**MYKOLO ROMERIO UNIVERSITETAS**
**VIEŠOJO SAUGUMO AKADEMIJA**

**DEIMANTĖ TRAŠKEVIČIŪTĖ**

TEISĖS IR POLICIJOS VEIKLOS: SPECIALIZACIJOS IKITIEISMINIO PROCESO PROGRAMA

# KIBERNETINIO SAUGUMO TEISINIS REGLAMENTAVIMAS IR PRAKTINĖS PROBLEMOS

Magistro baigiamasis darbas

**Darbo vadovė:**

**dr. Erika Matulionytė – Jarašūnė**

Kaunas, 2022

**TURINYS**

## SANTRUMPŲ SĄRAŠAS

ANK – Lietuvos Respublikos administracinių nusižengimų kodeksas

BK – Lietuvos Respublikos baudžiamasis kodeksas

BUSP – 2019 m. gegužės 17 d. Tarybos sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais

CERT (angl. *Computer emergency response team*) arba CSIRT (angl. *Computer Security Incident Response Team*) – reagavimo į kompiuterius incidentus komanda

CRRT (angl. *Cyber Rapid Response Teams*) – Europos Sąjungos Kibernetinės greitojo reagavimo komandos

EC3 (angl. *The European Cybercrime Centre*) – Europos kovos su elektroniniu nusikalstamumu centras

ENISA (angl. *European network and information security agency*) – Europos tinklų ir informacijos apsaugos agentūra

ES – Europos Sąjunga

IRT – informacinės ir ryšių technologijos

JAV – Jungtinės Amerikos Valstijos

NATO (angl. North Atlantic Threat Organization) – Šiaurės Atlanto sutarties organizacija

NKSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministeri

# ĮVADAS

**Baigiamojo darbo aktualumas:** šiuolaikinis pasaulis tapo neatsiejamas nuo informacinių ir ryšių technologijų, kurių raida neabejotinai tobulėja. Šios technologijos veikia beveik visose šiuometinės visuomenės srityse, o jų sistemos saugo tam tikrus duomenis, informaciją. Teisė į duomenų apsaugą reglamentuota Visuotinėje žmogaus teisių deklaracijoje, todėl turi būti užtikrintas informacijų ir ryšių technologijų produktų, paslaugų ir procesų saugumas. Informacinių ir ryšių technologijų įrenginiai ir komponentai yra vienas nuo kito priklausomi, o vieno veikimo sutrikimas gali turėti įtakos kitam įrenginiui ar komponentui. Be to, gerai išvystytų informacinių ir ryšių technologijų paplitimas visuomenėje, lėmė, kad kompiuteriai tapo ne tik teisėtos veiklos, tačiau ir vykdomų kibernetinėje erdvėje nusikalstamų veikų įrankiais bei klasikinių nusikaltimų pagalbine priemone[1]. 2020 m. Lietuvos Respublikoje registruota 4 330 kibernetinių incidentų ir tai yra 25 % daugiau nei 2019 m. Prognozuojama, jog kibernetinių incidentų skaičius bei jų vykdoma žala, vis didės[2]. Saugumas kibernetinėje erdvėje tampa vienas svarbiausių aspektų ne tik asmenims ar įmonėms, bet ir nacionaliniam saugumui. Kadangi kibernetinių atakų panaudojimas gali būti ir prieš valstybę, siekiant sutrikdyti jos svarbias informacinių ir ryšių sistemas, infrastruktūras. Kibernetinė erdvė sukuria skaitmeninį pasaulį bei sudaro naujas galimybes, įvykdyti nusikalstamas veikas, sąlygas atsirasti naujiems nusikalstamų veikų būdams. Akivaizdu, jog kibernetiniai incidentai tampa vis didesnė ir pavojingesnė problema.

**Baigiamojo darbo mokslinis naujumas:** darbe ne mažas dėmesys skiriamas Europos Sąjungos ir Lietuvos teisės aktams, užtikrinantiems informacinių ir ryšių technologijų saugumą. Temos naujumą lemia tai, jog kibernetinių atakų skaičius nemažės, jos taps pažangesnės ir sunkiau aptinkamos. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos pateiktoje 2020 m. ataskaitoje analizuotas nusikalstamų veikų kibernetinėje erdvėje mastas, poveikis bei tendencijos. Ataskaita atskleidė, jog Lietuvoje veikiantys asmenys dažnu atveju veikia ne pavieniui, o gerai organizuotose grupėse, kurių identifikavimas bei pačios nusikalstamos veikos ištyrimas yra sudėtingas ir komplikuotas dėl nusikalstamai veikai panaudotų informacinių ir ryšių technologijų gausos, dėl teisinių sunkumų bei dėl ikiteisminiam tyrimui svarbių duomenų gavimu iš trečiųjų šalių. Taigi, vyraujančios nusikalstamos veikos kibernetinėje erdvėje kelia problematiką informacinių ir ryšių technologijų vartotojams bei valstybei. Siekiant užkirsti kelią sparčiai modernėjančioms

[1] Nikolaj Goranin ir Dalius Mažeika „Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos“ (UAB TEV, 2011) 7.
[2] „2020 m. Nacionalinio kibernetinio saugumo ataskaita“ *Lietuvos Respublikos krašto apsaugos ministerija* (Vilnius, 2021 m. balandžio 7 d.)

nusikalstamoms veikoms kibernetinėje erdvėje, ieškoma efektyvių sprendimų ir priemonių jų užkardymui. Kadangi 2020 m. elektroninių sukčių Lietuvoje gyventojams padaryta žala perkopė 4,5 mln. eurų, visuomenėje vis plačiau kalbama apie saugumą kibernetinėje erdvėje, tačiau visgi ši tema Lietuvoje nėra plačiai nagrinėjama. Šios temos naujumą lemia ir tai, jog informacinių ir ryšių technologijų vartotojai iš dalies patys yra atsakingi už savo naudojamų informacinių ir ryšių technologijų saugumą, todėl turi turėti bazinių kibernetinio saugumo žinių, nuosekliai gilinti šias žinias, didinant kibernetinių grėsmių atsparumą ir mažinant kylančią riziką.

Lietuvoje kibernetinio saugumo temą daugiausia nagrinėja nacionalinės institucijos, autorius plačiau nagrinėjantis kibernetinio saugumo temą – Darius Štitilis, kuris analizavo kibernetinio saugumo teisinį reguliavimą susijusį su Europos Sąjungos kibernetinio saugumo strategija, vertino Lietuvos kibernetinio saugumo programą, nagrinėjo teisinius elektroninių nusikaltimų aspektus bei tokių nusikaltimų teisinį reglamentavimą Europos Sąjungoje, užsienio valstybėse ir Lietuvoje[3]. Nusikalstamas veikas elektroninėje erdvėje nagrinėja ir Renata Marcinauskaitė. Mindaugas Kiškis analizavo interneto teisę siaurąją ir plačiąja prasme, teisinius intelektinės nuosavybės elektroninėje erdvėje aspektus bei teisinius nano-, biotechnologijų ir robotikos gaires. Tadas Limba nagrinėjo elektroninių įrodymų sampratą, jų svarbą teismo procesui. Darius Štitilis, Paulius Pakutinskas, Uldis Kinis ir Inga Malinauskaitė analizavo kibernetinio saugumo strategijas, jų pobūdį, svarbą, privalomumą bei kibernetinio saugumo užtikrinimo principus, jų skirtumus atskirose valstybėse. Užsienio autoriai plačiau analizuoja kibernetinį saugumą. Kibernetinio saugumo sampratą analizavo Darko Galinec, Darko Mažnik ir Boris Guberina[4], elektroninio nusikaltimo sampratą Sarah Gordon ir Richard Ford[5]. Dimitra Markopoulou, Vagelis Papakonstantinou ir Paul de Hert, analizavo būtent 2016 m. liepos 6 d. Europos Parlamento ir Tarybos Direktyvą (ES) 2016/1148 [6], Alexandre de Streel ir Hocepied, Christian analizavo 2018 m. gruodžio 11 d. priimtą Europos Parlamento ir Tarybos direktyvą (ES) Nr. 2018/1972, kuria nustatytas Europos elektroninių ryšių kodeksas [7], Annegret

[3] Darius Štitilis „Elektroniniai nusikaltimai“ (Mykolo Romerio universitetas, 2011) https://repository.mruni.eu/bitstream/handle/007/16884/9789955193296.pdf?sequence=1&isAllowed=y

[4] Darko Galinec, Darko Mažnik ir Boris Guberina *"*Cybersecurity and cyber defence: national level strategic approach*"* 2017 https://www-tandfonline-com.skaitykla.mruni.eu/doi/pdf/10.1080/00051144.2017.1407022?needAccess=true

[5] Sarah Gordon, Richard Ford „On the definition and classification of cybercrime“ http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.302.2178&rep=rep1&type=pdf

[6] Dimitra Markopoulou, Vagelis Papakonstantinou ir Paul de Hert „*Computer Law & Security Review, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*“ (2019) https://reader.elsevier.com/reader/sd/pii/S0267364919300512?token=2FCDD8A5D808316F4E93B494FCCC3591F0C822356B57CC5D8655712DB31481BC00AA50A23F14C63B9CBF5A4AABB781FD&originRegion=eu-west-1&originCreation=20220202192714

[7] Alexandre de Streel ir Hocepied, Christian, „*The EU Regulation of electronic communications networks and services*“ (P.L. Parcu and E. Brogi (eds), Research handbook on EU media law and policy, E. Elgar, forthcoming, 2021), 1. https://ssrn.com/abstract=3897368

Bendiek ir Eva Pander Maat, nagrinėjo Europos Sąjungos teisinį reglamentavimą kibernetinio saugumo aspektu, Europos Sąjungos skaitmenizavimo kylančias problemas bei privalumus [8], Maxime Puys, Jean-Pierre Krimm ir Raphael Collado analizavo 2019 m. balandžio 17 d. priimtą Europos Parlamento ir Tarybos reglamentą (ES) 2019/881. Visgi darbe daugiausia remiamasi nacionalinių ir tarptautinių institucijų, tokių kaip NATO, ENISA, CERT, teikiama informacija, aktualiais straipsniais, ataskaitomis.

**Tiriama problema:** Europos Sąjungos ir Lietuvos Respublikos kibernetinio saugumo teisinės sistemos ypatumai.

**Tyrimo objektas:** kibernetinis saugumas.

**Tyrimo tikslas:** atskleisti kibernetinio saugumo teisinio reguliavimo ypatumus bei kylančias problemas.

**Tyrimo uždaviniai:**

1. Išnagrinėti kibernetinio saugumo bei nusikalstamų veikų kibernetinėje erdvėje sampratas;
2. Atskleisti kibernetinį saugumą užtikrinančias institucijas;
3. Išanalizuoti Europos Sąjungos ir Lietuvos Respublikos kibernetinio saugumo teisinį reglamentavimą;
4. Atskleisti Lietuvos Respublikos teismų praktikoje nusikalstamų veikų kibernetinėje erdvėje problemas bei nusikalstamų veikų kibernetinėje erdvėje formalių straipsnio nuostatų visumos vertinimą teisminio proceso metu.

**Tyrimo metodai:** Baigiamajame darbe panaudoti *kokybiniai duomenų rinkimo* ir *analizės* metodai.

- *Kokybinis duomenų analizės/aprašomasis metodas* – naujai vertinta informacija moksliniuose straipsniuose, monografijose. Taikant šį metodą taip pat buvo atlikta teisės aktų, reglamentuojančių kibernetinį saugumą, analizė.
- *Dokumentų analizės metodas.* Šio metodo pagalba analizuojami Lietuvos Respublikos ir Europos Sąjungos mokslininkų straipsniai, teisės aktai, Lietuvos Respublikos teismų praktika.
- *Lingvistinis metodas* buvo taikomas baigiamojo darbo temai aktualių sąvokų ir teiginių išaiškinimui.
- *Lyginamosios analizės metodas.* Taikant šį metodą buvo lyginami Lietuvos Respublikos kibernetinio saugumo teisinės sistemos ypatumai pagal Europos Sąjungos keliamus reikalavimus.

[8] Annegret Bendiek ir Eva Pander Maat „The EU‘s Regulatory Approach to Cyber-security“ *German institute for International and Security Affairs* (2019), 12. https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf

**Baigiamojo darbo struktūra.** Magistro baigiamąjį darbą sudaro įvadas, kuriame pateikiamas tyrimo aktualumas, iškeliamas tyrimo tikslas ir suformuojami uždaviniai. Darbas susideda iš keturių pagrindinių dalių. Pirmame skyriuje aptariami kibernetinio saugumo teoriniai aspektai. Antrame skyriuje analizuojamas Europos Sąjungos kibernetinio saugumo teisinis reglamentavimas, o trečiame skyriuje Lietuvos Respublikos kibernetinio saugumo teisinis reglamentavimas. Ketvirtasis skyrius yra tiriamoji dalis, kuriame analizuojama nusikalstamų veikų kibernetinėje erdvėje problematika bei kvalifikavimo ypatumai. Darbe yra pateikiamos išvados ir pasiūlymai, literatūros sąrašas, santrauka ir priedai.

**Ginamasis teiginys.** Lietuvos Respublikoje yra pakankama kibernetinį saugumą reglamentuojanti teisinė bazė.

# 1. KIBERNETINIO SAUGUMO TEORINIAI ASPEKTAI

Psichologas Abrahamas Haroldas Maslou 1943 m. savo straipsnyje "Žmogaus motyvacijos teorija" yra pateikęs žmogaus poreikių piramidę. Kaip nurodo pats Abrahamas Haroldas Maslou, pagrindinis motyvacijos teorijos atspirties taškas yra fiziologiniai žmogaus poreikiai. Tik tada, kai žmogaus fiziologiniai poreikiai yra pakankamai patenkinti, atsiranda naujas poreikių rinkinys – saugumo poreikiai[9]. Nors Abrahamas Haroldas Maslou aptaria bazinį fizinį ir emocinį saugumą, šiais laikais labai svarbus ir saugumas kibernetinėje erdvėje, kurį taip pat galima būtų įvardinti kaip vieną iš sudedamųjų saugumo poreikių dalių. Jei iki šiol valstybės, įmonės, piliečiai nesijautė priklausomi nuo informacinių sistemų, ketvirtosios pramonės revoliucijos pokyčiai leido visiems suprasti, kad be informacinių technologijų šiuolaikinis pasaulis yra neįmanomas. Jeigu informacinės sistemos neveikia sklandžiai ir iškyla įvairių problemų, gali kilti įvairaus pobūdžio pasekmių, kurie reikalauja naujo požiūrio į šių sistemų saugumą. Kibernetinis saugumas yra įvardijamas ne tik kaip saugus naudojimasis kompiuteriu ir saugus naršymas internete. Šiuolaikinis pasaulis yra neįsivaizduojamas be interneto, kai ryšių tinklų ir informacinės sistemos yra įdiegtos į esmines bei būtinąsias paslaugas: energetika, transportas, sveikata, finansai. Visos šios išvardintos paslaugos tampa labiau skaitmenizuotos, todėl iškyla pareiga apsaugoti valstybę ir piliečius nuo įvairių kibernetinių grėsmių ir pavojų, sumažinti riziką ypatingos svarbos infrastruktūroms. Todėl siekiant apsisaugoti nuo galimų grėsmių kibernetinėje erdvėje, užtikrinti būtinųjų paslaugų nenutrūkstamą tiekimą, kurti aukštą apsaugos lygį yra būtina įtraukti veiksmingą techninę sistemą, politiką, diplomatinius įrankius, ir žinoma teisinius įrankius, kurie apsaugotų nuo įvairių pavojų.

## 1.1. Kibernetinio saugumo samprata

Pasaulyje atsiradus pirmiesiems modernesniems kompiuteriams ir pastebėjus jų netobulumams, pradėjo formuotis kibernetinio saugumo samprata. Jau 1976 m. Nacionalinis standartų biuras (angl. k. – National Bureau of Standart) dokumente "Operacinių sistemų struktūros palaikyti saugumą ir programinės įrangos patikimumą" nurodoma, kad: "Saugumas tapo svarbiu iššūkiu, kuriant kompiuterines sistemas."[10] Tame pačiame šaltinyje yra pateikiamos vienos pirmųjų pagrindinių sąvokų apibrėžtys - "Sistemos saugumas yra kompiuterinės sistemos (techninės ir programinės įrangos) būsena, kuri sudaro pagrįstą saugumo užtikrinimą. Sistemos saugumas užtikrina

[9] A. H. Maslow „A Theory of Human Motivation", Psychological Review, 50, 370-396, (1943)
Prieiga internetu: [http://psychclassics.yorku.ca/Maslow/motivation.htm]
[10] U.S. Department of commerce, National Bureau of standards, Washington. Theodore A. Linden „Operating System Structures To Support Security and Reliable Software". 1976 m. 1 psl.

tinkamas priemones fizinei kompiuterio apsaugai, eksploatacijai ir sistemos priežiūrai, taip pat sistemos vartotojų identifikaciją ir autentifikaciją."[11] Remiantis šia sąvoka, sistemos saugumas yra suprantamas kaip techniniai prietaisai, t. y. kompiuteriai ir juose naudojamos programos. Taigi, atsiradus pirmiesiems kompiuteriams bei programinėms sistemoms, tuo pačiu atsirado ir poreikis sukurti saugią aplinką kompiuterių naudotojams. Kaip matyti, saugi aplinka yra susijusi su privačių duomenų saugumu.

Teisė į duomenų apsaugą pirmą kartą buvo reglamentuota Jungtinių Tautų Generalinės Asamblėjos 1948 m. priimtoje "Visuotinėje žmogaus teisių deklaracijoje" 12 straipsnyje, kuriame įtvirtinta teisė į privatumą, šeimos gyvenimą, buitį ar susirašinėjimą. Taip pat, numatyta, kad kiekvienas asmuo turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi. Taigi, jau XX a. 5-ajame dešimtmetyje, buvo nustatyta teisė į asmens privatumą bei pareiga kitiems subjektams, įskaitant ir valstybes, nesikišti į asmenų privatų gyvenimą[12]. Europos Taryba „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje", kurioje abstraktūs žmogaus teisės principai paversti į konkrečius teisinius įsipareigojimus, 8 straipsnyje, įtvirtino teisę į asmens duomenų apsaugą, asmeninio ir jo šeimos gyvenimo gerbimą, susirašinėjimo slaptumą[13].

Vystantis naujoms technologijoms bei didėjant poreikiui plačiau įtvirtinti asmens duomenų apsaugą, Europos Taryba pasirašė konvenciją „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)". Ši konvencija yra pagrindinis teisės aktas nustatantis duomenų apsaugą ir kuris galioja iki šių dienų. Konvencijoje yra nustatytos pagrindinės sąvokos, taikymo sritis numatyta tiek privačiam, tiek valstybiniam sektoriui. Joje pažymimi principai, kurie pirmiausia yra susiję su sąžiningumu ir teisėtumu gaunant, t. y. renkant tam tikrus duomenis ir automatizuotai juos tvarkant, siekiant konkrečių teisėtų tikslų ir nenaudojant kitiems prieštaraujantiems tikslams ar duomenų laikymui ilgesnį laikotarpį, nei tai yra būtina. Konvencijoje uždraustas ypatingų duomenų automatizuotas tvarkymas bei numatytas laisvas asmens duomenų srautas tarp valstybių bei nustatomi tokių srautų ribojimai[14].

---

[11] U.S. Department of commerce, National Bureau of standards, Washington. Theodore A. Linden „Operating System Structures To Support Security and Reliable Software". 1976 m. 4 psl.

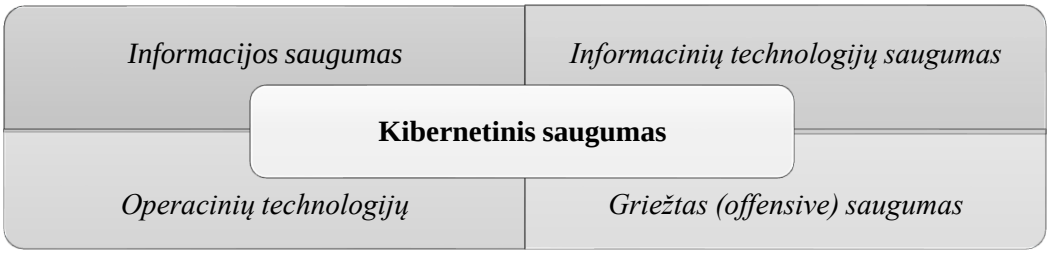
[12] JT Generalinės asamblėja „Visuotinė žmogaus teisių deklaracija" 1948 m. Gruodžio 10 d. Prieiga internetu: < https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385>

[13] Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija 1950 m. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841

[14] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis. 1981 m. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872

Galima pastebėti, kad Europos Sąjungoje išaugo tarpvalstybinis asmens duomenų judėjimas, rinkimo ir keitimosi mastas, be to fiziniai asmenys internetinėje erdvėje ėmė viešinti asmeninę informaciją, todėl siekiant užtikrinti aukštą asmens duomenų apsaugos lygį, suderinti apsaugos sistemą 2016 m. priimtas Europos Parlamento ir Tarybos reglamentas (ES) (2016/679) „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“. Reglamente įtvirtintas asmens duomenų tvarkymo saugumas, įkuriamas priežiūros institutas, kuris stebi ir užtikrina šio reglamento įgyvendinimą, įsteigiamas duomenų apsaugos pareigūnas[15]. Taigi, jei nebūtų įtvirtinta teisė į duomenų apsaugą ir šių duomenų teisėtą bei kokybišką rinkimą, apdorojimą bei saugojimą, nekiltų ir poreikis analizuoti kibernetinio saugumo institutą. Šie du objektai (duomenų apsauga ir kibernetinis saugumas) yra vienas nuo kito priklausantys bei vienas kitą papildantys elementai. Kibernetinis saugumas prarastų prasmę jei nebūtų tvarkomi asmens duomenys kompiuterizuotai.

Kroatai D. Galinec, D. Mažnik ir B. Guberina (2017) savo straipsnyje „Kibernetinis saugumas ir gynyba: strateginis požiūris nacionaliniu lygmeniu“ pateikia kibernetinio saugumo apibrėžimą. Kibernetinis saugumas yra informacijos saugumo, operacinių bei informacinių technologijų saugumo valdymas, tvarkymas, plėtra bei įrankių ir metodų panaudojimas, tam kad būtų laikomasi teisės aktų ir užtikrintas turto saugumas[16]. Anot minėtų autorių, kibernetinis saugumas yra rinkinys, kurį sudaro informacijos saugumas, informacinių ir operacinių technologijų saugumas ir griežtas saugumas *(offensive security – aktyvus būdas apsaugoti sistemas, tinklus ir asmenis nuo atakų. Griežto saugumo priemonės yra nukreiptos į nusikaltėlių paiešką bei kai kuriais atvejais jų kompiuterinių operacijų išjungimą ar bent sutrikdymą)*[17]. Pirmame paveikslėlyje yra pateikiami visi šie kibernetinio saugumo elementai (žr.1 pav.).




1 pav. Kibernetinio saugumo elementai (D. Galinec, D. Mažnik ir B. Guberina, 2017)

[15] Europos Parlamento ir Tarybos reglamentas (ES) (2016/679) „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“. 2016 m. Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679.

[16] Darko Galinec, Darko Mažnik, Boris Guberina “Cybersecurity and cyber defence: national level strategic approach” 2017 m. Prieiga internetu: https://www-tandfonline-com.skaitykla.mruni.eu/doi/pdf/10.1080/00051144.2017.1407022?needAccess=true

[17] *Ibid*

Kibernetinis saugumas naudoja elementų (informacijos saugumo, informacinių ir operacinių technologijų) priemones ir metodus, siekiant sumažinti pažeidžiamumą, išlaikyti sistemos vientisumą, leisti prieigą tik patvirtintiems vartotojams bei ginti turtą.[18] Taigi, remiantis minėtais autoriais, kibernetinis saugumas susideda iš elementų, kurių priemonės ir metodai yra skirtos užtikrinti būtent teisės aktų laikymąsi bei iš jų išplaukiančių vertybių apsaugą (turto, duomenų, apsaugą nuo nusikalstamo kėsinimosi ir pan.).

Jungtinių Amerikos Valstijų vyriausybės, Kibernetinio saugumo ir infrastruktūros saugumo agentūros *(angl. k. CISA-The Cybersecurity and Infrastructure Security Agency)* oficialioje svetainėje kibernetinis saugumas apibūdinamas kaip *„menas apsaugoti tinklus, įrenginius ir duomenis nuo neteisėtos prieigos ar nusikalstamo kėsinimosi bei užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą*.“[19] CISA įtvirtina pagrindinius kibernetinio saugumo tikslus, kurie yra orientuoti į apsaugą nuo kenkėjiškų programų, kurios gali ištrinti visą kompiuterio sistemą, o taip pat nuo užpuolikų, kurie gali įsilaužti į sistemą ir pakeisti failus ar naudojantis užgrobtu kompiuteriniu užpulti kitus vartotojus. Taip pat reikia pažymėti, kad svarbu apsaugoti kreditinių kortelių informaciją, nes esama daugybė kitų pavojų, kurie yra vienas už kitą rimtesni.[20]

Kibernetinio saugumo samprata yra randama ir Jungtinių Amerikos Valstijų privačios įmonės *„TechTarget“* svetainėje. Ši įmonė teikia duomenų rinkodaros paslaugas verslo modeliams ir technologijų pardavėjams[21]. Jų paskelbtame straipsnyje kibernetinis saugumas apibrėžiamas kaip *„prie interneto prijungtų sistemų, tokių kaip techninė įranga, programinė įranga ir duomenys, apsauga nuo kibernetinių grėsmių. <...> naudojama asmenims ir įmonėms apsisaugoti nuo neteisėtos prieigos prie duomenų centrų ir kitų kompiuterizuotų sistemų“*[22]. Techninė įranga yra laikomos visos fizinės kompiuterio dalys: procesorius, atmintis, kietasis diskas, klaviatūra, mikroschemų rinkinys ir t.t.[23] Programinė įranga yra intelektualus produktas, kuri sudaro informacijos apdorojimo sistemos

[18] Darko Galinec, Darko Mažnik ir Boris Guberina *“*Cybersecurity and cyber defence: national level strategic approach*”* 2017, 3. https://www-tandfonline-com.skaitykla.mruni.eu/doi/pdf/10.1080/00051144.2017.1407022?needAccess=true
[19] „Security Tip (ST04-001) What is Cybersecurity?“ *The Cybersecurity and Infrastructure Security Agency* 2009 m. gegužės 6 d. https://us-cert.cisa.gov/ncas/tips/ST04-001
[20] *Ibid*
[21] „About us“ *TechTarget*. https://www.techtarget.com/about-us/
[22] Sharon Shea, Alexander S. Gillis, Casey Clark “Cybersecurity” *TechTarget.* 2021 m. rugpjūtis. https://searchsecurity.techtarget.com/definition/cybersecurity
[23] „Informacinių technologijų žodynas“ *ISO*. https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en

programų, taisyklių, procedūrų visumą arba tos visumos dalį kartu su atitinkama dokumentacija.[24] Pateiktas apibrėžimas turi panašumų su ankščiau minėtu apibrėžimu, kuris buvo paminėtas 1976 m. Nacionalinio Standartų Biuro. Galima teigti, kad kibernetinis saugumas suprantamas kaip priemonė, kuri padeda pasiekti didesnį kompiuterinių sistemų saugumo lygį, kuris yra skirtas tiek fiziniams asmenims, tiek privačioms įmonėms ir net valstybėms apsisaugoti nuo grėsmių kylančių kibernetinėje erdvėje.

2011 m. Darius Štilis, Paulius Pakutinskas, Marius Laurinaitis bei Inga Dauparaitė Mykolo Romerio universiteto kolektyvinėje mokslo monografijoje „Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo teisinio reguliavimo aspektai“ pateikė informacinio saugumo sąvoką – „*tai informacijos ir sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio poveikio, galinčio padaryti žalos informacijos ar sistemos infrastruktūros savininkams ir vartotojams*[25]*“*. Generolo Jono Žemaičio Lietuvos karo akademijos metodinėje medžiagoje teigiama, kad kibernetinis saugumas yra informacinio saugumo dalis, kuri yra susijusi su informacinių technologijų naudojimu. Audronė Petrauskaitė, Rolanda Kazlauskaitė Markelienė, Rasa Gedminienė pateikia kibernetinio saugumo išaiškinimą – „*tai apsauga nuo netinkamo interneto infrastruktūros naudojimo, piktnaudžiavimo ar tiesiog žlugdymo*[26].

Taip pat 2013 m. Europos Sąjungos kibernetinio saugumo strategijoje, kuria siekiama padidinti atsparumą kibernetinėms grėsmėms ir užtikrinti, kad piliečiai ir įmonės gautų naudos iš patikimų skaitmeninių technologijų[27], o *kibernetinis saugumas apibrėžiamas kaip priemonės ir veiksmai, naudojami turint tikslą apsaugoti kibernetinę platformą, apimant civilinę ir karinę sritis, nuo grėsmių, kurios gali padaryti žalos elektroninių ryšių tinklams ar informacinėms infrastruktūroms*[28].

Šiaurės Atlanto Sutarties Organizacija (NATO) 2016 m. išleido „Kibernetinio saugumo nuorodų programą“ (angl. k. *The Cybersecurity Reference Curriculum)* skirtą jos narėms vystyti

---

[24] „Kas yra kompiuterinė įranga“ *Micron Technology, Inc*. https://www.crucial.com/articles/pc-builders/what-is-computer-hardware

[25] Darius Štilis ir kt. „*Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo teisinio reguliavimo aspektai*“. (Mykolo Romerio universitetas, 2011) 206. https://repository.mruni.eu/handle/007/16821

[26] Audronė Petrauskaitė, Rolanda Kazlauskaitė, Markelienė Rasa Gedminienė „*Šalies saugumas ir gynyba*“ (Generolo Jono Žemaičio Lietuvos karo akademija, 2016) 16.

[27] „Kibernetinio saugumo strategija“ *Europos komisija*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[28] Bendras komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir regionų komitetui Europos Sąjungos kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“, 2013. https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A52013JC0001

karinio kibernetinio saugumo mokymo programas. Šiame dokumente pateikiami keli apibrėžimai. Kibernetinio saugumo sąvoka plačiąja prasme apima šias sritis:

- *kibernetines strategijas;*
- *politikos saugumo ir operacijų standartus virtualioje erdvėje;*
- *apima visas grėsmių, pažeidžiamumo mažinimo strategijas;*
- *tarptautinių institucijų dalyvavimus,*
- *reagavimą į incidentus,*
- *atsparumo ir atkūrimo politiką bei veiklas, įskaitant kompiuterių tinklo operacijas;*
- *informacijos užtikrinimą, įstatymų vykdymą, diplomatiją;*
- *karines ir žvalgybos misijas, kurios neretai susijusios su Europos saugumo ir saugumo stabilumu informacijos ir ryšių infrastruktūroje*[29].

Galima pastebėti, kad kibernetiniu saugumu siekiama efektyviais būdais, nustatytais tarptautiniais standartais, tarpvalstybiniu bendradarbiavimu, greitu reagavimu į kompiuterinius išpuolius, kibernetinės gynybos atsparumo užtikrinimu apsisaugoti nuo kibernetinių incidentų. Taigi, kibernetinis saugumas - *veikla ar procesas, kai informacinės ir ryšių sistemos yra apsaugotos bei ginamos nuo neleistino informacijos naudojimo, pakeitimo ar sugadinimo.*[30] D. Shoemakeris ir A. Conklinas (2013) kibernetinį saugumą sieja su procesu, kuris glaudus su kylančių kibernetinių grėsmių identifikavimu bei sąnaudomis pagrįstų kontrapriemonių taikymu, kūrimu bei palaikymu. [31]

2019 m. balandžio 17 d., priimtame Europos Parlamento ir Tarybos reglamente (ES) 2019/881, kuriuo užtikrinamas vidaus rinkos veikimas ir siekiama kelti kibernetinio saugumo bei atsparumo lygį Sąjungoje, 2 straipsnyje nustatytas kibernetinio saugumo terminas. *„Kibernetinis saugumas – visa veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių".*[32] Remiantis šiuo apibrėžimu, išskiriamas pagrindinis kibernetinio saugumo tikslas - apsauga nuo kibernetinių grėsmių, tačiau nėra išskiriamos priemonės

[29] Šiaurės Atlanto Sutarties Organizacija (NATO) „*The Cybersecurity Reference Curriculum"* (2016), 63. 1610-cybersecurity-curriculum.pdf (nato.int)
[30] *Ibid*
[31] Darius Štitilis "Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos". (2013), 2. https://repository.mruni.eu/bitstream/handle/007/10657/489-843-2-PB.pdf?sequence=1&isAllowed=y>
[32] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 Dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas), 2 str. 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019R0881&from=LTrepository.mruni.eu/bitstream/handle/007/10657/489-843-2-PB.pdf?sequence=1&isAllowed=y>

šiam tikslui pasiekti. Pagal priimtą Reglamentą, šiai apsaugai priklauso absoliučiai visa veikla, kuri galėtų būti naudinga siekiant įvardinto tikslo.

Lietuvos Respublikos kibernetinio saugumo įstatymo 2 straipsnio 10 punkte, taip pat yra apibrėžta kibernetinio saugumo sąvoka -*"visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą"*[33].

Galima pastebėti, kad kibernetinis saugumas apibrėžiamas skirtingai įvairių valstybių kibernetinio saugumo strategijose. Analizuojant 2 paveikslėlyje sudarytą lentelę matoma, kad skirtingų valstybių kibernetinio saugumo strategijose apibrėžiama sąvoka yra skirtinga. Kanados atveju, aiškinant kibernetinio saugumo sampratą, įtraukiamas kibernetinės atakos išaiškinimas. O Prancūzija tvirtina, kad kibernetinis saugumas tai sistema, kuri leidžia pasipriešinti kibernetinėms atakoms. Austrija kibernetinį saugumą įvardina kaip kibernetinės erdvės infrastruktūrų saugumą. Reikia pabrėžti, kad visos valstybės kibernetinį saugumą sieja su informacinėmis sistemomis ir ryšių tinklais bei jų saugumo užtikrinimu.

| Šalis | Kibernetinio saugumo apibrėžimas |
|---|---|
| **Kanada** | Tinkamo saugumo lygio užtikrinimas (kibernetinės atakos metu, t. y. tyčinio neteisėtos prisijungimo, naudojimo, valdymo ar sunaikinimo atveju) kurios metu naudojamasi elektroninės informacijos priemonėmis ir (arba) naudojant fizinę infrastruktūrą. |
| **Prancūzija** | Informacijos sistema leidžianti pasipriešinti įvykiams, kurie gali pakenkti prieinamumui, vientisumui ar saugumui duomenų, kurie yra saugojami, apdorojami ar perduodami tarp informacijos ir ryšių sistemų. |
| **Vokietija** | Globalaus kibernetinio saugumo tikslas yra informacinių technologijų saugumo rizikų sumažinimas iki priimtino lygio. |
| **Austrija** | Infrastruktūrų saugumas kibernetinėje erdvėje, kurioje asmenys keičiasi duomenimis |

2 pav. Kibernetinio saugumo samprata skirtingose šalyse (Užkuraitytė, 2014)

[33] 2018 m. birželio 27 d. Lietuvos Respublikos Kibernetinio saugumo įstatymas Nr. XIII-1299 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c>

Taigi, jau atsiradus pirmiems moderniems kompiuteriams buvo pradėta kalbėti apie būtiną kompiuterio naudotojo, pačios kompiuterio sistemos, jos techninės ir programinės įrangos apsaugojimą. Pastebima, kad kibernetinis saugumas yra vienas naujausių bei populiariausių tyrimų sričių, kuriam priskiriami išskirtiniai požymiai, tokie kaip asimetrinė prigimtis, anonimiškumas, globalios sklaidos galimybės, galimybė paveikti fizinius asmenis, sudėtingas nustatymas.[34]. Analizuojant aukščiau pateiktas įvairių šaltinių sąvokas randama panašumų: visi autoriai laikosi vieningos pozicijos, kad kibernetinio saugumo pagrindinis tikslas yra apsaugoti informacinių sistemų ir ryšių tinklus bei juose esančią informaciją nuo kylančių grėsmių. Vertinant visas anksčiau pateiktas kibernetinio saugumo sąvokas, būtent Lietuvos Respublikos kibernetinio saugumo įstatymas detalizuoja, kokiomis priemonėmis yra siekiama įgyvendinti atsparumą kibernetinėms grėsmėms. Susikūrus naujiems socialiniams reiškiniams (kasdienis informacinių technologijų naudojimas darbe, asmeniniame gyvenime, valstybiniu lygiu) yra būtinas šių reiškinių teisinis reglamentavimas, teisinio pobūdžio suteikimas konkrečiomis teisės normomis. Be to, svarbi ir pačios informacijos sklaidos gerinimas ir vystymasis, kadangi tirti nusikalstamas veikas, kurios yra atliktos kibernetinėje erdvėje yra iššūkis teisėsaugos pareigūnams. Tokio pobūdžio tyrimas reikalauja daug išteklių, o kartais ir atlikus išsamų tyrimą nėra nustatomas kaltininkas, todėl turi būti skatinama interneto naudotojų ir organizacijų kibernetine higiena. Galima teigti, kad kibernetinis saugumas yra vienas iš svarbiausių prioritetų, siekiant užtikrinti ne tik diplomatiją, įstatymų vykdymą, bet ir karines ir žvalgybos misijas, kurios yra susijusios su Europos saugumu ir stabilumu informacinėje infrastruktūroje. Taip pat dėmesys turi būti skiriamas šalių vidaus rinkos veikimui bei nenutrūkstamumui, kokybiškam esminių paslaugų teikimui (energetikos, transporto, sveikatos, finansų ir kt.). Apibendrinant visas aukščiau pateiktas sąvokas, galima teigti, kad kibernetinis saugumas yra visuma apimanti teisinių, techninių, informacinės sklaidos, priemonių, kurios padeda mažinti kibernetinio pažeidžiamumo riziką.[35]

### 1.2. Kibernetinis saugumas ir nusikalstamos veikos kibernetinėje erdvėje

Pasaulinis kompiuterinis tinklas plačiai naudojamas beveik visose žmogaus veiklos srityse. Be abejonės šiuolaikinės technologijos yra technologinis raidos pasiekimas, kuris toliau vystosi, tobulėja, atneša tiek teigiamų padarinių, tiek ir neigiamų pasekmių. Elektroniniai nusikaltimai, anksčiau, iki 2001 m. lapkričio 23 d. Konvencijos dėl elektroninių nusikaltimų priėmimo, buvo

[34] Miglė Stašikytė "Kibernetinio saugumo diskursas Lietuvos internetinėje žiniasklaidoje" (magistro baigiamasis darbas, Vytauto Didžiojo universitetas, 2014)

[35] Goda Užkuraitytė „Kibernetinio saugumo valdymo užtikrinimas: Pasaulinė patirtis ir Lietuvos perspektyva" (magistro baigiamasis darbas Mykolo Romerio universitetas, 2015) 24 puslapis.

vadinami kompiuteriniais nusikaltimais. Konkrečios kompiuterinių nusikaltimų sąvokos tuo metu nebuvo, o įvairios tarptautinės organizacijos sąmoningai neapibrėžinėjo kompiuterinio nusikaltimo, kadangi buvo manoma, jog keičiantis technologijoms, toks apibrėžimas greitai taptų nebeaktualus[36]. Kompiuteriniais nusikaltimais laikoma bet kokia neteisėta veikla, kurioje pasitelkiamos informacinės technologijos. Kompiuterinio nusikaltimo samprata pirmiausia reiškia, jog kompiuteriai ar jų tinklai gali būti naudojami kaip priemonė darant įprastas nusikalstamas veikas, tokias kaip sukčiavimas, klastojimas, vagystė, pinigų plovimas, seksualinis priekabiavimas ir pan., kurie egzistavo ir iki atsirandant internetui ar kompiuteriui. Taip pat, kompiuterinis nusikaltimas apima ir specifiškas kompiuterines veikas, kurios vykdomos kibernetinėje erdvėje, t. y. kurie be interneto ir kompiuterio būtų neįmanomi[37]. Tokios nusikalstamos veikos susijusios su įsilaužimais į kompiuterines sistemas, informacinių sistemų darbo sutrikdymais, kompiuterinių virusų platinimu. Kaip matyti, kompiuteriniai (elektroniniai) nusikaltimai suprantami plačiąja ir siaurąją prasmėmis. Šiuo metu, kai kur girdimas kibernetinio nusikaltimo terminas (cybercrime). „Cybercrime“ terminas yra lygiavertis elektroninio nusikaltimo terminui. Tačiau, pažymėtina, kad Lietuva ratifikavo Konvenciją dėl elektroninių nusikaltimų ir taip buvo įteisintas elektroninio nusikaltimo terminas[38]. Kaip ir tradiciniai nusikaltimai, elektroniniai nusikaltimai pasireiškia įvairiomis aplinkybėmis, turi daug galimų scenarijų. Autoriai Sarah Gordon ir Richard Ford elektroninį nusikaltimą apibrėžia kaip bet kokį nusikaltimą, kuris buvo padarytas naudojant kompiuterį, tinklą arba įrenginį[39]. Minėtų autorių pateikia samprata apima elektroninius nusikaltimus plačiąja prasme, kai kompiuterinė informacija yra nusikaltimo dalykas arba kai kompiuteris panaudojamas kaip nusikaltimo priemonė[40]. Nacionalinis kibernetinio saugumo centras bendrai platųjį ir siaurąjį nusikalstamų veikų modelius vadina – nusikalstamomis veikomis kibernetinėje erdvėje[41].

