KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Deimantė Boreišaitė

Delninukų antivirusinės programinės įrangos tyrimas

Magistro darbas

Darbo vadovas
doc. dr. E. Toldinas

Kaunas, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Deimantė Boreišaitė

Delninukų antivirusinės programinės įrangos tyrimas

Magistro darbas

Recenzentas
lekt. dr. A. Janavičiūtė
2011-05-

Vadovas
doc. dr. E. Toldinas
2011-05-

Atliko
IFN9-3 gr. studentė
Deimantė Boreišaitė
2011-05-25

Kaunas, 2011

TURINYS

1. ĮVADAS

Mobilūs įrenginiai plinta taip pat greitai, kaip ir auga jų pajėgumai bei plečiasi jų panaudojimo galimybės. Rankiniai mobilūs įrenginiai, tokie kaip delniniai kompiuteriai ar sumanieji telefonai, pradeda keisti nešiojamus kompiuterius, kaip ir nešiojami kompiuteriai keičia stalinius kompiuterius. Tačiau ribotas šių įrenginių baterijos gyvavimo laikas sumažina jų panaudojimo galimybes. Energijos valdymas tampa vienu didžiausiu iššūkiu tarp nešiojamų kompiuterinių įrenginių. Tyrėjai teigia, kad ir pagerinus baterijų chemines savybes, kažin ar to užtektų norint išspręsti energijos valdymo problemą, o norint pasiekti efektyvų energijos valdymą, reikia išsiaiškinti, kaip ir kur pasiskirsto energija mobiliajame įrenginyje.

Ši silpna mobilaus įrenginio vieta dar gali būti pabloginta ir mobilių piktavališkų programų, eikvojančių baterijos energiją. Tokias piktavališkas programas dažniausiai sunku aptikti, susekti ir apsisaugoti nuo jų, juolab, kad pastoviai atsiranda vis daugiau naujų piktavališkų programų. Virusas vartotojui sukelia nemažų problemų, kadangi nustoja veikti dauguma mobiliojo įrenginio funkcijų. Taip pat senka ir įrenginio baterija.

Mobiliuosiuose įrenginiuose gali būti saugomi ne ką mažiau svarbūs duomenys nei asmeniniame ar stacionariajame kompiuteryje. Augantis mobilių įrenginių skaičius tapo dar patrauklesniu taikiniu piktavališkų programų kūrėjams. Nors įrenginiuose naudojamos pažangios operacinės sistemos, šių sistemų saugumas yra pažeidžiamas piktavališkų programų. Norint apsisaugoti nuo kenkėjiškų programų, naudojama antivirusinė programinė įranga. Taigi, svarbu yra užtikrinti mobilaus įrenginio saugumą bei kiek galima ilgiau išlaikyti veikiantį mobilųjį įrenginį, tad, prieš diegiant antivirusinę programinę įrangą, naudotojui pravartu būtų žinoti, kiek mobiliojo įrenginio energijos sąnaudų ji išeikvoja.

Šio magistrinio darbo tyrimo sritis – mobilių įrenginių sistemų sauga ir energijos suvartojimas. Tyrimo objektas – delniniai kompiuteriai su Windows Mobile operacine sistema.

Magistrinio darbo tikslas – ištirti įvairių antivirusinių programų įtaką delninukų energijai. Priklausomai nuo vartotojo pasirenkamų parametrų (darbas su failais, darbas tinkle, darbas taikomosios programos lygmenyje) taikomosios programos lygmenyje bus išanalizuota įvairių antivirusinių programų įtaka delninuko energijos suvartojimui.

Darbo uždaviniai:

- Atlikti kitų mokslininkų tyrimų rezultatų analizę magistrinio darbo tema.
- Sukurti programinę įrangą, kurios pagalba bus atliekama delninuko energijos suvartojimo analizė, įdiegus atitinkamą antivirusinę programą.

- Sukurti tyrimo metodiką, sudaryti reikiamus duomenis tyrimui, nustatyti reikalingus tyrimui parametrus.
- Ištestuoti sukurtą programinę įrangą.
- Atlikti tyrimą užfiksuojant tyrimo metu gautus rezultatus.
- Ištirti, kiek delninuko energijos suvartojama be antivirusinės programos.
- Ištirti, kiek delninuko energijos suvartojama su antivirusinėmis programomis.
- Palyginti delninuko energijos suvartojimą su antivirusine programa ir be jos, bei įvairių antivirusinių programų įtaką energijai.
- Išanalizuoti gautus rezultatus bei pateikti juos grafiniu būdu.

Darbo struktūra:

- Analitinėje dalyje apžvelgta, kokie yra padaryti tyrimai, nagrinėjantys energijos sunaudojimą mobiliuosiuose įrenginiuose, kokie metodai taikomi energijos sunaudojimo sumažinimui, kokį poveikį įrenginio baterijai turi piktavališkos programos, kaip jos aptinkamos ir kokie tyrimai atlikti su antivirusinėmis programomis.

- Projektavimo dalyje aprašyta eksperimente naudojamos programinės įrangos struktūra, tyrimo duomenų struktūra, pateiktas failų atidarymo, uždarymo atveju algoritmas, panaudojimo atvejų schema. Pateiktos klasių diagramos, aprašyti rezultatų failo laukai, iškelti funkciniai ir nefunkciniai reikalavimai sistemai.

- Eksperimentinėje dalyje aprašytas energijos suvartojimo, panaudojant skirtingas antivirusines programines įrangas, tyrimas, jo metodika, pateikti skaitiniai ir grafiniai tyrimo rezultatai.

- Pabaigoje pateikti atlikto darbo rezultatai bei pagrindinės darbo išvados.

- Prieduose pateikta papildoma analizės dalyje bei eksperimente naudojama informacija.

2. ENERGIJOS SUVARTOJIMO MOBILIUOSE ĮRENGINIUOSE ANALIZĖ

Sumanieji telefonai, kišeniniai kompiuteriai, delniniai kompiuteriai ir kiti mobilieji įrenginiai užima vis didesnę rinkos dalį. Prieš pradedant nagrinėti mobilių įrenginių ypatybes suvartojamos energijos atžvilgiu, trumpai susipažinkime su pagrindinio šio darbo tyrimo objekto galimybėmis.

Delnininis kompiuteris (angl. *Personal Digital Assistant* arba *Palmtop*) – nedidelis mobilus įrenginys, galintis atlikti daugelį asmeninio kompiuterio atliekamų funkcijų. Tokiame įrenginyje dažniausia būna laikrodis, kalkuliatorius, kalendorius, priminimų bei adresų sąrašai, o taip pat yra galimybė įdiegti įvairias taikomąsias programas – pašto programas, dokumentų redaktorius, žaidimus. Viena svarbiausių delninukų savybių – galimybė sinchronizuoti duomenis su asmeniniu ar nešiojamu kompiuteriu. Delninukais galima peržiūrėti ar redaguoti MS Word, Excel, PowerPoint, PDF failus, juos spausdinti, siųsti elektroniniu paštu ar perkelti į paprastą kompiuterį. Delninuku patogu rinkti SMS ir MMS žinutes, klausytis muzikos. Visi delninukai turi infraraudonųjų spindulių jungtį. Yra galimybė naudotis naujausiomis bevielio ryšio technologijomis, sujungti vieną delninį kompiuterį su kitu, su mobiliuoju telefonu, su paprastu ar nešiojamuoju kompiuteriu.

Dažniausiai delniniuose kompiuteriuose naudojamos ličio jonų baterijos. Baterijos darbo laikas labai svyruoja nuo delninio kompiuterio modelio ir atliekamų darbų.

2.1. Mobilių įrenginių baterijos energiją naudojančių veiksnių analizė

2.1.1. Energijos valdymas mobiliuosiuose įrenginiuose

Mobilių įrenginių baterijos energijos sunaudojimas priklauso ir nuo vartotojų atliekamų veiksmų su įrenginiu. Funkcijos, kuriomis daugiausiai naudojasi mobilių įrenginių vartotojai (6517 respondentų 2005 m duomenimis) pateiktos 1 lentelėje. Kaip matome, daugiausiai yra naudojamasi SMS paslaugomis [14].

1 lentelė. Dažniausiai naudojamų mobilaus įrenginio funkcijų dešimtukas

Eil. Nr.	Funkcija	Naudojimasis
1.	SMS	83 %
2.	Žaidimai	61 %
3.	Kamera	49 %
4.	MMS paveiksliukai	46 %
5.	PDA funkcijos	36 %
6.	Internetas	31 %
7.	WAP	30 %
8.	Bluetooth	28 %
9.	Elektroninis paštas	27 %
10.	Video kamera	27 %

„Hewlett-Packard“ (HP) laboratorijų tyrėjai Marc A. Viredaz, Lawrence S. Brakmo ir Williams R. Hamburgen atliko energijos valdymo tyrimus su dviem įrenginias – Itsy (kišeninio kompiuterio prototipas) ir įrenginys, panašus į Itsy – iPAQ H36xx. Kiek energijos sunaudoja atskiri įrenginio komponentai bei veiksmai matome 2 lentelėje [17].

2 lentelė. Energijos suvartojimas

Įrenginys	Energiją suvartojantys parametrai	Minimali galia (esant miego rėžimui), mW	Maža galia, mW	Didelė galia, mW
Itsy v2.4	Sistemos galia	2	7	105
	Procesorius	0	13	233
	Atmintis (DRAM)	2	15	231
	Ekranas (LCD)	0	3	5
	Ekrano galinis apšvietimas (angl. *backlight*)	0	0	324
	Garsiakalbis	0	0	100
	Kita	3	12	139
iPAQ H36.xx	Ekranas (LCD)	0	0	39
	Ekrano priekinis apšvietimas (angl. *frontlight*)	0	0	960
	Gaunant duomenis bevieliu tinklu	60	805	950
	Perduodant duomenis bevieliu tinklu	60	805	1400

Tyrėjai daugiau dėmesio skyrė procesoriui, kuris suvartoja nemažą dalį sistemos energijos. Procesorius turi tris būsenas: veikimo, nieko neveikimo ir miego. Nagrinėjant energijos vartojimą atsižvelgiama į šiuos faktorius: veiksmas, galimas esamoje būsenoje; vėlinimas, reikalingas įeiti ir išeiti iš tam tikros būsenos (dažniausiai iš / į veikimo būseną); energija, suvartojama procesoriuje šioje būsenoje. Iš programinės pusės nieko neveikimo būsena laikoma kaip lengva būsena, nes vėlinimai įeinant ir išeinant iš šios būsenos yra gana maži. Tuo tarpu miego būsena turi daug didesnius vėlinimus ir laikoma sunkia būsena (3 lentelė).

3 lentelė. Procesoriaus suvartojama energija, priklausomai nuo jo būsenos

Būsena	Veiksmas	Techninės įrangos vėlinimai	Suvartojama energija
Miego	Aptinkami pertraukimai, galintys pažadinti procesorių	Įėjimui: 150µs Išėjimui 10-157ms	7,18mW
Neveikimo	Nevykdomos jokios instrukcijos. Pertraukimai perveda procesorių į veikimo būseną	Įėjimui <10 ciklų Išėjimui < 10 ciklų	55,5mW kai 59MHz 81,9mW kai 133Mhz 95,5mW kai 192MHz
Veikimo	Atlikimas yra procesoriaus funkcija	N/A	Priklauso nuo apkrovos

Energijos taupymui autoriai siūlo išjungti tam tikrą poblokį (angl. *subunit*), kai jis yra nenaudojamas. Norint pasiekti optimalų energijos taupymą, taip pat reikia ir tinkamai struktūrizuotos programinės įrangos. Sistemos techninė įranga turėtų būti suprojektuota kaip kolekcija tarpusavyje susijusių blokų, kurie galėtų ir nepriklausomai funkcionuoti, ir būti nepriklausomai įjungiami arba išjungiami. Šiuolaikiniai mobilūs įrenginiai tik iš dalies įvykdo šį reikalavimą. Išoriniai blokai (garsas, ekranas ir kt.) gali būti išjungiami jei jie nenaudojami,

tačiau neįmanoma išjungti tokių pagrindinių blokų kaip procesorius ar atmintis, nebent visą sistemą nustačius į miego rėžimą.

2.1.2. Mikromiego technologija

Lawrence S. Brakmo, Deborah A. Wallach, Marc. A.Videraz pasiūlė energiją mažinantį metodą mobiliems įrenginiams, kuris pavadintas mikromiegu (angl. *µSleep*). Mikromiegas perveda procesorių į miego rėžimą trumpiems laiko periodams (mažiau nei vieną sekundę) nepastebint vartotojui. Šis metodas naudingas tada, kai vartotojas skaito dokumentą ar Internetinį puslapį ir procesorius yra lengvai apkrautas. Tyrime buvo naudojamas kišeninio kompiuterio prototipas Itsy (naudojamas StrongARM SA-1100 procesorius su 32Mb dinaminės atminties (DRAM)), sukurtas Compaq laboratorijoje, Kalifornijoje. Tyrimas parodė, kad pritaikius mikromiegą įrenginio energijos suvartojimas sumažėjo iki 60 % [2].

Tarp vartotojo atliekamų veiksmų su mobiliu įrenginiu, būna ir daug neveikimo laiko, todėl, vietoje to, kad procesorius pereitų į neveikimo rėžimą (angl. *idle mode*), mikromiego metodas nustato procesorių į miego rėžimą trumpiems laiko momentams (nuo 40 ms iki 1 sekundės). Šis miego rėžimas skiriasi nuo praktikoje naudojamo įprastinio miego rėžimo tuom, jog vartotojas nežino, kad procesorius yra miego rėžime ir galvoja, kad įrenginys dirba kaip įprastai.

Mikromiegas turi du pagrindinius tikslus: pereiti į miego rėžimą vartotojui net neįtariant, kad jis yra miego rėžime bei sumažinti įrenginio energijos suvartojimą.

Kad būtų galima įvykdyti mikromiego metodą, turi būti įgyvendinti tam tikri techninės ir programinės įrangos reikalavimai.

Yra keturi techninės dalies reikalavimai: a) procesorius turi turėti miego rėžimą, b) įrenginys turi turėti galimybę rodyti statinį paveikslą, kol procesorius miega, c) sistema turi pajėgti „pabusti“ atsiradus tokiems išoriniams įvykiams kaip mygtukų aktyvavimas, d) įrenginys turi turėti programuojamą laikmatį (pageidautina su 1-10 ms rezoliucija, kad būtų galima „pažadinti“ sistemą).

Programinei daliai keliami reikalavimai: a) mikromiego kodas turi žinoti, kada bus kitas operacinės sistemos įvykis, b) kodas turi žinoti, ar tuo metu aktyvūs išoriniai veiksmai leis procesoriui įeiti į miego rėžimą, c) turi būti metodas kode, leidžiantis pereiti sistemai į miego būseną (turi būti įspėjamos įrenginio tvarkyklės (angl. *drivers*) prieš sistemai užmiegant ir po jos nubudimo).

1 paveiksle matome mikromiego rėžimo sistemos būsenas. Realaus laiko laikrodis (RTC) naudojamas kaip mikromiego žadintuvas. Pradinė būsena laikoma tokia, kada sistema yra veikimo būsenoje (angl. *running*). Tokiu atveju yra vykdomas tam tikras procesas arba

gija. Sistema gali pereiti į miego būseną jei paspaudžiamas mygtukas, arba dėl laikmačio neveiklumo. Operacinė sistema (OS) pereina į neveikimo būseną, kai paleidžiamas OS neveikimo procesas (kai neveikia joks procesas ar gija). Tada sistema gali pereiti į trumpą miegą (mikromiegą). Sprendžiama pagal tai, ar sistema gali pakankamai ilgai miegoti, kad sutaupytų energijos, ir ar visi įrenginiai leidžia pereiti procesoriui į šį rėžimą. Jei šios sąlygos tenkinamos, procesorius pereina į mikromiego būseną, kitu atveju sistema pereina į procesoriaus neveikimo būseną, taip pat tausojant energiją. Kai atsiranda koks pertraukimas, sistema vėl pereina į veikimo būseną. Iš mikromiego būsenos į veikimo būseną sistema pereina pasirodžius RTC signalui arba išoriniam įvykiui (mygtuko paspaudimas ar ekrano prilietimas).

1 pav. Mikromiego būsenų diagrama

Per mikromiegą (laikotarpio trukmė $T \geq t_s+t_r$)sunaudojama energija e paskaičiuojama pagal formulę:

$$e = e_s+e_r+p_s \cdot (T-t_s-t_r),$$

kur: T – mikromiego trukmė (įskaitant įėjimą ir išėjimą iš šios būsenos).

T_s – laikas, reikalingas įėjimui į miego rėžimą.

T_r – laikas, reikalingas išėjimui iš miego rėžimo (pereinama į veikimo rėžimą).

E_s – energija, sunaudojama įėjimui į miego rėžimą.

E_r – energija, sunaudojama išėjimui iš miego rėžimo.

P_s – miego rėžimo galia su veikiančiu LCD ekranu.

Mikromiego vėlinimo laikas – 12 ms. Taigi didžiausias mikromiego privalumas – iki 60 % sutaupytos įrenginio energijos. Trūkumas: įrenginys turi atitikti minėtus techninės ir programinės įrangos reikalavimus, o tai yra sudėtingiau, jei ši technika taikoma senesniems mobiliesiems įrenginiams.

2.1.3. Piktavališkų programų plitimas ir įtaka mobiliems įrenginiams

Virusai, kirminai ir trojanai jau senai paplitę tarp asmeninių kompiuterių. Pirmas mobilus kirminas, pavadintas Cabir vardu, ir pažeidęs mobilų įrenginį su Symbian operacine sistema (OS), pasirodė 2004 m. birželio 14 d. Šis kirminas pasižymėjo greitu baterijos eikvojimu ir plitimu per Bluetooth sąsają. Pirmas mobilus virusas, pavadintas Duts vardu, ir pažeidęs mobilius įrenginius su Windows Mobile operacine sistema, pasirodė 2004 m. liepos 17 d. Šie piktavališkų programų pasirodymai laikomi naujos eros mobilių virusų ir antivirusinių priemonių bendruomenės kūrimo pradžia. Laboratorijose aptinkamų mobilių piktavališkų programų ir jų modifikacijų skaičius nuo 2004 m. aptiktų pirmųjų virusų pastoviai auga. Kenkėjiškų programų mobiliems įrenginiams kiekis bei įvairovė didėja dėl didėjančio mobilių įrenginių populiarumo tiek tarp paprastų vartotojų, tiek verslo srityje [5].

