KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Žygimantas Kaupas

KONFIDENCIALIOS INFORMACIJOS RINKIMAS NAUDOJANT GALUTINIO VARTOTOJO LICENCIJOS SUTARTĮ

Baigiamasis magistro darbas

Vadovas
doc. dr. Jonas Čeponis

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

KONFIDENCIALIOS INFORMACIJOS RINKIMAS NAUDOJANT GALUTINIO VARTOTOJO LICENCIJOS SUTARTĮ

Baigiamasis magistro darbas
Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Doc. dr. Jonas Čeponis
(data)

Recenzentas
(parašas) Dr. Ignas Martišius
(data)

Projektą atliko
(parašas) Žygimantas Kaupas
(data)

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos fakultetas

(Fakultetas)

Žygimantas Kaupas

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga, 621E10003

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Konfidencialios informacijos rinkimas naudojant galutinio vartotojo licencijos sutartį“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 17 m. gegužės 22 d.

Kaunas

Patvirtinu, kad mano **Žygimanto Kaupo** baigiamasis projektas tema „Konfidencialios informacijos rinkimas naudojant galutinio vartotojo licencijos sutartį“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka)	*(parašas)*

Kaupas, Ž. „Konfidencialios informacijos rinkimas naudojant galutinio vartotojo licencijos sutartį“. Magistro baigiamasis projektas / vadovas doc. dr. Jonas Čeponis; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra.

Kaunas, 2017. 73 psl.

SANTRAUKA

Didėjant interneto naudotojų skaičiui bei daugėjant prie globalaus tinklo prijungiamų įrenginių kiekiui, sparčiai didėja ir programinės įrangos apimtys. Ji dažniausiai yra prieinama tik tuomet, kai vartotojas sutinka su jų kūrėjų nustatytomis sąlygomis. Galutinio vartotojo licencijos sutartis, geriau žinoma EULA akronimu, yra teisinis kontraktas tarp programinės įrangos kūrėjo ar platintojo ir galutinio šios įrangos naudotojo. Nors šis dokumentas buvo kuriamas norint apsaugoti autorines teises, tačiau šiandien EULA yra naudojama ir ribojant vartotojų pasirinkimo bei žodžio laisvę, išgaunant asmeninius duomenis ar įdiegiant kenkėjiškas programas.

Vartotojas gali sutikti su EULA sąlygomis įvairiais būdais – tiek paspausdamas „sutinku“ mygtuką programos įdiegimo metu, tiek atidarydamas programinės įrangos pakuote ar tiesiog ja naudodamasis (kartais ir pats nežinodamas apie duotą sutikimą). Vieni iš pagrindinių ir dažniausiai pabrėžiamų kritikos objektų yra EULA apimtis ir sudėtinga teisinė terminologija. Juridinis galutinio vartotojo licencijos sutarties aspektas kompiuterinių sistemų saugumui Lietuvoje nėra išsamiai išnagrinėtas. Nors dažnai EULA teksto pradžioje yra akcentuojama, kad tai – svarbus teisinis dokumentas, tačiau didesnio dėmesio jis nesulaukia tiek tarp akademinės bendruomenės narių, tiek ir viešajame diskurse. Tiek LR elektroninių ryšių įstatyme, tiek ir LR Asmens duomenų teisinės apsaugos įstatyme duomenų subjekto sutikimas rinkti jo asmeninius duomenys yra legalus juridinis pagrindas.

Vartotojo sistemos stebėsena, nuosavybės teisė į asmeninį turinį, atsakomybės už netinkamą programinės įrangos veikimą apribojimas - tai tik dalis praktikoje sutinkamų EULA sąlygų, kurios sukuria saugumo spragas vartotojo sistemoje arba pažeidžia informacijos konfidencialumo principą. Informacinių technologijų specialistų atliktų EULA akademinių tyrimų yra labai mažai. Taip pat galutinio vartotojo licencijos sutarties tekstą analizuojančių programinių sprendimų, kurie automatizuotų šį procesą bei pateiktų vartotojui peržiūrėti ir įvertinti tik galimai pavojingų sąlygų santrauką yra vos keletas. Nors ir nebeatnaujinamas „EULAyzer“ analizatorius yra tiksliausias ir patogiausias naudojimui šiuo metu rinkoje esantis produktas.

Interneto naudotojų pasitikėjimo galutinio vartotojo licencijos sutartimi tyrimui pasirinktas dažniausiai praktikoje naudojamas sutikimo su EULA sąlygomis būdas - specialus EULA dialogo langas programos įdiegimo metu. Siekiant gauti kuo tikslesnius duomenis, tiriamųjų imtis buvo fiksuota – 2016 metais į KTU bakalauro studijas Informatikos fakultete priimtų pirmo kurso studentų skaičius (653). Jiems buvo siūloma pasinaudoti testavimo platforma su pasirengiamaisiais Informacinių technologijų modulio egzamino klausimais. Iš visų tyrimo dalyvių, sutikusių su galutinio

vartotojo licencijos sutarties sąlygomis, paimama asmeninio įrenginio informacija – pastoviosios atminties dydis ir jame likusios laisvos vietos duomenys, tuo parodant galimą prieigą prie sisteminių resursų bei procesų.

EULA sutarties tekstas buvo pateiktas lietuvių kalba - tai tyrimo atlikimo metu vis dar nėra dažnai praktikoje sutinkamas atvejis. Taip pat įtrauktos daugiausiai kritikos sulaukiančios savybės: EULA ilgis (apie 3000 žodžių), sudėtinga teisinė kalba, programinės įrangos kūrėjo atsakomybės ribojimas ir kita. Sutarties tekste informuojama, kad asmeniniai duomenys iš vartotojo bus renkami be detalesnio pagrindimo, kodėl jų reikia ir kam jie bus naudojami. Taip pat įterpta nuoroda į pagalbinį puslapį, kuriame randama alternatyvi prieiga prie programos siūlomų resursų, išvengiant „kenksmingo“ programinio kodo paleidimo asmeninėje sistemoje.

Programinė įranga, reikalinga tyrimo tikslams pasiekti, sukurta naudojantis Java programavimo kalba. Testavimo programa parengta tiek asmeniniams „Windows“ kompiuteriams, tiek ir mobiliems „Android“ įrenginiams. Jose interaktyviai pateikti KTU bakalauro studijų Informatikos fakulteto Informacinių technologijų kurso egzamino pasirengiamieji klausimai. Studentai norėdami pasiekti pilną klausimų sąrašą turėjo arba įsidiegti programą, sutikti su specifiškai sumodeliuotomis žalingomis EULA sąlygomis, atsakyti bent 5 iš 10 klausimų teisingai ir taip gauti nuorodą į pageidaujamą resursą, arba perskaitę EULĄ tekstą pasiekti tą patį resursą per unikalią nuorodą jame. Programinė įranga išplatinta per fiktyvų internetinį puslapį. Tiriamiesiems tikslios nuorodos, kur galima atsisiųsti šias programas, pateiktos elektroniniame laiške iš kurso dėstytojo pašto dėžutės. Nors šiuo atveju siuntėjas ir nėra suklastotas (tokia galimybė praktikoje egzistuoja), vis dėlto tikrinama ar gavę laišką su įtartinomis nuorodomis tiriamieji jas vis vien aplankys.

Interneto vartotojų patiklumo EULA sutartimi eksperimentinis tyrimas buvo pradėtas 2016 m. gruodžio 5 d. Eksperimentui buvo skiriamos dvi savaitės po kurių tiriamieji buvo supažindinti su jo metodologija bei preliminariais rezultatais. „Windows“ operacinei sistemai skirtos eksperimentinės programos versijos įdiegimo failas buvo atsiųstas 245 kartus, testas išlaikytas 130 kartų bei gauta informacija apie 103 įrenginių kietųjų diskų duomenis. Atsižvelgiant į tai, kad šios paprastos programinės įrangos atveju beveik 80% įrenginių ne tik be kliūčių įvykdė kenksmingą kodą, bet ir vartotojui to nežinant išsiuntė duomenis į išorę, realu prognozuoti, jog profesionalaus įsilaužėlio parašytas kodas gali pasiekti efektyvumą artimą 100%.

„Android“ operacinei sistemai skirtos aplikacijos rezultatai nedaug skiriasi nuo jau analizuotos „Windows“ versijos. Programa buvo atsisiųsta 155 kartus, testas išlaikytas 73 kartus bei gauti duomenys iš 50 įrenginių. Tikėtina, kad mažesnis populiarumas buvo dėl to, kad dalis studentų atsisiuntė „Android“ programą tik norėdami pažiūrėti skirtumus su „Windows“ versija. Visais atvejais nė vienas programėlės naudotojas neperskaitė galutinio vartotojo licencijos sutarties ir neaplankė joje paminėtos nuorodos į papildomą resursą.

Eksperimentas atskleidė ir daugiau aktualių informacijos ir informacinių technologijų saugos problemų. Atliekant šios kenkėjiškos programinės įrangos kūrimo bei testavimo veiksmus buvo pastebėti itin neprognozuojami antivirusinių programų sprendimai jos įdiegimo ar duomenų išsiuntimo į išorę atžvilgiu: vienu atveju programos veikimas nebūdavo blokuodamas, kartais vartotojas gaudavo įspėjamąjį pranešimą. Tuo tarpu „Avast“ antivirusinė programa prie be savininko žinios siunčiamo elektroninio laiško su jo privačiais duomenimis pabaigoje pridėdavo tekstą „---Šis elektroninis laiškas buvo patikrintas nuo virusų „Avast“ antivirusine programa“.

Išanalizavus gautą informaciją apie kietųjų diskų duomenis, matoma, jog „Quizza“ programa nė karto nebuvo įdiegta į nuo pagrindinės sistemos atribotą virtualią mašiną. Nepaisant to, kad šis sprendimas yra vis dažniau naudojamas komercinėje veikloje, individualūs vartotojai jo teikiamais privalumais (ypač IT saugos srityje) vis dar nėra linkę naudotis. Dažnas vartotojas dirbdamas kompiuteriu turi prisijungęs bent vieną USB atmintinę, kuri yra potenciali kenkėjiško kodo platinimo aplinka, ypač jei kartais ji yra prijungiama prie neapsaugotų, viešai prieinamų ar jau užkrėstų kompiuterių.

Net ir paviešinus eksperimento tikslus bei metodiką programos naudojimas nesustojo ir vis dar buvo gaunami nauji duomenys iš sistemų į kurias „Quizza“ programa buvo įrašyta po gruodžio 20 d. Nėra aišku ar šiuos asmenis nepasiekė informacija apie atliekamą eksperimentą, ar jie net žinodami, jog buvo apgauti vieną kartą, vis vien nusprendė išbandyti viską savo sistemoje. Tarp visų tiriamųjų vienam studentui informacijos apie „Quizza“ programą išplatinimo metodas pasirodė įtartinas. Nors jis ir neperskaitė EULA sąlygų bei nepasiekė norimo failo alternatyviu būdų, tačiau, kaip pats teigė, programos į savo kompiuterį neįdiegė bei nuorodos, gautos teisingai išsprendus testavimo klausimus, iš kolegų neprašė.

Kaupas, Žygimantas. End-User License Agreement as a Tool to Gather Confidential Information. Master‘s thesis in Informatics Engineering / supervisor doc. dr. Jonas Čeponis. The Faculty of Informatics, Kaunas University of Technology.

Research area and field: Information and Information Technology Security

Key words: end-user license agreement, EULA, acceptance without reading

Kaunas, 2017. 73 p.

SUMMARY

As more and more data is stored online and the number of internet users is constantly increasing, creators of malicious software are persistently looking for some innovative ways to acquire valuable confidential information. When recent malware, spyware, ransomware and other digital attacks were disclosed publicly and attracted a lot of attention, common trust in online information decreased notably. It is a commendable general practice to use an antivirus solution, do not open suspicious links or give your confidential data to an untrusted source. However, one attack vector is often forgotten.

Digital world is no longer imaginable without countless number of various software. Almost all of it asks the user to accept the end-user license agreement (EULA) before the start of an installation process. Following part is frequently overlooked by most of the users, even though real security threats might be hidden there. This work analyses the concept of EULA and its drawbacks. Users trust in the information found online is tested with a software, which is made for this experiment and has a specifically designed EULA text. Obtained results enable identification of the problem scope and propose actions, which could help in closing this security gap.

EULA is a legal contract between a software application author or publisher and the user of that application. It is often criticized because of its length (on average, it reaches 3000 words) and difficult legal terminology. Even well-known companies use EULA with potentially harmful terms for the end-user. It is still a shortage of court decisions related to the discussed document not only in Lithuania, but also in the EU, however in the US, statistics are in favor of EULA and some widely-publicized trials ended in supporting this document and thus strengthened its legal power even more. Only few researches could be found regarding this document and its impact to confidential information or IT infrastructure. Also, there are just a few solutions to evaluate and automatically guard yourself against potential threats written in EULA.

The experiment of users trust in EULA was performed at the end of 2016. 653 first year students of Informatics faculty of Kaunas University of Technology were selected for this investigation. Experiment was carried out in the form of knowledge testing application for a specific university course. When user wanted to install the testing application on either Windows operating

system machine or Android mobile device, it prompted the EULA to be accepted otherwise installation will be canceled. If users accepted the specifically modified EULA document, the installed software not only performed expected and visible functions, but also collected and sent some data from the machine it was running in.

Specific EULA text was developed for this experiment that mimic the standard agreement as close as possible, but also has multiple statements indicating its unusual purpose. In addition, applications for Windows and Android operating systems for the testing program “Quizza” were created. Together with expected functionality both solutions used standard Java libraries to collect information about memory devices and third party email client Gmail to send data to the mailbox prepared for this experiment. Also, a bogus website quizza.tk was created as a distribution environment for these applications. Each link visit in that website was monitored and later analyzed as a part of the experiment results.

The conducted experiment confirmed that users tend to skip the EULA and agree with any text written in it. Nobody has read this license agreement and thus shared their confidential data with the author. In addition, this experiment showed more alarming IT security trends. More than 60% of data received came within the first 24 hours from the start of the experiment. This tendency favors zero-day exploits or new fraud schemas and as it was visible no home antivirus solutions provide sufficient protection against data theft. Also, home users do not benefit by virtualization technology to increase their systems security and in many instances connected external USB flash drives were detected when user installed this untrusted application thus allowing easy spread of the malware.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

BBC (angl., *British Broadcasting Corporation*)	–	Britų transliavimo agentūra
BYOD (angl., *bring-your-own-device*)	–	naudokis savo prietaisu
DDoS (angl., *Distributed Denial of Service*)	–	paskirstyta atkirtimo nuo paslaugos ataka
DoS (angl., *Denial of Service*)	–	atkirtimo nuo paslaugos ataka
ES	–	Europos Sąjunga
EULA (angl., *End-User License Agreement*)	–	galutinio vartotojo licencijos sutartis
GB	–	gigabaitai
Gbps	–	gigabitai per sekundę
IoT (angl., *Internet of Things*)	–	daiktų internetas
IT	–	informacinės technologijos
JAV (angl., *USA - United States of Amerika*)	–	Jungtinės Amerikos Valstijos
KTU	–	Kauno technologijos universitetas
LR	–	Lietuvos Respublika
MAC (angl. *Media Access Control*)	–	unikalus 12 simbolių tinklo įrenginio adresas
RAT (angl., *Remote Access Trojan*)	–	nuotolinės prieigos Trojos arklio programa
RRT	–	Lietuvos Respublikos ryšių reguliavimo tarnyba
VPN (angl., *virtual private network*)	–	virtualus privatus tinklas
www (angl. *World Wide Web*)	–	pasaulinis tinklas

ĮVADAS

Informacinių technologijų plėtra šiandien yra neatsiejama nuo nuolatos didėjančio programinės įrangos kiekio. Dauguma (net ir nemokamų) programų ar elektroninės paslaugų yra prieinamos tik tuomet, kai vartotojas sutinka su jų kūrėjų nustatytomis sąlygomis – galutine vartotojo licencijos sutartimi (geriau žinoma EULA akronimu). Nors vis įtariau yra vertinama internete randama informacija, žmonės norėdami naudotis siūlomais resursais nedvejodami pritaria su šio dokumento tekstui.

Šiame darbe analizuojama galimybė rinkti vartotojo konfidencialią informaciją pasinaudojant EULA tekstu. Visų pirma šiam tikslui pasiekti yra detaliai išnagrinėjama EULA koncepcija ir įvertinamos dažniausiai praktikoje sutinkamos potencialiai kenkėjiškos sąlygos. Remiantis jomis yra parengiama specifinė licencijos sutarties versija lietuvių kalba, kuri leistų patikrinti, ar tiriamieji skaito jiems pateikiamą dokumento tekstą.

Siekiant pabrėžti analizuojamos problematikos svarbą informacijos saugumui, sukuriama ir išplatinama programinė įranga tiek asmeniniams „Windows“ kompiuteriams, tiek ir mobiliesiems „Android“ įrenginiams, kuri lygiagrečiai matomo funkcionalumo turi ir paslėptą konfidencialių duomenų rinkimo galimybę. Būtent vartotojo sprendimas dėl EULA perskaitymo nulemia, ar jo asmeninės sistemos saugumas nėra pažeidžiamas.

Tyrimo metu gautų rezultatų analizė atskleidžia šio kenkėjiško informacijos rinkimo vektoriaus efektyvumą. Taip pat identifikuoja vartotojų elgesio niuansus, kurie gali būti išnaudojami, siekiant pažeisti jo sistemos apsaugą arba pasisavinti konfidencialius duomenis. Gauti rezultatai leidžia identifikuoti šios informacijos saugos problemos apimtį ir pasiūlyti veiksmus, kaip sumažinti galimybę vartotojui pačiam įsirašyti kenkėjišką programinę įrangą į savo asmeninį įrenginį.

Darbo problematika ir aktualumas

Problematika. Pasitikėjimas internete randamais ištekliais neatsižvelgiant į galimas pasekmes informacijos ir informacinių technologijų saugumui. Įpratimas sutikti su pateikiamomis EULA sąlygomis jų neperskaičius.

Aktualumas. Skaitmeniniame formate saugomos informacijos kiekiui nuolat augant, įvairiais techniniais metodais siekiama kuo geriau užtikrinti jos konfidencialumą. Vis dėlto, dažnai ignoruojama situacija, kai vartotojas, sutikdamas su jam pateikiamomis EULA sąlygomis, pats to nežinodamas neprieštarauja dalintis savo privačia informacija su trečiąja

šalimi. Darbe analizuojama licencijos sutartis yra legalus informacijos rinkimo pagrindimas, todėl tikėtina, kad jos panaudojimas vartotojui nepriimtinais tikslais netolimoje ateityje išaugs.

Darbo tikslas ir uždaviniai

Magistrinio darbo tikslas – ištirti vartotojų pasitikėjimą internete randama informacija ir išanalizuoti jos galimas neigiamas pasekmes informacijos ir informacinių sistemų saugumui.

Tyrimo uždaviniai:

- Išanalizuoti EULA tipus, įvertinti dokumento kritiką, teisinę galią ir praktikoje naudojamus kenkėjiško pobūdžio punktus. Taip pat išnagrinėti pagrindines grėsmes su kuriomis susiduriama naudojantis internete randamais ištekliais, atliktus EULA tyrimus bei esamus programinius sprendimus;
- Paruošti sistemą (asmeniniams „Windows“ kompiuteriams ir mobiliesiems „Android“ įrenginiams), kuri suteiktų prieigą prie turinio tik sutikus su specifiškai sumodeliuotomis EULA taisyklėmis;
- Išplatinti sistemą pirmo kurso Informatikos fakulteto studentų tarpe, siekiant pritraukti kuo didesnę vartotojų auditoriją;
- Išanalizuoti gautus rezultatus, įvertinant aukštą kompiuterinį raštingumą turinčių žmonių veiksmus informacijos ir informacinių technologijų saugos kontekste.

Darbo rezultatai ir jų svarba

Tyrimo metu sukurta programinė įranga, leidžianti įvertinti, ar kompiuterių naudotojai pasitiki internete gaunama informacija ir prieš įdiegdami nepatikimą programinę įrangą į savo asmeninę sistemą perskaito EULA sąlygas.

Tyrimo rezultatai atskleidžia tipinius vartotojų veiksmus susidūrus su nepatikrinta informacija internete ir jų galimas neigiamas pasekmes informacijos ir informacinių sistemų saugai. Taip pat tyrimu siekiama padidinti interneto naudotojų kibernetinio saugumo žinias ir tokiu būdų sustiprinti jų asmeninių sistemų bei konfidencialios informacijos saugumą.

Darbo struktūra

1) Probleminės srities analizės dalyje išnagrinėta galutinio vartotojo licencijos sutarties koncepcija. Įvertinami būdai vartotojui sutikti su pateikiamo dokumento sąlygomis bei išskiriamos daugiausiai kritikuojamos sutarties savybės. Taip pat šioje dalyje trumpai pristatoma teisinė dokumento reikšmė bei pateikiami pavyzdžiai, kaip programinės įrangos gamintojai jį išnaudoja savo naudai. Pabaigoje supažindinama su atliktais EULA tyrimais ir esamais programiniais

sprendimais, kurie padeda vartotojui įvertinti šios sutarties grėsmę jo sistemos ar informacijos saugumui.

2) Tyrimo projekto dalyje pristatomas ir pagrindžiamas tyrimo aplinkos ir renkamų duomenų pasirinkimas. Taip pat, atsižvelgiant į analitinėje dalyje pristatytą problematiką, parengiama specifinė galutinio vartotojo licencijos sutartis lietuvių kalba. Paruošiamas programos asmeniniams „Windows“ kompiuteriams ir mobiliesiems įrenginiams, naudojantiems „Android“ operacinę sistemą, projektai. Pristatoma, kaip sumodeliuota EULA bus integruojama į sukurtą programinę įrangą.
3) Sistemos realizavimo dalyje pateikiami detalūs sukurtos programinės įrangos realizacijos modeliai. Išskiriamas paslėpto kenkėjiško funkcionalumo, kuris aktyvuojamas tik vartotojui sutiktus su EULA sąlygomis, integravimas į programų architektūrą bei šiam funcionalumai pasiekti naudojamos programinės priemonės. Taip pat pristatoma tyrimo įrankių išplatinimo aplinka – sukurtas fiktyvus programinės įrangos internetinis puslapis.
4) Eksperimentinio tyrimo dalyje nagrinėjama tyrimo vykdymo eiga bei atliekama gautų rezultatų analizė. Tyrimas apibendrinamas atsižvelgiant į informacijos ir informacinių technologijų saugos problematiką. Įvertinama kaip kenkėjiškų tikslų turintis veikėjas ar programinė įranga gali pasinaudoti tyrimo metu pasireiškusiais vartotojo elgesio ypatumais.

1. GALUTINIO VARTOTOJO LICENCIJOS SUTARTIES ANALIZĖ INFORMACIJOS SAUGOS KONTEKSTE

„Didžiausias melas internete – „Aš perskaičiau ir sutinku su terminais ir sąlygomis“
– Terms of Service; Didn’t Read Project [1]

1.1. Vartotojų pasitikėjimas internete randama informacija

2015 metų pabaigoje internetu naudojosi 3 366 261 156 žmonės [2]. Nors šis skaičius palyginti su 2000 metais išaugo net 832,5 %, tačiau jis vis dar nesiekia pusės viso pasaulio gyventojų (46,4 %). Atsižvelgiant į pastarųjų metų tendencijas, prognozuojama, kad interneto naudotojų skaičius sparčiai augs ir artimiausioje ateityje, kartu didindamas ir informacijos bei paslaugų kiekį globaliame tinkle. Tuo siekia pasinaudoti kenkėjiškos programinės įrangos kūrėjai, kurie nuolatos ieško būdų, kaip iš įvairių sistemų išgauti kuo daugiau svarbios konfidencialios informacijos.

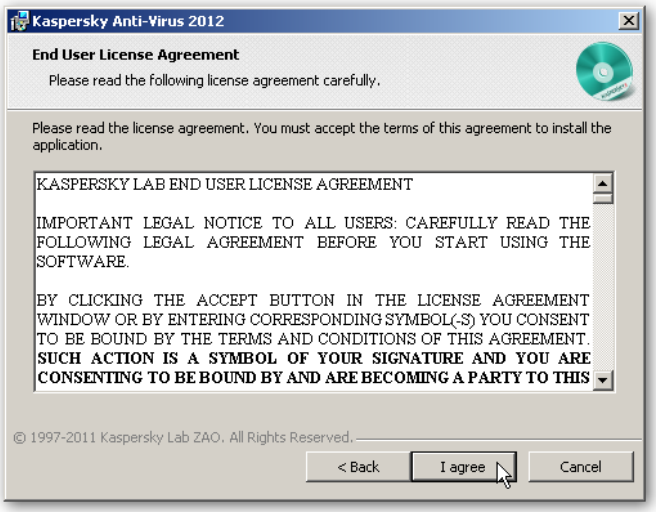
Informacinių technologijų plėtra lemia nuolatos didėjantį programinės įrangos skaičių. IoT vizija, kuri dar prieš porą dešimtmečių buvo tik fantastinių kūrinių siužetuose, šiandien yra suvokiama kaip artimiausias išmaniųjų technologijų žingsnis pirmyn. Vis daugiau kiekvieną dieną naudojamų įrenginių yra prijungiami prie interneto, turi konfigūruojamą programinę įrangą ir suteikia vartotojui didelę veiksmų laisvę. Tačiau beveik visos (net ir nemokamos) programos ar elektroninės paslaugos yra prieinamos tik tuomet, kai vartotojas sutinka su jų kūrėjų nustatytomis sąlygomis.

Šiandien informacijos, patarimų, pramogų, prekių ar paslaugų paieškos dažniausiai atliekamos internete, kur tarp didelio informacijos kiekio vartotojas turi atsirinkti jam aktualius ir naudingus duomenis. Nors paviešinti šnipinėjimo atvejai, kenkėjiškos programinės įrangos paplitimas bei dažnos apgavystės daro neigiamą poveikį žmonių pasitikėjimui internete randama informacija, tačiau modernios visuomenės tendencijos neleidžia išvengti nuolatinio kontakto su naujais duomenimis, programomis ar procesais. Siekdami apsisaugoti nuo galimos žalos vartotojai taiko įvairius informacijos saugos sprendimus ir rekomendacijas: naudoja antivirusines programas, neatidaro įtartinų nuorodų, nepateikia savo asmeninių duomenų, kai tam nėra būtinybės. Vis dėlto, net ir nepasitikėdami didžiąja dalimi internete randamos informacijos, žmonės įdiegdami programinę įrangą ar pradėdami naudotis elektroninėmis paslaugomis nedvejodami sutinka su galutinio vartotojo licencijos sutarties tekstu.

1.2. EULA naudojimas ir kritika

Galutinio vartotojo licencijos sutartis, geriau žinoma EULA akronimu, yra teisinis kontraktas tarp programinės įrangos kūrėjo ar platintojo ir galutinio šios įrangos vartotojo [3]. Šis elektroninis dokumentas išpopuliarėjo XX amžiaus 9-tojo dešimtmečio viduryje kaip programinės įrangos kūrėjų įrankis, siekiant apsisaugoti nuo jų produktų kopijavimo, klonavimo (pasitelkus atvirkštinę inžineriją į rinką paleisti konkurencingus produktus) ir atsakomybės, kai dėl nenumatytų programos klaidų klientai patirdavo didelių nuostolių [4]. Kaip bus matoma kitose šio skyriaus dalyse, šiandien EULA koncepcija neapsiriboja vien tik tiesioginiu programinės įrangos apsaugojimu ar apsidraudimu nuo galimų teisminių procesų, tačiau yra naudojama ir ribojant vartotojų pasirinkimo bei žodžio laisvę, išgaunant asmeninius duomenis ar įdiegiant kenkėjiškas programas.

Egzistuoja įvairūs variantai, kaip vartotojas gali sutikti (kartais ir pats to nežinodamas) su EULA sąlygomis. Populiariausias būdas, kuris bus naudojamas ir šio darbo eksperimentinėje dalyje – paspaudimas „sutinku“ mygtuko programos įdiegimo ar paslaugų naudojimo pradžios metu. Kaip matoma iš 1.1 pav. pateikto pavyzdžio, vartotojui pateikiamas pasirinkimas arba sutikti su programinės įrangos kūrėjo sąlygomis, arba nutraukti pradėtą diegimą. Atsižvelgiant į tai, kad licencijos tekstas būna pateiktas sudėtinga teisine kalba, didelė jo dalis parašyta didžiosiomis raidėmis (nepatogu skaityti), o vidutinė apimtis siekia beveik 3000 žodžių (tai atitinka 11 puslapių teksto su dvigubais tarpais tarp eilučių), vieša paslaptis, jog tik itin retais atvejais naudotojas perskaito visas EULA sąlygas [5].



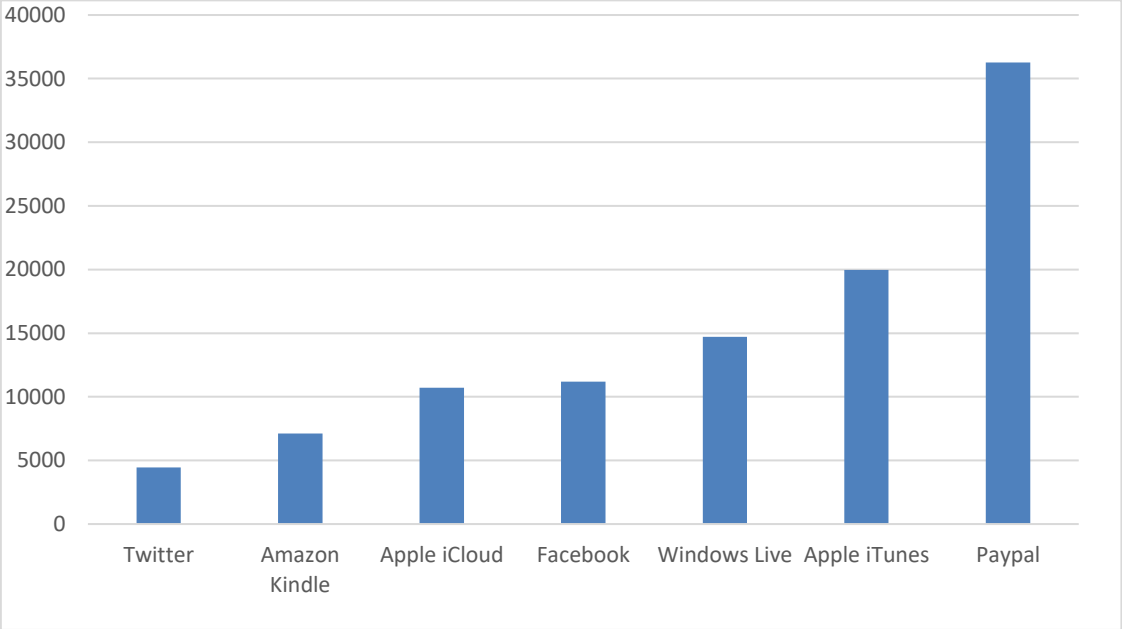
1.1 pav. Pavyzdinis EULA langas, matomas programinės įrangos diegimo metu

Kiti naudojami vartotojo sutikimo būdai:

- pakuotės (angl. *shrink wrap*) atidarymas;
- apsauginės juostos (angl. *seal*) perplėšimas;
- registracijos dokumento išsiuntimas programinės įrangos platintojui;
- programos įdiegimas (kai nėra prašoma sutikti su EULA sąlygomis įdiegimo metu. Dažnas atvejis naudojant UNIX pagrindo operacines sistemas);
- programos naudojimas.

Išanalizavus šiuos būdus matyti, kad galutinio vartotojo informavimas apie jį suvaržančias sąlygas nėra pirminis programinės įrangos kūrėjų tikslas – priešingai, vartotojų abejingumas EULA koncepcijai yra jiems labai parankus. Esant tokiai situacijai nestebina, kad galutinio vartotojo licencijos sutartis sulaukia nemažai kritikos tiek tarp akademinės bendruomenės narių, tiek ir tarp sutinkančiųjų su jos sąlygomis [6].

