MYKOLO ROMERIO UNIVERSITETO
VIEŠOJO SAUGUMO AKADEMIJA

ARŪNAS KOCHANKA
TEISĖS IR POLICIJOS VEIKLOS: SPECIALIZACIJOS IKITIEISMINIO PROCESO PROGRAMA

KIBERNETINIO SAUGUMO TEISINIS REGLAMENTAVIMAS IR PRAKTINIAI ASPEKTAI

Magistro baigiamasis darbas

Vadovas: Dr. Erika Matulionytė-Jarašūnė

.....
(parašas)

Kaunas, 2026

TURINYS

ĮVADAS

Baigiamojo darbo aktualumas. Kibernetinės grėsmės tapo svarbia problema tiek nacionaliniu, tiek tarptautiniu lygiu. Šiuolaikinių grėsmių globalumas lemia ir sudėtingą jų tyrimą – nors išpuoliai vykdomi konkrečioje teritorijoje, juos dažnai įvykdo fiziniai ar juridiniai asmenys, priklausantys skirtingoms jurisdikcijoms, todėl atsakomybės priskyrimas tampa komplikuotas. Tai rodo, kad vien globalinis ar regioninis bendradarbiavimas, nors ir būtinas, nėra pakankamas – svarbus vaidmuo tenka ir nacionaliniam reguliavimui bei strategijoms.[1] 2024 m. Nacionalinis kibernetinio saugumo centras (toliau - NKSC) iš viso užregistravo 3 874 kibernetinius incidentus. Daugiausia registruotų incidentų priskiriama socialinei inžinerijai, kai siekiama išvilioti asmeninius ir svarbius duomenis (angl. „phishing“). Pažymėtina, kad 2024 m. šio tipo incidentai sudarė net 59 proc. visų NKSC registruotų incidentų. Antroje vietoje pagal incidentų grupes buvo fiksuota auganti neteisėta įtaka ryšių ir informacinių sistemų veiklai ir (ar) teikiamoms paslaugoms, o trečioje vietoje nepageidaujamų laiškų ir (ar) klaidinančios informacijos platinimas.[2] Valstybinė duomenų apsaugos inspekcija 2025 m. gavo 223 pranešimus apie asmens duomenų saugumo pažeidimus, dėl kurių Lietuvoje buvo paveikti 1 249 409 duomenų subjektai, o 29 proc., šių pažeidimų įvyko dėl kibernetinių incidentų.[3] Lietuvoje kibernetinio saugumo reguliavimą nustato Lietuvos Respublikos kibernetinio saugumo įstatymas (toliau - KSĮ), kuris įsigaliojo 2014 m. ir vėliau buvo ne kartą keistas siekiant pritaikyti prie besikeičiančių grėsmių ir Europos Sąjungos teisės aktų. Tarptautiniu lygmeniu reikšmingi teisės aktai šia tema yra Europos Sąjungos direktyvos, tokios kaip Direktyva (ES) 2022/2555 (NIS2), Bendrasis duomenų apsaugos reglamentas (BDAR), Reglamentas (ES) 2019/881 (Kibernetinio saugumo aktas). „Dėl kibernetinio saugumo specifiškumo, jo iki galo užtikrinti neįmanoma, o vis labiau tobulėjant technologijoms atsiranda naujų grėsmių darančių įtaką kibernetiniam saugumui.“ [4] Atsižvelgiant į tai, aktuali tampa kibernetinio saugumo teisinio reglamentavimo ir jo praktinio taikymo analizė.

Baigiamojo darbo naujumas. „Remiantis 2024 m. Nacionalinės kibernetinio saugumo būklės ataskaita, dėl kibernetinių incidentų, reikšmingai išaugo Lietuvoje paveiktų subjektų skaičius. Šie faktai rodo, kad kibernetinės atakos prieš Lietuvą, kaip ir kitas demokratines valstybes, ne tik tobulėja, bet ir tampa dažnesnės. Didelių iššūkių nacionaliniam saugumui taip pat

---

[1] Darius Štitilis ir kt., „National Cyber Security Strategies: Management, Unification and Assessment“, Independent Journal of Management & Production (2020): 2342, https://cris.mruni.eu/server/api/core/bitstreams/2edb4036-99b4-44db-8fda-51ba446afe1b/content.

[2] „2024 Nacionalinė kibernetinio saugumo būklės ataskaita“, Lietuvos Respublikos krašto apsaugos ministerija, žiūrėta 2026 m. kovo 17 d., https://kam.lt/leidiniai/nacionaline-kibernetinio-saugumo-bukles-ataskaita-kam-2024/.

[3] „Asmens duomenų saugumo pažeidimai 2025 m. apibendrinimas“, Valstybinė duomenų apsaugos inspekcija, žiūrėta 2026 m. kovo 19 d., https://vdai.lrv.lt/public/canonical/1770804989/1276/2025%20m.%20ADSP%20apibendrinimas_suredaguotas.pdf.

[4] Marija Tamošaitytė, „Kibernetinio saugumo aktualizavimas Lietuvos nacionalinio saugumo strategijoje“ (magistro darbas, Klaipėdos universitetas, 2020), https://gs.elaba.lt/object/elaba:47757480.

kelia tiekimo grandinėje dalyvaujančių subjektų nepakankamas dėmesys kibernetiniam saugumui.[5] Kibernetinio saugumo klausimai Lietuvos mokslinėje literatūroje nagrinėti įvairiai. Darius Štitilis analizavo kibernetinio saugumo teisinio reguliavimo teorinius pagrindus bei ES strategijų įtaką nacionaliniam reguliavimui.[6] Robertas Stunžinas nagrinėjo kibernetinio saugumo terminiją ir jos atitikmenis Lietuvos teisės kalboje. [7] Gabrielė Želvienė kibernetinio saugumo problematiką analizavo nacionalinio saugumo strategijų kontekste, [8] o Mantas Anužis su bendraautoriais tyrė kibernetinio saugumo grėsmes nuo valstybės iki individualaus vartotojo lygmens. [9] Aurimo Šidlausko daktaro disertacijoje nagrinėjamas asmens duomenų saugumo modelis, orientuotas į vadybinį ir techninį rizikos mažinimą.[10]

Kibernetinio saugumo tema plačiai nagrinėjama tarptautiniu mastu. Nacionalinių kibernetinio saugumo strategijų vaidmuo gerinant kibernetinio saugumo švietimą nagrinėjo Saleh Aldaaje ir kiti. [11] Apie kibernetinį saugumą Latvijoje ir saugumo stiprinimą susiduriant su kylančiomis grėsmėmis nagrinėjo Mihails Potapovs ir Kate E. Kanasta. [12] Apie kibernetinio saugumo ir privatumo teisinio reguliavimo internete formavimo ir plėtros konceptualumo pagrindus nagrinėjo Volodymyr Polishchuk ir kiti. [13]Nors panašios temos yra nagrinėtos tiek Lietuvos, tiek užsienio mokslinėje literatūroje, tačiau ši tema išlieka aktuali, atsižvelgiant į besikeičiančias kibernetines grėsmes ir vis dažniau registruojamus nusikaltimus elektroninėje erdvėje. Darbe analizuojamos naujausios teisės aktų redakcijos, kurios reglamentuoja kibernetinį saugumą, tad atsižvelgiant į teisės aktų pakeitimus ši tema išlieka aktuali. Baigiamajame darbe taip pat remiamasi Lietuvos Aukščiausiojo Teismo nutartimis, kurios yra aktualios dėl nusikaltimų

---

[5] „2024 Nacionalinė kibernetinio saugumo būklės ataskaita“, *supra note*, 2:5.

[6] Darius Štitilis, „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos“, Socialinės technologijos 3, 1 (2013): 189–207, https://cris.mruni.eu/server/api/core/bitstreams/952d2a4c-b86e-46c4-bb02-dc53a4dbdd2a/content.

[7] Robertas Stunžinas, „Europos Sąjungos kibernetinio saugumo terminai su dėmeniu „kibernetinis, (-ė): reikšmės, kilmė, sinonimija ir variantai““, *Terminologija* (2017), https://talpykla.elaba.lt/elaba-fedora/objects/elaba:26398612/datastreams/MAIN/content.

[8] Gabrielė Želvienė, „Kibernetinio saugumo iššūkiai ir grėsmės Lietuvos nacionalinio saugumo strategijoje“ (magistro darbas, Vytauto Didžiojo universitetas, 2024), https://www.vdu.lt/cris/entities/etd/c3da6bf9-8887-4aea-91c6-9ec3833afc00.

[9] Mantas Anužis, Paulius Šakalys ir Aleksej Lichovidov, „Kibernetinis saugumas: nuo valstybės iki asmens“, *Verslas, technologijos*, biomedicina: inovacijų įžvalgos 1 (13) (2022): 16–24, https://vb.kvk.lt/object/elaba:134773098/index.html.

[10] Aurimas Šidlauskas, „Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis“ (daktaro disertacija, Mykolo Romerio universitetas, 2024), https://cris.mruni.eu/server/api/core/bitstreams/9a26a2be-e862-4425-a208-083239c86338/content.

[11] Aleh Aldaaje ir kt., „The role of national cybersecurity strategies on the improvement of cybersecurity education“, Computers & Security 119 (2022), https://doi.org/10.1016/j.cose.2022.102754.

[12] Mihails Potapovs ir Kate E. Kanasta, *Cybersecurity in Latvia: Forging Resilience Amidst Emerging Threats* (Routledge, 2026), https://www.mod.gov.lv/sites/mod/files/document/Cybersecurity%20in%20Latvia_25_08_07_15_01_13.pdf.

[13] Volodymyr Polishchuk, Vitalii Yurakh, Olena Kravchenko, Wolodymyr Warawa ir Inna Kulchii, „Legal Regulation of Cybersecurity and Privacy on the Internet as SDG's“, *Journal of Lifestyle and SDGs Review* 4, 1 (2024), https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01666.

elektroninėje erdvėje. Atsižvelgiant į tai, darbo naujumas grindžiamas tiek teorine teisės aktų ir mokslinių šaltinių analize, tiek praktine teismų nutarčių analize.

Baigiamojo darbo problema. Ar kibernetinio saugumo teisinis reglamentavimas Lietuvoje perkelia pagrindines tarptautines ir ES teisės nuostatas, ir ar bylų, susijusių su kibernetiniais nusikaltimais, nagrinėjimas teisme yra specifinis ir problematiškas?

Tyrimo objektas – kibernetinio saugumo teisiniai ir praktiniai aspektai.

Tyrimo tikslas – išanalizuoti kibernetinio saugumo teisinį reglamentavimą ir praktinius aspektus.

Tyrimo uždaviniai:

1. Apžvelgti kibernetinio saugumo sampratą ir kibernetines grėsmes.

2. Išanalizuoti kibernetinio saugumo teisinį reglamentavimą Europos Sąjungoje bei tarptautiniu lygmeniu.

3. Išnagrinėti kibernetinio saugumo teisinį reglamentavimą Lietuvoje.

4. Atskleisti teismų praktikoje taikomų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kvalifikavimo problematiką ir šių veikų specifinius ypatumus.

Ginamasis teiginys. Kibernetinio saugumo teisinis reguliavimas Lietuvoje yra pakankamas ir atitinka tarptautines ir ES nuostatas.

Metodologinis pagrindas. *Dokumentų analizės metodas* – šis metodas naudotas nagrinėjant tarptautinius, Europos Sąjungos ir Lietuvos teisės aktus, mokslinės literatūros šaltinius, susijusius su kibernetiniu saugumu. Taip pat šis metodas naudotas analizuojant Lietuvos Respublikos teismų praktiką. *Lyginamasis metodas* – naudotas analizuojant ir lyginant moksliniuose straipsniuose, teisės aktuose pateiktas sąvokas, principus. Taip pat naudotas lyginant Lietuvos, tarptautinių bei ES teisės aktų suderinamumą bei lyginant teismų nutartis. *Apibendrinimo metodas* – taikytas formuojant ir pateikiant išvadas bei pasiūlymus.

Baigiamojo darbo struktūra. Baigiamąjį darbą sudaro keturi skyriai. Pirmajame skyriuje apžvelgiama kibernetinio saugumo samprata ir kibernetinio saugumo grėsmės. Antrajame darbo skyriuje analizuojamas kibernetinio saugumo tarptautinis ir Europos Sąjungos teisinis reglamentavimas. Trečiajame darbo skyriuje nagrinėjamas kibernetinio saugumo teisinis reglamentavimas Lietuvoje. Ketvirtajame darbo dalyje nagrinėjama teismų praktika, analizuojant baudžiamąsias bylas dėl nusikalstamų veikų elektroninėje erdvėje, siekiant atskleisti šių veikų kvalifikavimo probleminius aspektus ir specifinius ypatumus. Darbe pateikiamos išvados bei pasiūlymai.

1. KIBERNETINIO SAUGUMO TEORINIAI ASPEKTAI

„Kibernetinis saugumas yra neatsiejama šiuolaikinės valstybės ir visuomenės saugumo dalis“.[14] „Skaitmeninių technologijų tobulėjimas skatina daugiau žmonių pasirinkti ne tradicines, o interneto paslaugas. Technologijos, ypač interneto paslaugos, leidžia greitai ir efektyviai pasiekti norimą tikslą, gauti prekę ar paslaugą. Neabejotinai auga ne tik naudojamų technologijų skaičius, bet ir informacijos, kurią asmuo pateikia internete, kiekis. Norint naudotis paslaugomis būtina pateikti savo asmeninę informaciją nuo vardo ir elektroninio pašto iki konfidencialios informacijos, tokios kaip asmens kodas ar banko sąskaitos numeris“.[15] Tad šiame skyriuje bus analizuojama kibernetinio saugumo samprata, jos ištakos bei principai, taip pat bus apžvelgtos kibernetinės grėsmės ir incidentai. Tai svarbu analizuoti, kadangi tai sudaro tiek visuomenės duomenų, tiek valstybės saugumo pagrindą kibernetinėje erdvėje.

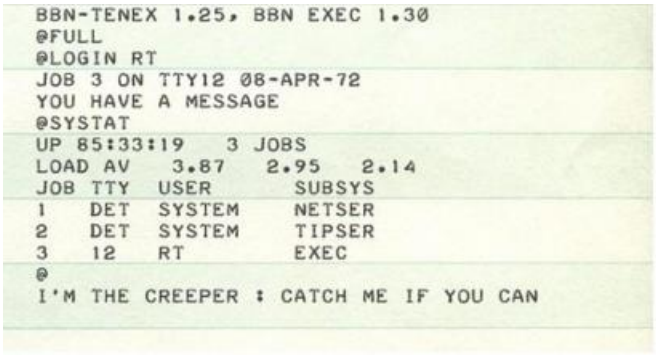
1.1. Kibernetinio saugumo samprata

„Žodis „kibernetika“ imtas vartoti netrukus po Antrojo pasaulinio karo. Jis reiškia mokslo šaką, tiriančią mašinų valdymą bei sąveiką tarp žmonių ir mašinų. Šis žodis kilęs iš graikų kalbos ir reiškia „valdytoją, vairininką“. Išpopuliarėjo XX amžiaus 8-ojo dešimtmečio pradžioje kartu su nauju mokslinės fantastikos žanru, pavadintu „kiberpanku“ (angl. Cyberpunk)“.[16] Tačiau tuo metu šis žodis nebuvo siejamas su kompiuteriais ar kibernetiniu saugumu. XX a. šeštajame dešimtmetyje telefonai buvo pažangiausia ryšio technologija. Telefoniniai apgavikai, išmoko valdyti telefono linijas klausydamiesi garsų, kai operatoriai sujungdavo skambučius, skaitė telefonų bendrovių techninius žurnalus, isilaužinėjo į biurus ir kūrė savo techninę įrangą. Galima daryti išvadą, kad telefoniniai įsilaužėliai pradėjo įsilaužimo mąstyseną dar prieš atsirandant kompiuteriui, į kurį būtų galima įsilaužti.[17] Pirmasis išsamus publikuotas darbas „Kompiuterinių sistemų saugumo kontrolė“ yra tapęs kibernetinio saugumo srities pagrindu. Tai buvo techninė ataskaita, paprastai vadinama „Ware“ ataskaita. 1970 m. paskelbta ataskaita buvo Jungtinių Amerikos Valstijų gynybos departamento organizuotos kompiuterių saugumo darbo grupės atlikto tyrimo rezultatas. Ataskaitoje padaryta išvada, kad visapusiškam kompiuterinės sistemos saugumui reikalingas aparatinės ir programinės įrangos, ryšių, fizinės, personalo ir administracinės

---

[14] „2024 Nacionalinė kibernetinio saugumo būklės ataskaita“, *supra note*, 2:55.
[15] Irma Šileikienė ir Ana Usovaitė, „Kibernetinio saugumo situacijos Lietuvoje grėsmių analizė Europos Sąjungos kontekste“, *Technologijos ir menas* Nr. 15 (2024): 14, https://vb.vtdko.lt/object/elaba:215140351/215140351.pdf#page=14.
[16] Aušrius Juozapavičius ir kt., *Nacionalinis saugumas ir krašto gynyba,* (Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2025), 59.
[17] „Kibernetinio saugumo istorija“, CyberPhish, žiūrėta 2026 m. kovo 11 d., https://cyberphish.knf.vu.lt/lt/learn/kibernetinio-saugumo-istorija/20.

kontrolės priemonių derinys.[18] Galima teigti, kad kibernetinio saugumo istorija prasidėjo 1971 m., kai pasaulis pamatė kompiuterinį virusą realiame pasaulyje. DEC PDP-10 kompiuteriai, veikiantys TENEX operacinėje sistemoje, pradėjo rodyti pranešimus: „Aš esu šliaužtinukas, pagauk mane, jei gali!“ angl. „I am the creeper, catch me if you can „(žr. pav 1.)



1 pav. Kompiuterinio viruso pranešimo pavyzdys.[19]

Nors šis virusas buvo sukurtas tik tam, kad būtų galima patikrinti, ar ši koncepcija įmanoma, tačiau jis padėjo pamatus virusų atsiradimui. Vėliau kuriant kompiuterines sistemas saugumas tapo svarbiu ir sudėtingu tikslu. Jau 1974 metais buvo nustatyta 339 su kompiuteriais susijusių nusikalstamų veikų. Dauguma incidentų buvo susiję su paprastu sukčiavimu, kurį vykdė darbuotojai, turėję prieigą prie kompiuterizuotų finansinių įrašų. [20] Tad jau tada kompiuterinių sistemų vystymosi laikotarpiu išryškėjo poreikis užtikrinti griežtesnį jų saugumą. Kartu buvo akcentuotina būtinybė didinti sistemų patikimumą ir kurti sprendimus, sudarančius prielaidas patikimų programų, įskaitant apskaitos ir saugumo audito programas, kūrimui.[21] Pirmasis JAV kibernetinio saugumo patentas buvo suteiktas 1983 m. rugsėjį.[22] Aštuntajame dešimtmetyje pirmasis plataus masto tinklas (ARPANET) išsivystė į dabartinį internetą. Kompiuteriams tampant vis labiau tarpusavyje sujungtiems, kompiuteriniai virusai taip pat tapo sudėtingesni ir labiau paplitę.

Galima teigti, kad pradinė kibernetinio saugumo samprata formavosi kartu su technologijomis ir jų raida. Tačiau toliau augant interneto naudotojams ir jį palaikančioms bei valdančioms technologijoms, buvo pereitą į naująjį skaitmeninį amžių. Technologiniai proveržiai tokiose srityse kaip natūralios kalbos apdorojimas, mašininis ir gilusis mokymasis iš esmės

---

[18] Shahid Alam, Cybersecurity: *Past, Present and Future* (Adana: Adana Alparslan Turkes Science and Technology University, 2022), 4, https://arxiv.org/pdf/2207.01227.
[19] *Ibid*.
[20] Theodore A. Linden, *Operating System Structures to Support Security and Reliable Software* (Washington, D.C.: U.S. Government Printing Office, 1976), 1, https://csrc.nist.gov/files/pubs/conference/1998/10/08/proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/lind76.pdf.
[21] *Ibid.*
[22] „Cryptographic Communications System and Method“, U.S. Patent No. 4,405,829, 1983 m. rugsėjo 20 d., žiūrėta 2026 m. kovo 3 d., https://patentimages.storage.googleapis.com/49/43/9c/b155bf231090f6/US4405829.pdf.

pagerino socialinių tinklų, debesų kompiuterijos ir kitų sistemų veikimą. Šie pasiekimai neabejotinai pagerino verslo, organizacijų, vyriausybių, visos visuomenės bei kiekvieno individo kasdienį gyvenimą. Todėl kibernetinio saugumo sampratą buvo aiškinama įvairiai.[23] Kroatų tarptautiniame mokslo žurnale „Automatika“, kuris skirtas valdymui, matavimams, elektronikai, kompiuterijai ir ryšiams, straipsnyje apie kibernetinį saugumą ir kibernetinę gynyba, autoriai išskyrė kibernetinio saugumo sampratos sudedamąsias dalis ir kibernetinį saugumą aiškino, kad tai yra informacijos saugumo, operacinių technologijų saugumo ir informacinių saugumo priemonių bei technikų valdymas, kūrimas, administravimas ir naudojimas, siekiant užtikrinti atitiktį teisės aktų reikalavimams, apsaugoti turtą ir pažeisti (kompromituoti) priešininkų turtą.[24] Kiek plačiau šią sąvoką aiškinama straipsnyje „Link labiau reprezentatyvaus kibernetinio saugumo apibrėžimo“. Šiame straipsnyje kibernetinį saugumą, aiškino, kaip priemonių, politikų, saugumo koncepcijų, apsaugos mechanizmų, gairių, rizikos valdymo metodų, veiksmų, mokymų, gerosios praktikos principų, užtikrinimo priemonių ir technologijų visuma, kuri gali būti naudojama siekiant apsaugoti kibernetinę aplinką, organizacijas ir jų turtą.[25] Straipsnyje Kibernetinio saugumo samprata (angl. Defining Cybersecurity), autoriai išnagrinėja įvairias kibernetinio saugumo sampratas, pateikė savo išvadas, pateikdami apibendrintą kibernetinio saugumo apibrėžimą. Autoriai kibernetinį saugumą aiškino, kad tai yra išteklių, procesų ir struktūrų organizavimas ir visuma, naudojama apsaugoti kibernetinę erdvę ir kibernetinės erdvės įgalintas sistemas nuo įvykių, kurie nesutampa de jure su de facto nuosavybės teisėmis.[26]

Išanalizavus užsienio literatūroje pateiktas kibernetinio saugumo sampratas apibendrinama, kad kibernetinis saugumas dažnai aiškinamas panašiai, tai yra kaip priemonių, procesų, technologijų ir politikų visuma, skirta apsaugoti informaciją, sistemas ir turtą. Lietuvių autorių parengtame straipsnyje „Kibernetinis saugumas: nuo valstybės iki asmens“ į kibernetinio saugumo sampratą buvo žiūrima per penkias šios sistemos dimensijas - „kibernetinio saugumo politikos planavimo, teisinio reguliavimo, kibernetinės kultūros lygio, švietimo mokyklose, universitetuose ir profesinio ugdymo įstaigose bei kibernetinio saugumo gerųjų praktikų taikymo valstybiniame ir privačiame sektoriuje.“[27]

---

[23] Alam, supra note, 18.
[24] D. Galinec, D. Možnik ir B. Guberina, „Cybersecurity and cyber defence: national level strategic approach“, Automatika 58 (3), (2017): 273, https://doi.org/10.1080/00051144.2017.1407022.
[25] Daniel Schatz, Rabih Bashroush ir Julie Wall, „Towards a More Representative Definition of Cyber Security“, *Journal of Digital Forensics, Security and Law* 12, nr. 2 (2017): 67–68, https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl.
[26] Dan Craigen, Nadia Diakun-Thibault ir Randy Purse, „Defining Cybersecurity“, *Technology Innovation Management Review* (2014): 17–18, https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf.
[27] Mantas Anužis, Paulius Šakalys ir Aleksej Lichovidov, „Kibernetinis saugumas: nuo valstybės iki asmens“, Verslas, technologijos, biomedicina: inovacijų įžvalgos 1, 13 (2022): 18, https://www.kvk.lt/wp-content/uploads/2022/06/KVK_2022_06_23_2022-1-13.pdf.

Generolo Jono Žemaičio Lietuvos karo akademijos parengtame vadovėlyje kibernetinis saugumas įvardijimas, kaip „praktika, siekianti apsaugoti kompiuterinius tinklus, prietaisus, žmones ir duomenis nuo nesankcionuotos prieigos ar neteisėto naudojimo.“[28] Straipsnyje apie kibernetinio saugumo tendencijas Lietuvoje ir Pasaulyje, Kibernetinio saugumo samprata buvo pateikta gan plati ir aprašoma buvo kaip „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, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.“[29] Tad Lietuvos moksliniuose straipsniuose, kibernetinio saugumo sampratą yra aiškinama panašiai, ir pačios sampratos apibrėžimas kardinaliai neišsiskirią iš užsienio literatūros autorių.

Direktyvoje (ES) 2018/1972 (Kibernetinio saugumo aktas) įtvirtinta, kad kibernetinis saugumas– tai „ visa veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių“[30], tačiau šiame teisės akte yra pabrėžiama, kad „tai nėra vien su technologijomis susijęs klausimas, vienodai svarbus yra žmonių elgesys.“[31] Tad šioje direktyvoje yra skatinama propaguoti „kibernetinę higieną“, tai yra atlikti „nesudėtingas įprastines priemones, kurias įgyvendinę ir reguliariai taikydami piliečiai, organizacijos ir įmonės kiek įmanoma labiau sumažintu kibernetinių grėsmių jiems keliamą riziką“ [32] Net 95 proc. kibernetinių saugumo atakų įvyksta dėl neatsargaus žmonių elgesio internete, o dažniausiai kibernetiniai nusikaltimai įvyksta dėl „silpnų“ slaptažodžių.[33] Matant šią, problemą, svarbu išanalizuoti, kaip saugiai elgtis internete. Siekiant išvengti kibernetinių grėsmių reikėtų:

1. Kad darbas kompiuteriu vyktų iš paskyros, neturinčios administratoriaus teisių, o . prisijungimai prie kompiuterinės darbo vietos ir naudojamų paskyrų turi būti apsaugoti sudėtingais slaptažodžiais.[34]

---

[28] Juozapavičius ir kt, *supra note*, 16.
[29] Gabrielė Blevičiūtė, Justas Kidykas ir Rūta Beinoriūtė, Kibernetinio saugumo tendencijos Lietuvoje ir pasaulyje (2019), 2, https://data.kurklt.lt/wp-content/uploads/2023/04/Esama-situacija-su-VK.pdf.
[30] „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)“, 2019 m. balandžio 17 d., EUR-Lex, žiūrėta 2026 m. vasario 4 d., https://eur-lex.europa.eu/eli/reg/2019/881/oj/lt.
[31] *Ibid*.
[32] *Ibid*.
[33] Anužis, Šakalys, Lichovidov, supra note., 27.
[34] Miglė Laima Žukauskaitė, „Kibernetinės higienos pagrindai“, VDAI, 2024 m. rugsėjo 26 d., žiūrėta 2026 m. kovo 19 d., https://vdai.lrv.lt/public/canonical/1727673277/613/Kibernetines%20higienos%20pagrindai_Migle.pdf.

2. Rinktis stiprius slaptažodžius. Pavyzdžiui „slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių, slaptažodį turi sudaryti ne mažiau kaip dvylika simbolių, nerekomenduojama slaptažodyje naudoti reikšminius žodžius arba asmeninio pobūdžio informaciją“.[35]

3. Kompiuterio ekraną užrakinti paliekant darbo vietą, skaitmeninius duomenis laikyti sistemose užšifruotus.

4. Darbinių įrenginių nenaudoti asmeniams poreikiams, o asmeninių įrenginių darbinėms funkcijoms atlikti.

5. Dirbant svarbu nesinaudoti viešais Wi-Fi tinklais, nesilankyti su darbu nesusijusiose interneto svetainėse, naudoti VPN, dirbti tik su darbdavio suteiktais įrenginiais ir programomis bei nepalikti įrenginių be priežiūros.[36]

6. Naudoti kelių faktorių autentifikavimą. Šio proceso metu „naudotojas, norėdamas patvirtinti savo tapatybę, turi pateikti du skirtingus faktorius - pavyzdžiui, pateikti statinį slaptažodį ir žetoną, kuris buvo sugeneruotas naudojant slaptažodžių generatorių. Vėliau šis metodas buvo apibendrintas ir pavadintas kelių faktorių autentifikacija, kuomet naudotojas turi pateikti du ar daugiau faktorių, norėdamas patvirtinti savo tapatybę“.[37]

Svarbu pabrėžti, kad net ir laikantis visų šių kibernetinės higienos rekomendacijų visiškai apsisaugoti nuo kibernetinių grėsmių nėra įmanoma, tačiau jų laikymasis gali sumažinti galimų incidentų riziką ir padėti užtikrinti saugesnį darbą skaitmeninėje erdvėje. Taigi galima daryti išvadą, kad kibernetinio saugumo terminas glaudžiai susijęs su kibernetinės higienos terminu. Juo įvardijama kompiuterių sistemų bei įvairių prietaisų apsauga bei priežiūra laikantis gerosios kibernetinio saugumo praktikos bei higienos.[38] Kibernetinė higiena yra svarbi norint išlaikyti kibernetinį saugumą, bet šios dvi panašios sąvokos neturėtų būti laikomos kaip sinonimai. Kadangi kibernetinis saugumas „yra tam tikri veiksmai, kurių imamasi siekiant išlaikyti saugumą ir išlaikyti atsparumą prieš kibernetines atakas, o kibernetinė higiena daugiau yra susijusi su žinojimu apie skaitmeninį saugumą ir praktika susijusia su siekiu didinti kibernetinį saugumą“.[39]

---

[35] „Dėl Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatų ir elektroninės informacijos saugos politiką įgyvendinančių dokumentų patvirtinimo“, TAR, žiūrėta 2026 m. balandžio 11 d., https://e-tar.lt/portal/lt/legalAct/45942bf096a911eb9fecb5ecd3bd711c.
[36] Žukauskaitė, *op.cit.*
[37] Konstantinas Jurgilas, „Dviejų faktorių (2FA) skaitmeninio autentifikavimo metodas nuotolinei prieigai prie kritinės infrastruktūros sistemos“ (magistro baigiamasis darbas, Kauno technologijos universitetas, 2021), 21, https://talpykla.elaba.lt/elaba-fedora/objects/elaba:95730204/datastreams/MAIN/content.
[38] Robertas Stunžinas, „Europos Sąjungos kibernetinio saugumo terminai su dėmeniu kibernetinis, (-ė): reikšmės, kilmė, sinonimija ir variantai“, *Terminologija* 24 (2017): 151, https://ceeol.com/search/article-detail?id=702496.
[39] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya ir G. M. Hancock, „Holistic cyber hygiene education: Accounting for the human factors“, *Computers & Security* 92 (2020): 1, https://doi.org/10.1016/j.cose.2020.101731.

Analizuojant kibernetinio saugumo sampratą, svarbu suprasti ir išanalizuoti kibernetinio saugumo principus. 1977 m. buvo pristatyta Jungtinių Amerikos Valstijų (toliau - JAV) Centrinė žvalgybos valdybos (toliau- CŽV) trikampio koncepcija, apimanti konfidencialumą, integralumą ir prieinamumą. Tai trys pagrindiniai kibernetinio saugumo principai:

1. Konfidencialumas – tai užtikrinimas, kad konfidenciali informacija ir duomenys nepatektų į netinkamas rankas. Tai reiškia, kad prieiga prie sistemos elementų, jų naudojimas ir atskleidimas yra kontroliuojami, o tik įgalioti naudotojai gali pasiekti jautrią informaciją.

2. Integralumas – tai informacijos ir duomenų apsauga nuo neteisėto pakeitimo ar sugadinimo. Tai apima sistemos elementų modifikavimo, manipuliavimo ar naikinimo kontrolę, užtikrinant, kad duomenys būtų tikslūs ir patikimi.

3. Prieinamumas – tai užtikrinimas, kad informacija ir duomenys būtų prieinami visada, kai jų reikia. Tai reiškia, kad sistema turi būti veikianti, paslaugos – tęstiniai, o atkūrimo mechanizmai padeda greitai atstatyti sistemą ar jos funkcijas gedimo ar kibernetinės atakos atveju. Visi šitie principai buvo kaip pagrindas kibernetiniame saugume. [40]

NATO išskiria tris principus: „1. Prevencija (angl. Prevention); 2. Atsistatymo (angl. Resilence/Recovery); 3. Nekartojimo (angl. Non-dublication)“[41]. Visų pirma prevencija yra skirta užkirsti kelią pavojams, kad jie nevirstų incidentais, arba sumažinti galimų incidentų poveikį. Atsistatymo principas apima veiklą ir programas, įgyvendinamas reagavimo metu ir po jo, skirtas grąžinti subjektą į įprastą būseną.[42]

Tuo tarpu Europos Sąjungos kibernetinio saugumo strategijoje- „Atvira, saugi ir patikima kibernetinė erdvė“ yra išskirti 5 principai:

1. ES pagrindinės vertybės galioja ir skaitmeniniame, ir fiziniame pasaulyje.

2. Pagrindinių teisių, žodžio laisvės, asmens duomenų ir privatumo apsauga.

3. Prieiga visiems.

4. Demokratiškas ir veiksmingas daugelio suinteresuotųjų šalių dalyvavimu grindžiamas valdymas.

5. Bendra atsakomybė siekiant užtikrinti saugumą.[43]

Lietuvos Respublikos kibernetinio saugumo įstatyme (toliau- KSĮ), taip pat yra įtvirtinti kibernetinio saugumo principai:

---

[40] Alam, *supra note*, 18: 5.
[41] Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis ir Inga Malinauskaitė-van de Castel, *Lietuvos kibernetinio saugumo strategijos modelis* (Vilnius: Mykolo Romerio universitetas, 2017), 33.
[42] Alexander Klimburg (red.), National Cyber Security Framework Manual (Talinas: NATO CCDCOE, 2018), 23, https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.
[43] „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““, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52013JC0001.

„1) kibernetinės erdvės nediskriminavimo;

2) kibernetinio saugumo rizikos;

3) kibernetinio saugumo proporcingumo;

4) viešojo intereso viršenybės;

5) standartizacijos ir technologinio neutralumo;

6) subsidiarumo“ [44]

Lyginant ES strategijoje įtvirtintus principus su KSĮ įtvirtintais galima pastebėti tam tikru principų aiškinimo panašumu. Pavyzdžiui kibernetinės erdvės nediskriminavimo principai pilna apimtimi sutampa su strategijoje numatytu principu, kad teisės normos taikomos vienodai tiek skaitmeniniame, tiek fiziniame pasaulyje. Pagrindinių teisių, asmens duomenų ir privatumo apsaugos principas atitinka viešojo intereso viršenybės ir proporcingumo principus. Prieigos visiems principas KSĮ nėra tiesiogiai įtvirtintas, tačiau jį netiesiogiai galima sieti su viešojo intereso viršenybės principu, kadangi interneto prieigą galima lyginti su viešu interesu. Prieigos visiems viena iš idėjų yra, kad kiekvienas turėtų turėti galimybę saugiai naudotis internetu ir netrukdomai gauti informaciją. Taip pat pažymėtina, kad ES strategijoje akcentuojami daugelio suinteresuotųjų šalių dalyvavimo ir bendros atsakomybės principai yra artimi KSĮ įtvirtintam subsidiarumo principui, pagal kurį atsakomybė už kibernetinį saugumą tenka patiems tinklų ir informacinių sistemų valdytojams bei paslaugų teikėjams. Tarp analizuojamų principų taip pat galima pastebėti tam tikrų skirtumų. ES strategijoje pateikiami principai yra labiau orientuoti į vertybinius aspektus, tokius kaip žmogaus teisės, demokratinis valdymas ir visuotinė prieiga prie interneto, tuo tarpu KSĮ principai yra labiau praktinio ir teisinio pobūdžio, orientuoti į kibernetinio saugumo užtikrinimo mechanizmus. Pavyzdžiui, KSĮ aiškiai įtvirtina rizikos valdymo, standartizacijos ir technologinio neutralumo principus, kurie nėra tiesiogiai išskiriami ES strategijoje.

