėta 2023-04-05]. Prieiga per internetą: https://www.nexans.com/en/dam/jcr:717293e8-cb52-4dba-81f3-fd5370159a7b/Nexans%20Offshore%20Wind%20Farm%20WEB.pdf

49. (Paveikslėlis) By Barry Manz for Mouser Electronics. Wind Turbines: Tiny Sensors Play Big Role. [Žiūrėta 2022-05-05]. Prieiga per internetą: https://eu.mouser.com/applications/tiny-Sensors-Role-in-Wind-Turbines/

50. National Institute of Standards and Technology. [Žiūrėta 2023-03-28]. Prieiga per internetą: https://nvd.nist.gov/

51. Common Vulnerabilities and Exposures (CVE) Program. [Žiūrėta 2022-03-17]. Prieiga per internetą: https://www.cve.org/ResourcesSupport/FAQs

52. Common Vulnerability Scoring System version 3.1 Specification Document. [Žiūrėta 2023-04-25]. Prieiga per internetą: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

53. Common Vulnerability Scoring System Calculator. [Žiūrėta 2023-05-05]. Prieiga per internetą: https://nvd.nist.gov/vuln-metrics/cvss

54. Lietuvos vėjo elektrinių asociacija (LVEA) [Žiūrėta 2023-03-05]. Prieiga per internetą: https://lvea.lt/statistika/lietuvos-statistika/

55. Nacionalinis kibernetinio saugumo centras – NKSC, Kibernetinės gynybos departamento kritinės informacinės infrastruktūros saugumo skyrius, Viktoras Pinkevičius. Ką daryti įvykus kibernetiniam incidentui?. [Žiūrėta 2023-02-16]. Prieiga per internetą:

https://www.vrk.lt/documents/10180/718344/NKSC+-+K%C4%85%20daryti+%C4%AFvykus+kibernetiniam+incidentui.pdf/8f0b466b-df02-4627-b126-d96636707976

56. Litgrid (2023). Išankstinės prisijungimo sąlygos vėjo elektrinių jūrinėje teritorijoje prijungimui prie elektros perdavimo tinklo. [Žiūrėta 2023-03-03]. Prieiga per internetą: https://offshorewind.lt/wp-content/uploads/2023/02/IPS_JUP-prie-Darbenu_TP.pdf

57. Litgrid (2023). Informaciją apie Lietuvos jūrinį vėjo parką. [Žiūrėta 2023-05-04]. Prieiga per internetą: https://offshorewind.lt/lt/sample-page/

58. ESO – Energijos skirstymo operatorius. Elektros kainos sudedamosios dalys. [Žiūrėta 2023-04-08]. Prieiga per internetą: https://www.eso.lt/lt/verslui/elektra_99/tarifai-kainos-atsiskaitymai-ir-skolos/kas-sudaro-elektros-kaina_1876.html

59. Lietuvos Respublikos energetikos ministerija. Vėjo parko Baltijos jūroje projektas. [Žiūrėta 2023-04-08]. Prieiga per internetą: https://enmin.lrv.lt/lt/veiklos-sritys-3/elektra/vejo-parko-baltijos-juroje-projektas?fbclid=IwAR2dV8PoF7vuK2g5doztbNHBAuw2BDVwzZvBHJZLqD2IlWCr4wlaIn904MA

60. Lietuvos Respublikos energetikos ministerija (2022). Sektoriaus veikla. [Žiūrėta 2023-02-01]. Prieiga per internetą: https://enmin.lrv.lt/lt/veiklos-sritys-3/elektra/sektoriaus-veikla-3

61. Lietuvos Respublikos nacionalinis energetikos ir klimato srities veiksmų planas 2021-2030. [Žiūrėta 2023-02-05]. Prieiga per internetą: https://am.lrv.lt/uploads/am/documents/files/KLIMATO%20KAITA/Integruotas%20planas/Final%20NECP.pdf

62. Lietuvos Respublikos vyriausybė (2021). Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo. [Žiūrėta 2023-01-26]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

