MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERSLO FAKULTETAS

BIRUTĖ UŽKURIENĖ

Kibernetinio saugumo valdymas

DUOMENŲ APSAUGOS VALDYMO YPATUMAI INTERNETO SOCIALINIUOSE TINKLUOSE

Magistro baigiamasis darbas

Darbo vadovas –

Prof. dr. Tadas Limba

Vilnius, 2018

MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR VERSLO FAKULTETAS

DUOMENŲ APSAUGOS VALDYMO YPATUMAI INTERNETO SOCIALINIUOSE TINKLUOSE

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų programa 6211LX066

Vadovas
Prof. dr. T. Limba
2018 12 05

Atliko
KSVvmns 17-1 gr. stud.
B. Užkurienė
2018 12 05

VILNIUS, 2018

Turinys

ĮVADAS 7

1. DUOMENŲ APSAUGOS VALDYMO YPATUMŲ INTERNETO SOCIALINIUOSE TINKLUOSE TEORINIAI ASPEKTAI 10

1.1. Duomenų apsaugos sampratų analizė ir raida 10

1.2. Socialinių tinklų samprata ir jų raida 13

1.3. Socialinių tinklų tipų analizė 15

1.3.1. Socialiniai tinklai 16

1.3.2. Multimedios bendrinimo tinklai 16

1.3.3. Profesiniai tinklai 16

1.3.4. Mokslo ir akademiniai socialiniai tinklai 17

1.3.5. Socialinių bendruomenių ir diskusijų tinklai 17

1.3.6. Anoniminiai socialiniai tinklai 17

1.4. Duomenų apsaugos valdymo problematika interneto socialiniuose tinkluose 18

1.5. Duomenų apsaugos valdymo analizė 20

1.5.1. Vartotojo vaidmens aspektai 22

1.5.2. Socialinio tinklo vaidmens aspektai 24

2. DUOMENŲ APSAUGOS VALDYMO YPATUMŲ INTERNETO SOCIALINIUOSE TINKLUOSE ATVEJŲ ANALIZĖ 27

2.1. *Twitter* atvejo analizė 27

2.2. *LinkedIn* atvejo analizė 35

2.3. *Facebook* atvejo analizė 44

3. DUOMENŲ APSAUGOS VALDYMO YPATUMŲ INTERNETO SOCIALINIUOSE TINKLUOSE TYRIMAS 54

3.1. Tyrimo metodologija 54

3.2. Tyrimo duomenų analizė 60

IŠVADOS 69

REKOMENDACIJOS 70

LITERATŪROS SĄRAŠAS 71

SANTRAUKA 76

SUMMARY 77

PRIEDAI 78

PAVEIKSLAI

Pav. 1 Magistro baigiamojo darbo struktūros loginė schema 9
Pav. 2 CIA triados modelis 11
Pav. 3 Interneto socialinių tinklų laiko juosta 14
Pav. 4 Interneto socialinio tinklo koncepcija. 15
Pav. 5 Asmens duomenų tvarkymas 19
Pav. 6 Internetinių tinklų ledkalnio modelis 21
Pav. 7 Privatumo nustatymai SNS ir jų palyginimai 23
Pav. 8 Atakų prieš SNS valdymo politika 25
Pav. 9 Patvirtintas profilis 28
Pav. 10 Netikra *Facebook* paskyra 59
Pav. 11 Priimti kvietimai ir *Facebook* siūlymai 59
Pav. 12 Pasiskirstymas pagal lytį 60
Pav. 13 Pasiskirstymas pagal amžių. 61
Pav. 14 Naudojimosi SNS trukmė metais. 61
Pav. 15 Jungimosi prie SNS dažnumas. 62
Pav. 16 *Facebook* pranešimas 62
Pav. 17 *Facebook* siūlymas 63
Pav. 18 Paskyrų matomumo nustatymai 63
Pav. 19 *Facebook* tinkle turimų draugų skaičiai 63
Pav. 20 Socialinių tinklų pasiskirstymas 64
Pav. 21 Naudojimosi socialiniais tinklais priežastys 65
Pav. 22 Viešai pateikiama informacija socialiniuose tinkluose 65
Pav. 23 Žinios apie socialinių tinklų naudojimosi ir privatumo taisykles 66
Pav. 24 Priimami kvietimai draugauti 67
Pav. 25 Informacijos matomumo nustatymai 67
Pav. 26 Privatumo nustatymų keitimas 68

LENTELĖS

1 Lentelė. Socialinio tinklo *Facebook* naudojimosi ir privatumo taisyklių santrauka 34
2 Lentelė. Socialinio tinklo *LinkedIn* naudojimosi ir privatumo taisyklių santrauka 44
3 Lentelė. Socialinio tinklo *Facebook* naudojimosi ir privatumo taisyklių santrauka 53
4 Lentelė. Tyrimo instrumento klausimyno sudedamosios dalys. 56

SANTRUMPOS / PAAIŠKINIMAI

BDAR (angl. GDPR – General Data Protection Regulation**)** – Bendrasis duomenų apsaugos reglamentas.

CIA – (angl. Confidentiality, Integrity, Availability) konfidencialumas, vientisumas, pasiekiamumas.

DDOS (angl Distributed Denial of Service) – paskirstytoji paslaugos trikdymo paslauga.

Deep linking – gilioji nuoroda. Nukreipia į konkretų programos puslapį. Paprastos paskirties URL, pvz., www.example.com nukreipiama į svetainės puslapį, o gilioji nuoroda nukreipia tiesiai į produkto puslapį svetainėje. Tam naudojamas kitoks URL, kuriame pateikiama šiek tiek daugiau informacijos, pvz., www.example.com/product_1234.

Duomenų subjektas – asmuo, kurio duomenys saugomi įstatymo.

Duomenų tvarkytojas – tvarko asmens duomenis tik duomenų valdytojo vardu. Tai gali būti trečioji šalis.

Duomenų valdytojas – fizinis arba juridinis asmuo, kuris teisėtai tvarko duomenis.

Grėsmė – (angl. threat) būsena, kai yra potenciali saugumo pažeidimo tikimybė.

Grotažymė/saitažymė – (angl. hashtag) socialinės žiniasklaidos svetainėse, tokiose kaip *Twitter* žodis ar frazė, prieš kurią yra grotelių simbolis (#) naudojamas tam tikros temos pranešimams identifikuoti.

Profilis/Paskyra/Anketa – (angl. account) socialinio tinklo vartotojo duomenys, individualizuojantys jo darbą socialiniame tinkle.

Social network sites (SNS‘s) – interneto socialiniai tinklai.

TCP (Transmission Control Protocol) – taisyklių visuma, apibrėžianti duomenų mainų būdą tarp dviejų kompiuterinių sistemų.

TOR – (angl. The Onion Router), sluoksninio maršrutizatorius technologija, veikianti sluoksninio maršruto parinkimo principu, skirta anonimiškai siųsti ir gauti užšifruotą informaciją internetu.

UDP (User Datagram Protocol) – tinklinio protokolo duomenų vienetas. Alternatyva TCP protokolui. Trumpa žinutė datagrama persiunčiama greičiau nei per TCP nes nereikalingi paketai sesijai pradėti, taip pat mažiau siunčiama antrašės duomenų

Žiniatinklis – pasaulinis tinklas (angl. World Wide Web arba WWW). Resursai, kuriuos internete galima pasiekti naudojant URL (universalus informacijos šaltinio adresas).

PRIEDAI

1. Priedas. Tyrime panaudota anketa

ĮVADAS

Temos aktualumas. Interneto socialinių tinklų pradžia laikoma interneto atsiradimas. Tačiau būtent XX amžiaus antrojoje pusėje sparčiai pradėjo kurtis socialinių tinklų svetainės. Jos suteikė vartotojams galimybę bendrauti, dalintis informacija raštu, grafiniu pavidalu, garsiniais ir vaizdo įrašais, bei kurti virtualias bendruomenes.

Pagrindinė interneto socialinių tinklų populiarumo priežastis yra ta, kad interneto vartotojai juose gali komunikuoti. Bendravimas vyksta tiek su pažįstamais, tiek su nepažįstamais asmenimis. Pokalbių formos labai įvairios, tai gali vykti pokalbiais žinutėmis, komentarais po nuotraukomis, įrašais ar straipsniais, taip pat dalyvavimu įvairiose grupėse. Yra nurodomos kelios priežastys (Grimmelmann J. 2008), kurios interneto socialinius tinklus daro tokius populiarius ir skatina jais naudotis įvairaus amžiaus asmenis:

- Tapatybė – viena iš priežasčių, kuri vartotojams leidžia save realizuoti bei atskleisti savo tapatybę, ją sukuriant ir pateikiant kaip patys to nori.
- Santykiai – kitas svarbus faktorius, kuris lemiantis interneto vartotojų jungimąsi į socialinius tinklus. Asmenys gali susirasti draugų, atnaujinti ar sustiprinti ryšius su jau pažįstamais.
- Bendruomenė – dar vienas svarbus aspektas darantis socialinius tinklus populiarus, tai noras būti bendruomenės dalimi ir būti pripažintiems.

Socialinių tinklų kūrėjai atsižvelgdami į kylančius vartotojų poreikius, tobulina teikiamas paslaugas bei plečia jų spektrą. Socialiniai tinklai išplečiančia tradicinės komunikacijos ribas, todėl šiuo metu interneto socialinių tinklų svetainės tapo neatsiejama kasdiene veikla kiekvienam interneto vartotojui. Todėl, dažnai vartotojai naudodamiesi interneto socialiniais tinklais, nepastebi juose esančių rizikų arbe apie tai negalvoja. Atidžiau paanalizavus socialinių tinklų veikimą, matoma, kad šios paslaugos kelia klausimų bei nagrinėjamų problemų. Šiame darbe bus nagrinėjami duomenų apsaugos valdymo ypatumai interneto socialiniuose tinkluose.

Temos ištirtumas. Bendrai apie informacinės visuomenės ir tinklų kūrimąsi, bei jų poveikį aplinkai, savo knygose daug rašo Manuel Castells. Duomenų apsaugos ir saugumo pažeidimus interneto socialinių tinklų svetainėse klausimu daugiausia atlikta užsienyje. Iš jų galima paminėti Jianqiang Hao, Hongying Dai, D.Haynes ir L.Robinsom atliktus tyrimus. Socialinių tinklų saugumas ir pažeidžiamumas tyrinėtas Jensen Zhao ir Sherry Y. Zhao mokslinėse studijose.

Tyrimų Lietuvoje, kur būtų analizuojami ne interneto socialiniai tinklai, o būtent duomenų apsauga jose, nėra daug. Galima paminėti D. Štitilio ir kt. straipsnį, kuriame kalbama apie asmens duomenų apsaugos internetiniuose socialiniuose tinkluose problemas ir teisinį reguliavimą.

Mokslinė problema: mokslo šaltiniuose pasigendama standartizuotų ir/arba specifinių metodų ir priemonių duomenų apsaugos valdymo užtikrinimui interneto socialiniuose tinkluose.

Tyrimo objektas: duomenų apsaugos valdymo interneto socialiniuose tinkluose ypatumai.

Tyrimo tikslas: nustačius duomenų apsaugos valdymo ypatumus interneto socialiniuose tinkluose, pateikti duomenų apsaugą socialiniuose tinkluose didinančias strategines kryptis bei pateikti rekomendacijas.

Uždaviniai:

1. išanalizuoti duomenų apsaugos valdymo interneto socialiniuose tinkluose teorinius aspektus;
2. remiantis atvejų analizės metodu, išanalizuoti pasirinktų interneto socialinių tinklų duomenų valdymą vartotojo ir socialinio tinklo vaidmens aspektu;
3. įvertinti duomenų apsaugos būklę interneto socialiniuose tinkluose.

Magistro baigiamajame darbe keliama **hipotezė**, kad vartotojai, duomenų apsaugos valdyme interneto socialiniuose tinkluose yra silpniausia grandis, todėl kyla grėsmė, kad išnaudojant žmogiškąjį faktorių per socialinės inžinerijos atakas, taps kibernetinių atakų taikiniu.

Ginamieji teiginiai. Vartotojai neišmano ir neįsigilina į teikiamas naudojamų socialinių tinklų saugumo rekomendacijas ir pilnai neišnaudoja visų įmanomų priemonių duomenų apsaugai interneto socialiniuose tinkluose.

Socialiniai tinklai siekia užtikrinti, kad jų platformos būtų skaidrios, saugios ir vykdytų įstatymus dėl asmens duomenų valdymo ir tvarkymo, įskaitant duomenų apie asmens elgesį internete rinkimą ir algoritmų naudojimą.

Duomenų rinkimo metodai ir šaltiniai. Rengiant darbą, buvo taikomi literatūros šaltinių analizės metodas. Jo pagalba buvo susipažinta su nagrinėjamos temos mokslininkų darbais, publikacijomis. Remtasi literatūros analize, atvejo analize, atlikta vartotojų kiekybinė apklausa. Darbe atliktos teorinė aprašomoji, sisteminė, lyginamoji analizės. Taikyta mokslinės literatūros analizė siekiant išanalizuoti duomenų valdymo socialiniuose tinkluose teorinius aspektus. Daugiausia remtasi elektroniniais informacijos šaltiniais – teisinių dokumentų, duomenų apsaugą tiriančių specialistų recenzuotais straipsniais, organizacijų, ir kitų institucijų, besirūpinančių asmens duomenų apsauga, pranešimais. Išanalizuota ir atlikta socialinių tinklų skelbiamų duomenų apsaugos ir privatumo politikų analizė ir palyginimas. Darbe pristatomam kokybiniam tyrimui „Vartotojų požiūrio į duomenų apsaugą socialiniuose tinkluose“ taikytas anketinės apklausos metodas, taip pat atliktas natūralusis eksperimentas.

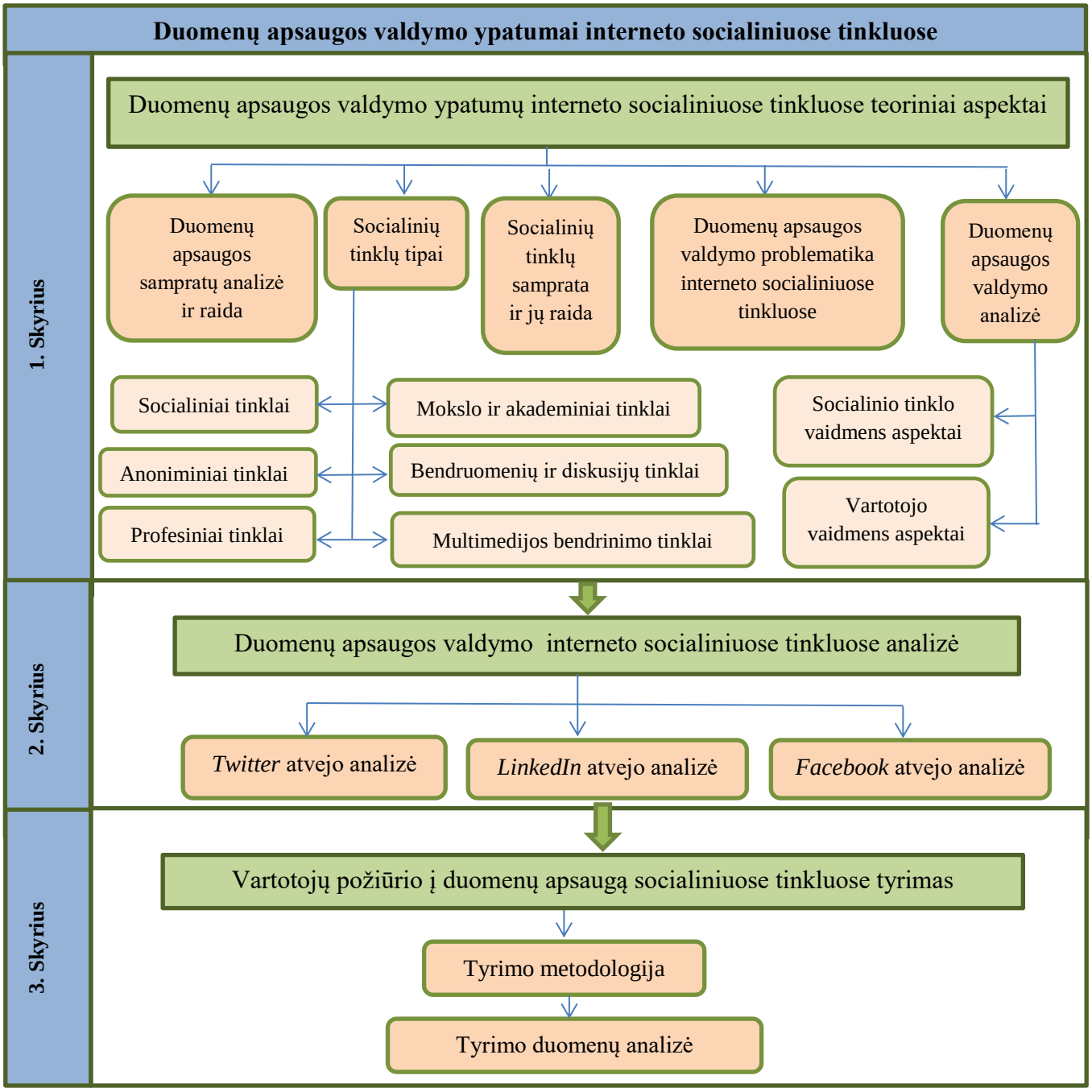
Darbo struktūra. Darbą sudaro 3 dalys. Pirmoje dalyje nagrinėjami duomenų apsaugos valdymo interneto socialiniuose tinkluose teoriniai aspektai: duomenų apsaugos sampratų analizė ir raida, socialinių tinklų samprata, vartotojo ir socialinių tinklų vaidmenų aspektai ir duomenų apsaugos valdymo problematika interneto socialiniuose tinkluose.

Antroje dalyje apžvelgiamos pasirinktų populiarių socialinių tinklų svetainių skelbiamos asmens duomenų apsaugos politikos. Analizuojami duomenų apsaugos valdymo atvejai didžiuosiuose

socialiniuose tinkluose: Jungtinių Amerikos Valstijų – *Facebook Inc., LinkedIn Corporation, Twitter Inc*. atvejai.

Trečioje dalyje aprašomi pasirinkti tyrimo metodai. Nagrinėjami, anketinės apklausos ir eksperimento metodais gauti duomenys. Darbo pabaigoje pateikiamos išvados ir rekomendacijos.

Darbo praktinis reikšmingumas. Darbo praktinį reikšmingumą atspindi pateikiamos išvados naudingos sprendžiant padidėjusį visuomenės susirūpinimą bei suaktyvėjusį dėmesį duomenų interneto socialiniuose tinkluose apsaugos klausimus. Darbe taip pat pateikiamos naudingos rekomendacijos socialinių tinklų vartotojams, besirūpinantiems duomenų apsauga interneto socialiniuose tinkluose. Darbo naujumas pasireiškia tuo, kad nagrinėjamas ganėtinai „jaunas“ reiškinys - interneto socialiniai tinklai. Su jais susijusi problematika duomenų apsaugos kontekste.



Pav. 1 Magistro baigiamojo darbo struktūros loginė schema

1. DUOMENŲ APSAUGOS VALDYMO YPATUMŲ INTERNETO SOCIALINIUOSE TINKLUOSE TEORINIAI ASPEKTAI

Pasaulinė patirtis rodo, kad interneto socialiniai tinklai visiškai pakeitė bendravimo įpročius. Jau keletą metų socialinių tinklų vartojai yra ne vien fiziniai asmenys, žymūs visuomenės nariai, politikai, bet ir privačios įmonės ir valstybinės institucijos. Moksliniai tyrimai taip pat parodė, kad tinkamai naudojami socialiniai teigiamai įtakoja įmonių pajamas ir pelną (Zhao & Zhao, 2015). Tačiau didėjantys interneto socialinių tinklų populiarumas taip pat kelia pavojų asmenų, įmonių ir vyriausybių privatumui ir saugumui. Pavyzdžiui 2014 m. 70% sukompromituotos informacijos socialiniuose tinkluose buvo pasidalinta „rankiniu būdu“. Vartotojai labiau linkę dalintis įrašais, kuriuos jau yra paskelbę jų draugai arba žinomi visuomeniniai veikėjai (Symantec, 2015).

Apskritai kibernetinių nusikaltėlių pagrindinis tikslas socialiniuose tinkluose ir pagrindinis atakų vektorius – pavogti vartotojų duomenis, kompromituoti žymių asmenų profilius ir žinomus prekių ženklus, manipuliuoti rinkomis siekiant finansinio pelno (McNurlin & Sprague, 2005).

Šioje darbo dalyje apžvelgsiu duomenų apsaugos sampratą, socialinius tinklus. Analizuosiu galimas duomenų apsaugos valdymo problemas vartotojo ir socialinio tinklo atžvilgiu.

1.1. Duomenų apsaugos sampratų analizė ir raida

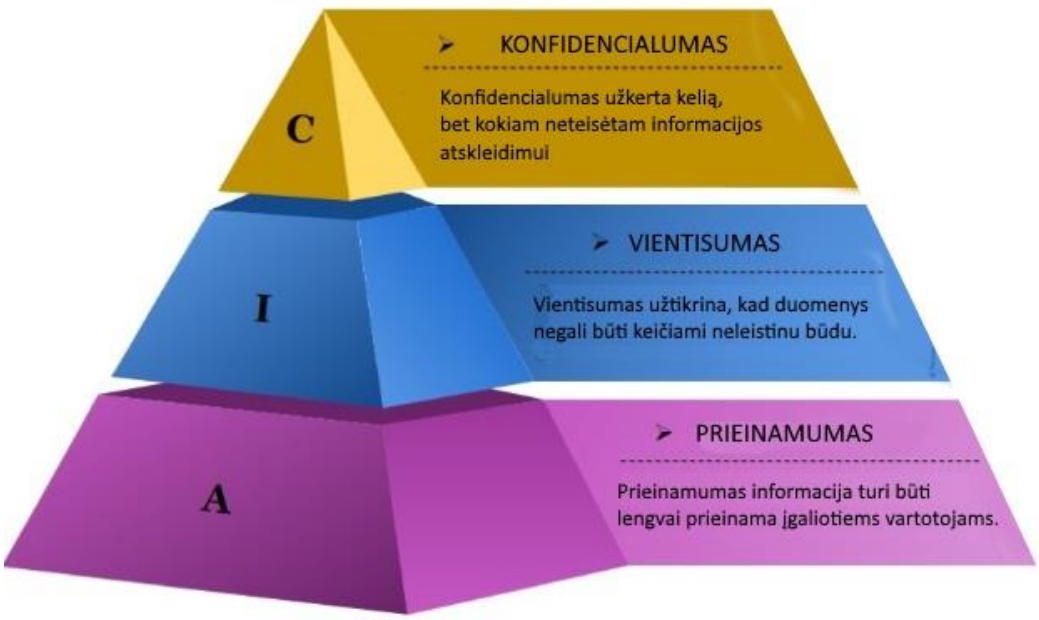
Siekiant atlikti duomenų apsaugos interneto socialiniuose tinkluose valdymo analizę, tikslinga atskleisti duomenų sąvokos prasmę, kuri yra probleminė kadangi angliškas žodis *data* turi kelias reikšmes. Anglų kalboje terminas *data* neišskiriamas, vadovaujantis Oksfordo žodynu, jis apibūdinimas kaip simbolis ar kiekis simbolių, kuriais atliekami veiksmai kompiuteriu ir kurie gali būti saugomi, perduodami ir įrašomi į laikmeną. Tuo tarpu žodis *data* į lietuvių kalbą verčiamas tokiomis sąvokomis kaip: duomenys, informacija ir faktai. Įdomu, kad dabartinės lietuvių kalbos žodyne nėra apibrėžimo apibūdinančio sąvoką „duomenys“. Tačiau prie termino informãcij‖a (1) pateikiamas apibrėžimas - specialiai kaupiamos, laikomos ir perduodamos žinios: ~os teorija. ~os srautas, tvarkymas. **Bendriausia reikšme, galime sakyti**, kad duomenys – formalizuotas informacijos vaizdinys, tinkamas perduoti kitiems, suvokti ir apdoroti.

Terminas *security* verčiamas kaip saugumas, apsauga. Oksfordo žodynas šį terminą apibūdina labai trumpai, tai būsena kai nėra pavojau ar grėsmės. Dabartinės lietuvių kalbos žodynas terminą apsaug‖à (3 b) taip pat apibūdina labai trumai – apsaugojimas, gynimas. Lietuvių kabos instituto lietuvių kalbos žodyne šio termino apibūdinimas papildytas dar vienu paaiškinimu – saugojimo priemonės. Apibendrinant, galima sakyti, kad apsauga tai veiksmai, priemonės, kurių imamasi siekiant išvengti ar esant neigiamų padarinių, veiksnių rizikai.

Duomenų saugumo pažeidimą galima apibūdinti kaip situaciją kai, netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi duomenys arba prie jų be leidimo gaunama prieiga.

Informacinės technologijos plačiai naudojamos tiek organizacijose, tiek namų ūkiuose. Ši sąlyga reiškia, kad ir organizacijos ir namų ūkiai susiduria su iškylančiomis saugumo problemomis Informacijos saugos savybes apibrėžia informacijos CIA triados (angl. CIA triad) modelis, kuris taikomas *ISO/IEC 27001* standarte. Tai yra saugumo priemonių vadovas skirtas formuoti informacijos saugumo politiką..

Duomenų saugumo, pagrindinius tikslus galima apibrėžti labai trumpai – CIA triada. Tai – konfidencialumas, vientisumas ir prieinamumas (Andre T. 2017).



Šaltinis: parengta autorės pagal Microsoft.

Pav. 2 CIA triados modelis

Konfidencialumas (angl. confidentialitity) arba slaptumas yra duomenų ar išteklių (resursų) slėpimas, jis veikia principu – suteikti informaciją tik tiem, kuriems jos reikia. Šis informacijos saugumo aspektas užtikrina, kad duomenys ar informacija bus prieinama tik autorizuotiems vartotojams.

Vientisumas (angl. integrity). arba integralumas reiškia duomenų ar išteklių patikimumą, tai kad jie apsaugoti nuo neteisėto pakeitimo. Vientisumo užtikrinimas skiriasi nuo konfidencialumo. Kalbant apie konfidencialumą, tai duomenys yra atskleisti arba ne, o į vientisumo sąvoką įeina ir duomenų korektiškumas ir patikimumas. Labai svarbu duomenų kilmė, kaip patikimai buvo saugoti ir ar nebuvo sukompromituoti iki pasiekia vartotoją.

Prieinamumas (angl. availability) reiškia galimybę ir gebėjimą įgaliotiesiems asmenims prireikus netrikdomai naudotis reikiama informacija ar duomenimis. Informacija yra neprieinama ne tik tada, kai ji yra prarasta ar sunaikinta, bet ir tada, kai jos prieiga yra uždrausta ar apribota tiems, kuriems leidžiama ją naudoti. Todėl, norint užtikrinti prieinamumą, ryšių kanalai, naudojami prieigai prie informacijos, turi veikti teisingai ir laikantis informacijos saugumo politikos.

Kalbant apie socialinius tinklus, reiktų pabrėžti kad juose esantys duomenys daugiausia susiję su asmeniniais vartotojų duomenimis. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas asmens duomenis nusako „bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.“. Europos parlamento ir tarybos reglamente (ES) 2016/679 naudojamas toks apibūdinimas: *asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.*

Elektroninė erdvė lemia, kad informacija kaip pagrindinė asmens duomenų sąvokos apbrėžimo dalis, turi būti aiškinamas kaip apimantis iš esmės visus duomenis apie asmenį ar galinčius turėti ryšį su juo. Todėl duomenų apsaugos principai turėtų būti taikomi bet kokiai informacijai apie asmenį, kurio asmens tapatybė yra nustatyta arba gali būti nustatyta ne tik pagal fizinius asmens duomenis, bet ir pagal tai, kad ji yra ar gali būti susijusi su asmeniu tam tikrais ryšiais ar santykiais (pvz., adresas, automobilio valstybinis numeris, telefono numeris, sutuoktinio vardas ir kt.).

Neribota galimybė surasti bet kokią informaciją internete (ypač informaciją apie konkretų asmenį) iškėlė diskusijas visuomenėje ir klausimą dėl „teisės būti pamirštam“. 2014 gegužės 13 dieną Europos Sąjungos Teisingumo Teismas (ESTT), priėmė visiškai paieškos variklių praktiką pakeičiantį sprendimą „Google v. Spain“ byloje – esant tam tikroms sąlygoms, asmenys turi teisę „būti pamiršti“. Todėl norint pašalinti duomenis apie save įvairiose internetinėse paieškos platformose ir / ar socialiniuose tinkluose, galima kreiptis tiesiogiai į duomenis tvarkančią įstaigą su užklausa neviešinti asmens tapatybę atskleidžiančių duomenų.

Apibendrinant galima sakyti, kad duomenų saugumas – administracinių, techninių ir fizinių priemonių visuma, skirta apsaugoti duomenis nuo neteisėto arba atsitiktinio jų atskleidimo, pakeitimo arba sunaikinimo, tačiau vartojamas prieinama netrikdomai ir garantuojant, kad duomenys nesukompromituoti.

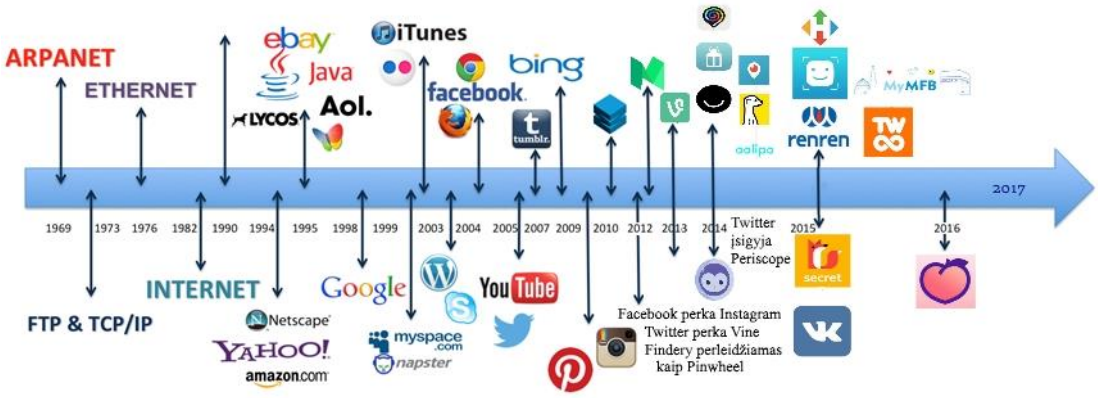
1.2. Socialinių tinklų samprata ir jų raida

Žmogus – socialinė būtybė, kuriai būtinas bendravimas. Realizuoti savo tikslus ir patenkinti komunikavimo poreikius jis gali tik tarp panašių į save, priklausydamas kokiai nors bendruomenei (šeimai, darbo kolektyvui, visuomeninei organizacijai). Socialinis gyvenimas – tai išorinė aplinka, kurioje asmuo atsiduria kiekvieną. Šio gyvenimo dalyviai – kiti žmonės darbas, verslas. Socialinio gyvenimo erdvėje siekiama tikslų ir uždirbami pinigai, čia susiduria skirtingų individų interesai, todėl būdinga konkurencija, taip pat vyksta mainai ir bendradarbiaujama. Šiandieniniame pasaulyje internetinis ryšys yra ypatingai svarbus ir itin aukšto lygio. Šiek tiek daugiau nei pusė viso pasaulio gyventojų naudojasi internetu (http://www.internetworldstats.com/stats.htm 2017). Todėl ir socialinis gyvenimas sunkiai įsivaizduojamas be interneto. Socialiniai ryšiai iš realaus pasaulio persikelia į virtualią erdvę, kurioje vyksta ne ką mažesnis aktyvus gyvenimas kaip ir realiame pasaulyje (Scott D. M., 2008, p. 225-252).