Vienas iš pagrindinių ir dažniausiai pabrėžiamų kritikos objektų yra EULA apimtis [7]. Grafike 1.2 pavaizduotas žodžių skaičius populiarios programinės įrangos licencijų sutartyse. Vien šiomis 7 programomis naudojasi itin didelis žmonių skaičius, tačiau neegzistuojant galimybei patikrinti, kiek iš jų perskaitė visą vartotojo licencijos tekstą, o kiek

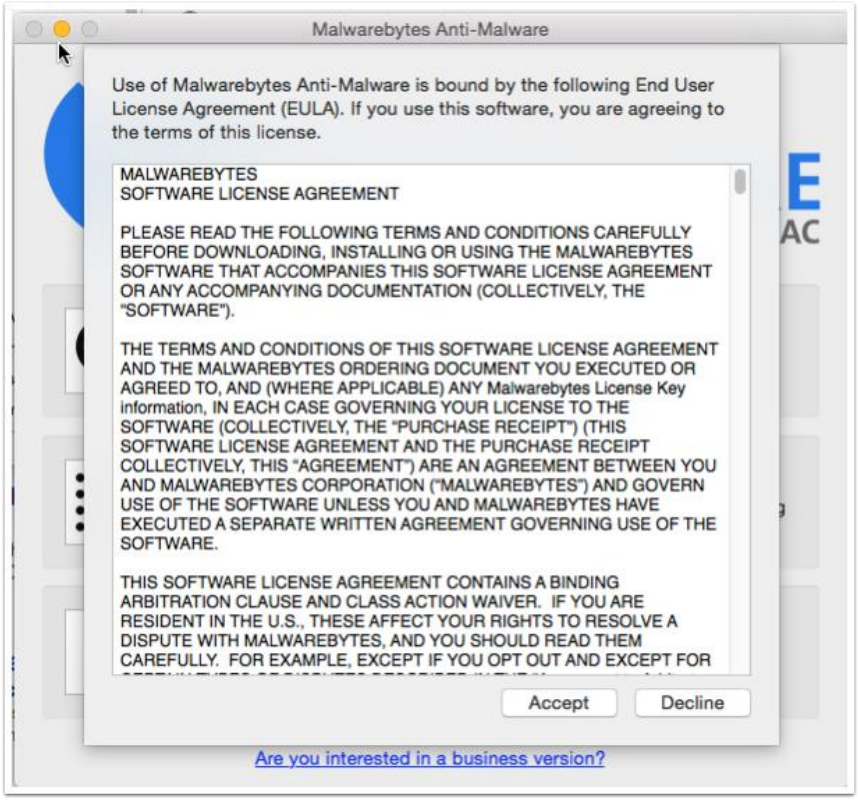


1.2 pav. Žodžių skaičius populiarių elektroninių produktų ir paslaugų EULA

tiesiog sutiko vienu iš aukščiau paminėtų būdų, galima tik daryti prielaidą, kad susipažinusių bent su vienos iš šių programų EULA yra itin mažai. Tokį teiginį pagrindžia prieš 10 metų atliktas, tačiau ir šiandien aktualus antivirusinės programinės įrangos gamintojos „PC Pitstop“ eksperimentas [8]. Jo metu ši kompanija į savo EULA sąlygas įterpė papildomą pastraipą,

kurioje pažadėjo prizą ją perskaičiusiam ir elektroniniu laišku apie tai pranešusiam asmeniui. Pirmasis klientas atsiliepė tik po 4 mėnesių ir daugiau nei 3000 atsisiuntimų.

Galutinio vartotojo licencijos sutartis dažnai kritikuojama ir dėl pernelyg sudėtingos teisinės terminologijos bei ilgų ir sunkiai suprantamų sakinių [9]. Nors šis dokumentas turėtų būti orientuotas į asmenis be jokio specializuoto išsilavinimo, tačiau praktikoje trumpos ir aiškios EULA yra išimtys iš taisyklės. Lengvą skaitymą (angl. *readability*) sunkina ir dažnas didžiųjų raidžių vartojimas tekste. Toks formatas yra naudojamas dėl Jungtinėse Amerikos Valstijose sutarčių teisėje įtvirtinto principo, kad svarbūs teiginiai turi būti išsiskiriantys (angl. *conspicuous*) ir aiškiai pastebimi [10]. Paveikslėlyje 1.3 matyti, kad net ir informacinių technologijų saugumo srityje dirbančios kompanijos piktnaudžiauja šia nuostata. Rezultatas –



1.3 pav. Teksto pabrėžimas (didžiosiomis raidėmis) EULA

minimalus skaičius bandančių perskaityti ir suprasti EULA sąlygas. Ir nors akademinė bendruomenė neturi vieningos nuomonės dėl šio dokumento, sutariama, jog galutinio vartotojo licencijos sutartis išliks aktuali ir artimiausioje ateityje [11]. Išnagrinėjus EULA detales, svarbu įvertinti galimą jos panaudojimą platinant kenkėjišką programinę įrangą.

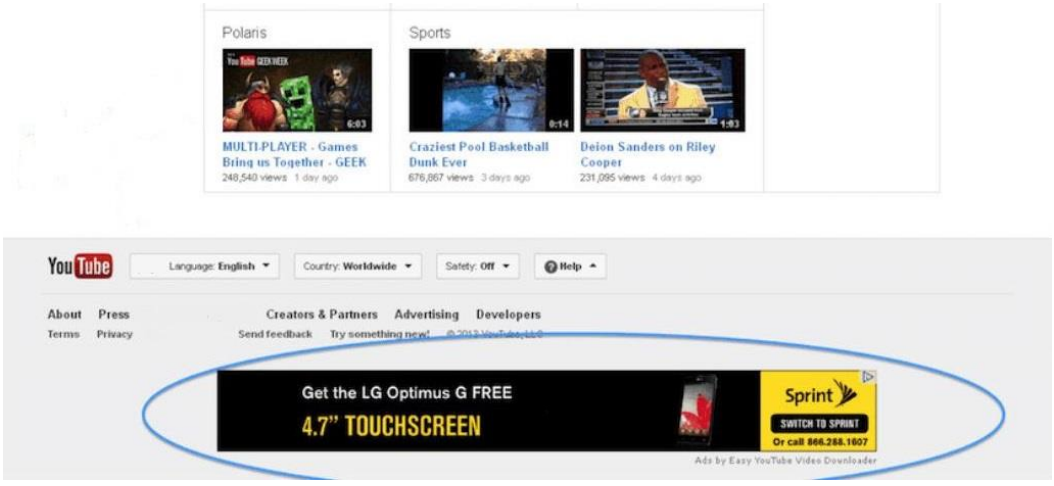
1.3. Kenkėjiškos programinės įrangos tipai

Šiandien kompiuterių virusai, „Trojos arkliai“, virusai kirminai (angl. *worms*), tapatybės vagystės ir sukčiavimas (angl. *phishing*) yra labai paplitę internete, todėl kiekvienas vartotojas siekia apsaugoti savo informacinę sistemą bei asmeninės informacijos konfidencialumą naudodamas įvairius saugumo sprendimus. Tačiau, kaip pabrėžiama JAV elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio medžiagoje, „vienas nuobodus mažas elementas (EULA – redaktoriaus pastaba) gali panaikinti visą gerą darbą, jei tik nebus elgiamasi atsargiai“ [12]. Būtent galutinio vartotojo licencijos sutarties ignoravimas suteikia papildomas galimybes kenkėjiškos programinės įrangos sklaidai.

Egzistuoja daug kenkėjiškos programinės įrangos tipų – vien saugumo įrangos gamintojos „Sophos“ ne informacinių technologijų specialistams parengtame žodyne išskiriama beveik 50 skirtingų rūšių [13]. Apibendrinant jas galima suskirstyti į dvi rūšis: informaciją renkančios ir sistemą (duomenis) keičiančios. Tiek vienos, tiek ir kitos gali būti įdiegtos vartotojo kompiuteryje pasinaudojant EULA sąlygomis.

Informaciją renkančios kenkėjiškos programos siekia surinkti kuo daugiau duomenų apie vartotoją (konfidencialios asmeninės medžiagos), jo sistemą ir naršymo internete įpročius ir perduoti juos savo kūrėjui ar valdytojui. Pagal tai, kokia informacija yra renkama ir kam ji yra panaudojama, šios programos dar yra skirstomos į reklamines (angl. *adware*) ir šnipinėjimo (angl. *spyware*). Būtina pabrėžti, kad informaciją renkančios programos nekeičia aukos kompiuteryje esančių duomenų ir nesiekia sutrikdyti sistemos darbo. Kuo ilgiau tokia programa išlieka nepastebėta, tuo daugiau naudos ji atneša savo valdytojui.

Pagrindinė reklaminės kenkėjiškos programos funkcija yra analizuoti, kokius internetinius puslapius lanko konkretus vartotojas ir kokių prekių ar paslaugų jis ieško tinkle.



1.4 pav. Reklaminės kenkėjiškos programos veikimo pavyzdys

Pagal šią informaciją jam vėliau yra pateikiamos specializuotos reklamos (angl. *targeted advertising*), kurios generuoja pelną tokio tipo kenkėjiškos programos kūrėjui, parduodančiam surinktą medžiagą savo produktų pardavimus norinčioms padidinti komercinėms kompanijoms [14]. Kaip šis principas veikia praktikoje, galima matyti 1.4 paveiksle: vartotojas lankydamasis populiarioje vaizdo įrašų svetainėje „Youtube“ mato išmanaus telefono pasiūlymą – tai leidžia daryti prielaidą, kad iš jo naudojamo kompiuterio internete jau buvo ieškoma būtent tokio ar labai panašaus įrenginio.

Pagal RRT interneto portale „esaugumas.lt“ pateiktą apibrėžimą: „šnipinėjimo programa yra tokia programinė įranga, kuri gali būti įdiegta į kompiuterį ar panašų įrenginį (pvz., išmaniuosius telefonus ar planšetinius kompiuterius) siekiant rinkti informaciją apie kompiuterio naudotoją be pastarojo žinios, tačiau kartais apie tai, jog bus renkami duomenys, naudotojas gali būti informuojamas, pvz., prieš sutikdamas su programos licencijos tekstu“ [15]. Vertinant iš saugumo perspektyvos, šnipinėjimo kenkėjiška programa yra daug labiau pavojinga ir galinti padaryti daug daugiau žalos nei reklaminė kenkėjiška programa, kadangi jos perimamos informacijos spektras ir vertė yra nepalyginamai didesnė. Dažnai tokio tipo kenkėjiškos programos yra įdiegiamos į vartotojo kompiuterį kartu su nemokamomis kitų ne kenkėjiškų programų versijomis, žaidimais ar nelegaliai „nulaužtomis“ programomis. RRT išskiria tokias pagrindinės šnipinėjimo programinės įrangos keliamas grėsmes:

- asmens duomenų rinkimas;
- tapatybės vagystės;
- konfidencialios informacijos perdavimas tretiesiems asmenims;
- kompiuterio konfigūracijos pakitimai ar papildomos kenkėjiškos programinės įrangos diegimas.

Būtent asmens duomenų rinkimas ir perdavimas tretiesiems asmenims yra dažnai įtraukiamas tarp EULA sąlygų. Detali tokio metodo analizė bus pateikta tolimesniuose poskyriuose.

Sistemą modifikuojanti kenkėjiška programinė įranga yra kuriama ir platinama dėl labai skirtingų motyvų [16]:

- finansinės naudos;
- siekiant parodyti kūrėjo įgūdžius;
- kerštaujant ar kovojant su konkurentais;
- tinklų ar sistemų darbo sutrikdymui.

Skirtingai nuo duomenis renkančios kenkėjiškos programinės įrangos, kurios pagrindinis tikslas yra gauti kuo daugiau informacijos iš kuo didesnio skaičiaus aukų, sistemą modifikuojančios programos dažnai nutaikomos prieš konkrečius asmenis ar kompanijas.

Šiandien bet kokia asmeniniuose kompiuteriuose ar kituose išmaniuosiuose įrenginiuose esanti kenkėjiška programa gali padaryti itin didelę žalą ir dėl paplitusios BYOD principo. Kaip savo atskaitoje pastebi gerai žinoma informacinių technologijų saugumo sprendimų bendrovė „Kaspersky Lab“ – „du trečdaliai viso pasaulio verslininkų ir jų darbuotojų (62 proc.) dirbdami naudoja asmeninius mobiliuosius įrenginius“ [17]. Juose dažnai yra laikoma konfidenciali įmonės informacija, elektroniniai laiškai, VPN slaptažodžiai nuotoliniam prisijungimui į darbinius tinklus. Laikas, reikalingas perskaityti į tokį kompiuterį ar telefoną norimų įdiegti programų EULA sąlygas, yra labai maža investicija, palyginus su potencialia žala to nepadarius.

Sistemą modifikuojančios kenkėjiškos programinės įrangos variacijų yra itin daug, todėl šiame darbe išskiriamos tik pagrindinės ir geriausiai žinomos. Atsižvelgiant į tai, ko siekia įsilaužėlis, galimas toks apibendrintas sugrupavimas:

- sistemos ar tinklo darbo sutrikdymas;
- duomenų pakeitimas, užvaldymas ar ištrynimas;
- kompiuterio valdymas nuotoliniu būdu.

Atkirtimo nuo paslaugos ataka (DoS) siekia paveikti kompiuterinę sistemą arba tinklą taip, kad jo teikiamos paslaugos taptų neprieinamos vartotojams. Siunčiant itin didelį kiekį falsifikuotų užklausų į aukos kompiuterį, išnaudojami jo turimi resursai ir tikrieji vartotojai nebeaptarnaujami [18]. Praktikoje itin dažnai vykdomos paskirstyto atsisakymo aptarnauti (DDoS) atakos, kurios yra veiksmingesnes ir sunkiau sustabdomos nei DoS, kadangi aukos sistema yra apkraunama užklausomis iš didelio žalingomis programomis užkrėsto ir nuotoliniu būdu valdomo kompiuterių tinklo (praktikoje dažniausiai vadinamu „kompiuterių zombių tinklu“, angl. *botnet*). Pastebėtina, kad vienas iš būdų, kaip įrenginiai tampa šio tinklo dalimi, yra kenkėjiškos programinės įrangos įdiegimas pasinaudojat specifiškai sumodeliuotomis EULA sąlygomis. DDos atakų galimybės nuolat auga, o aukomis dažnai pasirenkamos didžiausios pasaulio kompanijos. 2016 metų pradžioje vykdyta ataka prieš didžiausią pasaulio transliuotoją „BBC“ teksto rašymo metu buvo pati stipriausia iki šiol – generuotas kenkėjiškas duomenų srautas siekė net 602 Gbps [19]. Sistemai atsilaikyti nepavyko.

Kenkėjiškos programinės įrangos vykdomas duomenų pakeitimas, užvaldymas ar ištrynimas aukos kompiuteryje gali būti atliekamas tiek slaptai, tiek apie tai informuojant sistemos valdytoją. 2015 metais buvo užfiksuotas stiprus pastarojo tipo atakų skaičiaus padidėjimas [20]. Išpirkos reikalaujantys virusai (angl. *ransomware*) užšifruoja visą aukos kompiuteryje esančią informaciją ir už iššifravimo raktą pareikalauja užmokesčio (dažniausiai anonimine interneto valiuta – bitkoinais (angl. *bitcoin*)). Nors šio pažado įsilaužėliai dažniausiai laikosi (siekdami, kad aukos nenustotų jiems mokėti), tačiau tam tikrais atvejais, pavyzdžiui,

dėl programavimo klaidos ištrynus iššifravimo raktą, duomenys tampa neprieinami visam laikui [21]. Vienintelis saugus duomenų išsaugojimo metodas – nuolat daromos jų kopijos (rekomenduojama dubliuoti bent į porą skirtingų laikmenų).

Nuotoliniu būdu aukos kompiuterį valdančios kenkėjiškos programos gerai žinomos nuotolinės prieigos „Trojos arklio“ (angl. *RAT*) vardu. Dažnu atveju jos turi visą anksčiau aptartą kitų kenkėjų funkcionalumą, kadangi tokia programa įdiegta į aukos įrenginį leidžia atakuotojui jį valdyti savininko teisėmis. Tai apima, bet neapsiriboja:

- kompiuterio ekrano vaizdo stebėjimą, įrašymą;
- papildomos programinės įrangos įdiegimą;
- vartotojo klaviatūros paspaudimų sekimą (angl. *keystroke logging*);
- kietojo disko suformatavimą;
- kenkėjiškos programinės įrangos platinimą.

RAT aptikti yra pakankamai sudėtinga užduotis, kadangi ji sistemoje tarp veikiančių programų nėra rodoma. Veiksmingiausiai apsisaugoma nuolat atnaujinant antivirusinę programą, vengiant įsirašinėti produktus iš nepatikimų šaltinių ir kuo mažiau naudojant kompiuterį administratoriaus privilegijomis [22].

Atsižvelgiant į tai, kad kenkėjiškos programinės įrangos platinimas ir naudojimas yra laikomas nelegalia veikla, bet tam dažnai pasitelkiamas teisiškai suvaržantis EULA dokumentas, būtina išanalizuoti, ar jis turi juridinę galią ir neprieštarauja teisės aktams.

1.4. Teisinė EULA analizė

Juridinis galutinio vartotojo licencijos sutarties aspektas kompiuterinių sistemų saugumui Lietuvoje nėra išsamiai išnagrinėtas. Nors dažnai EULA teksto pradžioje yra akcentuojama, kad tai – svarbus teisinis dokumentas, tačiau didesnio dėmesio jis nesulaukia tiek tarp akademinės bendruomenės narių, tiek ir viešajame diskurse, kur tai laikoma tik formalumu, be jokio realaus poveikio su EULA sąlygomis sutikusiam vartotojui. Siekiant įvertinti galimybes panaudoti EULA kenkėjiškos programinei įrangai platinti, toliau šiame darbe bus analizuojami pagrindiniai su informacijos sauga susiję Lietuvos Respublikos (toliau – LR) teisės aktai ir juridinė praktika Europos Sąjungoje (toliau – ES) ir JAV.

2004 metais priimtas ir 2013 metų pabaigoje atnaujintas Lietuvos Respublikos elektroninių ryšių įstatymas yra vienas pagrindinių dokumentų reglamentuojančių viešųjų elektroninių ryšių paslaugų teikėjų ir galutinių paslaugų gavėjų teises ir pareigas [23][24]. Devintasis skirsnis „Duomenų, generuojamų arba tvarkomų teikiant viešąsias elektroninių ryšių paslaugas, tvarkymas ir privatumo apsauga“ yra tiesiogiai susijęs su šio darbo tyrimo objektu.

Su EULA analize susijusios 61 straipsnio „Ryšio konfidencialumas“ pirma, antra ir ketvirta dalys yra pateikiamos toliau tekste (pastaba – tekstas paryškintas autoriaus).

> 1. Draudžiama be faktinių elektroninių ryšių paslaugų **naudotojų sutikimo** klausytis, įrašyti, kaupti ar kitu būdu perimti pranešimų turinį ir srauto duomenis ar su jais susipažinti, išskyrus atvejus, kai tai galima teisėtai daryti pagal šio Įstatymo 66 ir 77 straipsnius (66 straipsnis reglamentuoja surinktų duomenų tvarkymą, o 77 straipsnis duomenų rinkimą kriminalinės žvalgybos tikslai – autoriaus papildymas). Be faktinių elektroninių ryšių paslaugų **naudotojų sutikimo** draudžiama atskleisti elektroninių ryšių tinklais perduodamų pranešimų turinį ir (ar) susijusius srauto duomenis arba sudaryti sąlygas sužinoti tokią informaciją ir (ar) susijusius srauto duomenis, išskyrus įstatymo nustatytus atvejus.
>
> 2. Šio straipsnio 1 dalies nuostatos nedraudžia nepažeidžiant konfidencialumo principo laikinai išsaugoti perduodamus pranešimus, jei tai būtina paslaugoms (pavyzdžiui, balso paštui, elektroniniam paštui ir kitoms) teikti. Taip pat šios nuostatos netaikomos informacijos ir susijusių srauto duomenų įrašymui, atliekamam teisėtos verslo praktikos metu, kai siekiama pateikti komercinio sandorio sudarymo, vykdymo ar kitokios verslo transakcijos, kuri, vadovaujantis teisės aktais, gali sukelti teisinių padarinių, įrodymus. Prieš pradedant įrašymą, faktiniai elektroninių ryšių paslaugų **naudotojai turi būti informuoti** apie tokį įrašymą ir jo tikslą. Įrašytų pranešimų turinys ir susiję srauto duomenys gali būti saugomi ne ilgesnį laikotarpį, negu tas, per kurį sandorio galiojimas gali būti teisiškai užginčytas.
>
> 4. Saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar faktinio elektroninių ryšių paslaugų naudotojo galiniame įrenginyje leidžiama tik su sąlyga, kad atitinkamam abonentui ar faktiniam elektroninių ryšių paslaugų naudotojui vadovaujantis Asmens duomenų teisinės apsaugos įstatymu suteikus aiškią ir išsamią informaciją, įskaitant informaciją apie tvarkymo tikslus, jis **davė sutikimą**. Šios nuostatos nedraudžia techninio saugojimo ar naudojimosi duomenimis, kurio vienintelis tikslas yra perduoti informaciją elektroninių ryšių tinklu, taip pat būtinais atvejais teikti informacinės visuomenės paslaugas, kurias užsako abonentas ar faktinis elektroninių ryšių paslaugų naudotojas.

Pagal pateiktas įstatymo dalis matoma, kad naudotojo sutikimas yra lemiamas veiksnys nusprendžiant ar duomenys yra renkami teisėtai, ar ne. Referuojant į dažniausiai sutinkamą EULA sąlygų pateikimą vartotojui programinės įrangos diegimo metu, kuomet jo yra prašoma mygtuko paspaudimu sutikti su licencijos dokumentu, juridiniu požiūriu naudotojas pasirinkęs „sutinku“ pats panaikina draudimą rinkti jo asmeninius duomenis.

Kitas svarbus dokumentas, reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas ir pareigas bei atsakomybę tvarkant asmens duomenis, yra LR Asmens duomenų teisinės apsaugos įstatymas. Šio 1996 metais priimto ir 2011 metais paskutinį kartą atnaujinto įstatymo tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis [25].

Prieš pradedant analizuoti svarbiausius įstatymo punktus, būtina detaliau panagrinėti asmens duomenų sąvoką. Pagal 2 straipsnio pirmą dalį – „Asmens duomenys – 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“. Kaip matyti iš pateikto apibrėžimo, jis yra pakankamai abstraktus ir nepritaikytas modernios visuomenės poreikiams. Pavyzdžiui, jeigu įsilaužėlis renka vartotojo naršymo internete istoriją, susiedamas gautus duomenis su unikaliu ir nekintančiu kompiuterio tinklo įrenginio adresu (angl., *MAC*), diskutuotina, ar tai gali būti laikoma asmens duomenimis šio apibrėžimo apimtimi, kadangi vien tik iš *MAC* adreso nustatyti asmens tapatybę nėra įmanoma.

5 straipsnyje „Asmens duomenų teisėto tvarkymo kriterijai“ nurodomos visos aplinkybės, kuriomis remiantis gali būti tvarkomi asmens duomenys. Dėl didelės apimties žemiau pateikiami tik su šio darbo objektu susiję punktai:

1. Asmens duomenys gali būti tvarkomi, jeigu:
   1) duomenų subjektas duoda sutikimą;
   2) sudaroma arba vykdoma sutartis, kai viena iš šalių yra duomenų subjektas;
2. Draudžiama tvarkyti ypatingus asmens duomenis, išskyrus atvejus, kai:
   1) duomenų subjektas duoda sutikimą;

Kaip ir LR elektroninių ryšių įstatymo tekste, taip ir LR Asmens duomenų teisinės apsaugos įstatyme duomenų subjekto sutikimas rinkti jo asmeninius duomenys yra legalus juridinis pagrindas.

Kadangi šio darbo eksperimentinėje dalyje bus atliekamas duomenų rinkimas mokslinio tyrimo tikslais, būtina paminėti ir LR Asmens duomenų teisinės apsaugos įstatymo 12 straipsnį „Asmens duomenų tvarkymas mokslinio tyrimo tikslais“:

> 1. Atliekant mokslinį tyrimą, asmens duomenys tvarkomi, jeigu duomenų subjektas davė sutikimą. Be duomenų subjekto sutikimo asmens duomenys mokslinio tyrimo tikslais gali būti tvarkomi tik pranešus Valstybinei duomenų apsaugos inspekcijai. Šiuo atveju Valstybinė duomenų apsaugos inspekcija privalo atlikti išankstinę patikrą.

2. Moksliniam tyrimui panaudoti asmens duomenys turi būti nedelsiant pakeisti taip, kad nebūtų galima nustatyti duomenų subjekto tapatybės.

3. Moksliniam tyrimui surinkti ir saugomi asmens duomenys negali būti naudojami kitais tikslais.

4. Tais atvejais, kai atliekamiems tyrimams nėra būtini asmens tapatybę nustatantys duomenys, duomenų valdytojas teikia duomenų gavėjui tokius asmens duomenis, iš kurių negalima nustatyti asmens tapatybės.

5. Tyrimo rezultatai skelbiami kartu su asmens duomenimis, jeigu duomenų subjektas duoda sutikimą, kad jo asmens duomenys būtų paskelbti.

Siekiant užtikrinti kuo didesnį surinktų duomenų konfidencialumą, atliekamame tyrime bus laikomasi visų šiame straipsnyje pateiktų nurodymų.

EULA vis dar yra neišnagrinėtas ir retai viešajame diskurse aptarinėjamas objektas tiek Lietuvoje, tiek ir ES. Pastebima, kad nors bendru vertinimu ši licencijos sutartis yra teisiškai įpareigojanti, tačiau toks principas turi būti patikrintas teismų praktikoje, o iki šiol su EULA susijusių bylų būta itin mažai [26]. Daugiausiai dėmesio internete sulaukė 2012 m. Europos Teisingumo Teismo sprendimas, kuris išaiškino, kad didžiųjų žaidimų kūrėjų EULA sąlygose įtrauktas draudimas vartotojui parduoti iš kūrėjo nusipirktą žaidimą prieštarauja ES teisei ir yra negaliojantis [27]. Nors remiantis šiuo nutarimu greitai paplito idėja, jog ES teismai panaikino EULA juridinę galią Europoje, tačiau tokios išvados nėra teisingos ir galėtų būti taikomos tik konkrečioms nuostatoms, o ne visam dokumentui. ES e-komercijos direktyvos (2000/31/EC) 9 straipsnis teigia, kad bet kokie (įskaitant EULA) juridinę galią turintys susitarimai gali būti sudaromi elektroniniu būdu, paliekant valstybėms teisę pašalinti elektroninės sutarties galimybę pasirinktinais atvejais [28]. 2016 metų pradžioje nė viena narė nebuvo nurodžiusi, kad ji nepripažįsta EULA, kaip teisinę galią turinčio susitarimo.

Nors EULA koncepcija buvo sugalvota JAV, net ir šioje šalyje teismai nėra priėmę vieningos nuomonės dėl šio dokumento galiojimo. Vis dėlto, statistika yra daug palankesnė galutinio vartotojo licencijos sutarties atžvilgiu, išskyrus tuos atvejus, kai programinės įrangos kūrėjas nesukuria sąlygų vartotojui tinkamai peržiūrėti EULA tekstą ar nėra informuojamas apie susitikimą su sąlygomis (jau aptarti atvejai, kaip pavyzdžiui, pakuotės atidarymas ar tiesiog programinės įrangos naudojimas) [6]. Palyginimui su ES, 2010 m. JAV Apeliacinis teismas priėmė sprendimą byloje, kurioje grafinės automatizuoto projektavimo sistemos „AutoCAD“ kūrėjai siekė uždrausti fiziniam asmeniui perpardavinėti senas jų programinės įrangos versijas „eBay“ aukcione. Teismas, remdamasis į EULĄ įtrauktomis sąlygomis, patenkino ieškovo reikalavimus taip sustiprindamas galutinio vartojo licencijos sutarties galią JAV teisėje [29].

1.5. Žalingos EULA sąlygos

Įvertinus juridinius EULA aspektus, būtina detaliau išanalizuoti praktikoje sutinkamas šio dokumento sąlygas, kurios sukuria saugumo spragas vartotojo sistemoje arba pažeidžia informacijos konfidencialumo principą. Pavyzdžiai nėra pateikiami pagal jų naudojimo dažnumą ar potencialios grėsmės dydį ir tai nėra galutinis kontraversiškai vertinamų nuostatų sąrašas. Vis dėlto, vien tik žinios apie šias sąlygas ir jų interpretacijas leistų vartotojams geriau įvertinti EULA neskaitymo pavojų.

Vartotojo sistemos stebėsena (angl., *monitoring*) yra dažnai į EULA turinį įtraukiama sąlyga. Vienas iš didžiausią atgarsį ir pasipiktinimą 2015 metais sukėlusių atvejų yra „Microsoft Windows 10“ operacinės sistemos licencijos sutartis. Įprastai (angl., *by default*) ši operacinė sistema persiunčia „Microsoft“ itin didelį asmeninės vartotojo informacijos kiekį: buvimo vietą (angl., *location*), žinutes, elektroninius laiškus, informaciją apie įdiegtas programas, naršymo internete istoriją ir kita [30]. Šie duomenys reikalingi norint išnaudoti visą „Microsoft“ virtualaus asistento „Cortana“ funkcionalumą, tačiau jų apimtis ir panaudojimas informaciją renkančioje pusėje gali turėti įvairių saugumo ir privatumo pasekmių. Nors įdiegus „Windows 10“ operacinę sistemą vėliau galima pakeisti visus nustatymus ir sustabdyti informacijos dalijimąsi su „Microsoft“, tačiau tam vartotojas turėtų peržiūrėti ir perkonfigūruoti savo pasirinkimą net 13-oje skirtingų privatumo langų (angl., *privacy screens*) [31]. Įvertinant tai, kad šia operacine sistema naudosis daug minimalius kompiuterinio raštingumo pagrindus turinčių žmonių, toks uždavinys dažnu atveju gali būti per sudėtingas.

1.55 milijardo aktyvių vartotojų per mėnesį turintis socialinis tinklas „Facebook“ į savo sąlygas yra įtraukęs tokią nuostatą – „Visam turiniui, tokiam kaip nuotraukoms ar vaizdo įrašai, kuriam yra taikomos intelektinės nuosavybės teisės, jūs suteikiate mums neišimtinę, perleidžiamą, sub-licencijuotą, neapmokestinamą pasaulinę licenciją naudoti visą jūsų patalpintą turinį. Licencija nustos galioti tuomet, kai jūs ištrinsite šį turinį iš savo paskyros, išskyrus tuos atvejus, kai jis yra pasidalintas su kitais, o jie nėra jo ištrynę“ (autoriaus pažodinis vertimas iš anglų kalbos) [32]. Sutikimas su šiomis sąlygomis suteikia teisę „Facebook“ naudoti visą vartotojų sukurtą turinį savo rinkodaros (oficiali versija) tikslais be jokio papildomo įspėjimo. Tuo tarpu tiek „Google“, tiek ir duomenų saugojimo paslaugas teikianti „Dropbox“ savo naudojimo sąlygose akcentuoja, kad visa vartotojo informacija bus pateikiama trečiosioms šalims, jeigu tai bus reikalinga pagal galiojančius įstatymus, teisinį procesą arba įgyvendinant valstybinės institucijos prašymą [33]. Kadangi subjektai neprivalo būti informuoti apie tokią prieigą, taip sukuriamos palankios sąlygos jų šnipinėjimui.

