KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Audrius Povilauskas

Energijos sąnaudos informacijos saugai mobiliuose įrenginiuose

Baigiamasis magistro darbas

Vadovas
Doc. dr. Jevgenijus Toldinas

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Energijos sąnaudos informacijos saugai mobiliuose įrenginiuose

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

Vadovas
Doc. dr. Jevgenijus Toldinas

Recenzentas
Doc. dr. Giedrius Ziberkas

Projektą atliko
Audrius Povilauskas

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos

(Fakultetas)

Audrius Povilauskas

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga, 621E10003

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Energijos sąnaudos informacijos saugai mobiliuose įrenginiuose“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 15 m. gegužės 19 d.

Kaunas

Patvirtinu, kad mano **Audriaus Povilausko** baigiamasis projektas tema „Energijos sąnaudos informacijos saugai mobiliuose įrenginiuose“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

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

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

Povilauskas, A. „Energijos sąnaudos informacijos saugai mobiliuose įrenginiuose“. Magistro baigiamasis projektas / vadovas doc. dr. Jevgenijus Toldinas; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra.

Mokslo kryptis ir sritis: Informatikos inžinerija.

Reikšminiai žodžiai: duomenų saugumas, AES, DoD, WPA2, mobilūs įrenginiai.

Kaunas, 2016. 46 psl.

SANTRAUKA

Įmonėse populiarėjant BYOD politikai bei darbuotojams vis dažniau naudojantis savo mobilius įrenginius darbo reikmėms, išauga rimta problema duomenų saugumui. Siekiant apsaugoti duomenis, dažniausiai naudojamas sprendimas – pilnas įrenginio disko šifravimas. Tačiau taikant šį metodą sulėtėja darbas su duomenimis bei atsiranda papildomos energijos sąnaudos, dėl ko greičiau iškraunama ir taip ribotos talpos baterijos energija.

Šiame darbe siūloma metodika, kuri skirta saugiam darbui su pavieniai dokumentais, kas leidžia sumažti energijos sąnaudas apdorojant tik svarbius duomenis. Metodiką sudaro trys saugumo metodai: duomenų šifravimas (AES), saugus duomenų trynimas (trijų ciklų DoD algoritmas) bei duomenų talpinimas nuotolinėje talpykloje, persiunčiant duomenis bevieliu ryšiu, naudojant saugos protokolą (WPA2). Metodika reikalauja atlikti saugumo metodų testavimą, kuris padeda apskaičiuoti numatomas energijos sąnaudas, apdorojant tam tikrą duomenų kiekį. Tai vartotojui leidžia planuoti energijos sąnaudas bei būti užtikrintu, jog įrenginys neišsikraus nebaigus apdoroti duomenis, paliekant juos neapsaugotus iškrautame įrenginyje.

Šio darbo pagrindiniai tikslai yra:

- Išanalizuoti pasirinktus saugumo metodus bei panašius darbus, kuriuose būtų nagrinėjami pasirinkti saugumo metodai.
- Pasiūlyti metodiką, kuri padėtų išspręsti duomenų saugumo problemą mobiliuose įrenginiuose leidžiant sumažinant ir valdyti energijos sąnaudas.
- Atlikti pasirinktų saugumo metodų energijos sąnaudų tyrimą, išanalizuoti rezultatus bei įvertinti jų įtaką siūlomam sprendimui.

Povilauskas, Audrius. Energy consumption securing information in mobile devices: Master‘s thesis/ supervisor assoc. prof. Jevgenijus Toldinas. The Faculty of Informatics, Kaunas University of Technology.

Research area and field: Informatics Engineering.

Key words: data security, AES, DoD, WPA2, mobile devices.

Kaunas, 2016. 45 p.

SUMMARY

As BYOD policy becomes more and more popular between companies, employees use their private mobile devices for work purposes, causing serious problems for data security. The most common solution to protect data is full disk encryption. Using this method, working with data becomes slower and additional energy consumptions speed up battery discharging.

In this paper I propose methodology, which allow to safely work with separate documents, to reduce energy costs working only with sensitive data. The methodology consists of three security methods: data encryption (AES), secure deletion (three cycles DoD algorithm) and remote data storage, transmitting data using wireless connection and security protocol (WPA2). Using this methodology, user must periodically perform security methods testing, in order to get more accurate estimated energy costs. It will allow for user to plan his mobile device energy consumptions and be sure that it will not turn off while proceeding the data, leaving it unprotected.

The main aims for this paper is:

- To analyze the selected security methods and similar works, where are investigated selected security methods.
- Propose a methodology that would help to solve the problem of data security on mobile devices allowing to reduce and manage of energy consumption.
- To perform selected security methods tests of energy consumptions and analyze the results to assess their impact on the proposed methodology.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

BYOD (Bring Your Own Device) – atsinešk savo įrenginį politika.
IV – inicializavimo vektorius.
DES (Data Encryption Standard) – duomenų kodavimo standartas
AES (Advanced encryption standard) – simetrinis šifravimo algoritmas.
ECB (Electronic Codebook) – elektroninės šifrų knygos režimas.
CBC (Cipher Block Chaining) – šifro bloko grandininis režimas.
CFB (Cipher Feedback) – grįžtamojo ryšio šifro režimas.
OFB (Output Feedback) – grįžtamojo ryšio išvesties.
PDE (Plausible deniable encryption)
FDE (Full Disk Encryption) – pilnas disko užšifravimas
USB (Removable media encryption) – universalioji jungtis
CD (Compact Disc) – optinis diskas informacijai skaitmenine forma įrašyti, saugoti ir platinti
DVD (Digital video disc) – optinis diskas informacijai skaitmenine forma įrašyti, saugoti ir platinti
HDD (Hard disk drive) – duomenų saugojimo įrenginys, kurio pagrindinės dalys yra besisukančios magnetinės plokštelės ir nuskaitymo galvutės.
SSD (solid-state storage) – duomenų saugojimo įrenginys, kuriame duomenys saugojami „Flash“ atminties tipo kortelėse.

ĮVADAS

Pastaruoju metu vis didėja mobilių įrenginių populiarumas. Dažnas vartotojas renkasi silpnesnių resursų, tačiau mobilius, lengvai transportuojamus įrenginius. Mobilieji įrenginiai turi ribotą naudojimosi laiką dėl ribotos baterijos talpos, todėl didelis dėmesys skiriamas baterijos energiją taupantiems metodams.

Įmonėms vis dažniau pritaikant BYOD politiką, išauga rimta problema duomenų saugumui. Atsiranda didelė gresmė saugumui jautiems duomenims. Darbuotojai informaciją, skirtą darbui, saugo tame pačiame įrenginyje, kaip ir savo asmeninius dokumentus. Puikus būdas apsaugoti duomenis – jų šifravimas. Tačiau pilno disko šifravimas reikalauja didelių skaičiavimo resursų, sulėtina darbą su duomenimis ir ženkliai padidina baterijos energijos sąnaudas. Tik jautrių duomenų šifravimas pagerina situaciją. Kitas būdas apsaugoti duomenis – jų talpinimas, ne darbo metu, nuotolinėje duomenų saugykloje. Norint visiškai apsaugoti jautrius duomenis reikia pasirūpinti ir saugiu duomenų trynimu, kad praradus įrenginį nebūtų galima atkurti ištrintų duomenų iš disko. Įgvendinant šiuos išvardintus metodus, vartotojas gali pasirūpinti tik jam aktualių dokumentų saugumu, taip sumažinant energijos sąnaudas.

Magistrinio darbo tyrimo sritis yra mobilieji įrenginiai. Nagrinėjama situacija - nešiojamų kompiuterių, skirtų kasdieniniam darbui, privalomų duomenų šifravimas. Šio tiriamojo darbo paskirtis ištirti šifravimo algoritmus, duomenų siuntimo saugos protokolus, bei saugaus trynimo algoritmus nešiojamuose kompiuteriuose, bei jų energijos sąnaudas. Taip pat pasiūlyti metodą, kuris suteikia vartotojui galimybę apsaugoti saugumui jautrius duomenis bei pateikia pasirinktų saugos metodų energijos sąnaudas.

Darbo problematika ir aktualumas

Darbo sprendžiama problema – duomenų saugumas mobiliuose įrenginiuose, jų ribotos baterijos energijos taupymas, taikant saugumo metodus, kurie suteikia galimybę dirbti su pavieniais dokumentais.

Darbo tikslas ir uždaviniai

Magistro darbo tikslas yra ištirti kokioje aplinkoje yra svarbus duomenų saugumas mobiliuose įrenginiuose. Pasiūlyti sprendimą, suteikiantį saugų darbą su saugumui jautriais duomenimis, kuris nereikalautų didelių energijos sąnaudų ir leistų vartotojui planuoti energijos sąnaudas naudojant saugumą padedančius užtikrinti metodus (pavienis duomenų šifravimas, saugus duomenų trynimas, duomenų talpinimas serveryje). Taip pat ištestuoti pasiūlytus metodus, juos palyginti, padaryti išvadas. Išsikelti tikslai:

- Išanalizuoti pasirinktų saugumo metodus.
- Išanalizuoti panašius darbus, kuriuose būtų nagrinėjami pasirinkti saugumo metodai.
- Pateikti organizacijos pavyzdį, kurioje būtų aktuali sprendžiama problema;
- Pasiūlyti bei suprojektuoti sprendimą, kuris padėtų išspręsti sprendžiamą problemą.
- Atlikti pasirinktų saugumo metodų tyrimą, išanalizuoti rezultatus bei įvertinti jų įtaką siūlomam sprendimui.
- Pateikti tyrimo išvadas.

Darbo rezultatai ir jų svarba

Atlikus šį tyrimą mobilių įrenginių vartotojams pateikta metodika leidžianti saugiai apdoroti pavienius dokumentus ir planuoti energijos sąnaudas. Atlikus pasirinktų saugumo metodų tyrimą bus galima išanalizuoti energijos sąnaudų apskaičiavimą pasiūlytoje metodikoje.

Darbo struktūra

Darbą sudaro nagrinėjamos srities analizė, kurioje apžvelgiama mobilių įrenginių technologinis progresas, bei jų panaudojimo tendencija įmonėse. Taip pat apžvelgiami pasirinkti saugumo metodai, trumpai apibūdinami populiariausi šifravimo ir trynimo algoritmai, bei belaidžio tinklo saugumo protokolai. Išnagrinėti panašūs darbai: Dariaus Nauniko atliktas darbas „Energijos

suvartojimo naudojant kriptografinius servisus delniniuose kompiuteriuose tyrimas“ ir Ingos Gudaitytės darbas pavadinimu „Delninukų belaidžio ryšio saugos protokolų tyrimas“. Juose apžvelgiami šifravimo algoritmų bei saugos protokolų energijos sąnaudos.

Antrame darbo skyriuje pateikiama siūloma saugaus darbo su pavieniais duomenimis metodika, kuri užtikrina minimalias energijos sąnaudos, bei jų planavimą.

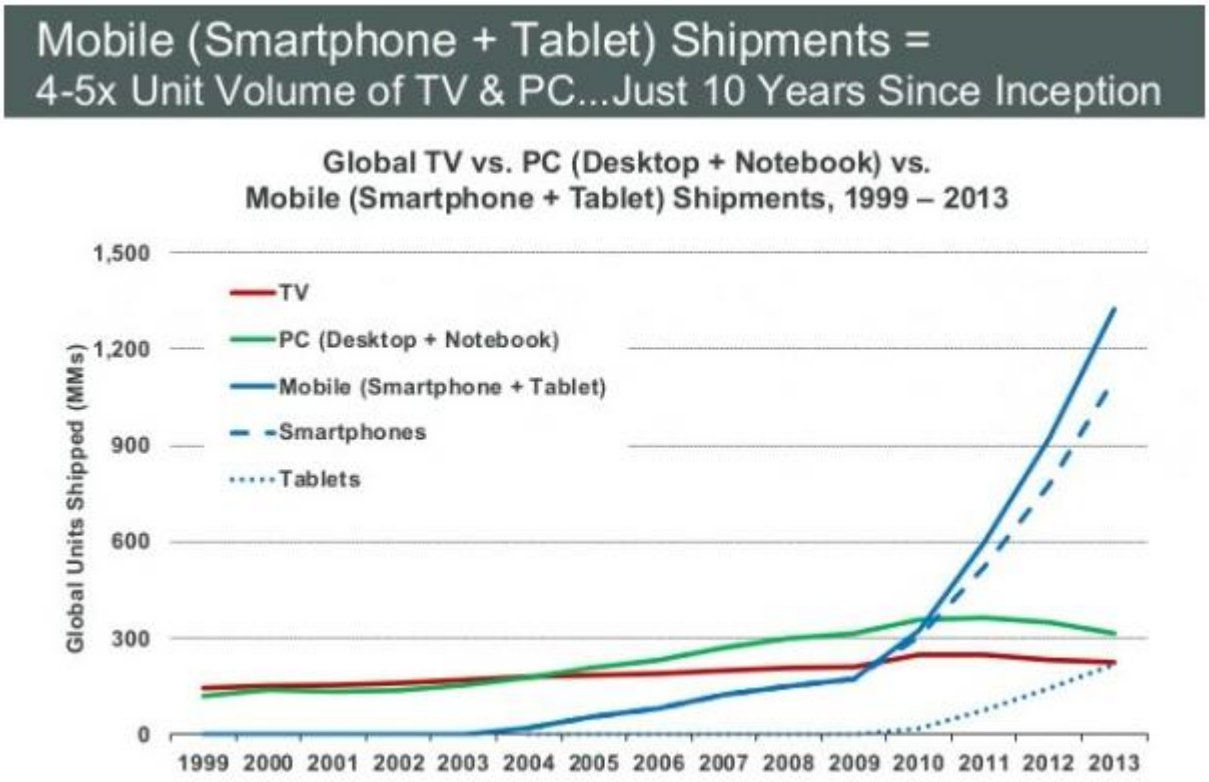
Trečiame skyriuje analizuojami pasirinktų metodų energijos sąnaudų testavimo rezultatai, pateikiamos išvados ir įtaka siūlomai metodikai.

1. INFORMACIJOS SAUGOS METODŲ IR ENERGIJOS SĄNAUDŲ MOBILIUOSE ĮRENGINIUOSE ANALIZĖ

Šio darbo analizės tikslas – trumpai apžvelgti mobiliųjų įrenginių perspektyvą BYOD politikoje, jos teikiamus privalumus ir trūkumus. Išanalizuoti šifravimo algoritmus, trumpai juos apibūdinti ir išsirinkti labiausiai tinkamus sekančiam darbui. Tai pat apžvelgti duomenų siuntimo saugos protokolus, saugų duomenų trynimą, skirtumus tarp SSD ir HDD. Peržvelgi publikuotus mokslinius straipsnius panašia tema. Suformuoti išvadas iš surinktos informacijos.