Palyginus visus analizuotus principus matoma, kad skirtinguose šaltiniuose kibernetinio saugumo principai formuluojami skirtingais aspektais, tačiau jų turinys iš esmės sutampa. JAV CŽV pateikti principai: konfidencialumas, integralumas ir prieinamumas yra laikoma fundamentiniu techniniu kibernetinio saugumo modeliu, kuris orientuotas į informacijos apsaugą. KSĮ principai iš esmės atspindi ES strategijoje įtvirtintas vertybines nuostatas, tačiau jos papildomos per praktinius kibernetinio saugumo įgyvendinimo aspektus.

Apibendrinant galima teigti, kad kibernetinio saugumo samprata keitėsi bei formavosi kartu su technologijų raida – nuo pirmųjų virusų ir kompiuterių atsiradimo iki šiuolaikinių

[44] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, TAR, žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr.

technologijų. Išanalizavus mokslinius straipsnius ir teisės aktus nustatyta, kad ši sąvoka apima priemonių, procesų, technologijų visumą, kuri yra skirta apsaugoti kibernetinę erdvę, informacines sistemas ir jose esančius duomenis nuo kibernetinių grėsmių. Taip pat analizuojant nustatyta, kad kibernetinis saugumas neapima vien tik technologijų, nes didelę dalį kibernetinių incidentų lemia neatsargus žmonių elgesys internete ir naudojantis išmaniosiomis technologijomis. Dėl šios priežasties turi būti skiriamas dėmesys kibernetinei higienai. Be to, kibernetinio saugumo užtikrinimas grindžiamas tam tikrais principais. Nors skirtinguose šaltiniuose šie principai formuluojami nevienodai, dauguma jų savo turiniu yra panašūs ir orientuoti į tą patį tikslą – užtikrinti informacijos apsaugą, sistemų patikimumą ir saugų jų veikimą, taip pat vartotojų, duomenų, sistemų ir pagrindinių asmens teisių ir laisvių apsaugą. Taigi galima teigti, kad kibernetinio saugumo samprata yra suprantama kaip įvairių priemonių, procesų, technologinių, informacijos sklaidos ir organizacinių, veiksmų visuma, skirta apsaugoti kibernetinę erdvę, informacines sistemas, kompiuterių tinklus, įrenginius ir juose esančius duomenis nuo kibernetinių grėsmių, nesankcionuotos prieigos ar neteisėto naudojimo. Ši sąvoka apima technines apsaugos priemones, teisinį reguliavimą, rizikos valdymą, saugumo politikos formavimą, darbuotojų mokymą bei saugaus elgesio kibernetinėje erdvėje principų taikymą.

1.2. Kibernetinės grėsmės

„Kibernetinės grėsmės vystėsi kartu su interneto plėtra“.[45] „Kibernetinės atakos yra labai įvairios, jų tikslai, metodai ir poveikis tiesiogiai priklauso nuo tipo. Dažniausiai užpuolikai siekia sutrikdyti, sugadinti, pavogti arba gauti neteisėtą prieigą prie kompiuterinės sistemos ar tinklo“ siekdamas gauti ar sugadinti duomenis“.[46] Žinoma kibernetinės grėsmės šiandien yra kitokios, nei tos, kurios buvo prieš dešimt metų ar net šiek tiek vėliau.

Paskelbtoje nacionalinėje kibernetinio saugumo atsąskaitotoje, 2023 m. daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje (angl. hosting), antroje vietoje – viešojo administravimo sektoriuje, trečioje vietoje – interneto paslaugų teikėjų infrastruktūroje ir prie jos prijungtuose fizinių asmenų galiniuose įrenginiuose. „Didžiausią žalą pagal kibernetinių atakų tipus ir metodus, 2023 m. darė elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusai“ (angl. ransomware), paskirstytų paslaugų trikdymo atakos (angl. Distributed Denial of Service, DDoS) (toliau – DDoS), tiekimo grandinės atakos (angl. Supply Chain Attacks) ir socialinės inžinerijos principais sukurtos atakos, kuriomis

[45] Juozapavičius ir kt, *supra note*, 16: 60.
[46] Šileikienė ir Usovaitė, *supra note*, 15:14.

siekiama išvilioti įvairius svarbius duomenis (angl. Social Engineering, phishing).“ [47]Remiantis Europos Sąjungos kibernetinio saugumo agentūros (toliau- ENISA) 2025 m. grėsmių apžvalgos ataskaita, penki labiausiai taikomi sektoriai ES pagal kibernetinių incidentų skaičių yra: viešasis administravimas, transportas, skaitmeninė infrastruktūra ir paslaugos, finansai bei gamyba, o esminiai subjektai sudaro 53,7 % visų užfiksuotų incidentų.[48] Toliau išanalizavus minėtą atskaitą matoma, kad viešojo administravimo sektoriuje vyravo mažo poveikio DDoS atakos (94,8 %), o išpirkos reikalaujanti programinė įranga ypač paveikė savivaldybes. „Phishing“ (liet. sukčiavimas apsimetant) buvo pagrindinis įsilaužimo faktorius, sudarantis apie 60 % atvejų, įskaitant kenkėjišką šlamštą, internetinį turinio generavimą ir kenkėjišką reklamą. Nepaisant pranešto 11 % sumažėjimo incidentų mažėjimo, išpirkos reikalaujanti programinė įranga išliko didžiausią įtaką turinčia kibernetinių nusikaltimų priemone.[49] Remiantis, tuo, kad „kenkėjiški kibernetiniai įvykiai vyksta kiekvieną dieną – nuo žemo lygio iki technologiškai sudėtingų atak“. [50] Taip pat atsižvelgiant tiek į Lietuvos, tiek į Europos Sąjungos kibernetinio saugumo situacija, akivaizdu, kad yra aktualu ir svarbu nustatyti ir išanalizuoti kibernetinių incidentų rūšys ir jų samprata.

Kibernetinis incidentas – yra suprantamas kaip „įvykis ar veika kibernetinėje erdvėje, galinti sukelti grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą“.[51] Vienos dažniausios kibernetinio saugumo grėsmės yra tokios kaip:

1. Duomenų vagystė (angl. „phishing“ kilęs nuo žodžių „password fishing“ - slaptažodžių žvejyba) – šis incidentas yra vienas iš labiausiai paplitusių kibernetinio saugumo atakų rūšių. [52]Tai tokia sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius bei kitus konfidencialius duomenis. Dažniausiai tokio pobūdžio atakos yra nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Vėliau tokiu būdu gauta informacija gali būti panaudota vykdant nusikalstamas veikas:

---

[47] „2023 Nacionalinė kibernetinio saugumo būklės ataskaita“, Lietuvos Respublikos krašto apsaugos ministerija, (Vilnius, 2023), 29,

[48] ENISA Threat Landscape 2025“, ENISA, žiūrėta 2026 m. kovo 6 d., https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf.

[49] *Ibid*.

[50] „Cyber Defence“, NATO, žiūrėta 2026 m. kovo 6 d., https://act.nato.int/activities/cyber/. https://www.act.nato.int/activities/cyber/#:~:text=NATO%20and%20its%20Allies%20rely%20on%20strong%20and,defence%2C%20crisis%20prevention%20and%20management%2C%20and%20cooperative%20security.

[51] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note*, 44.

[52] Meraj Farheen Ansari, Pawan Kumar Sharma ir Bibhu Dash, „Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training“, *International Journal of Smart Sensor and Adhoc Network* 3, 3 (2022): 61, https://www.researchgate.net/publication/362112009.

neteisėtus prisijungimus prie informacinių sistemų, pinigų vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis kortelėmis.[53] Todėl yra svarbu, kad vartotojai neturėtų persiųsti nepatvirtintų el. laiškų, spausti įtartinų nuorodų laiškuose ar naudoti paieškos sistemų ieškant internetinių aukų rinkimo ar labdaros organizacijų.[54]

2. Trojan - Trojos arkliai tai yra programos, turinčios kenkėjiškų funkcijų ir slepiasi kitose programose.[55] Kitaip nei virusai, trojos arkliai savaime nesidaugina – jie yra paskleidžiami per kitą kenkėjiška programinė įranga. Į kompiuterius dažniausiai patenka išnaudodami spragas naršyklėse arba parsiunčiami pačio vartotojo, juos pateikiant kaip naudingas programas. Užkrėstoje sistemoje atveria atgalines duris (angl. Backdoor), tokiu būdu įgalindamas nuotolinį įrenginio valdymą. [56] Šis programinis kodas skirstomas į dvi pagrindines kategorijas:

A. Nuotolinio prieigos Trojanus (angl. remote-Access Trojan)- Nuotolinio prieigos Trojanai leidžia užpuolikui nuotoliniu būdu kontroliuoti aukos kompiuterį, vogti konfidencialią informaciją ir vykdyti kitas kenksmingas operacijas.

B. Bendruosius Trojanus (angl. general trojan). Bendrieji Trojanai atlieka įvairias kenksmingas veiklas: gali manipuliuoti sistemos failais, nukreipti vartotojus į kitas svetaines, įdiegti kenksmingą programinę įrangą, stebėti vartotojo veiklą bei perduoti duomenis užpuolikui.[57]

3. Ransomware. Kenkėjiškos programinės įrangos rūšis, kuri neleidžia vartotojui pasiekti kompiuterio failų, sistemų ar tinklų ir reikalauja sumokėti išpirką už prieigos atkūrimą. Atakos gali sukelti didelius veiklos sutrikimus bei svarbios informacijos ir duomenų praradimą. Vartotojas gali netyčia atsisiųsti į kompiuterį atidaręs elektroninio laiško priedą, paspaudęs reklamą, sekęs nuorodą arba net apsilankęs interneto svetainėje, kurioje yra įterpta kenkėjiška programa. Kai kenkėjiškas kodas patenka į kompiuterį, jis užblokuoja prieigą prie paties kompiuterio arba jame saugomų duomenų ir failų. Pavojingesnės šios programos versijos gali užšifruoti failus ir aplankus vietiniuose diskuose, prijungtuose įrenginiuose bei tinklu sujungtuose kompiuteriuose. [58]

4. Paskirstytų paslaugos trikdymo atakos „DDoS“(toliau – DDoS). Šios atakos bando išnaudoti sistemos resursus ir smarkiai sumažinti paslaugų prieinamumą. [59]DDoS atakos metu

---

[53] „Phishing“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. kovo 5 d., https://www.nksc.lt/rekomendacijos/phishing.html.
[54] Farheen, Sharma, Dasr, *supra note,* 53.
[55] „Trojan/ObscuGen“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. kovo 5 d., https://www.nksc.lt/rekomendacijos/trojanmalwareobscugen.html.
[56] „Rekomendacija dėl kibernetinių incidentų prevencijos“. Valstybinė duomenų apsaugos inspekcija. Žiūrėta 2026 m. kovo 19 d. https://vdai.lrv.lt/public/canonical/1753770948/1018/Rekomendacija_kibernetiniai%20incidentai_2024%20m.pdf
[57] Rashid, Salar Jamal, Shatha A. Baker, Omar I. Alsaif ir Ali I. Ahmad. „Detecting Remote Access Trojan (RAT) Attacks based on Different LAN Analysis Methods“. *Engineering, Technology & Applied Science Research* 14, Nr. 5 (2024): 17294, https://doi.org/10.48084/etasr.8422.
[58] „Ransomware“. Federal Bureau of Investigation. Žiūrėta 2026 m. kovo 6 d. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware.
[59] „What Is a DDoS Attack?“, Akamai, žiūrėta 2026 m. kovo 6 d., https://www.akamai.com/glossary/what-is-ddos

robotų tinklas (angl. botnet) užtvindo tikslinę svetainę arba paslaugą dideliu kiekiu HTTP užklausų ir tinklo srauto. Tokios atakos metu daugybė kompiuterių vienu metu nukreipia užklausas į vieną sistemą, dėl ko teisėti vartotojai nebegali naudotis paslauga. Dėl to paslaugų veikimas gali būti reikšmingai sulėtintas arba visiškai sutrikdytas tam tikram laikotarpiui. Tam tikrais atvejais kibernetiniai nusikaltėliai gali bandyti pasinaudoti saugumo pažeidžiamumais ir įsiskverbti į sistemų duomenų bazes, siekdami gauti prieigą prie konfidencialios informacijos. DDoS atakos dažnai išnaudoja informacinių sistemų saugumo spragas ir gali būti nukreiptos į bet kurį viešai internete pasiekiamą tinklo galinį tašką. Tokios perkrovos atakos gali trukti nuo kelių valandų iki kelių dienų, o vienos atakos metu gali pasireikšti keli skirtingi sistemos veikimo sutrikimai.[60]

5. „Brute force“ atakos - tai bandymai atspėti ar parinkti vartotojo prisijungimo duomenis (slaptažodžius) prie informacinės sistemos, įvedinėjant atsitiktines simbolių sekas ir dažnai naudojamas kombinacijas.[61]

6. Tiekimo grandinės atakos (angl. Supply Chain Attacks) – tai yra kibernetinės atakos rūšis kuri yra nukreipta prieš mažiau saugius organizacijos tiekimo grandinės tinklo elementus. Šių atakų tikslas – pakenkti organizacijai, nukreipiant ją į pažeidžiamus jos tiekimo grandinės komponentus, įskaitant programinę įrangą, aparatinę įrangą ar išorinių tiekėjų teikiamas paslaugas.[62] Jungtinės Karalystė Nacionalinio kibernetinio saugumo centras (angl. National Cyber Security Centre) pateikia kelis pagrindinius tiekimo grandinės atakų tipus:

1. Trečiųjų šalių programinės įrangos tiekėjai (angl. Third-party software providers) – tai yra, kai atakos vykdomos kompromituojant programinės įrangos tiekėjus ir platinant kenkėjišku kodu užkrėstą programinę įrangą vartotojams. Tokiu būdu kenkėjiška programinė įranga patenka į organizacijų sistemas kartu su teisėta programine įranga. Žr. pav. 2.

2. Svetainių kūrimo platformos arba svetainių kūrėjai (angl. Website builders) – užpuolikai kompromituoja svetainių kūrimo platformas ar skaitmenines agentūras ir per jas į svetaines įterpia kenkėjišką kodą. Dėl to lankytojai gali būti nukreipiami į kenkėjiškas svetaines arba jų įrenginiai gali būti užkrėsti kenkėjiška programine įranga.

3. Trečiųjų šalių duomenų saugyklos (angl. Third-party data stores) – atakuojamos organizacijos, kurios saugo kitų įmonių ar klientų duomenis, siekiant gauti prieigą prie jautrios informacijos, pavyzdžiui, asmens ar finansinių duomenų.

---

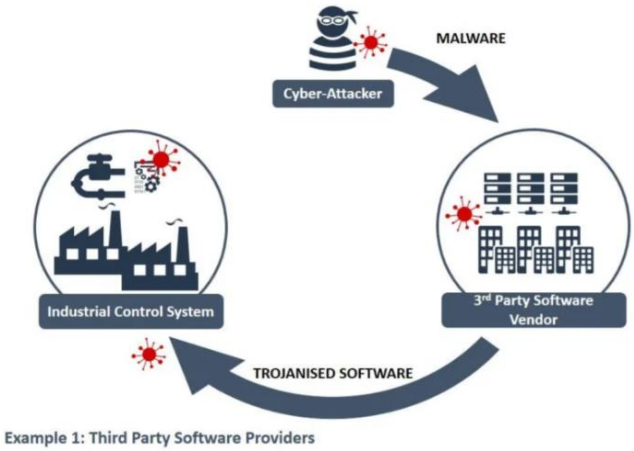
[60] „Kas yra „DDoS“ ataka?“, Microsoft, žiūrėta 2026 m. kovo 6 d., https://www.microsoft.com/lt-lt/security/business/security-101/what-is-a-ddos-attack.

[61] „„Brute force“ atakos“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. kovo 19 d., https://nksc.lt/rekomendacijos/brute_force_atakos.html

[62] „2023 Nacionalinė kibernetinio saugumo būklės ataskaita“, *supra note*, 47:25.

4. „Watering hole“ tipo atakos (angl. Watering hole attacks) – tai atakos, kai užpuolikai užkrečia dažnai tikslinės organizacijos darbuotojų lankomas interneto svetaines ir per jas platina kenkėjišką programinę įrangą, siekdami užkrėsti tikslinės organizacijos sistemas.[63]

7. Nulinės dienos atakos (angl. *zero day*)- Tai kai yra išnaudojama viena ar kelios nežinomos spragos.[64] Šios atakos yra nukreiptos į programinės įrangos kodo pažeidžiamumus, kurių organizacijos dar nėra aptikusios, todėl jie dar nėra ištaisyti ar pašalinti. Dažnu atveju įsibrovėliai gali išlikti aktyvūs organizacijos sistemose nepastebėti mėnesius ar net metus.[65]



2 pav. Trečiųjų šalių programinės įrangos tiekėjų atakos schema[66]

8. Kriptoresursų vagystė (angl. cryptojacking). Tai kibernetinė ataka, kuria yra perimama kompiuterio, mobiliojo įrenginio ar serverio kontrolę tam, kad galima būtų kasti virtualią valiutą. Ataka dažniausiai prasideda į kompiuterį įdiegus kenkėjišką programinę įrangą arba paleidus „JavaScript“ kodą, kuris įsiskverbia į vartotojo interneto naršyklę.[67] Šios atakos metu yra naudojami kompiuterio našumo resursus kriptovaliutų kasimui. Dažnai vienintelis kriptoresursų vagystės požymis yra sumažėjęs kompiuterio našumas arba intensyviai veikiantys aušinimo ventiliatoriai.

Analizuojant kibernetinius incidentus matoma, kad įvairios kenkėjiškos programinės įrangos, paslaugų trikdymo atakos ir įvairūs kiti metodai kelia grėsmę informacinių sistemų veikimui ir duomenų saugumui. Tačiau iškylą klausimas, kokie subjektai vykdo šias kibernetines atakas ir kokie yra jų pagrindiniai motyvai ir jų tikslai.

---

[63] „Third party software providers“, National Cyber Security Centre, žiūrėta 2026 m. kovo 6 d., https://www.ncsc.gov.uk/collection/supply-chain-security/third-party-software-providers.

[64] „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“, TAR, žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/legalAct.html?documentId=c8e268a0a00011efa605b9842742bf37

[65] „What Is a Cyber Attack?“. Fortinet. Žiūrėta 2026 m. kovo 19 d. https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack.

[66] Shahid, *supra note*, 18.

[67] „What Is a Cyber Attack?“, *op. cit.*

Kibernetinio saugumo agentūros (ENISA) išskiria šiuos subjektus:

1. Su valstybe susiję vykdytojai – tai grupės, vykdančios išpuolius (pvz. šnipinėjimą) politiniais ar strateginiais tikslais,

2. Kibernetinių nusikaltimų vykdytojai- siekia finansinės naudos vykdydami kibernetinius išpuolius.

3. Privačiojo subjekto piktavaliai vykdytojai – subjektai, kuriantys ir parduodantys kibernetinius įsilaužimo įrankius, dažnai vyriausybėms ir privatiems asmenims.

4. Isilaužėliai aktyvistai- jie dalyvauja sutrikdymo arba įsilaužimo veikloje politinių ar socialinių pokyčių tikslais, kartais remiami valstybinio veikėjo.[68]

Generolo Jono Žemaičio Lietuvos karo akademijos parengtame vadovėlyje „Nacionalinis saugumas ir krašto gynyba“ išskiriami šie kibernetinių nusikaltėlių tipai:

„1. „Programuotojai“- dažniausiai jauni mažai patyrę įsilaužėliai, kurie nelegalia veikla užsiima dėl pramogos, dažnu atveju nevisiškai suprasdami įrankius, kuriais naudojasi.

2. Vidiniai agentai- tai asmenis kurie tyčia ar netyčia įvykdo išorinės nusikalstamos grupuotės nurodymus, pavyzdžiui, įdiegia kenkimo programą.

3. Kibernetiniai aktyvistai ir teroristai- jie vykdo kibernetines atakas iš religinių ar ideologinių įsitikinimų, dažniausiai jų tikslas yra viešumas ir destrukcija“.[69] Taip pat šio tipo subjektai gali būti vadinami ir Haktyvistai – nes tai yra asmenys, kurių tikslas yra vienodas nes jie vykdo kibernetinius išpuolius ideologiniais ar politiniais motyvais. Tokie aljansai leidžia kryptingiau atakuoti konkrečias valstybes nacionaliniu lygmeniu. Viešai deklaruodami savo pasiekimus, haktyvistai siekia sukelti kuo daugiau sąmyšio.[70]

4. Organizuoti nusikaltėliai: teismų praktikoje „vienas iš organizuotą grupę apibrėžiančių požymių yra išankstinis bendrininkų susitarimas daryti nusikalstamą veiką, t. y. kuomet organizuotos grupės nariai iš anksto aptaria nusikalstamos veikos planą, numato įvykdymo mechanizmą, pasiskirsto užduotis, susitaria dėl nusikaltimo padarymo būdo, vietos ir laiko. Šios aplinkybės įtakoja glaudžių, besitęsiančių ryšių atsiradimą, suformuoja suvokimą apie priklausymą grupei“. [71] Tad ir kibernetinių nusikaltimų kontekste vieni asmenys „atsako už kenkimo programinės įrangos gamybą, kiti platina ir rašo apgaulingus laiškus, treti ja naudojasi

---

[68] „Kokios yra pagrindinės kibernetinės grėsmės ES?“, Europos Vadovų Taryba ir Europos Sąjungos Taryba, žiūrėta 2026 m. kovo 19 d., https://www.consilium.europa.eu/lt/policies/top-cyber-threats/

[69] Juozapavičius ir kt, *supra note*, 16: 63.

[70] „A Comparative Study of Russian Cyber Offensive Capabilities from 2022 to 2025“, National Cyber Security Centre, žiūrėta 2026 m. kovo 19 d., https://nksc.lt/doc/rkgc/A_Comparative_Study_of_Russian_Cyber_Offensive_Capabilities_from_2022_to_2025.pdf .

[71] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. rugsėjo 30 d. nutartis baudžiamojoje byloje Nr. 2K-254/2008“, LITEKO, žiūrėta 2026 m. balandžio 22 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=bed3a4fb-f5b3-471d-b90e-c63034a1d833.

užgrobdami kompiuterius ir vogdami duomenis, ketvirti surenka išpirkas, užsiima pinigų gryninimu, paskirsto grobį ir t. t. Taip pat šios grupuotės gali specializuotis, teikti paslaugas viena kitai, gali net rengti mokymus ar nuomoti kenkimo įrangą“.[72]

5. Valstybinės kibernetinės grupuotės- tai yra „įvairių saugumo tarnybų tiesiogiai ar netiesiogiai remiamos kibernetinių įsilaužėlių grupuotės, kurioms tikslus iškelia tos tarnybos. Dažniausi tikslai – kitų valstybių šnipinėjimas, duomenų vagystės, kompromituojančios informacijos paieška“.[73]

Apibendrinant galima teigti, kad kibernetinių atakų vykdytojai gali būti labai įvairūs – nuo pavienių asmenų ar finansiškai remiamų organizuotų, su valstybėmis susijusių kibernetinių grupuočių. Žinoma šių subjektų tikslai ir veikimo mastas gali skirtis. Pagrindiniai skirtumai dažniausiai pasireiškia jų motyvuose, veiklos organizuotume, siekiamuose rezultatuose – nuo finansinės naudos iki ideologinių tikslų ir politinių interesų įgyvendinimo.

Taigi, tiek Lietuvoje, tiek Europos Sąjungoje dažniausiai fiksuojami panašaus pobūdžio kibernetiniai incidentai – tiekimo grandinės atakos, duomenų vagystės „phishing“, socialinės inžinerijos atakos, išpirkos reikalaujančios kenkėjiškos programinės įrangos bei paskirstytų paslaugų trikdymo (DDoS) atakos. Nors šių incidentų pobūdis ir naudojamos technologijos iš esmės yra panašios, nes dažniausiai taikomi tie patys atakų metodai – socialinės inžinerijos (psichologinės manipuliacijos technika, kai sukčiai apgaulės būdu priverčia žmones atskleisti konfidencialią informaciją (slaptažodžius, banko duomenis) ar atlikti nesaugius veiksmus,[74] kenkėjiškos programinės įrangos naudojimas ar paslaugų trikdymo atakos, tačiau jų mastas ir poveikis gali skirtis. Skirtumai dažniausiai pasireiškia taikomais sektoriais, kritinės infrastruktūros svarba, atakų intensyvumu bei nusikaltėlių siekiamais tikslais – nuo finansinės naudos ar duomenų vagystės iki politinių ar kitų interesų įgyvendinimo. Pažymėtina, kad kibernetinių grėsmių sąrašas nėra galutinis, kadangi analizuoti tik aktualiausi incidentai. Taip pat svarbu pabrėžti, kad technologijų plėtra lemia nuolatinį naujų atakų formų ir metodų atsiradimą. Todėl kibernetinių incidentų rūšių, metodų, jų vykdytojų analizė sudaro svarbią kibernetinio saugumo sampratos dalį ir leidžia geriau suprasti kibernetinį saugumą.

---

[72] Juozapavičius ir kt, supra note, 16: 63.
[73] *Ibid.*
[74] „Cybersecurity: social engineering“, European Council, žiūrėta 2026 m. kovo 19 d., https://www.consilium.europa.eu/en/policies/cybersecurity-social-engineering/.

2. KIBERNETINIO SAUGUMO TEISINIS REGLAMENTAVIMAS TARPTAUTINIU IR EUROPOS SĄJUNGOS LYGMENIU

„Kibernetinis saugumas – labai svarbi ir specifinė veiklos rūšis, kuri reikalauja nuoseklaus ir detalaus teisinio reglamentavimo.“[75] Vienais iš pagrindinių kibernetinio saugumo užtikrinimo šaltinių laikomi įvairūs tarptautiniai ir Europos Sąjungos teisės aktai bei kibernetinio saugumo strategijos. Atsižvelgiant į tai, tikslinga išanalizuoti tarptautinių ir Europos Sąjungos teisės aktų ištakas, kibernetinio saugumo kontekste.

Kibernetinio saugumo teisinio reglamentavimo kontekste itin svarbi tampa asmens duomenų, privataus gyvenimo ir informacijos apsauga. Vienas iš pirmų ir pagrindinių tarptautinių dokumentų, nustatančių iš dalies šių teisių apsaugą yra 1950 metų priimta Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (toliau - EŽTK). Jos 8 straipsnis įtvirtina „teisę į privataus ir šeimos gyvenimo gerbimą,“ [76] kuri iš dalies sudaro pagrindą asmens duomenų, informacijos konfidencialumo ir komunikacijų slaptumo apsaugai skaitmeninėje erdvėje. Šio straipsnio 1 dalyje nustatyta, kad „kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas.“ [77] Taip pat pabrėžiama, kad valstybės institucijos gali riboti šią teisę tik įstatymų nustatytais atvejais ir tik tada, kai tai būtina demokratinėje visuomenėje – siekiant užtikrinti valstybės saugumą, viešąją tvarką, visuomenės sveikatą ar moralę, taip pat kitų asmenų teises ir laisves. [78]Todėl Konvencijos 8 straipsnį galima laikyti teisiniu pagrindu kibernetinio saugumo užtikrinimui, nes jis palaiko balansą tarp asmens teisės į privatumą ir valstybės pareigos užtikrinti visuomenės bei valstybės saugumą informacinėje erdvėje. Generalinės Asamblėjos priimtoje ir paskelbtoje 1948 m. gruodžio 10 d., Visuotinėje žmogaus teisių deklaracijoje 12 straipsnyje yra įtvirtinta, jog „niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją,“[79] o kiekvienas asmuo turi įstatymų numatyta apsaugą nuo tokio kišimosi. [80] Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7 straipsnyje numatyta, kad „kiekvienas asmuo turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir komunikacijos slaptumas“, o 8 straipsnis numato, kad kiekvienas turi teisę į savo asmens duomenų apsaugą. Tokie duomenys turi būti tinkamai tvarkomi ir naudojami tik konkretiems tikslams ir tik

---

[75] Štitilis, *supra note*, 6: 191.
[76] „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, TAR, žiūrėta 2025 m. lapkričio 4 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841?jfwid=-b2dkogt43.
[77] *Ibid.*
[78] *Ibid.*
[79] „Visuotinė žmogaus teisių deklaracija“, TAR, žiūrėta 2025 m. lapkričio 4 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385.
[80] *Ibid*.

atitinkamam asmeniui sutikus arba kitais įstatymo nustatytais teisėtais pagrindais. Kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis bei į tai, kad jie būtų ištaisomi. Taip pat yra pabrėžta, kad nepriklausoma institucija turi kontroliuoti, kaip laikomasi šių taisyklių [81]. Sutartyje dėl Europos Sąjungos veikimo (toliau- SESV) 16 straipsnyje įtvirtinta, kad kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą. [82] Apibendrinant matoma, kad šios sutartys sudaro tarptautinį ir ES teisinį pagrindą asmens privatumo apsaugai kibernetinėje erdvėje, įpareigojant valstybes užtikrinti, kad technologijų raida ir kibernetinio saugumo priemonės nepažeistų žmogaus teisių ir laisvių. Tai patvirtina ir Europos Žmogaus Teisių Teismo (toliau – EŽTT) praktika.

„Byloje K. U. prieš Suomiją pareiškėjas skundėsi, kad pažinčių svetainėje apie jį buvo pateiktas intymaus turinio skelbimas. Paslaugų teikėjas neatskleidė asmens, kuris paskelbė informaciją internete, tapatybės, nes turėjo laikytis Suomijos teisėje nustatytos konfidencialumo pareigos. Pareiškėjas skunde teigė, kad Suomijos teisėje nebuvo numatyta tinkama apsauga nuo privataus asmens veiksmų internete. EŽTT pateikė išvadą, kad valstybės ne tik turėjo pareigą susilaikyti nuo savavališko asmenų privataus gyvenimo apribojimo, bet ir turėjo imtis priemonių, kurios padėtų apsaugoti pagarbą privačiam gyvenimui net ir asmenų tarpusavio santykių srityje, nustatymu“. Pareiškėjo byloje praktinė ir veiksminga apsauga reiškė būtinybę imtis veiksmingų priemonių nusikaltėliui nustatyti ir patraukti jį baudžiamojon atsakomybėn. Tačiau valstybė tokios apsaugos neužtikrino, todėl buvo nustatyta, kad EŽTK 8 straipsnis buvo pažeistas“.[83]

Apibendrinant, galima teigti, kad šie analizuoti dokumentai iš dalies laikomi kibernetinio saugumo teisinio reglamentavimo ištakomis, nes juose pirmą kartą įtvirtintos pagrindinės asmens privatumo, duomenų apsaugos ir komunikacijų slaptumo teisės normos. Toliau analizuojant kibernetinio saugumo teisinį reglamentavimą, yra svarbu išanalizuoti tarptautinius ir Europos Sąjungos (toliau- ES) teisės aktus, kurie užtikrina kibernetinį saugumą. Ne ką mažiau svarbu apžvelgti pagrindinius NATO ir Europos Sąjungos kibernetinio saugumo strategijų aspektus. Todėl šiame skyriuje toliau bus analizuojamos NATO ir ES kibernetinio saugumo strateginės kryptys. Taip pat bus apžvelgti ir išanalizuoti pagrindiniai tarptautiniai ir Europos Sąjungos teisės aktai reglamentuojantys kibernetinį saugumą.

„Iki 2016 m. pagal NATO klasifikaciją egzistavo keturi operaciniai dėmenys: žemė, jūra, oras ir kosmosas. Nuo 2016 m. atsirado penktasis – kibernetinė erdvė, atitinkamai – karinės kibernetinės pajėgos. Bet kokie priešiški veiksmai vienos šalies kibernetinėje erdvėje yra

---

[81] „Europos Sąjungos pagrindinių teisių chartija“, EUR-Lex, žiūrėta 2025 m. lapkričio 4 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12012P/TXT.

[82] „Sutartis dėl Europos Sąjungos veikimo (suvestinė redakcija)“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12012E/TXT.