Atsakomybės už netinkamą programinės įrangos veikimą apribojimas yra viena iš svarbiausių EULA sąlygų šios įrangos kūrėjams. Naudotojo sutikimas su licencijos sutartimi

automatiškai panaikina bet kokią galimybę jam vėliau kreiptis į teismą ar kitas institucijas dėl blogai veikiančios programos, ištrintų ar sugadintų duomenų, nutraukto palaikymo. Tokią išlygą savo EULA turėjo labai populiari operacinė sistema „Microsoft XP“, tuo tarpu šiandien atsakomybės apribojimą galimą sutikti tarp jau paminėtos „Dropbox“ paslaugos teikimo sąlygų. Galima tik spėti ar vartotojas būtų linkęs naudotis tokia informacijos talpykla, kai pagal EULA jo failai galėtų pradingti be jokios paslaugos teikėjo atsakomybės bet kuriuo momentu.

Kartu su jau aptartomis sąlygomis dažnai įtraukiamas ir draudimas vartotojui kritikuoti naudojamą produktą ar jį viešai lyginti su konkurentų gaminiais. Tai apsunkina galimybę būsimiems klientams gauti papildomą nuomonę apie įvarius gaminius bei suvaržo žodžio laisvę. Ir nors 2003 metais saugumo sprendimus kurianti kompanija „McAfee“ (dabar esanti procesorių gamintojos „Intel“ dalimi) buvo nubausta už į EULA įtrauktą draudimą be išankstinio raštiško sutikimo publikuoti bet kokius palyginamųjų (angl., *benchmark*) testų rezultatus, tačiau šiandien tokie apribojimai vis dar naudojami puikiai žinomų informacinių technologijų produktų („SQL Server“ ar „VmWare Workstation“) licencijos sutartyse [4]. Pagal tai galima spręsti, kad net ir didžiosios kompanijos nevengia į savo EULA sąlygas įtraukti nuostatas, kurios teisminio proceso metu jau buvo pripažintos kaip pažeidžiančios įstatymus.

Dar vienas su informacinių technologijų sauga susijęs EULA reikalavimas nurodo, kad naudojamai programinei įrangai suteikiamas leidimas autonomiškai įdiegti, ištrinti, suteikti ar atimti prieigą prie kitos programinės įrangos, įskaitant ją pačią. Pavyzdžiui, „Microsoft paslaugų susitarimo“ (angl., *Microsoft Services Agreement*), su kuriuo vartotojas turi sutikti sukurdamas savo asmeninę „Microsoft“ paskyrą („Windows 10“ EULA pakeitimas), 7 b dalyje teigiama, kad – „mes galime automatiškai tikrinti jūsų turimos programinės įrangos versijas ir įdiegti atnaujinimus ar konfigūracijos pakeitimus, kurie užkirstų kelią naudotis tam tikromis paslaugomis, įskaitant nelegalius žaidimus ir neautorizuotus išorinis įrenginius“ [34]. Panašaus pobūdžio įgaliojimus į savo EULA sąlygas yra įdiegusios ir kitos didžiosios informacinių technologijų kompanijos, tokios kaip „Apple“ ar „Google“. Nors pateikto pavyzdžio atveju „Microsoft“ akcentuoja kovą su nelegalia ir potencialiai pavojinga programine įranga (įdomu, kad „Google“ vienintelė yra realiai pasinaudojusi šia sąlyga, ištrindama iš naudotojų kompiuterių vieną kenkėjišką programą), tačiau pastaroji naudoja tokią pat strategiją, siekdama kuo ilgiau išbūti sistemoje. Viena populiari lygiarangio ryšio (angl., *peer-to-peer (P2P)*) failų dalijimosi programa savo EULA sąlygose pamini, kad į naudotojo sistemą kartu su ja yra įdiegiama ir trečiosios šalies (angl., *third-party*) programinė įranga, kuriai suteikiamos prieigos teisės į sistemoje esančius failus. Dar daugiau, licencijos sutartyje įrašyta, jog vartotojas negali vienašališkai nuspręsti šias programas pašalinti [12]. Svarbu atkreipti dėmesį, kad tokia trečiųjų

šalių programinė įranga taip pat turi savo EULA sąlygas, su kuriomis vartotojas dažniausiai „sutinka“ tiesiog ja naudodamasis.

Paskutiniam šiame darbe nagrinėjamam EULA punktui iliustruoti puikiai tinka ištrauka iš „Google Chrome“ naršyklės paslaugų teikimo sąlygų :

„18. Sąlygų pakeitimai

18.1 Kartais „Google“ gali keisti Bendrąsias ir Papildomas sąlygas. Atlikusi šiuos pakeitimus, „Google“ paskelbs naują Bendrųjų sąlygų kopiją, galimą šiuo adresu: http://www.google.com/chrome/intl/lt/eula_text.html, ir bet kokios naujos Papildomos sąlygos bus galimos naudojantis Paslaugomis arba per Paslaugas, kurias tokie pakeitimai paveiks.

18.2 Suprantate ir sutinkate, kad jei naudositės Paslaugomis pasikeitus Bendrosioms ar Papildomoms sąlygomis, „Google“ laikys, kad sutinkate su Bendrųjų ar Papildomų sąlygų pakeitimais“ [35].

Kaip akivaizdžiai matoma iš šių punktų, EULA sąlygos gali būti pakeistos bet kuriuo momentu be jokio papildomo perspėjimo. Nors pateikiama nuoroda, kur vartotojas visada gali rasti naujausią dokumento versiją, tačiau autorius daro prielaidą, kad periodiškai tikrinančių tokį turinį yra vienetai (optimistiškiausiu atveju). Dar daugiau, programinės įrangos kūrėjas, tokiu būdu atnaujinęs sąlygas, preziumuoja, kad tolesnis šios programos naudojimas automatiškai patvirtinta vartotojo sutikimą su visais pakeitimais. Nors neabejotina, kad tokios kompanijos kaip „Google“ ar „Microsoft“ nerizikuotų savo gera reputacija, išnaudodamos šią saugumo spragą, tačiau dideliam skaičiui internete nemokamai platinamų programų galimybė keisti EULA sąlygas yra puikus būdas legaliai pasinaudoti vartotojo aplaidumu.

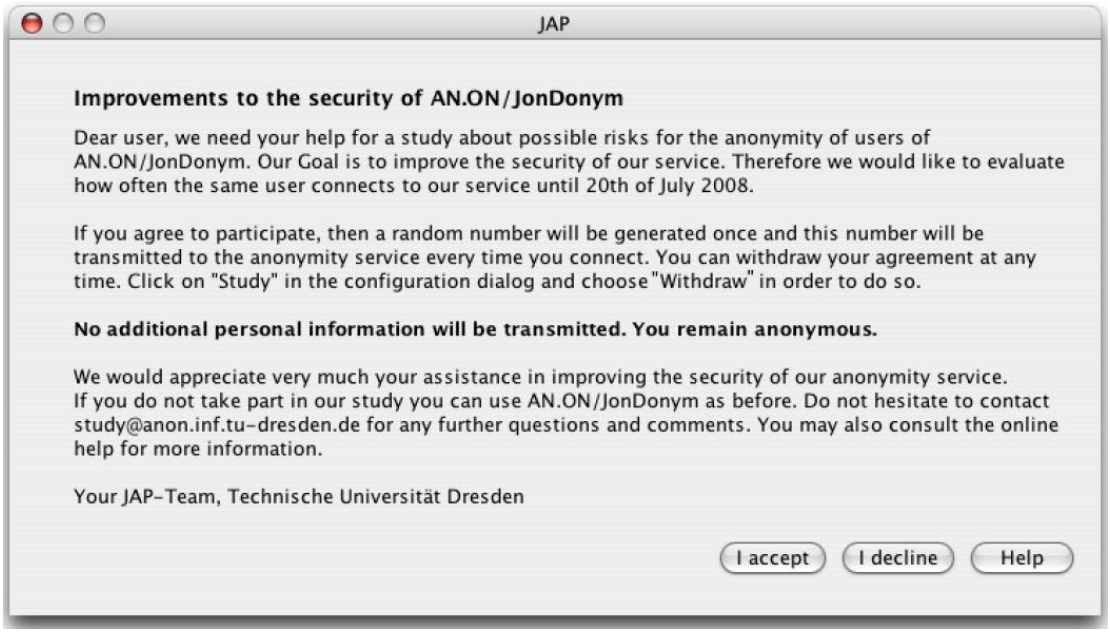
1.6. Atlikti EULA tyrimai

Lietuvoje galutinio vartotojo licencijos sutartis nėra sulaukusi tinkamo akademinės bendruomenės dėmesio. Kadangi šis dokumentas visų pirma yra teisinės paskirties, vieninteliai iki šiol atlikti tyrimai analizuoja EULA tik iš komercinio programinės įrangos kūrėjų požiūrio taško. Nors iš ankstesniuose poskyriuose pateiktos licencijos sutarties analizės matyti, kad galimas jos poveikis informacijos ir informacinių sistemų saugumui yra ne tik labai platus, bet ir akivaizdžiai nuvertintas vartotojų, tačiau jų švietimas apie EULA grėsmes nėra vykdomas. Tik vieninteliame KTU absolventės Almos Ravinytės 2014 metų magistriniame darbe „Programinės įrangos licencijos sutarties automatinio įvertinimo galimybių tyrimas“ analizuojamas ryšys tarp kenkėjiškos programinės įrangos ir galutinio vartotojo licencijos sutarties. Tačiau ir jame nėra atliekamas joks empirinis tyrimas, kuris leistų padaryti išvadas ar lietuviai skaito EULA tekstą, ar tiesiog norėdami kuo greičiau naudotis įdiegiama programine

įranga automatiškai paspaudžia sutikimo mygtuką. Išanalizavus viešojoje erdvėje (daugiausiai informacinių technologijų forumuose) randamą informaciją, matoma tendencija, kad dažniausiai kartu su akronimu EULA vartojamas žodžių junginys – „kurios niekas neskaito“. Šio teiginio teisingumą bus siekiama patikrinti darbo eksperimentinėje dalyje.

Kaip ir Lietuvoje, taip ir globaliu mastu informacinių technologijų specialistų atliktų EULA akademinių tyrimų yra labai mažai. Šiame kontekste išsiskiria privačios iniciatyvos kompanijų, vykdančių veiklą informacijos ir kompiuterinių sistemų saugos užtikrinimo srityje. Kadangi nėra įmanoma empiriškai išmatuoti ar vartotojas tikrai perskaitė licencijos tekstą (vienu ar kitu atveju visi galiausiai vis tiek pasirenka „perskaičiau ir sutinku“ parinktį), įvertinimui reikalingi papildomi kriterijai. Šiam tikslui gali būti tiriamas laikas, kurį vartotojas užtruko „sutikimo su EULA sąlygomis“ lange, arba į licencijos tekstą įterpiamos papildomos sąlygos, kurios turėtų priversti vartotoją su jomis nesutikti. Esant galimybei išnagrinėti subjektų elgesį pagal skirtingą metodologiją, gautų rezultatų palyginimas leidžia atlikti daug tikslesnę tiriamos problemos analizę.

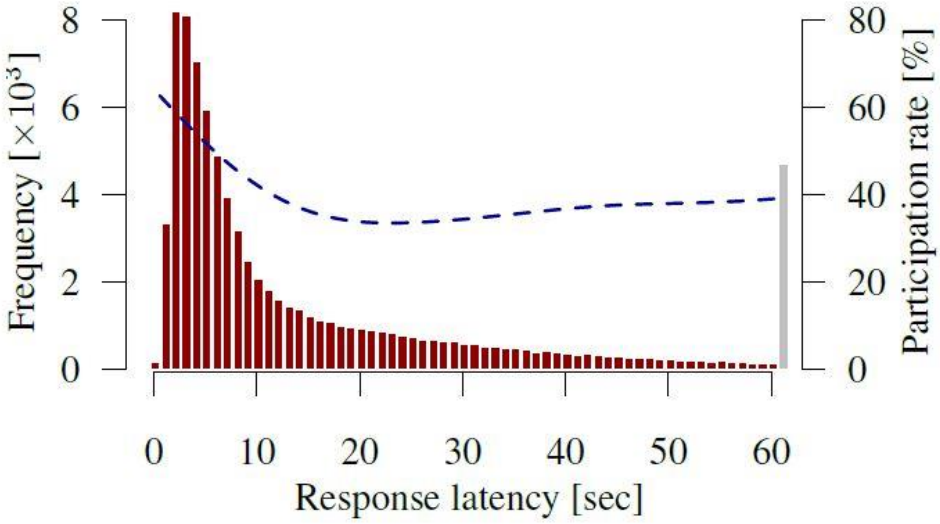
2010 metais tarptautinė akademikų komanda pristatė didelės apimties eksperimentinį tyrimą, karikatūriškai pavadintą „Išmokinti sutikti? Pritarimo langų (angl., *dialogs*) tyrimas“ [36]. 80 000 respondentų programinės įrangos atnaujinimo metu buvo pateiktas sutikimo prisidėti prie tyrimo langas (pateiktas 1.5 pav.). Nors tai nebuvo tiksli EULA kopija ar papildomų sąlygų įterpimas, tačiau tyrėjai panaudojo visus įprastai naudojamus principus:



1.5 pav. Tyrimo metu respondentams pateiktas langas (MAC OS X sistemai)

standartinis langa dydis, operacinei sistemai pritaikytas (angl., *native*) stilius, sutikimo mygtukas (atsisakymo ir pagalbos pasirikimai retai būna EULA lango dalis), šriftas ir teksto dydis.

Gauti tyrimo rezultatai buvo apibendrinti remiantis laiku, kurį vartotojas užtruko priimdamas sprendimą Iš 1.6 paveikslo matyti, kad daugiau nei 50% tiriamųjų priėmė sprendimą ir paspaudė mygtuką per mažiau nei 8 sekundes. Net ir atsižvelgiant į naudotojams



1.6 pav. Vartotojų pasirinkimo laikas

pateiktą sąlyginai trumpą tekstą, toks laiko tarpas yra nepakankamas norint susipažinti su lango turiniu. Ši informacija leidžia daryti prielaidą, kad jeigu sutikimo dalyvauti tyrime langą pakeistų EULA sąlygos (kurių ilgis, kaip jau minėta, vidutiniškai yra 3000 žodžių), pasirinkimo laiko grafike būtų matomi labai panašūs ar net vienodi rezultatai. Statistikos kompanijos „MeasuringU“ įkūrėjo atlikta 2500 programinės įrangos naudotojų analizė patvirtina tokią hipotezę [37]. Jo gauti rezultatai rodo, kad EULA lange, kurio greitas perskaitymas turėtų trukti bent 2 minutes, vidutiniškai buvo užtrunkama 6 sekundes. Tokie skaičiai leidžia 95% tikslumu teigti, jog licencijos sutarties tekstą perskaitė ne daugiau nei 8% su juo sutikusių asmenų.

Privačios kompanijos, kurios eksperimentus atliko pakeisdamos EULA tekstą, dažniausiai į sąlygas įtraukdavo itin neįprastus ar absurdiškus teiginius. Priminimui jau minėtas „PC Pitstop“ prizas pirmam parašiusiam apie perskaitytą pažadą, kuomet teko laukti net 4 mėnesius iki pirmo laiško. Tuo tarpu informacinių technologijų saugos sprendimų bendrovė „F-Secure“ Londone pasiūlė nemokamą prieigos prie interneto tašką (angl., *hotspot*), jeigu vartotojas sutiks „mainais į nemokamą *Wi-fi* prieigą amžinybei atiduoti mums savo pirmagimį vaiką“ [38]. Per pusvalandį prie šio prieigos taško prisijungė net 33 asmenys. Nors šis eksperimentas gali būti traktuojamas kaip geras pokštas, tačiau jis tik dar kartą parodė, kad

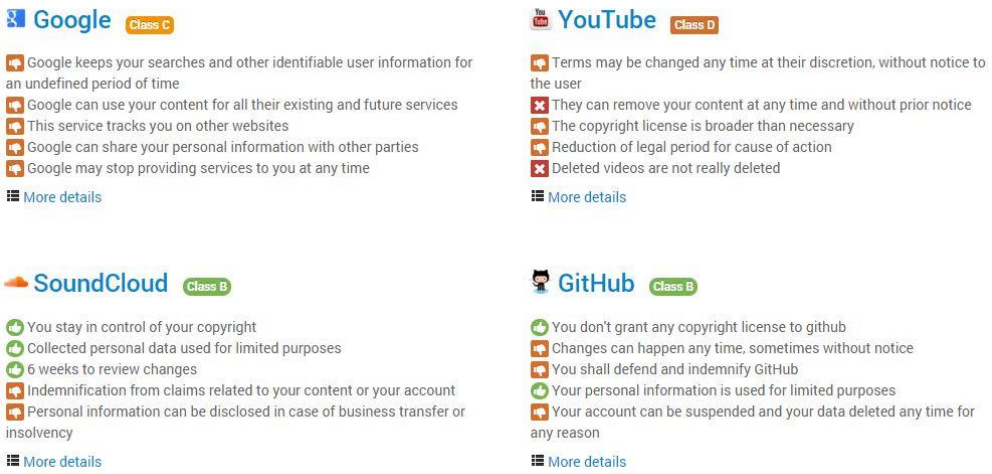
didelė dalis informacinių technologijų naudotojų sutinka su pateikiamomis sąlygomis jų net neskaitę.

Panašų eksperimentą 2010 metais atliko ir Didžiosios Britanijos žaidimų pardavėja „GameStation“, kuri į EULA įdėjo sąlygą, kad tų pačių metų balandžio 1 dieną visi sutikę su šiuo tekstu bus priversti atiduoti savo „nemirtingas sielas“ [39]. Tačiau nenorintys to padaryti klientai galėjo paspausti ant pateiktos nuorodos, tokiu būdu anuliuodami šį pasižadėjimą. Rezultatai parodė, kad daugiau nei 7500 vartotojų nepasinaudojo šia galimybe, o likusieji 12%, kurie pasirinko neatiduoti savo sielos ir paspaudė ant pateiktos nuorodos, vėliau sulaukė paskatinamosios dovanos. Šiuo eksperimentu kaip ir kitais jau aptartais buvo dar kartą įrodyta, kad į EULA sąlygas galima įrašyti praktiškai bet kokį tekstą ir didžioji dauguma vis tiek su juo sutiks per 6-8 sekundes.

1.7. Programiniai sprendimai

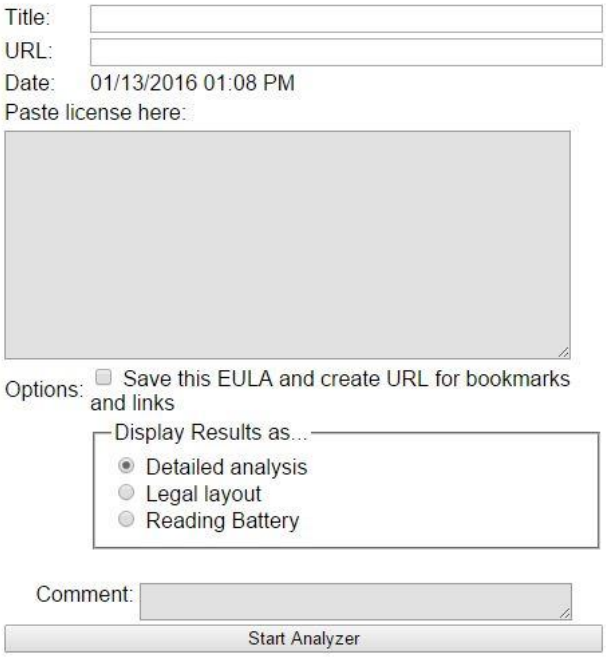
Kadangi informacinių sistemų naudotojai dėl aptartų priežasčių dažniausiai neskaito EULA teksto, galima būtų tikėtis surasti įvairių programinių sprendimų, kurie automatizuotų šį procesą bei pateiktų vartotojui peržiūrėti ir įvertinti tik galimai pavojingų sąlygų santrauką. Vis dėlto, galutinio vartotojo licencijos sutarties tekstą analizuojančių programų yra vos pora. Pastebėtina, kad ir jos gali būti naudojamos tik anglų kalba parašytoms EULA sąlygoms, todėl kitomis kalbomis (tarp jų ir lietuvių) pateikto sutarties teksto išanalizuoti specializuotomis programomis nėra įmanoma. Šiame poskyryje bus pristatomi sprendimai, padedantys vartotojui suprasti EULA turinį.

2012 metų viduryje internete startavo daug palaikymo ir tarptautinės žiniasklaidos dėmesio sulaukęs projektas „Paslaugų teikimo sąlygos; Neskaičiau“ (angl., *“Terms of Service; Didn't Read”*) [1]. Akcentuodami faktą, kad niekas neskaito EULA sąlygų, šio projekto iniciatyvinė grupė užsibrėžė ištaisyti esamą situaciją. Paveiksle 1.6 matomas jų internetiniame puslapyje pateiktų reitingų pavyzdys. Pagal programos ar paslaugos EULA sąlygas joms yra suteikiama klasė (A – geriausia, E – blogiausia) bei išskiriami pagrindiniai teigiami ir neigiami licencijos sutarties aspektai. Nepaisant patogios ir aiškios vartotojo sąsajos, projektas nėra aktyviai plėtojamas. Tai patvirtina faktas, kad per beveik ketverius metus įvertintų yra tik 11 EULA dokumentų, o paskutinis įrašas naujienų eilutėje (angl., *feed*) datuojamas 2014 metų liepos mėn. Kadangi galutinio vartotojo licencijos sutarties sąlygos laikui bėgant keičiamos, nuolat neatnaujinant tokio formato internetinio puslapio, informacija jame greitai tampa nebeaktuali ir netgi klaidinanti.



1.7 pav. Ištrauka iš „Terms of Service; Didn't Read" internetinio puslapio

Tuo tarpu bendrovės „SecurityLabs" sukurtas ir puslapyje http://www.spywareguide.com/analyze/analyzer.php patalpintas EULA sutarties analizatorius veikia visiškai kitu principu. Jis leidžia į interaktyvų langą įdėti norimos išnagrinėti licencijos sutarties tekstą anglų kalba ir pasirinkus rezultatų pateikimo būdą iš karto gauti rezultatą. 1.7



1.8 pav. „Spyware guide" EULA analizatorius

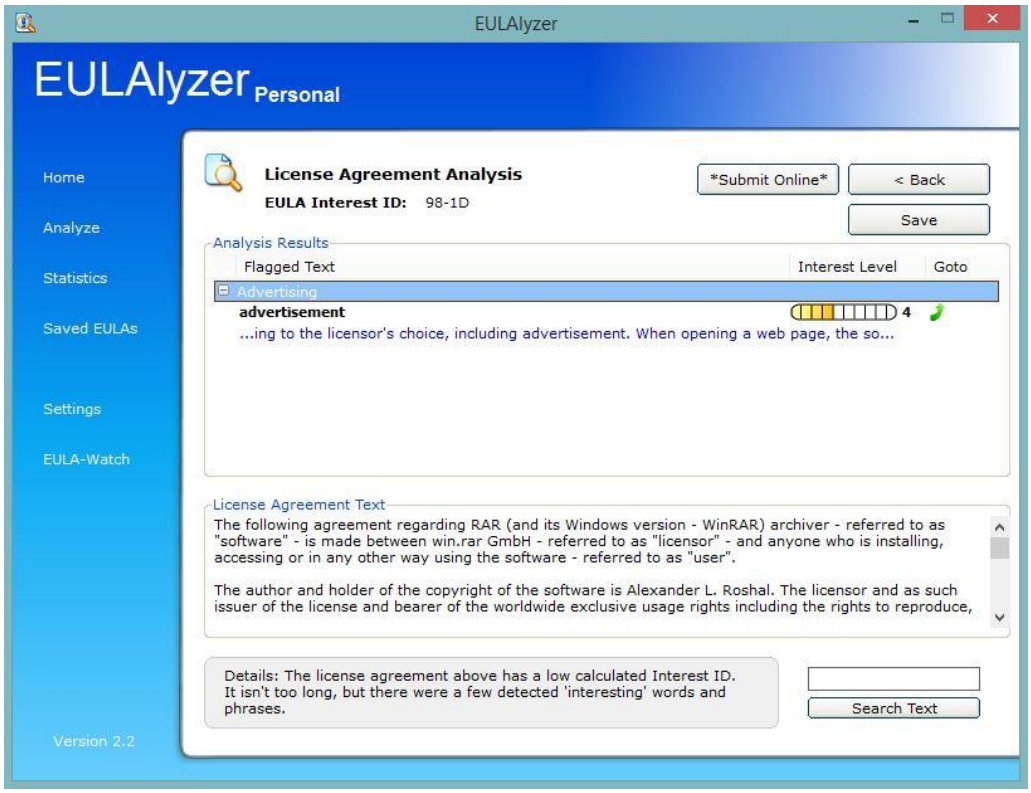
pav. pateiktas šios programos vartotojo sąsajos atvaizdas, iš kurio galima matyti, kad šio produkto naudojimas yra aiškus ir greitas. Paslaugos išbandymui buvo pasirinktos itin trumpos (1087 žodžiai) plačiai naudojamo archyvavimo ir duomenų suspaudimo įrankio „WinRAR"

EULA sąlygos [40]. „Spyware guide“ analizatorius išskyrė 4 galimas problemas: užuominas į reklamą, vartotojo sistemos stebėjimą, draudimą ištrinti šią programinę įrangą ir draudimą ištrinti trečiųjų šalių programinę įrangą. Darbo autoriaus vertinimu, iš išskirtų punktų „WinRAR“ EULA tekste aiškiai pastebimos tik užuominos į reklamą.

Populiariausias ir lengviausiai randamas įrankis EULA sąlygų automatiniam nagrinėjimui yra kompanijos „BrightFort“ sukurta „EULAlyzer“ programa. Skirtingai nuo aukščiau paminėtų sprendimų, pastaroji turi tiek nemokamą, tiek ir mokamą versiją komerciniams klientams [41]. Oficialiame puslapyje išskiriami šie programos privalumai:

- Suranda programos, kurią norite įdiegti, paslėptą veikimą;
- Pabrėžia punktus, kuriuos jūs galėjote praleisti skaitydami susitarimą;
- Duomenų bazėje saugo visas vartotojo analizuotas EULA;
- Iš karto pateikiami rezultatai;

Vis dėlto, programa turi ir akivaizdžių trūkumų. Vienas iš jų – sustojęs „EULAlyzer“ vystymas. Tokią išvadą galima padaryti įvertinus sisteminius reikalavimus. Pagal pateiktą informaciją „EULAlyzer“ galima įrašyti į Windows 2000, XP, 2003, Vista, 7. Atsižvelgiant į tai, kad 2016 metų pradžioje „Microsoft“ paskelbė, jog nutraukia „Windows 8“ operacinės sistemos palaikymą [42], tokie „EULAlyzer“ reikalavimai yra seniai neatnaujinti. Įdiegus programą, jos naudojimas yra labai paprastas: galima įkopijuoti tekstą tiesiai į interaktyvų langą arba pridėti failą, kuriame yra EULA sąlygos. Išbandžius ir šį įrankį su „WinRAR“ galutinio



1.9 pav. „EULAyzer“ analizatoriaus veikimo pavyzdys

vartotojo licencijos sutarties tekstu, buvo pateiktas vienas perspėjimas dėl galimos reklamos. Autoriaus vertinimu, būtent šis „EULAyzer“ analizatorius yra tiksliausias ir patogiausias naudojimui.

1.8. Analizės išvados

Augant interneto naudotojų skaičiui bei daugėjant prie globalaus tinklo prijungiamų įrenginių kiekiui, sparčiai didėja ir programinės įrangos apimtys. Vis dėlto, beveik visos (net ir nemokamos) programos ar elektroninės paslaugos yra prieinamos tik tuomet, kai vartotojas sutinka su jų kūrėjų nustatytomis sąlygomis. Galutinio vartotojo licencijos sutartis, geriau žinoma EULA akronimu, yra teisinis kontraktas tarp programinės įrangos kūrėjo ar platintojo ir galutinio šios įrangos naudotojo. Nors šis dokumentas buvo kuriamas norint apsaugoti autorines teises, tačiau šiandien EULA yra naudojama ir ribojant vartotojų pasirinkimo bei žodžio laisvę, išgaunant asmeninius duomenis ar įdiegiant kenkėjiškas programas.

Vartotojas gali sutikti su EULA sąlygomis įvairiais būdais – tiek paspausdamas „sutinku“ mygtuką programos įdiegimo metu, tiek atidarydamas programinės įrangos pakuote ar tiesiog ja naudodamasis (kartais ir pats nežinodamas apie duotą sutikimą). Dėl tokio neapibrėžtumo galutinio vartotojo licencijos sutartis yra dažnai kritikuojama. Vienas iš pagrindinių ir dažniausiai pabrėžiamų kritikos objektų yra EULA apimtis, taip pat akcentuojama sudėtinga teisinė terminologija bei ilgi ir sunkiai suprantami sakiniai. Nors akademinė bendruomenė neturi vieningos nuomonės dėl šio dokumento, sutariama, jog galutinio vartotojo licencijos sutartis išliks aktuali ir artimiausioje ateityje.

Šiandien kompiuterių virusai, Trojos arkliai, kirminai, tapatybės vagystės ir sukčiavimas yra labai paplitę internete, todėl kiekvienas vartotojas siekia apsaugoti savo informacinę sistemą bei asmeninės informacijos konfidencialumą naudodamas įvairius saugumo sprendimus. Apibendrinant kenkėjiškos programinės įrangos tipus, ją galima suskirstyti į dvi rūšis: informaciją renkančios ir sistemą (duomenis) keičiančios. Tiek vienos, tiek ir kitos gali būti įdiegtos vartotojo kompiuteryje pasinaudojant EULA sąlygomis.

Juridinis galutinio vartotojo licencijos sutarties aspektas kompiuterinių sistemų saugumui Lietuvoje nėra išsamiai išnagrinėtas. Nors dažnai EULA teksto pradžioje yra akcentuojama, kad tai – svarbus teisinis dokumentas, tačiau didesnio dėmesio jis nesulaukia tiek tarp akademinės bendruomenės narių, tiek ir viešajame diskurse. Lietuvos Respublikos elektroninių ryšių įstatymas yra vienas pagrindinių dokumentų reglamentuojančių viešųjų elektroninių ryšių paslaugų teikėjų ir galutinių paslaugų gavėjų teises ir pareigas. Kitas svarbus dokumentas, reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu

būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas ir pareigas bei atsakomybę tvarkant asmens duomenis, yra LR Asmens duomenų teisinės apsaugos įstatymas. Kaip ir LR elektroninių ryšių įstatymo tekste, taip ir LR Asmens duomenų teisinės apsaugos įstatyme duomenų subjekto sutikimas rinkti jo asmeninius duomenys yra legalus juridinis pagrindas.

Europos Sąjungoje EULA taip pat yra vis dar neišnagrinėtas ir retai viešai aptarinėjamas objektas. Pastebima, kad nors bendru vertinimu ši licencijos sutartis yra teisiškai įpareigojanti, tačiau toks principas turi būti patikrintas teismų praktikoje, o iki šiol su EULA susijusių bylų būta itin mažai. Panaši situacija yra ir JAV, kur nėra vieningos nuomonės dėl šio dokumento galiojimo, tačiau teismų statistika yra daug palankesnė galutinio vartotojo licencijos sutarties atžvilgiu.

Vartotojo sistemos stebėsena, nuosavybės teisė į asmeninį turinį, atsakomybės už netinkamą programinės įrangos veikimą apribojimas, draudimas vartotojui kritikuoti naudojamą produktą, leidimas autonomiškai įdiegti, ištrinti, suteikti ar atimti prieigą prie kitos programinės įrangos, bei sąlygų keitimas bet kuriuo momentu be jokio papildomo perspėjimo yra tik dalis dažnai praktikoje sutinkamų EULA sąlygų, kurios sukuria saugumo spragas vartotojo sistemoje arba pažeidžia informacijos konfidencialumo principą.