„Dalyvavimas ar nedalyvavimas tinkle bei kiekvieno tinklo dinamika yra svarbiausios dominavimo bei kitimo prielaidos mūsų visuomenėje, kuri pagrįstai gali būti vadinama tinklaveikos visuomene, o jai būdingas socialines morfologijos pranašumas socialinio veiksmo atžvilgiu“ [p. 454]. Taip apie dabartinę visuomenę trilogijoje „Informacijos amžius: ekonomika, visuomenė ir kultūra“ (2010) rašo M. Castell.

Terminą „socialiniai tinklai“ 1954 metais panaudojo Mančesterio sociologas James Barnes. Šiuo terminu buvo apibrėžiamas žmogaus kontaktų ratas. Tačiau šis apibrėžimas neturėjo nieko bendro su internetu. Pirmasis kompiuterinis tinklas atsirado 1971 m., tai buvo kariuomenės naudojamas ARPA Net tinklas.

Socialiniams tinklams persikėlus į virtualią erdvę iš pradžių jie buvo pavadinti virtualiomis bendruomenėmis. Pačia socialinių tinklų pradžia galima būtų laikyti elektronines skelbimų lentas (angl. *bulletin board services*, BBC), kurių veiklos pradžia laikomi 1978 metai. Šios internetinės skelbimų lentos lengvai ir patogiai leido vartotojams bendrauti tarpusavyje, suteikė galimybes susisiekti su centrine sistema, kur galėjo talpinti įvairias failų rinkmenas, siųsti pranešimus kitiems vartotojams, kurti kambarius privatiems pokalbiams. Tačiau dėl tuometinių techninių apribojimų, duomenys buvo tik tekstinio formato. Tokios elektroninės skelbimų lentos išpopuliarėjo aštuntame ir devintame dešimtmetyje, kai labai sparčiai pradėjo vystytis internetas. Šiuolaikinių socialinių tinklų pradžia galima vadinti *AOL* (America Online), kuris buvo sukurtas 1983 m. kaip *Control Video Corporation*. Pirmaisiais šiuolaikiniais socialiniais tinklais laikomi *Classmates.com* (pradžia 1995 m.) ir *SixDegrees.com* (pradžia 1995 – 1996 m.). Metais vėliau atsirado įrankiai leidžiantys, kurti socialinius tinklus, kuriuose buvo palaikomi įvairūs paskyrų ir viešai matomų draugų variantai. Tinklų vartotojai galėjo identifikuoti draugus savo profiliuose neprašydami patvirtinti ryšių.



Šaltinis: sudaryta autorės pagal Challita K. (2010), Zoe A. (2017).

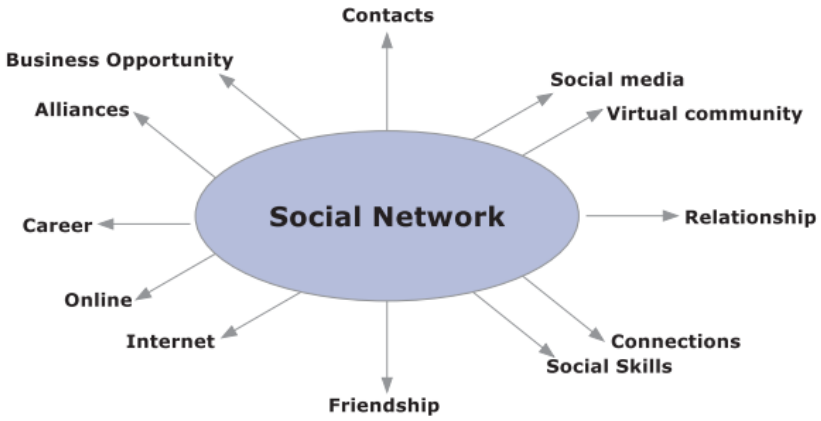
Pav. 3 Interneto socialinių tinklų laiko juosta

Socialinio tinklo sąvoka naudojama norint ją susieti su elektronine erdve ir komunikacija jos viduje. Internetiniai socialiniai tinklai – tai socialinė struktūra, kuri vienija tam tikras grupes, kurių nariai (vartotojai) susiję įvairiais ryšiais (draugyste, giminyste, ekonominiais santykiais, religija, pomėgiais, socialine padėtimi). Asmenys yra suinteresuoti diskutuoti tarpusavyje įvairiais klausimais, dalintis ir keistis turima informacija, muzika, vaizdo medžiaga. (Coy P., 2017) Svarbiausias internetinių socialinių tinklų elementas – vartotojų paskyros, kuriuose yra įkelti duomenys apie profilio savininką. Asmuo norintis būti interneto socialinio tinklo nariu, turi susikurti savo anketą, kurioje dažniausiai reikia nurodyti asmeninius duomenis, tokius kaip vardas, pavardė, amžius, gyvenamoji vieta, pomėgiai ir kita informacija. Taip pat dauguma socialinių tinklų svetainių leidžia vartotojams į savo profilį įsikelti nuotraukas ir kitą vaizdinę medžiagą. Taip pat, prisijungus prie socialinio tinklo, vartotojui siūloma susirasti pažįstamus asmenis, taip kaip įmanoma greičiau išplečiant vartotojo socialinį tinklą. (Štitilis D. ir kt. 2012)

Pasak Danah M. Boyd ir Nicole B. Ellison (2007), socialinio tinklo sąvoka apibrėžiama kaip viena iš žiniatinklio paslaugų, kurios pagalba vartotojai gali formuoti viešą arba iš dalies viešą savo profilį tam tikros sistemos viduje.

Kiti autoriai socialinius tinklus apibūdina pagal Golbeck pateiktą apibrėžimą, kad kai yra tenkinamos tokios sąlygos: tarpusavio ryšiai nurodomi vartotojų, o ne sukurti automatinės sistemos; ryšiai tarp vartotojų yra saugomi ir tvarkomi naudojant tokias technologijas kaip duomenų bazė, valdymo sistemos, leidžiančios analizuoti santykius ir reguliuoti duomenų paiešką; vartotojai gali gauti informaciją apie kitus vartotojus su kuriais yra nurodę turintys bendrų ryšių. (Carminati B., Ferrari E., 2008).

Socialinis tinklas turi itin plačią suvokimo reikšmę, tačiau pačia paprasčiausia forma gali būti apibūdinamas kaip socialinė sandara, kurioje susitelkia tam tikros asmenų grupės ar organizacijos, kurias sieja tarpusavio ryšiai, paremti bendrais pomėgiais arba panašiu požiūriu į vienus ar kitus dalykus ir kuriuose vartotojai gali siųsti vieni kitiems žinutes, kurti grupes, diskusijų forumus ir kt.



Šaltinis: Rathore S. et al. (2017)

Pav. 4 Interneto socialinio tinklo koncepcija.

Apibendrinant galima teigti, jog socialiniai tinklai turi plačią suvokimo prasmę įvairiose terpėse. Kadangi šiame darbe didesnis dėmesys skiriamas interneto socialinių tinklų duomenų apsaugos valdymo ypatumams, tai šiuo atveju jų sąvoką galima apibrėžti kaip interaktyvią interneto struktūrą (interneto svetainę) vienijančią tam tikrą bendrų interesų turinčią narių grupę, kuri kuria konkretaus socialinio tinklo svetainės turinį ir virtualiai bendrauja tarpusavyje, automatizuotomis priemonėmis keisdamiesi ar dalindamiesi asmenine įvairia tekstine, grafine, audio (garsine) ir video (vaizdo) informacija.

1.3. Socialinių tinklų tipų analizė

Yra daug ir labai skirtingų socialinių tinklų. Sparčiai plėtojantis internetinių socialinių tinklų svetainėms atsirado daugybė duomenų apie vartotojus paieškos galimybių. Visuose tinkluose yra skirtingos ryšių tarp vartotojų nustatymo taisyklės. Jos leidžia vartotojams peržiūrėti ir patvirtinti ryšius tarp vartotojų ir netgi pasiūlyti tolesnius galimus ryšius, pagrįstus asmens sukurtu tinklu.

Kai kurios socialinių tinklų svetainės, pvz. *LinkedIn*, naudojamos profesinėms jungtims kurti, o tokie socialiniai tinklai, kaip pavyzdžiui *Facebook*, peržengia liniją tarp privačių ir profesionalių jungčių. Taip pat yra daug tinklų, kurie yra sukurti konkrečiai tikslinei vartotojų grupei. Pavyzdžiui kultūrinėms ar politinėms grupėms tam tikroje teritorijoje, ar finansų rinkų prekybininkams. Užsienio autoriai (Tang L., Liu H., 2011; Musial K., Kazienko P., 2013; Barnhart B., 2017) sutelkė dėmesį į socialinių tinklų klasifikavimą.

Apibendrinus skirtingus šaltinius, galima matyti, kad interneto socialiniai tinklai daugiausia grupuojami pagal esančios juose informacijos sklaidos pobūdį, turinį bei tame turinyje skelbiamų failų formatų tipą ir pagal tai, ką vartotojai tikisi atlikti juos naudodami.

1.3.1. Socialiniai tinklai

Socialiniai tinklai (angl. *social networking*) leidžia vartotojams neformaliai bendrauti su kitais, rasti kitus asmenis ir dalintis panašiais interesais. Vienas iš didžiausių šių tinklų privalumų yra ryšiai su draugais ir šeimos nariais. Žinomiausi tokie tinklai būtų kaip: *Facebook, Google+, Friendster, Xanga, Asian Avenue, VKontakte*.

Tai pačiai grupei galima priskirti ir tinklaraščius (angl. *blogging*). Tai – internetinis dienoraštis, ar automatiškai formatuojami naujienų puslapiai. Šiems tinklams priskiriamos specializuotos interneto svetainės, kuriose talpinamos dažnai rašomos publikacijos, išdėstytos chronologine tvarka. Autoriai, taip vadinami *blogeriai* (tinklaraštininkai), aprašo įvykius, pastebėjimus, dalinasi ir platina savo mintis ir pažiūras. Dažniausiai komentuojamas pasirinktos temos turinys, kaip pavyzdžiui, muzika, kinas, maistas, politika ar kt. Didžioji dalis tinklaraščių rašomi kaip asmeniniai dienoraščiai.

Prie šių socialinių žiniatinklių priskiriami ir tokie tinklai kaip *Twitter* ir *Tumblr*. Tai yra mikrotinklaraščiai (angl. *microblogging*). Juose publikuojami nedidelės apimties tekstiniai pranešimai, matomi visiems skaitytojams arba vartotojo pasirinktai jų grupei. Leidžia naudotojams kurti ir dalytis raktiniais žodžiais, grotažymėmis (angl. *hashtags*), kad būtų galima bendrinti turinį apie susijusius dalykus. Žinomiausios tinklaraščių platformos būtų: *Wordpress, Blogger, Weebly, Wix, Tumblr, Squarespace.*

1.3.2.Multimedios bendrinimo tinklai

Multimedios bendrinimas (angl. *media sharing*) – šie socialiniai tinklai leidžia lengvai dalintis vaizdo įrašų ir fotografijos turiniu internete. Vartotojai vaizdo įrašais ir grafinio tipo failais gali dalintis tiek viešai (angl. *public*), tiek tik su savo draugais. Šia tinklai leidžia vartotojams įterpti ir platinti savo įrašus ir kituose socialiniuose tinkluose, kaip *Facebook, Twitter* ar kt. Populiariausi tokio tipo socialiniai tinklai būtų: *YouTube, SoundCloud, 500px, Flickr, Instagram, Flickr, Snapchat, Pinterest, Vimeo, Periscope*.

Atskirai reiktų paminėti *Snapchat* tinklą, dėl jo ypatybės. Šis tinkas aktualiausias žmonėms, nes leidžia, siųsti tiesiogiai savo draugams arba paskyros sekėjams sukurtas greitai dingstančias žinutes, nuotraukas ar vaizdo įrašus. Visa informacija dingsta iš virtualaus tinklo vos tik gavėjas ją peržiūri.

1.3.3.Profesiniai tinklai

Profesionalūs socialiniai tinklai (angl. *professional social networks*) yra skirti sutelkti į verslą ir vartotojų galimybes kurti karjerą. Kai kurie iš šių tinklų tipų yra bendras forumas, kuriame

profesionalai gali prisijungti bendravimui, informacijos dalinimuisi ir pan.. Kiti orientuoti į konkrečias profesijas ar interesus. Tokio tinklo paslauga naudojama verslo subjektams, siekiant sukurti ir palaikyti profesinius kontaktus ir būdus, kaip rasti darbą ar siekti karjeros, kurti profesinius ryšius. Žinomiausi tokio tipo socialiai tinklai būtų*: LinkedIn, Classroom 2.0, Networking for Professionals, Konnects, Xing, Spoke, Ryze.*

1.3.4. Mokslo ir akademiniai socialiniai tinklai

Mokslo (angl. *educational*) ir akademiniai (angl. *academic*) socialiniai tinklai vienija studentus ir mokslininkus.

Mokslo / švietimo tinklai skirti studentams bendradarbiauti su kitais studijuojančiais vartotojais, kurti bendrus akademinius projektus, atlikti mokslinius tyrimus ar bendrauti su dėstytojais ar mokytojais per tinklaraščius ir forumus. Tokie socialiniai tinklai populiarūs švietimo sistemoje. Toliau pateikiami tokie mokslo socialinių tinklų pavyzdžiai: *The Student Room, The Math Forum, ePALS School Blog, Edmodo, TeacherTube.*

Akademiniai socialiniai tinklai skirti moksliniams darbuotojams, dėstytojams. Moksliniai darbuotojai, norintys pasidalinti savo tyrimais ir apžvelgti kolegų pasiektus rezultatus. Daugelio akademinių socialinių tinklų svetainių bendras gebėjimas yra sukurti internetinę saugyklą, kurioje vartotojai gali įkelti ir dalytis mokslinių tyrimų straipsniais. Keletas populiariausių akademikų internetinių bendruomenių yra šios: *Academia.edu, Google Scholar, ResearchGate, Connotea Collaborative Research.*

1.3.5. Socialinių bendruomenių ir diskusijų tinklai

Bendruomenių diskusijų forumai (ang. *Social Community and Discussion Sites*) yra vieni seniausių socialinių tinklų tipų. Šie tinklai skirti vartotojams diskutuoti, keistis naujienomis, informacija ir nuomonėmis. Nors yra socialinių tinklų turinčių žymiai platesnį funkcionalumą, forumai iki šiol nepraranda savo populiarumo. Keletas tokio tipo tinklų pavyzdžių: *GidHub, Redit, Quora, Digg.*

1.3.6. Anoniminiai socialiniai tinklai

Pastaraisiais metai populiarėja anoniminiai socialiniai tinklai (angl. *anonymous social networks*). Šių tinklų pagrindinė bendra ypatybė yra ta, kad vartotojų tapatybės yra nežinomos. Vartotojai yra skatinami išlikti nežinomais arba susikurti pseudonimus, o visa informacija yra

dalinamasi anonimiškai. Informacija šiuose tinkluose gali būti dalinamasi tiek su turimais kontaktais, tiek viešai. Keletas tokio tipo socialinių tinklų pavyzdžių: *Whisper, Ask.fm, Diaspora, After School, Yik Yak.*

Reiktų išskirti, kad šalia anoniminių tinklų, *Facebook* vartotojams pasiūlė galimybes naudotis jų tinklu neatsisakant anonimiškumo. Ši paslauga pasiūlyta naudojant TOR (sluoksninio maršrutizatoriaus) tinklo paslaugas – *Facebook over Tor*. *Twitter* savo vartotojams pradėjo siūlyti šifruotų *end-to-end encryption* paslaugą.

1.4. Duomenų apsaugos valdymo problematika interneto socialiniuose tinkluose

Duomenų valdymas yra abstrakti sąvoka, kuri apibrėžia daugelį su duomenis susijusių veiklų. Pagrindinis duomenų valdymo tikslas yra užtikrinti, kad duomenys būtų prieinami reikiamiems vartotojams, tinkamu laiku ir tinkama forma. Valdyti duomenų apsaugą yra sudėtinga dėl įvairių priežasčių: senus duomenis reikia saugoti, nuolat atsiranda naujų; duomenys yra pasklidę, kaupiami skirtingais metodais ir prietaisais; saugomi keliuose skirtinguose, nutolusiuose serveriuose ar apdorojimo sistemose; naudojami skirtingi formatai ir kalbos; būtina užtikrinti duomenų saugumą, kokybę ir vientisumą. Pasak G. Skersio (2011), grėsmes duomenims galima skirstyti į keturias pakankamai plačias grupes:

- atskleidimas – neteisėta prieiga prie informacijos;
- apgavystė, kai klaidingi duomenys priimami kaip teisingi;
- nutraukimas – korektiškos operacijos nutraukimas ar sutrikdymas;
- užgrobimas – neteisėtas, kurios nors sistemos dalies valdymas.

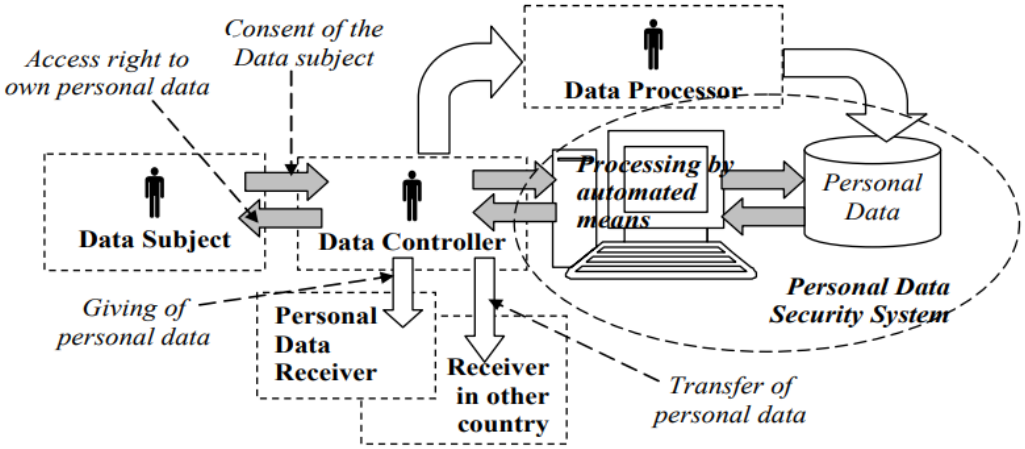
Šios grėsmės kyla ne tik dėl internete paplitusių kenkimo programų, sistemų saugumo spragų, bet ir dėl vartotojų žinių stokos apie galimas rizikas naudojantis internetu.

Pagrindiniai saugumo reikalavimai socialiniuose tinkluose yra privatumas (angl. *privacy*,) prieinamumas (angl. *availability*) ir atsakingumas (angl. *accountalibility*) (Becker J., Chen H., 2009). Kai šios sąlygos įvykdytos, vartojai apsaugomi nuo galimų privatumo pažeidimų, asmens tapatybės vagystės ar konfidencialių duomenų praradimo.

Socialiniuose tinkluose „asmens duomenys“ apibūdina informaciją, leidžiančią tiesiogiai ar netiesiogiai identifikuoti asmenį. Tai gali būti atlikta naudojant identifikavimo numerį arba vienu ar keliais veiksniais, būdingais jo fizinei, fiziologinei, psichinei, ekonominei, kultūrinei ar socialinei tapatybei (Romansky R. 2014).

LR asmens duomenų apsaugos įstatymas duomenų tvarkymą apibūdiną kaip – duomenų rinkimą, kaupimą, apdorojimą, saugojimą, teikimą. Taigi, bet koks veiksmas ar veiksmų rinkinys su asmens duomenimis (naudojant automatines ar neautomatines priemones) vadinamas „asmens

duomenų tvarkymu“. Pagrindiniai asmens duomenų tvarkymo principai reikalauja griežtų asmens duomenų apsaugos taisyklių (BDAR). Asmens duomenų tvarkymo organizavimas yra apibendrintas penktame paveikslėlyje. Šiame procese dalyvauja „duomenų subjektas“ (asmens duomenų savininkas), „duomenų valdytojas“, kuris nustato tvarkymo tikslą ir priemones, taip pat yra atsakingas už visus „duomenų tvarkytojus“ ir „asmens duomenų gavėjas“. Reikia nepamiršti, kad asmens duomenų pateikimas gali būti pagrįstas tik teisėtais tikslais.



Šaltinis: Romansky R.2014, p 72

Pav. 5 Asmens duomenų tvarkymas

Viena didžiausių problemų interneto socialinių tinklų domenų valdyme yra privatumo problema. Privatumas socialinių tinklų kontekste suprantamas kaip: vartotojo tapatybės anonimiškumas; vartotojo erdvės privatumas; vartotojo bendravimo privatumas. Socialiniai tinklai pagrįsti asmens duomenų atskleidimu ir jų naudojimu ir visi teikiami duomenys (gyvenamoji vieta, pomėgiai, šeimyninė padėtis ir kt) gali sukurti išsamų vartotojų interesų ir veiklos profilį. Valdant didelius duomenų kiekius apie vartotojus, dažnai kyla „antrinio panaudojimo“ rizika (Solove D.J. 2006), kai asmeniniai socialinio tinklo vartotojų duomenys naudojami visai ne tais tikslais, kuriems jie buvo surinkti. Naujausi, 2018 m. kovo/balandžio *Cambridge analitica* įvykiai parodė kiek daug duomenų galima gauti apie socialinių tinklų vartotojus, susisteminus visą turimą informaciją. Ir kaip valdant tokią informaciją galima manipuliuoti visuomenės nuomonę.

Apibendrinant galima teigti, kad duomenų valdymo interneto socialiniuose tinkluose pagrindinė problema yra tame, kad už saugumą yra atsakingi ne tik duomenų valdytojai, tvarkytojai, bet ir patys vartotojai. Nepageidaujamas asmeninės informacijos atskleidimas gali įvykti ne tik dėl paslaugos teikėjo netinkamos saugumo politikos, bet ir dėl vartotojų neišprusimo bei saugumo / privatumo taisyklių ir rekomendacijų nesilaikymo.

1.5. Duomenų apsaugos valdymo analizė

Asmeninės informacijos tvarkymas ir asmeninių duomenų atskleidimas interneto socialiniuose tinkluose kelia vis didesnį susirūpinimą. Posey ir kt. (2010 m.) nustatė, kad socialinė įtaka ir pasitikėjimas interneto svetainėmis padidino vartotojų duomenų viešinimą interneto socialiniuose tinkluose. Kiti autoriai teigia, kad duomenų atskleidimas yra svarbesnis interneto svetainių ar socialinių tinklų nustatymuose, kur galima likti anoniminiu vartotoju (Altschuller, Benbunan-Fich, 2013 m.) ar pateikti netikslią, gal net klaidinančią, informaciją apie savo asmenį ir tokiu būdu jaustis mažiau pažeidžiamam.

Socialinių tinklų tyrimai atskleidė, kad vartotojų suvokimu, liekant anoniminiu vartotoju mažina jų privatumo susirūpinimą, o tai savo ruožtu daro įtaką duomenų atskleidimui (Jiang ir kt., 2013 m.). Nustatyta, kad atskleidimo laipsnis skiriasi priklausomai nuo „santykio tarp komunikuojančių asmenų, pasirinkto komunikacijos būdo ir dažnumo“ (Nguyen ir kt., 2012, Trepte ir Reinecke (2013)). Kitaip sakant, kuo dažniau naudojamasi interneto socialiniais tinklais, tuo dažniau ir daugiau vartotojai atskleidžia savo duomenis.

Reikia atkreipti dėmesį į tai, kad interneto socialiniuose tinkluose „niekas nepamirštama“. Nors kartą paviešinus informaciją ar duomenis, visa tai vienokia ar kitokia forma išliks virtualioje erdvėje. Dar viena rizika yra klaidingas vartotojų suvokimas apie tai, kiek socialiniai tinklai yra uždari ir kam yra pasiekiama jų pateikiama informacija. Vartotojai mato tik mažą dalį informacijos ir nesuvokia, kad jų veiksmai, paspaudimai „patinka“ ar kitos reakcijos, paliktos šalia kitų SNS vartotojų paskelbimų, lieka užfiksuotos jų veiklos istorijoje. Paprastam vartotojui lieka nematoma kaip ir kokia informacija yra kaupiama, kaip ji gali būti ar yra panaudojama trečiųjų šalių komerciniais tikslais. Tai labai aiškiai parodė *Beacon* skandalas, kuris internetinių tinklų vartotojams leido suprasti kokia tai didelė duomenų rinkimo ir vartotojų elgesio stebėjimo sistema.

Beacon buvo socialinio tinklo *Facebook* reklamos sistemos dalis, kuri siuntė duomenis iš išorinių *Facebook* tinklalapių, siekdama rodyti vartotojams tikslines reklamas ir leisti jiems dalintis savo veikla su draugais. Visa gauta informacija būdavo perduodama net ir tada kai vartotojai nebūdavo prisijungę prie *Facebook* socialinio tinklo. Visi duomenų perdavimai vyko be vartotojų žinios (Story L., Stonenov B., 2007). Didžiausia problema buvo tai, kad *Beacon* nesuteikė vartotojams galimybės blokuoti informacijos siuntimą. Po skandalo *Facebook* pakeitė strategiją ir buvo imtasi privatumo modelio keitimo. Taip pat buvo nuspręsta, kad matoma dalis, kaip vartotojų profiliai ir socialinė veikla turi būti kruopščiai atskirtos nuo nematomų dalių. Kaip ir ledkalnio atveju, matoma dalis sudaro tik nedidelę visumos dalį.



Šaltinis: Pagal Lovejoy E.W. at all 2010 m

Pav. 6 Internetinių tinklų ledkalnio modelis

Tačiau, nematoma „ledkalnio“ dalis nuolat yra pildoma informacija ir duomenimis, kurie renkami iš matomoje dalyje esančių vartotojų sąveikų ir paskyrų aprašymų. Interneto socialiniai tinklai siekia atskirti „ledkalnio“ dalis, skatinti vartotojo motyvaciją teikti ir nuolat savanoriškai atnaujinti savo asmeninius duomenis.

Interneto socialinių tinklų svetainių svarba žmogaus socialinei plėtrai yra svarbi, tačiau reikia nepamiršti, kad socialinio tinklo privatumas ir saugumas yra aktuali problema, nes vartotojai ne visada sąmoningai SNS pateikia savo asmeninius duomenis.

Trumpai apibendrinant, privatumą interneto socialiniuose tinkluose galima vertinti labai daugiareikšmiškai. Dažniausiai sutariama, kad privatumas internete yra vertybė, nors *Facebook* įkūrėjas M. Zuckerberg viename interviu teigė, kad privatumas nebėra visuomenės norma (angl. <...> privacy no longer a social norm <...>)(Johsson, 2010). Vis dėl to, šį teiginį reiktų vertinti kaip išimtį, o privatumo apibrėžimą galima taikyti skirtingai, priklausomai kieno atžvilgiu ir kokiu atveju jis yra taikomas.

Socialinių tinklų kūrėjai turi suprasti privatumo sąvoką ir sukurti privatumo modelį, kuris atitiktų vartotojų poreikius ir apsaugotų jų duomenis. Deja dauguma socialinių tinklų vartotojų nežino apie privatumo ir saugumo problemas, kurios paprastai gali kelti grėsmę duomenų saugumui ir toliau naudoja socialinių tinklų svetaines dalindamiesi asmenine, o kartais ir jautria informacija.

1.5.1. Vartotojo vaidmens aspektai

Sparti interneto paslaugų plėtra, augantis naudojimasis šiomis paslaugomis atskleidžia tiek savo privalumus, tiek ir grėsmes, ypač privatumo srityje. Šios grėsmės pirmiausia liečia visus vartotojus, kurie ypač aktyviai naudojasi interneto socialiniais tinklais. Dažnai situacija kai vartotojų žinios ir gebėjimai šioje srityje yra nepakankami, tad kyla tiesioginė grėsmė, kad vartotojas bus pažeidžiamas. Dažniausiai grėsmės yra susijusios su privačios informacijos paviešinimu, neteisėtu asmens duomenų ar atvaizdo naudojimu, nepageidaujamais pranešimais (SPAM). Taip pat žala kompiuteriui ir jame esantiems duomenims. Tokiais būdais kaip: virusai – kenksmingi failai, dažnai plintantys el. paštu; kirminai – labai sparčiai besidauginantys virusai, galintys sukurti tunelį į vartotojo kompiuterį ir leisti jį ir jo duomenis valdyti nuotoliniu būdu; trojos arkliai (trojanai) – kenksmingos kompiuterinės programos, besislepiančios kitose programose ir išoriškai atrodančios kaip naudingos; šnipinėjimo programinė įranga (angl. *spyware*) – programos, kurios renka informaciją apie vartotojo veiksmus bei lankomus tinklalapius internete ir perima asmens duomenis. Šios kenkėjiškos programos perduoda surinktus duomenis jų kūrėjams ar nusikalstamų ketinimų turintiems asmenims be vartotojo žinios. Svarbu suvokti ir vertinti ne tik interneto teikiamas galimybes, bet ir įžvelgti galimas grėsmes, bet imtis veiksmų galinčių užkristi kelią kylančioms rizikoms išvengti ar bent sumažinti iki minimumo.

2014 m. vasarą JAV įvykęs *Cambridge Analytica* atvejis labai akivaizdžiai parodė, kad daugelis vartotojų, neįsigilinę į privatumo ir naudojimo taisykles, duoda sutikimus „prieiti“ prie jų duomenų trečiosioms šalims. Politinė konsultacinė firma *Cambridge Analytica* nusamdė tyrėją rinkti pagrindinę *Facebook* vartotojų profilio informaciją, taip pat informaciją, kurią vartotojai pasirinko paspaudę mygtuką „patinka“. Beveik 300 000 *Facebook* vartotojų sumokėjo nedidelę sumą, kad parsiųstų programą, pavadinimu „Tai yra jūsų skaitmeninis gyvenimas“. Ši programa pateikė daugybę apklausų, kurios surinko ne tik, programą parsisiuntusių, vartotojų, bet ir jų, socialiniame tinkle *Facebook* esančių, draugų duomenis. Jei vartotojų privatumo nustatymai leido tai padaryti. Taip vartotojų, kurių duomenys tapo pasiekiami, skaičius nuo 50 mln. išaugo iki 87 mln. Programoje pagal paslaugų teikimo sąlygas buvo pateikta, kad ji rinktų tinklo narių ir jų draugų duomenis.

