ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2026, Vol. 38, Nr. 2

KIBERNETINIŲ NUSIKALTIMŲ POVEIKIS ŽMOGUI

Gediminas BUČIŪNAS
Mykolo Romerio Universitetas
Maironio g. 27, LT-44211 Kaunas
Vytauto Didžiojo Universitetas
Jonavos g.66, LT-44318 Kaunas
Klaipėdos Universitetas
S. Nėries g. 5, LT-92227 Klaipėda
El. paštas: gediminas1967@mruni.eu
ORCID ID: 0000-0002-1826-0527

Kornelija GARUCKAITĖ
Mykolo Romerio Universitetas
Ateities g. 20, LT-08303, Vilnius
El. paštas: kornelijagaruc@gmail.com
ORCID ID: 0009-0003-3513-6119

DOI: 10.13165/PSPO-25-38-02-02

Anotacija. *XXI amžius vadinamas skaitmeniniu amžiumi, kuris iš esmės palietė įvairias žmonių gyvenimo sritis, valstybės valdymo procesus, kardinaliai pakeitė informacijos rinkimo, apdorojimo, sklaidos ir saugojimo procesus, formatus. Dar prieš trisdešimt metų, galimybė neišeinant iš namų nuotoliu užregistruoti verslo įmonę, gauti leidimus iš valstybinių institucijų tam tikroms ūkinėms veikloms vykdyti, atrodė nepasiekiama svajonė, lyg iš fantastikos pasaulio nužengęs scenarijus. Sparčiais tempais besivystančios technologijos sukūrė galimybes komunikuoti nuotoliu, perduoti didžiulius informacijos kiekius per kelias sekundes iš vieno kontinento į kitą, atlikti finansines transakcijas, bet tuo pačiu sukūrė naujas grėsmes individų, visuomenės, valstybių saugumui. Tos grėsmės yra įvardijamos terminu „kibernetiniai nusikaltimai“ ir egzistuoja greta jau seniai žinomų grėsmių, įvardijamų terminais „korupcija“, „organizuotas nusikalstamumas“, „terorizmas“. Kibernetiniai nusikaltimai akademinėje literatūroje dar vadinami terminu „aukštųjų technologijų nusikaltimai“ ir daro didelę žalą tiek atskiram individui, tiek visuomenei, verslams, kuomet neteisėtais veiksmais, sukčiaujant ar kitaip, yra vykdomos tapatybės vagystės, duomenų vagystės, įvairūs finansiniai nusikaltimai, klaidinančios informacijos skelbimas, manipuliacija, kenkėjiškos programos, šnipinėjimas, įvairios atakos prieš valstybines institucijas ir kt. Europos Sąjungos (toliau – ES) teisėsaugos agentūra (toliau – Europolas) pažymi, kad kibernetiniai nusikaltimai didžiausią pavojų kelia tiek valstybių nacionaliniam saugumui, tiek individualiems asmenims ir visuomenei. Kibernetiniai nusikaltėliai tampa vis agresyvesni, o jų vykdomos veikos tampa vis pavojingesnės ir labiau organizuotos, koordinuotos, siekiant užsibrėžto konkretaus tikslo.*
Šio tyrimo objektas yra kibernetinių nusikaltimų poveikis žmogui. Šio tyrimo objektas apsprendė ir šio tyrimo tikslą, kurio siekiant bus išanalizuotas kibernetinių nusikaltimų poveikis per asmeninio saugumo prizmę žmogui. Siekiant šio tyrimo tikslo atlikta mokslinių straipsnių publikuotų tiek Lietuvoje, tiek užsienyje analizė, įvardijanti kibernetinių nusikaltimų taikinius, kryptis ir poveikį žmogaus finansiniam stabilumui, psichologinei būsenai bei sukeltus neigiamus padarinius. Tyrimu nustatyta, kad pirmiausiai žmogus patiria žalą, kuri gali būti išmatuojama ir išreiškiama pinigine verte. Po to seka daug sunkiau pastebima, išmatuojama ir ne visada vizualiai pastebima neturtinė žala, pasireiškianti žmogaus psichinės sveikatos pablogėjimu, darančiu įtaką įvairioms žmogaus gyvenimo sritims. Šiame straipsnyje siekiama atsakyti į tyrimo iškeltus klausimus: kokias esmines žmogaus teises įtvirtintas nacionaliniuose ir tarptautiniuose teisės aktuose pažeidžia kibernetiniai nusikaltimai? Kokią žalą patiria žmogus tapęs kibernetinio incidento taikiniu? Kaip žmogus reaguoja į kibernetinę ataką? Kaip kibernetinis incidentas paveikia žmogaus finansinį stabilumą, psichiką, savijautą? Tyrime naudojami šie kokybiniai ir kiekybiniai tyrimo metodai: dokumentų analizė, lyginamasis, abstrakcijos, loginis ir kiti tyrimo metodai.

Pagrindinės sąvokos: *kibernetiniai nusikaltimai, poveikis, žmogus, visuomenė, saugumo jausmas, žala, psichinė būsena.*

ISSN 2029-1701
ISSN 2335-2035 (Online)

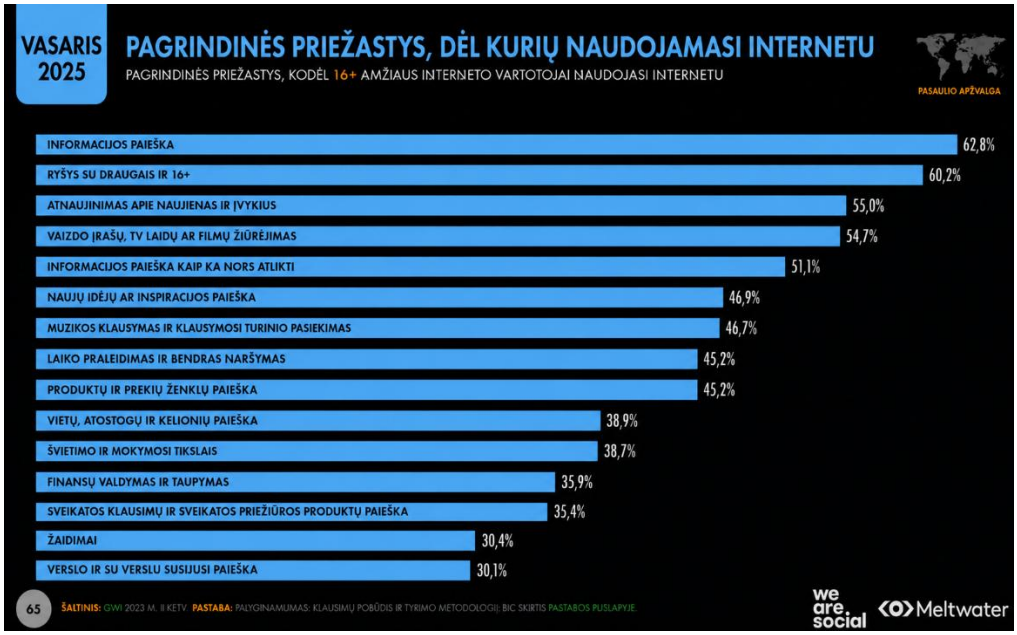
Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2026, Vol. 38, Nr. 2

Įvadas

Gyvenimą gali nugyventi dvejopai: taip, tarsi nieko nėra stebuklingo, arba taip, tarsi viskas yra stebuklinga.

(Albert Einštein)

Skaitmeninis amžius iš esmės pakeitė kasdienės informacijos pateikimą, sklaidą, apdorojimą, saugojimą bei supratimą, tačiau tuo pat metu sukūrė prieigas prie įvairių paslaugų gavimo nuotoliu, atlikti pavestas kai kurias užduotis būnant namuose. Daugelis valstybinių institucijų, privačių ūkio subjektų sudaro galimybes atlikti darbo užduotis darbuotojui nevykstant į darbą. Interneto vartotojų skaičius kasmet auga. Remiantis „Digital 2025“ tyrimo duomenimis, šiuo metu yra 5,56 mlrd. Interneto vartotojų – tai 136 mln. daugiau nei praėjusių metų ataskaitoje, o tai reiškia 2,5 % augimą. Palyginti su pasaulio gyventojų skaičiumi, tai sudaro 67,9 % visų planetos gyventojų. Jei šiuos skaičius suskirstytume pagal lytį, pastebėtume, kad yra skirtumas, 65,7 % visų vartotojų sudaro moterys, o 70 % – vyrai. Kyla klausimas, kokios priežastys skatina žmones naudotis internetu? Atsakymą pateikia „Digital 2025“ ataskaita, kurioje išvardijamos priežastys verčiančios naudotis internetu. Pirmiausiai, ieškoti informacijos, po to, palaikyti ryšius su draugais. Visos priežastys verčiančios naudotis internetu yra išvardintos pav. 1.