Kaip ir Lietuvoje, taip ir globaliu mastu informacinių technologijų specialistų atliktų EULA akademinių tyrimų yra labai mažai. Eksperimentais įrodyta, kad teoriškai į EULA sąlygas galima įrašyti bet kokį tekstą ir didžioji dauguma naudotojų vis tiek su juo sutiks per 6-8 sekundes (t. y. jo neskaitę). Galutinio vartotojo licencijos sutarties tekstą analizuojančių programinių sprendimų, kurie automatizuotų šį procesą bei pateiktų vartotojui peržiūrėti ir įvertinti tik galimai pavojingų sąlygų santrauką yra vos keletas. Nors ir nebeatnaujinamas „EULAyzer“ analizatorius yra tiksliausias ir patogiausias naudojimui šiuo metu rinkoje esantis produktas.

Remiantis atlikta EULA analize, šiame darbe numatoma parengti ir kartu su sukurta programine įranga išplatinti specifinę licencijos sutartį. Joje bus įtraukta dalis 1.2 ir 1.5 poskyriuose analizuotų neigiamų aspektų, tačiau vartotojui bus siūlomas ir alternatyvus resursų pasiekimo kelias, nesutinkant su akivaizdžiai žalingomis dokumento sąlygomis. Pagal vartotojo veiksmus programinės įrangos įdiegimo metu bus įvertinama, ar jis prieš duodamas sutikimą susipažino su EULA turiniu.

2. INTERNETO VARTOTOJŲ PATIKLUMO GALUTINIO VARTOTOJO LICENCIJOS SUTARTIMI TYRIMO PROJEKTAS

Šiame skyriuje analizuojamas vartotojų pasitikėjimo EULA sutartimi tyrimo projektas. Pagrindinis dėmesys bus skiriamas vartotojų sutikimo bei duomenų rinkimo klausimams, tyrimui pritaikytos galutinio vartotojo licencijos sutarties parengimui, asmeninių „Windows“ kompiuterių bei mobiliųjų „Android“ įrenginių tyrimo aplinkos pristatymui.

2.1. Tyrimo aplinkos ir renkamų duomenų pasirinkimas

Siekiant atlikti interneto naudotojų pasitikėjimo galutinio vartotojo licencijos sutartimi tyrimą, būtina atsižvelgti į pirmoje darbo dalyje pristatytus įvairius programinės įrangos kūrėjų taikomus metodus, kurie yra vertinami kaip sutikimas su EULA sąlygomis. Kadangi šis projektas bus vykdomas remiantis pasauliniame tinkle (angl. *World Wide Web*) išplatintais resursais, visi fiziniai būdai (pakuotės atidarymas, apsauginės juostos perplėšimas ar registracijos dokumento išsiuntimas programinės įrangos platintojui) nėra tinkami. Kiti dažnai taikomi vartotojo sutikimo būdai, tokie kaip programos įdiegimas (kai nėra prašoma sutikti su EULA sąlygomis įdiegimo metu) ar programos naudojimas, šio darbo tyrimui taip pat nėra tinkami dėl jų nedeklaruoto tikslo išvengti detalaus skaitymo bei diskutuotinos juridinės galios. Dėl šių priežasčių tyrimui pasirinktas itin dažnai naudojamas ir kitų, šiame darbe paminėtų, metodų trūkumų neturintis variantas – sutikimas su galutinio vartotojo licencijos sutartimi specialiame EULA dialoge.

Prieš pradedant detalizuoti tyrimo įgyvendinimo projektą, būtina apibrėžti kokia informacija bus renkama ir analizuojama jo eigoje. Siekiant gauti kuo tikslesnius duomenis, tiriamųjų imtis bus fiksuota – 2016 metais į KTU bakalauro studijas Informatikos fakultete priimtų pirmo kurso studentų skaičius. Objektas, kurį norint pasiekti bus prašoma sutikti su specifiškai sumodeliuotomis EULA sąlygomis – testavimo platforma su pasirengiamaisiais Informacinių technologijų modulio egzamino klausimais (toliau – tyrimo įrankis). Informaciją apie tyrimo įrankį bus išplatinta modulio dėstytojo paskaitų metu. Toks modelis atkartoja ir praktikoje labai populiarų socialinės inžinerijos metodą: patikimas šaltinis (pastaba – internete juo dažniausiai apsimetinėjama) ir trokštamas resursais. Pagrindinė informacija, kuri bus renkama – kiek vartotojų sutiko su pateiktomis EULA sąlygomis jų neskaitę, kiek buvo perskaičiusių sutarties tekstą ir nesutikusių su asmeninės informacijos rinkimu (prieiga prie testavimo aplinkos jiems bus suteikta ir šiuo atveju). Siekiant parodyti galutinio vartotojo licencijos sutarties teksto ignoravimo pavojų, iš visų tyrimo dalyvių, sutikusių su EULA sąlygomis, bus gauta asmeninio įrenginio informacija – pastoviosios atminties dydis ir jame

likusios laisvos vietos duomenys. Šis parametras pasirinktas kaip indikatorius, kad vartotojui sutikus, programa gali rinkti informaciją ar vykdyti nustatytą kodą jo asmeninėje sistemoje, tuo pačiu nepažeidžiant galiojančių teisės aktų (jeigu toks rinkimas įvardintas EULA tekste). Taip pat toks matmuo yra labai individualus ir tik itin retais atvejais gali sutapti tarp dviejų įrenginių, tačiau tuo pačiu jis neidentifikuoja konkretaus asmens ir todėl be jokių apribojimų gali būti panaudojamas tyrimo duomenų analizei ar viešinimui. Atsižvelgiant į tai, kokia informacija bus renkama, toliau analizuojama tyrimo įgyvendinimo aplinka.

Kasdieninio vartotojo naršymo internete metu patvirtinimo, jog jis sutinka su pateiktomis sąlygomis, įprastai gali būti prašoma dviem atvejais. Pirmasis – naršyklėje (angl. *browser*) naudojant išplėtimus (angl. *extensions*) arba įskiepius (angl. *plugin*), kurie startuoja papildomus (dažnai specifinius (angl. *custom*)) procesus ar prašo prieigos prie tam tikros informacijos (pavyzdžiui, vartotojo buvimo vietos). Antrasis – atsisiunčiant programą į asmeninį įrenginį ir startuojant įdiegimo procedūrą. Vartotojo sutikimas su EULA sąlygomis naršyklėje netinkamas tyrimui dėl šių priežasčių:

- Kiekviena naršyklė turi savo veikimo specifiką, todėl standartizuotas sprendimas nėra įmanomas;
- Be papildomų išplėtimų arba įskiepių informacija apie vartotojo įrenginį yra apribota standartiniais HTTP duomenimis, o prieiga prie tokių parametrų kaip kietojo disko dydis yra ribojama pasitelkiant smėlio dėžės (angl. *sandbox*) principą;
- Įdiegti išplėtimai tampa integralia naršyklės dalimi (jie nėra apriboti tik vieno internetinio puslapio), todėl naršyklių gamintojai jiems nustatę griežtus saugos reikalavimus;
- Įskiepiai („Flash“, „Adobe Reader“, „Java“ ir kiti) papildo naršyklę tam tikru funkcionalumu (pavyzdžiui, *pdf* failo atidarymu ar vaizdo medžiagos rodymu), kuris standartinėje konfigūracijoje nebūtų įmanomas. Siekiant kuo didesnio saugumo naršant internete, įskiepių veikimo zona taip pat apribota smėlio dėžės ribomis ir tiesioginio ryšio su vartotojo sistema nėra suteikiama.

Įvertinant šiuos apribojimus, tyrimui pasirinktas EULA sąlygų pateikimo įdiegiant programinę įrangą būdas. Detali šio metodo analizė bus pateikiama 2.3 ir 2.4 poskyriuose.

2.2. Tyrimui sumodeliuotos galutinio vartotojo licencijos sutarties parengimas

Tyrime bus naudojama specifiškai parengta galutinio vartojo licencijos sutartis. Siekiant nesukelti įtarimų, kad šiuo dokumentu yra analizuojamas interneto naudotojų elgesys,

bus pateikiama maksimaliai standartizuota sutarties versija, papildant reikalinga informacija dėl duomenų rinkimo tyrimo tikslais. Nuo dažniausiai praktikoje sutinkamos EULA versijos naudojamas variantas skirsis ir savo kalba. Kadangi didžioji dalis internete randamos programinės įrangos yra orientuota į tarptautinę rinką, galutinio vartotojo licencijos sutartis pateikiama tik anglų arba anglų ir dar keliomis populiariausiomis Vakarų Europos kalbomis (vokiečių, prancūzų, ispanų) bei, rečiau, rusų ar kinų. Lietuvių kalba pateiktos EULA sąlygos dažniausiai sutinkamos tik didžiųjų programinės įrangos kūrėjų, tokių kaip „Microsoft“, „Apple“ ir kt., produktuose. Šiame tyrime galutinio vartotojo licencijos sutarties tekstas bus pateikiamas ne anglų, o lietuvių kalba dėl dviejų priežasčių. Visų pirma, siekiama kuo labiau atitikti juridinę praktiką - pagal LR įstatymus sutartys turi būti sudaromos nacionaline kalba (arba būti dvikalbės). Be to, lietuvių kalbos pasirinkimas leis tuo pačiu įvertinti, ar gimtąją kalba pateikiamos EULA turi pastebimą poveikį jų skaitomumui.

Pilnas galutinio vartotojo licencijos sutarties tekstas, parengtas pagal antivirusinės programinės įrangos „Kaspersky“ praktikoje naudojamą sutartį, kuris bus naudojamas atliekamame tyrime, yra pateikiamas priede Nr. 1. [43]. Atsižvelgiant į tai, kad šio dokumento apimtis atitinka praktikoje pasitaikančius atvejus, detalesnei analizei pateikiami tik svarbiausi jo aspektai.

Apibendrinant pateiktą galutinės vartotojo licencijos sutarties projektą, matoma, kad joje atspindi visos, pirmoje darbo dalyje pateiktos ir daugiausiai kritikos sulaukiančios savybės: EULA ilgis (apie 3000 žodžių), sudėtinga teisinė kalba, programinės įrangos kūrėjo atsakomybės ribojimas ir kitos. Vis dėlto, tyrimui aktualiausi yra 6 ir 7 punktai (strategiškai pasirinkta šios dalies vieta – pateikta ties 2/3 viso dokumento apimties, skaičiuojant nuo pradžios).

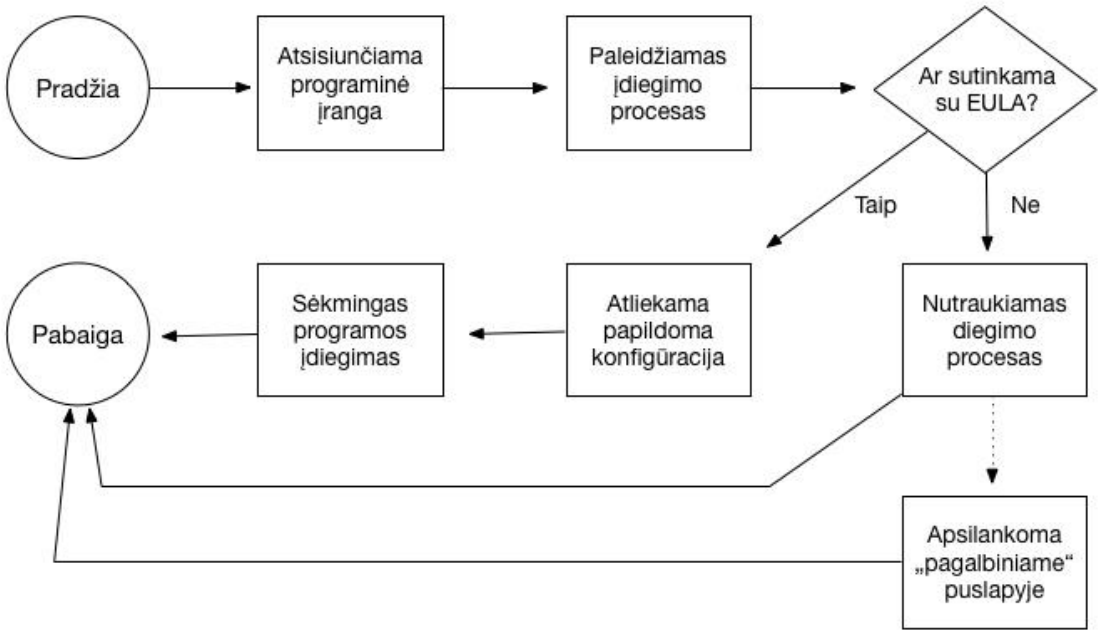
6 punktas – „Techninė pagalba“ – pateikia nuorodą į pagalbinį puslapį, kuriame bus pateikta alternatyvi prieiga prie programos siūlomų resursų, išvengiant kenksmingo programinio kodo paleidimo asmeninėje sistemoje. Visi vartotojai, kurie pažymės savo apsilankymą minėtame puslapyje, bus vertinami kaip perskaitę EULA dokumentą ir kritiškai įvertinę jame pateiktas sąlygas.

7 punkto pavadinimas („Informacijos rinkimas“) turėtų automatiškai atkreipti vartotojo dėmesį, jog šiai teksto daliai reikėtų skirti ypatingą dėmesį. 7.1 dalis akcentuoja informacijos apie įvykusias klaidas persiuntimą. Tai yra įprasta programinės įrangos kokybės gerinimo politikos dalis. Tačiau 7.2 punktas jau yra ypač kenksmingas informacijos saugos požiūriu. Nors juo sukuriamas dirbtinis saugumo įvaizdis („Kad būtų didesnis saugumas darbo metu“), tačiau tuo pačiu metu išvardinama, kokia informacija iš vartotojo bus renkama be detalesnio pagrindimo, kodėl jos reikia ir kam ji bus panaudota. Vertinant iš juridinės pusės, šis

punktas bus duomenų apie vartotojo kietojo disko dydį ir jame likusios laisvos vietos duomenų rinkimo pagrindimas. Nors šiuo atveju tai yra nekenksmingi duomenys, tačiau panašiame kontekste piktavalis galėtų į EULA įterpti jam priimtinas sąlygas. 7.3. punktas įtrauktas kaip dar vienas vartotojų atidumo patikrinimas. Šiuo punktu nurodoma į LR Asmens duomenų teisinės apsaugos įstatymo straipsnį apie duomenų rinkimą mokslinio tyrimo tikslais. Akivaizdu, kad tokia nuoroda programinės įrangos galutinio vartotojo licencijos sutarties tekste turėtų sukelti įtarimų dėl tikrosios šio dokumento ar pačios programos paskirties. Tuo atveju jeigu naudotojas perskaitys ir nesutiks su pateiktomis EULA sąlygomis, jam 7.4 punkte rekomenduojama nutraukti šios įrangos diegimo procedūrą ir apsilankyti 6.1 punkte nurodytame techninės pagalbos tarnybos puslapyje. Ši galutinio vartotojo licencijos sutartis privalo būti susieta su tam tikra programine įranga, todėl kitose šio skyriaus dalyse bus pristatomi tyrime naudojamų programų projektai.

2.3. Programos asmeniniams kompiuteriams projektas

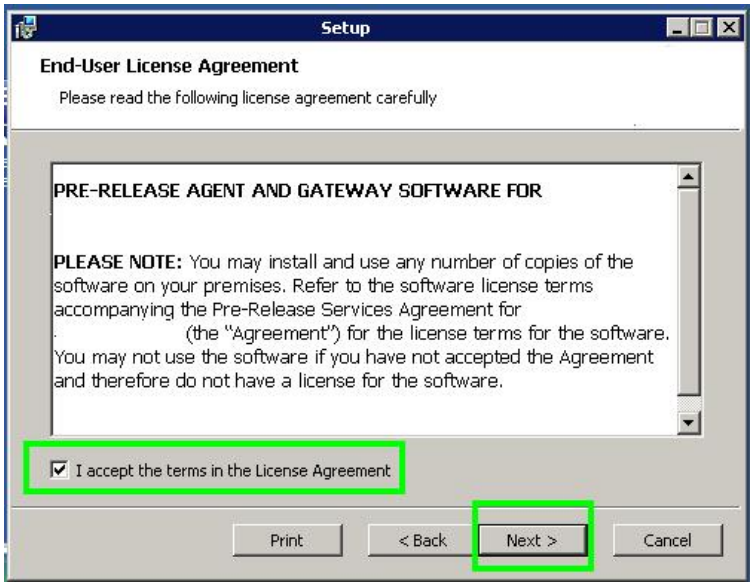
„Microsoft Windows“ operacinėje sistemoje paprastesnės programos (ne, pavyzdžiui, žaidimai ar brangūs programiniai paketai) yra įdiegiamos naudojant standartinį „Windows Installer“ servisą (paleidžiamas .msi paketo failas). Jo itin paprasta grafinė vartotojo sąsaja padaro šį procesą suprantamą net ir mažą kompiuterinį raštingumą turintiems asmenims. Paveiksle 2.1 pavaizduota tyrimui sukurtos programinės įrangos įdiegimo schema. Nuo



2.1 pav. Tyrime naudojama programinės įrangos įdiegimo schema asmeniniams kompiuteriams

standartinės (praktikoje sutinkamos) procedūros ji skiriasi tik tuo, kad dėl bet kokių priežasčių nutraukus šį procesą, naudotojui lieka galimybė pasiekti visus pageidaujamus resursus internetiniame puslapyje (punktyrinė rodyklė schemoje).

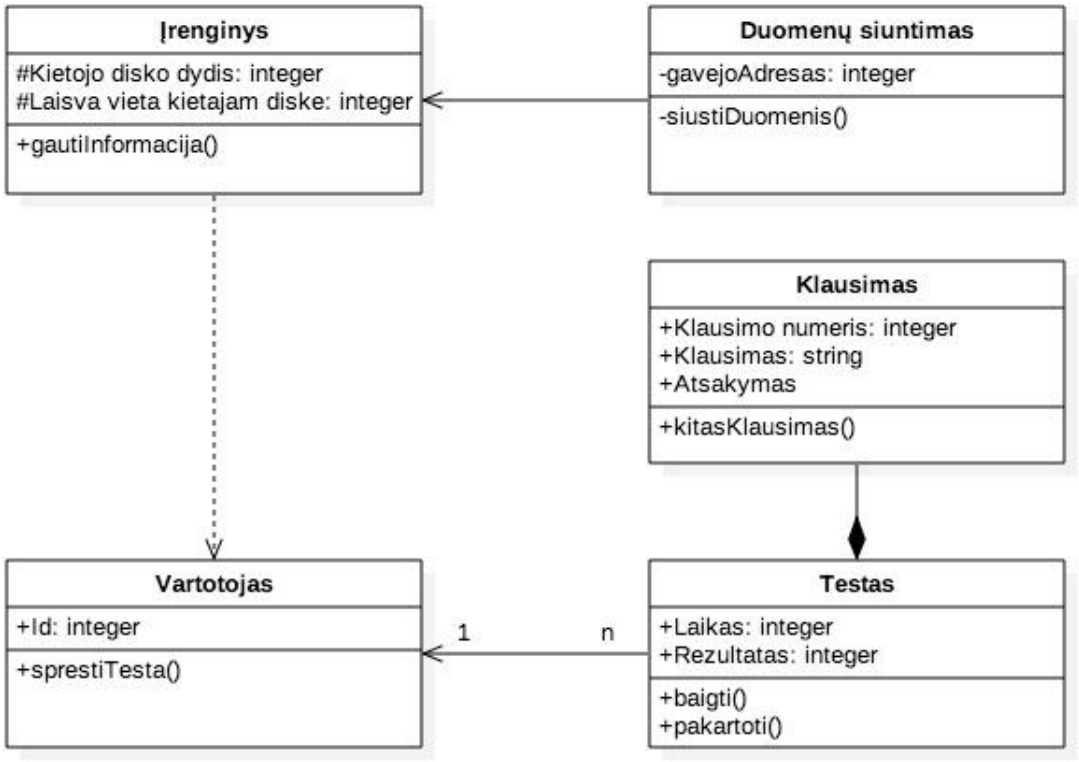
Programinės įrangos diegimo metu, sutikimui su EULA sąlygomis yra skiriamas atskiras dialogo langas. 2.2 paveiksle pateikiamas įprastinis jo variantas. Šis dialogas



2.2 pav. Standartinis EULA langas

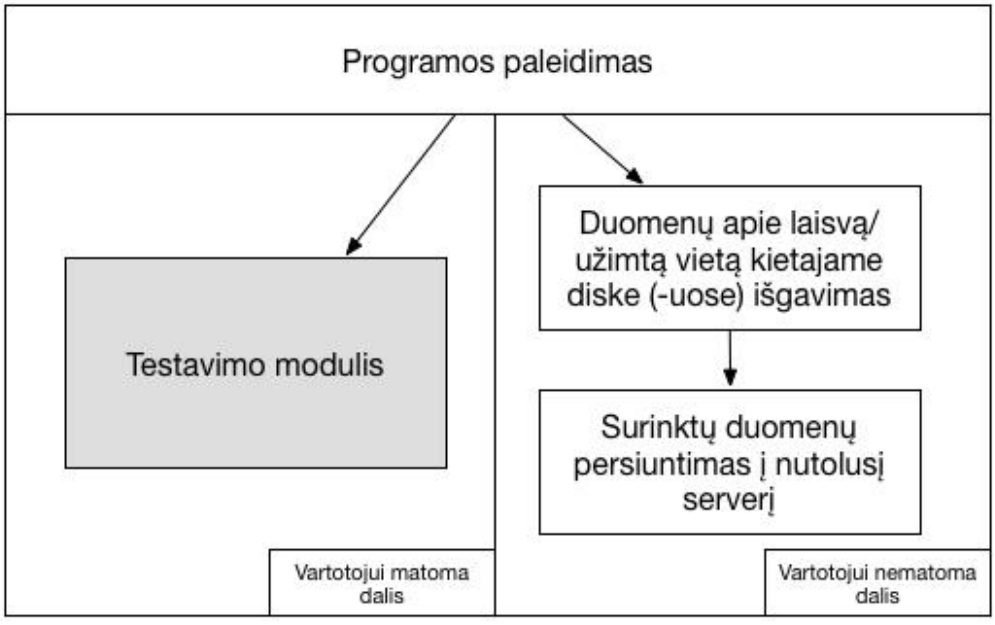
pasižymi tokiomis išskirtinėmis savybėmis: lango dydis yra fiksuotas – nėra įmanoma išsididinti teksto plotą patogesniam skaitymui; mygtukas „toliau“ (angl. *next*) aktyvuojamas tik tada, kai naudotojas pažymi varnelę, jog jis sutinka su pateikta galutinio vartotojo licencijos sutartimi (2.2 paveiksle žaliai pažymėtos zonos). Kadangi dažnas programinės įrangos vartotojas automatiškai spaudžia „toliau“ mygtuką net nežiūrėdamas, koks turinys yra pateikiamas tame lange, papildomo pažymėjimo reikalavimas bent teoriškai padidina tikimybę, kad į EULA sąlygas bus atkreiptas dėmesys.

Kaip aprašyta skyriaus pradžioje, interneto vartotojų patiklumas bus tikrinamas pasitelkiant šiam tyrimui sukurtą testavimo programą. Ji bus parašyta Java programavimo kalba pagal 2.3 paveiksle pavaizduotą schemą. Kadangi šio darbo tikslas nėra tiesiogiai susietas su programos funkcionalumu, jos architektūra yra maksimaliai supaprastinta, paliekant tik tiesiogiai su tyrimu surištas funkcijas. Java kalba pasirinkta dėl objektinio programavimo principo, kuris leidžia sukurti modulines programas su pernaudojamu kodu, taip pat dėl nepriklausomumo nuo platformos – esminės detalės bus pritaikytos ir kuriant analogiško funkcionalumo įrankį „Android“ sistemai.



2.3 pav. Testavimo programos klasių diagrama

Įjungus šią programą, grafinėje vartotojo sąsajoje bus atidaromas testavimo modulis, kuris leis studentams pasitikrinti savo žinias. Tuo tarpu fone (angl., *background*) bus automatiškai iškviečiamos kitos, pačios savaime nepavojingos, tačiau šiuo atveju „kenkėjiškiems“ tikslams panaudotos funkcijos/klasės. Pirmoji, kuri surinks duomenis apie

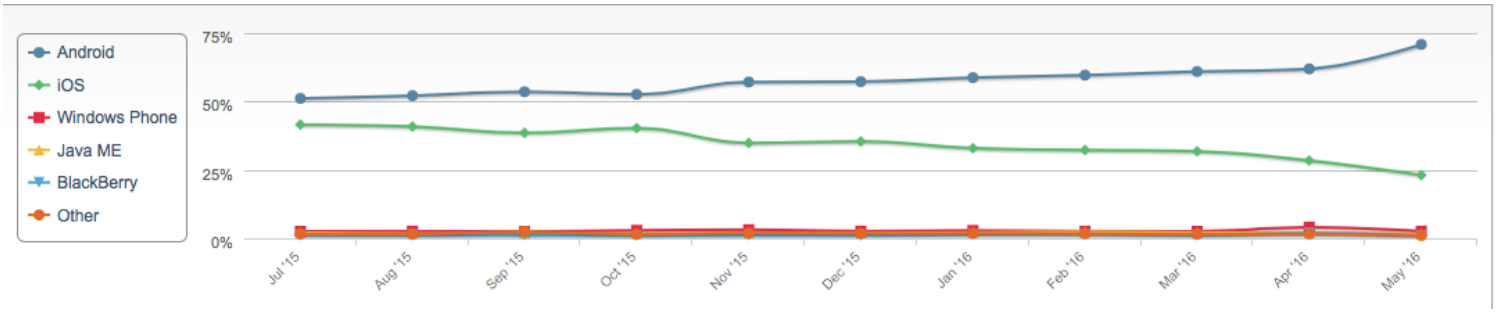


2.4 pav. Sumodeliuotos programos architektūros schema

asmeninio įrenginio informaciją – kietojo disko dydį ir jame likusią laisvą vietą; antroji – išsiųs surinktus duomenis į nurodytą serverį, kur jie bus saugomi iki apdorojimo tyrimo rezultatams. Minėtų funkcijų kodo ištraukos ir detalesnė jų veikimo analizė pateikiama 3-čiame šio darbo skyriuje. Toliau pristatoma analogiško veikimo programa „Android“ operacinei sistemai.

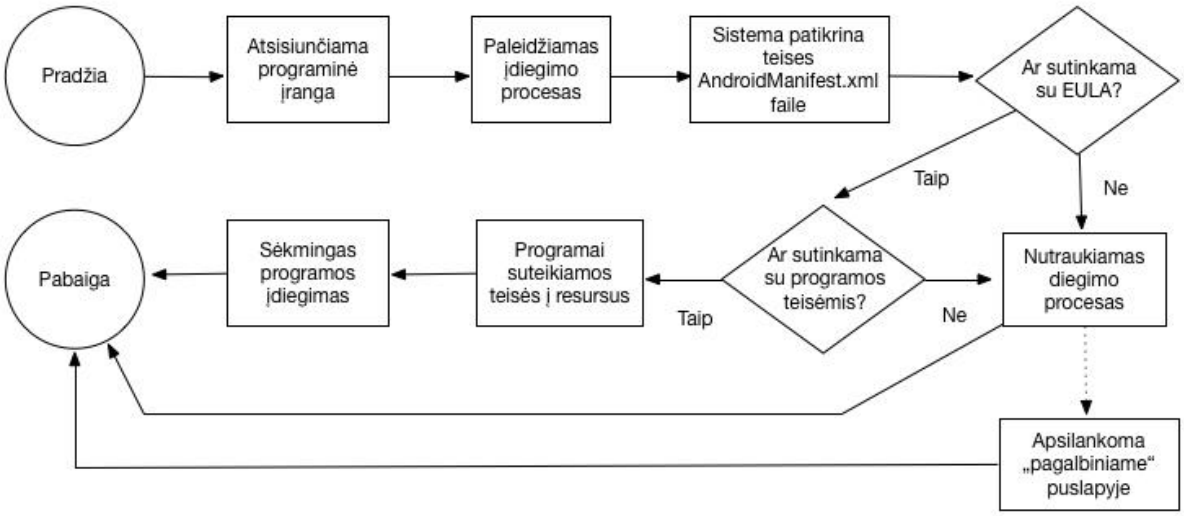
2.4. Programos mobiliesiems įrenginiams, naudojantiems „Android“ operacinę sistemą, projektas

Pagal „Netmarketshare“ duomenis „Android“ operacinė sistema mobiliesiems įrenginiams yra be konkurencijos populiariausia pasaulyje ir atotrūkis tik auga (pav. 2.4) [44]. Tokio paplitimo grėsmė – bet koks pažeidžiamumas ar kenkėjiška programa, pritaikyta šiai sistemai, gali turėti neigiamos įtakos itin dideliam ratui jos naudotojų. Kadangi sėkmingam šio darbo tikslui pasiekti yra būtina įvertinti kuo didesnio skaičiaus vartotojų elgesį, tarp mobiliųjų įrenginių naudotojų būtent „Android“ programinė įranga turi daugiausiai potencialo būti panaudota.



2.5 pav. „Android“ įrenginių rinkos dalis

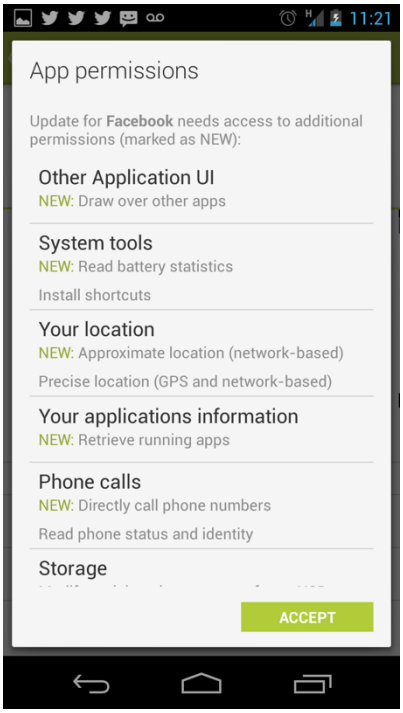
Programinės įrangos įdiegimo požiūriu, „Android“ programa turi daug panašumų su asmeniniams kompiuteriams pritaikyta versija. Vartotojas į savo mobilų įrenginį atsisiunčia .apk formato failą, kurio paleidimas startuoja diegimo procesą (schema 2.5 pav.). Pačioje pradžioje naudotojui parodomas EULA langas su pasirinkimu sutikti ar atmesti siūlomas sąlygas (dažniausiai papildomų pažymėjimų nėra reikalaujama). Pasirinkus teigiamą opciją ir tęsiant įdiegimą, kitas langas pateikia informaciją apie programai suteikiamas privilegijas (angl., *permissions*) (pav. 2.6). Tai yra unikalus tik „Android“ sutinkamas informacinis pranešimas vartotojui, kuris patogiu jam formatu leidžia pamatyti svarbią ir glaudžiai su jo



2.6 pav. „Android“ programos įdiegimo schema

duomenų konfidencialumo užtikrinimu susijusią informaciją. Šiam tyrimui sukurta programa „prašys“ akivaizdžiai daugiau privilegijų, nei tokio tipo aplikacija turėtų: pavyzdžiui, skaitymo iš išorinės atminties (angl., *read external storage*) ar prieigos prie įrenginio statuso duomenų.

Kaip ir asmeninio kompiuterio atveju, naudotojui sėkmingai įdiegus tyrimo programinę įrangą ir ją startavus, bus pradėti keli lygiagretūs procesai, iš kurių tik testavimo aplinkos grafinė vartotojo sąsają bus matoma ir žinoma vartotojui (pav. 2.3). Tuo tarpu



2.7 pav. „Android“ teisių suteikimo langas

duomenys apie sistemos kietojo disko informaciją bus gaunami pasitelkiant „Android“ Aplikacijų programavimo sąsają (angl., *Application Programming Interface, API*). Kadangi ši operacinė sistema yra atvirto kodo ir turinti daug galimybių skirtų programuotojams, tyrimui reikalingus duomenis galima gauti pasitelkiant įvarius metodus. Praktikoje dažnai naudojama *StatFs* vieša „Java“ klasė (skirta „Android“ įrenginiams), kuria bus remiamasi ir šiame darbe. Iš mobiliųjų įrenginių gauti tyrimo duomenys turės ir papildomą žymę, siekiant juos lengviau atskirti nuo duomenų iš asmeninių kompiuterių. Tai leis išanalizuoti ir palyginti vartotojų elgesį įvairesniais pjūviais. Programinis šios „Android“ aplikacijos kodas bus pateiktas kitame darbo skyriuje.