63. Lietuvos respublikos energetikos ministro įsakymas (2012 m. birželio 18 d.). Nr 1-116 „Dėl elektros tinklų naudojimo taisyklių patvirtinimo. [Žiūrėta 2022-06-05]. Prieiga per internetą: https://e-seimas.lrs.lt/rs/legalact/TAD/TAIS.428001/

64. (Raspberry Pi įrenginio nuotrauka). Prieiga per internetą: https://www.windpowermonthly.com/article/1753020/researcher-access-wind-turbine-using-20-gadget-safe-technology

65. BBC News by Gordon Corera Security correspondent (2022). Ukraine war: The Russian ships accused of North Sea sabotage. [Žiūrėta 2023-05-01]. Prieiga per internetą: https://www.bbc.com/news/world-europe-65309687

66. Bloomberg by Naureen S Malik(2023). Attacks on US Power Grids Rose to All-Time High in 2022. [Žiūrėta 2023-04-07]. Prieiga per internetą: https://www.bloomberg.com/news/articles/2023-02-01/attacks-on-us-power-grids-rise-to-all-time-high-in-2022#xj4y7vzkg

67. Valiutų kursai. Nasdaq. [Žiūrėta 2023-05-03]. Prieiga per internetą: https://www.nasdaq.com/market-activity/currencies/eurusd

68. Knyga: Ažubalis, V. (1989). Statinis ir dinaminis elektros sistemų stabilumas: mokymo priemonė. Kaunas: Spausdino KPI

PRIEDAI

1 Priedas - 700 MW VJP atsijungimo scenarijų dažnio kitimo rezultatai 330 kV mazguose

Scenarijus	700 MW VJP žiemos maks.				700 MW VJP vasaros min.			
330kV mazgas	Klaipėdos	Alytus	KHAE	VAE	Klaipėdos	Alytus	KHAE	VAE
Dažnio mažėjimo amplitudė s.v.	-0,00095 (0,25s)	-0,00085 (0,25s)	-0,0009 (0,25s)	-0,00079 (0,25s)	-0,00067 (6,7s)	-0,00067 (6,7s)	-0,00066 (6,7s)	-0,00065 (6,7s)
Nusistovėjęs dažnis s.v.	-0,00062				-0,00041			
Nusistovėjimo laikas, s	24s				24s			

2 Priedas – 700 MW VJP atsijungimo scenarijų įtampos kitimo rezultatai 330 kV mazguose

Scenarijus	700 MW VJP žiemos maks.				700 MW VJP vasaros min.			
330kV mazgas	Klaipėdos	Alytaus	KHAE	VAE	Klaipėdos	Alytus	KHAE	VAE
330kV Pradinė įtampa s.v.	1,075	1,053	1,066	1,074	1,07	1,056	1,055	1,086
Įtampos kitimo amplitudė s.v.	-0,062	-0,0105	-0,011	-0,0095	-0,023	0,004	0,003	0,004
Nusistovėjusi įtampa s.v.	1,049	1,052	1,065	1,072	1,06	1,055	1,065	1,085
Nusistovėjimo laikas, s	5s	5s	5s	5s	14s	5s	5s	5s

3 Priedas - 1400 MW VJP atsijungimo scenarijų įtampos kitimo rezultatai 330 kV mazguose

Scenarijus	1400 MW VJP atsijungimas žiemos maks.				1400 MW VJP atsijungimas vasaros min.			
330kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
330kV Pradinė įtampa s.v.	1,101	1,0574	1,0675	1,0725	1,0975	1,0575	1,07	1,0825
Įtampos kitimo amplitudė s.v.	-0,098	-0,015	0,0175	0,005	-0,075	-0,01	0,0125	0,005
Nusistovėjusi įtampa s.v.	1,0475	1,0574	1,065	1,0725	1,0575	1,055	1,068	1,085
Nusistovėjimo laikas, s	19s	5s	5s	5s	14s	6s	6s	6s