Pav. 1. Pagrindinės priežastys, dėl kurių naudojamasi internetu

Kitą vertus, atsivėrusiomis galimybėmis naudotis internetu sumaniai pasinaudojo kibernetiniai nusikaltėliai, dar kai kuriuose tyrimuose įvardijami terminu „finansiniai sukčiai.“ Terminijos vartojimas kibernetinėje erdvėje įvardijant asmenis darančius teisės pažeidimus, kaip kibernetiniai nusikaltėliai, finansiniai sukčiai, gali būti kito tyrimo objektu. Šio tyrimo autoriai terminą finansiniai sukčiai vartos kalbėdami apie kibernetinius nusikaltimus virtualioje erdvėje. Skaitmeninis amžius sukūrė ir naujas grėsmes žmonių, visuomenės, valstybinių institucijų ar net valstybių kibernetiniam saugumui. Kibernetiniai nusikaltimai daro didelę žalą plačiam spektrui skaitmeninių technologijų vartotojams, pradedant ūkio subjektais, valstybinėmis institucijomis ir baigiant fiziniais asmenimis, kuomet atskirų asmenų, ar

organizuotų grupių ar net valstybių neteisėtais veiksmais, sukčiaujant ar kitaip, yra vykdomos duomenų vagystės, įvairūs finansiniai ir ekonominiai nusikaltimai, klaidinančios informacijos skelbimas, kenkėjiškų taikomųjų programų platinimas, pramoninis šnipinėjimas, verbavimo operacijos diversijos aktų atlikimui, strateginę reikšmę valstybei turinčiuose objektuose.

Europolas, atlikdamas kasmetinį grėsmių vertinimą Europos Sąjungoje pažymi, kad kibernetiniai nusikaltėliai tampa vis agresyvesni, o jų vykdomos veikos vis pavojingesnės ir labiau organizuotos. Remiantis Europolo vykdomomis Internet Organised Crime Threat Assessment (toliau – IOCTA) metinėmis ataskaitomis, nuo 2023 m. iki 2024 m. pažymima, kad *milijonai žmonių ES šalyse kiekvieną dieną patiria įvairias kibernetines atakas. Labiausiai vyrauja išpuoliai prieš smulkius bei vidutinius verslus, taip pat skaitmeninės duomenų vagystės ir jų pardavimai, investiciniai sukčiavimai bei nepilnamečių išnaudojimo atvejai pornografijai, įskaitant dirbtinio intelekto sugeneruotą medžiagą*. Remiantis Europolo IOCTA metine ataskaita 2025 m. duomenų vagystės yra įvardijamos kaip didelė grėsmė ekonomikai, valstybinio valdymo procesams. Lietuvoje, remiantis Nacionalinio Kibernetinio Saugumo Centro prie Krašto Apsaugos Ministerijos (toliau – NKSC) teikiamomis metinėmis ataskaitomis apie fiksuotus kibernetinius incidentus, 2024 m. NKSC užregistravo 3 874 kibernetinius incidentus – tai 63 procentais daugiau nei 2023 m. Kibernetinio pobūdžio nusikaltimai yra auganti problema ES valstybėms narėms, kadangi daugumoje yra gerai išvystyta interneto infrastruktūra. Svarbu paminėti, kad *kibernetiniai nusikaltimai įgauna vis didesnį geopolitinį pobūdį – jie taip pat tampa ir viena iš hibridinio karo priemonių. Valstybės vis dažniau pasitelkia kibernetines atakas siekdamos daryti neigiamą įtaką kitoms šalims, pradedant nuo politinių ar ekonominių sistemų, baigiant karinėmis. Tokiu būdu kibernetinės operacijos peržengia tradicines konfliktų ribas ir perauga ne tik į nusikalstamumo, bet ir tarpvalstybinių konfliktų šiuolaikišką formą ir tampa „skaitmeniniu frontu“, kuriame valstybėms tenka ginti savo nacionalinį saugumą ne tik pasitelkiant kariuomenės pajėgas, bet ir skaitmeninės erdvės priemones*

Elektroninė erdvė suteikia naujų galimybių daryti nusikaltimus, sudaro sąlygas atsirasti naujiems nusikaltimų būdams ir vykdyti naujas veikas, iki tol nežinomas teisinėje praktikoje. Kibernetinės atakos tampa viešojo bei nacionalinio saugumo klausimu, o tokių atakų staigus progresavimas didina nepasitikėjimą skaitmenine aplinka ir valstybių gebėjimu joms atsilaikyti. Šiuolaikinės kibernetinės atakos vis dažniau nukreipiamos tiek į asmenų duomenų vagystes, tiek į valstybių kritinę infrastruktūrą ir viešąsias sistemas.

Sutinkamai su Maslow poreikių hierarchija, kuri yra psichologijos idėja, pasiūlyta amerikiečių psichologo Abrahamo Maslow 1943 m. straipsnyje „Žmogaus motyvacijos teorija“ žurnale „Psychological Review“, *saugumo poreikis yra vienas iš esminių žmogaus poreikių hierarchijoje.* Būtent saugumo jausmo nebuvimas ir veda prie to, kad žmonės gana dažnai yra nepatenkinti teisėsaugos institucijų darbu, naujovėmis darbe ir kasdieniniame gyvenime, kurios susijusios su naujų technologijų atsiradimu ir skirtos palengvinti tam tikrų užduočių atlikimą, padidinti darbo produktyvumą.

Žmogus, kuris pajudina kalną, pirmiausia pradeda nešti mažus akmenis.

(Konfucijus)

Kibernetinių nusikaltimų poveikis žmogui

Kibernetiniai nusikaltimai nėra suprantami vien tik kaip techninės prigimties incidentai, jie taip pat akcentuoja ir esminius asmens teisių pažeidimus. Skaitmeninėje erdvėje atliekamos nusikalstamos veikos, dažnai tiesiogiai pažeidžia Lietuvos Respublikos Konstitucijoje

įtvirtintas žmogaus teises. Pvz., Lietuvos Respublikos Konstitucijos 21 str. skelbia, kad „*Žmogaus orumą gina įstatymas*“, o skaitmeninėje erdvėje tai gali apimti priekabiavimą, šmeižtą, patyčias, intymaus turinio platinimą. Lietuvos Respublikos Konstitucijos 22 str. skelbia, kad „*Žmogaus privatus gyvenimas neliečiamas*“, taip pat „*Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami*, *o informacija apie privatų asmenų gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir remiantis įstatymu*.“ Kibernetinių nusikaltimų kontekste tai apima neteisėtą prisijungimą prie paskyrų ar jų perėmimą, šnipinėjimą, duomenų nutekinimą. Tokios veikos be teisėto pagrindo pažeidžia asmens privataus gyvenimo bei susižinojimo neliečiamumą. Skaitmeniniai nusikaltimai taip pat gali pažeisti ir Lietuvos Respublikos Konstitucijos 23 str., skelbiantį, kad „*Nuosavybė neliečiama“* ir *„Nuosavybės teises saugo įstatymai.*“ Tai reiškia, kad neteisėtas skaitmeninėje erdvėje esančio turto (lėšų, kriptoturto vagystės, paskyrų užvaldymas) pasisavinimas nėra tik techninė žala, tokie veiksmai kvalifikuotini kaip konstituciškai saugomos nuosavybės teisės pažeidimas, kuomet dėl nusikalstamų veikų yra patirta turtinė žala. Svarbu paminėti, kad kibernetinė erdvė sukuria ploną ribą tarp informacijos laisvės ir netinkamo informacijos skleidimo. Lietuvos Respublikos Konstitucijos 25 str. nurodo, kad „*Žmogui neturi būti kliudoma ieškoti, gauti ir skleisti informaciją bei idėjas“*, tačiau aiškiai numatomi ribojimai, kuomet „*Laisvė reikšti įsitikinimus ir skleisti informaciją nesuderinama su nusikalstamais veiksmais – tautinės, rasinės, religinės ar socialinės neapykantos, prievartos bei diskriminacijos kurstymu, šmeižtu ir dezinformacija.*“ Tai leidžia teisėtai riboti apgaulingą ar žalingą turinį, neteisėtai gautų duomenų sklaidą ar sukčiavimų mechanizmą, kuomet tai tiesiogiai žeidžia Konstitucijoje ginamas vertybes.

Jeigu kibernetiniai nusikaltimai pažeidžia šalies pagrindiniame įstatyme - Konstitucijoje ginamas žmonių teises ir laisves, valstybės pozityvioji pareiga – jas aktyviai ginti. Tačiau skaitmeniniame amžiuje kibernetinis nusikalstamumas yra plačiai paplitusi problema, kuri virsta iššūkiu tiek visuomenei, tiek valstybei ir nacionaliniam jos saugumui. Kad būtų užtikrintas žmonių kibernetinis saugumas, svarbi tinkama kompetentingų institucijų veikla. Kibernetiniai nusikaltimai neigiamai veikia beveik visus valstybinius sektorius. O tai savo ruožtu paveikia ir žmones. Sutinkamai su Europos Sąjungos kibernetinio saugumo agentūros (ENISA) duomenimis, 2024 m. pagrindinė grėsmė Europoje buvo DDoS atakos, kurios paveikė viešojo administravimo, transporto, bankininkystės ir skaitmeninės infrastruktūros sektorius, taip pat pastebima, kad informacijos manipuliavimo kampanijos daugumoje fiksuotų incidentų, buvo nukreiptos į visuomenę. Todėl kibernetinių nusikaltimų valdymas tampa viešosios politikos bei nacionalinio saugumo klausimu, kuomet valstybės turi užtikrinti efektyvias priemones kovoje su kibernetiniu nusikalstamumu ir tikslu apsaugoti valstybę ir jos žmones (K. Garuckaitė, (2025)). Ryan Shandler ir Miguel Alberto Gomez (2022) pastebi, kad didesnę grėsmę valstybei sukuria ne pati kibernetinė ataka ar „fizinė katastrofa“, o pirmiausia mažėjantis visuomenės pasitikėjimas valdžia bei institucijomis. 2020 m. ransomware kibernetinio viruso pagalba buvo sutrikdyta Diuseldorfo universitetinės ligoninės (Vokietijos Federacinė Respublika) veikla. Dėl atakos sustabdžius dalį paslaugų, pacientai buvo nukreipiami į kitas įstaigas. Atlikus empirinį tyrimą ir po incidento apklausus 707 gyventojus, nustatyta, kad po kibernetinių atakų, ypatingai tokiose įstaigose, ženkliai sumažėja visuomenės pasitikėjimas valdžios gebėjimu apsaugoti nuo kibernetinių išpuolių. Pabrėžiama, kad po kibernetinių atakų, vyriausybės negali tikėtis vieningumo valstybėje, nes visuomenė linkusi manyti, kad valstybė nepakankamai pasirengusi gintis nuo tokio pobūdžio nusikalstamų veikų ir ateityje. Visuomenėje susidaręs požiūris, kad vyriausybė yra atsakinga už kritinės infrastruktūros ir viešųjų institucijų apsaugą kibernetinių atakų kontekste. Tačiau net ir turint pačias sudėtingiausias kibernetinio saugumo priemones, vienas vartotojas, ignoruojantis