2.5. Tyrimo projekto išvados

Interneto naudotojų pasitikėjimo galutinio vartotojo licencijos sutartimi tyrimui pasirinktas dažniausiai praktikoje naudojamas sutikimo su EULA sąlygomis būdas - specialus EULA dialogo langas programos įdiegimo ar paslaugos naudojimo pradžios metu.

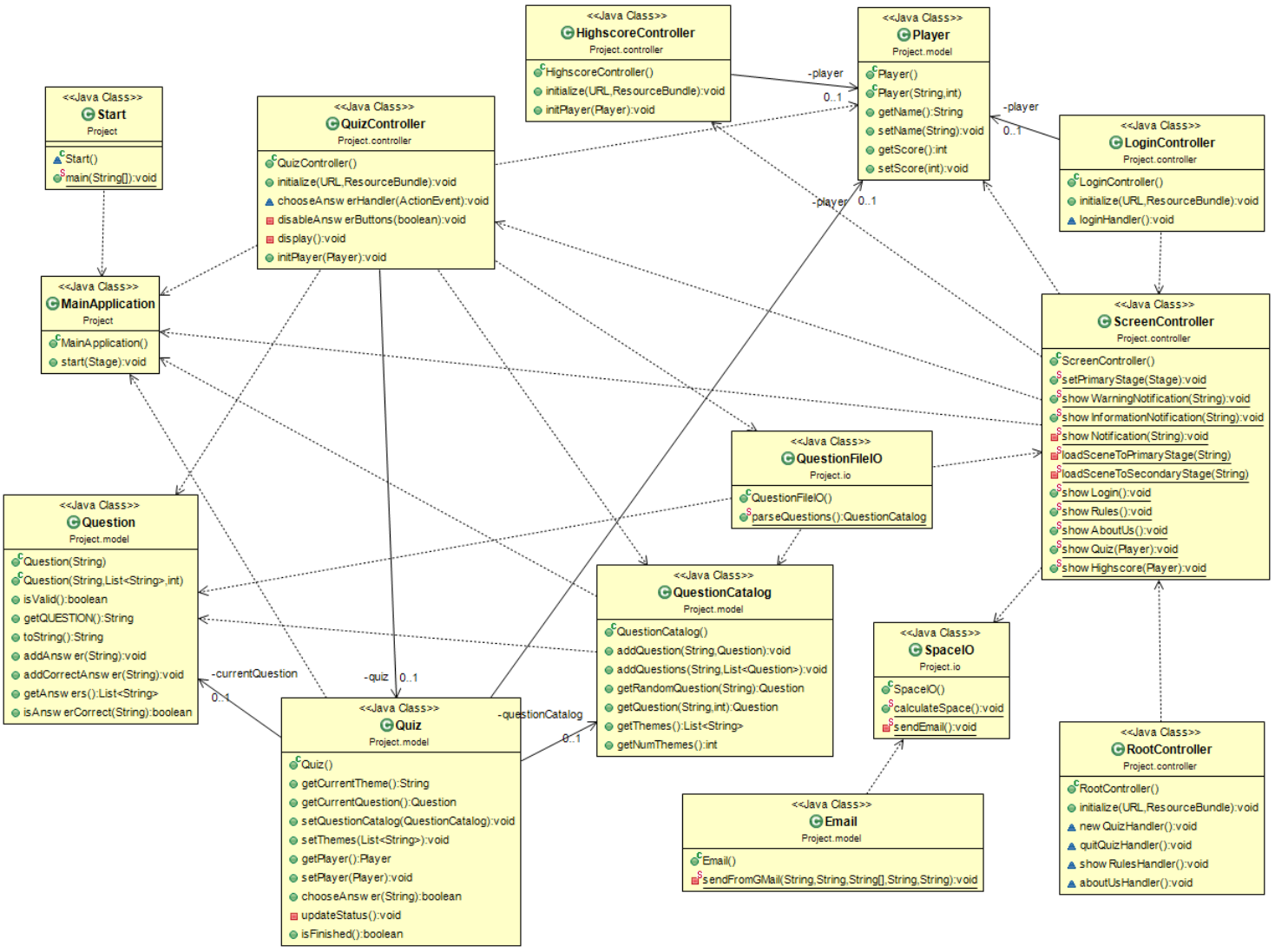
Siekiant gauti kuo tikslesnius duomenis, tiriamųjų imtis bus fiksuota – 2016 metais į KTU bakalauro studijas Informatikos fakultete priimtų pirmo kurso studentų skaičius. Jiems bus siūloma pasinaudoti testavimo platforma su pasirengiamaisiais Informacinių technologijų modulio egzamino klausimais. Šios programinės įrangos įdiegimo metu jų bus prašoma sutikti su specifiškai sumodeliuotomis EULA sąlygomis. Iš visų tyrimo dalyvių, sutikusių su galutinio vartotojo licencijos sutarties sąlygomis, bus paimama asmeninio įrenginio informacija – pastoviosios atminties dydis ir jame likusios laisvos vietos duomenys, tuo parodant galimą prieigą prie sisteminių resursų bei procesų.

Siekiant lokalizuoti šį tyrimą, EULA sutarties tekstas bus pateikiamas ne anglų, o lietuvių kalba - tai tyrimo atlikimo metu vis dar nėra dažnai sutinkamas atvejis praktikoje. Galutinės vartotojo licencijos sutarties tekste, kuris visa apimtimi yra pateikiamas priede Nr. 1, atspindi visos, pirmoje darbo dalyje pateiktos ir daugiausiai kritikos sulaukiančios savybės: EULA ilgis (apie 3000 žodžių), sudėtinga teisinė kalba, programinės įrangos kūrėjo atsakomybės ribojimas ir kita. Sutarties tekste informuojama, kad asmeniniai duomenys iš vartotojo bus renkami be detalesnio pagrindimo, kodėl jų reikia ir kam jie bus panaudoti. Tačiau šalia taip pat bus pateikiama nuoroda į pagalbinį puslapį, kuriame randama alternatyvi prieiga prie programos siūlomų resursų, išvengiant „kenksmingo“ programinio kodo paleidimo asmeninėje sistemoje.

Programinė įranga, reikalinga tyrimo tikslams pasiekti, bus sukurta naudojantis Java programavimo kalba. Kadangi vis daugiau interneto vartotojų turinį pasiekia per mobilius įrenginius, kurių didžioji dalis veikia su „Android“ operacine sistema, testavimo programa bus parengta tiek asmeniniams „Windows“ kompiuteriams, tiek ir mobiliems „Android“ įrenginiams. Veikimo principas abejoms platformoms bus panašus: įjungus šią programą, grafinėje vartotojo sąsajoje bus atidaromas testavimo modulis, kuris leis studentams pasitikrinti savo žinias, tuo tarpu fone bus automatiškai iškviečiamos kitos, pačios savaime nepavojingos, tačiau šiuo atveju „kenkėjiškiems“ tikslams panaudotos funkcijos/klasės. Pirmoji, kuri surinks duomenis apie asmeninio įrenginio informaciją – kietojo disko dydį ir jame likusią laisvą vietą; antroji – išsiųs surinktus duomenis į nurodytą serverį, kur jie bus saugomi iki apdorojimo tyrimo rezultatams.

3. INTERNETO VARTOTOJŲ PATIKLUMO GALUTINIO VARTOTOJO LICENCIJOS SUTARTIMI PROGRAMINĖS ĮRANGOS PROTOTIPO REALIZAVIMAS

Šiame skyriuje pateikiamas programinės įrangos, skirtos vartotojų pasitikėjimo EULA sutartimi tyrimui, realizavimo modelis. Kadangi tyrimui bus naudojamos dvi programos, asmeniniams kompiuteriams su „Windows“ operacine sistema ir mobiliesiems įrenginiams su „Android“ operacine sistema, atitinkamai pristatomi ir jų modeliai. Abiem atvejais iš pradžių pateikiama apibendrinta visos programos sistemos komponentų diagrama, o toliau trumpai pristatoma kiekviena dalis individualiai, pabrėžiant jos išskirtinumą ir, kur įmanoma, ryšį su paslėptu duomenų rinkimo ir išsiuntimo veiksmu – vienu iš šio tyrimo pagrindinių sudedamųjų komponentų.



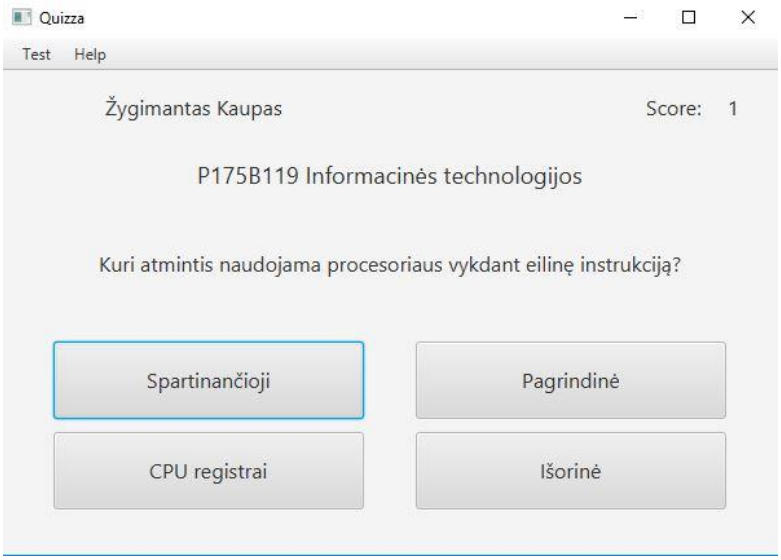
3.1 pav. „Windows“ operacinei sistemai skirtos programos sistemos komponentų diagrama

3.1. „Windows“ operacinei sistemai skirtos programinės įrangos realizacijos modelis

Visų „Windows“ operacinei sistemai skirtoje programoje naudojamų klasių ir metodų modelis pateiktas 3.1 paveiksle. Nors, kaip jau minėta ankstesniame skyriuje, tyrimui naudojama programa yra pakankamai nesudėtinga, tačiau schemoje matomas jos kompleksiškumas susidaro dėl grafinės vartotojo sąsajos bei pagrindinio vartotojui matomo funkcionalumo (ne šio darbo tyrimo objekto). Realizacijoje visos klasės suskirstytos į 6 grupes (paketus): pagrindinė globalių nustatymų dalis, programos valdymo dalis, įvesties ir išvesties į ekraną dalis, sudedamųjų komponentų (klasių) dalis, išorinių resursų (klausimų, logotipų) dalis, grafinės vartotojo sąsajos dalis. Pirmosios 4 grupės šiame skyriuje bus pristatytos individualiai, tuo tarpu iš likusių dviejų dalių paminėjimui svarbūs tik tam tikri aspektai.

Klausimai bus patalpinti .txt formato faile, kurį tyrimo programinė įranga atidarys per *QuestionFileIO* klasę. Paminėtina, kad kiekvienas klausimas turės po 4 atsakymų variantus. Patys klausimai kaip ir atsakymų eiliškumas vartotojui bus pateikiami kas kartą atsitiktine tvarka. Už teisingą atsakymą vartotojui bus skiriamas 1 taškas, už neteisingą – 0. Jeigu vartotojas nesurinks bent 5 taškų, ankstesniame skyriuje minėta nuoroda į pilną Informacinių technologijų modulio egzamino klausimų failą jiems nebus suteikiama. Kaip matoma, be savo paslėpto veikimo programa turi ir vartotojui naudingą ir įtarimų nesukeliantį funkcionalumą.

Grafinė vartotojo sąsajos dalis šiai, „Windows“ operacinei sistemai skirtai, programai sukurta „JavaFX“ paketo pagalba. Juo dizainas kuriamas .fxml tipo failais, kurie turi daug panašumų su „Android“ programinėje įrangoje apipavidalinimui naudojamais .xml tipo failais. 3.2 paveiksle matoma tyrimo programos atsakinėjimo aplinkos grafinė vartotojo sąsaja. Paminėtina, kad kol tiriamasis spręs jam pateiktus klausimus, tuo pat metu lygiagrečiai bus

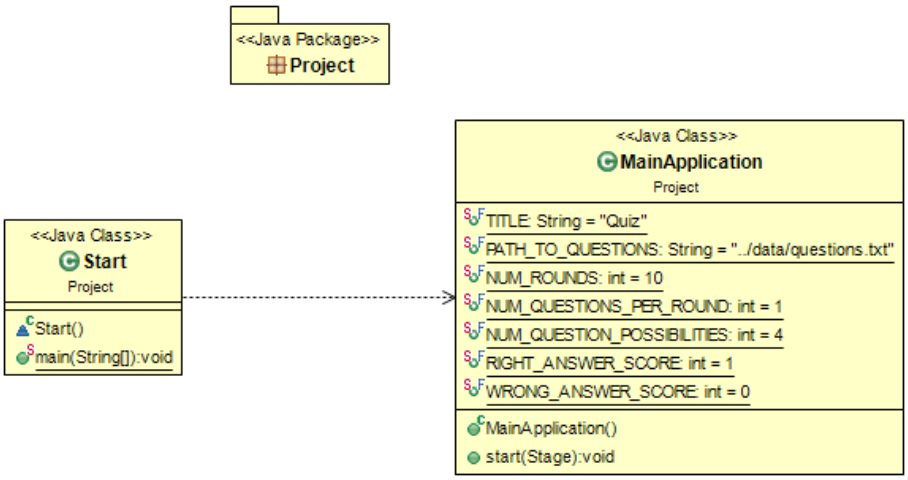


3.2 pav. Tyrimo programos „Windows“ sistemoje grafinė vartotojo sąsaja

surenkami ir išsiunčiami jo kompiuterio duomenys.

Detaliau analizuojant pagrindinę schemą, pateiktą 3.1 pav., nesunku pastebėti, kad *SpaceIO* ir *Email* klasės yra atsietos nuo likusių programos komponentų. Taip yra todėl, kad šios klasės pagrindiniam programos veikimui neturi jokios įtakos – jos atlieka tik kenkėjišką funkciją vartotojo atžvilgiu. Taikant tokią modulinę struktūrą įmanoma nesudėtingai keisti ar dalinti kenkėjišką kodą tarp įvairaus profilio „Java“ aplikacijų. Tyrimo metu naudojamas, jokios žalos vartotojo sistemai nedarantis ir jokių jautrių duomenų iš sistemos neplatinantis kodas, šioje testavimo programoje galėtų labai nesudėtingai būti pakeistas į daug pavojingesnį variantą. Toliau darbe trumpai pristatomas naudojamų klasių funkcionalumas pagal jų suskirstymą į paketus.

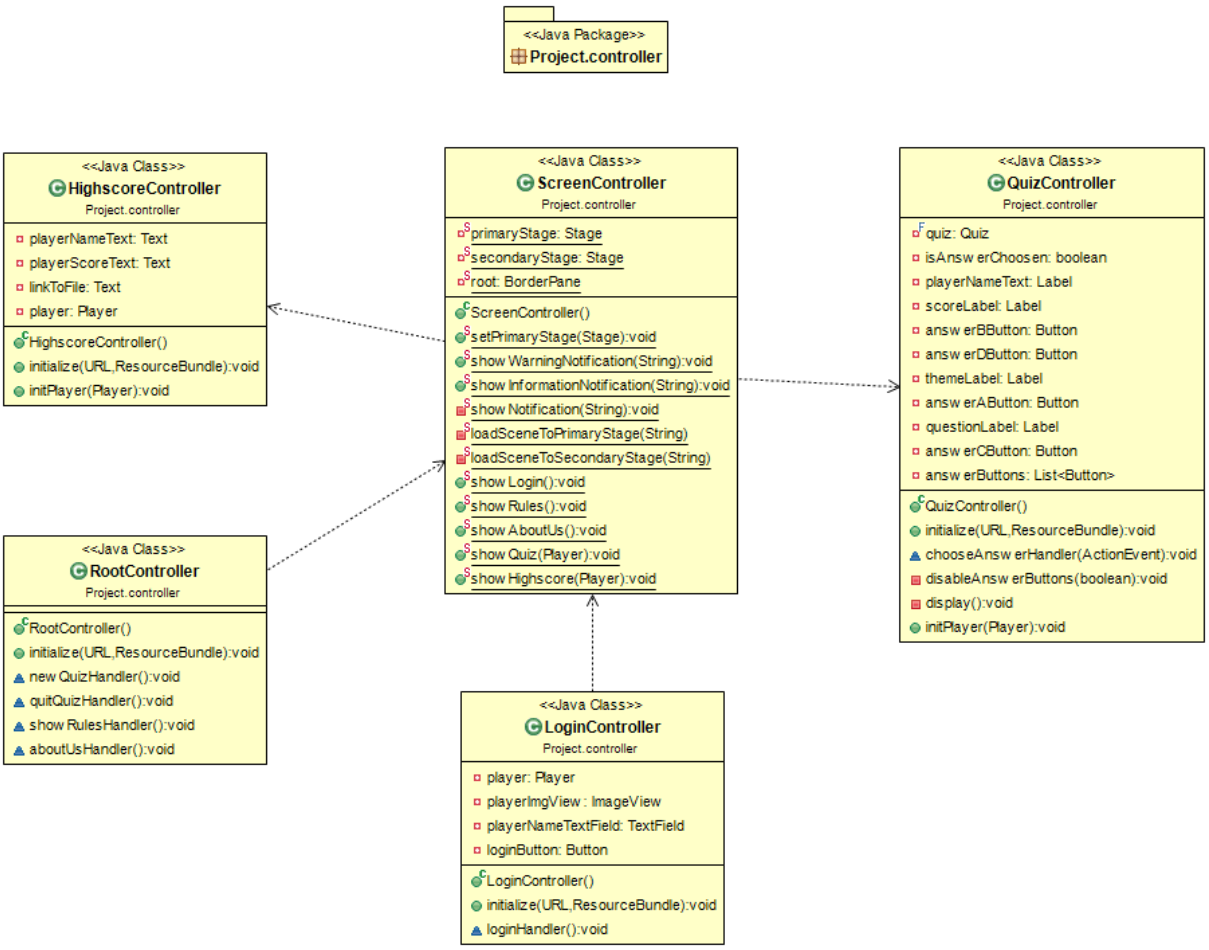
Pagrindinė globalių nustatymų dalis apima programos paleidimo bei globalius kintamuosius nustatančią klases (3.3 pav.). Pastarojoje galima pakeisti kiek klausimų bus pateikiama naudotojui, iš kelių skirtingų temų jie bus parenkami, kiek duodama atsakymo variantų ir kaip jie vertinami. Vertinant iš laiko perspektyvos, šiuo momentu testavimo programa dar neatlieka jokių paslėptų veiksmų.



3.3 pav. Globalių nustatymų paketo struktūra

Sekančiame žingsnyje programos kontrolė perduodama 5 valdiklio klasėms, kurių centre yra ekrano valdiklis *ScreenController*, atsakingas už grafinę vartotojo sąsają (3.4 pav.). Šiame etape prasideda kenkėjiškas programos funkcionalumas. Kai jau minėtas ekrano valdiklis programos pradžioje užkrauna vartotojo identifikavimo (vardo ir pavardės įvedimo) langą, lygiagrečiai paleidžiamas ir kompiuterio kietojo disko duomenų nuskaitymo metodas. Pastebėtina, kad siekiant tyrimo metu nepažeisti jo dalyvių konfidencialumo, studentų įvesti

asmens duomenys nėra sugrupuojami su jų programinės įrangos duomenimis ar kitaip išsiunčiami iš jų asmeninių kompiuterių.

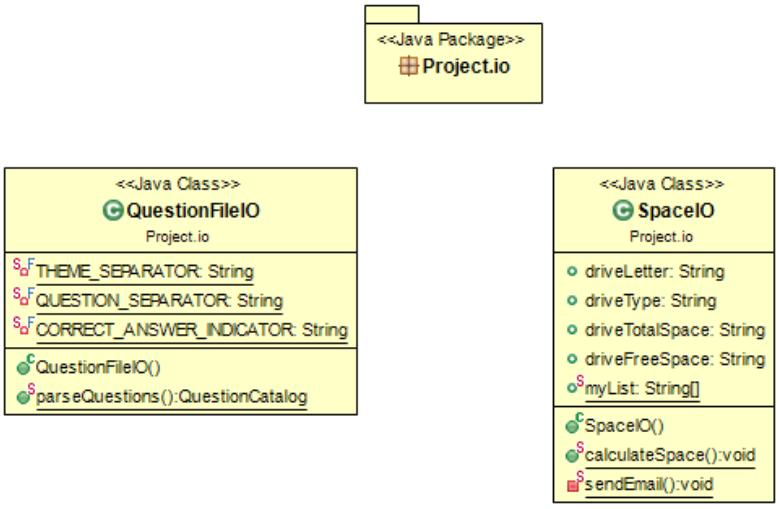


3.4 pav. Programos valdiklių paketo struktūra

Kietojo disko duomenų surinkimo klasė yra sugrupuota kartu su klausimų failo užkrovimo į programą klase, nors kaip matoma 3.5 pav. bendro ryšio šie sistemos komponentai neturi. Informacijos surinkimo klasė sukonfigūruota taip, kad iš sistemos gautų duomenis apie daugiausiai 3 kietuosius diskus (įskaitant ir CD/DVD, jeigu toks yra įdėtas, bei USB tipo atmintines). Kaip matoma iš pateiktos schemos, iš vartotojo sistemos nuskaitomi keturi parametrai: kietajam diskui paskirta raidė (identifikatorius), kietojo disko tipas, disko talpa ir laisvos vietos diske dydis. Sėkmingai surinkus šiuos duomenis jie yra perduodami į elektroninio laiško siuntimo metodą.

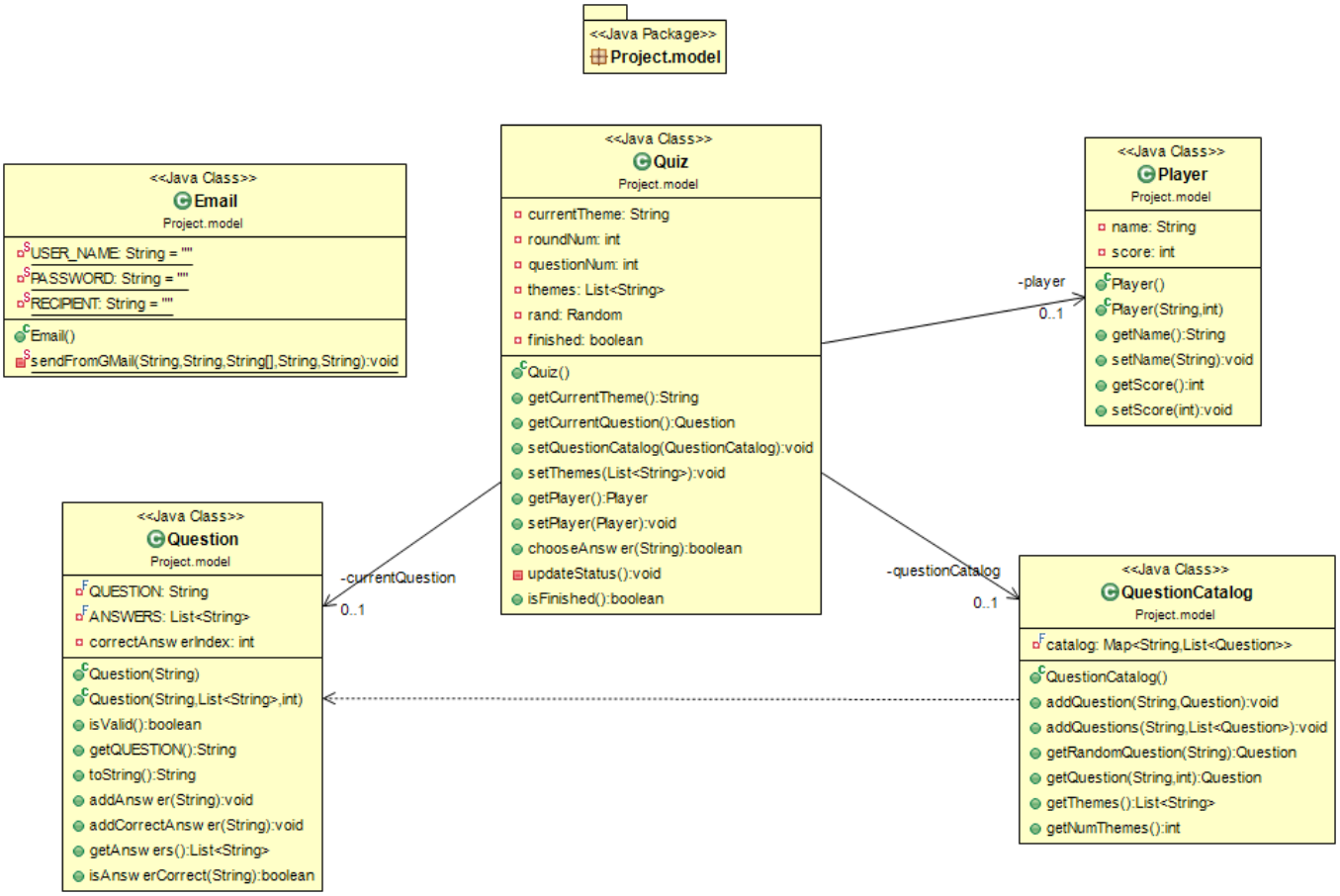
Paskutinis pristatomas klasių paketas apima komponentines (modelines) klasės. Jos yra pateiktos 3.6 pav. Standartinį programos funkcionalumą užtikrinančios klasės yra save paaiškinančios ir papildomas detalizavimas joms nebūtinas, tuo tarpu vartotojui nežinant elektroninį laišką su jo sistemos duomenimis išsiunčianti klasė pasinaudoja „Gmail“ pašto

kliento paslaugomis. Kaip matyti iš pateiktos schemos, klasė naudoja 3 statinius kintamuosius: vartotojo vardą, slaptažodį (pašto kliento, kurio vardu išsiunčiamas laiškas) bei laiško gavėją.



3.5 pav. Įvesties ir išvesties paketo struktūra

Šiam tyrimui atlikti bus sukurtos atskiros siuntėjo ir gavėjo pašto dėžutės, kurių duomenys bus statiškai įvedami į šią programą.

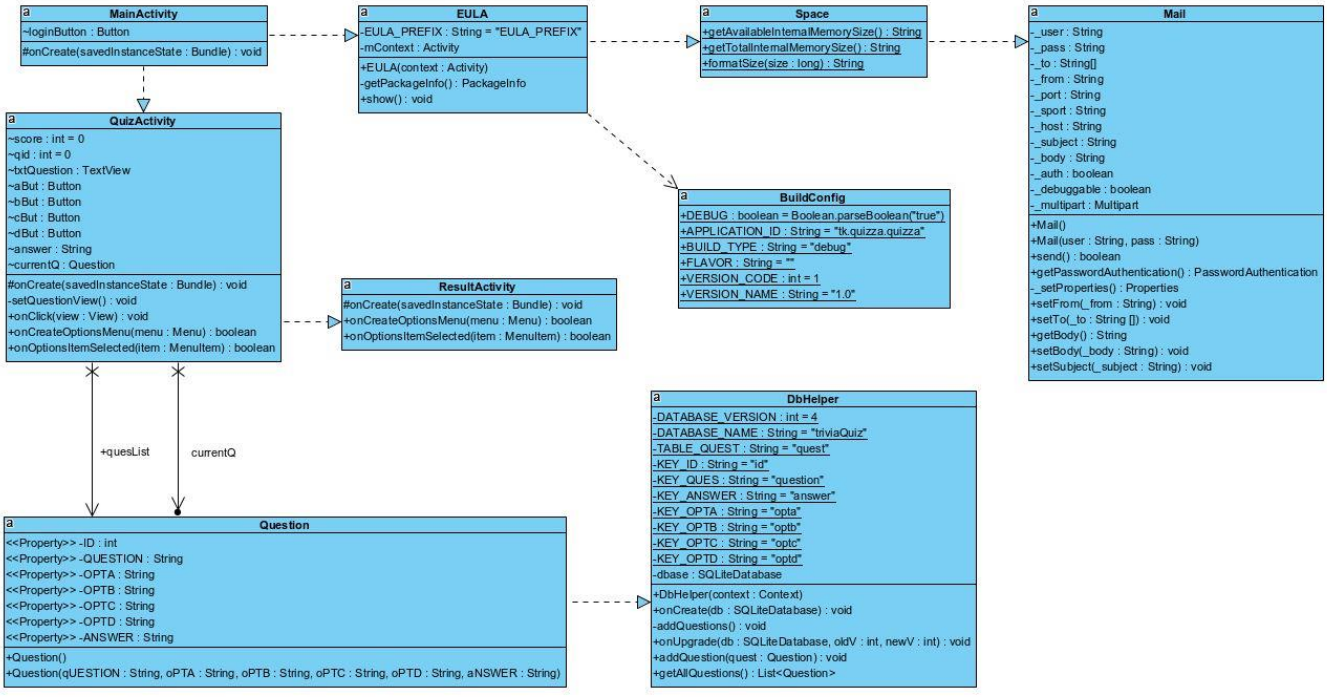


3.6 pav. Modelinių klasių paketo struktūra

3.2. „Android“ operacinei sistemai skirtos programinės įrangos realizacijos modelis

„Android“ sistemai pritaikyta programa savo pamatiniais principais bei funkcionalumu nesiskiria nuo „Windows“ operacinei sistemai skirtos versijos. Vis dėlto, panaudojant specifinius „Android“ resursus bus supaprastinta programos architektūra, optimizuotas jos veikimas bei sumažinta tikimybė, kad kodas neveiks dėl jo nesuderinamumo su konkrečiu mobiliu įrenginiu ar jo programinės įrangos versija. Visų „Android“ operacinei sistemai skirtoje programoje naudojamų klasių ir metodų modelis pateiktas 3.7 paveiksle. Jau iš pirmo žvilgsnio matoma, kad diagrama, palyginus su 3.1 paveiksle pateiktu „Windows“ atitikmeniu, yra akivaizdžiai paprastesnė. Taip yra todėl, kad grafinės vartotojo sąsajos valdymas „Android“ sistemoje yra intuityvesnis ir gali būti lengvai valdomas be papildomų klasių kūrimo.

3.7 paveiksle pateiktą diagramą galima detaliau išskaidyti dvejopai: pagal funkcionalumą arba pagal klasės tipą. Funkcionalumo prasme EULA ir kitos su ja susijusios klasės yra skirtos išimtinai tik šio tyrimo tikslui – įvertinti ar naudotojai skaito jiems pateikiamą licencijos sutartį bei, sutikimo atveju, paimti iš jų kietojo disko duomenis. Tuo tarpu klasės susijusios su *QuizActivity* yra naudojamos nekenkėjiškam ir vartotojo matomam programos veikimui išpildyti. Skirstant pagal klasės tipą šioje „Android“ programoje yra trys veiklos (angl. *activity*) klasės, kurios valdo programos veikimą pasitelkdamos kitų klasių funkcionalumą. Toliau bus detaliau pristatoma šios programos architektūra grupuojant pagal klasių



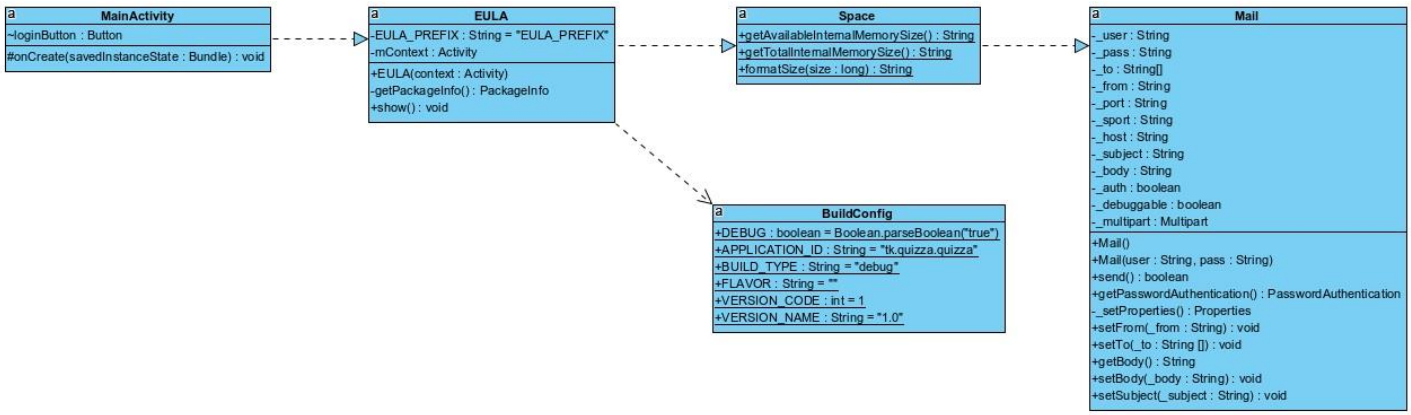
3.7 pav. „Android“ operacinei sistemai skirtos programos klasių diagrama

funkcionalumą.