Analizuojant elektroninio nusikaltimo sampratą, bene, vienas svarbiausių tarptautinės teisės aktų, tai anksčiau minėta 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų. Nors konvencijoje nėra apibrėžta elektroninio nusikaltimo sąvoka, tačiau konvencijoje pateikiami konkretūs elektroniniai nusikaltimai, kurie kelia šalių susirūpinimą bei už kurių įvykdymą nustatomas

[36] Darius Štitilis „Elektroniniai nusikaltimai“ (Mykolo Romerio universitetas, 2011) https://repository.mruni.eu/bitstream/handle/007/16884/9789955193296.pdf?sequence=1&isAllowed=y
[37] Vaidas Kalpokas „Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos“ (2009), 79. https://teise.org/wp-content/uploads/2016/10/2009-1-kalpokas.pdf
[38] Metodinė priemonė Darius Štitilis „Elektroniniai nusikaltimai“ Mykolo Romerio Universitetas 2011 m. https://repository.mruni.eu/bitstream/handle/007/16884/9789955193296.pdf?sequence=1&isAllowed=y
[39] Sarah Gordon, Richard Ford „On the definition and classification of cybercrime“ http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.302.2178&rep=rep1&type=pdf
[40] Darius Štitilis „Elektroniniai nusikaltimai“ *op. Cit.,* 6.
[41] „2020 m. Nacionalinio kibernetinio saugumo ataskaita“ *Lietuvos Respublikos krašto apsaugos, supra note,* 2: 55.

baudžiamumas, taip formuojama bendra elektroninių nusikaltimų baudžiamoji politika. Konvencijoje yra pateikiamos elektroninių nusikaltimų rūšys ir jų apibrėžimai, pavyzdžiui:

- *nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui* apima šiuos nusikalstamus veiksmus: neteisėta prieiga, neteisėta perimtis, poveikis duomenims, poveikis sistemai, netinkamas įtaisų naudojimas[42]. Šios nusikalstamos veikos ir jų išaiškinimai yra įtvirtinti Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje – nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui. Pažymėtina, jog išvardintos nusikalstamos veikos pagal Lietuvos Respublikos baudžiamojo kodekso 10 straipsnį laikomi nusikaltimais, o ne baudžiamaisiais nusižengimais.

- *Kompiuteriniai nusikaltimai*:

a) Kompiuterinės klastotės – neteisėtas kompiuterių duomenų įvedimas, pakeitimas, sunaikinimas arba galimybe naudotis informacija panaikinimas, kurios pasekmė neautentiški duomenys, su tikslu, kad jie būtų laikomi autentiškais ar jais būtų naudojamasi teisėtiems tikslams.

b) Kompiuterinis sukčiavimas – sąmoningi neteisėti veiksmai, dėl kurių kitas asmuo praranda nuosavybę[43].

Šie nusikaltimai (išskyrus kompiuterinį sukčiavimą) atitinka siaurąjį elektroninio nusikaltimo aiškinimą, juos sieja bendras objektas – kompiuteriniai duomenys.

Informacinės technologijos tapo prieinamos nusikaltėliams bei teroristinėms grupuotėms, kurie naudojantis kompiuterinėmis sistemomis kaip informacijos rinkimo, veiksmų planavimo ir duomenų mainų įrankį[44], vykdo nusikaltimus elektroninėje erdvėje. Todėl literatūroje išskiriama ir plačioji elektroninių nusikaltimų sampratos prasmė. 2001 m. lapkričio 23 d. Konvencijoje elektroniniais nusikaltimais laikomi: *turinio nusikaltimai, susijęs su vaikų pornografija*, kuomet produkcija gaminama, siūloma, pateikiama, platinama, įgyjama, laikoma kompiuterinėje sistemoje. Taip pat, konvencijoje elektroniniais nusikaltimais laikomi ir *nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais*[45]. Taip pat ir kompiuteriniai sukčiavimai, kurie yra vieni dažniausiai pasitaikančių nusikalstamų veikų.

---

[42] 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų (Budapeštas). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195

[43] *Ibid*

[44] Nikolaj Goranin, Dalius Mažeika „Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos“ (Vilnius: UAB „TEV“, 2011), 10. http://www.esparama.lt/documents/10157/490675/Nusikaltimai_elektronineje_erdveje_ir_ju_tyrimo_metodikos.pdf

[45] 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195

Kaip matyti, konvencija nustatydama elektroninius nusikaltimus ir juos kriminalizuodama, laikosi plačiojo elektroninių nusikaltimų aiškinimo, kai kompiuteris yra nusikaltimo įrankis, o nusikalstamu būdu kėsinamasi į informaciją, kuri apdorojama kompiuterinėje sistemoje[46]. Pažymėtina, jog jau 2001 m. buvo iškeltas susirūpinimas nusikaltimų, vykdomų kompiuteriniais tinklais ir elektronine informacija, Konvencijoje dėl elektroninių nusikaltimų buvo nustatyti esminiai elektroninių nusikalstamų veikų apibrėžimai bei pažymimas būtinumas šalims taikyti veiksmingas, proporcingas ir atgrasančias sankcijas. Be to, 2003 m. sausio 28 d. Strasbūre, priimtas konvencijos dėl elektroninių nusikaltimų Papildomas Protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterių sistemomis, kriminalizavimo. Taigi, 2001 m. Konvencija dėl elektroninių nusikaltimų buvo papildyta ir prie elektroninių nusikaltimų priskirtos rasistinio ir ksenofobinio pobūdžio veikos, padarytos kompiuterių sistemomis, kurios priskiriamos elektroniniams nusikaltimams plačiąja prasme.

Taip pat, Europos Sąjungos kibernetinio saugumo strategijoje yra apibrėžta elektroninių nusikaltimų sąvoka, *elektroniniai nusikaltimai* – tai įvairaus pobūdžio nusikalstama veika, „kuriai kaip pirminės priemonės ar pirminis tikslas naudojami kompiuteriai ir informacinės sistemos“[47]. Elektroniniai nusikaltimai apima įprastas nusikaltimų veikų rūšis (pavyzdžiui, sukčiavimą, klastojimą ir tapatybės vagystę), su turiniu susijusias nusikaltimas veikas (pavyzdžiui, vaikų pornografijos platinimą internete arba rasinės neapykantos kurstymą) ir specifinius kompiuterių bei informacinių sistemų nusikaltimas veikas (pavyzdžiui, išpuolius prieš informacines sistemas, siekimą nutraukti sistemos veiklą ir kenkimo programinę įrangą)[48].

Taigi, apibendrinant elektroninių nusikaltimų sampratą, kurių pobūdis, atsižvelgiant į technologinius pasikeitimus, visada gali kisti, matyti, jog elektroninių nusikalstamų veikų aiškinime išskiriamas platusis ir siaurasis modeliai. Europos Sąjunga laikosi plačiosios elektroninių nusikaltimų aiškinimo pozicijos. Lietuva būdama jos nare, prisiima būtent šį elektroninio nusikaltimo aiškinimą. Elektroniniais nusikaltimais vadinami, ne tik unikalūs su kompiuteriais bei informacinėmis sistemomis susijusios nusikalstamos veikos, bet jiems priskiriamos ir kitos baudžiamuosiuose kodeksuose įtvirtintos nusikalstamos veikos, kurias įvykdyti buvo panaudotos informacinių ir ryšių technologijos. Bendrai plačiosios ir siaurosios elektroninės nusikalstamos veikos, vadinamos nusikalstamomis veikomis kibernetinėje erdvėje.

---

[46] Darius Štitilis ir kt. „*Interneto ir technologijų teisė*“ (Mykolo Romerio Universitetas, 2016) 403. https://repository.mruni.eu/bitstream/handle/007/16211/17_Interneto%20or%20technologij%c5%b3%20teis%c4%97.pdf?sequence=1&isAllowed=y

[47] Europos kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“ *supra note,* 28.

[48] *Ibid*

### 1.3. Kibernetinį saugumą užtikrinančios institucijos

Visos valstybės vieningai sutinka, kad kibernetinio saugumo svarbos negalima nuvertinti. Būtina imtis visų techninių ir organizacinių priemonių užkardant ardomąjį poveikį turinčius kibernetinius incidentus. Kadangi kibernetinių incidentų keliamas pavojus yra realus, padaroma organizacijoms, valstybių institucijoms bei gyventojams žala[49], tai reikalauja neatidėliotinų ir plataus pobūdžio koordinuotų veiksmų. Šiuo aspektu užtikrinant kibernetinį saugumą padeda institucijos, kurios specializuojasi kibernetinėje gynyboje.

2004 m. kovo 10 d. priėmus Reglamentą Nr. 460/2004, buvo įsteigta Europos tinklų ir informacijos apsaugos agentūrą (ENISA), kuria buvo siekiama užtikrinti Europos Sąjungos valstybių narių bei verslo bendruomenės tinklų ir informacijos saugumą. Šių dienų dėmesio centre yra ketvirtoji pramonės revoliucija, kuri pasižymi technologijų sinteze – fizine, skaitmenine ir biologine sąveika[50]. Atsirandančios tokios technologijos, kaip didieji duomenys, dirbtinis intelektas, daiktų internetas, robotika, 3D spausdinimas, skatina stiprinti Europos tinklų ir informacijos apsaugos agentūrą bei tobulinti jos veiklos sritis. ENISA įgaliojimai ir reguliavimo struktūra yra įtvirtinti Europos Parlamento ir Europos Sąjungos Tarybos Reglamente (ES) 2019/881. ENISA atlieka pagrindinį vaidmenį skatinant aktyvų valstybių narių, suinteresuotųjų šalių ir Europos Sąjungos institucijų bei agentūrų bendradarbiavimą, skatina kibernetinio saugumo įtraukimą į visas ES politikos sritis, operatyvinį bendradarbiavimą, kad kibernetinių išpuolių ir kibernetinių krizių metu būtų galima greitai reaguoti ir tinkamai koordinuoti pastangas visais lygmenimis (strateginiu, veiklos, techniniu ir ryšių), investuoja į kibernetinio saugumo kompetencijų ugdymą, gebėjimų susidoroti su kibernetinėmis grėsmėmis stiprinimą. Be to, ENISA skatina išlaikyti pusiausvyrą tarp visuomenės, skaitmeninių produktų rinkos, ekonominių ir kibernetinio saugumo poreikių, gerina Europos Sąjungos atsparumą kibernetinio saugumo grėsmėms, vykdydama numatymo metodiką, kai vystant arba jau beveik pradedant taikyti naujas technologijas, apibrėžiamos ankstyvos strategijos, kurios padeda rasti sprendimus kylantiems iššūkiams. Bene svarbiausias ENISA siekis yra tas, jog kibernetinio saugumo specialistų išanalizuotomis, apibendrintomis žiniomis ir informacija, būtų dalijamasi bei taikoma, ir tokiu būdu būtų užtikrinta Europos Sąjungos kibernetinio saugumo ekosistema[51].

---

[49] „Nacionalinė kibernetinio saugumo būklės ataskaita 2020“ *Lietuvos Respublikos krašto apsaugos ministerija* (2021 m. balandžio 7 d.) https://www.nksc.lt/doc/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf

[50] „Pramonė 4.0“ *Lietuvos Respublikos ekonomikos ir inovacijų ministerija*. https://eimin.lrv.lt/lt/veiklos-sritys/pramone/pramone-4-0

[51] Europien Union Agency for Cybersecurity „*Apie ENISA*“. https://www.enisa.europa.eu/about-enisa

EUROPOLAS – tai Europos Sąjungos teisėsaugos agentūra, kurios pagrindinis tikslas – padėti užtikrinti, kad Europa taptų saugesnė, nes tai teikia naudą visiems ES piliečiams[52]. Kovoje su nusikalstamomis veikomis kibernetinėje erdvėje 2013 m. įkurta Europos kovos su elektroniniu nusikalstamumu centras (EC3), kuris yra dalis Europolo. EC3 didžiausią dėmesį skiria elektroniniams nusikaltimams:

- kurias vykdo organizuotos nusikalstamos grupuotės, o iš nusikalstamų veikų yra gaunamas didelis neteisėtas pelnas, pavyzdžiui, sukčiavimas internete;
- kurių aukos patiria didelę žalą, pavyzdžiui, seksualinis vaikų išnaudojimas internete;
- kurių metu nukenčia ypatingos svarbos infrastruktūros objektai ir informacinės sistemos (įskaitant atsisakymo aptarnauti išpuolius, kuriais siekiama, kad konkrečios svetainės būtų nenaudojamos) Europos Sąjungoje[53].

EC3 keturios pagrindinės funkcijos:

- *būti pagrindiniu Europos kovos su elektroniniu nusikalstamumu informacijos centru*. Informacijos apie elektroninius nusikaltimus iš įvairiausių viešųjų, privačiųjų ir atvirų šaltinių rinkimas pildanti policijos duomenis;
- *sutelkti žinias siekiant padėti ES šalims stiprinti gebėjimus.*, Kad būtų sumažintas elektroninis nusikalstamumas, suteikti valstybėms narėms reikalingų praktinių žinių bei padėti rengti mokymus;
- *teikti operatyvinę paramą valstybėms narėms* tiriant elektroninius nusikaltimus, pvz., kuriant jungtines elektroninių nusikaltimų tyrimų grupes, o per vykdomus tyrimus keistis informacija;
- *tapti centru atstovaujančiu bendrą Europos elektroninių nusikaltimų tyrėjų, dirbančių teisėsaugos ir teisminėse institucijose, poziciją*[54].

Priimant Europos Parlamento ir Tarybos Direktyvą (ES) 2016/1148, 2016 m. liepos 6 d., valstybėms įtvirtinta pareiga paskirti vieną ar kelias Reagavimo į kompiuterinius saugumo incidentus tarnybas (CSIRT). Šios tarnybos turėtų veikti saugiose vietose, turėtų pakankamai darbuotojų užtikrinant pasiekiamumą bet kuriuo metu bei nustatytų keletą susisiekimo būdų. Taip pat CSIRT tarnybos turėtų turėti rezervinių komponentų sistemas ar atsargines darbo patalpas, užtikrintų ryšio

[52] Europolo oficialus tinklalapis. Prieiga internetu: https://www.europol.europa.eu/about-europol
[53] Europos kovos su elektroniniu nusikalstamumu centras Europole. Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:230806_1
[54] Europos Komisijos komunikatas Tarybai ir Europos Parlamentui „Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas“ 2012. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52012DC0140&from=LT

paslaugų prieinamumą be trikdžių[55]. Įsteigiant kiekvienoje valstybėje Reagavimo į kompiuterinius saugumo incidentus tarnybas, pirmiausia siekiama stebėti incidentus nacionaliniu lygiu, operatyviai reaguoti į incidentus, vykdyti rizikos ir incidentų analizę, užtikrinti informuotumą apie padėtį, teikti išankstinius įspėjimus, skelbimus atitinkamiems suinteresuotiems subjektams[56]. Taigi, atsakingam reagavimui į incidentus ir veiksmingam tarpvalstybiniam bendradarbiavimui, buvo priimta direktyva, kuria valstybės narės įpareigotos įsteigti nacionalines Reagavimo į kompiuterinius saugumo incidentus tarnybas (CSIRT). Pažymėtina kad, kiekviena valstybė narė iš savo Reagavimo į kompiuterinius saugumo incidentus tarnybų paskiria atstovus, kurie kartu su Europos Sąjungos Reagavimo į kompiuterinius saugumo incidentus tarnybų (CERT-EU) atstovais sudaro bendrą – Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklą (CSIRT tinklą). Tokiu būdu, keičiantis naudinga informacija, dalinantis geraja praktika, teikiant savitarpio pagalbą, užtikrinamas aukštas bendras tinklų ir informacinių sistemų saugumo lygis visoje Sąjungoje. Komisija CSIRT tinkle dalyvauja stebėtojos teisėmis. Reagavimo į kompiuterinius saugumo incidentus tarnybų tinkle ENISA atlieka sekretoriato paslaugas, t. y., tvarko svetainę, teikia visuomenei bendro pobūdžio informaciją apie didelio masto incidentus ir aktyviai remia Reagavimo į kompiuterinius saugumo incidentus tarnybų tarpusavio bendradarbiavimą[57]. ENISA internetinėje svetainėje pateikiama subendrinta informacija apie kiekvienoje valstybėje įsikūrusias Reagavimo į kompiuterinius saugumo incidentus tarnybas.

| Šalis | Komandos pavadinimas | Rinkimų apygarda | Esminių paslaugų operatoriai | CSIRT tinklas | Patikimas įvadininkas | PIRMAS | kontaktas |
|---|---|---|---|---|---|---|---|
| Lietuva | | All types | All types | Any status | Any status | Bet kokia būsena | |
| Lietuva | BITE SOC | Pramonės sektorius | | Ne narys | Į sąrašą neįtraukta | narys | bite.lt |
| Lietuva | CERT-LT | Nacionalinis | | narys | Akredituota | narys | nksc.lt/en/ |
| Lietuva | KVTC-CERT | Vyriausybė | | Ne narys | Akredituota | Ne narys | Vieša svetainė nepasiekiama |
| Lietuva | LITNET CERT | NREN | | Ne narys | Akredituota | narys | cert.litnet.lt |
| Lietuva | LTU NCSC | Vyriausybė, kariuomenė | | Ne narys | Į sąrašą įtraukta | narys | kam.lt |
| Lietuva | NRD CIRT | Komercinė organizacija | | Ne narys | Akredituota | narys | nrdcs.lt |
| Lietuva | SVDPT-CERT | Vyriausybė | | Ne narys | Akredituota | Ne narys | svdpt.gov.lt/ |
| Lietuva | TEO-CERT | IPT klientų bazė | | Ne narys | Į sąrašą neįtraukta | narys | teo.lt |

3 pav. Reagavimo į kompiuterinius saugumo incidentus tarnybos Lietuvoje (European Union Agency for Cybersecurity, 2022)

[55] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) Nr. 2016/1148, dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, 1 priedas. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=LT

[56] *Ibid*

[57] *Ibid*, 12 straipsnis.

3 paveikslėlyje yra pateikiamos Lietuvoje įsikūrusios Reagavimo į kompiuterinius saugumo incidentus tarnybos. Iš viso yra aštuonios tarnybos, tačiau tik viena iš jų priklauso Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklui. Lyginant su Baltijos valstybėmis, Lietuvoje Reagavimo į kompiuterinius saugumo incidentus tarnybų yra daugiausia, Latvijoje ir Estijoje – po dvi ir tik viena iš jų priklauso Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklui[58].

Be to, direktyvos Nr. 2016/1148 11 straipsniu įsteigta Bendradarbiavimo grupė, kurią sudaro valstybių narių, Komisijos (sekretoriato) ir ENISA atstovai. Atsižvelgiant į tarptautinio bendradarbiavimo kibernetinio saugumo srityje svarbą, Bendradarbiavimo grupės vaidmuo yra palengvinti strateginį bendradarbiavimą ir keitimąsi informacija tarp valstybių narių bei padėti ugdyti pasitikėjimą[59]. Bendradarbiavimo grupės veikimas detaliau paaiškintas 2017 m. vasario 1 d. Komisijos įgyvendinimo sprendime (ES) 2017/179, kuriuo pagal Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti 11 straipsnio 5 dalį nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti. Svarbu pažymėti, kad įgyvendinimo sprendime yra teigiama, kad Bendradarbiavimo grupė sprendimus priima bendru susitarimu[60], veiksmingumo sumetimais, konkretiems klausimams nagrinėti gali įsteigti pogrupius[61]. Bendradarbiavimo grupė savo užduotis, nustatytas direktyvoje Nr. 2016/1148 11 straipsnio 3 dalyje, vykdo remdamasi parengtomis dvimetėmis darbo programomis[62].

2017 m. gruodžio 11 d. 25 Europos Sąjungos valstybės narės pritarė Lietuvos iniciatyvai stiprinti ES bendradarbiavimą kibernetinės gynybos srityje[63]. Lietuvos iniciatyva sukurtas Europos Sąjungos Kibernetinės greitojo reagavimo komandos (angl. k. *Cyber Rapid Response Teams* – CRRT), kurios leidžia valstybėms narėms padėti viena kitai užtikrinti aukštesnį kibernetinį atsparumą ir kolektyviai reaguoti į kibernetinius incidentus. CRRT aprūpintos bendrai kuriamais, diegiamais kibernetiniais įrankių rinkiniais, skirtais kibernetinėms grėsmėms aptikti, atpažinti ir sušvelninti.

[58] „CSIRT pagal šalį – interaktyvus žemėlapis“ *European Union Agency for Cybersecurity*. (2022) https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Estonia
[59] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) Nr. 2016/1148, dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, 12 straipsnis. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=LT
[60] 2017 m. vasario 1 d. Komisijos įgyvendinimo sprendime (ES) 2017/179, kuriuo pagal Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti 11 straipsnio 5 dalį nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti, 6 straipsnio 1 dalis. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32017D0179&from=GA
[61] *Ibid*, 8 straipsnio 1 dalis.
[62] *Ibid*, 3 punktas.
[63] „Nuolatinis struktūrizuotas bendradarbiavimas (PESCO)“ *Lietuvos Respublikos krašto apsaugos ministerija*, 2017 m. gruodžio 19 d. https://kam.lt/lt/tarptautinis_bendradarbiavimas/europos_sajunga_612/pesco.html

Komandos gali padėti mokymuose, pažeidžiamumo vertinimuose ir kitose prašomose pagalbos srityse[64]. Komandas sudaro nacionaliniai kibernetinio saugumo ekspertai, deleguoti projekte dalyvaujančių valstybių narių. Pagrindinė CRRT funkcija – valdyti kibernetinius incidentus, jei pagalbos prireikia valstybei narei, ES institucijai, misijai, operacijai arba šaliai partnerei[65]. Pirmiausia norint aktyvuoti CRRT, nacionalinė institucija kibernetinio saugumo srityje, įgaliota veikti valstybės vardu, kreipiasi į Tarybos pirmininką, prašydama CRRT paramos po šalyje įvykusio kibernetinio incidento. Tarybos pirmininkas informuoja valstybių narių kontaktinius centrus ir perduoda jiems valstybės prašymą aktyvuoti CRRT[66]. Taryba svarsto, ar CRRT turėtų būti aktyvuota siekiant paremti nukentėjusią valstybę narę[67]. Priėmus sprendimą dėl aktyvinimo, Tarybos pirmininkas informaciją apie įvykį perduoda misijos koordinatoriui. Misijos koordinatorius sudaro ekspertų komandą (kompetencijų rinkinį, pagrįstą įvykio specifika ir jo valdymui reikalingais įgūdžiais). Misijos koordinatorius palaiko ryšius su dviem nacionaliniais ryšių punktais (techniniais ir logistikos), kad susitartų dėl sėkmingo misijos vykdymo[68].

Pagrindinė Lietuvos Respublikoje veikianti institucija atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimą ir kontrolę, ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją yra Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC)[69]. NKSC teikia šias paslaugas:

- kibernetinių incidentų valdymas;
- reagavimo į kibernetinius incidentus Krašto apsaugos sistemos Duomenų perdavimo tinkle;
- kibernetinio saugumo subjektų organizacinių ir techninių kibernetinio saugumo reikalavimų stebėsena ir vertinimas;
- įslaptintos informacijos ir ryšių informacinių sistemų akreditacija;
- kibernetinio saugumo informacinio tinklo (KSIT) paslaugų teikimas KSIT nariams;
- kibernetinio saugumo mokslinių tyrimų ir inovacijų kūrimas;

[64] „Cyber rapid response teams and mutual assistance in cyber security (CRRT)“ *Permanent Structured Cooperation (PESCO)*. https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
[65] Cyber Rapid Response Teams and mutual assistance in cyber security. Memo for Mutual Assistance in Cyber Security Key Roles and Procedures for the CRRTs' Operations Lessons Learnt from the Cyber Shield. Amber Mist 2018 Exercise.
[66] *Ibid,* 15.
[67] *Ibid,* 17.
[68] Cyber Rapid Response Teams and mutual assistance in cyber security. Memo for Mutual Assistance in Cyber Security Key Roles and Procedures for the CRRTs' Operations Lessons Learnt from the Cyber Shield. Amber Mist 2018 Exercise. 21.
[69] „Veikla“ *Nacionalinis kibernetinio saugumo centras*. Veikla, uždaviniai, sritys | NKSC

- regioninio bendradarbiavimo, technologinių priemonių ir ekspertinės kompetencijos apsikeitimo paslaugas[70].

NATO ryšių ir informacijos agentūra (NCI) valdo NATO kibernetinio saugumo centrą, kuris atsakingas už visų kibernetinio saugumo gyvavimo ciklo valdymo veiklų planavimą ir vykdymą, įgyja, dislokuoja ir gina ryšių sistemas NATO politinius sprendimus priimantiems asmenims ir vadovybėms, gina NATO tinklus 24 valandas per parą, 7 dienas per savaitę. Taip pat yra glaudžiai bendradarbiaujama su valstybių vyriausybėmis ir pramone, siekiant išvengti kibernetines atakas, įvairius incidentus. Kibernetinis saugumas apima NATO kompiuterinio reagavimo į incidentus pajėgumo (NCIRC) techninį centrą, teikiantį specialistų paslaugas, skirtas užkirsti kelią kibernetinio saugumo incidentams, juos aptikti, reaguoti ir po jų atsistatyti[71].

NATO ryšių ir informacijos agentūra 2019 m. vasario 12 d. įkūrė techninių kibernetinių gynėjų bendruomenę, t. y. prie NATO saugomo verslo tinklo (*angl. k. NATO's protected business network*) prisijungė pirmųjų penkių valstybių – Belgijos, Prancūzijos, Nyderlandų, Jungtinės Karalystės ir JAV Reagavimo į kompiuterinius saugumo incidentus tarnybos. Tokios bendruomenės įkūrimas leis valstybėms greitai ir saugiai dalintis informacija tarpusavyje ir su NATO ryšių ir informacijos agentūra, be to tokiu būdu siekiama geriau apsaugoti NATO tinklus. Pažymėtina, kad saugiam ir moderniam tarpvalstybiniam bendradarbiavimui el. paštas ir telefonai neturi įtakos, todėl siekiant apsiginti nuo dinamiškų grėsmių reikia veikti greitai, o šioje vietoje būtent ir padės kibernetinio saugumo bendradarbiavimo centras, kuris sukuria NATO suinteresuotųjų šalių bendruomenę prasmingiems informacijos mainams[72]. Lietuvos Respublikos Nacionalinis kibernetinio saugumo centras vykdydamas kibernetinių incidentų valdymą, prevenciją, stebėseną ir kontrolę šalyje bendradarbiauja su NATO ryšių ir informacijos agentūra bei dalyvauja jų organizuojamuose mokymuose bei pratybose. Pavyzdžiui 2021 m. „Locked Shields“, kuriuose kompiuteriu imituojamos pratybos vyksta realiu laiku simuliuotoje virtualioje aplinkoje, kurioje treniruojasi specialistai iš įvairių šalių. 2021 m. „Locked Shields“ pratybose dalyvavo daugiau nei 2000 ekspertų iš beveik 30 šalių. Nors ir pratybų scenarijus, ir aplinka yra išgalvoti, jame naudojami metodai, įgyvendinami ir realiame gyvenime[73].

---

[70] „Paslaugų sąrašas“ *Nacionalinis kibernetinio saugumo centras.* Paslaugos | NKSC
[71] „Partneriai“ *Nacionalinis kibernetinio saugumo centras* https://www.nksc.lt/en/partners.html
[72] „New NATO hub will gather the Alliance's cyber defenders“ *NCIA-NATO Communications and Information Agency* ( 2019 m. vasario 12 d.) https://www.ncia.nato.int/about-us/newsroom/new-nato-hub-will-gather-the-alliances-cyber-defenders.html
[73] „Locked Shield“ *NATO kooperatyvo kibernetinės gynybos kompetencijos centras* https://ccdcoe.org/exercises/locked-shields/

1990 m. buvo įkurtas reagavimo į incidentus ir saugumo komandų forumas „FIRST“, kurios nariai tuo metu išsprendė su saugumu susijusių išpuolių ir incidentų srautą, įskaitant tūkstančių saugumo spragų, turinčių įtakos kompiuterių sistemų ir tinklų visame pasaulyje, kuriuos jungia vis didėjantis internetas, valdymą[74]. Šiai dienai „FIRST“ suburia įvairias saugumo ir reagavimo į incidentus komandas iš visų pasaulio šalių.

Dar viena internacionalinė organizacija užtikrinanti kibernetinį saugumą, tai INTERPOLAS – tarptautinė kriminalinės policijos organizacija, kuriai šiuo metu priklauso 192 valstybės[75]. Ši organizacija skatina šalių narių bendradarbiavimą tiriant įvairius nusikaltimus įskaitant ir kibernetinius nusikaltimus. INTERPOLAS padeda šalims narėms nustatyti, suskirstyti ir koordinuoti atsaką į kibernetines grėsmes. *Cyber Fusion Centre (CFC)* vienija teisėsaugos ir pramonės kibernetinius ekspertus, kad surinktų ir analizuotų visą turimą informaciją apie nusikalstamą veiklą kibernetinėje erdvėje, kad suteiktų šalims nuoseklią bei veiksmingą žvalgybinę informaciją. CFC skelbia ataskaitas, kad įspėti šalis apie naujas, neišvengiamas ar besivystančias kibernetines grėsmes.

Taigi, išanalizavus kiekvienos, kibernetinį saugumą užtikrinančios, institucijos pagrindinius tikslus kibernetinio saugumo srityje, pastebimas esminis siekis, t. y. bendradarbiavimu didinti kiekvienos šalies kibernetinį atsparumą bei efektyviai užkardyti kibernetinius incidentus, kadangi kibernetinis saugumas yra visų šalių atsakomybė. Pažymėtina, jog būtent bendradarbiavimu yra pasiekiami geriausi rezultatai, kadangi kibernetinio pobūdžio grėsmės sunaikina laiko ir erdvės barjerus, sukuria galimybę kontaktuoti su neribotu kiekiu žmonių, sudaro prielaidas anonimiškumui.

Kaip jau buvo minėta anksčiau, be informacinių sistemų neįsivaizduojamas šiuolaikinis pasaulis, todėl vykstant pasauliniam skaitmenizavimui yra svarbus kibernetinis saugumas. Būtent kibernetinio saugumo institutas naudodamasis priemonėmis ir metodais, mažina informacinių ir ryšių sistemų pažeidžiamumą nuo neteisėtų veiksmų. Šie neteisėti veiksmai yra elektroniniai nusikaltimai, kurių sampratos aiškinimas išsišakoja į du aspektus – siaurąjį ir platųjį. Kadangi informacinės technologijos tobulėja ir reikalauja daugiau specialiųjų žinių, siekiant sklandaus ryšių tinklų ir informacinių sistemų veikimo, atitinkamos specialios organizacijos užtikrina kibernetinį saugumą internacionaliniu bei nacionaliniu mastu.

[74] „About FIRST“ *Forum of Incident Response and Security Teams*. https://www.first.org/about/
[75] „Interpol“ Lietuvos Respublikos Vyriausybė. https://policija.lrv.lt/lt/tarptautinis-bendradarbiavimas/musu-partneriai/tarptautines-organizacijos/interpol

# 2. KIBERNETINIO SAUGUMO TEISINIS REGLAMENTAVIMAS EUROPOS SĄJUNGOJE

Sparčiai besivystantys ryšių tinklai ir informacinės sistemos, dažniną susidūrimą su kibernetiniais incidentais, todėl siekiant užtikrinti Europos Sąjungoje bendrą kibernetinio saugumo lygį, sukurti atsparią kibernetinę aplinką, buvo būtina išvystyti kvalifikuotą teisinę sistemą visoje Europos Sąjungoje. Europos Parlamentas ir Taryba nustatė tam tikras technines ir organizacines priemones valstybėms narėms tam, kad būtų užtikrintas bazinis kibernetinis saugumas, teikiamų skaitmeninių paslaugų tęstinumas ir sumažinta galima rizika fizinėms infrastruktūroms. Šiame skyriuje aptariama chronologinė kibernetinio saugumo teisinė sistema egzistuojanti Europos Sąjungoje, jos vystymasis, raida, kibernetinio saugumo institucijų tikslai ir uždaviniai, kuriais kryptingai siekiama užtikrinti vieningą sistemą Europos Sąjungos šalyse, aptariama kibernetinio saugumo sertifikavimo sistema, jos būtinumas, tikslai ir nauda.

Atsiradus naujiems socialiniams reiškiniams, valstybės suprato būtinumą rūpintis ryšio tinklų ir informacinių sistemų saugumu. Europos Sąjungoje apie saugumą elektroninėje erdvėje bei valstybių narių elektroninių ryšių tinklų ir paslaugų suderintą teisinį reguliavimą pradėta kalbėti labai anksti. Jau 1995 m. spalio 24 d. Europos Parlamentas ir Taryba priėmė direktyvą Nr. 95/46/EB[76] „dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“. Ši direktyva reikalavo, kad kontroliuojantis asmuo, vykdydamas duomenų perdavimą per tinklus, įgyvendintų atitinkamas technines ir organizacines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto jų sunaikinimo arba atsitiktinio jų netekimo, pakeitimo, neleistino atskleidimo ar prieigos prie jų [77].

2002 m. kovo 7 d. buvo priimta Europos Parlamento ir Tarybos direktyva Nr. 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo (Leidimų direktyva)[78]. Direktyva suteikė valstybėms narėms teisę prie bendrojo leidimo reikalavimo prijungti sąlygas dėl viešųjų tinklų apsaugos nuo neteisėtos prieigos[79]. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyvoje 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva)[80], buvo reikalaujama, kad tiekėjai, teikiantys viešųjų ryšių tinklų arba viešai prieinamų elektroninių ryšių

[76] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB). https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:31995L0046&from=LT
[77] 2004 m. kovo 10 d. Europos Parlamento ir Tarybos Reglamentas (EB) Nr. 460/2004, 8 punktas. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32004R0460&from=EN
[78] 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva Nr. 2002/20/EB https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0020&from=LT
[79] 2004 m. kovo 10 d. Europos Parlamento ir Tarybos Reglamentas (EB) Nr. 460/2004, 6 punktas. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32004R0460&from=EN
[80] 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB. Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0021&from=LT

paslaugas, įgyvendintų atitinkamas saugumo priemonės, apsaugant teikiamų paslaugų vientisumą ir saugumą. Nacionalinės reguliavimo institucijos buvo įpareigotos tam tikrais atvejais informuoti agentūrą apie saugumo pažeidimų ar vientisumo praradimo atvejus, kurie turi didelės įtakos tinklų veikimui ar paslaugų teikimui bei pateikti Europos Komisijai ir agentūrai metines apibendrintas gautų pranešimų ir įvykdytų veiksmų ataskaitas[81]. Be to, 2002 m. kovo 7 d. buvo priimta direktyva Nr. 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (Universaliųjų paslaugų direktyva)[82]. Ši direktyva reikalavo, kad valstybės nares imtųsi būtinų priemonių užtikrinti viešojo telefono ryšio tinklų vientisumą ir prieinamumą bei, kad įmonės, teikiančios viešai prieinamas telefono ryšio paslaugas, imtųsi visų reikiamų priemonių siekiant užtikrinti nenutrūkstama galimybę naudotis avarinėmis tarnybomis[83]. Pažymėtina, kad šiuo metu šios trys direktyvos: Nr. 2002/20/EB, 2022/21/EB ir Nr. 2002/22/EB, yra negaliojančios. 2002 m. liepos 12 d. Europos Parlamentas ir Taryba priėmė direktyvą, Nr. 2002/58/EB, dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)[84]. Ši direktyva 2009 m. lapkričio 25 d. buvo pakoreguota. Direktyva reikalauja, kad viešai prieinamų elektroninių ryšių paslaugų teikėjas imtųsi tinkamų techninių ir organizacinių priemonių, kad užtikrintų savo teikiamų paslaugų saugumą, bei reikalauja, kad būtų užtikrinamas ir ryšių bei susijusių srauto duomenų konfidencialumas. Taigi, buvęs neišsamus teisinis reguliavimas paskatino Europos Parlamentą ir Tarybą imtis priemonių įgyvendinti valstybėse narėse vieningas technines ir organizacines priemones užtikrinant vidaus rinką. Todėl, jau 2004 metais, Europos Parlamentas ir Taryba atsižvelgdami į tai, kad informacinės sistemos ir ryšių tinklai tapo esminiu ekonominės ir socialinės plėtros veiksniu bei kompiuterinės ir ryšio tinklų paslaugos pradėtos plačiai naudoti ir tai beveik tapo tokiomis svarbiomis komunalinėmis paslaugomis kaip ir elektros energija ar vandens tiekimas[85]. 2004 m. kovo 10 d. priėmė reglamentą Nr. 460/2004, kuriuo įsteigė Europos tinklų ir informacijos apsaugos agentūrą (ENISA).

Europos tinklų ir informacijos apsaugos agentūros tikslas teikti rekomendacijas ir patarimus, sumažinti saugumo pažeidimų skaičių bei užtikrinti Europos Sąjungos narių nuoseklumą

[81] 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos Reglamentas (ES) Nr. 526/2013 dėl Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA), kuriuo panaikinamas Reglamentas (EB) Nr. 460/2004 https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32013R0526&from=EN
[82] 2002 m. kovo 7 d. Europos Parlamento ir Tarybos Reglamentas Nr. 2002/22/EB Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0022&from=LT
[83] Reglamentas (EB) Nr. 460/2004, *supra note,* 79: 7 punktas.
[84] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos Reglamentas Nr. 2002/58/EB Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0058&from=lt
[85] Reglamentas (EB) Nr. 460/2004, *op. Cit.*

įgyvendinant saugumo priemones. Sąjungoje taikomi nevienodi reikalavimai, paskatintų priimti neveiksmingus sprendimus bei sudarytų kliūtis vidaus rinkai, jos vystymuisi. Dėl suderinto reguliavimo tikslingumo buvo iškeltas klausimas ir Teisingumo Teismo 2006 m. gegužės 2 d. byloje C-217/04, Jungtinė Karalystė/Parlamentas ir Taryba, kurioje Jungtinė Didžiosios Britanijos ir Šiaurės Airijos Karalystė nurodė, kad įsteigtos Europos tinklų ir informacijos apsaugos agentūros patarimai, kurie nėra privalomi valstybėms narėms, gali padidinti tarp nacionalinių teisės aktų egzistuojančius skirtumus bei nepalengvins 2002/21/EB, 2002/19/EB, 2002/20/EB, 2002/22/EB, 2002/58/EB, 1999/93/EB, 2000/31/EB direktyvų įgyvendinimą. Tačiau Teisingumo Teismas išaiškino, kad tokio organo kaip ENISA įsteigimas yra tinkama priemonė užkirsti kelią Valstybių Narių teisiniams skirtumams, kurie galėtų sudaryti kliūtis sklandžiam vidaus rinkos nagrinėjamoje srityje veikimui, atsirasti[86].