saugumo nurodymus ir paspaudęs užkrėstą nuorodą, gali atverti kelią žalingai atakai. Pažymima, kad priklausomai nuo užpuoliko motyvų, pagrindinis atakos tikslas gali būti baimės sėjimas ir visuomenės pasitikėjimo vyriausybės gebėjimu apsaugoti savo piliečius silpninimas (kiberterorizmas). Išskiriama ir kita kibernetinių atakų savybė – jos sukelia bejėgiškumo jausmą. Kalbant apie tradicinius smurto veiksmus, pavyzdžiui raketų ar kitų ginklų atakas, visuomenė žino, kaip nuo jų apsisaugoti – eiti į slėptuves ar vengti tamsių gatvių. Tačiau kibernetinėje erdvėje, dėl jos sudėtingumo kyla bejėgiškumo jausmas, kadangi susidaro įspūdis, kad susiduriama su visagaliais užpuolikais, ir tai gali pakeisti žmonių reagavimo modelius ir paveikti visuomenės pasitikėjimą. Kad būtų užtikrintas saugumas ir kova su nusikaltimais skaitmeninėje erdvėje veiktų kuo efektyviau, svarbus tinkamas valstybės institucijų ir teisėsaugos vaidmuo.

Lietuvoje kibernetinio saugumo užtikrinimas padalytas į politiką formuojančių, ją įgyvendinančių bei priežiūrą vykdančių institucijų sistemą, kurių sąveiką reguliuoja Lietuvos Respublikos kibernetinio saugumo įstatymas. „Kibernetinio saugumo politiką formuoja jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. Kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Lietuvos policija ir Valstybinė duomenų apsaugos inspekcija.“ Nacionalinis kibernetinio saugumo centras aptinka grėsmes, analizuoja kibernetinio saugumo spragas ir incidentus, valdo juos pagal Vyriausybės tvirtinamą nacionalinį planą, teikia įspėjimus ir pagalbą subjektams, o prireikus gali duoti nurodymus paslaugų tiekėjams riboti paslaugas ar blokuoti kenkėjiškų svetainių domenus, taip ribojant jų poveikį bei plitimą. Valstybinė duomenų apsaugos inspekcija vykdo kibernetinio saugumo politiką asmens duomenų apsaugos srityje, atlieka priežiūros institucijos užduotis pagal bendrąjį duomenų apsaugos reglamentą (toliau – BDAR) – taip užtikrinant duomenų apsaugos ir kibernetinio saugumo sąveiką bei nuosekliai valdant asmens duomenis paveikusius incidentus. Lietuvos Policija sustiprina ir įgyvendina kibernetinio saugumo politiką ir turi teisę gauti bei tvarkyti duomenis ar informaciją apie incidentus nusikalstamų veikų, prevencijos, analizės, tyrimo ar atskleidimo tikslais bei gauti informaciją iš kibernetinio saugumo subjektų, reikalingą analizuojant ir vertinant, ar incidentas turi nusikalstamos veikos požymių. Taip pat, jei elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų gavėjas dalyvauja ar jo naudojama informacinių technologijų įranga naudojama nusikalstamai veikai, turi teisę duoti nurodymą riboti paslaugų teikimą (ne ilgiau kaip 48 valandoms) (K. Garuckaitė (2025)).

Kibernetinių nusikaltimų poveikis neišvengiamai kelią grėsmę žmonių saugumui ir yra nukreiptas į šias tris kryptis: finansinę, psichologinę bei reputacinę. Finansinė žala suprantama, kaip dėl patirtų kibernetinių atakų norint atgauti užšifruotus duomenis tenka mokėti išpirkas, kenkėjiškomis programomis sutrikdyta įmonių veikla lemia negautas pajamas, taip pat pagal suklastotus laiškus atlikti piniginiai mokėjimai patenka į sukčių banko ar virtualių pinigų sąskaitas ir pan. Tuo pat metu gana dažnai patiriamas netiesioginis finansinis poveikis. Pavyzdžiui, paslaugų ar paskyrų praradimas. Lietuvos Pinigų plovimo prevencijos kompetencijų centras išskiria penkis sukčiavimo būdus daromus kibernetinėje erdvėje: 1) romantinis, 2) investicinis, 3) telefoninis, 4) avansinis ir 5) phishingas

2023-2025 m. statistiniai duomenys rodo, kad kibernetiniais nusikaltimais padaroma vis didesnė žala vertinant pinigine išraiška. Pvz., Jungtinių Amerikos Valstijų Federalinio Tyrimo Biuro (toliau – FTB) parengtoje internetinių nusikaltimų ataskaitoje (2025) nurodoma, kad 2024 m. buvo gauta 859 532 skundų dėl įtariamų internetinių nusikaltimų, o nuostoliai viršijo 16 mlrd. JAV dolerių. Tai 33 % daugiau nei 2023 m. Trys dažniausiai pasitaikantys kibernetiniai nusikaltimai, skaičiuojant pagal 2024 m. pareiškėjų nukentėjusių nuo kibernetinių nusikaltimų pateiktų skundų skaičių, buvo: 1) sukčiavimas elektroniniu būdu

(phishing/spoofing), 2) reketas, 3) asmens duomenų pažeidimai. Didžiausius nuostolius – iš viso daugiau nei 6,5 mlrd. JAV dolerių – patyrė investicinio sukčiavimo aukos, ypač susijusios su kriptovaliuta. Vokietijos internetinė platforma „Statista“, kurios specializacija yra duomenų rinkimas ir vizualizavimas, pateikia duomenis apie kibernetiniais nusikaltimais padaromą žalą, įvertindama tai pinigine išraiška. Remiantis skaičiavimais, 2025 m. kibernetiniai nusikaltimai kainavo 10,29 trilijono JAV dolerių visame pasaulyje, o iki 2029 m. ši suma, kaip prognozuojama, išaugs iki maždaug 16 trilijonų JAV dolerių. „Cybersecurity Ventures“ (2020) prognozuoja, kad per ateinančius penkerius metus pasaulinės išlaidos, susijusios su kibernetiniais nusikaltimais, augs 15 procentų per metus ir 2025 m. pasieks 10,5 trilijono JAV dolerių per metus, palyginti su 3 trilijonais JAV dolerių 2015 m. Tai yra didžiausias ekonominės gerovės perkėlimas istorijoje, keliantis grėsmę inovacijų ir investicijų skatinimui, ir yra eksponentiškai didesnis už per metus stichinių nelaimių padarytą žalą ir bus pelningesnis nei visų pagrindinių nelegalių narkotikų pasaulinė prekyba kartu sudėjus. Kibernetinių nusikaltimų išlaidos apima duomenų sugadinimą ir sunaikinimą, pavogtus pinigus, prarastą produktyvumą, intelektinės nuosavybės vagystę, asmeninių ir finansinių duomenų vagystę, pasisavinimą, sukčiavimą, įprastos verslo veiklos sutrikdymą po atakos, kriminalistinį tyrimą, įsilaužtų duomenų ir sistemų atkūrimą bei ištrynimą ir reputacijos pažeidimą.

Kibernetiniai nusikaltimai pasireiškia įvairiomis formomis – tarp jų yra sukčiavimas elektroniniu paštu, išpirkos reikalaujantys virusai, prisijungimo duomenų vagystės, sukčiavimas ir kt. Iš pateiktos informacijos nėra aišku, ar į sąvoką „kibernetiniai nusikaltimai“ įtraukiami ir kibernetiniai incidentai, nusikalstamos veikos, apie kurias nebuvo pranešta teisėsaugos institucijoms. Kibernetiniai incidentai ir kibernetiniai nusikaltimai nėra tapatūs reiškiniai. Lietuvos Respublikos krašto apsaugo ministro 2023 m. spalio 16 d. įsakymu Nr. V-840 „Dėl tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo” 2 punkto „Vartojamos sąvokos“ 2.1 papunktyje pateikiama „kibernetinio incidento“ samprata, kuri išdėstoma taip: „*Kibernetinis incidentas – įvykis ar veika kibernetinėje erdvėje, galintis sukelti arba sukeliantis grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintis trikdyti arba trikdantis ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą*.“ Atkreiptinas dėmesys, kad ne kiekvienas kibernetinis incidentas turi nusikalstamos veikos požymių (informacijos sunaikinimas ar pakeitimas, kompiuterių tinklo trikdymas, neteisėtas prisijungimas ir informacijos pasisavinimas, neteisėtas disponavimas kitais įrenginiais ir duomenimis ar pan.). Taigi, jei kibernetinis incidentas nepriskiriamas incidentų kategorijai, turinčiai nusikalstamos veikos požymių, tai į nusikalstamų veikų registrą nepatenka. Tik baudžiamasis kodeksas/baudžiamasis įstatymas nustato kriterijus, kas gali būti laikoma nusikalstama veika. Pvz., Lietuvos Respublikos baudžiamojo kodekso 2 str. 2 d. skelbia, kad šis kodeksas:1) apibrėžia, kokios veikos yra nusikaltimai ir baudžiamieji nusižengimai, bei jas uždraudžia. Žmogus, ketinantis padaryti nusikalstamą veiką įvertina ir tikimybę būti nubaustas kriminaline bausme už kėsinimąsi į baudžiamuoju įstatymu ginamas vertybes. Naujausių technologijų pasiekimai suteikia pakankamai geras galimybes išvengti baudžiamojo persekiojimo, o dalies socialinių grupių, ypatingai senyvo amžiaus, kibernetinės higienos pradmenys nėra pakankami. Mokslininkai Sergiu Cernomoreț ir Andrei Nastas (2023, p. 54), analizuodami kibernetinius nusikaltimus ir baudžiamosios atsakomybės taikymo ypatumus akcentuoja, kad šiuolaikinėje teisinėje sistemoje kibernetiniai nusikaltimai pasižymi tam tikromis ypatybėmis ir kelia tam tikrus iššūkius atskleidžiant aukštųjų technologijų nusikaltimus, o būtent:

1. Techninis sudėtingumas*. Kibernetiniai nusikaltimai dažnai susiję su pažangių ir sudėtingų technologijų, pavyzdžiui, įsilaužimo ar kenkėjiškų programų, naudojimu. Tai kelia sunkumų nustatant ir sekant nusikaltėlius, renkant skaitmeninius įrodymus bei suprantant su nusikaltimais susijusias technines detales;*

2. Tarptautinis pobūdis. *Internetas nepripažįsta sienų, o tai reiškia, kad kibernetiniai nusikaltimai gali būti padaromi nuotoliniu būdu, o nusikaltėliai gali būti kitose jurisdikcijose. Tai kelia jurisdikcijos ir tarptautinio bendradarbiavimo klausimus atliekant nusikaltimų tyrimą ir baudžiamąjį persekiojimą;*

3. Anonimiškumas ir pseudonimiškumas. *Naudojimasis internetu leidžia nusikaltėliams veikti anonimiškai arba paslėpti savo tikrąją tapatybę už pseudonimų ar netikrų IP adresų. Dėl to tampa sunkiau identifikuoti nusikaltėlius ir patraukti juos baudžiamojon atsakomybėn;*

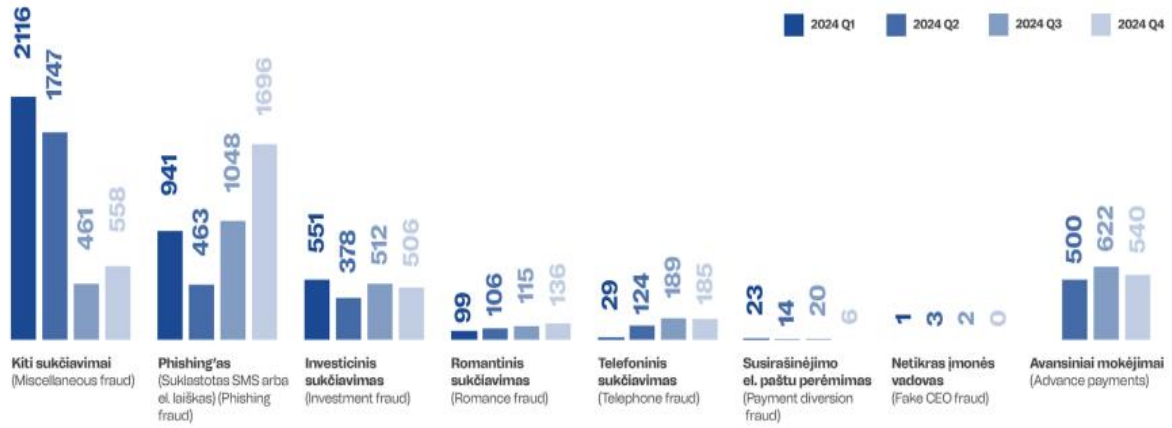
4. Žalos nematerialus pobūdis*. Kibernetinių nusikaltimų atveju žalą gali būti sunku įvertinti, nes ji dažnai yra nematerialaus pobūdžio, pavyzdžiui, informacijos vagystė, reputacijos sugadinimas ar duomenų praradimas. Tai gali turėti įtakos baudžiamojo persekiojimo procesui ir žalos atlyginimui;*

5. Technologijų pokyčių sparta. *Technologijos sparčiai tobulėja, o kibernetiniai nusikaltėliai nuolat randa naujų būdų nusikaltimams daryti. Baudžiamosios teisės sistema turi nuolat prisitaikyti prie šių pokyčių ir atnaujinti teisės aktus, kad galėtų reaguoti į naujas grėsmes.*

Visuma veiksnių, išvardintų šiame tyrime aukščiau, skatina kibernetinius nusikaltėlius perkelti savo veikas iš materialaus pasaulio į virtualų.

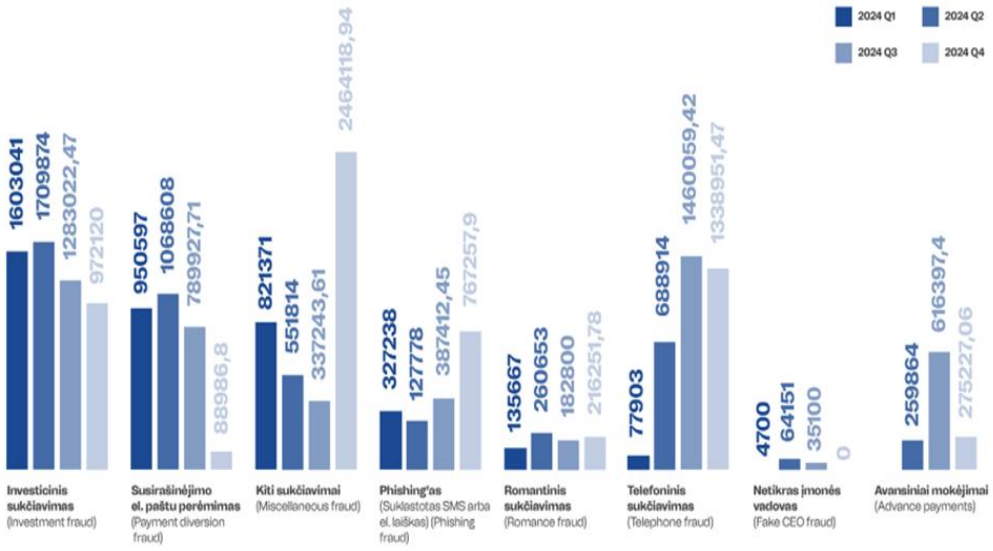
Lietuvos Respublikos Pinigų plovimo prevencijos kompetencijų centro atlikta analizė nurodo, kad Lietuvoje didžiausią riziką verslams kelia socialinės inžinerijos pagrindu vykdomos nusikaltimų schemos, kurios *apima investicinį, telefoninį sukčiavimą, elektroninių paštų perėmimą, „netikrą įmonės vadovą“. Kibernetinės atakos dažnai yra nusitaikiusios į įmonių darbuotojus ir finansinius procesus. Nuostoliai susidaro ne tik iš į sukčių sąskaitas pervestų lėšų, bet ir iš operacinių trikdžių ir skiriamų išteklių siekiant atkurti sutrikdytą veiklą.*

Lietuvos Respublikos Pinigų plovimo prevencijos kompetencijų centras (toliau - PPPKC) pagal iš finansų įstaigų AB „Swedbank“, Revolut Bank, AB SEB banko, UAB, Luminor Bank AS Lietuvos skyriaus, AB Šiaulių banko, OP Corporate Bank plc. Lietuvos filialo, AS „Citadele bankas“ Lietuvos filialo ir UAB URBO banko pateiktus duomenis 2024 m. pateikia sukčiavimo atvejų analizę ir išsamią statistikos analizę apie finansinių sukčių vykdomas neteisėtas veikas kibernetinėje erdvėje. PPPKC atlikta analizė rodo, kad sukčių atakos kibernetinėje erdvėje tampa vis intensyvesnės. Pvz., pirmąjį 2024 m. ketvirtį finansiniai sukčiai kėsinosi išvilioti 6,9 mln. Eur, o antrąjį ketvirtį ši suma išaugo iki 8,3 mln. Eur. Trečiąjį ketvirtį siekiama išvilioti suma pasiekė 8,9 mln. Eur. O ketvirtą 2024 m. ketvirtį ši suma siekė net 10,1 mln. Eur. Pateikti statistiniai duomenys vaizdžiai iliustruoja kibernetinių nusikaltimų mastus, daromą žalą žmogui ar tai būtų fizinis asmuo, ar ūkio subjekto vadovas. Finansiniai sukčiai taikosi apgaulės būdu išvilioti turtą, kuris yra išmatuojamas pinigine išraiška. Žemiau pateikiamos dvi lentelės apie sukčiavimo tipologijas pagal incidentų skaičių, matuojant vienetais ir pagal iš gyventojų išviliotas lėšas, matuojamas pinigine išraiška – Eurais, suskirstant 2024 m. į keturis ketvirčius - 2024 m. 1 ketvirtis (sausis - kovas) toliau - Q1, 2 ketvirtis (balandis-birželis) toliau - Q2, 3 ketvirtis (liepa-rugsėjis) toliau Q3 ir 2024 m. 4 ketvirtis (spalis-gruodis) toliau - Q4.