[83] „2009 m. kovo 2 d. Europos Žmogaus Teisių Teismo sprendimas byloje K. U. prieš Suomiją, Nr. 2872/02“, HUDOC, žiūrėta 2025 m. sausio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62009CJ0092.

traktuojami kaip visų NATO šalių užpuolimas, kaip ir veiksmai bet kurioje kitoje srityje.“[84]Rusijos karas prieš Ukrainą visgi dar labiau išryškino, kad kibernetinė veikla yra integrali šiuolaikinių konfliktų dalis. [85] NATO kibernetinės gynybos strategija grindžiama kolektyvinės gynybos ir atsparumo principais. Šią strategiją įgyvendina dvejais būdais– Kibernetinės gynybos politika (ir jai pridedamas veiksmų planas) (angl. Cyber Defence Policy and Action Plan) bei Kibernetinės gynybos įsipareigojimas (*angl. Cyber Defence Pledge*)[86] NATO visą laiką saugojo savo ryšių ir informacines sistemas, 2002 m. NATO viršūnių susitikime Prahoje pirmą kartą kibernetinė gynyba buvo įtraukta į Aljanso politinę darbotvarkę. Tuo metu Aljanso lyderiai susitikime išreiškė poreikį užtikrinti papildomą šių informacinių sistemų apsaugą. Dėl 2007 m. įvykdytų kibernetinių išpuolių prieš Estijos valstybines ir privačias įstaigas sąjungininkų gynybos ministrai sutarė, kad šioje srityje reikia skubiai imtis veiksmų. Todėl 2008 m. NATO patvirtino savo pirmąją kibernetinės gynybos politiką.[87] Strategijoje buvo nustatytas poreikis apsaugoti pagrindines informacines sistemas, dalytis geriausia praktika ir plėtoti gebėjimus padėti sąjungininkams kibernetinių atakų atveju, todėl buvo įsteigta Kibernetinės gynybos valdymo institucija ir Bendradarbiaujantis kibernetinės gynybos kompetencijos centras (angl. the Cyber Defense Management Authority (CDMA) and the Cooperative Cyber Defense Center of Excellence (CCDCOE)).[88]

2011 m. NATO patvirtino antrąją NATO kibernetinės gynybos politiką, kurioje išdėstyta koordinuotų kibernetinės gynybos pastangų visame Aljanse vizija, atsižvelgiant į sparčiai besikeičiančią grėsmių ir technologijų aplinką.[89] 2012 m. liepos mėn., buvo įsteigta NATO Ryšių ir informacijos agentūra. 2014 m. buvo patvirtinta nauja kibernetinės gynybos politiką. Šioje politikoje kibernetinė gynyba buvo pripažinta pagrindinės NATO kolektyvinės gynybos užduoties dalimi, o tai reiškia, kad kibernetinė ataka gali būti pagrindas taikyti NATO steigimo sutarties 5 straipsnį. [90] Penktas Šiaurės Atlanto sutarties straipsnis numato, kad „Šalys susitaria, kad vienos ar kelių iš jų ginkluotas užpuolimas Europoje ar Šiaurės Amerikoje bus laikomas jų visų užpuolimu, ir todėl susitarė, kad tokio ginkluoto užpuolimo atveju kiekviena iš jų, įgyvendindama individualios ar kolektyvinės savigynos teisę, pripažintą Jungtinių Tautų Chartijos 51 straipsnyje,

---

[84] Juozapavičius ir kt, *supra note*, 16: 60.
[85] „2023 Nacionalinė kibernetinio saugumo būklės ataskaita“, *supra note,* 47:25.
[86] Justina Lukaševičiūtė, EU and NATO Cyber Security Policy (magistro darbas, Vytauto Didžiojo universitetas, 2019), žiūrėta 2026 m. kovo 19 d., https://portalcris.vdu.lt/server/api/core/bitstreams/7779f711-92a6-4392-bfa9-a40831f7e01a/content.
[87] „Cyber defence“, NATO, žiūrėta 2026 m. kovo 10 d., https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.
[88] Jason Healey ir Klara Tothova Jordan, NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow (Atlantic Council, 2014), žiūrėta 2026 m. kovo 10 d., https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf.
[89] Aleksander Olech ir Damjan Štruc, The Evolution of Cyber Forces in NATO Countries (NATO Cooperative Cyber Defence Centre of Excellence, 2025), žiūrėta 2026 m. kovo 19 d., https://ccdcoe.org/uploads/2025/07/The_evolution_of_cyber_forces_in_NATO_countries.pdf.
[90] *Ibid.*

nedelsdama suteiks pagalbą užpultai ar užpultoms Šalims, individualiai ir kartu su kitomis Šalimis, imdamasi tokių veiksmų, kokie atrodys būtini, įskaitant ginkluotos jėgos panaudojimą, Šiaurės Atlanto regiono saugumui atkurti ir palaikyti“.[91] Todėl, 2016 m. Varšuvoje vykusiame NATO viršūnių susitikime sąjungininkų valstybių ir vyriausybių vadovai dar kartą patvirtino NATO gynybos mandatą ir pripažino kibernetinę erdvę operacijų sritimi, kurioje NATO privalo gintis. Taip pat šiame susitikime sąjungininkai priėmė įsipareigojimą dėl kibernetinės gynybos, pagal kurį įsipareigojo šalis stiprinti savo nacionalinių tinklų ir infrastruktūros kibernetinę apsaugą.[92] 2018 m. NATO viršūnių susitikime Briuselyje sąjungininkų lyderiai susitarė įsteigti naują Kibernetinės erdvės operacijų centrą kaip sustiprintos NATO vadovavimo struktūros dalį. Šis Centras užtikrina situacijos suvokimą ir koordinuoja NATO operacinę veiklą kibernetinėje erdvėje ir per ją. 2023 m. NATO viršūnių susitikime Vilniuje sąjungininkai pritarė naujai koncepcijai. Ši koncepcija yra skirtą sustiprinti kibernetinės gynybos indėlį į bendrą NATO atgrasymo ir gynybos poziciją. Koncepcijoje integruotos tris NATO kibernetinės gynybos lygius – politinį, karinį ir techninį, užtikrindama nuolatinį civilinį ir karinį bendradarbiavimą tiek taikos, tiek krizės ar konflikto metu, taip pat – bendradarbiavimą su privačiu sektoriumi, kai tai tinkama. [93]Taip pat susitikimo Vilniuje metu savo veiklą pradėjo ir buvo sėkmingai išbandytas naujas NATO virtualus reagavimo į kibernetinius incidentus pajėgumas (angl. Virtual Cyber Incident Support Capability, VCISC), kuris sutelkia sąjungininkių pastangas reaguojant į didelio masto kibernetinius incidentus.[94]

Apibendrinant galima teigti, kad NATO kibernetinės gynybos strategija vystėsi kartu su augančiomis kibernetinėmis grėsmėmis. Laikui bėgant kibernetinė erdvė buvo pripažinta viena iš svarbių operacijų sričių, o kibernetinė gynyba tapo neatsiejama kolektyvinės gynybos dalimi. NATO strategijoje ypatingas dėmesys skiriamas valstybių narių bendradarbiavimui, nacionalinių pajėgumų stiprinimui ir greitam reagavimui į kibernetinius incidentus. Todėl NATO veikla kibernetinės gynybos srityje yra svarbi siekiant užtikrinti Aljanso valstybių saugumą ir atsparumą. Kadangi technologijos nuolat tobulėja, o skaitmeninė aplinka tampa vis sudėtingesnė, NATO vaidmuo šioje srityje išlieka svarbus.

---

[91] The North Atlantic Treaty, NATO, 1949 m. balandžio 4 d., žiūrėta 2026 m. kovo 19 d., https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty.
[92] Olech, Štruc „*supra note,* 90:11.
[93] Olech, Štruc „*supra note,* 92:20.
[94] „NATO kibernetinės gynybos iniciatyvos“, Lietuvos Respublikos krašto apsaugos ministerija, žiūrėta 2026 m. kovo 19 d., https://kam.lt/duk/nato-kibernetines-gynybos-iniciatyvos/.

2013 m., buvo priimta rezoliucija- ES kibernetinio saugumo strategija „atvira, saugi ir patikima kibernetinė erdvė“ kuria siekiama didinti atsparumą kibernetinėms grėsmėms. [95] Pagrindiniai 2013 m. strategijos aspektai buvo- kibernetinis atsparumas, pramonės ir technologijų ištekliai, elektroniniai nusikaltimai, kibernetinė gynyba, tarptautinė politika. Galima teigti, kad strategija padėjo pagrindus ES kibernetinio saugumo politikai[96]. Tačiau keičiantis grėsmėms, tai yra keičiantis jų mastui, būdui 2021 m. kovo 22 d. Taryba priėmė išvadas dėl ES kibernetinio saugumo strategijos. Naujoji skaitmeninio dešimtmečio kibernetinio saugumo strategija buvo pristatyta 2020 m. gruodžio mėn. Joje numatytas ES veiksmų pagrindas, skirtas apsaugoti piliečius ir įmones nuo kibernetinių grėsmių, skatinti saugias informacines sistemas ir apsaugoti pasaulinę, atvirą, laisvą ir saugią kibernetinę erdvę.[97] Naująja strategija yra siekiama užtikrinti visuotinį ir atvirą internetą su apsaugos priemonėmis. Strategijoje yra pateikiami konkretūs pasiūlymai dėl trijų pagrindinių priemonių taikymo. Šios priemonės apims:

- atsparumą, technologinį suverenumą ir lyderystę;
- veiklos pajėgumą užkirsti kelią, atgrasyti ir reaguoti;
- bendradarbiavimą siekiant plėtoti pasaulinę ir atvirą kibernetinę erdvę.[98]

Taip pat valstybės narės buvo paragintos apsaugoti ES nuo kibernetinių grėsmių, sukurti saugią ryšių aplinką, be kita ko, naudojant kvantinį šifravimą, užtikrinti prieigą prie duomenų teisminiais ir teisėsaugos tikslais.[99] Nuo pat strategijos pradžios buvo imtasi įvairių priemonių pavyzdžiui, tokių kaip preliminarūs ministrų susitarimai dėl kibernetinio saugumo, išsakytos pozicijos dėl įvairių tesės aktų priėmimo, sankcijų skyrimas dėl teisės aktų nesilaikymo. Taip pat Europos Vadovų Taryba eile metų ragindavo imtis priemonių, kad Europos Sąjungoje būtų užtikrintas tvirtas kibernetinis saugumas. Tačiau vienos svarbiausių priemonių buvo teisės aktų priėmimas ir svarstymas.

Tiek NATO, tiek Europos Sąjunga kibernetinį saugumą laiko svarbia saugumo politikos dalimi. Abi organizacijos siekia stiprinti valstybių atsparumą kibernetinėms grėsmėms ir plėtoti tarptautinį bendradarbiavimą šioje srityje. NATO daugiau dėmesio skiria kolektyvinei gynybai ir kariniams kibernetinės gynybos pajėgumams, o Europos Sąjunga – teisės aktų kūrimui,

---

[95] Europos Parlamento rezoliucija „Europos Sąjungos kibernetinio saugumo strategija: atvira, saugi ir patikima kibernetinė erdvė“ (2013/2606(RSP)), EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52013IP0376.
[96] *Ibid.*
[97] Wahl, T. „Council Conclusions on Cybersecurity Strategy“, (*eucrim*, 2021)., žiūrėta 2026 m. kovo 19 d., https://eucrim.eu/news/council-conclusions-on-cybersecurity-strategy/.
[98] Europos Komisija. „ES kibernetinio saugumo strategija“, žiūrėta 2026 m. kovo 19 d., https://digital-strategy.ec.europa.eu/lt/policies/cybersecurity-strategy.
[99] Europos Vadovų Taryba. „Kibernetinis saugumas ES: strategija ir pagrindinės politikos priemonės“, žiūrėta 2026 m. kovo 19 d., https://www.consilium.europa.eu/lt/policies/cybersecurity/.

technologiniam atsparumui ir saugios skaitmeninės erdvės užtikrinimui. Tačiau bendras šių organizacijų tikslas yra užtikrinti saugią kibernetinę erdvę.

Apžvelgus kibernetinio saugumo strategijas, toliau šiame skyriuje bus nagrinėjami su kibernetiniu saugumu susiję teisės aktai. Jų analizė yra svarbi, kad galima būtų apibrėžti tiek tarptautinį, tiek ES teisinį reglamentavimą kibernetinio saugumo srityje.

Pirmoji pasaulyje tarptautinė sutartis Budapešto konvencija dėl elektroninių nusikaltimų yra sutartis, skirta kovai su nusikalstamomis veikomis elektroninėje erdvėje. Ši konvencija buvo priimta 2001 m. lapkričio mėn., o nuo to laiko ji tapo pagrindiniu tarptautiniu dokumentu, reglamentuojančiu kibernetinių nusikaltimų prevenciją, tyrimą ir baudžiamąjį persekiojimą. Tai jau du kartus papildyta sutartis: pirmasis papildomas protokolas, priimtas 2003 m., numatė, kad bet koks rasistinio ar ksenofobinio pobūdžio turinio perdavimas kompiuterinėmis sistemomis bus laikomas nusikalstama veika, o antrasis, priimtas 2022 m., sustiprino tarptautinį bendradarbiavimą bei elektroninių įrodymų apsikeitimą tarp valstybių. Šiuo metu „Budapešto konvenciją“ yra ratifikavusios 66 valstybės, dar 13 pakviestos prisijungti, o su Europos Taryba bendradarbiauja daugiau nei 140 šalių, siekiančių sustiprinti savo nacionalinius teisės aktus kovai su elektroniniais nusikaltimais.[100] Analizuojant Budapešto konvenciją dėl elektroninių nusikaltimų, tikslinga yra apibrėžti ir išnagrinėti pačią Budapešto konvenciją dėl elektroninių nusikaltimų, jos pirmąjį papildomą protokolą, kriminalizuojantį rasistinio bei ksenofobinio pobūdžio veikas, padarytas naudojantis kompiuterinėmis sistemomis, bei antrąjį protokolą kuris yra skirtas glaudesniam tarptautiniam bendradarbiavimui ir elektroninių įrodymų atskleidimui. Be to, bus išnagrinėtas Europos Sąjungos sprendimas (ES) 2023/436, kuriuo valstybės narės įgaliojamos ratifikuoti Konvencijos dėl elektroninių nusikaltimų antrąjį papildomą protokolą Europos Sąjungos interesais. Šių dokumentų analizė leis įvertinti tiek konvencijos esmę, tiek teisinį reglamentavimą tarptautinėje kibernetinio saugumo srityje.

Į Europos Tarybos konvencija dėl elektroninių nusikaltimų (Budapešto konvencija) (Europos Tarybos sutarčių serija Nr. 185) yra įtrauktos nuostatos, kuriomis:

„1) nusikalstamų veikų nacionalinės baudžiamosios materialinės teisės aspektai suderinami su susijusiomis nuostatomis elektroninių nusikaltimų srityje;

2) nustatyti nacionalinio baudžiamojo proceso įgaliojimai, būtini tokioms nusikalstamoms veikoms, taip pat kitoms, baudžiamosioms veikoms, kurios padarytos naudojantis kompiuterine sistema arba kurių įrodymų forma yra elektroninė, tirti ir baudžiamajam persekiojimui vykdyti;

---

[100] Lietuvos Respublikos užsienio reikalų ministerija. „Lietuva pasirašė Antrąjį papildomą Konvencijos dėl elektroninių nusikaltimų protokolą“, 2022 m. gegužės 12 d., žiūrėta 2026 m. kovo 19 d., https://urm.lt/naujienos/141/lietuva-pasirase-antraji-papildoma-konvencijos-del-elektroniniu-nusikaltimu-protokola:25366.

3) siekiama nustatyti greitą ir veiksmingą tarptautinio bendradarbiavimo tvarką;“ [101]

Pagrindinis šios konvencijos tikslas, yra nurodytas preambulėje – „vykdyti bendrą baudžiamąją politiką, skirtą visuomenės apsaugai nuo kibernetinių nusikaltimų, ypač priimant atitinkamus teisės aktus ir skatinant tarptautinį bendradarbiavimą“.[102]

Konvencijos II skyriuje yra įtvirtintos priemonės, kurių reikalaujama imtis nacionaliniu lygiu šalims. Todėl konvencijos 2 str.- 6 str., yra numatyta, kad kiekviena šalis turi priimti tokius teisėkūros ir kitus priemonių rinkinius, kurie yra būtini tam, kad pagal nacionalinę teisę tam tikros veikos būtų laikomos nusikalstamomis. Visų pirma nurodoma kriminalizuoti neteisėtą prieigą prie visos kompiuterinės sistemos ar jos dalies, taip pat neteisėtą neviešų kompiuterinių duomenų perdavimo perėmimą techninėmis priemonėmis. Konvencijoje taip pat numatoma baudžiamoji atsakomybė už neteisėtą kompiuterinių duomenų sugadinimą, ištrynimą, pakeitimą ar slopinimą, taip pat už kompiuterinių sistemų veikimo trikdymą įvedant, perduodant ar keičiant duomenis. Be to, valstybės įpareigojamos kriminalizuoti piktnaudžiavimą įrenginiais, įskaitant programų ar kitų priemonių kūrimą, platinimą ar laikymą, kai jos skirtos vykdyti nusikalstamas veikas prieš kompiuterines sistemas ar duomenis. Svarbu paminėti, kad konvencijos nuostatos yra taikomos ir LAT praktikoje. Pavyzdžiui LAT byloje 2K-138/2015 „Neteisėtas prisijungimas prie informacinės sistemos BK 198^1 straipsnyje numatytas atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų 2 straipsnį. Įgyvendinant šį teisės aktą neteisėtas prisijungimas BK 198^1 straipsnyje kriminalizuotas kaip savarankiška nusikalstama veika, t. y. be tiesioginio ryšio su kitomis jau sistemoje padaromomis veikomis“. [103] Tad tai pagrindžią, kad Lietuvoje yra perkeltos šios konvencijos nuostatos kurio yra aiškinamos praktikoje.

Toliau analizuojant Budapešto konvencija, tikslinga apžvelgti ir šio teisės akto papildomą protokolą „dėl rasistinio ir ksenofobinio pobūdžio veikos, padarytos naudojantis kompiuterinėmis sistemomis, kriminalizavimo“. [104] Šis protokolas išskiria kelis pagrindinius aspektus. Šiuo protokolu išplečiama konvencijos taikymo sritis, įtraukiant ksenofobinę ir rasistinę propagandą, skleidžiamą per kompiuterines sistemas, taip užtikrinant didesnę aukų apsaugą. Be to, protokolas sustiprina teisinę sistemą, nustatydamas gaires ksenofobijos ir rasistinės propagandos kibernetinėje erdvėje kriminalizavimui, ir gerina tarptautinio bendradarbiavimo

---

[101] „Konvencija dėl elektroninių nusikaltimų (ETS Nr. 185)“, žiūrėta 2026 m. kovo 19 d., https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.

[102] „Details of Treaty No. 185: Convention on Cybercrime“, žiūrėta 2026 m. kovo 19 d., https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

[103] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. sausio 6 d. nutartis baudžiamojoje byloje Nr. 2K-138/2015“, LITEKO, žiūrėta 2026 m. balandžio 22 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=78d6aacb-1ea9-4173-901f-86f4db6f2d33.

[104] „Papildomas protokolas prie Konvencijos dėl elektroninių nusikaltimų dėl rasistinio ir ksenofobinio pobūdžio veikų kriminalizavimo (ETS Nr. 189)“, žiūrėta 2026 m. kovo 19 d., https://rm.coe.int/168008160f.

mechanizmus, skirtus tirti rasistinius bei ksenofobinius nusikaltimus internete bei vykdyti baudžiamąjį persekiojimą už juos.[105] Šiuo protokolu kiekviena šalis įpareigojama priimti tokius teisės aktus ir kitas priemones, kurių gali prireikti pagal vidaus teisę nustatyti baudžiamąją atsakomybę už tokias sąmoningas ir neteisėtas veikas kaip rasistinės ir ksenofobinės medžiagos skleidimas naudojantis kompiuterinėmis sistemomis, rasistiniais ar ksenofobiniais ketinimais grindžiami grasinimai ir įžeidimai, genocido ar nusikaltimų žmoniškumui neigimas, šiurkštus menkinimas, pritarimas ar jų pateisinimas, taip pat už sąmoningą ir neteisėtą bendrininkavimą ar kurstymą padaryti kurią nors iš šių nusikalstamų veikų.[106] Apibendrinant, matoma, kad šis protokolas išplečia Konvencijos dėl elektroninių nusikaltimų taikymo sritį, įskaitant jos materialines, procesines ir tarptautinio bendradarbiavimo nuostatas, kad ji apimtų ir rasistinės ar ksenofobinės propagandos nusikaltimus. Taigi, be tokio elgesio materialinės teisės elementų suderinimo, protokolu siekiama pagerinti Šalių galimybes pasinaudoti Konvencijoje nustatytomis tarptautinio bendradarbiavimo priemonėmis ir būdais šioje srityje.[107]

Antrasis papildomas protokolas Konvecijoje yra įvardintas - „Dėl glaudesnio bendradarbiavimo ir elektroninių įrodymų atskleidimo“. Šiuo papildomu protokolu siekiama sustiprinti tarptautinį bendradarbiavimą kovojant su elektroniniais nusikaltimais. Šiuo protokolu yra sprendžiama ypatinga elektroninių įrodymų, laikomų užsienio jurisdikcijose paslaugų teikėjų, kurių teisėsaugos įgaliojimai apsiriboja nacionalinėmis sienomis, prieinamumo problema.[108] Šis papildomas protokolas nustato teisinį pagrindą domenų ir informacijos atskleidimui bei tiesioginiam bendradarbiavimui su paslaugų teikėjais siekiant gauti abonentų informaciją. Taip pat numatomos veiksmingos priemonės abonentų informacijai ir srauto duomenims gauti bei įtvirtinami tarpusavio teisinės pagalbos mechanizmai ir asmens duomenų apsaugos garantijos.[109] Vadovaujantis šiuo protokolų „šalis gali prašyti labai operatyviai teikiamos savitarpio pagalbos, kai ji mano, kad yra skubus atvejis“.[110] Apibendrinant antrąjį papildomą protokolą, darytina išvada, kad juo buvo sudarytos veiksmingesnes sąlygos gauti elektroninius įrodymus iš užsienio jurisdikcijų ir užtikrinti operatyvesnį bendradarbiavimą su paslaugų teikėjais.

---

[105] „Papildomas protokolas prie Konvencijos dėl elektroninių nusikaltimų dėl rasistinio ir ksenofobinio pobūdžio veikų kriminalizavimo“, *supra note,* 105.
[106] Ibid.
[107] „Details of Treaty No. 189“, žiūrėta 2026 m. kovo 19 d., https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189 .
[108] „Europos Parlamento rezoliucija „Konvencija dėl elektroninių nusikaltimų: antrasis papildomas protokolas dėl glaudesnio bendradarbiavimo ir elektroninių įrodymų atskleidimo“ (2023/C 214/17)“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52023AP0002.
[109] „Details of Treaty No. 224“, Council of Europe, žiūrėta 2026 m. kovo 19 d., https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.
[110] „Konvencija dėl elektroninių nusikaltimų: antrasis papildomas protokolas dėl glaudesnio bendradarbiavimo ir elektroninių įrodymų atskleidimo“, *op. cit*.

Apibendrinant galima teigti, kad Budapešto konvencija ir jos papildomi protokolai sudaro svarbų teisinį pagrindą kovai su kibernetiniais nusikaltimais. Konvencijoje nustatomos pagrindinės nusikalstamų veikų kategorijos, kurias valstybės turi perkelti į savo nacionalinę teisę. Papildomi protokolai papildo konvenciją naujomis nuostatomis, susijusiomis su rasistinio ir ksenofobinio pobūdžio nusikalstamomis veikomis bei elektroninių įrodymų gavimu tarp valstybių. Todėl galima teigti, kad Budapešto konvencija laikoma vienu iš svarbiausių tarptautinių dokumentų kibernetinio saugumo srityje, nes ji reglamentuoja kovą su nusikalstamomis veikomis elektroninėje erdvėje.

Budapešto konvencijos nuostatos taip pat atspindi „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.“ [111]Šios direktyvos vienas iš tikslų yra „suderinti valstybių narių baudžiamąją teisę atakų prieš informacines sistemas srityje, nustatant būtiniausias taisykles, susijusias su nusikalstamų veikų apibrėžtimi, ir atitinkamas sankcijas šioje srityje“.[112]

Direktyva 2013/40/ES dėl atakų prieš informacines sistemas reglamentuoja nusikalstamas veikas, susijusias su neteisėtais išpuoliais prieš informacines sistemas. Direktyva atitinka Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų nuostatas, kurios yra laikomos pagrindiniu tarptautinės teisės aktu kibernetinių nusikaltimų srityje. [113] Šia direktyva pristatomos naujos taisyklės, kuriomis suderinamas baudžiamosios atsakomybės ir sankcijų taikymas įvairioms nusikalstamoms veikoms, nukreiptoms prieš informacines sistemas. Šios direktyvos 3-6 straipsniuose yra numatyta, kad „valstybės narės turi imtis būtinų priemonių užtikrinti, kad už neteisėtą prieigą prie informacinių sistemų, neteisėtas įsikišimas į sistemą, neteisėtas įsikišimas į duomenis, neteisėtas duomenų perėmimas, jei tai padaryta tyčia ir neturint tam teisės, būtų baudžiama kaip už nusikalstamą veiką, bent tais atvejais, kurie nėra mažareikšmiai“. [114] Šioje direktyvoje taip pat išskiriami dar keli aspektai: kad už kurstymą, pasikėsinimą veiką ar pagalbą ir bendrininkavimą ją darant taip pat turi būti baudžiama, o už nusikalstamas veikas turi būti numatytos veiksmingos, proporcingos ir atgrasančios baudžiamosios sankcijos. Pagrindiniai nusikalstamų veikų tipai, kurie apima šią direktyvą, yra atakos prieš informacines sistemas - nuo atsisakymo aptarnauti atakų (angl. DDoS) iki duomenų

[111] „Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:32013L0040.
[112] *Ibid.*
[113] „Europos Parlamento ir Tarybos direktyva (ES) 2019/713 dėl kovos su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu“, žiūrėta 2026 m. kovo 19 d., https://data.consilium.europa.eu/doc/document/ST-12181-2017-INIT/lt/pdf.
[114] „Europos Parlamento ir Tarybos direktyva 2013/40/“, *op. cit*.

perėmimo ir botnetų atakų.[115] „Botnet – tai tinklas, sudarytas iš kompiuterių, vadinamų „robotais“, kurie užkrėsti kenkėjiškomis programomis ir nuotoliniu būdu kontroliuojami kibernetinių nusikaltėlių. Šie kompiuteriai gali būti naudojami įvairioms žalingoms užduotims atlikti. Pagrindinė botnetų grėsmė – DDoS atakos, kai užkrėsti įrenginiai siunčia daugybę užklausų į serverį“.[116] Siekiant užtikrinti geresnę kovą su elektroniniais nusikaltimais, direktyva taip pat ragina siekti geresnio tarptautinio bendradarbiavimo tarp teisminių ir teisėsaugos institucijų. Todėl yra numatyta, kad ES šalys turi:

1. turėti veikiantį nacionalinį informacinį punktą;
2. naudotis esamu informacinių punktų, veikiančių ištisą parą be poilsio dienų, tinklu;
3. reaguoti į skubius prašymus dėl pagalbos per 8 valandas, nurodant, ar į prašymą bus atsakyta;
4. rinkti statistinius duomenis apie elektroninius nusikaltimus.[117]

Apibendrinant galima teigti, kad Direktyva 2013/40/ES yra reikšminga kibernetinio saugumo teisinio reglamentavimo dalis ES, nes joje nustatoma pareiga valstybėms narėms užtikrinti, kad nacionalinėje teisėje būtų numatyta baudžiamoji atsakomybė už nusikalstamas veikas, nukreiptas prieš informacines sistemas ir elektroninius duomenis. Taip pat šia direktyva yra siekiama suvienodinti kibernetinių nusikaltimų teisinį reglamentavimą ES narėse, stiprinti valstybių bendradarbiavimą bei didinti informacinių sistemų bei elektroninių duomenų apsaugą kibernetinėje erdvėje.

2022 m. buvo paskelbta antroji Tinklų ir informacinių sistemų saugumo direktyva (TIS2 direktyva). Pirmoji direktyva, priimta 2016 m. TIS 1 buvo pirmasis išsamus ES teisės aktas, kuriuo siekiama didinti tinklų ir informacinių sistemų kibernetinį saugumą, kad būtų apsaugotos ES ekonomikai ir visuomenei gyvybiškai svarbios paslaugos. 2020 m. gruodžio mėn. Komisija pasiūlė peržiūrėti TIS 1 ir priimti TIS 2, kuris įsigaliojo 2023 m. sausio mėn. Valstybės narės TIS 2 direktyvą į nacionalinę teisę turėjo perkelti iki 2024 m. spalio 17 d. TIS 2 nuo 2024 m. spalio 18 d. panaikino TIS 1.[118] TIS 2 direktyva buvo priimta, siekiant reaguoti į naujas skaitmeninimo keliamas grėsmes ir bendrą kibernetinių atakų skaičiaus augimą, buvo nuspręsta pertvarkyti šią sistemą, siekiant sustiprinti saugumo reikalavimus, spręsti tiekimo grandinės saugumo klausimus,

---

[115] „Atakos prieš informacines sistemas“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/lt/legal-content/summary/attacks-against-information-systems.html.
[116] „Kibernetinių atakų žodynas: ką privalo žinoti kiekvienas“, ESET, žiūrėta 2026 m. kovo 19 d., https://eset.com/lt/apie/naujienos/straipsniai/pranesimai-spaudai/kibernetiniu-ataku-zodynas-ka-privalo-zinoti-kiekvienas/.
[117] „Atakos prieš informacines sistemas“, *op.cit*.
[118] „TIS 2 direktyva: tinklų ir informacinių sistemų apsauga“, Europos Komisija, žiūrėta 2026 m. kovo 19 d., https://digital-strategy.ec.europa.eu/lt/policies/nis2-directive.

supaprastinti ataskaitų teikimą ir nustatyti griežtesnes priežiūros bei vykdymo užtikrinimo priemones.[119] Pagrindiniai skirtumai – NIS1 ir NIS2 kibernetinio saugumo srityje:

1. Taikymo srities išplėtimas. Perėjimas nuo NIS1 prie NIS2 gerokai praplečia subjektų, kuriems taikoma direktyva, aprėptį. Nors NIS1 daugiausia buvo skirtas esminių paslaugų operatoriams tokiuose sektoriuose kaip energetika, transportas, sveikatos apsauga ir skaitmeninė infrastruktūra, NIS2 šią sritį išplečia, įtraukdama pašto ir kurjerių paslaugas, maisto gamybą, atliekų tvarkymą, vandens tiekimą ir su kosmosu susijusias paslaugas. Ši taikymo sritis išsamiai aprašyta NIS2 direktyvos I ir II prieduose. Dabar direktyvoje organizacijos skirstomos į dvi kategorijas: Esminiai subjektai: tokie sektoriai kaip energetika, transportas, sveikatos apsauga ir skaitmeninė infrastruktūra. Svarbūs subjektai: tokie kaip maisto gamyba, perdirbimas, chemijos pramonė ir pašto paslaugos. NIS2 taip pat sumažina dydžio ribą, o tai reiškia, kad daugelis mažų ir vidutinių įmonių dabar patenka į taikymo sritį, jei jos atlieka svarbų vaidmenį šiuose sektoriuose.[120]

2. NIS2 nustato daug griežtesnius saugumo ir valdymo įsipareigojimus. NIS2 direktyva nustato griežtesnius reikalavimus organizacijoms, įpareigodama jas taikyti pažangesnes kibernetinio saugumo rizikos valdymo priemones. Šios priemonės apima privalomą rizikos vertinimą, reguliarius saugumo testus ir saugumo auditus, tiekimo grandinės saugumo užtikrinimą bei trečiųjų šalių rizikos valdymą, taip pat šifravimo ir daugiasluoksnių saugumo priemonių taikymą.[121]

3. Pranešimų apie incidentus teikimas. Incidentų pranešimo įsipareigojimai tapo išsamesni ir turi tam tikrą laiką. Pagal TIS2 23 straipsnį organizacijos dabar privalo: pranešti apie svarbius incidentus nacionalinei CSIRT per 24 valandas nuo sužinojimo apie juos. Pateikti tarpinę ataskaitą po 72 valandų. Pateikti galutinę ataskaitą per vieną mėnesį, įskaitant pagrindinę priežastį, poveikį ir mažinimo veiksmus. Šios ataskaitos turi atitikti standartizuotus protokolus ir būti teikiamos per centrinę ES platformą, skirtą supaprastinti ataskaitų teikimą ir pagerinti koordinavimą tarp valstybių narių.[122]

4. Suderinimas visose ES valstybėse narėse NIS1 suteikė diskrecija nustatyti, kurioms organizacijoms taikomos taisyklės. NIS2 nustato suderintus kriterijus visose ES šalyse. Tai užtikrina nuoseklų kibernetinio saugumo lygį ir padeda išvengti reguliavimo susiskaidymo. Direktyva

---

[119] Niels Vandezande, „Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor“, Computer Law & Security Review 52 (2024), https://doi.org/10.1016/j.clsr.2023.105890.

[120] „5 Key Changes from NIS1 to NIS2“, heyData, žiūrėta 2026 m. kovo 19 d., https://heydata.eu/en/magazine/5-key-changes-from-nis1-to-nis2/.

[121] „NIS2 vs. NIS1: Key Differences and New Challenges“, NIS2 Cyber Security, žiūrėta 2026 m. kovo 19 d., https://nis2cybersecurity.org/nis2-vs-nis1-key-differences-and-new-challenges/://nis2cybersecurity.org/nis2-vs-nis1-key-differences-and-new-challenges/.

[122] „Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2 direktyva)“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32022L2555.

taip pat stiprina tarpvalstybinį bendradarbiavimą, įskaitant: informacijos mainų mechanizmus tarp kompetentingų institucijų. Bendraus reagavimo į krizes pratybas.[123]

5. Sankcijos. Vienas iš NIS2 atnaujinimų yra jos vykdymo užtikrinimo modelis. Esminiams priskirtiems subjektams gresia 10 000 000 Eur arba 2% nuo praėjusių finansinių metų metinės apyvartos dydžio bauda, priklausomai nuo to kuri suma didesnė. Svarbiems subjektams baudos šiek tiek mažesnės – 7 000 000 Eur arba 1,4% nuo praėjusių finansinių metų metinės apyvartos, priklausomai nuo to kuri suma didesnė.[124]

TIS2 direktyvoje taip pat yra įtvirtinta, kad saugumo rizikų valdymas, yra kompleksinis ir nuolatinis procesas, kuris leidžia organizacijoms identifikuoti, vertinti ir efektyviai mažinti saugumo rizikas. Šis procesas apima rizikų identifikavimą, jų vertinimą, rizikų mažinimo ir prevencijos priemonių taikymą, incidentų aptikimą ir reagavimą į juos, sistemų atkūrimą po incidentų bei nuolatinį saugumo priemonių vertinimą ir tobulinimą. Toks ciklinis procesas leidžia organizacijoms efektyviau prisitaikyti prie nuolat kintančių kibernetinio saugumo grėsmių ir užtikrinti tinkamą tinklų bei informacinių sistemų apsaugą.[125]

Direktyva buvo sukurtas reagavimo į kompiuterių saugumo incidentus tarnybų tinklas (CSIRT). CSIRT tinklas, įsteigtas pagal NIS direktyvą ir vėliau sustiprintas NIS2 direktyva, siekia stiprinti pasitikėjimą ir skatinti operacinį bendradarbiavimą tarp ES narių. Šio tinklo veikla apima informacijos mainus, incidentų valdymo koordinavimą bei pagalbos teikimą valstybėms narėms tarpvalstybinių kibernetinių incidentų atvejais. Tinklo veikla taip pat apima koordinuotą pažeidžiamumų atskleidimą tais atvejais, kai jie gali turėti reikšmingą poveikį daugiau nei vienai valstybei narei. CSIRT tinklą sudaro valstybių narių paskirtos kompiuterinių saugumo incidentų tyrimo komandos (CSIRT) ir CERT-EU (ES institucijų kompiuterinių incidentų reagavimo komanda).[126] Siekiant valdyti didelio masto kibernetinio saugumo incidentus ar krizes, direktyva buvo sukurtas Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe). Šis tinklas remia koordinuotą valdymą ir užtikrina reguliarų valstybių narių ir ES institucijų keitimąsi informacija didelio masto incidentų ir krizių atveju. Šis tinklas pradėjo veikti 2020 m., o oficialiai įtvirtintas 2023 m. sausio 16 d., kai įsigaliojo TIS2 direktyvos 16 straipsnis.[127]

Išanalizavus atnaujinta TIS2 direktyva nustatyta, kad ją yra siekiama sustiprinti ES gebėjimą atsispirti ir reaguoti į kibernetines grėsmes, taip pat užtikrinti, kad visos valstybės narės imtųsi atitinkamų saugumo priemonių, užkirstų kelią incidentams ir sumažintų pasekmes, jei jie

---

[123] „5 Key Changes from NIS1 to NIS2“, *op.cit.*
[124] „TIS2 direktyva“, IT skyrius, žiūrėta 2026 m. kovo 19 d., https://itskyrius.lt/tis2-direktyva/.
[125] Šileikienė ir Usovaitė, *supra note*, 5:80.
[126] „CSIRTs Network“, ENISA, žiūrėta 2026 m. kovo 19 d., https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network.
[127] „TIS 2 direktyva: tinklų ir informacinių sistemų apsauga“, *supra note*, 118.

įvyksta. Tai svarbu ne tik dėl saugumo, bet ir dėl ekonomikos stabilumo bei piliečių pasitikėjimo skaitmeninėmis paslaugomis, kurios yra vis labiau integruotos į kasdienį gyvenimą. TIS2 direktyva perteikia ES požiūrį, kad tik bendromis pastangomis galima pasiekti efektyvų ir ilgalaikį kibernetinį saugumą. Taip pat TIS2 direktyva nustato bendrą teisinę sistemą, kuria siekiama užtikrinti kibernetinį saugumą 18-oje ypatingos svarbos sektorių visoje ES. Direktyva įpareigoja valstybes nares apibrėžti nacionalines kibernetinio saugumo strategijas ir bendradarbiauti su ES tarpvalstybinio reagavimo ir vykdymo užtikrinimo srityje.