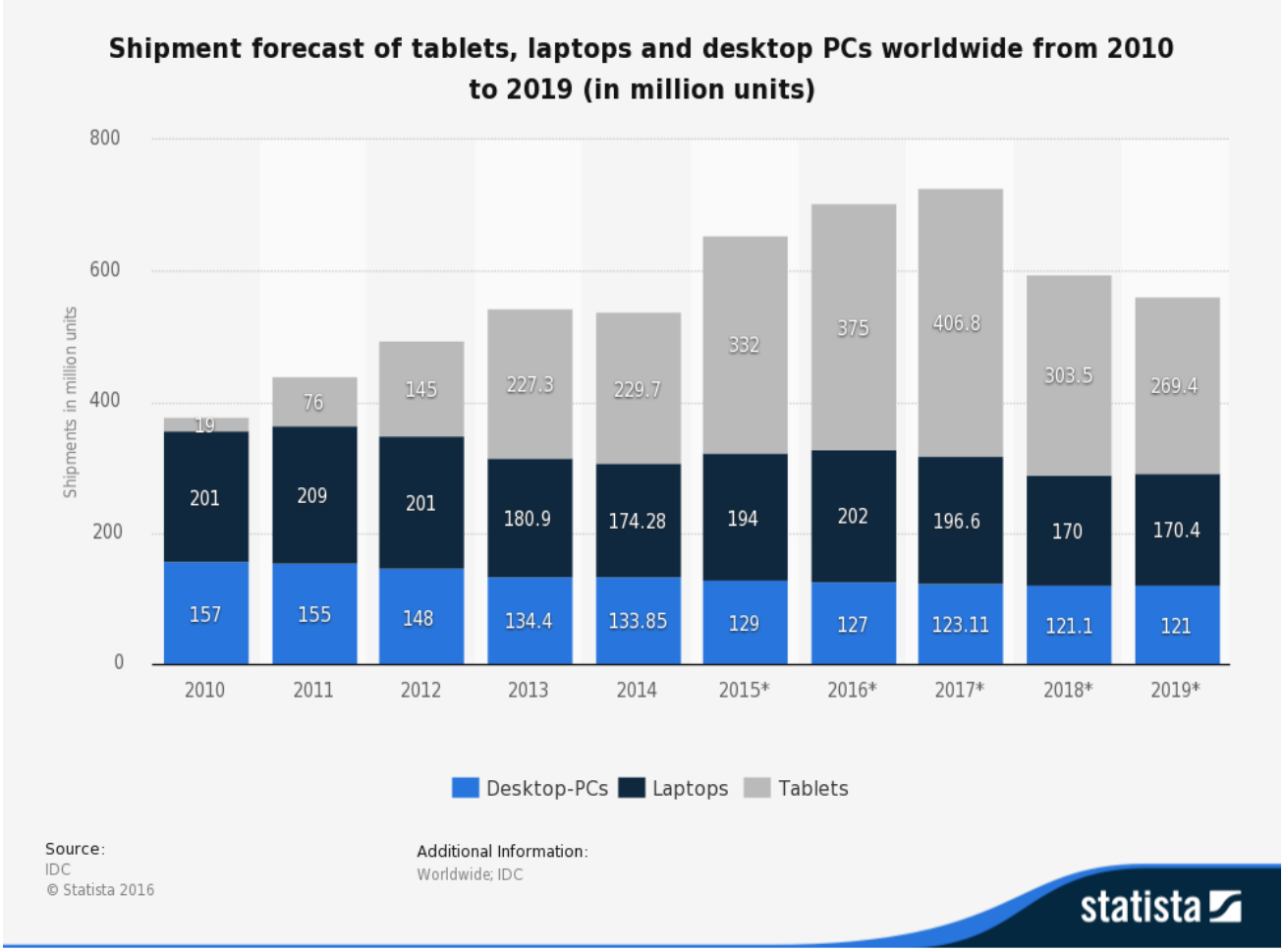
1.1. Mobiliųjų įrenginių tendencijos

Remiantis Danylo Bosomworth'o straipsniu [1] mobiliųjų įrenginių pardavimai pradėjo sparčiai augti nuo 2009 metų. Kaip matome 1.1 pav., nuo 2009 iki 2013 metų pardavimų skaičius išaugo bent 4 kartus. Ir, atrodo, ši situacija artimu metu nežada keistis.



1.1 pav. Elektronikos įrenginių pardavimai [1].

„Statista" (http://www.statista.com/) surinktuose duomenyse [2] matyti planšetinių, nešiojamųjų ir stalinių kompiuterių siuntų statistika nuo 2010 iki 2014 metų. Tai pat ir prognozė iki 2019 metų. 1.2 paveikslėlyje matyti stacionarių stalinių bei nešiojamųjų kompiuterių paklausos kritimas, tačiau nešiojamiesiems kompiuteriams numatomas stabilizavimas per ateinančius metus, tuo tarpu stacionariųjų stalinių populiarumas ir toliau mažės. Tuo tarpu planšetinių kompiuterių paklausa smarkiai išaugo nuo 2011 metų ir žadamas tolesnis kilimas.



1.2 pav. Pasaulinis planšečių, nešiojamųjų bei stalinių kompiuterių siuntų grafikas [2].

Vis didėjant mobilių įrenginių pardavimams, dauguma žmonių turi ne vieną, o kelis mobiliuosius įrenginius. Todėl nenuostabu, kad įmonės vis palankiau žiūri į BYOD (angl. *Bring Your Own Device*) politiką. Tačiau, nepaisant to, ar yra įmonėje įgyvendinta BYOD politika, 67 proc. darbuotojų darbo metu naudojasi savo asmeniniais įrenginiais ir 35 proc. išsaugo darbo elektroninio pašto duomenis savo telefone [3].

1.1.1. Asmeninių įrenginių naudojimo įmonese politika

BYOD (angl. *Bring Your Own Device*) – tai darbo politika, kai darbuotojas dirba su savo darbo priemonėmis – nešiojamuoju kompiuteriu, išmaniuoju telefonu ar planšetiniu kompiuteriu. Pagal atliktą tyrimą [4] paaiškėjo, kad BYOD darbuotojas dirba bent 2 valandomis ilgiau ir per dieną parašo 20 laiškų daugiau, nei darbuotojas besinaudojantis įmonės darbo priemonėmis. Vienas iš trijų BYOD darbuotojų el. paštą pasitikrina prieš pradėdamas darbą. Trys iš keturių IT administratorių teigia, kad BYOD yra efektyvesnio darbo būdo padidinimas. Prognozuojama, kad iki 2018 metų su savo asmeniniais įrenginiais dirbs apie 70 proc. mobiliojo personalo.

BYOD privalumai ir trūkumai:

Privalumai:

- Darbuotojai, kurių įmonėje įgyvendinta BYOD politika, dirba efektyviau;
- Nereikia investuoti į techninę įrangą, nes viskas yra paties darbuotojo;
- Reikalingi debesies sprendimai yra pigesni, nei pilnos programų versijos;
- Darbuotojai yra pasiekiami savaitgaliais ir per atostogas, tad kitų komandos narių darbas nestringa taip dažnai;
- Nereikia įrenginėti ir išlaikyti darbo vietos.

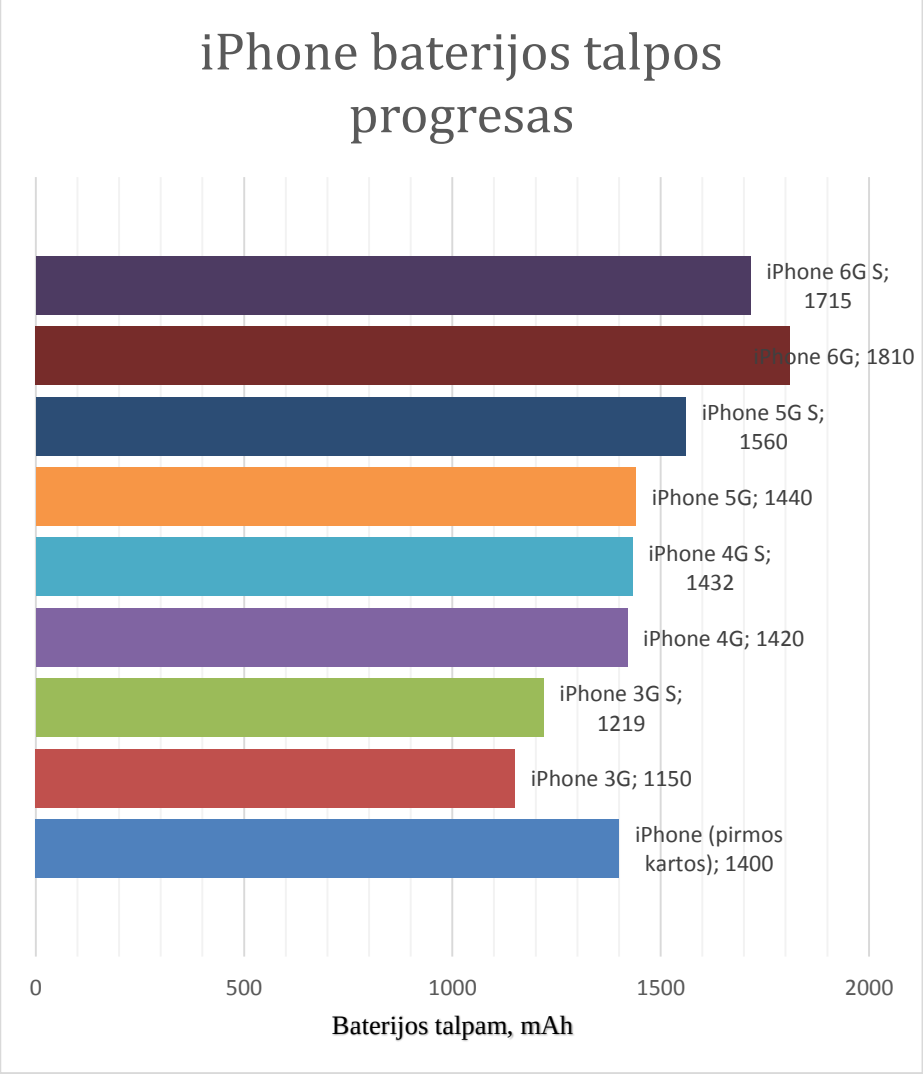
Trūkumai:

- Nesaugu, nes darbui naudojami menkai apsaugoti belaidžiai tinklai;
- Galimas informacijos nutekėjimas pametus prietaisus ar palikus prietaisą be priežiūros;
- Mobiliųjų prietaisų baterijos tarnavimo laikas dirbant intensyviu režimu nepakankamas užtikrinti pilną darbo dienos režimą;
- Tie patys prietaisai ir paskyros naudojami ir darbui, ir asmeniniams reikalams.

Dauguma BYOD trūkumų susiję su duomenų saugumu, tai ir yra didžiausias iššūkis įmonėms pritaikant šią politiką. Šią problemą galima išspręsti darbuotojui patogiu įrankiu, kuris leistų apdoroti pavienius dokumentus pasitelkiant skirtingus poreikius patenkinančius saugumo metodus, tokius kaip: duomenų šifravimu, duomenų talpinimu apsaugotuose išoriniuose įrenginiuose bei saugiu trynimu.

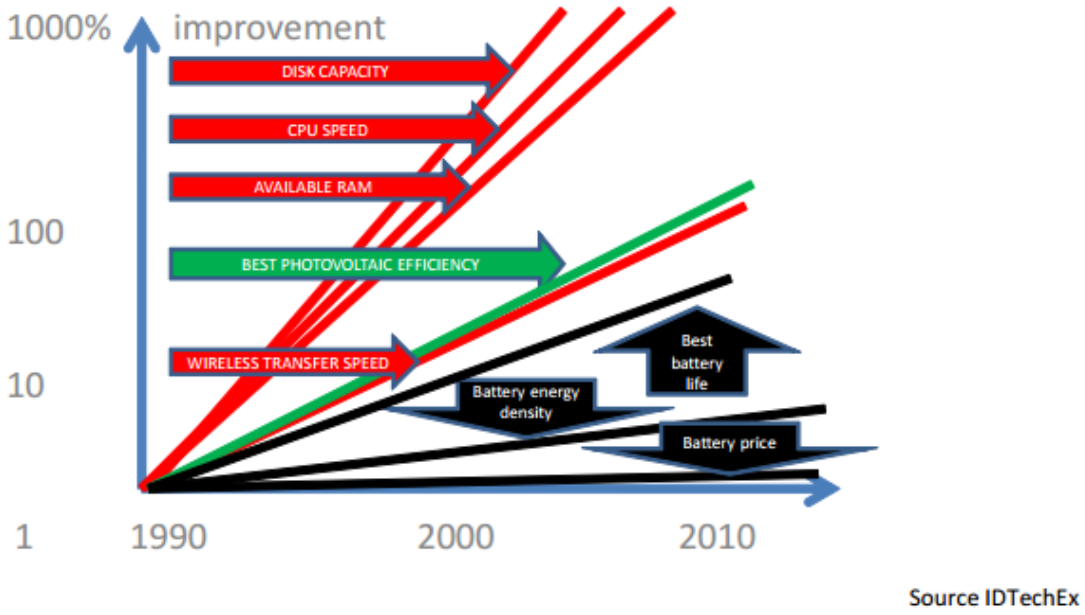
1.1.2. Mobiliųjų įrenginių techninės galimybės

Šiuolaikiniai mobilieji įrenginiai, tokie kaip nešiojamieji kompiuteriai, PDA (angl. *Personal digital assistant*), išmanieji telefonai, delniniai kompiuteriai ir panašūs įrenginiai sparčiai tobulėja, savo procesorių sparta ir technologijomis artėja prie stalinių kompiuterių lygio. Tačiau visi mobilieji įrenginiai susiduria su ta pačia problema – ribotas baterijos darbo laikas. Nors technologijos, susijusios su užduoties atlikimo sparta, sparčiai tobulėja, tuo pačiu baterijų progresas pasigirti negali.



1.3 pav. „iPhone“ baterijų talpos grafikas (Duomenys paimti iš „Wikipedia“ [5]).

1.3 paveikslėlyje matomas „Apple“ išmaniojo telefono „iPhone“ baterijos talpos progresas nuo pirmosios kartos. Pirmasis „iPhone“ turi tik ~30 proc. talpesnę bateriją nei pažangiausias šiuo metu modelis (neskaitant „iPhone plius“, dėl žymiai didesnio korpuso), atsižvelgiant tik į baterijos talpą. Šiam progresui prireikė ~ 8 metų. Tuo tarpu skaičiavimo pajėgumai skiriasi keliasdešimtis kartų nuo pirmojo išleisto „iPhone“.



1.4 pav. Skaičiavimo resursų ir energijos talpos progresas [6].

Ta pati situacija ir su kitų gamintojų įrenginiais. 1.4 paveikslėlyje lyginami skaičiavimo resursų ir baterijos progresas. Aiškiai matyti, jog baterijų vystymas sparčiai atsilieka nuo skaičiavimo resursų.

1.2. Informacijos saugos metodai

Šifravimas – tai procesas, kuriuo metu informacija pakeičiama taip, kad nebūtų įmanoma jos perskaityti, kol neiššifruojama į originalą atitinkamu būdu. Tai puikus būdas apsaugoti duomenis nuo neautorizuotų asmenų. Šifravimo strategijos:

- Pilno disko šifravimas (angl. *Full disk encryption*, FDE) – šifruojama visas informacija esanti įrenginio kietajame diske. Jei įrenginys prarastas, FDE užtikrina, kad duomenys būtų nenuskaitomi.
- Aplanko ir dokumentų šifravimas (angl. *Folder and file encryption*) – užšifruojami tik atskiri dokumentai ar aplankai su jam priskirtais dokumentais. Vartotojui reikalingas raktas arba slaptažodis, norint iššifruoti informaciją.
- Išorinių įrenginių šifravimas (angl. *Removable media encryption*) – leidžia apsaugoti nukopijuotus duomenis, esančius USB įrenginiuose, kompaktiniame diske (angl. *compact disc*, CD) ar skaitmeniniuose vaizdo diskuose (angl. *digital video disc*, DVD).

Yra du duomenų šifravimo metodai:

- Simetrinis,
- Asimetrinis.

1.2.1. Simetrinė kriptografija

Simetrinis šifravimas yra seniausiai naudojama schema. Šiuo būdu siuntėjo tekstas užšifruojamas slaptu raktu, o gavėjas dešifruoja tuo pačiu raktu, tai reiškia, jog raktas turi būti iš anksto išplatintas ir tai sukelia šias problemas:

- kaip tą raktą pasidalyti tarpusavyje;
- kiekvienai porai komunikuoti tarpusavyje reikalingas atskiras slaptas raktas;
- raktų platinimas didelį kiekį vartotojų turinčių sistemų. Šią problemą įmanoma išspręsti įvairiais algoritmais [7], [8].

Simetrinę šifravimo schemą sudaro 3 dalys:

1. Šifravimo algoritmas – generuoja užšifruotą kodą panaudojus slaptą raktą.
2. Dešifravimo algoritmas – užšifruotą kodą atstato į pradinį (originalų) tekstą panaudojus slaptą raktą.

Rakto generavimo algoritmas – sugeneruoja atsitiktinį slaptą raktą.

1.2.2. Asimetrinė kriptografija

Išsprendžia simetrinio rakto perdavimo problemą. Šioje sistemoje gavėjas turi slaptą raktą, o siuntėjas viešą. Slaptas ir viešas raktai tarpusavyje susiję, iš privačiojo generuojamas viešasis. Teoriškai įmanoma iš viešojo rakto apskaičiuoti privatųjį, tačiau praktiškai tai sunkiai įgyvendinama: kuo raktas ilgesnis, tuo daugiau resursų ir laiko prireiktų tai atlikti. Rekomenduojamas saugus rakto ilgis – 2048 bitų.