Pav. 2. Sukčiavimo tipologijos pagal incidentų skaičių, vnt.
Šaltinis: *Pinigų plovimo prevencijos kompetencijų centras, „Sukčiavimo atvejų statistikos analizė: 2024 m. IV ketvirtis“, https://amlcenter.lt/wp-content/uploads/2025/02/2024-m.-Sukciavimo-atveju-analize-IV-ketvirtis.pdf.*

Kaip matome iš pav. 2 pateiktų duomenų apie sukčiavimo tipologijas pagal incidentų skaičių tai 2024 m. spalio – gruodžio mėnesiais dominavo „Phishing'as“ (suklastotos SMS arba el.laiškai) (angl. Phishing fraud), kurie sudarė 1 696 atvejus.



Pav. 3. Sukčiavimo tipologijos pagal iš gyventojų išviliotas lėšas, Eur
Šaltinis: *Pinigų plovimo prevencijos kompetencijų centras, „Sukčiavimo atvejų statistikos analizė: 2024 m. IV ketvirtis“, https://amlcenter.lt/wp-content/uploads/2025/02/2024-m.-Sukciavimo-atveju-analize-IV-ketvirtis.pdf.*

Kaip matome iš pav. 3 pateiktų duomenų apie sukčiavimo tipologijas pagal iš gyventojų išviliotas lėšas Eurais, tai 2024 m. Q4 pastebimas ženklus sumažėjimas, kai finansiniai sukčiai išgaudavo lėšas perimdami susirašinėjimą elektroniniu paštu, tačiau telefoninis sukčiavimas kelia nerimą. 2024 m. Q3 išviliota suma siekė virš 1.4 mln. Eur, Q 4 – virš 1.3 mln. Eur.

Kibernetiniais nusikaltimais greta turtinės žalos, kurią įmanoma iš dalies įvertinti pinigine išraiška, dar padaroma ir neturtinė žala. Kibernetinio incidento, teisės pažeidimo atveju nukentėjęs asmuo gali patirti ir dvasines, psichines kančias bei specifinius fiziologinius pokyčius. Visa tai neigiamai veikia dvasinę žmogaus savijautą. Lietuvos Respublikos Konstitucijos 30 str. skelbia, jog asmeniui padarytos materialinės ir moralinės žalos atlyginimą nustato įstatymas. Taigi, Lietuvos Respublikos piliečių priimta 1992 m. spalio 25 d. referendume Lietuvos Respublikos Konstitucija įtvirtino Lietuvos teisės istorijoje moralinės žalos atlyginimo nuostatą Konstituciniu lygmeniu. Šiuo atveju kyla klausimas, kas tai yra moralinė žala? Ar moralinė žala ir neturtinė žala yra vienas ir tas pats? Mokslininkas A. Rudzinskas pateikia neturtinės žalos sampratos paaiškinimą, kuris skamba taip: „*neturtinė žala yra ne kas kita kaip pakenkimas fizinio asmens sveikatai, tiksliau – psichinei sveikatai, kuri yra valstybės teisinės apsaugos objektas.*“ Taigi tiksliausiai neturtinę (moralinę) žalą apibūdintume kaip psichinę žalą, nes tada aiškiai suprastume, koks teisinės apsaugos objektas yra pažeistas. A. Rudzinskas atkreipia dėmesį, jog terminai „neturtinė žala“ ir „moralinė žala“ neatspindi, kokioms vertybėms padaroma žala, o tarpusavyje jie skiriasi tik lingvistine prasme. Šiuo metu galima konstatuoti, jog dabar teisės sistemoje ir teisininkų sąmonėje stipriai įsitvirtinę du terminai – „moralinė žala“ ir „neturtinė žala“, kurie vartojami kaip sinonimai. A. Rudzinskas apibendrinęs neturtinės žalos sampratas tiek užsienio, tiek Lietuvos konstatavo, jog neturtinė žala – tai tam tikri glausti neigiami asmens psichikos pakitimai, kurie būtinai įvyksta jo sąmonėje pažeidus asmenines neturtines ir turtines vertybes. Tai gali pasireikšti nemaloniais kūno pojūčiais (pakilusiu kraujo spaudimu, pykinimu ir pan.), sutrikusiomis emocijomis, elgesio pakitimais, nerviniais tikslais. Visa tai paveikia fizinio asmens savijautą. Nukentėję nuo kibernetinių nusikaltimų žmonės dažnai patiria emocinę ir psichologinę įtampą. 2019 m. Jungtinėje Karalystėje apklausus 2 450 sukčiavimo ir kibernetinių nusikaltimų aukų, net 83 proc. teigė jaučiantys pyktį, 73 proc. – nerimą, o beveik pusė apklaustųjų nurodė sumažėjusį pasitikėjimą kitais (48 proc.) ir 29 proc. – mažesnį norą naudotis internetu. Kibernetinio smurto ar nusikaltimų kontekste, reputacinė žala paveikia galimybes susirasti darbą ar būstą, taip pat gali būti panaudojama kaip spaudimo ir šantažo instrumentas (Muaadh Mukred, Umi Asma' Mokhtar, Fahad Abdullah Moafa, Abdu Gumaei, Ali Safaa Sadiq, Abdulaleem Al-Othmani (2024), 1-18). Tapimas kibernetinio nusikaltimo auka gali turėti daug neigiamų pasekmių. Pavyzdžiui, finansinių nuostolių ir psichologinio poveikio (Sarkki (Pirkka) P.A.H. & others (2025)).

Mokslininkai Whitty M. T. ir Buchanan T. interviu būdu 2016 m. apklausė 20 nukentėjusiųjų nuo kibernetinių nusikaltimų Jungtinėje Karalystėje. Whitty M. T. ir Buchanan T. apklausos rezultatus padalino į 7 kategorijas (šiame tyrime autoriai pristato tris kategorijas asmenų nukentėjusių nuo kibernetinių nusikaltimų, kurie akcentavo patirtą neturtinę žalą, jos padarinius psichinei būsenai). 1. „Emocinė/psichologinė būsena po romantinio sukčiavimo“. Visi apklaustieji, neatsižvelgiant į tai, ar jie patyrė turtinę/neturtinę žalą buvo neigiamai paveikti romantinio sukčiavimo. Jie patyrė emocinius išgyvenimus – gėdos jausmą, sumišimą, šoką, pyktį, susirūpinimą ir stresą (ypač tie, kurie buvo įtraukti į pinigų plovimą ar padėjo nusikaltėliams įgyti vizą), baimę ir pyktį dėl to, jog buvo psichiškai išprievartauti. 2. „Kiti asmenys nukentėjusiųjų gyvenime“. Svarbūs asmenys romantinio sukčiavimo aukai, pavyzdžiui nukentėjusiojo šeima, draugai, bendradarbiai dažniausiai nesuteikė socialinės paramos. Aukos teigia, jog kiti asmenys galvojo, jog jos yra kvailos, jie buvo pikti ar nusivylę dėl to, jog aukos patyrė turtinę žalą (iššvaistė jų palikimą) ir dėl to nesuteikė jokios socialinės paramos. Didžioji dalis respondentų dėl galimo neigiamo požiūrio *į juos apie tai, jog buvo apgauti nepranešė niekam išskyrus teisėsaugos institucijų pareigūnus bei apklausos atlikėją. 3. „Nukentėjusiojo pasikeitimas ir socialinė situacija“. Nukentėjusieji patvirtino, jog jų elgesys*

pasikeitė. Tai buvo neigiamo pobūdžio pasikeitimas. Kai kuriems šis pasikeitimas sumažino pasitikėjimą kitais žmonėmis. Taip pat nukentėjusieji sumažino bendravimą su savo draugais, aplinkiniais asmenimis. Taigi, minėtas tyrimas patvirtino, kad nukentėjusieji romantinio sukčiavimo modelio metu patiria ne tik turtinę, bet ir psichologinę žalą.