Europos tinklų ir informacijos apsaugos agentūra renka atitinkamą informaciją, kuri yra susijusi su ryšių tinklo ir informacijos saugumu. Padeda analizuoti esančias ar kylančias rizikas, gali atlikti įvairias apklausas, teikti patarimus, organizuoti mokymosi kursus[87]. ENISA veiklos nauda valstybėms yra neabejojama, kadangi rinkdama informaciją skirtą esančiai ir kylančiai rizikai, ji teikia konkrečias rekomendacijas, patarimus kaip sumažinti kibernetinių incidentų pavojų. Pavyzdžiui, rekomendacijas dėstytojams, mokytojams, vykdant formaliojo ir neformaliojo švietimo veiklą, privatiems skaitmeninių technologijų naudotojams, taip pat rengia mokymus darbuotojams, pratybas technikos ekspertams[88]. Pažymėtina, kad reglamentu įgyvendinamos specialiosios direktyvos 2002/21/EB, 2002/19/EB, 2002/20/EB, 2002/22/EB, 2002/58/EB, 1999/93/EB, 2000/31/EB ir vidaus rinka elektroninių ryšių srityje. ENISA buvo įsteigta penkerių metų laikotarpiui, todėl 2008 m. Europos Parlamentas ir Taryba priėmė reglamentą (EB) Nr. 1007/2008, kuriuo iš dalies pakeitė Europos Parlamento ir Tarybos 2004 m. kovo 10 d. reglamentą Nr. 460/2004. Įsteigtos Europos tinklų ir informacijos apsaugos agentūros veiklos atžvilgiu ir jos įgaliojimai pratęsti iki 2012 m. kovo mėnesio, o remiantis reglamentu (ES) Nr. 580/2011, agentūros įgaliojimai buvo pratęsti iki 2013 m. rugsėjo 13 d[89].

---

[86] 2006 m. gegužės 2 d. Teisingumo Teismo (didžiosios kolegijos) sprendimas byloje Nr. C-217/04. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:62004CJ0217&qid=1644940795442&from=EN

[87] *Ibid*

[88] „ECSM – Recommendations for ALL“ *European Union Agency for cybersecurity*. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month/2014/ecsm-recommendations-for-all-lt

[89] Reglamentas (ES) Nr. 526/2013, *supra note*: 81.

Didėjant elektroninių ryšių, infrastruktūros ir paslaugų saugumo, jų vientisumo, prieinamumo ir konfidencialumo iššūkiams, užtikrinant esmines visuomenei ypač svarbias paslaugas, nuspręsta stiprinti Europos tinklų ir informacijos apsaugos agentūrą[90]. Dėl tos priežasties, 2013 m. gegužės 21 d. Europos Parlamentas ir Taryba priėmė reglamentą Nr. 526/2013, kuriuo panaikino reglamentą (EB) Nr. 460/2004 ir vėl įsteigė Europos Sąjungos tinklų ir informacijos apsaugos agentūrą (ENISA). Europos Sąjungos Taryba 2010 m. lapkričio 25 d. pateikė pažangos ataskaitą dėl Europos tinklų ir informacijos apsaugos agentūros (ENISA) veiklos, kurioje nurodė, kad ENISA turėtų tęsti savo darbą tinklų ir informacijos saugumo srityje. Dėl šios priežasties reikia pratęsti ENISA įgaliojimus, modernizuoti ir sustiprinti pačią ENISA, išplėsti paskirtas užduotis bei didinti ENISA finansinius ir žmogiškuosius išteklius[91]. Pagal reglamentą numatyta, kad ENISA turėtų išlaikyti, plėtoti, užtikrinti susidariusią praktinę tvarką, sklandžią ir veiksmingą ENISA veiklą, padėti Sąjungos institucijoms įgyvendinant teisinius ir norminius reikalavimus tinklų ir informacijos saugumo aspektu, skatinti bendradarbiavimą ir sudaryti palankias sąlygas aukštos kvalifikacijos darbuotojams įdarbinti ir išlaikyti[92]. Atsižvelgus į elektroninių tinklų ir komunikacijų didėjančią svarbą, šiame 2013 m. gegužės 21 d. reglamente, lyginant su ankstesniu 2004 m. kovo 10 d. reglamentu, nustatytos ENISA užduotys bei jos veiklos tikslai jau yra labiau detalizuotos. Reglamentuotos užduotys padeda kryptingai siekti tinklų ir informacijos saugumo, asmens duomenų saugumo bei tikslingai vykdyti veiklą.

2013 m. pabaigoje agentūra surengė Briuselyje aukšto lygio konferenciją, kuria buvo siekiama tiesiogiai paremti naująją ES kibernetinio saugumo strategiją, suburiant daugiau nei 200 suinteresuotųjų šalių, kad būtų sukurta nuoseklesnė kibernetinio saugumo politika. Renginys padėjo gerokai padidinti ENISA matomumą tarp suinteresuotųjų šalių[93]. ENISA remdama savanorišką kompetentingų įstaigų tarpusavio bendradarbiavimą ir informavimo skatinimą, skatina geriausios praktikos kūrimą ir dalijimąsi, siekiant aukšto lygio tinklų ir informacijos saugumo[94]. 2013 m. ENISA pateikė metinę ataskaita apie didelius incidentus telekomunikacijų sektoriuje. Ataskaitoje buvo pateikta daugiau medžiagos tendencijoms ir modeliams analizuoti, taip pat buvo paskelbtos ENISA metinės ataskaitos apie grėsmių aplinką, kurios buvo pristatytos pagrindinėms suinteresuotosioms

[90] *Ibid*
[91] 2010 m. lapkričio 25 d. Europos Sąjungos Taryba pažangos ataskaita Nr. 16835/10. Prieiga internetu: https://data.consilium.europa.eu/doc/document/ST%2016835%202010%20INIT/EN/pdf
[92] (ES) Nr. 526/2013, *op. Cit.*
[93] „ENISA annual report“ *European Union Agency for Network and Information Security* (2013), 8. https://www.enisa.europa.eu/publications/corporate/enisa-annual-report-2013
[94] Reglamentas (ES) Nr. 526/2013, *op. Cit.*

šalims bei taip pat sulaukė didelio pripažinimo[95]. Taigi, metinė ataskaita įrodo, jog ENISA remia mokslinius tyrimus, jų plėtrą, padeda nustatant rizikos valdymo ir elektroninių produktų, tinklų ir paslaugų standartus. Taip siekiama veiksmingumo reaguojant į tinklų ir informacijos saugumo rizikas bei grėsmes[96]. 2013 m. gegužės 21 d. priimtas reglamentas (EB) Nr. 526/2013 modernizavo jau įsteigtos ENISA veiklos veiksmingumą.

Kibernetinis saugumas yra labai svarbus plėtojant ES veiksmų atsparumą, technologinį suverenumą, saugant piliečius, įmones ir institucijas nuo galimų kibernetinių grėsmių. Bendrajame komunikate Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui įtvirtinta Europos Sąjungos kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“, kuria nustatyta veiklos kryptis ir planas. Europos Sąjungos kibernetinio saugumo strategijoje įtvirtinti kibernetinio saugumo principai:

1. ES pagrindinės vertybės galioja tiek kibernetinėje, tiek fizinėje erdvėje;
2. pagrindinių teisių, žodžio laisvės, asmens duomenų ir privatumo apsauga, prieiga visiems (kiekvienas turėtų turėti galimybę naudotis internetu ir netrukdomai gauti informaciją, užtikrinti interneto vientisumą ir saugumą);
3. demokratiškas ir veiksmingas suinteresuotųjų šalių dalyvavimu grindžiamas valdymas (kibernetinės erdvės nekontroliuoja vienas subjektas, todėl dabartiniam interneto valdymo modeliui svarbus visų suinteresuotųjų šalių dalyvavimas);
4. bendra atsakomybė siekiant užtikrinti saugumą (atsakomybė yra bendra, todėl reikia imtis savisaugos veiksmų ir prireikus koordinuotai sureaguoti)[97].

Pagrindinių teisių, žodžio laisvės, asmens duomenų ir privatumo apsaugos principo įtvirtinimas ES strategijoje kelia abejonių dėl jo būtinumo, kadangi šio principo kaip specifinio ar bendrojo kibernetinio saugumo principo išskyrimas neatneša nieko naujo. Šio principo turinys yra ganėtinai aiškus, išsamiai reglamentuotas tarptautiniuose norminiuose aktuose[98]. Visų svarbių principų pateikimas vienoje vietoje vertingas tuo, kad visi principai turi būti taikomi kaip sistemos dalis, o principus išskiriant ir įtraukiant į vieną dokumentą leidžiama aiškiau įvertinti principų visumą ir sistemą[99]. Kibernetinio saugumo strategijoje išskirti penki strateginiai prioritetai, tokie kaip:

1. „pasiekti kibernetinį atsparumą;

[95] „ENISA annual report“ *supra note*: 93
[96] Reglamentas (ES) Nr. 526/2013, *supra note*: 81.
[97] Europos Sąjungos kibernetinio saugumo strategija *supra note:* 28.
[98] Darius Štitilis ir kt. „Concepts and principles of cyber security strategies“. (Mykolo Romerio universitetas, 2016). 204. http://jssidoi.org/jssi/uploads/papers/22/Stitilis_Concepts_and_principles_of_cyber_security_strategies.pdf
[99] *Ibid*.

2. radikaliai sumažinti elektroninių nusikaltimų skaičių;

3. sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika;

4. plėtoti pramoninius ir technologinius išteklius kibernetiniam saugumui užtikrinti;

5. sukurti nuoseklią tarptautinę Europos Sąjungos kibernetinės erdvės politiką ir remti pagrindines ES vertybes“[100].

Taigi, kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“ siekiama užkirsti tam tikrų veiklų, vykdomų informacijų ir ryšių technologijomis, sutrikdymą bei aktyviai remti atsakomąsias priemones. Visi kibernetinio saugumo dalyviai, siekdami užtikrinti kibernetinį saugumą tiek nacionaliniu, tiek ir ES lygiu, turėtų dirbti kartu[101], o minėta strategija yra planas, kurio laikantis kryptingai siekiama Europos Sąjungoje didinti saugumą, atsparumą, mažinti incidentų skaičių. Tai nėra teisės aktas, kurio nuostatos Europos Sąjungos valstybėms narėms yra privalomos, tačiau nuo šio dokumento priklauso kiekvienos Europos Sąjungos narės kibernetinio saugumo politika.

Ne ką mažiau svarbi yra 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222TVR. Šia direktyva siekiama suderinti Europos Sąjungos valstybių narių baudžiamąją teisę atakų prieš informacines sistemas srityje. Kadangi gresiančių galimų atakų riziką kaskart vis didėja, yra būtina sukurti saugią informacinę visuomenę, kurioje galioja griežtos sankcijos pažeidžiant informacinių sistemų naudojimosi vientisumą. Šia direktyva nustatomas bendras požiūris į nusikalstamų veikų sudėties požymius, todėl yra aiškiai numatytos nusikalstamos veikos, kurios turi būti įtrauktos į nacionalinę teisinę sistemą ir už kurias turi kiekvienoje valstybėje narėje grėsti baudžiamoji atsakomybė. Pavyzdžiui, neteisėtos prieigos prie informacinių sistemų, neteisėto įsikišimo į sistemą, į duomenis, neteisėto duomenų perėmimo atvejais, taip pat ir išvardintoms nusikalstamoms veikoms vykdyti naudojamų priemonių gamyba, perdavimas, įsigijimas, naudojantis importu ar kitokiu platinimu[102]. Direktyva nereglamentuojamos tradicinės nusikalstamos veikos kibernetinėje erdvėje, kurios yra laikomos nusikalstamomis veikomis kibernetinėje erdvėje plačiąją prasme. Taigi, šia direktyva yra formuojamas bendras visų ES valstybių narių požiūris į kibernetinių grėsmių riziką bei panašaus bausmių dydžio taikymo praktika. Direktyvoje imperatyviai nustatyti nusikalstamų veikų padarymo atveju skirtini bausmės dydžiai, kurie taikomi, kai nusikalstamos veikos

[100] Europos Sąjungos kibernetinio saugumo strategija, *supra note*,: 27.
[101] [101] Darius Štitilis ir kt. „Concepts and principles of cyber security strategies“, *supra note*: 98: 470.
[102] Renata Marcinauskaitė „Nusikalstamos veikos elektroninėje erdvėje ir teritorinė baudžiamoji jurisdikcija“ (Mykolo Romerio universitetas, 2021), https://ojs.mruni.eu/ojs/jurisprudence/article/download/6620/5421

yra tyčinės ir nėra mažareikšmės. Informacinių sistemų apsaugos priemonių pažeidimas yra būtinas anksčiau išvardintų elektroninių nusikalstamų veikų sudėčiai inkriminuoti, o baudžiamoji atsakomybė už šias nusikalstamas veikas kyla nemažareikšmiais atvejais[103]. Direktyvoje vyrauja siauroji nusikalstamų veikų samprata, į kurią patenka specifinės nusikalstamos veikos, susijusios su elektroniniais tinklais[104]. Taip pat už elektroninių nusikalstamų veikų padarymą atsako ne tik fizinis asmuo, bet ir juridinis. Juridiniams asmenims gali būti skiriama – teisės į valstybės teikiamas lengvatas arba pagalbą atėmimas, laikinas ar nuolatinis teisės verstis komercine veikla atėmimas, teisminės priežiūros skyrimas, teismo paskirtas likvidavimas, laikinas ar galutinis įmonių, kurios buvo naudojamos nusikalstamai veikai įvykdyti, uždarymas[105]. Taigi, bendras atitinkamų sankcijų taikymas už konkrečias kibernetines nusikalstamas veikas, sukuria vienodą teisinę sistemą visoje Europos Sąjungos kibernetinėje erdvėje. Pažymėtina, jog direktyvoje yra nustatytos ir jurisdikcijos taisyklės, taigi jurisdikcija direktyvoje įtvirtintoms nusikalstamoms veikoms turi būti nustatyta tais atvejais „kai: a) nusikalstama veika arba jos dalis padaryta jų teritorijoje; b) nusikalstamą veiką padarė vienas iš jų piliečių, bent tais atvejais, kai veiksmas yra nusikalstama veika toje vietoje, kurioje jis buvo įvykdytas“[106]. Analizuojant nusikalstamos veikos padarymo vietos klausimą matyti, jog nusikalstamos veikos padarymo vieta yra siejama ne tik su kaltininko, bet ir su informacinės sistemos fizinio buvimo vieta[107]. Nors elektroninių nusikaltimų specifika siejasi su elektronine erdve, tačiau visgi elektroninę erdvę sukuria informacinės sistemos, kurios egzistuoja fizinėje erdvėje, todėl informacinės sistemos buvimo vieta leidžia susieti elektroninę nusikalstamą veiką su fizine erdve, su tam tikra teritorija, kurią galima taikyti elektroninės veikos padarymo atveju[108]. Sprendžiant dėl elektroninių nusikalstamų veikų vietos nustatymo, pasitaiko problema, jog visgi ikiteisminio tyrimo metu nenustatoma veikos padarymo vieta, kurioje kaltinamasis vykdė neteisėtus veiksmus, dėl to gali kilti ir teismingumo klausimų, kurių metu, baudžiamosios bylos nagrinėjimas vilkinamas ir ji perduodama iš vieno teismo į kitą. Taigi, pavojingų didelės apimties atakų atveju prieš informacines sistemas,

[103] Renata Marcinauskaitė „Nusikalstamos veikos elektroninėje erdvėje ir teritorinė baudžiamoji jurisdikcija“ *supra note:* 102.
[104] Renata Marcinauskaitė „Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai ir kvalifikavimo problemos“ (Vytauto Didžiojo universitetas, 2016), https://portalcris.vdu.lt/server/api/core/bitstreams/82500ab8-69a0-43ec-adb6-12997b9b88d4/content
[105] *Ibid,* 10 straipsnis.
[106] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR, 12 straipsnio 1 dalis. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32013L0040
[107] Renata Marcinauskaitė „Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai ir kvalifikavimo problemos“, *op. Cit.*
[108] *Ibid,* 207 psl.

kurios gali sukelti didžiulę žalą, direktyvos nuostatomis sukuriamas bendras požiūris į elektronines nusikalstamas veikas, jų įvykdymo atveju įtvirtinamas sankcijų proporcingumas.

Iki 2016 m. Europos Sąjungos valstybių narių, vartotojų bei įmonių tinklų ir informacinių sistemų saugumo lygis buvo labai skirtingas, nebuvo nustatytų bendrų reikalavimų esminių paslaugų operatoriams ir teikėjams[109]. Todėl siekiant veiksmingumo sprendžiant tinklų ir informacinių sistemų saugumo problemas, 2016 m. liepos 6 d. buvo priimta Europos Parlamento ir Tarybos Direktyva (ES) 2016/1148, dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. Šios direktyvos šaknys yra 2009 m. Europos Komisijos komunikate, kuriame pagrindinis dėmesys skiriamas prevencijai ir informuotumui bei, kuriame apibrėžiamas neatidėliotinų veiksmų planas siekiant sustiprinti saugumą ir pasitikėjimą informacine visuomene[110]. Po to, 2013 m. buvo paskelbtas bendras Europos Komisijos ir Europos Sąjungos vyriausiosios įgaliotinės užsienio reikalams ir saugumo politikai komunikatas dėl Europos Sąjungos kibernetinio saugumo strategijos[111]. 2013–2015 m. Komisija, Taryba ir Parlamentas intensyviai diskutavo dėl Komisijos pateikto projekto, o šių diskusijų rezultatas – direktyva Nr. 2016/1148, kuri įsigaliojo 2016 m. rugpjūtį. Galutinis ES valstybių narių direktyvos nuostatų perkėlimo į nacionalinę teisę terminas buvo 2018 m. gegužės 9 d.[112] Šia direktyva yra nustatomos priemonės, užtikrinančios aukštą bendrą tinklų ir informacinių sistemų saugumo lygį, kuris gerintų vidaus rinkos veikimą [113]. Dėl tos priežasties, visoms valstybėms narėms buvo nustatyta pareiga priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją. Buvo sukurta Bendradarbiavimo grupė, kuri remtų ir lengvintų valstybių narių strateginį bendradarbiavimą ir keitimąsi informacija, didintų atsakomybę ir tarpusavio pasitikėjimą. Pažymima, kad sukurtas Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklas (CSIRT), nustatyti esminių paslaugų operatoriam ir skaitmeninių paslaugų teikėjams saugumo ir pranešimo reikalavimai, valstybėms narėms nustatyta pareiga paskirti nacionalines kompetentingas institucijas, bendruosius informacinius centrus ir CSIRT, kuriems pavedamos užduotys, susijusios su tinklų ir informacinių sistemų saugumu.[114] Kadangi šia direktyva yra keliami tam tikri reikalavimai konkretiems subjektams, 4 straipsnyje bei 6 straipsnyje yra numatyti šių subjektų apibrėžimai (žr. 3 priedą). Direktyva yra nustatyta pareiga Europos Sąjungos narėms, identifikuoti jų teritorijoje

[109] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos Reglamentas (ES) Nr. 2016/1148. 5 punktas. Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=LT
[110] Dimitra Markopoulou, Vagelis Papakonstantinou ir Paul de Hert „*Computer Law & Security Review, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*“ *supra note:* 6.
[111] Europos Sąjungos kibernetinio saugumo strategija, *supra note,*: 28.
[112] Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert *supra note*, 6: 2.
[113] Reglamentas (ES) Nr. 2016/1148, *supra note*, 109: 1 straipsnis.
[114] Reglamentas (ES) Nr. 2016/1148, *supra note, 109:*

esančius esminių paslaugų sektorius ir subsektorius bei ne rečiau kaip kas du metus peržiūrėti ir prireikus atnaujinti identifikuotų esminių paslaugų operatorių sąrašą. 2019 m. Europos Komisijai atlikus valstybių narių vertinimą, buvo pastebėta, jog įpareigojimas identifikuoti esminių paslaugų operatorius beveik visose valstybėse narėse paskatino atlikti išsamų rizikos, susijusios su operatoriais, užsiimančiais ypatingos svarbos veikla ir veikiančiais šiuolaikinių tinklų ir informacinių sistemų srityse, vertinimą[115]. Direktyva įtvirtintos Bendradarbiavimo grupės padeda valstybėms narėms šiame identifikavimo procese laikytis nuoseklumo[116]. Pažymėtina, kad direktyva nereikalauja, kad valstybės narės identifikuotu skaitmeninių paslaugų teikėjus. Nemažai įmonių teikdamos savo paslaugas yra priklausomos nuo skaitmeninių paslaugų, todėl skaitmeninės paslaugos sutrikimas gali turėti įtakos pagrindinei ekonominei ir visuomeninei veiklai Sąjungoje[117]. Tačiau, reglamentu Nr. 2016/1148 buvo pasirinktos reguliuoti trys skaitmeninių paslaugų rūšys, nes vis daugėja verslų, kurie pasikliauja šiomis paslaugomis teikdami savo paslaugas. Taigi, ne visi esminių paslaugų operatoriai patenka į direktyvos Nr. 2016/1148 taikymo sritį, o būtent esminių paslaugų operatoriai apima bet kurį privatų ar viešąjį subjektą, atitinkantį konkrečius kriterijus (teikia ypatingos svarbos visuomeninės, ekonominės veiklos vykdymo paslaugą, paslauga priklauso nuo tinklų ir informacinių sistemų, incidentas turėtų didelį poveikį paslaugos teikimui) ir tuo pačiu metu įtrauktus į direktyvos Nr. 2016/11 II priedą. Visi subjektai, kuriems taikoma ši apibrėžtis, turėtų atitikti ir laikytis direktyvos saugumo ir pranešimo reikalavimų. Direktyvos II priede pateikiamas sektorių ir subsektorių sąrašas, taip pat subjektų, kurie priskiriami esminių paslaugų operatorių kategorijai, tipų sąrašas. Kai subjektas priskiriamas vienai iš priede išvardytų tipų, kitas žingsnis tenka valstybėms narėms, kurios yra atsakingos už identifikavimo procesą, kad nustatytų, kurios atskiros įmonės atitinka papildomus operatorių apibrėžimo kriterijus[118].

Kitas svarbus aspektas, kuris įtvirtintas analizuojamoje direktyvoje, tai nacionalinė tinklų ir informacinių sistemų saugumo strategija. Pagal direktyvos 7 straipsnį, kiekviena Europos Sąjungos valstybė narė turi priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją. Tinklų ir informacinių sistemų saugumo strategijoje turi būti apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės aukšto lygio tinklų ir informacinių sistemų saugumui pasiekti ir

[115] Europos Komisijos atskaita Europos Parlamentui ir Tarybai, kurioje pagal Direktyvos 2016/1148/ES dėl tinklų ir informacinių sistemų saugumo 23 straipsnio 1 dalį vertinamas požiūrio, kurio laikosi valstybės narės identifikuodamos esminių paslaugų operatorius, nuoseklumas, (2019). https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52019DC0546&from=EN
[116] Reglamentas (ES) Nr. 2016/1148, *supra note*, 109: 4 straipsnio 17 punktas.
[117] Dimitra Markopoulou, Vagelis Papakonstantinou ir Paul de Hert, *supra note*, 6: 4.
[118] *Ibid*, 3.

išlaikyti. Ji apima energetikos (elektros energijos, naftos, dujų), transporto (oro, geležinkelių, vandens, kelių), bankininkystės, finansų rinkos infrastruktūros objektus, sveikatos priežiūros, geriamo vandens tiekimo ir paskirstymo, skaitmeninės infrastruktūras sektorius bei elektroninės prekyvietės, interneto paieškos sistemos[119]. Kadangi direktyvoje yra numatyta pareiga pranešti atitinkamoms institucijoms arba CSIRT apie didelį poveikį turinčius incidentus, buvo būtina detalizuoti ir nustatyti incidento poveikio mastą. Todėl pirmiausia analizuojant incidento poveikio mastą, reikia atsižvelgti į naudotojų skaičių, kuriuos paveikė esminės paslaugos sutrikdymas, taip pat į incidento trukmę bei geografinę teritorijos aprėptį, kurią paveikė incidentas.[120] Direktyvoje yra įtvirtinta ir pareiga skaitmeninių paslaugų teikėjams nustatyti tokias technines ir organizacines priemones, kad jais remiantis būtų suvaldyta rizika, kylanti tinklų ir informacinių sistemų, kuriais jie naudojasi teikdami elektronines prekyvietės, interneto paieškos sistemos bei debesijos kompiuterijos paslaugas Europos Sąjungoje, saugumui. Be to, skaitmeninių paslaugų teikėjai turi imtis priemonių, kad būtų išvengta jų tinklų ir informacinių sistemų saugumo incidentų bei kompetentingai institucijai arba CSIRT pranešti apie incidentą, kuris turi didelį poveikį elektroninėms prekyvietėms, interneto paieškos sistemoms bei debesijos kompiuterijos paslaugoms.[121] Šių pareigų vykdymą turi užtikrinti valstybės narės. Taip pat kaip ir esminių paslaugų operatoriams, taip ir skaitmeninių paslaugų teikėjams yra nustatyti parametrai pagal kuriuos yra vertinamas incidento poveikio mastas. Analizuojant šiuos parametrus matyti, kad jie iš esmės vienodi, tačiau skaitmeninių paslaugų teikėjams vertinant ar incidentas sukėlė didelį poveikį, pridedamas dar vienas vertinimo kriterijus – tai poveikio mastas ekonominei ir visuomeninei veiklai.[122] Pabrėžtina, kad valstybės narės yra nustačiusios sankcijas, taikomas pažeidus pagal šią direktyvą priimtas nacionalines nuostatas[123].

Europos Parlamentas ir Taryba nusprendė: tam, kad būtų veiksmingai sprendžiamos tinklų ir informacinių sistemos problemos, reikia sukurti Bendradarbiavimo grupę. Ji palengvintų Europos Sąjungos narių tarpvalstybinį bendradarbiavimą, suinteresuotųjų subjektų, tiek viešojo, tiek privačiojo sektoriaus bendradarbiavimą, skatintų keitimąsi gerąja patirtimi vengiant kibernetinių krizių, užtikrintų veiksmingą informacijos teikimą, padėtų įvertinti nacionalines tinklų ir informacinių sistemų saugumo strategijas ir pan. Taip pat sukurtas Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklas (CSIRT). Be to, siekiant suvienodinti kibernetinio saugumo lygį, užtikrinti vidaus rinkos veikimą Europos Sąjungoje, valstybės narės buvo įpareigotos įkurti nacionalines

[119] Reglamentas (ES) Nr. 2016/1148, *supra note,* 109: 7 straipsnis.
[120] *Ibid*. 14 straipsnis
[121] Reglamentas (ES) Nr. 2016/1148, *op. Cit.,* 16 straipsnis.
[122] *Ibid*
[123] *Ibid,* 21 straipsnis.

kompetentingas institucijas, bendruosius informacinius centrus, kurie būtų atsakingi už tinklų ir informacinių sistemų saugumą, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu. Pažymėtina, kad ši direktyva yra taikoma tik tiems esminių paslaugų operatoriams, kurie yra identifikuoti. Identifikavimas reiškia, kad esminių paslaugų operatorius vykdo realią veiklą. Todėl, valstybėms narėms buvo nustatyta pareiga iki 2018 m. lapkričio 9 d. sudaryti sąrašą galiojančių ir įsisteigusių jų teritorijoje esminių paslaugų t. y. energetikos (elektros energijos, naftos, dujų), transporto (oro, geležinkelių, vandens, kelių), bankininkystės, finansų rinkos infrastruktūros objektų, sveikatos priežiūros, geriamo vandens tiekimo ir paskirstymo, skaitmeninės infrastruktūros sektorių operatorių ir ne rečiau kaip kas dvejus metus peržiūrėti šį sąrašą ar jį koreguoti[124]. Tam, kad esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai vykdytų direktyva įtvirtintas užduotis ir būtų įgyvendinami direktyvos tikslai, valstybės narės savo nacionalinėje teisėje privalėjo nustatyti atsakomybę už direktyvos nuostatų ar taisyklių pažeidimus. Taigi, šia direktyva yra skatinama rizikos valdymo kultūra.

Elektroninių ryšių tinklais klausytojams ir žiūrovams yra teikiamas tam tikras žiniasklaidos turinys. Elektroninių ryšių tinklai apima transliavimą belaidžiais tinklais, transliavimą palydovu, kabelinės televizijos tinklais, radijo ryšio kanalais, taip pat plačiajuosčiu internetu. Elektroninių paslaugų teikimas ryšių tinklai ir paslaugos Europos Sąjungoje buvo visiškai liberalizuoti 1998 metais, o šių tinklų ir paslaugų reguliavimas suderintas ES lygmeniu. Nuo 1998 metų ES reguliavimo sistema buvo peržiūrėta tris kartus – 2002 metais, 2009 metais ir 2018 metais.[125] 2018 m. gruodžio 11 d. buvo priimta Europos Parlamento ir Tarybos direktyva (ES) Nr. 2018/1972, kuria nustatytas Europos elektroninių ryšių kodeksas. Ši direktyva parengta apimant keturias direktyvas, t. y. 2002/19/EB, 2002/20/EB, 2002/21/EB ir 2002/22/EB, ir Europos Parlamento ir Tarybos reglamentą (EB) Nr. 1211/2009. Šios direktyvos apima priemones, taikomas elektroninių ryšių tinklų ir elektroninių ryšių paslaugų teikėjams.[126]. Šiuo Europos elektroninių ryšių kodeksu siekiama vieningai sureguliuoti telekomunikacijų, žiniasklaidos ir informacijos technologijos sektorius. Direktyva sukuriama teisinė sistema, kuri užtikrina laisvę teikti elektroninių ryšių tinklus ir paslaugas laikantis

[124] Reglamentas (ES) Nr. 2016/1148, *supra note, 109:* 16 straipsnis.
[125] Alexandre de Streel ir Hocepied, Christian, „*The EU Regulation of electronic communications networks and services*“ (P.L. Parcu and E. Brogi (eds), Research handbook on EU media law and policy, E. Elgar, forthcoming, 2021), 1. https://ssrn.com/abstract=3897368
[126] 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) Nr. 2018/1972. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32018L1972&from=LT

šioje direktyvoje nustatytų sąlygų valstybėse narėse, taip pat šioje direktyvoje atkreipiamas dėmesys ir į tinklų ir paslaugų saugumą.[127].

Europos elektroninių ryšių kodeksu nustatoma teisinė bazė, šis kodeksas nereguliuoja elektroninių ryšių tinklais transliuojamo turinio[128]. Elektroninių ryšių tinklai – tai perdavimo sistemos, įrangos rinkiniai, kurie leidžia perduoti signalus, neatsižvelgiant į perduodamos informacijos pobūdį[129]. Jie apima visų tipų tinklus, neatsižvelgiant į naudojamą technologiją, todėl toks teisinis apibrėžimas pakankamai lankstus, kad prisitaikytų prie ateities technologijų raidos[130]. Valstybės narės turi užtikrinti, kad viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių teikiamų tinklų ir paslaugų saugumui užtikrinti. Kilusią riziką atitinkantis saugumo lygis turi būti užtikrinamas naujausiais technikos laimėjimais. Direktyvoje kaip pirminė priemonė siekiant užkirsti kelią su saugumu susijusiems incidentams arba sumažinti jų poveikį naudotojams ir kitiems tinklams ir paslaugom, yra nurodomas šifravimas. Šifravimas, tai duomenų algoritminis, kriptografinis pakeitimas, kai sukuriamas pseudoatsitiktinių simbolių sekos tekstas.[131] Be to, kaip ir esminiams paslaugų operatoriams bei skaitmeninių paslaugų teikėjams, viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjai, nedelsiant privalo pranešti kompetentingai institucijai apie saugumo incidentą, kuris turėjo didelės įtakos tinklų veikimui arba paslaugų teikimui.[132] Incidento poveikio mastas nustatomas taip pat kaip ir direktyvoje Nr. 2016/1148, skaitmeninių paslaugų teikėjams, t. y. pagal naudotojų skaičių, saugumo incidento trukmę, paveiktą teritoriją, poveikį tinklo veikimui arba paslaugos teikimo mastą ir pagal poveikio ekonominei ir visuomeninei veiklai mastą.[133] Valstybių narių kompetentingoms institucijoms suteikti įgaliojimai viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjams, duoti privalomus nurodymus, kurie susiję su priemonėmis siekiant ištaisyti saugumo incidentą arba užkertant kelią tokiems incidentams.[134] Kompetentingos institucijos gali reikalauti anksčiau minėtų paslaugų teikėjų teikti informaciją susijusią su jų tinklų ir paslaugų saugumu bei leisti atlikti saugumo auditą[135].

[127] direktyva (ES) Nr. 2018/1972, *supra note*, 126: 1 straipsnis.
[128]Alexandre de Streel ir Hocepied, Christian, *supra note,* 125: 2.
[129] direktyva (ES) Nr. 2018/1972, *op. Cit.*, 2 straipsnio 1 dalis.
[130] Alexandre de Streel ir Hocepied, Christian, *supra note,* 125: 2.
[131] „Šifravimas reikšmė“ *Lietuvių žodynas*, https://www.lietuviuzodynas.lt/terminai/Sifravimas
[132] direktyva (ES) Nr. 2018/1972, *op. Cit.*, 40 straipsnis.
[133] *Ibid*, 40 straipsnis.
[134] *Ibid*, 41 straipsnis.
[135] *Ibid*

Valstybės narės Europos elektroninio ryšių kodekso nuostatas iki 2020 m. gruodžio 21 d. turėjo perkelti į nacionalinę teisę.

Užtikrinant ekonomikos pagrindinių sektorių, tokių kaip sveikatos, energetikos, finansų ir transporto tinkamą funkcionavimą, vidaus rinkos veikimą, naudojamasi sudėtingomis informacinių ir ryšių technologijų (IRT) sistemomis[136]. Šiuo metu vis daugiau piliečių, organizacijų ir verslo įmonių savo įrenginius prijungia prie ryšio tinklų ir informacinių sistemų, todėl projektuojant šiuos įrenginius būtina didelį dėmesį skirti jų saugumui ir atsparumui kibernetinėms grėsmėms. Numatoma, kad per ateinantį dešimtmetį Europos Sąjungoje bus įdiegtas didelis skaičius susietųjų skaitmeninių įrenginių. Dėl tokio išaugusio skaitmeninimo ir susietumo didėja rizika, kad visuomenė gali labiau nukentėti nuo kibernetinių grėsmių. Be to, pavieniai naudotojai, organizacijos, verslo įmonės negauna pakankamai informacijos apie IRT produktus, jų kibernetinio saugumo savybes, dėl šios priežasties mažėja pasitikėjimas skaitmeniniais sprendimais[137]. 2019 m. balandžio 17 d. Europos Parlamentas ir Taryba priėmė Kibernetinio saugumo aktą, reglamentą (ES) 2019/881, dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikino Reglamentą (ES) Nr. 526/2013. Kibernetinio saugumo aktas yra galiojantis ir šiuo metu juo vadovaujasi visos Europos Sąjungos šalys. Šiuo Kibernetinio saugumo aktu siekiama parengti išsamų priemonių rinkinį dėl valstybių narių ir įmonių pajėgumų ir parengties gerinimo, be to siekiama valstybių narių ir Sąjungos institucijų, įstaigų, organų ir agentūrų bendradarbiavimo, dalijimosi informacija ir veiksmų koordinavimo kibernetinių incidentų ir krizių atveju[138]. Reglamente 2019/881 yra įtvirtinti praplėsti bei patobulinti ENISA (Europos Sąjungos kibernetinio saugumo agentūros) tikslai, užduotys, organizaciniai aspektai, kurie atitiktų kintančią bei progresuojančią tinklų ir informacinių sistemų raidą. Be to, viena esminių įtvirtintų naujovių – yra Europos kibernetinio saugumo sertifikavimo sistema, kuri orientuota į informacijų ir ryšių technologijų produktų, paslaugų, procesų saugumą bei pasitikėjimo internetu išsaugojimą. Sertifikavimo schemos gali žymiai padidinti informacinių technologijų produktų ir paslaugų saugumą bei leisti klientams priimti pagrįstus sprendimus, didinant pasitikėjimą rinka ir mažinant sąnaudas. Valstybių narių nacionalinių sertifikavimo schemų skirtumai iki reglamento priėmimo lėmė

[136] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos Reglamentas (ES) Nr. 2019/881 (Kibernetinio saugumo aktas), 1 punktas. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019R0881&from=LT
[137] *Ibid*, 2-3 punktai.
[138] *Ibid*, 6 punktas.

susiskaidymą ir didesnes išlaidas[139]. Kibernetinio saugumo sertifikavimo sistema turi padėti didinti kibernetinio saugumo lygį Europos Sąjungoje ir Sąjungos lygmeniu suderintai taikyti Europos kibernetinio saugumo sertifikavimo schemas, tokiu būdu kuriama IRT produktų, paslaugų ir procesų bendroji rinka.

ES kibernetinio saugumo sertifikavimo schemų projektus rengia ES kibernetinio saugumo agentūra (ENISA) pagal Europos Komisijos arba ES valstybių narių prašymus. ENISA pagalbą teikia ekspertų grupė „Ad-hoc darbo grupė“, kuri glaudžiai bendradarbiauja su Europos Komisija, valstybėmis narėmis ir atitinkamomis suinteresuotomis šalimis[140]. Taigi, Europos kibernetinio saugumo sertifikavimas užtikrina, kad IRT produktai, paslaugos ir procesai būtų apsaugoti, būtų užtikrintas jų prieinamumas, autentiškumas, vientisumas ir konfidencialumas, pagal Europos Sąjungos nustatytus reikalavimus. Vienoda valstybėse narėse sertifikavimo sistema užtikrina, kad Sąjungoje nebus besidubliuojančių arba prieštaraujančių kibernetinio saugumo sertifikavimo schemų skaičius, o tai sumažina bendrojoje skaitmeninėje rinkoje veikiančių įmonių išlaidas[141]. „*Europos kibernetinio saugumo sertifikavimo schema – išsamus Sąjungos lygmeniu nustatytų taisyklių, techninių reikalavimų, standartų ir procedūrų, kurie taikomi konkrečių IRT produktų, paslaugų arba procesų sertifikavimui arba atitikties vertinimui, rinkinys*“[142]. Kibernetinio saugumo sertifikavimo schemų yra ne viena, kibernetinio saugumo sertifikatai bus naudojami kaip atskiros sudedamosios dalys atskiriems sprendimams, sistemoms (dalims) ir specifinėms technologijoms sertifikuoti. Pavyzdžiui viena schema apima IRT produktus, kita apima debesijos paslaugas, o trečioji – 5G tinklus[143]. Reglamento 51 straipsnyje numatyti Europos kibernetinio saugumo sertifikavimo schemų saugumo tikslai[144], kurie yra naudingi:

1. *piliečiams ir galutiniams naudotojams* – priimti teisinga informacija pagrįstus sprendimus dėl gyvenime dažnai naudojamų produktų ir paslaugų pirkimo. Pavyzdžiui: pilietis, kuris svarsto dėl išmaniojo įrenginio įsigijimo galės ieškoti informacijos ES kibernetinio saugumo agentūros Europos

[139] Annegret Bendiek ir Eva Pander Maat „The EU‘s Regulatory Approach to Cyber-security“ *German institute for International and Security Affairs* (2019), 12. https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf

[140] „What are EU cybersecurity certification schemes?“ *European Union Agency for cybersecurity*. https://www.enisa.europa.eu/topics/standards/certification/certification-schemes-and-cabs/certification-schemes-and-cabs-faq

[141] Reglamentas (ES) Nr. 2019/881 *supra note:* 136, 69 punktas.