Asimetrinė šifravimo schema panaši į simetrinę, kurią sudaro 3 dalys, tačiau jos nežymiai skiriasi:

1. Šifravimo algoritmas – generuoja užšifruotą kodą panaudojus viešą raktą.
2. Dešifravimo algoritmas – užšifruotą kodą atstato į pradinį (originalų) tekstą panaudojus slaptą raktą.
3. Rakto generavimo algoritmas – sugeneruoja du tarpusavyje susijusius raktus, viešąjį ir privatųjį. Paprastai abu žymiai ilgesni už simetrinį slaptą raktą [9].

1.2.3. Informacijos šifravimo metodai

- **AES** (angl. *Advanced Encryption Standard*) – blokinis, simetrinis šifravimo algoritmas, 2001 metais paskelbtas standartu. Šis šifravimo būdas 2002 metais pakeitė DES, kuris iki tol buvo pagrindinis duomenų šifravimo standartas, nes pastarasis tapo nebepatikimas dėl per trumpo (56 bitų) rakto ilgio. Dar vadinamas Rijndaelo algoritmu, jo autoriai yra du belgų kriptografai: Joanas Daemenas ir Vincentas Rijmenas. Rakto ilgiai gali būti 128, 192 arba 256 bitų. Kiekvieną raktą sudaro tam tikras žodžių skaičius (Nk), kuris tiesiogiai priklauso nuo rakto dydžio. AES algoritmo ciklų skaičius (Nr) priklauso nuo rakto (žr. Lentelė 1.1.)

Lentelė 1.1. Žodžių ir ciklų skaičiaus priklausomybė nuo rakto ilgio.

Algoritmai	Rakto ilgis (Nk žodžiai)	Ciklų skaičius (Nr)
AES-128	4	10
AES-192	6	12
AES-256	8	14

Baitas laikomas aštuonių bitų sekos polinomu:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 = \sum_{i=0}^{7} b_i x^i$$

Pavyzdžiui, skaičiaus 77 (dvejetainė reikšmė 1001101) atitinka polinomą: $x^7 + x^4 + x^3 + 1$.

AES standarte duomenys šifruojami 128 bitų blokais. Kiekvieną raktą sudaro tam tikras skaičius žodžių, kuris tiesiogiai priklauso nuo rakto dydžio. Taip pat ir AES algoritmo ciklų skaičius priklauso nuo rakto. Užšifravimą bei dešifravimą sudaro keturios transformacijos:

1. Būsenos baitų pakeitimas naudojant pakeitimų lenteles.
2. Būsenos eilučių cikliniai postūmiai.
3. Būsenos stulpelių maišymas.

Būsenos sudėtis su vis kitu porakčiu kiekviename šifravimo cikle.

- **DES** (angl. *Digital Encryption Standard*) – Duomenų kodavimo standartas, sukurtas Horsto Feistelio 1977 metais. Tai blokinio tipo šifravimo architektūra, kurioje64 bitų duomenų blokai užšifruojami naudojant 56 bitų privatųjį raktą. DES architektūra paremta 16 ciklų pakartojimu, kurių metu 64 bitų duomenų 10 blokas yra pastumiamas ir sukeičiamas, o po to paduodamas kitam ciklui. Tikslas yra įvesti painiavą ir iškraipyti užšifruojamą tekstą kiekvieno ciklo metu. Šifruojant daugiau nei 64 bitus yra naudojami keturi metodai:
  - ECB (angl. *Electronic Codebook*) – elektroninės šifrų knygos režimas. Pats paprasčiausias blokinio šifro režimas. Pradinė tekstograma suskaidoma į blokus ir kiekvienas blokas šifruojamas nepriklausomai. Paskutinis tekstogramos blokas papildomas iki pilno kripto sistemos bloko panaudojant specialų užpildą. Algoritmas nenaudoja slapto rakto.
  - CBC (angl. *Cipher Block Chaining*) – šifro bloko grandininis režimas. Algoritme naudojamas atsitiktinis režimo inicializavimo vektorius (IV), kurį būtina žinoti, norint pilnai iššifruoti pranešimą. Šifrogramos blokai yra susieti, todėl įvykus šifravimo ar perdavimo klaidai, perduodama sekančiam blokui.
  - CFB (angl. *Cipher Feedback*) – grįžtamojo ryšio šifro režimas. Leidžia apdoroti duomenis mažesnėmis už bloką dalimis. Blokinį šifrą paverčia srautiniu. Didžiausias algoritmo trūkumas – sparta.
  - OFB (angl. *Output Feedback*) – grįžtamojo ryšio išvesties režimas. Pasižymi didesne sparta nei CFB režimas, nes raktų srautas gali būti sugeneruotas nepriklausomai nuo tekstogramos ar šifrogramos. Šiuo algoritmu neperduodamos klaidos sekantiems blokams.
- **3DES** (angl. *Triple DES*) – tekstas užšifruojamas 3 kartus su DES algoritmu naudojant 3 skirtingus raktus, laikomas saugiu nes reikalauja 2^{112} operacijų, o tai yra laikoma nepasiekiama šiuolaikinėms technologijoms. Ganėtinai lėtas programiniuose sprendimuose, nes buvo suprojektuotas siekiant našumo naudojant techninėje aparatūroje.
- **RC4** (angl. *Rivest Cipher 4*) – srautinis simetrinis algoritmas dar vadinamas ARC arba ARCFOUR (angl. *Alleged RC4*). Išsiskiria savo paprastumu ir greičiu. Naudojami įvairaus rakto ilgiai nuo 40 iki 2048 bitų. Galimas būsenos dydis yra 2064, tačiau tik 1684 bitai yra efektyvūs. RC4 iš esmės yra pseudo-atsitiktinių skaičių generatorius (PRGA), kuris yra XOR operacijos su koduojamais duomenimis rezultatas. Dėl aptiktų pažeidžiamumų laikomas nesaugiu [10].
- **MD5** (angl. *Message digest 5*) – saugus maišos algoritmas. Naudojamas viešojo rakto kripto-sistemose skaitmeniniams parašams kurti, taip pat failams palyginti.
- **RSA** (angl. *Rivest Shamir Adleman*) – asimetrinis algoritmas, kuris gali būti naudojamas ir šifravimui bei skaitmeniniam parašui. Nėra labai greitas algoritmas. DES iki 100 kartų greitesnis, tačiau ir silpnesnis už RSA.
- **SHA-1, SHA-256, SHA-384, SHA-512** – standartiniai saugūs maišos algoritmai.

1.3. Belaidžio tinklo protokolai

Siunčiant duomenis belaidžiu tinklu svarbu užtikrinti: duomenų konfidencialumą, kad duomenys išlinktų apsaugoti ir neperimti trečių asmenų; vientisumą, kad duomenys pasiektų tikslą nepakeisti ir nepažeisti; autentiškumą, kad duomenys būtų prieinami tik nustatytos tapatybės

vartotojams. Šiems uždaviniams išspęsti naudojami belaidžio tinklo saugos protokolai, iš kurių pagrindiniai yra: WEP, WPA ir WPA2.

1.3.1. WEP saugos protokolas

WEP (angl. *Wired Equivalent Privacy*) – pirmasis pristatytas šifravimo mechanizmas kaip dalis IEEE 802.11 saugos standarto 1999 metais. Paremtas RC4 šifravimo algoritmu, kuris naudoja slaptą 40 arba 104 bitų ilgio raktą, sujungtas su 24 bitų inicializavimo vektoriumi (IV). Užšifruotas tekstas nustatomas pagal formulę:

$$C = [M \| ICV(M)] + [RC4(K \| IV)],$$

kur $\|$ yra jungimo operatorius, o + XOR operatorius. IV yra WEP protokolo saugumo pagrindas, taigi norint išlaikyti pakankamą saugumo lygį ir sumažinti IV atskleidimo tikimybę, reikia jį padidinti kas kartą siunčiant duomenų paketą, taip užšifruojant kiekvieną paketą skirtingais raktais. WEP trūkumai: silpna kriptografija, raktų valdymo nebuvimas, mažas rakto ilgis, pakartotinai panaudojami IV, turi autentifikavimo problemų, neapsaugo nuo paketų klastojimų, tinklo užtvindymo (angl. *flooding*) [11], [12]. Laikomas minimaliai saugiu protokolu.

1.3.2. WPA saugos protokolas

WPA (angl. *Wi-Fi Protected Access*) – 2003 metais sukurtas pakeisti WEP protokolui, siekiant išspręsti šias problemas: mažą WEP rakto ilgį, raktų valdymo nebuvimą, inicializavimo vektoriaus pakartotinį naudojimą realizuojant RC4 algoritmą, lengvą autentifikuotų žinučių klastojimą, vartotojų tapatybės nustatymą [13]. WPA naudoja laikinojo rakto vientisumo protokolą (TKIP). Dinamiškai kiekvienam paketui sukuriamas naujas 128 bitų ilgio raktas. Duomenų vientisumui tikrinti naudojamas Michalo algoritmas, kuris generuoja žinutės integralumo kodą (MIC), tuo tarpu WEP naudojama CRC-32 maišos (angl. *hash*) funkcija. Naudojami du autentifikavimo mechanizmai [12]:

- WPA-Personal arba WPA-PSK (angl. *Pre-Shared Key*) – tai statinis raktas, platinamas tarp dviejų šalių inicializuojant sujungimą. Įrenginiams autentifikuoti naudojami 256 bitų ilgio raktai.
- WPA-Enterprise – skirtas įmonės tinklams, reikalaujantis RADIUS autentifikavimo serverio. Suteikia stipresnį autentifikavimą, naudojant EAP (angl. *Extensible Authentication Protocol*) protokolą.

1.3.3. WPA2 saugos protokolas

WPA2 (angl. *Wi-Fi Protected Access 2*) – dar žinomas kaip IEEE 802.11i standartu pristatytas 2004 metais. Kaip ir WPA, naudoja 802.1X/EAP karkasą, kuris užtikrina centralizuotą abipusio autentiškumo patvirtinimą ir dinaminį raktų valdymą. Taip pat turi du autentifikavimo mechanizmus asmeninį (angl. *personal*) ir įmonės (angl. *enterprise*). Didžiausias skirtumas tarp šių dviejų protokolų yra tai, kad WPA2 duomenims šifruoti naudoja pažangųjį šifravimo standartą (AES), vietoj TKIP. Duomenis šifruoja 128 bitų ilgio blokais. Naudoja tris skirtingus raktus (128, 192 ir 256 bitų ilgių), trijose skirtingose iteracijose [13], [14].

1.4. Saugus duomenų trynimas iš duomenų saugojimo įrenginių

Saugus duomenų trynimas tai neatkuriamas duomenų panaikinimas iš fizinės duomenų talpyklos. Programiniame lygmenyje ištrynus duomenis iš šiukšliadėžės, panaikinami tik tam tikri metaduomenys, kurie aprašo pačių duomenų buvimo vieta laikmenoje, tačiau patys duomenys išlieka fiziškai nepaliesti, kol nėra perrašomi. Ištrynus dokumento metaduomenis, dokumento užimti sektoriai kietajame diske pažymimi kaip laisvi. Tokius duomenis galima lengvai atkurti panaudojant įvairius įrankius. Norint saugiai ištrinti duomenis, būtina perrašyti dokumento sektorius duomenų laikmenoje.

1.4.1. Duomenų trynimas duomenų talpyklose

Kietajame diske duomenys įrašomi magnetinėje plokštelėje pakeičiant mikroskopinių segmentų magnetinį kryptį. Kai segmento magnetinis laukas yra pakeistas, plokštelės dalis nebegali būti atstatomas į savo tikslią originalią būseną. Dėl to saugus duomenų trynimas magnetiniuose

diskuose neapsiriboja tik vienu duomenų sektorių perrašymo ciklu. Perrašyti duomenys gali būti atkurti dėl disko liekamojo magnetizmo. Taigi HDD reikalingas kelių ciklų duomenų perrašymas.

Saugus duomenų trynimas SSD diske skiriasi nuo HDD įrenginio. Duomenų perrašymas skiriasi dėl disko nusidėvėjimo prevencijos savybių [15]. Kai SSD gauna komandą perrašyti tam tikrą egzistuojantį duomenų sektorių, jis vietoj to, kad jį pakeistų, perrašo duomenis į kitą rečiau naudotą sektorių. Duomenys senajame sektoriuje paliekami, pakeičiama tik nuoroda į atnaujintą duomenų sektorių. Net ir atliekant viso disko trynimą, nėra 100% tikimybės, jog visi duomenys bus panaikinti. Norint Saugiai ištrinti visą diską galima naudoti „ATA Secure Erase“ komandą. Bet ne visi SSD gamintojai įdiegia tokią funkciją į savo įrenginius. Šiuolaikinėse moderniuose failų sistemose nėra visiškai saugaus būdo saugiai ištrinti pavienius dokumentus.

Šiame darbe koncentruosimės ties saugiu trynimu HDD diskuose, tuo tarpu saugiu trynimu SSD diske laikysime vieno ciklo duomenų perrašymu, vildamiesi, kad bus perrašyta pakankamas dokumento segmentų skaičius, iš kurių atkurti visą originalų dokumentą neįmanomą.

1.4.2. Saugaus duomenų trynimo algoritmai

Šiame skyriuje pateiksiu trumpą informaciją apie saugaus trynimo algoritmus iš kurių išsirinksiu tinkamiausius tolesniam darbui (Lentelė 1.2).

Lentelė 1.2. Saugaus trynimo algoritmai.

Metodo pavadinimas	**Ciklų skaičius**	**Aprašymas**
Atsitiktinių duomenų perrašymas (angl. *Pseudorandom data*)	1	Greičiausia trynimo schema. Duomenys perrašomi atsitiktinių bisų seka.
Britų HMG IS5 (Baseline) 1 ciklo	1	Duomenys perrašomi nuliais.
Rusų GOST P50739-95	2	GOST P50739-95 dviejų ciklų duomenų perrašymas nuliais ir atsitiktine duomenų seka.
JAV armijos AR380-19	3	AR380-19 duomenų trynimo schema apibrėžta ir publikuota JAV armijos. AR380-19 yra trijų ciklų duomenų perrašymo algoritmas: pirmas ciklas – perrašoma su atsitiktiniais duomenimis, antras – su atsitiktine bitų seka ir trečias ciklas – pirmo ir antro ciklo duomenų suma.
JAV DoD (angl. *Department of Defense*) 5220.22-M (E)	3	DoD 5220.22-M (E) yra trijų ciklų duomenų perrašymas: pirmas ciklas – nuliais, antras ciklas – vienetais ir trečias ciklas – atsitiktinė duomenų seka.
JAV oro pajėgų 5020	3	JAV oro pajėgų 5020 yra trijų ciklų duomenų perrašymas: pirmame cikle perrašoma atsitiktine bitų seka, kiti du ta pati bitų seka paslinkta 8 ir 16 bitais į dešinę.
JAV DoD (angl. *Department of Defense*) 5220.22-M(ECE)	7	DoD 5220.22-M (ECE) yra 7 ciklų perrašymo algoritmas: pirmas, ketvirtas ir penktas ciklai perrašomi atsitiktine bitų seka, ketvirtame cikle pirmo ciklo bitų seka pastumta 8 bitais į dešinę penktame cikle 16 bitų; antras ir šeštas ciklai perrašomi nuliais, o trečias ir septintas ciklai – atsitiktiniais duomenimis.
Kanados RCMP TSSIT OPS-II	7	RCMP TSSIT OPS-II yra 7 ciklų perrašymo algoritmas: 3 pakartotini ciklai perrašant nuliais ir vienetais, o paskutinis ciklas – atsitiktinių bitų seka.
Vokiečių VSITR	7	7 7 ciklų perrašymo algoritmas: 3 pakartotini ciklai perrašant nuliais ir vienetais, o paskutinis ciklas – atsitiktiniais duomenimis.

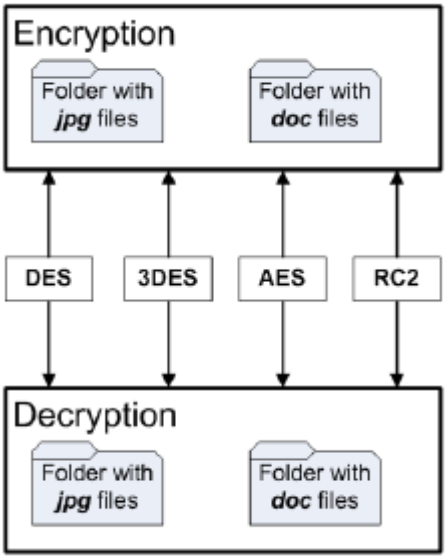
Schneier algoritmas	7	Bruco Schneierio algoritmas turi 7 ciklus: pirmas ciklas – perrašymas vienetais, antras – nuliais tada 5 kartus atsitiktiniais duomenimis.