Standartiškai kiekviena „Android“ programa startuoja *MainActivity* klasėje, kuri šiame projekte atlieka svarbų vaidmenį galutinio vartotojo licencijos sutarties parodyme bei vartotojų duomenų išsiuntime tyrimo autoriui. Kaskart naudotojui įsijungus šią „Android“ programą visų pirma yra iškviečiame EULA klasė, kuri:

1. Patikrina programos versiją;
2. Patikrina ar sistemos nustatymuose egzistuoja kintamasis *eulaKey*;
3. Jeigu anksčiau paminėtas kintamasis neegzistuoja arba jis nesutampa su programos versija – vartotojui parodomas EULA sutarties tekstas;
4. Jeigu vartotojas sutinka su pateiktu tekstu, iškviečiame *Space* klasė ir atnaujinamas *eulaKey* kintamasis, priešingu atveju programos paleidimas yra sustabdomas ir resursai nėra pasiekiami.

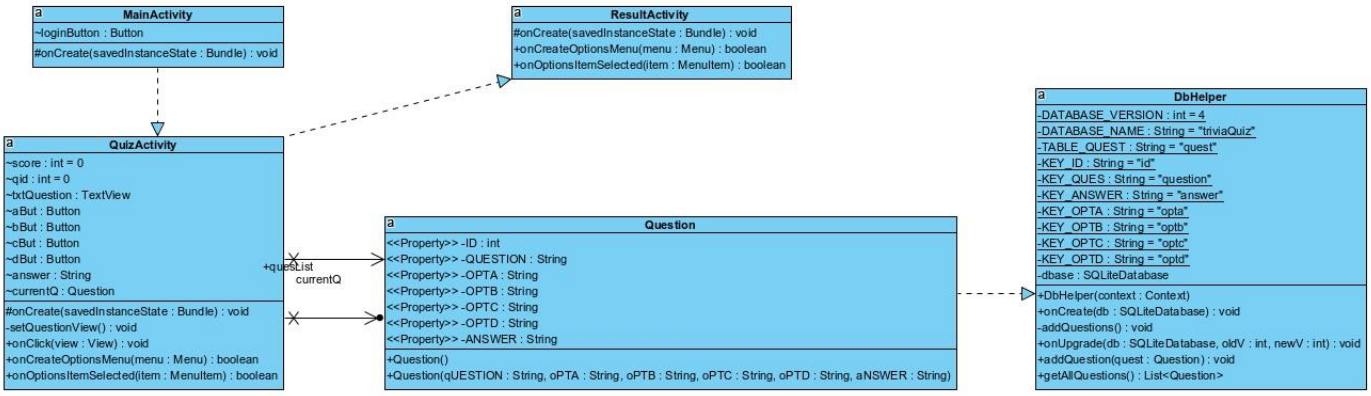
Tiek *Space*, tiek ir *Mail* klasės yra identiškos savo funkcionalumu „Windows“ programoje naudotoms *SpaceIO* ir *Email* klasėms. Tuo tarpu galimybė nesudėtingai išsaugoti kintamąjį „Android“ sistemoje, leidžia išvengti pakartotinio EULA teksto rodymo bei duomenų siuntimo nei ir tuo atveju jeigu programa yra paleidžiama iš naujo po sistemos perkrovimo. Paveiksle 3.8 pavaizduota aptartų klasių schema, kuri yra sąlyginai paprasta ir save paaiškinanti.



3.8 pav. Klasės, susijusios su EULA rodymų bei duomenų siuntimo „Android“ aplinkoje

Vartotojui sutikus su EULA sąlygomis ir paslėptam procesui išsiuntus kietojo disko duomenis į tyrėjo specialiai šiam tyrimui sukurtą pašto dėžutę, tolesnis programos veikimas perduodamas *QuizActivity* klasei, kuri reguliuoja klausimų pateikimą ekrane ir atsakymų registravimą (paveikslas 3.9). Kaip ir „Windows“ programos atveju, naudotojui pateikiami 10 klausimų atsitiktine tvarka su 4 atsakymų variantais. Jis turi atsakyti bent 5 iš jų teisingai, kad

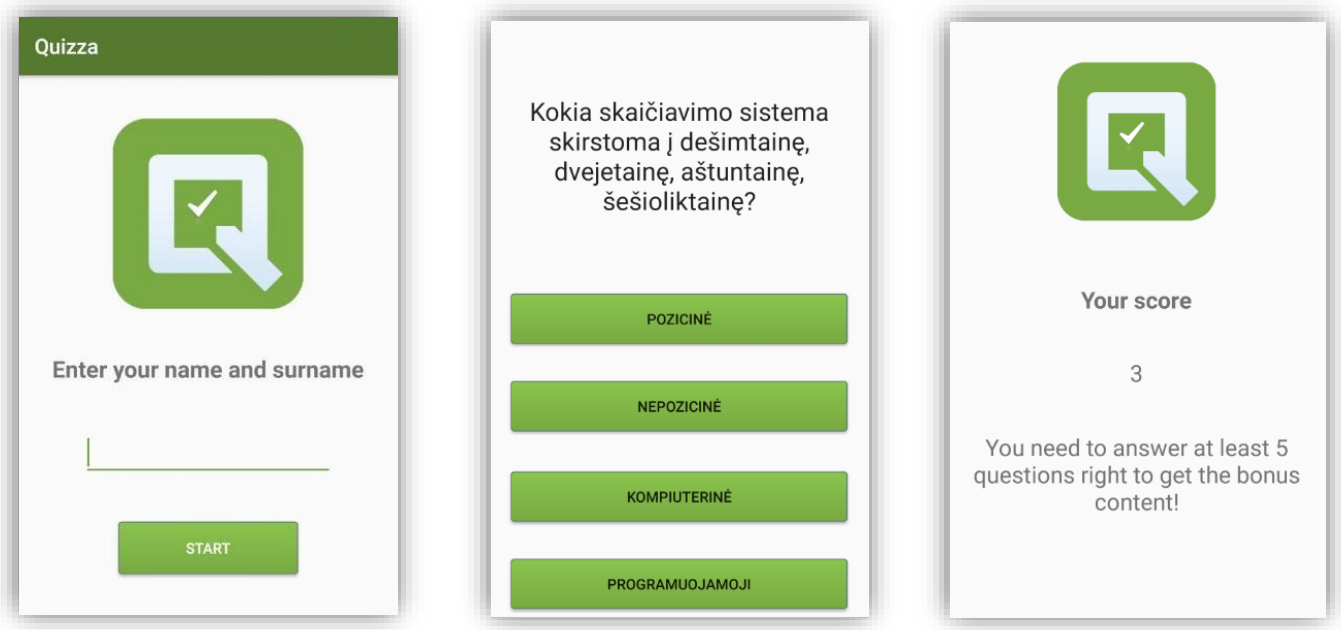
galutiniame rezultatų lange pamatytų nuorodą į failą su visais pasirengiamaisiais „Informacinių technologijų“ kurso egzamino klausimais. Vienas iš šios programos skirtumų nuo „Windows“



3.9 pav. Pagrindinio programos funkcionalumo klasės „Android“ aplinkoje

varianto yra toks, kad dėl „Android“ patogaus suderinamumo su „SQLite“ duomenų baze, klausimų saugojimui buvo panaudota būtent ši technologija. Esant poreikiui padidinti jų skaičių, atsakymų variantų skaičių ar perkelti šiuos duomenis į kitą programą, „SQLite“ naudojimas itin palengvintų tokį procesą.

„Android“ programoje grafinė vartotojo sąsaja susideda iš 3 langų: naudotojo vardo ir pavardės įvedimas (saugoma tik iki programos išjungimo, iš įrenginio neišsiunčiama), klausimų sprendimo lango bei rezultatų lango, kuriame atsakius į bent 5 klausimus teisingai



3.10 pav. „Android“ grafinės vartotojo sąsajos pavyzdžiai

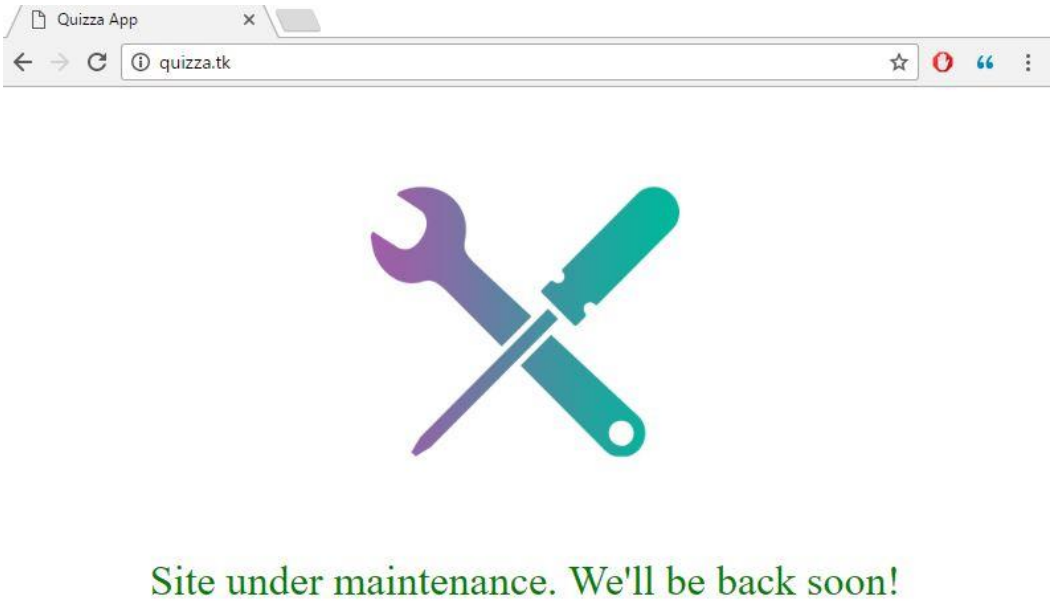
pateikiama nuoroda į išorinį resursą (nesaugoma įrenginyje). Šie langai pavaizduoti paveiksle 3.10. Vartotojui taip pat suteikiama galimybė pradėti testą iš naujo, tačiau nėra įmanoma grąžinti praėjusį klausimą pakartotinam atsakymui.

3.3. Tyrimo programinės įrangos išplatinimo aplinka

Siekiant atlikti sėkmingą eksperimentinį tyrimą vien tik parengtos programinė įrangos nepakanka – ne mažiau svarbus ir jos išplatinimo metodas. Norint kuo labiau atkartoti realius galimus scenarijus, nuspręsta sukurti fiktyvų internetinį programinės įrangos puslapį, kuriame būtų pasiekiami tiek įdiegimo failai, tiek ir dokumentas, į kurį nuorodą suteikiama teisingai atsakius į bent 5 klausimus testinėje programoje.

Fiktyvaus internetinio puslapio kūrimui buvo pasirinktos tik nemokamos visiems prieinamos priemonės: nemokama lietuviška priegloba (angl. *hosting*) bei nemokama domeno suteikimo paslauga. Nors šios paslaugos turi savo trūkumus, kaip kad suteikiamos vietos bei srauto apribojimus, galiojimo trukmę ir kt., tačiau egzistuoja ir tam tikri kenkėjiškai veiklai itin patrauklūs privalumai. Visų pirma, nemokėjimas už paslaugas leidžia sukurti daugelį tokių svetainių kopijų/alternatyvų, o taip pat neatliekant jokių finansinių perlaidų galima tik dar lengviau išlaikyti tokios sistemos savininko anonimiškumą registracijos metu pateikiant neegzistuojančio asmens duomenis.

Pagrindinis programinės įrangos puslapis (www.quizza.tk) viso tyrimo metu informuos apie laikinus jo atnaujinimo darbus (paveikslas 3.11). Tokia apgaulė buvo pasirinkta



3.11 pav. Fiktyvus programinės įrangos puslapis

dėl poros priežasčių. Visų pirma, šio eksperimentinio tyrimo tikslas yra vartotojų patiklumo internete nustatymas, o tam būtina surinkti bei įvertinti kiekybinius duomenis. Siekiant kuo didesnio jų įvairumo, šiame puslapyje bus patalpinti 6 vienas nuo kito nepriklausomi skaitliukai, skaičiuojantys, kiek kartų: atsiųsta „Windows“ sistemai skirta programėlė, atsiųsta „Android“ sistemai skirta programėlė, pasiektas visus klausimus talpinantis failas pagal nuorodą „Windows“ EULA tekste, pasiektas visus klausimus talpinantis failas pagal nuorodą „Android“ EULA tekste, pasiektas visus klausimus talpinantis failas išsprendus testą su „Windows“ skirta programa, pasiektas visus klausimus talpinantis failas išsprendus testą su „Android“ skirta programa.

Be kita ko, tvarkomo puslapio įvaizdis sukuria iliuziją, kad tai yra normaliai veikianti nuoroda, kuri tik šiuo metu yra neprieinama. Tuo tarpu kenkėjiškos programinės įrangos platintojui toks maketas leidžia sutaupyti laiko ir resursų kopijuojant ar kuriant fiktyvų puslapį su pilnu funkcionalumo išpildymu.

Kaip matoma iš pateikto paveikslo, jokios papildomos nuorodos pradiniame puslapyje nėra pateikiamos. Tiriamiesiems nuorodos į „Windows“ operacinei sistemai skirtą programą (www.quizza.tk/windows) ir „Android“ operacinei sistemai skirtą programą (www.quizza.tk/android) bus išplatintos iš kurso dėstytojo pašto dėžutės. Nors šiuo atveju siuntėjo laukas bus nesuklastotas, tačiau praktikoje dažnai pasitaiko atvejų, kai ši informacija yra sufalsifikuojama ar nuo žinomo siuntėjo skiriasi tik minimaliomis detalėmis. Tokiu būdų taip pat bus patikrinama ar elektroniniu paštu siunčiamos nežinomos nuorodos vis vien yra aplankomos.

3.4. Tyrimo programinės įrangos prototipo realizavimo išvados

Interneto vartotojų patiklumo eksperimentiniam tyrimui bus naudojamos dvi savo veikimo principais itin panašios programos: asmeniniams kompiuteriams su „Windows“ operacine sistema ir mobiliesiems įrenginiams su „Android“ operacine sistema. Jose bus interaktyviai pateikti KTU bakalauro studijų Informatikos fakulteto Informacinių technologijų kurso egzamino pasirengiamieji klausimai. Studentai norėdami pasiekti pilną klausimų sąrašą turės arba įsidiegti programą, sutikti su specifiškai sumodeliuotomis žalingomis EULA sąlygomis, atsakyti bent 5 iš 10 klausimų teisingai ir taip gauti nuorodą į pageidaujamą resursą, arba perskaitę EULĄ tekstą pasiekti tą patį resursą per nuorodą jame.

Jeigu vartotojas sutiks su galutinio vartotojo sutartimi bet kurioje iš sukurtų programų, jam sprendžiant testą programa nepastebimai surinks duomenis apie sistemos kietojo disko duomenis ir išsiųs juos į išorinę specifiškai šiam tyrimui sukurtą pašto dėžutę. Naudotojas apie

šį veiksmą nebus informuojamas. Duomenys kiek tiriamųjų atsisiuntė programą, išsprendė testą sėkmingai ir taip pasiekė pageidaujamą resursą iš „Windows“ ar „Android“ įrenginio, ar be programos įdiegimo pasinaudojo nuoroda EULA tekste, bus analizuojami kitoje šio darbo dalyje.

Tiek „Windows“ operacinei sistemai, tiek ir mobiliesiems įrenginiams su „Android“ operacine sistema parengtos programos bus išplatintos per fiktyvų internetinį puslapį, kuris taip pat sukurtas specifiškai tik šio tyrimo atlikimui. Tiriamiesiems tikslios nuorodos, kur galima atsisiųsti šias programas bus pateiktos elektroniniame laiške iš kurso dėstytojo pašto dėžutės. Nors šiuo atveju siuntėjas ir nėra suklastotas (tokia galimybė praktikoje egzistuoja), vis dėlto bus tikrinama ar gavę laišką su įtartinomis nuorodomis tiriamieji jas vis vien aplankys.

4. INTERNETO VARTOTOJŲ PATIKLUMO GALUTINIO VARTOTOJO LICENCIJOS SUTARTIMI EKSPERIMENTINIS TYRIMAS

Šiame skyriuje pateikiami eksperimentinio tyrimo rezultatai. Pradžioje detalizuojama eksperimento vykdymo aplinka, toliau pristatomi gauti duomenys, juos grupuojant pagal naudotos operacinės sistemos tipą. Skyriaus pabaigoje atliekama surinktos informacijos analizė didžiausią dėmesį skiriant informacijos ir informacinių technologijų saugumui. Pabrėžiama kokią įtaką stebėtas eksperimento dalyvių elgesys ar naudota sistemos konfigūracija turi konfidencialios informacijos apsaugai.

4.1. Eksperimento vykdymas

Interneto vartotojų patiklumo EULA sutartimi eksperimentinis tyrimas buvo pradėtas 2016 m. gruodžio 5 d., kuomet KTU Informatikos fakulteto pirmo bakalauro studijų kurso studentams buvo išplatintas elektroninis laiškas (pav. 4.1), kviečiantis pasitikrinti Informacinių technologijų modulio egzamino žinias. Jame buvo pateiktos nuorodos tiek į „Windows“ operacinei sistemai skirtą programą, tiek ir „Android“ operacinės sistemos analogą. Taip pat laiške buvo paaiškintos sąlygos, kurias išpildžius pasiekiamas papildomas turinys.

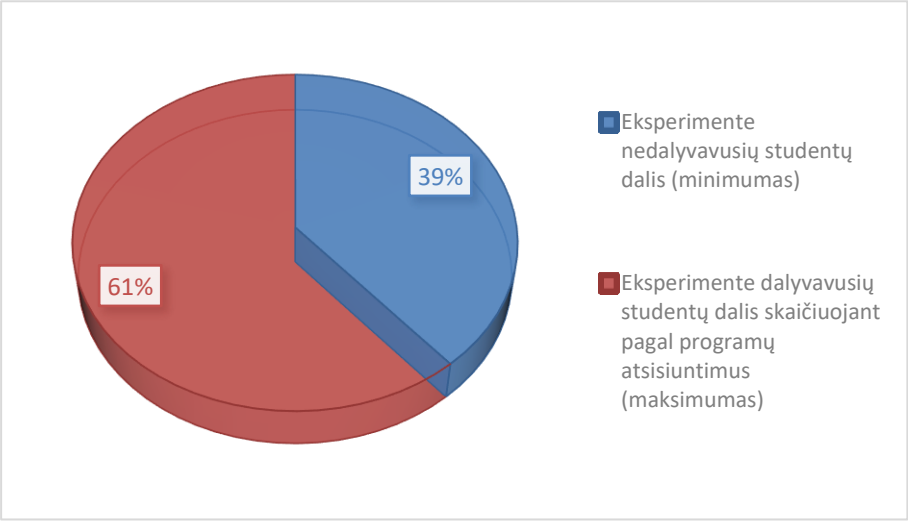
Vis dėlto, tame pačiame pranešime pateikiamos ir indikacijos, kad siūloma programine įranga nereikėtų pasitikėti besąlygiškai. Visų pirma, tai nėra komercinė ar universiteto sukurta/palaikoma žinių pasitikrinimo platforma. Vertinant iš informacijos saugos perspektyvos, bet kokią savanoriškais pagrindais sukurtą programinę įrangą reikėtų diegti į asmenines sistemas tik gerai įvertinus jos patikimumo lygį, esant galimybei naudoti saugią aplinką (virtualią mašiną) ar bent papildomai pasitikrinti, jog siuntėjas tikrai asmeniškai pasidalino nuoroda ar jos įdiegimo failu. Būtina pastebėti, kad 4.1 paveiksle matomą elektroninį laišką išsiuntęs dėstytojas per paskaitas apie šią žinių patikrinimo galimybę studentams neužsiminė. Dar daugiau, pranešimo turinyje matomos gramatinės klaidos (itin dažna savybė „*phishing*“ tipo laiškuose), o pridėta šypsena indikuoja neformalų teksto stilių, nebūdingą pateikiamam kontekstui. Taip pat siuntėjo parašas nėra pilnas – trūksta pareigų, oficialių įstaigos duomenų, papildomų kontaktų bei logotipo.

Pirminiame pranešime apie programinė įrangos naudojimosi terminus (ir tuo pačiu eksperimento trukmę) nebuvo užsimenama, tačiau tyrimas buvo pradėtas semestro pabaigoje, o tai natūraliai paskatino studentus pasinaudoti esama galimybe. Eksperimentui buvo skiriamos dvi savaitės po kurių tiriamieji buvo supažindinti su jo metodologija bei preliminariais rezultatais. Detalūs tyrimo rezultatai pateikiami kitoje šio skyriaus dalyje.

4.1 pav. Tyrimo dalyviams išplatintas elektroninis laiškas

4.2. Eksperimento rezultatai

Eksperimentui parengtų programų įdiegimo failai iš viso buvo atsisiųsti 400 kartų. Darant prielaidą, kad kiekvienas atsisiuntimas buvo atliktas unikalaus vartotojo, eksperimente iš viso dalyvavo 61% numatytų tiriamųjų (4.2 pav.). Vis dėlto, tikėtina, jog dalis studentų naudojo programinę įrangą tiek savo asmeniniuose kompiuteriuose, tiek ir mobiliuosiuose įrenginiuose, todėl realus tyrime dalyvavusių asmenų skaičius buvo apie 50% visos tiriamųjų imties.



4.2 pav. Tyrimo dalyvių aktyvumas

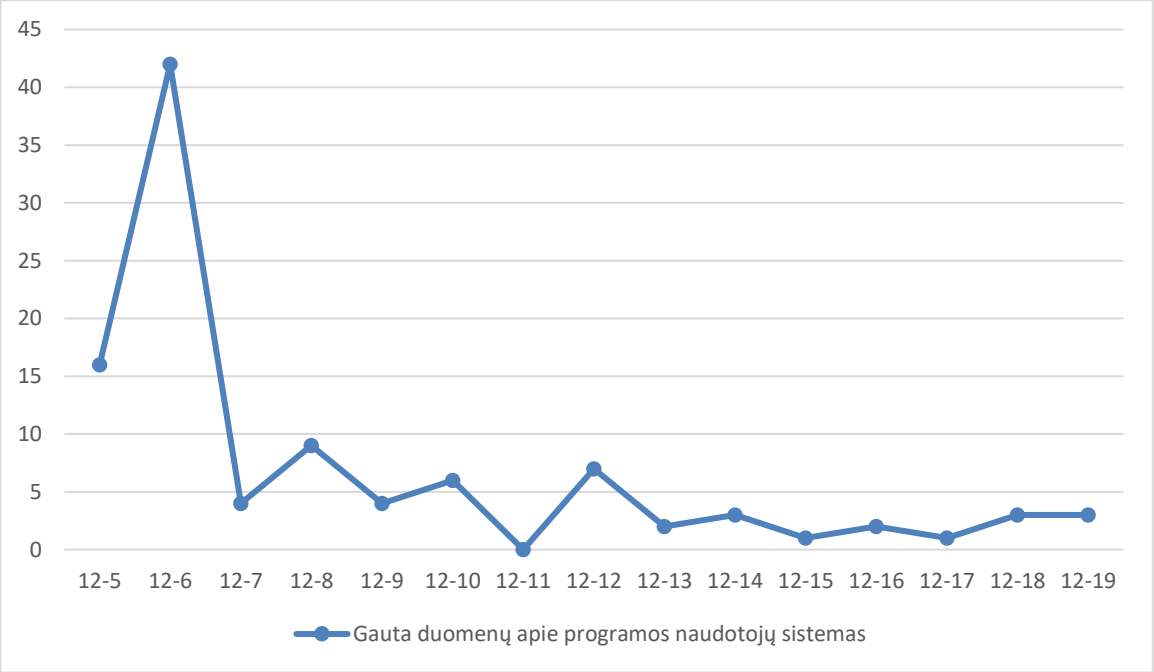
Kaip matoma pirmoje lentelėje, „Windows“ operacinei sistemai skirtos eksperimentinės programos versijos įdiegimo failas buvo atsiųstas 245 kartus, tačiau papildomas turinys teisingai išsprendus testinius klausimus pasiektas tik vos daugiau nei 50% tokių atsisiuntimų atvejų. Vis dėlto, šis skirtumas nerodo, kad likusi dalis studentų perskaitė galutinio vartotojo licencijos sutartį ir pasirinko alternatyvų būdą pasiekti papildomą resursą per nuorodą EULA tekste. Viso tyrimo metu ji nebuvo nė karto aplankyta.

1 lentelė. „Windows“ operacinei sistemai skirtos programinės įrangos naudojimo statistika

Įdiegimo failas atsisiųstas	Testas išlaikytas	Duomenys apie įrenginį gauti	EULA perskaityta
245	130	103	0

Kaip matoma iš pateiktos lentelės, buvo gauti detalūs duomenys apie vartotojų kietųjų diskų duomenis iš 103 sistemų – beveik 80% nuo visų išlaikiusiųjų testą. 4.2 grafike matomas gautų duomenų apie „Windows“ programos naudotojų sistemas kitimas tyrimo laikotarpiu. Informacija iš 62 įrenginių (60% viso kiekio) buvo surinkta per pirmas 24 valandas. Šie duomenys leidžia daryti dvi išvadas:

1. Asmeniniai kompiuteriai dažniausiai nėra tinkamai sukonfigūruoti, nenaudoja reikalingų IT saugos sprendimų ir be vartotojo aktyvių veiksmų negali apsaugoti privačios informacijos. Atsižvelgiant į tai, kad šios paprastos programinės įrangos atveju beveik 80% įrenginių ne tik be kliūčių įvykdė kenksmingą kodą, bet ir vartotojui to nežinant išsiuntė duomenis į išorę, realu prognozuoti, jog profesionalaus įsilaužėlio parašytas kodas gali pasiekti efektyvumą artimą 100%.
2. Statistikoje matomas naudotojų aktyvumo pikas pirmąją parą yra itin palankus veiksnys kenkėjiškam programišiui. Tikėtina, jog bet kokio naujo pažeidžiamumo (angl. *zero-day*), naujos apgaulės schemos ar naujai modifikuotos kenkėjiškos programinės įrangos poveikis iki pasirodant atnaujinimams bei naujiems antivirusinės įrangos parašams (angl. *signatures*) duos gerų rezultatų puolančiajam.



4.3 pav. Gautų duomenų apie „Windows“ programos naudotojų sistemas kitimas tyrimo laikotarpiu

„Android“ operacinei sistemai skirtos aplikacijos rezultatai nedaug skiriasi nuo jau analizuotos „Windows“ versijos. Kaip matoma 2 lentelėje, mobiliesiems įrenginiams skirta programėle nebuvo tokia populiari ir iš viso ji atsisiųsta tik 155 kartus (-37% lyginant su „Windows“). Taip pat testas joje išlaikytas mažiau nei pusei atsisiuntimų atvejų – 47%. Tikėtina,

2 lentelė. „Android“ operacinei sistemai skirtos programinės įrangos naudojimo statistika

Įdiegimo failas atsisiųstas	Testas išlaikytas	Duomenys apie įrenginį gauti	EULA perskaityta
155	73	50	0

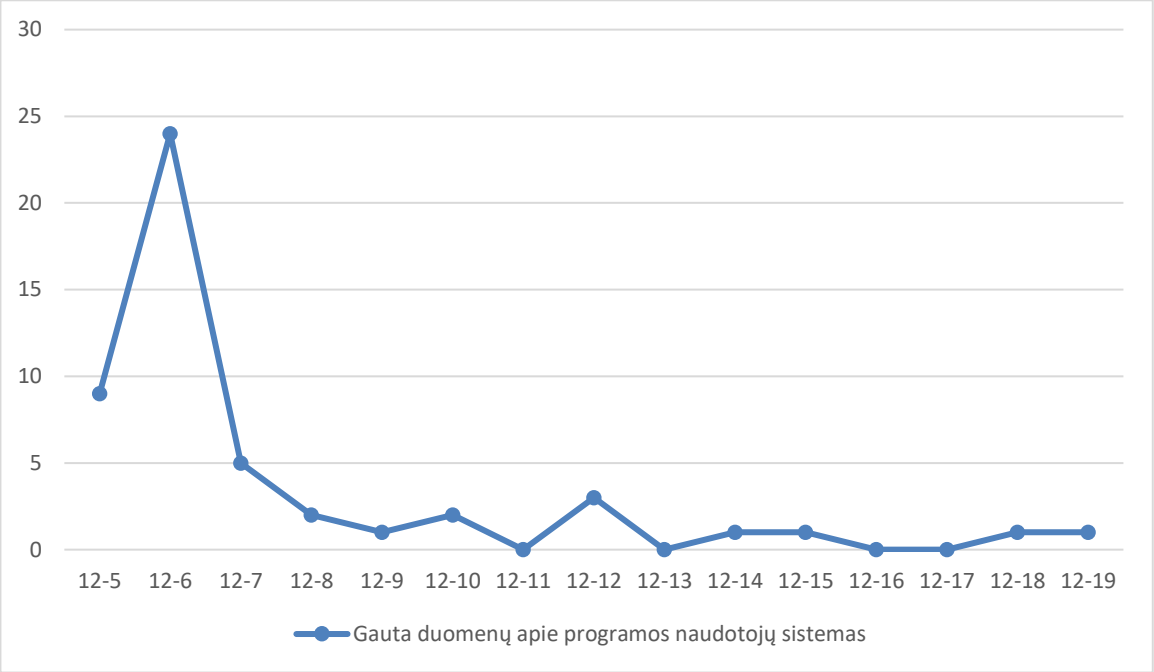
kad šis sumažėjimas yra dėl to, kad dalis studentų atsisiuntė „Android“ programą tik norėdami pažiūrėti skirtumus su „Windows“ versija. Kadangi abiem atvejais buvo naudojami tie patys klausimai, papildomos motyvacijos sėkmingai užbaigti testą ir mobiliajame įrenginyje nebuvo. Programinės įrangos naudojimo statistika pagal operacinę sistemą pateikiama 3 lentelėje.

3 lentelė. Programinės įrangos naudojimo statistika pagal operacinę sistemą

Įdiegimo failas atsisiųstas	Windows įrenginiai %	Android įrenginiai %	Testas išlaikytas	Windows įrenginiai %	Android įrenginiai %	Duomenys apie įrenginį gauti	Windows įrenginiai %	Android įrenginiai %	Eula perskaityta (bendrai)
400	61,25	38,75	203	64	36	153	67	33	0

Vertinant gautų duomenų iš „Android“ įrenginių apimtį, netikėtai ji siekia tik 70% išlaikytų testų programėlėje skaičiui. Tai yra net 10% mažiau nei „Windows“ operacinės sistemos atveju, nepaisant to, kad mobiliuosiuose įrenginiuose dažniausiai nėra jokių papildomų saugumą užtikrinančių programų kaip antivirusai ar ugniasienės. Daugiausiai tikėtina, kad tokią statistiką lėmė tai, jog testas buvo sprendžiamas neprijungus įrenginio prie interneto ryšio arba tiriamieji sėkmingai išsprendę užduotis neišsisaugodavo papildomų resursų failo ir daugiau nei vieną kartą naudodavosi gauta nuoroda taip padidindami išlaikyto testo skaitiklio reikšmę (antrą kartą duomenys iš to pačio įrenginio nebuvo siunčiami).