Iki 2009 metų rugpjūčio vidurio „Kaspersky“ laboratorijoje buvo užfiksuotos 106 piktavališkų programų šeimos bei 514 jų variantų. Iki 2010 metų pabaigos šis skaičius padidėjo iki 153 šeimų ir virš 1000 variantų, t.y. 2010 m. buvo aptikta 65,12 % daugiau piktavališkų programų, atakuojančių mobilius įrenginius, nei 2009 m. 2 paveiksle matome 2010 m. pabaigos mobilių piktavališkų programų paplitimą skirtingose operacinėse sistemose [10]:

Platforma	Šeimų skaičius	Variantų skaičius
J2ME	45	613
Symbian	74	311
Python	5	60
Windows Mobile	16	54
AndroidOS	7	15
Sgold	3	4
MSIL	2	4
IphoneOS	1	2

2 pav. Piktavališkų programų paplitimo šeimų ir variantų skaičius pagal platformas

Kad piktavališka programa atakuotų tam tikrą operacinę sistemą ar platformą, turi būti įvykdytos trys sąlygos [10]:

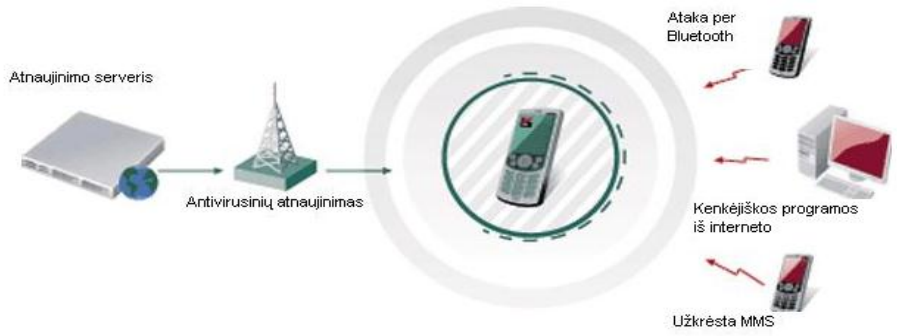
1. Platforma turi būti populiari.
2. Turi būti gerai dokumentuoti kūrimo įrankiai taikomajai programai.
3. Programavimo ar pažeidžiamumo klaidų buvimas.

Piktavališka programa mobiliam įrenginiui gali pridaryti daug žalos [10, 18]:

- Siuntinėti be įrenginio savininko žinios didelį kiekį SMS ar MMS žinučių, už kurias tenka savininkui ir susimokėti.

- Ištrinti įrenginio savininko asmeninę informaciją (pvz. adresų knygą, failus) ar pavogti konfidencialią informaciją.
- Neleisti vykdyti kai kurių funkcijų (SMS, kamera) ar visiškai neleisti valdyti įrenginio, užblokuoti atminties kortelę.
- Modifikuoti arba pakeisti piktogramas ar sistemos taikomąsias programas.
- Eikvoti įrenginio bateriją daug greičiau nei įprastai.
- Užkrėsti failus.
- Nusiųsti užkrėstus failus mobilaus įrenginio savininko vardu kitiems vartotojams (per elektroninį paštą, WiFi, Bluetooth ir pan.).
- Perduoti pavojingą kodą iš mobilaus įrenginio į asmeninį kompiuterį per sąsają.

Piktavališka programa gali pasiekti mobilų įrenginį per: Bluetooth ryšį, MMS žinutes, atsisiunčiant ir instaliuojant programą į mobilų įrenginį iš nepatikimo šaltinio [5] (parodyta 3 paveiksle). Bluetooth virusas gali užkrėsti visus Bluetooth naudojimui aktyvuotus mobilius įrenginius 10-30 metrų spinduliu, vaizdo žinučių (MMS) virusas, kaip daugybė kompiuterių virusų, plinta per adresų knygą.



3 pav. Piktavališkų programų atakos

Nors dauguma virusų grupuojami pagal elgesį, atakuojamą mobilaus įrenginio operacinę sistemą ir šeimos variantus, mobiliuosius virusus sunku suklasifikuoti, nes dauguma kenkėjiškos programinės įrangos yra mišrios ir jų sudėtyje yra įvairių sutampančių funkcijų, tačiau grupelė mokslininkų iš Malaizijos universiteto [3] suskirstė išmanaus telefono virusus (žiūrėti 4 lentelę) pagal jų užkrato nešiotojus (angl. *Infection vector*).

4 lentelė. Mobilių virusų suskirstymas pagal užkrato nešiotojus [19]

Užkrato nešiotojas	**Mobilaus viruso pavyzdžiai (pavadinimas)**
Mobiliojo ryšio tinklas (telefono skambučiai, SMS, MMS)	CommWarriors, Mabir
Bluetooth sąsaja	Cabirs, CommWarrior
Infraraudonųjų spindulių jungtis	Phage

4 lentelės tęsinys kitame puslapyje

4 lentelės tęsinys

Elektroninis paštas	MSIL.Letum
Momentiniai pranešimai	Opanki.d
Mobilus žiniatinklis (Internetas per WiFi/GPRS/EDGE/UMTS/3GPP jungtis)	Skulls, Doomboot
Sąveika- Mobilus įrenginys-asmeninis kompiuteris – Mobilus įrenginys (USB/Active Sync/ kitas sujungimas/pritvirtinimas)	Croosover, Mobler
Išoriniai įrenginiai (atminties kortelė, SIM kortelė)	Cardtrap

Detalesni 4 lentelėje išvardintų ir kitų paplitusių mobiliuosiuose įrenginiuose piktavališkų programų aprašymai pateikti 1 priede.

2.1.4. Antivirusinių programų analizė

Viena tinkamiausių priemonių apsaugai nuo piktavališkų programų – antivirusinės programos su nuolat atnaujinamomis virusų duomenų bazėmis.

Piktavališkų programų peržiūrėjimas (angl. *scanning)* – vienas seniausių ir populiariausių metodų aptikti kenkėjiškas programas. Pagrindinė peržiūrėjimo idėja – ieškoti baitų eilutės, kuri priklausytų žinomai kenkėjiškai programai. Mobilioje aplinkoje dauguma antivirusinių programinių įrangų naudoja šį metodą. Šis metodas leidžia aptikti piktavališką programą dar prieš jai pradėjus veikti įrenginyje [12].

Piktavališkų programų kūrėjai nenori, kad jų kenkėjiški kūriniai būtų susekti, analizuojami ir filtruojami, kai išplinta į tinklą, tačiau tai ir yra pagrindinis aptikimo sistemų tikslas, kuris tiria ateinančias programas ir lygina jas su piktavališkų programų parašais [5]. Virusų aptikimas gali būti: pagrįstas parašu (kai ieškoma tam tikros baitų sekos, kuri ir identifikuoja virusą) bei pagrįstos elgesiu – šiuo atveju yra didesnė galimybė aptikti dar nežinomus virusus [13,18].

Dauguma antivirusinių programinių įrangų paketų naudoja atitinkamas peržiūrėjimo (ang. *scanning*) technikas tam, kad patikrintų, ar failas yra užkrėstas, ar ne. Yra du pagrindiniai naudojimo modeliai, vykdomi paleidžiant antivirusinę programinę įrangą: 1) pagal reikalavimą (angl. *on-demand*) ir 2) pagal prieigą (angl. *on-access*). Pirmas modelis apima vartotoją, kuris nurodo, kuriuos failus antivirusinei programinei įrangai peržiūrėti. Šiuo atveju antivirusinė programinė įranga veiks tam tikrą laiką, tikrindama failus. Tikrinimas paprastai atliekamas vartotojui nesinaudojant kompiuteriu. Antras modelis veikia foniniame rėžime, yra stebimos sistemos lygio bei vartotojo lygio operacijos ir atliekamas peržiūrėjimas, kai iš anksto pasirodo koks įvykis. Dauguma antivirusinių programų sukonfigūruotos dirbti šiuo modelio principu.

Taip pat antivirusinės programos naudoja įvairius algoritmus įvairių failų formatų (.dll, .doc, .exe, .html, .jpg, .mp3, .ppt, .xls ir kitų) peržiūrėjimui. [16].

Yra įvairių antivirusinių programų gamintojų ir kiekvienas jų turi savo antivirusinę programą ir mobiliems įrenginiams, tokiems kaip delninukai. Antivirusinių programų reitingą pagal austrų nepriklausomos laboratorijos „AV-Comparatives“ atliktų testų rezultatus (2009 m. rugpjūtis) matome 5 lentelėje [6].

5 lentelė. Antivirusinių programų reitingas

Bendri testavimo rezultatai	**Antivirusinė programa**	**Aptikimo procentas**	**Bendri testavimo rezultatai**	**Antivirusinė programa**	**Aptikimo procentas**
1	G DATA	99.8 %	**9**	Trustport	97.6%
2	AVIRA	99.4 %	**10**	ESET	97.2%
3	McAfee	98.7%	**11**	Kaspersky	94.7%
4	Symantec	98.4%	**12**	AVG	94.0%
5	Avast	98.0%	**13**	Sophos	91.3%
6	F-Secure	97.9%	**14**	Microsoft	90.0%
7	Bitdefender	97.8%	**15**	Kingsoft	86.4%
8	eScan	97.7%	**16**	Norman	84.8%

Iš viso teste dalyvavo 16 gerai žinomų antivirusinių programų gamintojų produktų. Kiekviena teste dalyvavusi antivirusinė programa buvo atakuojama beveik 1,6 milijonų skirtingų kenkėjiškų programų atmainų (iš jų - 69.5% trojanų, 20.7% robotų, 6.1% kirminų, 1.8% kitų kenkėjiškų programų, 1.5% Windows virusų, 0.4% skriptų ir makrovirusų). Pagal laboratorijos rezultatus matome, kad kompiuterinius kenkėjus geriausiai sugaudė vokiečių sukurta „G DATA“ antivirusinė programa (99,8 % tikslumu).

Savo tyrimui pasirinksime skirtingose reitingo vietose esančias antivirusines programas ir pažiūrėsime, kaip jos įtakoja delninuko bateriją.

2.2. Panašių sistemų, metodų ir įrankių analizė

2.2.1. Delninuko energijos suvartojimo įvertinimas taikomosios programos lygmenyje

KTU Informatikos fakulteto, Programų inžinerijos katedros habil.dr. Vytautas Štuikys ir doktorantas Jonas Valančius 2007 m. pasiūlė metodą delninuko energijos suvartojimui įvertinti taikomosios programos lygmenyje bei įvertinti energijos suvartojimą delninuko multimedia taikymams. Energijos suvartojimo įvertinimui taikomosios programos lygmenyje buvo naudojamas juodos dėžės principas [1].

Eksperimentui atlikti buvo naudojamas delninukas Palm Zire 72. Išskirti delninuko energiją vartojantys komponentai ir jų veiksenos parodytos 6 lentelėje.

6 lentelė. Delninuko energiją vartojantys komponentai ir jų veiksenos

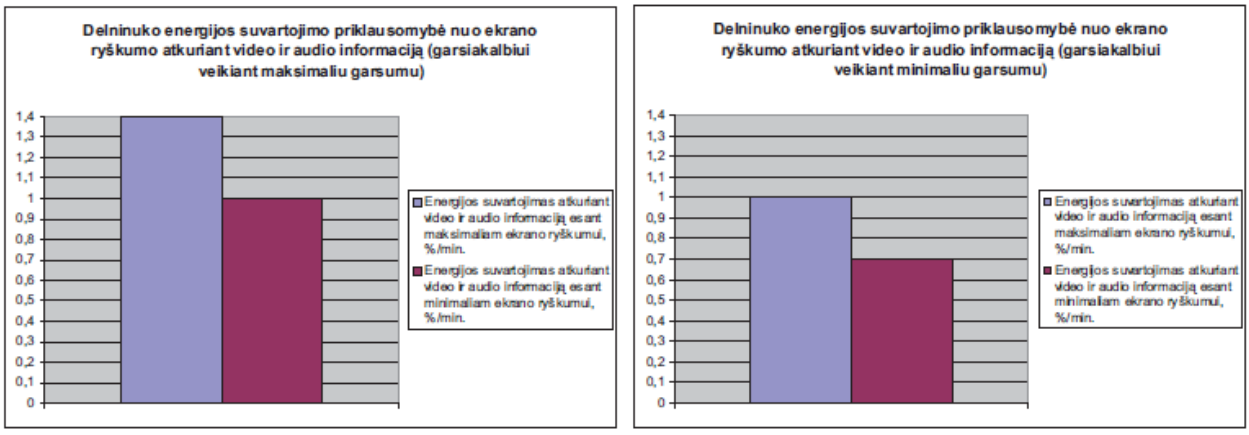
Komponento pavadinimas	Veiksenos būsena
Procesorius ir atmintis (CPĮ)	Visada jungti
Garsiakalbis (G)	Minimalus, maksimalus, tarpinis garsumas
Ausinės (A)	Minimalus, maksimalus, tarpinis garsumas
Ekranas (E)	Minimalus, maksimalus, tarpinis ryškumas
Ryšys (R)	Bluetooth ryšys (BT), Infrared ryšys (IR), Plačiajuostis ryšys (WIFI)

Darbe buvo nagrinėjami keturi energiją vartojantys komponentai: ausinės (A), garsiakalbis (G), ryšio susijungimas (R) ir ekranas (E) (7 lentelė).

7 lentelė. Palm Zire 72 delninuko energiją naudojantys komponentai, jų veiksenos ir parametrai

Eil. nr.	G	A	R	E	Galimas taikymas	Garso l.		Vaizdo ryškumas		Perdavimo būdas	
						Min	Max	Min	Max	BT	WIFI
1	0	0	0	1	+	-	-	+	+	-	-
2	0	0	1	0	taikymas negalimas						
3	0	0	1	1	+	-	-	+	+	+	+
4	0	1	0	0	+	+	+	-	-	-	-
5	0	1	0	1	+	+	+	+	+	-	-
6	0	1	1	0	taikymas negalimas						
7	0	1	1	1	+	-	-	+	+	+	+
8	1	0	0	0	+	+	+	-	-	-	-
9	1	0	0	1	+	+	+	+	+	-	-
10	1	0	1	0	taikymas negalimas						
11	1	0	1	1	+	-	-	+	+	+	+
12	1	1	0	0	taikymas negalimas						
13	1	1	0	1	taikymas negalimas						
14	1	1	1	0	taikymas negalimas						
15	1	1	1	1	taikymas negalimas						

Eksperimentas parodė, kad delninukas daugiausiai energijos suvartoja video taikyme atkurdamas informaciją maksimaliu garsumu ir ryškumu (1,4 %/min) bei perduodamas failą bevielio ryšio sistema Wifi (1,2 %/min) ir Bluetooth (1 %/min). Įjungtas ekranas suvartojo 0,9 %/min delninuko energijos. Mažiausiai energijos audio taikyme sunaudojo ausinukas (0,02 %/min) ir garsiakalbis (0,05 %/min), klausant muziką minimaliu garsumu. 4 paveiksle matome, kaip skiriasi energijos suvartojimas naudojant maksimalų ir minimalų rėžimus:



a) b)

4 pav. Vidutinis delninuko taikymų energijos suvartojimas, priklausantis nuo veiksenų: a) ekrano ryškumo maksimaliu garsumu, b) ekrano ryškumo minimaliu garsumu

Taigi, keičiant veiksenos būseną, kinta ir suvartojamos energijos kiekis. Pasirinkus minimalų rėžimą, energijos suvartojama mažiau nei maksimaliu rėžimu.

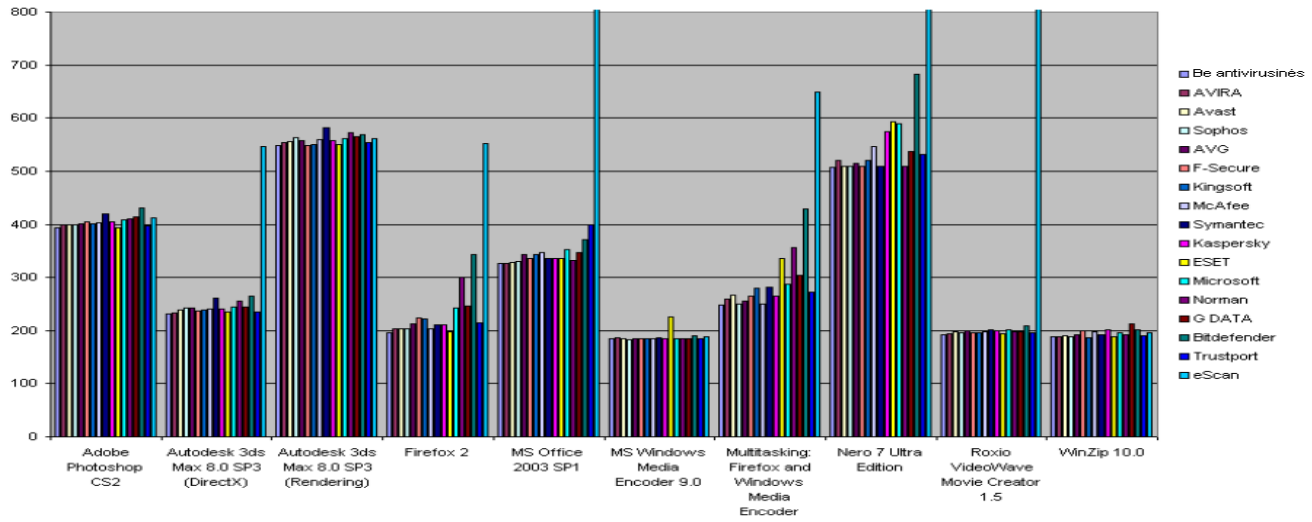
2.2.2. Antivirusinės programinės įrangos įtaka įrenginio sistemos darbui pagal „AV-Comparatives“ testavimo rezultatus

Nepriklausoma austrų laboratorija „AV-Comparatives“ 2009 m. gruodį atliko tyrimus su 16 antivirusinių programų [6]. Buvo atliekami tokie testai (veiksmai):

- Failų kopijavimas iš vienos vietos į kitą (buvo naudojama 2GB duomenų su skirtingomis failų kategorijomis-paveiksliukai, filmai, muzika, įvairūs Microsoft (MS) Office 2003 ir 2007 dokumentai, PDF failai, taikomosios / vykdomosios programos, Windows XP sistemos failai, archyvai ir kita).
- Failų suarchyvavimas / išarchyvavimas (tiriamas antivirusinės programinės įrangos poveikis – kiek laiko užtrunka sukurti naujiems archyvams ar išarchyvuoti failus iš jau esančių archyvų).
- Kodavimas / perkodavimas (audio, video failų – konvertavimas MP3 failų į WAV, MP3 į WMA, AVI į MPG ir MPG į AVI).
- Programų diegimas / šalinimas, (Visual C++, . NET Framework ir kitų – tiriama, kiek laiko užtrunka jų įdiegimas ir pašalinimas).
- Programų paleidimas (dažniausiai naudojami - Microsoft Office ir PDF failai (su Adobe Acrobat Reader) – buvo atidaromi ir uždaromi, ir matuojamas dokumentų atidarymo laikas).
- Failų parsisiuntimas iš Interneto (tam, kad būtų išvengta išorinių poveikių, naudojamas Apache žiniatinklio serveris (wget), sujungtas su 1 GB LAN. Matuojamas atsisiuntimo laikas).
- „Worldbench“ testavimo komplektas (naudojamas „Worldbench 6“ - buvo atliekama 10 testų su: Adobe Photoshop CS2, Autodesk 3ds Max 8.0 SP3, Mozilla Firefox 2, Microsoft Office 2003 su SP1, Microsoft Windows Media Encoder 9.0, Mozilla Firefox ir Windows Media Encoder, Nero 7 Ultra Editon, Rodžio VideoWave Movie Creator 1.5 ir WInzip 10.0).

Testai buvo atliekami Intel Core 2 Duo E8300 (Worldbench sistemoje su Intel Core 2 Duo E6600) kompiuteriu su 2 GB RAM ir SATAII kietaisiais diskais. Pirmiausia testai buvo atliekami tiesiog su Windows XP Professional SP3 sistema, o po to su įdiegta antivirusine programine įranga.