Tyrime naudosiu nagrinėsiu tik HDD diskus, kuriam pasirinkau optimalų variantą: DoD 5220.22-M (E). Duomenys bus perrašomi 3 kartus siekiant sumažinti liekamąjį magnetizmą, to pakanka siekiant užtikrinti duomenų panaikinimo iš kietojo disko.

1.5. Kriptografinių algoritmų energijos sąnaudos mobiliuose įrenginiuose

Dariaus Nauniko atliktas darbas „Energijos suvartojimo naudojant kriptografinius servisus delniniuose kompiuteriuose tyrimas“ [16] kuriuo metu buvo registruojama PDA (techniniai duomenys: Intel PXA270 520 MHz CPU, 256 MB RAM, Windows Mobile © 6 Professional CEOS 5.2) energijos sąnaudos atliekant įvairius šifravimo algoritmus.

Tyrimui naudoti įvairių dydžių, dviejų tipų failai (paveikslėlis ir „Word“ dokumentas), bei skirtingi šifravimo, dešifravimo algoritmai (DES, 3DES, AES, RC2) 1.5 pav.



1.5 pav. Tyrime pasirinkti algoritmai ir failų tipai.

Kiekvienas algoritmas buvo leidžiami kaip servisai (angl. *Crypto Service Provider*) .NET karkase, stebint baterijos pokytį. Lentelė 1.3 pavaizduota paveikslėlių šifravimo bei dešifravimo rezultatai. Daugiausiai užšifruotos informacijos pateikė DES algoritmas sunaudojus ~80 % baterijos energijos. Tuo tarpu dešifravime geriausiai pasirodė AES, kuris sugebėjo dešifruoti daugiausiai, bei greičiausiai sunaudojus mažiausiai energijos.

Lentelė 1.3. Paveikslėlių šifravimo/dešifravimo rezultatai.

Šifravimas			
Šifravimo algoritmas	Informacijos kiekis MB	Šifravimo laikas hh:mm	Baterijos energijos sunaudojimas %
DES	10308	06:19	80
3DES	6873	05:39	74
AES	1374	05:58	78
RC2	687	06:32	75
Dešifravimas			
Dešifravimo algoritmas	Informacijos kiekis	Dešifravimo laikas	Baterijos energijos sunaudojimas %

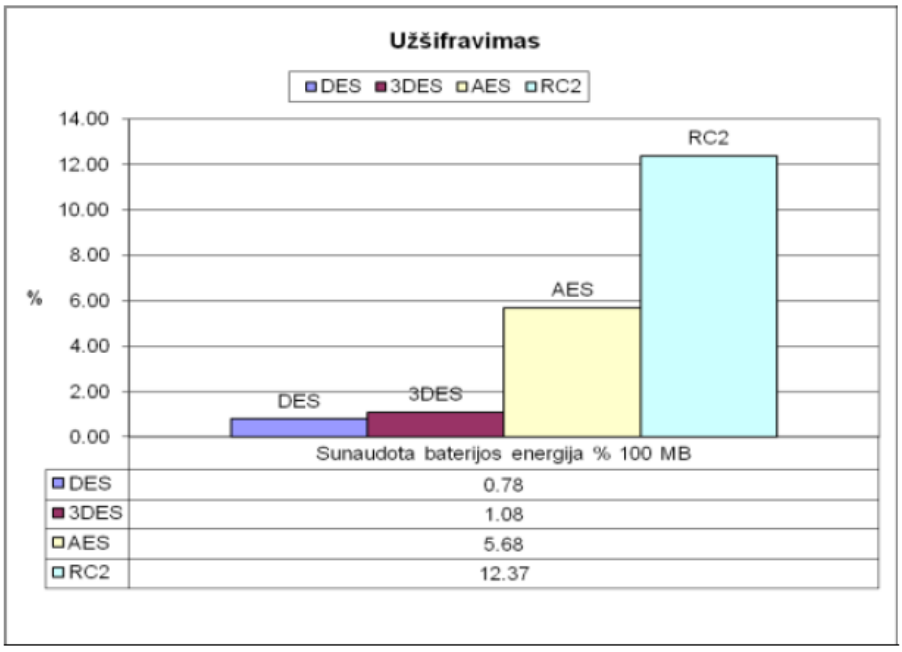
	MB	hh:mm	
DES	550	06:51	79
3DES	482	06:06	72
AES	962	04:58	64
RC2	550	07:10	84

Lentelė 1.4 pavaizduoti „Word“ dokumentų šifravimo bei dešifravimo rezultatai, kurie panašūs naudojant paveikslėlius.

Lentelė 1.4. „Word“ dokumentų šifravimo/dešifravimo rezultatai.

Šifravimas			
Šifravimo algoritmas	Informacijos kiekis MB	Šifravimo laikas hh:mm	Baterijos energijos sunaudojimas %
DES	10301	06:01	79
3DES	6868	05:35	73
AES	1294	06:08	79
RC2	647	07:15	81
Dešifravimas			
Dešifravimo algoritmas	Informacijos kiekis MB	Dešifravimo laikas hh:mm	Baterijos energijos sunaudojimas %
DES	549	06:38	77
3DES	482	06:30	75
AES	961	04:52	63
RC2	518	07:21	83

Žemiau pateiktas grafikas (1.6 pav.), kuriame pavaizduotas kiek reikia baterijos energijos norint užšifruoti 100 MB duomenų.



1.6 pav. Baterijos energijos sąnaudos 100 MB užšifravimui skirtingai algoritmais.

Tyrimo pateiktos išvados:

- RC2 algoritmas reikalauja dvigubai daugiau energijos, nei AES ir 12 kartų daugiau nei 3DES
- AES ir RC2 reikalauja apytiksliai tiek energijos tam pačiam duomenų kiekiui.
- DES ir 3DES dešifravimas reikalauja apytiksliai 15 kartų daugiau energijos, nei užšifravimui.
- Rezultatai gali būtų pateikti skirtingi atsižvelgus į įvairius kriterijus, tokius kaip algoritmo tipas, klasė, blokų dydis, dokumento dydis.

Kitas tyrimas [17] atliktas Ingos Gudaitytės pavadinimu „Delninukų belaidžio ryšio saugos protokolų tyrimas“. Darbe nagrinėjamos delninių kompiuterių energijos sąnaudos taikant tam tikrus belaidžio tinklo saugos protokolus. Tyrimas atliktas siunčiant paveikslėlį iš PDA į fiziškai arti esantį serverį. Testavimo dokumentas siuntimo metu talpinamas į FTP serverį. Tyrimui atlikti ir užfiksuoti rezultatus buvo naudojama tam tikslui sukurta programinė įranga.

Darbas atliktas su penkiomis skirtingomis prieigos taško belaidžio tinklo konfigūracijomis (Lentelė 1.5): Be protokolo, WEP, WPA-PSK, WPA-PSK ir WPA2-PSK.

Lentelė 1.5. Eksperimente naudotų prieigos taško belaidžio tinklo konfigūracijos nustatymai.

Saugos protokolas	**Duomenų šifravimo algoritmas**	**Tinklo raktas**
Be protokolo	–	–
WEP	128Bit	10 simbolių
WPA-PSK	AES	10 simbolių
WPA-PSK	TKIP	10 simbolių
WPA2-PSK	AES	10 simbolių

Naudotos penkios skirtingomis PDA belaidžio tinklo konfigūracijos (Lentelė 1.6):

Lentelė 1.6. Eksperimente naudotų PDA belaidžio tinklo konfigūracijos nustatymai.

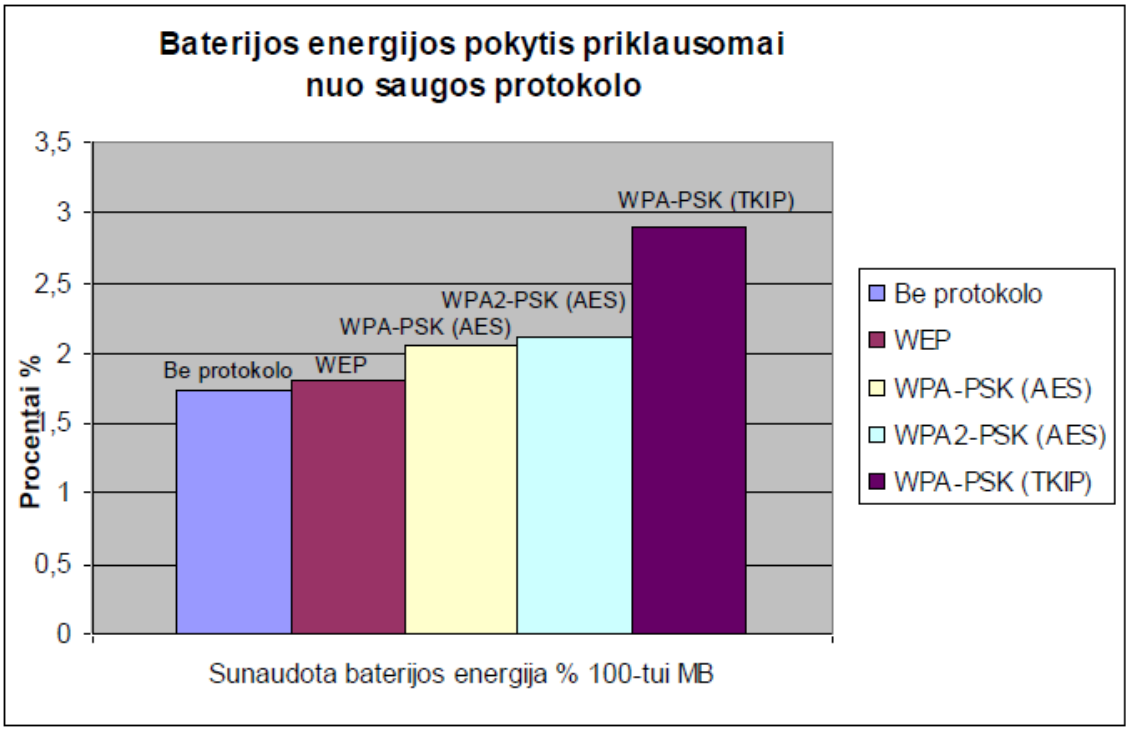
Saugos protokolas	**Duomenų šifravimo algoritmas**	**Tinklo raktas**
Be protokolo	–	–
WEP	Open	10 simbolių
WPA-PSK	AES	10 simbolių
WPA-PSK	TKIP	10 simbolių
WPA2-PSK	AES	10 simbolių

Tyrimo rezultatuose (Lentelė 1.7) matyti, kad mažiausiai energijos suvartojo duomenų siuntimas be saugos protokolo, daugiausiai energijos suvartojo WPA2-PSK AES protokolas. WPA-PSK TKIP protokolas ženkliai įtakoja siuntimo greitį.

Lentelė 1.7. PDA energijos sąnaudų tyrimo rezultatai.

Nr.	**Saugos protokolas**	**Bendras apdorojimo laikas**	**Baterijos pokytis, %**	**Atsisiųstų duomenų kiekis, MB**
1.	–	01:29:46	65%	3750
2.	WEP	01:28:18	68%	3750
3.	WPA-PSK AES	01:33:14	77%	3750
4.	WPA2-PSK AES	01:36:29	80%	3750
5.	WPA-PSK TKIP	01:28:03	76%	2625

Žemiau pateiktas grafikas (1.7 pav.), kuriame pavaizduotas kiek reikia baterijos energijos norint išsiųsti 100 MB.



1.7 pav. Baterijos energijos sąnaudos 100 MB išsiuntimui belaidžio ryšiu.

WPA2 – PSK, rezultatai: 1,73%, 1,81%, 2,05%, 2,13%. Tuo tarpu WPA – PSK ženkliais skiriasi - 2,9%.

1.6. Analizės išvados

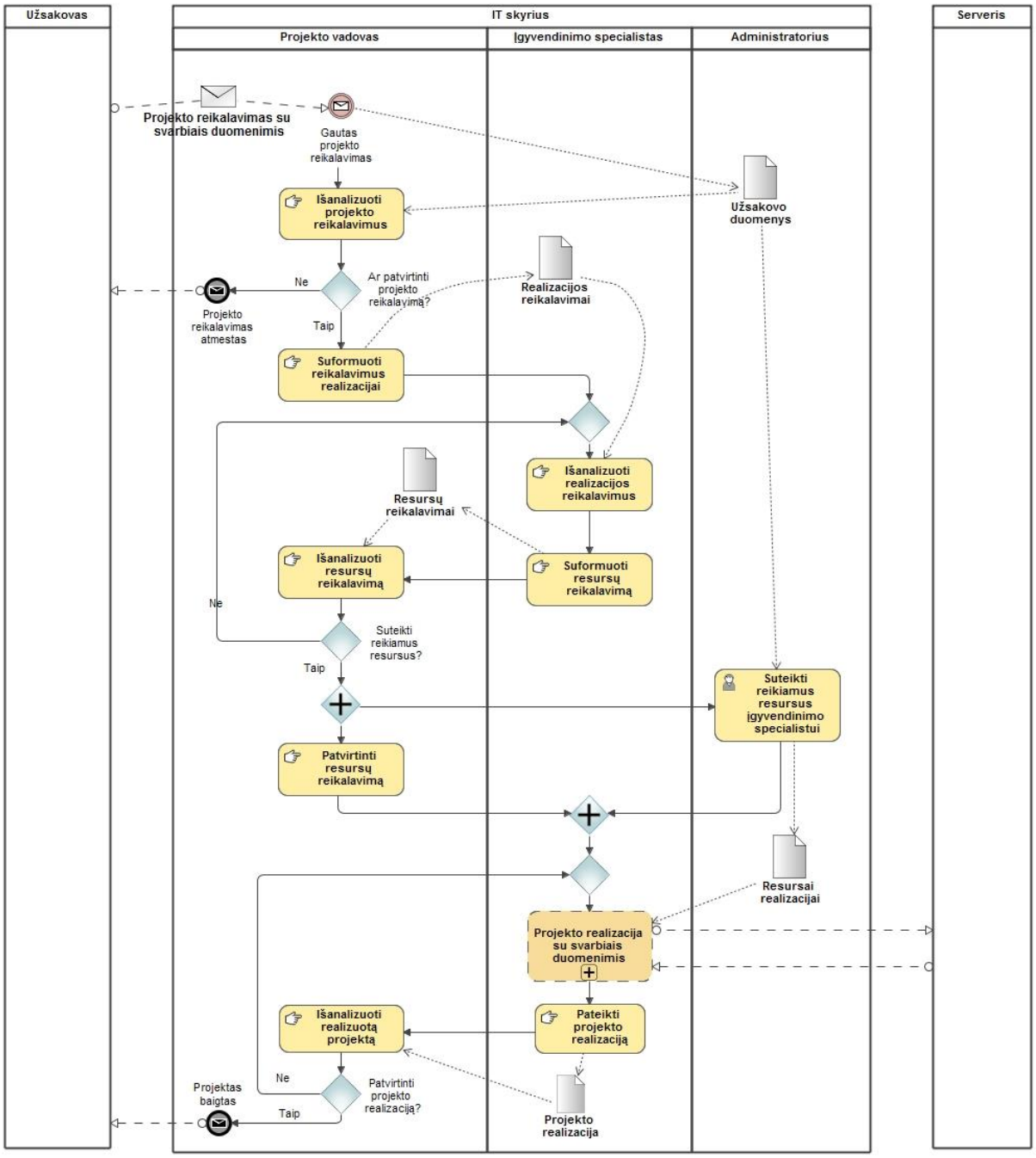
1. Mobilių įrenginių techninės charakteristikos sparčiai tobulėja, kai tuo tarpu baterijos technologijos neužtikrina išaugusios energijos paklausos. Todėl trumpėja mobiliojo įrenginio darbo laikas.
2. Mobiliųjų įrenginių paklausos ir techninių charakteristikų augimas skatina verslo įmones išnaudoti asmeninius darbuotojų įrenginius. Tai leidžia sumažinti išlaidas skirtas darbuotojų reikiama įrangą aprūpinimui, bei didinti darbo efektyvumą.
3. Didžiausias asmeninių įrenginių naudojimo įmonėse iššūkis - informacijos saugumas. Užtikrinti informacijos saugą galima naudojant viso disko šifravimą. Tačiau tai reikalauja didelių skaičiavimų resursų ir atitinkamai energijos sąnaudų.
4. Išanalizavus šifravimo algoritmų energijos sąnaudas mobiliuose įrenginiuose magistro darbo tyrimams pasirinktas AES šifravimo algoritmas dėl vidutinių energijos sąnaudų informacijos saugumui užtikrinti.
5. Išanalizavus belaidžio tinklo saugos protokolų energijos sąnaudos mobiliuose įrenginiuose magistro darbo tyrimams pasirinktas WPA2-PSK protokolas ir AES algoritmas perduodamų duomenų šifravimui, dėl vidutinių energijos sąnaudų perduodamos informacijos saugumui užtikrinti.