4 Priedas – 1400 MW VJP atsijungimo scenarijų dažnio kitimo rezultatai 330 kV mazguose

Scenarijus	1400 MW VJP atsijungimas žiemos maks.				1400 MW VJP atsijungimas vasaros min.			
330kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Dažnio mažėjimo amplitudė s.v.	-0,0027 (0,25s)	-0,0025 (0,25s)	-0,0025 (0,25s)	-0,0019 (6,75s)	-0,00145 (6,75s)	0,0013 (6,75s)	-0,00137 (6,75s)	-0,0010 (6,75s)
Nusistovėjęs dažnis s.v.	-0,00145	-0,00145	-0,00145	-0,00145	-0,0008	-0,0008	-0,0008	-0,0008
Dažnio nusistovėjimo laikas, s	20s	20s	20s	20s	19s	19s	19s	19s

5 Priedas - 700 MW VJP t.t.j., žiemos maksimalių apkrovų dažnio kitimo rezultatai

Scenarijus	700 MW VJP, t.t.j. = 0,15 žiemos maks.				700 MW VJP, t.t.j. = 0,25 žiemos maks.			
330 kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Dažnio mažėjimo amplitudė s.v.	-0,00095 (0,15s)	-0,00032 (0,9s)	-0,00032 (0,9s)	-0,00024 (0,9s)	-0,00088 (0,15s)	-0,00074 (1,1s)	-0,00074 (1,1s)	-0,00048 (1,1s)
Dažnio didėjimo amplitudė s.v.	0,0004 (0,3s)	0,00024 (1,4s)	0,00024 (1,4s)	0,00015 (1,4s)	0,00075 (0,3s)	0,00045 (1,7s)	0,00045 (1,7s)	0,00031 (1,75s)
Laikas per kuri dažnis nusistovi pradinėje vertėje	5s	5s	5s	5s	7s	7s	7s	7s

6 Priedas - 700 MW VJP t.t.j., žiemos maksimalių apkrovų įtampos kitimo rezultatai

Scenarijus	700 MW VJP, t.t.j. = 0,15 žiemos maks.				700 MW VJP, t.t.j. = 0,25 žiemos maks.			
330 kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Pradinė įtampa s.v.	1,07	1,06	1,07	1,08	1,07	1,06	1,07	1,08
Įtampos mažėjimo amplitudė s.v. t.t.j. metu	-1,07	-0,25	-0,025	-0,11	-1,07	-0,27	-0,27	-0,13
Laikas per kuri įtampa nusistovėjo pradinėje vertėje	0,25s	0,25s	0,25s	0,25s	0,35s	0,35s	0,35s	0,35s

7 Priedas - 700 MW VJP t.t.j., vasaros minimalių apkrovų įtampos kitimo rezultatai

Scenarijus	700 MW VJP, t.t.j. = 0,15 vasaros min.				700 MW VJP, t.t.j. = 0,25 vasaros min.			
330kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Pradinė įtampa s.v.	1,06	1,06	1,075	1,09	1,06	1,06	1,075	1,09
Įtampos mažėjimo amplitudė s.v. t.t.j. metu	1,05	0,11	0,12	0,07	1,06	0,19	0,25	0,1075
Nusistovėjusi įtampa s.v.	1,05	1,05	1,05	1,06	1,0575	1,055	1,068	1,085
Laikas per kuri įtampa nusistovėjo	0,3s	0,3s	0,3s	0,3s	0,5s	0,5s	0,5s	0,5s

8 Priedas - 700 MW VJP t.t.j., vasaros minimalių apkrovų dažnio kitimo rezultatai

Scenarijus	700 MW VJP, t.t.j. = 0,15 vasaros min.				700 MW VJP, t.t.j. = 0,25 vasaros min.			
330kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Žemiausia dažnio vertė	-0,00059 (0,2s)	-0,00027 (0,9)	-0,00027 (0,9)	-0,0002 (0,9)	-0,00059 (1s)	-0,00048 (1s)	-0,00048 (1s)	-0,00048 (1s)
Didžiausia dažnio vertė	0,00026 (0,33s)	0,00017 (1,4)	0,00017 (1,4)	0,00011 (1,4)	0,00035 (1,5s)	0,00026 (1,5s)	0,00026 (1,5s)	0,00035 (1,5s)
Laikas per kuri dažnis nusistovi pradinėje vertėje	8s	8s	8s	8s	8s	8s	8s	8s