5 paveiksle matome sunaudojamą laiką (sekundėmis) skirtingų produktų, skirtinguose „WorldBench6“ testuose (žemesni stulpeliai parodo, kad testui atlikti antivirusinė programa sunaudoja mažiau laiko). Kaip matome, daugumoje atvejų nėra ryškaus skirtumo tarp produktų, išskyrus keletą atvejų.



5 pav. WorldBench6 testų rezultatai

Suminiai testavimo rezultatai (kartu su „WorldBenc“h testais) pateikti 8 lentelėje.

8 lentelė. Bendri testavimo rezultatai

Eil. nr.	Antivirusinė programa	Failų kopijavimas (vidurkis)*	Suarchyvavimas /išarchyvavimas	Kodavimas /perkodavimas	Įdiegimas /pašalinimas	Parsisiuntimas	Programų paleidimas (Word+PDF vidurkis)	World Bench	Bendri rezultatai
1.	AVIRA	Greitas (10)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	114	199
2.	Kingsoft	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	Labai greitas (15)	Labai greitas (15)	111	196
3.	F-Secure	Labai greitas (8)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	112	195
4.	Sophos	Greitas (10)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	112	193
5.	Kaspersky	Labai greitas (13)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	Labai greitas (15)	Labai greitas (15)	110	193
6.	Microsoft	Labai greitas (8)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	107	190
7.	Avast	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	Greitas (10)	Greitas (10)	113	188
8.	Symantec	Labai greitas (13)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	Greitas (10)	Labai greitas (15)	110	188
9.	ESET	Greitas (10)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	Greitas (10)	108	183
10.	McAfee	Labai greitas (13)	Labai greitas (15)	Labai greitas (15)	Vidutinis (5)	Vidutinis (5)	Greitas (10)	111	174
11.	Norman	Vidutinis (5)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	Labai greitas (15)	Vidutinis (5)	104	169
12.	AVG	Greitas (8)	Greitas (10)	Labai greitas (15)	Vidutinis (5)	Lėtas (0)	Labai greitas (15)	111	164
13.	Bitdefender	Labai greitas (13)	Labai greitas (15)	Labai greitas (15)	Lėtas (0)	Lėtas (0)	Labai greitas (15)	96	154
14.	G DATA	Labai greitas (8)	Labai greitas (15)	Labai greitas (15)	Lėtas (0)	Lėtas (0)	Greitas (10)	104	152
15.	eScan	Vidutinis (3)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Labai greitas (15)	Greitas (10)	64	137
16.	Trustport	Labai greitas (8)	Greitas (10)	Labai greitas (15)	Lėtas (0)	Lėtas (0)	Vidutinis (5)	90	125

* Kelis kartus buvo atliekami bandymai

Be antivirusinės programinės įrangos WorldBench testai bendroje sumoje surinko 116 balų.

Vertinimas buvo vykdomas pagal 9 lentelėje esančius kriterijus.

9 lentelė. Vertinimo kriterijai

Veiksmas	**Pasirinktas kriterijus**	**Kriterijaus įvertinimas**
Failų kopijavimas	Nuo +0 % iki +25 %	Labai greitas
	Nuo +25 % iki +50 %	Greitas
	Nuo +50 % iki +100 %	Vidutinis
	Virš +100 %	Lėtas
Suarchyvavimas/išarchyvavimas	Nuo +0 % iki +20 %	Labai greitas
	Nuo +20 % iki +40 %	Greitas
	Nuo +40 % iki +80 %	Vidutinis
	Virš +80 %	Lėtas
Kodavimas/perkodavimas	Nuo +0 % iki +15 %	Labai greitas
	Nuo +15 % iki +30 %	Greitas
	Nuo +30 % iki +50 %	Vidutinis
	Virš +50 %	Lėtas
Įdiegimas /pašalinimas	Nuo +0 % iki +25 %	Labai greitas
	Nuo +25 % iki +50 %	Greitas
	Nuo +50 % iki +100 %	Vidutinis
	Virš +100 %	Lėtas
Programų paleidimas	Nuo +0 % iki +50 %	Labai greitas
	Nuo +50 % iki +100 %	Greitas
	Nuo +100 % iki +200 %	Vidutinis
	Virš +200 %	Lėtas
Failų parsiuntimas iš Interneto	Nuo +0 % iki +25 %	Labai greitas
	Nuo +25 % iki +50 %	Greitas
	Nuo +50 % iki +100 %	Vidutinis
	Virš +100 %	Lėtas

Tyrėjai įspėja, kad sistemos testavimo rezultatams daug įtakos turi ir pasenusi techninė įranga, neišvalytas kietasis diskas (turi būti palikta bent 20 % laisvos disko vietos).

2.2.3. Anomalinių aptikimų stebėjimas sumaniuosiuose telefonuose

Aubrey-Derrick Schmidt, Frank Peters ir Florinan Lamour analizavo, kaip galima stebėti sumaniojo telefono būseną ir panaudoti tai anomaliniams aptikimams. Stebimos savybės nusiunčiamos į nutolusį serverį. Testavimui buvo naudojamas Nokia E61 sumanusis telefonas su Symbian operacine sistema (OS 9.1), turintis 64 Mb įterptą atminties kortelę, kuri leidžia talpinti joje įvairius failus (pavyzdžiui, video). Į telefoną įdiegtas Symbian C++ stebėjimo klientas (angl. *monitoring client*), kuris kas 20 sekundžių siunčia savybių vektorių (angl. *feature vector*) į testuojamą serverį su viešu IP adresu ir turinčiu duomenų bazę. Siunčiamo savybių vektoriaus dydis apie 8 Kb, ir talpina savyje apie 50 savybių [14].

Stebėjimo klientas susideda iš trijų pagrindinių komponentų:

1) Vartotojo sąsajos – ji leidžia įvesti komandas (tokias kaip serverio ar prievado pakeitimus). Šis komponentas gali būti panaudojamas ir kliento būsenai patikrinti, pavyzdžiui, siuntimo ar parodyti anomalinių rezultatų aptikimui.

2) Komunikacijos modulio – atsakingas už ryšio būsenų valdymą ir savybių vektorių siuntimą. Jei klientas negali prisijungti dėl dingusio signalo, šis modulis laiko duomenis buferyje tol, kol vėl atsiranda ryšys. Jei ryšio nėra dar prieš tai, kol buferis yra pripildytas, tai yra pridedamas paskutinis vektorius ir pašalinamas pirmas. Komunikavimui su serveriu šis modelis naudoja SOAP (Simple Object Access Protocol) žiniatinklio paslaugas. Tačiau tiek duomenų siuntimas, tiek pasiruošusio siųsti rėžimas gan brangiai atsiliepia baterijos energijai. Tam, kad būtų kuo mažiau energijos sąnaudų, visi duomenys laikomi lokaliai ir siunčiami masiškai po to, kai pasiekia slenkstinį lygį (angl. *threshold level*).

3) Savybių išskleidėjo (angl. *feature extractor*). Jis turi keletą skirtingų komponentų, kurie renka ir skaičiuoja savybes. Savybės apibūdina stebimo įrenginio būseną. Jis buvo sukurtas paėmimui naujų stebimų duomenų kas 30 s. Duomenys yra laikomi lokaliai ir vėliau, kai pasiekiamas slenkstis, siunčiami serveriui naudojant atitinkamą paslaugą.

Gali būti tiriamos tokios savybės:

- Atminties talpa – savybė, kuri gali būti ir lengvai plečiama. Parodo laisvos atminties kiekį, Kb. Programoms reikia mažiau ar daugiau atminties resursų, tam, kad galėtų tinkamai dirbti. Taigi kiekviena piktavališka programa šią vertę turėtų paveikti.
- Vartotojo neveiklumas – parodo, ar buvo nuspaustas koks nors mygtukas per paskutines 10 s.
- Procesų skaičius – parodo veikiančių procesų skaičių.
- CPU (procesoriaus) naudojimas - parodo išnaudotą CPU procentais.
- Siųstų SMS skaičius – parodo siųstų SMS skaičių siuntimo kataloge.

Norint ištirti šias sistemos savybes veikiant piktavališkai programai, pirmiausia buvo tiriamos normalios sistemos būsenos savybės. Buvo tiriama 10 atvejų:

- SMS siuntimas (a) siunčiant tuščią žinutę, b) rašant ir siunčiant 150 simbolių žinutę, c) rašant ir siunčiant 300 simbolių žinutę ir d) rašant ir siunčiant 150 simbolių žinutę daugybei vartotojų),
- taip pat testavimui buvo naudojami trys skirtingi žaidimai,
- siunčiamos tuščios MMS žinutės,
- rašoma ir siunčiama 150 simbolių MMS žinutė, rašoma ir siunčiama MMS žinutė su prisegtu paveikslėliu,
- PDF failo skaitymas,

- naršymas Internete (kai atidaromos skirtingos nuorodos ir atsiunčiamas paveiksliukas),
- Bluetooth technologijos veikimas,
- įvairių elektroninių paštų panaudojimas,
- atsisiuntimas iš Interneto 8Mb MP3 failo ir jo klausymas,
- naujo įrašo darymas kalendoriuje.

Gauti rezultatai parodė, kad kiekvienas šis atliktas veiksmas pateikia skirtingus savybių pakitimo rezultatus (pavyzdžiui, žaidimas daug daugiau išnaudoja CPU negu MMS žinutės). Atlikus šį testą buvo vykdomas kitas, kuriame panaudota piktavališka programa, tam, kad ištirti kenkėjišką elgesį. Aktyvuota piktavališka programa siuntė SMS žinutę kiekvienąkart, kai buvo paspaudžiamas klavišas „2“. Užfiksuota, kad kiekvienąkart, kai siunčiamų žinučių kiekis padidėja, padidėja ir procesų skaičius bei CPU naudojimas, bet sumažėja atmintis.

Šis metodas, kai perduodami savybių vektoriai į nutolusį serverį, parodo piktavališkų programų veiklą. Tai leidžia aptikti ir dar nežinomas piktavališkas programas.

2.2.4. Energiją eikvojančių piktavališkų programų aptikimas

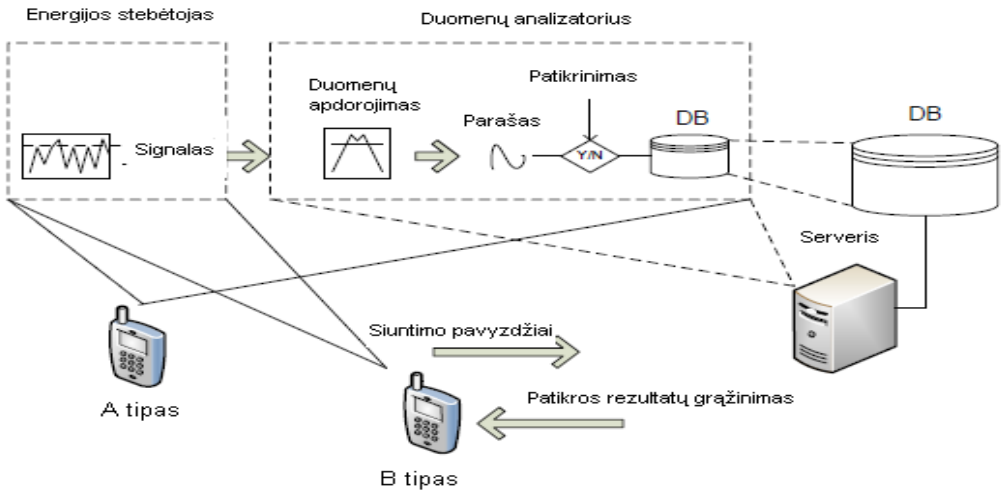
Hahnsang Kim, Joshua Smith ir Kang G. Shin, Mičigano universiteto darbuotojai, atliko tyrimą su energiją eikvojančių anomalijų aptikimo sistema, kuri stebi, aptinka ir analizuoja anksčiau nežinomas mobilaus įrenginio energijos išeikvojimo grėsmes. Tyrime naudojamas HP iPAQ rx4200 įrenginys su Windows Mobile 5 operacine sistema [5].

Universiteto darbuotojų sukurta piktavališkų programų aptikimo sistema susideda iš dviejų pagrindinių komponentų:

1) Energijos stebėtojo – jis renka energijos pavyzdžius ir iš šių pavyzdžių sudaro energijos išeikvojimo istoriją.

2) Duomenų analizatoriaus – jis generuoja energijos parašą iš suformuotos istorijos. Energijos parašo generavimui naudojamas efektyvus triukšmo filtravimo metodas ir duomenų suspaudimas, taip mažinant aptikimo sąnaudas.

Šie du komponentai veikia ir kartu, ir atskirai (parodyta 6 paveiksle).



6 pav. Anomalijas aptinkančios sistemos architektūra

Energijos stebėtojas sąveikauja su mobiliu įrenginiu imdamas energijos išeikvojimo pavyzdžius, kurie panaudojami energijos išeikvojimo istorijos suformavimui. Duomenų analizatorius apdoroja energijos sunaudojimo istoriją su A tipo įrenginiu (pagrindinis mobilus įrenginys) arba su B tipo įrenginiu (nutolęs serveris ar duomenis sinchronizuojantis kompiuteris). Energijos išeikvojimo istorija iš mobilaus įrenginio perduodama serveriui ar duomenis sinchrozinuojančiam kompiuteriui per USB jungtį. Duomenų perdavimas antru atveju nesuvartoja baterijos energijos, nes sumaniųjų telefonų baterija per USB jungtį dar ir pasikrauna. Energijos išeikvojimo istorijos perdavimas oru naudoja baterijos energiją, tačiau jos sunaudojama mažiau nei perduodant lokaliai (ištirta, kad, pavyzdžiui, 32 Kb duomenų perdavimas WiFi radijo bangomis aktyviu rėžimu mobiliame įrenginyje suvartoja 1,4 džaulio mažiau energijos negu skaitant duomenis iš mažos atmintinės laukimo rėžimu). Taip pat patogu ir tai, kad apie 1 Kb dydžio energijos išeikvojimo istorijos gali būti perduodamos vienu WiFi paketu.

Šio tyrimo metu buvo sukurtos keturios piktavališkos programos ir nagrinėjami mobiliajame įrenginyje jų veiksmai, formuojantys energijos parašą.

Ši piktavališkas programas aptinkanti sistema sutaupo apie 95 % talpos, neprarandant aptikimo tikslumo, ir 99% tikslumu atpažįsta piktavališkas programas.

2.3. Analizės išvados

Atliekami tyrimai, parodantys kiek energijos išeikvoja pagrindiniai mobilaus įrenginio komponentai (procesorius, atmintis, ekranas, garso, vaizdo sistema, bevielis ryšys). Ieškoma ir metodų, kaip sumažinti energijos sąnaudas, reikalingas šių komponentų veikimui.

Plintančios piktavališkos programos padaro žalos ir silpniausiajai mobilaus įrenginio vietai – baterijai, todėl ieškoma naujų būdų ir metodų kaip apsaugoti mobilius įrenginius nuo šių kenkėjiškų programų ir sutaupyti įrenginio baterijos energiją.

Norint apsisaugoti nuo piktavališkų programų, naudojami parašais bei elgesiu pagrįstų virusų aptikimo metodai. Parašais pagrįstas virusų aptikimas nelabai tinka mobiliems įrenginiams dėl jų ribotų išteklių (procesoriaus, atminties, baterijos energijos). Mobilių įrenginių piktavališkoms programoms aptikti geriau yra naudoti elgesiu pagrįstus aptikimo metodus, juolab, kad šiuo atveju yra daugiau galimybių aptikti ir dar nežinomas piktavališkas programas.

Pagrindinė apsisaugojimo nuo piktavališkų programų priemonė – antivirusinės programos. Antivirusinių programų gamintojai atlieka daugybę testų, tokių kaip aptiktų klaidingų aliarmų skaičius, peržiūrėjimo greitis, ir t.t. Tačiau nėra pateikta duomenų, kiek procentų įrenginio energijos išeikvoja antivirusinė programa. Tai ypač aktualu delniniams kompiuteriams, kurių baterijos gyvavimo laikas, naudojantis įvairiomis šio mobilaus įrenginio funkcijomis, ir taip ribotas.

3. PROGRAMINĖS ĮRANGOS DELNINUKO ENERGIJOS SUVARTOJIMO TYRIMUI PROJEKTAVIMAS

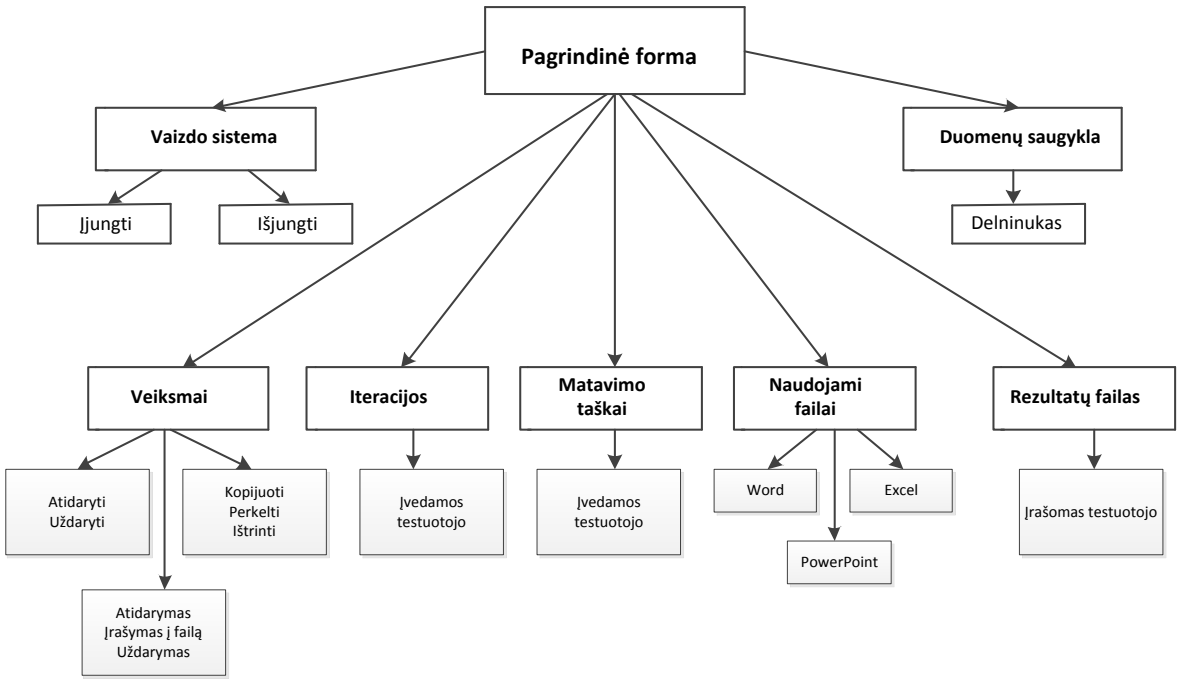
Eksperimentui atlikti sukurta programinė įranga. Panaudotos šios priemonės:

- Microsoft Windows operacinės sistemos .NET Compact Framework sandara (pasirinkta ši, nes saugos atžvilgiu ji suteikia saugesnį programavimą šioje aplinkoje, bei tinka mobiliems įrenginiams su Windows Mobile OS).
- Visual Studio 2008 Professional Edition.
- Objektiškai orientuota programavimo kalba C#.
- Delninukas su Windows Mobile Professional 6 SDK OS.