Labiausiai paplitusi vartotojų apsaugos strategija, mažinti profilio matomumą ribojant prieigą prie draugų. Vartotojams apriboti profilio matomumą kitiems skirtingose socialinės žiniasklaidos svetainėse yra labai paprasta, tam užtenka kelių žingsnių. Pavyzdžiui:

Facebook: privatumo nustatymas naujiems vartotojams galima nurodyta, kad matytų tik asmenys esantys draugų sąraše - *Friends Only*. Norint įjungti šį nustatymą užtenka nustatymuose pakeisti pasirinkimus ties Nustatymai > Privatumas > Kas gali matyti būsimus jūsų pranešimus?

Twitter: Pranešimai > Nustatymai > Sauga ir privatumas > Privatumas > Privatumo privatumas > Apsaugokite mano žinutes.

LinkedIn: Norėdami pakeisti šį: Nustatymai> Paskyra> Naudingos nuorodos> Redaguoti savo viešąjį profilį.

Tai greitas ir pakankamai paprastas sprendimas, bet tuo pačiu ir silpnas mechanizmas, o ne sistemingas požiūris į privatumo ir duomenų apsaugą. (Debatin B. Jennette P. at all, 2009) Dauguma vartotojų nesuvokia, jog apriboti prieigą prie jų duomenų nepakanka, būtina atsižvelgti į riziką, kurią kelia jų teikiamų duomenų dydis, kokybė ir saugojimas interneto socialiniuose tinkluose. Kol vartotojai, nematomai „ledkalnio“ daliai, tiekia asmens duomenis, kuriuos jie atnaujina savanoriškai ir nuolat, jų privatumui ir duomenų saugumui kylanti rizika išlieka pastovi, o kai kada net ir didėja.

Buvo atliktas tyrimas (Senthil Kumar N. et al. 2016 m), kurio rezultatai parodė, kad vartotojai žino apie galimybę patiems tvarkyti savo privatumo ir saugumo nustatymus. Tačiau tik 52% yra bent iš dalies susipažinę su interneto socialinių tinklų taisyklėmis. Žemiau esančioje lentelėje pavaizduoti skirtingi privatumo mechanizmai, kuriuos siūlo interneto socialiniai tinklai.

Table 1. Privacy concerns in Social Media site and its comparisons

Privacy options	FaceBook	Twitter	LinkedIn	Google+
Restrict the visibility of the active users	Yes	No	No	No
Set the control on how others can find you	Yes	Yes	Yes	No
Block the users for their photo tag	Yes	No	No	Yes
Set login Alerts	Yes	No	No	Yes
Block Spam Users	Yes	Yes	Yes	Yes
Control who can message you	Yes	No	Yes	Yes

Šaltinis: Pagal Senthil Kumar N. at al 2016 m

Pav. 7 Privatumo nustatymai SNS ir jų palyginimai

Vartotojai patys gali nustatyti privatumo nustatymus. Tokios funkcijos kaip galimybė keisti nustatymus nurodant kaip kiti socialinio tinklo vartotojai gali rasti norimo asmens anketą ar užblokuoti nepageidaują asmenį yra siūlomos visų socialinių tinklų. Išskirtinai *Facebook* socialinis tinklas leidžia nurodyti kas ir kaip gali matyti vartotojo profilį, taip pat valdyti gaunamų žinučių nustatymus – iš ko gauti asmeninius pranešimus.

Vis dėlto tyrimo metu nustatyta, kad daugelis socialinių tinklų vartotojų mano, kad SNS neatsižvelgia ir net nebūtinai laikosi tokių privatumo ir saugos nustatymų, kuriuos pasirenka patys socialinio tinklo vartotojai.

Apibendrinant galima teigti, kad derinant švietimą ir mokymasis su geriausios kokybės technologijomis, diegiant technines kontrolės priemones, sistemingai kuriant ir populiarinant kibernetinio saugumo kultūrą (angl. *cyber security culture*) gali būti geriausias būdas vartotojo

atžvilgiu sušvelninti ir sumažinti galimas rizikos grėsmes kylančias socialiniuose tinkluose, gerinti duomenų valdymą interneto socialiniuose tinkluose.

1.5.2.Socialinio tinklo vaidmens aspektai

Interneto socialiniai tinklai tapo populiariausia komunikacijos priemone. SNS vartotojų skaičius visame pasaulyje yra nuolatinis ir kasmet didėja. Statistikos portalo *Statista* duomenimis naudotojų skaičius keičiasi milijardais, prognozuojama, kad iki 2021 m. socialinių tinklų vartotojų bus daugiau kaip 3 milijardai.

Saugumo iššūkiai ir privatumas yra interneto socialinių tinklų svetainių reikalavimai. Tačiau kibernetinių atakų skaičius kiekvienais metais vis didėja (Symantec, 2017) ir socialiniai tinklai patiria vis daugiau išpuolių, nuo kurių, socialinių tinklų analitikai ir kūrėjai, turi apsaugoti potencialius vartotojus. Ta pati ataskaita teigia, kad SNS tapo pagrindiniu užpuolikų, užsiimančių tapatybės vagystėmis, taikiniu.

Pagrindiniai kibernetiniai išpuoliai prieš socialinius tinklus gali būti suskirstyti į tris kategorijas. (Deepa K. 2016)

- Privatumo pažeidimas – ieškoma tinklo apsaugos pažeidžiamumų, kuriais būtų galima pasinaudoti.
- Pasyvios atakos – tai visiškai anoniminės ir neaptinkamos.
- Aktyvios atakos – ne tik ieško pažeidžiamumų, bet ir bando prisijungti prie sistemos kur toliau naudojantis nesutvarkytais arba blogai sukonfigūruotais nustatymais skverbiasi gilyn į sistemą.

Žemiau pateiktoje lentelėje parodyta, kokias atakas patiria interneto socialiniai tinklai ir kokie siūlomi galimi sprendimų būdai kaip saugiai valdyti tokius išpuolius.

Pagrindiniai atakų vektoriai nukreipti į socialinių tinklų infrastuktūrą tam naudojant TCP SYN Flood atakas kai išnaudojama TCP protokolu paremto *3-way handshake* silpnybė. Tarnybinis serveris gauna iš naudotojo TCP protokolo sinchronizaciją inicijuojantį paketą su SYN „vėliavų“ rinkiniu. Nurodyta tarnybinė stotis siunčia naudotojui atgal TCP protokolo paketą ir laukia iš kliento galutinio TCP protokolo paketo, kuris turi patvirtinti TCP protokolo *3-way handshake* paremtą susijungimą. Remiantis šiuo principu atakos iniciatorius siunčia didelį kiekį TCP protokolo paketų tarnybiniai stočiai, o gavęs iš tarnybinės stoties sinchronizacijos patvirtinimą, nebesiunčia tarnybinei stočiai susijungimo patvirtinimo. Tarnybinė stotis siunčia atgal sinchronizacijos patvirtinimo paketus ir toliau laukia susijungimo patvirtinimo paketo iš kliento, galiausiai tarnybinės stoties buferis persipildo, dėl susikaupusio didelio kiekio eilėje laukiančių paketų. Taip yra sutrikdoma tarnybinė stoties veikla nepaliekant galimybės priimti bei apdoroti teisėtų naudotojų siunčiamų TCP protokolų. Panašiu principu naudojamos ir UDP *Flood* ar *DDOS* atakos.

Kiti prieš socialinius tinklus naudojami būdai yra įvairios kenkėjiškos programos kaip trojanai, kirminai (angl. *worms*), šnipinėjimui (angl. *spyware*) skirtos aplikacijos. Didelę riziką kelia socialinė inžinerija, dažniausiai naudojant fišingą (angl. *phishing*) nes gali būti pritaikyta ir platinama praktiškai bet kokiomis skaitmeninėmis priemonėmis: elektroniniais laiškais, pokalbių programomis, trumposiomis žinutėmis, įmonių administruojamomis sistemomis ar skaitmeninėmis anketomis.

Table 2. Major attacks, sub-attacks, and possible preventive policies [10]

Major domain of attacks [10]	Sub-attacks	Solution to handle the attacks
Social Networking Infrastructure attacks	TCP SYN Flood Attack, Smurf IP Attack, UDP Flood Attack, Ping of death, Tear Drop	-Use Anti-Virus and Anti-Malware Software. -Install appropriate Intrusion Detection System.
Malware Attacks	Crimeware, Spyware, Adware, Browser Hijackers, Downloader, Tool Bars	-Use of Anti-Virus. -Do not go for unknown links, friends, applications, email attachments etc., -Disable Cookies, Sessions, ActiveX if unknown or no counter-measures available.
Phishing Attacks	Deceptive phishing (emails), Malware-based phishing, Keyloggers, Search engine phishing	-Examine the emails carefully. -Validate the source of the data. - Beware of ads with offers
Evil Twin Attacks	Social engineering attack	-Careful about having friends and sharing information. -Authenticate the user profile and share the data. -Try to completely understand the policies of having friends in the social networking sites.
Identity Theft Attacks	Dumpster diving	-Use complex passwords, avoid password re-usage. -Shred your email or documents properly.
Cyberbullying	Cyberbullying	-Do not acknowledge the messages that are intended to hurt or threat. -Save and Archive the messages as evidences. -Take all threats seriously -Do not share personal information with all users.
Physical Attacks	Impersonation, Harassment through messages	-Need a well defined social networking policy. -Background security and privacy checks. -Properly make use of privacy settings options.

Šaltinis: Deepa K. 2016

Pav. 8 Atakų prieš SNS valdymo politika

Šiuo metu daugelis socialinių tinklų turi privatumo funkcijas leidžiančias tvarkyti vartotojų duomenis ir neskelbti jų viešai. Tačiau socialinių tinklų naudojamos trečiųjų šalių programos taip pat kelia didelę grėsmę duomenų saugumui ir privatumui. Pvz.: daugelis SNS, tokių kaip *Facebook*, savo vartotojams pateikia žaidimų ar kitas programas, kurios reikalauja vartotojo kredito kortelės duomenų, kitos asmeninės informacijos. Trečiosioms šalims teikiami duomenys didina duomenų praradimo tikimybę.

Per pastaruosius kelerius metus interneto socialinių tinklų saugumas pritraukė daugelio saugumo srities mokslininkų dėmesį tiek pramonės, tiek akademinėse srityse. Siekiant išspręsti šias minėtas grėsmes saugumui, buvo pasiūlyti įvairūs sprendimai. (Jeong Y. 2017)

Naudoti antivirusines programas, taip pat ir nuo kenkėjiškų programų saugančią programinę įrangą. Įdiegti įsilaužimus fiksuojančią sistemą, riboti sesijų laiką, nenaudoti slapukų. Tikrinti ar patikimi duomenų šaltiniai.

Deja daugelis socialinių tinklų neturi savo duomenų centrų ir paprastai vartotojų duomenys būna saugomi trečiųjų šalių duomenų centruose. Tai kelia riziką, kad šie centrai gali dalytis turimais duomenimis su kitais duomenų platintojais ar gali atskleisti vartotojų duomenis kitoms organizacijoms be jų leidimo ar pranešimo apie tai. Todėl vartotojų duomenys turėtų būti saugomi šifruotoje formoje, kad apsaugotų ją nuo kenkėjiškų teikėjų ar kitų organizacijų. Yra keletas kriptografinių technologijų, kurias galima įdiegti socialiniuose tinkluose ir leisti vartotojams efektyviai saugoti ir atkurti savo duomenis, nesidalinant su trečiosiomis šalimis kaip paslaugų teikėjai ar debesų kompiuterijos (angl. *cloud computing*) paslaugų teikėjui. Yra ir kitų sprendimų, daugiausia dėmesio skiriant daugialypės terpės duomenų šifravimui (Tierney M. 2013) Pagrindinis šių sprendimų privalumas yra tas, kad jei kas nors sėkmingai gaus tiesioginę prieigą prie bendrai naudojamos daugialypės terpės duomenų, jie negalės pasiekti duomenų, kol neturės tinkamo dešifratoriaus.

Apibendrinat galima teigti, kad socialiniams interneto tinklams būtina turėti rizikų valdymo strategijas, pavyzdžiui tokias kaip rekomenduoja SANS (*The SysAdmin, Audit, Network, and Security Institute*) CC20 (CIS *Critical Security Controls*). Be abejo, socialinių tinklų apsauga yra nuolatinė mokslinių tyrimų kryptys su daugybe galimybių ir iššūkių, naujų rūšių privatumo ir grėsmių saugumo tyrimams, kaip keisti ir tobulinti SNS saugumo sprendimus, kad nesikartotų tokie masiniai duomenų vagysčių atvejai kaip 2018 m rugsėjo mėnesį kai *Facebook* prarado virš 50 mln. vartotojų duomenų.

2. DUOMENŲ APSAUGOS VALDYMO YPATUMŲ INTERNETO SOCIALINIUOSE TINKLUOSE ATVEJŲ ANALIZĖ

Šiame skyriuje apžvelgti trys skirtinų socialinių tinklų atvejai. Vienas populiariausių pasaulyje ir Lietuvoje socialinis tinklas *Facebook*, taip pat mikrotinklaraščiams (angl. microblogging) priskiriamas, kur publikuojami nedidelės apimties pranešimai, *Twitter* socialinis tinklas. Trečias aptariamas atvejis yra profesinis socialinis tinklas *LinkedIn* skirtas bendrauti su verslo partneriais, užmegzti naujus profesinius ryšius ir ieškoti darbo ar darbuotojų.

Visi trys socialiniai tinklai savo privatumo ir paslaugų teikimo taisykles yra paruošusios dviem variantais. Vienos jų skirtos "paskirtosioms šalims", t.y. galioja į Europos Sąjungos (ES) šalyse, Europos ekonominės erdvėje (EEE) ir Šveicarijoje. Visų tinklų atstovybės ES, EEE šalims ir Šveicarijai yra įsikūrusios Airijoje.

2.1. *Twitter* atvejo analizė

Šalyse kaip Jungtinės Amerikos Valstijos ar Jungtinė Karalystė *Twitter* yra vienas iš pagrindinių žiniasklaidos, žinomų visuomenės veikėjų bei pramogų pasaulio įžymybių informacinės sklaidos kanalų kur pirmiausia skelbiamos karščiausios naujienos, paskalos bei skandalai. Šis socialinis tinklas buvo sukurtas 2006 m.

Twitter – nemokama socialinių tinklų ir „microblogging“ paslauga, kuri leidžia registruotiems tinklo vartotojams skelbti ir skaityti trumpus pranešimus, taip vadinamuosius „tweetus“ (angl. tweets). Viena pagrindinių ir išskirtinių *Twitter* savybių yra kiekvienos žinutės apribojimas iki 280 simbolių. Tai reiškia, kad mintys turi būti dėstomos trumpai, aiškiai, bei patraukliai. Vartotojai taip pat gali įkelti nuotraukas ar trumpus vaizdo įrašus. Kita labai svarbi ir visiems gerai žinoma šios platformos savybė yra grotažymės # (angl. hashtags). Būtent *Twitter* yra šios, visą pasaulį užvaldžiusios manijos savininkė. *Twitter* yra vienas iš 10 lankomiausių interneto puslapių pasaulyje. Statistikos portalo *Statista* 2018 m. antro ketvirčio duomenimis *Twitter* turėjo 335 milijonus registruotų vartotojų. *Kantar TNS* rinkos tyrimų bendrovės 2017 m. duomenimis Lietuvoje iš 79 % besinaudojančių socialiniais tinklais šalies gyventojų 20,4 % naudojasi pastaruoju tinklu.

Socialinis tinklas *Twitter* praktiškai yra realaus laiko platforma. Informacijos srautas yra labai didelis, pavyzdžiui, kiekvieną sekundę šioje platformoje yra išsiunčiami ~6000 pranešimų. Priešingai nei kituose socialiniuose tinkluose, kur įprasta praktika yra pasidalinti 1-2 žinutėmis per parą, *Twitter* vartotojai žinutes skelbia po 5-10 ar net 20 kartų per dieną. Todėl vienos žinutės gyvavimo ciklas yra vos iki 20 minučių. Vėliau ji tiesiog pradingsta sraute ir paprasčiausiai tampa nebematoma.

Lietuvoje *Twitter* tinklas nėra toks populiarus kaip kitose šalyse. Dažniausiai šiuo tinklu vartotojais tampama tuomet, kai taikomasi į užsienio rinką. Vienos iš populiariausių lietuviškų *Twitter* paskyrų turi ir sėkmingai naudoja LR prezidentė, bei Užsienio reikalų ministerija ir ypač ministras.

Norint šiame socialiniame tinkle susikurti paskyrą, registruojantis reikia nurodyti vardą ir el. paštą arba telefoną. Pirminei registracijai užtenka šitų duomenų. Vėliau prisijungus yra galimybė pildyti ir keisti asmeninius duomenis. Viešai iškarto yra matomas pasirinktas prisijungimo vardas, elektroninis paštas ir telefono numeris (priklausomai kaip buvo registruojamasi) nėra skelbiami kitiems vartotojams. Sukurto vartotojo vardas yra matomas *Twitter* URL nuorodoje (pvz.: https://twitter.com/BiruteUz), kuri priskiriama iškarto kai tik užsiregistruojama *Twitter*, tačiau yra galimybė keisti savo vartotojo vardą. Toks pakeitimas neturi įtakos esantiems stebėtojams, tiesioginiams pranešimams ar atsakymams. Pakeitus jį stebėtojai tiesiog pamatys naują naudotojo vardą šalia profilio nuotraukos. SNS rekomenduoja prieš keičiant naudotojo vardą įspėti savo stebėtojus. Tai pat šis socialinis tinklas leidžia turėti ir valdyti kelias asmenines paskyras. Tačiau rekomenduojama tai daryti jungiantis per naršyklę arba naudoti *TweetDeck*. Galimybės sujungti, turimus kelis profilius, nėra.



Šalinis: https://twitter.com/Grybauskaite_LT

Pav. 9 Patvirtintas profilis

Socialinis tinklas *Twitter* turi patvirtintas paskyras. Mėlynas ženklelis šalia *Twitter* paskyros vardo leidžia vartotojams žinoti, kad profilis yra autentiškas. Ženklas rodomas šalia paskyros profilio pavadinimo ir šalia paskyros pavadinimo paieškos rezultatuose. Tai visada yra ta pati spalva ir pateikiama toje pačioje vietoje, nepriklausomai nuo profilio ar temos spalvų pritaikymų. Paskyrose, kuriose nėra šio ženklo šalia jų vardo, o jis rodomas kitur, pvz., profilio nuotraukoje, antraštėje arba šalia biografijos, nėra patvirtintos paskyros. Patvirtintas ženklelis nereiškia *Twitter* patvirtinimo.

Vartotojo profilis gali būti patvirtintas, jei yra nustatyta, kad tai yra viešojo intereso paskyra. Paprastai tai apima anketas, kurias tvarko muzikos, mados, režisūros, vyriausybės, sporto, politikos, religijos, žurnalistikos, žiniasklaidos, verslo ir kitų svarbių sričių vartotojai.

Visus iš *Twitter* gaunamus pranešimus vartotojas gali sekti *Notifications timeline*. Pranešimų laiko juostoje galima pamatyti, kuris iš vartotojo paskelbtų *tweets* buvo pamėgtas, taip pat naujausius pranešimus, kurie paskelbimai pasidalinti (angl. *retweets*), skirti vartotojui (atsakymai ir paminėjimai) ir informacija apie naujus stebėtojus. Tinklas leidžia nustatyti ką vartotojas mato ir su kuo bendrauja. Pranešimų nustatymuose yra trys parinktys, pagal kuriuos filtruojami gaunami pranešimai: kokybės filtras, neaktyvūs žodžiai ir išplėstiniai filtrai.

Vartotojas renkasi ką nori stebėti, tačiau taisyklėse numatyta, kad kiekvienas profilis „*by default*“, t.y. pagal nutylėjimą, gali sekti/stebėti 5000 kitų vartotojų profilių. Ši riba skiriasi kiekvienai paskyrai ir yra pagrįsta individualiu stebėtojų santykiu su kitais. Pvz.: paskyra negali stebėti 10 000 žmonių, jei tik pati turi tik 100 sekėjų/stebėtojų. Kitų paskyrų stebėjimas *Twitter* yra skirtingas nuo kitų socialinių tinklų. *Twitter* leidžia asmenims pasirinkti (arba atsisakyti) gauti asmens atnaujinimus, nereikalaujant abipusių santykių patvirtinimo.

Socialinis tinklas perspėja, kad vartotojai norėdami padidinti sekėjų skaičių, ar patys norėdami sekti/stebėti daugiau paskyrų gali susidurti su tinklalapiais ar programomis, kurie skelbiasi galintys padėti greitai įgyti daug sekėjų. Šios programos gali prašyti apmokėti stebėtojus arba prašyti sekti kitų paskyrų sąrašą, Naudojant šių trečiųjų šalių paslaugas yra pažeidžiamos *Twitter* taisykles.

Siekdamas išlaikyti socialinio tinklo aplinką saugią vartotojams, *Twitter* tinklas turi galimybę ir gali laikinai sustabdyti paskyras, pažeidžiančias jų saugumo ir privatumo taisykles. Dažniausios sustabdymo priežastys gali būti tokios:

- Šlamštas (angl. SPAM): dauguma laikinai sustabdytų paskyrų būna dėl to, kad tai yra šlamštas arba tiesiog netikros paskyros, kurios kelia pavojų *Twitter* ir tinklo vartotojų saugumui. Šios paskyros neatitinka *Twitter* taisyklių.
- Užgaulūs / įžeidžiantys pranešimai arba elgesys: sustabdoma paskyra, jei apie tai pranešta kiti socialinio tinklo vartotojai. Pavyzdžiui, kai paskyra naudojama piktnaudžiavimui siunčiant grėsmingus pranešimus kitiems asmenims ar įžeidžia kitus vartotojus.
- Saugumo rizikos valdymas: kilus įtarimų, kad paskyra buvo nulaužta ar sukompromituota, ji yra stabdoma tol, kol bus apsaugota ir atkurta paskyros savininkui. Taip siekdama, kad būtų sumažinta potencialiai kenksminga veikla, kurią sukelia įsilaužimas.

Nusprendus nebesinaudoti socialiniu tinklu, turimą paskyrą siūloma deaktyvuoti. Vartotojui išjungus savo profilį, *Twitter* paskyra, įskaitant rodomą vardą, naudotojo vardą ir viešąjį profilį, nebebus prieinama peržiūrai. Ne ilgiau kaip per 30 dienų po išjungimo vis dar galima atkurti *Twitter* paskyrą, jei ji buvo išjungta netyčia arba neteisingai. Neatkūrus anketos per 30 dienų, to padaryti nebegalima, o norint naudotis *Twitter* teikiamomis paslaugomis reikia kurti naują profilį. Socialinis tinklas iš karto įspėja, kad nekontroliuoja turinio, indeksuojamo paieškos sistemų, tokių kaip *Google* ar *Bing*.

Paskyroms naudojamos verslo tikslais *Twitter* siūlo naudoti sukurtus analitinius įrankius ir analizuoti bei suprasti, kaip paskyros kuriamas turinys gali padėti verslui. Žinomumui didinti socialinis tinkas pateikia net kelis pasiūlymus:

- *Twitter Ads* – galimybė pasirinkti labai tiksliai išprofiliuotas tikslines grupes, kurioms būtų skirtos reklamos.
- *Twitter Promote Mode* – automatinis paskyros reklamavimas už mėnesinį mokestį.

- *Twitter Ads for agencies* – programa padedanti agentūroms kurti strategijas, valdyti didelius projektus, planai, kaip pritaikyti *Twitter* įmonės reklamavimui didinant pardavimus.

Twitter paslaugų teikimo ir privatumo sąlygos

Paslaugų teikimo sąlygos reglamentuoja vartotojo prieigą prie tinklo paslaugų ir jų naudojimo, įskaitant įvairias svetaines, SMS, API, el. Pašto pranešimus, programas, valdiklius, skelbimus, komercines paslaugas ir kitas socialinio tinklo teikiamas paslaugas ir bet kokią informaciją, tekstą, nuorodas, grafiką, nuotraukas, garso įrašus, vaizdo įrašus ar kitas medžiagas atsisiųstas ar rodomas tinkle. Vartotojai naudodamiesi tinklo paslaugomis sutinka laikytis šių sąlygų. Reikia pastebėti, kad paslaugų teikimo sąlygos yra skirtingos gyvenantiems JAV ir kitose valstybėse. Šiuo atveju nagrinėjamos ES šalims galiojančios taisyklės.

Kas gali naudotis? Naudotis *Twitter* paslaugomis tik tuo atveju, kai sutinkama su *Twitter* sudaryti privalomą sutartį. Paslaugų gavėjo amžius turi būti nemažesnis kaip 13 metų, o *Periscope* atveju 16 metų.

Privatumas. Vartotojai naudodamiesi paslaugomis sutinka, kad bus renkama ir naudojama informacija apie juos, ir kad šie duomenys bus perduoti Jungtinėms Amerikos Valstijoms, Airijai ir (arba) kitoms valstybėms saugoti, apdoroti ir naudoti *Twitter* ir jos filialams.

Turinys. Vartotojas atsakingas už naudojimąsi paslaugomis ir bet kokį turinį, kurį pateikia, įskaitant turinio atitinkamą įstatymams, taisyklėms ir nuostatų laikymuisi. Socialinis tinklas pasilieka teisę pašalinti turinį, kuris pažeidžia Vartotojų sutartį, įskaitant, pvz., autorių teisių ar prekių ženklų pažeidimus, neteisėtus veiksmus, priekabiavimą ir pan.

Vartotojo teisės. Vartotojas išsaugo savo teises į bet kurį turinį, kurį pateikia, skelbia ar rodo socialiniame tinkle. Pateikdamas, skelbdamas ar rodydamas turinį vartotojas suteikia tinklui, visame pasaulyje be apribojimų naudoti, kopijuoti, dauginti, apdoroti, pritaikyti, modifikuoti, publikuoti, perduoti, rodyti ir platinti turinį, bet kurioje žiniasklaidos priemonėje. Ši leidimas įgalina tinklą vartotojo turinį padaryti prieinamą kitiems, neapribotą geografiškai ir leisti kitiems vartotojams dalintis informacija. Vartotojas sutinka su *Twitter* teise teikti, reklamuoti ir tobulinti paslaugas, bei pateikti turinį kitoms bendrovėms, organizacijoms ar asmenims, kad galėtų sindikuoti, transliuoti, platinti, reklamuoti, laikantis socialinio tinklo turinio naudojimo sąlygų. Tokie papildomi *Twitter* ar kitų įmonių, organizacijų ar asmenų naudojimai gali būti atliekami be jokios kompensacijos, mokamos vartotojui dėl turinio, kurį pateikė per socialinį tinklą.

Vartotojas garantuoja, kad turi arba gavo visas teises, licencijas, sutikimus, leidimus, įgaliojimus reikalingus dėl bet kurio turinio, kurį pateikia soc. tinkle arba per jo paslaugas. Vartotojas sutinka, kad

neskelbs turinio, kuriam taikomas autorinės ar kitos nuosavybės teisės, nebent turi reikiamą leidimą ar kitaip teisėtai gali paskelbti medžiagą.

Naudojantis paslaugomis. Būtina susipažinti su *Twitter* ir *Persicope* taisyklėmis, kurios yra vartotojo sutarties dalis. *P*aslaugomis galima naudotis tik laikantis visų galiojančių įstatymų, taisyklių ir nuostatų. Paslaugos gali keistis. Tinklas gali sustabdyti (visam laikui ar laikinai) teikti paslaugas ar visas tam tikras funkcijas konkrečiam vartotojui ar visiems vartotojams apskritai. *Twitter* pasilieka teisę bet kuriuo metu savo nuožiūra kurti naudojimo ir saugojimo apribojimus. Taip pat gali pašalinti arba atsisakyti platinti bet kurį turinį, sustabdyti ar nutraukti paskyras ir išieškoti vartotojo informaciją be jokios atsakomybės prieš vartotoją.

Gaudamas *Twitter* paslaugas vartotojas sutinka, kad tinklas ir jo trečiųjų šalių tiekėjai bei partneriai gali pateikti reklamą soc. tinklo teikiamose paslaugose ar kartu su rodoma informacija iš kitų paskyrų.

Vartotojui, naudojant *Twitter* paslaugas, draudžiama:

- pasiekti, pažeisti arba naudoti ne viešąsias paslaugų sritis, *Twitter* kompiuterių sistemas ar *Twitter* teikėjų technines pristatymo sistemas;
- zonduoti, nuskaityti arba išbandyti bet kokios sistemos arba tinklo pažeidžiamumą arba pažeisti arba apeiti bet kokias saugumo ar autentiškumo nustatymo priemones;
- pasiekti, ieškoti arba bandyti pasiekti ir/arba ieškoti paslaugų bet kokiomis priemonėmis (automatizuotomis ar kitomis priemonėmis);
- kurti bet kokią TCP / IP paketų antraštę ar bet kurią antraštės informacijos dalį el. pašte ar skelbime, arba bet kokiu būdu naudoti paslaugas siųsti pakeistą, apgaulingą ar klaidingą šaltinio identifikavimo informaciją;
- kištis arba sutrikdyti (arba bandyti tai padaryti) bet kurio vartotojo, prieigą prie tinklo, įskaitant, bet tuo neapsiribojant, viruso siuntimą, perkrovimą, *buffering*, šlamštą, pašto užkimšimo (SPAM) paslaugas arba sukūrus turinį tokiu būdu, kad trukdytų arba sukurtų nepagrįstą srauto apkrovą.

Tinklas pasilieka teisę susipažinti, skaityti, išsaugoti ir atskleisti bet kokią informaciją, kurią pagrįstai mano kad būtina jog:

- įvykdytų bet kokius taikomus įstatymus, reglamentus, teisinius procesinius veiksmus ar vyriausybės prašymus;
- kad aptiktų, užkirstų kelią ar kitaip spręstų sukčiavimo, saugumo ar techninių problemų klausimus;
- atsakytų į naudotojų palaikymo užklausas
- apsaugotų vartotojų ir visuomenės teises, nuosavybę ar saugumą.

Twitter neatskleidžia asmeninės informacijos trečiosioms šalims, išskyrus pagal nustatytas privatumo taisykles ir politiką.

Vartotojas atsakingas už savo paskyros apsaugą, todėl turo naudoti saugų ir sudėtingą slaptažodį. Socialinis tinklas negali ir neprisiima atsakomybės už jokius nuostolius ar žalą, atsiradusius dėl to, kad vartotojas nesilaikė taisyklių. Vartotojas gali kontroliuoti daugumą pranešimų. Tinklo paslaugų ir administraciniai pranešimai yra laikomi paskyros dalimi, todėl jų negalima atsisakyti. Jei į paskyrą pridėtas asmeninis telefono numeris, o vėliau jis pakeistas ar deaktyvuotas, reikia atnaujinti paskyros informaciją.

Twitter suteikia asmeninę, geografiškai neapribotą nemokamą, neperduodamą ir neišimtinę licenciją naudoti programinę įrangą, kuri vartotojui teikiama kaip paslaugų dalis.

Bet kada galima nutraukti teisinį susitarimą su *Twitter*, deaktyvuojant profilį ir nutraukiant naudojimąsi paslaugomis. Tinklas bet kada gali laikinai sustabdyti ar nutraukti paskyrą ar nutraukti paslaugų teikimą, jei mano, kad yra pagrįstas spėjimas jog sulaužytos paslaugų teikimo taisyklės.