[142] *Ibid*, 2 straipsnio 9 dalis.

[143] ”Certification Schemes and CABs – FAQ“ *European Union Agency for cybersecurity ENISA* https://www.enisa.europa.eu/topics/standards/certification/certification-schemes-and-cabs/certification-schemes-and-cabs-faq

[144] Reglamentas (ES) Nr. 2019/881 *supra note:* 136, 51 straipsnis

kibernetinio saugumo sertifikavimo svetainėje ir ten surasti tam tikrą įrenginio modelį, kuris buvo sertifikuotas pagal kibernetinio saugumo reikalavimus[145];

2. *produktų ir paslaugų pardavėjams ir teikėjams* – sutaupys lėšų ir laiko, nes bus vienintelis Europos sertifikato išdavimo procesas, o sertifikatas galios visose valstybėse narėse[146];

3. *valdžios įstaigoms* – bus lengviau priimti teisinga informacija pagrįstus sprendimus dėl pirkimo[147].

Kibernetinio saugumo sertifikavimo schemos yra dvejopos, t. y. Europos lygmeniu ir nacionaliniu, kai išsamias taisykles, techninius reikalavimus, standartus ir procedūras, taikomas IRT produktams, keliamiems pagal Europos kibernetinio saugumo sertifikavimo schemą, priima būtent nacionalinės valdžios institucijos. 2021 m. birželio 17 d. Lietuvos Respublikos Seimui priėmus Kibernetinio saugumo įstatymo pataisas, Lietuva atliko reikiamus teisinius žingsnius įgyvendinama Europos Sąjungos Kibernetinio saugumo akto nuostatas ir kartu su kitomis Europos Sąjungos valstybėmis nuo 2021 m. birželio 28 d. sukūrė bendrą erdvę, kurioje galioja Europos kibernetinio saugumo sertifikatai[148]. Lietuvoje bazinio ir vidutinio lygio sertifikatus išduoda nacionalinės atitikties vertinimo įstaigos (apibrėžtos 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamente (EB) Nr. 765/2008, nustatančiame su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinančiame reglamentą (EEB) Nr. 339/93), Lietuvoje tai yra Nacionalinis akreditacijos biuras[149]. Aukščiausio lygio sertifikatus išduoda nacionalinė kibernetinio saugumo sertifikavimo institucija, t. y. Nacionalinis kibernetinio saugumo centras[150]. Kibernetinio saugumo sertifikavimo sistema užtikrina, kad IRT duomenys apsaugoti nuo neteisėto atskleidimo, sunaikinimo, pakeitimo ir pan., prie tam tikrų duomenų gali prieiti tik specifiniai subjektai, t. y. tik turintys prieigos teisę ir tik prie tokio duomenų kiekio, kurie numatyti jų prieigų teisėse, nėra žinomų pažeidžiamumo spragų bei IRT yra aprūpintos saugaus naujinimo mechanizmais.[151] Kai įvykdoma kibernetinio saugumo sertifikavimo schema, įgyvendinami tikslai, užduotys, techniniai reikalavimai yra išduodamas Europos kibernetinio saugumo sertifikatas. Tai yra dokumentas, kuriuo patvirtinamas IRT

---

[145] „Klausimai ir atsakymai. ES kibernetinis saugumas“ *Europos Komisija (*2019 m. birželio 26 d.) https://ec.europa.eu/commission/presscorner/detail/lt/QANDA_19_3369

[146] „Klausimai ir atsakymai. ES kibernetinis saugumas“ *Europos Komisija*, *supra note:* 143.

[147] *Ibid*

[148] „NKSC vykdys nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas“ *Nacionalinis kibernetinio saugumo centras* (2021), https://www.nksc.lt/naujienos/nksc_vykdys_nacionalines_kibernetinio_saugumo_sert.html

[149] Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 6, 8, 9, 13 straipsnių, V skyriaus pavadinimo, priedo pakeitimo ir įstatymo papildymo 17 straipsniu ir VI skyriumi įstatymo ir Lietuvos Respublikos administracinių nusižengimų kodekso papildymo $480^1$ straipsniu ir 589 straipsnio bei priedo pakeitimo įstatymo projektų aiškinamasis raštas, 1.1 papunktis.

[150] Nacionalinis kibernetinio saugumo centras, *op. Cit*.

[151] European Union Agency for cybersecurity, *supra note,* 143.

produkto, paslaugos ar proceso atitikimas konkretiems Europos kibernetinio saugumo sertifikavimo schemoje nustatytiems reikalavimams.[152] IRT sprendimų vartotojai kibernetinio saugumo sertifikatus gali laikyti įrodymu, kad konkretus sprendimas atitinka apibrėžtus saugumo reikalavimus[153].

Reglamente 2019/881, numatyti ir Europos kibernetinio saugumo sertifikavimo schemų saugumo užtikrinimo lygiai, kuriais siekiama patvirtinti, kad atitinkamas IRT produktas, procesas ar paslauga atitinka kibernetinio saugumo sertifikavimo schemos tam tikrus saugumo reikalavimus. Europos kibernetinio saugumo sertifikatas patvirtina vieną iš saugumo užtikrinimo lygių (žr. 4 priedą)[154] Saugumo užtikrinimo lygis atitinka IRT produkto, paslaugos ir proceso rizikos lygį, kuris nustatomas atsižvelgiant į incidento tikimybę ir poveikį[155]. Kiekvienas lygis turi savo reikalavimus bei funkcines galimybes, todėl nuo saugumo užtikrinimo lygio priklauso ir atliekamas vertinimas, jo griežtumas bei išsamumas[156]. Gali būti atliekamas savarankiškas vertinimas, taikomas tik nedidelės rizikos IRT produktams, paslaugoms ir procesams, t. y., kurie atitinka bazinį saugumo užtikrinimo lygį [157]. Programinės įrangos tiekėjams kibernetinio saugumo sertifikavimas yra sudėtingas procesas reikalaujantis papildomų finansinių išteklių. Dėl sertifikavimo gali vėluoti naujų sistemų paleidimas, o tai turi didelį ekonominį poveikį. Be to, nors ir plačiai yra kalbama apie būtiną kibernetinio saugumo užtikrinimą, tačiau ne visos įmonės, bendrovės ar įstaigos suvokia saugumo ir privatumo funkcijų reikalingumą[158]. Projekte „Kurk Lietuvai“ buvo atliktos Lietuvos smulkaus ir vidutinio verslo įmonių apklausos dėl viešo liudijimo ir/ar dokumento parodančio, kad įmonės kibernetinio saugumo lygis yra įvertintas ir ji yra įsidiegusi tam tikrą standartą atitinkančias kibernetinio saugumo priemones. Rezultatai parodė, kad 37 proc. smulkaus ir vidutinio verslo įmonių vadovų sutinka, kad kibernetinio saugumo įvertinimo sertifikatas atneštų naudos jų įmonei ir net 78 proc. įmonių įžvelgia tokio sertifikato naudą bei sutiktų mokėti už tokią paslaugą[159]. Kibernetinio saugumo sertifikavimas yra savanoriškas, tačiau Europos Komisija iki 2023 m. gruodžio 31 d. atliks vertinimą dėl priimtų Europos kibernetinio saugumo sertifikavimo schemų veiksmingumo ir spręs klausimą, ar nereikėtų nustatyti privalomo sertifikavimo konkretiems sektoriams. Deja, bet kibernetinio saugumo aktu neskubama

[152] Reglamentas (ES) Nr. 2019/881 *supra note,* 136: 51 straipsnis.
[153] European Union Agency for cybersecurity, *supra note,* 142.
[154] Reglamentas (ES) Nr. 2019/881 *op. Cit*., 86 punktas.
[155] *Ibid*, 52 straipsnis 1 dalis.
[156] *Ibid*, 52 straipsnio 3 dalis.
[157] *Ibid*, 53 straipsnio 1, 2 dalys.
[158] J. L. Hernandez-Ramos, S. N. Matheu ir A. Skarmeta, "*The Challenges of Software Cybersecurity Certification"(*2021), 1. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9336084
[159] Justas Kidykas, Rūta Beinoriūtė ir Gabrielė Bilevičiūtė „Pasiūlymai dėl smulkaus ir vidutinio verslo kibernetinio saugumo brandos kėlimo Lietuvoje“ *„Kurk Lietuvai“ projektas*, (2020), 13. http://kurklt.lt/wp-content/uploads/2020/03/Rekomendacijos-KAM-ir-NKSC-Kurk-Lietuvai.pdf

įtvirtinti privalomos kibernetinio saugumo sertifikavimo sistemos. Pažymėtina, kad plati sertifikavimo sistema suteiktų ES stipresnes pozicijas siekti pasaulinių IRT produktų saugumo normų, be to privalomi kibernetinio saugumo standartai turi didesnį potencialą[160].

Europos kompetentingoms institucijoms reiškiant susirūpinimą dėl padidėjusios kibernetinės kenkimo veiklos, buvo priimti spendimai labiau saugoti Sąjungos, jos valstybių narių ir piliečių saugumą nuo kibernetinių grėsmių, aiškiai parodyti galimą atsaką į kibernetinę kenkimo veiklą, kuri įtakotų galimų agresorių elgesį kibernetinėje erdvėje. Taip pat griežtai pasmerkti piktavališką informacinių ir ryšių technologijų naudojimą, stiprinti kovos su už Sąjungos ribų ateinančiomis grėsmėmis pajėgumus.[161] 2019 m. gegužės 17 d. Taryba priėmė sprendimą (BUSP) Nr. 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais. Šis sprendimas yra diplomatinio atsako sistema, kuri demonstruoja bendrus, koordinuotus, diplomatinius atsakomuosius veiksmus, nesusijusius su ginkluotu pasipriešinimu, su rimtas kibernetinius išpuoliais, t. y. kad užpuolikai būtų įtikinti susilaikyti nuo kenkėjiškų veiksmų prieš Europos Sąjungą[162].

(BUSP) sprendimo nuostatos yra orientuotos būtent į pasikėsinimo stadijoje esančius kibernetinius išpuolius ir į jau egzistuojančius kibernetinius išpuolius, dėl kurių kyla išorinė grėsmė Sąjungos arba jos valstybių narių saugumui[163]. Kibernetinių išpuolių veiksmai susiję su elektroninėmis nusikalstamomis veikomis, pavyzdžiui: prieiga prie informacinių sistemų, įsikišimu į informacinę sistemą, į duomenis arba duomenų perėmimu ir t.t.[164]. Pagal sprendimą (BUSP), kiekviena valstybė narė yra laisva pati spręsti dėl kibernetinių išpuolių priskyrimo trečiajai valstybei[165] ir pati sprendžia ar ji pritars kitų ES valstybių skelbiamiems (per diplomatiją ar per žiniasklaidą) priskyrimams, todėl tai sumažina kibernetinių sankcijų poveikį[166]. Kibernetinio išpuolio priskyrimas trečiajai valstybei yra pagrindinė kibernetinių išpuolių tyrimų problema ir yra didelis iššūkis ES kibernetinei diplomatijai ir jos kibernetinių sankcijų režimui. ES valstybės narės nelinkusios dalintis jautria žvalgybos informacija ES lygmeniu, nes tai leidžia susidaryti

[160] Annegret Bendiek ir Eva Pander Maat, *supra note,* 8: 12
[161] 2019 m. gegužės 17 d. Tarybos sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019D0797&qid=1629630537371&from=EN
[162] Annegret Bendiek ir Matthias Schulze „*Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW*“ (2021), https://www.swp-berlin.org/en/publication/attribution-a-major-challenge-for-eu-cyber-sanctions
[163] *Ibid*, 1 straipsnio 1 dalis.
[164] sprendimas (BUSP) 2019/797, *op. Cit.*, 1 straipsnis.
[165] *Ibid*, 9 punktas.
[166] Annegret Bendiek ir Matthias Schulze, *supra note*, 160: 9.

konsekvenciją apie nacionalinius kibernetinės gynybos pajėgumus. Dalijimasis žvalgybos informacija gali pakenkti valstybės šaltiniams ir prieigai prie įslaptintos informacijos. Pažymėtina, kad suskaidytas priskyrimo procesas silpnina ES kibernetinės diplomatijos patikimumą, teisėtumą ir veiksmingumą. Darnos trūkumas, kai kalbama apie priemones, yra viena iš pasekmių: Rusijos žvalgybos pareigūnams, kuriems 2020 m. buvo taikytos kibernetinės sankcijos – draudimai keliauti ir įšaldytas turtas, jau buvo taikytos tos pačios ribojančios priemonės pagal skirtingą ES sankcijų režimą prieš keletą metų. Todėl priemonės dubliavosi ir neturėjo jokio papildomo poveikio[167]. Be to, neskaitant šio žingsnio pertekliaus, kyla abejonių, kiek kelionių apribojimai ir įšaldytos sąskaitos iš tikrųjų turi atgrasantį poveikį agresoriams, ar galiausiai tai yra tik simbolinė politika. Be to, kibernetinių sankcijų veiksmingumas ir teisėtumas nukenčia, jei valstybių narių vyriausybės neremia kibernetinių atakų vykdytojų viešo įvardijimo[168].

Sprendimo (BUSP) 1 straipsnio 4 dalyje taip pat išvardinti išpuoliai, kuriais daromas poveikis informacinėms sistemoms. Kaip kibernetiniai išpuoliai, kurie kelia grėsmę Sąjungai, įvardijami ir išpuoliai prieš Sąjungos institucijas, įstaigas, organus ir agentūras, jos delegacijas trečiosiose valstybėse arba tarptautinėse organizacijose, Sąjungos bendrosios saugumo ir gynybos politikos operacijas ir misijas ir jos specialiuosius įgaliotinius[169]. Sprendžiant klausimą, ar kibernetinis išpuolis daro reikšmingą poveikį, pirmiausia analizuojamas kibernetinio išpuolio mastas, intensyvumas, poveikis arba juo padaryto ardomojo poveikio sunkumas, ekonominei ir visuomeninei veiklai, esminėms paslaugoms, esminėms valstybės funkcijoms, viešajai tvarkai ar visuomenės saugumui. Taip pat, analizuojamas fizinių ar juridinių asmenų, subjektų ar įstaigų skaičius, kurie pajautė poveikį, susijusių valstybių narių skaičius, padaryta ekonominė žala (pavyzdžiui, didelio masto lėšų, ekonominių išteklių arba intelektinės nuosavybės vagystė). Be to, analizuojama ir vykdytojo gauta ekonominė nauda sau arba kitiems, pavogtų duomenų kiekis, pobūdis, duomenų pažeidimų mastas, arba komerciškai jautrių duomenų, prie kurių gauta prieiga, pobūdis[170]. Pažymėtina, kad šio Tarybos sprendimo nuostatos yra taikomos būtent reikšmingą poveikį darantiems kibernetiniams išpuoliams, todėl yra būtina nustatyti įvykdyto išpuolio reikšmingą poveikį, kuris atitiktų aptartus kriterijus. Siekiant užkardyti ir pasmerkti piktavališkus veiksmus, numatyta, kad valstybės narės turi imtis priemonių, kad į jų teritorijas atvykti arba vykti per jas tranzitu negalėtų fiziniai asmenys, kurie atsakingi už kibernetinius išpuolius arba mėginimus įvykdyti kibernetinius išpuolius, taip pat asmenys

[167] Stefan Soesanto "Europe Has No Strategy on CyberSanctions" (2020) https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions
[168] Annegret Bendiek ir Matthias Schulze, *supra note*, 160: 9.
[169] sprendimas (BUSP) 2019/797, *supra note,* 161: 1 straipsnis.
[170] sprendimas (BUSP) 2019/797, *supra note,* 161: 3 straipsnis.

teikiantys finansinę, techninę ar materialinę paramą arba kitaip susiję su kibernetiniais išpuoliais arba pasikėsinimais įvykdyti kibernetinius išpuolius, įskaitant planavimą, rengimą, dalyvavimą, vadovavimą, pagalbos teikimą, skatinimą, sąlygų sudarymą, veiksmais arba neveikimu[171]. 2016 m. prasidėjo kibernetinė ataka „Cloud Hopper 2016“, kuri leido įsilaužti į debesų valdymo infrastruktūras[172]. Buvo paveiktos Vokietijos įmonės[173], buvo pažeista 40 JAV karinio jūrų laivyno kompiuterių, pavogta 100 000 karinio jūrų laivyno darbuotojų asmeninė informacija[174]. 2018 m. gruodį JAV vyriausybė viešai priskyrė ataką grupei „APT 10“, kuri yra susijusi su Kinijos valstybės saugumo ministerijos Tiandzino valstybinio saugumo biuru. JAV teisingumo departamentas paskelbė kaltinimus dviem Kinijos piliečiams[175]. 2019 m. Europos Sąjunga nusprendė pradėti politinį atsaką pagal Tarybos analizuojamą sprendimą (BUSP) prieš „Cloud Hopper 2016“ išpuolį. Tuometinė Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai Federica Mogherini 2019 m. balandžio 12 d. pareiškė, kad kenkėjiška kibernetinė veikla, kenkianti Sąjungos vientisumui, saugumui ir ekonominiam konkurencingumui ir susijusi su intelektinės nuosavybės vagystėmis, nebus toleruojama. Pranešimas buvo skirtas „APT 10“ grupei[176], tačiau tik po metų, 2020 m. liepos mėn. pabaigoje, Taryba žengė žingsnį toliau, priimdama įgyvendinimo reglamentus 2020/1125[177] ir 2020/1744[178], kuriais 2020 m. lapkričio mėn. buvo įvestos sankcijos kaltininkams, t. y. ribojamosios priemonės, kurios pagrįstos sprendimo (BUSP) 4 straipsniu. Žinoma, šis įpareigojimas nėra besąlygiškas, valstybės narės gali įleisti į teritoriją savo piliečius, taip pat kai reikia laikytis tarptautinio įsipareigojimo, kai kelionės yra pateisinamos dėl kitų priežasčių (žr. 5 priedą).

Kovojant su reikšminga neigiamą poveikį darančiais kibernetiniais išpuoliais, nustatyta, kad įšaldomos visos lėšos ir ekonominiai ištekliai fiziniams ar juridiniams asmenims, subjektams ar organizacijoms. Visi šie objektai yra atsakingi už kibernetinius išpuolius arba mėginimus įvykdyti

---

[171] sprendimas (BUSP) 2019/797, *supra note, 161:* 4 straipsnis.
[172] Annegret Bendiek ir Matthias Schulze, *supra note*, 160: 26 puslapis.
[173] „German security office warned German firms about Chinese hacking – report“ *Reauters* (2018) https://www.reuters.com/article/uk-germany-security-idUKKBN1OI0HS
[174] „Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information“ *Jungtinių Valstijų Teisingumo departamento Viešųjų reikalų ministerija,* (2018) https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[175] *Ibid*
[176] „Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace“ *European Council Council of the European Union* (2019 m. gegužės 6 d.) https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/
[177] 2020 m. liepos 30 d. Tarybos įgyvendinimo reglamentas (ES) 2020/1125, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32020R1125&from=EN
[178] *Ibid*

kibernetinius išpuolius bei teikiantys finansinę, techninę ar materialinę paramą arba kitaip susiję su kibernetiniais išpuoliais arba pasikėsinimais įvykdyti kibernetinius išpuolius, įskaitant planavimą, rengimą, dalyvavimą, vadovavimą, pagalbos teikimą, skatinimą, sąlygų sudarymą, veiksmais arba neveikimu[179]. 2015 m. įvyko išpuolis prieš Vokietijos Federalinį Parlamentą (*Deutscher Bundestag*), kuris buvo nukreiptas į Parlamento informacinę sistemą ir sutrikdė jos veikimą keletą dienų. Buvo pavogta daug duomenų ir padarytas poveikis kelių parlamento narių bei kanclerės Angelos Merkel elektroninio pašto paskyroms[180]. 2020 m. spalio 22 d. Europos Sąjungos Taryba priėmė sankcijas Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) 85-tajam pagrindiniam specialiųjų tarnybų centrui (GTsSS) ir jo karinės žvalgybos pareigūnams Dmitrijui Badinui ir Igoriui Kostjukovui, įgyvendindama reglamentą (ES) 2020/1536[181]. Buvo paskirtos ekonominės sankcijos pagal reglamento (ES) 2019/796 3 straipsnį[182] ir atvykimo apribojimai pagal Tarybos sprendimo (BUSP) 2019/797 4 straipsnį[183]. Tarybos įgyvendinimo reglamente 2020/1536 teigiama, kad Dmitrijus Badinas kaip karinės žvalgybos pareigūnas dalyvavo kibernetinėje atakoje, kuri turėjo reikšmingą poveikį Vokietijos Federaliniam Parlamentui (*Deutscher Bundestag*). Igoris Kostjukovas būdamas Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) vadovas, buvo atsakingas už GTsSS įvykdytus reikšmingą poveikį turinčius kibernetinius išpuolius, kurie kėlė išorinę grėsmę Sąjungai ar jos valstybėms narėms. Taip pat, GTsSS karinės žvalgybos pareigūnai dalyvavo vykdant kibernetinį išpuolį prieš Vokietijos Federalinį Parlamentą (*Deutscher Bundestag*) ir 2018 m. balandžio mėn.[184] Nyderlanduose mėginant įvykdyti kibernetinį išpuolį, kuriuo buvo siekiama įsilaužti į Cheminio ginklo uždraudimo organizacijos (OPCW) belaidį tinklą[185]. Nustatyta, kad nuo (BUSP) 2019/797 reguliavimo galima nukrypti, tai yra valstybių narių kompetentingos institucijos gali nutraukti tam tikrų lėšų arba ekonominių išteklių įšaldymą arba leisti jais naudotis tokiomis sąlygomis, kurios yra tinkamos (žr. 6 priedą).

Taigi, daugėjant įvairaus masto, trukmės, intensyvumo, sudėtingumo rafinuotumo ir poveikio kibernetiniams išpuoliams, priimtos tam tikros priemonės, kurios padeda apsaugoti Europos Sąjungą,

---

[179] sprendimas (BUSP) 2019/797, *supra note,* 161: 5 straipsnio 1 dalis.
[180] 2020 m. spalio 22 d. Tarybos įgyvendinimo reglamentas (ES) 2020/1536, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32020R1536&from=EN
[181] *Ibid*
[182] 2019 m. gegužės 17 d. Tarybos reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32019R0796&from=EN#d1e486-1-1
[183] sprendimas (BUSP) 2019/797, *supra note,* 161: 4 straipsnio 6 dalis.
[184] reglamentas (ES) 2020/1536, *op. Cit*.
[185] reglamentas (ES) 2020/1125, *supra note*, 177.

jos valstybes nares ir piliečius nuo kibernetinių grėsmių. Šių ribojamųjų priemonių tikslas ne tik apsisaugoti nuo kibernetinės kenkimo veiklos, bet ir vykdyti prevencinę funkciją, kuri atgrasytų vykdyti kibernetinę kenkimo veiklą Europos Sąjungoje. Turto įšaldymas asmenims, susijusiems su kibernetiniais išpuoliais, kaip ribojamoji priemonė taip pat yra įtvirtinta 2019 m. gegužės 17 d. Tarybos reglamente (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms 3 straipsnyje. Svarbu pabrėžti, kad šios ribojamosios priemonės taikomos ne bet kokiems kibernetiniams išpuoliams, o būtent tokiems, kurie turi reikšmingą poveikį. Išanalizavus (BUSP) sprendimą matyti, kad Taryba siekdama pasmerkti ir eliminuoti kibernetinius išpuolius ir numatydama taikymo išlygas, laikosi humaniškumo principo, taip pat užtikrina tarptautinių įsipareigojimų įgyvendinimą.

2019 m. gegužės 17 d. buvo priimtas Tarybos reglamentas (ES) 2019/796, kuris papildė Tarybos sprendimą (BUSP) 2019/797 ir užtikrino suderintą valstybių narių kibernetinio saugumo politikos įgyvendinimą. Fiziniams ir juridiniams asmenims, organizacijoms ir subjektams, kuriems taikomos ribojamosios priemonės, turi būti įtrauktos į sąrašus, kurie turi būti skelbiami viešai. Analizuojant šį reglamentą matyti, kad jame įtvirtintos nuostatos beveik identiškos Tarybos sprendimui 2019/797. Reglamentu nustatyta fizinių, juridinių asmenų, subjektų ir organizacijų, kuriems lėšos ar ekonominiai ištekliai pagal Tarybos sprendimą 2019/797 ir šį reglamentą turi būti įšaldyti paskelbimo schema. Pagal šį reglamentą valstybės narės ir Europos Komisija turėtų dalintis su šiuo reglamentu ir Tarybos sprendimu 2019/797 susijusia svarbia informacija, taip pat valstybėms narėms numatyta pareiga nustatyti taisykles dėl sankcijų taikymo už šio reglamento nuostatų pažeidimus ir užtikrinti jų įgyvendinimą[186].

Analizuojant kibernetinio saugumo reglamentavimą, ne ką mažiau svarbus ir 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/821, nustatantis Sąjungos dvejopo naudojimo prekių eksporto, persiuntimo, susijusių tarpininkavimo paslaugų, techninės pagalbos ir tranzito kontrolės režimą. Šis reglamentas reikšmingas tuo, kad nustato kibernetinio stebėjimo prekių eksporto kontrolę. „*Kibernetinio stebėjimo prekės – dvejopo naudojimo prekės, specialiai sukurtos tam, kad būtų galima slaptai stebėti fizinius asmenis stebint, išgaunant, renkant ar analizuojant duomenis iš informacinių ir telekomunikacijų sistemų*“.[187] Siekiant užkirsti sunkius žmogaus teisių arba tarptautinės humanitarinės teisės pažeidimus, tam, kad asmenys, kurie atsakingi

[186] Reglamentas (ES) 2019/796, *supra note*,182.
[187] 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/821, nustatantis Sąjungos dvejopo naudojimo prekių eksporto, persiuntimo, susijusių tarpininkavimo paslaugų, techninės pagalbos ir tranzito kontrolės režimą.

ar tiesiog prisideda prie tokių pažeidimų, nenaudotų į sąrašą neįtrauktų iš Sąjungos muitų teritorijos eksportuotas kibernetinio stebėjimo prekes, nuspręsta kontroliuoti tokių prekių eksportą[188]. Pažymėtina, kad 1996 m. buvo sudarytas Vasenaro (*Wassenaar*) susitarimas, kuris apima 42 valstybes. Tai savanoriška eksporto kontrolė, kuria reguliuojamas įprastinių ginklų ir dvejopo naudojimo prekių bei technologijų perdavimas, tokiu būdų užkertant kelią destabilizuojamoms sankaupoms. Dalyvaujančios valstybės, vykdydamos savo nacionalinę politiką, siekia užtikrinti, kad šių daiktų perdavimas neprisidėtų prie karinių pajėgumų[189]. Susitarimo valstybės narės turi pranešti apie savo sprendimus eksportuoti išvardytas prekes. Jei viena valstybė narė atsisako eksportuoti į sąrašą įtrauktą prekę, kita dalyvaujanti valstybė vis tiek gali patvirtinti eksportą[190]. Taigi, dar iki reglamento (ES) 2021/821 priėmimo buvo reguliuojama dvejopo naudojimo prekių bei technologijų eksporto kontrolė, tačiau Vasenaro (*Wassenaar*) susitarimo šalys už sprendimą perduoti ar neleisti perduoti bet kurį daiktą buvo atsakingos asmeniškai[191]. Taip buvo bandoma sumažinti riziką, kai kibernetinio stebėjimo prekės specialiai projektuojamos tam, kad pavyktų įsilaužti į informacines ir telekomunikacijų sistemas arba atlikti išsamų duomenų patikrinimą. Tikslas tas, kad būtų galima slapta stebėti fizinius asmenis, išgauti, rinkti ar analizuoti duomenis, taip pat ir biometrinius duomenis iš sistemų.[192]

Analizuojant reglamentą Nr. 2021/821 kibernetinio saugumo kontekste, šis reglamentas ypatingas tuo, kad nustato sąraše neišvardytoms kibernetinio stebėjimo prekėms būtiną eksporto leidimą. Leidimas yra reikalingas ne visoms kibernetinio stebėjimo prekėms, o būtent toms, kurios gali būti naudojamos vidaus represijoms ir (arba) sunkiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti[193]. Europos Tarybos pirmininkas pranešime spaudai teigė, kad naujosiomis taisyklėmis žmogaus teisėms suteikiama tokia svarba, kokios jos nusipelno. Griežta ES dvejopo naudojimo prekių kontrolė leis užkirsti kelią žmogaus teisių pažeidimams ir piktnaudžiavimo atvejams, kartu neatsiliekant nuo naujausių technologinių pokyčių[194]. Taigi, eksportuotojas žinodamas, kad eksportuoja neišvardintas sąraše kibernetinio stebėjimo prekes, kurias

---

[188] Europos Parlamento ir Tarybos reglamentas (ES) 2021/821, *supra note, 187.*
[189] „About us“ *The Wassenaar arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies* https://www.wassenaar.org/about-us/
[190] Roland Klein „*Trimming Pegasus Wings: International Export Control Law and Cyberweapons*“ (2021). Trimming Pegasus' Wings (vifa-recht.de)
[191] „Wassenaar arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies“ *Bureau of Nonproliferation Department of State* *https://1997-2001.state.gov/global/arms/np/mtcr/000322_wassenaar.html*
[192] Reglamentas (ES) 2021/821, *supra note,* 187.
[193] *Ibid*, 5 straipsnis.
[194] „Prekyba dvejopo naudojimo prekėmis: priimtos naujos ES taisyklės“ *Europos Vadovų Taryba Europos Sąjungos Taryba* (2021 m. gegužės 10 d.). https://www.consilium.europa.eu/lt/press/press-releases/2021/05/10/trade-of-dual-use-items-new-eu-rules-adopted/

ketinama naudoti, kuriam nors iš anksčiau išvardintų tikslų, t. y. vidaus represijoms ir (arba) sunkiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti, turi apie tai pranešti valstybės narės kompetentingai institucijai. Lietuvos Respublikos muitinė yra viena iš svarbiausių grandžių kontroliuojant strateginių ir dvejopos paskirties prekių judėjimą[195].

2022 m. sausio 25 d. Lietuvos Respublikos muitinė informavo, kad Vilniaus muitininkai sulaikė į Baltarusiją eksportuojamą dvigubos paskirties prekių siuntą. Iš Lietuvos be būtinų dokumentų buvo bandoma išvežti du serverius, kurių informacijos saugumo sistemos suprojektuotos arba buvo modifikuotos taip, kad įrangą būtų galima naudoti kriptografijai, t. y. informacijos šifravimui. Pažymėtina, kad Baltarusijos Respublikai taikomos ekonominės sankcijos ir į minėtą šalį draudžiama be atitinkamų leidimų iš Europos Sąjungos eksportuoti dvejopos paskirties prekes (technologijas, programinę įrangą ir pan.), kurias galima pritaikyti kariniams ar žvalgybiniams tikslams[196]. Įsigaliojus Europos Parlamento ir Tarybos reglamentui (ES) 2021/821, Lietuvos Respublikos muitinės pareigūnai sustiprino kontrolės priemones eksportuojamoms kibernetinio stebėjimo prekėms, skirtoms rinkti ir apdoroti duomenis iš informacinių ir telekomunikacinių sistemų – vykdyti žvalgybą, rinkti ir apdoroti informaciją[197]. Lietuvos Respublikos baudžiamajame kodekse ir administraciniame kodekse numatyta baudžiamoji ir administracinė atsakomybė asmenims už strateginių ir dvejopos paskirties prekių kontrabandą − gabenimą per Lietuvos Respublikos valstybės sieną nepateikiant jų muitinės kontrolei ar kitaip išvengiant šios kontrolės arba gabenant be licencijos[198].

Taigi, Europos Parlamento ir Tarybos reglamentu (ES) 2021/821 stiprinamas dvejopo naudojimo technologijų kontrolė ir valstybių narių bei Komisijos veiklos koordinavimas. Kadangi kibernetinio stebėjimo prekės kelia riziką, kad jos bus panaudotos vidaus represijoms arba sunkiems žmogaus teisių ir humanitarinės teisės pažeidimams, būtina stiprinti veiksmingą kibernetinio stebėjimo prekių eksporto kontrolę. Ši kontrolė turi būti vieninga daugiašaliu lygmeniu, todėl valstybės narės yra įpareigotos dalintis tiek tarpusavyje, tiek su Europos Komisija duomenimis, susijusiais su kibernetinio stebėjimo prekių technologijomis bei jų plėtra. Pažymėtina, kad 2022 m.

---

[195] „Strateginių ir dvejopos paskirties prekių licencijavimas ir kontrolė“ *Lietuvos Respublikos muitinė* (2021 m. lapkričio 15 d.) https://lrmuitine.lt/web/guest/verslui/apribojimai/strateginesprekes

[196] „Į Baltarusiją neleista eksportuoti dvigubos paskirties įrangos, pritaikytos informacijos šifravimui“, *Lietuvos Respublikos Muitinė,* 2022 m. sausio 25 d. https://lrmuitine.lt/web/guest/naujienos/aktualijos/aktualija?p_p_id=EXT_WPLISTALLNEWS&p_p_lifecycle=0&_EXT_WPLISTALLNEWS_obj_id=090004d28015ca9f

[197] *Ibid*

[198] „Strateginių ir dvejopos paskirties prekių licencijavimas ir kontrolė“ *Lietuvos Respublikos muitinė* (2021) https://lrmuitine.lt/web/guest/verslui/apribojimai/strateginesprekes

sausio 6 d. Europos Komisija paskelbė reglamentą (ES) 2022/1, atnaujinantį reglamento (ES) 2021/821 I priede pateiktą dvejopo naudojimo prekių sąrašą. Taigi, eksportuotojas norintis išvežti iš vienos valstybės narės į trečiąją šalį kibernetinio stebėjimo prekę, kuri nėra įvardinta sąraše ir kuri gali būti panaudota vidaus represijoms ir (arba) sunkiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti, turi pranešti valstybės narės kompetentingai institucijai. Tuomet kompetentinga institucija nusprendžia, ar būtent šiai eksportuojamai prekei reikalingas leidimas. Kompetentinga institucija nustačiusi, kad konkrečiai prekei yra reikalingas leidimas, informuoja savo muitinę, kitas atitinkamas nacionalines institucijas bei Europos Sąjungos valstybes nares. Kadangi tokia vykdoma kontrolė daro poveikį prekybai su trečiosiomis valstybėmis, todėl numatyta siekti plėtoti dialogą ir bendradarbiavimą su tomis šalimis bei siekti sudaryti vienodas sąlygas visoms pasaulio valstybėms, taip didinant tarptautinį saugumą[199].

Stebint besikeičiančią kibernetinę erdvę ir pastebint tiek privatiems, tiek viešiems subjektams kylančią kibernetinio saugumo riziką, Europos Sąjunga dar 1995 m. priėmė direktyvą, susijusią su asmens duomenų apsauga. Kaip anksčiau minėta kibernetinis saugumas glaudžiai susijęs su duomenų apsauga, tai du tarpusavyje koreliuojantys objektai. Europos Sąjunga priimdama reglamentus ir direktyvas išvystė bei iki šios dienos vysto efektyviai veikiančią teisinę sistemą. Europos Sąjungoje egzistuoja stipri kibernetinį saugumą užtikrinanti sistema. Veikia institucijos, kurios užtikrina kibernetinį saugumą bei padeda valstybėms narėms, teikdamos ataskaitas bei rekomendacijas. Europos Parlamentas ir Taryba nustatydami technines ir organizacines priemones, palaiko valstybių narių bazinį kibernetinio saugumo lygį bei skatina atkreipti dėmesį į kibernetinio saugumo lygį šalyje. Europos Sąjungoje esančių teisės aktų analizė išryškino įvykusio kibernetinio išpuolio priskyrimo problemą. Kadangi kiekviena valstybė yra autonomiška pati spręsti, ar kibernetinį išpuolį priskirti trečiajai valstybei, tai sumažina kibernetinių sankcijų poveikį. Darnos trūkumas minėtu klausimu, silpnina Europos Sąjungos diplomatijos patikimumą, veiksmingumą, teisėtumą. Be to, priimtu Europos Sąjungos kibernetinio saugumo aktu, nesiryžta konkretiems subjektams taikyti privalomo kibernetinio saugumo sertifikavimo. Tačiau tikėtina, kad nustatytu terminu atlikus kibernetinio saugumo sertifikavimo vertinimą, visgi bus įteisinta privaloma sertifikavimo sistema.

[199] Reglamentas (ES) 2021/821, *supra note*, 187: 39 punktas.

# 3. KIBERNETINIO SAUGUMO TEISINIS REGLAMENTAVIMAS LIETUVOJE

Išanalizavus Europos Sąjungoje vyraujančią teisės aktų, reglamentuojančių kibernetinio saugumo sistemą, matyti, kad tam tikri reglamentai ar direktyvos įpareigoja valstybes nares imtis tam tikrų veiksmų kibernetinio saugumo srityje. Lietuva būdama Europos Sąjungos narė prisiima nustatytus įsipareigojimus užtikrinant aukštą tinklų ir informacinės sistemos lygį. Taigi, šiame skyriuje bus išanalizuota Lietuvos Respublikos kibernetinio saugumo teisinė sistema, jos atitikimas Europos Parlamento ir Tarybos direktyvų bei reglamentų reikalavimams. Tinklams ir informacinėms sistemoms vykdant svarbią ekonominę ir visuomeninę veiklą, atliekant kasdienę sveikatos, energetikos, finansų ir transporto veiklas, išaugo kibernetiniam saugumui kylanti rizika. Siekiant apsaugoti bei palaikyti visoje Sąjungoje aukštą kibernetinio saugumo lygį, 2014 m. gruodžio 11 d. priimtas vienas pagrindinių įstatymų Lietuvoje – Lietuvos Respublikos Kibernetinio saugumo įstatymas. Šis įstatymas nustato principus, kuriais:

- įtvirtinamos pamatinės kibernetinio saugumo nuostatos, tokios kaip, kibernetinės erdvės nediskriminavimo (fizinės ir kibernetinės erdvės aspektu);
- taikomos priemonės turi būti proporcingos siekiamam tikslui, t. y. negali apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina (kibernetinio saugumo rizikos valdymo, kibernetinio saugumo proporcingumo);
- vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, bet nereikalauti taikyti konkrečios rūšies technologijos įgyvendinant kibernetinio saugumo priemones (viešojo intereso viršenybės, standartizacijos ir technologinio neutralumo);
- kibernetinio saugumo subjektai, sistemas valdantys ir paslaugas sistemomis teikiantys, yra atsakingi už kibernetinį saugumą (subsidiarumo)[200].

Be to, kibernetinio saugumo apimtyje dominuoja ir bendrieji principai, tokie kaip suvokimo, atsakomybės, reagavimo, demokratiškumo, rizikos įvertinimo, elektroninės informacijos saugos kultūros kėlimo principai[201].