Viena pagrindinių duomenų subjekto teisių, įtvirtinta dar 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvoje 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, yra duomenų subjekto teisė susipažinti su savo duomenimis. Tačiau šią direktyvą pakeitė bendrasis duomenų apsaugos reglamentas (BDAR) – tai Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. priimtas reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos, tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Šis dokumentas yra pagrindinis ES teisės aktas, reglamentuojantis asmens duomenų apsaugą ir privatumo teisę skaitmeninėje erdvėje. [128]Šis teisės aktas remiasi Chartijos 8 straipsnio 1 dalimi ir SESV 16 straipsnio 1 dalimi, kurioje nustatyta, kad „kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą, o tuo siekiama suderinti fizinių asmenų pagrindinių teisių ir laisvių apsaugą vykdant duomenų tvarkymo veiklą.“[129] Šio reglamento tikslas užtikrinti asmenų apsauga, kai jų duomenys yra tvarkomi privataus sektoriaus ir viešojo sektoriaus subjektų. Šiuo reglamentu asmenims sudaroma galimybė kontroliuoti savo asmens duomenis. Atnaujinamos ir suvienodinamos taisyklės, leidžiančios įmonėms sumažinti biurokratizmą ir užsitikrinti didesnį vartotojų pasitikėjimą. Taip pat šiuo reglamentu sukuriama visiškai nepriklausomų priežiūros institucijų, atsakingų už atitikties stebėseną ir vykdymo užtikrinimą, sistema. [130]

Pagrindiniai šio reglamento aspektai yra susiję su fizinių asmenų teisėmis ir taisyklėmis įmonėms.

Fizinių asmenų teisės:

- Teisė susipažinti – įstatyme yra numatyta, kad asmenys turi teisę prašyti prieigos prie savo asmens duomenų ir informacijos apie juos saugančią organizaciją. [131]

---

[128] „Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis (Bendrasis duomenų apsaugos reglamentas)“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016R0679.

[129] *Ibid.*

[130] „Bendrasis duomenų apsaugos reglamentas (BDAR)“, EUR-Lex santrauka, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/lt/legal-content/summary/general-data-protection-regulation-gdpr.html.

[131] Ina Nikolova, „What Are the Key Differences Between GDPR and NIS2?“, Dynamic Identity, PATECCO, žiūrėta 2026 m. kovo 19 d., https://patecco.com/what-are-the-key-differences-between-gdpr-and-nis2/.

- Teisė ištaisyti duomenis – tai reiškia, kad „duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištaisytų netikslius su juo susijusius asmens duomenis. Atsižvelgiant į tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys, be kita ko, pateikdamas papildomą pareiškimą“.[132]
- Teisė ištrinti duomenis– tai yra susiję su principu „teisė būti užmirštam internete“. 2014 m. gegužės 13 d. Europos Sąjungos Teisingumo Teismas nusprendė, kad „piliečiai turi teisę prašyti, jog „Google“ pašalintų jų duomenis iš paieškos rezultatų. Ši byla siekė išsiaiškinti, ar privatūs asmenys gali „pasitraukti“ iš paieškos sistemos rezultatų tinklo. Teismas taip pat nusprendė, kad „interneto paieškos sistemos operatorius yra atsakingas už asmens duomenų tvarkymą, kurį jis atlieka, kai tokie duomenys pateikiami trečiųjų šalių paskelbtuose interneto puslapiuose“.[133]Šis sprendimas, tapo precedentu BDAR įtvirtintai teisės į ištrynimą nuostatai.
- Teisė apriboti duomenų tvarkymą- Ši teisė yra alternatyva teisei reikalauti ištrinti asmens duomenis. [134]Įstatyme yra numatyta, kad duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas apribotų duomenų tvarkymą kai taikomas vienas iš šių atvejų[135] Tai nėra absoliuti teisė, todėl ji taikoma tik esant tam tikroms aplinkybėms.Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas apribotų asmens duomenų tvarkymą, kai egzistuoja bent viena iš įstatyme numatytu aplinkybių [136](ginčija asmens duomenų tikslumą, duomenų tvarkymas yra neteisėtas ir kt.).
- Duomenų perkėlimas – „Duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui, o duomenų valdytojas, kuriam asmens duomenys buvo pateikti, turi nesudaryti tam kliūčių„[137] Be to šios duomenų perkėlimo nuostatos didina prieigą prie duomenų ir jų dalijimąsi tarp skaitmeninių paslaugų bei platformų. Tai gali suteikti naudotojams galimybę aktyviau dalyvauti pakartotinai naudojant savo duomenis ir gali padėti skatinti

---

[132] „Europos Parlamento ir Tarybos reglamentas (ES) 2016/679“, *supra note*., 128.
[133] „Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González“, Europos Sąjungos Teisingumo Teismas (Didžioji kolegija), 2014 m. gegužės 13 d., byla C-131/12, žiūrėta 2025 m. sausio 16 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131.
[134] „Asmens duomenų apsaugos gairės duomenų subjektams“, Valstybinė duomenų apsaugos inspekcija, 2019, žiūrėta 2026 m. kovo 19 d., https://vdai.lrv.lt/uploads/vdai/documents/files/01%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20DUOMENU%20SUBJEKTAMS%202019-10-16%20(perziureta%202023-06-05).pdf.
[135] „Europos Parlamento ir Tarybos reglamentas (ES) 2016/679“, *supra note*, 128.
[136] „Asmens duomenų apsaugos gairės duomenų subjektams“, *op. cit.*
[137] „Europos Parlamento ir Tarybos reglamentas (ES) 2016/679“, *supra note*, 128.

konkurenciją bei inovacijas, skatinant sąveikumą ir mažinant paslaugų keitimo kaštus bei vartotojų „užrakinimo“ (angl. lock-in) efektą. Tačiau duomenų perkeliamumo veiksmingumas stiprinant konkurenciją priklauso nuo duomenų perdavimo sąlygų ir nuo to, kiek konkurentai gali veiksmingai pasinaudoti šiais duomenimis.[138]

- Teisė nesutikti – BDAR 21 straipsnyje yra įvirtinta ši teisė. Tai reiškia, kad asmenys turi teisę prieštarauti visų ar tik tam tikrų asmens duomenų tvarkymui, arba tvarkymui tam tikru tikslu. Svarbu pažymėti, kad teisė nesutikti su duomenų tvarkymu tiesioginės rinkodaros tikslu yra absoliuti. Tad jeigu nesutinkama, kad asmens duomenys būtų tvarkomi reklamos tikslais, įmonė privalo nemokamai patenkinti prašymą ir nutraukti asmens duomenų tvarkymą šiuo tikslu.[139]
- Pranešimai apie duomenų saugumo pažeidimus – pagal BDAR 33 straipsnio 1 dalį apie visus duomenų saugumo pažeidimus turėtų būti pranešta atitinkamai duomenų priežiūros institucijai, išskyrus tuos, kurie neturėtų kelti jokio pavojaus asmenims.
- Automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą- „Sprendimų priėmimas tik automatizuotu būdu reiškia, kad sprendimai bus priimami technologinėmis priemonėmis, be jokio žmogaus įsikišimo. Profiliavimas atliekamas tada, kai vertinami asmens asmeniniai aspektai, kad būtų padarytos prognozės, net jeigu nebus priimtas joks sprendimas. Pavyzdžiui, jeigu įmonė vertina duomenų subjekto asmens savybes (kaip antai, amžių, lytį ar ūgį) arba skirsto į tam tikras kategorijas, tai reiškia, kad taikomas profiliavimas.[140]“ BDAR 22 straipsnis numato, kad duomenų subjektas turi teisę, kad jam nebūtų taikomas sprendimas, pagrįstas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, jeigu toks sprendimas sukelia teisines pasekmes arba daro jam reikšmingą poveikį. Tačiau ši nuostata netaikoma tais atvejais, kai sprendimas yra būtinas siekiant sudaryti ar vykdyti sutartį tarp duomenų subjekto ir duomenų valdytojo, kai jis leidžiamas Europos Sąjungos ar valstybės narės teisėje ir nustatomos tinkamos duomenų subjekto teisių apsaugos priemonės, arba kai sprendimas priimamas gavus aiškų duomenų subjekto sutikimą.[141]

---

[138] Christian Reimsbach-Kounatze ir Andras Molnar, „The impact of data portability on user empowerment, innovation, and competition“, Going Digital Toolkit Note, Nr. 25 (OECD, 2024): 5, žiūrėta 2026 m. kovo 12 d., https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-impact-of-data-portability-on-user-empowerment-innovation-and-competition_ee329380/319f420f-en.pdf.

[139] „Asmens duomenų apsaugos gairės duomenų subjektams“, *supra note,* 134.

[140] Lina Novikovienė ir Oksana Pedaniuk, „Naujosios duomenų subjekto teisės bendrajame duomenų apsaugos reglamente“, Jurisprudencija 27, 2 (2020): 325, žiūrėta 2026 m. kovo 19 d., https://cris.mruni.eu/server/api/core/bitstreams/aaf0e76c-2ef7-4f03-8d69-d2e6d3519db/content.

[141] „Europos Parlamento ir Tarybos reglamentas (ES) 2016/679“, *supra note*, 128.

BDAR taip pat yra sukuriamos vienodos sąlygos visoms ES vidaus rinkoje veikiančioms įmonėms, taikomas technologijų atžvilgiu neutralus požiūris ir įvairiais būdais, įskaitant toliau nurodytus, skatinamos inovacijos. Pagrindinės įmonių taisyklės:

- Vienas ES taisyklių rinkinys - taikomas bendras ES duomenų apsaugos teisės aktas padidinantis teisinį tikrumą ir sumažinantis administracinę naštą.[142]
- Duomenų apsaugos pareigūnas- už duomenų apsaugą atsakingą asmenį turi paskirti valdžios institucijos ir įmonės. Duomenų apsaugos pareigūnas yra duomenų apsaugos ekspertas, kuris konsultuoja duomenų apsaugos atitikties organizacijoje klausimais. Pareigūnas turi būti tinkamai ir laiku įtrauktas į visus klausimus, susijusius su asmens duomenų apsauga.[143]
- Vieno langelio principas - BDAR preambulėje yra numatyta, kad „sutikimas turėtų būti duodamas aiškiu aktu patvirtinant, kad yra suteiktas laisva valia. Tai galėtų būti atliekama pažymint langelį interneto svetainėje[144]“. Šiuo principu siekiama užtikrinti, kad organizacijos ir asmenys galėtų spręsti su asmens duomenų tvarkymu susijusius tarpvalstybinius klausimus su priežiūros institucija, įsikūrusia toje pačioje valstybėje narėje, kurioje yra jų pagrindinė buveinė (dažniausiai jų ES būstinė), taip pat, kad tokie klausimai galėtų būti nuosekliai sprendžiami visoje ES. O tai reiškia, kad priežiūros institucijos turi bendradarbiauti, kad suteiktų viena kitai susijusią informaciją ir savitarpio pagalbą, kai to prašoma.
- Privatumo apsaugos būdai - siekiant apriboti duomenų tvarkymo atgrasumą, skatinama naudoti pseudonimus (kai atpažinimo sritys duomenų įraše keičiamos vienu ar keliais dirbtiniais identifikatoriais) ir šifravimą (kai duomenys koduojami taip, kad neturinčiam leidimo susipažinti asmeniui jie būtų nesuprantami).[145]
- Duomenų apsaugos poveikio vertinimai - tai yra procesas, skirtas „duomenų tvarkymo operacijai aprašyti ir tokios duomenų tvarkymo operacijos reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo, apimantis pavojaus įvertinimą ir jo pašalinimo priemonių nustatymą.“[146]

---

[142] „Bendrasis duomenų apsaugos reglamentas (BDAR)“ santrauka, *supra note*, 130.
[143] „Data Protection Officer“, European Data Protection Board, žiūrėta 2026 m. kovo 19 d., https://edpb.europa.eu/sme-data-protection-guide/data-protection-officer_en.
[144] „Europos Parlamento ir Tarybos reglamentas (ES) 2016/679“, *supra note*, 128.
[145] „Bendrasis duomenų apsaugos reglamentas (BDAR) santrauka“, *supra note*, 130.
[146] „Įsakymas dėl poveikio duomenų apsaugai vertinimo, duomenų valdytojo ir duomenų tvarkytojo duomenų tvarkymo veiklos įrašų rengimo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašų patvirtinimo“, žiūrėta 2026 m. sausio 12 d., https://ird.lrv.lt/public/canonical/1751287415/474/D%C4%97l%20Apra%C5%A1%C5%B3%20patvirtinimo.Elektroninio+dokumento+nuora%C5%A1as%20(1).pdf.

- Baudos- Reglamento nuostatas, gali būti skiriamos administracinės baudos, kurios kiekvienu konkrečiu atveju turi būti veiksmingos, proporcingos ir atgrasomos. Priklausomai nuo Reglamento pažeidimo pobūdžio bauda gali siekti nuo 2 iki 4 proc. ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, arba nuo 10 000 000 iki 20 000 000 EUR.[147]

Apibendrinant, galima daryti išvadą, kad BDAR, atnaujinant ankstesnę direktyvą 95/46/EB, užtikrina ES piliečių teisę apsaugoti savo asmens duomenis. Tačiau tuo pačiu įpareigoja organizacijas būti atsakingomis už asmens duomenų saugumą. BDAR laikomas vienu svarbiausių teisinio reglamentavimo dokumentų, kuris yra skirtas asmens duomenų apsaugai ir saugumui kibernetinėje erdvėje užtikrinti. Apžvelgus tiek TIS2 direktyvą, tiek BDAR, galima daryti išvadą, kad šie dokumentai turi tam tikrų panašumų, nes tiek BDAR, tiek TIS2 yra taikomi tiek viešajam, tiek privačiajam sektoriui. Taip pat TIS2 yra dar viena Europos Sąjungos direktyva, skirta informacijos ir kibernetinio saugumo stiprinimui. Tačiau BDAR daugiausia dėmesio skiria asmenų privatumo teisėms ir asmens duomenų apsaugai, o TIS2 direktyva – esminių paslaugų ir skaitmeninės infrastruktūros saugumui.[148] Abu šie dokumentai yra svarbūs veiksmingai duomenų privatumo apsaugai ir kibernetinio saugumo užtikrinimui.

„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)“.[149] Šiuo reglamentu yra siekiama užtikrinti tinkamą vidaus rinkos veikimą ir kartu aukštą kibernetinio saugumo, kibernetinio atsparumo ir pasitikėjimo lygį ES.

Šiame reglamente yra nustatomi:

1. „Europos Sąjungos kibernetinio saugumo agentūros (toliau- ENISA) tikslai, užduotys ir organizaciniai aspektai.

2. Europos kibernetinio saugumo sertifikavimo schemų nustatymo sistema, kuria siekiama užtikrinti tinkamą informacinių ir ryšių technologijų (toliau- IRT) produktų, paslaugų, procesų ir kibernetinio saugumo lygį“.[150]

ENISA tikslas yra- stiprinti pasitikėjimą sujungtos ekonomikos sąlygomis, didinti ES infrastruktūros ir paslaugų atsparumą ir pasitikėjimą jomis ir išlaikyti visuomenės ir piliečių skaitmeninį saugumą. [151] ES kibernetinio saugumo aktu agentūrai suteikiami nuolatiniai

---

[147] „Svarbiausi reformos pakeitimai“, Valstybinė duomenų apsaugos inspekcija, žiūrėta 2026 m. kovo 19 d., https://vdai.lrv.lt/lt/naudinga-informacija/2018-m-duomenu-apsaugos-reforma-1/svarbiausi-reformos-pakeitimai/.
[148] Nikolova: 132.
[149] „Reglamentas (ES) 2019/881“, *supra note*, 30.
[150] *Ibid*.
[151] *Ibid*.

įgaliojimai, daugiau išteklių ir naujų užduočių. ENISA, parengdama konkrečių sertifikavimo schemų techninį pagrindą, atlieka svarbų vaidmenį kuriant ir prižiūrint Europos kibernetinio saugumo sertifikavimo sistemą. Ji yra atsakinga už visuomenės informavimą apie sertifikavimo schemas ir išduotus sertifikatus tam skirtoje interneto svetainėje.[152] Viena iš pagrindinių ENISA veiklos krypčių yra kibernetinio saugumo politika. Oficialiame organizacijos tinklapyje pabrėžiama, kad kibernetinis saugumas yra vienas iš pagrindinių skaitmeninės transformacijos elementų ir būtina sąlyga svarbiausiuose ES ekonomikos ir visuomenės sektoriuose, tad ENISA teikiamos rekomendacijos, nuomonės ir analizės siekia užtikrinti nuoseklų, įrodymais pagrįstą ir į ateitį orientuotą šios politikos priemonių įgyvendinimą, daugiausia dėmesio skiriant kibernetinio atsparumo stiprinimui kritiniuose sektoriuose.[153]

Europos kibernetinio saugumo sertifikavimo sistema- IRT produktų kibernetinio saugumo sertifikavimo sistema suteikia galimybę naudoti pritaikomas, rizika pagrįstas sertifikavimo schemas, kurios didina pasitikėjimą skaitmeniniais produktais ir paslaugomis. Sertifikavimas užtikrina, kad IRT produktai atitiktų reikalavimus ir kad sertifikatai būtų pripažįstami visoje ES, taip palengvinant prekybą ir didinant saugumo informuotumą.[154] Pirmoji schema, yra pagrįsta gerai žinomu tarptautiniu standartu „Bendrieji kriterijai“, kuris jau beveik 30 metų naudojamas sertifikatams išduoti Europoje. [155]Šis standartas yra vienas plačiausiai pripažintų ir išsamiausių informacinių technologijų saugumo standartų pasaulyje, kuris gali būti naudojamas sertifikuoti bet kurią IT sistemą ar įrenginį, turintį saugumo funkcijas. [156] Schema taikoma visoje ES savanoriškai ir joje daugiausia dėmesio yra skiriama IRT produktų kibernetinio saugumo sertifikavimui per jų gyvavimo ciklą, įskaitant: biometrines sistemas, platformas, maršrutizatoriai, jungikliai, specializuota programinė įranga ir kt. Tačiau 2026-01-20 Europos Komisija pateikė naują kibernetinio saugumo priemonių paketą, kuriuo siekiama dar labiau sustiprinti Europos Sąjungos kibernetinį atsparumą ir gebėjimus. Juo siekiama didinti kibernetinio saugumo pajėgumus ir atsparumą bei išvengti susiskaidymo ES skaitmeninėje bendrojoje rinkoje. Šiuo pasiūlymu yra siekiama užtikrinti, kad produktai, pasiekiantys ES piliečius, būtų kuriami laikantis „kibernetinio saugumo pagal projektavimą“ (angl. cyber-secure by design) principo, taikant paprastesnę sertifikavimo sistemą. [157]Šis principas numato, kad kibernetinis saugumas turi būti integruojamas į skaitmeninių sistemų kūrimą nuo pat pradžių ir užtikrinamas viso jų gyvavimo

[152] „ES kibernetinio saugumo aktas, santrauka“, Europos Komisija, žiūrėta 2026 m. kovo 19 d., https://digital-strategy.ec.europa.eu/lt/policies/cybersecurity-act.
[153] „Reglamentas (ES) 2019/881“, *supra note,* 30.
[154] „European cybersecurity certification framework“, European Commission, žiūrėta 2026 m. kovo 19 d., https://digital-strategy.ec.europa.eu/en/node/15665/printable/pdf.
[155] *Ibid.*
[156] „Common Criteria“, Brightsight (SGS), žiūrėta 2026 m. kovo 19 d., https://www.brightsight.com/common-criteria
[157] „European cybersecurity certification framework“, *op.cit*.

ciklo metu. Tai apima rizikos valdymą, saugių technologijų naudojimą, nuolatinį saugumo stebėjimą, incidentų aptikimą bei daugiasluoksnės apsaugos taikymą. Apibendrinant matoma, kad Reglamentu yra įtvirtinamas ENISA vaidmuo bei nustatoma bendra informacinių ir ryšių technologijų produktų, paslaugų ir procesų kibernetinio saugumo sertifikavimo sistema. Tuo siekiama didinti Europos Sąjungos informacinių sistemų bei infrastruktūros atsparumą kibernetinėms grėsmėms, skatinti saugių informacinių ir ryšių technologijų produktų kūrimą ir naudojimą.

2024 m. spalio 23 d. buvo priimtas „Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas)“ [158] Kibernetinio atsparumo aktas yra horizontalioji (ES) reguliavimo sistema, kuri yra taikoma aparatinės ir programinės įrangos produktams. Tokie produktai apima tiek galutinius produktus, tiek atskirai rinkai pateikiamas sudedamąsias dalis. Juo siekiama nustatyti saugios aparatinės ir programinės įrangos kūrimo Sąjungoje sąlygas, kad būtų sustiprintas ES požiūris į kibernetinį saugumą ir pagerintas vidaus rinkos veikimas. [159] Aktas numato specialų požiūrį į nemokamą ir atvirojo kodo programinę įrangą, pripažindamas jos svarbą kibernetiniam saugumui. Reglamentas taikomas tik tai atvirojo kodo programinei įrangai, kuri yra tiekiama rinkai komerciniais tikslais. Programinė įranga, kuri kuriama ir platinama nekomerciniais tikslais, taip pat kūrėjai, kurie tik prisideda prie atvirojo kodo projektų, į teisės akto taikymo sritį nepatenka. Be to, reglamente numatyta atvirojo kodo programinės įrangos tvarkytojų kategorija, kuriems taikomas specialus, švelnesnis reguliavimas. [160] Svarbu pabrėžti, kad kai gamintojas rinkai teikia produktą su skaitmeniniais elementais, kuris yra nemokama atvirojo kodo programinė įranga, jam taikomos gamintojų pareigos. Kibernetinio atsparumo aktu pripažįstama, kad už kibernetinį saugumą yra atsakingi visi gamintojai visoje tiekimo grandinėje. Pagrindinė gamintojų pareiga yra, kad jie atsakingi ne tik už galutinius produktus, tokius kaip išmanieji telefonai ar programėlės, bet ir jų komponentus, pavyzdžiui, lustus ar operacines sistemas. Todėl įmonės, parduodančios techninės ar programinės įrangos produktus, privalo užtikrinti, kad šie produktai būtų saugūs jau projektavimo stadijoje. Tai reiškia, kad turi būti taikomas saugumas pagal numatytuosius nustatymus, užtikrinama tinkama

[158] „Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų produktams su skaitmeniniais elementais ir iš dalies keičiantis reglamentus (ES) Nr. 168/2013 ir (ES) 2019/1020 bei direktyvą (ES) 2020/1828 (Kibernetinio atsparumo aktas)“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847.

[159] „Kibernetinio atsparumo aktas. Teisės akto teksto santrauka“, Europos Komisija, žiūrėta 2026 m. kovo 19 d., https://digital-strategy.ec.europa.eu/lt/policies/cra-summary.

[160] „Kibernetinio atsparumo aktas. Atvirasis šaltinis“, Europos Komisija, žiūrėta 2026 m. kovo 19 d., https://digital-strategy.ec.europa.eu/lt/policies/cra-open-source.

prieigos kontrolė, naudojamos kriptografinės apsaugos priemonės ir įdiegiami automatiniai saugumo atnaujinimai. Be to, gamintojai privalo užtikrinti produktų priežiūrą ir palaikymą visą laikotarpį, kol numatoma, kad produktas bus naudojamas.[161]

Apibendrinant, matoma, kad Kibernetinio atsparumo aktu yra siekiama užtikrinti, jog visi skaitmeniniai produktai būtų saugūs nuo kibernetinių grėsmių. Šis reglamentas užtikrina suderintas taisykles produktams ar programinei įrangai su skaitmeniniais elementais visoje ES. Šios taisyklės reikalauja, kad įrenginiai ir programinė įranga būtų suprojektuoti, atnaujinti ir prižiūrimi siekiant apsaugoti naudotojus.

2024 m. gruodžio 19 d. priimtas Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas).[162] Šiuo reglamentu nustatomos priemonės, kuriomis ES stiprinami pajėgumai aptikti kibernetines grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti, sukuriant:

1. Visos ES kibernetinio saugumo centrų tinklą (toliau – kibernetinio saugumo įspėjimų sistema).

2. Reagavimo į kibernetinio saugumo krizes mechanizmą.

3. Europos kibernetinio saugumo incidentų peržiūros mechanizmą.[163]

Kibernetinio saugumo įspėjimų sistema – yra pagrindinė Kibernetinio solidarumo akto dalis. Juo siekiama kovoti su didėjančia kibernetinių grėsmių aplinka. Ši sistema stiprina ES gynybą nuo kibernetinių išpuolių, todėl atsakas tampa greitesnis ir atsparesnis. Sistemos tikslas – pagerinti kibernetinių grėsmių nustatymą ir dalijimąsi jomis.[164] Taip pat svarbu paminėti, kad Įspėjimo sistemoje yra įvairių tipų įspėjimai apie įvairias grėsmes. Šie įspėjimai svyruoja nuo paprastų įspėjimų iki skubių pranešimų apie dideles grėsmes. Pavyzdžiui, įspėjimai gali įspėti apie pavojus sveikatos priežiūros, transporto ir energetikos srityse.[165]Sistema naudoja dirbtinį intelektą (AI) ir duomenų analizę, kad greitai išsiųstų įspėjimus. Tai padeda kiekvienam greitai gauti reikiamą informaciją. Šią sistemą sudaro visa ES infrastruktūra, kurią sudaro nacionaliniai ir

---

[161] „Kibernetinio atsparumo aktas. Gamintojai“, Europos Komisija, žiūrėta 2026 m. kovo 19 d., https://digital-strategy.ec.europa.eu/lt/policies/cra-manufacturers.

[162] „Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas)“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32025R0038.

[163] *Ibid.,* 1 straipsnis.

[164] „Cyber Solidarity Act Launches European Cybersecurity Alert System“, Secure Privacy, žiūrėta 2026 m. kovo 19 d., https://cybersecurity-act.eu/blog/cyber-solidarity-act-launches-european-cybersecurity-alert-system/.

[165] *Ibid.*

tarpvalstybiniai kibernetiniai centrai, atsakingi už paramą aptinkant kibernetines grėsmes ir incidentus.[166]

Reagavimo į kibernetinio saugumo krizes mechanizmas yra sukurtas siekiant „padėti didinti ES atsparumą kibernetinėms grėsmėms ir solidariai pasirengti trumpalaikiam reikšmingų kibernetinio saugumo incidentų, didelio masto kibernetinio saugumo incidentų ir didelio masto incidentams lygiaverčių kibernetinio saugumo incidentų poveikiui ir jį sumažinti“. [167] Mechanizmu remiami šių rūšių veiksmai:

1. Parengties veiksmai, įskaitant subjektų itin svarbiuose sektoriuose (sveikatos priežiūros, transporto, energetikos ir kt.) testavimą, siekiant nustatyti galimą pažeidžiamumą, remiantis bendrais rizikos scenarijais ir metodikomis.[168]

2. ES kibernetinio saugumo rezervo sukūrimas- rezervo sukūrimas yra numatytas Kibernetinio solidarumo akto 14 straipsnyje. Rezervas pirmiausiai apima reagavimo į incidentus paslaugas (pvz., informacinio saugumo incidentų analizė, artefaktų ir įrodymų analizė, reagavimas į kibernetinio saugumo incidentus, kibernetinio saugumo incidentų koordinavimas ir kt.), kurias teikia patikimi valdomų saugumo paslaugų teikėjai (angl., managed security service providers). 14 straipsnyje numatyti naudotojai (pvz. valstybių narių kibernetinio saugumo krizių valdymo institucijos ir Kompiuterinių saugumo incidentų valdymo komanda (angl. Computer Security Incident Response Team) gali prašyti ES kibernetinio saugumo rezervo paslaugų, kad „padėtų reaguoti į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus arba didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus ir inicijuoti veiklos atkūrimą po tokių incidentų“.[169]

Savitarpio pagalba- vienos valstybės narės teikiama techninė pagalba kitai yra teikiama dotacijų forma. [170]

3. Europos kibernetinio saugumo incidentų peržiūros mechanizmas yra skirtas konkretiems kibernetinio saugumo incidentams vertinti ir peržiūrėti. Komisijos arba nacionalinių institucijų (EU-CyCLONe) prašymu ES kibernetinio saugumo agentūra (ENISA) bus atsakinga už konkretaus reikšmingo arba didelio masto kibernetinio saugumo incidento peržiūrą ir turėtų

[166] „Kibernetinis saugumas ES: strategija ir pagrindinės politikos priemonės“, Europos Vadovų Taryba ir Europos Sąjungos Taryba, žiūrėta 2026 m. kovo 19 d., https://www.consilium.europa.eu/lt/policies/cybersecurity/.
[167] „Europos Parlamento ir Tarybos reglamentas (ES) 2025/38“, *supra note*, 162.
[168] „Kibernetinio saugumo dokumentų rinkinys: Taryba priėmė naujus teisės aktus kibernetinio saugumo pajėgumams ES stiprinti“, Europos Vadovų Taryba ir Europos Sąjungos Taryba, žiūrėta 2026 m. kovo 19 d., https://www.consilium.europa.eu/lt/press/press-releases/2024/12/02/cybersecurity-package-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/.
[169] „Europos Parlamento ir Tarybos reglamentas (ES) 2025/38“, *supra note*, 162.
[170] *Ibid*.

pateikti ataskaitą, kurioje būtų pateikta įgyta patirtis ir, kai tinkama, rekomendacijos, kaip pagerinti Sąjungos kibernetinį atsaką.

Apibendrinant galima daryti išvada, ES kibernetinio solidarumo aktu yra reglamentuojami veiksmai kuriais yra siekiama stiprinti ES pajėgumus aptikti dideles ir didelio masto kibernetinio saugumo grėsmes ir išpuolius, jiems pasirengti ir į juos reaguoti. Aktas apima Europos kibernetinio saugumo įspėjimo sistemą, sudarytą iš visoje ES sujungtų saugumo operacijų centrų, ir išsamų kibernetinio saugumo ekstremaliųjų situacijų mechanizmą, skirtą ES kibernetiniam atsparumui didinti.

Atlikus pastarųjų teisės aktų analizę ir palyginus juos tarpusavyje nustatyta, kad Europos Sąjungos Kibernetinio atsparumo aktas nustato privalomus saugumo reikalavimus techninės ir programinės įrangos produktams viso jų gyvavimo ciklo metu, ypatingą dėmesį skiriant saugiam projektavimui. Kibernetinio saugumo aktu sustiprinama ENISA ir nustatoma produktų ir paslaugų kibernetinio saugumo sertifikavimo sistema. ES kibernetinio solidarumo aktu siekiama stiprinti ES pajėgumus nustatyti dideles ir didelio masto kibernetinio saugumo grėsmes ir išpuolius, jiems pasirengti ir į juos reaguoti.

Dar vienas svarbus teisės kibernetinio saugumo teisinio reglamentavimo prasme yra „2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas**.** Minėtu reglamentu įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (toliau – Kompetencijos centras) ir Nacionalinių koordinavimo centrų tinklas (toliau – Tinklas).“[171]Šiame reglamente taip pat nustatomos nacionalinių koordinavimo centrų skyrimo ir Kibernetinio saugumo kompetencijos bendruomenės (toliau – Bendruomenės) įsteigimo taisyklės. [172]

Kompetencijos centro ir Tinklo misija yra stiprinti Europos Sąjungos lyderystę ir strateginę autonomiją kibernetinio saugumo srityje, plėtojant mokslinių tyrimų, technologinius, pramonės ir akademinius pajėgumus bei gebėjimus, kurie būtini pasitikėjimui ir saugumui bendrojoje skaitmeninėje rinkoje užtikrinti. Pagrindiniai Kompetencijos centro tikslai – stiprinti Europos kibernetinio saugumo pajėgumus, gebėjimus, žinias ir infrastruktūrą, siekiant užtikrinti naudą pramonės dalyviams, ypač mažoms ir vidutinėms įmonėms, mokslinių tyrimų bendruomenei, viešajam sektoriui ir pilietinei visuomenei. Taip pat siekiama skatinti kibernetinį

[171] „Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32021R0887.
[172] *Ibid*.

atsparumą, diegti geriausią saugumo praktiką, taikyti saugumo projektavimo principą ir plėtoti skaitmeninių produktų bei paslaugų saugumo sertifikavimą, papildant kitų viešųjų institucijų veiklą [173] Kibernetinio saugumo kompetencijos bendruomenė taip pat prisideda vykdant Kompetencijos centro ir Tinklo misiją, dalijasi kibernetinio saugumo ekspertinėmis žiniomis ir jas skleidžia. Bendruomenę sudaro pramonės sektoriaus, įskaitant mažąsias [174](mažoji įmonė turi iki 50 darbuotojų, jos apyvarta arba bendras balansas yra iki 10 mln. eurų;) ir vidutines įmones (vidutinė įmonė turi iki 250 darbuotojų, jos apyvarta neviršija 50 mln. eurų ir bendras balansas neviršija 43 mln. eurų;), [175] akademinės bendruomenės, mokslinių tyrimų organizacijų ir pilietinės visuomenės asociacijų atstovai, taip pat standartizacijos organizacijos, viešojo sektoriaus subjektai ir kiti subjektai, kurie susiduria su kibernetinio saugumo iššūkiais.[176]

Išanalizavus reglamentą, matoma, kad Kompetencijos centras ir Tinklas buvo įsteigti siekiant stiprinti Europos Sąjungos lyderystę ir savarankiškumą kibernetinio saugumo srityje. Jų tikslas yra plėtoti mokslinius tyrimus, technologijas ir pramonės gebėjimus, jog būtų užtikrintas tinklų, informacinių sistemų saugumas. Bendruomenės yra svarbios tuo, kad dalinasi žiniomis ir patirtimi tarp įvairių sektorių atstovų.

Apibendrinant galima teigti, kad tarptautinio ir ES kibernetinio saugumo teisinio reglamentavimo ištakos grindžiamos pagrindinėmis žmogaus teisių ir laisvių apsaugos nuostatomis. Šias nuostatas įtvirtina EŽTK, Visuotinė žmogaus teisių deklaracija, Chartija. Šie teisės aktai įtvirtina esmines asmens privatumo, duomenų apsaugos garantijas, todėl tai sudaro pagrindą kibernetinio saugumo teisiniam reglamentavimui. Tarptautiniu lygmeniu svarbią reikšmę turi Budapešto konvencija dėl elektroninių nusikaltimų ir jos papildomi protokolai, kurie įtvirtina pagrindinius nusikaltimus elektroninėje erdvėje. ES kibernetinio saugumo srityje yra svarbūs šie teisės aktai: Direktyva 2013/40/ES dėl atakų prieš informacines sistemas, TIS2 direktyva, BDAR, Kibernetinio saugumo aktas, Kibernetinio atsparumo aktas bei Kibernetinio solidarumo aktas. Direktyva 2013/40/ES reglamentuoja nusikalstamas veikas, susijusias su neteisėtais išpuoliais prieš informacines sistemas, derinant valstybių narių baudžiamojoje teisėje. TIS2 direktyva sustiprino tinklų ir informacinių sistemų saugumo reikalavimus, praplėtė subjektų skaičių, kuriems taikomi kibernetinio saugumo įsipareigojimai, bei nustatė incidentų pranešimo ir rizikų valdymo mechanizmus. BDAR reglamentuoja asmens duomenų apsaugą ir užtikrina asmenų teisę kontroliuoti savo asmens duomenis elektroninėje erdvėje. Kibernetinio saugumo aktu

[173] *Ibid*.
[174] „Europos kibernetinio saugumo tinklas ir kompetencijos centras“ (teisės akto santrauka), EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/lt/legal-content/summary/european-cybersecurity-network-and-competence-centre.html.
[175] „Komisijos rekomendacija dėl labai mažų, mažų ir vidutinių įmonių apibrėžties (2003/361/EB)“, EUR-Lex, žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/eli/reco/2003/361/oj.

sustiprinamas ENISA vaidmuo ir sukuriama bendroji informacinių ir ryšių technologijų produktų, paslaugų ir procesų kibernetinio saugumo sertifikavimo sistema. Kibernetinio atsparumo aktu nustatomi privalomi saugumo reikalavimai produktams su skaitmeniniais elementais, užtikrinant, kad programinė įranga būtų kuriama laikantis saugumo principų viso produkto gyvavimo ciklo metu. Tuo tarpu Kibernetinio solidarumo aktu siekiama stiprinti gebėjimą aptikti kibernetines grėsmes, joms pasirengti ir reaguoti į kibernetinius incidentus. Taip pat kibernetinio saugumo teisinio reglamentavimo formavimuisi, svarbų vaidmenį atlieka ir NATO bei ES kibernetinio saugumo strategijos, kurios apibrėžia politikos kryptis, orientuotas į valstybių kibernetinio saugumo stiprinimą.