Atsakomybės apribojimai. Naudodamiesi tinklo paslaugomis vartotojai sutinka, kad *Twitter* bei jo padalinių, susijusių kompanijų, pareigūnų, darbuotojų ir partnerių atsakomybė yra visiškai apribota, bet nedaugiau, nei tą leidžia šalies įstatymai, kurioje yra vartotojas.

Bendrai. Tinklas gali keisti šias sąlygas. Pakeitimai nevykdomi atgaline data, o naujausia sąlygų versija skelbiama twitter.com/tos. Apie pakeitimus, susijusius su naujomis funkcijomis ar dėl teisinių priežasčių, pranešama prieš 30 dienų.

Privatumo taisyklės

Twitter reikalauja tam tikros informacijos, kad suteiktų paslaugas. Nereikia kurti paskyros jei norima naudotis kai kuriomis paslaugomis, kaip pvz., ieškoti ir žiūrėti viešuosius *Twitter* profilius. Jei vartotojas nori dalintis savo turiniu – būtina turėti paskyrą. Reikia patiekti tokius asmeninius duomenis: vartotojo vardas (pvz., @TwitterVartotojas), slaptažodis ir el. pašto adresas arba telefono numeris. Vardas ir vartotojo vardas (slapyvardis) visada yra vieši. Galima naudoti tiek savo tikrąjį vardą, tiek slapyvardį. Kai vartotojas tampa registruotu tinklo nariu, *Twitter* renka vartotojo informaciją ir naudoja ją, kaip teigiama, tinklo paslaugų teikimui.

Vieša informacija.

Didžioji *Twitter* veikla yra vieša, įskaitant profilio informaciją, vartotojo laiko juostą (angl. *home*), kalbą, pranešimus, bei tam tikrą informaciją apie paskelbtas žinutes (angl. *tweets*). Tai pvz., datą, laiką, programą bei *Twitter* versiją, kuria naudojantis buvo paskelbtas pranešimas. Galima pasirinkti ar viešai skelbti savo buvimo vietą. Vartotojo sukurti sąrašai, asmenys, kuriuos seka ir kurie seka/stebi vartotoją, pamėgti (angl. *Tweets you Like*) ir/ar pasidalinti (angl. *retweet*) pranešimai, taip pat vieši.

Vartotojo „širdis“ (angl. *like*), komentarai, gautų „širdžių“ skaičius ar kitas turinys, kurį vartotojas prisideda prie paskyros taip pat yra vieši. Visiems matoma ir kai kiti asmenys pažymi vartotoją nuotraukoje (jei leidžia nustatymai) arba pamini komentare. Tinklo vartotojas pats atsakingas už savo komentarus ir kitą informaciją, kurią pateikia *Twitter* paslaugose.

Be tiesioginės viešosios informacijos gavimo tiesiogiai iš vartotojo, *Twitter* taip pat naudoja tokias technologijas kaip programų programavimo sąsajos (API) ir įterpimo funkcijos, kad ši informacija būtų prieinama svetainėms, programoms ir kitiems naudotojams.

Kontaktinė informacija ir adresų knygos.

Twitter naudoja tokią kontaktinę vartotojo informaciją kaip el. paštas ar telefono numeris. Tai būtina paskyros autentifikavimui, apsaugai, užtikrintų teikiamas SNS paslaugas, bei užkirstų kelią šlamštui, sukčiavimui ir piktnaudžiavimui. Kontaktinė informacija taip pat naudojama paslaugų individualizavimui, atskirų funkcijų įgalinimui (pvz., prisijungimo patvirtinimui). Pateikus telefono numerį, pagal nutilėjimą duodamas sutikimas gauti tekstinius pranešimus iš *Twitter*. Kontaktinė informacija taip pat skirta parduoti, kaip leidžia konkrečios šalies įstatymai, padėti kitiems surasti vartotojo paskyrą (jei leidžia nustatymai), įskaitant trečiųjų šalių ir kliento programas.

Teikiama paslauga leidžianti pasirinkti ar įkelti ir sinchronizuoti vartotojo adresų knygą, kad galėtų greičiau rasti, susisiekti su žmonėmis. Šią informaciją *Twitter* taip pat renka, kaip teigia, norėdami geriau rekomenduoti turinį.

Funkcionalumas leidžiantis užsiregistruoti naudojant paskyrą iš kitos paslaugos, tokios kaip *Google* ar *Facebook* taip pat leidžia *Twitter* naudoti šios paslaugos informaciją, įskaitant el. pašto adresą, draugus ar kontaktų sąrašą. Gautus el. laišką, išsaugo su pranešimo turiniu, el. adresu ir kontaktine informacija.

Tiesioginiai pranešimai ir ne viešieji ryšiai.

Tinklas teikia funkcijas, kurios leidžia bendrauti privačiau arba kontroliuoti, kas mato turinį. Kai bendraujama su kitais, siunčiant ar priimant tiesiogines žinutes, *Twitter* saugo ir apdoroja vartotojo ryšius ir su jais susijusią informaciją. Tai apima kenkėjiško turinio nuorodų nuskaitymą, nuorodų sutrumpinimą į URL adresus (pvz.: http://t.co), šlamšto ir draudžiamų vaizdų aptikimą bei apie praneštų problemų peržiūrą. Taip pat tinklas naudoja informaciją, su kuo ir kada buvo susisiekta (bet ne pranešimų turiniu).

Mokėjimo informacija.

Šis funkcionalumas leidžia įsigyti reklamos paslaugas ar kitus mokamus pasiūlymus, kurie yra *Twitter* paslaugų dalis. Tuo pačiu reikia pateikti mokėjimo informaciją, įskaitant kredito arba debeto kortelės numerį, kortelės galiojimo datą, CVV kodą ir atsiskaitymo adresą.

Kaip kontroliuojama informacija, kuria vartotojas dalinasi su *Twitter*

Vartotojo privatumo ir saugos nustatymai leidžia nuspręsti: ar vartotojo pranešimai yra viešai pasiekiami *Twitter*; ar kiti gali pažymėti nuotraukoje; ar galima gauti tiesiogines žinutes iš bet kurio *Twitter* ar tik pasekėjų; ar kiti gali rasti pagal pateiktą el. pašto adresą ar telefono numerį; ar įkelta adresų knygą *Twitter* saugojimui ir/ar naudojimui; kada ir kur galima pamatyti *Twitter* jautrų turinį; ar norima blokuoti ar išjungti kitas *Twitter* paskyras.

Apibendrinant galima teigti kad, skirtingai nuo *Facebook* ar *LinkedIn* šio tinko vartotojams nėra būtinybės „draugauti“ tinkle, nereikalingas abipusis patvirtinimas.

Twitter turi platų funkcionalumą leidžianti socialinio tinklo vartotojams patiems pasirinkti privatumo ir saugumo nustatymus. Tuo pačiu renka labai didelį informacijos kiekį apie savo vartojus nuo gyvenamosios vietos iki kreditinių kortelių numerių, tuos duomenis išnaudodama rinkodaros tikslais. Remdamasis gautais filtruotais ir išanalizuotais asmeniniais duomenimis, *Twitter* verslo paskyrom teikia reklamos paslaugas. Visais atvejais, kai prašoma vartotojo duomenų yra pagrindžiama paslaugų teikimo kokybe – < ...kad geriau suprastumėte mūsų paslaugų naudojimą, kad apsaugotumėte mūsų platformos saugumą ir vientisumą bei rodytume labiau tinkamą turinį...>. *Twitter* taip pat gali užrakinti paskyrą arba nustatyti tam tikrų paskyros funkcijų laikinuosius apribojimus, jei, tik manys, kad vartotojo paskyra pažeista arba pažeidžia *Twitter* taisykles arba paslaugų teikimo sąlygas.

1 Lentelė. **Socialinio tinklo *Facebook* naudojimosi ir privatumo taisyklių santrauka**

Pirminė reikalinga informacija registruojantis	El. pašto adresas arba telefono numeris, prisijungimo vardas.
Naudojimosi amžius	Privatumo taisyklėse nurodoma amžiaus riba 13 metų, registruojantis – 16 metų.
Skelbiamų žinučių dydis	Iki 280 simbolių.
Privatumo nustatymai	Taip
Galimybė blokuoti nepageidaujamus asmenis	Taip
Draudimas žymėti skelbiamame turinyje / nuotraukose	Taip / Taip
Galimybė pasirinkti kas gali susisiekti per SNS	Ne
Vietos nustatymas	Taip
Dviejų veiksmų autentifikacija	Taip
Pasirinktų saitažodžių (angl. *hashtags*) blokavimas	Taip
Galimybė matyti sekėjus	Taip

2.2. *LinkedIn* atvejo analizė

LinkedIn – „Microsoft“ bendrovės profesinis socialinis tinklas. Šis tinklas skirtas bendrauti su verslo partneriais, užmegzti naujus profesinius ryšius ir ieškoti darbo ar darbuotojų. Tinklas uždirba iš reklamos bei mokamų paskyrų verslui. *LinkedIn* buvo sukurtas 2002 m.

Statistikos portalo *Statista* 2018 m. antro ketvirčio duomenimis *LinkedIn* turėjo 294 milijonus registruotų vartotojų. *Kantar TNS* rinkos tyrimų bendrovės 2017 m. duomenimis Lietuvoje iš 79 % besinaudojančių socialiniais tinklais šalies gyventojų 9 % naudojasi *LinkedIn* socialinio tinklu. „Lietuvą“ kaip dabartinę darbo vietą, nurodo apie ~105 tūkstančiai vartotojų.

2015 metais *LinkedIn* oficialiai aplenkė *Facebook* ir pakilo į pirmąją vietą kaip svarbiausias socialinis tinklas B2B sektoriuje.

LinkedIn galima vadinti įrankiu, kuris skirtas darbui, tai tarsi interaktyvus gyvenimo aprašymas su rekomendacijomis ir papildomomis galimybėmis. Šis socialinis tinklas naudoja protingus duomenų analitikos algoritmus, kurie patys rekomenduoja vartotojams įmones ar konkrečias darbo pozicijas, kurios pastariesiems galėtų būti įdomios. Algoritmai *LinkedIn* vartotojams automatiškai rekomenduoja kitus tinklo narius, su kuriais gali būti verta susipažinti.

LinkedIn vartotojai turi savo asmeninį profilį, kuriame galima patiekti informaciją apie save: darbo sritį ir šalį, dabartinę ir buvusias darbo vietas ir pareigas, išsilavinimą, įgūdžius, trumpą aprašymą apie save, profilio nuotrauką, draugų/kolegų sąrašą. Taip pat galima prašyti rekomendacijų patvirtinančių asmenį ir nurodytus duomenis. *LinkedIn* taip pat siūlo sąrašą asmenų, kuriuos vartotojas gali pažinoti (angl. *People You May Know*). Visi asmenys skirstomi pagal pažinčių lygius: pirmo lygio pažintys – asmenys, kurie prisijungė prie vartotojo pažinčių rato, antro lygio – pažįstamų pažįstami, trečio – pažįstamų pažįstamų pažįstami.

Darbo pasiūlymai ir darbuotojų paieška yra viena iš labiausiai vertinamų *LinkedIn* funkcijų. Dėl ypatingai patogios paieškos, daug vartotojų šią platformą naudoja ieškodami darbų arba potencialių kandidatų. Vartotojai gali ieškoti darbų pagal pasirinktus raktažodžius, darbo vietą, atstumą nuo miestų, reikalingą patirtį, atlyginimą. Taip pat gali išnaudoti ir įvairias aplikacijas, tokias kaip *WordPress, Slideshare, Amazon reading list* ir kt. Tai leidžia vartotojams automatiškai pasidalinti savo paskyros įrašais, įkelti prezentacijas ar pavyzdžiui pasidalinti įdomių knygų sąrašu. Vienas iš tinklo funkcionalumų – grupės. Jos gali būti labai įvairios, nuo mažų grupių (pvz.: klasės draugai), iki labai didelių, aprėpiančių plačias sritis.

LinkedIn taip pat leidžia sukurti oficialų įmonės puslapį, kuriame galima dalintis paskutinėmis naujienomis, darbo skelbimais, pagrindinėmis paslaugomis ir panašiai. Šiuos įmonių puslapius gali sekti visi vartotojai.

Pagrindinės šio socialinio tinklo funkcijos vartotojams yra nemokamos, tačiau *LinkedIn* siūlo planų turinčių daugiau galimybių. Pavyzdžiui nemokamo įprastinio (Basic Account) plano vartotojai paieškoje mato tik 100 rezultatų, aukštesnių lygių planai (Business Account, Business Account Plus, Pro Account) leidžia išnaudoti daugiau šio tinklo funkcijų.

LinkedIn paslaugų teikimo ir privatumo sąlygos

Paspaudus *Join Now, Join LinkedIn, Sign Up* – registruojantis, jungiantis prie šio tinklo paslaugų, vartotojas išreiškia sutikimą sudaryti teisiškai įpareigojančią sutartį su *LinkedIn* (net jei paslaugos naudojamos bendrovės vardu). Jei vartotojas nesutinka su šia sutartimi, tiesiog turi nesijungti prie *LinkedIn* tinklo teikiamų paslaugų. Jei norima nutraukti sutartį, tai galima padaryti bet kada, uždarant sukurtą paskyrą ir nebesinaudojant socialinio tinklo paslaugomis.

Sutartis taikoma LinkedIn.com, *LinkedIn* prekės ženklo programoms, *Slideshare, LinkedIn* mokymuisi ir kitoms su *LinkedIn* susijusiomis svetainėmis, programomis, ryšiais ir kitomis paslaugomis, įskaitant duomenis kai naudojami tinklo skelbimai ir papildiniai „*Taikyti su LinkedIn*“ (angl. *Apply with LinkedIn*) ir „*Dalinkitės su LinkedIn*“ (angl. *Share with LinkedIn*). Registruoti vartotojai yra „Nariai“ (angl. *Members*), o neregistruojami vartotojai – „Lankytojai“ (angl. *Visitors*). Ši sutartis taikoma tiek nariams, tiek lankytojams.

Naudojamas terminas „paskirtos šalys“, tai nuorodos į Europos Sąjungos (ES), Europos ekonominės erdvės (EEE) šalis ir į Šveicariją. Jei vartotojas gyvena kurioje nors iš „nurodytų šalių“, sutartis sudaroma su *LinkedIn Ireland Unlimited*. *LinkedIn Ireland* kontroliuoja, valdo, renka, tvarko visus vartotojo asmens duomenis, kuriuos jis pateikia naudodamasis tinklo teikiamomis paslaugomis.

LinkedIn gali keisti sutartį, privatumo ir slapukų politiką. Padarius esminių pakeitimų, vartotojui pranešama per tinklo paslaugas arba kitomis priemonėmis. Pakeitimai negali būti daromi atgaline data. Jei vartotojas prieštarauja bet kokiems pakeitimams, gali uždaryti savo paskyrą. Jei po paskelbimo apie pakeitimus paslaugų teikimo sąlygose vartotojas toliau nenutrūkstamai naudojasi paslaugomis, reiškia sutinka su pakeitimais.

Įsipareigojimai. Paslaugas draudžiama naudoti asmenims iki 16 metų. Norint naudotis paslaugomis, vartotojas patvirtina kad:

- yra „minimalus amžius“ arba vyresnis. „Minimalus amžius“ – 16 metų. Tačiau, jei įstatymai reikalauja kad *LinkedIn* nariu galima teisėtai būti nuo didesnio amžiaus, tai toks minimalus amžius ir bus.
- Turi tik vieną *LinkedIn* paskyrą (ir (arba) vieną *SlideShare* paskyrą (jei taikoma), kuri turi būti tikrasis vardas;

- neturi apribojimų naudotis *LinkedIn* paslaugomis. Paskyros sukūrimas pateikiant klaidingą informaciją yra sąlygų pažeidimas.

Nariai yra paskyros savininkai. Patvirtina kad: pasirinks stiprų ir saugų slaptažodį; saugos slaptažodį ir laikysis konfidencialumo, bei laikysis įstatymų ir profesinės bendruomenės politikos taisyklių. Vartotojas atsakingas už viską, kas vyksta paskyroje, nebent ją uždaro arba praneša apie piktnaudžiavimą.

Perkant bet kurią iš mokamų paslaugų sutinkama mokėti *LinkedIn* taikomus mokesčius ir mokesčius bei papildomas sąlygas, susijusias su mokamomis paslaugomis. Nesumokėjus šių mokesčių, mokamos paslaugos nutraukiamos. Vartotojas taip pat sutinka, kad pirkimui gali būti taikomi užsienio valiutos mokesčiai arba kainų skirtumai. Tinklas gali saugoti ir tęsti mokėjimo metodo atsiskaitymą net ir pasibaigus jo galiojimo laikui. Visi paslaugų pirkimai priklauso nuo *LinkedIn* grąžinimo politikos.

Vartotojas sutinka, kad informacija bus pateikiama šiais būdais: paslaugoje arba išsiųsta pagal pateiktą kontaktinę informaciją. Vartotojas įsipareigoja, kad kontaktinė informacija visada bus atnaujinta.

Tinklo paslaugos leidžia įvairiais būdais keistis informacija ir pranešimais. Informacija ir turinys, kurį vartotojas bendrina ir / arba skelbia, gali matyti kiti nariai, lankytojai. Tinklas „gerbs“ vartotojo privatumo pasirinkimus, kas gali matyti turinį ar informaciją. *LinkedIn* neįsipareigoja skelbti kokios nors informacijos ar turinio paslaugoje ir gali ją pašalinti savo nuožiūra su įspėjimu ar be jo.

Teisės ir apribojimai. Vartotojui priklauso turinys ir informacija, kurią jis pateikia ar skelbia tinkle ir suteikia *LinkedIn* ir tinklo filialams neišimtinę licenciją. Visame pasaulyje, perleidžiama ir sublicencijuojama teisė naudoti, kopijuoti, modifikuoti, platinti, skelbti ir apdoroti informaciją bei turinį, kurį vartotojas teikia per socialinio tinklo ir kitų tarnybų paslaugas be jokio kito sutikimo, pranešimo ir (arba) kompensacijos vartotojui ar kitiems. Teisės ribojamos šiais būdais: galima nutraukti licenciją konkrečiam turiniui, ištrynus turinį arba apskritai uždarius paskyrą. Vartotojo turinys nebus pridėtas prie turinio trečiųjų šalių produktų ir paslaugų reklamoje be vartotojo sutikimo. Tačiau tinklas turi teisę be vartotojo pateikti skelbimus šalia savo turinio ir informacijos, o vartotojo socialiniai veiksmai gali būti matomi ir įtraukti į skelbimus, kaip nurodyta privatumo politikoje. Tinklas gaus vartotojo sutikimą, jei norės suteikti kitiems teisę skelbti turinį už paslaugų ribų. Įrašui esant „viešam“ veiks įgalinta funkcija, leidžianti kitiems nariams įterpti tokį viešąjį įrašą į trečiųjų šalių paslaugas, ir turinys bus pasiekiamas paieškos varikliams.

LinkedIn gali redaguoti turinį (pvz., verčiant į kitą kalbą, dėl dydžio, išdėstymo ir pan), nekeičiant turinio išraiškos reikšmės. Vartotojas sutinka, kad SNS gali pasiekti, saugoti, apdoroti ir naudoti bet kokią pateiktą informaciją ir asmeninius duomenis pagal privatumo politikos sąlygas ir vartotojo pasirinkimus (įskaitant nustatymus). Vartotojas pateikdamas pasiūlymus ar kitus atsiliepimus

apie paslaugas *LinkedIn*, sutinka, kad jie gali būti panaudoti ir/arba pasidalinti be jokios kompensacijos.

Vartotojas sutinka pateikti tik tokį turinį ar informaciją, kuri nepažeidžia jokių įstatymų ir teisių (įskaitant intelektinės nuosavybės teises). Taip pat patvirtina, kad profilio informacija bus teisinga. Pagal įstatymą gali būti reikalaujama, kad *LinkedIn* pašalintų tam tikrą informaciją ar turinį tam tikrose šalyse.

LinkedIn gali pakeisti ar nutraukti bet kurią paslaugą. *LinkedIn* nėra saugykla, todėl vartotojas sutinka, kad tinklas neturi jokio įsipareigojimo saugoti, išlaikyti ar pateikti turinio ar informacijos kopiją, išskyrus tuos atvejus, kai tai reikalaujama pagal galiojančius įstatymus ir kaip nurodyta privatumo politikoje.

Vartotojas sutinka, kad *LinkedIn* nėra atsakingas už kitų socialinio tinklo narių skelbiamą turinį ir jo pobūdį. Tai pat prisiima atsakomybę už naudojamas trečiųjų šalių programas, svetaines, kurios susietos su socialinio tinklo paslaugomis. Leidus trečiosios šalies programai ar svetainei patvirtinti autentiškumą arba prisijungti prie asmeninės *LinkedIn* paskyros, naudojama programa arba svetainė gali pasiekti *LinkedIn* informaciją, susijusią su vartotojo paskyra ar ryšiais.

Socialinis tinklas turi teisę apriboti, kaip prisijungti ir bendrauti su jo paslaugomis. Įsipareigoja informuoti vartotoją apie intelektinės nuosavybės teisės pažeidimus.

LinkedIn „Dos ir Don'ts". „Dos" – vartotojas sutinka, kad laikytis visų galiojančių įstatymų, įskaitant privatumo, intelektinės nuosavybės, kovos su šlamštu taisyklių, mokesčių įstatymų ir kitų reikalavimų. Pateiks tikslią informaciją apie save ir nuolat ją atnaujins, taip pat naudos tikrąjį vardą savo profilyje ir profesionaliai naudosis *LinkedIn* paslaugomis.

„Don'ts" – vartotojas sutinka, kad nekurs neteisingų tapatybių, nenaudos ir nesijungs prie kito vartotojo paskyros. Nekurs ir nenaudos, programų, įrenginių ar bet kokių kitų priemonių (įskaitant skaitytuvus, naršyklių įskiepius ir papildinius ar bet kurią kitą technologiją), kad pakenktų „Linkedin paslaugoms". Nebandys apgaulės būdu išvengti apsaugos funkcijų, nekopijuos, nenaudos, neatskleis ar/ir neplatins bet kokios informacijos tiesiogiai arba per trečiąsias šalis (pvz., paieškos sistemas) be *LinkedIn* sutikimo. Jei neturi sutikimo, neatskleis informacijos (pvz., kitų asmenų konfidencialią informaciją (įskaitant ir vartotojo darbdavį)). Nepažeis kitų intelektinės nuosavybės teisių, įskaitant autorines teises, patentus, prekių ženklus, komercines paslaptis ar kitas nuosavybės teises. Nesidalins turiniu, kuriame yra programinės įrangos virusų, kirminų ar kitų kenksmingų kodų. Nenaudos reversinės inžinerijos, dekompiliavimo, deišifravimo ar kitaip nebandys gauti *LinkedIn* ar bet kokios susijusios technologijos šaltinio pirminio kodo, kuris nėra atvirojo kodo. Neužsiims nuoma, paskola, prekyba, pardavimais ar kitaip nesieks gauti pajamų iš tinklo teikiamų paslaugų ar susijusių duomenų be *LinkedIn* sutikimo. Nenaudos *deep linking* bet kokiam kitam tikslui, išskyrus reklamuoti savo profilį arba paslaugų grupę, be socialinio tinklo sutikimo. Nebus naudojami automatiniai metodai,

pridėti ar atsisiųsti kontaktams, siųsti arba peradresuoti pranešimams. Nestebės paslaugų prieinamumo, našumo ar funkcionalumo bet kokiam konkurenciniam tikslui.

Tinklas gali keisti sąlygas. Vartotojas sutinka, kad vienintelis būdas pateikti teisinį pranešimą yra užpildyti internetinę formą arba siųsti laišką nurodytu adresu. Kiek leidžia įstatymų normos, paslaugų sutarties versija anglų kalba yra privaloma, o kiti vertimai - tik patogumui.

Privatumo taisyklės

LinkedIn.com privatumo politika taikoma, *LinkedIn* autorinėms programoms, *Slideshare*, *LinkedIn* mokymuisi ir kitoms su *LinkedIn* susijusiomis svetainėmis, programomis, ryšiais ir paslaugomis. Pavyzdžiui skelbimų paslaugomis ir/ar „Taikyti su LinkedIn“ (angl. *Apply with LinkedIn*) ir „Dalintis su LinkedIn“ (angl. *Share with LinkedIn*) papildiniais. Socialinis tinklas *LinkedIn* gali keisti privatumo politiką ir po pakeitimų, tinklas informuos pranešimu per savo paslaugas arba kitomis priemonėmis. Jei vartotojas prieštarauja bet kokiems pakeitimams, tiesiog gali uždaryti savo paskyrą. Po privatumo politikos pakeitimų, toliau naudodamasis tinklo paslaugomis, vartotojas išreiškia savo sutikimą dėl pakeitimų atnaujintoje privatumo politikoje ir jo asmens duomenų rinkimo, naudojimo ir dalijimo.

Duomenys, kurie renkami.

Vartotojo teikiama informacija. Registracijos metu reikia patiekti tokius duomenis kaip, vardą, pavardę, el. pašto adresą ir /arba mobiliojo telefono numerį bei slaptažodį. Jei užsakoma aukščiausios kokybės paslauga (angl. Premium), reikia pateikti mokėjimo (pvz., kredito kortelės numeris) ir atsiskaitymo informaciją.

Paskyra. Paskyroje savo nuožiūra galima patiekti informaciją apie išsilavinimą, darbo patirtį, įgūdžius, nuotrauką, miestą ar vietovę ir patvirtinimus. Tinklo nariai gali užpildyti atskirą „ProFinder“ profilį. Vartotojas neprivalo pateikti papildomos informacijos apie save, tačiau patiekta profilio informacija padeda patogiau ir efektyviau naudotis tinklo funkcionalumais. Vartotojas pats sprendžia ar įtraukti jautrią informaciją į savo profilį ir viešai ją skelbti.

Skelbimas ir duomenų atnaujinimas. *LinkedIn* renka asmens duomenis, kuriuos pateikia vartotojas, skelbdamas arba įkeldamas tam tikrą turinį naudojantis tinklo paslaugomis. Pvz., užpildžius formą (naudojami demografiniai duomenys ar informacija apie atlyginimą). Sinchronizavus kontaktus ar kalendorių, SNS renka visą kontaktinę informaciją bei susitikimų istoriją ir planus.

Informacija iš kitų šaltinių. Vartotojas ar kiti tinklo nariai gali skelbti turinį, kuriame yra informacijos apie vartotoją (pvz.: straipsniai, įrašai, komentarai, vaizdo įrašų dalis). Tinklas kaupia asmeninius duomenis (įskaitant kontaktinę informaciją) apie tai, kai kiti nariai importuoja ar sinchronizuoja savo kontaktus ar kalendorių, susieja savo kontaktus su nario profiliais arba siunčia

pranešimus naudodamiesi *LinkedIn* paslaugomis (įskaitant kvietimus ar prisijungimo užklausas). Klientai ir partneriai gali pateikti duomenis. SNS gauna asmeninius duomenis, kai naudojamos klientų ir partnerių paslaugas. Taip pat duomenys gaunami kai vartotojas naudoja kai kurias kitas *LinkedIn* ar jo filialų, įskaitant *Microsoft*, teikiamas paslaugas.

Registruojami duomenys, kai lankomasi tinkle, įskaitant svetaines, programų ir platformų technologijas, atliekama paieška, įdiegiama arba atnaujinama kuri nors iš mobiliųjų programų, bendrinami straipsniai ar pateikiamos paraiškos dėl darbo. Naudojami slapukai, įrenginio informacija ir interneto protokolas (IP) adresai. Vartotojas gali valdyti slapukus per naršyklės nustatymus ir kitus įrankius, taip pat gali atsisakyti jų ir kitų technologijas, stebinčių vartotojų elgesį trečiųjų šalių reklamai.

Po vartotojo apsilankymo, *LinkedIn* išsaugo URL adresus iš kurių buvo nukreipta į šį socialinį tinklą. Taip pat gaunamas IP adresas, proxy serveris, operacinės sistemos, naršyklės ir priedų informacija, įrenginio identifikatorius ir funkcijos bei interneto paslaugų teikėjo arba mobiliojo ryšio operatoriaus informacija. Jei paslaugomis naudojamasi iš mobiliojo prietaiso, įrenginys siunčia duomenis apie vartotojo buvimo vietą pagal telefono nustatymus.

Renkama informacija apie vartotoją kai siunčiami ar gaunami pranešimais. Pavyzdžiui, gavus *LinkedIn* ryšio užklausą, stebimas, vartotojo elgesys, jei su gautu ryšiu nevykdomi jokie veiksmai, siunčiami priminimai. Taip pat renkami duomenys kai nariai (pvz.: darbdavys) perka mokamas paslaugas ir pateikia kito vartotojo (darbuotojo) asmeninius duomenis. Tinklas gauna duomenis, kai vartotojas apsilanko svetainėse, kuriose yra *LinkedIn* papildiniai, skelbimai arba slapukai, kai prisijungia prie kitų paslaugų savo *LinkedIn* paskyroje.

Kaip naudojama turima informacija.

Asmeninių duomenų naudojimas priklauso nuo vartotojo pasirinktų paslaugų ir kokie nustatymai yra asmeniniame profilyje. Tinklas naudoja turimus duomenis, kad galėtų pateikti ir individualizuoti turinį vartotojui, taip pat naudoja automatines sistemas duomenų analizavimui, savo paslaugų pritaikymui.

Naudojami tokie vartotojo duomenys kaip profilio informacija, peržiūrėtos kitų tinklo narių paskyros, duomenys pateikti atnaujinat adresatus. Tinklo teigimu tai reikalinga kad vartotojai galėtų rasti norimą profilį. Taip pat tam, kad būtų galima naudotis teikiamu funkcionalumu *near* – pasiūlyti kitiems tinklo nariams esantiems netoliese susisiekti, apskaičiuoti kelionės į darbą naują laiką arba pranešti apie savo ryšius, su kuriais vartotojas gali būti tame pačiame profesiniame renginyje. Visa tai yra vartotojo pasirinkimas: pakviesti, siųsti „ryšio“ užklausą ar leisti kitam nariui tapti „draugu“. Kai siunčiamas kvietimas, tinklas naudoja kvietime esančią informaciją: vardą, nuotrauką, kontaktinę informaciją. *LinkedIn* įsimina kvietimą ir po kurio laiko, pakartoja pakvietimo priminimus asmeniui, kuris buvo kviestas. Tinklas naudoja turimus duomenis apie vartotoją, kurias paslaugas jis renkasi, ką dalinasi ir seka. Taip gali naudoti automatines sistemas profiliui ir jo turinio analizei.

„Premium“ klientų aptarnavimo tarnyba gali saugoti arba saugo informaciją apie vartotoją, įskaitant papildomą informaciją, kontaktinę ar pardavimų istoriją. Kitų įmonių paslaugos ir funkcijos, kuriomis naudojami vartotojo duomenys, apima *TeamLink* ir *Elevate* (socialinio turinio reklama).
Tinklas bendravimui su nariais naudoja ir renka kontaktinę informaciją: el. paštas, mobilaus telefono numeris, tinklalapiuose ar programose paskelbtais pranešimais į vartotojo *LinkedIn* profilį. SNS gali siųsti informaciją apie paslaugų, saugumo ar kitų su paslaugomis susijusių problemų pasiekiamumą įvairiais būdais per savo paslaugas, įskaitant tekstinius pranešimus ir iššokančius pranešimus (angl. *push notifications*). Taip pat žinutes apie tai, kaip naudotis paslaugomis, tinklo naujinimais, priminimais, darbo pasiūlymais. *LinkedIn* įgalina bendravimą tarp socialinio tinklo narių per paslaugas, įskaitant, pavyzdžiui, kvietimus, *InMail* grupes ir pranešimus tarp ryšių.