9 Priedas – 1400 MW VJP t.t.j., vasaros minimalių apkrovų įtampos kitimo rezultatai

Scenarijus	1400 MW VJP, t.t.j. = 0,15 vasaros min.				1400 MW VJP, t.t.j. = 0,25 vasaros min.			
330kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Pradinė įtampa s.v.	1,1	1,07	1,09	1,08	1,1	1,07	1,09	1,08
Įtampos mažėjimo amplitudė s.v. t.t.j. metu	-1,1	-0,23	-0,25	-0,11	-1,1	-0,24	0,26	0,12
Laikas per kuri įtampa nusistovėjo pradinėje vertėje	0,3s	0,3s	0,3s	0,3s	0,5s	0,5s	0,5s	0,5s

10 Priedas - 1400 MW VJP t.t.j., vasaros minimalių apkrovų dažnio kitimo rezultatai

Scenarijai	1400 MW VJP, t.t.j. = 0,15 vasaros min.				1400 MW VJP, t.t.j. = 0,25 vasaros min.			
330kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Mažiausia dažnio vertė s.v.	-0,0009 (0,25s)	-0,0007 (0,25)	-0,0007 (0,25)	-0,0005 (0,25)	-0,00125 (0,4s)	-0,0008 (0,4s)	-0,0008 (0,4s)	-0,0008 (0,4s)
Didžiausia dažnio vertė s.v.	0,00025 (0,5s)	0,00012 5 (1,25)	0,00012 5 (1,25)	0,00007 (1,25)	0,00037 (0,7s)	0,00025 (1,4s)	0,00025 (1,4s)	0,0002 (1,4s)
Laikas per kuri dažnis nusistovi pradinėje vertėje	13s	13s	13s	13s	13s	13s	13s	13s

11 Priedas - 1400 MW VJP t.t.j., žiemos maksimalių apkrovų įtampos kitimo rezultatai

Scenarijai	1400 MW VJP, t.t.j. = 0,15 žiemos min.				1400 MW VJP, t.t.j. = 0,25 žiemos min.			
330kV mazgas	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
330kV Pradinė įtampa s.v.	1,1	1,07	1,08	1,08	1,1	1,07	1,08	1,08
Įtampos mažėjimo amplitudė s.v. t.j. metu	-1,1	-0,23	-0,25	-0,11	-1,1	-0,27	0,28	0,12
Laikas per kuri įtampa nusistovėjo pradinėje vertėje	0,3s	0,3s	0,3s	0,3s	0,5s	0,5s	0,5s	0,5s

12 Priedas – 1400 MW VJP t.t.j., žiemos maksimalių apkrovų dažnio kitimo rezultatai

	1400 MW VJP, t.t.j. = 0,15 žiemos maks.				1400 MW VJP, t.t.j. = 0,25 žiemos maks.			
330kV Mazgai	Klaipėda	Alytus	KHAE	VAE	Klaipėda	Alytus	KHAE	VAE
Mažiausia dažnio vertė s.v.	-0,00118 (0,25s)	-0,00075 (0,3)	-0,00075 (0,3)	-0,00075 (0,3)	-0,00144 (0,4s)	-0,0009 (0,4s)	-0,0009 (0,4s)	-0,0008 (0,4s)
Didžiausias vertės padidėjimas s.v.	0,00037 5 (0,6s)	0,00025 (1,4)	0,00025 (1,4)	0,0002 (1,45)	0,00025 (1,5s)	0,00025 (1,5s)	0,00025 (1,5s)	0,0002 (1,5s)
Laikas per kuri dažnis nusistovi pradinėje vertėje	7s	7s	7s	7s	7s	7s	7s	7s