3.1. Programos struktūra

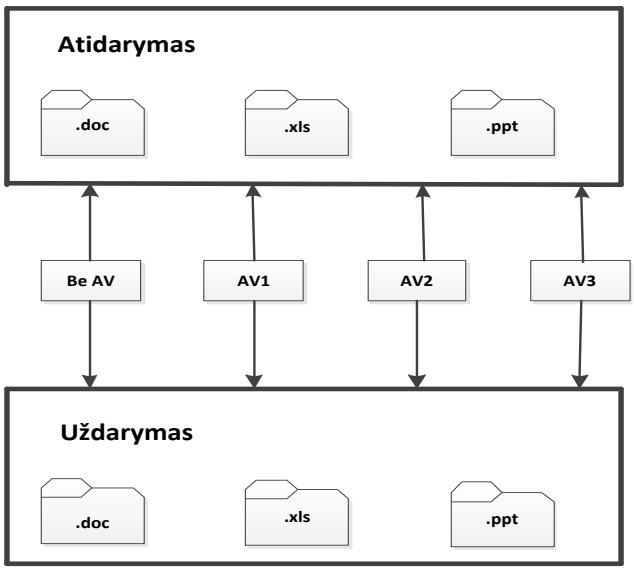
Programinė įranga atidaro, uždaro skirtingų formatų Microsoft Office failus; kopijuoja, perkelia šiuos failus iš vieno katalogo į kitą, ištrina perkeltus failus; atidaro failą ir į jį įrašinėja nustatytą simbolių eilutę. Atliekant šiuos veiksmus stebimas delnininio kompiuterio baterijos energijos likutis, kuris, kartu su kitais stebimais parametrais, fiksuojamas rezultatų failuose.

Programos struktūra pavaizduota 7 paveiksle.



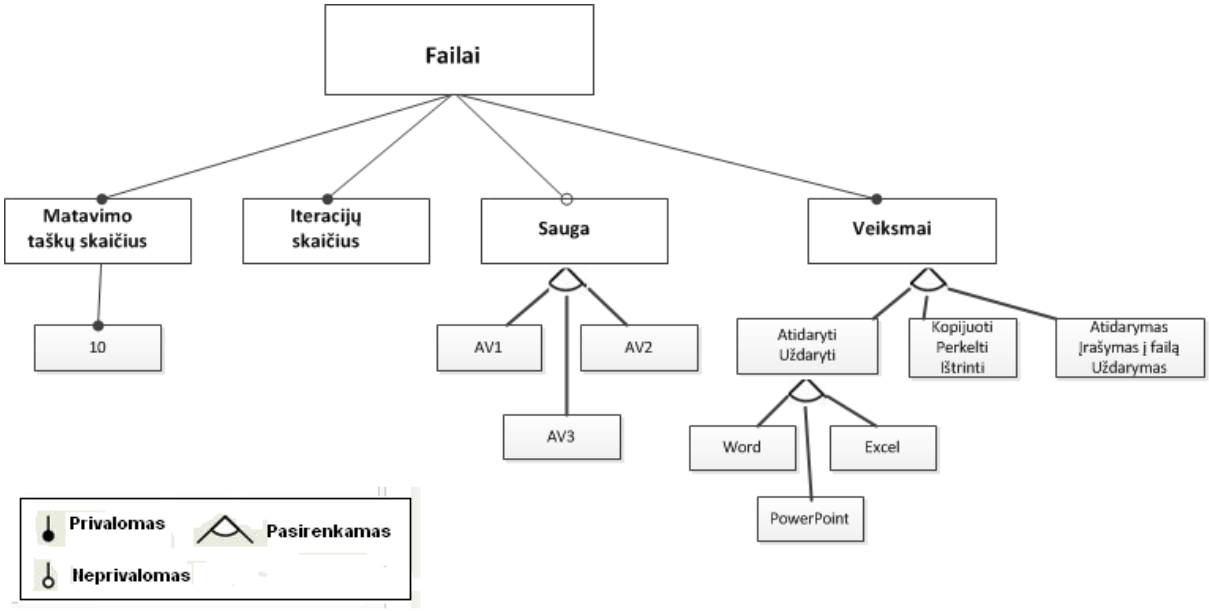
7 pav. Programos struktūra

Tyrimas bus atliekamas įdiegiant pasirinktą programinę įrangą į delninį kompiuterį. Duomenų tyrimui failų struktūra pavaizduota 8 paveiksle.



8 pav. Duomenų tyrimui failų struktūra [15]

Sukurta programinė įranga leis atlikti aukščiau minėtus su veiksmus su failais. „Windows Mobile Device Center“ programinė įranga leidžia sėkmingai sąveikauti mobiliam įrenginiui su kompiuteriu keičiantis programomis ir duomenimis (kompiuteryje turi būti įdiegta Microsoft Windows operacinė sistema). Tyrimui sukurtas katalogas „Tyrimas“, kurio turinį matome 20 paveiksle. Failų pavadinimai ir kelias iki katalogo nurodytas programoje. Neįkėlus į katalogą „Tyrimas“ programoje nurodytų failų arba įkėlus juos kitokiais pavadinimais, nei yra nurodyti programoje, programa neveiks ir bus gaunamas atitinkamas klaidos pranešimas.

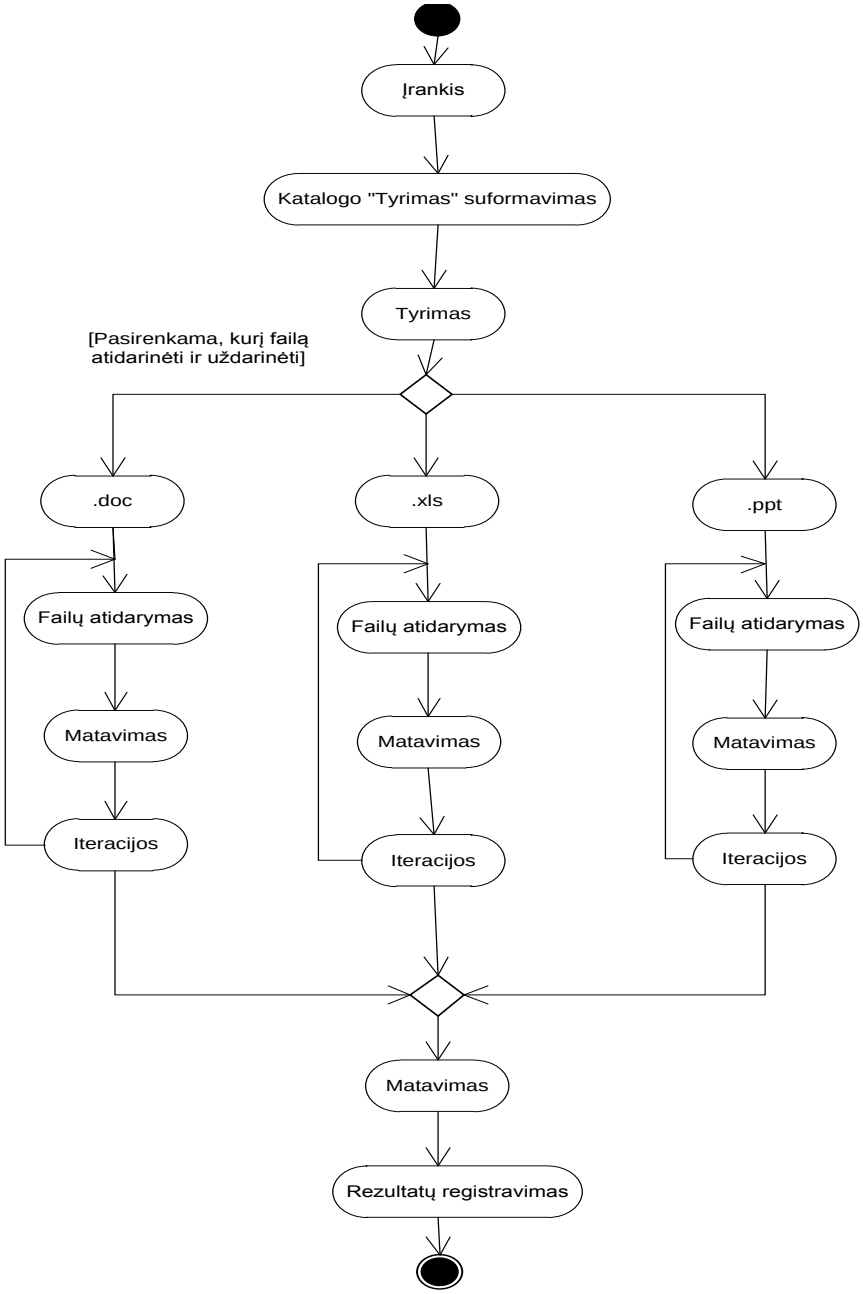


9 pav. Požymių diagrama

Iš failų požymių diagramos (9 pav.) matome, kad būtina nurodyti matavimo taškų skaičių, iteracijų skaičių, atliekamus veiksmus. Saugumo pasirinkimas nebūtinas (kai tyrimas

atliekamas be antivirusinės programinės įrangos). Būtina pasirinkti vieną iš galimų veiksmų darbui su failais.

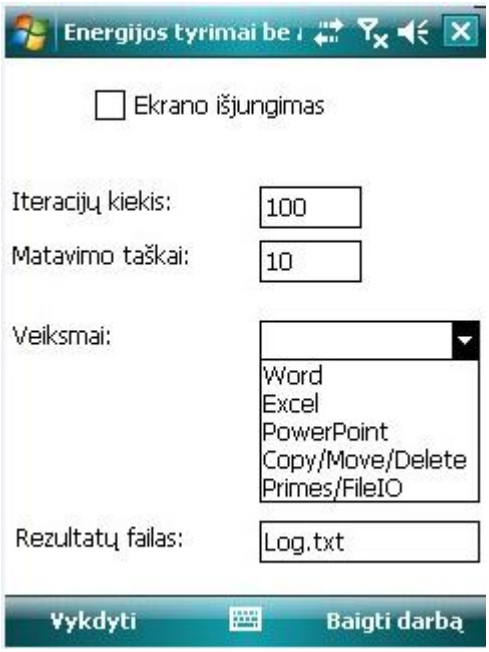
Kad nebūtų naudojama energija vaizdo rodymui atliekant veiksmus su failais ir būtų gaunami kuo tikslesni tyrimo rezultatai, yra sukurta funkcija „Video Power Off“, leidžianti išjungti delninuko vaizdo sistemą, kai yra nustatomi 9 pav. pavaizduoti būtini parametrai ir tada paleidžiama vykdyti programa. Kadangi delninio kompiuterio atmintis nėra tokia didelė kaip asmeninio ar stacionaraus kompiuterio, tyrime naudojami iki 1MB dydžio failai ir su jais atliekami veiksmai tiek kartų, kiek iteracijų nustatome (10 pav.).



10 pav. Matavimų algoritmas failų atidarymui,uždarymui

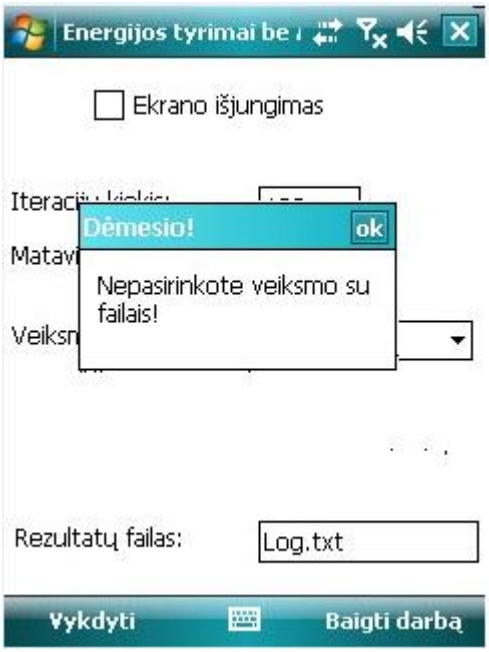
Eksperimento rezultatai saugomi delninio kompiuterio flash atmintyje, CSV tipo „Log“ faile (.txt). Tokį failą patogu importuoti į Microsoft Excel programą ir ten atlikti grafinius duomenų apdorojimus.

Pagrindinis programos delninuko langas pateiktas 11 paveiksle.



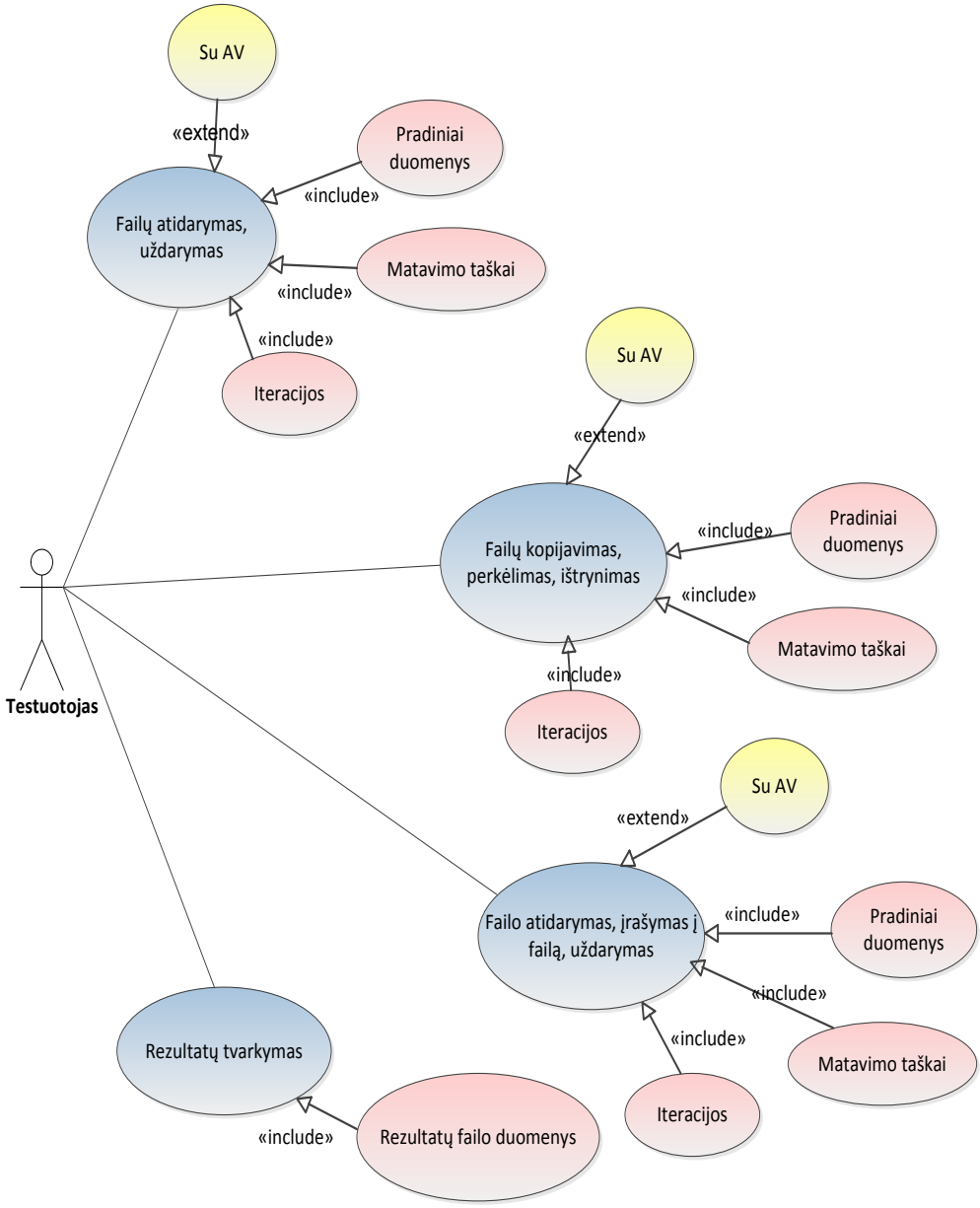
11 pav. Programos langas

Laukelyje nepasirinkus kokius veiksmus vykdyti su failais ir paspaudus mygtuką „Vykdyti“, pagrindiniame programos lange atsiranda pranešimas (žiūrėti 12 paveikslą.)



12 pav. Pagrindinis programos langas su klaidos pranešimu

Panaudojimo atvejų schema pateikta 13 paveiksle. Šiuo atveju yra tik vienas, inicijuojantis aktorius – žmogus, kuris testuoja sukurtą programinę įrangą.



13 pav. Panaudojimo atvejų schema

3.2. Programos aprašymas

Matavimai atliekami kelis kartus, su įdiegta pasirinkta antivirusine programine įranga ir be jos. Prieš atliekant tyrimą nurodomi būtini parametrai: iteracijų skaičius, matavimo taškų skaičius, veiksmas su failais, išjungiamas ekranas.

Pasibaigus programos vykdymui ekranas automatiškai įsijungia. Suformuojamas rezultatų failas. Kadangi atliekamas ne vienas tyrimas, tai patogu kiekvienąkart, prieš paleidžiant vykdyti programą, nurodyti vis kitą rezultatų failo pavadinimą, kuriuo būtų išsaugoti matavimų duomenys.

Rezultatų faile saugoma informacija apie failus (kokio tipo ir dydžio failas buvo atidarytas, kiek kartų); koks buvo atliekamas veiksmas; iteracijų skaičius, parodantis kiek ciklų buvo atlikta, fiksuojami matavimo taškai; laikas prieš atliekant veiksmus su failu bei po atlikimo; delninuko baterijos energija procentais. Matavimo intervalas gaunamas iteracijų skaičių padalinus iš matavimo taškų skaičiaus. Detalesnis rezultatų failo laukų aprašymas pateiktas 10 lentelėje.