Vartotojams teikiami pritaikyti skelbimai. SNS siūlo pasirinkti individualizuotus skelbimus, bet vartotojas negali atsisakyti kitų skelbimų. *LinkedIn* taiko ir vertina skelbimų našumą nariams, lankytojams ir savo paslaugoms, tiesiogiai ar per įvairius partnerius, naudodamas tokius duomenis, atskirai arba kartu: duomenis iš reklamavimo technologijų naudodamas švyturius (angl. *web beacons*), skelbimų žymas, slapukus, įrenginių identifikatorius, narių pateiktą informaciją apie save ir duomenis apie jų naudojimąsi paslaugomis (pvz. tokius kaip paieškos istorija, skaitomas turinys, dalyvavimas grupėse, puslapių apsilankymai, žiūrėti vaizdo įrašai, paspaudimai ant skelbimo ir t.t.). Taip pat naudoja informaciją gautą iš reklamos partnerių ir leidėjų.

Renkami duomenys naudojami paslaugų vystymui, kaip viešieji atsiliepimai, asmeniniai duomenys apie darbą, amžių, stažą, lytį, kvalifikaciją, vietovę ir pan. Kai kuriais atvejais kai dirbama su trečiosiomis šalimis ir gali skelbti arba leisti kitiems skelbti ekonomines įžvalgas, sukauptą informaciją pateikiant kaip suvestinius duomenis. Tinkas atlieka apklausas ir renka informaciją iš vartotojų sukurtų ir vykdomų apklausų. Naudoja vartotojų duomenis, kad galėtų kurti savo narių, jų profesijų ar pramonės statistinius duomenis, apskaičiuoti skelbtų parodymų, paspaudimų ar skelbimų lankytojų demografinius rodiklius. Renka ir naudoja duomenis (įskaitant bendravimą) saugumo tikslais, jei mano kad tai būtina, arba reikia ištirti galimą sukčiavimą ar privatumo politikos pažeidimus ir/ar bandymus pakenkti *LinkedIn* nariams ar lankytojams.

Kaip skelbiama/dalinamasi informacija.

Visi duomenys, kuriuos socialinio tinklo narys įtraukia į savo profilį ir bet koks jo paskelbtas turinys (pvz., „patinka“, komentarai, pasidalinimai) matomas kitiems tinklo vartotojams. Socialinio tinklo nario profilis yra pilnai matomas visiems paslaugos nariams ir klientams. Atsižvelgiant į nustatymus, jis taip pat gali būti matomas kitoms su *LinkedIn* susijusioms paslaugoms ar trečiųjų šalių paieškos sistemų naudotojams. Kaip aprašyta SNS pagalbos centre, profilio prieinamumą galima tvarkyti vartotojo nustatymuose.

LinkedIn paslaugos leidžia žiūrėti ir dalintis informacija, įskaitant pranešimus, mėgstamus puslapius, sekti ir komentuoti. Kai bendrinamas straipsnis ar įrašas, jį gali peržiūrėti visi, ir atsižvelgiant į nustatymus, su kuo norima bendrinti skelbiamą informaciją. Nariai, lankytojai ir kiti gali rasti ir pamatyti vartotojo viešai pasidalintą turinį, įskaitant vardą (ir nuotrauką, jei įkelta į profilį). Narystė grupėje yra vieša profilio dalis, įrašai matomi kitiems grupės nariams, bet galima keisti matomumą nustatymuose. Bet kokia informacija, kurią pasidalinta naudojantis įmonių ar kitų organizacijų puslapiais, bus matoma ir kitiems tinklo nariams. Taip pat matoma informacija koks asmuo ar organizacija yra sekama (angl. *follow*). Priklausomai nuo nustatymų, nariui leidžiama žinoti, kai peržiūrimas jo profilis. Informacija, kurią vartotojas pakomentuoja, pasidalina (angl. *re-share*) ar pažymi kaip patikusią (angl. *like*), taip yra vieša. Kai naudojamos papildomos paslaugos tokios kaip pvz.: *Recruiter, Sales Navigator, LinkedIn Learning* arba reklaminės kampanijos tvarkyklės, darbdavys gali (priklausomai nuo paslaugos) peržiūrėti ir valdyti vartotojo, kuriam suteikė tokią paslaugą, duomenis susijusius šiuo funkcionalumu. Priklausomai nuo įmonės paslaugų, prieš naudojantis kuria nors paslauga, paprašoma leidimo bendrinti svarbius duomenis iš vartotojo profilio arba naudoti tinklo nekomercines paslaugas. Tam tikros veiklos rūšys, pvz., darbo paieška ir asmeniniai pranešimai, yra jautrūs, todėl tinklas tokių duomenų neviešina savo darbdaviu, nebent vartotojas nusprendžia šia informacija pasidalyti per tinklo paslaugas.

Atsižvelgiant į privatumo nustatymus, kitos paslaugos gali ieškoti vartotojo profilio. Jei yra pasirinkta susieti paskyrą su kitomis paslaugomis, asmeniniai duomenys bus prieinami ir toms paslaugoms. Pavyzdžiui, galima susieti paskyrą su *Twitter* ar *WeChat* paskyromis, kad būtų galimybė dalintis turiniu iš *LinkedIn* arba el. pašto paslaugų teikėjas gali suteikti galimybę atsisiųsti kontaktus į *LinkedIn*. Tinklas dalinasi vartotojo duomenimis su skirtingų paslaugų tiekėjais, kad galėtų teikti paslaugas tokią kaip techninę priežiūrą, analizę, auditą, mokėjimus, sukčiavimo aptikimą, rinkodarą ir plėtrą. Tiekėjai turės prieigą prie vartotojo informacijos, jei pagrįstai bus reikalinga užduotims atlikti *LinkedIn* vardu, ir yra įpareigoti neatskleisti ar naudoti vartotojo duomenis kitais tikslais.

Teisiniai atskleidimai. Gali tekti dalintis vartotojo duomenimis, kai manoma, kad to reikalauja įstatymai. Taip pat gali pasidalinti duomenimis, kai verslas parduodamas kitiems, tačiau ir toliau turi būti naudojamas pagal privatumo politiką pasirašytą su vartotoju.

Vartotojo pasirinkimai ir įsipareigojimai.

Asmeniniai duomenys saugomi tiek, kiek vartotojo paskyra egzistuoja arba reikalinga. Tai apima vartotojo ar kitų pateiktus duomenis ir duomenis, sukurtus ar sugeneruotus iš naudojamų *LinkedIn* paslaugų. Net jei *LinkedIn* naudojamas tik darbo paieškom kas kelerius metus, informacija bus išsaugota ir vartotojas galės atsidaryti profilį, kol nuspręs uždaryti savo paskyrą. Kai kuriais atvejais gali būti nuspręsta išsaugoti tam tikrą informaciją depersonalizuota ar apibendrinta forma (pvz.: apsilankymai svetainėse, kuriose naudoti papildiniai „dalintis su LinkedIn“ ar „taikomi su LinkedIn“).

Teisės gauti ir tvarkyti asmeninius duomenis. Yra platus pasirinkimas kaip rinkti, naudoti ir bendrinti, ištrinti arba taisyti duomenis, kurie įtraukti į profilį. Kaip kontroliuoti pranešimų matomumą, reklamos atsisakymus, valdyti bendravimo nustatymus. Paskirtose šalyse gyvenantys asmenys gali turėti papildomų teisių pagal savo gyvenamosios vietos įstatymus.

Tinkas įsipareigoja, kad vartotojas savo asmens duomenis:

- gali paprašyti ištrinti ar ištrinti pats visus ar kai kuriuos asmeninius duomenis;
- redaguoti kai kuriuos savo asmeninius duomenis per paskyrą. Taip pat gali paprašyti tinklo pakeisti, atnaujinti ar taisyti duomenis tam tikrais atvejais, ypač jei jis yra netikslus;
- gali paprašyti, kad *LinkedIn* nebegalėtų naudoti visų ar kai kurių asmeninių duomenų arba apriboti jų naudojimą:
- gali paprašyti pateikti savo asmens duomenų kopiją.

Paskyros uždarymas. Net ir uždarius paskyrą, kai kurie duomenys bus išsaugoti. Jei vartotojas nuspręs uždaryti savo *LinkedIn* paskyrą, jo asmeniniai duomenys nebebus matomi kitiems tinklo paslaugose per 24 valandas. Uždarytos paskyros informacija ištrinama per 30 dienų nuo sąskaitos uždarymo.

Tinklas išsaugo asmeninius duomenis ir po paskyros uždarymo, jei pagrįstai manoma, kad būtina laikytis teisinių įsipareigojimų (įskaitant teisėsaugos prašymus), norminių reikalavimų, ginčų sprendimui, išlaikyti saugumą, užkirsti kelią sukčiavimui ir piktnaudžiavimui, įgyvendinant naudotojo sutartį. Informacija, kuri buvo bendrinta su kitais liks viešai matoma ir uždarius paskyrą ar ištrynus informaciją iš savo profilio ar pašto dėžutės. *LinkedIn* nekontroliuoja duomenų, kuriuos kiti nariai galėjo pasidalinti per savo paskyras ar išsisaugoti kokiu nors būdu (pvz *screen shot*). Grupių turinys ir reitingai arba apžvalgos turinys, susijęs su uždaromis paskyromis, šaltinį rodys kaip nežinomą naudotoją. Vartotojo profilis gali būti rodomas kitų paslaugų (pvz., paieškos rezultatų) paslaugose, kol jie atnaujins duomenų saugyklą.

Kita svarbi informacija.

LinkedIn stebi ir bando užkirsti kelią saugumo pažeidimams. Įgyvendintos apsaugos priemones, skirtas apsaugoti duomenis, pvz., HTTPS. Reguliariai stebimos sistemas dėl galimų pažeidimų ir išpuolių tačiau negarantuoja turimos informacijos saugumo. Nesuteikia jokios garantijos, kad negalima pasiekti, atskleisti, keisti ar sunaikinti duomenų, pažeidus bet kurią iš fizinių, techninių ar valdymo priemonių garantijų. Rekomenduoja domėtis saugiu paslaugų naudojimųsi, įskaitant dviejų veiksnių autentifikavimą. Turi teisėtus pagrindus surinkti, naudoti ir keistis duomenis apie vartotoją. Vartotojas gali kuriuo metu atsiimti sutikimą, kurį pateikė.

LinekdIn renka ir apdoroja vartotojo asmeninius duomenis, kuriuos gauna teisėtais pagrindais. Teisėti pagrindai – sutikimas kurį vartotojas duoda pradėdamas naudotis socialinio tinklo paslaugomis.

Apibendrinant galima teigti kad, skirtingai nuo *Facebook* ar *Twitter* šio tinko vartotojus vienija profesiniai ryšiai, todėl ir bendravimo kultūra, ir turinys yra visiškai kitoks. *LinkedIn* turi pakankamai platų funkcionalumą leidžianti socialinio tinklo vartotojams patiems pasirinkti privatumo ir saugumo nustatymus. Jei tinklas turi prieigą prie vartotojo adresų knygos ar telefono sąrašo, nepaisydamas nustatymų siunčia kvietimus draugauti visiems sąrašuose esantiems asmenims. Tai gerokai paspartina kontaktų rato augimą, nes sistema atranda visus asmenis, su kuriais kada nors bendrauta. Tačiau išlieka rizika, kad kvietimus gaus ir tie asmenys, su kuriais vartotojas profesine veikla nėra susijęs. Be to, *LinkedIn* siunčia laiškus ne tik tinkle užsiregistravusiems nariams.

LinkedIn kiekvienam privatumo taisyklių ir naudojimosi sąlygų punkte nuolat primena, kad vartotojas gali bet kada gali keisti savo nustatymus. Tuo pačiu šalia visada mini, kad jei neturės naujausių duomenų, negalės vartotojui pateikti naujausių paslaugų ir vartotojas apribos savo galimybes augti ir bendradarbiauti jų teikiamose paslaugose.

2 Lentelė. **Socialinio tinklo *LinkedIn* naudojimosi ir privatumo taisyklių santrauka**

Pirminė reikalinga informacija registruojantis	Elektroninio pašto adresas, vardas, pavardė.
Naudojimosi amžius	16 metų
Skelbiamų žinučių dydis	1750 simbolių
Privatumo nustatymai	Taip
Galimybė blokuoti nepageidaujamus asmenis	Taip
Draudimas žymėti skelbiamame turinyje / nuotraukose	Taip / Ne
Galimybė pasirinkti kas gali susisiekti per SNS	Taip
Vietos nustatymas	Taip
Dviejų veiksmų autentifikacija	Taip
Pasirinktų saitažodžių (angl. *hashtags*) blokavimas	Ne
Galimybė matyti sekėjus	Taip

2.3. *Facebook* atvejo analizė

Facebook didžiausias socialinis tinklas pasaulyje. Sukurtas 2004m. Pradžioje buvo skirtas tik Harvardo universiteto studentams. Vėliau – visų JAV universitetų studentams, dar vėliau – įmonių darbuotojams, organizacijų nariams, 2006 m. rugsėjo mėnesį – užsienio studentams. 2008 m. pavasarį platforma išversta į vokiečių, ispanų, prancūzų kalbas. Šiuo metu šis tinklas prieinamas visiems asmenims virš 13 metų amžiaus, o kai kuriose šalyse socialinis tinklas *Facebook* yra uždraustas.

Užsiregistravę nariai gali patalpinti savo profilį (asmens aprašą), įkelti nuotraukų, paveikslėlių, vaizdo įrašų bei užmegzti ryšius su draugais, pažįstamais asmenimis ir kt. Internetinėje bendruomenėje

gali būti kuriami virtualūs nuotraukų albumai, renginiai (angl. *events*), apklausos (angl. *pool*), vidinės grupės (pagal interesus, pomėgius ir kt. kriterijus), keičiamasi žinutėmis, failais tarp grupės narių ir bendraujama kitomis formomis. Tinklas turi daug susietų programų iš kurių *Instagram, Facebook Messenger, WhatsApp* savo populiarumu nenusileidžia *Facebook.*

Norint šiame socialiniame tinkle susikurti paskyrą, registruojantis prašo tokių duomenų kaip: vardas, pavardė, el. pašto adresas arba telefono numeris, gimimo data ir lytis.

Statistikos portalo *Statista* 2018 m. antro ketvirčio duomenimis *Facebook* turėjo 2234 milijonus registruotų vartotojų. *Kantar TNS* rinkos tyrimų bendrovės 2017 m. duomenimis Lietuvoje iš 79 % besinaudojančių socialiniais tinklais šalies gyventojų 97,4 % naudojasi *Facebook* socialinio tinklu.

Paslaugų teikimo sąlygos

Šios sąlygos apibrėžia, kaip galima naudoti *Facebook*, siūlomus produktus, funkcijas, programas, paslaugas, technologijas ir programinę įrangą, išskyrus tuos atvejus, kai aiškiai nurodyta, kad taikomos atskiros sąlygos .

***Facebook* paslaugos.** *Facebook* turinys yra unikalus pradedant įrašais, istorijomis, renginiais, reklamomis ir kitu turiniu, kuris matomas naujienų sklaidos kanale, vaizdo įrašų platformose, ar puslapiuose, kuriuos vartotojas stebi. Naudojant turimus duomenis, *Facebook* vartotojams teikia pasiūlymus. Vartotojai tinkle bendrauti, bendrinti būsenos naujinimus, nuotraukas, vaizdo įrašus ir istorijas, siųsti pranešimus vienam ar keliems tinklo nariams, kurti renginius, grupes ar kitaip į profilį kelti norimą turinį. *Facebook* teigimu, jie nuolat atnaujina ir diegia naujoviškas technines sistemas, netinkamo produktų naudojimo atvejams, nederamo elgesio su kitais žmonėmis ir situacijos aptikti. Tai pat naudojamas ir kuriamas dirbtinis intelektas, mašininio mokymosi sistemos ir papildytoji realybė, skirtos vienokią ar kitokią negalią ar sutrikimus turintiems asmenis suprasti, kas yra nuotraukose ar vaizdo įrašuose, bendrintuose sistemoje *Facebook* ar *Instagram*. Tinklas taip naudoja duomenis apie žmones, su kuriais vartotojai bendrauja sistemoje *Facebook, Instagram* ar *Messenger*.

Visas platinamas turinys ir duomenys yra saugomi duomenų centruose ir sistemose visame pasaulyje, įskaitant užsienio šalis. Šią infrastruktūrą gali valdyti arba kontroliuoti *Facebook, Inc., Facebook Ireland Limited* ar jų padaliniai.

Duomenų politika ir vartotojo privatumo pasirinkimai. Renkami ir naudojami asmens duomenys, paslaugoms teikti. Kaip renkama ir naudojama aprašo duomenų politika. Paskyros nustatymuose galima peržiūrėti esančius privatumo pasirinkimus, kaip naudojami duomenys.

Vartotojo įsipareigojimai. Socialinis tinklas argumentuodamas saugumo ir privatumo nustatymais reikalauja vartotojų laikytis taisyklių:

- Naudoti tuos pačius vardą ir pavardę, kuriuos naudojate kasdieniame gyvenime.
- Pateikti tikslią informaciją apie save.
- Sukurti tik vieną paskyrą (savo) ir laiko juostą / sieną naudoti asmeniniais tikslais.
- Neatskleisti savo slaptažodžio, nesuteikti kitiems žmonėms prieigos prie savo *Facebook* paskyros ir neperduoti jiems savo paskyros (be atskiro tinklo leidimo).

Facebook negali naudoti vartotojai kurie: jaunesni nei 13 metų amžiaus; teisti už seksualinius nusikaltimus; anksčiau buvo išjungtos jų paskyros dėl tinklo sąlygų ar politikos pažeidimų; pagal taikomus įstatymus uždrausta gauti tinklo produktus, paslaugas ar programinę įrangą.

Taip pat vartotojas sutinka, kad nesielgs, kaip nurodyta paslaugų teikimo sutartyje ir taip pat nepadės kitiems asmenims taip elgtis bei nepalaikys tokio elgesio.

- Nenaudos produktų ar nebendrins turinio, jei tai pažeidžia naudojimosi tinklu sąlygas, tinklo bendruomenės standartus ir kitas sąlygas bei politiką, taikomą naudojantis *Facebook.* Jei turinys yra neteisėtas, klaidingas, diskriminacinio pobūdžio, apgaulingas ar pažeidžia kitų asmenų teises.
- Negali kelti virusų ar kenkėjiškų kodų arba bet kaip kitaip elgtis siekiant sugadinti, apsunkinti ar pakenkti *Facebook* produktų veikimui ar išvaizdai.
- Naudodamasis automatinėmis priemonėmis negali pasiekti ar rinkti duomenų iš tinklo produktų (be išankstinio leidimo) ar bandyti pasiekti duomenis, kurių pasiekti neturi leidimo.

Pažeidus šias nuostatas socialinis tinklas gali pašalinti bendrinamą turinį ir, jei taikytina, gali imtis veiksmų su paskyra. Taip pat gali išjungti paskyrą, jei pakartotinai bus pažeistos kitų asmenų intelektinės nuosavybės teises. Užfiksavus tokį turinį ar elgesį, imamasi veiksmų, pvz.: susisiekiama su teisėsaugos pareigūnais.

Facebook prašo tokių leidimų:

- Leidimas naudoti vartotojo sukurtą ir bendrintą turinį. Turinys, kuris kuriamas ir bendrinamas *Facebook* nepanaikina vartotojo teisių į turinį. Galima bendrinti asmenį turinį kaip nori. Tačiau tinklui reikia vartotojo teisinio leidimo naudoti šį turinį – suteikti neišimtinę, perleidžiamą, sublicencijuojamą, nemokamą geografiškai neapribotą licenciją nuomoti, naudoti, platinti, keisti, tvarkyti, kopijuoti, viešai atlikti ar rodyti, versti ir kurti antrinius kūrinius iš vartotojo. Nutraukti šią licenciją galima bet kuriuo metu, ištrinant turinį ar visą paskyrą. Dėl techninių priežasčių ištrintas turinys tam tikrą ribotą laikotarpį gali likti atsarginėse kopijose (tačiau jis nebus matomas kitiems naudotojams). Bet ištrintas turinys gali būti toliau rodomas, jei buvo bendrintas su kitais asmenimis ir jie jo neištrynė.
- Leidimas naudoti vardą, pavardę, profilio nuotrauką ir informaciją apie veiksmus, susijusius su reklamomis ir remiamu turiniu. Vartotojas nemokamai suteikia leidimą naudoti vardą, pavardę, profilio nuotrauką ir informaciją apie veiksmus sistemoje *Facebook*, atliekamus greta arba

susijusius su reklamomis, pasiūlymais ir kitu remiamu turiniu, kuris rodomas *Facebook* produktuose.

- Leidimas atnaujinti programinę įrangą, kurią vartotojas naudoja ar atsisiunčia. Suteikia leidimą programinei įrangai atsisiųsti ir įdiegti atnaujinimus, naujovinimus ir papildomas funkcijas, skirtas programinei įrangai tobulinti, plėsti ir toliau kurti.

Apribojimai naudoti intelektinę nuosavybę. Jei naudojamas turinys, kuriam taikomos intelektinės nuosavybės teisės, kuris priklauso *Facebook* ir kuriuo dalijamasi *Facebook* produktuose, socialinis tinklas pasilieka visas teises į šį turinį (bet ne vartotojo sukurtą turinį). Galima naudoti tinklo autorių teises ir prekių ženklus (arba panašius prekių ženklus) tik tada, kai tai aiškiai leidžiama pagal tinklo prekės ženklo naudojimo vadovą, arba gautas išankstinis raštiškas leidimas. Galima modifikuoti, kurti išvestinius kūrinius, dekompiliuoti ar kitaip bandyti gauti iš *Facebook* šaltinio kodą, tik jei gautas raštiškas leidimas (arba leidimą pagal atvirojo kodo licenciją).

Papildomos nuostatos. Sąlygų atnaujinimas. *Facebook* gali atnaujinti paslaugų teikimas sąlygas, kad jos tiksliai aprašytų paslaugas ir įprastą praktiką. Jei pagal įstatymus nereikalaujama kitaip, bent prieš 30 dienų pranešama vartotojui (el. paštu arba per *Facebook* produktus) apie sąlygų pakeitimus ir suteikiama galimybė peržiūrėti jas iki jų įsigaliojimo. Jei, įsigaliojus atnaujintoms sąlygoms, toliau naudojamasi produktais, pagal nutylėjimą sutinkama su taisyklių pakeitimais ir yra privaloma jų laikytis. Jei nesutinkama su atnaujintomis sąlygomis, bet kuriuo metu galima ištrinti paskyrą. Nustačius, kad šiurkščiai ar pakartotinai pažeistos sąlygas ar politika, tinklas gali sustabdyti ar visam laikui panaikinti prieigą prie paskyros. Taip pat gali sustabdyti ar visam laikui išjungti paskyrą pagal įstatymų reikalavimus.

Tinklas siekia, kad aplinka būtų saugi ir be klaidų, bet negali garantuoti, kad produktai visada veiks be sutrikimų, vėlavimų ar trūkumų. *Facebook* neprisiima atsakomybės už: nuostolius, nesusijusius su sąlygų pažeidimu ir kitais veiksmais; nuostolius, kurių nebuvo galima pagrįstai numatyti, sudarant šias sąlygas; bet kokį įžeidžiantį, nederamą, nepadorų, neteisėtą ar kitaip nepageidaujamą turinį, kuris buvo kitų paviešintas ir su kuriuo gali būti susidurta; įvykius, kurių neįmanoma kontroliuoti. Tačiau nuostatos nepanaikina ir neapriboja *Facebook* atsakomybės dėl mirties, asmens sužalojimo ar apgaulingai klaidingos informacijos atvejų, kurie galimi dėl socialinio tinklo aplaidumo. Nepanaikina ir neapriboja atsakomybės visais kitais atvejais, kai panaikinti ar riboti atsakomybę draudžia įstatymai.

Kilus ginčui, jei vartotojas yra nuolat gyvenantis Europos Sąjungos valstybėje narėje, tos valstybės narės teisė bus taikoma bet kokiam reikalavimui, ieškinio pagrindui ar ginčui SNS atžvilgiu, kuris kyla arba yra susijęs su šiomis sąlygomis arba *Facebook* produktais. Vartotojas gali kreiptis į bet kurį šalies kompetentingą teismą, kurio jurisdikcijai priklauso. Visais kitais atvejais sutinka, kad

ginčas turi būti sprendžiama kompetentingame Airijos Respublikos teisme ir kad šioms sąlygoms bei bet kokioms pretenzijoms taikoma Airijos teisė, neatsižvelgiant į teisės aktų nuostatų prieštaravimus.

Kita. Naudojimosi sąlygos sudaro visą vartotojo ir *Facebook Ireland Limited* sutartį dėl produktų naudojimo. Kai kuriems produktams taip pat taikomos papildomos sąlygos. Jei kuri nors iš šių sąlygų būtų pripažinta neįgyvendinama, likusi dalis lieka galioti visa. Negalima perduoti jokių savo teisių ar įsipareigojimų pagal šias sąlygas jokiems kitiems asmenims be tinklo sutikimo. Galima paskirti asmenį (palikimo kontaktiniu asmeniu), kuris galėtų valdyti paskyrą vartotojui mirus. Šiomis sąlygomis nesuteikiamos jokios teisės jokių trečiųjų asmenų naudai. Visas savo teises ir pareigas pagal šias sąlygas *Facebook* gali perleisti, kiek tai reikalinga įmonių sujungimo, įsigijimo ar turto pardavimo atvejais, įstatymo nustatyta tvarka ar kitaip. Tam tikromis aplinkybėmis tinklui gali tekti pakeisti vartotojo paskyros naudotojo vardą. *Facebook* gali naudoti atsiliepimus ar pasiūlymus be jokio apribojimo ar įsipareigojimo sumokėti, taip pat niekaip neįsipareigoja laikytis konfidencialumo.

Yra ir kitos sąlygos ir politikos nuostatos, kurios gali būti taikomos. Tai būtų: bendruomenės standartai, komercinės sąlygos, reklamavimo politika, savitarnos reklamų sąlygos, puslapių, grupių ir įvykių politika, *Facebook* platformos politika, kūrėjo mokėjimo sąlygos, bendruomenės mokėjimo sąlygos, komercinės nuostatos, *Facebook* prekių ženklų ištekliai, muzikos gairės

Privatumo taisyklės

Šiose taisyklėse aprašoma informacija ir kokios duomenų tvarkymo taisyklės taikomos *Facebook, Instagram, Messenger* ir kitiems *Facebook* teikiamiems produktams ir funkcijoms.

Kokio pobūdžio informacija renkama.

Vartotojo pateikta informacija ir turinys. Renkamas turinys, pranešimai ir kita informacija, kurią vartotojas teikia naudodamasis *Facebook* produktais, įskaitant informaciją, kurią pateikia registruodamas paskyrą, kurdamas, bendrindamas turinį ar/ ir susirašinėdamas bei bendraudamas su kitais. Tai gali būti ir informacija, esanti pateikto turinio viduje (metaduomenys) ar informacija apie šį turinį (pvz.. nuotraukos vieta ar failo sukūrimo data). Sistemos automatiškai tvarko visų vartotojų pateiktą turinį ir pranešimus.

Tinklai ir ryšiai. Renkami duomenys apie asmenis, puslapius, paskyras, grotažymes/saitažymes (angl. *hashtag*) ir grupes, prie kurių vartotojas prisijungęs. Bei informaciją apie tai, kaip sąveikaujama naudojant SNS produktus. Taip pat renkama kontaktinė informaciją, jei ji siunčiama, sinchronizuojama ar importuojama iš įrenginio kuriame yra naudojamas kuris nors iš *Facebook* produktų.

Vartotojo naudojimo įpročiai. Kaupiama informacija apie tai, kaip naudojami produktai (naudojamos funkcijas, paskyras su kuriom sąveikaujama, veiklos laiką, dažnumą ir trukmę).

Informacija apie operacijas atliktas naudojant *Facebook* produktus. Jei per tinklo produktus įsigyti pirkiniai ar atliekamos finansines operacijos (pirkimas, aukojimas), renkama informaciją apie pirkinį ar operaciją. Tai apima mokėjimo informaciją (kredito ar debeto kortelės numerį ir kitą kortelės informaciją; paskyros ir autentifikavimo informaciją; ir sąskaitų, pristatymo ir kontaktinius duomenis).

Kitų žmonių veikla ir jų pateikiama informacija apie vartotoją. Taip pat gaunamas ir analizuojamas turinys, pranešimai ir informacija, kurią pateikia kiti žmonės. Tai apima informaciją apie vartotoją, kai kiti asmenys bendrina ar komentuoja jo nuotraukas, žymi (angl. *tag*) vartotoją savo paskelbimuose, siunčia pranešimus, siunčia, sinchronizuoja ar importuoja kontaktinę informaciją.

Renkama įrenginio informacija. Iš kompiuterių, telefonų, prijungtų TV įrenginių ir kitų prie interneto prijungtų naudojamų įrenginių, kurie gali būti susieti su *Facebook* produktais, bei informacija apie šiuos įrenginius. Ši informacija sujungiama su vartotojo naudojamų skirtingų įrenginių informacija. Informacija, kuri gaunama iš įrenginių, sudaro tokie duomenys:

- įrenginio savybės: informacija apie operacinę sistemą, techninės ir programinės įrangos versijas, akumuliatoriaus lygį, signalo stiprumą, laisvą vietą saugykloje, naršyklės tipą, programų ir failų pavadinimus ir tipus bei papildinius;
- įrenginio operacijos: informacija apie operacijas ir veiksmus, atliekamus su įrenginiu. Pvz.: ar langas yra priekyje, ar fone, arba apie judesius pele;
- identifikatoriai: unikalūs identifikatoriai, įrenginio ID ir kiti identifikatoriai. Kaip ir identifikatoriai iš naudojamų žaidimų, programų ar paskyrų, ir šeimos įrenginio ID;
- įrenginio signalai: Bluetooth signalai ir informacija apie greta esančius Wi-Fi prieigos taškus, siųstuvus ir mobiliojo ryšio bokštus,
- duomenys iš įrenginio nustatymų: informacija, kurią vartotojas leidžiate gauti įjungdamas įrenginio nustatymus, kaip pavyzdžiui prieigą prie GPS, fotoaparato arba nuotraukų;
- tinklas ir ryšiai: informacija, iš mobiliojo ryšio operatoriaus arba interneto paslaugų teikėjo pavadinimas, kalba, laiko zona, mobiliojo telefono numeris, IP adresas, interneto sparta ir, kai kuriais atvejais, informacija apie kitus netoliese arba vartotojo tinkle esančius įrenginius;
- slapukų duomenys: iš įrenginyje išsaugotų slapukų, įskaitant slapukų ID ir nustatymus.