2. INFORMACIJOS SAUGOS METODŲ IR ENERGIJOS SĄNAUDŲ MOBILIUOSE ĮRENGINIUOSE PROJEKTAS

Projektinės dalies tikslas yra pateikti sprendimą, kuris padėtų mobilių įrenginių vartotojui sumažinanti energijos sąnaudas, užtikrinant jautrių duomenų saugumą. Apibūdinti kokioje įmonės struktūroje tai aktualu. Pateikti saugumo metodų testavimo procesą.

2.1. Problemos formulavimas ir jos sprendimo metodas

Dažna įmonė turi puikiai išvystytus projekto valdymo procesus, tačiau to negalima pasakyti apie duomenų saugumo politiką. 2.1 paveikslėlyje pavaizduotas projekto valdymo procesas, kuriame duomenys atėję kartu su užsakovo užsakymu nukeliauja pas IT skyrių administratorių ir šis gavus nurodymus priskiria duomenis įgyvendinimo specialistui.



2.1 pav. Projektų vykdymo procesas.

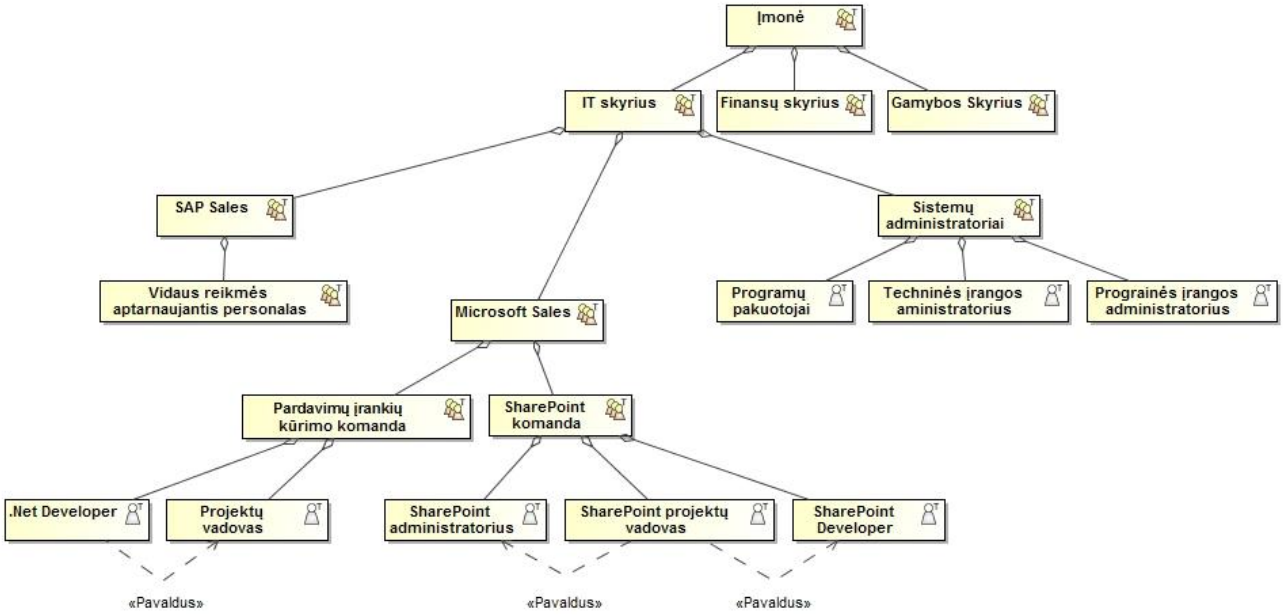
Visa sauga čia ir pasibaigia ir duomenys atsiduria pavojuje, ypač jei darbuotojas dirba savo asmeniniu įrenginiu. Praradus įrenginį galimi dideli nuostoliai, ypač jei įrenginyje buvo saugomi svarbūs ir slapti duomenys.

Šio darbo projektinės dalies uždaviniai:

- Pasiūlyti metodą suteikiantį darbuotojui galimybė užtikrinti duomenų saugumą mobiliuose įrenginiuose.
- Apibrėžti kokioje įmonės struktūroje taikytinas siūlomas metodas.
- Suprojektuoti procesą, kuris padėtų mobilių įrenginių vartotojams dirbti su saugumo jautriais duomenimis, bei planuoti savo energijos sąnaudas vykdant duomenų saugumą užtikrinančius metodus.
- Aprašyti duomenų saugumo metodų testavimo procesą.

2.2. Apibendrintas organizacijos struktūros modelis

Siūlomas metodas bus taikomas tipinėje organizacijoje, kuri netik teikia paslaugas išoriniams klientams, bet ir taip pat ir savo reikmėms. Duomenų saugumą būtina užtikrinti darbuotojams iš įvairių komandų, bei skyrių atliekantiems užduotis su svarbiais duomenimis.



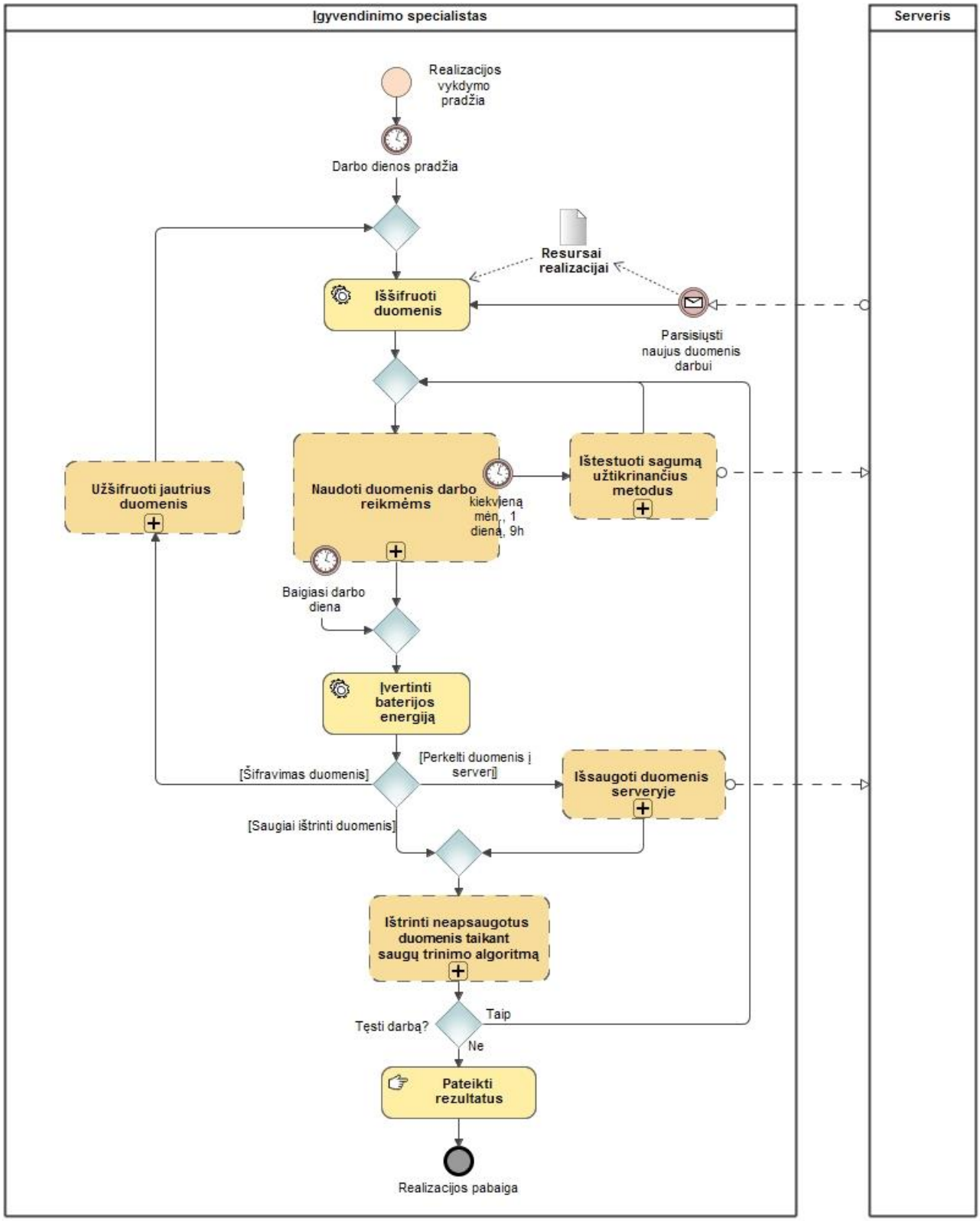
2.2 pav. Pavyzdinė įmonės struktūra.

Įmonės pavyzdys pateiktas 2.2 pav. Įmonę sudaro IT, finansų ir gamybos skyriai. IT skyrių sudaro poskyriai: „Microsoft Sales“, „SAP Sales“, bei „Sistemų administratoriai“. „Microsoft Sales“ poskyriai aprūpina produktais sukurtais „Microsoft“ įrankiais, dažniausiai kuriami įrankiai tiek vidinėms tiek išorinėms reikmėms; „SAP Sales“ komandos aprūpina vidaus personalą SAP įrankiais sukurtais sprendimais. Sistemų administratoriai aprūpina įmonės vidaus personalą technine, bei programine įranga. Kiekviena įgyvendino komanda turi projektų vadovą ir įgyvendinimo specialistus (programuotojus).

2.3. Informacijos saugos asmeniniuose įrenginiuose užtikrinimo metodo modeliavimas

Darbuotojo duomenų saugumo užtikrinimo procesas pavaizduotas 2.3 pav. Darbuotojai turi prieigą prie užšifruotų resursų, reikalingų realizuoti užduotį, parsisiuntę juos iššifruoja. Ne darbo metu savo įrenginyje saugo tik užšifruotus darbui skirtus duomenis. Prireikus apdoroti duomenų su vienu iš siūlomu metodu (duomenų šifravimu, saugiu trynimu, duomenų talpinimu serveryje), įvertinama baterijos energijos lygis, programinė įranga apskaičiuoja kiek duomenų galima apdoroti su tam tikru metodu. Duomenys patalpinti serveryje automatiškai užšifruojami, juos galima bet kada pasiekti, jų

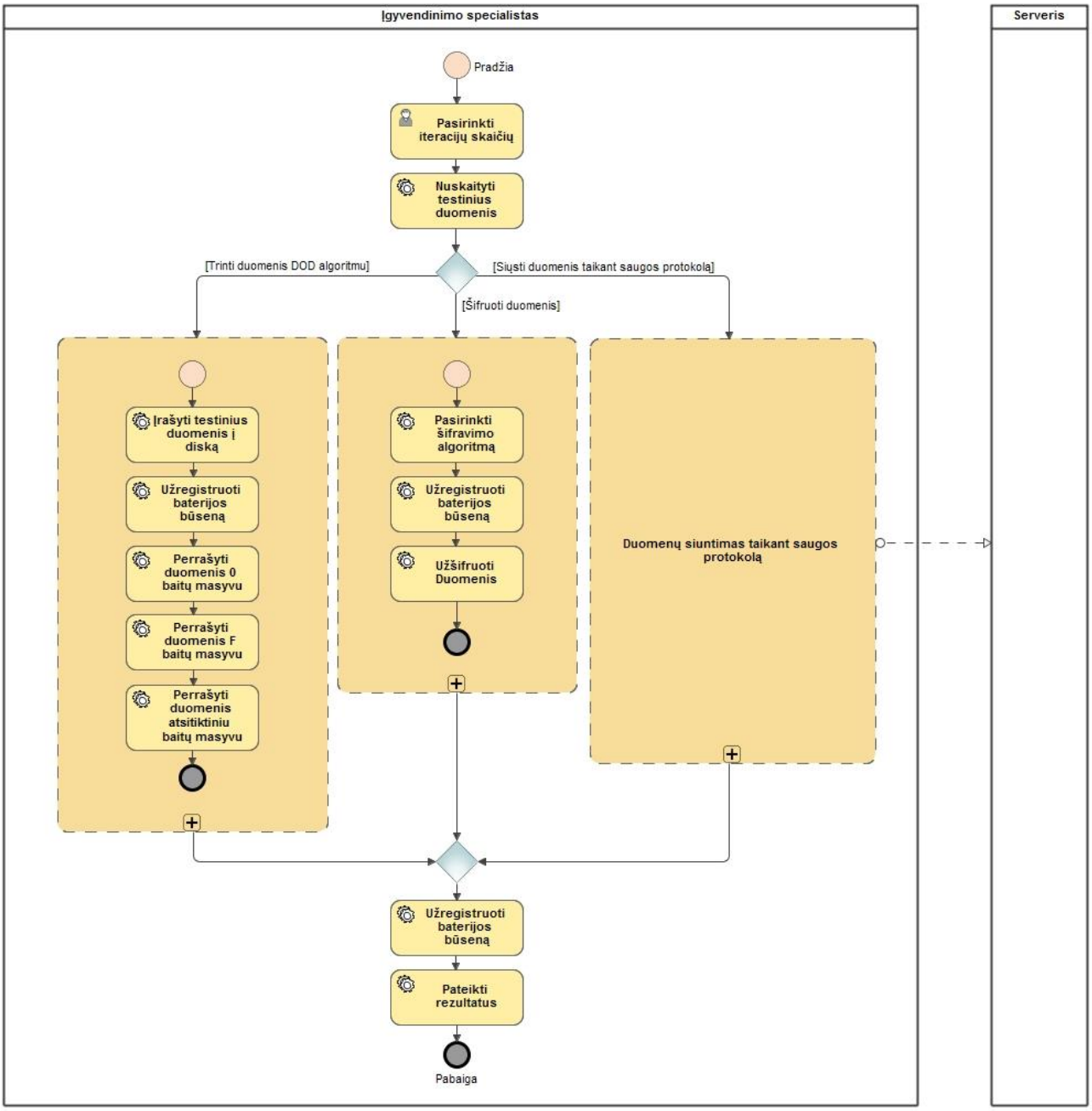
saugumas apribojamas vartotojų teisėmis. Kiek galima apdoroti duomenų yra paskaičiuojama tik tada, jei atlikti saugumo metodų testavimas. Taigi kas mėnesį arba gavus naują mobilų įrenginį, privaloma atlikti taikytinų saugos metodų testavimą su tam tikrais paruoštais duomenimis. Tokiu būdu nustatomas taikytinų metodų energijos sąnaudos mobiliam įrenginiui.



2.3 pav. „Projekto realizacija su svarbiais duomenimis“ procesas (žiūrėti 2.1 pav.).