10 lentelė. Rezultatų failo laukų sąrašas ir aprašymas

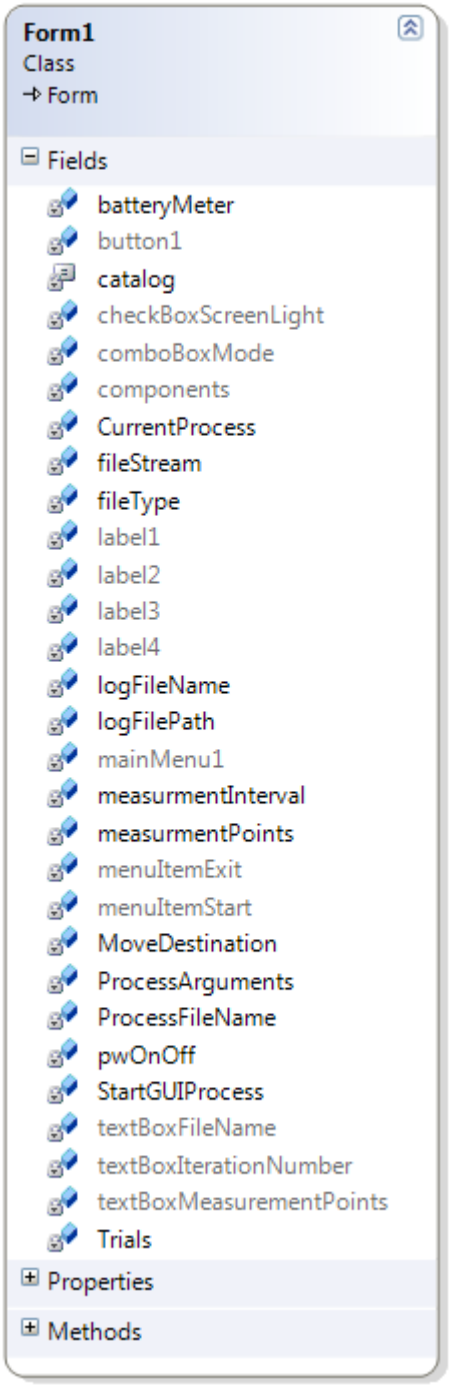
Eil. Nr.	**Lauko pavadinimas**	**Lauko aprašymas**
1.	FileType	Failo tipas arba atliekamas veiksmas
2.	Iteration	Iteracijų skaičius
3.	Measurement	Matavimo taškai
4.	ByteCount	Cikle prasuktų baitų skaičius
5.	Date	Tyrimo vykdymo data (metai, mėnuo, diena)
6.	Time	Vykdymo laikas
7.	ACLineStatus	Eilutės būsena
8.	BatteryLifePercentage	Baterijos gyvavimo laikas, %
9.	BatteryVoltage	Baterijos įtampa
10.	BatteryCurrent	Baterijos srovė
11.	BatteryTemperature	Baterijos temperatūra

Kaskart, nurodžius iteracijų bei matavimo taškų skaičių ir pasirinkus norimą veiksmą su failais, CSV faile fiksuojami rezultatai. Rezultatų failo pavyzdys matomas 14 paveiksle.

```
FileType;Iteration;Measurement;ByteCount;Date;Time;ACLineStatus;BatteryLifePercentage;BatteryLifeTime;BatteryFullLifeTime;BatteryVoltage;BatteryCurrent;BatteryTemperature;
Word;0;0;0;11.01.26;09:41:43;Offline;100;4294967295;4294967295;0;0;0;
Word;35;1;28761600;11.01.26;10:00:33;Offline;93;4294967295;4294967295;0;0;0;
Word;70;2;57523200;11.01.26;10:19:24;Offline;86;4294967295;4294967295;0;0;0;
```

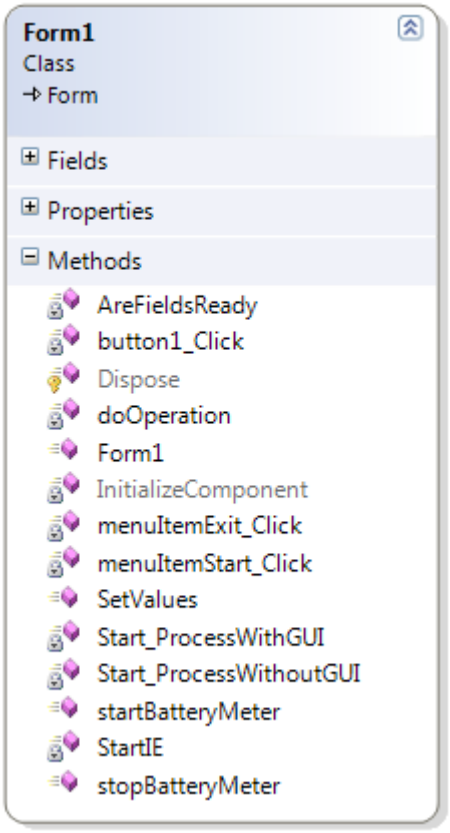
14 pav. Tekstinio failo pavyzdys su tyrimo rezultatų duomenimis

Programoje sukurta standartinė forma `public partial class Form1 : Form.` Joje aprašyti naudojami metodai ir kintamieji, kurie įjungia, išjungia ekraną, nuskaito pradinius duomenis, įrašo gautus duomenis į rezultatų failus.



15 pav. Naudojamų kintamųjų sąrašas

Ne visi 15 paveiksle matomi kintamieji (kaip kad „fileType“, „measurmentPoints“) yra įrašomi į rezultatų failus, dalis jų naudojami programoje kaip tarpiniai ar pagalbiniai kintamieji.



16 pav. Naudojamų metodų sąrašas

Trumpas 16 paveikslo piktogramų paaiškinimas:

„protected“-metodas, matomas tik klasės kūrėjui;

„private“-metodas, matomas tik klasės kūrėjui;

„public“-metodas, matomas visiems.

Pagrindinių metodų paaiškinimas:

Metodu „AreFieldsReady“ patikrinama, ar pasirinktas vykdyti veiksmas su failu. Baterijos matavimas pradedamas metodu „StartBatteryMeter“, o stabdomas metodu „StopBatteryMeter“. Pradiniai nustatymai atliekami metodu „SetValues“. Metodu „doOperation“ atliekami failų atidarymo ir baterijos matavimo veiksmai.

3.3. Reikalavimai sistemai

3.3.1. Funkciniai reikalavimai

1. Programa turi leisti pasirinkti ir atidaryti suformuotą katalogą „Tyrimas“.
2. Programa turi leisti atidaryti ir uždaryti failus kataloge.
3. Programa turi leisti išjungti grafinę kortą bei jos maitinimą.
4. Programa turi leisti nustatyti norimą iteracijų kiekį.
5. Programa turi leisti nustatyti norimą matavimo taškų skaičių.

6. Programa turi fiksuoti matavimus.

7. Programa turi leisti registruoti ir išsaugoti rezultatus.

8. Programa turi leisti įrašyti norimą rezultatų failo pavadinimą.

9. Programa turi leisti atlikti eksperimentą su antivirusine programine įranga ir be jos.

3.3.2. Nefunkciniai reikalavimai

1. Programa turi būt realizuota C# programavimo kalba.

2. Paleista programa turi veikti cikle (atidarinėti failus nustatytą iteracijų skaičių bei registruoti rezultatus) be vartotojo įsikišimo iki išseks delninuko baterija.

3. Delninuke turi būti galimybė suformuoti katalogą iš Word, Excel ir PowerPoint programų failų.

4. Delninuke turi būti palaikoma Windows Mobile Professional 6 SDK operacinė sistema.

5. Pasirinkta antivirusinė programinė įranga turi būti tinkama delninukui.

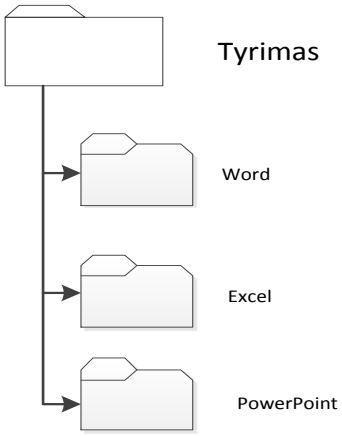
4. EKSPERIMENTINIS DELNINUKO ENERGIJOS SUVARTOJIMO TYRIMAS

Eksperimentas atliekamas panaudojant delninį kompiuterį ASUS P750. Jo pagrindiniai parametrai:

- Procesorius: PXA270 520 MHz.
- Atmintis: 256 MB.
- OS: Window Mobile 6 Professional.

4.1. Eksperimento metodika

Eksperimente naudojami įvairių formatų Microsoft Office failai. Rankiniu būdu suformuojamas katalogas „Tyrimas“ (žiūrėti 17 pav.), kuriame patalpinami .doc, .xls, .ppt formato failai.



17 pav. Katalogo „Tyrimas“ turinys

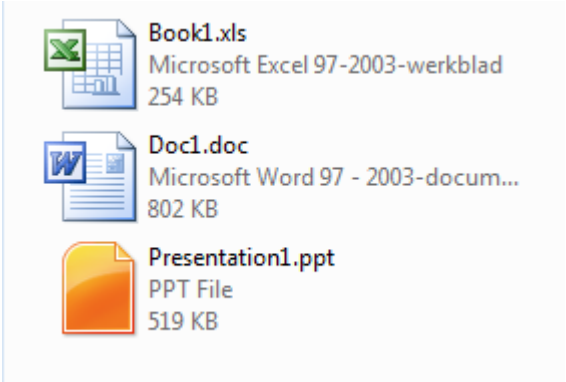
Prieš atliekant eksperimentą yra pilnai pakraunama delninuko baterija. Kad eksperimento rezultatai būtų tikslūs, grafinė korta ir jos maitinimas išjungiami, taigi, veiks tik procesorius ir atmintis.

Eksperimentas atliekamas pagal kelis kompanijos „PassMark Software“ 2010 m. rugsėjo 30 d. antivirusinės programinės įrangos testavimo etalonus [11] (3 priedas; trečias, dešimtas ir penkioliktas etalonai).

Eksperimente tiriama, kiek procentų delninuko baterijos išeikvos šie veiksmai:

1. Delninuko MS Office failų atidarymas / uždarymas:
   a) Word,
   b) Excel,
   c) Power Point.

Eksperimente naudojami atsitiktinai naudotojo kompiuteryje parinkti MS Office failai (žr. 18 pav., 2 priedas). Jie yra įkelti į katalogą „Tyrimas“.



18 pav. Eksperimente naudojami MS Office failai

Tiriama, kiek laiko ir delninuko energijos bus sunaudota šių failų atidarymui, uždarymui.

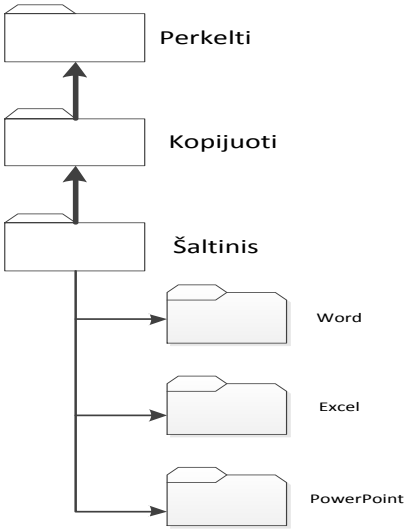
2. Failų kopijavimas, perkėlimas ir ištrynimas.

Paleidus programą, automatiškai yra sukuriami trys katalogai: „Šaltinis“, „Kopijuoti“ ir „Perkelti“. Į pradinį katalogą („ Šaltinis“) rankiniu būdu patalpinami tie patys eksperimente naudojami kelių formatų failai (18 paveikslas). Tada atliekami šie veiksmai (žiūrėti 19 pav.) :

a) iš katalogo „Šaltinis“ visi jame esantys failai nukopijuojami į katalogą „Kopijuoti“,

b) iš katalogo „Kopijuoti“ visi jame atsiradę failai perkeliami į katalogą „Perkelti“,

c) iš katalogo „Perkelti“ ištrinami visi jame esantys perkelti failai.



19 pav. Katalogai funkcijai „Kopijavimas-perkėlimas-ištrynimas“ atlikti

Tiriama, kiek laiko ir delninuko energijos bus sunaudota kataloge esančių failų kopijavimui, perkėlimui ir ištrynimui.

3. Įrašymas į failą, atidarymas ir uždarymas.

Programiškai yra sukuriamas failas testing.txt, failas atidaromas, į jį įrašoma eilutė „Writing this to a file.\n“, tada failas uždaromas. Po šių veiksmų failas vėl atidaromas, įrašoma dar viena tokia pati eilutė ir failas uždaromas. Taip, kartojant tuos pačius žingsnius, į failą yra įrašoma 100 eilučių.

Tiriama, kiek laiko ir delninuko energijos bus sunaudota įrašymui į failą, jo atidarymui ir uždarymui.

Visi minėti veiksmai yra atliekami programiškai, imituojamas naudotojo darbas. Matavimai atliekami kelis kartus: be antivirusinės programinės įrangos, su viena antivirusine programine įranga, su antra antivirusine programine įranga ir su trečia antivirusine programine įranga.

Eksperimente naudojamos antivirusinės programinės įrangos atrinkimo kriterijai:

a) reitingo pozicija (viena pozicija iš reitingo pradžios, kita - iš vidurio, trečia - iš galo (20 pav),

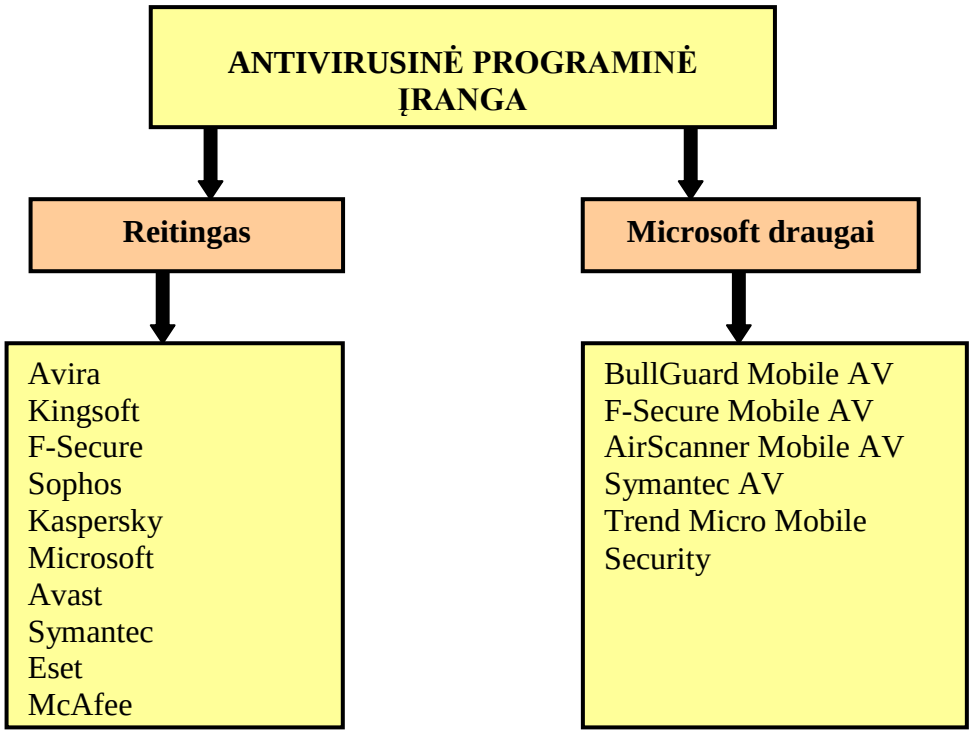
b) bent viena jų yra Microsoft partnerių rekomenduojamų antivirusinių programinių įrangų mobiliems įrenginiams sąraše (20 pav.),

c) tinkamumas delniniams kompiuteriams,

d) tinkamumas Windows Mobile 6.0 operacinei sistemai,

e) bandomasis periodas – ne mažesnis nei viena savaitė.

Antivirusinė programinė įranga atsisiunčiama iš gamintojų pagal nepriklausomos laboratorijos „AV-comparatives“ reitingų rezultatus (2009 m. gruodis) dešimtuke pavaizduotos antivirusinės programinės įrangos) bei pagal Microsoft partnerių rekomenduojamas antivirusines programas mobiliems įrenginiams (žiūrėti 20 pav.).



20 pav. Antivirusinė programinė įranga delninukams

Pagal aukščiau minėtus kriterijus parinkta ši antivirusinė programinė įranga ir įdiegta į delninį kompiuterį iš gamintojų oficialių internetinių šaltinių [7,8,9]:

1. „Kaspersky 9.0“. Šios antivirusinės programinės įrangos galimybės bei nustatymai, naudojami tyrime, pateikti 11 lentelėje.

11 lentelė. „Kaspersky“ AV programinės įrangos galimybės ir nustatymai

Funkcija	Aprašymas	Nustatymai
Apsauga nuo virusų	Apsaugo nuo kenkėjiškų programų. Failai yra peržiūrimi nuo jų pirmo pasirodymo įrenginyje, paleidžiant programą, atidarant failus ir pan.	Apsauga nuo virusų: Įjungta Peržiūrėjimo objektai: • Visi failai • Tik vykdomi failai Jei aptinkamas virusas: • Izoliuoti • Ištrinti • Paklausti naudotojo, ką daryti toliau
Apsauga nuo vagystės	Apsaugo duomenis, esančius įrenginyje nuo nesankcionuotos prieigos. Funkcija naudinga, kai prietaisas pametamas ar yra pavogtas.	Blokavimas: Išjungta Duomenų valymas: Išjungta SIM stebėjimas: Išjungta GPS paieška: Išjungta
Privati apsauga	Apsaugo konfidencialius duomenis, kol kiti asmenys laikinai naudojasi įrenginiu. Yra paslepiami asmeniniai duomenys (kaip įrašai ar kontaktai), susirašinėjimas SMS žinutėmis, duomenys skambučių žurnale, įeinantys skambučiai ir pan.	Rėžimas: • Normalus • Privatus (kontaktų sąrašas, paslėpti objektai)
Užšifravimas	Saugo duomenis įrenginyje nuo jų peržiūrėjimo, naudojantis įrenginiu pašaliniams asmenims. Galima užšifruoti norimą katalogų kiekį.	Katalogų sąrašas Blokavimo prieiga Ši paslauga neįjungta.
Apsauga prieš brukalus (angl. *spam*)	Apsaugo nuo nepageidaujamų skambučių ir SMS žinučių. Yra filtruojami skambučiai ar žinutės, panaudojant Juodąjį ir Baltąjį sąrašus.	Rėžimas: • Išjungta • Naudojami abu sąrašai • Baltasis sąrašas • Juodasis sąrašas
Esanti (angl. *parental*) kontrolė	Filtruoja išeinančias žinutes ir skambučius, remiantis Juoduoju ir Baltuoju sąrašais. Šiuose sąrašuose yra telefono numeriai, kuriuos šis komponentas arba blokuoja, arba leidžia siųsti žinutes ir skambinti.	Išjungta
Ugniasienė	Analizuoja visus įrenginio tinklo ryšius. Leidžia pasirinkti, kurie sujungimai galimi (pavyzdžiui, el. pašto peržiūrėjimas), o kuriuos blokuoti (pavyzdžiui., paiešką internete, failų atsiuntimą).	Rėžimas: • Išjungta • Minimali apsauga • Maksimali apsauga • Blokuoti viską

11 lentelės tęsinys kitame puslapyje

11 lentelės tęsinys

Papildomos funkcijos	Leidžia siųsti komandą į kitą įrenginį, tam, kad būtų inicijuotas nuotolinis blokavimas, nuslėpti duomenys ar aptikta įrenginio buvimo vieta. Komanda siunčiama šifruotos SMS žinutės pavidalu	Licencija Komandos siuntimas Blokavimas Duomenų ištrynimas GPS paieška Privati apsauga Telefono nr Nuotolinis kodas Duomenų bazė
Apsaugos būsena	Parodo, kokie yra pasirinkti nustatymai įrenginyje	• Apsauga: Duomenų bazės: Išjungta • Ugniasienė : Išjungta • Apsauga nuo vagystės: Išjungta • Privati apsauga: Normali (įprasta) • Licencijos galiojimas: 31 d

2. „F-Secure“. Analogiškai pagrindiniai nustatymai antros antivirusinės programos - „F-Secure“ - parodyti 12 lentelėje.