Informacija iš partnerių. Reklamuotojai, programėlių kūrėjai ir leidėjai gali siųsti informaciją per naudojamas *Facebook* technologijas, įskaitant socialinius papildinius (pvz.: mygtukas „Patinka“), *Facebook Login* ir kt. Partneriai teikia informaciją apie vartotojo veiklą už *Facebook* ribų, įskaitant informaciją apie įrenginį, lankomas interneto svetaines, įsigytus pirkinius, matomas reklamas bei informaciją apie tai, kaip naudojatės jų paslaugomis. Ši informacija teikiama nepaisant to ar vartotojas turi *Facebook* paskyrą ir ar yra prie jos prisijungęs. Taip pat gaunama informacija apie vartotojo

veiksmus internete ir prisijungimus bei pirkinius iš trečiųjų šalių duomenų teikėjų, kurie turi teisę pateikti informaciją *Facebook* apie vartotoją.

Kaip naudojama gauta informacija.

Visa informacija skirta teikti, asmeniškai pritaikyti ir pagerinti produktus, įskaitant asmeniškai pritaikytas funkcijas ir turinį. Tuo tikslu *Facebook* naudoja informaciją apie vartotojo ryšius, nuostatas, pomėgius ir veiklą. Tai pat renkama informacija ir apie kitus vartotojus (įskaitant duomenis, kuriems taikoma speciali apsauga). Sujungiama informacija apie visą vartotojo veiklą naudojant įvairius *Facebook* produktus ir įrenginius. Naudoja su vieta susijusi informacija, tokia kaip, duomenys apie dabartinę gyvenamąją vietą, vietas į kurias vykstama, bei netoliese esančias įmones ir asmenis. Su vieta susijusi informacija gali būti grindžiama tokiais duomenimis kaip tiksli įrenginio vieta, IP adresai. Naudojama veido atpažinimo technologija.

Tinklas turi ir kaupia informaciją (įskaitant duomenis apie veiklą ne *Facebook* produktuose), pavyzdžiui, lankomas interneto svetaines ir matomas reklamas. Apibendrinti duomenys teikiami reklamuotojams ir kitiems partneriams.

Kaip bendrinama informacija.

Kai bendrinama informacija, pasirenkama auditorija kuriai informacija bus skirta. Pavyzdžiui: grupė, visi draugai, visi asmenys arba pritaikytas žmonių sąrašas. Kiti vartotojai, priklausomai nuo privatumo nustatymų, gali matyti ar nematyti siunčiamą turinį.

Viešą informaciją gali matyti bet kurie asmenys, nepriklausomai ar yra registruoti socialinio tinklo narių ar neturėdami paskyros. Tai apima: naudotojo vardą, bei bet kokią informaciją, turinį kuris bendrintas su vieša auditorija, ir pasidalintas *Facebook* puslapyje, viešoje *Instagram* paskyroje ar bet kokiame kitame viešame forume. Viešą informaciją taip pat galima peržiūrėti, pasiekti, pakartotinai bendrinti arba atsisiųsti per trečiosios šalies paslaugas, pavyzdžiui, paieškos variklius, API ir prie interneto neprijungtas medijas.

Kitų žmonių bendrinamas ir pakartotinai bendrinamas turinys apie vartotoją. Kiti tinklo nariai, kurie mato vartotojai veiklą, gali ją bendrinti su kitais tinklo nariais, įskaitant asmenis ir įmones, nepriklausančias auditorijai, su kuria buvo bendrintas turinys. Kai komentuojamas kitų narių įrašas arba reaguojama (emocijų piktogramomis) į jų skelbiamą turinį, komentaras arba reakcija matomi visiems, galintiems stebėti šių žmonių turinį, ir šie žmonės vėliau gali pakeisti auditoriją. Tinklui priklausantys vartotojai gali matyti ženklus, nurodančius, ar vartotojas aktyvus, įskaitant ar šiuo metu prisijungęs prie *Instagram, Messenger* arba *Facebook,* ir kada paskutinį kartą buvo aktyvus.

Pasirinkus naudoti trečiosios šalies programėles, interneto svetaines ar kitas paslaugas, šios gali gauti informacijos apie vartotojo skelbiamą ar bendrinamą turinį. Be to, kai atsisiunčiamos arba naudojamos trečiosios šalies paslaugos, jos gali pasiekti viešą *Facebook* profilį ir visą su jomis bendrinamą informaciją. Pavyzdžiui gali gauti draugų sąrašą, jei vartotojas nuspręs jį bendrinti.

Trečiosios šalies paslaugų renkamai informacijai taikomos jų pačių sąlygos ir politika. Jei pasikeičia visų ar dalies produktų arba jų išteklių savininkas arba valdytojas, *Facebook* gali perduoti informaciją naujajam savininkui.

Bendrinimas su trečiosios šalies partneriais

Bendradarbiaujant su trečiosios šalies partneriais *Facebook* informacijos niekam neperduoda. Nustatyti apribojimai kaip partneriai gali naudoti ir atskleisti gautus duomenis. Trečiųjų šalių tipai:

- Partneriai, kurie naudojasi *Facebook* analizės paslaugomis. Jiems teikiami apibendrinti statistiniai duomenys ir įžvalgos.
- Reklamuotojai. Teikiamos ataskaitas apie tai, kokie vartotojai mato jų reklamas, ir apie šių reklamų veiksmingumą, tačiau be atskiro vartotojo leidimo nebendrinama jokia, tapatybę atskleidžianti, informacija.
- Vertinimo partneriai. Informacija apie vartotojus dalinamasi su bendrovėmis, kurios ją apibendrina ir teikia analizės bei vertinimo ataskaitas.
- Partneriai, produktuose siūlantys prekes ir paslaugas. Turinio kūrėjas arba pardavėjas gali gauti viešos informacijos ir kitos informacijos, kuri su jais bendrinta, taip pat informacijos, reikalingos operacijai atlikti, įskaitant pristatymo ir kontaktinius duomenis.
- Pardavėjai ir paslaugų teikėjai. Teikiama informacija ir turinys pardavėjams ir paslaugų teikėjams, teikiantiems techninės infrastruktūros paslaugas.
- Tyrėjai ir akademinės bendruomenės atstovai. Teikiama informacija ir turinys tyrimų partneriams ir akademinės bendruomenės atstovams.
- Teisėsaugos institucijos arba teisiniai prašymai. Bendrinama informacija su teisėsaugos institucijomis.

Kokiu teisiniu pagrindu tvarkomi duomenys.

Renka, naudoja ir bendrina turimus duomenis:

- kai būtina vykdyti *Facebook* paslaugų ir papildomų produktų sąlygas;
- su vartotojo sutikimu, kurį bet kada galima atšaukti privatumo ir saugumo nustatymuose;
- kai būtina laikytis teisinių prievolių;
- kai reikia apsaugoti gyvybinius vartotojo ir kitų interesus;
- kai būtina užtikrinti viešuosius interesus;
- kai būtina užtikrinti *Facebook* (arba kitų) teisėtus interesus, įskaitant paties tinklo interesą teikti naujoviškas, asmeniškai pritaikytas, saugias ir pelningas paslaugas vartotojams ir partneriams, išskyrus atvejus, kai už šiuos interesus yra viršesni vartotojo interesai arba pagrindinės teisės ir laisvės, dėl kurių reikia apsaugoti asmens duomenis.

Kaip vartotojas gali įgyvendinti BDAR suteiktas teises?

Pagal Bendrąjį duomenų apsaugos reglamentą turi teisę susipažinti su savo duomenimis, juos perkelti, reikalauti juos ištaisyti ir ištrinti. Taip pat turi teisę nesutikti su tam tikru duomenų tvarkymu ir jį apriboti. Tai apima:

- teisę nesutikti, kad duomenys būtų tvarkomi tiesioginės rinkodaros tikslais
- teisę nesutikti, kad duomenys būtų tvarkomi atliekant užduotis viešaisiais interesais ar siekiant teisėtų tinklo arba trečiosios šalies interesų.

Duomenų saugojimas, paskyros išaktyvinimas ir ištrynimas.

Duomenys saugomi tol, kol jie tampa nebereikalingi paslaugos teikimui arba iki tol, kol vartotojas pats ištrina paskyrą (priklausomai nuo to, kas įvyksta anksčiau). Duomenų reikalingumas nustatomas kiekvienu atveju atskirai ir priklauso nuo duomenų pobūdžio, kodėl jie renkami ir tvarkomi, bei atitinkamų teisinių ar veiklos sąlygų palaikymo poreikių. Pavyzdžiui, kai ko nors ieškota *Facebook,* tokią užklausą galima bet kada ištrinti iš paieškos istorijos, tačiau paieškos žurnalas bus ištrintas po 6 mėnesių. Jei paskyrai patikrinti buvo pateikta valstybės institucijų išduoto asmens dokumento kopija, ši kopija bus ištrinta praėjus 30 dienų nuo jos pateikimo.

Ištrynus paskyrą, bus ištrinta šioje paskyroje skelbta informacija ir jos nebebus galima atkurti. Informacija apie vartotoją, kurią bendrino kiti žmonės, nėra paskyros dalis ir ji nebus ištrinta. Jei nenorima ištrinti paskyros, paskyrą galima padaryti neaktyvią.

Apie vartotoją gautą informaciją (įskaitant finansinių operacijų duomenis, susijusius su *Facebook* įsigytais pirkiniais) galima pasiekti ir saugoti ilgesnį laikotarpį. Tai atvejais kai ši informacija yra teisinio prašymo ar pareigos, valdžios institucijų tyrimo ar tyrimų dėl galimo tinklo sąlygų ar politikos pažeidimų objektas, arba ji reikalinga kad būtų išvengta žalos kitais būdais. Taip pat mažiausiai metus saugoma paskyrų informacija, kurios buvo išjungtos dėl sąlygų pažeidimų.

Apibendrinant galima teigti kad, skirtingai nuo *LinkedIn* ar *Twitter, Facebook* tinklas bando „išlipti“ iš įprastos socialinio tinklo sąvokos apibrėžimo vis labiau didindamas savo teikiamų paslaugų ratą, pvz.: 360° vaizdo įrašai. Dabartinis funkcionalumas leidžia vartotojui susikurti asmeninį profilį išreiškiant save, ne tik trumpais pasisakymais ar darbine patirtim, bet plačiu aprašymu, galimybe smulkiai nurodyti savo pomėgius, užsiėmimus, vykdyti tiesiogines transliacijas. Daugėja atvejų, kai asmenys tinkle bando sukurti naujas, jų manymų geresnes, savo tapatybes. Bendravimo kultūra ir turinys yra visiškai kitokie nei prieš tai aptartuose socialiniuose tinkluose. *Facebook* turi labai platų funkcionalumą leidžianti socialinio tinklo vartotojams patiems pasirinkti privatumo ir saugumo nustatymus ir nuolat pats primena vartotojams saugoti savo duomenis ir įsitinkinti, kad tikrai pažįsta į draugus kviečiamus asmenis. *Facebook* plačiai ir išsamiai aprašo naudojimosi ir duomenų saugojimo, bei skelbimo taisykles. Tuo pačiu pabrėžia, kad pasilieka visas teises, kurios nėra aiškiai suteiktos vartotojui.

Registruojantis, šis socialinis tinklas prašo daugiausiai duomenų, o ir vėliau jau turint, paskyrą nuolat „primena“ kad reiktų patiekti daugiau informacijos apie paskyrą. Išvardintas platus ratas kam *Facebook* teikia informaciją ir turinį, tačiau paslaugų teikimo ir privatumo sąlygose nenurodoma kokie konkrečiai vartotojų duomenys yra perleidžiami trečiosioms šalims.

Duomenų politikoje kalbama apie galimybę ištrinti arba išaktyvinti, tačiau nenurodyti jokie terminai per kiek laiko tai bus atlikta. Net ir *Facebook* pagalbos centre, prie klausimo apie paskyros pašalinimą, nėra tiesioginio atsakymo. Kaip visam laikui ištrinti savo *Facebook* paskyrą? (angl. How do I permanently delete my Facebook account?) pateiktas atsakymas ne kaip ištrinti, o kas bus jei paskyra bus ištrinta visam laikui (angl. What happens if I permanently delete my Facebook account?).

3 Lentelė. **Socialinio tinklo *Facebook* naudojimosi ir privatumo taisyklių santrauka**

Pirminė reikalinga informacija registruojantis	Elektroninio pašto adresas, vardas, pavardė, gimimo data, lytis.
Naudojimosi amžius	13 metų
Skelbiamų žinučių dydis	8000 simbolių
Privatumo nustatymai	Taip
Galimybė blokuoti nepageidaujamus asmenis	Taip
Draudimas žymėti skelbiamame turinyje / nuotraukose	Taip /Taip
Galimybė pasirinkti kas gali susisiekti per SNS	Taip
Vietos nustatymas	Taip
Dviejų veiksmų autentifikacija	Taip
Pasirinktų saitažodžių (angl. *hashtags*) blokavimas	Ne
Galimybė matyti sekėjus	Taip

3. DUOMENŲ APSAUGOS VALDYMO YPATUMŲ INTERNETO SOCIALINIUOSE TINKLUOSE TYRIMAS

Šiame skyriuje pateikiami vartotojų požiūrio į duomenų apsaugą socialiniuose tinkluose tyrimo metodai, aprašyta tyrimo eiga ir aptarti gauti rezultatai. „Tyrimas yra kompleksinis, savo etapus turintis procesas – tai siekimas išsiaiškinti tam tikrus rūpimus klausimus, remiantis visais turimais mokslinio darbo metodais“ (Zuzevičiūtė, 2006). Atsižvelgiant į gautus rezultatus, pateikiami siūlymai vartotojams dėl taikytinų priemonių duomenų apsaugos interneto socialiniuose tinkluose stiprinimo. Tyrimo tikslas – vartotojų požiūrio analizė į duomenų apsaugą socialiniuose tinkluose.

3.1. Tyrimo metodologija

Siekiant įvertinti interneto socialinių tinklų vartotojų požiūrį ir suvokimą apie duomenų apsaugą socialiniuose tinkluose tyrimui buvo pasirinkti du metodai: kokybinis – natūralusis eksperimentas ir kiekybinis anketinės apklausos metodas.

Buvo vykdomas natūralus eksperimentas. Šio eksperimento metu tyrimo objektas neišskiriamas iš natūralios aplinkos, o eksperimentinė situacija iš esmės nesiskiria nuo įprastų gyvenimo sąlygų. (Kardelis, 2002) Tyrimo metu, panaudojant socialinės inžinerijos technologijų priemones, buvo atliktas natūralus eksperimentas, siekiant nustatyti kaip socialinių tinklų vartotojai vertina savo anketų/profilių privatumą, ar naudojasi saugumo nustatymais, bei taip pat ar kritiškai vertina kiekvieną socialinio tinklo vartotojo pakvietimą draugauti. Vykstant eksperimentui išryškėjo probleminės prielaidos ir susidarė sąlygos suformuoti anketą ir atlikti apklausą.

Anketinės apklausos metodas dažniausiai naudojamas socialiniuose tyrimuose, kiekybinių duomenų rinkimui. T.y. reikalingi duomenys gauti užduodant klausimus. Iš kitų duomenų rinkimo būdų, šis metodas išsiskiria tuo, kad pagrindinė paklausos priemonė yra klausimynas, kuris yra numatytos formos, struktūros, bei sudarytas remiantis klausimų formulavimo taisyklėmis (Gaižauskaitė I., Mikienė S., 2014). Apklausos metodu atliekamas tyrimas leidžia suprasti, kokios yra sąsajos tarp teorijos ir faktinės situacijos

Tyrimo eiga. Tyrimas atliktas šiais etapais:

- Tyrimo parametrų suformulavimas;
- Tyrimo instrumento (netikros paskyros) sukūrimas;
- Eksperimento socialiame tinkle *Facebook* vykdymas;
- Tyrimo instrumento (klausimyno) sudarymas bei pagrindimas, remiantis atlikta teorinių šaltinių analize.

- Tyrimo duomenų rinkimas – anketinės apklausos vykdymas, taikant uždaro tipo klausimyną.
- Tyrimo duomenų apdorojimas.
- Tyrimo duomenų analizė.
- Tyrimo rezultatų interpretavimas.
- Išvadų ir rekomendacijų parengimas.

Tyrimo etikos principai. Atliekant tyrimą, užtikrinami šie tyrimo etikos principai:

- Savanoriškas sutikimas dalyvauti tyrime ir informuotumas. Jis įgyvendintas respondentams pristatant atrankos kriterijus, būdus ir priežastis, kodėl būtent jie pakviesti dalyvauti šiame tyrime. Prieš atsakant į klausimus tyrimo dalyviai informuojami, jog jų dalyvavimas apklausoje yra asmeninis apsisprendimas ir jie gali atsisakyti dalyvauti tyrime arba savo dalyvavimą nutraukti bet kuriame tyrimo etape.
- Anonimiškumo ir gautos informacijos konfidencialumo užtikrinimo principas. Neprašoma nurodyti asmeninės informacijos, kuri leistų atpažinti konkretų asmenį. Darbe pateikiant tyrimo rezultatus, respondentų charakteristikos pristatomos, pateikiant bendras charakteristikas, nenurodant jokios asmeninės informacijos. Nėra galimybės nustatyti kuris respondentas, kurį klausimyną pildė.

  Eksperimentui pasibaigus visi kviesti ir kvietimus draugauti priėmę asmenys pašalinti iš „draugų“. Eksperimentui sukurtas profilis pašalintas.
- Žalos respondentams vengimas. Klausimai pateikiami pagarbiu stiliumi, nesudarant prielaidų respondentams prarasti privatumą. Klausimynas neturi gluminti, kelti įtampos ar kitaip versti tyrimo dalyvį jaustis nepatogiai.

Tyrimo imtis.

Apklausa. Tikslinė tyrimo grupė – bent vieno socialinio tinklo vartotojai. Remiantis Statistikos departamento duomenis buvo manoma, kad 2017 m. Lietuvoje yra 2 mln. 848 tūkst. gyventojų iš kurių 2017 m. vasario–balandžio mėnesiais atliktais interneto auditorijos tyrimais internetu ir socialiniais tinklais Lietuvoje naudojasi 79,1% gyventojų (2848000 * 0,79 ~ 2249920 interneto ir socialinių tinklų vartotojų). Siekiant užtikrinti 5% klaidų lygį reikėjo apklausti maždaug 384 respondentus. Tyrimas buvo atliktas 2018 m. rugsėjo - lapkričip mėn., naudojant „sniego gniūžtės“ duomenų rinkimo metodo principus.

Tyrimo imties atrankos būdas.

Tyrime dalyvavo asmenys nuo 13 metų, kurie yra interneto socialinių tinklų vartotojai. Šie amžiaus kriterijai imčiai pasirinkti atsižvelgiant į interneto socialinių tinklų taisykles. *Facebook* ir

Twitter socialinių tinklų paslaugos nėra skirtos asmenims iki 13 metų. *LinkedIn* vartotojais gali būti asmenys nuo 16 metų.

Tyrimo metodai

Tyrimas. Naudotos „sniego gniūžtės“ ir „patogioji“ (angl. *availability sampling*) atrankos. „Sniego gniūžtės“ principas numato, kad vykdant tyrimą didėja, plečiasi imties dydis. Pirmiausiai parinkti keletas žinomų, pasiekiamų tiriamųjų. Kiti apklausiamieji pasirinkti atsižvelgiant į pirmesniųjų duotas nuorodas ir/ar rekomendacijas. Tiriamieji taip pat davė kitų, tyrimui reikalingų apklausti žmonių, kontaktinę informaciją. „Patogioji atranka“ numato, jog tyrimui parinkti pirmi pasitaikę ar lengviausiai pasiekiami individai, naudojantys interneto socialinius tinklus. Pradžioje apklausai buvo parinkti artimos aplinkos žmonės: kaimynai, bendradarbiai, kurso bendramoksliai ir draugai. Kadangi apklausa vykdoma elektroninėje erdvėje, iki minimumo mažėja rizika, kad tiriamosios populiacijos nariai nepapuls į imtį. (Gaižauskaitė S. 2014)

Duomenų rinkimo metodai: anketinė apklausa, statistinė tyrimo duomenų analizė bei natūralus eksperimentas. Tyrimo duomenų analizė atlikta taikant MS Office „Excel 2010“ programinę įrangą.

Klausimyną sudarė tokios struktūrinės dalys: informacija apie respondentus – demografinės charakteristikos, informacija apie naudojamus interneto socialinius tinklus ir aktyvumą juose, bei respondentų kibernetinio saugumo žinios apie duomenų apsaugą naudojamuose socialiniuose tinkluose. Klausimynas buvo sukurtas el. erdvėje naudojant „apklausa.lt“ sistemą, todėl lengvai ir patogiai prieinamas potencialiems respondentams atitinkantiems keliamus kriterijus tiek kompiuteriu, tiek išmaniaisiais įrenginiais. Anketa platinta naudojant socialinius tinklus *Facebook, Twitter, LinkedIn*.

Tyrimo instrumentas

Uždaro tipo klausimynas, skirtas respondentų nuostatoms apie duomenų apsaugą interneto socialiniuose tinkluose atskleisti. Klausimynas apima 14 klausimų, kurie suskirstyti į tris dalis: demografinius klausimus respondentų gyvenamajai teritorijai, amžiui ir lyčiai nustatyti; klausimus leidžiančius atskleisti socialinį aktyvumą; .klausimus atliepiančius kibernetinio saugumo raštingumo kriterijus (saugaus elgesio, duomenų dalinimosi socialiniuose tinkluose specifikai nustatyti).

4 Lentelė. **Tyrimo instrumento klausimyno sudedamosios dalys.**

Klausimyno dalies pavadinimas	**Klausimyno dalies tyrimo aprašymas**	**Klausimų/teiginių kiekis konkrečioje dalyje ir pobūdis**
I. Demografinės charakteristikos	Respondentų gyvenamajai teritorijai, amžiui ir lyčiai atskleisti.	1. Atviro tipo klausimas 2. - 3. Uždaro tipo klausimai

Klausimyno dalies pavadinimas	**Klausimyno dalies tyrimo aprašymas**	**Klausimų/teiginių kiekis konkrečioje dalyje ir pobūdis**
II. Socialinis aktyvumas	Dalyvavimo socialiniuose tinkluose specifikai nustatyti.	4.-7. Uždaro tipo klausimai.
III. Kibernetinio saugumo raštingumas	Saugaus elgesio ir duomenų dalinimosi socialiniuose tinkluose specifikai nustatyti.	8-14 Uždaro tipo klausimai

Rengiant instrumentą naudotasi kitų, daugiausia užsienio, mokslininkų atliktais tyrimais. Anketinės apklausos metodas buvo taikytas daugelyje užsienio tyrimų, siekiant nustatyti ir išanalizuoti interneto socialinių tinklų vartotojų žinias, požiūrį į saugumą internetinėje erdvėje ir saugumo priemonių naudojimą. Užsienio atliktuose tyrimuose klausimai buvo formuluojami siekiant išsiaiškinti, kokius SNS funkcionalumus vartotojai naudoja siekdami apsaugoti savo paskyras. Sudarinėjant klausimyną Lietuvos socialinių tinklų vartotojams, papildomai siekta išsiaiškinti ar vartotojai susipažinę su skelbiamomis naudojimosi taisyklėmis ir privatumo politika. Ar imasi kokių nors veiksmų saugoti savo skelbiamus duomenis ar saugo savo privatumą.

Tyrimo apribojimai

Tyrimo metu respondentams buvo taikomi tokie apribojimai:

1. Amžius. Siekiant atskleisti vartotojų požiūrį į duomenų apsaugą interneto socialiniuose tinkluose, dalyvių amžius nuo 13 metų, kadangi tokią amžiaus ribą numato socialinių tinklų naudojimo taisyklės. Tyrime nedalyvaus jaunesni nei 13 metų respondentai.
2. Priklausymas nors vienam socialiniam tinklui. Tyrimo efektyvumui ir patikimumui apklausiami tik interneto socialinių tinklų nariai turintys aktyvias anketas. Tyrime nedalyvavo socialinių tinkluose neturintys anketų interneto vartotojai.

Eksperimentas

Kiekybiniai tyrimai nepritaikyti paaiškinti žmonių elgesio, suvokimo ir produkto vertinimo. Tiems trūkumams kompensuoti buvo išplėtoti kokybiniai tyrimo metodai. Kokybinis tyrimas – sistemingas situacijos, įvykio, atvejo, individo ar grupės tyrimas natūralioje aplinkoje. Šie tyrimai apima skirtingas tyrimo metodikas, kurios skirstomos į keletą stambių grupių: giluminiai (asmeninis) interviu; pusiau-struktūrizuoti (formalizuoti) interviu; grupinės diskusijos (fokus grupės); stebėjimai; eksperimentai; projekciniai metodai; asociatyviniai metodai; ekspertinis vertinimas.

Eksperimentu vadinamas empirinis bandymas patikrinti dėsnį arba atskleisti nežinomą reiškinį, tuo tikslu sukeliant tam tikrą tikslingą reiškinį (Kittel B., Morton R.B., 2012). Paprastai eksperimentiniai tyrimai skirstomi į tris kategorijas:

- laboratorinius,
- lauko,
- natūraliuosius eksperimentus.

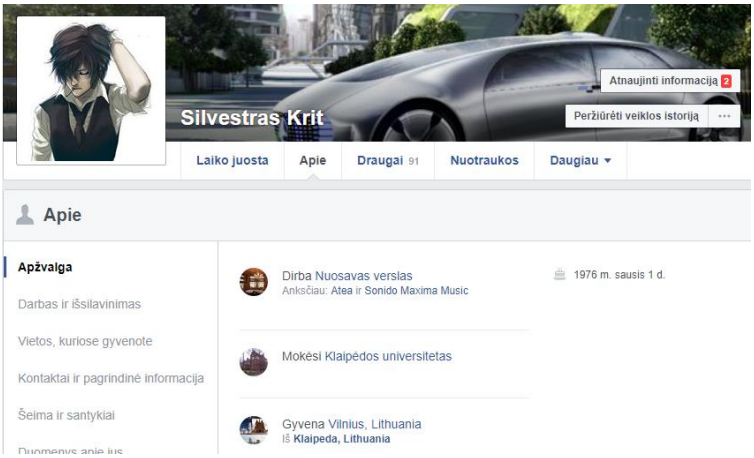
Laboratorinis yra toks eksperimentas, kai sudarant dirbtinę aplinką specialiai įrengtoje patalpoje tikrinama tiriamoji idėja griežtos požymių kontrolės sąlygomis (Stonkus S., 2002).

Vykdant lauko eksperimentą naudojama visiškai kita aplinka. Eksperimento metu tyrimo objektas neišskiriamas iš natūralios aplinkos, o eksperimentinė situacija nesiskiria nuo įprastų gyvenimo sąlygų (Kittel B., Morton R.B. ,2012).

Natūralusis eksperimentas – jam taip pat būdinga maksimaliai natūrali situacija, kai tiriamo objekto sistema funkcionuoja įprastinėmis sąlygomis. Literatūroje (Dunning S., 2012; Kittel B., Morton R.B., 2012, kt.) nurodoma, kad natūralusis eksperimentas skiriasi nuo lauko tyrimo tuo, kad pastarojo metu pavieniai asmenys ar jų grupės yra veikiami tyrėjo nekontroliuojamų veiksnių ir veikia nuo tyrėjo nepriklausančiomis aplinkybėmis. Tai reiškia, kad tyrėjas nedaro visiškai jokio poveikio tiriamam objektui, nesikiša į vykstančių procesų kaitą, o tik stebi, fiksuoja pokyčius, jei jų yra ir daro išvadas. Taikant šią tyrimo strategiją, nėra jokio dirbtinumo. Pagrindinis natūralaus eksperimento pranašumas yra tas, kad iki minimumo sumažėja dirbtinės situacijos tikimybė. Visi tiriamojo objekto santykiai, ryšiai, aplinka, lieka beveik nepakitę.

Tyrimo metu, panaudojant socialinės inžinerijos technologijų priemones, buvo atliktas natūralus eksperimentas, siekiant nustatyti kaip interneto socialinių tinklų vartotajai administruoja asmenines paskyras, ar laikosi socialinių tinklų nurodomų saugumo rekomendacijų. Pasirinktas natūralaus eksperimento metodas todėl, kad tyrimas atliekamas natūralioje aplinkoje, todėl gauti duomenys yra objektyvūs. Eksperimentui atlikti buvo pasirinktas socialinis tinklas *Facebook*, kadangi pagal *Kantar TNS* 2017 m. tyrimų duomenis, šis tinklas išlieka populiariausiu socialiniu tinklu Lietuvoje.

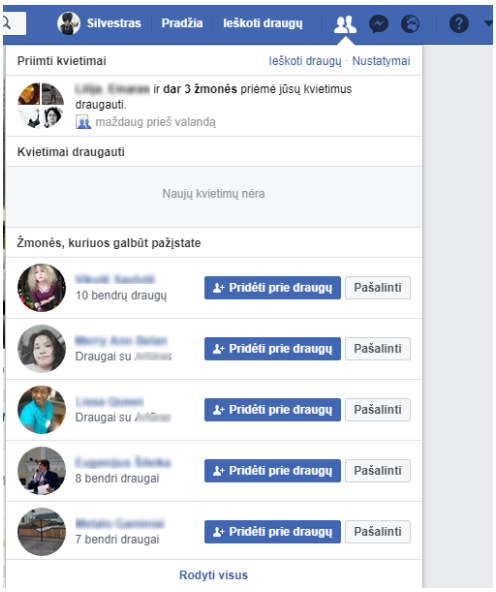
Eksperimentui vykdyti sukurta netikra vartotojo paskyra *Facebook* socialiniame tinkle. 2018 m. kovo mėnesį sukurta paskyra Silvestro Krit vardu. Buvo kuriamas aukštąjį išsilavinimą įgijusio, gyvenančio Vilniuje ir turinčio nuosavą verslą 42 m amžiaus vyro įvaizdis. Profilio nuotraukai panaudotas, internete rastas, pieštas paveikslėlis atvaizduojantis jauną vaikiną. Šalia pagrindinės informacijos apie baigtą mokslo instituciją, buvo įkelta nuotraukų, su pažymėtais (angl. *tag*) miestais, imituojančių keliones po Europą. Nurodyta mėgstama muzika, knygos, filmai, mėgstamos sporto komandos. Mėnesį paskyros sienoje buvo dalinamasi įvairia informacija, skelbiamos nuotraukos.



Pav. 10 Netikra *Facebook* paskyra

Po mėnesį trukusio informacijos skelbimo pradėti siųsti kvietimai „draugauti“ asmenims, kurie savo anketose nurodę, kad yra baigę tą pačią aukštąją mokyklą kaip ir netikros paskyros naudotojas. Asmenims priėmus kvietimą „draugauti“, toliau buvo siunčiami kvietimai draugauti jų draugams.

Reikia išskirti tai, kad kuo daugiau bendrų draugų Silvestras Krit turėjo su kitomis anketomis, tuo greičiau ateidavo pranešimai apie tai kad „priėmė jūsų kvietimus draugauti“. Taip pat, augant draugų ratui, pats *Facebook* vis dažniau rodė pasiūlymus „žmonės, kuriuos galbūt pažįstate“.