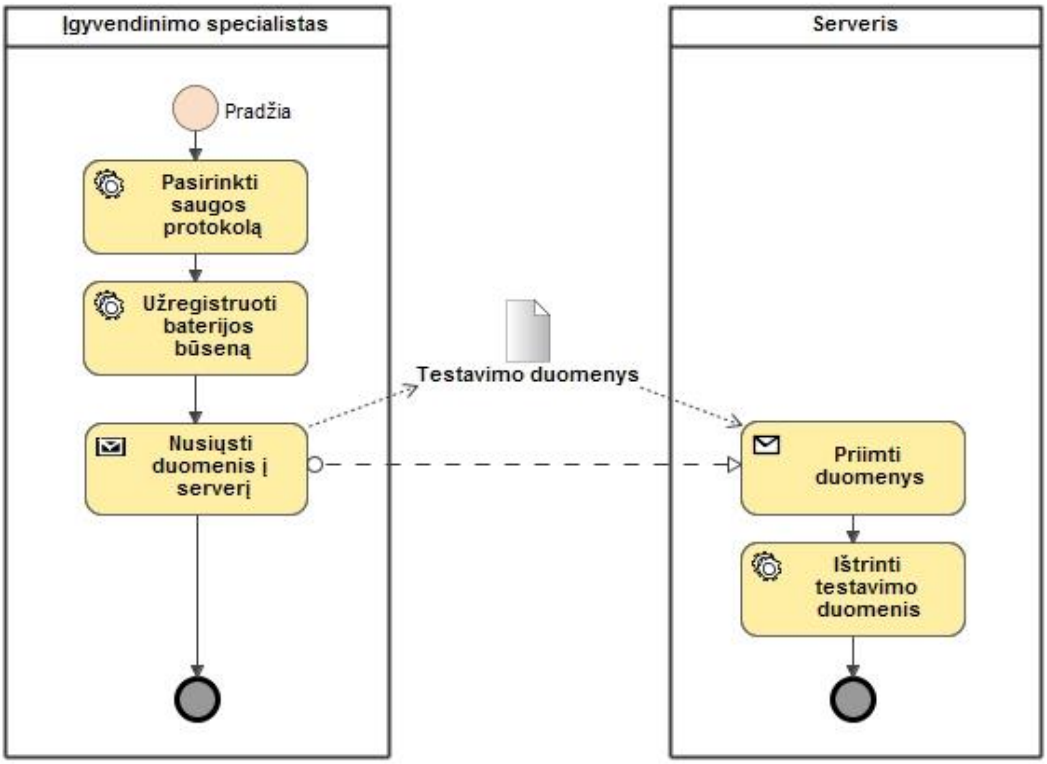
Testavimo metų atliekama paruošti testavimo scenarijai (2.4 pav.):

- Duomenų šifravimas mobiliame įrenginyje. Skirtas išmatuoti energijos sąnaudas, bei sugaištą laiką algoritmus vykdant įrenginyje.
- Duomenų siuntimas į serverį (duomenų talpyklą). Plačiau apibūdintas 2.5 pav. Skirtas išmatuoti energijos sąnaudas, siunčiant duomenis į serverį naudojant saugos protokolą.
- Duomenų trynimas 3 ciklų DoD algoritmu. Skirtas išmatuoti energijos sąnaudas ir sugaištą laiką, duomenis trinant specialiu metodu. Testavimo duomenys perkopijuojami į diską, perrašomi nuliais baitais (0000 0000), po to F baitais (1111 1111) ir galiausiai atsitiktiniu baitų masyvu lygiu 1 disko sektoriaus ilgiui.



2.4 pav. „Ištestuoti saugumą užtikrinančius metodus“ subprocesas (žiūrėti 2.3 pav.).

Testai atliekami pasirinktą iteracijų kiekiu, siekiant gauti tikslesnių matavimų. Atlikus testus, pateikiami rezultatai.

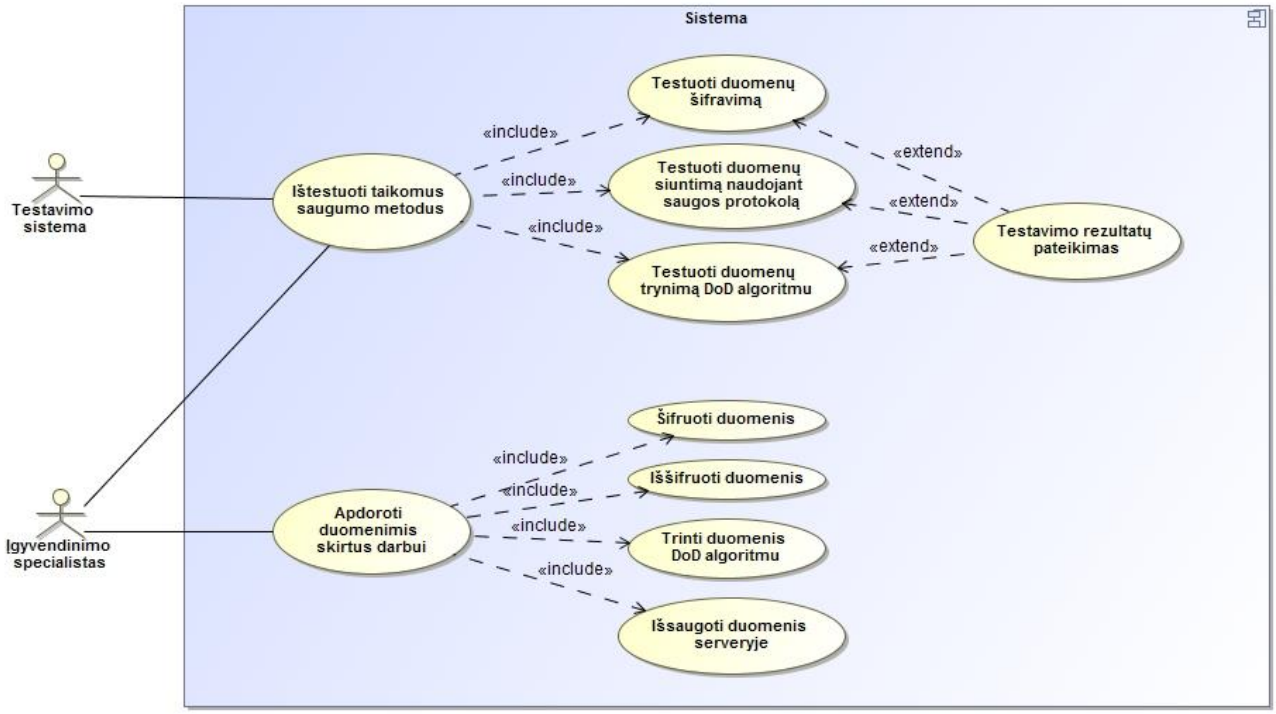


2.5 pav. „Duomenų siuntimas taikant saugos protokolą“ subprocesas (žiūrėti 2.4 pav.).

Toliau darbe bus nagrinėjami pagrindiniai šio projekto panaudos atvejai skirti saugumo metodų testavimui.

2.4. Informacijos saugumo užtikrinimo mobiliuose įrenginiuose vartotojo reikalavimų modelis

Vartotojo panaudojimo atvejų diagrama pateikta 2.6 paveikslėlyje. Pagrindiniai panaudos atvejai – naudojimų saugos metodų testavimas ir jų pritaikymas darbui. Ištestavus metodus pateikiami testavimo rezultatai.



2.6 pav. Sistemos panaudojimų atvejų diagrama.

Lentelė 2.1. PA „Duomenų šifravimas lokaliame įrenginyje“ specifikacija.

Panaudos Atvejis: „Testuoti duomenų šifravimą“		
Tikslas: Ištestuoti šifravimo algoritmu energijos sąnaudas mobiliajame įrenginyje		
Aprašymas: Energijos sąnaudos matuojamos prieš pat pradedant algoritmo veiksmus, kartojant tiek kartų kiek nurodyta iteracijos kiekiu.		
Sąlyga prieš:		Įgyvendinimo specialistas turi paleisti testavimo programą ir pasirinkti iteracijų kiekį.
Sužadinimo sąlyga:		Paleista testavimo sistema
Aktorius:		„Įgyvendinimo specialistas“
Susiję PA	**Išplečiantys PA**	„Testavimo rezultatų pateikimas“
	Apimami PA	„Ištestuoti taikomus saugumo metodus“
	Specializuoti PA	-
Pagrindinis įvykių srautas		**Sistemos reakcija**
1. Nurodomas iteracijų kiekis.		1.1. Šifravimo ciklas kartojamas tiek kiek vartotojas nurodė iteracijų.
2. Pasirenkamas testavimo dokumentas.		
3. Testavimo dokumentas užšifruojamas.		
4. Matuojamas energijos suvartojimas.		
Po sąlygos:		Pateikiami testavimo rezultatai, nurodantys kiek energijos suvartota, koks duomenų kiekis užšifruotas (iteracijų kiekis * testavimo dokumento dydis) ir kiek sugaišta laiko.
Alternatyvūs scenarijai		
1. Nespėjus įvykdyti visų iteracijų, baterija artėja ties išsikrovimo riba.		1.1. Algoritmas nutraukiamas pasibaigus pilnam ciklui.
		1.2. Pateikiami rezultatai. Rezultatuose įrašomas pranešimas dėl susidariusios situacijos.

Lentelė 2.2. PA „Išsaugoti duomenis serveryje“ specifikacija.

Panaudos Atvejis: „Testuoti duomenų siuntimą naudojant saugos protokolą“		
Tikslas: Ištestuoti duomenų siuntimo naudojant saugos protokolą energijos sąnaudas...		
Aprašymas: Energijos sąnaudos matuojamos tik siunčiant duomenis, kartojant tiek kartų kiek nurodyta iteracijos kiekiu.		
Sąlyga prieš:		Įgyvendinimo specialistas turi paleisti testavimo programą ir pasirinkti iteracijų kiekį.
Sužadinimo sąlyga:		Paleista testavimo sistema
Aktorius:		„Įgyvendinimo specialistas“
Susiję PA	**Išplečiantys PA**	„Testavimo rezultatų pateikimas“
	Apimami PA	„Ištestuoti taikomus saugumo metodus“
	Specializuoti PA	-
Pagrindinis įvykių srautas		**Sistemos reakcija**
1. Nurodomas iteracijų kiekis.		1.1 Siuntimo ciklas kartojamas tiek kiek vartotojas nurodė iteracijų.

2. Pasirenkamas testavimo dokumentas.	
3. Testavimo dokumentas išsiunčiamas.	
4. Matuojamas energijos suvartojimas.	
Po sąlygos:	Pateikiami testavimo rezultatai, nurodantys kiek energijos suvartota, koks duomenų kiekis išsiųstas (iteracijų kiekis * testavimo dokumento dydis) ir kiek sugaišta laiko.
Alternatyvūs scenarijai	
1. Nespėjus įvykdyti visų iteracijų, baterija artėja ties išsikrovimo riba.	1.1 Algoritmas nutraukiamas pasibaigus pilnam ciklui.
	1.2 Pateikiami rezultatai. Rezultatuose įrašomas pranešimas dėl susidariusios situacijos.

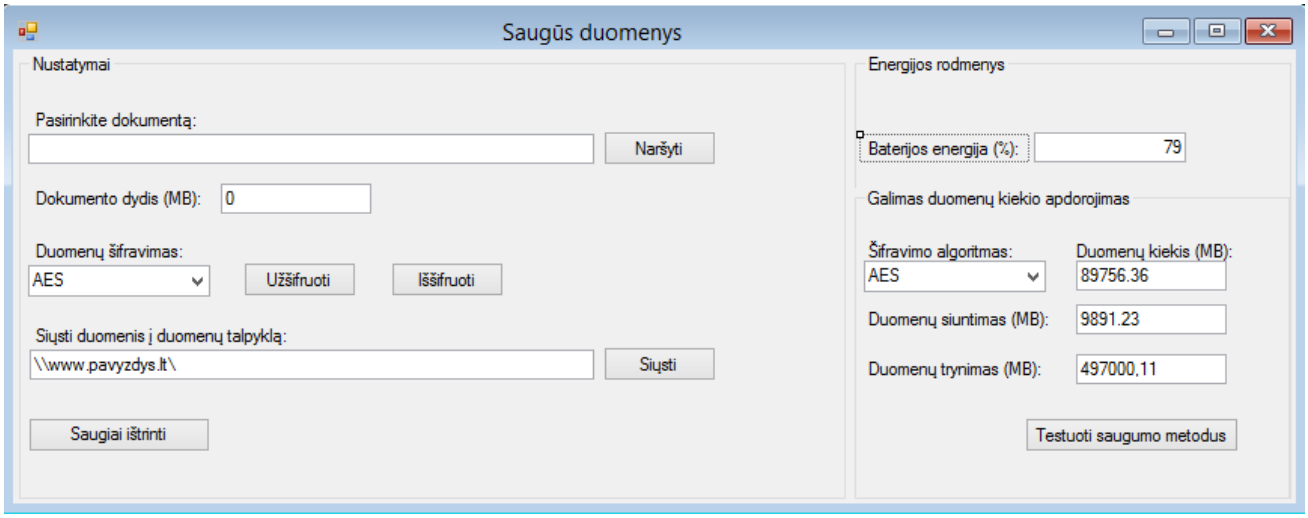
Lentelė 2.3. PA „Duomenų trynimas DoD algoritmu“ specifikacija.

Panaudos Atvejis: „Testuoti duomenų trynimą DoD algoritmu“		
Tikslas: Ištestuoti duomenų trynimą DoD algoritmu energijos sąnaudas mobiliajame įrenginyje		
Aprašymas: Energijos sąnaudos matuojamos prieš pat pradedant algoritmo veiksmus, kartojant tiek kartų kiek nurodyta iteracijos kiekiu.		
Sąlyga prieš:		Įgyvendinimo specialistas turi paleisti testavimo programą ir pasirinkti iteracijų kiekį.
Sužadinimo sąlyga:		Paleista testavimo sistema
Aktorius:		„Įgyvendinimo specialistas“
Susiję PA	**Išplečiantys PA**	„Testavimo rezultatų pateikimas“
	Apimami PA	„Ištestuoti taikomus saugumo metodus“
	Specializuoti PA	-
Pagrindinis įvykių srautas		**Sistemos reakcija**
1. Nurodomas iteracijų kiekis.		1.1 Šifravimo ciklas kartojamas tiek kiek vartotojas nurodė iteracijų.
2. Pasirenkamas testavimo dokumentas.		
3. Testavimo dokumentas perrašomas 0 baitų masyvu.		
4. Testavimo dokumentas perrašomas F baitų masyvu.		
5. Testavimo dokumentas perrašomas A baitų masyvu.		
6. Matuojamas energijos suvartojimas.		
Po sąlygos:		Pateikiami testavimo rezultatai, nurodantys kiek energijos suvartota, koks duomenų kiekis užšifruotas (iteracijų kiekis * testavimo dokumento dydis) ir kiek sugaišta laiko.
Alternatyvūs scenarijai		
1. Nespėjus įvykdyti visų iteracijų, baterija artėja ties išsikrovimo riba.		1.1 Algoritmas nutraukiamas pasibaigus pilnam ciklui.

	1.2 Pateikiami rezultatai. Rezultatuose įrašomas pranešimas dėl susidariusios situacijos.

2.5. Testavimo sistemos grafinė vartotojos sąsajos prototipas

Pagal pasiūlyto sprendimo, saugumo metodų testavimo procesą, sekančiame skyriuje bus atliekami pasirinktų metodų testavimas. 2.7 paveikslėlyje pavaizduota pagrindinis programos prototipo langas skirtas saugumo metodų testavimui. Vartotojas gali pasirinkti norimą dokumentą bei norimą saugumo metodą. Pasirinkęs dokumentą, bei saugumo metodą vartotojas pamatys perspėjimą jei dokumento dydis bus didesnis, nei numatomos energijos sąnaudos.



2.7 pav. Grafinė vartotojo sąsaja, algoritmų testavimas.

Programa parašyta C# kalboje, panaudojant „Windows Forms“ grafinės sąsajos klasės biblioteką. Programos prototipas skirtas tik nešiojamiems kompiuteriams su „Windows“ operacine sistema.

2.6. Išvados

Pasiūlytas informacijos saugos asmeniniuose įrenginiuose užtikrinimo metodika suteikianti vartotojui galimybę saugiai apdoroti duomenis.

Duomenų saugumo metodika asmeniniuose įrenginiuose apibrėžta modeliu. Vartotojas turi galimybė duomenis užšifruoti, perkelti į nuotolinį serverį, panaudojant belaidį tinklą su saugos protokolu arba juos ištrinti panaudojant saugaus trynimo algoritmą.

3. ENERGIJOS SĄNAUDŲ INFORMACIJOS SAUGAI MOBILIUOSE ĮRENGINIUOSE EKSPERIMENTINIS TYRIMAS

Eksperimentui atlikti buvo naudojamas nešiojamas kompiuteris Acer Aspire V17, kurio pagrindinės techninės specifikacijos:

- 1000GB 5400 aps. SATA kietasis diskas (modelio numeris: WD10JPVX);
- 8 GB DDR3 RAM atminties;
- Intel® Core™ i7-4720HQ procesorius;
- Atheros AR5BWB222 belaidžio tinklo adapteris (b/g/n);
- 52 Wh ličio jonų baterija.