12 lentelė. „F-Secure“ AV programinės įrangos galimybės ir nustatymai

Funkcija	**Nustatymai**
Peržiūrėti (angl.scan) viską	Nenaudojama
Apsauga nuo virusų	Realaus laiko apsauga: Įjungta Automatiniai atnaujinimai: • Visada • Namų tinkle • Niekada
Ugniasienė	Saugumo lygis: • Uždrausti viską • Aukštas • Normalus • Leisti viską • Įprastas
Apsauga nuo vagysčių	Nuotolinis užrakinimas: Išjungta Nuotolinis trynimas: Išjungta Paskutinis užrakinimo laikas: Nebuvo Paskutinis užrakinimas: Nebuvo Prieš tai buvęs užrakinimas: Nebuvo
Naršymo internete apsauga	Įjungta

3. „ESET“. Pagrindiniai nustatymai trečios antivirusinės programos - „ESET“ - parodyti 13 lentelėje.

13 lentelė. „ESET“ AV programinės įrangos galimybės ir nustatymai

Funkcija	**Nustatymai**
Peržiūrėti (angl.*scan*) viską, pasirinktą katalogą	Nenaudojama
Tikrinami praplėtimai	• Exe • Dll • Msi • Dat • Com • Cab • Ocx • Archyvai • Kiti
Ugniasienė	Saugumo lygis: • Leisti viską • Blokuoti viską • Įprastas
Apsauga nuo vagysčių	Neijungta
Naršymo internete apsauga	Įjungta

4 priede pateikta smulkesnė informacija apie šias mobiliųjų įrenginių antivirusinių programų funkcijas ir funkcijų palyginimas tarp šių antivirusinių programų [6].

Kadangi delninio kompiuterio baterijos gyvavimo laikas yra ribotas, o delninuko bateriją eksperimente ketinama iškrauti iki ~20%, tai, kad programa spėtų užfiksuoti tyrimo rezultatus, pradžioje pabandymui parenkame iteracijų skaičių 10-50 (tą patį bandymą atliekame be antivirusinės programinės įrangos ir su viena bet kuria antivirusine programine įranga kiekvienam atskiram atvejui). Pagal gautus bandymo rezultatus, atsižvelgdami į baterijos išsikrovimą procentais, paskaičiuojame, kiek reikia iteracijų, norint delninuko bateriją iškrauti iki leistinos ribos. Parinktas eksperimentui atlikti iteracijų skaičius pateiktas 14 lentelėje.

14 lentelė. Eksperimentui parinktų iteracijų kiekis

Saugumas	**Veiksmai su failais**				
	Delninuko MS Office failų atidarymas/uždarymas			Failų kopijavimas, perkėlimas ir ištrynimas	Įrašymas į failą, atidarymas ir uždarymas
	Word	Excel	PowerPoint		
Be AV	400	2000	6000	5000	1200
Su AV	350	1500	4500-5000	4500	1000

Visi matavimai atliekami nurodžius vienodą matavimo taškų skaičių – 10.

Gauti eksperimento rezultatai iš delninuko perkeliami i stacionarų kompiuterį detalesniam apdorojimui.

4.2. Eksperimento rezultatai

4.2.1. Skaitiniai eksperimento rezultatai

Eksperimento duomenys pateikti 15- 26 lentelėse.

Gauti rezultatai, atlikus tyrimą be antivirusinės programinės įrangos, pateikti 15-17 lentelėse.

15 lentelė. Eksperimento su Word ir Excel failų atidarymu, uždarymu rezultatai be antivirusinės programinės įrangos

Matavimo taškai	Iteracijos		Baitų kiekis		Laikas		Baterijos likutis, %	
	Word	**Excel**	**Word**	**Excel**	**Word**	**Excel**	**Word**	**Excel**
0	0	0	0	0	07:52:30	17:49:15	100	100
1	40	200	32870400	52121600	08:14:03	18:12:11	91	94
2	80	400	65740800	104243200	08:35:37	18:35:07	83	88
3	120	600	98611200	156364800	08:57:11	18:58:03	76	80
4	160	800	131481600	208486400	09:18:43	19:20:58	68	72
5	200	1000	164352000	260608000	09:40:17	19:43:53	60	64
6	240	1200	197222400	312729600	10:01:50	20:06:49	52	57
7	280	1400	230092800	364851200	10:23:24	20:29:43	44	49
8	320	1600	262963200	416972800	10:44:58	20:52:39	37	42
9	360	1800	295833600	469094400	11:06:31	21:15:37	29	35
10	400	2000	328704000	521216000	11:28:04	21:38:32	22	28
Iš viso:					**03:35:34**	**03:49:17**	**78**	**72**

16 lentelė. Eksperimento su Power Point failo atidarymu, uždarymu ir failų kopijavimu, perkėlimu, ištrynimu rezultatai be antivirusinės programinės įrangos

Matavimo taškai	Iteracijos		Baitų kiekis		Laikas		Baterijos likutis, %	
	Power Point	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**
0	0	0	0	0	01:52:26	03:33:01	100	100
1	600	500	318873600	806912000	03:03:32	03:51:25	92	91
2	1200	1000	637747200	613824000	04:14:40	03:51:25	87	83
3	1800	1500	956620800	2420736000	05:25:50	04:28:08	79	76
4	2400	2000	1275494400	3227648000	06:37:02	04:46:30	70	68
5	3000	2500	1594368000	034560000	07:48:17	05:04:52	62	60
6	3600	3000	1913241600	4841472000	08:59:32	05:23:13	53	52
7	4200	3500	2232115200	5648384000	10:10:47	05:41:36	46	45
8	4800	4000	2550988800	6455296000	11:22:05	05:59:58	38	38
9	5400	4500	2869862400	7262208000	12:33:27	06:18:19	30	31
10	6000	5000	3188736000	8069120000	13:44:52	06:36:41	22	24
Iš viso:					**11:52:26**	**03:03:40**	**78**	**76**

17 lentelė. Eksperimento su įrašymu į failą, atidarymu ir uždarymu rezultatai be antivirusinės programinės įrangos

Matavimo taškai	Iteracijos	Baitų kiekis	Laikas	Baterijos likutis, %
	Primes /FileIO			
0	0	0	21:07:12	100
1	120	300000	21:26:05	92
2	240	600000	21:44:57	84
3	360	900000	22:03:47	76
4	480	1200000	22:22:37	68
5	600	1500000	22:41:29	59
6	720	1800000	23:00:19	50
7	840	2100000	23:19:09	43
8	960	2400000	23:38:01	35
9	1080	2700000	23:56:51	27
10	1200	3000000	00:15:44	19
Iš viso:			**03:08:32**	**81**

Gauti rezultatai, atlikus tyrimą su „Kaspersky“ antivirusine programine įranga, pateikti 18-20 lentelėse.

18 lentelė. Eksperimento su Word ir Excel failų atidarymu, uždarymu rezultatai su pirma antivirusine programine įranga

Matavimo taškai	**Iteracijos**		**Baitų kiekis**		**Laikas**		**Baterijos likutis, %**	
	Word	**Excel**	**Word**	**Excel**	**Word**	**Excel**	**Word**	**Excel**
0	0	0	0	0	13:43:31	21:02:25	99	100
1	35	150	28761600	39091200	14:02:23	21:19:50	90	91
2	70	300	57523200	78182400	14:21:15	21:37:16	82	83
3	105	450	86284800	117273600	14:40:10	21:54:40	73	77
4	140	600	115046400	156364800	14:59:04	22:12:04	66	69
5	175	750	143808000	195456000	15:17:54	22:29:29	58	61
6	210	900	172569600	234547200	15:36:51	22:46:56	49	54
7	245	1050	201331200	273638400	15:55:42	23:04:22	42	47
8	280	1200	230092800	312729600	16:14:36	23:21:46	34	40
9	315	1350	258854400	351820800	16:33:30	23:39:13	27	33
10	350	1500	287616000	390912000	16:52:19	23:56:38	19	26
Iš viso:					**03:08:48**	**02:54:13**	**80**	**74**

19 lentelė. Eksperimento su Power Point failo atidarymu, uždarymu ir failų kopijavimu, perkėlimu, ištrynimu rezultatai su pirma antivirusine programine įranga

Matavimo taškai	**Iteracijos**		**Baitų kiekis**		**Laikas**		**Baterijos likutis, %**	
	Power Point	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**
0	0	0	0	0	03:20:06	02:50:38	100	100
1	500	450	265728000	726220800	04:22:27	03:08:50	91	93
2	1000	900	531456000	1452441600	05:24:50	03:27:02	82	84
3	1500	1350	797184000	2178662400	06:27:16	03:45:15	73	78
4	2000	1800	1062912000	2904883200	07:29:41	04:03:26	64	70
5	2500	2250	1328640000	3631104000	08:32:07	04:21:36	54	62
6	3000	2700	1594368000	4357324800	09:34:33	04:39:49	46	54
7	3500	3150	1860096000	5083545600	10:36:58	04:58:01	37	47
8	4000	3600	2125824000	5809766400	11:39:26	05:16:13	29	40
9	4500	4050	2391552000	6535987200	12:41:55	05:34:24	20	33
10	5000	4500	2657280000	7262208000	13:44:17	05:52:36	11	26
Iš viso:					**10:24:11**	**03:01:58**	**89**	**74**

20 lentelė. Eksperimento su įrašymu į failą, atidarymu ir uždarymu rezultatai su pirma antivirusine programine įranga

Matavimo taškai	**Iteracijos**	**Baitų kiekis**	**Laikas**	**Baterijos likutis, %**
	Primes /FileIO			
0	0	0	17:17:18	100
1	100	250000	17:34:49	91
2	200	500000	17:52:19	82
3	300	750000	18:09:51	74
4	400	1000000	18:27:23	67
5	500	1250000	18:44:54	59
6	600	1500000	19:02:24	50
7	700	1750000	19:19:58	43
8	800	2000000	19:37:28	36
9	900	2250000	19:54:59	28
10	1000	2500000	20:12:32	21
Iš viso:			**02:55:14**	**79**

Gauti rezultatai, atlikus tyrimą su „F-Secure“ antivirusine programine įranga, pateikti 21-23 lentelėse.

21 lentelė. Eksperimento su Word ir Excel failų atidarymu, uždarymu rezultatai su antra antivirusine programine įranga

Matavimo taškai	**Iteracijos**		**Baitų kiekis**		**Laikas**		**Baterijos likutis, %**	
	Word	**Excel**	**Word**	**Excel**	**Word**	**Excel**	**Word**	**Excel**
0	0	0	0	0	09:41:43	01:23:42	100	100
1	35	150	28761600	39091200	10:00:33	01:41:02	93	97
2	70	300	57523200	78182400	10:19:24	01:58:21	86	90
3	105	450	86284800	117273600	10:38:15	02:15:43	78	83
4	140	600	115046400	156364800	10:57:03	02:33:01	70	77
5	175	750	143808000	195456000	11:15:53	02:50:19	62	69
6	210	900	172569600	234547200	11:34:42	03:07:37	54	62
7	245	1050	201331200	273638400	11:53:32	03:24:56	47	54
8	280	1200	230092800	312729600	12:12:20	03:42:14	40	47
9	315	1350	258854400	351820800	12:31:13	03:59:33	33	40
10	350	1500	287616000	390912000	12:50:02	04:16:51	26	34
Iš viso:					**03:08:19**	**02:53:09**	**74**	**66**

22 lentelė. Eksperimento su Power Point failo atidarymu, uždarymu ir failų kopijavimu, perkėlimu, ištrynimu rezultatai su antra antivirusine programine įranga

Matavimo taškai	**Iteracijos**		**Baitų kiekis**		**Laikas**		**Baterijos likutis, %**	
	Power Point	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**
0	0	0	0	0	22:11:40	04:09:22	100	100
1	450	450	239155200	726220800	23:06:12	04:27:30	94	95
2	900	900	478310400	1452441600	00:00:41	04:45:37	87	86
3	1350	1350	717465600	2178662400	00:55:13	05:03:46	80	81
4	1800	1800	956620800	2904883200	01:49:42	05:21:53	72	72
5	2250	2250	1195776000	3631104000	02:44:13	05:40:02	64	64
6	2700	2700	1434931200	4357324800	03:38:45	05:58:10	57	56
7	3150	3150	1674086400	5083545600	04:33:15	06:16:16	50	49
8	3600	3600	1913241600	5809766400	05:27:46	06:34:26	43	41
9	4050	4050	2152396800	6535987200	06:22:18	06:52:34	36	35
10	4500	4500	2391552000	7262208000	07:16:49	07:10:42	29	29
Iš viso:					**09:05:09**	**03:01:20**	**71**	**71**

23 lentelė. Eksperimento su įrašymu į failą, atidarymu ir uždarymu rezultatai su antra antivirusine programine įranga

Matavimo taškai	**Iteracijos**	**Baitų kiekis**	**Laikas**	**Baterijos likutis, %**
	Primes /FileIO			
0	0	0	03:07:12	100
1	100	250000	03:24:37	93
2	200	500000	03:42:01	86
3	300	750000	03:59:29	78
4	400	1000000	04:16:52	70
5	500	1250000	04:34:19	62
6	600	1500000	04:51:42	53
7	700	1750000	05:09:07	44
8	800	2000000	05:09:07	38
9	900	2250000	05:43:57	30
10	1000	2500000	06:01:25	24
Iš viso:			**02:54:13**	**76**

Gauti rezultatai, atlikus tyrimą su „ESET“ antivirusine programine įranga, pateikti 24-26 lentelėse.

24 lentelė. Eksperimento su Word ir Excel failų atidarymu, uždarymu rezultatai su trečia antivirusine programine įranga

Matavimo taškai	**Iteracijos**		**Baitų kiekis**		**Laikas**		**Baterijos likutis, %**	
	Word	**Excel**	**Word**	**Excel**	**Word**	**Excel**	**Word**	**Excel**
0	0	0	0	0	09:54:25	22:35:22	100	100
1	35	150	28761600	39091200	10:13:06	22:52:56	91	94
2	70	300	57523200	78182400	10:31:45	23:10:30	82	87
3	105	450	86284800	117273600	10:50:23	23:28:05	74	80
4	140	600	115046400	156364800	11:09:03	23:45:34	67	72
5	175	750	143808000	195456000	11:27:42	00:03:04	59	66
6	210	900	172569600	234547200	11:46:20	00:20:33	51	58
7	245	1050	201331200	273638400	12:04:59	00:38:05	44	50
8	280	1200	230092800	312729600	12:23:39	00:55:33	37	43
9	315	1350	258854400	351820800	12:42:18	01:13:03	29	39
10	350	1500	287616000	390912000	13:00:56	01:30:33	22	29
Iš viso:					**03:06:31**	**02:55:11**	**78**	**71**

25 lentelė. Eksperimento su Power Point failo atidarymu, uždarymu ir failų kopijavimu, perkėlimu, ištrynimu rezultatai su trečia antivirusine programine įranga

Matavimo taškai	**Iteracijos**		**Baitų kiekis**		**Laikas**		**Baterijos likutis, %**	
	Power Point	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**	**Power Point**	**Copy, Move, Delete**
0	0	0	0	0	17:33:26	02:59:55	100	100
1	450	450	239155200	726220800	18:28:49	03:17:48	92	92
2	900	900	478310400	1452441600	19:24:11	03:35:41	83	84
3	1350	1350	717465600	2178662400	20:19:33	03:53:32	74	77
4	1800	1800	956620800	2904883200	21:14:56	04:11:25	67	70
5	2250	2250	1195776000	3631104000	22:10:18	04:29:16	58	62
6	2700	2700	1434931200	4357324800	23:05:38	04:47:08	49	54
7	3150	3150	1674086400	5083545600	00:01:00	05:04:59	41	47
8	3600	3600	1913241600	5809766400	00:56:22	05:22:53	33	40
9	4050	4050	2152396800	6535987200	01:51:44	05:40:44	25	33
10	4500	4500	2391552000	7262208000	02:47:06	05:58:37	17	29
Iš viso:					**09:13:40**	**02:58:42**	**83**	**74**

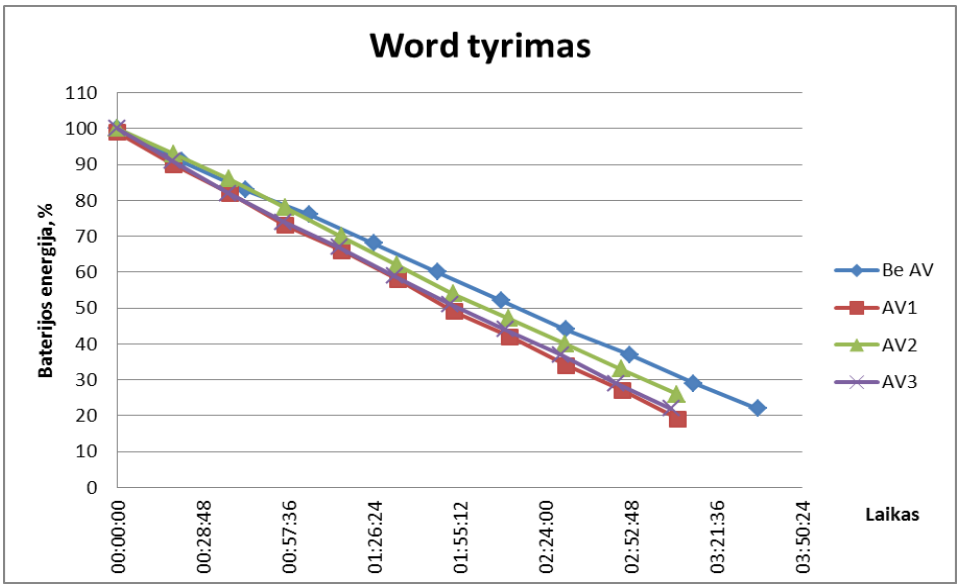
26 lentelė. Eksperimento su įrašymu į failą, atidarymu ir uždarymu rezultatai su trečia antivirusine programine įranga

Matavimo taškai	**Iteracijos**	**Baitų kiekis**	**Laikas**	**Baterijos likutis, %**
	Primes /FileIO			
0	0	0	06:15:51	100
1	100	250000	06:32:29	93
2	200	500000	06:49:03	86
3	300	750000	07:05:38	78
4	400	1000000	07:22:14	70
5	500	1250000	07:38:50	62
6	600	1500000	07:55:25	53
7	700	1750000	08:12:00	44
8	800	2000000	08:28:36	38
9	900	2250000	08:45:12	30
10	1000	2500000	09:01:48	24
Iš viso:			**02:45:57**	**73**

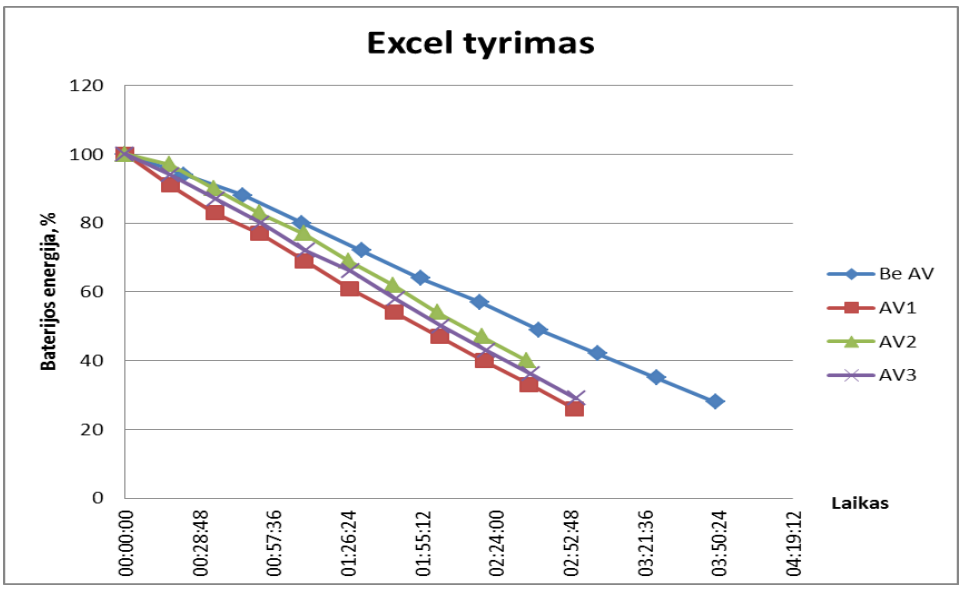
4.2.2. Grafiniai eksperimento rezultatai

Pagal pavaizduotus grafinius rezultatus (21, 22 pav.) matome, kad delninuko baterijai išsikrauti be antivirusinės programinės įrangos prireikė apie 4 valandų, o įdiegus antivirusinę programinę įrangą – apie 3 valandų. Failų kopijavimo veiksmams bei įrašymui į failą delninuko baterijai išsikrauti prireikė maždaug vienodai laiko vykdant tyrimą tiek su antivirusine programine įranga, tiek be jos, tačiau atliekant tyrimus su antivirusine programine įranga buvo nustatytas mažesnis iteracijų skaičius (15-26 lentelės). Šiems veiksmams atlikti pirma antivirusinė programinė įranga sunaudojo 2-8 % daugiau energijos nei antroji ir trečioji per praktiškai tą patį laiką.