Taip pat atkreiptas dėmesys, kad kibernetinių nusikaltimų kontekste pažeidžiamiausių asmenų grupei priskiriami vyresnio amžiaus žmonės, tačiau labai svarbu paminėti augantį ir nerimą keliantį vaikų išnaudojimą skaitmeninėje erdvėje. Finansinių veiksmų darbo grupės (FATF) ataskaitoje (2025) „**Detecting, Disrupting and Investigating Online Child Sexual Exploitation**“ konstatuojama, kad seksualinis vaikų išnaudojimas tampa dominuojančia bei kibernetiškai sudėtinga nusikalstama veika. Išskiriami du šio nusikaltimo tipai: tiesiogiai transliuojamas seksualinis vaikų išnaudojimas, siekiant finansinės naudos, kai vaikas vaizduojamas užsiimantis seksualine veikla vienas ar su kitais asmenimis, o vartotojai moka, kad galėtų tokį turinį stebėti nuotoliniu būdu ir finansinis vaikų seksualinis šantažas, kuris apima grasinimus paviešinti vaikų seksualinio pobūdžio nuotraukas ar vaizdo įrašus, jei aukos nepatenkins finansinių reikalavimų. Pabrėžiama, kad šių nusikaltimų mastas yra labai didelis ir 300 mln. vaikų visame pasaulyje, arba 1 iš 8 vaikų, kasmet patiria seksualinį išnaudojimą ir prievartą internete. Padariniai aukoms ir jų šeimoms yra sunkūs ir ilgalaikiai, o kai kurios situacijos netgi baigėsi savižudybe. Įdomu tai, kad tokiomis veikomis užsiima tiek vyrai, tiek moterys, o seksualiai išnaudojančios vaikus moterys itin dažnai pačios turi vaikų. Ataskaitoje aprašomi realūs pavyzdžiai, kaip vyksta seksualinis vaikų išnaudojimas internete. Dažniausiai pasitaikantys atvejai, kuomet vaikams virtualiai bendraujant su nepažįstamu asmeniu jis įgauna vaiko pasitikėjimą, tuomet atsiunčia intymaus turinio nuotraukas ir prašo to paties iš vaiko, vaikui įvykdžius nusikaltėlio prašymą, gaunama žinutė su nuoroda sumokėti tam tikrą pinigų sumą, kitu atveju nuotrauka bus paviešinta internete. Aukų pranešimai yra daugelio nusikaltimų atskleidimo būdas, tačiau šiuo atveju taip nėra, kadangi aukos jaučia gėdą ir nenori, kad kas nors apie tai sužinotų. Atskaitoje teigiama, kad seksualinis vaikų išnaudojimas internete yra mažai pranešamas nusikaltimas, nors jo mastas yra didelis. Pasak šio straipsnio bendraautorės K. Garuckaitės (2025) susidariusi situacija kelia didelį susirūpinimą, kadangi nusikaltėliai veikia koordinuotai ir organizuotai, o mažas pranešimų kiekis jiems leidžia ir toliau netrukdomai vykdyti amoralias nusikalstamas veikas, kuriose figūruoja ir vaikai. Mokslininkų Babu J., Justin, P. J., Rejina P. V. & kitų (2025) atliktas tyrimas nustatė, kad tarp neigiamą poveikį asmenims sukeliančių veikų skaitmeninėje erdvėje, išskiriamas ir virtualus smurtas. Jis gali apimti kibernetines patyčias, neapykantos kurstymą ar intymaus turinio platinimą, tokie veiksmai daro ne tik psichologinę, tačiau ir reputacinę žalą, kuri pasireiškia socialine atskirtimi ir sukelia kliūčių įsidarbinti ar susirasti būstą. Pastebimas ryšys tarp kibernetinių patyčių ir depresijos, nerimo bei savižudiškų minčių, o tai ilgainiui mažina visuomenės įsitraukimą ir pasitikėjimą skaitmenine erdve.

Kibernetinių nusikaltimų latentiškumas visame pasaulyje yra didelis. Priežastys, veiksniai sąlygojantys tokią situaciją yra įvairūs. Dalis jų įvardintos Cernomoreț S. ir Nastas A. (2023, p. 54) jau cituotos šiame straipsnyje, kita priežastis, kuriai šio tyrimo autoriai irgi pritaria, yra ta, kad teisėsaugos veikloje pirmenybė teikiama sudėtingiausiems ir didžiausią rezonansą sukeliantiems atvejams, kuriuos reikia **nedelsiant išspręsti** (Komarov, A. A. 2024). Kaip matome, tik tam tikra dalis kibernetinių nusikaltimų tampa matomais, t. y. užregistruoti pranešimų apie nusikalstamas veikas registre. Kita dalis lieka už oficialiosios statistikos. Kodėl? Šio tyrimo vienas iš bendraautorių G. Bučiūnas atliko interviu su dviem verslininkais, esant jų sutikimams apie situacijas, jeigu kibernetinis nusikaltimas būtų nukreiptas prieš juos ar jų įmones. Šio tyrimo bendraautorius uždavė klausimą: ar jie iš karto informuotų teisėsaugos institucijas apie kibernetinį nusikaltimą? Pvz., finansinių sukčių išviliotus pinigus iš jų

asmeniškai ir iš jų įmonės. Respondentai atsakė, kad jie gerai pagalvotų, prieš kreipdamiesi į teisėsaugos institucijas. Pirmiausia, tai gėdos jausmas, reputacijos išlaikymas tarp kolegų verslininkų. Dabartinėje visuomenėje svarbu išlaikyti sėkmingo žmogaus statusą, o čia sukčiai išviliojo pinigus gana įprastoje situacijoje. Kitas klausimas, ar policija gebės ištirti, kiek laiko man teks su jais bendrauti, o jei jau policija užregistruos nusikalstamą veiką, tai kas gali paneigti, kad neteks turėti reikalų su kitomis valstybinėmis institucijomis. Pvz., Valstybine Asmens duomenų inspekcija. Bendravimas su policija, kitomis institucijomis pareikalaus laiko sąnaudų. Taigi, vien tik iš šio interviu galima išskirti keletą priežasčių, kodėl nenorima kreiptis į teisėsaugos institucijas ir informuoti apie įvykį. McLeodas, daugiau kaip 30 m. dirbantis kibernetinio saugumo srityje įvardijo žmogaus nenorą informuoti apie kibernetinį nusikaltimą įvykdytą jo ar ūkio subjekto atžvilgiu. *Verslo atstovai stengiasi apie tai kuo mažiau kalbėti, jie nerimauja dėl jų reputacijos verslo aplinkoje. Kai tai nutinka pavieniams asmenims, atsiranda visai kitas veiksnys, verčiantis žmones apie tai tylėti. Dažniausiai tai susiję su gėda ir nepatogumu (David Burke, CBC News, 2019).*

Taigi, nusikaltimai skaitmeninėje erdvėje nėra vien tik techniniai incidentai, jie pažeidžia Konstitucijoje, kituose teisės aktuose ginamas vertybes ir padaro žalą asmenų informaciniam saugumui. Asmuo, patyręs kibernetinę ataką, ne visada tai pajaučia tiesiogiai, pvz., sulėtėjęs kompiuterio darbas. Fizinis asmuo pastebi kibernetinį nusikaltimą, pirmiausiai kai pajunta turtinę žalą. Pvz., pinigai iš jo banko sąskaitos nukeliavo finansiniams sukčiams. Galima kita situacija, kuomet gali kilti finansiniai nuostoliai paviešinus internete tam tikrą informaciją apie fizinį asmenį. Pvz., apie jo sveikatos būklę. Gavus iš kibernetinių nusikaltėlių reikalavimą mokėti pinigus ar praradus pinigines lėšas reikia priimti sprendimą. Iškyla dilema: viešinti faktą, kad buvai apgautas ar palikti tai paslaptyje. Jei viešinti, tai kam patikėti informaciją. Ar įtraukti šeimos narius, artimiausius draugus į negatyvaus įvykio aptarimą, sprendimų paiešką. Tai sukelia stresą, koreguoja psichologinę asmens būseną. Tai gali pasireikšti užsidarymu, suirzimu, nenoru bendrauti. Tai gali sukelti papildomų neigiamų pasekmių nuo kibernetinio nusikaltimo finansiškai nukentėjusiam žmogui. Aplinkiniai tai gali priimti kaip arogantiškumo, pasipūtimo ženklus, o jeigu paviešinsi – tai galimos patyčios, ypač tai aktualu jauno amžiaus asmenų grupėse. Naujausi tyrimai rodo, kad Lietuvoje patyčių mokyklose ir internete mastas išlieka vienas didžiausių Europoje – patyčias patiria trečdalis paauglių (Luščinskytė, J., Bieliauskaitė, K., LRT RADIJO laida „Lietuvos diena“, LRT.lt. (2025). Jei priimtas sprendimas nesikreipti į teisėsaugos institucijas dėl patirtos turtinės žalos, tai siekis suvaldyti neturtinės žalos padarinius, pablogėjusią nuotaiką, suirzimą, veda į paieškas priemonių, kurios padėtų atstatyti psichologinę pusiausvyrą, suvaldyti stresą. Įvairiose socialinėse grupėse. Pvz., verslininkų, paauglių tarpe labiau gerbiami sėkmingi asmenys, o ne tie, kuriems nepasisekė. Juo labiau, kad daugelis yra socialinių tinklų vartotojai, susieti vienas su kitu ir vyraujantis interneto reiškinys, kuris įvardijamas terminu „patinka kultūra.“ Socialinių tinklų vartotojų aktyvumas ir socialinis pripažinimas vertinami pagal statistinius rodiklius (kiek kartų paspausta nuoroda „patinka“, kiek buvo pasidalijimų, peržiūrų skaičius). Žmogus dažnai negyvena uždaroje erdvėje, o siekia būti tam tikrame rate, dar kitaip galima pavadinti informaciniame burbule. Tai skatina jį kurti tam tikrą skaitmeninį turinį internete, pvz., patalpinant nuotraukas, pasidalijant savo įspūdžiais apie kelionę ir platinti tam tikrame rate. Pvz., socialiniame tinkle „Facebook“ draugų rate ir žinoma sulaukti paspaudimų „patinka.“ Tai pakelia nuotaiką, savivertę. Juk retas kuris išdrįs pateikti informaciją, kad buvo apgautas finansinių sukčių, ir laukti aplinkinių reakcijos. Neturtinės žalos poveikis padaromas fiziniam asmeniui sunkiai gali būti įvertinamas pinigine išraiška. Priežastys, kodėl fizinis asmuo nenori kreiptis į teisėsaugos institucijas, šio tyrimo autorių nuomone, remiantis praktinio darbo patirtimi teisėsaugos srityje tiriant nusikalstamas veikas gali būti įvairios, pradedant gėda, juk tokioje paprastoje situacijoje