3. KIBERNETINIO SAUGUMO TEISINIS REGLAMENTAVIMAS LIETUVOJE

„Europos Sąjunga gali efektyviai funkcionuoti tik visoms narėms laikantis bendrų taisyklių. Europos Sąjungos teisės aktų, – kūrimas, derinimas ir tobulinimas yra gana ilgas ir sudėtingas procesas. Pasiekus kompromisą ir priėmus ES teisės aktą, kiekviena šalis narė privalo užtikrinti, kad šis teisės aktas valstybėje veiktų“.[177] Europos Sąjungos reikalų koordinavimo taisyklės reguliuoja Lietuvos Respublikos pozicijų Europos Sąjungos (toliau – ES) institucijose nagrinėjamais klausimais rengimą, derinimą, svarstymą, pristatymą, ES teisės perkėlimą į Lietuvos Respublikos nacionalinę teisę (toliau – nacionalinė teisė) ir jos įgyvendinimą.[178] Reglamentai – yra privalomi visa apimtimi ir tiesiogiai taikomi (tiek institucijų, tiek privačių asmenų) valstybėse narėse. Svarbu yra tai, kad valstybės privalo užtikrinti jų veikimą, imtis veiksmų reglamentų numatytiems įpareigojimams įvykdyti ir tik būtinais atvejais priimti juos įgyvendinančius nacionalinius teisės aktus. Tuo tarpu Direktyvos – privalomos valstybei narei rezultato, kurį reikia pasiekti, atžvilgiu. Kiekviena valstybė narė turi pasirinkti direktyvų perkėlimo būdą ir formas. Direktyvos nuostatoms perkelti rengiami nacionalinės teisės aktai. Sprendimai – priimami taikant ES teisę konkrečiam atvejui ir privalomi visa apimtimi bei taikomi tiesiogiai jų adresatams (valstybėms narėms, fiziniams ar juridiniams asmenims).[179] Tad šiame skyriuje bus apžvelgta, kaip Lietuvos Respublikoje perkelti Europos Sąjungos priimti reglamentai, direktyvos ir sprendimai, susiję su kibernetiniu saugumu. Taip pat bus aptarta Nacionalinė kibernetinio saugumo strategija ir su ja susiję dokumentai.

Pagrindinis teisės aktas užtikrinantis kibernetinį saugumą yra Lietuvos Respublikos kibernetinio saugumo įstatymas. Šis įstatymas buvo priimtas dar 2014 m. gruodžio 11 d., tačiau paskutiniai pakeitimai įsigaliojo 2024 m. spalio 18 d. Šis teisės aktas įgyvendina ankstesniame skyriuje nagrinėtus ES teisės aktus:

1. 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).

---

[177] Milda Masevičiūtė, ES poveikis darbo santykių reguliavimui Lietuvoje (magistro baigiamasis darbas, Vytauto Didžiojo universitetas, 2009), žiūrėta 2026 m. kovo 19 d., https://portalcris.vdu.lt/server/api/core/bitstreams/0717c60d-7145-40df-be21-ce0731f760e8/content.

[178] „Lietuvos Respublikos Vyriausybės nutarimas Nr. 21 „Dėl Europos Sąjungos reikalų koordinavimo““, TAR, žiūrėta 2026 m. kovo 19 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.224896/asr.

[179] „Europos Sąjungos reikalų koordinavimas“, Lietuvos Respublikos teisingumo ministerija, žiūrėta 2026 m. kovo 19 d., https://tm.lrv.lt/lt/veiklos-sritys-1/es-reikalu-koordinavimas/.

2. 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas.

3. 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva).

TIS 2 direktyvos tikslas yra padidinti ES svarbiuose sektoriuose veikiančių organizacijų tinklų ir informacinių sistemų kibernetinį atsparumą, o įvykus kibernetiniam incidentui – efektyviau suvaldyti sukeliamą žalą. Atsižvelgiant į tai, kad TIS1 ir TIS2 direktyvų skirtumai, kurių didžioji dalis buvo perkelta į Kibernetinio saugumo įstatymo (toliau- KSĮ) nuostatas buvo išanalizuotos ankstesniame skyriuje, todėl šiame skyriuje bus nagrinėjamos pagrindinės KSĮ nuostatos bei naujausi ir aktualiausi teisės akto pakeitimai.

KSĮ nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones.[180] „Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija.[181] Tuo tarpu užsienio reikalų ministerija formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek reikia nustatyti diplomatinių priemonių taikymo reaguojant į kibernetines grėsmes ir kibernetinius incidentus teisinį reguliavimą“.[182]

Kibernetinio saugumo politiką Lietuvoje įgyvendina:

1. NKSC- kurio visos funkcijos yra numatytos KSĮ 7 str., tačiau pagrindinė veiklos sritis yra susijusi su kibernetinių grėsmių paieškos priemonių taikymu kibernetinėje erdvėje. Tai yra, kad NKSC stebi, renka ir analizuoja informaciją apie kibernetines grėsmes, tinklų ir informacinių sistemų spragas kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus, taip pat teikia pagalbą kibernetinio saugumo subjektams, susijusią su jų tinklų ir informacinių sistemų stebėjimu. Taip pat atsinaujinus įstatymui yra numatyta, kad NKSC koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie kibernetinius incidentus, kurių viena Lietuvos Respublika nepajėgia suvaldyti;

---

[180] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note*, 44.
[181] *Ibid*.
[182] *Ibid*.

2. Lietuvos policija- jos funkcijos ir uždaviniai kibernetinio saugumo srityje yra numatytos KSĮ 10 str. Tačiau bendra prasme įgyvendindama kibernetinio saugumo politiką gauna ir tvarko duomenis ir (ar) informaciją apie kibernetinius incidentus nusikalstamų veikų prevencijos, analizės, tyrimo ar atskleidimo tikslais. Taip pat policija turi teisę iš kibernetinio saugumo subjektų gauti informaciją, reikalingą analizuojant ir vertinant, ar kibernetinis incidentas turi galimų nusikalstamos veikos požymių.[183]

3. Valstybinė duomenų apsaugos inspekcija- įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir atlieka 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)[184] su visais pakeitimais nustatytas priežiūros institucijos užduotis.[185]

Atnaujinus KSĮ jis yra taikomas skirtinguose sektoriuose ir yra nustatomos dvi grupės kibernetinio saugumo subjektų (esminiais ir svarbiais), kurie skiriasi pagal NKSC vykdoma priežiūra. „Esminiams subjektams taikoma išsami *ex ante* ir *ex post* priežiūros tvarka, o svarbiems subjektams taikoma negriežta, tik *ex post*, priežiūros tvarka. Svarbių subjektų patikrinimas turėtų būti pradedamas tik gavus duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, padarė KSĮ nustatytų reikalavimų pažeidimą. Esminiams ir svarbiems subjektams numatoma pareiga pranešti apie bet kokį incidentą, darantį didelį poveikį subjektų paslaugų teikimui. KSĮ nustatyta, kad kibernetinio saugumo subjektai praneša NKSC apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones[186]“ Bendrųjų esminių ir bendrųjų svarbių kibernetinio saugumo subjektų identifikavimo kriterijai yra numatyti KSĮ 11 str., tačiau pagrindai skirtumai yra susiję su vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančiomis ribomis. Taip pat kai kuriuose sektoriuose veikiantys subjektai, gali būti priskirti prie esminių subjektų kategorijai neatsižvelgiant į subjekto dydį (finansų dydį, darbuotojų skaičių), kadangi šie subjektai gali būti ypatingos svarbos visuomeninei, gali daryti didelį poveikį viešajam saugumui, ir teikti paslaugas, kurios yra gyvybiškai svarbioms valstybės funkcijoms atlikti ir pan. Šie subjektai gali būti- aukščiausio lygio domenų vardų registravimo paslaugas teikiantys subjektai, valdomų paslaugų teikėjai, valdomų kibernetinio saugumo paslaugų teikėjai, centrinės valdžios viešojo administravimo subjektai.[187]

---

[183] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note,* 44.
[184] „Europos Parlamento ir Tarybos reglamentas (ES) 2016/679“, *supra note,* 128.
[185] *Ibid.*
[186] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note,* 44.
[187] *Ibid.*

KSĮ yra numatyta, kad kibernetinio saugumo subjektai turi imtis tinkamų kibernetinio saugumo priemonių, kuriomis būtų siekiama valdyti savo informacijos saugumo riziką. Šie saugumo subjektai privalės užtikrinti savo tinklų ir informacinių sistemų atitiktį kibernetinio saugumo reikalavimams. Pagal naujuosius kibernetinio saugumo reikalavimus, nuo šiol už šių reikalavimų įgyvendinimą yra tiesiogiai atsakingas organizacijos vadovas, taip pat organizacijos turės pasirūpinti už kibernetinį saugumą atsakingų asmenų paskyrimu. Subjektai turės griežčiau vykdyti tiekimo grandinės saugumo užtikrinimą, taikyti kriptografines saugos priemones ir fizinės prieigos kontrolę, žinoti ir vykdyti griežtesnę savo IT turto kontrolę, naudoti kelių veiksnių tapatumo nustatymo priemones. Naujųjų kibernetinio saugumo reikalavimų įgyvendinimui yra taikomas 12 mėn., o tam tikriems techniniams reikalavimams įgyvendinti – 24 mėn. pereinamasis laikotarpis nuo subjekto įtraukimo į registrą pradžios.[188]

„2024 m. lapkričio 6 d. Lietuvos Respublikos Vyriausybė priėmė nutarimą Nr. 945 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, kuriuo buvo pakeistas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“. Šiuo nutarimu buvo priimtas nacionalinis kibernetinių incidentų valdymo planas“. [189] Šis planas numato ir nustato kibernetinių incidentų valdymą, vertinimą ir informavimą. [190]

Patvirtinus naują valdymo planą, jame keitėsi incidentų klasifikavimas, pranešimo terminai ir būdai. „Kibernetinio saugumo subjekto Saugumo operacijų centras apie kibernetinius incidentus informuoja NKSC, juos registruodamas Kibernetinio saugumo informacinės sistemos posistemyje – Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma)“. [191]Nuo šiol kibernetiniai incidentai skirstomi į didelius, nedidelius ir vos neįvykusius incidentus. „Vos neįvykęs kibernetinis incidentas- yra įvykis, dėl kurio galėjo būti sukeltas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui, bet kuriam įvykti buvo sėkmingai užkirstas kelias arba kuris neįvyko“.[192]

Didelis kibernetinis incidentas laikomas tada, kai:

---

[188] „Vyriausybė patvirtino Kibernetinio saugumo įstatymo įgyvendinimą reglamentuojančius dokumentus“, Lietuvos Respublikos krašto apsaugos ministerija, 2024 m. lapkričio 8 d., žiūrėta 2026 m. kovo 19 d., https://kam.lt/vyriausybe-patvirtino-kibernetinio-saugumo-istatymo-igyvendinima-reglamentuojancius-dokumentus/.

[189] „Lietuvos Respublikos Vyriausybės nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo““, TAR, žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/lt/legalAct/aea15050a53411e8acb39f2e6db7935b/asr.

[190] *Ibid.*

[191] *Ibid.*

[192] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note*, 45.

1. Kibernetinio saugumo subjektas patiria arba gali patirti didelių paslaugų teikimo sutrikimų, kai kibernetinis incidentas atitinka bent vieną įstatyme numatytų kriterijų. Taip pat kriterijai laikomi atitinkamais, kai „kibernetinio saugumo subjektas nebegali užtikrinti jo veiklai teisės aktuose nustatytų reikalavimų įgyvendinimo, kai prarastos arba atskleistos komercinės paslaptys arba įslaptinta informacija, arba kai per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas, incidentų pagrindinė priežastis sutampa, o finansiniai nuostoliai siekia arba viršija 500 000 eurų arba 5 procentus kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos, atsižvelgiant į tai kuri suma yra mažesnė.

2. Kibernetinio saugumo subjektas patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur, arba 5 procentų kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė)

3. Kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą, atitinkančią bent vieną iš šių kriterijų: galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų. Galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 Eur. Buvo sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo.[193]

Apie tokio tipo incidentą nuo to sužinojimo momento, kai kibernetinio saugumo subjektai sužino apie didelį kibernetinį incidentą, nedelsdami, bet ne vėliau kaip per 24 valandas pateikia ankstyvąjį perspėjimą. Perspėjime turėtų būti nurodyta, ar įtariama, kad didelį incidentą sukėlė neteisėti arba piktavališki veiksmai, ir ar tikėtina, kad jis turės tarpvalstybinį poveikį. Taip pat kibernetinio saugumo subjektai nedelsdami, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie didelį kibernetinį incidentą momento pateikia pranešimą apie kibernetinį incidentą. Kuriame pagal galimybes atnaujinama pirminė informacija ir nurodomas didelio kibernetinio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi įsilaužimo įrodymai, jeigu tokių yra. Tada subjektas ne vėliau kaip per vieną mėnesį nuo minėto pranešimo apie kibernetinį incidentą pateikimo dienos pateikia galutinė ataskaita, kurioje pateikiamas išsamus kibernetinio incidento, įskaitant jo sunkumą ir poveikį, aprašymas. Grėsmės arba pagrindinės priežasties, dėl kurios kibernetinis incidentas galėjo įvykti, rūšis. taikomos ir įgyvendinamos kibernetinio incidento poveikio mažinimo priemonės. Tarpvalstybinis kibernetinio incidento poveikis, jeigu toks buvo.[194]

---

[193] „Nacionalinis kibernetinių incidentų valdymo planas“, *supra note,* 189.

[194] „Atnaujintas kibernetinio saugumo įstatymas“, Lietuvos Respublikos krašto apsaugos ministerija, 2024 m. lapkričio 29 d., žiūrėta 2026 m. kovo 19 d., https://kam.lt/wp-content/uploads/2024/12/TIS2-brosiura_Pilnas_2024-11-29.pdf.

Nedidelis kibernetinis incidentas laikomas tada, kai jis neatitinka didelio kibernetinio incidento kriterijų. Apie tokį incidentą Kibernetinio saugumo subjekto Saugumo operacijų centras NKSC informuoja pateikdamas:

„1. nedelsdamas, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie kibernetinį incidentą momento, pranešimą apie nedidelį kibernetinį incidentą, jame pateikdamas nurodomas kibernetinio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi įsilaužimo įrodymai, jeigu tokių yra;

2. per vieną mėnesį nuo pranešimo apie kibernetinį incidentą registravimo dienos galutinę ataskaitą apie nedidelį kibernetinį incidentą;

3. galutinė ataskaita apie nedidelį kibernetinį incidentą neteikiama, jei pranešime apie kibernetinį incidentą pateikta visa galutinės ataskaitos informacija“.[195]

Vienas iš svarbių šių laikų procesų kibernetinėje erdvėje yra tiekimo grandinė. Tiekimo grandinė sujungia veiksmus, reikalingus žaliavoms paversti vartotojams paruoštu gatavu produktu. Grandinė prasideda nuo žaliavų gamintojų ir baigiasi galutiniu pristatymu vartotojams[196]. Taigi KSĮ yra įtvirtinti kibernetinio saugumo reikalavimai, kurie apima ir tiekimo grandinės saugumą, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais. [197] Tad įgyvendinant kibernetinio saugumo įstatymą, yra numatyta pareiga subjekto vadovams. Pastarieji turi „nustatyti tiekimo grandinės saugumo valdymo tvarką, kuri yra taikomą paslaugų, darbų ar įrangos pirkimams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu, kibernetinio saugumo užtikrinimu. Tuo yra siekiama mažinti galimas rizikas tinklų ir informacinėms sistemoms. Taip pat, kibernetinio saugumo subjektas, nustatydamas tiekimo grandinės saugumo valdymo tvarką, turi numatyti tinklų ir informacinių sistemų tiekėjų atrankos kriterijus“.[198] Taigi, kibernetinio saugumo subjektai privalės įsitikinti, kad tiekėjai atitinka saugumo reikalavimus, pavyzdžiui galima bus tikrinti ar turi incidentų valdymo planus, atitinkamus saugumo sertifikatus, įvykus kibernetiniam incidentui bendradarbiaus su kibernetinio saugumo subjektu ir pan.

Kadangi NIS2 nustato daug griežtesnius saugumo ir valdymo įsipareigojimus, kuo siekiama įdiegti darbuotojų mokymo ir informavimo programas. Tad KSĮ yra numatyta, kad kibernetinio saugumo reikalavimai apima kibernetinės higienos praktiką ir reguliarius „kibernetinio saugumo mokymus. Kibernetinio saugumo subjekto valdymo organų nariai, vadovas ir jo įgaliotas asmuo, jeigu toks yra, ar kibernetinio saugumo subjektas, jeigu jis yra fizinis asmuo,

---

[195] „Nacionalinis kibernetinių incidentų valdymo planas“, *supra note,* 189.
[196] Adam Hayes, „Optimizing Supply Chains: From Raw Materials to Consumers“, Investopedia, atnaujinta 2025 m. rugpjūčio 1 d., žiūrėta 2026 m. kovo 19 d., https://www.investopedia.com/terms/s/supplychain.asp.
[197] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note*, 45.
[198] „Nacionalinis kibernetinių incidentų valdymo planas“, *supra note,* 189.

privalo ne rečiau kaip kartą per 2 metus Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka išklausyti kibernetinio saugumo mokymus ir užtikrinti kibernetinio saugumo subjekto darbuotojų, jeigu tokių yra, nuolatinį švietimą kibernetinio saugumo srityje.“[199] Mokymai yra svarbus tuo, kad jie ne tik „suteikia galimybę plėsti žinias kibernetinio saugumo klausimais, bet ir keičia žmonių mąstyseną, požiūrį ir elgesį. Aiškios politikos ir procedūros susitirpiną žinių įsisavinimą. Vadovai paskirstydami išteklius, nustatydami suprantamą politiką ir būdami pavyzdžiu, laikantis kibernetinio saugumo praktikų, parodytų aiškų įsipareigojimą kibernetiniam saugumui. Visi šie elementai padeda kurti stiprią kibernetinio saugumo kultūrą organizacijose.“[200] Taip pat yra svarbu, kad organizacijos vadovas privalo užtikrinti, kad jo organizacija laikytųsi kibernetinio saugumo reikalavimų. Už reikalavimų nevykdymą ar kitus pažeidimus NKSC gali skirti įvairias poveikio priemones žr. pav 2. Baudos nustatytos atsižvelgiant į TIS 2 direktyvos nuostatas.

3. pav. Baudų dydis esminiams ir svarbiems subjektams nustatytas atsižvelgiant į TIS 2 direktyvos nuostatas.[201]

Išanalizavus KSĮ, galima patvirtinti, kad šis teisės aktas įgyvendina svarbiausius ES teisės aktus, o ypač NIS2 direktyvą. Šis įstatymas nustato kibernetinio saugumo politiką Lietuvoje tai yra nustato kibernetinio saugumo subjektų pareigas, atsakomybę ir taikomas saugumo priemones.

---

[199] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note*, 45.
[200] Inga Šimonienė, „Kibernetinio saugumo kultūros vertinimas Lietuvos ligoninėse“ (magistro baigiamasis darbas, Mykolo Romerio universitetas, 2024), žiūrėta 2026 m. kovo 19 d., https://cris.mruni.eu/server/api/core/bitstreams/a4bca602-9cc8-4729-949e-0d4c8c8713ac/content.
[201] „Atnaujintas kibernetinio saugumo įstatymas“, supra note, 195.

Atnaujintas įstatymas, perkeliantis TIS2 nuostatas, įtvirtino esminių ir svarbių kibernetinio saugumo subjektų klasifikavimą, jų priežiūrą bei griežtesnius reikalavimus. KSĮ pakeitimai sustiprino organizacijų kibernetinį atsparumą, padidino vadovų atsakomybę ir įtvirtino sisteminį rizikų, incidentų bei tiekimo grandinės saugumo valdymą.

Analizuojant kibernetinio saugumo teisinį reglamentavimą Lietuvoje yra svarbu suvokti ir pačią Nacionalinė kibernetinio saugumo strategiją. Vadovaujantis KSĮ nacionalinė kibernetinio saugumo strategija yra suprantama kaip nuosekli sistema, apimanti Lietuvos Respublikos kibernetinio saugumo srities strateginius tikslus. Pagrindinis nacionalinio kibernetinio saugumo tikslas yra – „efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų (toliau – IRT) teikiamomis galimybėmis“.[202]

Lietuvos Respublikos Seimo nutarime dėl Nacionalinės saugumo strategijos yra įtvirtinti kibernetinio saugumo bei atsparumo sustiprinimo uždaviniai - kuriais yra siekiama „plėtoti kibernetinio saugumo ir gynybos pajėgumus, siekiant užtikrinti nuolatinę nacionalinės kibernetinio saugumo ir gynybos sistemos plėtrą, efektyvų kibernetinių incidentų atpažinimą, prevenciją, užkardymą ir valdymą, vystyti veiksmingą viešojo ir privataus sektorių bendradarbiavimą šioje srityje“.[203] Taip pat yra siekiama skatinti kibernetinio saugumo kultūrą kibernetinio saugumo raštingumą, bei plėtoti bendradarbiavimą NATO, ES ir daugiašaliais formatais kibernetinio saugumo ir kovos su dezinformacija srityje.[204] Lietuvos Respublikos Vyriausybė patvirtintame 2021–2030 metų nacionalinį pažangos plane yra numatyta stiprinti kibernetinį saugumą, gynybą ir veiksmingai valdyti kibernetinius incidentus. Įgyvendinant uždavinį numatoma skatinti viešojo ir privataus sektorių bendradarbiavimą, diegti mokslinių tyrimų, eksperimentinės plėtros ir inovacijų sprendinius, kelti visuomenės (taip pat ir įmonių) kibernetinio saugumo kultūrą, stiprinti tarptautinį bendradarbiavimą – aktyviai dalyvauti kuriant ES kibernetinio greitojo reagavimo pajėgas ir teikti tarpusavio pagalbą kibernetinio saugumo srityje.[205] Lietuvos Respublikos Seimo patvirtintoje Krašto apsaugos sistemos stiprinimo ir plėtros programoje taip pat yra numatyti kibernetinio saugumo strateginiai planai. Šiame plane numatyta, kad bus plėtojami gynybiniai kibernetinio saugumo pajėgumų komponentai, kurie yra reikalingi

---

[202] „Nacionalinė kibernetinio saugumo strategija“, Lietuvos Respublikos krašto apsaugos ministerija, žiūrėta 2026 m. kovo 19 d., https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf.
[203] „Lietuvos Respublikos Seimo nutarimas Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo““, TAR, žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2/asr.
[204] *Ibid*.
[205] „Lietuvos Respublikos Vyriausybės nutarimas Nr. 998 „Dėl 2021–2030 metų Nacionalinio pažangos plano patvirtinimo“, TAR, žiūrėta 2026 m. kovo 19 d., https://www.e-tar.lt/portal/lt/legalActEditions/d492e050f7dd11eaa12ad7c04a383ca0.

viso spektro kibernetinėms operacijoms. Taip pat siekiant sukurti sisteminį požiūrį į kibernetinį saugumą, bus nustatytos į valstybinių kibernetinio saugumo pajėgumų komponentų problematiką ir plėtrą bei stiprinimą orientuotos priemonės. Programoje yra numatytas ir plėtojamas tarptautinis, tarpvalstybinis, tarpinstitucinis ir Baltijos regiono šalių bendradarbiavimas kibernetinio saugumo srityje, siekiant stiprinti nacionalinius ir regioninius pajėgumus ir teikti paramą Ukrainai bei Sakartvelui kibernetinio saugumo srityje.[206] Lietuvos Respublikos Vyriausybės patvirtintoje 2023–2030 metų plėtros programoje valdytojos – Lietuvos Respublikos Krašto apsaugos ministerijos Nacionalinės kibernetinio saugumo plėtros programoje, taip pat yra numatyti kibernetinio saugumo stiprinimo tikslai. Taigi išanalizavus minėtus dokumentus, darytina išvada, kad nacionalinė kibernetinio saugumo strategija siekiama:

- „stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą;
- užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą;
- skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą;
- stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą;
- stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą“.[207]

Nors ankstesniame skyriuje buvo nustatyta, kad BDAR turi svarbią reikšmę kibernetinio saugumo teisiniame reglamentavime, ypač kas liečia asmens duomenis, tačiau KSĮ nėra įtvirtinta, kad šis įstatymas įgyvendina minėtą reglamentą. Šį reglamentą „įgyvendina Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Šis įstatymas taikomas kartu su BDAR ir jo įgyvendinamaisiais teisės aktais. Šis įstatymas nustato „asmens duomenų tvarkymo ypatumus, Valstybinės duomenų apsaugos inspekcijos (toliau- VDAI) teisinį statusą ir įgaliojimus, žurnalistų etikos inspektoriaus įgaliojimus, VDAI ir žurnalistų etikos inspektoriaus atliekamo asmens duomenų ir privatumo apsaugą reglamentuojančių teisės aktų pažeidimų nagrinėjimo ir administracinių baudų skyrimo tvarką“. [208] VDAI atstovauja BDAR taikymo priežiūros institucijoms pagal Reglamentą (ES) 2016/679 įsteigtoje Europos duomenų apsaugos valdyboje ir 2025 m. VDAI priėmė sprendimus viešosioms ir privačiosioms įstaigoms skirti 5 baudas (bendra suma 27 529 eurų) už nustatytus BDAR nuostatų pažeidimus. Be to VDAI teikė 9 nurodymus duomenų valdytojams arba duomenų tvarkytojams suderinti duomenų tvarkymo operacijas su BDAR nuostatomis.“ Taip pat buvo pateiktos 22 rekomendacijos duomenų valdytojams, kurios

---

[206] „Lietuvos Respublikos Seimo nutarimas Nr. XIV-2505 „Dėl Krašto apsaugos sistemos stiprinimo ir plėtros programos patvirtinimo““, TAR, žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/lt/legalAct/e3acb430e78f11ee9fdedfc979ae62a9.

[207] „Lietuvos Respublikos Vyriausybės nutarimas Nr. 998 „Dėl 2021–2030 metų Nacionalinio pažangos plano patvirtinimo“, *supra note,* 206.

[208] „Asmens duomenų saugumo pažeidimai Lietuvoje 2025 m.“, Valstybinė duomenų apsaugos inspekcija, žiūrėta 2026 m. kovo 19 d., https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2025-m-lx/.

padės užtikrinti, kad asmens duomenų tvarkymas atitiktų BDAR reikalavimus, o VDAI, vykdydama priežiūros funkcijas, įvertino, kaip duomenų valdytojai laikosi pareigos pranešti apie asmens duomenų saugumo pažeidimus per 72 valandas, ir nustatė, kad 2025 m. 63 proc. duomenų valdytojų šią pareigą įvykdė laiku, o 37 proc. – pavėlavo.[209] Tokie duomenys patvirtina, kad BDAR nuostatų taikymas yra neatsiejamas nuo nacionalinio reguliavimo ir institucinio kontrolės mechanizmo, kuris užtikrina asmens duomenų apsaugą kibernetinio saugumo teisinio reguliavimo kontekste.

Lietuvos Respublikos administracinių nusižengimų kodekse (toliau- ANK) yra įgyvendinamos Europos Sąjungos teisės aktų nuostatos kurios yra susijusios su kibernetiniu saugumu. Visu pirma „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)[210]“ ir „2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)“. [211]479 straipsnyje yra numatyta atsakomybė už KSĮ nuostatų dėl pareigos teikti informaciją, reikalingą analizuojant ir vertinant, ar kibernetinis incidentas turi galimų nusikalstamos veikos požymių, pažeidimus. Atsakomybė kyla tada, kai informacija, kuri yra reikalinga analizuojant ir vertinant, ar kibernetinis incidentas turi galimų nusikalstamos veikos požymių, nepateikiama policijai. 480 straipsnyje yra numatyta atsakomybė už KSĮ nustatytų kibernetinio saugumo užtikrinimo pareigų atlikimo pažeidimus. Tai yra- teisėtų policijos nurodymų, susijusių su kibernetinio saugumo užtikrinimu, neįvykdymas laiku ir Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų reikalavimų kibernetinio saugumo subjektų vadovams ar jų įgaliotiems asmenims pažeidimas. [212] 480-1 straipsnyje administracinė atsakomybė yra numatyta, dėl Reglamente (ES) 2019/881 nustatytos kibernetinio saugumo sertifikavimo tvarkos pažeidimų.[213] Apibendrinant matoma, kad šis teisės aktas numato atsakomybę už tam tikrų KSĮ numatytų nuostatų sertifikavimo tvarkos pažeidimus.

„2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvos 2013/40/ES dėl atakų prieš informacines sistemas, tikslas yra suderinti valstybių narių baudžiamąją teisę atakų prieš informacines sistemas srityje, nustatant būtiniausias taisykles“.[214] Įgyvendinant šį tikslą ir

---

[209] „Asmens duomenų saugumo pažeidimai Lietuvoje 2025 m.“, *supra note*, 208.
[210] „Reglamentas (ES) 2019/881“, *supra note*, 30.
[211] „Europos Parlamento ir Tarybos direktyva (ES) 2022/2555“, *supra note*, 122.
[212] „Lietuvos Respublikos administracinių nusižengimų kodeksas“, TAR, žiūrėta 2026 m. kovo 19 d., https://www.e-tar.lt/portal/lt/legalAct/4ebe66c0262311e5bf92d6af3f6a2e8b/asr.
[213] *Ibid*.
[214] „Europos Parlamento ir Tarybos direktyva 2013/40/ES“, *supra note,* 111.

teises aktą Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“ yra numatyta baudžiamoji atsakomybė už šias nusikalstamas veikas:

196 straipsnis „Neteisėtas poveikis elektroniniams duomenims“;

197 straipsnis „Neteisėtas poveikis informacinei sistemai“;

198 straipsnis „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“;

198¹ straipsnis „Neteisėtas prisijungimas prie informacinės sistemos“;

198² straipsnis „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis“.[215] Lietuvos Respublikos generalinės prokuratūros internetinėje svetainėje nurodoma, kad išvardintu nusikalstamų veikų pagrindinis kėsinimosi objektas yra elektroninių duomenų ir informacinių sistemų saugumas: neteisėtas poveikis elektroniniams duomenims (pvz., tinklalapio „nulaužimas“, neteisėtas prisijungimas prie tinklalapio turinio valdymo sistemos ir elektroninių duomenų pakeitimas ar pašalinimas); neteisėtas poveikis informacinei sistemai (pvz.: DoS ir DDoS atakos prieš internetinius puslapius) neteisėtas elektroninių duomenų perėmimas ir panaudojimas (pvz. Sodros, Vidaus reikalų ministerijos CDB duomenys, bankų neviešo pobūdžio informacija ir pan.), neteisėtas prisijungimas prie informacinės sistemos (pvz. prisijungimas prie svetimos elektroninės bankininkystės paskyros, elektroninės pašto dėžutės, Facebook, ICQ paskyrų, prisijungimai prie įvairių neviešo pobūdžio duomenų talpyklų, registrų), neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (pvz. disponavimas kenkėjiška programine įranga, kuri renka klientų duomenis taip pat neteisėtas disponavimas svetimų elektroninių paskyrų slaptažodžiais, prisijungimo kodais.[216]

Įgyvendinant direktyvą dėl atakų prieš informacines sistemas, 14 straipsnį, yra priimtas įsakymas, kuriuo yra pavestas Informatikos ir ryšių departamentas prie Vidaus reikalų ministerijos kasmet iki kovo 1 d. teikti Europos Komisijai statistinius duomenis už praėjusius kalendorinius metus apie pradėtų ikiteisminių tyrimų skaičių bei asmenų, įtariamų, kaltinamų ir nuteistų pagal Lietuvos Respublikos baudžiamojo kodekso 196, 197, 198, 198¹, 198² straipsnius, skaičių.[217]

Konvencijos dėl elektroninių nusikaltimų ir direktyvos dėl atakų prieš informacines sistemas normos yra taikomos ir teismų praktikoje. Pavyzdžiui LAT byloje 2K-262-489/2022, dėl BK 196 straipsnio 1 dalies taikymo teismas aiškino, kad „Neteisėtumo nustatymo reikalavimas yra siejamas su 2001 m. Europos Tarybos konvencijos dėl elektroninių

---

[215] „Lietuvos Respublikos baudžiamasis kodeksas“, TAR, žiūrėta 2026 m. kovo 19 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr.

[216] „Nusikaltimai elektroninėje erdvėje“, Lietuvos Respublikos prokuratūra, žiūrėta 2026 m. kovo 19 d., https://www.prokuraturos.lt/lt/veikla/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185.

[217] „Europos Parlamento ir Tarybos direktyvos 2013/40/ES dėl atakų prieš informacines sistemas“, *supra note*, 111.

nusikaltimų 4 straipsnio nuostatomis, reikalaujančiomis kriminalizuoti ne bet kokį, o sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą arba galimybės naudotis tokiais duomenimis panaikinimą. Taip pat neteisėtumo požymis nurodomas ir 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – Direktyva), 5 straipsnyje. Atitinkamai Direktyvos 2 straipsnio d punkte nurodoma, kad požymis *neturint tam teisės* yra suprantamas kaip elgesys, kuriam sistemos ar jos dalies savininkas ar kitas teisės turėtojas nesuteikė leidimo arba kuris neleidžiamas pagal nacionalinę teisę“.[218]

LAT byloje 2K-27-976/2023 dėl BK 198[1] straipsnio 1 dalies ir BK 198 straipsnio 1 dalies taikymo teismas taip pat pažymėjo, kad „neteisėtumo nustatymo reikalavimas yra susijęs su 2001 m. lapkričio 23 d. Konvencijos dėl elektroninių nusikaltimų 2 straipsnio ir Direktyvos 2013/40/ES 3 straipsnio nuostatomis, reikalaujančiomis kriminalizuoti ne bet kokią, o neteisėtą prieigą prie informacinės sistemos. Vadovaujantis Direktyvos 2013/40/ES 2 straipsnio d punktu, neteisėtumas konstatuotinas, kai prieiga prie informacinės sistemos gauta neturint informacinės sistemos (ar jos dalies) savininko ar teisėto valdytojo leidimo jungtis prie šios sistemos arba kai toks prisijungimas yra neleidžiamas pagal nacionalinę teisę“.[219] Taip pat šioje byloje teismas pažymėjo, „elektroniniai (kompiuteriniai) duomenys – tai bet kokia faktų, informacijos ar sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programa, pagal kurią kompiuterinė sistema gali atlikti tam tikrą funkciją (Direktyvos 2013/40/ES 2 straipsnio b punktas)“. Taigi atsižvelgiant į LAT praktika galima daryti išvada, kad tarptautiniai ir ES aktai yra ne tik perkelti formaliai į nacionalinę teisė, bet ir taikomi formuojant bendrą teismų praktika.