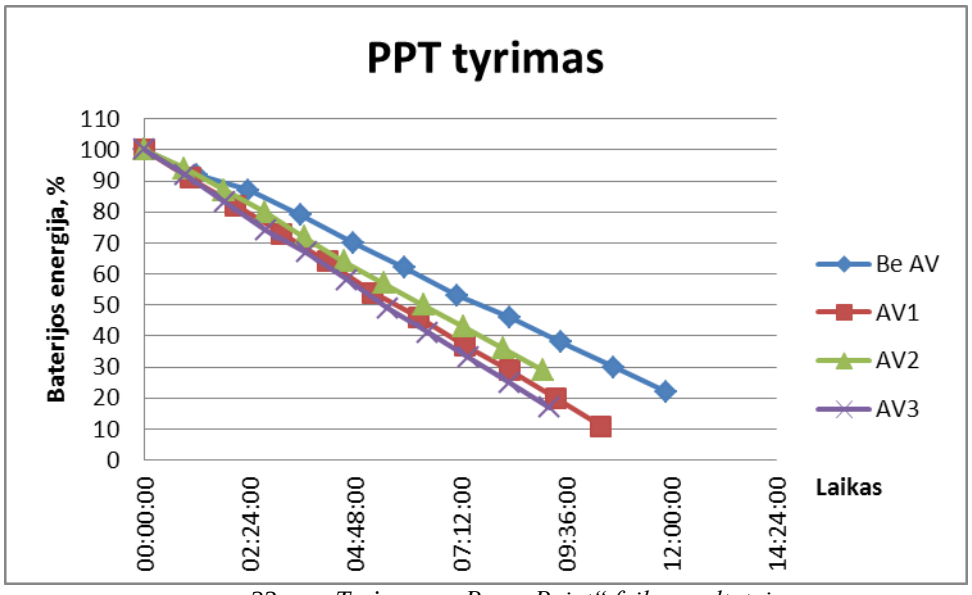
Tyrime su Power Point failo atidarymu, uždarymu po 4500 iteracijų be antivirusinės programinės įrangos buvo sunaudota 58% energijos, pirma antivirusinė programinė įranga po tiek pat iteracijų sunaudojo 80 % delninuko baterijos energijos, antroji – 71 %, trečioji net 83 %. Taigi antivirusinė programinė įranga tiems patiems veiksmams atlikti sunaudojo 13 – 25 % energijos daugiau. Šiuo atveju trečioji antivirusinė programinė įranga esant tam pačiam iteracijų skaičiui bei per praktiškai tą patį laiką (esant 8 min. skirtumui) sunaudojo 3-12 % daugiau energijos nei likusios dvi.



21 pav. Tyrimo su „Word“ failu rezultatai



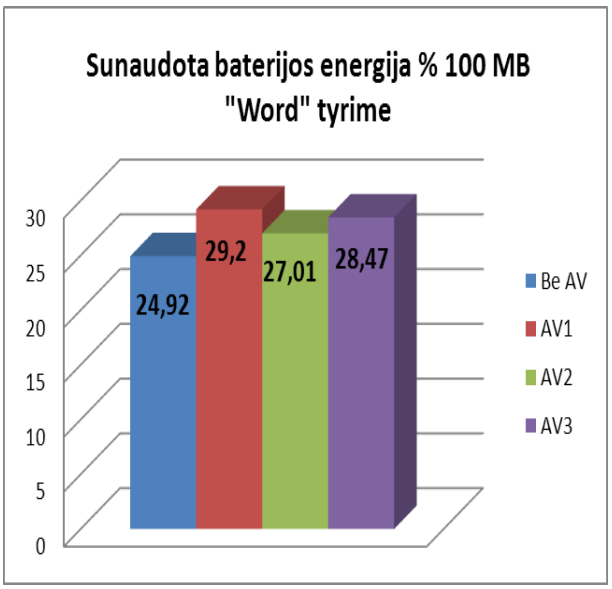
22 pav. Tyrimo su „Excel“ failu rezultatai“



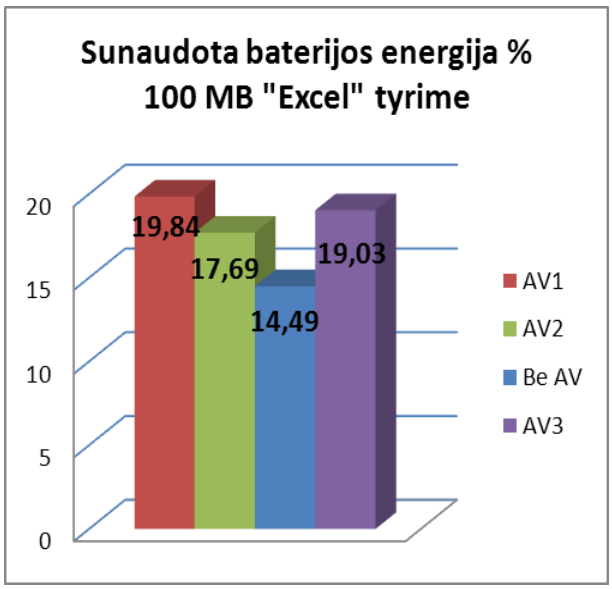
23 pav. Tyrimo su „PowerPoint“ failu rezultatai

Norint pamatyti detalesnius tyrimo rezultatus, buvo paskaičiuotas ir baterijos energijos suvartojimas procentais šimtui megabaitų duomenų (24-28 pav.).

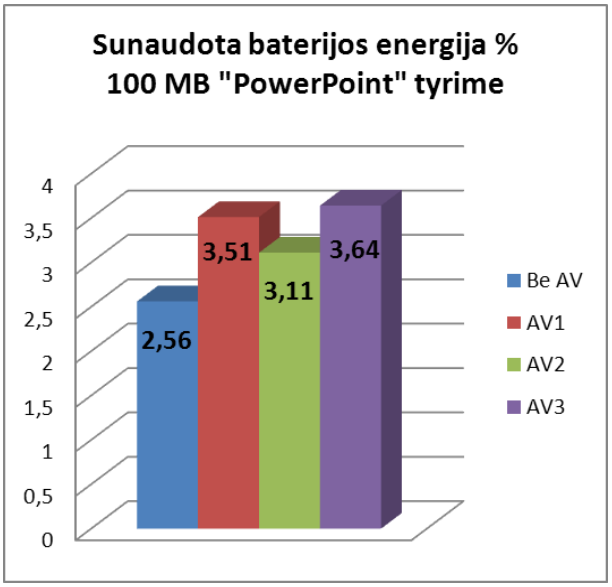
Kadangi suformuoto failo dydis paskutiniajame tyrime buvo labai nedidelis, 30 paveiksle pateiktas baterijos energijos sunaudojimas procentais šimtui kilobaitų duomenų. Tyrimuose nustatytų iteracijų skaičius nėra vienodas, kadangi, atlikus eksperimentą kiekvienam atvejui (su antivirusine programine įranga ir be jos), yra paskaičiuotas reikalingas iteracijų skaičius delninuko išsikrovimui iki nustatytos išsikrovimo ribos (iki ~20%).



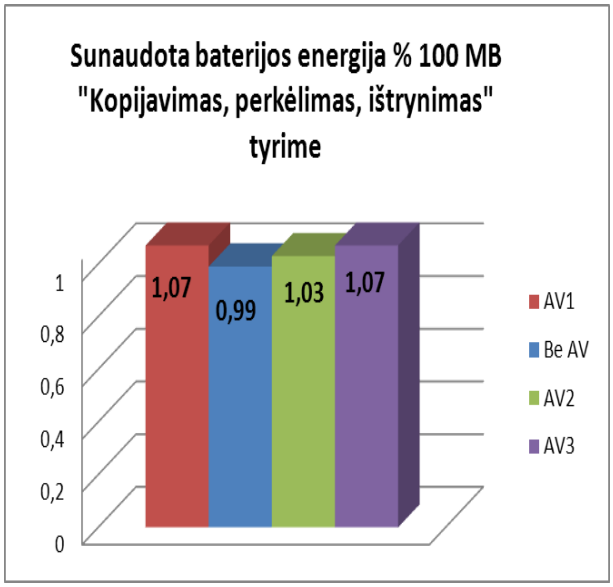
24 pav. Pirmo tyrimo palyginimas



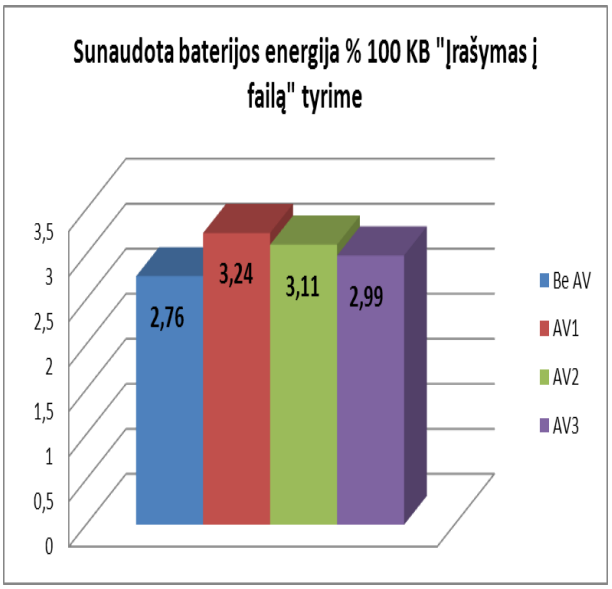
25 pav. Antro tyrimo palyginimas



26 pav. Trečio tyrimo palyginimas



27 pav. Ketvirto tyrimo palyginimas



28 pav.Penkto tyrimo palyginimas

Kaip matome iš pateiktų paveikslų (24-28 pav.) energijos suvartojimo pasiskirstymas tarp skirtingų antivirusinių programų kito: tris kartus dominavo pirmoji antivirusinė programinė įranga, sunaudojus iki 2,21 % daugiau energijos nei likusios dvi (100 MB). Trečiojo tyrimo atveju energijos suvartojime 100 MB duomenų dominavo trečioji antivirusinė programinė įranga, sunaudojus iki 0,13 % daugiau energijos nei kitos dvi programinės įrangos. Taigi labai ryškaus skirtumo energijos suvartojimo atvejais 100 MB duomenų tarp tirtų skirtingų antivirusinių programinių įrangų nėra. Be antivirusinės programinės įrangos 100 MB duomenų yra sunaudojama iki 5,35 % mažiau baterijos energijos, o 100 KB duomenų (įrašymui į failą atlikti) – iki 0, 48%.

4.3. Išvados

- Delninuko baterija, atliekant tuos pačius veiksmus, išsikrauna 1,14 – 1,31 karto greičiau, kai jame yra įdiegta antivirusinė programinė įranga.
- Veikiant delninuke antivirusinei programai per tą patį laiko tarpą yra sunaudojama 6-15% daugiau baterijos energijos nei be antivirusinės programinės įrangos veiksmams su MS Office failais atlikti.
- Skirtingų antivirusinių programinių įrangų sunaudojamos energijos sąnaudos, esant panašiems nustatymams, taip pat skiriasi 3-12 %.
- Imant tą patį iteracijų skaičių (pavyzdžiui, 350) tame pačiame tyrime, pastebima, jog antivirusinė programinė įranga sunaudoja 7-14% daugiau baterijos energijos (atliekant Word failo atidarymą, uždarymą) nei atliekant tą patį tyrimą be jokios antivirusinės. Atliekant Excel failo atidarymą, uždarymą ir praėjus tam pačiam iteracijų skaičiui (pavyzdžiui, 1500) antivirusinė programinė įranga energijos sunaudoja 11-19 % daugiau nei tas pats tyrimas be jos.
- Be antivirusinės programinės įrangos, iki kol išsikrauna delninuko baterija, galima atlikti daugiau veiksmų: pavyzdžiui, 50 kartų daugiau atidaryti ir uždaryti Word failą, 500 kartų daugiau atlikti veiksmus su failais - kopijuoti juos, perkelti iš vieno katalogo į kitą.

5. IŠVADOS

- Analizės dalyje apžvelgti atliekami tyrimai darbo tematika. Išsiaiškinta, kokie tyrimai atliekami su antivirusinėmis programomis, kiek energijos išeikvoja pagrindiniai mobilaus įrenginio komponentai (procesorius, atmintis, ekranas, garso, vaizdo sistema, bevielis ryšys), išnagrinėti metodai, sumažinantys energijos sąnaudas, reikalingas šių komponentų veikimui.

- Projektavimo dalyje aprašyta eksperimente naudojamos programinės įrangos struktūra, tyrimo duomenų struktūra, pateiktas failų atidarymo, uždarymo matavimų algoritmas, panaudojimo atvejų schema. Pateiktos kintamųjų ir metodų diagramos, registruojamų tyrimo parametrų aprašymas.

- Eksperimentinėje dalyje aprašytas energijos suvartojimo, panaudojant skirtingas antivirusines programines įrangas, tyrimas, jo metodika, pateikti skaitiniai ir grafiniai tyrimo rezultatai.

- Nustatyta, kad veikiant delninuke antivirusinei programai per tą patį laiko tarpą (pavyzdžiui, per dvi valandas) failų atidarymui – uždarymui sunaudojama 6-15% daugiau baterijos energijos nei be antivirusinės programinės įrangos. Be antivirusinės programinės įrangos šimtui megabaitų duomenų eksperimento veiksmams atlikti yra sunaudojama iki 5,35 % mažiau baterijos energijos.

- Delninuko baterija, atliekant analogiškus veiksmus, išsikrauna 1,14 – 1,31 karto greičiau, kai jame yra įdiegta antivirusinė programinė įranga.

- Skirtingų antivirusinių programinių įrangų sunaudojamos energijos sąnaudos, esant panašiems nustatymams ir atliekant tuos pačius eksperimento tyrimus, taip pat skiriasi 3-12 %.

- Įvertindamas saugumo poreikį savo mobiliam įrenginiui, pageidaujamą įrenginio gyvavimo laiką, naudojimosi įrenginio funkcijų darbui su MS Office failais dažnumą, naudotojas gali spręsti, ar verta jam įsidiegti atitinkamą antivirusinę programinę įrangą.

6. LITERATŪRA

1. **Valančius J., Štuikys V.** Delninuko energijos suvartojimo įvertinimas taikomosios programos lygmenyje, 2007, KTU Informatikos fakultetas.

2. **Brakmo L.S., Wallach D.L., Viredaz M. A.** µSleep: A technique for reducing energy consumption in handheld devices. HP Laboratories, 2004.

3. **Ho Li Y., Heng S.H.** Mobile and ubiquitous malware. Malaysia Multimedia University, 2009.

4. **Yan W., Ansari N.**. Why Anti-Virus products slow down your machine? USA, 2009.

5. **Kim H., Smith J., Shin K. G.** Detecting Energy-Greedy Anomalies and Mobile Malware Variants. The University of Michigan, USA, 2008, p.239-252.

6. Kompanijos „**Anti-Virus Comparatives“ oficialus puslapis.** „Impact of Anti-Virus Software on system performance“, 2009-12-21. [Žiūrėta 2010-01-21]. Prieiga per internetą: <http://www.av-comparatives.org>.

7. Kompanijos **„ESET“ oficialus puslapis.** „ESET mobile security“. [Žiūrėta 2011-03-20]. Prieiga per internetą: <http://www.eset.com>.

8. Kompanijos **„F-Secure“ oficialus puslapis.** „Mobile Security“, [Žiūrėta 2011-01-16]. Prieiga per internetą: <http://www.f-secure.com>.

9. Kompanijos **„Kaspersky Lab“ oficialus puslapis**. „Kaspersky Mobile Security“, [Žiūrėta 2010-12-29]. Prieiga per internetą: <http://www.kaspersky.com>.

10. Kompanijos **„Kaspersky“ puslapis**. Mobile Malware Evolution: An Overview, Part 1; Mobile Malware Evolution: An Overview, Part 4 [Žiūrėta 2011-03-26]. Prieiga per internetą: <http://www.securelist.com/en/analysis>.

11. Kompanijos „**PassMark Software“ oficialus puslapis.** „Consumer Antivirus Performance Benchmarks“, 2010-09-30. [Žiūrėta 2010-12-21]. Prieiga per internetą: <http://www.passmark.com>.

12. **Lee J.S., Kim T.H., Kim J.** Energy-efficient Run-time Detection of Malware-infected Executables and Dynamic Libraries on Mobile Devices. Pohang University of Science and Technology, Korea, 2009.

13. **Morales J. A., Clarke P.J., Deng Yi, Kibria R.M.G.** Testing and evaluating virus detectors for handheld devices. Florida International University, 2006.

14. **Schmidt A.-D., Peters F., Lamour F., Scheel C., Campete S. A., Albarayak S.** Monitoring smartphones for anomaly detection, 2008, p.92-106.

15. **Toldinas J., Štuikys V., Ziberkas G., Naunikas D.** Power Awareness Experiment for Crypto Service-Based Algorithms, Kaunas University of Technology, 2010.

16. **Uluski D., Moffie M., Kaeli D.**. Characterizing Antivirus Workload Execution. Computer Architecture Research Laboratory, Northeastern University Boston, MA, 2005, p. 90-98.

17. **Viredaz M. A., Brakmo L.S, Hamburgen W. R.** Energy management on handheld devices. 2003, p.44-52.

18. **Wagener G., State R., Dulaunoy A.** Malware behaviour analysis. 2007.