4.3 grafike matomas gautų duomenų apie „Android“ programos naudotojų sistemas kitimas tyrimo laikotarpiu. Per pirmas 24 valandas gautų duomenų santykis buvo dar didesnis nei „Windows“ atveju – 66% (33 įrenginiai). Pastebėtina, kad „Android“ operacinei sistemai pritaikytos kenkėjiškos programinės įrangos kiekis tik auga, todėl jau aptarta saugumo problematika, susijusi su vartotojų siekiu kuo greičiau pabandyti turimas aplikacijas, gautos statistikos kontekste tampa dar grėsmingesnė. Dar daugiau, kaip ir „Windows“ atveju nė vienas programėlės naudotojas neperskaitė galutinio vartotojo licencijos sutarties ir neaplankė joje paminėtos nuorodos į papildomą resursą. Atliktas eksperimentas ne tik patvirtino prielaidą, jog praktikoje įprasta sutikti su EULA sąlygomis jų neperskaičius, tačiau atskleidė ir daugiau aktualių vartotojų elgesio niuansų, kurie gali turėti reikšmingos įtakos privačios informacijos ar informacinių technologijų saugumui.



4.4 pav. Gautų duomenų apie „Android“ programos naudotojų sistemas kitimas tyrimo laikotarpiu

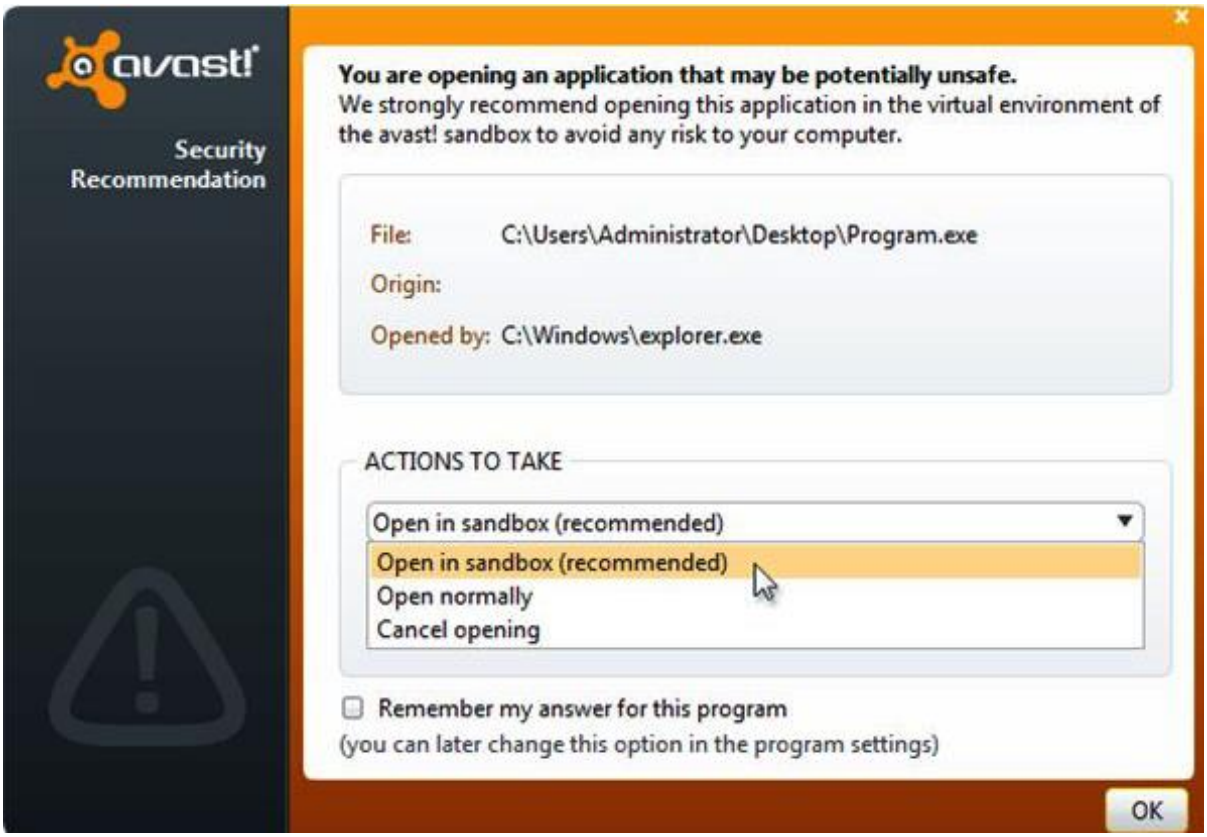
4.3. Eksperimento metu gautos informacijos analizė

Atliekant šios kenkėjiškos programinės įrangos kūrimo bei testavimo veiksmus buvo pastebėti itin neprognozuojami antivirusinių programų sprendimai jos įdiegimo ar duomenų išsiuntimo į išorę atžvilgiu. Svarbu paminėti, kad pradėjus „Quizza“ diegimo procesą „Windows“ operacinėje sistemoje pasirodydavo įspėjamasis pranešimas dėl nepatikimos programos veiklos. Taip nutikdavo todėl, kad aplikacijos kodas nebuvo pasirašytas su jokiu galiojančiu sertifikatu. Pastebėtina, kad šios mokamos paslaugos tikslas yra patvirtini, kad programa yra sukurta būtent tam tikros kompanijos ar asmens ir jos kodas po to nebuvo neautorizuotai pakeistas. Net ir turimas sertifikatas negarantuoja, jog programa nėra kenkėjiška ar neturi didelių saugumo sprangų, dėl kurių galėtų būti sukompromituota informacijos ar IT technologijų sauga.

Kai kurie dažnai naudojami IT saugumo sprendimai, pavyzdžiui, „Windows Defender“, nuo sėkmingo programos įdiegimo momento nerodydavo vartotojui jokių perspėjimų dėl galimai žalingos veiklos, tuo pačiu nestabdydavo ir duomenų išsiuntimo į išorę proceso. Kiti komerciniai produktai, priklausomai nuo jų versijos, arba parodydavo papildomą saugumo pranešimą (kartais paprašydavo vartotojo patvirtinimo paleidžiant programą), arba atkartodavo „Windows Defender“ veiksmus. Kadangi „Quizza“ skaitmeninis parašas/maišos

kodas (*angl. hash*) nebuvo įtrauktas į antivirusinių programų duomenų bazes, dažnu atveju jos neblokuodavo programos veikimo.

Tuo tarpu itin populiari „Avast“ antivirusinė programa, kuri dažname namų kompiuteryje yra naudojama dėl patogios vartotojo sąsajos, gerų rekomendacijų bei mažesnio poveikio sistemos spartai [45], eksperimento metu pademonstravo itin nevienareikšmiškus rezultatus. Kartais prieš paleidžiant „Quizza“ programą būdavo parodomas įspėjimas rinktis smėlio dėžės (angl. *sandbox*) rėžimą (pav. 4.4), retais atvejais buvo parodytas kodo tikrinimo pranešimas, kuris informuodavo kompiuterio naudotoją apie laikiną (30 minučių) programos



4.4 pav. „Avast“ smėlio dėžės pasirinkimo dialogas

paleidimo sustabdymą. Įdomu, kad net ir skirtinguose kompiuteriuose naudojant tą pačią „Avast“ versiją su identiška duomenų baze rezultatai ne visada buvo vienodi. Dar daugiau, kenkėjiškai programai be įrenginio savininko žinios siunčiant elektroninį laišką su jo privačiais duomenimis, „Avast“ kartais pabaigoje pridėdavo tokį tekstą: „---Šis elektroninis laiškas buvo patikrintas nuo virusų „Avast“ antivirusine programa. https://www.avast.com/antivirus“ (angl. *“---This email has been checked for viruses by Avast antivirus software. https://www.avast.com/antivirus”*). Nors įterptas tekstas nemelavo ir išeinančiame laiške virusų tikrai nebuvo, tačiau pridedamą saugumo patvirtinimą prie privačių duomenų pasisavinimo veiksmo galima vertinti kaip ironišką ir tai nesuteikia daugiau pasitikėjimo šiuo produktu.

Eksperimentas taip pat atskleidė, kad net ir IT srityje studijuojantys asmenys (tikėtina, jog turintys daugiau žinių bei įgūdžių nei vidutinis interneto naudotojas) mažai dėmesio skiria savo asmeninių sistemų saugumui. Išanalizavus gautą informaciją apie kietųjų diskų duomenis, matoma, jog „Quizza“ programa nė karto nebuvo įdiegta į nuo pagrindinės sistemos atribotą virtualią mašiną. Mažiausias užfiksuotas kietojo disko talpos rodiklis (neįtraukiant padalintų diskų ar daugiau nei 1 rasto fizinio įrenginio) – 128 GB. Nors nėra techninių kliūčių tokio dydžio virtualiai mašinai, tačiau (ypač namų kompiuteryje) tai nėra dažnai sutinkamas variantas be to šis dydis atitinka fizinės įrangos parametrus, tuo tarpu praktikoje virtualių mašinų talpa dažniausiai yra 10 kartotinis. Nepaisant to, kad šis sprendimas yra vis dažniau naudojamas komercinėje veikloje, individualūs vartotojai jo teikiamais privalumais (ypač IT saugos srityje) vis dar nėra linkę naudotis.

Gauti duomenys rodo, kad dažnas vartotojas dirbdamas kompiuteriu turi prisijungęs ir bent vieną USB atmintinę. Toks elgesio modelis, vertinant iš IT saugumo perspektyvos, gali turėti neigiamų pasekmių bei išplėsti tolimesnių atakos vektorių sąrašą. USB atmintinės yra potenciali kenkėjiško kodo platinimo aplinka, ypač jeigu jos bent kartais yra prijungiamos prie neapsaugotų, viešai prieinamų ar jau užkrėstų kompiuterių. Įsilaužėliui nebūtų sudėtinga modifikuoti „Quizza“ programą, kad ji, gavus duomenų apie prie sistemos prijungtą atminties laikmeną, be jau aprašyto funkcionalumo patalpintų ir kirmino (angl. *worm*) tipo kodą joje.

Ypač stebina tai, kad net ir paskelbus informaciją apie šį eksperimentą jo dalyviams, programos naudojimas nesustojo ir vis dar buvo gaunami nauji duomenys iš sistemų į kurias „Quizza“ programa buvo įrašyta po gruodžio 20 d. Net 14 naujų elektroninių laiškų buvo gauta iš „Windows“ operacinės sistemos įrenginių bei 3 iš „Android“. Paskutinis duomenų siuntimas iš asmeninio kompiuterio užfiksuotas vasario 19 d. – beveik po 2 mėnesių nuo eksperimento metodikos paviešinimo dienos. Įdomu, kad pastarasis elektroninis laiškas taip pat buvo pažymėtas jau aptartu „Avast“ antivirusinės programos parašu, tik šįkart jau be šypsenos gale. Galima tik spėti ar šiuos paskutinius 14-17 (priklausomai nuo to ar „Android“ programėlė buvo naudota tų pačių asmenų, kurie naudojosi ir „Windows“ versija) įsirašiusiųjų „Quizza“ programą nepasiekė informacija apie atliekamą eksperimentą, ar jie net žinodami, jog buvo apgauti vieną kartą, vis vien nusprendė išbandyti viską savo sistemoje. Bet kuriuo atveju tokia žmonių elgesio tendencija yra palanki įsilaužėliams. Pasirodžius naujoms kenkėjiškoms programoms ar socialinės inžinerijos metodams informacijos sklaidos problema tampa svarbiu efektyvumo veiksniu, tuo tarpu perdėtas pasitikėjimas internete randama informacija garantuoja vartotojo sistemos ar duomenų saugos pažeidimą. Vis dėlto, tarp visų tiriamųjų buvo vienas studentas, kuriam informacijos apie „Quizza“ programą išplatinimo metodas pasirodė įtartinas. Nors jis ir neperskaitė EULA sąlygų bei nepasiekė norimo failo alternatyviu būdų,

tačiau, kaip pats teigė, programos į savo kompiuterį neįdiegė bei nuorodos, gautos teisingai išsprendus testavimo klausimus, iš kolegų neprašė – tiesiog nusirašė klausimus iš draugo kompiuterio. Galima bent pasidžiaugti, kad pasitikėjimas internete pateikta informacija nėra absoliutus.

4.4. Eksperimentinio tyrimo apibendrinimas

Interneto vartotojų patiklumo EULA sutartimi eksperimentinis tyrimas buvo pradėtas 2016 m. gruodžio 5 d., kai KTU Informatikos fakulteto pirmo bakalauro studijų kurso studentams buvo išplatintas elektroninis laiškas, kviečiantis pasitikrinti informacinių technologijų modulio egzamino žinias. Eksperimentui buvo skiriamos dvi savaitės po kurių tiriamieji buvo supažindinti su jo metodologija bei preliminariais rezultatais.

„Windows“ operacinei sistemai skirtos eksperimentinės programos versijos įdiegimo failas buvo atsiųstas 245 kartus, testas išlaikytas 130 kartų bei gauta informacija apie 103 įrenginių kietųjų diskų duomenis. Atsižvelgiant į tai, kad šios paprastos programinės įrangos atveju beveik 80% įrenginių ne tik be kliūčių įvykdė kenksmingą kodą, bet ir vartotojui to nežinant išsiuntė duomenis į išorę, realu prognozuoti, jog profesionalaus įsilaužėlio parašytas kodas gali pasiekti efektyvumą artimą 100%.

„Android“ operacinei sistemai skirtos aplikacijos rezultatai nedaug skiriasi nuo jau analizuotos „Windows“ versijos. Programa buvo atsisiųsta 155 kartus, testas išlaikytas 73 kartus bei gauti duomenys iš 50 įrenginių. Tikėtina, kad mažesnis populiarumas buvo dėl to, kad dalis studentų atsisiuntė „Android“ programą tik norėdami pažiūrėti skirtumus su „Windows“ versija. Visais atvejais nė vienas programėlės naudotojas neperskaitė galutinio vartotojo licencijos sutarties ir neaplankė joje paminėtos nuorodos į papildomą resursą.

Eksperimentas atskleidė ir daugiau aktualių informacijos ir informacinių technologijų saugos problemų. Atliekant šios kenkėjiškos programinės įrangos kūrimo bei testavimo veiksmus buvo pastebėti itin neprognozuojami antivirusinių programų sprendimai jos įdiegimo ar duomenų išsiuntimo į išorę atžvilgiu: vienu atveju programos veikimas nebūdavo blokuodamas, kartais vartotojas gaudavo įspėjamąjį pranešimą. Tuo tarpu „Avast“ antivirusinė programa prie be savininko žinios siunčiamo elektroninio laiško su jo privačiais duomenimis pabaigoje pridėdavo tekstą „---Šis elektroninis laiškas buvo patikrintas nuo virusų „Avast“ antivirusine programa“.

Išanalizavus gautą informaciją apie kietųjų diskų duomenis, matoma, jog „Quizza“ programa nė karto nebuvo įdiegta į nuo pagrindinės sistemos atribotą virtualią mašiną. . Nepaisant to, kad šis sprendimas yra vis dažniau naudojamas komercinėje veikloje,

individualūs vartotojai jo teikiamais privalumais (ypač IT saugos srityje) vis dar nėra linkę naudotis. Dažnas vartotojas dirbdamas kompiuteriu turi prisijungęs bent vieną USB atmintinę, kuri yra potenciali kenkėjiško kodo platinimo aplinka, ypač jei kartais ji yra prijungiama prie neapsaugotų, viešai prieinamų ar jau užkrėstų kompiuterių.

Net ir paviešinus eksperimento tikslus bei metodiką programos naudojimas nesustojo ir vis dar buvo gaunami nauji duomenys iš sistemų į kurias „Quizza“ programa buvo įrašyta po gruodžio 20 d. Nėra aišku ar šiuos asmenis nepasiekė informacija apie atliekamą eksperimentą, ar jie net žinodami, jog buvo apgauti vieną kartą, vis vien nusprendė išbandyti viską savo sistemoje. Tarp visų tiriamųjų vienam studentui informacijos apie „Quizza“ programą išplatinimo metodas pasirodė įtartinas. Nors jis ir neperskaitė EULA sąlygų bei nepasiekė norimo failo alternatyviu būdų, tačiau, kaip pats teigė, programos į savo kompiuterį neįdiegė bei nuorodos, gautos teisingai išsprendus testavimo klausimus, iš kolegų neprašė.

IŠVADOS

Atlikus EULA analizę pastebėta, kad nors dokumentas buvo kuriamas siekiant apsaugoti autorines teises, tačiau šiandien yra naudojamas ribojant vartotojų pasirinkimo laisvę, išgaunant asmeninius duomenis ar įdiegiant kenkėjiškas programas. Šią prielaidą įrodo dažnai praktikoje sutinkamos EULA sąlygos, sukuriančios saugumo spragas vartotojo sistemoje arba pažeidžiančios informacijos konfidencialumo principą: vartotojo sistemos stebėsena, nuosavybės teisė į asmeninį turinį, draudimas vartotojui kritikuoti naudojamą produktą, sąlygų keitimas bet kuriuo momentu be jokio papildomo perspėjimo.

Parengus pasitikėjimo galutinio vartotojo licencijos sutartimi tyrimą, pasirinktas dažniausiai praktikoje naudojamas sutikimo su EULA sąlygomis būdas - specialus dialogo langas programos įdiegimo metu. Tai leidžia iš visų tyrimo dalyvių, sutikusių su galutinio vartotojo licencijos sutarties sąlygomis, paimti asmeninio įrenginio informaciją – pastoviosios atminties dydį ir jame likusios laisvos vietos duomenis, tuo parodant galimą prieigą iš išorės prie sisteminių resursų bei procesų.

Sukūrus tyrimo programinę įrangą „Windows“ asmeniniams kompiuteriams ir mobiliesiems „Android“ įrenginiams, išanalizuota, kad efektyviausiai ji gali būti išplatinta panaudojus fiktyvų internetinį puslapį. Toks modelis atkartoja praktikoje dažniausiai naudojamus scenarijus ir leidžia stebėti tiriamųjų veiksmus jiems aplankant unikalias nuorodas.

Gavus tyrimo rezultatus pastebėta, kad eksperimentinė programinė įranga dažniau buvo naudojama „Windows“ kompiuteriuose – 245 atsisiuntimai, lyginant su 155 „Android“ atveju. Taip pat „Windows“ sistemos dažniau nei „Android“ be jų naudotojų žinios išsiųsdavo konfidencialius duomenis – atitinkamai 103 ir 50 kartų . Šie rezultatai leidžia daryti išvadą, kad EULA panaudojimas vartotojų sistemos stebėsenai yra efektyvesnis asmeninių kompiuterių atveju, tuo labiau atsižvelgiant į tai, kad nė vienas programėlės naudotojas neperskaitė galutinio vartotojo licencijos sutarties ir neaplankė joje paminėtos nuorodos į papildomą resursą.

Realizavus eksperimentą buvo matomi itin neprognozuojami antivirusinių programų sprendimai „Quizza“ įdiegimo ar duomenų išsiuntimo į išorę atžvilgiu. Tai parodo, kad šis, dažname asmeniniame kompiuteryje vienintelis taikomas saugos sprendimas, nėra efektyvus užtikrinant konfidencialios informacijos apsaugą.

Išanalizavus gautą informaciją apie kietųjų diskų duomenis pastebėta, jog programa nė karto nebuvo įdiegta į nuo pagrindinės sistemos atribotą virtualią mašiną, o dažnas vartotojas dirbdamas kompiuteriu turi prisijungęs bent vieną USB atmintinę. Tai atskleidžia, kad dirbdami su nepatikrinta programine įranga naudotojai nesiima būtinų apsaugos priemonių ir taip sumažina savo asmeninių sistemų saugos lygį.

Reziumuojant gautus rezultatus matoma, kad informacinių sistemų naudotojai, siekdami apsaugoti konfidencialią informaciją, turėtų didesnį dėmesį skirti EULA tekstui. Net ir žinomų kompanijų licencijos sutartis turėtų būti perskaitoma ar bent patikrinama esamais automatiniais analizės įrankiais, o susidūrus su nepriimtinomis sąlygomis nutraukiamas programinės įrangos įdiegimas. Tyrimo rezultatai įrodė, kad asmeniniuose kompiuteriuose naudojami saugos sprendimai neužtikrina pakankamos duomenų apsaugos, todėl retai naudojama ar iš nepatikimų šaltinių gauta programinė įrangą turėtų būti įrašoma tik į dedikuotas pilnai nuo pagrindinės sistemos atribotas virtualias mašinas. Siekiant apsisaugoti nuo EULA tekste paslėptų grėsmių vartotojo atidumas ir atsargumas šiuo metu yra efektyviausias sprendimas.

LITERATŪRA

[1] Terms of Service; Didn't Read. [žiūrėta 2015-10-10] Prieiga per internetą https://tosdr.org/

[2] Internet Worlds Stats. Top 20 countries with the highest number of internet users. [žiūrėta 2015-10-10] Prieiga per internetą http://www.internetworldstats.com/top20.htm

[3] Rouse, M. Techtarget. End User License Agreement (EULA) [žiūrėta 2015-10-15] Prieiga per internetą http://searchcio.techtarget.com/definition/End-User-License-Agreement

[4] Newitz, A. Electronic Frontier Foundation (2005). Dangerous Terms: A User's Guide to EULAs [žiūrėta 2015-10-09] Prieiga per internetą https://www.eff.org/wp/dangerous-terms-users-guide-eulas

[5] Grossklags, J. and Good, N. (2007) Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers. *Financial Cryptography and Data Security*, 4886, 341-355.

[6] Gomulkiewicz, R.W. (2004) Getting Serious about User-Friendly Mass Market Licensing for Software. *George Mason Law Review*, 12, 687-718.

[7] Gardner, T. (2012) To read, or not to read... the terms and conditions: PayPal agreement is longer than Hamlet, while iTunes beats Macbeth [žiūrėta 2015-10-03] Prieiga per internetą http://www.dailymail.co.uk/news/article-2118688/PayPal-agreement-longer-Hamlet-iTunes-beats-Macbeth.html

[8] The Pit Crew (2012) It Pays To Read License Agreements (7 Years Later) [žiūrėta 2015-10-07] Prieiga per internetą: http://techtalk.pcpitstop.com/2012/06/12/it-pays-to-read-license-agreements-7-years-later/

[9] EULA Definition [žiūrėta 2015-10-07] Prieiga per internetą http://www.linfo.org/eula.html

[10] Cadden & Fuller LLP. Commercial Law: Express and Implied Warranties Under the Uniform Commercial Code [žiūrėta 2015-10-10] Prieiga per internetą http://www.caddenfuller.com/Articles/Commercial-Law-Express-and-Implied-Warranties-Under-the-Uniform-Commercial-Code.shtml

[11] Hillman, R.A. and Rachlinski, J.J. (2002) Standard-Form Contracting in the Electronic Age. *N.Y.U. Law Review*, 77(2), 429-495.

[12] Desautels, E. (2012) Software License Agreements: Ignore at Your Own Risk [žiūrėta 2015-10-07] Prieiga per internetą https://www.us-cert.gov/security-publications/software-license-agreements-ignore-your-own-risk

[13] Threatsaurus. The A-Z of computer and data security threats [2015-10-07] Prieiga per internetą https://www.sophos.com/en-us/security-news-trends/security-trends/threatsaurus.aspx

[14] Gordon, W. (2014) Many Browser Extensions Have Become Adware or Malware. Check Yours Now [žiūrėta 2015-10-20] Prieiga per internetą http://lifehacker.com/many-browser-extensions-have-become-adware-or-malware-1505117457

[15] Šnipinėjimo programos [žiūrėta 2015-10-09] Prieiga per internetą http://www.esaugumas.lt/lt/snipinejimo-programos.html

[16] Whitty, B. (2007) Why do People Create Computer Viruses? [žiūrėta 2015-10-12] Prieiga per internetą https://www.technibble.com/why-do-people-create-computer-viruses

[17] „Kaspersky Lab“: smulkiojo verslo įmonės dažnai pamiršta apie BYOD grėsmę (2015) [žiūrėta 2015-10-10] Prieiga per internetą http://www.kaspersky24.lt/index.php?route=information/news/news&news_id=175

[18] Litnet Cert DUK [žiūrėta 2015-10-10] Prieiga per internetą https://cert.litnet.lt/duk

[19] Korolov, M. (2016) DDoS attack on BBC may have been biggest in history [žiūrėta 2016-01-08] Prieiga per internetą http://www.networkworld.com/article/3020220/malware-cybercrime/ddos-attack-on-bbc-may-have-been-biggest-in-history.html#tk.rss_security

[20] (2015) Ransomware on the Rise [žiūrėta 2015-11-03] Prieiga per internetą https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise

[21] (2015) Badly coded ransomware locks away data forever [žiūrėta 2015-10-24] Prieiga per internetą http://www.bbc.com/news/technology-34765484

[22] Rouse, M. RAT (remote access Trojan) [žiūrėta 2015-10-27] Prieiga per internetą http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan

[23] (2011) Įsigaliojo pakeistas Lietuvos Respublikos elektroninių ryšių įstatymas [žiūrėta 2015-10-25] Prieiga per internetą http://www.rrt.lt/lt/naujienos/archive/p190/isigaliojo-pakeistas-lietuvos-x8rv.html

[24] Lietuvos Respublikos elektroninių ryšių įstatymas [žiūrėta 2015-10-26] Prieiga per internetą http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=463812

[25] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas [žiūrėta 2015-10-26] Prieiga per internetą http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=400103

[26] TermsFeed (2015) What are EULA agreements [žiūrėta 2015-11-26] Prieiga per internetą https://termsfeed.com/blog/what-are-eula-agreements

[27] Yin-Poole, W. (2012) EU rules publishers cannot stop you reselling your downloaded games [žiūrėta 2015-10-26] Prieiga per internetą http://www.eurogamer.net/articles/2012-07-03-eu-rules-publishers-cannot-stop-you-reselling-your-downloaded-games

[28] Europos Parlamento ir Tarybos Direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos Direktyva) [žiūrėta 2015-11-05] Prieiga per internetą http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000L0031

[29] Anderson, N. (2010) No, you don’t own it: Court upholds EULAs, threatens digital resale [žiūrėta 2015-11-07] Prieiga per internetą http://arstechnica.com/tech-policy/2010/09/the-end-of-used-major-ruling-upholds-tough-software-licenses

[30] Microsoft Privacy Statement [žiūrėta 2015-11-16] Prieiga per internetą https://www.microsoft.com/en-us/privacystatement/default.aspx?tduid=(58e1bf5c5e75cb8aeecc04987910cc0f)(256380)(2459594)(TnL5HPStwNw-4Oe3fBjmr7hSw.BGmr1olg)()

[31] Goldman, D. (2015) Is Windows 10 really a privacy nightmare? [žiūrėta 2015-11-12] Prieiga per internetą http://money.cnn.com/2015/08/17/technology/windows-10-privacy/

[32] Facebook Statement of Rights and Responsibilities [žiūrėta 2015-11-12] Prieiga per internetą https://www.facebook.com/legal/terms

[33] Newman , J. (2012) Top EULA Gotchas: Website Fine-Print Hall of Shame [žiūrėta 2015-11-02] Prieiga per internetą http://www.pcworld.com/article/249396/top_eula_gotchas_website_fine_print_hall_of_shame.html

[34] (2016) Microsoft Services Agreement [žiūrėta 2016-07-16] Prieiga per internetą https://www.microsoft.com/en-us/servicesagreement/?tduid=(58e1bf5c5e75cb8aeecc04987910cc0f)(256380)(2459594)(TnL5HPStwNw-8.KwhQ2ctxJfbTNUlWkFHg)()

[35] „Google Chrome“ paslaugų teikimo sąlygos [žiūrėta 2015-11-12] Prieiga per internetą https://www.google.lt/intl/lt/chrome/browser/privacy/eula_text.html

[36] Böhme, R and Köpsell, S. (2010) Trained to accept?: a field experiment on consent dialogs. *CHI '10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 2403-2406.

[37] Sauro, J. (2011) Do Users Read License Agreements? [žiūrėta 2015-11-15] Prieiga per internetą http://www.measuringu.com/blog/eula.php

[38] F-Secure (2014) Tainted Love – How Wi-Fi Betrays Us [žiūrėta 2015-11-12] Prieiga per internetą https://fsecureconsumer.files.wordpress.com/2014/09/wi-fi-experiment_uk_2014.pdf

[39] Brownlee, J. (2010) GameStation EULA collects 7,500 souls from unsuspecting customers [žiūrėta 2015-11-02] Prieiga per internetą http://www.geek.com/games/gamestation-eula-collects-7500-souls-from-unsuspecting-customers-1194091

[40] RAR and WinRAR END USER LICENSE AGREEMENT (EULA) [žiūrėta 2016-01-13] Prieiga per internetą http://www.win-rar.com/winrarlicense.html?&L=0

[41] EULAlyzer [žiūrėta 2016-01-13] Prieiga per internetą https://www.brightfort.com/eulalyzer.html

[42] Jonnalagadda, H. (2016) Microsoft ends support for Windows 8, asks users to upgrade to Windows 8.1 or 10 [žiūrėta 2016-01-13] Prieiga per internetą http://www.windowscentral.com/microsoft-ends-support-windows-8-asks-users-upgrade-windows-81-or-10

[43] „Kaspersky Lab“ galutinio vartotojo licencijos sutartis [žiūrėta 2016-03-30] Prieiga per internetą http://www.kaspersky24.lt/kis/Licence%20agreement%20LT.pdf

[44] Mobile/Tablet Top Operating System Share Trend [žiūrėta 2016-05-10] Prieiga per internetą https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=9&qpcustomb=1

[45] Rubenking, N.J. (2017) The Best Free Antivirus Protection of 2017 [žiūrėta 2017-03-03] Prieiga per internetą http://www.pcmag.com/article2/0,2817,2388652,00.asp

PRIEDAI

1 priedas. Tyrime naudojamos galutinio vartotojo licencijos sutarties tekstas

„QUIZZA“ GALUTINIO VARTOTOJO LICENCIJOS SUTARTIS

SVARBUS TEISINIS PRANEŠIMAS VISIEMS VARTOTOJAMS: ATIDŽIAI PERSKAITYKITE LICENCINĘ SUTARTĮ, PRIEŠ PRADĖDAMI VARTOTI PROGRAMINĘ ĮRANGĄ.

PASPAUDĘ MYGTUKĄ "SUTINKU" LICENCINĖS SUTARTIES LANGE ARBA ĮVESDAMI ATITINKAMUS SIMBOLIUS (-Į), JŪS SUTINKATE LAIKYTIS ŠIOS SUTARTIES TERMINŲ IR SĄLYGŲ. TOKS VEIKSMAS BUS LAIKOMAS JŪSŲ PARAŠU IR REIKŠ, KAD JŪS SUTINKATE BŪTI ŠIOS SUTARTIES ŠALIMI IR KAD ŠI SUTARTIS GALIOJA TAIP PAT, KAIP BET KURIS JŪSŲ APSVARSTYTAS IR PASIRAŠYTAS RAŠYTINIS SUSITARIMAS. JEIGU JŪS NESUTINKATE SU VISOMIS ŠIOS SUTARTIES NUOSTATOMIS IR SĄLYGOMIS, NUTRAUKITE PROGRAMINĖS ĮRANGOS DIEGIMĄ IR NEĮDIEKITE PROGRAMINĖS ĮRANGOS.