Apibendrinus Lietuvos kibernetinio saugumo teisinį reglamentavimą, galima daryti išvadą, kad Lietuvos kibernetinio saugumo teisinis reglamentavimas yra įtvirtinęs ES direktyvas ir reglamentus. Pagrindinis nacionalinis teisės aktas – KSĮ – perkelia svarbiausias ES nuostatas ir nustato kibernetinio saugumo subjektų pareigas, rizikų ir incidentų valdymą, priežiūrą. Nacionalinė kibernetinio saugumo strategija nustato svarbiausias nacionalinės kibernetinio saugumo politikos kryptis. ANK numatyta atsakomybė už KSĮ saugumo įstatymo pažeidimus, todėl kibernetinio saugumo subjektai privalo laikytis įstatyme nustatytų reikalavimų. BK numato baudžiamąją atsakomybę už nusikaltimus elektroninių duomenų ir informacinių sistemų

[218] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. gruodžio 15 d. nutartis baudžiamojoje byloje Nr. 2K-262-489/2022“, LITEKO, žiūrėta 2026 m. balandžio 22 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=eb024162-eaa7-45f8-b88c-cdac3127bef9.
[219] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 15 d. nutartis baudžiamojoje byloje Nr. 2K-27-976/2023“, LITEKO, žiūrėta 2026 m. balandžio 22 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9b33ec46-8901-4d5e-af56-d751b3520f97.

saugumui. LAT praktikoje taip pat yra taikomos direktyvų ir reglamentų nuostatos, o tai reiškia efektyvų teisės aktų įgyvendinimą praktikoje.

4. TEISMŲ PRAKTIKOJE TAIKOMŲ NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI PROBLEMINIAI KVALIFIKAVIMO ASPEKTAI IR SPECIFINIAI YPATUMAI

Šiame skyriuje bus analizuojama teismų praktika, nagrinėjant baudžiamąsias bylas dėl nusikalstamų veikų elektroninėje erdvėje, siekiant nustatyti šių veikų specifinius ypatumus ir probleminius kvalifikavimo aspektus. Lietuvos Respublikos baudžiamojo kodekso (toliau - BK) XXX skyriuje yra numatyta baudžiamoji atsakomybė už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui. „Nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui gali būti daroma žala ne tik elektroninių duomenų arba informacinės sistemos konfidencialumui, bet ir jų integralumui ar prieinamumui“. [220] „Nusikalstamų veikų, nurodytų minėtame skyriuje, baudžiamojo įstatymo saugomas objektas yra elektroninių duomenų ir informacinių sistemų saugumas. Duomenų saugumas apibrėžiamas šiais keturiais požymiais: duomenų konfidencialumas (duomenys nėra atskleidžiami ar pasiekiami subjektams, neturintiems tokios teisės), vientisumas (duomenys nebuvo pakeisti ar sunaikinti neteisėtu būdu), prieinamumas (duomenys reikiamu metu yra prieinami teisę turintiems subjektams), autentiškumas (duomenų savybė, užtikrinanti, kad duomenys saugojimo, kaupimo, apdorojimo ir perdavimo metu nebūtų iškraipomi)“. [221] Remiantis Informatikos ir ryšių departamento duomenimis, laikotarpiu nuo 2020 m. iki 2026 m. vasario mėn., iš viso užregistruotos 4026 nusikalstamos veikos, iš kurių 1375 bylos buvo perduotos teismui, 265 bylos baigtos teismo baudžiamuoju įsakymu, o 2779 bylos nutrauktos.[222] Atsižvelgiant į tai, aktualu išanalizuoti nusikalstamų veikų, susijusių su elektroninių duomenų ir informacinių sistemų saugumu, problematiką ir jų kvalifikavimo ypatumus.

Lietuvos Aukščiausiasis Teismas (toliau- LAT) yra įtvirtinęs, kad „kriminalizuojant nusikalstamas veikas, pažeidžiančias elektroninių duomenų ir informacinių sistemų saugumą, numatyta baudžiamoji atsakomybė ne už bet kokį, o būtent už neteisėtą prisijungimą prie informacinės sistemos ar jos dalies (BK 198[1] straipsnis), neteisėtą neviešų elektroninių duomenų

---

[220] Renata Marcinauskaitė, „ Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 1981 straipsniai)“(daktaro disertacija, Mykolo Romerio universitetas, 2013),157, https://cris.mruni.eu/server/api/core/bitstreams/9b222ea8-bb14-453a-a4ed-1fda10663f13/content.

[221] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2024 m. lapkričio 6 d. nutartis baudžiamojoje byloje Nr. 2K-214-489/2024“, LITEKO, žiūrėta 2025 m. balandžio 5 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=28bccd40-739d-43f7-a8cc-f1eecddab2d2.

[222] Informatikos ir ryšių departamentas, nusikalstamumo duomenų rinkiniai, žiūrėta 2026 m., balandžio 1 d., https://ird.lt/lt/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/nusikalstamumo-duomenu-rinkiniai/family.NU?DT%5B%5D=2026-02&DT%5B%5D=2025-12&DT%5B%5D=2024-12&DT%5B%5D=2023-12&DT%5B%5D=2022-12&DT%5B%5D=2021-12&DT%5B.%5D=2020-12&SAV%5B%5D=LR&BK%5B%5D=XXX&cols=DT&sids=.

perėmimą ir panaudojimą (BK 198 straipsnis)“.[223] arba už neteisėtą poveikį elektroniniams duomenims (BK 196 straipsnis). Todėl XXX skyriuje inkriminuojant veikas „būtina atskleisti ir pagrįsti poveikio neteisėtumo požymį pateiktame kaltinime aiškiai nurodant, kuo jis pasireiškė, kodėl asmens veiksmai laikytini neteisėtais, kokius teisės aktus pažeidė, kokių nustatytų draudimų nesilaikė. Neteisėtumas, jei jis siejamas su asmens, neturinčio jokio teisinio pagrindo prieiti prie elektroninių duomenų šaltinio (pavyzdžiui, duomenų talpyklos, serverio), veiksmais, gali pasireikšti pačiu veikimo būdo neteisėtumu (pvz., neteisėtas prisijungimas prie elektroninių duomenų talpyklos, serverio turinio valdymo sistemos panaudojant programinę įrangą ir ten esančių duomenų tyčinis sunaikinimas, pakeitimas, pašalinimas)“.[224] Neteisėtumo nustatymo reikalavimas numatytas ir Konvencijoje dėl elektroninių nusikaltimų ir joje yra įtvirtina, kad „šalys turi nustatyti baudžiamajai atsakomybei už sąmoningą ir neteisėtą kompiuterinių duomenų sugadinimą, sunaikinimą, apgadinimą, pakeitimą arba galimybės naudotis tokiais duomenimis panaikinimą“.[225] Neteisėtumo požymis taip pat įtvirtintas direktyvos dėl atakų prieš informacines sistemas 3-6 straipsniuose, kuris apimta neteisėta prieiga prie informacinių sistemų, neteisėta įsikišimą į sistema ir į duomenis, neteisėta duomenų perėmimą.[226] Direktyvos 2 straipsnio d punkte nurodoma, kad požymis neturint tam teisės yra suprantamas kaip „elgesys, nurodytas šioje direktyvoje, įskaitant prieigą, įsikišimą ar duomenų perėmimą, kuriam sistemos ar jos dalies savininkas ar kitas teisės turėtojas nesuteikė leidimo, arba kuris neleidžiamas pagal nacionalinę teisę“.[227]

Analizuojant LAT nutartį baudžiamojoje byloje Nr. 2K-262-489/2022, buvo nustatyta, kad kaltinamasis buvo nuteistas pagal BK 196 str., už tai, kad du kartus, „autentifikavęs savo tapatybę ir prisijungęs kaip koordinatorius e. mokymosi sistemoje prie dėstomo modulio neteisėtai pašalino, t. y. ištrynė, Lietuvos sporto universiteto nuosavybę – medžiagą studentams pagal patvirtintą modulio aprašą“. [228] Kasaciniame skunde teigta, kad kaltinamojo veiksmuose nebuvo nusikaltimo dalyko ir neteisėtumo požymio, kadangi kaltinamasis buvo teisėtas duomenų valdytojas ir naudotojas.[229] Kasacinės instancijos teismas nurodė, kad nagrinėjant bylą pirmosios ir apeliacinės instancijos teismuose BK 196 straipsnio 1 dalies nuostato minėto BK straipsnio aiškinimo aspektus buvo atskleidžiamos ir taikomos netinkamai. Visų pirma nustatyta, kad

[223] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 15 d. nutartis baudžiamojoje byloje Nr. 2K-27-976/2023“, LITEKO, žiūrėta 2025 m. vasario 18 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9b33ec46-8901-4d5e-af56-d751b3520f97.
[224] „Nutartis baudžiamojoje byloje 2K-262-489/2022“, *supra note*, 218.
[225] „Konvencija dėl elektroninių nusikaltimų“ (ETS Nr. 185)“, *supra note*, 102.
[226] „Europos Parlamento ir Tarybos direktyva 2013/40/ES“, *supra note,* 111.
[227] *Ibid.*
[228] „Nutartis baudžiamojoje byloje 2K-262-489/2022“, *op. cit.*
[229] *Ibid.*

kaltinamasis turėjo teisėtą prieigą, todėl neteisėtumo kriterijus nebuvo tinkamai pagrįstas. Be to, konstatuota, kad žemesnės instancijos teismai vertino tik elektroninių duomenų pobūdį ir jų turinį, tačiau neįvertino konkrečių poveikio (ištrynimo) aplinkybių pavojingumo. Nebuvo atsižvelgta į tai, kad ištrinti duomenys yra autorių teisių saugomas intelektinės nuosavybės objektas, taip pat į tai, kad duomenys nebuvo visiškai sunaikinti, nes medžiaga buvo naudojama kitose institucijose.[230]

Byla buvo netinkamai kvalifikuota, nes buvo nustatyta, kad tai darbo ginčas, kurio metu įvyko elektroninės formos intelektinės nuosavybės objekto ištrynimas, ir tai yra privatinės teisės prigimties (pobūdžio). Atitinkamai šis teisinis ginčas turėjo būti sprendžiamas privatinės teisės gynimo priemonėmis – darbo ginčo procese ir (ar) reikalaujant žalos atlyginimo civilinio proceso tvarka, o ne pasitelkiant baudžiamąją justiciją. Byloje nebuvo tinkamai įvertinta tyčia. Pirmosios instancijos teismas apie R. P. kaltės turinį nepasisakė, o apeliacinės instancijos teismas nurodė, kad R. P. veikė tiesiogine neapibrėžta tyčia. Tačiau kasacinis teismas konstatavo, kad apeliacinės instancijos teismo nutartyje nėra tinkamai atskleistas nei netiesioginės tyčios turinys, nei kaltininko psichinis santykis su padaryta veika ir jos padariniais. [231]Byloje, buvo nustatyti šie probleminiai kvalifikavimo ypatumai: pirmosios ir apeliacinės instancijos teismai netinkamai taikė BK 196 straipsnio 1 dalį, kadangi nebuvo tinkamai pagrįstas neteisėtumo poveikis elektroninėms duomenims, neįvertintas veikos pavojingumas ir neišsamiai atskleista kaltė. Be to, konstatuotina, kad ginčas turėjo privatinės teisės pobūdį, todėl turėjo būti sprendžiamas civilinio proceso tvarka.

2024 m., LAT baudžiamojoje byloje Nr. 2K-214-489/2024, kaltinamasis pagal BK 198 straipsnio 1 dalį nuteistas už tai, kad „būdamas įmonės darbuotoju ir turėdamas teisėtą prieigą prie neviešų elektroninių duomenų, sudarančių komercinę paslaptį, nesilaikydamas konfidencialumo įsipareigojimo, pagal kurį jis negalėjo kopijuoti ir dauginti jokiu būdu ir priemonėmis komercinės (gamybinės) paslapties ar jos dalies, be atsakingų darbuotojų leidimo tyčia ją nusikopijavo ir įrašė į išorinę laikmeną, t. y. įgijo neviešus elektroninius duomenis“.[232] Esminis nagrinėjamos bylos klausimas buvo susijęs ar teismai teisingai nustatė šios nusikalstamos veikos sudėties požymius. Teisėjų kolegija tenkindama nuteistojo gynėjo kasacinį skundą ir nutraukdamas baudžiamąją bylą, išskyrė kelis reikšmingus aspektus. „Tais atvejais, kai kaltininkas, esant teisiniams santykiams (pavyzdžiui, darbiniams ar kitokiems sutartiniams teisiniams santykiams), turi galimybę prieiti prie neviešos informacinės sistemos ar duomenų, jo tyčinio veikimo (poveikio) neteisėtumas turi būti nustatomas aiškiai nurodant, kokius teisės aktus jis pažeidė, kokių draudimų, susitarimų,

[230] „Nutartis baudžiamojoje byloje 2K-262-489/2022“, *supra note*, 218.
[231] *Ibid*.
[232] „Nutartis baudžiamojoje byloje 2K-214-489/2024“, *supra note*, 221.

įgaliojimų tyčia nesilaikė“. [233] Tačiau nagrinėjome byloje Nr. 2K-214-489/2024 abiejų instancijų teismai nenustatė, iš kokių bendrovės vidaus teisės aktų ar sutarčių išplaukia darbuotojo teisė kopijuoti ir įrašyti į išorines laikmenas informaciją, sudarančią komercinę paslaptį, tik esant įmonės atsakingų darbuotojų leidimui. Na, o vertindama neteisėtumo aspektą, t. y. konfidencialumo nesilaikymo susitarimą, teisėjų kolegija pažymėjo, kad teismai nepakankamai kreipė dėmesio į tai, kad susitarimo tarp darbuotojo ir bendrovės minėta taisyklė nėra besąlyginė, nes joje yra nurodyta išlyga, kada tokie darbuotojo veiksmai yra galimi, t. y. kopijuoti ir dauginti informaciją leidžiama tais atvejais, kai tai reikalinga komercinės (gamybinės) paslapties pateikimo tikslui įgyvendint.[234] Kasacinio teismo praktikoje laikomasi nuomonės, kad „sudarant sutartis dėl materialinių vertybių tarp asmenų paprastai atsiranda civiliniai teisiniai santykiai, kurie gali peraugti į baudžiamuosius teisinius santykius tik esant tam tikroms papildomoms sąlygom“.[235] Tačiau byloje kaltinamojo atžvilgiu tuo buvo nesivadovaujama, tai yra nebuvo nustatyta, kad gynimas civilinio proceso tvarka būtų apsunkintas.

Nagrinėjamoje LAT nutartyje 2K-214-489/2024 buvo išaiškinta, kad „byloje nuo pat ikiteisminio tyrimo pradėjimo momento buvo būtina nustatyti teisinio santykio, iš kurio kilo ginčas tarp bendrovės ir darbuotojo, prigimtį ir pobūdį, įvertinti, kokiomis teisės normomis vadovaujantis sprendžiamas“. [236] Todėl tarp konfidencialumo įsipareigojimą pasirašiusių šalių kilę ginčai ir galimi konfidencialumo įsipareigojimo pažeidimai turėjo būti sprendžiami ta tvarka, dėl kurios yra susitarta, nesant pagrindo taikyti griežčiausią teisinės atsakomybės rūšį – baudžiamąją atsakomybę, nes susiklostęs byloje teisinis ginčas turi būti sprendžiamas pirmiausia civilinės teisės gynimo priemonėmis.[237] Byloje taip pat aktualu, kad asmens veiksmai, susiję su komercinės paslapties įgijimu, kriminalizuoti ne BK 198 straipsnyje, o BK 210 straipsnyje. Tačiau dėl to tarnybiniu pranešimu nusikalstama veika, kvalifikuota pagal BK 211 straipsnį, perkvalifikuota pagal BK 198 straipsnio 1 dalį, nenustačius, kad konfidencialūs elektroniniai duomenys buvo atskleisti kitai įmonei.[238]

Apibendrinant nagrinėtą baudžiamąją bylą, konstatuotina, kad kvalifikavimo problema buvo susijusi su neteisėtumo požymio nustatymu tais atvejais, kai asmuo turi teisėtą prieigą prie elektroninių duomenų. Pirmosios ir apeliacinės instancijos teismai netinkamai aiškino ir taikė BK

---

[233] „Teismų praktika biuletenis Nr. 62“, Lietuvos Aukščiausiasis Teismas, žiūrėta 2026 m. balandžio 20 d., https://www.lat.lt/data/public/uploads/2025/09/teismu_praktika_nr_62.pdf.
[234] „Nutartis baudžiamojoje byloje 2K-214-489/2024“, *supra note*, 221.
[235] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 26 d. nutartis baudžiamojoje byloje Nr. 2K-46-699/2018“, LITEKO, žiūrėta 2025 m. kovo 14 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=7d67b8c5-779f-4d0e-ac1a-2cbe17b92f57.
[236] „Nutartis baudžiamojoje byloje 2K-214-489/2024“, *supra note*, 221.
[237] „Teismų praktika biuletenis Nr. 62“, *op.cit*.
[238] *Ibid.*

198 straipsnio 1 dalį, nes neįrodė, kokius konkrečius teisės aktus ar susitarimus kaltinamasis pažeidė, taip pat neatsižvelgė į konfidencialumo įsipareigojime numatytas išimtis, leidžiančias duomenų kopijavimą darbo funkcijų vykdymo tikslais. Be to, buvo nustatyta, kad konfidencialumo įsipareigojimo pažeidimai turi būti sprendžiami ta tvarka (civilinės teisės gynimo priemonėmis.), dėl kurios yra susitarta, nesant pagrindo taikyti baudžiamąją atsakomybę.

Vilniaus apskrities vyriausiojo policijos komisariato oficialioje interneto svetainėje buvo pateikta informacija, kurioje nurodoma, kad byla buvo perduota teismui pagal LR BK 198 str. 1 d., 198[1] str. 1 d., už tai, kad asmuo „neteisėtai – pasinaudodamas jam žinomais prisijungimo duomenimis, nedirbamas įmonėje ir nevykdydamas savo tiesioginių darbo funkcijų, neturėdamas įmonės sutikimo ir taip pažeisdamas informacinės sistemos apsaugos priemones, prisijungė prie įmonei priklausančios elektroninės pašto dėžutės ir įmonės naudojamos dokumentų valdymo ir saugojimo sistemos bei prisijungimo laiku neteisėtai – neturėdamas dokumentų valdymo ir saugojimo sistemos naudotojo sutikimo, stebėjo sistemoje patalpintus neviešus elektroninius duomenis.[239] Priešingai nei LAT bylose (2K-262-489/2022 ir 2K-214-489/2024), kuriose dėl teisėtos prieigos prie duomenų nebuvo tinkamai nustatytas neteisėtumo požymis, nagrinėjamu atveju konstatuota, kad asmens veiksmai buvo neteisėti, nes jis prie duomenų bazių jungėsi jau nutraukus darbo santykius.

Taip pat internete paskelbtame pranešime buvo nurodyta, kad įmonės „vengia investuoti į informacinių technologijų ir sistemų apsaugą, todėl tokie atvejai teisėsaugos praktikoje nėra vienetiniai. Visų įstaigų, įmonių vadovai ar kiti atsakingi darbuotojai, nutraukdami darbo santykius su darbuotojais, nedelsdami turėtų panaikinti prieigą prie įmonės informacinių sistemų ar pakeisti prisijungimo duomenis“.[240]

Išnagrinėjus policijos pranešimą, apie perduota bylą į teismą, nustatyta, praktinė problema, kad įmonės nesiimdamos priemonių užtikrinti jų duomenų saugumą (keisti slaptažodžius, panaikinti buvusiu darbuotojų prisijungimo duomenis), sudaro prielaidas asmenims paveikti įmonės duomenis.

LAT byloje Nr. 2K-45-697/2026 A. Š.-G. nuteista pagal BK 198[1] straipsnio 1 dalį už tai, kad tyčia pažeidė informacinės sistemos apsaugos priemonę – kompiuterio įeigos slaptažodį ir taip neteisėtai prisijungė prie kompiuterio informacinės sistemos. Kasacinio skundo argumentai, kad žemesnės instancijos teismai netinkamai pritaikė baudžiamąjį įstatymą ir nepagrįstai nuteisė pagal

[239] „Dar viena byla dėl nusikaltimų elektroninėje erdvėje perduota teismui“, Vilniaus apskrities vyriausiasis policijos komisariatas, žiūrėta 2026 m. balandžio 10 d.,https://vilnius.policija.lrv.lt/lt/naujienos/dar-viena-byla-del-nusikaltimu-elektronineje-erdveje-perduota-teismui/.
[240] *Ibid*.

BK 198[1] straipsnio 1 dalį, buvo atmesti. [241] Byloje nustatyta, kad kaltinamoji nežinodama prisijungimo duomenų ir neturėdama sistemos valdytojo leidimo, prisijungė prie nukentėjusiojo kompiuterio, taip pažeisdama informacinės sistemos apsaugos priemones (slaptažodį). Šioje byloje teismas pabrėžė, kad neteisėtumas siejamas su prisijungimu be leidimo, nepriklausomai nuo nuosavybės teisės į įrenginį („nusikaltimu kėsinamasi ne į nuosavybę, o į elektroninių duomenų ir informacinių sistemų saugumą)“.[242] Todėl šioje byloje priešingai nei prieš tai nagrinėtose (2K-4-507/2016, 2K-214-489/2024), buvo tinkamai pagrįstas neteisėtumo požymis.

LAT byloje 2K-555-788/2015 iškilo problematika dėl veikos kvalifikavimo pagal BK 198[1] straipsnio 1 dalį. Prokuroras Kasaciniame skunde nesutiko su tuo, kad kaltinamasis buvo išteisintas pagal BK 198[1] straipsnio 1 dalį, tai yra, kad prie „informacinių sistemų neteisėtai jungėsi naudodamasis tikrais, nors ir neteisėtai gautais elektroninių mokėjimo priemonių naudotojo tapatybės patvirtinimo veiksmais ir informacinių sistemų apsaugos priemonių nepažeidė (nebuvo sudėties požymių)“. [243] Prokuroras teigė, kad teismų išvada, kad asmuo atlikęs kaltinime nurodytus veiksmus, nepažeidė informacinės sistemos apsaugos priemonių, neteisinga, kadangi elektroninėje erdvėje vykdomas sukčiavimas, panaudojant svetimus elektroninės mokėjimo priemonės duomenis, tarp jų ir prisijungimo kodus, neįmanomas be neteisėto prisijungimo prie informacinės sistemos – kito asmens banko sąskaitos, t. y. nepadarius atskiro baigto nusikaltimo, numatyto BK 198[1] straipsnio 1 dalyje. Pasak prokuroro teismas taip pat nepagrįstai nurodė, kad šį straipsnį galima taikyti tik tada, kai, jungdamasis prie informacinės sistemos, kaltininkas siekia pamatyti informacinės sistemoje laikomas duomenų bylas, susipažinti su duomenų turiniu, atlikti kitus veiksmus (juos keisti, trinti, kopijuoti ir t. t.), kad neteisėtai jungdamasis prie informacinės sistemos.[244] Kasacinio teismo praktikoje yra numatyta, kad asmuo „vykdydamas šios kategorijos nusikalstamas veikas kaltininkas iš pradžių neteisėtai įgyja nukentėjusiojo elektroninės mokėjimo priemonės duomenis (BK 214 straipsnis), po to, pasinaudodamas šiais neteisėtai įgytais duomenimis, pažeisdamas informacinės sistemos apsaugos duomenis, t. y. save identifikuodamas kaip teisėtą duomenų naudotoją, prisijungia prie internetinės bankininkystės sistemos (198[1] straipsnis) ir atlieka neteisėtas finansines operacijas, pervesdamas pinigus iš nukentėjusiojo banko

[241] „Lietuvos Aukščiausiojo Teismo 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-45-697/2026“, LITEKO, žiūrėta 2025 m. sausio 19 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=eb98a3a4-f7b8-49ce-a392-85a9263ce010.
[242] „Nutartis baudžiamojoje byloje Nr. 2K-45-697/2026“, *op.cit.*
[243] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gruodžio 8 d. nutartis baudžiamojoje byloje Nr. 2K-555-788/2015“, LITEKO, žiūrėta 2025 m. sausio 28 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=c82c82f2-9d67-4971-be81-bd574e1aa5a0.
[244] *Ibid.*

sąskaitos į savo ar juos paimdamas grynais pinigais, ir taip apgaule įgyja svetimą turtą[245]“ Kasacinis teismas dėl veikos kvalifikavimo pagal BK 198[1] straipsnio 1 dalį, nurodė kad „teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir atitinka neteisėto prisijungimo prie informacinės sistemos veikos padarymo būdą“. [246] Todėl BK 198[1] straipsnio 1 dalies inkriminavimas nagrinėjamoje byloje buvo reikalingas.

Baudžiamojoje byloje Nr. 2K-4-507/2016 asmuo taip pat išteisintas pagal BK 198[1] straipsnio 1 dalį dėl kaltinimo, kad jis naudodamasis kompiuteriu per interneto prieigas, neteisėtai, pažeisdamas, t. y. suklaidindamas, informacinės sistemos apsaugos priemones, įvesdamas neteisėtai įgytus nukentėjusiosios D. B. vardu išduotus internetinės prieigos duomenis – elektroninės bankininkystės vartotojo identifikavimo kodą, asmeninį prisijungimo slaptažodį, prisijungimo prie elektroninės bankininkystės banko suteiktus slaptažodžius, prisijungė prie informacinės sistemos. Pirmosios instancijos teismo nuosprendžiu E. J. taip pat nuteistas pagal BK 182 str. 1 d., 214 str. 1 d., 215 str., 1 d. [247] Kasatorius tai yra prokuroras teigė, kad teismai netinkamai pritaikė baudžiamąjį įstatymą pagal BK 198[1], nes bankų elektroninės bankininkystės sistemos atitinka informacinės sistemos požymius. [248] BK informacinės sistemos sąvoka nėra apibrėžta pačiame kodekse, todėl ji aiškinama remiantis tarptautiniais ir Europos Sąjungos teisės aktais. Konvencijoje dėl elektroninių nusikaltimų, kompiuterinė sistema - „tai įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis“.[249] Direktyvoje dėl atakų prieš informacines sistemas, įvirtinta, kad informacinė sistema – tai „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais.“[250] Prokuroras taip pat nesutiko su apeliacinės instancijos teismo išvadomis, „dėl BK 198[1] str. 1 d., kaip bendrosios, ir BK 215 straipsnio 1 dalies, kaip specialiosios, normų konkurencijos, teigia, kad šios dvi normos saugo skirtingus teisinius gėrius: BK 198[1] straipsnio objektas –informacinių sistemų bei jose esančių elektroninių duomenų saugumas (konfidencialumas), BK 215 straipsnio – teisės

---

[245] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. birželio 26 d. nutartis baudžiamojoje byloje Nr. 2K-375/2012“, LITEKO, žiūrėta 2025 m. vasario 12 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=57620acd-4a52-40c8-8ef7-7176a7989480.
[246] „Nutartis baudžiamojoje byloje Nr. 2K-555-788/2015“, *supra note,* 243.
[247] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. sausio 26 d. nutartis baudžiamojoje byloje Nr. 2K-4-507/2016“, LITEKO, žiūrėta 2025 m. vasario 18 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=1fdbcaf1-a5e2-41cc-8d4b-944c5a14eefc.
[248] *Ibid*.
[249] „Konvencija dėl elektroninių nusikaltimų“ (ETS Nr. 185), *supra note*, 102.
[250] „Europos Parlamento ir Tarybos direktyva 2013/40/ES“, *supra note,* 111.

aktais įtvirtinta elektroninių mokėjimo priemonių naudojimo ir disponavimo tvarka.“ [251]Teismas sutiko su prokuroro pateiktais kasacinio skundo teiginiais.

Nagrinėtoje byloje 2K-555-788/2015 yra išaiškinta, kad veika turi būti kvalifikuojama pagal BK 198[1] straipsnį nustačius, kad prie informacinės sistemos buvo prisijungta pažeidžiant šios sistemos apsaugos priemones. „Aiškinant informacinės sistemos apsaugos priemonių pažeidimo požymį, kasacinėse nutartyse pažymėta:

1) vartotoją informacinėje sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių,

2) teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir

3) neteisėtas prisijungimas prie informacinės sistemos (internetinės bankininkystės sistemos) pažeidžiant autentifikavimo priemonėmis nustatytų prisijungimo prie informacinės sistemos apribojimus (reikalavimus) paprastai negali būti laikomas nereikšmingu, vertinant jį iš baudžiamosios teisės pozicijų, ypač jei tai leido padaryti kitus neteisėtus veiksmus sistemoje“.[252]

Byloje nuteistojo veiksmai, atitinka ir BK 198[1] straipsnio 1 dalyje numatytos nusikalstamos veikos požymius, o veikos (veikų) kvalifikavimas pagal BK 215 straipsnį nepašalina veiksmų neteisėtai prisijungiant prie informacinės sistemos kvalifikavimo pagal BK 198[1] straipsnį galimybės. Tai patvirtina ir Kasacinio teismo nutartis Nr. 2K-138/2015, kad „neteisėtas prisijungimas BK 198[1] straipsnyje turi būti kriminalizuojam kaip savarankiška nusikalstama veika, t. y. be tiesioginio ryšio su kitomis jau sistemoje padaromomis veikomis“.[253]

Nagrinėtose LAT bylose 2K-555-788/2015, 2K-4-507/2016, asmenims buvo nepagrįstai netaikomas BK 198[1] straipsnis. Tačiau nagrinėjant LAT byloje 2K-157-895/2020, nustatyta, kad asmuo teigė, kad buvo nepagrįstai „nuteistas pagal BK 198[1] straipsnio 1 dalį ir BK 215 straipsnio 1 dalį, nes jis turėjo S. G. leidimą panaudoti jos elektroninę mokėjimo priemonę ir prisijungti prie informacinės sistemos, o po S. G. mirties prie sistemos prisijungė kaip verslo ir sąskaitose sukauptų lėšų bendraturtis. Taigi, pasak kasatoriaus, prisijungimui panaudoti duomenys buvo teisingi ir gauti teisėtai“. [254]Tačiau šie argumentai teismo buvo atmesti ir Kasacinis teismas nurodė, kad „baudžiamasis įstatymas pritaikytas tinkamai, jo padaryta nusikalstama veika –

---

[251] „Nutartis baudžiamojoje byloje Nr. 2K-4-507/2016“, *op. cit.*
[252] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gruodžio 8 d. nutartis baudžiamojoje byloje Nr. 2K-555-788/2015“, LITEKO, žiūrėta 2025 m. sausio 19 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=c82c82f2-9d67-4971-be81-bd574e1aa5a0.
[253] *Ibid*.
[254] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. birželio 9 d. nutartis baudžiamojoje byloje Nr. 2K-157-895/2020“, LITEKO, žiūrėta 2025 m. kovo 30 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=6f9576fa-606f-496d-93ed-247e29295dda.

neteisėtas prisijungimas prie banko elektroninės bankininkystės, neteisėtai įvedant mirusios S. G. tapatybę patvirtinančius duomenis, taip suklaidinant šią sistemą, teisingai kvalifikuota pagal BK 198[1] straipsnio 1 dalį“.[255]Taikant šią nuostata yra įtvirtinta, kad „aiškinant informacinės sistemos apsaugos priemonių pažeidimo požymį, ne kartą atkreiptas dėmesys, jog vartotoją informacinėje sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių. O teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir atitinka neteisėto prisijungimo prie informacinės sistemos veikos padarymo būdą“.[256]

Byloje Nr. 2K-199-648/2019 asmuo buvo nuteistas pagal BK 198[2] str., 1 d., dėl to, kad įgijo bei laikė įrangą, kuri yra skirtą slaptažodžiams keisti ir (ar) šalinti. Taip pat asmuo nuteistas pagal BK 198[1] str. 1 d. ir BK 198 str. 1 d., už tai, kad „darbo vietoje, naudodamas programa, neteisėtai prisijungė prie kompiuterio, pašalino administratoriaus slaptažodį, sukūrė naują slaptažodį ir papildomą vartotojo paskyrą taip pažeisdamas informacinės sistemos apsaugą bei neteisėtai perimdamas ir panaudodamas neviešus elektroninius duomenis“. [257] Kasaciniame skunde, teigta, kad byloje „neįrodyti BK 198[2] str., 1 d. nusikalstamos veikos subjektyvieji požymiai, kad veikė tiesiogine tyčia ir įgijo bei laikė programinę įrangą turėdamas tikslą daryti nusikalstamas veikas. BK 198[2] numatyta atsakomybė už neteisėtą disponavimą įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis“[258]. Teismų praktikoje yra išaiškinta, kad „BK 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. Tačiau siekiant išvengti nepagrįsto baudžiamosios atsakomybės taikymo, kai tokios priemonės yra pagamintos ir pateiktos vartotojams teisėtiems tikslams (pavyzdžiui, skirtos informacinių technologijų produktų patikimumui, saugumui testuoti), būtina nustatyti tiesioginį ketinimą panaudoti tokias priemones nusikalstamai veikai daryti“. [259] Nagrinėjamoje byloje nenustatyta, kad įsigydamas programinę įrangą, turėjo tikslą ją panaudoti nusikalstamais tikslais. Programa buvo įgyta teisėtai, vykdant kompiuterių remonto veiklą, o neteisėtas jos panaudojimas

---

[255] *Ibid.*

[256] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2019 m. gruodžio 10 d. nutartis baudžiamojoje byloje Nr. 2K-314-895/2019“, LITEKO, žiūrėta 2025 m. kovo 30 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=7fb54312-36da-4157-b6b9-03d6989a7f2f.

[257] „Lietuvos Aukščiausiojo Teismo 2015 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019“, LITEKO, žiūrėta 2025 m. kovo 14 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=26323413-d1e7-491a-9d15-673638b54d6f.

[258] *Ibid*

[259] „Teismų praktika biuletenis Nr. 52“, Lietuvos Aukščiausiasis Teismas, žiūrėta 2026 m. balandžio 20 d., https://www.lat.lt/data/public/uploads/2020/07/d1_teismu_praktika_nr_52.pdf .

įvyko tik po beveik metų. Tačiau teismas nustatė, kad asmuo įsidiegė programą ir ją laikė ir panaudojo neteisėtai prisijungdamas prie sistemos. Kadangi asmuo neturėjo teisės naudoti šios programos ir jos naudojimas nebuvo susijęs su jo teisėta veikla, konstatuota, kad programinė įranga buvo laikoma nusikalstamais tikslais, veikiant tyčia.[260] Taigi, teismas atsižvelgęs į nustatytas aplinkybes, iš veikos pagal BK 198² str. 1 d., pašalino aplinkybę dėl programinės įrangos įgijimo nusikalstamoms veikoms daryti.

Priešingai nei ankstesniuose bylose, pirmosios ir apeliacinės instancijos teismai teisingai įvertino, neteisėtumo požymį. Pagal byloje esamas aplinkybes, nustatyta, kad „kaltinamasis prie kompiuterio prisijungė panaudodamas programinę įrangą, sudariusią jam galimybę gauti specialų, sistemos apribojimus apeinantį ir jos nustatytoms funkcijoms prieštaraujantį prieigos prie jos kelią. Informacinės sistemos veikimo ypatumai prie jos prisijungiant E. J. nebuvo naudojami taip, kaip darbuotojams leido šioje sistemoje nustatytos funkcijos. Būtent tokiu darbuotojams nenumatytu būdu prisijungus prie informacinės sistemos buvo gautos paskyros „Administrator“ vartotojo teisės“.[261] Tad toks prisijungimas buvo laikomas neteisėtu. Kasaciniame skunde taip pat teigiama, kad E. J. neperėmė ir nepanaudojo neviešų elektroninių duomenų, o administratoriaus teisės nelaikytinos tokiais duomenimis, todėl nėra BK 198 straipsnio sudėties. Šiuo atveju nustatyta, kad įgytos administratoriaus teisės nelaikytinos neviešais elektroniniais duomenimis, o jų gavimas siejamas su neteisėtu prisijungimu (BK 198¹ str.).