Kibernetinio saugumo įstatyme įtvirtintais principais turi vadovautis visos nacionalinės institucijos, įgyvendindamos savo veiklą bei taikydamos teisės normas, kurios reguliuoja kibernetinį

[200] Lietuvos Respublikos Kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428, 3 straipsnis.
[201] 2006 m. birželio 19 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 601 dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo, 4 punktas.

saugumą. Nė vienam principui negali būti suteikta pirmenybė, visi principai turi būti derinami tarpusavyje[202]. 2017 m. rekomendacijose dėl Lietuvos Respublikos kibernetinio saugumo įstatymo, nurodoma, kad svarbūs yra ir asmeninės atsakomybės principas, jis sudaro prielaidas ir viešojo intereso apsaugai, o taip pat visuotinės gynybos principas, įtvirtintas fizinės gynybos reguliavime, nes netinkamas, neatsakingas elgesys, priemonės, kibernetinis neraštingumas, gali skatinti kibernetinius incidentus[203]. Tačiau pažymėtina, kad priimant Kibernetinio saugumo įstatymą į šias rekomenduojamas sąvokas neatsižvelgta ir jos nebuvo įtvirtintos įstatyme. Taip pat šiame įstatyme yra įvardintos ir kibernetinio saugumo formavimo ir įgyvendinimo institucijos, jų įgaliojimai kibernetinio saugumo srityje. Lietuvos Respublikos Vyriausybė nustato kibernetinio saugumo politikos strateginius tikslus, pažangos uždavinius ir jiems pasiekti būtinas priemones. Lietuvos Respublikos krašto apsaugos ministerijai yra paskirtos užduotys – formuoti kibernetinio saugumo politiką, organizuoti, kontroliuoti ir koordinuoti jos įgyvendinimą. Įgyvendinti kibernetinio saugumo politiką padeda Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu. Įstatyme nustatytas kibernetinio saugumo subjektas bei jam keliamos bendrosios ir specialiosios pareigos (žr. 7 priedą). Ypatingos svarbos informacinės infrastruktūros valdytojams, didelėms įmonėms teikiančioms skaitmenines paslaugas, elektroniniams informacijos prieglobos bei skaitmeninių paslaugų teikėjams taip pat yra priskirtos pareigos, susijusios su kibernetinių incidentų valdymu.

Taigi, dėl išaugusio tinklų ir informacinių sistemų naudojimo, dėl būtinumo užtikrinti veiksmingą, nenutrūkstamą gyvybiškai svarbių, kasdienių veiklų funkcionavimą, buvo teisiškai įtvirtinti kibernetinio saugumo principai, kurių paskirtis visapusiškai garantuoti pamatines kibernetinio saugumo nuostatas. Tokie pamatiniai kibernetinio saugumo principai turi padėti suvaldyti kibernetinio saugumo krizes, mažinti kibernetinių incidentų skaičių. Įstatyme kibernetinio saugumo subjektams nustatytų bendrųjų ir specialiųjų pareigų tikslas užtikrinti, pagerinti tinklų ir informacinių sistemų apsaugą, sukurti vieningą, veiksmingą ir skaidrią sistemą.

Kibernetinio saugumo įstatymu nenustačius tam tikriems subjektam pareigos pranešti apie kibernetinius incidentus, 16 straipsnyje yra numatyta galimybė savarankiškai pranešti apie jų įvykusius incidentus. Tokie pranešimai yra pateikiami Nacionaliniam kibernetinio saugumo

[202] Kibernetinio saugumo įstatymas, *supra note,* 200: 2 straipsnio 8 punktas.
[203] D. Štitilis ir kt. *„Rekomendacijos Lietuvos Respublikos kibernetinio saugumo įstatymui“* (Mykolo Romerio universitetas, 2017), https://repository.mruni.eu/bitstream/handle/007/14643/Rekomendacijos_Kibernetinio_saugumo_istatymui(galutinis).pdf?sequence=1

centrui[204]. Kadangi ryšių ir informacinės sistemos turi tam tikrų spragų, kurios gali didinti kibernetinių incidentų skaičių šalyje, todėl skatinamas spragų nustatymas, kuris sumažina kylančią riziką. Spragų paieška gali naudotis asmenys turintys piktavališkų ketinimų, atliekant kibernetines atakas. Todėl, nacionalinės spragų atskleidimo tvarkos apraše, kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše ir Kibernetinio saugumo įstatymo 17 straipsnio 2 dalyje yra nustatyti atvejai, kai kibernetinio saugumo spragų paieška ir šių spragų atskleidimas laikomas teisėtu, o tokių veiksmų atlikimas asmeniui neužtraukia teisinės atsakomybės.[205] Nacionalinis kibernetinio saugumo centras savo internetiniame tinklalapyje yra nurodęs, kad atsakingas spragų atskleidimas yra laikomas, „kai informacija apie aptiktas spragas yra pirmiausiai pateikiama pačiai organizacijai, kurios sistemose ar produktuose jos buvo aptiktos, ir/ar spragų atskleidimo procesą koordinuojančiai institucijai – NKSC“[206]. Spragų paieška ir jų atskleidimas yra laikomi teisėtais, kai vykdant tokią veiklą nėra trikdomas ar keičiamas ryšių ir informacinės sistemos darbas, funkcionalumas, teikiamos paslaugos ir duomenų prieinamumas ar vientisumas. Aptikus spragą nutraukiama spragos paieškos veikla, be priežasties nesiekiama daugiau, negu reikia spragai patvirtinti, stebėti, fiksuoti, perimti, įgyti, laikyti ir pan., nebandoma atspėti slaptažodžių, nenaudojami slaptažodžiai gauti neteisėtu būdu, nėra daroma įtaka kibernetinio saugumo subjekto darbuotojams ar kitiems asmenimis, kai nedalijama aptiktos spragos informacija [207]. Taigi, visi šie aspektai užtikrina, kad spragų paieška ir jų atskleidimas būtų vykdomas sąžiningai, nepažeidžiant kitų interesų ir nesudarant galimybės, prisidengiant tokia veikla, įgyvendinti kibernetinius išpuolius.

Spragų paieška ir jų atskleidimą įtvirtina Lietuvos Respublikos Krašto apsaugos ministro 2021 m. liepos 9 d. įsakymas Nr. V-484, dėl nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo. Šiame įsakyme yra detalizuojama nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarka NKSC. Nurodyti būdai, kaip turi būti pateikta informacija apie spragų paieškos rezultatus, kokie yra NKSC pirminiai veiksmai gavus tokią informaciją, numatytas informacijos apie spragas paieškos rezultatų turinys bei aptiktos spragos atskleidimo kitiems asmenims terminai[208]. Kibernetinio saugumo įstatymo 17 straipsnio 3 dalis nustato, kad asmuo po spragų paieškos atlikimo, ne vėliau kaip per 24 valandas, turi parengti

[204] Kibernetinio saugumo įstatymas, *supra note*, 200: 16 straipsnis.
[205] *Ibid*, 17 straipsnis.
[206] Pranešti apie spragą“ *Nacionalinis kibernetinio saugumo centras* https://www.nksc.lt/pranesti-spraga.html
[207] Kibernetinio saugumo įstatymas, *op. Cit.*, 17 straipsnis.
[208] 2021 m. liepos 9 d. Lietuvos Respublikos Krašto apsaugos ministro įsakymas Nr. V-484, Dėl nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/270e6bd1e08911eb866fe2e083228059

informaciją apie spragų paieškos rezultatus ir ją pateikti NKSC ir (arba) kibernetinio saugumo subjektui, kurio informacinėje sistemoje atlikta spragų paieška [209]. Siekiant, kad informacijos apie spragas pateikimas būtų efektyvus ir paprastas, NKSC internetinėje svetainėje yra sukurta speciali pranešimų forma (žr. 8 priedą) [210]. Be to, yra nustatytas 90 kalendorinių dienų terminas informacijos apie aptiktą spragą atskleidimo kitiems[211], kuris gali būti trumpinamas, jei kibernetinio saugumo subjektas paneigia informaciją apie spragos egzistavimą (žr. 9 priedą). Tokiu būdu siekiama, kad ankstyvas tam tikros saugumo spragos išviešinimas nebūtų panaudotas kaip įrankis kibernetinėms atakoms. Pažymėtina, kad ne daug kibernetinio saugumo subjektų yra įtvirtinę spragų atskleidimo tvarką, o tai mažina šalies kibernetinį saugumą. Todėl reikėtų skatinti organizacijų įsitraukimą į įteisintą spragų atskleidimo modelį, kuris gali užkirsti kelią kibernetiniams incidentams. Lietuvoje egzistuoja įmonių, kurios taiko spragų atskleidimo politiką, tačiau jų kol kas yra ne daug, štai pavyzdžiui, „Paysera“ savo internetiniame tinklalapyje pateikė saugumo spragų pranešimo programą, kurioje nurodė reikalavimus, sąlygas ir atlygį, kuris įvertinamas pagal spragos riziką ir poveikio sunkumą[212]. Taip pat įmonė „SpectroCoin“ savo internetinėje svetainėje pristatė „Surask klaidą“ programą ir nustatė, jog asmenims pranešusiems apie saugumo pažeidimus skirs atlygius Bitcoin arba Ether kriptovaliutomis[213] .

Taigi, siekiant užtikrinti kibernetinį saugumą nacionaliniu lygiu buvo priimtas Lietuvos Respublikos Kibernetinio saugumo įstatymas. Šiuo teisės aktu nustatytos esminės teisės normos reglamentuojančios kibernetinio saugumo institutą, sukurtos pamatinės nuostatas kibernetinio saugumo srityje, įtvirtintos tam tikrų subjektų teisės bei pareigos. Šiuo įstatymu siekiama sumažinti kibernetinių atakų rizikas, didinti visuomenės pasitikėjimą teikiamomis paslaugomis kibernetiniu aspektu, užkirsti kelią galimiems kibernetiniams išpuoliams. Būtent kibernetinio saugumo įstatyme bei nacionalinės spragų atskleidimo tvarkos apraše yra nustatyti konkretūs apribojimai, kurių laikantis asmeniui nekyla baudžiamoji atsakomybė, atliekant spragų paiešką.

2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148, įpareigojo Europos Sąjungos nares priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją. Atsižvelgus į tai, 2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybė priėmė nutarimą Nr. 818, kuriuo įtvirtino nacionalinę kibernetinio saugumo strategiją, nustatė nacionalinės kibernetinio

[209] Kibernetinio saugumo įstatymas, *supra note,* 200: 17 straipsnis.
[210] „Pranešti apie spragą“ *Nacionalinis kibernetinio saugumo centras* https://www.nksc.lt/pranesti-spraga.html
[211] Kibernetinio saugumo įstatymas *op. Cit.,* 17 straipsnio 5 dalis
[212] „Informavimas apie saugumo spragas“ *Paysera* https://www.paysera.lt/v2/lt-LT/saugumas/pranesimai-apie-saugumo-spragas
[213] „Surask klaidą programa“ *SpectroCoin* https://spectrocoin.com/lt/surask-klaida-programa.html

saugumo politikos viešajame ir privačiame sektoriuose kryptis bei siekius[214]. Lietuvos Respublikos kibernetinio saugumo strategijos tikslas – užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų (IRT) teikiamomis galimybėmis[215]. Nutarime yra išskirti penki kibernetinio saugumo strategijos tikslai, atitinkamai jų įgyvendinimui numatyti uždaviniai.

2010 m. naudojant kenkėjišką programą buvo įvykdyta kibernetinė ataka, kuri sukėlė fizinį centrifugų pakenkimą Irano branduolinės energetikos objekte. 2015 m kibernetinės atakos sukėlę dalį Ukrainos elektros tinklo griūties[216]. Kibernetinė erdvė pradedama naudoti kaip karo erdvė arba kaip viena iš hibridinio karo priemonių[217]. Kadangi, Lietuva turi išplėtotą plačiajuosčio ryšio infrastruktūrą bei aktyviai naudojasi IRT teikiamomis galimybėmis, tai sudomina kibernetinius nusikaltėlius įvykdyti neteisėtus veiksmus prieš Lietuvą ar Lietuvos teritorijoje, taigi kyla grėsmė Lietuvos nacionaliniam saugumui. Dėl to kibernetinio saugumo strategija pirmiausia siekiama „*stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą*“[218]:

1. kuriant sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą. Uždavinys orientuotas į geresnį kibernetinio saugumo rizikos nustatymą, vertinimą ir prognozavimo būdus, atsižvelgiant į atskiriems sektoriams būdingas rizikas, taip pat į tinkamą visuomenės informavimą. Pavyzdžiui 2019 m. įkurta informacinė sistema (LITIS arba MAPPI (*MAP of Public Internet*). LITIS renka reikiamą informaciją iš viešai prieinamų šaltinių, jungia juos į vieną visumą ir pavaizduoja Lietuvos arba kitų šalių interneto infrastruktūros loginę struktūrą – jos komponentus ir ryšius tarp jų [219].

2. didinant kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, mažinant administracinę naštą kibernetinio saugumo subjektams. Tokiu būdu tobulinamas kibernetinio saugumo teisinis reguliavimas. 2020 m. spalio 1 d. Krašto apsaugos ministerija organizavo seminarą skirtą kibernetinio saugumo srities teisės aktų apžvalgai ir praktiniam taikymui viešajame ir privačiame sektoriuose[220].

3. skatinant nacionalinių pratybų vykdymą ir dalyvavimą tarptautinėse pratybose. Nuotoliniu būdu NKSC atstovai 2020 m. birželio 9–11 d. dalyvavo „SANS“ instituto organizuotose „vėliavos paėmimo“ (angl. k. *Capture The Flag* (CTF)) tipo pratybose. 2020 m. birželio 23–25 d. tarptautinėse

[214] 2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
[215] *Ibid*, 4 punktas.
[216] „Kibernetinio saugumo apžvalga“ Apžvalga http://apzvalga.eu/images/kibernetinis_saugumas.pdf 13 p.
[217] „Nacionalinė kibernetinio saugumo strategija“ *Lietuvos Respublikos krašto apsaugos ministerija* (2019 m. vasario 22 d.)
[218] *Ibid*, 5 punktas.
[219] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019 metų vertinimo kriterijų rezultatai.
[220] *Ibid*

organizacijos „First“ organizuotose „vėliavos paėmimo“ tipo pratybos. 2020 m. spalio 1–2 d. „vėliavos paėmimo“ tipo pratybose „Cybershock 2020“, kurias organizavo Latvijos Reagavimo į tinklų ir informacijos saugumo incidentus grupės (CERT.LV). [221].

4. plėtojant valstybės kibernetinės gynybos pajėgumus, t. y. įsigyjant reikiamą techninę ir programinę įrangą.[222]

2016 m. NATO viršūnių susitikime kibernetinė erdvė pripažinta penktuoju kariavimo domenu. Taigi, Lietuvos kariuomenė yra Lietuvos Respublikos kibernetinės erdvės gynybos subjektas[223]. Analizuojant teisinį kibernetinio saugumo institutą karo kontekste pastebėta, jog Lietuvos mokslinėje doktrinoje yra labai mažai autorių analizavusių šią temą. Priešiškai nusiteikusių šalių kibernetinio puolimo veiksmų neriboja geografinės valstybių sienos, tai yra naujas reiškinys, todėl aktualu išanalizuoti teisinį kibernetinio karo reguliavimą, identifikuoti teisinio reguliavimo problemas ir pasiūlyti galimus jų sprendimų būdus.

Be to, nusikalstamos veikos šiuo metu yra vykdomos ir kibernetinėje erdvėje, jos nuolat kinta, įgauna naujų formų. Policijos generalinis komisaras Renatas Požėla nurodo, kad Lietuvos Respublikoje vis didėja elektroninių arba nusikalstamų veikų kibernetinėje erdvėje, todėl minėti nusikaltimai yra prioritetiniai policijos veikloje. Pažymėjo, jog nusikaltimus darantys asmenys kibernetinėje erdvėje naudojasi pokyčių neapibrėžtumu bei ypatingai greitai prisitaiko prie kintančių aplinkybių siekdami nusikalstamų tikslų[224]. Todėl antrasis strategijos tikslas – „*užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą*“[225]. Lietuvos policija stebi nusikalstamumo pokyčius kibernetinėje erdvėje, identifikuoja kriminogenines rizikas ir imasi veiksmų joms šalinti. Be to, Lietuvos policija vykdydama strategijos antrąjį tikslą įgyvendina ir pirmąjį strategijos tikslą, kibernetinių pajėgumų plėtrą[226]. Kibernetinio saugumo būklės ataskaitoje nurodyta, kad 2020 m. kibernetinių incidentų priežastimi dažniausiai tapdavo žinomų pažeidžiamumų išnaudojimas, interneto naudotojų kibernetinio saugumo higienos trūkumas ir socialinės inžinerijos metodais paremti elektroniniai laiškai. Neretai pasitaiko, kad kibernetiniai sukčiai siunčia įvairias nuorodas ar dokumentus, kuriuos neapdairiai atvėrus sudaromos sąlygos iš galinių įrenginių neteisėtai

[221] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019 metų vertinimo kriterijų rezultatai.
[222] Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, *supra note,* 214: 14 punktas.
[223] „Kibernetinio saugumo apžvalga“ *Apžvalga, supra note:* 216, 13 p.
[224] „2020 m. Nacionalinio kibernetinio saugumo ataskaita“ , Lietuvos Respublikos krašto apsaugos ministerija *supra note,* 2: 54
[225] Lietuvos Respublikos Vyriausybės. nutarimas Nr. 818, *op. Cit.*
[226] „2020 m. Nacionalinio kibernetinio saugumo ataskaita“ Lietuvos Respublikos krašto apsaugos ministerija *supra note,* 2: 54 puslapis.

gauti informaciją ir (ar) toliau vykdyti kitus kibernetinius incidentus[227]. Todėl, net ir taikant visas esamas technines kibernetinio saugumo priemones, gali įvykti kibernetinis incidentas dėl kibernetinio saugumo įgūdžių stokos[228]. Kadangi kompiuteriuose bei išmaniuosiuose telefonuose yra kaupiama vis daugiau asmeninės, darbinės ir konfidencialios informacijos, „Samsung“ atliko apklausą, kuri parodė, kad „30 % respondentų, patyrusių kibernetines atakas nenutuokia, kaip įsilaužėliai pasiekė jų asmeninius duomenis ir net daugiau nei 60 % nežino, kokių veiksmų imtis, jei įsilaužta į jų įrenginius ar paskyras“[229]. Kibernetinio saugumo ekspertai teigia, jog žmogus – silpniausia vieta kibernetinio saugumo grandinėje, jį lengva paveikti naudojantis socialinės inžinerijos metodais. Minėti metodai vykdomi naudojant psichologinį poveikį bei manipuliuojant emocijomis, priverčiant atlikti žalingus veiksmus, t. y. atverti įvairias nuorodas, svetaines, parsisiųsti dokumentus, paleisti veikti žalingą kodą, pateikti asmens ar prisijungimo duomenis [230].

Taigi, trečiasis kibernetinio saugumo strategijos tikslas – *„skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą“*[231]. Tai yra plėtojami moksliniai tyrimai, kibernetinio saugumo iniciatyvos, kibernetinio saugumo kompetencijų modeliai, formuojami kibernetinio saugumo kompetencijų standartai, plėtojami kibernetinio saugumo srities mokymai, tobulinamos kibernetinio saugumo žinios, skatinamas bendradarbiavimas viešojo ir privataus sektoriaus bei mokslo ir studijų institucijų, kuriant kibernetinio saugumo inovacijas [232]. NKSC 2020 m. tęsė du inovatyvius kibernetinio saugumo srities projektus, vieną skirtą saugiam kriptografiniais metodais pagrįstam dalijimosi informacija būdui sukurti, kitą – ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo sistemai [233].

Įvykus pavojingam ar didelės reikšmės turinčiam kibernetiniam incidentui tiek nacionalinėms tarnyboms, tiek įmonėms, tiek ypatingos svarbos informacinės infrastruktūros valdytojams yra sunku vienoms kovoti ir užkardyti incidento keliamus pavojus. Todėl, vienas iš svarbiausių, visapusiško kibernetinio saugumo užtikrinimo tikslų – *viešojo ir privataus sektoriaus bendradarbiavimas*[234]. Šio tikslo siekiama keičiantis aktualia informacija apie kibernetines grėsmes, įvykusius kibernetinius incidentus, išmoktas pamokas, plėtojant ankstyvojo perspėjimo sistemą[235]. Pavyzdžiui, UAB „Critical

[227] Lietuvos Respublikos krašto apsaugos ministerija *supra note,* 2: 9 puslapis.
[228] Lietuvos Respublikos vyriausybės nutarimas Nr. 818, *supra note,* 214: 24 punktas.
[229] „Esate tikras, kad niekada nepatyrėte kibernetinės atakos? Pasitikrinkite, ar tikrai“ *Samsung,* 2019 m. spalio 3 d. https://www.samsung.com/lt/news/local/esate-tikras-kad-niekada-nepatyrete-kibernetines-atakos-pasitikrinkite-ar-tikrai/
[230] „Kibernetinio saugumo hakatonas“ *DELTA1* https://delta1.lt/wp-content/uploads/2021/10/DELTA1-temos.pdf
[231] Lietuvos Respublikos vyriausybės nutarimas Nr. 818, *op. Cit.,* 23 punktas.
[232] *Ibid,* 32 punktas.
[233] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019 metų vertinimo kriterijų rezultatai.
[234] Lietuvos Respublikos vyriausybės nutarimas Nr. 818, *op. Cit.,* 34 punktas.
[235] *Ibid,* 38.1 punktas.

Security“ specialistai pranešė NKSC apie tam tikro, populiaraus, maršrutizatoriaus modelio gamyklinio slaptažodžio pažeidžiamumą. NKSC išanalizavęs gautą informaciją bei atlikęs kitų, esančių rinkoje, naudojamų bevielio tinklo prietaisų gamyklinių nustatymų saugumo vertinimą, nustatė, kad Lietuvoje plačiai naudojami tinklo maršrutizatoriai turi pažeidžiamumą, kuriuo pasinaudojus per trumpą laiką galima išgauti belaidžio tinklo (Wi-Fi) slaptažodį. Kas leistų įsilaužėliams naudotis naudotojo namų interneto prieiga, šnipinėti duomenų srautą, vykdyti kitas nusikalstamas veikas. NKSC nuomone, tai parodo, kaip viešojo ir privataus sektorių bendradarbiavimas gali vykti praktikoje ir užtikrinti ankstyvą problemos išsprendimą [236]. Taigi, kibernetinis saugumas yra visų atsakomybė, todėl bendradarbiaujant yra atveriamos didesnės galimybės pasiekti tiek asmeninių, tiek bendrų tikslų, yra dalijamasi naujausia aktualia praktika, keliamas šalies kibernetinis atsparumas.

Siekiant užtikrinti aukštą nacionalinio kibernetinio saugumo lygį bei šį lygį nuolatos stiprinti, tikslinga įgyvendinti *aktyvų tarptautinį, tarpvalstybinį bendradarbiavimą*, kurio metu būtu keičiamasi gerąja patirtimi bei aktualia informacija. Stiprinant tarptautinius kibernetinio saugumo pajėgumus ir gebėjimus, inicijuojamas Nuolatinio struktūrizuoto bendradarbiavimo projektas, kuris stiprina Europos Sąjungos valstybių narių bendradarbiavimą kibernetinio saugumo ir gynybos srityje[237]. Nuolatinio struktūrizuoto bendradarbiavimo projektas yra „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“. Budinčių pajėgų rotacijai 2020 m. vadovavo Lietuva, pajėgas sudarė kibernetinio saugumo specialistai iš Lietuvos, Lenkijos Rumunijos ir Nyderlandų. Šios pajėgos kibernetiniai gebėjimai ir veikimo procedūros 2020 m. buvo išbandytos atliekant kibernetinio saugumo pažeidžiamumų vertinimą VRK informacinėje sistemoje[238]. Taip pat, plečiant bendradarbiavimą su Jungtinėmis Amerikos Valstijomis kibernetinės gynybos srityje, plėtojamas dvišalis Lietuvos ir Jungtinių Amerikos Valstijų veiklų vykdymas, kuris stiprintų Lietuvos kibernetinę gynybą ir saugumą[239]. O būtent, 2021 m. liepos 14 d. įkurtas Regioninis kibernetinės gynybos centras[240]. 2021 m. spalį Nacionalinis kibernetinio saugumo centras pradėjo vykdyti centro funkcijas, o JAV patvirtino skirsiančios 10 mln. dolerių kibernetinio saugumo mokymų infrastruktūros sukūrimui Kaune. Centras pagrindinė Lietuvos ir JAV dvišalio bendradarbiavimo

[236] Lietuvos Respublikos krašto apsaugos ministerija *supra note,* 2: 45 puslapis.
[237] Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, *supra note,* 214: 42.2 punktas.
[238] Lietuvos Respublikos krašto apsaugos ministerija *supra note,* 2: 18
[239] Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, *op. Cit.,* 42.3 punktas.
[240] „Veiklą oficialiai pradeda Regioninis kibernetinės gynybos centras“ *Lietuvos Respublikos krašto apsaugos ministerija,* (2021 m. liepos 15 d.)
http://kam.lt/lt/naujienos_874/aktualijos_875/veikla_oficialiai_pradeda_regioninis_kibernetines_gynybos_centras

kibernetinėje srityje platforma, taip pat bus bendradarbiaujama su Sakartvelo bei Ukrainos kibernetinio saugumo specialistais[241].

Lietuvos kibernetinio saugumo strategijoje apibrėžiami penki strateginiai tikslai, kuriuos įgyvendinant užtikrinamas sklandus informacinės ir ryšių technologijos veikimas, naudojimas. Tikslų bei uždavinių reglamentavimas nustato kibernetinio saugumo kryptį, visuomenei bei privačiam sektoriui yra demonstruojamas aiškus skatinimas, kai kuriais atvejais ir įpareigojimas rūpintis savo duomenimis, gilinti žinias kibernetinio saugumo srityje. Pažymėtina, kad 2021 m. birželio 29 d. Jungtinių Tautų Tarptautinės telekomunikacijų sąjunga ITU sudarė tarptautinį kibernetinio saugumo indeksą, kuris skirtas valstybių priimamiems sprendimams, vykdomiems veiksmams ir požiūriui į kibernetinį saugumą įvertinti[242]. Lietuva minėtame indekse pateko į dešimtuką ir užėmė šeštą vietą, o Europos valstybių sąraše ji yra ketvirta[243].

Kadangi Lietuvos Respublikoje egzistuoja infrastruktūros neatsiejamos nuo šiuo metu vyraujančio įprasto valstybei gyvenimo (energetikos, transporto, krašto apsaugos, informacinių technologijų ir elektroninių ryšių, geriamojo vandens ir pan.). O kibernetinių nusikaltėlių taikinys ne tik individualių kompiuterių vartotojai, bet ir tarpusavyje sujungtos informacinės sistemos, kuriomis naudojasi bankai, vyriausybė, pramonė ir kitos, remiančios visuomenės veiklą, institucijos[244]. Lietuvos Respublikos Vyriausybė įtvirtino ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką. Minėtos infrastruktūros turi būti saugomos aukščiausiam lygyje, nes gresiantis pavojus jų teikiamų paslaugų vientisumui gali padaryti didelę žalą. Be to, valstybėms narėms buvo nustatyta pareiga iki 2018 m. lapkričio 9 d. sudaryti ir ne rečiau kaip kas dvejus metus peržiūrėti sąrašą ypatingos svarbos informacinių infrastruktūrų, tam, kad įvykęs kibernetinis incidentas būtų greičiau likviduotas bei būtų išvengtas nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams didelis neigiamas poveikis. Lietuvoje yra sukurtas infrastruktūros objektų, užtikrinančių ypatingos svarbos paslaugų teikimą, vertinimo klausimynas, kuris padeda identifikuoti konkrečius objektus. Nustatyta, kad pagal klausimyno kriterijus surinkus šešiolika ar daugiau balų, laikoma, kad teikiamų paslaugų sutrikdymo neigiamas poveikis yra didelis ir tokie infrastruktūros objektai priskiriami – ypatingos svarbos infrastruktūros objektams[245].

---

[241] Lietuvos Respublikos krašto apsaugos ministerija *op. Cit.,* 18

[242] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019 metų vertinimo kriterijų rezultatai..

[243] „Lietuva – ketvirta geriausiai kibernetinį saugumą užtikrinanti Europos valstybė“ *Nacionalinis kibernetinio saugumo centras* (2021 m. birželio 29 d.) https://www.nksc.lt/naujienos/lietuva__ketvirta_geriausiai_kibernetini_sauguma_u.html

[244] „Kibernetinio saugumo apžvalga“ *supra note,* 216

[245] Lietuvos Respublikos vyriausybės nutarimas Nr. 818, *supra note,* 214: 6.4. punktas.

Taip pat, svarbu paminėti, kad kibernetinio saugumo subjektams pagal 2018 m. rugpjūčio 5 d. Lietuvos Respublikos Vyriausybės nutarimą Nr. 818 keliami tam tikri organizaciniai ir techniniai kibernetinio saugumo reikalavimai. Užtikrinant kibernetinio saugumo subjektų paslaugų įprastą veikimą, procesų stabilumą ir atsižvelgiant į didėjančią pažeidžiamumo riziką, svarbu laiku aptikti ir pašalinti galimas grėsmes. Dėl šios priežasties yra numatytas ryšių ir informacinių sistemų rizikos vertinimas, kurio metu nustatomos grėsmės ir pažeidžiamumai, galintys turėti įtakos kibernetiniam saugumui. Taip pat yra įvertinama tikimybė, numatomos pasekmės, nustatomas rizikos lygis[246].

Kibernetinio saugumo srityje yra svarbu įvykus incidentui tinkamai bei greitai reaguoti į informaciją ir apie kibernetinį incidentą pranešti atitinkamoms institucijoms. NKSC, Valstybinė duomenų apsaugos inspekcija ir Lietuvos policija, yra paskyrusi asmenis atsakingus už informacijos keitimąsi kibernetinio incidento valdymo metu su kuriais būtų galima susisiekti visą parą[247]. Taip pat plane yra nustatyti kriterijai, pagal kuriuos yra vertinamas incidento poveikio mastas. Yra išskiriamos keturios kategorijos:

1) pavojingi kibernetiniai incidentai;
2) didelio poveikio kibernetiniai incidentai;
3) vidutinio poveikio kibernetiniai incidentai;
4) nereikšmingo poveikio kibernetiniai incidentai[248].

Svarbu tai, kad kibernetinį incidentą priskirti pavojingam gali tik Nacionalinis kibernetinio saugumo centras, jei incidentas atitinka tam tikrus kriterijus (žr. 10 priedą). Kibernetiniu incidentu galima prarasti duomenis, gali būti sutrikdyta internetinės svetainės veikla, banko ar mokėjimo kortelių duomenų, pinigų vagystė, sutrikdyta prekyba, prarastas verslas, sukelti finansiniai nuostoliai bei ekonominiai padariniai[249]. Kibernetiniai incidentai gali būti labai įvairūs: nepageidaujami laiškai, klaidinančios ar žeidžiančios informacijos platinimas; kenkimas programinei įrangai; elektroninės informacijos sunaikinimas, pakeitimas ar ištrynimas; įsilaužimas į informacinę sistemą; taikomosios programinės įrangos ar paslaugos naudojimas ir t.t. Kibernetiniai incidentai gali sukelti įvairių padarinių, be to Lietuvos Respublikos administracinių nusižengimo kodekso (toliau – ANK) 479 straipsnyje nustatyta atsakomybė juridinių asmenų vadovams ar kitiems atsakingiems asmenims už pareigos teikti informaciją pažeidimą, t. y. informacijos apie kibernetinius incidentus ir taikytas

[246] *Ibid* 3 punktas.
[247] 2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, Nacionalinis kibernetinių incidentų valdymo planas, 3 p. 818 Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo (lrs.lt)
[248] *Ibid*, 9 p.
[249] Irma Kirklytė „I. Kirklytė: kas yra kibernetinis incidentas ir ko imtis jam įvykus“ *Infolex* (2021 m. spalio 11 d.) https://www.infolex.lt/portal/start.asp?act=news&Tema=54&str=89117

kibernetinių incidentų valdymo priemones nepateikimą NKSC arba šios informacijos teikimo tvarkos pažeidimą, informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamų veikų požymių, nepateikimą policijai arba šios informacijos teikimo tvarkos pažeidimą[250]. Taigi, įmonės ne tik gali nukentėti nuo pačių kibernetinių incidentų, bet ir nevykdydamos, 2018 m. rugpjūčio 5 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 818, nustatytų pareigų, gali sulaukti administracinių nuobaudų – įspėjimo arba baudos. Kaip matyti, kibernetiniai incidentai atitinka elektroninių nusikalstamų veikų sampratą Lietuvos Respublikos baudžiamojo kodekso prasme. Minėtas kibernetinis incidentas, kuomet siekiama vienaip ar kitaip panaudoti elektroninę informaciją, atitinka BK 196 straipsnį, o įsilaužimas į informacinę sistemą galėtų būti kvalifikuojamas kaip BK 198[1], taikomosios programinės įrangos ar paslaugos naudojimas pagal BK 198[2] straipsnį. Nacionalinis kibernetinio saugumo centras pateikė metinę statistiką, pagal kurią matyti, kad 2020 m. šalyje užfiksuota – 4 330 kibernetinių incidentų, iš jų 4 262 nereikšmingo poveikio, 67 – vidutinio poveikio ir 1 – didelio poveikio[251]. Lyginant su 2019 metais, fiksuojamas 25% kibernetinių incidentų prieaugis (žr. 11 priedą)[252].

Iš NKSC duomenų matyti, kad išskiriant kibernetinius incidentus pagal grupes, daugiausia incidentų buvo susijusių su kenkimo programine įranga, per metus jų padaugėjo 49 %. Pastebimas net 67 % didesnis incidentų kiekis susijęs su paslaugų sutrikdymu bei 73 % didesnis incidentų kiekis, kuris yra susijęs su mėginimais įsilaužti į informacines ir ryšių sistemas. Pažymima, kad net 62 % sumažėjo neteisėtos veiklos ir sukčiavimo kibernetinėje erdvėje atvejų. Tačiau elektroninis sukčiavimas išlieka vienas dažniausių kibernetinių nusikaltimų[253]. Pabrėžiama, kad šie duomenys gauti lyginant 2019 ir 2020 metus, tuo laikotarpiu, kai prasidėjo Covid-19 pandemija. Sąlygojant pandemijai, daug žmonių pradėjo dirbti nuotoliniu būdu, be to kiekvienais metais yra pastebimas tendencingas kibernetinių incidentų augimas. Lietuvoje yra nustatytas kibernetinių incidentų tyrimas, kurio metu tiriami tik vidutinio arba didelio masto kibernetiniai incidentai. Kibernetinių incidentų tyrimo atžvilgiu svarbu pažymėti, kad kibernetinio saugumo subjektai turi kibernetinio saugumo teisės aktais reglamentuoti incidentų tyrimo atlikimo tvarką[254]. Nustatyta kibernetinių incidentų tyrimo tvarka skatina, kad kibernetinis incidentas būtų kuo greičiau ir efektyviau ištirtas. Be to, tiriant kibernetinius incidentus vykdomas ne tik tarpinstitucinis bendradarbiavimas, bet ir tarptautinis.

Taigi, siekiant gerinti kibernetinio saugumo būklę Lietuvoje, užtikrinti tinkamą valstybės kibernetinio saugumo politikos formavimą ir įgyvendinimą, priimtas Nacionalinis kibernetinių

[250] Lietuvos Respublikos administracinių nusižengimų kodeksas 479 straipsnis, https://www.infolex.lt/ta/336765:str479
[251] Lietuvos Respublikos krašto apsaugos ministerija *supra note*, 2: 25
[252] *Ibid*
[253] *Ibid*, 7
[254] Nacionalinis kibernetinių incidentų valdymo planas, *supra note, 247:* IV skyrius.

incidentų valdymo planas, kuriame nustatytos pagrindinės taisyklės, kuriomis vadovaujamasi įvykus kibernetiniam incidentui. Bene svarbiausi Nacionalinio kibernetinių incidentų valdymo plano sprendimai, yra tai, jog nustatytos kibernetinio incidento kategorijos bei konkretūs kriterijai, kuriems vyraujant kibernetinis incidentas priskiriamas tam tikrai kategorijai, taip pat kibernetinių incidentų tyrimas.

Išanalizavus Lietuvos teisinę struktūrą kibernetinio saugumo srityje matyti, jog Lietuva didina kibernetinį atsparumą, stiprina kibernetinę gynybą, kovoja su elektroniniais nusikaltimais, saugo ypatingos svarbos infrastruktūrą. Lietuva vykdo visas Europos Sąjungos imperatyviąsias pareigas, įtvirtino direktyvomis bei reglamentais nustatytas teisės normas bei jas perkėlė į nacionalinius teisės aktus. Atsižvelgus į Jungtinių Tautų Tarptautinės telekomunikacijų sąjungos ITU sudarytą tarptautinio kibernetinio saugumo indekso rezultatą, darytina išvada, jog Lietuvos Respublikos teisinė bazė kibernetinio saugumo politikoje yra pakankama.

# 4. NUSIKALSTAMŲ VEIKŲ KIBERNETINĖJE ERDVĖJE PROBLEMINIAI ASPEKTAI IR PRAKTINIAI KVALIFIKAVIMO YPATUMAI TEISMŲ PRAKTIKOJE

Šioje darbo dalyje siekiama aptarti baudžiamąsias bylas, kuriose nusikalstamos veikos buvo atliktos kibernetinėje erdvėje. Analizės metu siekiama išsiaiškinti nusikalstamų veikų kibernetinėje erdvėje, kai informacinės ir ryšių technologijos panaudojamos kaip nusikaltimo priemonės, taikymo teismų praktikoje problematiką. Taip pat nusikalstamų veikų kibernetinėje erdvėje, siaurojo sampratos aiškinimo, kvalifikavimą praktikoje, t. y. teisminio nagrinėjimo metu. Analizuojant aktualias bylas siekiama išsiaiškinti praktines problemas, formalias straipsnio nuostatas, visumos vertinimą ir teismo išvadas, aktualias nusikalstamų veikų kibernetinėje erdvėje nagrinėjimo aspektu. Mokslinį tyrimą gerai iliustruoja teismų praktikos pavyzdžiai, kurie parinkti išstudijavus baudžiamąsias bylas, kuriose buvo įžvelgiamos problemos, keliami tam tikri neaiškumai, taip pat aktualios baudžiamosios bylos, kurios atspindi esminius teismų motyvus nusikalstamų veikų kibernetinėje erdvėje kvalifikavimo srityje.

Lietuvos Aukščiausias Teismas nekartą yra konstatavęs, jog teismo išvados turi būti pagrįstos įrodymais, patvirtinančiais kaltinamojo kaltę padarius nusikalstamą veiką, o apkaltinamasis nuosprendis negali būti grindžiamas prielaidomis[255]. Be to, ikiteisminio tyrimo pareigūnai, prokuroras ir teismas privalo siekti, kad būtų išsiaiškintos visos reikšmingos aplinkybės byloje[256].

Organizacija Fraud.org, kuri vykdo vartotojų švietimo bei internetinio sukčiavimo prevenciją, pateikė 2021 m. sukčiavimo ataskaitą, kurioje nurodė, jog sukčiai ir toliau naudojosi pandemija, darant nusikalstamas veikas pelningesnes, o prieiga prie vartotojų kredito kortelių informacijos buvo pagrindinis būdas, kuriuo sukčiai siekė gauti lėšų. Tačiau tarp sukčių populiarėja kiti mokėjimo būdai, dovanų kortelės, kriptovaliutos. Galimai tai yra dėl to, nes vienu iš šių būdų išsiųstos lėšos sukčiams pasiekiamos greitai ir dažnai anonimiškai[257]. Ankstesniuose skyriuose buvo identifikuota, kad informacinių ir ryšių technologijos greitai keičiasi bei nuolat tobulėja, dėl tos priežasties viena iš problemų, susijusių su šių nusikaltimų ištyrimu bei nagrinėjimu teisminio proceso metu, yra būtent tai, jog ikiteisminio tyrimo metu nepakankamai ir netinkamai surenkami bylai svarbūs duomenys, o kaltininkai lieka nenubausti. Pavyzdžiui, Lietuvos apeliacinio teismo baudžiamojoje byloje Nr. 1A-311-396/2018, *D. Š., nenustatytu laiku ir nenustatytoje vietoje, susitaręs su tyrimo metu nenustatytu*

[255] Lietuvos Aukščiausiojo Teismo 2018 m. liepos 3 d. nutartis baudžiamojoje byloje Nr. 2K-228-895/2018
[256] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2021 m. kovo 29 d. nutartis baudžiamojoje byloje Nr. 2K-25-628/2021
[257] „Top Sams of 2021“ Fraud.org (2022) https://fraud.org/wp-content/uploads/2022/01/2021-top-scams-report-final.pdf

*asmeniu panaudoti kenkėjišką programinę įrangą (kompiuterinius virusus) ir jos pagalba neteisėtai perimti kaip įmanoma didesnį skaičių Lietuvoje veikiančių bankų klientų (fizinių ir juridinių asmenų) elektroninių mokėjimo priemonių naudotojų tapatybės patvirtinimo priemonių duomenų – elektroninės bankininkystės paskyrų vartotojų nuolatinius slaptažodžius, naudotojų autentifikavimo kodus (ID) bei sesijos kintamus slaptažodžius (kodus), neteisėtai prisijungti prie minėtų bankų informacinių sistemų ir jų klientų banko sąskaitų, pasinaudojus šiais duomenimis, atlikti neteisėtas finansines operacijas su minėtose banko sąskaitose esančiomis piniginėmis lėšomis, neteisėtai pervedant minėtas pinigines lėšas iš asmenų banko sąskaitų į savo bendrininkų banko sąskaitas Lietuvoje veikiančiuose bankuose, po to šias svetimas lėšas išgryninti ir taip apgaule įgyti minėtą svetimą turtą*[258].