19. **Zhong L., Jha N.K**. Energy efficiency of handheld computer interfaces: limits, characterization and practice. Departament of Electrical Engineering, Princeton University, 2005, p. 247-260.

7. SUMMARY

Mobile devices are spreading as fast as their capabilities are growing and their usability is expanding. Hand-held mobile devices such as handheld computers or smart phones are starting to change portable computers, as well as notebooks are replacing desktop PCs. However, because of the limited battery's lifetime usefulness of these devices reduces. Power management is becoming one of the biggest challenge for the portable computing device. This weakness of the mobile facility is yet to be prejudiced with malicious programs for a mobile device, which also reduces battery's energy. Therefore it is important to ensure the security of a mobile device and to keep it working as long as possible.

The main defense against the malicious software tool is an anti-virus software. Anti-virus software manufacturers perform many tests, such as found false alarms, scanning speed and other. A number of investigations, showing how much energy expended major components of a mobile device (processor, memory, screen, sound, video system, wireless connectivity) are found and different kind of methods are created to reduce the consumed energy of these components, but there is no data about how many percent of mobile device energy anti-virus program consumes. So, before installing antivirus software on the mobile device, it would be useful for a user to know how much battery's energy this software uses.

The aim of this work is to investigate the influence of different anti-virus programs on a Pocket PCs energy. For this purpose we perform different actions with Microsoft Office files: open them and close; copy, move, delete them in different catalogues; write into a file. The analysis is made depending on the user's chosen parameters in the level of application program.

8. PRIEDAI

8.1. Populiarios piktavališkos programinės įrangos, plintančios mobiliuosiuose įrenginiuose ir kitur, pavyzdžiai

27 lentelė. Mobilių piktavališkų programų pavyzdžiai ir savybės

Mobili piktavališka programa	**Savybės**
Cabir	Dauginasi per Symbian OS įdiegimo failą (.SIS failą) ir platinamas per Bluetooth sąsają, ieško kitų prietaisų, kuriuose įjungtas Bluetooth, mažina baterijos gyvavimo laiką bei Bluetooth veikimo galimybes.
Lasco	Panašus į Cabir, bet gali sukurti savo .SIS įdiegimo failą ir užkrėsti visus .SIS failus mobiliuosiuose įrenginiuose su Symbian OS, keičia įrenginio failų katalogus.
Skulls	Symbian OS priklausantis Trojos arklys, kuris pakeičia originalius Symbian dvejetainius kodus, naudojamus bendrose taikomosiose programose su nefunkciniais dvejetainiais failais, uždraudžia visas taikomąsias programas ir tik leidžia prietaisui priimti bei atlikti telefono skambučius.
Mquito	Siunčia neleistinas SMS žinutes į telefono numerius Didžiojoje Britanijoje, Vokietijoje, Šveicarijoje, Olandijoje.
Duts	Užkrečia visus vykdomus, didesnius nei 4kB failus, prisisega prie failo ir neleidžia nieko daryti su failu, kai jis bandomas vykdyti.
Metal Gear	Trojos arklys, plintantis per Bluetooth sąsają, išjungia antivirusinę programą telefone ir įdiegia Cabir.G.kirminą.
Gavno	Trojos arklys, pašalinantis svarbius duomenis Symbian operacinėje sistemoje, iššaukia sistemos klaidas Nokia 6600 ir Nokia 6630 telefonuose ir perkrauna įrenginį.
Commwarrior	Panašus i Lasco, bet taip pat gali plisti per MMS, siunčia MMS žinutes su užkrėstu .SIS failu visiems telefone esantiems adresatams.
Mabir	Panašus į Cabir, bet taip pat plinta per MMS, skaito telefonų adresų knygą, peržiūri gautas žinutes ir siunčia suklastotus atsakymus kartu su viruso kopija.
Phage	Perrašo Palm operacinės sistemos vykdomųjų failų pradžią ir sunaikina visas įdiegtas programas, plinta per infraraudonųjų spindulių jungtį ar kai sinchronizuojasi įrenginys su PalmOS per kompiuterį.
RedBrowser	Java aplinka pagrįstas Trojos arklys, siunčia SMS žinutes telefono numeriams.
Flexispy	Symbian OS pagrįstas Trojos arklys, siunčia visą mobilaus įrenginio naudojimo informaciją į serverį, FlexiSpy.
CardTrap	Daugiaplatformis virusas, išjungiantis mobiliąją sistemą ir visas „trečios šalies“ programas mobiliajame įrenginyje, užkrečia atminties kortelę Windows pagrįsta asmeninio kompiuterio piktavališka programa.
Doomboot	Trojos arklys, įdiegiantis Commwarrior.B kirminą ir kai kuriuos sugadintus sistemos dvejetainius kodus, kas sukelia prietaiso gedimą per kitą paleidimą, taip pat plinta per Bluetooth ryšį.
Crossover	Visur esantis daugiaplatformis virusas (plintantis mobiliuosiuose įrenginiuose bei asmeniniuose kompiuteriuose), atakuojantis .NET ar .NET CF Windows operacinėje sistemoje.
Mobler	Visur esantis Trojos arklys, plintantis per prieinamą rašyti terpę, išjungia žinomas Windows funkcijas asmeniniame kompiuteryje ir pradedantis DoS atakas.

8.2. Kompanijos „Passmark“ elektroninis atsakymas į užklausą

Data: Tue, 21 Dec 2010 12:13:06 +1100 [2010-12-21 03:13:06 EEST]
Nuo: PassMark Support <help@passmark.com>
Kam: deimante.boreisaite@stud.ktu.lt
Tema: Re: Sample of files

Hi Deimante

Thanks for your e-mail.

The report you have linked in your e-mail is actuall an older report from 2009; the latest report from 2010 can be found at: http://www.passmark.com/ftp/antivirus_11-performance-testing-ed2.pdf

To answer your request, unfortunately, we're not able to make our sample files available to the public at this time.
I can advise that there's nothing special or unique about the Word/Excel/Powerpoint sample files that we've used, they are a random, standard selection of files which could be typically found on user machines.
If you'd like to create sample sets similar to those we have used, we've included a detailed breakdown of file sets used for each metric in the Methodology section on page 30 of the report linked above.

Otherwise, if you have any specific questions about our methodology, please let me know.
Thanks, Deimante!

Karen Lai
PassMark Software
Suite 202, Level 2
35 Buckingham Street
Surry Hills 2010 Australia
P : +61 2 9690 0444
F : +61 2 9690 0445
W: www.passmark.com

On Mon, 20 Dec 2010, deimante.boreisaite@stud.ktu.lt wrote:

[Hide Quoted Text]
Hello,

I am a student from Kaunas University of Technology. We are doing some researches with antivirus programs. I am wondering is it possible to get from somewhere some sample of files (only word, excel and power point are needed, used in your researches http://www.passmark.com/ftp/antivirus_10-performance-testing-ed3.pdf), cause we want to make some testing according to your benchmarks there, and I would like to use similar files. Of course, if it is possible.

Thank you.

Deimante Boreisaite
KTU

8.3. Kompanijos „Passmark“ antivirusinių programinių įrangų tyrimų etalonai

Performance Metrics Summary

We have selected a set of objective metrics which provide a comprehensive and realistic indication of the areas in which an antivirus may impact system performance for end users. Our metrics test the impact of the antivirus software on common tasks that end-users would perform on a daily basis.

All of PassMark Software's test methods can be replicated by third parties using the same environment to obtain similar benchmark results. Detailed descriptions of the methodologies used in our tests are available as "***Appendix 2 – Methodology Description***" of this report.

Benchmark 1 – Boot Time

This metric measures the amount of time taken for the machine to boot into the operating system. Security software is generally launched at Windows startup, adding an additional amount of time and delaying the startup of the operating system. Shorter boot times indicate that the application has had less impact on the normal operation of the machine.

Benchmark 2 – Scan Time

All antivirus solutions have functionality designed to detect viruses and various other forms of malware by scanning files on the system. This metric measured the amount of time required to scan a set of clean files. Our sample file set comprised a total file size of 1.2 GB and was made up of files that would typically be found on end-user machines, such as media files, system files and Microsoft Office documents.

Benchmark 3 – User Interface Launch Time

This metric provides an objective indication as to how responsive a security product appears to the user, by measuring the amount of time it takes for the user interface of the antivirus software to launch from Windows. To allow for caching effects by the operating system, both the initial launch time and the subsequent launch times were measured. Our final result is an average of these two measurements.

Benchmark 4 – Browse Time

It is common behavior for security products to scan data for malware as it is downloaded from the internet or intranet. This behavior may negatively impact browsing speed as products scan web content for malware. This metric measures the time taken to browse a set of popular internet sites to consecutively load from a local server in a user's browser window.

Benchmark 5 – Memory Usage during System Idle

This metric measures the amount of memory (RAM) used by the product while the machine and antivirus software are in an idle state. The total memory usage was calculated by identifying all antivirus software processes and the amount of memory used by each process.

The amount of memory used while the machine is idle provides a good indication of the amount of system resources being consumed by the antivirus software on a permanent basis. Better performing products occupy less memory while the machine is idle.

Benchmark 6 – Internet Explorer Launch Time

This metric is one of many methods to objectively measure how much a security product impacts on the responsiveness of the system. This metric measures the amount of time it takes to launch the user interface of Internet Explorer 8. To allow for caching effects by the operating system, both the initial launch time and the subsequent launch times were measured. Our final result is an average of these two measurements.

Benchmark 7 – Installation Time

The speed and ease of the installation process will strongly influence the user's first impression of the antivirus software. This test measures the minimum installation time required by the antivirus software to be fully functional and ready for use by the end user. Lower installation times represent antivirus products which are quicker for a user to install.

Benchmark 8 – Installation Size

In offering new features and functionality to users, antivirus software products tend to increase in size with each new release. Although new technologies push the size limits of hard drives each year, the growing disk space requirements of common applications and the increasing popularity of large media files (such as movies, photos and music) ensure that a product's installation size will remain of interest to home users.

This metric aims to measure a product's total installation size. This metric is defined as the total disk space consumed by all new files added during a product's installation.

Benchmark 9 – Registry Keys Added

A large registry increases a machine's use of resources. This may negatively impact system performance, especially on much older machines. This test measures the amount of keys and values added to registry, after

rebooting the test machines, following a successful product installation. Lower numbers mean that a product has added fewer keys during installation and had less impact on the registry.

Benchmark 10 – File Copy, Move and Delete

This metric measures the amount of time taken to move, copy and delete a sample set of files. The sample file set contains several types of file formats that a Windows user would encounter in daily use. These formats include documents (e.g. Microsoft Office documents, Adobe PDF, Zip files, etc), media formats (e.g. images, movies and music) and system files (e.g. executables, libraries, etc).

Benchmark 11 – Installing Third Party Applications

This metric measures the amount of time taken to install and uninstall third party programs. The installation speed of third party applications may be impacted by antivirus behavior such as heuristics or real time malware scanning.

Benchmark 12 – Network Throughput

The metric measures the amount of time taken to download a variety of files from a local server using the HyperText Transfer Protocol (HTTP), which is the main protocol used on the web for browsing, linking and data transfer. Files used in this test include file formats that users would typically download from the web, such as images, archives, music files and movie files.

Benchmark 13 – File Format Conversion

This test measures the amount of time taken to convert an MP3 file to a WAV and subsequently, convert the same MP3 file to a WMA format.

Benchmark 14 – File Compression and Decompression

This metric measures the amount of time taken to compress and decompress different types of files. Files formats used in this test included documents, movies and images.

Benchmark 15 – File Write, Open and Close

This benchmark was derived from Oli Warner's File I/O test at http://www.thepcspy.com (please see ***Reference #1: What Really Slows Windows Down***). This metric measures the amount of time taken to write a file, then open and close that file.

Benchmark 16 – Scan Time of a Solid State Drive (SSD)

This metric measured the amount of time required to scan a set of clean files that are stored on a Solid State Drive (SSD). Our sample file set comprised of 18,000 files and was made up of files that would typically be found on end-user machines, such as media files, system files and Microsoft Office documents.

8.4. Mobilių įrenginių antivirusinių programų savybių sąrašas ir palyginimas

28 lentelė. „ESET“, „F-Secure“ ir „Kaspersky“ programinių įrangų palyginimas pagal funkcijas

Windows Mobile OS			
Produkto pavadinimas	**“ESET” mobilioji apsauga**	**“F-Secure” mobilioji apsauga**	**“Kaspersky “mobilioji apsauga**
Palaikomos OS versijos	Windows Mobile 5.0-6.5	Windows Mobile 5.0-6.5	Windows Mobile 5.0-6.5
Palaikomos programos kalbos	Anglų kalba	Anglų, arabų, supaprastinta kinų, tradicinė kinų, danų, ispanų, suomių, prancūzų, vokiečių, italų, japonų, norvegų, lenkų, portugalų, švedų, tailandiečių, turkų, korėjiečių.	Anglų, rusų, vokiečių, prancūzų, italų, lenkų, ispanų, portugalų, danų, norvegų, suomių, švedų, supaprastinta kinų, tradicinė kinų, arbaų, turkų, čekų, olandų.
Užrakinimo funkcijos			
Užrakinti kontaktus	-	Taip	Taip
Užrakinti paveikslus/failus	-	Taip	Taip
Užrakinti SMS/MMS	-	Taip	Taip
Užrakinti SIM	-	Taip	Taip
Brukalų naikinimo funkcijos			
Baltieji/Juodieji sąrašai skambučiams	-	-	Taip
Baltieji/Juodieji sąrašai SMS	Taip	-	Taip
Baltieji/Juodieji sąrašai MMS	Taip	-	-
Žinomų SMS/MMS brukalų blokavimas	Taip	-	-
Galimybė vienu mygtuko paspaudimu pažymėti kaip brukalą	-	-	Taip
Įtraukimas į Baltuosiuos ir Juoduosius sąrašus naudojant pakaitos simbolį	-	-	Taip
Blokavimo priedai/taikomosios programos/failų plėtiniai	Taip	-	-
Kontrolė			
Mokėjimo numerio užraktas	-	-	Taip
SMS paieška (išmaniojo telefono vietos radimas)	-	Taip	Taip
Įrašai po apsilankymų URL	-	-	-
Ugniasienės funkcijos			
Realaus laiko apsauga gaunamam /išeinančiam srautui	Taip	Taip	Taip
App įtraukimas į Juoduosius ir Baltuosius sąrašus	Taip	-	-
Mokymosi funkcijos	Taip	-	-
Skirtingas apsaugos lygis	Taip	Taip	Taip
Skirtingi taisyklių rinkiniai	Taip	Taip	Taip
WiFi/Bluetooth ryšių apsauga	Taip	Taip	-
Veiklos įrašai	Taip	Taip	Taip
Apsaugos įrašai	Taip	Taip	Taip
Pritaikomos ugniasienės taisyklės	Taip	Taip	Taip
Įsimenamoji paketų apžiūra (sąlyginės taisyklės)	Taip	Taip	Taip
Nuotolinės savybės			
Nuotolinis pavogto išmaniojo telefono valdymo įrenginys	Taip	Taip	Taip
Nuotolinis susisiekimas su Exchange Server 2007/2010/Outlook Web Access/Active Sync	Taip	Per valdymo portalą ir įrenginio valdymą	-
Nuotolinis GPS	-	Taip	Taip
SIM kortelės priežiūra (SIM kortelės pakeitimas)	Taip	Taip	Taip
Nuotolinis diegimas	-	Per įrenginio valdymą arba per F-Secure mobilių paslaugų portalą	Įmonės versija
Nuotolinis konfigūravimas		Per įrenginio valdymą	Įmonės versija
Nuotoliniai atnaujinimai	Taip	Taip	-
Nuotolinis užšifravimas	-	-	-

Užšifravimo funkcijos			
Failų sistemos užšifravimas	-	Per partnerių sprendimus	**Taip**
Užšifravimas slaptažodžiu	-	Per partnerių sprendimus	Taip
Užšifravimas pagal duomenų rūšis (Outlook, Word, Excel, PDF ir kt.) ir pagal duomenų buvimo vietą (įrenginyje, prieduose, atminties kortelėse irk t.)	-	Per partnerių sprendimus	Tik pagal duomenų buvimo vietą
Iššifravimo galimybė administratoriaus teisėmis be slaptažodžio	-	Per partnerių sprendimus	-
Tapatybės nustatymas			
Saugumo politika kontroliuojama autentifikacija	-	-	-
Prieigos ir užšifravimo kontrolė	-	-	Taip
Jungčių kontrolė: USB, atminties kortelės, Bluetooth, WiFi ryšys	-	Taip	-
Išteklių prieinamumo kontrolė: IR, kamera, balso įrašymas	-	-	-
Slaptažodžio politika: stiprumas, ilgis ir kt.	-	Taip	Taip
Maksimalus nepavykusių bandymų kiekis	-	Taip	-
Lengvatinis laikotarpis	-	Taip	Taip
Ekrano užrakinimas su slaptažodžio apsauga	-	Taip	Taip
AV funkcijos			
Failų apsauga	Taip	Taip	Taip
Tinklo apsauga	Taip	Taip	-
SMS/MMS peržiūrėjimas	Taip	Taip	Taip
Elektroninio pašto peržiūrėjimas	Taip	Taip	Taip
Įvairūs atnaujinimų profiliai	Taip	Taip	Įmonės versija
Savo tarptinklinio ryšio profilio atnaujinimas	Taip	Taip	Taip
Archyvų peržiūra	Taip	Taip	Taip
Uždrausta prieiga prie pavojingų svetainių	-	Taip	-
Apsaugos nuo vagysčių savybės			
Pakeitus SIM kortelę pranešama apie vagies vietą	-	Taip	-
Vagies telefono numerio pranešimas SMSu	Taip	Taip	Taip
Galimybė gauti skambučius ir po užrakinimo	-	Taip	-
Galimybė paskambinti į greitą pagalbą ir po užrakinimo	-	Taip	-
Priežiūra			
El. pašto priežiūra	Taip	Taip	Taip
Pagalba internetu	Taip	Taip	Taip
Pagalba internetu (specialus URL, sukurtas telefono naršymui)	-	Taip	Taip
Naudotojo vadovas	Taip	Taip	Taip
Naudotojo forumas	-	-	Taip
Interneto pokalbiai	-	-	-
Parama telefonu	Taip	Taip	Taip
Palaikomos kalbos	Visos	Visos	Visos
Kita			
Tiesioginis įdiegimas į įrenginį per atsisiuntimo nuorodą	Taip	Taip	Taip
AK tvarkymo programinė įranga	-	-	-
Centrinio valdymo programinė įranga	-	Per F-Secure paslaugų portalus prieinama tik administratoriams	Įmonės versija
Sinchronizacija	Taip	-	-
AK taikomųjų programų įdiegimas	Taip	Įmanoma per Active Sync	Taip
Atnaujinimai per AK	Taip	Įmanoma per Active Sync	Įmanoma per Active Sync
Nepasiekiamumo aktyvacija	-	-	-
Jokios SIM aktyvacijos	Taip	Taip	Taip
Atnaujinimai (pagal pareikalavimą)	Taip	Taip	Taip
Karantinas	Taip	Taip	Taip
Klajojančių duomenų blokavimas	Taip-	-	Taip
SIM atitikimas	Taip	-	-
Statistika	Taip	Taip	Įmonės versija