kvailai pasielgiau, pasiteisinant, kad buvo užkluptas staiga, netinkamu laiku ir vietoje. Kita dažna priežastis stabdanti paviešinti informaciją, kad tapai kibernetinio nusikaltimo taikiniu ir nukentėjai yra stoka pasitikėjimo teisėsaugos institucijomis. Pvz., policijai trūksta įgūdžių ir žinių, specialios programinės įrangos nustatyti kibernetinius nusikaltėlius ir beveik netikint kad pavyks susigrąžinti išviliotus pinigus. Reputacijos praradimas taikytinas tiek ūkio subjektams/ pvz., įmonės bijo, kad atskleidus apie kibernetinio saugumo pažeidimą įmonės informacinėje sistemoje, ar elektroninių duomenų pavogimas, sumažins jų reputaciją, klientų pasitikėjimą ir įmonės rinkos vertę. Tai dar gali patraukti institucijų, atsakingų už kibernetinį saugumą, duomenų apsaugą dėmesį. Fiziniai asmenys, ypač paaugliai, ar asmenys užimantys visuomenės hierarchijoje aukštą vietą, pvz., sėkmingas verslininkas ir tuo pačiu verslo draugijų narys gerai įvertins rizikas, keliančias jo reputacijai, prieš viešindamas faktą, kad nukentėjo nuo finansinių sukčių. Kita priežastis nesikreipti, gali būti patirtos turtinės žalos suma dėl kibernetinio nusikaltimo. Jei suma nedidelė vertinant ūkio subjekto apyvartos mastu, tai nukentėjusysis gali laikyti nusikaltimą pernelyg nereikšmingu, kad vertėtų kreiptis į teisėsaugos institucijas. Kita priežastis dėl kurios nukentėjusieji nesikreipia, tai dėl žinių stokos apie kibernetinę higieną, dažnai žmonės net nesuvokia, kad tapo kibernetinės atakos taikiniu.

Kibernetinių nusikaltimų poveikis žmogui pasireiškia ne tik finansiniais praradimais, o taip pat, tiesiogiai daro įtaką žmogaus sveikatos būklei, pradedant pablogėjusia psichine būkle. Oliveira, C., Saka, M., Bone, L. and Jacob, R. (2023) atliko tyrimą, kuriuo siekė išnagrinėti psichinės sveikatos ir prarasto darbo našumo sąsajas. Atlikus tyrimą buvo rasta aiškių įrodymų, kad prasta psichinė sveikata, paprastai vertinama kaip depresija ir (arba) nerimas, buvo susijusi su darbo našumo sumažėjimu, kuris Lietuvoje dar stipriai atsilieka nuo ES vidurkio (**Assessment of the labour productivity developments in Lithuania and the EU, 2022**). Su žmogaus saugumo jausmu yra susijęs ir Pasaulio laimės indeksas (angl. World Happiness Report), kuriame Lietuvos Respublika nukrito iš 16 vietos 2025 m. net į 28 vietą 2026 m. (World Happiness Report 2026). Laimės vertinimo indeksas paprastai siejamas su šešiais pagrindiniais veiksniais, iš kurių su šiuo tyrimu sietini šie du veiksniai: laisvė priimti sprendimus ir pasitikėjimas valdžia. Ekonomistas Nerijus Mačiulis neseniai analizavo, kodėl Lietuva nusmuko Pasaulio laimės indekso vertinime, juk nebuvo drastiškų pokyčių šalyje. Lietuvos Respublikos vertinime didelės įtakos turėjo socialinės paramos veiksnys, pagal jį iš 3 nukrista į 33 vietą. Tai siejama su saugumo jausmu, o būtent kiek žmogus jaučiasi palaikomas aplinkos, o ne tik su gaunamomis pašalpomis ar finansine parama.

Pažymima, kad kibernetiniai nusikaltimai daro kompleksinį poveikį asmenims, apimantį tiek psichinę būklę, tiek finansinę padėtį. Tyrimai rodo, kad nukentėję nuo kibernetinių atakų asmenys dažnai patiria padidėjusį stresą, nerimą, miego sutrikimus bei sumažėjusį saugumo jausmą, nes tokio pobūdžio nusikaltimai pažeidžia asmens privatumo ir kontrolės suvokimą (Bada, M., Nurse, J. R. C. (2019)). Be to, daugelis kibernetinių nusikaltimų yra paremti socialinės inžinerijos metodais, kurie kaip jau buvo minėta, išnaudoja žmogaus emocijas - pasitikėjimą, baimę ar skubos jausmą, todėl aukos neretai susiduria su kaltės, gėdos jausmais bei sumažėjusiu pasitikėjimu savimi. Tokios patirtys gali lemti ilgalaikius psichologinius padarinius, panašius į potrauminio streso simptomus. Kartu kibernetiniai nusikaltimai turi tiesioginį poveikį asmens finansinei padėčiai, nes dėl sukčiavimo ar tapatybės vagystės patirti nuostoliai dažnai nėra visiškai kompensuojami, o tai gali sukelti ilgalaikį finansinį nestabilumą. Finansiniai sunkumai savo ruožtu didina psichologinę įtampą, nerimą ir socialinę atskirtį, taip sukurdami uždarą neigiamų pasekmių ratą, kuriame ekonominiai praradimai stiprina psichologinius sunkumus, o pastarieji mažina asmens gebėjimą efektyviai atkurti savo finansinę padėtį (Council of the European Union, 2024).

Išvados

Nusikaltimai skaitmeninėje erdvėje nėra vien tik techniniai incidentai, jie taip pat sistemingai pažeidžia Lietuvos Respublikos Konstitucijoje ginamas vertybes.

Kibernetiniais nusikaltimais padaroma turtinė žala, kuri gali būti išmatuojama pinigine išraiška ir neturtinė žala, kurios deja ne visada įmanoma įvertinti pinigais.

Neturtinė žala sietina su žmogaus psichine būkle, kuri daro įtaką tiek fizinio asmens sveikatai, tiek darbo našumui, taip pat daranti įtaką šalies gebėjimui konkuruoti pasaulyje.

Kibernetiniai nusikaltimai dėl įvairių priežasčių pasižymi latentiškumu ir paveikia žmogaus nuostatas į įvairius procesus.

Literatūros sąrašas

1. Assessment of the labour productivity developments in Lithuania and the EU (2022). https://economy-finance.ec.europa.eu/system/files/2023-06/ECFIN-2023-00035-00-00-EN-TRA-00.pdf
2. Babu, J., Justin, P. J.,Rejina P. V. & others (2025). Exploring the impact of cyberbullying on mental health through social media: A visualization and trend analysis. Salud, Ciencia y Tecnología – Serie de Conferencias, 4:1577, p. 1-13. https://www.researchgate.net/publication/390679915_Exploring_the_impact_of_cyberbullying_on_mental_health_through_social_media_A_visualization_and_trend_analysis
3. Bada, M., Nurse, J. R. C. (2019). The Social and Psychological Impact of Cyber-Attacks. P. 1-21. https://arxiv.org/pdf/1909.13256.
4. Bieliauskaitė, K. & Velykis, M. Pasaulio laimės reitinge Lietuva krito 12 vietų: noras lygintis yra peilis. https://www.lrt.lt/naujienos/laisvalaikis/13/2880210/pasaulio-laimes-reitinge-lietuva-krito-12-vietu-noras-lygintis-yra-peilis
5. Bieliauskaitė, K. & Luščinskytė, J., (2025). Patyčių mastas Lietuvoje – vienas didžiausių Europoje: kada paaugliai nebeieško pagalbos? https://www.lrt.lt/naujienos/lietuvoje/2/2449687/patyciu-mastas-lietuvoje-vienas-didziausiu-europoje-kada-paaugliai-nebeiesko-pagalbos
6. Bone, L., Oliveira, C., Saka, M. and · Jacob, R. (2023). The Role of Mental Health on Workplace Productivity: A Critical Review of the Literature. Applied Health Economics and Health Policy, Vol. 21, p. 167–193. https://doi.org/10.1007/s40258-022-00761-w https://pmc.ncbi.nlm.nih.gov/articles/PMC9663290/pdf/40258_2022_Article_761.pdf
7. Burke, D., (2019). Why shame prevents people from reporting cybercrime. CBC News. https://www.cbc.ca/news/canada/nova-scotia/cybercrime-halifax-police-data-computers-1.5055078#:~:text=%22You%20know%2C%20they're,things%20like%20shame%20and%20embarrassment.%22
8. Cernomoreț, S., & Andrei Nastas, A. (2023). Comparative Analysis of Cybercrime in the criminal law system. Adjuris, Bucharest. p. 1-81. https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf
9. Cybercrime magazine. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
10. Cybercrime worldwide - statistics & facts. https://www.statista.com/topics/13546/cybercrime-worldwide/

11. Council of Europe. Convention on Cybercrime. https://rm.coe.int/1680081561
12. Council of the European Union (2024). A cybersecure society – EU policy on cybercrime. https://www.consilium.europa.eu/lt/policies/a-cybersecure-society/ .
13. European Union Agency For Cybersecurity (ENISA). Cyber Hygiene. https://www.enisa.europa.eu/topics/cyber-hygiene
14. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
15. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2022. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf.
16. Europol. Crime Areas / Cyber-attacks. https://www.europol.europa.eu/crime-areas/cybercrime.
17. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf
18. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.
19. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025. Steal, deal and repeat. How criminals trade and exploite your data. https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf
20. FBI Releases Annual Internet Crime Report (2025). https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report
21. Garuckaitė, K., (2025). Kibernetinių nusikaltimų vaidmuo skaitmeniniame amžiuje. Baigiamasis darbas. https://apps.mruni.eu/ords/f?p=110:96:13884723306320:::96:P96_STNR,P96_S,P96_DEST,P96_D,P96_DARBO_TIPAS,P96_T:221096,221096,1277,1277,B,B
22. Gražūs žodžiai apie laimę. Albertas Einšteinas. https://mintys.lt/aforizmai/grazus-zodziai-apie-laime
23. Hellveik, PM., Haugen, L-EA & Överlien, C. (2025). Outcomes of image-based sexual abuse among young people: a systematic review. Forensic and legal psychology. Volume 16 - 2025 | https://doi.org/10.3389/fpsyg.2025.1599087 https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2025.1599087/full
24. Home Office. Research and analysis Experiences of Victims of Fraud and Cyber Crime. https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime/experiences-of-victims-of-fraud-and-cyber-crime
25. How many Internet users are there in the world? https://www.telefonica.com/en/communication-room/blog/internet-users/
26. Kemp, S., & Pérez, N. E., (2023). Consumer Fraud against Older Adults in Digital Society: Examining Victimization and Its Impact. International Journal of Enviromental Research and Public Health, 20/7, p. 1-17. https://www.researchgate.net/publication/369842625_Consumer_Fraud_against_Older_Adults_in_Digital_Society_Examining_Victimization_and_Its_Impact