Šioje baudžiamojoje byloje buvo nuteisti keturi asmenys. D. Š. subūręs organizuotą grupę nuteistas padaręs 8 nusikalstamas veikas, jam inkriminuota: BK 214 straipsnio 1 dalis (3 nusikalstamos veikos), BK 25 straipsnio 3 dalis ir BK 214 straipsnio 1 dalis, BK 25 straipsnio 3 dalis ir BK 215 straipsnio 1 dalis, BK 25 straipsnio 3 dalis ir BK 198[1] straipsnio 1 dalis, BK 182 straipsnio 2 dalis[259]. Tačiau, vienas asmuo taip ir liko nenustatytas.

Ikiteisminio tyrimo metu nebuvo nustatyti visi organizuotos grupės nariai, tiksliai nenustatyta vieta, kurioje neteisėtai, nuotoliniu būdu buvo inicijuotos finansinės operacijos, taip pat nenustatytas kompiuteris ar kitas elektroninis ryšio perdavimo įrenginys, kuriame buvo įdiegta žalinga virusinė programa. Atkreiptinas dėmesys į tai, kad tiek ikiteisminio tyrimo metu, tiek pirmosios instancijos teisminio nagrinėjimo metu nebuvo surinkta papildomų duomenų dėl minėtų faktinių bylos aplinkybių. Analizuojant bylą, manytina, kad būtent nenustatytas asmuo, turėjo atitinkamų programavimo žinių, kuris atliko visą techninį darbą, neteisėtai panaudojęs žalingą kompiuterinį virusą, prisijungė prie fizinių ir juridinių asmenų elektroninės bankininkystės ir banko sąskaitų, iš kurių pervedė arba pasikėsino pervesti pinigines lėšas. Tačiau, visgi jis liko nenustatytas. Asmuo turintis specialiųjų žinių greitai prisitaiko prie besikeičiančių aplinkybių, naudojasi pokyčių neapibrėžtumu siekiant pasisavinti pinigines lėšas. Iš bylos duomenų matyti, jog nebuvo nustatyti elektroninių ryšio perdavimo įrenginiams priskirti IP adresai, t. y. iš kokio IP adreso buvo prisijungta prie nukentėjusiųjų banko sąskaitų bei kas šio adreso galinis vartotojas. Svarbu pabrėžti, kad žinant IP adresą, galima sužinoti, kam priklauso įrenginys, tačiau šiuo atveju nebuvo nustatytas esminis organizuotos grupės narys, kuris atliko visą techninį darbą. Tačiau, nepaisant to, kad nebuvo surinkta

[258] Lietuvos apeliacinio teismo 2018 m. liepos 13 d. nuosprendis baudžiamojoje byloje Nr. 1A-311-396/2018
[259] *Ibid*

pakankamai informacijos dėl IP adresų, keturių kaltinamųjų kaltė dėl tam tikrų nusikalstamų veikų padarymo, visgi buvo pagrįsta kitais bylos duomenimis. Teisiamojo posėdžio metu saugumo incidentų tyrimų departamento vadovas nurodė, jog apžiūrėjus kompiuterį, iš kurio buvo padarytas neteisėtas pavedimas, nustatyta, kad klientas elektroninio laiško pavidalu gavo virusą, virusas pats save įsidiegė į kompiuterį, modifikavo kompiuterį bei komunikavo su komandų serveriu, kuris jam perdavinėjo instrukcijas[260]. Tai rodo, jog siekiant išvengti galimų kibernetinių grėsmių labai svarbi yra „kibernetinė higiena“, tinkami įpročiai bei žinios padedančios atpažinti kibernetines rizikas.

Taigi, Lietuvos Respublikos Konstitucinis Teismas yra konstatavęs, jog ikiteisminis tyrimas turi būti atliktas objektyviai, kvalifikuotai, nešališkai ir išsamiai, atliekant tyrimą turi būti surinkta tiek informacijos, kad jos pakaktų teisingai išspręsti baudžiamąją bylą teisme[261]. Tiriant nusikalstamas veikas kibernetinėje erdvėje pastebima, jog asmenys dažnai naudoja efektyvias tam tikro pobūdžio programines įrangas, kurių pagalbą siekiama paslėpti informaciją, bylai reikšmingus faktus bei tokiu būdu išvengti atsakomybės. Anksčiau išanalizuotoje Lietuvos apeliacinio teismo baudžiamojoje byloje Nr. 1A-311-396/2018, D. Š. nuteistas ir už tai, kad *realizuodamas bendrą nusikalstamą susitarimą ir veikdamas kartu su tyrimo metu nenustatytu organizuotos grupės nariu, ir į šios organizuotos grupės nusikalstamą veiklą įtrauktu V. R., elektroninių ryšių tinklais atlikęs neteisėtai iš V. R. įgytų ir laikytų svetimų, t. y. V. R. elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonės duomenų, pakankamų finansinei operacijai inicijuoti, perdavimą tyrimo metu nenustatytam organizuotos grupės nariui, o šiam realizavus organizuotos grupės nusikalstamą susitarimą ir tiksliai nenustatytoje vietoje, neteisėtai, nuotoliniu būdu panaudojus nenustatytą personalinį kompiuterį ar kitokį elektroninio ryšio perdavimo įrenginį su jame įdiegta interneto naršyklės kompiuterine programa, ir kaip tarpinę tarnybinę stotį, t. y. žalinga virusine programa užkrėstą kompiuterį, priklausantį kitam vartotojui, taip nuslėpus jo naudotam tyrimo nenustatytam personaliniam kompiuteriui ar kitokiam elektroninio ryšio perdavimo įrenginiui priskirtą IP adresą, bei neteisėtai įgytus AB D. banko elektroninės bankininkystės paskyrų naudotojų Šilutės rajono savivaldybės administracijos, UAB „L“ ir Pasvalio rajono savivaldybės administracijos nuolatinius slaptažodžius, naudotojų indentifikavimo kodus (ID) bei sesijos kintamus slaptažodžius (kodus)*[262]. Iš baudžiamosios bylos matyti, jog asmens nešiojamame kompiuteryje buvo įdiegta programinė įranga, kuri užšifruoja kompiuterio duomenis bei neleidžia įrašyti informacijos apie darbo istoriją bei visus

[260] Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 27 d. nuosprendis baudžiamojoje byloje Nr. 1-17-744/2018

[261] Lietuvos Respublikos Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas byloje Nr. 7/03-41/03- 40/04-46/04-5/05-7/05-17/05. http://www.lrkt.lt/dokumentai/2006/ n060116.htm .

[262] Nuosprendis baudžiamojoje byloje Nr. 1A-311-396/2018, *supra note*, 268.

pakeitimus, susijusius su kompiuterio instaliacija ir prie jo prijungtais įrenginiais, pvz.: jei programa yra įjungta, pajungus interneto modemą, jokių duomenų neišlieka. Taip pat kompiuteryje buvo įdiegta programinė įranga, kuri užrakina kompiuterio katalogus, t. y. tam tikri failai tampa nematomi ir neprieinami. Tačiau, perdavus minėtą kompiuterį specialistui, visgi kompiuterio standžiajame diske buvo rasti bylai reikšmingi duomenys[263]. Šiaulių apygardos teismo baudžiamojoje byloje Nr. 1S-87-316/2021 asmuo „*suklastojo transporto priemonės ridą, o būtent, jis <...> pasinaudodamas ikiteisminio tyrimo metu tiksliai nenustatytame kompiuteryje įdiegta programine įranga, skirta automobilių odometrų parodymų korekcijai, prisijungė prie automobilio centrinio kompiuterio duomenų sistemos ir neteisėtai sumažino automobilio ridą nuo apie 670 000 km iki 389 105 km, taip kaltinamas padarė nusikalstamą veiką, numatytą BK 306[2] straipsnio 1 dalyje*“[264]. Be to, įgyvendinant nusikalstamas veikas dažnai yra naudojamas Virtualus privatus tinklas (VPN), kurį kibernetinio saugumo ekspertai rekomenduoja naudoti viešose vietose jungiantis prie viešojo interneto. Tačiau, kaip matyti, ši programa naudojama ir vykdant nusikalstamas veikas, pavyzdžiui Klaipėdos apygardos teismo baudžiamojoje byloje Nr. 1A-177-417/2021, *asmuo pasinaudodamas, ikiteisminio tyrimo metu nenustatyta IP adresų nustatymo ir keitimo programa, iš IP adreso (duomenys neskelbtini) prisijungė prie „BIGBANK AS“ filialo tinklalapio ir A. M. vardu interneto svetainėje info@bigbank.lt užpildė paraišką 15 000 Eur kreditui gauti, asmuo vykdydamas kitus nusikalstamus veiksmus, apgaule savo ir kitų naudai įgijo ir pasikėsino įgyti svetimą turtą ir suklastojo dokumentus*[265]. VPN yra mokama paslauga, kurios pagalba naudojantis interneto ryšiu tarp kelių kompiuterių sukuriamas visiškai privatus tinklas, kuris pagal funkcionalumą turėtų atstoti fizišką dviejų kompiuterių sujungimą tinklo laidu[266]. IP adresas suteikiamas prie interneto prijungtam prietaisui, todėl tam, kad nebūtų atskleista skaitmeninė tapatybė, VPN paslauga išsaugo privatumą internete[267]. Be to, Vilniaus apygardos teismo baudžiamojoje byloje Nr. 1-285-870/2017, tarnybiniu pranešimu buvo nustatyta, jog į tam tikrą įrenginį buvo įdiegta anoniminio naršymo interneto naršyklė „Onion browser“, kuri pagal savo funkcionalumą yra tokia pati, kaip „Tor“ naršyklė, o būtent ja naudojantis leidžiama prisijungti prie interneto tinklapių, kurie nėra viešai prieinami eiliniams interneto vartotojams (vadinamų „deep web“

[263] Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 27 d. nuosprendis baudžiamojoje byloje Nr. 1-17-744/2018
[264] Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus 2021 m. liepos 15 d. nutartis baudžiamojoje byloje Nr. 1S-87-316/2021
[265] Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2021 m. lapkričio 25 d. nutartis baudžiamojoje byloje Nr. 1A-177-417/2021
[266] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2017 m. rugpjūčio 1 d. nuosprendis baudžiamojoje byloje Nr. 1-285-870/2017
[267] „IP adreso slėpimas naudojant „NordVPN“ *NordVPN* https://nordvpn.com/lt/features/hide-ip/

– „gilusis internetas“ ar „dark net“ – „tamsusis internetas“). Ši naršyklė suteikia visišką anonimiškumą internete ir nepalieka jokių naršymo internete istorijos pėdsakų įrenginyje, kuriame tokia naršyklė yra naudojama. Norint prisijungti prie „deep web“ interneto parduotuvių, kuriose paprastai prekiaujama nelegaliomis prekėmis ar paslaugomis (narkotinės, psichotropinės medžiagos, ginklai, vogti tapatybės duomenys, padirbti tapatybės duomenys ir pan.) neužtenka turėti vien anoniminio naršymo naršyklės, tam reikalaujama, kad prie internetinės parduotuvės būtų jungiamasi naudojantis VPN paslauga[268].

Kaip jau minėta anksčiau, ikiteisminio tyrimo metu surinkti duomenys yra labai svarbūs, todėl nepakankamai ar netinkamai juos surenkant, kyla problema priimti teisingą sprendimą teisme. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo baudžiamojoje byloje Nr. 2K-77-1073/2020, asmuo *„tiksliai ikiteisminio tyrimo metu nenustatytu laiku ir vietoje, iš ikiteisminio tyrimo metu nenustatyto asmens, neteisėtai, neturėdamas elektroninių mokėjimo priemonių naudotojų sutikimo bei leidimo, įgijo devynių svetimų banko KeyBank, esančio JAV, debetinių mokėjimo kortelių MASTERCARD duomenis bei keturių svetimų banko Credit Agricole, esančio Prancūzijoje, debetinių mokėjimo kortelių MASTERCARD duomenis, pakankamus finansinėms operacijos inicijuoti“*[269]. Teisminio nagrinėjimo metu kilo ginčas dėl baudžiamojo kodekso dispozicijos, t. y., ar asmuo įgijo tikrus svetimų elektroninių mokėjimo priemonių duomenis. Siekiant tai išsiaiškinti, teismo posėdžio metu „GOOGLE“ paieškos sistemoje buvo įvesti žodžiai „Credit Card Generator“. Šių veiksmų metu, teismas patvirtino, kad banko kortelių tikrumas internetinėje svetainėje www.binlist.net negali būti nustatytas. Teismas, remdamasis „GOOGLE“ paieškos sistemos duomenimis, kurioje buvo pateikta apie 304,000,000 rezultatų, konstatavo, jog „*byloje nėra jokių objektyvių duomenų ir įrodymų, kad kaltinime išvardinti trylikos elektroninių mokėjimo priemonių duomenys, kuriuos <...>, neva, be leidimo įgijo, laikė ir neteisėtai perdavė, yra tikri ir jų pakanka realiai finansinei operacijai inicijuoti, ir kad jų tariami naudotojai ar kredito įstaigos nėra išreiškusios sutikimo jais naudotis“*[270]. Todėl, teismas, remdamasis nekaltumo prezumpcijos principu, pagal kurį visos abejonės ir (ar) neaiškumai dėl nusikalstamos veikos padarymu kaltinamo asmens kaltės ar kitų aplinkybių, turinčių reikšmės bylai išspręsti teisingai, vertinami nusikalstamos veikos padarymu kaltinamo asmens naudai, sprendė, kad asmuo nepadarė veikų, turinčių nusikaltimo ar baudžiamojo nusižengimo požymių, todėl pagal BK 214 straipsnio 1 dalį buvo išteisintas. Tačiau, apeliacinės instancijos teismas, kitaip įvertino teisiamojo posėdžio metu gautus „GOOGLE“ duomenis bei ikiteisminio tyrimo surinktus duomenis.

[268] Nuosprendis baudžiamojoje byloje Nr. 1-285-870/2017, *op. Cit.*
[269] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2020 m. kovo 24 d. nutartis baudžiamojoje byloje Nr. 2K-77-1073/2020.
[270] Utenos apylinkės teismo Ignalinos rūmų 2019 m. balandžio 29 d. nuosprendis Nr. N1-81-286/2019

Apeliacinės instancijos teismas pasisakė, jog *apylinkės teismas asmens veiksmus dėl trylikos svetimų elektroninių mokėjimo priemonių duomenų, pakankamų realiai finansinei operacijai inicijuoti, įgijimo, laikymo bei perdavimo įvertino atsietai, išskirdamas juos iš bendro nusikalstamo konteksto ir nepagrįstai juos supaprastino, remiantis teismo posėdžio metu atliktu, atsitiktiniu būdu sugeneruotos kortelės tikrumo patikrinimu, kuris net nebuvo aprašytas ir įformintas teismo posėdžio protokole*[271]. Be to, Apeliacinės instancijos teismas savo sprendimą motyvavo tuo, kad: *asmuo ikiteisminio tyrimo metu davė parodymus, jog mokėjimo kortelių duomenis įsigijo www.validcc.su internetiniame puslapyje; veiksmų neatskleidžiant savo tapatybės atlikimo protokole, kuriame užfiksuotas asmens susirašinėjimas su vartotoju „E.“, taip pat buvo nurodoma, kad mokėjimo kortelių duomenis jis įsigijo www.validcc.su; vienas iš liudytojų patvirtino, jog internetinis puslapis www.validcc.su yra svetimų mokėjimo priemonių birža, kuri garantuoja, kad joje parduodamos tik tikros kortelės; kita liudytoja nurodė, kad mokėjimo kortelių duomenų tikrumas paprastai nustatomas per viešai prieinamus interneto šaltinius (www.binlist.net, www.bincodes.com ir kt.), ir jei banko kortelės yra JAV, trečiųjų šalių piliečių, ne Europos Sąjungos, teisinės pagalbos prašymai dažniausiai nesiunčiami* [272]. Todėl, apeliacinės instancijos teismas padarė išvadą, jog kaltinime nurodytų mokėjimo priemonių duomenys yra tikri, o svetainėje www.binlist.net pateikiama informacija yra patikima, ir pripažino esant įrodyta, kad asmuo padarė tęstinę nusikalstamą veiką, nurodytą BK 214 straipsnio 1 dalyje. Tačiau, Lietuvos Aukščiausiasis Teismas, nesutiko su apygardos teismo įrodymu vertinimu dėl mokėjimo priemonės (jos duomenų) tikrumo ir pažymėjo, jog *nusikalstamos veikos padarymas, negali būti pagrįsta vien tik internetinio tinklalapio (www.binlist.net) rezultatais. Nors šis tinklalapis teikia viešą mokėjimo kortelių metaduomenų paieškos paslaugą, tačiau šaltinis, iš kurio gaunami ir tinklalapyje pateikiami duomenys, yra nežinomas. Kai kurie tinklalapio pateikiami duomenys yra grindžiami prielaida. Taip pat, paslauga gali turėti trūkumų, tinklalapyje pateikiama informacija tik apie mokėjimo kortelę išdavusią įstaigą (pagal kortelės numerio 6 ar 8 skaičius) ir kai kuriuos kitus kortelės duomenis. Naudojantis šia paslauga negalima nustatyti jos savininko duomenis, kortelės galiojimo laiką. Šias teismo išvadas patvirtino ir liudytojo parodymai, kuris nurodė, jog internetiniame tinklalapyje pateikus kortelės numerį www.binlist.net yra nustatomas tik mokėjimo priemonės išleidėjas (bankas) ir valstybė*[273]. Taigi, ikiteisminio tyrimo metu nebuvo surinkta pakankamai įrodymų pagrindžiančių kaltinamojo kaltę, skirtingų instancijų teismai priešingai vertino

[271] Panevėžio apygardos teismo Baudžiamųjų bylų skyriaus 2019 m. rugsėjo 11 d. nuosprendis baudžiamojoje byloje Nr. 1A-171-334/2019

[272] Nuosprendis baudžiamojoje byloje Nr. 1A-171-334/2019, *supra note*, 280.

[273] Nutartis baudžiamojoje byloje Nr. 2K-77-1073/2020, *supra note*, 278.

surinktas bylos aplinkybes dėl mokėjimo kortelių duomenų tikrumo. Be to, ikiteisminiame tyrime nedalyvavo specialistas. Mokėjimų kortelių tikrumą tikrino pareigūnai, atliekantys ikiteisminį tyrimą. Manytina, jog specialisto, turinčio specialių žinių dalyvavimas, būtų padėjęs išsiaiškinti kilusį klausimą dėl mokėjimo kortelių tikrumo, kadangi specialistai turi tam tikrų specialių žinių.

2001 m. lapkričio 23 d. Konvencijoje dėl elektroninių nusikaltimų elektroniniu nusikaltimu laikomi turinio nusikaltimai, susiję su vaikų pornografija. BK 309 straipsnio 2 dalyje nustatyta atsakomybė už disponavimą pornografinio turinio dalykais, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas bei atsakomybė už pasinaudojimą informacinėmis ir ryšių technologijomis ar kitomis priemonėmis įgyjant ar suteikiant prieigą prie pornografinio turinio dalykų, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas. Lietuvos policija įgyvendindama Lietuvos Respublikos kibernetinio saugumo strategijos tikslą „*užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir užkardymą*“[274], tam tikras pornografinio turinio interneto svetaines įtraukia į „STOP POLICIJA“ sąrašą, t. y. internetinėse svetainėse naršant ir stebint pornografiją, kuriose vaizduojami vaikai arba asmuo pateikiamas kaip vaikas, iššoka pranešimai „STOP POLICIJA“, kurie perspėja apie tokios informacijos neskelbtinumą ir draudžiamumą. Pavyzdžiui, Kauno apygardos teismo baudžiamojoje byloje Nr. 1A-357-530/2021 asmuo „*pasinaudodamas informacinėmis ir ryšių technologijomis įgijo ir laikė pornografinio turinio dalykus, kuriuose vaizduojami vaikai, o būtent: <...> pasinaudodamas stacionariu kompiuteriu „Nexus“ ir interneto ryšio paslaugos teikėjo akcinės bendrovės „Telia Lietuva“ jam suteiktu internetinės prieigos adresu (IP) (duomenys neskelbtini), iš internetinio tinklalapio „(duomenys neskelbtini)“ parsisiuntė ir tokiu būdu įgijo pornografinio turinio audiovizualinę elektroninę bylą (animacinį filmą), <...> kuriame vaizduojami du apytiksliai 8-10 metų berniukai, demonstruojantys savo lytinius organus ir šią elektroninę bylą laikė savo kompiuterio duomenų laikmenoje „Adata SSD Ultimate SU650“, identifikacinis numeris „(duomenys neskelbtini)“, kol <...> kratos metu pareigūnai ją paėmė.“*[275]. Asmuo ikiteisminio tyrimo metu nurodė, kad pornografinio turinio informaciją, kuriose vaizduojami vaikai rasdavo įvairiuose internetiniuose tinklalapiuose. Suvokė, kad tokia informacija disponuoti negalima, nes naršant ir stebint pornografiją su vaikais ne kartą yra iššokę pranešimai „STOP POLICIJA“, kurie perspėjo, kad tokia informacija yra draudžiama[276]. Kitoje panašioje situacijoje, Vilniaus apygardos teismo baudžiamojoje byloje Nr. 1-301-211/2018, kaltinamasis taip pat nurodė, kad jam naršant tam tikruose

[274] Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, *supra note*, 257.
[275] Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2021 m. gruodžio 8 d. nuosprendis baudžiamojoje byloje Nr. 1A-357-530/2021
[276] *Ibid*

tinklapiuose, kompiuterio ekrane kartais pasirodydavo užrašas "STOP POLICIJA", bet jis manydavo, kad tai kažkieno juokai tame tinklapyje, nes paspaudus ant to užrašo, jis iš ekrano dingdavo, o jis toliau žiūrėdavo nuotraukas bei vaizdo failus[277]. Iš bylų medžiagos matyti, jog nusikalstamas veikas įvykdė asmenys neturintys specialių žinių, kadangi ikiteisminio tyrimo metu nebuvo nustatyta, jog kaltinamieji naudojosi įdiegtomis specifinėmis programomis, siekiant paslėpti nusikaltimo pėdsakus. Tačiau, elektroninė erdvė suteikia didelių galimybių vykdyti nusikalstamas veikas, sudaro palankias sąlygas nusikalstamoms veikoms vystytis, todėl neaišku, ar asmuo sukūręs pornografinio turinio informaciją, kuriose vaizduojami vaikai ir ją patalpinęs į skaitmeninę erdvę, buvo nubaustas. Taigi, kompiuteriniai tinklai ir elektroninė informacija gali būti panaudojama darant nusikalstamas veikas. Kai vykdant nusikalstamą veiką yra naudojama tam tikra įranga, internetas ar kitoks tinklas, jis tampa elektronine nusikalstama veika.

Dažnai praktikoje pasitaikantis nusikaltimas, tai neteisėtas disponavimas narkotinėmis ar psichotropinėmis medžiagomis. Esame įpratę, jog šis nusikaltimas vyksta „čia ir dabar“, gatvėse, kažkokiose patalpose, pasilinksminimo vietose ir pan. Asmuo iš prekiautojo įsigyja tam tikrą kiekį narkotinių medžiagų ir iš karto grynaisiais pinigais, auksu, juvelyriniais dirbiniais ar kitais daiktais už jas atsiskaito. Tačiau, kaip minėta anksčiau, atsiradus informaciniams tinklams ir jų sistemoms, įprastos nusikalstamos veikos persikėlė į kibernetinę erdvę. Covid-19 pandemija taip pat paskatino elektroninėje erdvėje ieškoti galimybių įsigyti narkotikų[278]. Vykdant tarptautinę teisėsaugos operaciją, buvo sulaikyta 150 įtariamų tamsiojo interneto „Darknet“ narkotinių ir psichotropinių medžiagų prekeivių ir kitų nusikaltėlių, kurie Australijoje, Bulgarijoje, Prancūzijoje, Vokietijoje, Italijoje, Nyderlanduose, Šveicarijoje ir Jungtinėje Karalystėje pardavinėjo dešimtis tūkstančių neteisėtų prekių ir paslaugų. Tamsiajame internete „Darknet“ pardavėjų paskyros taip pat buvo nustatytos ir priskirtos tikriems asmenims, parduodantiems neteisėtas prekes internetinėse prekyvietėse[279]. Taigi, narkotikų prekybai plečiantis, ji persikėlė į skaitmeninę erdvę, tapo dar pavojingesnė. Pavyzdžiui, Vilniaus apygardos teismo baudžiamojoje byloje Nr. 1-127-576/2022, asmuo, *„būdamas savo namuose <...> iš savo nešiojamo kompiuterio "MacBookAir", prisijungęs prie tamsiojo internetinio tinklalapio „World Market“ per „Tor Browser“ naršyklę prie savo paskyros slapyvardžiu "(duomenys*

[277] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. lapkričio 21 d. nuosprendis baudžiamojoje byloje Nr. 1-301-211/2018

[278] Christina Carrega „Justice Department announces 150 arrests in operation targeting international darknet opioid trafficking“ *CNNpolitics* (2021 m. spalio 26 d.) https://edition.cnn.com/2021/10/26/politics/darknet-opioid/index.html

[279] ”Department of Justice Announces Results of Operation Dark HunTor“ *United States Drug Enforcement Administration* (2021 m. spalio 26 d.) https://www.dea.gov/press-releases/2021/10/26/department-justice-announces-results-operation-dark-huntor

*neskelbtini)", iš ikiteisminio tyrimo konkrečiai nenustatyto asmens slapyvardžiu „(duomenys neskelbtini)“ Nyderlandų Karalystėje, neturėdamas tikslo parduoti ar kitaip platinti, užsisakė nedidelį kiekį psichotropinės medžiagos – LSD (LSD popieriaus lapelį, perforacijos būdu padalintą į penkis kvadratinius mini lapelius, kurio masė 0,0503 g ir kuriame yra 0,00025 g gryno LSD), <...> už kurią sumokėjo 15,71 eurų ir nurodė šią psichotropinę medžiagą atsiųsti paštu jo vardu ir jo gyvenamosios vietos, esančios (duomenys neskelbtini), adresu ir tokiu būdu inicijavo šios psichotropinės medžiagos siuntimą, o nenustatytam asmeniui vykdant susitarimą ir šią psichotropinę medžiagą, supakuotą į pašto siuntą Nr. (duomenys neskelbtini), išsiunčiant jo nurodytu adresu bei pašto (kurjerių) tarnybų darbuotojams gabenant siuntą Nr.(duomenys neskelbtini) su minima psichotropine medžiaga nurodytu adresu, jis tokiu būdu neteisėtai, neturėdamas tikslo parduoti ar kitaip platinti, <...> iš Nyderlandų Karalystės į Lietuvos Respubliką, per Lietuvos Respublikos valstybės sieną, Vilniaus teritorinės muitinės Pašto postą, esantį Metalo g. 5, Vilniuje, siuntėsi nedidelį kiekį psichotropinės medžiagos LSD, kurios grynasis kiekis yra 0,00025 g.“*[280] Vilniaus teritorinės muitinės Mobiliųjų grupių posto vyresnioji inspektorė nurodė, jog pagal iš anksto nustatytą grafiką buvo paskirta tikrinti siuntas iš rizikingų šalių, dėl tos priežasties atrinko siuntą iš Nyderlandų karalystės. Atidarius voką, viduje rado vakumuotą permatomą maišelį, o jame – maišelį su styga, kuriame buvo spalvotas popieriaus lapelis perforacijos būdu padalintas į 5 daleles[281]. Asmuo padaręs nusikalstamą veiką buvo nuteistas pagal BK 259 straipsnio 2 dalį ir 199 straipsnį. Pažymėtina, kad tamsiajame internete „Darknet“ galima įsigyti ir kitokių prekių, štai pavyzdžiui, Klaipėdos apygardos teismo baudžiamojoje byloje Nr. 1-106-651/2018, asmuo *internete rado informaciją apie tai, kad vaistai „Modalert“ skatina smegenų veiklą, kad juos vartoja studentai, nes jie leidžia lengviau įsisavinti informaciją. Tuo metu planavo studijuoti universitete, manė, kad šie vaistai padės mokantis. Rado informaciją apie tai, kad šių vaistų galima įsigyti per tam tikrą naršyklę, t. y. tamsųjį internetą, todėl į savo kompiuterį įsidiegė programą. Žinodamas, kad šiame internete galima atsiskaityti tik virtualia valiuta „bitkoinais“, jų įsigijo atsiskaitydamas iš savo banke esančios sąskaitos už 120 eurų. „Bitkoinai“ buvo pervesti į virtualią piniginę, iš šios piniginės juos persivedė į kitą piniginę, o jau iš pastarosios pinigus pervedė vaistų pardavėjui.*[282] Kaip matyti, asmuo būdamas savo gyvenamojoje vietoje, neišeidamas iš namų, nusipirko 100 tablečių vaistų „Modalert“, kurių sudėtyje yra psichotropinės medžiagos – modafinilio. Pašto paslaugas teikianti įmonė atgabeno siuntą iš Indijos į

[280] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2022 m. vasario 7 d. nuosprendis baudžiamojoje byloje Nr. 1-127-576/2022
[281] *Ibid*
[282] Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. liepos 31 d. nuosprendis baudžiamojoje byloje Nr. 1-106-651/2018

Lietuvos Respubliką. Tačiau, teritorinės muitinės pareigūnai sulaikė minėta siuntą. Iš praktikos yra žinoma, kad siunta, užsakyta iš „darknet“ per anoniminio naršymo naršyklę iki Lietuvos paprastai yra atsiunčiama per 2–4 savaites[283]. Taigi, kaip matyti, šiai dienai užtenka prisijungti prie kompiuterinio tinklo ir taip įsigyti uždraustas prekes šalyje.

Elektroniniai nusikaltimai siaurąją prasme yra nustatyti BK XXX skyriuje, t. y. nusikaltimai, kurių dalykas elektroniniai duomenys ir informacinių sistemų saugumas. Pagal 2001 m. lapkričio 23 d. Konvenciją, vienas iš elektroninių nusikaltimų yra laikomas sąmoningas neteisėtas įtaiso, programos, kuriuo galima vykdyti elektroninius nusikaltimus bei kompiuterio slaptažodžio, kuriuo galima prieiti prie sistemos, gaminimas, pardavimas, įsigijimas, įvežimas, platinimas[284]. Tačiau pagal minėtą konvenciją šalys gali nelaikyti tokių veiksmų nusikalstamais, jei anksčiau minėtus įtaisus ar kodus nepardavinėja ar kitaip neplatina. 2020 m. įvyko „SolarWinds“ kibernetinis incidentas, kurios metu įsilaužėliai pažeidė bendrovės „SolarWinds Corp“ sukurtą programinę įrangą ir taip įsilaužėliai gavo prieigą prie JAV iždo, teisingumo ir prekybos departamentų bei kitų agentūrų elektroninių laiškų[285]. „Kibernetinės atakos buvo vykdomos kompromitavus tinklo stebėjimui ir valdymui skirtos „Orion“ programinės įrangos atnaujinimų procesą – organizacijos atsisiųsdavo atnaujinimus su kenkėjišku kodu.“[286] Be abejonės, asmenys vykdydami minėtą kibernetinę ataką, naudojosi tam tikra specialia programine įranga. Analizuojant Lietuvos teisinę sistemą šiuo klausimu matyti, jog BK 198[2] straipsnyje yra kriminalizuotas neteisėtas gaminimas, gabenimas, importavimas, pardavimas, prieigos suteikimas, kitoks platinimas ir laikymas. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo baudžiamojoje byloje Nr. 2K-199-648/2019, asmuo „*nenustatytu laiku iš nenustatyto tinklalapio į tyrimo metu nenustatytą įrenginį atsisiuntė kompiuterio programą „Spower Windows Password Reset Special“, skirtą pasirinktos operacinės sistemos „Windows“ vartotojo vardui ar slaptažodžiui pašalinti ir (arba) pridėti, ją [...] įdiegė į savo USB atmintinę „SP Silicon Power“ ir laikė iki <...> iki kratos atlikimo nuteistojo gyvenamojoje vietoje*“[287]. Be to, asmuo „*darbo metu, būdamas darbo vietoje, viešojo saugumo tarnybinėje vaizdo stebėjimo patalpoje, per interneto prieigą, kurios IP adresas (duomenys neskelbtini), naudodamasis stacionariu kompiuteriu „HP S/N CZC41521Q6*“

[283] Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2017 m. rugpjūčio 1 d. nuosprendis baudžiamojoje byloje Nr. 1-285-870/2017
[284] Konvencija dėl elektroninių nusikaltimų, *supra note,* 33
[285] Brad Heath „SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president“ *Reuters* https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R
[286] „NKSC atliko „SolarWinds” produktų kibernetinio incidento vertinimą Lietuvoje“ *Nacionalinis kibernetinio sauguo centras* (2021 m. sausio 21 d.) https://www.nksc.lt/naujienos/nksc_atliko_solarwinds_produktu_kibernetinio_incid.html
[287] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019. Teismų praktika. 2019, 52, p. 387-403

*(kompiuterio vardas „CKT-K004“), kuriame įdiegta „Microsoft Windows 7 Profesional“ operacinė sistema, prie kompiuterio USB jungties neteisėtai prijungė savo USB atmintinę „SP Silicon Power“, kurioje buvo įdiegta programa „Spower Windows Password Reset Special“, skirta pasirinktos operacinės sistemos „Windows“ vartotojo vardui ar slaptažodžiui pašalinti arba pridėti, [...] išjungė (paleido iš naujo) kompiuterį, po to vėl įjungė kompiuterį ir, panaudojęs USB atmintinėje „SP Silicon Power“ esančią programą „Spower Windows Password Reset Special“, pašalino AB „K“ paskyros „Administrator“ vartotojui priklausančius prisijungimo duomenis, t. y. tik minėtam vartotojui žinomą slaptažodį, ir sukūrė naują paskyros „Administrator“ vartotojo prisijungimo slaptažodį „Nesakysiu123““*[288]. Programa „*Spower Windows Password Reset Special*„ naudojama pamiršus slaptažodį, tačiau ją galima naudoti ir neteisėtai veiklai, t. y. pašalinti naudotoją, jei asmeniui nėra suteikta teisė naudotis kompiuteriu ar jo sistema. Programa veikia tokiu būdu: atmintinė prijungiama prie kompiuterio, kompiuteris perkraunamas, kad pasikrauti iš USB atmintinės, programa standžiajame diske suranda, kokie vartotojai sukurti ir tada su surastais operacinės sistemos vartotojais atlieka tam tikrus veiksmus, t. y. pašalinti vartotojų slaptažodžius. Pats vartotojas apie tai nieko nežinos, tol kol neprisijungs prie kompiuterio[289]. Taigi, ši programa pašalina slaptažodį, o pašalinus slaptažodį galima sukurti naują. Asmuo pirmosios instancijos teisme buvo nuteistas padaręs nusikalstamas veikas numatytas BK 198 straipsnio 1 dalyje, $198^1$ straipsnio 1 dalyje, $198^2$ straipsnio 1 dalyje. Nors BK $198^2$ dispozicijoje yra nustatyta atsakomybė asmeniui, kuris neteisėtai ar nusikalstamais tikslais įgijo ar laikė programinę įrangą, tiesiogiai skirtą ar pritaikytą nusikalstamoms veikoms daryti, tačiau kasacinis teismas savo praktikoje išaiškino, jog *$198^2$ straipsnio 1 dalyje nurodytos priemonės, tinkamos nusikalstamoms veikoms daryti, gali būti pagamintos ir teisėtu tikslu, t. y. jos gali būti dvigubo naudojimo priemonės (angl. dual-use), kurios gali būti panaudotos tiek teisėtiems, tiek ir nusikalstamiems tikslams*[290]. Kaip jau anksčiau minėta, Lietuvos teisės aktuose (nacionaliniame spragų atskleidimo tvarkos apraše, kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše ir Kibernetinio saugumo įstatymo 17 straipsnio 2 dalyje) nustatyta teisėta tam tikrų informacinių sistemų ir jų tinklų kibernetinio saugumo spragų paieška, be to asmuo užsiimantis kompiuterių ir elektroninės aparatūros priežiūra ir remontu, taip pat gali naudoti tam tikras programas. Lietuvos Aukščiausiasis Teismas, aiškindamas BK $198^2$ straipsnio 1 dalį, taip pat nurodo, jog siekiant išvengti nepagrįsto baudžiamosios atsakomybės taikymo, kai tokios priemonės yra

[288] *Ibid*
[289] Klaipėdos apylinkės teismo Klaipėdos miesto rūmų 2018 m. rugsėjo 19 . nuosprendis baudžiamojoje byloje Nr. 1-622-201/2018
[290] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015

pagamintos ir pateiktos vartotojams teisėtiems tikslams (pvz., skirtos informacinių technologijų produktų patikimumui, saugumui testuoti), būtina nustatyti tiesioginį ketinimą panaudoti tokias priemones nusikalstamai veikai daryti[291]. Be to, 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvos 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR reikalavimuose nustatomas ne tik bendras, bet ir tiesioginis ketinimas panaudoti tokias priemones vienai ar kelioms nusikalstamoms veikoms daryti[292]. Taigi, siekiant asmeniui inkriminuoti BK $198^2$ straipsnio 1 dalyje numatytą veiką, yra būtina nustatyti, jog asmuo įsigydamas programinę įrangą turi susiformavusį tikslą ją panaudoti nusikalstamais tikslais. 2001 m. lapkričio 23 d. Konvencijos 2 straipsnyje bei 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvos 2013/40/ES 3 straipsnyje nustatyta, jog kriminalizuojama neteisėta prieiga prie informacinės sistemos. Direktyvos 2013/40/ES 2 straipsnio d punkte reglamentuota, jog neteisėtumas egzistuoja, kai sistemos ar jos dalies savininkas ar kitas teisės turėtojas nesuteikė leidimo prieiti prie informacinės sistemos arba toks prisijungimas neleidžiamas pagal nacionalinę teisę[293]. Baudžiamojoje byloje Nr. 2K-199-648/2019 teismas vertindamas, ar asmuo turėjo teisėtą prieigą prie informacinės sistemos vertino:

- ar kompiuteryje, prie kurio buvo prisijungta, buvo nustatyti konfigūravimai, užtikrinę atitinkamo lygio prieigos prie šios sistemos apribojimus;
- kokiu tikslu naudojamas kompiuteris (pavyzdžiui, ruošti tarnybinius dokumentus, naudotis tarnybiniu elektroniniu paštu, taip pat, ar yra suteikta interneto prieiga);
- pareigybės aprašymą (ar nustatytos funkcijos susijusios su kibernetinio saugumo užtikrinimu, apeinant kompiuteryje įdiegtus apribojimus);
- prisijungimo prie sistemos būdą (kokia programine įranga naudojantis buvo prisijungta prie kompiuterinės sistemos);
- galiojančias įstaigos vidaus taisykles. Šiuo aspektu pažymėtina, jog įstaiga tik po įvykio priėmė VST prie VRM vado 2016 m. vasario 26 d. įsakymą dėl Viešojo saugumo tarnybos prie Vidaus reikalų ministerijos elektroninės informacijos apsaugos reikalavimų aprašo patvirtinimą, kuriame būtų nurodyta, kad sargybos viršininkui draudžiama jungtis prie kompiuterio ar prijungti išorinius

[291] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015

[292] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32013L0040&from=LT 16 punktas.