PASPAUDĘ MYGTUKĄ "SUTINKU" LICENCINĖS SUTARTIES LANGE ARBA ĮVEDĘ ATITINKAMĄ SIMBOLĮ (-IUS), JŪS SUTINKATE LAIKYTIS ŠIOS SUTARTIES NUOSTATŲ IR SĄLYGŲ.

1. Apibrėžtys 1.1. Programinė įranga reiškia programinę įrangą su bet kuriais atnaujinimais ir su jais susijusia medžiaga.

1.2. Kompiuteris (-iai) reiškia techninę (-es) priemonę (-es), įskaitant asmeninius kompiuterius, nešiojamus kompiuterius, kompiuterizuotas darbo vietas, asmeninius skaitmeninius asistentus, „išmaniuosius telefonus“, rankinius įtaisus, ar kitus elektroninius prietaisus, kuriems Programinė įranga buvo sukurta, kur Programinė įranga bus įdiegta ir (arba) naudojama.

1.3. Galutinis vartotojas (Jūs / Jūsų) reiškia asmenį (-is), diegiantį (-čius) arba naudojantį (-čius) Programinę įrangą savo vardu, arba kuris (-ie) legaliai naudoja Programinės įrangos kopiją, arba, jeigu Programinė įranga parsiųsta ar įdiegta organizacijos vardu, pavyzdžiui, darbdavio, "Jūs" toliau reiškia organizaciją, kuriai Programinė įranga buvo parsiųsta ar įdiegta ir kuriai atstovauja autorizuotas atstovas, įgaliotas sutikti su Sutartimi jos vardu. Šiuose punktuose terminas "organizacija" be apribojimų taikomas visiems partneriams, ribotos atsakomybės bendrovėms, korporacijoms, asociacijoms, uždarosioms akcinėms bendrovėms, koncernams, bendroms įmonėms, darbo organizacijoms, neįregistruotoms organizacijoms arba valstybinėms įstaigoms.

1.4. Partneris (-iai) reiškia organizacijas ar asmenį (-is), kuris (-ie) platina Programinę

įrangą pagal susitarimą ir licenciją, gautą iš Teisių turėtojo.

1.5. Atnaujinimas (-ai) reiškia visus atnaujinimus, peržiūrėjimus, kodus, patobulinimus, pataisymus, pakeitimus, kopijas, papildymus ar techninės priežiūros paketus ir t. t.

1.6. Vartotojo vadovas reiškia vartotojo vadovą, administratoriaus instrukcijas, žinyną ir susijusią aiškinamąją ar kitokią medžiagą.

2. Licencijos suteikiamos teisės

2.1. Teisių turėtojas garantuoja Jums neišskirtinę licenciją saugoti, laikyti, įdiegti, vykdyti, ir rodyti ("naudoti") Programinę įrangą nustatytame skaičiuje kompiuterių, ir atsižvelgiant į šios Sutarties ("Licencija") sąlygas, Jūs sutinkate su šios licencijos reikalavimais:

Bandomoji versija. Jei gavote, parsisiuntėte ir (arba) įdiegėte Programinės įrangos bandomąją versiją, Jums yra suteikiama bandomoji Programinės įrangos licencija, Jūs galite naudoti Programinę įrangą tik vertinimo tikslams ir tik per vieną taikytiną vertinimo laikotarpį, nebent jei nurodyta kitaip, nuo pirminio įdiegimo datos. Bet koks Programinės įrangos naudojimas kitiems tikslams arba pasibaigus vertinimo laikotarpiui yra griežtai draudžiamas.

Kelių programinių aplinkų Programinė įranga; daugelio kalbų Programinė įranga; dvigubos laikmenos Programinė įranga; keletas kopijų; rinkiniai. Jei naudojate skirtingas Programinės įrangos versijas ar skirtingų kalbų Programinės įrangos versijas, jei Jūs gaunate Programinę įrangą daugialypėje laikmenoje, jei kitaip gaunama daug Programinės įrangos kopijų, arba jei gavote Programinę įrangą kartu su kita Programine Įranga, bendras leidžiamas skaičius Jūsų kompiuterių, kuriuose įdiegta Programinė įranga, turi atitikti kompiuterių skaičių, nurodytą licencijoje, gautoje iš Teisių turėtojo, nebent licencija leidžia kitaip.

2.2. Jūs turite teisę pasigaminti Programinės įrangos kopiją tik atsarginiais tikslais ir tik pakeičiant teisiškai priklausančią kopiją, jei tokia kopija yra prarasta, sunaikinta arba tampa netinkama naudoti. Ši atsarginė kopija negali būti naudojama kitais tikslais ir turi būti sunaikinta, kai Jūs prarandate teisę naudotis Programine įranga, arba kai Jūsų licencija baigiasi arba yra nutraukiama dėl bet kokios kitos priežasties, atsižvelgiant į galiojančius teisės aktus toje šalyje, kurioje Jūs naudojate Programinę įrangą.

2.3. Jūs galite perleisti neišimtinę licenciją naudotis Programine įranga kitiems asmenims pagal licenciją, suteiktą Jums Teisių turėtojo su sąlyga, kad gavėjas sutinka būti saistomas visų šios sutarties sąlygų ir pakeisti Jus visiškai pagal suteiktą licenciją iš Teisių turėtojo. Jei Jūs visiškai perleisite Teisių turėtojo suteiktas teises naudotis Programine įranga, Jūs privalote sunaikinti visas Programinės įrangos kopijas, įskaitant atsargines kopijas. Jei Jūs esate perduodamos licencijos gavėjas, Jūs turite sutikti ir laikytis visų šios Sutarties

nuostatų ir sąlygų. Jei Jūs nesutinkate laikytis visų šios Sutarties nuostatų ir sąlygų, Jūs negalite įdiegti ir (arba) naudoti Programinę įrangą. Jūs taip pat sutinkate, kad kaip perleistos licencijos gavėjas Jūs neturite jokių papildomų ar geresnių teisių nei originalus galutinis vartotojas, kuris įsigijote Programinę įrangą iš Teisių turėtojo.

2.4. Nuo Programinės įrangos įdiegimo laiko (bandomajai Programinės įrangos versijai taikoma išimtis), Jūs turite teisę gauti šias paslaugas per apibrėžtą laikotarpį, nurodytą ant Programinės įrangos paketo (jei Programinė įranga buvo įsigyta fizinėje laikmenoje) arba nurodytą gavimo metu (jeigu Programinė įranga buvo gauta internetu):

- Programinės įrangos atnaujinimus internetu, kai Teisių turėtojas paskelbia juos savo interneto svetainėje arba per kitas interneto paslaugas. Bet kokie atnaujinimai, kai juos galite gauti, tampa Programine įranga ir jiems taikomos šios Sutarties sąlygos;

3. Aktyvizacija ir terminai

3.1. Jei Jūs pakeisite savo kompiuterį arba keisite jame įdiegtą kitų gamintojų programinę įrangą, Teisių turėtojas gali Jūsų pareikalauti pakartotinai sutikti su šia Sutartimi.

3.2. Jei Programinė įranga buvo įsigyta fizinėje laikmenoje, Programinė įranga, Jums priėmus šią Sutartį, gali būti naudojama tuo laikotarpiu, kuris yra nurodytas ant pakuotės ir prasideda priėmus šią Sutartį.

3.3. Jei Programinė įranga buvo įsigyta internetu, kai Jūs patvirtinate šią Sutartį, ji gali būti naudojama tuo laikotarpiu, kuris buvo nurodytas įsigyjant, nebent individuali licencija leidžia kitaip.

3.4. Jei Programinė įranga buvo įsigyta fizinėje laikmenoje, skirtoje pratęsti teisę naudotis anksčiau įgyta Programine įranga, Jūs galite pakartoti Programinės įrangos aktyvizavimą tik tuomet, jei aktyvizacijos kodas anksčiau įsigytai Programinei įrangai tebegalioja. Jei tokio aktyvizavimo kodo nėra, laikotarpis veiksmingai naudoti Programinę įranga bus ribojamas atsižvelgiant į informaciją, nurodytą ant Programinės įrangos paketo.

3.5. Jūs turite teisę naudoti bandomąją Programinės įrangos versiją vienam taikytinam vertinimo laikotarpiui (30 dienų) nuo Programinės įrangos aktyvizavimo pagal šią Sutartį su sąlyga, kad bandomoji versija nesuteikia Jums atnaujinimų ir techninės pagalbos internetu bei Techninės pagalbos telefono linija. Jei Teisių turėtojas nustatys kitą vieną taikytiną vertinimo laikotarpį, Jūs būsite informuoti pranešimu.

3.6. Jūsų licencija naudoti Programinę įrangą galioja tik tam tikrą laikotarpį, likęs laikas gali būti peržiūrėtas kaip tai aprašyta Vartotojo vadove. Pasibaigus šiame punkte nurodytam galiojimo laikui, Programinė įranga gali būti automatiškai išjungta ir gali pereiti

į neaktyvią būseną arba toliau veikti su ribotomis funkcijomis.

3.7. Jei Jūs įsigijote Programinę įrangą, kuri skirta naudoti daugiau nei viename kompiuteryje, tada Jūsų Programinės įrangos naudojimo licencija galioja tik tam tikrą laikotarpį, skaičiuojamą nuo Programinės įrangos aktyvinimo ar licencijos rakto failo įdiegimo į pirmąjį kompiuterį.

3.8. Neapribojant jokių kitų Teisių turėtojo turimų teisių gynimo būdų pagal teisę ar teisingumą, jeigu Jūs pažeidžiate kurias nors šios Sutarties sąlygas, Teisių turėtojas visais atvejais turi teisę, nepateikdamas Jums pranešimo, panaikinti šią licenciją naudoti Programinę įrangą, neatlyginant dėl to patirtų nuostolių.

3.9. Jūs sutinkate, kad naudodamiesi Programine įranga ir bet kokia ataskaita ar informacija, gauta naudojantis šią Programine įranga, Jūs laikysitės visų taikomų tarptautinių, nacionalinių, valstybinių, regioninių ir vietinių įstatymų ir taisyklių, įskaitant, be apribojimų, privatumo, autoriaus teisių, eksporto kontrolės ir padorumo įstatymus.

3.10. Išskyrus atvejus, kai Sutartyje aiškiai numatyta kitaip, Jūs negalite perleisti Jums suteiktų teisių pagal šią Sutartį arba šioje Sutartyje numatytų įsipareigojimų.

3.11. Teisių turėtojas pasilieka teisę apriboti aktyvizavimo galimybę ne tame regione, kuriame Programinė įranga buvo įsigyta iš Teisių turėtojo ir (arba) jo partnerių.

3.12. Jei Jūs įsigijote Programinę įrangą su aktyvizavimo kodu galiojančiu kalbos lokalizacijos programinei įrangai tame regione, kuriame ji buvo įsigyta iš Teisių turėtojo arba jo partnerių, Jūs negalite įjungti Programinės įrangos taikydami aktyvizavimo kodą, skirtą kitos kalbos lokalizacijai.

3.13. 3.11 ir 3.12 punktuose nurodytais apribojimų atvejais informacija apie šiuos apribojimus yra pateikiama ant pakuotės ir (arba) Teisių turėtojo ir (arba) jo partnerių svetainėje.

3.14. Kad galėtų patikrinti Programinės įrangos naudojimo teisėtumą, Teisių turėtojas pasilieka teisę naudoti priemones, tikrinančias, ar naudojate licencijuotą Programinės įrangos kopiją.

Programinė įranga gali persiųsti Teisių turėtojui licencinę informaciją, reikalingą patvirtinti Programinės įrangos naudojimo teisėtumą. Jei patikrinimo neįmanoma atlikti per tam tikrą laikotarpį, nurodytą Naudotojo vadove, Programinė įranga veiks su ribotomis funkcijomis.

4. Apribojimai

4.1. Jūs negalite imituoti, klonuoti, nuomoti, skolinti, išnuomoti, parduoti, pakeisti, dekompiliuoti ar perdaryti Programinės įrangos arba išardyti ar kurti išvestinius darbus,

remiantis Programine įranga ar jos dalimi; vienintelė išimtis gali būti galiojančiais teisės aktais Jums suteikta neatšaukiama teisė, ir Jūs jokiu kitokiu būdu nesupaprastinsite bet kokios Programinės įrangos dalies į žmogui suprantamą skaitymo formą ar perkelsite licencijuotą programinę įrangą arba bet kokią licencijuotos programinės įrangos dalį, nei leisite tai atlikti bet kuriai trečiajai šaliai, išskyrus kiek šis apribojimas yra aiškiai uždraustas galiojančių teisės aktų. Nei Programinės įrangos dvejetainis kodas, nei šaltinio kodai, negali būti naudojami atvirkštinei duomenų inžinerijai iš naujo atkurti patentuotą programos algoritmą. Teisių turėtojas ir (arba), priklausomai nuo atvejo, jo tiekėjai išlaiko visas teises, kurios nėra aiškiai suteikiamos pagal šį dokumentą. Bet koks neteisėtos Programinės įrangos naudojimo padarinys yra neatidėliojamas ir automatiškas Sutarties ir pagal šį dokumentą suteiktos licencijos nutraukimas ir dėl to Jūs galite būti traukiamas baudžiamojon ir (arba) administracinėn atsakomybėn.

4.2. Jūs negalite perduoti teises naudoti Programinę įrangą trečiajai šaliai, išskyrus kaip nurodyta šios Sutarties 2.3 punkte.

4.3. Jūs negalite suteikti aktyvizavimo kodo ir (arba) licencijos rakto failo trečiosioms šalims arba leisti trečiosioms šalims susipažinti su aktyvavimo kodu ir (arba) licencijos raktu, kurie yra laikomi Teisių turėtojo konfidencialiais duomenimis, ir Jūs prideramai saugosite aktyvizavimo kodą ir (arba) licencijos raktą su sąlyga, kad Jūs galėsite perduoti aktyvizavimo kodą ir (arba) licencijos raktą trečiosioms šalims tik kaip nurodyta šios Sutarties 2.3 punkte. Laikykite aktyvizavimo kodą saugioje vietoje iki licencijos galiojimo laikotarpio pabaigos.

4.4. Jūs negalite nuomoti, nuomoti išpirktinai ar skolinti Programinės įrangos jokiai trečiajai šaliai.

4.5. Jūs negalite naudoti Programinės įrangos kurti duomenims ar Programinei įrangai, naudojamai aptikti, blokuoti ar šalinti grėsmes, kurios aprašytos Vartotojo vadove.

4.6. Teisių turėtojas turi teisę blokuoti licencijos Programinei įrangai naudojimą, jei Jūs pažeisite bet kurią iš šios Sutarties nuostatų arba sąlygų, ir be jokių grąžinamųjų išmokų Jums.

4.7. Jei Jūs naudojate bandomąją Programinės įrangos versiją, Jūs neturite teisės perleisti licencijos ar teisės naudotis Programine įranga bet kuriai trečiajai šaliai.

5. Ribota garantija ir atsakomybės apribojimas

5.1. Teisių turėtojas garantuoja, kad Programinė įranga veiks pagal specifikacijas ir aprašymą, išdėstytą Vartotojo vadove, tačiau su ta sąlyga, kad tokia ribota garantija netaikoma: (w) Jūsų kompiuterio trūkumams ir su jais susijusiems pažeidimams, dėl kurių Teisių turėtojas aiškiai atsisako bet kokių garantijų ir atsakomybės; (x) sutrikimams,

defektams arba gedimams, atsirandantiems dėl neteisingo naudojimo; piktnaudžiavimo; avarijos; aplaidumo; netinkamo įdiegimo, veikimo ar techninės priežiūros; vagystės; vandalizmo; stichinių nelaimių; teroro aktų; maitinimo įtampos gedimų ir šuolių; avarijų; įtampos kitimo, neleistino modifikavimo ar remonto bet kurios šalies, išskyrus gavusių Teisių turėtojo leidimą; arba bet kokios trečiosios šalies ar Jūsų veiksmų ir priežasčių, kurių Teisių turėtojas negali kontroliuoti; (y) bet kokių defektų jei apie juos nepranešta Teisių turėtojui, kai tik defektas atsiranda pirmą kartą; ir (z) nesuderinamumų, sukeltų aparatūros ir (arba) Programinės įrangos sudėtinių dalių, įdiegtų Jūsų kompiuteryje.

5.2. Jūs suvokiate, pripažįstate ir sutinkate, kad nėra Programinės įrangos be klaidų; patariame pasidaryti atsargines kompiuterio informacijos kopijas pasirenkant Jums tinkamus intervalus ir laikmenų patikimumą.

5.3. Teisių turėtojas nepateikia jokios garantijos, kad Programinė įranga veiks tinkamai, jeigu bus pažeistos Vartotojo vadove ar šioje Sutartyje aprašytos nuostatos.

5.4. Teisių turėtojas negarantuoja, kad Programinė įranga veiks tinkamai, jei Jūs reguliariai neatsisiųsite atnaujinimų, kaip nurodyta šios Sutarties 2.4 punkte.

5.5. Teisių turėtojas negarantuoja apsaugos nuo Vartotojo vadove aprašytų grėsmių, po to, kai Programinės įrangos naudojimo licencija yra nutraukiama dėl bet kokios priežasties.

5.6. PROGRAMINĖ ĮRANGA YRA PATEIKIAMA "KAIP YRA" IR TEISIŲ TURĖTOJAS NEPRIIMA JOKIŲ NUSISKUNDIMŲ IR NEPATEIKIA JOKIŲ GARANTIJŲ JOS NAUDOJIMUI AR JOS VEIKIMUI. IŠSKYRUS BET KURIĄ GARANTIJĄ, SĄLYGĄ, PAREIŠKIMĄ ARBA GALIOJIMO TERMINĄ, KURIE NEGALI BŪTI NETAIKOMI ARBA APRIBOJAMI PAGAL GALIOJANČIUS ĮSTATYMUS, TEISIŲ TURĖTOJAS IR JO PARTNERIAI NENUMATO JOKIOS GARANTIJOS, SĄLYGOS, PAREIŠKIMO ARBA GALIOJIMO TERMINO (AIŠKIAI IŠREIKŠTO ARBA NUMANOMO, AR TAI BŪTŲ PAGAL ĮSTATUS, BENDRĄJĄ TEISĘ, PAPROČIUS, PANAUDOJIMĄ AR KITAIP) DĖL BET KURIO KLAUSIMO, ĮSKAITANT, BET TUO NEAPSIRIBOJANT, TREČIOJO ASMENS TEISIŲ NEPAŽEIDIMĄ, TINKAMUMĄ REALIZUOTI, TINKAMĄ KOKYBĘ, INTEGRAVIMĄ ARBA PRITAIKOMUMĄ TAM TIKRAI PASKIRČIAI. JŪS PRISIIMATE VISUS TRŪKUMUS IR VISĄ RIZIKĄ, VYKDYMUI IR ATSAKOMYBĘ UŽ PROGRAMINĖS ĮRANGOS PASIRINKIMĄ PASIEKTI SAVO NORIMŲ REZULTATŲ, JOS ĮDIEGIMĄ, NAUDOJIMĄ BEI REZULTATUS, GAUTUS IŠ PROGRAMINĖS ĮRANGOS. NERIBOJANT ANKŠČIAU IŠDĖSTYTŲ NUOSTATŲ, TEISIŲ TURĖTOJAS NEATSAKO UŽ JOKIUS NUSISKUNDIMUS IR NETEIKIA JOKIŲ GARANTIJŲ, KAD PROGRAMINĖ ĮRANGA BUS BE KLAIDŲ IR VEIKS BE PERTRAUKŲ AR KITŲ GEDIMŲ ARBA KAD PROGRAMINĖ ĮRANGA ATITIKS BET KURIUOS ARBA VISUS ATSKLEISTUS AR NEATSKLEISTUS TEISIŲ

TURĖTOJUI JŪSŲ REIKALAVIMUS.

6. Techninė pagalba

6.1. Techninės pagalbos tarnybą ir jos taisykles galima rasti: www.quizza.tk/support/pc (/android)

7. Informacijos rinkimas

7.1. Įvykus klaidai Programinės įrangos diegimo metu, Jūs sutinkate automatiškai persiųsti informaciją apie klaidos kodą, naudojamos Programinės įrangos platinamąjį paketą, informaciją apie kompiuterį bei diegimo programos duomenis apie Programinės įrangos diegimą.

7.2. Kad būtų didesnis saugumas darbo metu, Jūs sutinkate automatiškai teikti informaciją apie Programinės įrangos klaidų statistiką, sistemos techninius parametrus, taip pat informaciją apie Programinės įrangos versiją ir aktyvinimą.

7.3. Remiantis LR Asmens duomenų teisinės apsaugos įstatymo 12 straipsniu, Programine įranga gali būti apdorojami asmenį identifikuojantys duomenys.

7.4. Jei nenorite, kad Programine įranga surinkta informacija būtų siunčiama Programinės įrangos kūrėjui, nutraukite programinės įrangos diegimo procedūrą ir apsilankykite 6.1 punkte nurodytame techninės pagalbos tarnybos puslapyje.

8. Išimtys ir Atsakomybės apribojimas

8.1. TIEK, KIEK LEIDŽIA GALIOJANTIS ĮSTATYMAS, JOKIU ATVEJU TEISIŲ TURĖTOJAS ARBA JO PARTNERIAI NEBUS ATSAKINGI UŽ BET KOKIUS ATSITIKTINIUS, BAUDŽIAMUOSIUS, NETIESIOGINIUS AR PASEKMIŲ NUOSTOLIUS (ĮSKAITANT, BET NEAPSIRIBOJANT, NUOSTOLIAIS DĖL PELNO ARBA KONFIDENCIALUMO ARBA KITA INFORMACIJA, VERSLO TRIKDŽIUS, DĖL PRIVATUMO PRARADIMO, DĖL KORUPCIJOS, PATIRTOS ŽALOS AR DUOMENŲ AR PROGRAMOS PRARADIMO, UŽ NESUGEBĖJIMĄ ĮVYKDYTI BET KOKIOS PAREIGOS, ĮSKAITANT IR BET KOKIĄ ĮSTATYMŲ NUSTATYTĄ PAREIGĄ, TARNYBINIO SĄŽININGUMO AR PAGRĮSTO RŪPESTINGUMO PAREIGĄ, DĖL NERŪPESTINGUMO, DĖL EKONOMINIŲ NUOSTOLIŲ, IR UŽ VISUS KITUS MATERIALINIUS ARBA KITUS NUOSTOLIUS) KURIE ATSIRANDA DĖL ARBA KOKIU NORS BŪDU, KURIS YRA SUSIJĘS SU NAUDOJIMO AR NEGALĖJIMO NAUDOTIS PROGRAMINE ĮRANGA, TEIKIMU IR NEVEIKIMU, NEGALĖJIMU TEIKTI PARAMĄ AR KITAS PASLAUGAS, INFORMACIJĄ, PROGRAMINĘ ĮRANGĄ, IR SUSIJUSĮ TURINĮ PER ĮRANGĄ AR GALI KITAIP NE PAGAL SUSITARIMĄ NAUDOTI PROGRAMINĘ ĮRANGĄ, ARBA KITOKIU BŪDU

NE PAGAL BET KOKIAS SU ŠIO SUSITARIMO NUOSTATAS, ARBA ATSIRANDANČIAS DĖL SUTARTIES PAŽEIDIMO AR (ĮSKAITANT APLAIDUMĄ, KLAIDINGĄ PAAIŠKINIMĄ, BET KOKĮ GRIEŽTOS ĮSIPAREIGOJIMĄ ARBA PAREIGĄ) ARBA BET KOKIŲ ĮSTATYMUOSE NUMATYTŲ PAREIGŲ PAŽEIDIMĄ, ARBA TEISIŲ TURĖTOJO GARANTIJOS ANULIAVIMO, ARBA BET KURIO IŠ PARTNERIŲ PAŽEIDIMAS, NET JEIGU TEISIŲ TURĖTOJAS ARBA BET KURIS PARTNERIS BUVO PERSPĖTAS APIE TOKIŲ NUOSTOLIŲ GALIMYBĘ.

JŪS SUTINKATE, KAD TUO ATVEJU, KAI TEISIŲ TURĖTOJAS IR (ARBA) JO PARTNERIAI YRA ATSAKINGI, TEISIŲ TURĖTOJO ATSAKOMYBĖ / ARBA JOS PARTNERIŲ ATSAKOMYBĖ BUS APRIBOTA PROGRAMINĖS ĮRANGOS

ŠIOJE SUTARTYJE NENUMATOMI ARBA NERIBOJAMI IEŠKINIAI DĖL MIRTIES IR ASMENS SUŽALOJIMO ATVEJO. ESANT BET KOKIAM ATSAKOMYBĖS APRIBOJIMUI, IŠIMČIAI AR APRIBOJIMUI, ŠIS SUSITARIMAS NEGALI BŪTI IŠSKIRTAS ARBA APRIBOTAS PAGAL GALIOJANČIUS ĮSTATYMUS, TUOMET TIK TOKS ATSAKOMYBĖS APRIBOJIMAS, IŠIMTIS AR APRIBOJIMAS NETAIKOMA JUMS, O JŪS IR TOLIAU PRIVALOTE LAIKYTIS VISŲ LIKUSIŲ ĮSIPAREIGOJIMŲ, IŠIMČIŲ IR APRIBOJIMŲ.

9. Intelektinė nuosavybė

9.1. Jūs sutinkate, kad Programinė įranga ir Autoriaus teisių, sistemos, idėjos, veiklos metodai, dokumentacija ir kita informacija, esanti Programinėje įrangoje, yra intelektinė nuosavybė ir (arba) labai vertinga Teisių turėtojo arba jo partnerių komercinė paslaptis ir kad Teisių turėtojas ir jo partneriai, kai taikoma, yra saugomi pagal civilinę ir baudžiamąją teisę ir Autoriaus teisių įstatymą, prekybos paslapčių, prekių ženklų ir patentų reikalavimus Lietuvos Respublikoje, Europos Sąjungoje ir Jungtinėse Amerikos Valstijose, taip pat kitose šalyse bei pagal tarptautinių sutarčių teises. Ši Sutartis nesuteikia Jums jokių teisių į intelektinę nuosavybę, įskaitant bet kokius Prekių ar Paslaugų ženklus, priklausančius Teisių turėtojui ir (arba) jo partneriams ("Prekių ženklai"). Prekių ženklus galite naudoti tik tam, kad būtų galima identifikuoti Programinės įrangos atspausdintus gaminius pagal priimtą Prekės ženklų praktiką, įskaitant savininko pavadinimo Prekės ženklo identifikavimą. Toks bet kokio Prekės ženklo naudojimas nesuteikia Jums jokių nuosavybės teisių į Prekės ženklus. Teisių turėtojas ir (arba) jo partneriai išlaiko visas teises į nuosavybės teisę ir interesus, susijusius su Programine įranga, įskaitant be apribojimų, bet kokius klaidų pataisymus, patobulinimus, atnaujinimus ar kitus pakeitimus, susijusius su Programine įranga, ar paties Teisių turėtojo arba bet kurios trečiosios šalies ir visų Teisių, patentų, komercinių paslapčių teises, prekių ženklus ir kitas intelektinės nuosavybės teises, nurodytas šiame dokumente. Jūsų žinioje esančios Programinės įrangos instaliacija ar naudojimas nesuteikia Jums jokių nuosavybės teisių į Programinės įrangos intelektinę

nuosavybę ir Jūs neįsigysite jokių teisių į Programinę įrangą, išskyrus aiškiai nustatytas šioje Sutartyje. Visos

Programinė įrangos kopijos turi turėti tuos pačius firminius ženklus, kurie yra ir Programinėje įrangoje. Išskyrus atvejus, nurodytus šioje Sutartyje, ši Sutartis nesuteikia Jums jokių intelektinės nuosavybės teisių į Programinę įrangą ir Jūs suprantate, kad licencija, kaip toliau apibrėžta šiame dokumente, suteikiama pagal šią Sutartį, tik suteikia Jums riboto naudojimo pagal šią Sutartį teisę. Teisių turėtojas pasilieka sau visas teises, kurios aiškiai nesuteiktos Jums pagal šią Sutartį.

10.2. Jūs sutinkate jokiu būdu nekeisti Programinės įrangos. Jūs negalite pašalinti arba pakeisti autoriaus teisės apsaugos ženklų ar kitų nuosavybės teisės ženklų bet kokioje Programinės įrangos kopijoje.

11. Valdantysis įstatymas

11.1. Išskyrus 11.2 ir 11.3 punktuose numatytus atvejus, ši sutartis sudaryta remiantis ir jai taikomi šalies ar teritorijos, kurioje įsigijote Programinę įrangą, teisės aktai, neatsižvelgiant ir netaikant teisės aktų konfliktų principų.

a. Europos Sąjunga (ES). Jei Programinę įrangą įsigijote Europos Sąjungos šalyje-narėje, galioja Lietuvos Respublikos teisės aktai.

b. Jungtinės Valstijos. Jei Programinę įrangą įsigijote Jungtinėse Valstijose, taikomi JAV Masačusetso valstijos teisės aktai, su sąlyga, kad JAV valstijos, kurioje gyvenate, teisės aktai bus taikomi ieškiniams dėl valstijos taikomos vartotojų apsaugos, nesąžiningos konkurencijos ir pan. Jūs ir Teisų savininkas tiesiogiai atsisakote teisės į prisiekusiųjų teismą, kiek tik tai leidžia teisės aktai.

j. Bet kuri kita šalis ar teritorija. Jei įsigijote Programinę įrangą bet kurioje kitoje šalyje, taikomi pagrindiniai šalies, kurioje ją įsigijote, teisės aktai.

11.2. Nepaisant aukščiau nurodytų nuostatų, jei bet kurios šalies ar teritorijos, kurioje ši Sutartis yra įgyvendinama ar sudaroma, teisės aktai arba viešoji politika neleidžia taikyti čia nurodytų teisės aktų, bus taikomi tos šalies ar teritorijos teisės aktai, kiek to reikalauja įstatymas ar viešoji politika. Taip pat, jei esate individualus vartotojas, 11.1 punkto nuostatos neturės jokio poveikio teisės aktuose numatytoms teisėms savo šalyje imtis veiksmų remiantis tos šalies teisės aktais.

12. Visa Sutartis; Atskyrimas; Atsisakymų nebuvimas

12.1. Ši Sutartis yra galutinis susitarimas tarp Jūsų ir Teisių turėtojo ir pakeičia visus kitus ankstesnius žodinius ir rašytinius susitarimus, pasiūlymus, pranešimus arba reklamą,

susijusią su Programine įranga arba šios Sutarties dalyku. Jūs pripažįstate, kad perskaitėte šią Sutartį, ją supratote ir sutinkate būti jos saistomas. Jeigu kompetentingos jurisdikcijos teismas pripažįsta kurią nors šios Sutarties nuostatą ar jos dalį negaliojančia, niekine arba neįgyvendinama dėl kokių nors priežasčių, tokia nuostata bus aiškinama siauriau, kad ji taptų teisėta ir įgyvendinama, ir Sutartis išliks galioti visa apimtimi pagal teisę ir teisingumą, išlaikant jos pradinį tikslą, kiek tai yra įmanoma. Bet kurios šios Sutarties nuostatos arba sąlygos atsisakymas galioja tik tokiu atveju, jeigu jis įforminamas raštiškai ir pasirašomas Jūsų ir Teisių turėtojo įgalioto atstovo, su sąlyga, kad joks atsisakymas pasinaudoti teisėmis, susijusiomis su šios Sutarties bet kurios nuostatos pažeidimu, negali būti aiškinamas kaip atsisakymas pasinaudoti teisėmis, susijusiomis su bet kuriuo ankstesniu, esamu arba vėlesniu tokios nuostatos pažeidimu. Teisių turėtojui nepareikalavus įvykdyti kurią nors šios Sutarties nuostatą arba įgyvendinti kurią nors teisę arba priverstinai neįvykdžius kurios nors šios Sutarties nuostatos arba neįgyvendinus kurios nors teisės, tai nereikš tokios nuostatos arba teisės atsisakymo.