Taigi, byloje nebuvo nustatyta, kad asmuo būtų perėmęs ar panaudojęs kitus neviešus elektroninius duomenis, nusikalstamos veikos pagal BK 198 straipsnį sudėtis neįrodyta. Apibendrinant, nustatyta, kad teismai iš dalies netinkamai vertino BK 198² straipsnio aplinkybes, kadangi buvo nustatyta, kad programinė įranga buvo teisėtai įgyta (kaip dvigubo naudojimo priemonė), todėl neįrodytas pirminis tikslas ją naudoti nusikalstamai. Tačiau jos laikymas ir panaudojimas nusikalstamai veiklai buvo nustatytas. Kasacinis teismas patvirtino, kad asmuo neteisėtai prisijungė prie sistemos, nes sąmoningai apeidamas techninius apribojimus įgijo administratoriaus teises, nors tokių įgaliojimų neturėjo. Tuo tarpu dėl BK 198 straipsnio konstatuota, kad administratoriaus teisės nelaikytinos neviešais elektroniniais duomenimis.

Baudžiamojoje byloje Nr. 2K-188-489/2015, asmuo buvo nuteistas: pagal BK 198² str. 1 d., – už programinės įrangos, skirtos DDoS atakoms ir interneto serverių skenavimui, įsigijimą ir laikymą; pagal BK 197 str. 3 d., už kibernetines atakas prieš tinklapius vykdymą. LAT šioje byloje pasisakė, keliais apsektais: [262]

---

[260] „Nutartis baudžiamojoje byloje Nr. 2K-45-697/2026“, *supra note*, 241.
[261] „Nutartis baudžiamojoje byloje 2K-199-648/2019“, *supra note,* 257.
[262] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015“, LITEKO, žiūrėta 2025 m. vasario 12 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9b3513d4-6e5a-43a4-bc24-14cebf44c4b2..

1. „Apeliacinės instancijos teismas netinkamai atskleidė BK 198^1 straipsnio 1 dalyje numatytą prisijungimo pažeidžiant informacinės sistemos apsaugos priemones požymį, taigi nepagrįstai išaiškino, kad baudžiamoji atsakomybė už neteisėtą „SQL Injection“ tipo atakos panaudojimą (siekiant aptikti saugumo spragas) BK apskritai nenumatyta“.[263]

2. „Apeliacinės instancijos teismo išvados, kad neįrodyta, jog nuteistasis dalyvavo padarant kaltinime nurodytas dvi nusikalstamas veikas (dėl programinės įrangos DDoS atakoms vykdyti įsigijimo bei laikymo ir dėl programinės įrangos interneto tarnybinėms stotims skenuoti įsigijimo ir laikymo), kurios pirmosios instancijos teismo kvalifikuotos pagal BK 198^2 straipsnio 1 dalį, yra neteisingos.“ [264] „Šiuo aspektu aktualu tai, kad tiesiogiai nusikalstamoms veikoms daryti skirtos priemonės neturėtų būti tapatinamos tik su specialiai pritaikytomis priemonėmis. Esant minėtam tikslui, dvigubo naudojimo priemonės pasitelkiamos konkrečiai nusikalstamai veikai daryti, todėl ir tampa tiesiogiai skirtos šiai veikai daryti. Teisėjų kolegija pažymi, kad esant nustatytam tikslui daryti nusikalstamą veiką, šių priemonių įgijimas ar laikymas kelia grėsmę elektroninių duomenų ir informacinių sistemų saugumui. Atsižvelgiant į tai, konstatuotina, kad apeliacinės instancijos teismas BK 198^2 straipsnyje nurodytą dalyką aiškino per siaurai, neatkreipė dėmesio į dvigubo naudojimo priemonių specifiką ir padarė neteisingą išvadą, kad A. V. P. P. perduota programinė įranga nėra BK 198^2 straipsnio 1 dalyje numatytos nusikalstamos veikos dalykas“.[265]

3. Dėl BK 197 straipsnyje numatytų požymių – žalos ir neteisėtumo – aiškinimo. „Kasacinio teismo teisėjai, teigė, kad apeliacinės instancijos neįvertino žalos dydžiui nustatyti reikšmingų aplinkybių visumos, kad: DDos atakomis buvo trikdomas tinklalapių, susijusių su visuomenės informavimu, darbas; šiomis atakomis sukelta problemų tinklalapių funkcionavimui; intensyvi DDos ataka truko keletą dienų, jos padariniai likviduoti ne iš karto; panaudotos DDos atakos mechanizmas sudėtingas, atakos kompleksinės, kintančios; trikdymams sukelti naudotas didelis užkrėstų kompiuterių tinklas (botnet tinklas)“.[266]

4. Apeliacinės instancijos teismas rėmėsi CK 6.246 straipsnio 1 dalimi ir neteisėtumo sąvoką sutapatino su CK vartojama sąvoka. Neteisėtumo požymio aiškinimui nagrinėjamoje byloje turėjo remtis Direktyva 2013/40/ES dėl atakų prieš informacines sistemas. Šiame teisės aktuose požymis neturint tam teisės „reiškia veiksmus, kuriems nėra suteiktas sistemos ar jos dalies savininko (valdytojo) leidimas arba kurio neleidžia nacionalinės teisės aktai“.[267]

---

[263] *Ibid*.
[264] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015“, *supra note*, 262.
[265] *Ibid.*
[266] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015“, *supra note,* 262.
[267] „Europos Parlamento ir Tarybos direktyva 2013/40/ES“, *supra note,* 111.

5. Dėl baudžiamosios jurisdikcijos įgyvendinimo. Šioje byloje nustatyta, kad sistemos darbo sutrikdymas buvo fiksuotas Švedijoje. Tačiau organizuotos DDos atakos prieš tinklalapius buvo įvykdytos Lietuvos Respublikoje. Taigi, kasatorės nuomone, kilo abejonių, ar Lietuvos Respublikos teismai turėjo jurisdikcijos teisę nagrinėti baudžiamąją. Byloje teisėjų kolegija konstatavo, kad Lietuvos Respublikos jurisdikcija šioje byloje įgyvendinta tinkamai. Nagrinėjant jurisdikcijos įgyvendinimo abejones buvo nustatyta, kad Pagal BK 4 str. 2 d., „nusikalstamos veikos padarymo vieta yra vieta, kurioje asmuo veikė arba turėjo ir galėjo veikti, arba vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai“. [268] Šią nuostatą pagrįsti galima ir Direktyva 2013/40/ES dėl atakų prieš informacines sistemas „a) pažeidėjas nusikalstamą veiką įvykdo fiziškai būdamas jos teritorijoje, nepriklausomai nuo to, ar nusikalstama veika yra nukreipta ar nenukreipta prieš jos teritorijoje esančią informacinę sistemą; arba b) nusikalstama veika yra nukreipta prieš jos teritorijoje esančią informacinę sistemą nepriklausomai nuo to, ar pažeidėjas nusikalstamą veiką daro fiziškai būdamas jos teritorijoje“.[269]

Taigi, byloje nustatyta problematika buvo susijusi su netinkamu nusikaltimų požymių aiškinimu – ypač dėl neteisėto prisijungimo, dvigubo naudojimo priemonių vertinimo, žalos dydžio nustatymo. Taip pat iškilo problemų aiškinant neteisėtumo sampratą. Atsakant į kasacinį skundą buvo išsiaiškintas jurisdikcijos taikymo klausimas.

Kasacinėse nutartyse Nr. 2K-4-507/2016, 2K-199-648/2019, 2K-27-976/2023, 2K-45-697/2026, yra įtvirtinta pozicija dėl BK 37 straipsnio taikymo neteisėto prisijungimo prie informacinės sistemos mažareikšmiškumo aspektu. Pagal BK 37 str. „asmuo, padaręs baudžiamąjį nusižengimą, neatsargų, nesunkų ar apysunkį nusikaltimą, gali būti teismo atleistas nuo baudžiamosios atsakomybės, jeigu dėl padarytos žalos dydžio, nusikalstamos veikos dalyko ar kitų jos požymių ypatumų veika pripažįstama mažareikšme.“[270]Tačiau dėl XXX skyriuje numatytų veikų, kasacinės instancijos teismo praktikoje yra išaiškinta, kad neteisėtas prisijungimas prie informacinės sistemos paprastai negali būti laikomas nereikšmingu, vertinant iš baudžiamosios teisės pozicijų, ypač jeigu toks prisijungimas leido padaryti kitus neteisėtus veiksmus sistemoje.[271]

Kasacinės instancijos teismo praktikoje pripažįstama, kad nustatant nagrinėjamai bylai reikšmingas aplinkybes specialiųjų žinių panaudojimas yra tinkama įrodinėjimo priemonė. [272]Tai patvirtina ir Baudžiamojoje byloje Nr. 1A-477-498/2016, nustatytos aplinkybes. Pagal BK 196 str., 3 d., 197 str. 3 d., 198 str., 1 d., 198-1 str. 1 d., asmuo nuteistas už tai, kad „panaudodamas

---

[268] „Lietuvos Respublikos baudžiamasis kodeksas“, *supra note*, 215.
[269] „Europos Parlamento ir Tarybos direktyva 2013/40/ES“, *supra note,* 111.
[270] „Lietuvos Respublikos baudžiamasis kodeksas“, *supra note*, 215.
[271] „Nutartis baudžiamojoje byloje Nr. 2K-45-697/2026“, *supra note*, 241.
[272] Lietuvos Aukščiausiasis Teismas, „2019 m. kovo 28 d. Baudžiamojo proceso kodekso normų, reglamentuojančių specialiųjų žinių panaudojimą, taikymo teismų praktikoje apžvalga“, žiūrėta 2026 m. balandžio 10 d., https://www.lat.lt/lat-praktika/lat-praktikos-tam-tikrose-teises-srityse-apzvalgos/baudziamuju-bylu-apzvalgos/68

personalinį kompiuterį, priklausantį interneto klientei ir panaudodamas kompiuterinę programinę įrangą pažeisdamas informacinės sistemos apsaugos priemones, neteisėtai, be žinios ir sutikimo, įsilaužė į klientės nuomojamus serverius ir perėmė juose saugomus neviešus elektroninius duomenis, taip pat sunaikino serverių naudotojų elektroninius duomenis, serverio failus, statistiką bei iš kliento serverio atakavo kitus serverius bei pakeitė prisijungimo ir valdymo slaptažodžius ir taip apribojo naudojimąsi duomenimis ir neteisėtai sutrikdė informacinės sistemos darbą“.[273]

Nuteistasis šioje byloje apeliaciniu skundu pageidavo panaikinti esamą teismo nuosprendį ir bylą nutraukti. Vienas iš argumentų buvo, kad teismas netinkamai vertino Lietuvos ekspertizės centro specialisto išvadą. Apeliacinis teismas dėl įrodymų vertinimo, teigė, kad nusikalstamos veikos tyčios turinį įrodo, byloje esanti medžiaga, nukentėjusiojo parodymai, *specialisto išvada*. Specialisto išvadoje, buvo pateikta „ kaltinamojo pokalbių per programą „Skype“ istorija, kurioje buvo matyti, kad nuteistasis nežinomam pašnekovui pasakoja kaip jis nusikopijavo serverių failus- kaip pakeitė vps (virtualių privačių serverių) slaptažodžius, pasidalino informacija su nežinomu asmeniu, informacijos prašė neplatinti. Tad teismas padarė išvadą, kad įsilaužęs į nukentėjusiojo serverį jis žinojo, kad perima konfidencialią informaciją susijusią nukentėjusiojo klientų mokėjimais, užsakymais, tame tarpe klientų asmens duomenis ir tai darė sąmoningai, t. y. suvokė, kad jo perimama informacija yra nevieši duomenys.

Skunde buvo iškeltas klausimas, kaip su standartine įranga „(PuTTY, TightVNC) kaltinamasis galėjo pažeisti informacinės sistemos apsaugos priemones ir įsilaužti į serverius, atsakytas specialisto parodymais. „Specialistas byloje nurodė, kad žinant slaptažodžius, juos prieš tai neteisėtai gavus, tai toks prisijungimas su išvardintomis priemonėmis yra galimas.“[274] Byloje apelianto argumentai, jog jis į savo kompiuterį parsisiųsdamas duomenų bazę atsisiuntė ir virusą, kuris už jį padarė visus veiksmus paneigta specialisto išvada, specialisto parodymais duotais pirmos ir apeliacinės instancijos teismuose, byloje esančiu pokalbiu per Skype programą. Specialistas, nurodė, kad nuteistojo kompiuterio standžiame diske nebuvo rasta virusų ar kitų kenkėjiškų programų, kurie aktyvuotųsi įjungiant kompiuterį ir galėtų savarankiškai pakenkti, dar kartą patvirtino specialistas nurodydamas, kad nors kompiuteryje buvo rasta virusų, tačiau nei vienas pats savaime nesiaktyvuoja, vartotojui neatlikus papildomų veiksmų. [275]Taigi išanalizavus bylą galima daryti išvadą, kad specialisto vaidmuo buvo svarbus ir reikšmingas ko pasėkoje leido pagrįsti kaltinamojo tyčios turinį, paneigti apeliaciniame skunde nurodytas versijas ir tinkamai įvertinti technines nusikalstamos veikos aplinkybes. Tai rodo, kad kibernetinių (elektorininių)

[273] „Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2016 m. gruodžio 21 d. nutartis baudžiamojoje byloje Nr. 1A-477-498/2016“, LITEKO, žiūrėta 2025 m. balandžio 16 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=ed6b4b34-8972-4060-b90d-5677c455bb46.
[274] *Ibid*.
[275] *Ibid.*

nusikaltimų bylose specialisto žinios yra svarbios ir būtinos tinkamam įrodymų vertinimui ir nusikalstamos veikos kvalifikavimui.

Byloje Nr. 1-2663-917/2018, „buvo nustatyta, kad kaltinamasis subūrė ir vadovavo organizuotai asmenų grupei, kurios nariai buvo susitarę daryti neaptartą skaičių nusikalstamų veikų – sukčiauti, apgaule įgyjant Lietuvoje veikiančių bankų klientų sąskaitose esančias pinigines lėšas, ir dalyvavo šios organizuotos asmenų grupės veikloje kartu su M. P., A. B., P. Ž., T. B., A. C., V. G., A. A., I. Č., ir ikiteisminio tyrimo metu nenustatytu asmeniu.“[276] Taigi, iš kaltinamo matyti, kad nagrinėjant tokio pobūdžio bylas iškyla problema nustatyti visus asmenis dalyvaujančius nusikalstamoje veikoje. Tačiau byloje galima išskirti dar keletą ypatumų bylose elektroninių duomenų ir informacinių sistemų saugumui, vadovaujantis liudytojos parodymais tuo metu dirbusios banke „Swedbank“. Liudytoja paaiškino, kad „klientų kompiuteriuose buvo instaliuotos kenkėjiškos programos, kurios nukreipdavo interneto banko vartotojus į kitus puslapius, kuriuose buvo surenkami klientų slaptažodžiai ir pateikiami kažkam. Klientai nežinodavo, kad patenka į kenkėjiškas programas, jie suvesdavo savo kodus, galvodavo, kad susisiekia su banku. Žmogus, kuris naudodavosi kenkėjiška programa sužinodavo kliento prisijungimo kodus. Pasinaudojant kenkėjiškomis programomis asmenų pinigai buvo pervesti į kitų asmenų sąskaitas jiems to nežinant. Pas banko klientą, kuris pasinaudojo suklastotu puslapiu tas suklastotas puslapis atsirasdavo tuomet, kai klientas į kitą svetainę įėjęs paspausdavo pranešimą „ok“, taip suinstaliuodavo kenkėjišką programą pats to nežinodamas. Jei banko klientas nebūtų vykdęs nuorodų kompiuteryje nebūtų atsiradusi kenkėjiška programa. Na, o žinant duomenis galima vykdyti operaciją būnant bet kurioje pasaulio vietoje, kur yra internetinis ryšys“.[277]

Atsižvelgiant į liudytojos parodymus ir bylos esmę galimą daryti išvada, kad tokio pobūdžio elektroniniai nusikaltimai, pasižymi, tuo, kad panaudojus kenkėjiškas programas ir suklastotus elektroninius puslapius, kurie vizualiai yra beveik identiški apsunkina apgaulės atpažinimą nukentėjusiems asmenims. Taip pat tokių programų naudojimas apsunkina nusikalstamų veikų tyrimą, nes duomenimis galima pasinaudoti iš bet kurios šalies. Taigi, naudojantis elektroninėmis paslaugomis ir naršant internete vartotojai turi būti atidesnį, vengti įtartinų ir neaiškių nuorodų, svetainių. Nepaisant, to, kad ši byla, pasižymi techninių sudėtingumu, tačiau tai, taip patvirtina, kad vartotojų „kibernetinė higiena“ yra esminis faktorius užtikrinantis duomenų saugumą.

---

[276] „Kauno apylinkės teismo 2018 m. rugpjūčio 2 d. nuosprendis baudžiamojoje byloje Nr. 1-2663-917/2018“, LITEKO, žiūrėta 2025 m. sausio 28 d., https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=140433c1-7373-44c9-b6e4-ed5bb9746c5f.

[277] „Nutartis baudžiamojoje byloje 1-2663-917/2018“, *op.cit.*

Išanalizavus bylas dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui, buvo parengtas priedas Nr. 1, kuriame pateikiama analizuotų bylų kvalifikavimo problematika bei šių veikų ypatumai. Taigi, apžvelgus priede nurodytus duomenis galima daryti išvadą, kad nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kvalifikavimas Lietuvos teismų praktikoje susiduria su įvairiais probleminiais aspektais. Be to, tokio pobūdžio bylos pasižymi specifiniais ypatumais.

Bylose matoma problematika nustatant neteisėtumo požymį, ypač tada, kai nenustatoma, kad asmuo turi teisėtą prieigą prie elektroninių duomenų. Tokiais atvejais Kasacinis teismas yra pažymėjęs (LAT nutartys 2K-27-976/2023, 2K-262-489/2022), kad teismai turi nustatyti, kokius konkrečius teisės aktus ar susitarimų įpareigojimus asmuo pažeidė, nes analizuojant bylas nustatyta, kad šios aplinkybės ne visada nustatomos. Taip pat nenustačius, kokie įpareigojimai buvo pažeisti ir kitais atvejais kyla problema atribojant civilinius santykius nuo baudžiamosios teisės taikymo. Analizuojant bylas buvo nustatyta, kad tam tikri ginčai, kylantys iš darbo santykių ar sutartinių santykių (konfidencialumo įsipareigojimų pažeidimai ar intelektinės nuosavybės pašalinimas) nepagrįstai nagrinėjami taikant baudžiamosios teisės normas. Taip pat nustatyta problematika dėl dvigubo naudojimo (angl. dual-use) priemonių vertinimo. Programinė įranga gali būti naudojama tiek teisėtiems tikslams, tiek nusikalstamoms veikoms vykdyti. Todėl iškyla problema įrodinėjant, kokiu tikslu įranga buvo įsigyta ir laikoma. Analizės metu nustatyta BK normų atribojimo problematika ir remiantis LAT praktika nustatyta, kad BK 198[1] ir BK 215 straipsniai saugo skirtingus teisinius gėrius, todėl jie taikytini atskirai ir BK 215 straipsnis neapima BK 198[1]. Analizės metu nustatyta, kad teismai ne visada atsižvelgė į tai, kad „teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas atitinka neteisėto prisijungimo prie informacinės sistemos veikos padarymo būdą.“[278] Skirtingiems teismams taip pat iškilo problema nustatant žalos dydį, kas lėmė skirtingų BK 197 straipsnio dalių taikymą ir nevienodą veikos kvalifikavimą. Tad nustatant straipsnio dalį reikia vertinti tiek turtinę, tiek neturtinę žalą. Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui paprastai negali būti laikomi mažareikšmiškais, o specialisto vaidmuo dalyvaujant tokio pobūdžio bylose yra svarbus.

Galiausiai nagrinėjant elektroninių nusikaltimų bylas nustatyti tam tikri šių veikų specifiniai ypatumai. Tai yra, ne visada pavyksta nustatyti visus nusikalstamą veiką padariusius asmenis, kadangi nusikaltimai gali būti daromi naudojant įvairią programinę įrangą iš įvairių šalių, tad tai lemia sudėtingesnį asmenų nustatymo ir kaltinimo procesą. Taip pat dėl įvairių kenkėjiškų programų, suklastotus elektroninius puslapius asmenims tampa sunkiau atpažinti, dėl to būna

[278] Remigijus Merkevičius, „Baudžiamoji teisė (II dalis)“, Infolex, žiūrėta 2026 m. balandžio 20 d., https://www.infolex.lt/sa/apzvalgos/savaites-apzvalga/nr-253/baudziamoji-teise-ii-dalis/index.html.

prarandami svarbūs duomenys. Be to, nustatyta, kad siekiant išvengti duomenų pažeidžiamumo, įmonės turi stiprinti kibernetinio saugumo priemones.

Apibendrinant galima teigti, kad nepaisant tam tikrų kvalifikavimo problemų pirmosios ir apeliacinės instancijos teismuose, LAT praktika formuoja bendrą, nagrinėtų nusikalstamų veikų aiškinimą, taikymą bei kvalifikavimą. Be to, šių nusikalstamų veikų specifiškumas yra susijęs su pačių asmenų saugiu elgesiu internete ar įmonių kibernetinio saugumo priemonių taikymo efektyvumu. Nesilaikant „kibernetinės higienos“ ir įmonėms netaikant efektyvių apsaugos priemonių yra sudaromos prielaidos elektroniniams nusikaltimams.

IŠVADOS

1. Kibernetinio saugumo samprata formavosi kartu su technologijų raida ir interneto plėtra. Apžvelgus įvairias kibernetinio saugumo sampratas nustatyta, kad tai yra įvairių priemonių, procesų, technologinių, informacijos sklaidos, politinių ir organizacinių veiksmų visuma, kuria yra siekiama apsaugoti elektroninę erdvę, informacines sistemas, kompiuterių tinklus, įrenginius ir juose esančius duomenis nuo kibernetinių grėsmių. Kartu su technologijų plėtra formavosi ir įvairios kibernetinės grėsmės - tokios kaip: tiekimo grandinės atakos, duomenų vagystės „phishing“, socialinės inžinerijos atakos, išpirkos reikalaujančios kenkėjiškos programinės įrangos bei paskirstytų paslaugų trikdymo (DDoS) atakos. Dažnu atveju elektroninėje erdvėje esantys duomenys pažeidžiami ne tik techninėmis priemonėmis, tačiau ir dėl aplaidaus asmenų elgesio elektroninėje erdvėje. Taigi galima teigti, kad kibernetinio saugumo samprata apima ne tik technines apsaugos priemones, teisinį reglamentavimą, saugumo politikos formavimą, bet ir asmenų mokymą bei saugų elgesį kibernetinėje erdvėje.

2. Tarptautinis ir Europos Sąjungos kibernetinio saugumo teisinis reglamentavimas yra didelės apimties ir apima įvairias kibernetinio saugumo sritis. Tokie teisės aktai kaip Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, Visuotinė žmogaus teisių deklaracija, Europos Sąjungos pagrindinių teisių chartija, sudaro duomenų, asmens privatumo ir informacijos apsaugos teisinį pagrindą. Budapešto konvencija dėl elektroninių nusikaltimų ir Direktyva 2013/40/ES dėl atakų prieš informacines sistemas nustato ir kriminalizuoja pagrindines nusikalstamas veikas elektroninėje erdvėje. Be to, ES teisinis reglamentavimas apima tinklų ir informacinių sistemų saugumą, duomenų apsaugą, produktų ir paslaugų kibernetinio saugumo sertifikavimo sistemą. Taip pat apima pasirengimą reaguojant į kibernetinio saugumo incidentus, jų aptikimą ir reagavimą visoje ES.

3. Lietuvos Kibernetinio saugumo įstatymas nustato pagrindines nacionalines kibernetinio saugumo užtikrinimo nuostatas. Kibernetinių incidentų valdymo planas įtvirtina principus, kuriais remiamasi reaguojant į kibernetines grėsmes. Administracinių nusižengimų kodeksas numato atsakomybę už kibernetinio saugumo reikalavimų pažeidimus, o Baudžiamasis kodeksas nustato baudžiamąją atsakomybę už nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui. Tarptautinių teisės aktų, Europos Sąjungos direktyvų ir reglamentų pagrindinės kibernetinio saugumo nuostatos yra perkeltos į Lietuvos teisinę sistemą, kas lemia pakankamą teisinį reglamentavimą kibernetinio saugumo srityje. Be to, Lietuvos Aukščiausiojo Teismo nutartyse remiamasi tarptautinių konvencijų ir ES direktyvų nuostatomis, kas reiškia efektyvų praktinį teisės aktų įgyvendinimą.

4. Nusikalstamų veikų - elektroninių nusikaltimų ir informacinių sistemų saugumui nagrinėjimas teismų praktikoje susiduria su kvalifikavimo problemomis. Visų pirma, susiduriama su problematika nustatant nusikalstamos veikos neteisėtumo požymį, kai yra vertinamas neteisėtas poveikis elektroniniams duomenims. Taip pat pastebima problema atribojant civilinės ir baudžiamosios teisės normas. Be to, pastebėta kvalifikavimo problematika, taikant ir aiškinant Baudžiamojo kodekso normas, taip pat dėl dvigubo naudojimo priemonių vertinimo ir patirtos žalos dydžio nustatymo. Nepaisant nustatytos problematikos, Lietuvos Aukščiausiasis Teismas formuoja vieningą šių nusikalstamų veikų taikymo praktiką. Šios nusikalstamos veikos taip pat pasižymi ir specifiniais ypatumais. Tai yra ne visais atvejais nustatomi nusikalstamą veiką padarę asmenys, nes nusikaltimai vykdomi naudojant programinę įrangą ir gali būti įvykdomi iš bet kurios vietos. Tokiose bylose yra svarbus specialisto dalyvavimas, kad būtų galima tinkamai pagrįsti neteisėtą techninių priemonių panaudojimą. Be to, bylų analizės metu nustatyta, kad asmenims nesilaikant saugumo naudojantis internetu ir išmaniosiomis technologijomis, ir įmonėms netaikant apsaugos priemonių yra sudaromos prielaidos šių veikų atsiradimui.

Taigi, baigiamojo darbo ginamasis teiginys, kad kibernetinio saugumo teisinis reguliavimas Lietuvoje yra pakankamas ir atitinka tarptautines ir ES nuostatas, pasitvirtino.

PASIŪLYMAI

1. Interneto ir išmaniųjų technologijų naudotojams domėtis pagrindiniais „kibernetinės higienos“ principais, taip pat esant galimybei dalyvauti saugaus elgesio internete mokymuose. Tai galima įgyvendinti vartotojams dažniau pateikiant informaciją televizijoje, socialiniuose tinkluose ar dažnai lankomose interneto svetainėse apie prieinamus kibernetinio saugumo mokymus, pavyzdžiui, Nacionalinio kibernetinio saugumo centro internetiniame puslapyje.

2. Įmonėms, pagal galimybes, taikyti kibernetinio saugumo priemones, ypač panaikinti prieigas prie informacinių sistemų buvusiems darbuotojams. Nepaisant to, kad dauguma įmonių tuo pasirūpina, tačiau darbuotojui nutraukus darbo santykius, kiekvienai įmonei reikėtų atlikti prieigų prie informacinių sistemų panaikinimą, pavyzdžiui automatizuojant procesą, arba už tai paskiriant atsakingus asmenis.

LITERATŪROS SĄRAŠAS

TEISĖS AKTAI

1. „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“. TAR. Žiūrėta 2025 m. lapkričio 4 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.

2. „Visuotinė žmogaus teisių deklaracija“. TAR. Žiūrėta 2025 m. lapkričio 4 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385.

3. „Europos Sąjungos pagrindinių teisių chartija“. EUR-Lex. Žiūrėta 2025 m. lapkričio 4 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12012P/TXT.

4. „Sutartis dėl Europos Sąjungos veikimo (suvestinė redakcija)“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12012E/TXT.

5. „Konvencija dėl elektroninių nusikaltimų (ETS Nr. 185)“. Žiūrėta 2026 m. kovo 19 d., https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.

6. „Papildomas protokolas prie Konvencijos dėl elektroninių nusikaltimų dėl rasistinio ir ksenofobinio pobūdžio veikų kriminalizavimo (ETS Nr. 189)“. Žiūrėta 2026 m. kovo 19 d., https://rm.coe.int/168008160f.

7. „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)“. EUR-Lex. Žiūrėta 2026 m. vasario 4 d., https://eur-lex.europa.eu/eli/reg/2019/881/oj/lt.

8. „Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32021R0887.

9. „Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų produktams su skaitmeniniais elementais ir iš dalies keičiantis reglamentus (ES) Nr. 168/2013 ir (ES) 2019/1020 bei direktyvą (ES) 2020/1828 (Kibernetinio atsparumo aktas)“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847.

10. „Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas)“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32025R0038.

11. „Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:32013L0040.

12. „Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2 direktyva)“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32022L2555

13. „Europos Parlamento ir Tarybos direktyva (ES) 2019/713 dėl kovos su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu“. Žiūrėta 2026 m. kovo 19 d., https://data.consilium.europa.eu/doc/document/ST-12181-2017-INIT/lt/pdf.

14. „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““. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52013JC0001.

15. „Europos Parlamento rezoliucija „Konvencija dėl elektroninių nusikaltimų: antrasis papildomas protokolas dėl glaudesnio bendradarbiavimo ir elektroninių įrodymų atskleidimo“ (2023/C 214/17)“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52023AP0002.

16. „Komisijos rekomendacija dėl labai mažų, mažų ir vidutinių įmonių apibrėžties (2003/361/EB)“. EUR-Lex. Žiūrėta 2026 m. kovo 19 d., https://eur-lex.europa.eu/eli/reco/2003/361/oj.

17. „Lietuvos Respublikos baudžiamasis kodeksas“. TAR. Žiūrėta 2026 m. kovo 19 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr.

18. „Lietuvos Respublikos administracinių nusižengimų kodeksas“. TAR. Žiūrėta 2026 m. kovo 19 d., https://www.e-tar.lt/portal/lt/legalAct/4ebe66c0262311e5bf92d6af3f6a2e8b/asr.

19. „Lietuvos Respublikos kibernetinio saugumo įstatymas“. TAR. Žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr.

20. „Lietuvos Respublikos Seimo nutarimas Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo““. TAR. Žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2/asr.

21. „Lietuvos Respublikos Seimo nutarimas Nr. XIV-2505 „Dėl Krašto apsaugos sistemos stiprinimo ir plėtros programos patvirtinimo““. TAR. Žiūrėta 2026 m. kovo 19 d., https://e-tar.lt/portal/lt/legalAct/e3acb430e78f11ee9fdedfc979ae62a9.

22. „Lietuvos Respublikos Vyriausybės nutarimas Nr. 21 „Dėl Europos Sąjungos reikalų koordinavimo““. TAR. Žiūrėta 2026 m. kovo 19 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.224896/asr.

23. „Lietuvos Respublikos Vyriausybės nutarimas Nr. 998 „Dėl 2021–2030 metų Nacionalinio pažangos plano patvirtinimo““. TAR. Žiūrėta 2026 m. kovo 19 d., https://www.e-tar.lt/portal/lt/legalActEditions/d492e050f7dd11eaa12ad7c04a383ca0.

24. „Įsakymas dėl poveikio duomenų apsaugai vertinimo, duomenų valdytojo ir duomenų tvarkytojo duomenų tvarkymo veiklos įrašų rengimo ir asmens duomenų saugumo pažeidimų valdymo tvarkos aprašų patvirtinimo“. Žiūrėta 2026 m. sausio 12 d., https://ird.lrv.lt/public/canonical/1751287415/474/D%C4%97l%20Apra%C5%A1%C5%B3%20patvirtinimo.Elektroninio+dokumento+nuora%C5%A1as%20(1).pdf.

25. „Įsakymas „Dėl 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, 14 straipsnio įgyvendinimo““. TAR. Žiūrėta 2026 m. kovo 19 d., https://www.e-tar.lt/portal/lt/legalAct/6c445bb05c4b11e589fccd6fa118e11c.

MOKSLINIAI ŠALTINIAI

1. Aldaaje, Saleh, ir kt. „The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education“. *Computers & Security* 119 (2022). https://doi.org/10.1016/j.cose.2022.102754.

2. Ansari, Meraj Farheen, Pawan Kumar Sharma ir Bibhu Dash. „Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training“. *International Journal of Smart Sensor and Adhoc Network* 3, nr. 3 (2022): 61–66.

3. Anužis, Mantas, Paulius Šakalys, ir Aleksej Lichovidov. „Kibernetinis saugumas: nuo valstybės iki asmens“. *Verslas, technologijos, biomedicina:* inovacijų įžvalgos 1, nr. 13 (2022): 16–24. https://vb.kvk.lt/object/elaba:134773098/index.html.

4. Craigen, Dan, Nadia Diakun-Thibault ir Randy Purse. „Defining Cybersecurity“. *Technology Innovation Management Review* (2014): 13–21.

5. Dasgupta, Meghna. „Nato’s Cyber Defence Pledge 2.0: How The Alliance Is Strengthening Eastern Flank Security In The Digital Age“. *International Journal of Creative Research Thoughts* 13, nr. 4 (2025): 1637–1645. https://ijcrt.org/papers/IJCRT25A4360.pdf.

6. Galinec, D., D. Možnik ir B. Guberina. „Cybersecurity and Cyber Defence: National Level Strategic Approach“. *Automatika* 58, nr. 3 (2017): 273–280. https://doi.org/10.1080/00051144.2017.1407022.

7. Linden, Theodore A. „Operating System Structures to Support Security and Reliable Software“. Washington, D.C.: U.S. Government Printing Office, 1976. https://csrc.nist.gov/files/pubs/conference/1998/10/08/proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/lind76.pdf.

8. Neigel, A. R., V. L. Claypoole, G. E. Waldfogle, S. Acharya ir G. M. Hancock. „Holistic Cyber Hygiene Education: Accounting for the Human Factors“. *Computers & Security* 92 (2020): 1–12. https://doi.org/10.1016/j.cose.2020.101731.

9. Novikovienė, Lina, ir Oksana Pedaniuk. „Naujosios duomenų subjekto teisės bendrajame duomenų apsaugos reglamente“. *Jurisprudencija* 27, nr. 2 (2020): 317–335. https://cris.mruni.eu/server/api/core/bitstreams/aaf0e76c-2ef7-4f03-8d69-d2e6d3519db/content.

10. Polishchuk, Volodymyr, Vitalii Yurakh, Olena Kravchenko, Wolodymyr Warawa ir Inna Kulchii. „Legal Regulation of Cybersecurity and Privacy on the Internet as SDG's“. *Journal of Lifestyle and SDGs Review* 4, nr. 1 (2024). https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01666.

11. Rashid, Salar Jamal, Shatha A. Baker, Omar I. Alsaif ir Ali I. Ahmad. „Detecting Remote Access Trojan (RAT) Attacks Based on Different LAN Analysis Methods“. *Engineering, Technology & Applied Science Research* 14, nr. 5 (2024): 17294–17300. https://doi.org/10.48084/etasr.8422.

12. Reimsbach-Kounatze, Christian, ir Andras Molnar. „The Impact of Data Portability on User Empowerment, Innovation, and Competition“. *Going Digital Toolkit Note*, nr. 25 (OECD, 2024). https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-impact-of-data-portability-on-user-empowerment-innovation-and-competition_ee329380/319f420f-en.pdf.