[293] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32013L0040&from=LT 2 straipsnio d punktas

prietaisus ir keisti nustatymus[294]. Šios bylos kontekste, aktualu ir kitoms įstaigoms, įmonėms ar organizacijoms laiku priimti vidaus dokumentus reglamentuojančius kibernetinį saugumą bei informuoti darbuotojus apie taikomus reikalavimus. Kaip minėta anksčiau kibernetiniai incidentai gali sukelti fizinę žalą, ji gali būti tiesioginė, t. y. pajamų praradimas ir netiesioginė – baudos (pavyzdžiui, dėl bendrojo duomenų apsaugos reglamento nesilaikymo ar partnerių, klientų sankcijos, ieškiniai teismui dėl duomenų nutekėjimo patirtos žalos atlyginimo). Kibernetinis saugumas turi tapti veiklos proceso dalimi, todėl kibernetinio saugumo politikos suformavimas, leidžia įstaigoms, įmonėms ir organizacijoms pasiekti kibernetinio saugumo atsparumo ir sąmoningumo. Be to, įmonių, įstaigų ir organizacijų kibernetinis saugumas priklauso būtent nuo žmogaus. Taigi, neįgyvendinus organizacinių kibernetinio saugumo kontrolės mechanizmų, sudaromos palankos sąlygos kibernetiniams nusikaltėliams patekti į tinklą[295].

Baudžiamojoje byloje Nr. 2K-199-648/2019, kaltinamasis skunde Lietuvos Aukščiausiajam Teismui nurodė, jog padarytas nusikaltimas nesiekia tokio pavojingumo, jog būtų tikslinga jį už šį nusikaltimą traukti baudžiamojon atsakomybėn. Tačiau kasacinės instancijos teismas baudžiamojoje byloje Nr. 2K-4-507/2016 dėl neteisėto prisijungimo prie informacinės sistemos mažareikšmiškumo yra išaiškinęs, kad neteisėtas prisijungimas prie informacinės sistemos paprastai negali būti laikomas nereikšmingu, vertinant iš baudžiamosios teisės pozicijų, ypač jei tai leido padaryti kitus neteisėtus veiksmus sistemoje[296]. Šios teisinės pozicijos laikėsi teismas ir baudžiamojoje byloje Nr. 2K-199-648/2019, jis vertindamas mažareikšmiškumą atsižvelgė į tai:

- kokioje įmonėje atlikti neteisėti prisijungimo veiksmai (analizuojamoje byloje veiksmai buvo atlikti strateginę reikšmę nacionaliniam saugumui turinčioje įmonėje);
- kokias pasekmes sukėlė ar galėjo sukelti neteisėtas prisijungimas;
- ar buvo naudojama speciali programinė įranga, kokia jos paskirtis;
- kokiais tikslais buvo prisijungiama prie sistemos;
- ar buvo susidariusi galimybė sistemoje atlikti kitus neleistinus veiksmus[297].

BK 198 straipsnio 1 dalyje nurodytos pavojingos veikos yra alternatyvios, todėl baudžiamajai atsakomybei pagal šį BK straipsnį kilti pakanka bent vienos iš jų padarymo. Todėl, aiškinant analizuojamoje situacijoje padarytas nusikalstamas veikas aktualu ir tai, kad elektroninių duomenų

[294] 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019, *supra note, 282*
[295] Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas. *Lietuvos Respublikos krašto apsaugos ministerija.* 16.
[296] kasacinė nutartis baudžiamojoje byloje Nr. 2K-4-507/2016.
[297] 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019, *supra note, 282*

panaudojimas yra galimas ne tik juos prieš tai perėmus, bet ir tokius duomenis neteisėtai įgijus ar pasisavinus. Direktyvos 2013/40/ES 6 straipsnyje, 2001 m. lapkričio 23 d. Konvencijos 3 straipsnyje nustatyta, jog elektroninių duomenų perėmimo veika yra pirmiausia siejama su informacinėje sistemoje perduodamų elektroninių duomenų gavimu, todėl toks duomenų pobūdis inkriminuojant šią BK 198 straipsnio 1 dalyje numatytą veiką turi būti įrodytas. Be to, BK 198 straipsnio 1 dalies taikymo aspektu, minėti alternatyvūs veiksmai turi būti atlikti panaudojus – neviešus elektroninius duomenis. Direktyvos 2013/40/ES 2 straipsnio b punkte nustatyta, kad elektroniniai (kompiuteriniai) duomenys – tai faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją[298]. Todėl, kasacinės instancijos teismas analizuojamoje byloje vertindamas, ar buvo panaudoti nevieši elektroniniai (kompiuteriniai) duomenys BK 198 straipsnio prasme, atsižvelgė į tai, ar asmuo neteisėtai prisijungęs prie informacinės sistemos, t. y. įgyvendinęs BK 198[1] straipsnyje numatytą veiką, gavo kitus sistemoje laikomus neviešus elektroninius duomenis[299].

Pirmąjį 2021 m. pusmetį, Lietuvoje fiksuotas išaugęs asmens duomenų nutekėjimas. Prieigos prie duomenų buvo įgautos nerafinuotais metodais, kadangi nukentėję subjektai netaikė pakankamų rizikos kontrolės priemonių. Pavyzdžiui, „CityBee“ kibernetinio incidento atveju, 2021 m. vasario 15-16 d. internetiniame forume su ribota prieiga paskelbti „CityBee“ vartotojų duomenys bei pilna „CityBee“ duomenų bazė, t. y. paskelbti elektroninio pašto adresai, slaptažodžiai, vardai, pavardės, asmens kodai, vairuotojų pažymėjimų numeriai, gyvenamosios vietos adresai, telefono numeriai[300]. Šis kibernetinis incidentas palietė apie 110 tūkst. „CityBee“ vartotojų[301], jis turėjo didelį poveikį, jo tyrime dalyvavo NKSC, tačiau visgi kaltininkas nebuvo nustatytas. Bet yra vykdomi ir mažesnio poveikio kibernetiniai incidentai, pavyzdžiui, Kauno apygardos teismo baudžiamojoje byloje Nr. 1A-477-498/2016 asmuo nuteistas už tai, kad *tam tikru laikotarpiu panaudodamas personalinį kompiuterį, kuriam priskirtas internetinės prieigos adresas IP (duomenys neskelbtini), priklausantį „(duomenys neskelbtini)" interneto klientei A. B., panaudodamas programinę įrangą – standartinę, bendros paskirties informacinių sistemų administravimo įrankius, kompiuterines komandas bei persiuntimo programą WinSCP, nuotolinio kompiuterio valdymo programas TightVNC ir PuTTY,*

[298] Direktyva 2013/40/ES, *supra note*, 106: 2 straipsnio b punktas.
[299] 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019, *supra note*, 281
[300] Nacionalinis kibernetinio saugumo centras prie krašto apsaugos ministerijos „2021 METŲ I PUSMEČIO NKSC CERT-LT ATASKAITA“ (2021 m. liepos 26 d., Vilnius), 11.
[301] Patricija Kilminavičienė „Kibernetinio saugumo ekspertai apie tai, kas ir kodėl atsitiko su „CityBee“: tiek slaptažodžių, tiek duomenų apsauga išties labai silpna“ *Lietuvos nacionalinis radijas ir televizija* (2021 m. vasario 18 d.) Kibernetinio saugumo ekspertai apie tai, kas ir kodėl atsitiko su „CityBee“: tiek slaptažodžių, tiek duomenų apsauga išties labai silpna - LRT

*pažeisdamas informacinės sistemos apsaugos priemones, neteisėtai, be G. K. žinios ir sutikimo, įsilaužė į G. K. nuomojamus serverius ir perėmė juose saugomus neviešus elektroninius duomenis – dvejas duomenų bazes su G. K. klientų asmens duomenimis, informacija apie mokėjimus ir užsakytas paslaugas, taip pat sunaikino ištrindamas serveriuose saugomą informaciją – serverių naudotojų elektroninius duomenis, serverio failus, statistiką bei iš G. K. serverio atakavo kitus serverius bei pakeitė prisijungimo ir valdymo slaptažodžius ir taip apribojo naudojimąsi duomenimis ir neteisėtai sutrikdė informacinės sistemos darbą, padarydamas nedidelę (2 896,20 eurų) žalą*[302]. Asmuo pripažintas kaltu pagal BK 196 straipsnio 3 dalį, 197 straipsnio 3 dalį, 198 straipsnio 1 dalį, 198[1] straipsnio 1 dalį. Analizuojamu atveju, nuteistasis nesinaudojo specifine programine įranga skirta įsilaužti į serverius, todėl apeliaciniame skunde buvo keltas klausimas, kaip su standartine įranga (PuTTY, TightVNC) galima pažeisti informacinės sistemos apsaugos priemones ir įsilaužti į serverius, ištrinti informaciją ir atakuoti kitus serverius. Tačiau teisminio nagrinėjimo metu dalyvavo specialistas, kuris nurodė, jog, jeigu yra tikslas pažeisti apsaugas ir gauti priėjimą prie sistemų nežinant slaptažodžių, tai su anksčiau išvardintomis priemonėmis to padaryti nėra galimybės. Bet, žinant prisijungimo slaptažodžius, juos prieš tai neteisėtai gavus, toks prisijungimas su išvardintomis priemonėmis, galimas. Be to, nuteistasis teigė, jog jis į savo kompiuterį parsisiųsdamas duomenų bazę atsisiuntė ir virusą, kuris už jį ir atliko neteisėtus veiksmus. Tačiau ikiteisminio tyrimo metu atlikta kompiuterio ekspertizė bei pateikta specialisto išvada, taip pat specialisto apklausa pirmos ir apeliacinės instancijos teismuose, paneigė šią asmens versiją. Specialistas šiuo aspektu paaiškino, kad teoriškai yra įmanoma prisijungti iš kito kompiuterio prie nuteistojo kompiuterio ir taip per jį įsilaužti į nukentėjusiojo kompiuterį, tačiau jam atliekant nuteistojo kompiuterio tyrimą, tokių požymių nebuvo nustatyta. Nuteistojo kompiuteryje tyrimo metu aptiktus esančius failus su virusais antivirusinė programa atpažino kaip infekuotus, tačiau tarp jų nebuvo rasta tam tikros programos (failo i.sql.exe), taigi nebuvo nustatyta, kad buvo aktyvuotas virusas. Taigi, specialisto išvada bei specialisto paaiškinimai patvirtino, kad į nukentėjusiojo serverius buvo įsilaužta naudojantis nuteistojo kompiuteriu ne automatiniu būdu, kas būtų įmanoma aktyvavus virusu infekuotą failą, o veikiant prie kompiuterio betarpiškai pačiam nuteistajam ir tuo tikslu panaudojant programas „WinSCP TightVNC“ ir „PuTTY“, kurios skirtos serverių administravimams nuotoliniu būdu[303]. Taigi, apeliacinės instancijos metu nuteistojo keliami klausimai buvo faktiškai paneigti specialisto išvada

[302] Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2016 m. gruodžio 21 d. nuosprendis baudžiamojoje byloje Nr. 1A-477-498/2016

[303] Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2016 m. gruodžio 21 d. nuosprendis baudžiamojoje byloje Nr. 1A-477-498/2016

bei jo parodymais. Prisimenant anksčiau analizuotą bylą Nr. Nr. 2K-199-648/2019, kurioje vertinant mokėjimo kortelių tikrumą nedalyvavo specialistas darytina išvada, kad bylose, kurios susijusios su informacinių ir ryšių technologijomis, specialisto dalyvavimas yra labai svarbus, siekiant nustatyti tiesą byloje. Specialisto išvada yra laikoma įrodymu ir nustatant bylos aplinkybes vertinama vadovaujantis tomis pačiomis taisyklėmis, kaip ir kiti byloje esantys įrodymai[304]. Kadangi informacinių ir ryšių technologijos turi išskirtinumą, jog nuolat kinta ir tobulėja, raida vyksta greitai, būtinas nuolatinis specialistų kvalifikacijos kėlimas.

2022 m. sausį kibernetinė ataka buvo nukreipta prieš Ukrainos vyriausybę. Kenkėjiška programa buvo užmaskuota taip, kad būtų panaši į išpirkos reikalaujančią programinę įrangą, tačiau iš tikrųjų buvo destruktyvi ir skirta įrenginius padaryti neveikiančius, o ne gauti išpirką. Taigi, kibernetine ataka buvo sugadintos Ukrainos vyriausybinės svetainės[305]. BK 196 straipsnyje nustatyta atsakomybė už neteisėtą poveikį elektroniniams duomenims. Ši nusikalstama veika yra padaroma alternatyviais veiksmais už kurių padarymą asmuo traukiamas atsakomybėn, t. y. elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas, pakeitimas arba galimybės naudotis tokiais duomenimis apribojimas technine, programine įranga ar kitais būdais. Taigi, anksčiau nurodytas Ukrainos atvejis, kai šalies vyriausybinės svetainės su tam tikra elektronine informacija buvo sugadintos, atitiktų BK 196 straipsnį. Norint asmeniui inkriminuoti BK 196 straipsnyje numatytą nusikalstamą veiką įstatymų leidėjas imperatyviai įtvirtino, kad nusikalstamais veiksmais turi būti padaryta žala. Dispozicijoje nėra nustatytas žalos dydis, todėl užtenka nustatyti patį žalos faktą. Nusikalstama veika yra tyčinė, gali būti padaroma tiek tiesiogine, tiek netiesiogine tyčia. Pavyzdžiui, Kauno apygardos teismo baudžiamojoje byloje Nr. 1A-543-966/2019 nuteistoji *neteisėtai prisijungė prie informacinės sistemos ir neteisėtai pašalino ir pakeitė elektroninius duomenimis padarydama žalos, t. y., būdama namuose, turėdama prisijungimo duomenis – prisijungimo vardus ir slaptažodžius, prie informacinės sistemos „TAVIS" ir UAB „A. G." VPN paskiros, kuriuos įgijo eidama Logistikos tarnybos vadovės ir informacinės sistemos "TAVIS" projekto vadovės pareigas, naudodamasi asmeniniu kompiuteriu „HP", pažeisdama UAB „T." informacinės sistemos „TAVIS" apsaugos priemones, t. y. suvesdama turėtus UAB „T." darbuotojų N. K. ir V. D. prisijungimo duomenis – prisijungimo vardus ir slaptažodžius, ir tokiu būdu informacinėje sistemoje save melagingai pristatydama šių paskyrų valdytojomis, neteisėtai prisijungė prie „TAVIS" informacinės*

[304] Baudžiamojo proceso kodekso normų, reglamentuojančių specialiųjų žinių panaudojimą, taikymo teismų praktikoje apžvalga Nr. AB-50-1.
[305] Mark Moore „Ukrainian government computer systems infected with malware: Microsoft" *New York Post* (2022 m. sausio 16 d.) https://nypost.com/2022/01/16/ukraine-gov-computer-systems-infected-with-malware-microsoft/

*sistemos ir neteisėtai pašalino bei pakeitė informacinės sistemos „TAVIS" elektroninius duomenis, dėl ko UAB „T." negalėjo atlikti būtinų ūkinės veiklos veiksmų ir patyrė 5 051,75 Eur turtinę žalą*[306]. Šioje situacijoje asmuo pripažintas kaltu pagal BK 196 straipsnio 1 dalį ir BK 198[1] straipsnio 1 dalį. Nuteistoji nesutinka, jog jos veiksmai buvo neteisėti, manė, kad jokių neteisėtų veiksmų ji neatliko, o inkriminuotų nusikalstamų veikų nepadarė, tai yra, ji teisėtai jungėsi prie informacinės sistemos bei nepažeidė sistemos apsaugos, sistemoje atliko tokius veiksmus, kuriuos turėjo teisę atlikti. Tačiau, teismas vertindamas teisėtumo klausimą nurodė, kad neteisėtumas yra viena iš baudžiamosios atsakomybės pagal BK 196 straipsnio 1 dalį sąlygų, pasireiškianti, jog asmuo atlikdamas anksčiau išvardintus alternatyvius veiksmus, nėra teisėtas elektroninių duomenų naudotojas, t. y. neturi teisėto duomenų savininko ar valdytojo leidimo naudotis ar dirbti su konkrečia informacija, atlikti jos keitimo, koregavimo veiksmus[307]. Šioje byloje, teismas vertindamas asmens neteisėtumo aspektą atsižvelgė į tai, kas yra teisėtas informacinės sistemos naudotojas, kokiu būdu buvo asmeniui paskirta dirbti su konkrečia informacine sistema (buvo paskirta sistemos administratore) bei į tai, ar veikos padarymo metu kaltinamoji dirbo įmonėje (tačiau išsiaiškinta, jog nuteistoji buvo atleista, vadinasi, neturėdama teisės minėtoje informacinėje sistemoje, kuri jai nepriklausė, negalėjo atlikti veiksmų). Pažymėtina, jog nuteistoji nusikalstamus veiksmus atliko atleidimo iš darbo dieną, tačiau teismas įvertino, jog ši aplinkybė teisinės reikšmės veiksmų kvalifikavimui neturi ir nuteistosios atsakomybės nešalina.

BK 196 straipsnio 1 dalyje numatytos nusikalstamos veikos pagrindinis objektas yra elektroninių duomenų saugumas, t. y. jų konfidencialumas, vientisumas, tapatumas ir pan., tačiau ši veika gali turėti ir fakultatyvinį objektą, kuris priklauso nuo to, kokio pobūdžio elektroniniai duomenys sunaikinami, sugadinami, pašalinami ar pakeičiami. Fakultatyviniu objektu gali būti nuosavybė, privataus gyvenimo neliečiamybė, literatūros, mokslo ar meno kūrinio autoriaus turtinės teisės ir teisėti interesai, valstybės saugumas, ekonominiai, finansiniai interesai ir kt.[308]

Kauno apygardos teismo baudžiamojoje byloje Nr. 1A-35-954/2022, asmuo *nuteistas už tai, kad būdamas ikiteisminio tyrimo metu nenustatytoje vietoje, naudodamasis nenustatyta ryšio priemone, kuriai tuo metu buvo suteiktas IP (duomenys neskelbtini) adresas, autentifikavęs savo tapatybę ir prisijungęs kaip koordinatorius e-mokymosi sistemoje prie dėstomo modulio, neteisėtai pašalino, t. y. ištrynė mokymosi įstaigos nuosavybę – medžiagą studentams pagal patvirtintą modulio*

[306] Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2019 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-543-966/2019
[307] Nutartis baudžiamojoje byloje Nr. 1A-543-966/2019, *supra note,* 301.
[308] Lietuvos Respublikos baudžiamojo kodekso komentaras 2 specialioji dalis. Vilnius, 2004. 417.

*aprašą su pateikta teorine medžiaga, seminarų užduotis, mokslinę literatūrą studentų mokymuisi, atsiskaitymų grafiką bei vertinimo metodiką. Taip padarė 1217,11 eurų turtinę žalą bei tokiu savo elgesiu pažemino dėstytojo vardą ir sumenkino mokymosi įstaigos autoritetą*[309]. Asmuo pripažintas kaltu pagal BK 196 straipsnio 1 dalį. Asmuo nurodė, kad jis pripažįsta, jog ištrynė duomenis, tačiau jo įsitikinimu ištrinti duomenys nebuvo mokymosi įstaigos nuosavybė. Nei vienas iš mokymo įstaigos atstovų, personalo darbuotojų, padalinių vadovų neinformavo, kad patalpinus į e-mokymą, jo medžiaga bus traktuojama kaip mokymo įstaigos nuosavybė. Todėl pateikus prašymą atleisti iš einamų pareigų, iš savo dėstyto modulio pasiėmė sau priklausančią medžiagą, kurią sukaupė per eilę metų[310]. Kaip matyti, šioje situacijoje nuteistasis nusikalstamos veikos padarymo metu, kaip dėstomo modulio koordinatorius ir dėstytojas, turėjo teisę prisijungti prie e-mokymosi sistemoje esančio jo dėstyto modulio, nes tuo metu jį ir mokymo įstaigą dar siejo darbiniai santykiai. Tačiau, esminis ginčas byloje buvo, ar minėta anksčiau medžiaga studentams priklauso mokymosi įstaigai ar dėstytojui. Dėl tos priežasties, teismas analizavo nuteistojo pasirašytą darbo sutartį su mokymosi įstaiga, mokymosi įstaigos vidaus teisės aktus. Teismas atlikęs analizę visgi nustatė, jog turtinės teisės į darbuotojų sukurtus autorių teisių objektus studijų srityje (studijų programas, paskaitų konspektus, metodines priemones, išskyrus vadovėlius ir monografijas), gretutinių teisių objektus 5 metams nuo sukūrimo, pereina universitetui, bei, kad turtinės autorių teisės į kūrinį, kurį sukūrė dėstytojas atlikdamas tarnybines pareigas ar darbo funkcijas, išskyrus kompiuterių programas, yra mokymosi įstaigos nuosavybė neterminuotai[311]. Tokių veiksmų atlikimas asmeniui užtraukė 5 000 eurų baudą. Taigi, šioje situacijoje asmuo savo paties subjektyviu supratimu bei vertinimu nusprendė, jog turi teisę atlikti duomenų trynimo veiksmus.

Taigi, išanalizavus baudžiamąsias bylas matoma, kad teismuose yra nusistovėjusi tam tikra praktika nagrinėjant elektroninius nusikaltimus, kuri formuoja stabilų ir nuoseklų bylos nagrinėjimą. Teismai pasisako apie būtinumą nustatyti tiesioginį ketinimą panaudoti tam tikras priemones nusikalstamai veikai daryti, išaiškino neteisėtumo aspektą, o išanalizavus elektroninių nusikaltimų, siaurąją aiškinimo prasme, bylas nustatyti kriterijai, pagal kuriuos teismai vertina, ar asmuo veikos padarymo metu turėjo teisėtą prieigą prie informacinės sistemos ar jos dalies. 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvoje 2013/40/ES nustatyta, jog elektroninių nusikaltimų atveju, tokių kaip neteisėta prieiga prie informacinių sistemų, neteisėtas įsikišimas į sistemą, neteisėtas

[309] Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2022 m. vasario 1 d. nutartis baudžiamojoje byloje Nr. 1A-35-954/2022
[310] *Ibid*
[311] Nutartis baudžiamojoje byloje Nr. 1A-35-954/2022, *op. Cit.,*

įsikišimas į duomenis, neteisėtas duomenų perėmimas, turi būti baudžiami kaip už nusikalstamą veiką, bent tais atvejais, kurie nėra mažareikšmiai[312]. Atlikus bylų analizę matyti, jog teismai turi nusistovėjusią praktiką ir laikosi tam tikrų kriterijų vertinant mažareikšmiškumo klausimą. Be to, matyti, jog specialistų dalyvavimas tiek ikiteisminiame etape, teisminio nagrinėjimo metu yra labai svarbus, kadangi padeda išaiškinti abejones, kilusius neaiškumus ar ginčus, kurie reikalauja specialių žinių. Taip pat, atlikus elektroninių bylų analizę matyti, jog įprastos, tradicinės nusikalstamos veikos, šiai dienai yra vykdomos ir kibernetinėje erdvėje, jos vykdomos naudojantis kompiuteriais bei jų sistemomis bei specialiomis programinėmis įrangomis. Išanalizuoti pavyzdžiai leidžia daryti išvadą, jog:

1. Vykdant elektroninių nusikaltimų tyrimą, pasitaiko atvejų jog stokojama informacijos, įrodančios nusikaltimo sudėties požymių. Dėl tos priežasties, lieka nenustatytas kaltinamasis, esminės faktinės bylos aplinkybės, nepakankamai surenkama duomenų pagrindžiančių kaltinamojo kaltę.

2. Žmogus yra silpniausia grandis kompiuterinėje sistemoje. Neatsakingas, lengvabūdiškas, jau tapusio įprasto laiško atvėrimas, gali sukelti didelių pasekmių. Todėl, svarbu skatinti „kibernetinę higieną“.

3. Lietuvos policija vykdo Nacionalinėje kibernetinio saugumo strategijoje įtvirtintą tikslą, t. y. kibernetinių nusikaltimų prevenciją, tačiau ši prevencija neužkerta kelio toliau vykti nusikaltimams susijusiems su vaikų pornografija.

[312] Direktyva 2013/40/ES, *supra note*, 106: 2 straipsnio b punktas.

# IŠVADOS

Magistro baigiamojo darbo ginamasis teiginys, kad Lietuvos Respublikoje yra pakankama kibernetinį saugumą reglamentuojanti teisinė bazė, pasitvirtino. Žemiau pateikiamos išvados ir pasiūlymai.

1. Kibernetiniai išpuoliai sukelia fizinį ardomąjį poveikį infrastruktūrų objektams, jų metu neteisėtai perimami asmens duomenys, pramoninė ar valstybinė informacija, kibernetinė erdvė naudojama kibernetinio puolimo veiksmams atlikti, o sukeltas poveikis sudaro grandininę reakciją. Kibernetinis saugumas yra priemonių ir metodų visuma, kuriomis siekiama sumažinti informacinių ir ryšių sistemų pažeidžiamumą nuo neteisėto poveikio, duomenų perėmimo, panaudojimo, prisijungimo prie informacinės sistemos. Kibernetinis saugumas naudoja technines, teisines bei informacinės sklaidos priemones užtikrinant informacinių ir ryšių sistemų vientisumą. Taikant veiksmingas priemones ir metodus realizuojama informacinių ir ryšių sistemų naudotojų ir kitų susijusių asmenų teisė į duomenų apsaugą. Nusikalstamų veikų kibernetinėje erdvėje sampratos aiškinimas yra dvejopas. Plačiąja prasme, tai įvairaus pobūdžio nusikalstama veika, kuri vykdoma naudojantis kompiuteriais ir informacinėmis sistemomis. Siauruoju nusikalstamų veikų kibernetinėje erdvėje sampratos aiškinimu, elektroniniais nusikaltimais laikomi specifiniai nusikaltimai kompiuteriams bei informacinėms sistemoms, išvardinti Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje, t. y. neteisėtas poveikis elektroniniams duomenims, informacinei sistemai, neteisėtas elektroninių duomenų perėmimas ir panaudojimas, neteisėtas prisijungimas prie informacinės sistemos bei neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis.

2. Europos Sąjungoje priimti reglamentai ir direktyvos sukūrė kibernetinį saugumą užtikrinančią teisinę sistemą, bendrą kibernetinės erdvės politiką bei suderintą baudžiamąją teisę atakų prieš informacines sistemas srityje. Taip pat nustatytos konkrečios priemonės bendram aukštam tinklų ir informacinių sistemų saugumo lygiui užtikrinti bei ribojamosios priemonės skirtos kovai su kibernetiniais išpuoliais. Lietuvos Respublika būdama Europos Sąjungos nare prisiėmė konkrečias direktyvomis bei reglamentais nustatytas pareigas. Lietuvos teisinė sistema pakankama didinant kibernetinį atsparumą, stiprinant kibernetinę gynybą, kovojant su nusikalstamomis veikomis kibernetinėje erdvėje, saugant ypatingos svarbos infrastruktūrą.

3. Nusikalstamos veikos kibernetinėje erdvėje turi išskirtinumą, jog vykdomos kaltininkui nutolus nuo įrenginių dideliu atstumu, virtualioje erdvėje, o žalos kilimo vieta nesutampa

su neteisėtų veiksmų padarymo vieta. Todėl užtikrinant kibernetinį saugumą dalyvauja atskiros specialios institucijos, kurių bendras siekis bendradarbiavimu užkardyti kibernetinius incidentus. Įsteigtos kompetentingos institucijos palengvina nusikalstamų veikų tyrimą, keitimąsi duomenimis bei aktualia informacija, gerąja praktika, didina kiekvienos šalies kibernetinį atsparumą.

4. Teismų praktikos analizė leidžia teigti, jog nusikalstamų veikų kibernetinėje erdvėje tyrimas bei nagrinėjimas yra specifiškas, reikalaujantis specialių žinių. Viena esminių problemų, kuri pastebima atlikus bylų analizę, jog ikiteisminio tyrimo metu nepakankamai surenkama duomenų, dėl ko lieka nenustatyti kaltinamieji, faktinės bylos aplinkybės. Be to pastebima, jog visgi žmogus yra silpniausia grandis kompiuterinėje sistemoje, todėl neužtenka turėti aukšto kibernetinio atsparumo priemonių, reikia skatinti „kibernetinę higieną“. Galiausiai atlikus teismų praktikos analizę nustatyti kriterijai, kuriais vertinama, ar asmuo veikos padarymo metu turėjo teisėtą prieigą prie informacinės sistemos ar jos dalies bei mažareikšmiškumo vertinimo aspektas.

## PASIŪLYMAI

1. Skatinti informacinių ir ryšių technologijų vartotojus dalyvauti baziniuose kibernetinio saugumo mokymuose, užtikrinant asmeninę „kibernetinę higieną“, kurių metu asmenys įgys praktinių bei kasdienių įgūdžių didinančių jų atsparumą prieš nusikalstamas veikas kibernetinėje erdvėje.

2. Įtvirtinti informacinių ir ryšių technologijų produktams, paslaugoms ir procesams, turintiems didelių atakų riziką, privalomą kibernetinio saugumo sertifikavimą, kuris apsaugos nuo galimų nusikalstamų veikų kibernetinėje erdvėje bei žinomų pažeidžiamumo spragų.

3. Skatinti kibernetinio saugumo subjektus įtvirtinti jų sistemose koordinuotą kibernetinio saugumo spragų paiešką, kurios metu etiški kompiuterių įsilaužėliai ieškos kibernetinio saugumo spragų, o radus praneš sistemų savininkui.

# LITERTŪROS SĄRAŠAS

Įstatymai ir kiti teisės aktai


1. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB). https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:31995L0046&from=LT
2. 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų (Budapeštas). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195
3. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva Nr. 2002/20/EB. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0020&from=LT
4. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos Reglamentas Nr. 2002/22/EB. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0022&from=LT
5. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0021&from=LT
6. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos Reglamentas Nr. 2002/58/EB https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32002L0058&from=lt
7. 2004 m. kovo 10 d. Europos Parlamento ir Tarybos Reglamentas (EB) Nr. 460/2004. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32004R0460&from=EN
8. 2006 m. birželio 19 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 601 dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo.
9. 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos Reglamentas (ES) Nr. 526/2013 dėl Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA), kuriuo panaikinamas Reglamentas (EB) Nr. 460/2004 https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32013R0526&from=EN
10. 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32013L0040&from=LT
11. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) Nr. 2016/1148, dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=LT

12. 2017 m. vasario 1 d. Komisijos įgyvendinimo sprendime (ES) 2017/179, kuriuo pagal Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti 11 straipsnio 5 dalį nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32017D0179&from=GA
13. 2018 m. birželio 27 d. Lietuvos Respublikos Kibernetinio saugumo įstatymas Nr. XIII-1299 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c>
14. 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) Nr. 2018/1972. 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (nauja redakcija)Tekstas svarbus EEE. (europa.eu)
15. 2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
16. 2018 m. rugpjūčio 13 d. Lietuvos Respublikos vyriausybės nutarimas Nr. 818, Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo. Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
17. 2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 818, Nacionalinis kibernetinių incidentų valdymo planas 818 Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo (lrs.lt)
18. 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 Dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas). https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019R0881&from=LTrepository.mruni.eu/bitstream/handle/007/10657/489-843-2-PB.pdf?sequence=1&isAllowed=y>
19. 2019 m. gegužės 17 d. Tarybos reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32019R0796&from=EN#d1e486-1-1
20. 2019 m. gegužės 17 d. Tarybos sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais. https://eur-

lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019D0797&qid=1629630537371&from=EN

21. 2020 m. lapkričio 20 d. Tarybos įgyvendinimo reglamentas (ES) 2020/1744, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32020R1744&from=en
22. 2020 m. liepos 30 d. Tarybos įgyvendinimo reglamentas (ES) 2020/1125, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32020R1125&from=EN
23. 2020 m. spalio 22 d. Tarybos įgyvendinimo reglamentas (ES) 2020/1536, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32020R1536&from=EN
24. 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/821, nustatantis Sąjungos dvejopo naudojimo prekių eksporto, persiuntimo, susijusių tarpininkavimo paslaugų, techninės pagalbos ir tranzito kontrolės režimą.
25. 2021 m. liepos 9 d. Lietuvos Respublikos Krašto apsaugos ministro įsakymas Nr. V-484, Dėl nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/270e6bd1e08911eb866fe2e083228059
26. Europos kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“ (Europos Komisijos Bendras komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui, 2013). https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52013JC0001&from=lt
27. Europos Parlamento ir Tarybos reglamentas (ES) (2016/679) „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“. 2016. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679.
28. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija 1950 m. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841
29. JT Generalinės asamblėja „Visuotinė žmogaus teisių deklaracija“ 1948 m. Gruodžio 10 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385

30. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis. 1981 m. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872
31. „Kibernetinio saugumo strategija“ Europos komisija. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
32. Lietuvos Respublikos administracinių nusižengimų kodeksas. https://www.infolex.lt/ta/336765:str479
33. Lietuvos Respublikos Kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428, 3 straipsnis.
34. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 6, 8, 9, 13 straipsnių, V skyriaus pavadinimo, priedo pakeitimo ir įstatymo papildymo 17 straipsniu ir VI skyriumi įstatymo ir Lietuvos Respublikos administracinių nusižengimų kodekso papildymo $480^1$ straipsniu ir 589 straipsnio bei priedo pakeitimo įstatymo projektų aiškinamasis raštas
35. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 5 d. nutarimas Nr. 818, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

**Specialioji literatūra**

1. „2020 m. Nacionalinio kibernetinio saugumo ataskaita“ *Lietuvos Respublikos krašto apsaugos ministerija* (Vilnius, 2021 m. balandžio 7 d.) https://www.nksc.lt/doc/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf
2. „ENISA annual report“ *European Union Agency for Network and Information Security* (2013). https://www.enisa.europa.eu/publications/corporate/enisa-annual-report-2013
3. 2010 m. lapkričio 25 d. Europos Sąjungos Taryba pažangos ataskaita Nr. 16835/10. https://data.consilium.europa.eu/doc/document/ST%2016835%202010%20INIT/EN/pdf .
4. A. H. Maslow „A Theory of Human Motivation“, Psychological Review, 50, 370-396, (1943) http://psychclassics.yorku.ca/Maslow/motivation.htm
5. Alexandre de Streel ir Hocepied, Christian, „*The EU Regulation of electronic communications networks and services*“ (P.L. Parcu and E. Brogi (eds), Research handbook on EU media law and policy, E. Elgar, forthcoming, 2021). https://ssrn.com/abstract=3897368
6. Annegret Bendiek ir Eva Pander Maat „The EU‘s Regulatory Approach to Cyber-security“ *German institute for International and Security Affairs* (2019). https://www.swp-

berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf

7. Audronė Petrauskaitė, Rolanda Kazlauskaitė, Markelienė Rasa Gedminienė „*Šalies saugumas ir gynyba*“ (Generolo Jono Žemaičio Lietuvos karo akademija, 2016).
8. Cyber Rapid Response Teams and mutual assistance in cyber security. Memo for Mutual Assistance in Cyber Security Key Roles and Procedures for the CRRTs' Operations Lessons Learnt from the Cyber Shield. Amber Mist 2018 Exercise.
9. Darius Štilis ir kt. „*Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo teisinio reguliavimo aspektai*“. (Mykolo Romerio universitetas, 2011). https://repository.mruni.eu/handle/007/16821
10. Darius Štitilis "Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos". (2013) https://repository.mruni.eu/bitstream/handle/007/10657/489-843-2-PB.pdf?sequence=1&isAllowed=y>
11. Darius Štitilis „Elektroniniai nusikaltimai“ (Mykolo Romerio universitetas, 2011) https://repository.mruni.eu/bitstream/handle/007/16884/9789955193296.pdf?sequence=1&isAllowed=y
12. Darius Štitilis ir kt. „Concepts and principles of cyber security strategies“. (Mykolo Romerio universitetas, 2016). http://jssidoi.org/jssi/uploads/papers/22/Stitilis_Concepts_and_principles_of_cyber_security_strategies.pdf
13. Darius Štitilis ir kt. „*Interneto ir technologijų teisė*“ (Mykolo Romerio Universitetas, 2016) https://repository.mruni.eu/bitstream/handle/007/16211/17_Interneto%20or%20technologij%c5%b3%20teis%c4%97.pdf?sequence=1&isAllowed=y
14. D. Štitilis ir kt. „Rekomendacijos Lietuvos Respublikos kibernetinio saugumo įstatymui“ (Mykolo Romerio universitetas, 2017). https://repository.mruni.eu/bitstream/handle/007/14643/Rekomendacijos_Kibernetinio_saugumo_istatymui(galutinis).pdf?sequence=1
15. Darko Galinec, Darko Mažnik ir Boris Guberina *"*Cybersecurity and cyber defence: national level strategic approach*"* 2017. https://www-tandfonline-com.skaitykla.mruni.eu/doi/pdf/10.1080/00051144.2017.1407022?needAccess=true
16. Dimitra Markopoulou, Vagelis Papakonstantinou ir Paul de Hert „*Computer Law & Security Review, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the*

*General Data Protection Regulation*“ (2019) https://reader.elsevier.com/reader/sd/pii/S0267364919300512?token=2FCDD8A5D808316F4E93B494FCCC3591F0C822356B57CC5D8655712DB31481BC00AA50A23F14C63B9CBF5A4AABB781FD&originRegion=eu-west-1&originCreation=20220202192714

17. Europos Komisijos komunikatas Tarybai ir Europos Parlamentui „Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas“ 2012. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52012DC0140&from=LT
18. Goda Užkuraitytė „Kibernetinio saugumo valdymo užtikrinimas: Pasaulinė patirtis ir Lietuvos perspektyva“ (magistro baigiamasis darbas Mykolo Romerio universitetas, 2015) 24 puslapis.
19. J. L. Hernandez-Ramos, S. N. Matheu ir A. Skarmeta, "*The Challenges of Software Cybersecurity Certification“(*2021), 1. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9336084
20. Justas Kidykas, Rūta Beinoriūtė ir Gabrielė Bilevičiūtė „Pasiūlymai dėl smulkaus ir vidutinio verslo kibernetinio saugumo brandos kėlimo Lietuvoje“ *„Kurk Lietuvai“ projektas,* (2020). http://kurklt.lt/wp-content/uploads/2020/03/Rekomendacijos-KAM-ir-NKSC-Kurk-Lietuvai.pdf
21. Miglė Stašikytė “Kibernetinio saugumo diskursas Lietuvos internetinėje žiniasklaidoje” (magistro baigiamasis darbas, Vytauto Didžiojo universitetas, 2014)
22. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019 metų vertinimo kriterijų rezultatai.
23. Nacionalinis kibernetinio saugumo centras prie krašto apsaugos ministerijos „2021 METŲ I PUSMEČIO NKSC CERT-LT ATASKAITA“ (2021 m. liepos 26 d., Vilnius).
24. Nikolaj Goranin, Dalius Mažeika „Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos“ (Vilnius: UAB „TEV“, 2011). http://www.esparama.lt/documents/10157/490675/Nusikaltimai_elektronineje_erdveje_ir_ju_tyrimo_metodikos.pdf
25. Renata Marcinauskaitė „Neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai ir kvalifikavimo problemos“ (Vytauto Didžiojo universitetas, 2016), https://portalcris.vdu.lt/server/api/core/bitstreams/82500ab8-69a0-43ec-adb6-12997b9b88d4/content