Pav. 11 Priimti kvietimai ir *Facebook* siūlymai

Balandžio – gegužės mėnesiais buvo išsiųsta 100 pakvietimų draugauti. Birželio pirmą savaitę buvo užfiksuotas kvietimų drauguti priėmusių asmenų skaičius. Taip pat analizuota kiek iš šių asmenų savo anketose yra keitę privatumo nustatymus. Buvo vizualiai lyginama, kokia informacija skelbiama

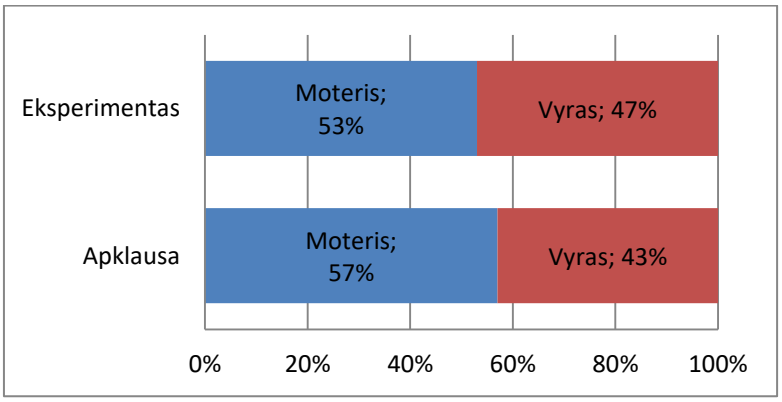
vartotojų sienose, kokias naujienas dalinasi ar nuotraukos yra matomos į draugus priimtam profiliui Silvestras Krit ir kitai anketai, kuri nėra įtraukta į tiriamųjų draugų sąrašus.

Baigus eksperimentą visi kviesti ir kvietimus draugauti priėmę asmenys pašalinti iš „draugų“. Eksperimentui sukurtas profilis ištrintas.

3.2. Tyrimo duomenų analizė

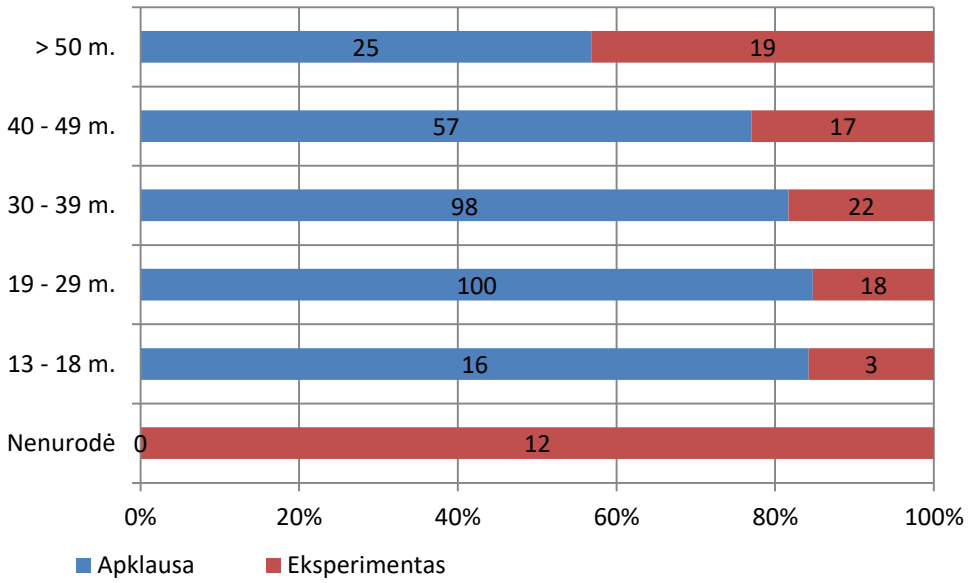
Šioje dalyje analizuoti tyrimo duomenys. Tyrimo metu naudoti apklausos ir natūralaus laboratorinio eksperimento metodai papildė vieni kitų duomenis, o tai sudarė galimybes padidinti bendrą tyrimo patikimumą. Buvo siekiama išsiaiškinti tiriamųjų gebėjimus ir žinias interneto socialinių tinklų duomenų saugumo valdymo ypatumus. Kiekvienas klausimas yra išsamiai aprašomas ir analizuojamas, pateikiamos įžvalgos. Tyrimo analizė pagrindžiama asmenine tyrinėtojos patirtimi ir gebėjimu sisteminti bei analizuoti surinktus duomenis.

Vertinat respondentų socio-demografines charakteristikas matyti, kad respondentai tiek anketinėje apklausoje, tiek vykdytame eksperimente pagal lytį pasiskirstę beveik tolygiai, procentinė išraiška labai panaši. Procentai skaičiuojami nuo respondentų, kurie dalyvavo apklausoje. (N=296) ir eksperimente (N = 91)



Pav. 12 Pasiskirstymas pagal lytį

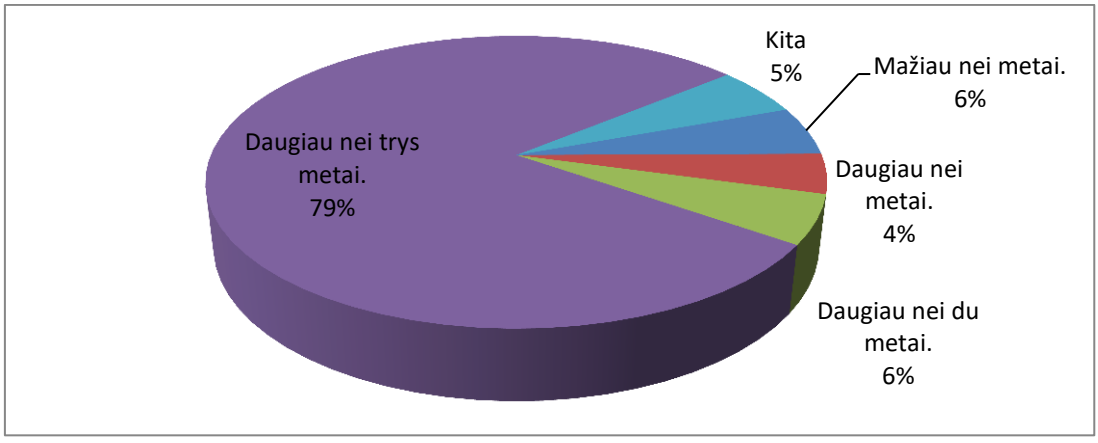
Labai panaši situacija lyginant tiriamųjų respondentų amžių. Statistiškai reikšmingai dažniau kasdien internetu naudojasi jaunesni nei 39 metų respondentai. Remiantis tiek anketinės apklausos, tiek eksperimento metu gautais duomenimis, matoma, kad socialiniai tinklai populiariausi dviejose amžiaus grupėse: jaunimo 19-29 m ir suaugusiųjų 30-39 m.



Pav. 13 Pasiskirstymas pagal amžių.

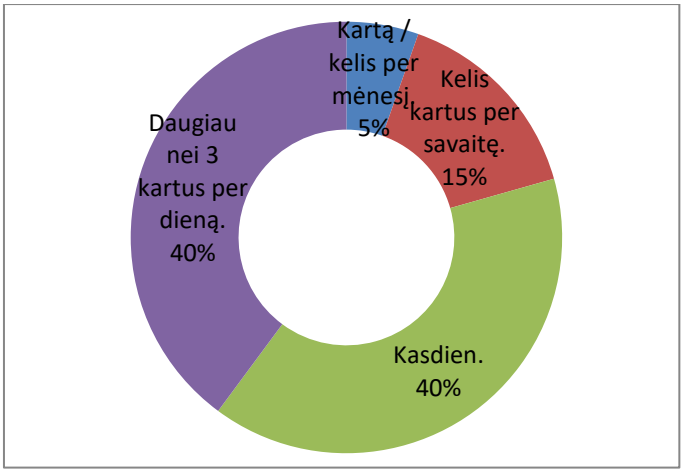
Reiktų atkreipti dėmesį į tai, kad galimybės jungtis prie socialinių tinklų pavieniams asmenims atsirado dar 2006 m. Anketinėje paklausoje iš visų dalyvavusių respondentų net 79 % nurodė, kad socialinių tinklų paslaugomis naudojasi ilgiau nei tris metus, o dar 6 % nurodė, kad jau apie 10-11 metų yra socialinių tinklų vartotojais. Procentai skaičiuojami nuo respondentų, kurie dalyvavo apklausoje. (N=296).

Ištyrus eksperimente dalyvavusių tiriamųjų anketų gyvavimo laiką, daugiau kaip 60% visų paskyrų buvo sukurtos vėliau nei prieš tris metus.



Pav. 14 Naudojimosi SNS trukmė metais.

Remiantis anketine apklausa, galima spręsti, kad naudojimasis socialiniais tinklais vyksta gana aktyviai. Bent kartą per dieną ir dažniau interneto socialiniai tinklai naudojasi 80 % visų respondentų. Jie teigia, kad kasdien jungiasi prie savo paskyrų, kur praleidžia ne mažiau kaip vieną valandą savo laiko.

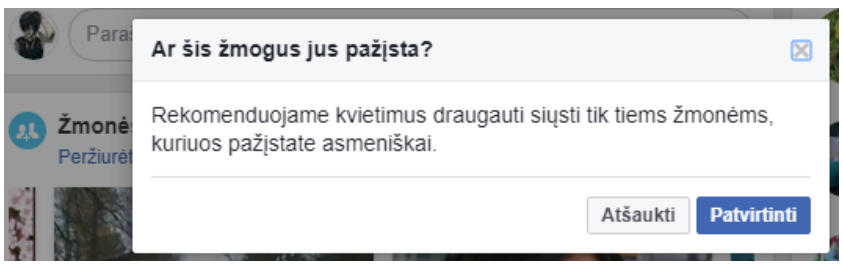


Pav. 15 Jungimosi prie SNS dažnumas.

Atsižvelgiant tai kad didžioji dalis tyrime dalyvavusių asmenų yra socialinių tinklų nariai daugiau kaip trys metai. Jų lankymosi ir jungimosi prie paskyrų dažnumas labai didelis, t.y. bent kartą per dieną, todėl visus tiriamuosius ir respondentus galima laikyti pažengusiais socialinių tinklų vartotojais. Taip pat, ir eksperimento, ir apklausos rezultatai pagal respondentų ir tiriamųjų lytį, amžių ir socialinių tinklų naudojimo įpročiais labai panašūs ir papildantys vienas kitą.

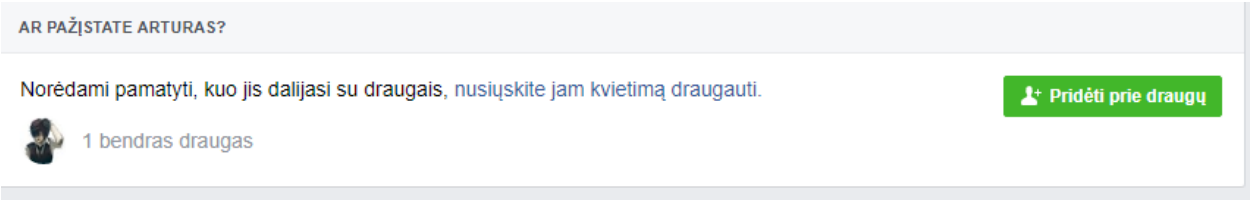
Eksperimentas

Tyrimui, panaudojus socialinės inžinerijos metodus sukurta netikra vartotojo paskyra. Vykdant eksperimentą buvo išsiųsta 100 kvietimų priimti į draugus. Pirmi kvietimai siųsti asmenims nurodžiusiems, kad yra baigę tą pačią aukštąją mokyklą kaip ir netikra paskyra. Vėliau kvietimai siųsti be atrankos visiems asmenims, kuriuos socialinis tinkas *Facebook* rodė sąraše „Žmonės, kuriuos galbūt pažįstate“. Reiktų paminėti, jog vienu metu išsiuntus daugiau nei 10 kvietimų draugauti socialinis tinklas *Facebook* parodydavo pranešimą rekomenduojantį kvietimus siųsti tik asmeniškai pažįstamiems žmonėms.



Pav. 16 *Facebook* pranešimas

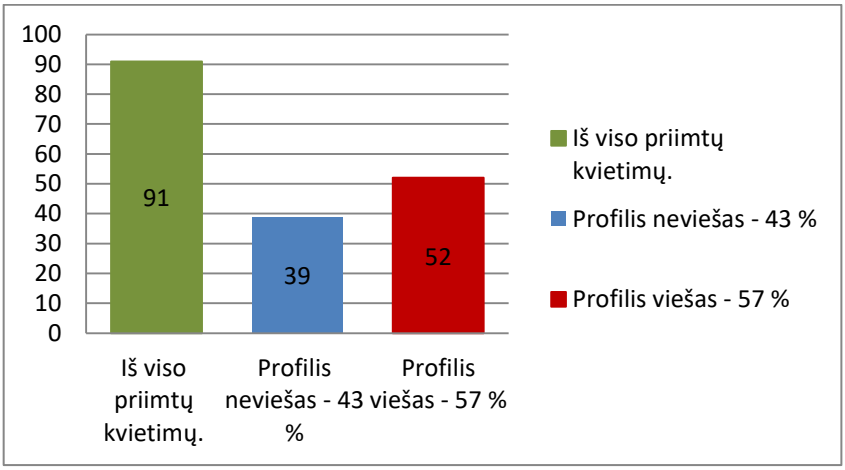
Kuo didesnis darėsi „draugų“ ratas, tuo daugiau pasiūlymų patekdavo ir pats socialinis tinklas.



Pav. 17 *Facebook* siūlymas

Mėnesio bėgyje, iš vieno šimto išsiųstų kvietimų draugauti, 91 kvietimas buvo priimtas. Netikros paskyros draugų sąraše buvo 91 asmeniškai nepažystamas asmuo.

Peržiūrėjus kiekvieną paskyrą nustatyta, kad didesnė pusė (52 anketos) nenaudoja socialinio tinklo teikiamo funkcionalumo leidžiančio skirtingus informacijos matomumo nustatymus, skirtingiems vartotojams. Procentai skaičiuojami nuo respondentų, kurie dalyvavo eksperimente. (N=91)



Pav. 18 Paskyrų matomumo nustatymai

Kita dalis (39 paskyros) asmenų, yra nusistatę skirtingus jų paskyrų matomumo nustatymus t.y. privatumo ir saugos reikalavimuose yra pažymėję, kad jų skelbiamą informaciją matytų tik draugai. Tačiau verta atkreipti dėmesį, kad kai kurios, iš tų anketų turi po 3428, 4927 ar net 5000 draugų.



Pav. 19 *Facebook* tinkle turimų draugų skaičiai

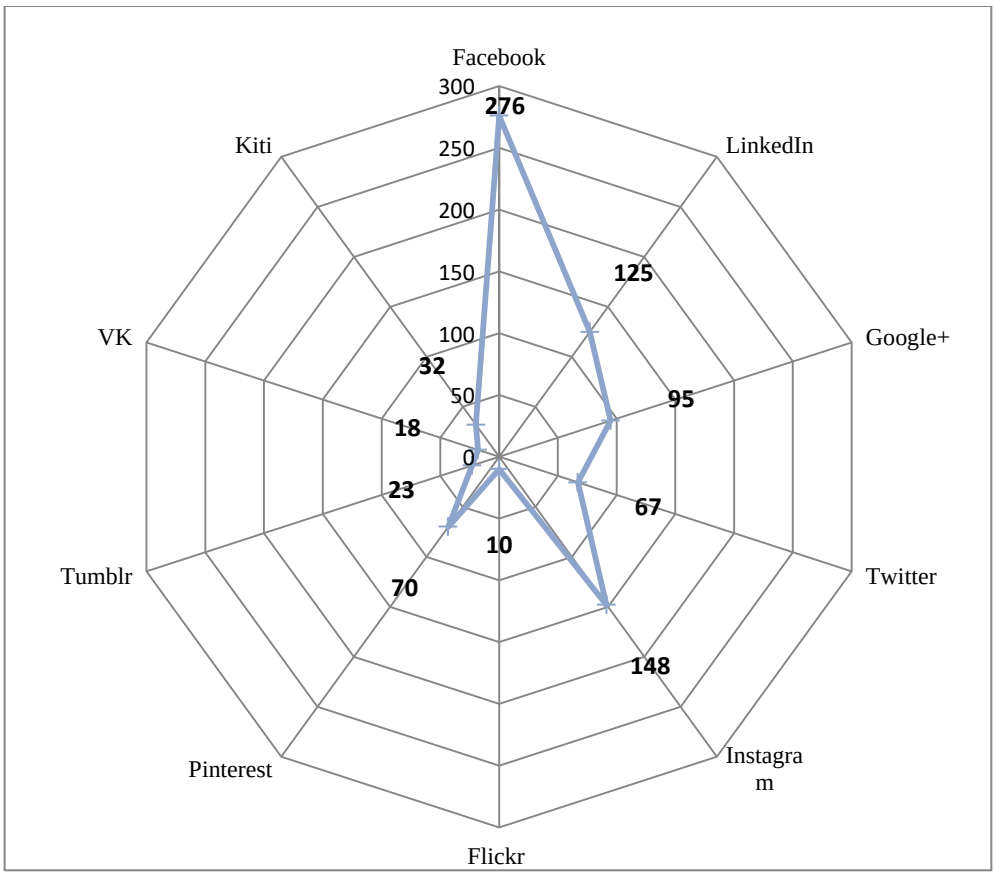
Taip pat dalyje anketų, kurios savo privatumo nustatymuose nurodę, kad jų sienoje skelbiama informacija matoma tik draugams, tačiau paskyrų viršelio paveikslėliai yra palikti vieši (angl. *public*) (matomi visiems tinklo nariams) ir naudojamos šeimos nuotraukas su mažamečiais vaikais.

Apibendrinant kokybinį tyrimą išryškėjusios tokios probleminės prielaidos, kaip intensyvus dalyvavimas socialiniuose tinkluose kritiškai nevertinant nepažystamų anketų kvietimų draugauti, asmeninių privatumo nustatymų nebuvimas ir nevertinimas kokia informacija gali būti skelbiama viešai, sudarė sąlygas suformuluoti kokybiniam tyrimui reikalingą intstrumentarijų.

Anketinė apklausa

Anketoje buvo pateikta 14 klausimų (žr. 1 priedą) norint ištirti Lietuvos vartotojų požiūrį į asmens duomenų apsaugą interneto socialiniuose tinkluose: *Facebook, Twitter* ir *LinkedIn*. Taip pat nustatyti, kokius duomenis vartotojai pateikia socialiniams tinklams, sužinoti vartotojų patirtį naudojantis soc. tinklais, galimas grėsmes, bei skelbiamos privatumo politikos žinojimą.

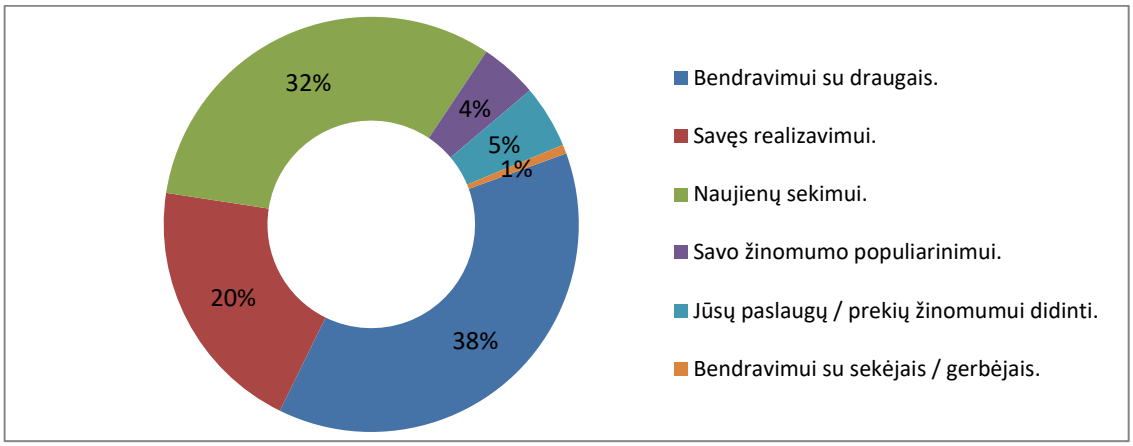
Atliekant tyrimą buvo siekiama nustatyti kokie socialiniai tinklai tarp Lietuvos gyventojų populiariausi. Procentai skaičiuojami nuo respondentų, kurie dalyvavo apklausoje. (N=296)



Pav. 20 Socialinių tinklų pasiskirstymas

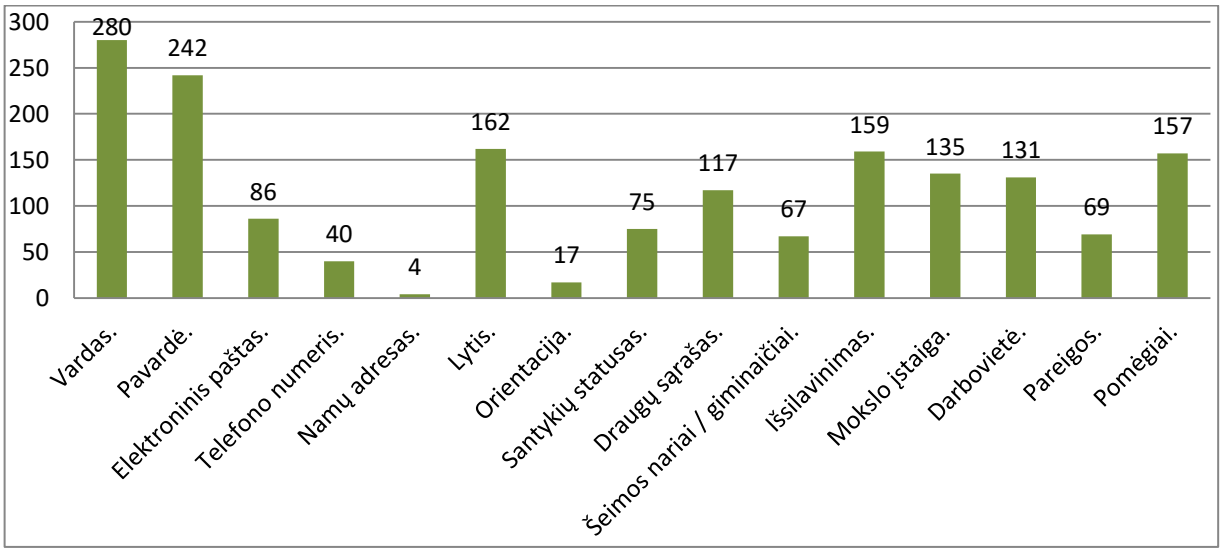
Geriausiai žinomas socialinis tinklas internete – *Facebook*. Juo naudojasi dauguma visų respondentų. Taip pat didelė dalis jų naudoja šiam tinklui prisiklausančią ir šiame tinkle integruotą, dalijimosi nuotraukomis ir paveikslėliais, *Instagram* platformą. Atsižvelgiant į anketose nurodytą amžių, verta paminėti, kad 4% respondentų papildomai nurodė naudojantys *Snaphat* socialinį tinklą. Kiti nemažiau populiarūs ir beveik trečdalio respondentų naudojami tinklai yra *LinedIn, Twitter.*

Svarbu buvo sužinoti, kokios priežastys lemia vartotojų poreikį naudotis interneto socialinių tinklų paslaugomis. Procentai skaičiuojami nuo respondentų, kurie dalyvavo apklausoje. (N=296)



Pav. 21 Naudojimosi socialiniais tinklais priežastys

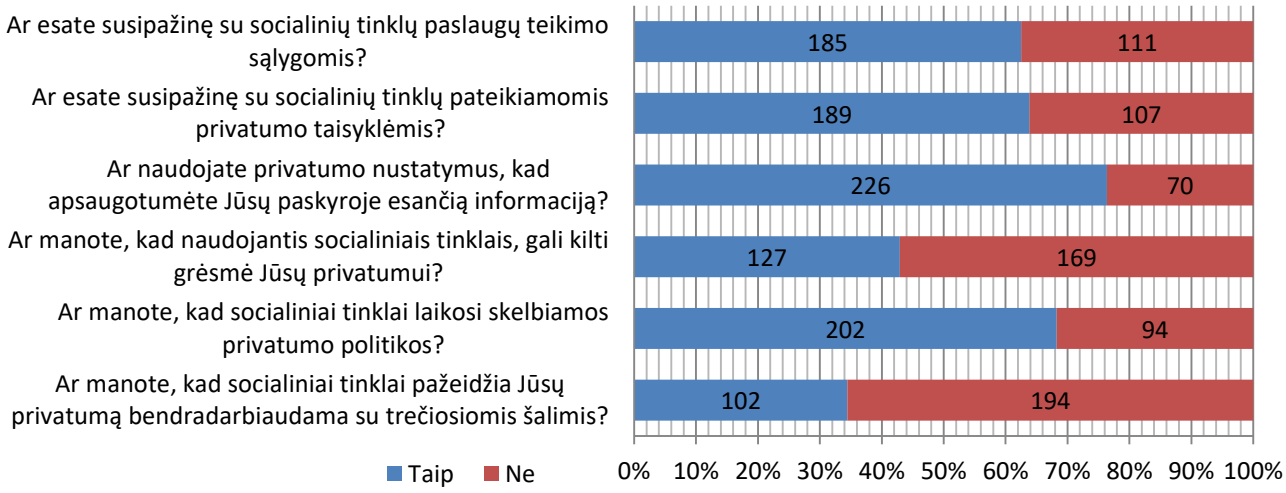
Priežastis paskatinusias prisijungti prie socialinių tinklų respondentai nurodė gana įvairias. Tačiau remiantis anketos atsakymais, socialiniai tinklai dažniausiai naudojami komunikacijai, naujienoms gauti ir asmeniniais reikalais saviraiškai. Rečiausiai naudojami asmeninio populiarumo siekimui, reklamai ar komunikacijai su sekėjais. Nors reiktų pastebėti, kad socialiniai tinklai po truputį keičia žiniasklaidos suvokimą ir didžioji dalis naujienų svetainių ateina į socialinius tinklus.



Pav. 22 Viešai pateikiama informacija socialiniuose tinkluose

Daugiau nei pusė respondentų nurodė, kad socialiniuose tinkluose pateikia savo pilną vardą ir pavardę, išsilavinimą, lytį ir pomėgius. Šiek tiek mažesnis respondentų skaičius (apie pusė atsakiusiųjų) Dalinasi tolia informacija kaip mokslo įstaiga, darbovietė, draugų sąrašas. Tik nedidelė dalis viešina kontaktinę informaciją, tokią kaip telefono numeris, elektroninis pašto adresas ar net gyvenamasis adresas.

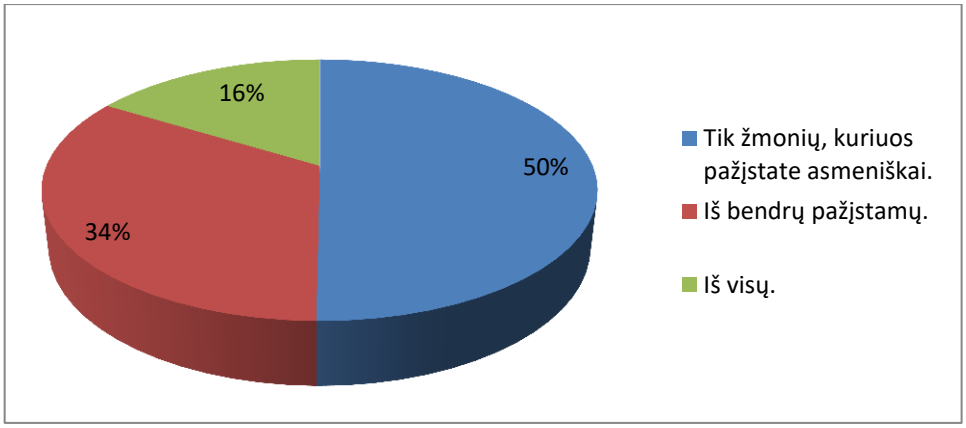
Procentai skaičiuojami nuo respondentų, kurie dalyvavo apklausoje. (N=296) Apklausus respondentus apie socialinių tinklų paslaugų teikimo sąlygas daugiau nei 60% respondentų atsakė kad yra su jomis susipažinę. Tokia pati respondentų dalis nurodė, kad yra susipažinę ir su bei pateikiamomis privatumo taisyklėmis. Virš 70 % respondentų nurodė, kad naudoja socialinių tinklų funkcionalumą leidžianti nurodyti kas gali matyti skelbiamą informaciją ir sutinka su teiginiu kad SNS laikosi skelbiamos privatumo politikos.



Pav. 23 Žinios apie socialinių tinklų naudojimosi ir privatumo taisykles

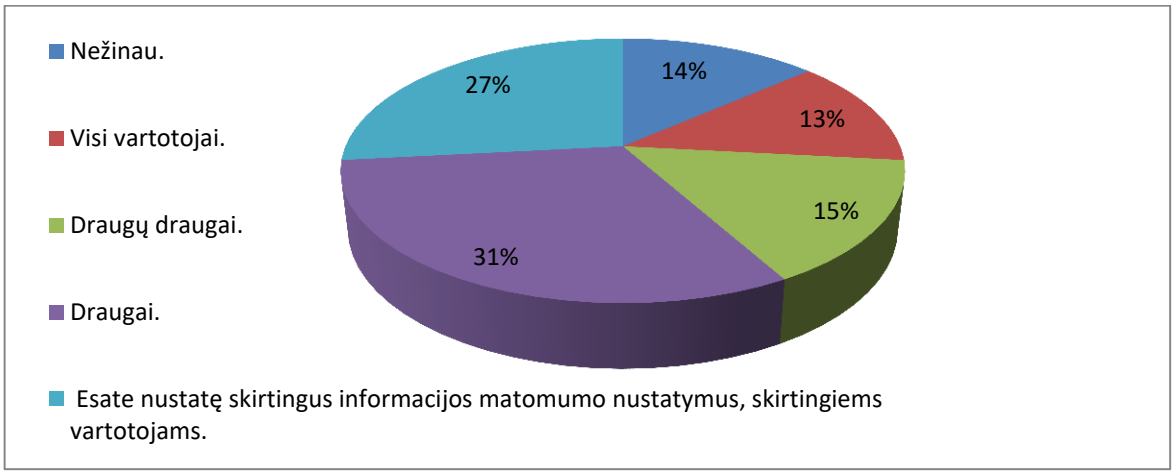
Beveik 57% nemano kad naudojimasis socialiniais tinklais gali kelti grėsmę jų duomenų saugumui. Tik nedidelis procentas (34 %) respondentų mano, kad socialinių tinklų bendradarbiavimas su trečiosiomis šalimis, perduodant joms duomenis, pažeidžia SNS vartotojų privatumą.

Asmenys, iš kurių priimami kvietimai draugauti. Procentai skaičiuojami nuo respondentų, kurie dalyvavo apklausoje. (N=296) Pusė respondentų nurodė, kad kvietimus draugauti priima tik asmeniškai pažįstamų. Trečdalis SNS vartotojų kvietimus draugauti priima ir iš bendrų pažįstamų.