13. Schatz, Daniel, Rabih Bashroush ir Julie Wall. „Towards a More Representative Definition of Cyber Security“. *Journal of Digital Forensics, Security and Law* 12, nr. 2 (2017): 53–74. https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl.

14. Stunžinas, Robertas. „Europos Sąjungos kibernetinio saugumo terminai su dėmeniu „kibernetinis, (-ė): reikšmės, kilmė, sinonimija ir variantai““. *Terminologija* 24 (2017): 145–160. https://ceeol.com/search/article-detail?id=702496.

15. Šileikienė, Irma, ir Ana Usovaitė. „Kibernetinio saugumo situacijos Lietuvoje grėsmių analizė Europos Sąjungos kontekste“. *Technologijos ir menas* Nr. 15 (2024): 14–19. https://vb.vtdko.lt/object/elaba:215140351/215140351.pdf.

16. Štitilis, Darius, Paulius Pakutinskas, Marius Laurinaitis ir Inga Malinauskaitė-van de Castel. „National Cyber Security Strategies: Management, Unification and Assessment“. *Independent Journal of Management & Production* (2020): 2341–2354. https://cris.mruni.eu/server/api/core/bitstreams/2edb4036-99b4-44db-8fda-51ba446afe1b/content.

17. Štitilis, Darius. „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos“. *Socialinės technologijos* 3, nr. 1 (2013): 189–207. https://cris.mruni.eu/server/api/core/bitstreams/952d2a4c-b86e-46c4-bb02-dc53a4dbdd2a/content.

18. Štitilis, Darius, Irmantas Rotomskis, Marius Laurinaitis, Sergiy Nadvynychnyy ir Nadiya Khorunzhak. „National Cyber Security Strategies: Management, Unification and Assessment“, Independent Journal of Management & Production (2020): 2342, https://cris.mruni.eu/server/api/core/bitstreams/2edb4036-99b4-44db-8fda-51ba446afe1b/content.

19. Vandezande, Niels. „Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor“. *Computer Law & Security Review* 52 (2024). https://doi.org/10.1016/j.clsr.2023.105890.

SPECIALIOJI LITERATŪRA

1. „A Comparative Study of Russian Cyber Offensive Capabilities from 2022 to 2025“. National Cyber Security Centre. Žiūrėta 2026 m. kovo 19 d. https://nksc.lt/doc/rkgc/A_Comparative_Study_of_Russian_Cyber_Offensive_Capabilities_from_2022_to_2025.pdf.

2. Alam, Shahid. *Cybersecurity: Past, Present and Future*. Adana: Adana Alparslan Türkeş Science and Technology University, 2022. https://arxiv.org/pdf/2207.01227.

Blevičiūtė, Gabrielė, Justas Kidykas ir Rūta Beinoriūtė. *Kibernetinio saugumo tendencijos Lietuvoje ir pasaulyje*. 2019. https://data.kurklt.lt/wp-content/uploads/2023/04/Esama-situacija-su-VK.pdf.

3. „Cryptographic Communications System and Method“. U.S. Patent No. 4,405,829, 1983 m. rugsėjo 20 d. Žiūrėta 2026 m. kovo 3 d. https://patentimages.storage.googleapis.com/49/43/9c/b155bf231090f6/US4405829.pdf.

4. Healey, Jason, ir Klara Tothova Jordan. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*. Atlantic Council, 2014. https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf.

5. Juozapavičius, Aušrius, ir kt. *Nacionalinis saugumas ir krašto gynyba*. Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2025. https://ekspertai.eu/static/uploads/2026-03-04/LKA%2012%20klases%20vadovelis%20vidus%201%20dalis_e-mokykla%20(1).pdf.

6. Jurgilas, Konstantinas. „Dviejų faktorių (2FA) skaitmeninio autentifikavimo metodas nuotolinei prieigai prie kritinės infrastruktūros sistemos“. Magistro baigiamasis darbas, Kauno

technologijos universitetas, 2021. https://talpykla.elaba.lt/elaba-fedora/objects/elaba:95730204/datastreams/MAIN/content.

7. Klimburg, Alexander, red. *National Cyber Security Framework Manual*. Talinas: NATO Cooperative Cyber Defence Centre of Excellence, 2018. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

8. Lietuvos Aukščiausiasis Teismas. „2019 m. kovo 28 d. Baudžiamojo proceso kodekso normų, reglamentuojančių specialiųjų žinių panaudojimą, taikymo teismų praktikoje apžvalga“. Žiūrėta 2026 m. balandžio 10 d. https://www.lat.lt/lat-praktika/lat-praktikos-tam-tikrose-teises-srityse-apzvalgos/baudziamuju-bylu-apzvalgos/68.

9. Lietuvos Aukščiausiasis Teismas. „Teismų praktika biuletenis Nr. 52“. Žiūrėta 2026 m. balandžio 20 d. https://www.lat.lt/data/public/uploads/2020/07/d1_teismu_praktika_nr_52.pdf.

Lietuvos Aukščiausiasis Teismas. „Teismų praktika biuletenis Nr. 62“. Žiūrėta 2026 m. balandžio 20 d. https://www.lat.lt/data/public/uploads/2025/09/teismu_praktika_nr_62.pdf.

10. Marcinauskaitė, Renata. „Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai)“. Daktaro disertacija, Mykolo Romerio universitetas, 2013. https://cris.mruni.eu/server/api/core/bitstreams/9b222ea8-bb14-453a-a4ed-1fda10663f13/content.

11. Masevičiūtė, Milda. „ES poveikis darbo santykių reguliavimui Lietuvoje“. Magistro baigiamasis darbas, Vytauto Didžiojo universitetas, 2009. https://portalcris.vdu.lt/server/api/core/bitstreams/0717c60d-7145-40df-be21-ce0731f760e8/content.

12. Merkevičius, Remigijus. „Baudžiamoji teisė (II dalis)“. Infolex. Žiūrėta 2026 m. balandžio 20 d. https://www.infolex.lt/sa/apzvalgos/savaites-apzvalga/nr-253/baudziamoji-teise-ii-dalis/index.html.

13. Olech, Aleksander, ir Damjan Štruc. *The Evolution of Cyber Forces in NATO Countries*. NATO Cooperative Cyber Defence Centre of Excellence, 2025. https://ccdcoe.org/uploads/2025/07/The_evolution_of_cyber_forces_in_NATO_countries.pdf.

14. Potapovs, Mihails, ir Kate E. Kanasta. *Cybersecurity in Latvia: Forging Resilience Amidst Emerging Threats*. Routledge, 2026. https://www.mod.gov.lv/sites/mod/files/document/Cybersecurity%20in%20Latvia_25_08_07_15_01_13.pdf.

15. Šidlauskas, Aurimas. „Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis“. Daktaro disertacija, Mykolo Romerio universitetas, 2024. https://cris.mruni.eu/server/api/core/bitstreams/9a26a2be-e862-4425-a208-083239c86338/content.

16. Šimonienė, Inga. „Kibernetinio saugumo kultūros vertinimas Lietuvos ligoninėse“. Magistro baigiamasis darbas, Mykolo Romerio universitetas, 2024. https://cris.mruni.eu/server/api/core/bitstreams/a4bca602-9cc8-4729-949e-0d4c8c8713ac/content.

17. Tamošaitytė, Marija. „Kibernetinio saugumo aktualizavimas Lietuvos nacionalinio saugumo strategijoje“. Magistro darbas, Klaipėdos universitetas, 2020. https://gs.elaba.lt/object/elaba:47757480.

18. Želvienė, Gabrielė. „Kibernetinio saugumo iššūkiai ir grėsmės Lietuvos nacionalinio saugumo strategijoje“. Magistro darbas, Vytauto Didžiojo universitetas, 2024. https://www.vdu.lt/cris/entities/etd/c3da6bf9-8887-4aea-91c6-9ec3833afc00.

TEISMŲ PRAKTIKA

1. „2009 m. kovo 2 d. Europos Žmogaus Teisių Teismo sprendimas byloje K. U. prieš Suomiją, Nr. 2872/02“. HUDOC. Žiūrėta 2025 m. sausio 19 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62009CJ0092.

2. „Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González“. Europos Sąjungos Teisingumo Teismas, 2014 m. gegužės 13 d., byla C-131/12. EUR- Lex. Žiūrėta 2025 m. sausio 16 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131.

3. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. rugsėjo 30 d. nutartis baudžiamojoje byloje Nr. 2K-254/2008“. LITEKO. Žiūrėta 2026 m. balandžio 22 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=bed3a4fb-f5b3-471d-b90e-c63034a1d833.

4. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. sausio 6 d. nutartis baudžiamojoje byloje Nr. 2K-138/2015“. LITEKO. Žiūrėta 2026 m. balandžio 22 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=78d6aacb-1ea9-4173-901f-86f4db6f2d33.

5. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2022 m. gruodžio 15 d. nutartis baudžiamojoje byloje Nr. 2K-262-489/2022“. LITEKO. Žiūrėta 2026 m. balandžio 22 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=eb024162-eaa7-45f8-b88c-cdac3127bef9 .

6. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 15 d. nutartis baudžiamojoje byloje Nr. 2K-27-976/2023“. LITEKO. Žiūrėta 2026 m. balandžio 22 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9b33ec46-8901-4d5e-af56-d751b3520f97.

7. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2024 m. lapkričio 6 d. nutartis baudžiamojoje byloje Nr. 2K-214-489/2024“. LITEKO. Žiūrėta 2025 m. balandžio 5 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=28bccd40-739d-43f7-a8cc-f1eecddab2d2 .

8. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2023 m. vasario 15 d. nutartis baudžiamojoje byloje Nr. 2K-27-976/2023“. LITEKO. Žiūrėta 2025 m. vasario 18 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9b33ec46-8901-4d5e-af56-d751b3520f97.

9. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2018 m. kovo 26 d. nutartis baudžiamojoje byloje Nr. 2K-46-699/2018“. LITEKO. Žiūrėta 2025 m. kovo 14 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=7d67b8c5-779f-4d0e-ac1a-2cbe17b92f57.

10. „Lietuvos Aukščiausiojo Teismo 2019 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-45-697/2026“. LITEKO. Žiūrėta 2025 m. sausio 19 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=eb98a3a4-f7b8-49ce-a392-85a9263ce010

11. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gruodžio 8 d. nutartis baudžiamojoje byloje Nr. 2K-555-788/2015“. LITEKO. Žiūrėta 2025 m. sausio 28 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=c82c82f2-9d67-4971-be81-bd574e1aa5a0.

12. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2012 m. birželio 26 d. nutartis baudžiamojoje byloje Nr. 2K-375/2012“. LITEKO. Žiūrėta 2025 m. vasario 12 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=57620acd-4a52-40c8-8ef7-7176a7989480.

13. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2016 m. sausio 26 d. nutartis baudžiamojoje byloje Nr. 2K-4-507/2016“. LITEKO. Žiūrėta 2025 m. vasario 18 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=1fdbcaf1-a5e2-41cc-8d4b-944c5a14eefc.

14. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gruodžio 8 d. nutartis baudžiamojoje byloje Nr. 2K-555-788/2015“. LITEKO. Žiūrėta 2025 m. sausio 19 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=c82c82f2-9d67-4971-be81-bd574e1aa5a0.

15. „Lietuvos Aukščiausiojo Teismo 2015 m. liepos 2 d. nutartis baudžiamojoje byloje Nr. 2K-199-648/2019“. LITEKO. Žiūrėta 2025 m. kovo 14 d.

https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=26323413-d1e7-491a-9d15-673638b54d6f.

16. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2015 m. gegužės 12 d. nutartis baudžiamojoje byloje Nr. 2K-188-489/2015“. LITEKO. Žiūrėta 2025 m. vasario 12 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9b3513d4-6e5a-43a4-bc24-14cebf44c4b2.

17. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2019 m. gruodžio 10 d. nutartis baudžiamojoje byloje Nr. 2K-314-895/2019“. LITEKO. Žiūrėta 2025 m. kovo 30 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=7fb54312-36da-4157-b6b9-03d6989a7f2f.

18. „Kauno apylinkės teismo 2018 m. rugpjūčio 2 d. nuosprendis baudžiamojoje byloje Nr. 1-2663-917/2018“. LITEKO. Žiūrėta 2025 m. sausio 28 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=140433c1-7373-44c9-b6e4-ed5bb9746c5f.

19. „Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2016 m. gruodžio 21 d. nutartis baudžiamojoje byloje Nr. 1A-477-498/2016“. LITEKO. Žiūrėta 2025 m. balandžio 16 d. https://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=ed6b4b34-8972-4060-b90d-5677c455bb46.

INTERNETINIAI ŠALTINIAI

1. „2023 Nacionalinė kibernetinio saugumo būklės ataskaita“, Lietuvos Respublikos krašto apsaugos ministerija, (Vilnius, 2023), 29.

2. „2024 Nacionalinė kibernetinio saugumo būklės ataskaita“. Lietuvos Respublikos krašto apsaugos ministerija. Žiūrėta 2026 m. kovo 17 d., https://kam.lt/leidiniai/nacionaline-kibernetinio-saugumo-bukles-ataskaita-kam-2024/.

3. „Asmens duomenų saugumo pažeidimai Lietuvoje 2025 m.“ Valstybinė duomenų apsaugos inspekcija. Žiūrėta 2026 m. kovo 19 d. https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2025-m-lfX/.

4. „Asmens duomenų apsaugos gairės duomenų subjektams“. Valstybinė duomenų apsaugos inspekcija. Žiūrėta 2026 m. kovo 19 d. https://vdai.lrv.lt/uploads/vdai/documents/files/01%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20DUOMENU%20SUBJEKTAMS%202019-10-16%20(perziureta%202023-06-05).pdf.

5. „Atnaujintas kibernetinio saugumo įstatymas“. Lietuvos Respublikos krašto apsaugos ministerija. Žiūrėta 2026 m. balandžio 13 d. https://kam.lt/leidiniai/atnaujintas-kibernetinio-saugumo-istatymas-ka-reiketu-zinoti/.

6. „Brute force atakos“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. kovo 19 d. https://nksc.lt/rekomendacijos/brute_force_atakos.html.

7. „CSIRTs Network“. ENISA. Žiūrėta 2026 m. kovo 19 d. https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network.

8. „Cyber defence“. NATO. Žiūrėta 2026 m. kovo 10 d. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.

9. „Cybersecurity: social engineering“. European Council. Žiūrėta 2026 m. kovo 19 d. https://www.consilium.europa.eu/en/policies/cybersecurity-social-engineering/.

10. „Dar viena byla dėl nusikaltimų elektroninėje erdvėje perduota teismui“. Vilniaus apskrities vyriausiasis policijos komisariatas. Žiūrėta 2026 m. balandžio 10 d. https://vilnius.policija.lrv.lt/lt/naujienos/dar-viena-byla-del-nusikaltimu-elektronineje-erdveje-perduota-teismui/.

11. „Denial – of service (DoS) ataka“. Studijok.lt. Žiūrėta 2026 m. kovo 19 d. https://studijok.lt/mokomoji-medziaga/studentu_darbai/UrbalityteAusra/denial.html.

12. „ENISA Threat Landscape 2025“. ENISA. Žiūrėta 2026 m. kovo 6 d. https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf.

13. „European cybersecurity certification framework“. European Commission. Žiūrėta 2026 m. kovo 19 d. https://digital-strategy.ec.europa.eu/en/node/15665/printable/pdf.

14. Hayes, Adam. „Optimizing Supply Chains: From Raw Materials to Consumers“. Investopedia. Žiūrėta 2026 m. kovo 19 d. https://www.investopedia.com/terms/s/supplychain.asp.

15. „Kibernetinio saugumo dokumentų rinkinys: Taryba priėmė naujus teisės aktus kibernetinio saugumo pajėgumams ES stiprinti“. Europos Vadovų Taryba ir Europos Sąjungos Taryba. Žiūrėta 2026 m. kovo 19 d. https://www.consilium.europa.eu/lt/press/press-releases/2024/12/02/cybersecurity-package-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/.

16. „Kibernetinio saugumo istorija“. CyberPhish, žiūrėta 2026 m. kovo 11 d., https://cyberphish.knf.vu.lt/lt/learn/kibernetinio-saugumo-istorija/20.

17. „Kibernetinio saugumo strategija“. Europos Komisija. Žiūrėta 2026 m. kovo 19 d. https://digital-strategy.ec.europa.eu/lt/policies/cybersecurity-strategy.

18. „Kibernetinis saugumas ES: strategija ir pagrindinės politikos priemonės“. Europos Vadovų Taryba ir Europos Sąjungos Taryba. Žiūrėta 2026 m. kovo 19 d. https://www.consilium.europa.eu/lt/policies/cybersecurity/.

19. „Kokios yra pagrindinės kibernetinės grėsmės ES?“ Europos Vadovų Taryba ir Europos Sąjungos Taryba. Žiūrėta 2026 m. kovo 19 d. https://www.consilium.europa.eu/lt/policies/top-cyber-threats/.

20. „Nacionalinė kibernetinio saugumo strategija“. Lietuvos Respublikos krašto apsaugos ministerija. Žiūrėta 2026 m. kovo 19 d. https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf.

21. „Nusikaltimai elektroninėje erdvėje“. Lietuvos Respublikos prokuratūra. Žiūrėta 2026 m. kovo 19 d. https://www.prokuraturos.lt/lt/veikla/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185.

22. „Nusikalstamumo duomenų rinkiniai“. Informatikos ir ryšių departamentas. Žiūrėta 2026 m. balandžio 1 d. https://ird.lt/lt/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/nusikalstamumo-duomenu-rinkiniai/.

23. „Phishing“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. kovo 5 d. https://www.nksc.lt/rekomendacijos/phishing.html.

24. „Ransomware“. Federal Bureau of Investigation. Žiūrėta 2026 m. kovo 6 d. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware.

25. „Rekomendacija dėl kibernetinių incidentų prevencijos“. Valstybinė duomenų apsaugos inspekcija. Žiūrėta 2026 m. kovo 19 d. https://vdai.lrv.lt/public/canonical/1753770948/1018/Rekomendacija_kibernetiniai%20incidentai_2024%20m.pdf.

26. „Svarbiausi reformos pakeitimai“. Valstybinė duomenų apsaugos inspekcija. Žiūrėta 2026 m. kovo 19 d. https://vdai.lrv.lt/lt/naudinga-informacija/2018-m-duomenu-apsaugos-reforma-1/svarbiausi-reformos-pakeitimai/.

27. „Third party software providers“. National Cyber Security Centre. Žiūrėta 2026 m. kovo 6 d. https://www.ncsc.gov.uk/collection/supply-chain-security/third-party-software-providers.

28. „Trojan/ObscuGen“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. kovo 5 d. https://www.nksc.lt/rekomendacijos/trojanmalwareobscugen.html.

29. „What Are the Key Differences Between GDPR and NIS2?“. Dynamic Identity, PATECCO. Žiūrėta 2026 m. kovo 19 d., https://patecco.com/what-are-the-key-differences-between-gdpr-and-nis2/.

30. „What Is a Cyber Attack?“ Fortinet. Žiūrėta 2026 m. kovo 19 d. https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack.

31. „What Is a DDoS Attack?“ Akamai. Žiūrėta 2026 m. kovo 6 d. https://www.akamai.com/glossary/what-is-ddos.

32. Žukauskaitė, Miglė Laima. „Kibernetinės higienos pagrindai“. VDAI. 2024 m. rugsėjo 26 d., žiūrėta 2026 m. kovo 19 d., https://vdai.lrv.lt/public/canonical/1727673277/613/Kibernetines%20higienos%20pagrindai_Migle.pdf.

PRIEDAI

1 PRIEDAS

Bylos Nr.	BK Straipsniai	Kaltinimo esmė	Pagrindinės kvalifikavimo problemos ir (ar) specifiniai bylų ypatumai.
2K-262-489/2022	BK 196 str. (Neteisėtas poveikis elektroniniams duomenims)	Neteisėtas elektroninių duomenų pašalinimas (ištrynimas), turint prieiga prie el. sistemos.	1. Neatskleistas ir nepagrįstas poveikio neteisėtumo elektroniniams duomenims požymis esant teisiniams santykiams. 2.Teismai netinkamai vertino patį elektroninių duomenų pobūdį, jų turinį ir nevertino konkrečių poveikio aplinkybių pavojingumo aspektu (duomenys yra autorių teisių ginamas intelektinės nuosavybės objektas, dėl intelektinės nuosavybės objekto sunaikinimu kilęs darbo ginčas, duomenys nėra visiškai sunaikinti). 3. Nėra aiškiai atskleisto netiesioginės tyčios turinio. 4. Teisinis ginčas turėjo būti sprendžiamas civilinio proceso tvarka. *Baudžiamoji byla nutraukta.*
2K-214-489/2024	BK 198 str. 1 d. (Neteisėtas elektroninių duomenų perėmimas ir panaudojimas)	Neviešu elektroninių duomenų, sudarančius komercinę paslaptį įgijimas.	1. Nenustatytas elektroninių duomenų įgijimo neteisėtumo požymis, esant teisiniams santykiams (nenurodyta, kokius teisės aktus asmuo pažeidė, kokių draudimų, susitarimų, įgaliojimų tyčia nesilaikė) 2. Tarp konfidencialumo įsipareigojimą pasirašiusių šalių kilę ginčai ir galimi konfidencialumo įsipareigojimo pažeidimai turėjo būti sprendžiami civilinės teisės gynimo priemonėmis.

			3. Veiksmai, susiję su komercinės paslapties įgijimu, kriminalizuoti ne BK 198 straipsnyje, o BK 210 straipsnyje. *Baudžiamoji byla nutraukta.*
Nr. 2K-4-507/2016	Išteisintas pagal BK 198[1] str. 1 d. (Neteisėtas prisijungimas prie informacinės sistemos) Nuteistas- 182 str. 1 d. 214 straipsnio 1 dalį, 215 str. 1 d.	Neteisėtas prisijungimas prie e. bankininkystės, turto įgijimas sukčiavimo būdu.	1. Teismų sprendimuose BK 198[1] straipsnio 1 dalies dispozicija aiškinama neteisingai 2. Veika turėjo būti kvalifikuojama pagal BK 198[1] straipsnį nustačius, kad prie informacinės sistemos buvo prisijungta pažeidžiant šios sistemos apsaugos priemones. 3. BK 198[1] ir 215 saugo skirtingus objektus, todėl apeliacinės instancijos teismo išvada, kad BK 215 str. yra specialioji norma BK 198[1] straipsnio atžvilgiu, yra klaidinga. Pripažintas kaltu ir pagal BK 198[1] str. 1 d.
2K-45-697/2026	BK 198[1] str. 1 d.	Neteisėtas prisijungimas prie informacinės sistemos	1. Teismai tinkamai atskleidė nuteistosios padarytos veikos neteisėtumo požymį(nežinodama prisijungimo duomenų ir neturėdama teisėto minėto daikto valdytojo sutikimo, prie nukentėjusiojo kompiuterio prisijungė neteisėtai, pažeisdama informacinės sistemos apsaugos priemones) 2. Nuosavybės klausimas veikos kvalifikavimui nėra aktualus nusikaltimu kėsinamasi ne į nuosavybę, o į elektroninių duomenų ir informacinių sistemų saugumą. *Kasacinis skundas atmestas.*

Nr. 2K-199-648/2019	BK 198² str. 1 d., 198¹ str. 1 d., 198 str. 1 d., (Neteisėtas prisijungimas prie informacinės sistemos, neteisėtas elektroninių duomenų perėmimas ir panaudojimas, neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis)	įgijo ir laikė programinę įrangą, tiesiogiai pritaikytą nusikalstamoms veikoms daryti, bei neteisėtai prisijungęs prie informacinės sistemos, pažeidė informacinės sistemos apsaugos priemones bei neteisėtai perėmė ir panaudojo neviešus elektroninius duomenis.	1. Dėl BK 198^2 priemonės 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.[279] * Byloje nėra duomenų, kad įsigydamas programinę įrangą turėjo tikslą ją panaudoti nusikalstamais tikslais. * Tačiau programinę įrangą laikė nusikalstamais tikslais ir tokią veiką padarė tyčine kaltės forma Šalintina aplinkybė, kad turėdamas tikslą daryti nusikalstamas veikas, įgijo programinę įrangą, tiesiogiai pritaikytą nusikalstamoms veikoms daryti. 2. Pagal BK 198^1 tinkamai nustatytas neteisėtumo požymis. 3. Dėl BK 198 str., nustatyta, kad administratoriaus teisės nelaikytinos neviešais elektroniniais duomenimis, o kitų tokių duomenų perėmimas ar panaudojimas neįrodytas . Pagal BK 198 str. 1 dalį veika nutraukta. Pagal BK 198^2 sumažinta bauda, pašalinus aplinkybę, dėl įsigijimo ir subendrinta su BK 198^1 str.
2K-188-489/2015	BK 197 str 3 d. (Neteisėtas poveikis informacinei sistemai)198^2	Įgijo, laikė programinę įrangą, skirtą elektroninės paslaugos trikdymo atakoms vykdyti, vykdė	1. BK 198^2 str. 1 d. nurodyto dalyko požymius šioje byloje atitinka ir dvigubo naudojimo priemonės (*angl.* dual-use), kurios gali

[279] „Nutartis baudžiamojoje byloje 2K-199-648/2019“, *supra note*, 257.

	str. 1 d.(Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis)	paslaugos trikdymo atakas (Ddos).	būti panaudotos tiek teisėtiems, tiek ir nusikalstamiems tikslams. *Tačiau teismai nepagrįstai padarė išvadą, kad programos, kurias A. V. įgijo, laikė ir panaudojo, nėra skirtos nusikalstamoms veikoms daryti. Tad programinė įranga pripažintina nusikalstamos veikos dalyku. 2. Apeliacinės instancijos neįvertino žalos dydžiui nustatyti reikšmingų aplinkybių visumos, priėjo neteisingos išvados, jog dėl neteisėto poveikio dviem tinklalapiams padaryta žala yra nedidelė. * Pagal BK 197 straipsnyje nurodytos žalos turinį sudaro ne tik turtinė, bet ir neturtinė žala. 3. Teismai veikos neteisėtumo požymį aiškino pagal CK, o ne pagal Tarybos pagrindų sprendimo 2005/222/TVR dėl atakų prieš informacines sistemas. Tačiau Kasacinis teismas teigė, kad aiškinimas netikslus, tačiau tai nereiškia, kad netinkamai pritaikytas baudžiamasis įstatymas. Panaikinta apygardos nuosprendžio dalis dėl išteisinimo pagal BK 198^2 str. 1 d. ir 1 dalies į 197 str 3 d., pakeitimo.
1A-477-498/2016	BK 196, 197, 198, 198^1 str.	Neteisėtai įsilaužė į serverius, perėmė juose saugomus neviešus elektroninius duomenis, sunaikino dalį informacijos, pakeitė	1. Specialisto vaidmuo buvo svarbus ir leido pagrįsti kaltinamojo tyčios turinį. 2. Argumentai, kad kaltinamasis į savo kompiuterį parsisiųsdamas duomenų bazę atsisiuntė ir virusą, kuris už jį

		prisijungimo duomenis ir sutrikdė informacinės sistemos veikimą.	padarė visus veiksmus paneigta specialisto išvada.
2K-4-507/2016, 2K-199-648/2019, 2K-27-976/2023, 2K-45-697/2026,	Pozicija dėl BK 37	Neteisėto prisijungimo prie informacinės sistemos mažareikšmiškumo aspektas	1. Neteisėtas prisijungimas prie informacinės sistemos negali būti laikomas nereikšmingu.
2K-555-788/2015	Išteisintas pagal BK 198[1] str. 1 d.	Neteisėtas prisijungimas prie e. bankininkystės, sukčiavimas, svetimo turto įgijimas.	1. Teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, atitinka neteisėto prisijungimo prie informacinės sistemos veikos padarymo būdą. Kasacinio teismo išvada turėjo būti taikomas 198[1] str. 1 d. str.
1-2663-917/2018	BK 24, 25, 214, 198[1], 215, 182	Neteisėtas elektroninių mokėjimo priemonių duomenų įgijimas ir panaudojimas, siekiant apgaule įgyti svetimą turtą. Kenkėjiškos programos naudojimas.	1. Problematika nustatant visus asmenis dalyvaujančius nusikalstamoje veikoje. 2. Dėl suklastotų puslapių asmenims sunku atpažinti apgaulę. 3. Kenkėjiškų programų naudojimas apsunkina nusikalstamų veikų tyrimą, nes duomenimis galima pasinaudoti iš bet kurios šalies. 4. „Kibernetinė higiena“ yra esminis faktorius užtikrinantis duomenų saugumą.
2K-157-895/2020	BK 198[1] str. 1 d. 215 str. 1 d., 182 str. 1 d.,	Neteisėtas prisijungimas prie e. bankininkystės ir sukčiavimas,	1. Neteisėtas prisijungimas prie banko el. bankininkystės, neteisėtai įvedant mirusios

		pasinaudojant mirusio asmens duomenimis. Mirusiosios testamentu buvo palikti dar ir kitiems asmenims.	patvirtinančius duomenis, taip suklaidinant šią sistemą buvo tinkamai kvalifikuotas pagal BK 198[1] str. 1.
Policijos komisariato byla perduota teismui.	BK 198 str. 1 d., 198[1] str. 1 d.	Buvęs darbuotojas, neturėdamas teisės, pasinaudojo prisijungimo duomenimis ir neteisėtai prisijungė prie įmonės sistemų bei peržiūrėjo neviešus duomenis.	1. Nurodytas ir pagrįstas neteisėtumo požymis. 2. Įmonės nesiimdamos priemonių užtikrinti jų duomenų saugumą (keisti slaptažodžius, panaikinti buvusiu darbuotojų prisijungimo duomenis), sudaro prielaidas asmenims paveikti įmonės duomenis.

1 lentelė. Bylų analizės lentelė, sudarytas darbo autoriaus, remiantis teismų praktikos analize.

SANTRAUKA LIETUVIŲ KALBA

Magistro baigiamojo darbo tema – „Kibernetinio saugumo teisinis reglamentavimas ir praktiniai aspektai“. Temos aktualumas grindžiamas vis nemažėjančiu kibernetinių incidentų ir nusikaltimų elektroninių duomenų bei informacinių sistemų saugumui fiksavimu ir teisės aktų atnaujinimu kibernetinio saugumo srityje. Baigiamąjį darbą sudaro keturi skyriai. Pirmajame skyriuje apžvelgiami kibernetinio saugumo teoriniai aspektai. Antrajame skyriuje analizuojamas tarptautinis ir Europos Sąjungos kibernetinio saugumo teisinis reglamentavimas. Trečiajame skyriuje nagrinėjamas kibernetinio saugumo teisinis reglamentavimas Lietuvoje. Ketvirtajame skyriuje analizuojama teismų praktika, nagrinėjant baudžiamąsias bylas dėl nusikalstamų veikų elektroninėje erdvėje, siekiant atskleisti šių veikų kvalifikavimo probleminius aspektus ir specifinius ypatumus. Darbe pateikiamos išvados ir pasiūlymai.

Tyrimo objektas – kibernetinio saugumo teisiniai ir praktiniai aspektai, o tikslas – išanalizuoti kibernetinio saugumo teisinį reglamentavimą ir praktinius aspektus. Šiam tikslui pasiekti iškelti keturi uždaviniai: pirmuoju siekta išanalizuoti kibernetinio saugumo sampratą ir kibernetines grėsmes, antruoju – išnagrinėti kibernetinio saugumo teisinį reglamentavimą Europos Sąjungoje bei tarptautiniu lygmeniu, trečiuoju – įvertinti kibernetinio saugumo teisinį reglamentavimą Lietuvoje, ketvirtuoju – atskleisti teismų praktikoje taikomų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui kvalifikavimo problematiką ir šių veikų specifinius ypatumus. Atlikus teisės aktų analizę nustatyta, kad Lietuvoje pakankamas teisinis reglamentavimas, kuris atitinka pagrindines tarptautines bei Europos Sąjungos kibernetinio saugumo nuostatas. Išnagrinėjus teismų praktiką nustatyti kvalifikavimo probleminiai aspektai taikant ir aiškinant baudžiamojo įstatymo normas dėl nusikaltimų elektroninėje erdvėje, tačiau Lietuvos Aukščiausiasis Teismas formuoja vieningą šių nusikalstamų veikų normų taikymo praktiką. Nusikalstamos veikos elektroninėje erdvėje pasižymi specifiniais ypatumais, kadangi jos gali būti vykdomos naudojant įvairią programinę įrangą ir iš bet kurios vietos, todėl sudėtinga nustatyti nusikalstamas veikas įvykdžiusius asmenis ir patraukti juos baudžiamojon atsakomybėn. Tokiose bylose yra svarbus specialistų dalyvavimas, siekiant tinkamai pagrįsti neteisėtą techninių priemonių panaudojimą.

Tiek teorinės medžiagos analizės metu, tiek bylų analizės metu nustatyta, kad asmenims nesilaikant saugumo principų naudojantis internetu ir išmaniosiomis technologijomis bei įmonėms netaikant apsaugos priemonių sudaromos prielaidos nusikalstamų veikų elektroninėje erdvėje atsiradimui. Todėl svarbu laikytis kibernetinės higienos principų, o įmonėms taikyti tinkamas kibernetinio saugumo priemones, ypač panaikinti prieigas prie informacinių sistemų buvusiems darbuotojams. Tyrime taikyti dokumentų analizės, lyginamasis ir apibendrinimo metodai.

SANTRAUKA ANGLŲ KALBA

The title of the Master's thesis is “Legal Regulation of Cybersecurity and Practical Aspects”. The relevance of the topic is based on the continuously increasing recording of cyber incidents and crimes against the security of electronic data and information systems, as well as the ongoing updates of legal acts in the field of cybersecurity. The thesis consists of four chapters. The first chapter reviews the theoretical aspects of cybersecurity. The second chapter analyzes the international and European Union legal regulation of cybersecurity. The third chapter examines the legal regulation of cybersecurity in Lithuania. The fourth chapter analyzes court practice by examining criminal cases related to offenses committed in cyberspace, aiming to reveal problematic aspects of the qualification of these offenses and their specific features. The thesis presents conclusions and recommendations.

The object of the research is the legal and practical aspects of cybersecurity, while the aim is to analyze the legal regulation of cybersecurity and its practical application. To achieve this aim, four objectives were set: the first was to analyze the concept of cybersecurity and cyber threats; the second – to examine the legal regulation of cybersecurity at the European Union and international levels; the third – to evaluate the legal regulation of cybersecurity in Lithuania; the fourth – to reveal the problems of qualification of criminal offenses against the security of electronic data and information systems in court practice, as well as the specific features of these offenses. The analysis of legal acts revealed that Lithuania has a sufficient legal framework that complies with the main international and European Union cybersecurity requirements. The analysis of court practice identified problematic aspects of qualification in the application and interpretation of criminal law norms related to cybercrime; however, the Supreme Court of Lithuania forms a consistent practice in the application of these legal norms. Criminal offenses in cyberspace have specific characteristics, as they can be committed using various software and from any location, which makes it difficult to identify perpetrators and bring them to criminal liability. Therefore, the involvement of specialists is important in such cases in order to properly substantiate the unlawful use of technical measures.

Both the analysis of theoretical material and case law showed that failure of individuals to comply with security principles when using the Internet and smart technologies, as well as the lack of protective measures by organizations, creates conditions for the occurrence of cybercrime. Therefore, it is important for internet users to follow the principles of cyber hygiene, and for organizations to implement appropriate cybersecurity measures, especially to remove access to information systems for former employees. The research applied document analysis, comparative, and generalization methods.