27. Kirsty, P., Davidson, J. C., Farr R. R., Burkhardt, Ch., Caneppele, S. & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences 2/2, p. 379-398. https://www.mdpi.com/2673-6756/2/2/28
28. Komarov, A. A., (2024). Measuring the latency of crimes committed with the help of information and communication technologies according to the matrix of A. A. Konev's punishability indices. Security Issues, issue 4, p. 31-48. DOI: https://doi.org/10.25136/2409-7543.2024.4.72451 https://journals.rcsi.science/2409-7543/article/view/393536
29. Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis Kodeksas. https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr?csrt=1917517698992855921
30. Lietuvos Respublikos kibernetinio saugumo įstatymas. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.
31. Lietuvos Respublikos Konstitucija. https://www.lrs.lt/home/Konstitucija/Konstitucija.htm
32. Lietuvos Respublikos krašto apsaugo ministro 2023 m. spalio 16 d. įsakymas Nr. V-840 Dėl tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo. https://www.e-tar.lt/portal/lt/legalAct/cea217b06c1011ee8f3cbca2fb16d96d
33. Maslow A. H. (1943). A Theory of Human Motivation. Psychological Review, 50, p. 370-396. https://psychclassics.yorku.ca/Maslow/motivation.htm
34. Microsoft. „Microsoft Digital Defense Report 2024. The foundations and new frontiers of cybersecurity. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf
35. Mukred, M., Mokhtar, U. A., Moafa, F. A., Gumaei,A., Sadiq A. S., Al-Othmani, A. (2024). The roots of digital aggression: Exploring cyber-violence through a systematic literature review. Internal Journal of Information Management Data Insights, Vol. 4 (2), p. 1-18. https://www.sciencedirect.com/science/article/pii/S2667096824000703
36. Nacionalinė kibernetinio saugumo būklės ataskaita: pernai 63 proc. išaugo kibernetinių incidentų skaičius. https://lkpb.policija.lrv.lt/lt/naujienos/nacionaline-kibernetinio-saugumo-bukles-ataskaita-pernai-63-proc-isaugo-kibernetiniu-incidentu-skaicius/
37. Nacionalinis Kibernetinio Saugumo Centras prie Krašto apsaugos ministerijos (NKSC). Nacionalinė Kibernetinio saugumo būklės ataskaita 2024 m. https://vdai.lrv.lt/public/canonical/1748429329/942/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf.
38. Oficialiosios statistikos portalas. „Skaitmeninė ekonomika ir visuomenė Lietuvoje (2023 m. leidimas)“. Žiūrėta 2025 m. spalio 5 d. https://osp.stat.gov.lt/skaitmenine-ekonomika-ir-visuomene-lietuvoje-2023/e-komercija/e-pirkejai.
39. Pinigų plovimo prevencijos kompetencijų centras. Sukčiavimo atvejų statistikos analizė: 2024 m. IV ketvirtis. https://amlcenter.lt/wp-content/uploads/2025/02/2024-m.-Sukciavimo-atveju-analize-IV-ketvirtis.pdf
40. Pinigų plovimo prevencijos kompetencijų centras. Sukčiavimo prevencija gyventojams. https://amlcenter.lt/sukciavimo-prevencija/sukciavimo-prevencija-gyventojams/

41. Rifkin J. (2012). Trečioji pramonės revoliucija. Kaip lateralinės jėgos keičia energetiką, ekonomiką ir visą pasaulį. Eugrimas Vilnius. https://www.lma.lt/uploads/files/KNYGOS/Trecioji_pramones_evoliucija__.pdf.
42. Rudzinskas A., (2001). Neturtinės žalos samprata bei jos kompensavimo problemos civilinėje ir baudžiamojo proceso teisėje. Jurisprudencija, t. 21(13), p. 69-79. https://ojs.mruni.eu/ojs/jurisprudence/article/view/3718/3509
43. Sarkki (Pirkka) P.A.H. & others (2025). Fear of cybercrime victimisation: Examining the relationship between fear and victimisation. Journal of Criminal Justice, Vol. 101, p. 1-9. https://www.sciencedirect.com/science/article/pii/S0047235225001801#bb0030
44. Shandler R. & Gomez M. A., (2022). The hidden threat of cyber-attacks – undermining public confidence in government. Journal of Information Technology & Politics, 20, 4, p. 359- 361, https://www.tandfonline.com/doi/epdf/10.1080/19331681.2022.2112796?needAccess=true
45. Smith, Z. M., Lostri, E. & Lewis J. A., (2020). The Hidden Costs of Cybercrime. Report McAfee. p.1-38. https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf
46. Statista. Global cybercrime estimated cost 2025. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide/
47. Statista. Number of internet and social media users worldwide as of February 2025. https://www.statista.com/statistics/617136/digital-population-worldwide/.
48. The Financial Action Task Force (FATF) (2025). Detecting, Disrupting and Investigating Online Child Sexual Exploitation. Using financial intelligence to protect children from harm. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Online%20Child%20Sexual%20Exploitation%20Report.pdf.coredownload.inline.pdf
49. Tomsu, M., Rosiková, V., Vojtek, P., & Hrabakova, M. Spear-phishing and its specifics within social engineering. 34th DAAAM International Symposium on Intelligent Manufacturing and Automation, Viena, Austrija, 2023 October. https://www.daaam.info/Downloads/Pdfs/proceedings/proceedings_2023/working_papers/dpn78056_b_2_Tomsu.pdf
50. Valstybės duomenų agentūra. Naudojimasis internetu ir toliau auga – prieigą turi per 90 proc. Lietuvos namų ūkių. https://vda.lrv.lt/lt/naujienos/naudojimasis-internetu-ir-toliau-auga-prieiga-turi-per-90-proc-lietuvos-namu-ukiu/
51. World Economic Forum. Global Cybersecurity Outlook 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
52. World Happiness Report 2026. https://www.worldhappiness.report/ed/2026/

ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2026, Vol. 38, Nr. 2

THE IMPACT OF CYBERCRIME ON HUMAN BEINGS

Gediminas BUCIUNAS
Mykolas Romeris University
Vytautas Magnus University
Klaipeda University
ORCID ID: 0000-0002-1826-0527

Kornelija GARUCKAITĖ
Mykolas Romeris University
ORCID ID: 0009-0003-3513-6119

Summary. The 21st century is known as the digital age, which has fundamentally impacted various aspects of people's lives and government processes, and has radically transformed the processes and formats of information collection, processing, dissemination, and storage. Just thirty years ago, the possibility of remotely registering a business and obtaining permits from government agencies to carry out certain economic activities without leaving home seemed like an unattainable dream, a scenario straight out of a science fiction story. Rapidly developing technologies have created opportunities for remote communication, the transmission of vast amounts of information from one continent to another in a matter of seconds, and the execution of financial transactions; yet, at the same time, they have created new threats to the security of individuals, society, and nations. These threats are referred to as "cybercrimes" and exist alongside long-established threats such as "corruption," "organized crime," and "terrorism." Cybercrime, still referred to in academic literature as "high-tech crime," causes significant harm to individuals, society, and businesses when identity theft, data theft, various financial crimes, the dissemination of misleading information, manipulation, malware, espionage, various attacks against state institutions, and more. The European Union (hereinafter "EU") law enforcement agency (hereinafter "Europol") notes that cybercrime poses the greatest threat to both national security and to individuals and society. Cybercriminals are becoming increasingly aggressive, and their activities are becoming more dangerous and more organized and coordinated, aimed at achieving a specific goal. The subject of this study is the impact of cybercrime on individuals. The subject of this study also determined its objective, which is to analyze the impact of cybercrime on individuals through the lens of personal security. To achieve the objective of this study, an analysis was conducted of scientific articles published both in Lithuania and abroad regarding the targets, trends, and impact of cybercrimes on individuals' financial stability, psychological state, and the resulting negative consequences. The study found that, first and foremost, individuals suffer harm that can be measured and expressed in monetary terms. This is followed by non-pecuniary damage, which is much harder to detect, measure, and is not always visually apparent, manifesting as a deterioration in an individual's mental health that affects various aspects of their life. This article aims to answer two questions raised by the study: which fundamental human rights enshrined in national and international legal acts are violated by cybercrimes? What harm does a person suffer when they become the target of a cyber incident? How do people react to cyberattacks? How does a cyber incident affect a person's financial stability, mental health, and well-being? The study employs the following qualitative and quantitative research methods: document analysis, comparative analysis, abstraction, logical analysis, and other research methods.

Keywords: cybercrimes, impact, individual, society, sense of security, harm, mental state.

This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 (CC BY 4.0) License.