26. Renata Marcinauskaitė „Nusikalstamos veikos elektroninėje erdvėje ir teritorinė baudžiamoji jurisdikcija“ (Mykolo Romerio universitetas, 2021), https://ojs.mruni.eu/ojs/jurisprudence/article/download/6620/5421
27. Sarah Gordon, Richard Ford „On the definition and classification of cybercrime“ http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.302.2178&rep=rep1&type=pdf
28. Stefan Soesanto “Europe Has No Strategy on CyberSanctions” (2020) https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions
29. U.S. Department of commerce, National Bureau of standards, Washington. Theodore A. Linden „Operating System Structures To Support Security and Reliable Software“. (1976)
30. Vaidas Kalpokas „Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos“ (2009). https://teise.org/wp-content/uploads/2016/10/2009-1-kalpokas.pdf

**Internetiniai puslapiai**

1. „About FIRST“ *Forum of Incident Response and Security Teams*. https://www.first.org/about/
2. „About us“ *TechTarget*. https://www.techtarget.com/about-us/
3. „About us“ *The Wassenaar arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies* https://www.wassenaar.org/about-us/
4. ”Certification Schemes and CABs – FAQ“ *European Union Agency for cybersecurity ENISA* https://www.enisa.europa.eu/topics/standards/certification/certification-schemes-and-cabs/certification-schemes-and-cabs-faq
5. ”Department of Justice Announces Results of Operation Dark HunTor“ *United States Drug Enforcement Administration* (2021 m. spalio 26 d.) https://www.dea.gov/press-releases/2021/10/26/department-justice-announces-results-operation-dark-huntor
6. „Cyber rapid response teams and mutual assistance in cyber security (CRRT)“ *Permanent Structured Cooperation (PESCO)*. https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
7. „CSIRT pagal šalį – interaktyvus žemėlapis“ *European Union Agency for Cybersecurity*. (2022). https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Estonia
8. „Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace“ *European Council Council of the European Union* (2019 m. gegužės 6 d.) https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/

9. „ECSM – Recommendations for ALL“ *European Union Agency for cybersecurity*. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month/2014/ecsm-recommendations-for-all-lt
10. „Esate tikras, kad niekada nepatyrėte kibernetinės atakos? Pasitikrinkite, ar tikrai“ *Samsung*, 2019 m. spalio 3 d. https://www.samsung.com/lt/news/local/esate-tikras-kad-niekada-nepatyrete-kibernetines-atakos-pasitikrinkite-ar-tikrai/
11. „German security office warned German firms about Chinese hacking – report“ *Reauters* (2018) https://www.reuters.com/article/uk-germany-security-idUKKBN1OI0HS
12. „Į Baltarusiją neleista eksportuoti dvigubos paskirties įrangos, pritaikytos informacijos šifravimui“, *Lietuvos Respublikos Muitinė,* 2022 m. sausio 25 d. https://lrmuitine.lt/web/guest/naujienos/aktualijos/aktualija?p_p_id=EXT_WPLISTALLNEWS&p_p_lifecycle=0&_EXT_WPLISTALLNEWS_obj_id=090004d28015ca9f
13. „Informacinių technologijų žodynas“ *ISO*. https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en
14. „Informavimas apie saugumo spragas“ *Paysera* https://www.paysera.lt/v2/lt-LT/saugumas/pranesimai-apie-saugumo-spragas
15. „Interpol“ Lietuvos Respublikos Vyriausybė. https://policija.lrv.lt/lt/tarptautinis-bendradarbiavimas/musu-partneriai/tarptautines-organizacijos/interpol
16. „IP adreso slėpimas naudojant „NordVPN““ *NordVPN* https://nordvpn.com/lt/features/hide-ip/
17. „Kas yra kompiuterinė įranga“ *Micron Technology, Inc.* https://www.crucial.com/articles/pc-builders/what-is-computer-hardware
18. „Kibernetinio saugumo apžvalga“ *Apžvalga* http://apzvalga.eu/images/kibernetinis_saugumas.pdf 13 p.
19. „Kibernetinio saugumo hakatonas“ *DELTA1* https://delta1.lt/wp-content/uploads/2021/10/DELTA1-temos.pdf
20. „Klausimai ir atsakymai. ES kibernetinis saugumas“ *Europos Komisija (*2019 m. birželio 26 d.) https://ec.europa.eu/commission/presscorner/detail/lt/QANDA_19_3369
21. „Lietuva – ketvirta geriausiai kibernetinį saugumą užtikrinanti Europos valstybė“ *Nacionalinis kibernetinio saugumo centras* (2021 m. birželio 29 d.) https://www.nksc.lt/naujienos/lietuva__ketvirta_geriausiai_kibernetini_sauguma_u.html

22. „Locked Shield“ *NATO kooperatyvo kibernetinės gynybos kompetencijos centras* https://ccdcoe.org/exercises/locked-shields/
23. „Nacionalinė kibernetinio saugumo strategija“ Lietuvos Respublikos krašto apsaugos ministerija (2019 m. vasario 22 d.)
24. „New NATO hub will gather the Alliance's cyber defenders“ *NCIA-NATO Communications and Information Agency* ( 2019 m. vasario 12 d.) https://www.ncia.nato.int/about-us/newsroom/new-nato-hub-will-gather-the-alliances-cyber-defenders.html
25. „NKSC atliko „SolarWinds” produktų kibernetinio incidento vertinimą Lietuvoje“ *Nacionalinis kibernetinio sauguo centras* (2021 m. sausio 21 d.) https://www.nksc.lt/naujienos/nksc_atliko_solarwinds_produktu_kibernetinio_incid.html
26. „NKSC vykdys nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas“ *Nacionalinis kibernetinio saugumo centras* (2021), https://www.nksc.lt/naujienos/nksc_vykdys_nacionalines_kibernetinio_saugumo_sert.html
27. „Nuolatinis struktūrizuotas bendradarbiavimas (PESCO)“ *Lietuvos Respublikos krašto apsaugos ministerija*, 2017 m. gruodžio 19 d. https://kam.lt/lt/tarptautinis_bendradarbiavimas/europos_sajunga_612/pesco.html
28. „Partneriai“ *Nacionalinis kibernetinio saugumo centras* https://www.nksc.lt/en/partners.html
29. „Paslaugų sąrašas“ *Nacionalinis kibernetinio saugumo centras.* Paslaugos | NKSC
30. „Pramonė 4.0“ *Lietuvos Respublikos ekonomikos ir inovacijų ministerija*. https://eimin.lrv.lt/lt/veiklos-sritys/pramone/pramone-4-0
31. „Pranešti apie spragą“ *Nacionalinis kibernetinio saugumo centras* https://www.nksc.lt/pranesti-spraga.html
32. „Prekyba dvejopo naudojimo prekėmis: priimtos naujos ES taisyklės“ *Europos Vadovų Taryba Europos Sąjungos Taryba* (2021 m. gegužės 10 d.). https://www.consilium.europa.eu/lt/press/press-releases/2021/05/10/trade-of-dual-use-items-new-eu-rules-adopted/
33. „Security Tip (ST04-001) What is Cybersecurity?“ *The Cybersecurity and Infrastructure Security Agency* 2009 m. gegužės 6 d. https://us-cert.cisa.gov/ncas/tips/ST04-001
31. Sharon Shea, Alexander S. Gillis, Casey Clark “Cybersecurity” *TechTarget.* 2021 m. rugpjūtis. https://searchsecurity.techtarget.com/definition/cybersecurity

34. „Strateginių ir dvejopos paskirties prekių licencijavimas ir kontrolė“ *Lietuvos Respublikos muitinė* (2021 m. lapkričio 15 d.) https://lrmuitine.lt/web/guest/verslui/apribojimai/strateginesprekes
35. „Surask klaidą programa“ *SpectroCoin* https://spectrocoin.com/lt/surask-klaida-programa.html
36. „Šifravimas reikšmė“ *Lietuvių žodynas*, https://www.lietuviuzodynas.lt/terminai/Sifravimas
37. „Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information“ *Jungtinių Valstijų Teisingumo departamento Viešųjų reikalų ministerija,* (2018) https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
38. „Veiklą oficialiai pradeda Regioninis kibernetinės gynybos centras“ *Lietuvos Respublikos krašto apsaugos ministerija,* (2021 m. liepos 15 d.) http://kam.lt/lt/naujienos_874/aktualijos_875/veikla_oficialiai_pradeda_regioninis_kibernetines_gynybos_centras
39. „Veikla“ *Nacionalinis kibernetinio saugumo centras*. Veikla, uždaviniai, sritys | NKSC
40. „What are EU cybersecurity certification schemes?“ *European Union Agency for cybersecurity*. https://www.enisa.europa.eu/topics/standards/certification/certification-schemes-and-cabs/certification-schemes-and-cabs-faq
41. „Wassenaar arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies“ Bureau of Nonproliferation Department of State https://1997-2001.state.gov/global/arms/np/mtcr/000322_wassenaar.html
42. Brad Heath „SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president“ *Reuters* https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R
43. Christina Carrega „Justice Department announces 150 arrests in operation targeting international darknet opioid trafficking“ *CNNpolitics* (2021 m. spalio 26 d.) https://edition.cnn.com/2021/10/26/politics/darknet-opioid/index.html
44. Europien Union Agency for Cybersecurity „*Apie ENISA*“. Prieiga internetu: https://www.enisa.europa.eu/about-enisa
45. Europolo oficialus tinklalapis. Prieiga internetu: https://www.europol.europa.eu/about-europol

46. Europos kovos su elektroniniu nusikalstamumu centras Europole. Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:230806_1
47. „Top Sams of 2021“ *Fraud.org* (2022) https://fraud.org/wp-content/uploads/2022/01/2021-top-scams-report-final.pdf
48. Irma Kirklytė „I. Kirklytė: kas yra kibernetinis incidentas ir ko imtis jam įvykus“ *Infolex* (2021 m. spalio 11 d.) https://www.infolex.lt/portal/start.asp?act=news&Tema=54&str=89117
49. Mark Moore „Ukrainian government computer systems infected with malware: Microsoft“ *New York Post* (2022 m. sausio 16 d.) https://nypost.com/2022/01/16/ukraine-gov-computer-systems-infected-with-malware-microsoft/
50. Patricija Kilminavičienė „Kibernetinio saugumo ekspertai apie tai, kas ir kodėl atsitiko su „CityBee“: tiek slaptažodžių, tiek duomenų apsauga išties labai silpna“ *Lietuvos nacionalinis radijas ir televizija* (2021 m. vasario 18 d.) Kibernetinio saugumo ekspertai apie tai, kas ir kodėl atsitiko su „CityBee“: tiek slaptažodžių, tiek duomenų apsauga išties labai silpna - LRT
51. Pranešti apie spragą“ *Nacionalinis kibernetinio saugumo centras* https://www.nksc.lt/pranesti-spraga.html
52. Roland Klein „*Trimming Pegasus Wings: International Export Control Law and Cyberweapons*“ (2021). Trimming Pegasus’ Wings (vifa-recht.de)
53. Šiaurės Atlanto Sutarties Organizacija (NATO) „*The Cybersecurity Reference Curriculum“* (2016), 63. 1610-cybersecurity-curriculum.pdf (nato.int)

**Teismų praktika**

1. 2006 m. gegužės 2 d. Teisingumo Teismo (didžiosios kolegijos) sprendimas byloje Nr. C-217/04. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:62004CJ0217&qid=1644940795442&from=EN
2. kasacinė nutartis baudžiamojoje byloje Nr. 2K-4-507/2016).
3. Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2016 m. gruodžio 21 d. nuosprendis baudžiamojoje byloje Nr. 1A-477-498/2016
4. Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2019 m. spalio 22 d. nutartis baudžiamojoje byloje Nr. 1A-543-966/2019
5. Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2021 m. gruodžio 8 d. nuosprendis baudžiamojoje byloje Nr. 1A-357-530/2021
6. Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2022 m. kovo 8 d. nutartis baudžiamojoje byloje Nr. 1A-29-383/2022

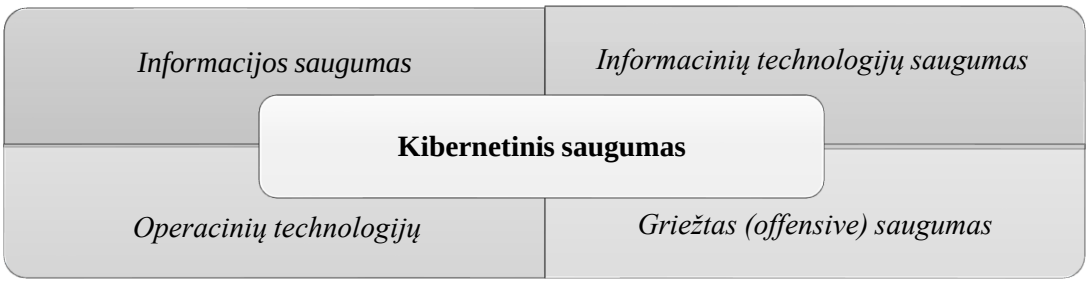
7. Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2022 m. vasario 1 d. nutartis baudžiamojoje byloje Nr. 1A-35-954/2022
8. Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2022 m. vasario 1 d. nutartis baudžiamojoje byloje Nr. 1A-35-954/2022
9. Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. liepos 31 d. nuosprendis baudžiamojoje byloje Nr. 1-106-651/2018
10. Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2021 m. lapkričio 25 d. nutartis baudžiamojoje byloje Nr. 1A-177-417/2021
11. Klaipėdos apylinkės teismo Klaipėdos miesto rūmų 2018 m. rugsėjo 19 . nuosprendis baudžiamojoje byloje Nr. 1-622-201/2018
12. Lietuvos apeliacinio teismo 2018 m. liepos 13 d. nuosprendis baudžiamojoje byloje Nr. 1A-311-396/2018
13. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015
14. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015
15. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019. Teismų praktika. 2019, 52, p. 387-403
16. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2020 m. kovo 24 d. nutartis baudžiamojoje byloje Nr. 2K-77-1073/2020.
17. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2021 m. kovo 29 d. nutartis baudžiamojoje byloje Nr. 2K-25-628/2021
18. Lietuvos Respublikos Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas byloje Nr. 7/03-41/03- 40/04-46/04-5/05-7/05-17/05 dėl Lietuvos Respublikos baudžiamojo proceso kodekso 131 straipsnio 4 dalies (2001 m. rugsėjo 11 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai, dėl Lietuvos Respublikos baudžiamojo proceso kodekso 234 straipsnio 5 dalies (2003 m. balandžio 10 d., 2003 m. rugsėjo 16 d. redakcijos), 244 straipsnio 2 dalies (2003 m. balandžio 10 d., 2003 m. rugsėjo 16 d. redakcijos), 407 straipsnio (2003 m. birželio 19 d. redakcija), 408 straipsnio 1 dalies (2002 m. kovo 14 d. redakcija), 412 straipsnio 2 ir 3 dalių (2002 m. kovo 14 d. redakcija), 413 straipsnio 5 dalies (2002 m. kovo 14 d. redakcija), 414 straipsnio 2 dalies (2002 m. kovo 14 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai ir dėl pareiškėjo – Šiaulių rajono apylinkės teismo prašymų ištirti, ar Lietuvos Respublikos

baudžiamojo proceso kodekso 410 straipsnis (2002 m. kovo 14 d. redakcija) neprieštarauja Lietuvos Respublikos Konstitucijai. http://www.lrkt.lt/dokumentai/2006/ n060116.htm.

19. Panevėžio apygardos teismo Baudžiamųjų bylų skyriaus 2019 m. rugsėjo 11 d. nuosprendis baudžiamojoje byloje Nr. 1A-171-334/2019
20. Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 27 d. nuosprendis baudžiamojoje byloje Nr. 1-17-744/2018
21. Šiaulių apygardos teismo Baudžiamųjų bylų skyriaus 2021 m. liepos 15 d. nutartis baudžiamojoje byloje Nr. 1S-87-316/2021
22. Utenos apylinkės teismo Ignalinos rūmų 2019 m. balandžio 29 d. nuosprendis Nr. N1-81-286/2019
23. Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2017 m. rugpjūčio 1 d. nuosprendis baudžiamojoje byloje Nr. 1-285-870/2017
24. Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. lapkričio 21 d. nuosprendis baudžiamojoje byloje Nr. 1-301-211/2018
25. Vilniaus apygardos teismo Baudžiamųjų bylų skyriaus 2022 m. vasario 7 d. nuosprendis baudžiamojoje byloje Nr. 1-127-576/2022

# PRIEDAI

1 PRIEDAS




1 pav. Kibernetinio saugumo elementai (D. Galinec, D. Mažnik ir B. Guberina, 2017)

| Šalis | Kibernetinio saugumo apibrėžimas |
|---|---|
| **Kanada** | Tinkamo saugumo lygio užtikrinimas (kibernetinės atakos metu, t. y. tyčinio neteisėtos prisijungimo, naudojimo, valdymo ar sunaikinimo atveju) kurios metu naudojamasi elektroninės informacijos priemonėmis ir (arba) naudojant fizinę infrastruktūrą. |
| **Prancūzija** | Informacijos sistema leidžianti pasipriešinti įvykiams, kurie gali pakenkti prieinamumui, vientisumui ar saugumui duomenų, kurie yra saugojami, apdorojami ar perduodami tarp informacijos ir ryšių sistemų. |
| **Vokietija** | Globalaus kibernetinio saugumo tikslas yra informacinių technologijų saugumo rizikų sumažinimas iki priimtino lygio. |
| **Austrija** | Infrastruktūrų saugumas kibernetinėje erdvėje, kurioje asmenys keičiasi duomenimis |

2 pav. Kibernetinio saugumo samprata skirtingose šalyse (Užkuraitytė, 2014)

Esminių paslaugų operatorius yra viešojo arba privačiojo sektoriaus subjektas, kuris teikia būtiną paslaugą, siekiant užtikrinti ypatingos svarbos visuomeninės ir (arba) ekonominės veiklos vykdymą. Šios paslaugos priklauso nuo tinklų ir informacinių sistemų ir įvykęs incidentas turėtų didelį trikdomąjį poveikį tos paslaugos teikimui (pavyzdžiui: elektros energijos įmonės, naftotiekių operatoriai, dujų tiekimo įmonės, oro uosto valdymo organai, geležinkelių infrastruktūros valdytojai, kredito įstaigos, sveikatos priežiūros paslaugų teikėjai ir t.t.). Esminių paslaugų operatoriai atlieka labai svarbų vaidmenį ekonomikoje bei visoje visuomenėje, todėl jie turi būti itin atsparūs kibernetiniams incidentams[313].

Skaitmeninių paslaugų teikėjas yra juridinis asmuo, kuris teikia skaitmenines paslaugas.[314] Skaitmeninė paslauga - tai bet kuri informacinės visuomenės paslauga, t. y. paprastai už atlyginimą per atstumą, elektroninėmis priemonėmis ir asmenišku paslaugų gavėjo prašymu teikiama paslauga.[315] Skaitmeninių paslaugų rūšys yra šios:

1. *elektroninė prekyvietė* – tai skaitmeninė paslauga, leidžianti vartotojams ir (arba) prekiautojams sudaryti elektroninės prekybos ar paslaugų sutartis prekybos svetainėse;

2. *interneto paieškos sistema* – tai skaitmeninė paslauga, leidžianti vartotojams vykdyti paieškas svetainėse pagal užklausą bet kuria tema

3. *debesijos kompiuterijos paslauga* – tai skaitmeninė paslauga, kuri suteikia prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės[316].

[313] Europos komisijos atskaita Europos Parlamentui ir Tarybai, kurioje pagal Direktyvos 2016/1148/ES dėl tinklų ir informacinių sistemų saugumo 23 straipsnio 1 dalį vertinamas požiūrio, kurio laikosi valstybės narės identifikuodamos esminių paslaugų operatorius, nuoseklumas, (2019). https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52019DC0546&from=EN

[314] Reglamentas (ES) Nr. 2016/1148, *op. Cit.*, 4 straipsnio 4, 6 dalys.

[315] 2015 m. rugsėjo 9 d. Europos Parlamento ir Tarybos Reglamentas (ES) Nr. 2015/1535. 1 straipsnio b punktas. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32015L1535&from=LT

[316] Reglamentas (ES) Nr. 2016/1148, *supra note*, 106: 4, 5 straipsniai.

• *Bazinį*. Garantuojamas IRT produktų, paslaugų ir procesų, atitikimas keliamiems saugumo reikalavimams, užtikrinama, kad minėtiems produktams, paslaugoms ir procesams buvo sumažinta žinoma bazinė kibernetinių incidentų ir išpuolių rizika[317]. Vertinimas apima atitikties vertinimo įstaigos atliekamą techninių dokumentų peržiūrą. Taip pat, gali būti numatyta galimybė atlikti savarankišką atitikties sertifikavimo schemai vertinimą[318]. Šis lygis taikomas nekritiniams vartotojų objektams, pavyzdžiui, išmaniems namams ar daiktų interneto (IoT) programėlėms[319].

• *Pakankamai aukštą*. Garantuojama, kad IRT produktai, paslaugos ir procesai, dėl kurių išduotas tas sertifikatas, tenkina atitinkamus saugumo reikalavimus. Užtikrinama, kad žinoma kibernetinė rizika ir kibernetinių incidentų bei kibernetinių išpuolių, kuriuos vykdo ribotų gebėjimų ir ribotų išteklių turintys subjektai, pavojus, kiek įmanoma sumažinti. Vertinama, ar nėra viešai žinomų pažeidžiamumo spragų ir išbandoma, ar minėtuose produktuose, paslaugose ar procesuose tinkamai įgyvendinamos reikiamos saugumo funkcinės galimybės.[320] Šis lygis taikomas vidutinės rizikos debesijos kompiuterijos paslaugoms ir nekritiniam pramoniniam daiktų internetui (IoT)[321].

• *Aukštą*. Garantuojama, kad IRT produktai, paslaugos ir procesai tenkina keliamus saugumo reikalavimus. Užtikrinama, kad naujausiomis technologijomis pagrįsta kibernetinių išpuolių rizika, kuriuos vykdo aukšto lygio įgūdžių ir didelių išteklių turintys subjektai, kiek įmanoma sumažinta. Vertinama, ar nėra viešai žinomų pažeidžiamumo spragų, išbandoma, ar minėtuose produktuose, paslaugose arba procesuose tinkamai įgyvendinamos būtinos naujausiomis technologijomis pagrįstos saugumo funkcinės galimybės; atliekamas skverbties bandymas ir įvertinamas jų atsparumą prieš aukšto lygio įgūdžių turinčių subjektų išpuolius (imituojama įsilaužėlio ataka).[322]. Taigi, šis lygis yra skirtas IRT produktams, paslaugoms ir procesams, turintiems didelių atakų riziką[323].

[317] Reglamentas (ES) Nr. 2019/881, *supra note,* 136: 52 straipsnis 5 dalis.
[318] *Ibid*, 88 punktas.
[319] Maxime Puys, Jean-Pierre Krimm ir Raphael Collado „*Towards Cybersecurity Act: A Survey on IoT Evaluation Frameworks*“ (2020), 69.
http://personales.upv.es/thinkmind/dl/conferences/securware/securware_2020/securware_2020_2_90_30036.pdf
[320] Reglamentas (ES) Nr. 2019/881 *supra note*, 136: 52 straipsnio 6 dalis.
[321] Maxime Puys, Jean-Pierre Krimm ir Raphael Collado, *op. Cit.*, 69.
[322] Reglamentas (ES) Nr. 2019/881, *op. Cit.*, 52 straipsnis 7 dalis.
[323] Maxime Puys, Jean-Pierre Krimm ir Raphael Collado, *op. Cit.*, 69.

- kaip tarptautinės tarpvyriausybinės organizacijos priimančioji šalis;
- kaip Jungtinių Tautų rengiamos ar globojamos tarptautinės konferencijos priimančioji šalis;
- pagal daugiašalį susitarimą dėl privilegijų ir imunitetų suteikimo, arba pagal 1929 m. Šventojo Sosto (Vatikano Miesto Valstybės) ir Italijos Taikinimo sutartį (Laterano paktą);
- kai valstybė narė yra Europos saugumo ir bendradarbiavimo organizacijos (ESBO) priimančioji šalis[324].

Be to, valstybės narės gali nevykdyti nustatytų priemonių, kai kelionė yra pateisinama dėl skubaus humanitarinio poreikio arba dalyvavimo tarpvyriausybiniuose susitikimuose, arba susitikimuose kuriuos remia ar kurių priimančioji šalis yra Sąjunga, arba kurių priimančioji šalis yra ESBO pirmininkaujanti valstybė narė, kuriuose vyksta politinis dialogas, kuriuo tiesiogiai padedama siekti ribojamųjų priemonių politikos tikslų, įskaitant ir saugumą bei stabilumą kibernetinėje erdvėje. Valstybės narės gali nevykdyti nustatytų priemonių, kai atvykimas ar vykimas tranzitu yra būtinas teisminio proceso vykdymui.

[324] sprendimas (BUSP) 2019/797, *supra note,* 159: 4 straipsnio 6 dalis.

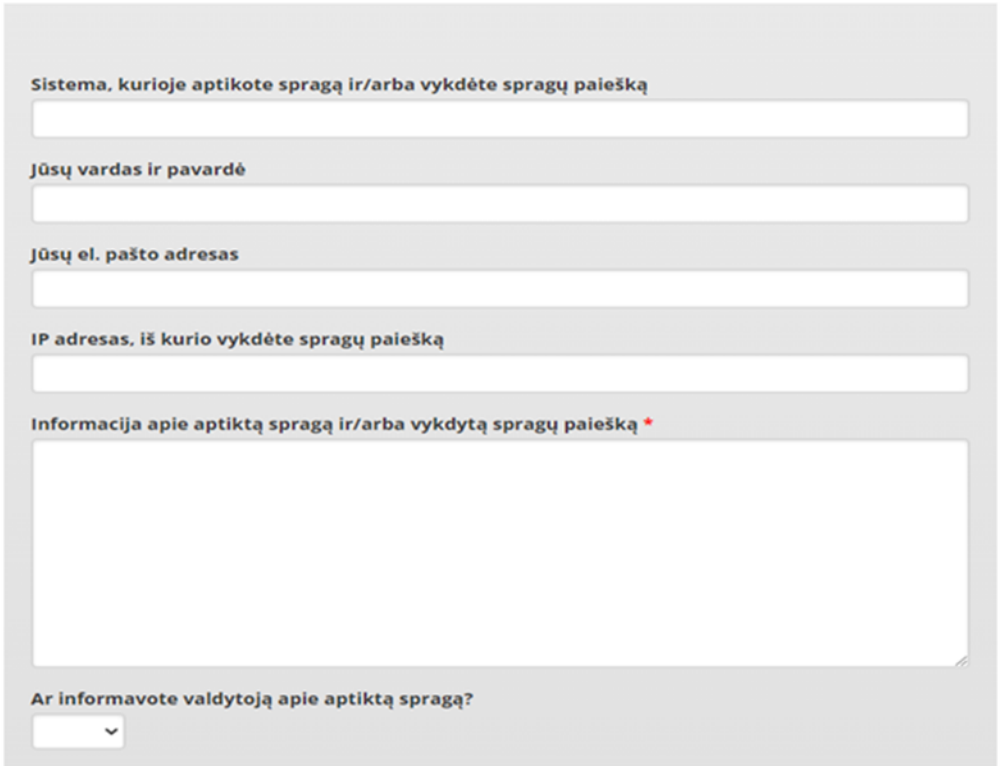
Pavyzdžiui, šeimos narių pagrindiniams poreikiams tenkinti (mokėjimas už maisto produktus, nuoma arba hipoteka, vaistai ir medicininis gydymas, mokesčiai, draudimo įmokos ir komunalinės paslaugos) yra skirti tik pagrįstiems profesiniams mokesčiams sumokėti ar patirtoms išlaidoms, susijusioms su teisinių paslaugų teikimu, kompensuoti, mokesčiams arba aptarnavimo mokesčiams už kasdienį įšaldytų lėšų arba ekonominių išteklių laikymą ar tvarkymą. Taip pat lėšos ypatingoms išlaidoms (dėl konkrečios priežasties, kuri nėra numatyta) arba į diplomatinės ar konsulinės atstovybės arba tarptautinės organizacijos, kurios pagal tarptautinę teisę naudojasi imunitetais[325].

[325] sprendimas (BUSP) 2019/797, *supra note,* 159.

Kibernetinio saugumo subjektas – tai subjektas, kuris valdo ir (arba) tvarko valstybės informacinius išteklius, taip pat, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas .

Kibernetinio saugumo subjektams nustatytos bendrosios pareigos, t. y. nustatyta atsakomybė už valdomų sistemų ar teikiamų paslaugų kibernetinį saugumą, nustatyta pareiga atlikti rizikos vertinimą, įdiegti kibernetinio saugumo priemones, pranešti apie kibernetinius incidentus ir taikytas priemones, taip pat teikti turinčią nusikalstamos veikos požymių informaciją policijai bei vykdyti kitus policijos nurodymus.

Pranešimo apie aptiktą spragą forma (NKSC, 2022)



Atsakingo atskleidimo proceso sudedamosios dalys („Kurk Lietuvai“, 2019)


Lentelėje pateikiamas atsakingo atskleidimo sudedamosios dalys chronologine seka. Pranešėjas pirmiausiai ne vėliau kaip per 24 val. turi informuoti NKSC ir (arba) kibernetinio saugumo subjektą apie nustatytas spragas. Gavusi pranešimą apie aptiktas spragas, koordinuojanti organizacija jį perduoda kibernetinio saugumo subjektui, kurio sistemoje aptikta spraga, ir įpareigoja jį per tam tikrą laikotarpį verifikuoti spragos egzistavimo faktą, pranešti apie spragos pašalinimą ir suteikti leidimą apie šią spragą informaciją atskleisti viešai[326].

[326] Žygimantas Robertas Tamošauskas „Atsakingo atskleidimo sąvokos, procesas, komunikacijos planas, principai ir tvarka“ *Kurk Lietuvai,* http://kurklt.lt/wp-content/uploads/2019/03/Atsakingo-atskleidimo-tvarka.pdf

- ryšių ir informacinė sistema (toliau – RIS) trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas;
- paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %. „RIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės durys“ (angl. back door), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. Botnet) infrastruktūros dalimi;
- 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[327].

[327] Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818, Nacionalinis kibernetinių incidentų valdymo planas, Kriterijų, kuriais vadovaujantis kibernetiniai incidentai priskiriami kibernetinių incidentų kategorijoms, sąrašas.

2020 m. kibernetinių incidentų statistika (Nacionalinis kibernetinio saugumo centras)

| Nr. | Kibernetinio incidento grupės | Kibernetinių incidentų kiekis | Pokytis palyginti su 2019 m. |
|---|---|---|---|
| 01 | Nepageidaujamų laiškų, klaidinančios informacijos platinimas | 739 | +29 % |
| 02 | Kenkimo PĮ | 1966 | +49 % |
| 03 | Informacijos rinkimas (angl. *phishing*) | 962 | –14 % |
| 04 | Mėginimas įsilaužti | 171 | +73 % |
| 05 | Sėkmingas įsilaužimas | 61 | –13 % |
| 06 | Paslaugų trikdymas (angl. DDoS) | 75 | +67 % |
| 07 | Neteisėta veikla, sukčiavimas | 85 | –62 % |
| 08 | Kiti incidentai (individualūs, neatitinkantys nė vienos iš nurodytų grupių aprašymų) | 271 | –24 % |
| | Iš viso: | 4330 | +25 % |

Traškevičiūtė D. (2022). *Kibernetinio saugumo teisinis reglamentavimas ir praktinės problemos* Kaunas: Mykolo Romerio universitetas

# ANOTACIJA

Magistro baigiamajame darbe išanalizuotas ir įvertintas esamas kibernetinio saugumo teisinis reglamentavimas, veiksmai, kuriais siekiama apsaugoti kibernetinę erdvę bei priemonės, kuriomis užtikrinamas informacinių ir ryšių technologijų saugumas, vientisumas bei informacinių ir ryšių sistemose saugomų elektroninių duomenų konfidencialumas, prieinamumas. Pirmame skyriuje nagrinėjami kibernetinio saugumo teoriniai aspektai, analizuojamos kibernetinio saugumo bei nusikalstamų veikų kibernetinėje erdvėje sampratos, aptariamos kibernetinį saugumą užtikrinančios institucijos. Antrame darbo skyriuje yra nagrinėjamas kibernetinio saugumo teisinis reglamentavimas Europos Sąjungoje. Trečiajame skyriuje nagrinėjamas kibernetinio saugumo teisinis reglamentavimas egzistuojantis Lietuvos Respublikoje, įvertinamas Europos Sąjungos kibernetinio saugumo teisės aktų įgyvendinimas. Ketvirtajame skyriuje analizuojamos baudžiamosios bylos, kuriose informacinės ir ryšių technologijos panaudojamos kaip nusikaltimo priemonės bei baudžiamosios bylos, kurių nusikalstamos veikos dalykas elektroniniai duomenys ir informacinių sistemų saugumas. Penktajame skyriuje yra pateikiamos išvados bei siūlymai, kaip didinti kibernetinį atsparumą.

Traškevičiūtė D. (2022). *Legal regulation and practical problems of cyber security* Kaunas: Mykolas Romeris University

# ANNOTATION

The Master's thesis analyses and evaluates the existing legal regulation of cyber security, the actions aimed at protecting cyberspace, and measures to ensure the security, integrity and confidentiality of information and communication technologies, as well as the availability of electronic data stored in information and communication systems. The first chapter examines the theoretical aspects of cybersecurity, analyses the concepts of cybersecurity and criminal acts in cyberspace, and discusses the institutions ensuring cybersecurity. The second chapter of the work deals with the legal regulation of cybersecurity in the European Union. The third chapter examines the legal regulation of cyber security in the Republic of Lithuania and assesses the implementation of the European Union cyber security legislation. The fourth chapter analyses criminal cases in which information and communication technologies are used as means of crime and criminal cases in which electronic data and security of information systems are the subject of criminal offences. The fifth chapter presents conclusions and suggestions on how to improve cyber resilience.

Key words: cybersecurity, information and communication technology security, cybercrime, cyber incidents.

Traškevičiūtė D. (2022). *Kibernetinio saugumo teisinis reglamentavimas ir praktinės problemos* Kaunas: Mykolo Romerio universitetas

# SANTRAUKA LIETUVIŲ KALBA

Šiuolaikinis pasaulis neįsivaizduojamas be informacinių ir ryšių technologijų, visuomenė skaitmenizuojasi, o informacinių ir ryšių technologijų įrenginiai bei komponentai, jose saugoma informacija, tampa kibernetinių nusikaltėlių taikiniu. Valstybės, įmonės, įstaigos, organizacijos ar piliečiai nepakankamai skirdami dėmesio kibernetinio saugumo užtikrinimui, tampa lengvomis aukomis ir patiria papildomų nuostolių. Be to, neapsaugoti tinklai ir įrenginiai sudaro galimybę įsiskverbti net ir į valstybinius tinklus. Todėl buvo nagrinėjama – Europos Sąjungos ir Lietuvos Respublikos kibernetinio saugumo teisinės sistemos ypatumai. Šio tyrimo tikslas yra atskleisti kibernetinio saugumo teisinio reguliavimo ypatumus bei kylančias problemas. Šiam tikslui pasiekti buvo iškelti tyrimo uždaviniai: išnagrinėti kibernetinio saugumo bei nusikalstamų veikų kibernetinėje erdvėje sampratas, atskleisti institucijas, kurios užtikrina kibernetinį saugumą, išanalizuoti Europos Sąjungos ir Lietuvos Respublikos kibernetinio saugumo teisinį reglamentavimą ir atskleisti nusikalstamų veikų kibernetinėje erdvėje kylančias problemas bei formalių straipsnio nuostatų visumos vertinimą Lietuvos Respublikos teismų praktikoje. Tyrimo metodika: kokybinis duomenų analizės/aprašomasis metodas, dokumentų analizės metodas, lingvistinis metodas, lyginamosios analizės metodas. Baigiamojo darbo ginamasis teiginys: Lietuvos Respublikoje yra pakankama kibernetinį saugumą reglamentuojanti teisinė bazė. Atlikus Europos Sąjungos ir Lietuvos Respublikos teisinio reglamentavimo bei baudžiamųjų bylų analizę buvo patvirtintas šis teiginys. 2021 m. vertinant valstybių priimamus sprendimus bei vykdomus veiksmus kibernetinio saugumo politikoje, sukurtas tarptautinis kibernetinio saugumo indeksas, kuriame Lietuva yra šeštoje vietoje. Baudžiamųjų bylų analizės metu nustatyta, jog nusikalstamų veikų kibernetinėje erdvėje tyrimas bei nagrinėjimas yra specifiškas, reikalaujantis specialiųjų žinių panaudojimo, taip pat atskleista Lietuvos Respublikos baudžiamojo kodekso normų, kuriose įtvirtintos nusikalstamos veikos kibernetiniam saugumui, aktualūs teismų išaiškinimai. Darbe buvo identifikuotos nusikalstamų veikų kibernetinėje erdvėje problemos susijusios su nepakankamu duomenų surinkimu ikiteisminio tyrimo metu, kibernetinio saugumo „higienos“ trūkumu. Galiausiai darbe pateiktos rekomendacijos, skatinti dalyvavimą įvairiuose mokymuose, seminaruose, paskaitose, kurių metų įgyjami praktiniai kasdieniai įgūdžiai, užtikrinantys kibernetinį saugumą. Taip pat įtvirtinti privalomą kibernetinio saugumo sertifikavimą informacinių ir ryšių technologijų produktams, paslaugoms ir procesams, turintiems didelių atakų riziką, kadangi vieša, skaidri informacija apie minėtų technologijų kibernetinį saugumą, sustiprintų

pasitikėjimą skaitmeniniais sprendimais. Bei skatinti kibernetinio saugumo subjektus savo veikloje įtvirtinti kibernetinio saugumo spragų paieškos politiką.

# SANTRAUKA ANGLŲ KALBA

Traškevičiūtė D. (2022). *Legal regulation and practical problems of cyber security* Kaunas: Mykolas Romeris University

The modern world is unimaginable without information and communication technologies, society is digitising, and information and communication technology devices and components, information stored in them, become the target for cyber criminals. States, businesses, bodies, organisations or citizens who do not pay sufficient attention to cybersecurity fall easy victims and incur additional losses. Moreover, unprotected networks and devices allow infiltration even of public networks. Therefore, the peculiarities of the legal system of cybersecurity of the European Union and the Republic of Lithuania were examined. The purpose of this research is to reveal the peculiarities of legal regulation of cybersecurity and emerging problems. In order to achieve this goal, the following research tasks were set: to examine the concepts of cybersecurity and criminal acts in cyberspace, to reveal the institutions that ensure cybersecurity, to analyse the legal regulation of cybersecurity of the European Union and the Republic of Lithuania and to reveal the problems arising from criminal acts in cyberspace and the assessment of the set of formal provisions of the Article in the case-law of the courts of the Republic of Lithuania. Research methodology: qualitative data analysis/descriptive method, document analysis method, linguistic method, comparative analysis method. Defence statement of the final thesis: The Republic of Lithuania has a sufficient legal framework regulating cybersecurity. The analysis of the legal regulation and criminal cases of the European Union and the Republic of Lithuania confirmed this statement. In 2021, an international cyber security index was created to assess the decisions and actions taken by countries in the field of cyber security, and Lithuania is ranked sixth in the index. The analysis of criminal cases has established that the investigation and examination of criminal offences in cyberspace is specific, requiring the use of special knowledge, as well as revealed the norms of the Criminal Code of the Republic of Lithuania, which enshrine criminal offences against cybersecurity, and relevant court interpretations. The work identified the problems of criminal offences in cyberspace related to insufficient data collection during the pre-trial investigation and the lack of cybersecurity hygiene. Finally, the work presents recommendations to promote participation in various training, seminars and lectures, during which practical everyday skills ensuring cybersecurity are acquired. Also, to introduce mandatory cybersecurity certification for information and communication technology products, services and processes with a high risk of attacks, as public, transparent information on the cybersecurity of these

technologies would build trust in digital solutions. And encourage cybersecurity entities to establish a policy for finding cybersecurity vulnerabilities in their activities.