Pav. 24 Priimami kvietimai draugauti

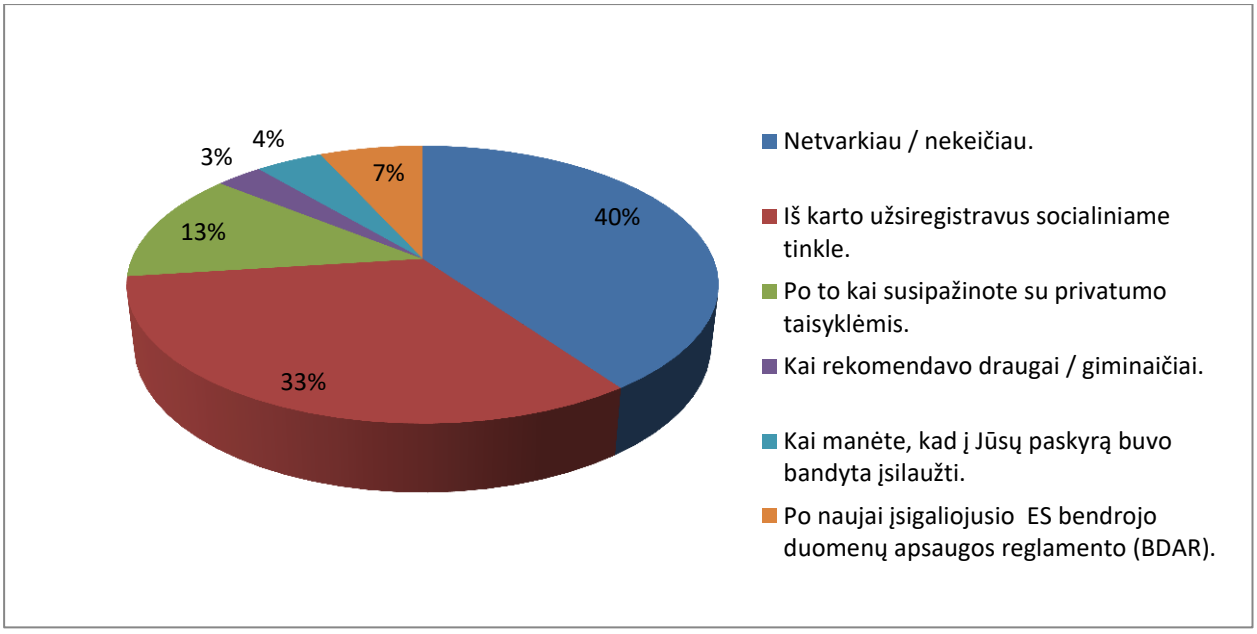
Paskyrų privatumo nustatymai. 27% interneto socialinių tinklų vartotojų teigia naudojantys skirtingus informacijos matomumo nustatymus skirtingiems vartotojams, panaši dalis vartotojų savo informacija skelbia tik asmenims esantiems draugų sąraše.



Pav. 25 Informacijos matomumo nustatymai

Nedidelė dalis respondentų savo skelbiama informacija dalinasi ir su draugų draugais. Likusi respondentų dalis (27 %) teigia, kad visa jų informacija yra vieša arba nežino kas gali matyti turinį, kuriuo jie dalinasi.

Privatumo nuostatų keitimas. Net 40 % apklausoje dalyvavusių socialinių tinklų vartotojų teigia, kad netvarko ar nekeičia savo privatumo nustatymų, kurie prisiregistravus prie socialinio tinklo „pagal nutylėjimą“ būna vieši.



Pav. 26 Privatumo nustatymų keitimas

Šiek tiek mažesnė dalis (40 %) nustatymus pasikeičia pagal save iškarto tik prisiregistravus socialiniame tinkle. Nedidelis procentas SNS narių nustatymus keitė tik galutinai susipažinus su tinklų paslaugų ir privatumo taisyklėmis, tokia pat dalis nustatymus keitė po naujai įsigaliojusio duomenų apsaugos reglamento.

Apibendrinant tyrimą, galima teigti, jog visiškai pasitvirtino iškelta **hipotezė**, kad vartotojai, duomenų apsaugos valdyme interneto socialiniuose tinkluose yra silpniausia grandis, nes tai įrodo eksperimento ir apklausos rezultatai. Taip pat galima teigti, kad pasitvirtino **ginamieji teiginiai.** Vartotojai neišmano ar neįsigilina į teikiamas naudojamų socialinių tinklų saugumo rekomendacijas ir pilnai neišnaudoja visų įmanomų priemonių duomenų apsaugai interneto socialiniuose tinkluose, nes eksperimento rezultatai patvirtino vartotojų neatsargų elgesį socialiniuose tinkluose, o apklausos rezultatai leidžia daryti išvadą, kad vartotojai net ir susipažinę su socialinių tinklų privatumo taisyklėmis ir galimybėmis apsaugoti savo duomenis, nemato didelės grėsmės ir elgiasi neapgalvotai. Socialiniai tinklai siekia užtikrinti, kad jų platformos būtų skaidrios ir saugios, nes eksperimento metu buvo nuolat gaunami parnešimai apie galimus privatumo nustatymus, perspėjimai įvertinti kokie asmenys kviečiami į draugų sąrašą.

IŠVADOS

1. Teorinio tyrimo metu išanalizavus užsienio autorių tyrimus galima teigti, kad interneto socialiniuose tinkluose duomenų saugumui didžiausią grėsmę kelia nesaugus vartotojų elgesys internete ir prieš vartotojus nukreiptos socialinės inžinerijos atakos. Kibernetiniai incidentai neigiamai veikia socialinių tinklų veiklą, ypatingai paveikiant jų reputaciją, taip prarandant vartotojus, gaunant teisines nuobaudas ir mokant kompensacijas nukentėjusioms trečiosioms šalims finansinius nuostolius.

2. Socialinių tinklų valdoma informacija, duomenys ir jos apdorojimo priemonės yra patrauklus kibernetinių atakų taikinys kurį galima pažeisti, sukompromituoti ar užvaldyti išnaudojant socialinių tinklų vartotojų neišprusimą ar pažeidžiamumus naudojamose technologijose. Pagrindiniai grėsmių vektoriai yra žmonės (SNS registruoti vartotojai). Didžiausia dalis kibernetinių atakų vykdoma naudojant socialinės inžinerijos priemones. Todėl labai svarbu, kad saugumo priemonės skirtos apsisaugoti nuo tokių išpuolių turi būti vienos svarbiausių.

Interneto socialiniai tinklai, šalia technologinių priemonių, turi nuolat kurti kibernetinio saugumo kultūrą šviesdami savo vartotojus.

3. Vykdant natūralųjį eksperimentą ir anketinę socialinių tinklų vartotojų apklausą nustatyta, kad vartotojai yra silpniausia duomenų apsaugos valdymo grandis socialiniuose tinkluose nes :

3.1. Eksperimento rezultatai įrodė, kad socialinių tinklų vartotojai nepasidomi ar tikrai asmeniškai pažįsta asmenis, kurių kvietimus „draugauti“ priima.

3.2. Atlikus apklausą, paaiškėjo, kad net 40 % (N=296) respondentų netvarko ar nekeičia savo privatumo nustatymų, kurie prisiregistravus prie socialinio tinklo „pagal nutylėjimą“ būna vieši. Todėl galima teigti duomenų saugumo sistemoje silpniausia grandis yra žmonės.

3.3. Eksperimento metu paaiškėjo, kad laikas per kiek patvirtinimas kvietimas „draugauti“ tiesiogiai priklauso nuo to, kiek bendrų draugų yra turima. Kuo didesnis bendrų draugų socialiniame tinkle skaičius, tuo greičiau patvirtinamas kvietimas priimti į draugus.

3.4. Eksperimento rezultatai įrodė, kad vartotojai net ir naudojantys skirtingus informacijos matomumo nustatymus skirtingiems vartotojams neįvertina rizikos ir patvirtina kvietimus draugauti iš visiškai nepažįstamų asmenų.

3.5. Taip pat eksperimento rezultatai įrodė, kad vartotojai nors ir naudoja skirtingus informacijos matomumo nustatymus savo draugų sąrašuose turi po kelis tūkstančius „draugų“. Tokių atveju, skirtingi privatumo nustatymai praranda prasmę.

3.6. Eksperimento metu nustatyta, kad socialiniai tinklai sistemingai vartotojams primena apie privatumo nustatymus, kaip juos įjungti ir keisti.

REKOMENDACIJOS

- Didinti vartotojų sąmoningumą, nes socialinių tinklų vartotojai turi suvokti, kad jei jie patys pirmiausia yra atsakingi už savo privatumą ir duomenų saugumą. Domėtis kas teikia socialinių tinklų paslaugas. Kuriai jurisdikcijai priklauso paslaugų teikėjas. Kokia privatumo politika. Kokias garantijas asmens duomenų atžvilgiu suteikia paslaugų teikėjas.
- Įvertinti kuriuose socialiniuose tinkluose verta profilyje nurodyti savo tikrąjį vardą ir/ar pavardę. Rekomenduojam naudoti pseudonimus. Gerai apgalvoti prieš paskelbiant asmeninę informaciją (ypač vardą, pavardę, adresą ir telefono numerį) socialinio tinklo profilyje. Kritiškai įvertinti visus gaunamus kvietimus draugauti, jei asmuo nepažįstamas, jokiu būdu netraukti į draugų sąrašą.
- Atsargiai elgtis su asmenine informacija, tiek savo, tiek kitų asmenų skelbiant įrašus socialiniuose tinkluose. Gerbiant kito asmens privatumą, be sutikimų nežymėti (angl. *tag*) asmenų nuotraukose, viešuose pasisakymuose, komentaruose. Būtinai naudoti privatumo nustatymus, iki minimumo riboti informacijos prieinamumą taip mažinant riziką atskleisti jautrią ar asmeninę informaciją.
- Nenaudoti vieno tokio paties slaptažodžio keliose skirtingose paskyrose, t.y kiekvienam tinklui turėti atskirą slaptažodį. Naudoti saugų slaptažodį – rekomenduojama jį sudaryti bent iš 9 simbolių kombinacijos, tarp kurių būtų didžiosios ir mažosios raidės, skaičiai, specialieji ženklai. Reguliariai, bent kas šešis mėnesius keisti slaptažodžius.
- Naudoti dviejų faktorių autentifikaciją. Šis papildomas apsaugos lygis, sumažina riziką, kad bus neleistinai prisijungta prie paskyros. Niekas negalės gauti prieigos prie paskyros net ir sužinojęs prisijungimo vardą ir slaptažodį. Sprendimas padės sumažinti duomenų pažeidimų, kylančių dėl silpnų slaptažodžių, grėsmę. Nesijungti prie socialinio tinklo paskyros viešo naudojimo įrenginiuose.

LITERATŪROS SĄRAŠAS

1. Altschuller S. Benbunan-Fich R. The pursuit of trust in ad hoc virtual teams: how much electronic portrayal is too much // *European Journal of Information Systems*, 2013 Vol. 22 No. 6, p. 619-636
2. Andre T. Cybersecurity: An Enterprise Risk Issue // *Healthcare Financial Management* 2017, Vol. 71 Issue 2, p. 6
3. Barnes S. B. A privacy paradox: Social networking in the United States // *First Monday* 2006, Vol.11, No. 9. Prieiga per internetą: URL: https://firstmonday.org/ojs/index.php/fm/article/ view /1394/1312 [žiūrėta 2018 02 03]
4. Barnhart B. Types of Social Media Every Marketer Needs to Know // *Sprout Social* 2017 June 27, Prieiga per internetą: URL: https://sproutsocial.com/insights/types-of-social-media/ [žiūrėta 2018 02 03]
5. Becker J., Chen H. Measuring Privacy Risk in Online Social Networks. // *UC Davis* 2009, p.28.
6. Benson V., el al. Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? // *Information Technology & People* 2015 No28 p. 426-441
7. Boyd M.Danah, Ellison B. Nicole, Social Network Sites: Definition, History, and Scholarship // *Journal of Computer-Mediated Communication* 2009, Volume 13, Issue 1 p. 210, 213 Prieiga per internetą: URL: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full [žiūrėta 2017 11 10]
8. Cambridge Analytica Files // *The Guardian* Sat 24 Mar 2018 Prieiga per internetą: URL: https://www.theguardian.com/news/series/cambridge-analytica-files [žiūrėta 2018-04-28]
9. Carminati B., Ferrari E., Access control and privacy in web-based social networks // *International Journal of Web Information Systems* 2008, Vol. 4 Issue: 4, pp.395-415 Prieiga per internetą: http://www.emeraldinsight.com/1744-0084.htm [žiūrėta 2017 09 14]
10. Castells M. *The Information Age Economy, Society, and Culture Volume I The Rise of the Network Society* – Oxford, UK, Blackwell, 2010 ISBN 978-1-4051-9686-4
11. Cryptagram: photo privacy for online social media / *COSN '13 Proceedings of the first ACM conference on Online social networks Matt Tierney* // Boston, Massachusetts, USA 2013 10 7-8 p. 75-88
12. Dagienė V. ir kt, *Enciklopedinis kompiuterijos žodynas* – Vilnius : TEV, 2008
13. Debatin B. el al. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences // *Journal of Computer - Mediated Comunication*, 2009 Volume15, p. 83-108
14. Dench S.,at al An EU Code of Ethics for Socio-Economic Reasearch // *The Institute for Employment Studies* 2004, p. 55- 76

15. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo // Prieiga per internetą: http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679 [Žiūrėta 2017 12 17]
16. Facebook Cambridge Analytica Scandal // Fortune 2018 04 Prieiga per internetą: http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/ [žiūrėta 2018-04-28]
17. Facebook over Tor, including the Facebook Onion Site Prieiga per internetą: https://www.facebook.com/ facebookcorewwwi/ [žiūrėta 2018-05-22]
18. *Facebook* paslaugų teikimo sąlygos Prieiga per internetą: https://www.facebook.com/legal /terms/update
19. *Facebook* privatumo ir duomenų politika Prieiga per internetą: https://www.facebook.com/ about/privacy
20. *Facebook* socialinio tinklo saugumas // NKSC prie KAM Informacinis biuletenis 2018 m. balandžio 9 d.
21. Gaižauskaitė I., Mikienė S., *Socialinių tyrimų metodai: Apklausa*. – MRU, Vilnius 2014
22. Grimmelmann. J, Saving Facebook // *NYLS Legal Studies Research Paper No. 08/09-7*; Iowa Law Review, 2009, vol. 94, p. 1137.
23. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data // Organisation for Economic Co-operation and Developmen (OECD) Prieiga per internetą: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflow sofpersonaldata.htm [žiūrėta2018-03-30]
24. Hughes B.N. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences // *Journal of Computer-Mediated Communication*, 2009 Vol. 15, Issue 1, Pages 83–108 https://academic.oup.com/jcmc/article/15/1/83/4064812 [žiūrėta 2018-07-15]
25. Yellen D. Pioneers of the share economy // *Forbes* 2014 Prieiga per internetą: https://www.forbes.com/pictures/eeji45emgkh/airbnb-snapgoods-and-12-more-pioneers-of-the-share-economy/#119ad44252cf
26. Imties dydžio skaičiuoklė [žiūrėta 2018-06-09] http://www.factus.lt/main-calculator/
27. Imties dydžio skaičiuoklė [žiūrėta 2018-06-09] https://www.surveysystem.com/sscalc.htm
28. InfoCuria – Teisingumo Teismo praktika. Teisingumo teismo (didžioji kolegija) sprendimas. Prieiga per internetą: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=170232 [žiūrėta 2017 12 28]
29. Jiang, Z.J., et. al Research note-privacy concerns and privacy- protective behavior in synchronous online social interactions // *Information Systems Research,* 2013 Vol. 24, p. 579-595

30. Johsson, B. Privacy no longer a social norm, says Facebook founder. // The Guardian 2010 Prieiga per internetą: http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy. [žiūrėta 2018-07-15]

31. Kayes I., Iamnitchi A. Privacy and security in online social networks: A survey // *Online Social Networks and Media*, 2017, Vol. 3–4 p1–21

32. KANTAR TNS Metinės žiniasklaidos tyrimų apžvalgos http://www.tns.lt/lt/top/paslaugos/ziniasklaidos-auditoriju-tyrimai/metine-ziniasklaidos-tyrimu-apzvalga/

33. Kantar TNS“ http://www.tns.lt/lt/top/paslaugos/ziniasklaidos-auditoriju-tyrimai/interneto-auditorijos-tyrimas/duomenys-4/

34. Khandelwal S. Hackers Stole 50 Million Facebook Users' Access Tokens Using Zero-Day Flaw 2018 Prieiga per internetą: https://thehackernews.com/2018/09/facebook-account-hack.html?m=1 [Žiūreta 2018-09-30]

35. Lei Tang L., Liu H. Leveraging social media networks for classification // *Data Mining and Knowledge Discovery* 2011, Volume 23, Issue 3, p 447–478

36. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/XSpzxvEjIg [Žiūrėta 2017 12 17]

37. Lietuvos statistikos departamentas Prieiga per internetą: https://osp.stat.gov.lt/naujienos?articleId=5526623

38. *LinkedIn* paslaugų teikimo sąlygos Prieiga per internetą: https://www.linkedin.com/legal/user-agreement

39. LinkedIn privatumo ir duomenų politika Prieiga per internetą: https://www.linkedin.com/legal/privacy-policy?trk=uno-reg-guest-home-privacy-policy

40. LoveToKnow.com Prieiga per internetą: http://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist [žiūrėta 2018 01 02]

41. McNurlin, B. C., & Sprague, R. H. Jr., *Information systems management in practice* (7thed.) – Prentice-Hall, Inc. Upper Saddle River, NJ, USA 2005 ISBN:0131854712

42. Musiał K., Kazienko P. Social networks on the Internet // *World Wide Web 2013*, Vol. 16, Issue 1, p 31–72 Prieiga per internetą: https://link-springer-com.skaitykla.mruni.eu/article/10.1007/s11280-011-0155-z [žiūrėta 2018 01 03]

43. Nguyen, M., et al Comparing online and offline self-disclosure:a systematic review // *Cyberpsychology, Behavior, and Social Networking*, 2012, Vol. 15 No. 2, pp. 103-111.

44. Peter C. Silicon Valley Is About to Spend a Lot of Time in Court // *Bloomberg.com* 2017 Prieiga per internetą: https://www.bloomberg.com/businessweek [žiūrėta 2018 04 14]

45. Posey, C., et al. Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities // European Journal of Information Systems 2010, Vol. 19 No. 2, p. 181-195.

46. Rathorea S. el. al. Social network security: Issues, challenges, threats, and solutions // *Information Sciences journal* 2017, Vol. 421 p. 43–69

47. Romansky R. Social media and personal data proctetion// *International Journal on Information Technologies & Security*, No 4, 2014

48. Scott, D. Meerman Naujosios rinkodaros ir viešųjų ryšių taisyklės // Verslo žinios – Vilnius 2008

49. Senthil Kumar N., Saravanakumar K.Deepa On Privacy and Security in Social Media – A Comprehensive Study // *Procedia Computer Science Volume* 2016, 78 p. 114-119

50. Symantec, Internet Security Threat Report, Prieiga per internetą: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en. [žiūrėta 2017-12-15]

51. Skarbalienė A. Natūralusis eksperimentas kaip socialinių mokslų pozityvistinio tyrimo strategija. // *Tiltai* - Klaipėdos universitetas, 2017, 2, 89–101 Prieiga per internetą: https://www.researchgate.net/publication/321362206_naturalusis_eksperimentas_kaip_socialiniu_mokslu_pozytivistinio_tyrimo_strategija [žiūrėta 2018-08-10]

52. Skersys G. *Informacijos sauga : mokomoji knyga* – Kaunas, 2011. ISBN: 9786094330766

53. Solove, D. J. A Taxonomy of Privacy. // Law Review University of Pennsylvania, 2006 Vol 154 Prieiga per internetą: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622. [žiūrėta: 2018-04-28]

54. Statista, Number of social media users worldwide from 2010 to 2021 (in billions) Prieiga per internetą: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

55. Stieglitza S., Mirbabaiea M et al., Social media analytics – Challenges in topic discovery, data collection, and data preparation // *International Journal of Information Management*, 2018, Vol. 39 p.156-168

56. Story L., Stonenov B. Facebook Retreats on Online Tracking By / *The New York Times*, 2007 Prieiga per internetą: https://www.nytimes.com/2007/11/30/technology/30face.html

57. Štitilis, D. Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. // Socialinės technologijos 2013, 3(1), 189–207

58. Terminai Prieiga per internetą: https://www.esaugumas.lt/lt/terminai/84

59. Trepte, S. and Reinecke, L. The reciprocal effects of social network site use and the disposition for self-disclosure: a longitudinal study // *Computers in Human Behavior*, 2013, Vol. 29 No. 3, p. 1102-1112

60. *Twitter* paslaugų teikimo sąlygos Prieiga per internetą: https://twitter.com/en/tos

61. *Twitter* privatumo ir duomenų politika Prieiga per internetą: https://twitter.com/en/privacy

62. Wojcik S. et al.Bots in the Twittersphere // *Pew Research Center Internet & Technology* Prieiga per internetą: http://www.pewinternet.org/2018/04/09/bots-in-the-twittersphere/ [žiūrėta 2018-03-30]

63. Wong R. Social Networking: Anybody is a Data Controller. // *Academic Legal Studies*. Nottingham Trent University Nottingham Law School 2008.

64. Zhao J. & Sherry Y. Zhao, Security and Vulnerability Assessment of Social Media Sites: An Exploratory Study //*Journal of Education for Business*, 2015, 90:8, 458-466,

65. Žydžiūnaitė V. *Tyrimo dizainas: struktūra ir strategijos*. Kaunas: Technologija 2007

66. Žitkienė R., Mačerinskienė I. *Magistro baigiamojo darbo rengimo tvarka. Mokomoji knyga* – Vilnius, 2014

Užkurienė B. *Duomenų apsaugos valdymo ypatumai interneto socialiniuose tinkluose* / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas prof. dr. T. Limba. – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir verslo fakultetas, 2018. – 82 p.

SANTRAUKA

Kibernetinio saugumo valdymo magistro baigiamojo darbo tema „Duomenų apsaugos valdymo ypatumai interneto socialiniuose tinkluose“ tema yra aktuali, kadangi sparčiai populiarėja interneto socialiniai tinklai, o vartotojai savo socialinį gyvenimą, kartu su įpročiais, perkelia į internetinę erdvę. Socialinių tinklų vartotojai neįvertina informacijos sklaidos internetinėje erdvėje ir iki galo nesuvokia padidėjusios rizikos duomenų saugumui.

Magistro baigiamajame darbe yra nagrinėjama duomenų saugumo sąvoka, interneto socialinių tinklų samprata, analizuojami socialinių tinklų tipų atvejai. Apžvelgiamos ir palyginamos trijų populiariausių socialinių tinklų paslaugų teikimo ir privatumo taisykles bei identifikuojami pagrindiniai šių tinklų panašumai ir skirtumai. Dviem skirtingais, vienas kitą papildančiais tyrimais, tiriamas socialinių tinklų vartotojų požiūris ir žinios apie duomenų apsaugos valdymo ypatumus interneto socialiniuose tinkluose. Tyrimo objektas – duomenų apsaugos valdymo interneto socialiniuose tinkluose ypatumai. Šio tyrimo tikslas, nustačius duomenų apsaugos valdymo ypatumus interneto socialiniuose tinkluose, pateikti duomenų apsaugą socialiniuose tinkluose didinančias strategines kryptis. Taip pat buvo iškelti uždaviniai: išanalizuoti duomenų apsaugos valdymo interneto socialiniuose tinkluose ypatumus; remiantis atvejų analizės metodu, išanalizuoti pasirinktų interneto socialinių tinklų duomenų valdymą vartotojo ir socialinio tinklo vaidmens aspektu; atlikti tyrimą, kuriuo, pasitelkiant gautus duomenis, galima išsiaiškinti vartotojų požiūrį ir žinias apie duomenų apsaugą interneto socialiniuose tinkluose. Tyrimo metu buvo iškelta pagrindinė hipotezė: vartotojai, duomenų apsaugos valdyme interneto socialiniuose tinkluose yra silpniausia grandis, todėl kyla grėsmė, kad išnaudojant žmogiškąjį faktorių per socialinės inžinerijos atakas, taps kibernetinių atakų taikiniu. Atlikus eksperimentą ir socialinių tinklų vartotojų anketinę apklausą, buvo patvirtinta ši hipotezė, t.y., tiek eksperimento, tiek apklausos rezultatai parodė, kad vartotojai neišmano ar neįsigilina į teikiamas naudojamų socialinių tinklų saugumo rekomendacijas ir pilnai neišnaudoja visų įmanomų priemonių duomenų apsaugai interneto socialiniuose tinkluose.

Atlikti tyrimai leidžia identifikuoti silpniausias duomenų valdymo dalis ir padės pagerinti pasirinktą duomenų apsaugos metodą. Magistro baigiamojo darbo pabaigoje pateikiamos išvados bei siūlymai socialinių tinklų vartotojų duomenų apsaugai.

Užkurienė B. *Specifics of Data Protection Management in Internet Social Networks* / Master's work in Cyber Security Management. Supervisor prof. dr. T. Limba. – Vilnius: Faculty of economics and business, Mykolas Romeris University, 2018. – 82 p.

SUMMARY

Cyber security management master thesis on „Specifics of Data Protection Management in Internet Social Networks" is actual because people moves their social life including habits to fast growing internet social networks. Usually social network users do not fully understand the increased risk of data security.

The master thesis examines the concept of data security, the concept of Internet social networks, analyzes cases of social network types. There are reviewed and compared the service rules and privacy policy of the three most popular social network service providers and identified the key similarities and differences between these networks. Two different, complementary research studies examine the attitudes of social networking users and knowledge of data protection management on the Internet social networks. The object of the research is the specifics of data protection management in Internet social networks. The aim of this study, with the identification of the specifics of data protection management on the Internet social networks, is to provide strategic directions which increase the data protection in social networks. The following challenges were also raised: analyze the specifics of data protection management in Internet social networks; analyze the management of selected online social networking data in the aspect of the role of the user and the social network, based on the case analysis method; with the help of the obtained data, carry out the study to discover consumer attitudes and knowledge about data protection in the Internet social networks. The main hypothesis of the study was following: users are the weakest chain in the management of data protection on social networking sites in the Internet, so there is a danger that using the human factor through social engineering attacks will become the target of cyber attacks. The hypothesis was confirmed by an experiment and a questionnaire survey of social network users. Both the experiment and the survey showed that users do not know or do not get used to the safety recommendations of the social networks they use and do not fully use all possibilities of data protection in the social networks of the Internet.

Researches identifies the weakest parts of data management and will help to improve the selected data protection method. At the end of the Master's thesis there are given conclusions and recommendations for data protection of social network users.

PRIEDAI

1 Priedas. Tyrime panaudota anketa

Sveiki,

esu Mykolo Romerio Universiteto, Ekonomikos ir verslo fakulteto šešto kurso studentė. Atlieku apklausą apie vartotojų požiūrį į duomenų apsaugą socialiniuose tinkluose ir kviečiu Jūs prisidėti prie mano magistrinio baigiamojo darbo.

Labai prašau Jūsų skirti porą minučių ir atsakyti į klausimus.

Iš anksto ačiū!

Šios anketos rezultatai viešai nepublikuojami

Iš kokio miesto esate?

Jūsų amžius?

- 13 - 18 m.
- 19 - 29 m.
- 30 - 39 m.
- 40 - 49 m.
- > 50 m.

Jūsų lytis?

- Moteris
- Vyras

Kurio socialinio tinklo vartotojas esate? (galimi keli variantai)

- Facebook

- [ ] LinkedIn
- [ ] Google+
- [ ] Twitter
- [ ] Instagram
- [ ] Flickr
- [ ] Pinterest
- [ ] Tumblr
- [ ] VK
- [ ]

Socialiniais tinklais naudojatės:

- [ ] Bendravimui su draugais.
- [ ] Savęs realizavimui.
- [ ] Naujienų sekimui.
- [ ] Savo žinomumo populiarinimui.
- [ ] Jūsų paslaugų / prekių žinomumui didinti.
- [ ] Bendravimui su sekėjais / gerbėjais.

Kiek laiko esate socialinio tinklo vartotojas?

- ( ) Mažiau nei metai.
- ( ) Daugiau nei metai.
- ( ) Daugiau nei du metai.
- ( ) Daugiau nei trys metai.

Kaip dažnai naudojatės/prisijungiate prie socialinio tinklo?

- Kartą / kelis per mėnesį.
- Kelis kartus per savaitę.
- Kasdien.
- Daugiau nei 3 kartus per dieną.

Kiek vidutiniškai laiko praleidžiate prisijungęs prie socialinio tinklo?

- ~ 15 min.
- ~ 30 min.
- ~ 1 val.
- Daugiau nei 1 valandą.
- Daugiau nei 3 valandas.

Pažymėkite kokią informaciją apie sava viešai pateikiate socialiniame tinkle esančioje Jūsų paskyroje:

- Vardas.
- Pavardė.
- Elektroninis paštas.
- Telefono numeris.
- Namų adresas.
- Lytis.
- Orientacija.
- Santykių statusas.

- [ ] Draugų sąrašas.
- [ ] Šeimos nariai / giminaičiai.
- [ ] Išsilavinimas.
- [ ] Mokslo įstaiga.
- [ ] Darbovietė.
- [ ] Pareigos.
- [ ] Pomėgiai.

Kieno kvietimus draugauti priimate socialiniame tinkle?

- ○ Tik žmonių, kuriuos pažįstate asmeniškai.
- ○ Iš bendrų pažįstamų.
- ○ Iš visų.

Pažymėkite Jums tinkantį atsakymo variantą (taip arba ne):

	Taip.	Ne.
Ar esate susipažinę su socialinių tinklų paslaugų teikimo sąlygomis?	○	○
Ar esate susipažinę su socialinių tinklų pateikiamomis privatumo taisyklėmis?	○	○
Ar naudojate privatumo nustatymus, kad apsaugotumėte Jūsų paskyroje esančią informaciją?	○	○
Ar manote, kad naudojantis socialiniais tinklais, gali kilti grėsmė Jūsų privatumui?	○	○
Ar manote, kad socialiniai tinklai laikosi skelbiamos privatumo politikos?	○	○
Ar manote, kad socialiniai tinklai pažeidžia Jūsų privatumą bendradarbiaudama su trečiosiomis šalimis (reklaminės akcijos ir pan.)?	○	○

Kaip dažnai keičiate privatumo nustatymus?

- Kartą per savaitę.
- Kartą mėnesį.
- Kartą per pusmetį.
- Kartą per metus.
- Nekeičiate.

Kas mato Jūsų paskyroje pateiktus duomenis?

- Nežinau.
- Visi vartotojai.
- Draugų draugai.
- Draugai.
- Esate nustatę skirtingus informacijos matomumo nustatymus, skirtingiems vartotojams.

Kada tvarkėte / keitėte privatumo nustatymus savo paskyroje?

- Netvarkiau / nekeičiau.
- Iš karto užsiregistravus socialiniame tinkle.
- Po to kai susipažinote su privatumo taisyklėmis.
- Kai rekomendavo draugai / giminaičiai.
- Kai manėte, kad į Jūsų paskyrą buvo bandyta įsilaužti.
- Po naujai įsigaliojusio ES bendrojo duomenų apsaugos reglamento (BDAR).