3.1. Eksperimento atlikimas

Bandymui atlikti parsisiųstas standartizuotas testavimui skirtas paveikslėlis „San Diego“ iš „University of Southern California“ svetainės (http://sipi.usc.edu/database/). Paveikslėlio charakteristikos:

- Pavadinimas: 2.2.01.tiff;
- Rezoliucija: 1024x1024 pikseliai;
- Dydis 3072kb (24 bitai/pikseliui);
- Pasiekiamas adresu: http://sipi.usc.edu/database/database.php?volume=aerials&image=13#top

Bandymai buvo atliekama baterijai esant 100 % įkrovimui, vienas testavimo algoritmas buvo kartojamas iteracijomis, tol kol pilnai iškrovė bateriją (likus 5 % baterijos energijos, „Windows“ operacinė sistema įjungia miego (angl. *hibernate*) režimą). Energijos sąnaudos matuojamos kas tūkstantį arba kelis tūkstančius iteracijų (priklausomai nuo algoritmo). Baterijos energijos lygis matuojamas 1 procento tikslumu, nes „Windows“ operacinė sistema neteikia tikslesnės informacija apie baterijos energijos lygį. Kiekvienas saugumo metodas buvo ištestuotas tris kartus, pilnai iškraunant bateriją, siekiant patikrinti ar rezultatai išlieka nepakitę pakartojant bandymą.

3.2. Eksperimento rezultatai

Pirmas ištestuotas saugumo metodas: AES šifravimo algoritmas. Pirmo, antro ir trečio bandymo rezultatai pateikti šiose lentelėse: Lentelė 3.1, Lentelė 3.2, Lentelė 3.3.

Lentelė 3.1. AES algoritmo tyrimo rezultatai, pirmas bandymas.

Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
1000	2	3,4	3,14
2000	5	6,8	6,29
3000	9	10,3	9,43
4000	12	13,8	12,58
5000	16	17,3	15,72
6000	20	20,7	18,87
7000	23	24,2	22,01
8000	27	27,7	25,16
9000	31	31,2	28,3
10000	34	34,6	31,45
11000	38	38,1	34,59
12000	42	41,6	37,74
13000	46	45,1	40,88
14000	49	48,5	44,03
15000	53	52	47,17
16000	57	55,5	50,32
17000	61	59	53,46

18000	65	62,5	56,61
19000	68	65,9	59,75
20000	73	69,4	62,9
21000	76	72,9	66,04
22000	80	76,3	69,19
23000	84	79,8	72,33
24000	88	83,3	75,48
25000	94	95,8	78,62

Lentelė 3.2. AES algoritmo tyrimo rezultatai, antras bandymas.

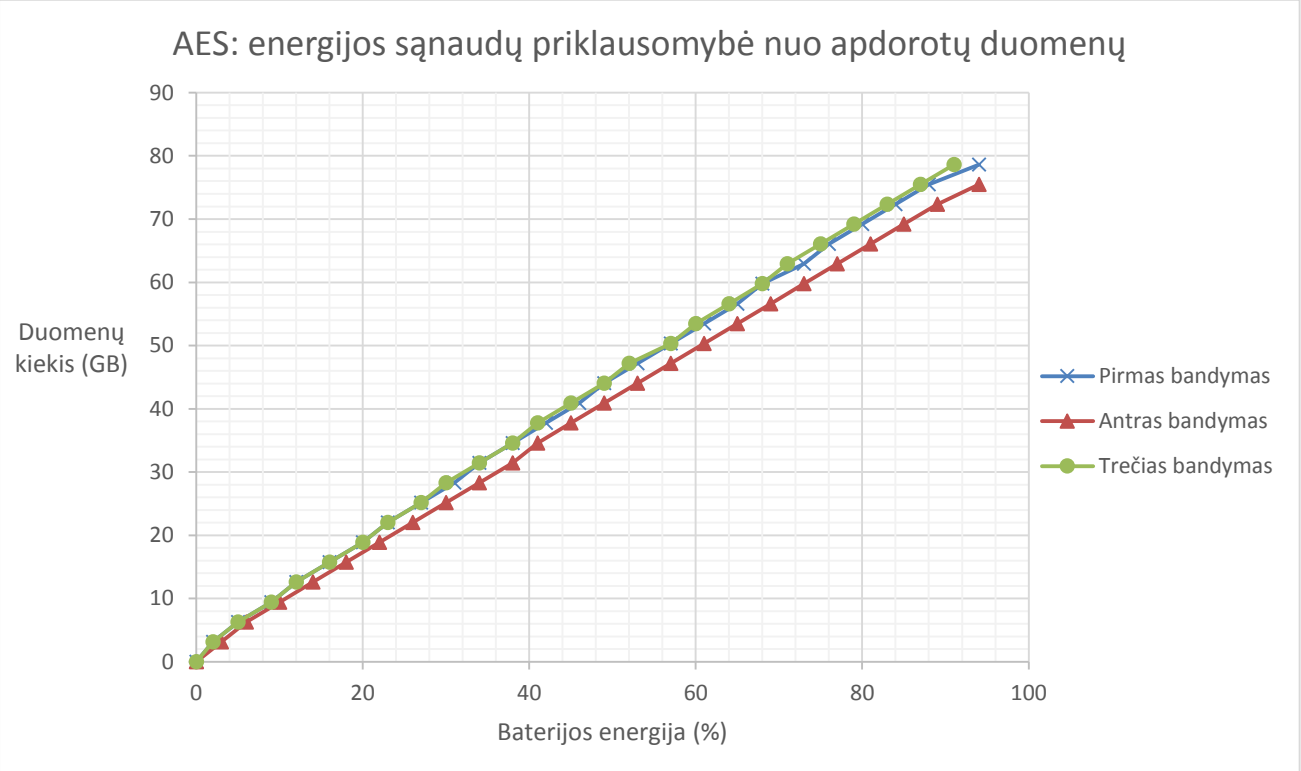
Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
1000	3	3,5	3,14
2000	6	7,1	6,29
3000	10	10,7	9,43
4000	14	14,3	12,58
5000	18	17,9	15,72
6000	22	21,5	18,87
7000	26	25,1	22,01
8000	30	28,7	25,16
9000	34	32,3	28,3
10000	38	36	31,45
11000	41	39,6	34,59
12000	45	43,2	37,74
13000	49	46,8	40,88
14000	53	50,4	44,03
15000	57	54	47,17
16000	61	57,6	50,32
17000	65	61,2	53,46
18000	69	64,8	56,61
19000	73	68,4	59,75
20000	77	72	62,9
21000	81	75,6	66,04
22000	85	79,2	69,19
23000	89	82,8	72,33
24000	94	97,5	75,48

Lentelė 3.3. AES algoritmo tyrimo rezultatai, trečias bandymas.

Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
1000	2	3,4	3,14
2000	5	6,8	6,29
3000	9	10,3	9,43
4000	12	13,8	12,58
5000	16	17,3	15,72
6000	20	20,8	18,87
7000	23	24,4	22,01
8000	27	27,8	25,16
9000	30	31,3	28,3
10000	34	34,9	31,45
11000	38	38,4	34,59
12000	41	41,9	37,74
13000	45	45,4	40,88

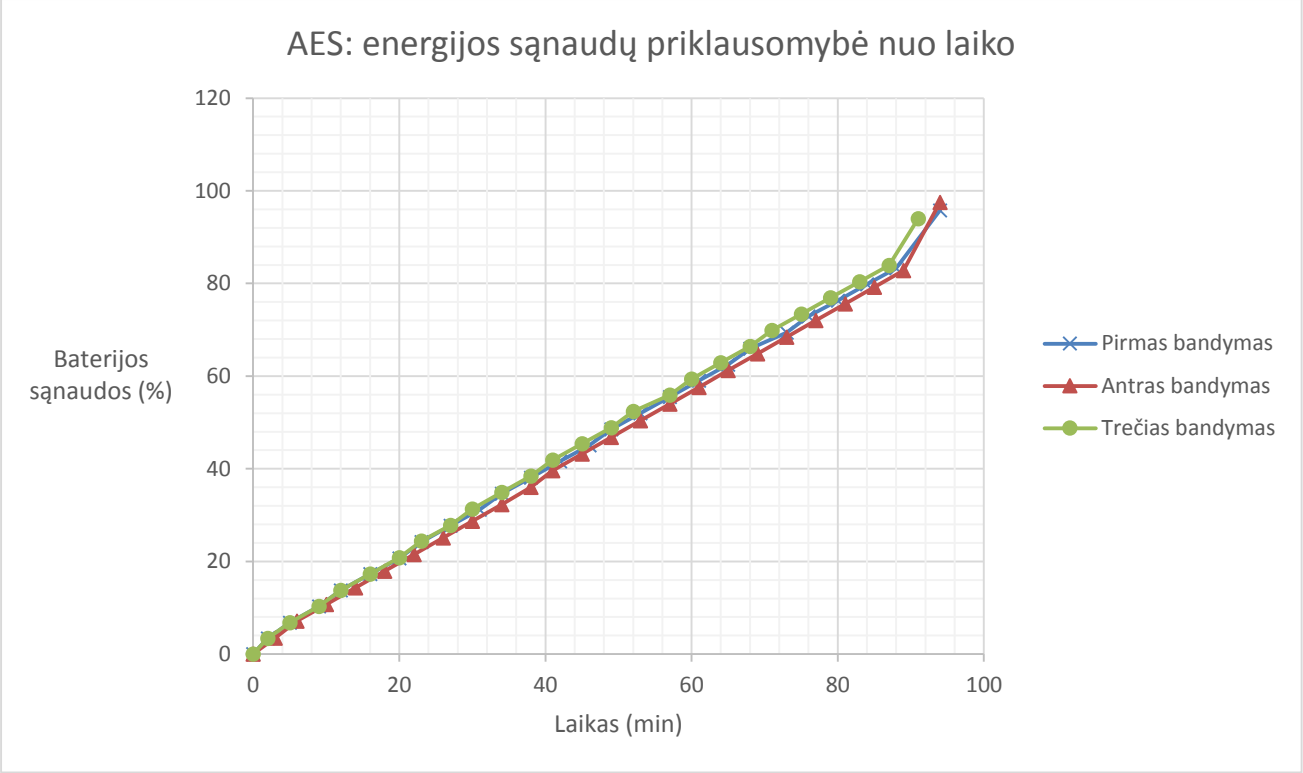
14000	49	48,9	44,03
15000	52	52,4	47,17
16000	57	55,9	50,32
17000	60	59,4	53,46
18000	64	62,9	56,61
19000	68	66,4	59,75
20000	71	69,9	62,9
21000	75	73,4	66,04
22000	79	76,9	69,19
23000	83	80,4	72,33
24000	87	83,9	75,48

Baterijos energijos lygis buvo registruotas kas 1000 iteracijų, apdorojant 3 GB duomenų. Kaip matyti 3.1 grafike visi trys bandymai davė panašius rezultatus. Antro bandymo metu apdorotas mažiausias duomenų kiekis 1 procentui baterijos energijos, kuris lygus 0,803 GB/%, o trečio bandymo metu daugiausiai - 0,864 GB/%, pirmu bandymu - 0,836 GB/%. Šių trijų atliktų bandymo vidutinis duomenų kiekio apdorojimas vienam baterijos procentui lygus 0,834 GB/%. Algoritmas vidutiniškai apdorojo 14,772 MB/s.



3.1 pav. AES algoritmo energijos sąnaudų priklausomybė nuo apdorotų duomenų.

3.2 paveikslėlyje pavaizduotas nešiojamo kompiuterio baterijos energijos sąnaudų priklausomybė nuo laiko, šifruojant duomenis AES algoritmu. Pirmu bandymu gautas vidutinis 0,0163 %/s baterijos energijos sąnaudos, antru - 0,016 %/s, o trečiu - 0,0161 %/s. Rezultatai labai panašūs. Vidutinis energijos sąnaudos lygios 0,0162 %/s.



3.2 pav. AES algoritmo energijos sąnaudų priklausomybė nuo apdorotų duomenų.

Antras ištestuotas saugumo metodas - duomenų trynimas DoD 3 ciklų algoritmu. Pirmo, antro ir trečio bandymo rezultatai pateikti šiose lentelėse: Lentelė 3.4, Lentelė 3.5, Lentelė 3.6.

Lentelė 3.4. Trijų ciklų DoD trynimo algoritmo rezultatai. Pirmas bandymas.

Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
5000	2	2,6	15,72
10000	5	5,4	31,45
15000	8	10,6	47,17
20000	11	15,5	62,9
25000	15	20,5	78,62
30000	18	25,7	94,35
35000	22	30,6	110,07
40000	26	35,5	125,8
45000	29	40,6	141,52
50000	33	45,6	157,25
55000	36	50,6	172,97
60000	40	55,5	188,7
65000	43	60,4	204,42
70000	47	65	220,15
75000	51	69,8	235,87
80000	54	74,7	251,6
85000	58	79,7	267,32
90000	62	84,9	283,05
95000	66	89,9	298,77
100000	69	95	314,5
105000	73	100	330,22
110000	77	105,1	345,95
115000	81	110,1	361,67
120000	85	115,1	377,4

125000	88	119,9	393,12
130000	94	130,9	408,85

Lentelė 3.5. Trijų ciklų DoD trynimo algoritmo rezultatai. Antras bandymas.

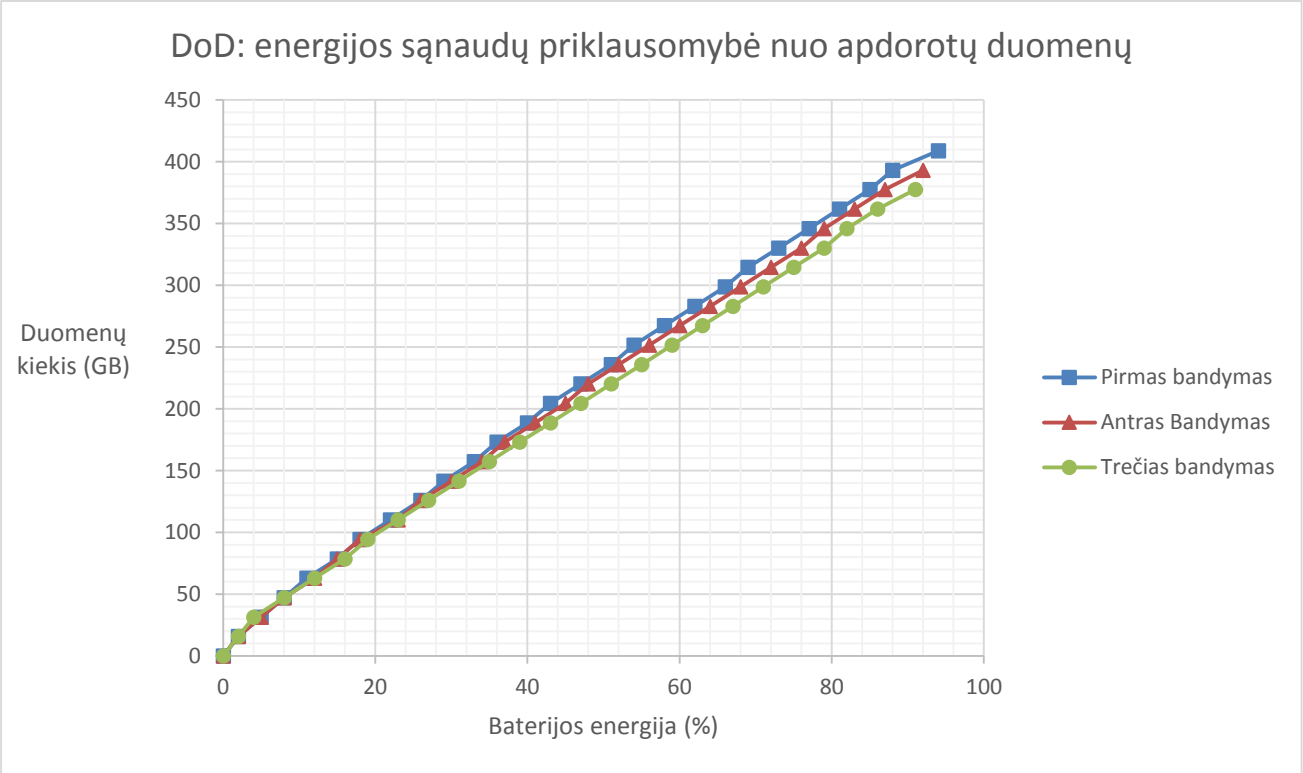
Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
5000	2	2,7	15,72
10000	5	6,2	31,45
15000	8	11,1	47,17
20000	12	16,4	62,9
25000	15	21,4	78,62
30000	18	26	94,35
35000	23	30,1	110,07
40000	26	35,2	125,8
45000	30	40	141,52
50000	34	44,9	157,25
55000	37	49,7	172,97
60000	41	54,6	188,7
65000	45	59,3	204,42
70000	48	64,1	220,15
75000	52	69	235,87
80000	56	74,2	251,6
85000	60	79,6	267,32
90000	64	84,7	283,05
95000	68	89,5	298,77
100000	72	94,5	314,5
105000	76	99,6	330,22
110000	79	104,6	345,95
115000	83	109,6	361,67
120000	87	114,7	377,4
125000	92	123,3	393,12

Lentelė 3.6. Trijų ciklų DoD trynimo algoritmo rezultatai. Trečias bandymas.

Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
5000	2	2,6	15,72
10000	4	5,6	31,45
15000	8	10,4	47,17
20000	12	15,2	62,9
25000	16	19,7	78,62
30000	19	24,6	94,35
35000	23	29,2	110,07
40000	27	34,1	125,8
45000	31	38,8	141,52
50000	35	43,6	157,25
55000	39	48,1	172,97
60000	43	53	188,7
65000	47	57,6	204,42
70000	51	62,5	220,15
75000	55	67,4	235,87
80000	59	71,9	251,6
85000	63	76,9	267,32
90000	67	81,8	283,05
95000	71	86,5	298,77
100000	75	91,5	314,5

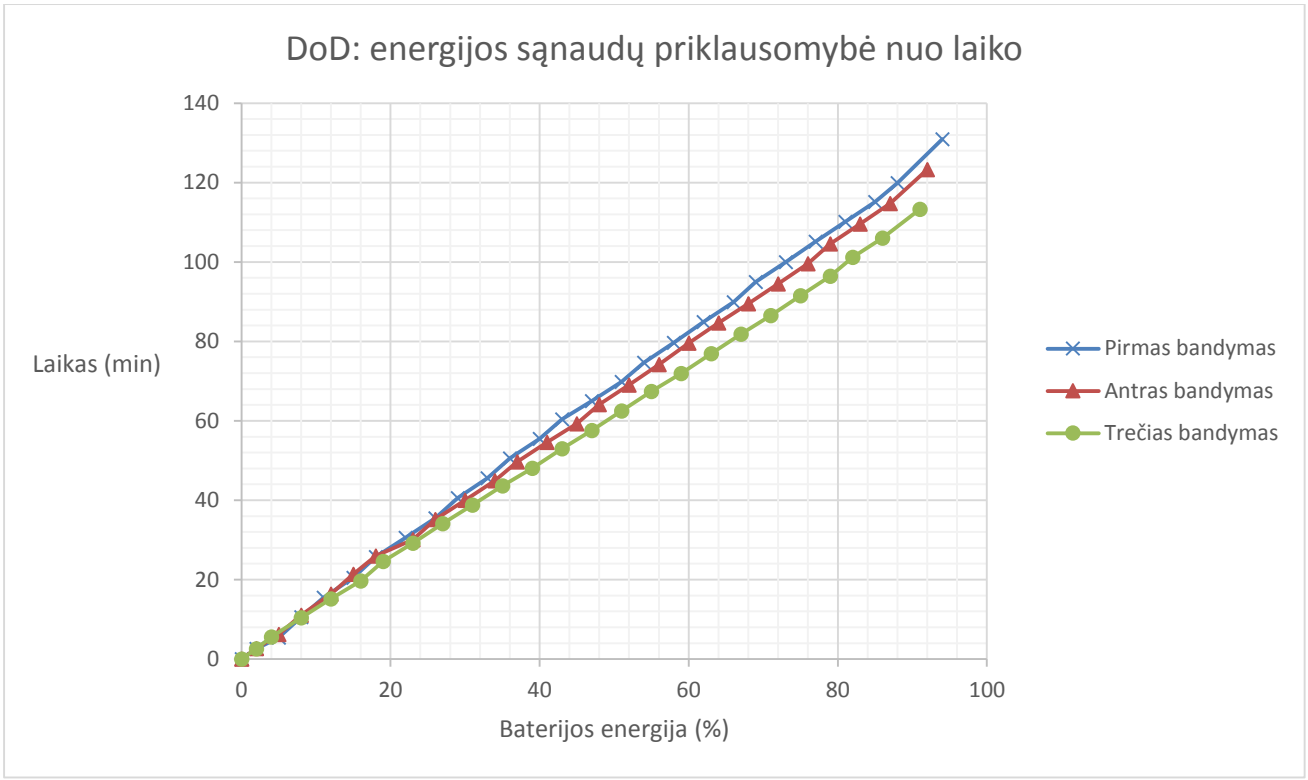
105000	79	96,4	330,22
110000	82	101,2	345,95
115000	86	106	361,67
120000	91	113,3	377,4
125000	93	516,3	393,12

Baterijos energijos lygis buvo registruotas kas 5000 iteracijų, per kurias apdorota 15 GB duomenų. Skirtingų bandymų rezultatai mažai kuo skiriasi tarpusavyje. Duomenų apdorojimo kiekis 1 baterijos procentui svyruoja nuo 4,147 GB/% (trečiu bandymu) iki 4,349 GB/% (pirmu bandymu), antru bandymu - 4,273 GB/%. Vidurkis lygus 4,257 GB/%. Vidutinis duomenų apdorojimo greitis lygus 57,121 MB/s.



3.3 pav. Trijų ciklų DoD trynimo algoritmo energijos sąnaudų priklausomybė nuo apdorotų duomenų.

3.4 paveikslėlyje pavaizduotas baterijos energijos sąnaudų priklausomybė nuo laiko, trinant duomenis trijų ciklų DoD algoritmu. Pirmu bandymu gautas vidutinis 0,012 %/s baterijos energijos sąnaudos, antru - 0,0124 %/s, o trečiu - 0,0134 %/s. Vidutinis energijos sąnaudos lygios 0,0126 %/s.



3.4 pav. Trijų ciklų DoD trynimo algoritmo energijos sąnaudų priklausomybė nuo apdorotų duomenų.

Paskutinis ištestuotas saugumo metodas – duomenų siuntimas belaidžiu ryšiu panaudojant WPA2-AES saugumo protokolą. Duomenys persiųsti panaudojant virtualų routerį „VirtualRouter Plus“ [18] naudojantį WPA2-AES kaip numatytąjį saugumo protokolą. Virtualus routeris įdiegtas į fiziškai šalia stovintį įrenginį. Duomenys buvo siunčiami į bendrai naudojamą aplankalą esančiame tame pačiame įrenginyje kaip ir virtualus routeris. Pirmo, antro ir trečio bandymo rezultatai pateikti šiose lentelėse: Lentelė 3.7, Lentelė 3.8, Lentelė 3.9.

Lentelė 3.7. WPA2 saugumo protokolo rezultatai. Pirmas bandymas.

Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
1000	9	24,6	3,14
2000	19	48,7	6,29
3000	29	72,7	9,43
4000	40	96,7	12,58
5000	50	120,7	15,72
6000	61	144,7	18,87
7000	72	169	22,01
8000	84	194	25,16

Lentelė 3.8. WPA2 saugumo protokolo rezultatai. Antras bandymas.

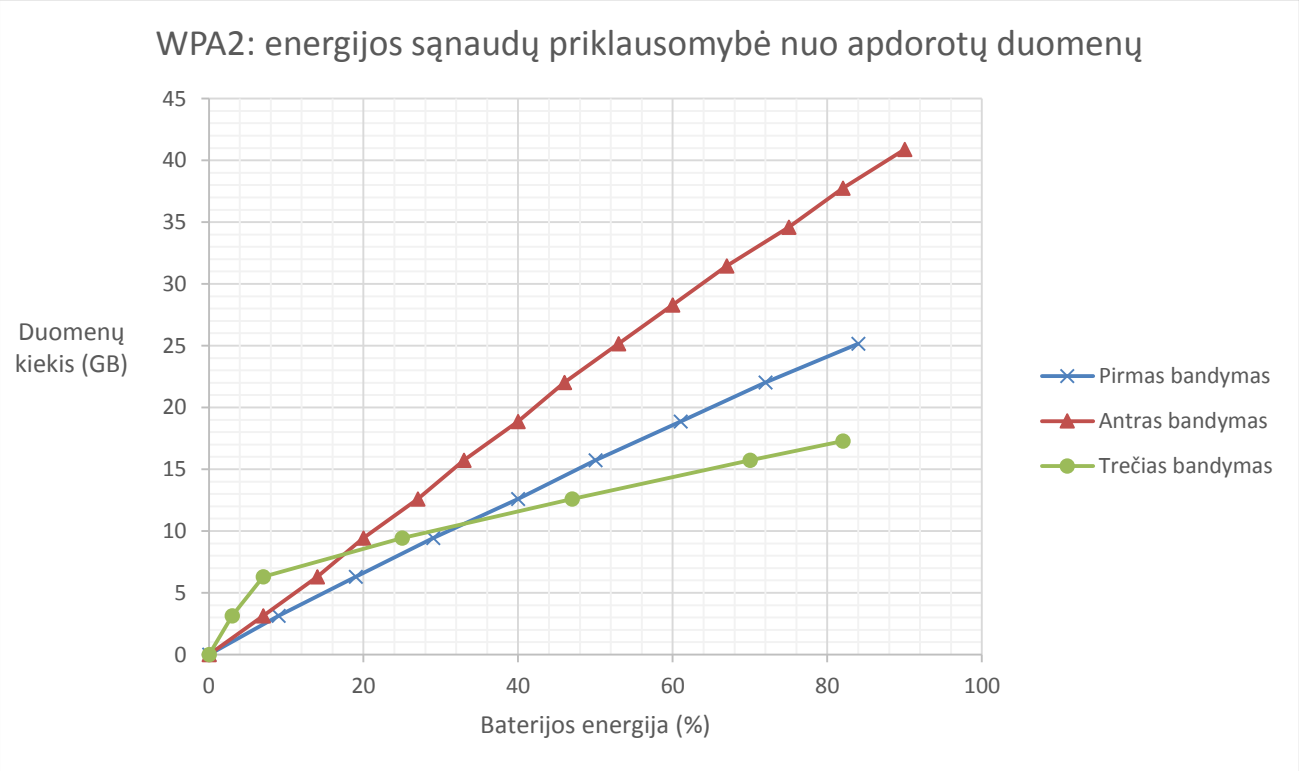
Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)
1000	7	13,8	3,14
2000	14	29	6,29
3000	20	44,4	9,43
4000	27	59,8	12,58
5000	33	75,4	15,72
6000	40	90,8	18,87
7000	46	106,9	22,01
8000	53	123,1	25,16
9000	60	139,1	28,3

10000	67	155,6	31,45
11000	75	171,9	34,59
12000	82	188,4	37,74
13000	90	205,1	40,88

Lentelė 3.9. WPA2 saugumo protokolo rezultatai. Trečias bandymas.

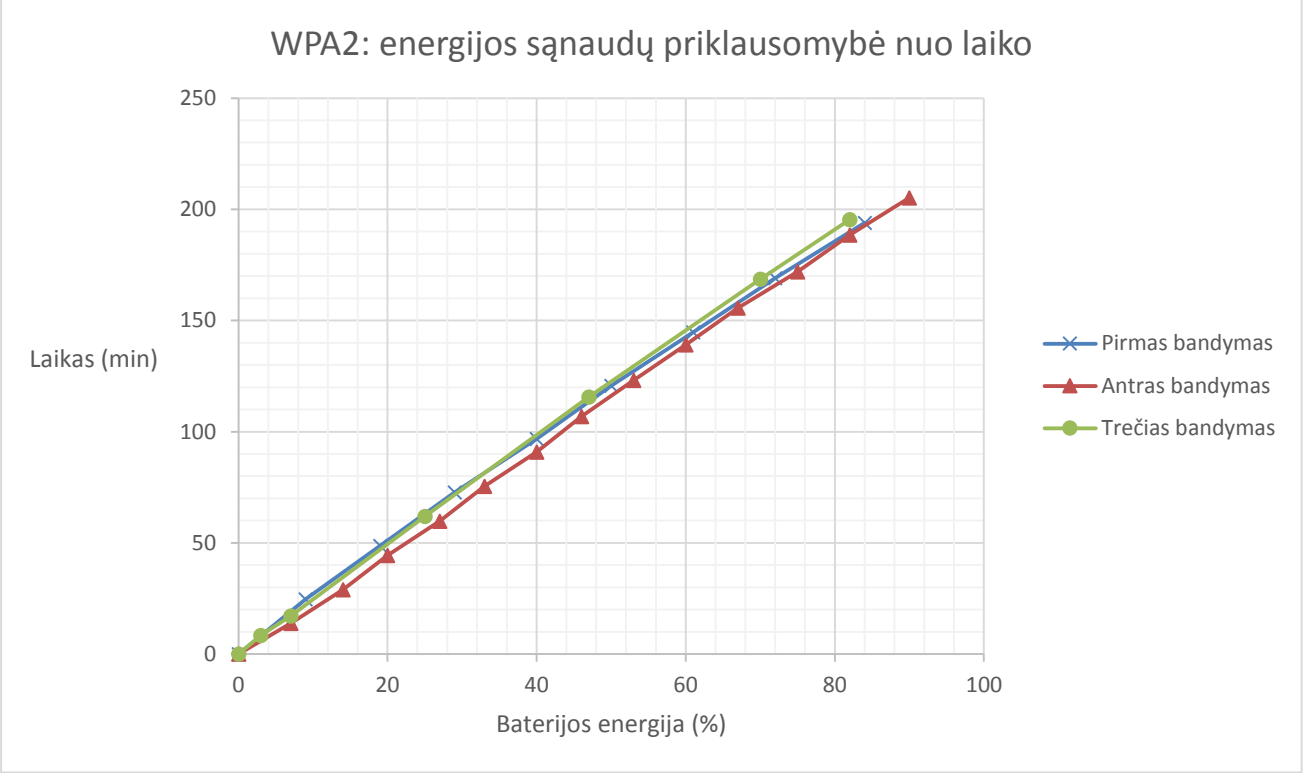
Iteracija	Sąnaudos (%)	Laikas (min)	Duomenys (GB)	Vidutinis siuntimo greitis	Sunaudota energijos
1000	3	8,4	3,14	6,196952663	0,00591716
2000	7	17,1	6,29	6,001908397	0,006789525
3000	25	61,9	9,43	1,17132216	0,006727664
4000	47	115,6	12,58	0,975193798	0,006771359
5000	70	168,6	15,72	0,990239295	0,006919047
5500	82	195,4	17,29	0,9761018	0,006991814

Baterijos energijos lygis buvo registruotas kas 1000 iteracijų, per kurias apdorota įvairūs kiekiai duomenų. Kaip matyti 3.5 paveikslėlyje skirtingų bandymų rezultatai stipriai skiriasi tarpusavyje. Pirmu bandymu vidutinis duomenų apdorojimo kiekis vienam procentui lygus 0,311 GB/%, antru - 0,466 GB/%, o trečiu - 0,275 GB/%, vidurkis - 0,351. Atsižvelgiant į tyrimo rezultatus, skaičiuoti energijos sąnaudas padalinant išsiųstą duomenų kiekį iš vidutinio apdorotų duomenų kiekio vienam baterijos procentui, būtų netikslinga.



3.5 pav. WPA2 saugumo protokolą energijos sąnaudų priklausomybė nuo apdorotų duomenų.

Išanalizavus 3.6 paveikslėlį, kuriame vaizduojamas baterijos sąnaudų priklausomybė nuo siuntimo laiko, galime daryti išvadas, kad baterijos sąnaudos nepriklauso nuo išsiųsto duomenų kiekio, bet priklauso nuo siuntimo laiko. Pirmu bandymu gautas vidutinis 0,0072 %/s baterijos energijos sąnaudos, antru - 0,0073 %/s, o trečiu - 0,007 %/s. Vidutinės energijos sąnaudos lygios 0,00717 % baterijos energijos.

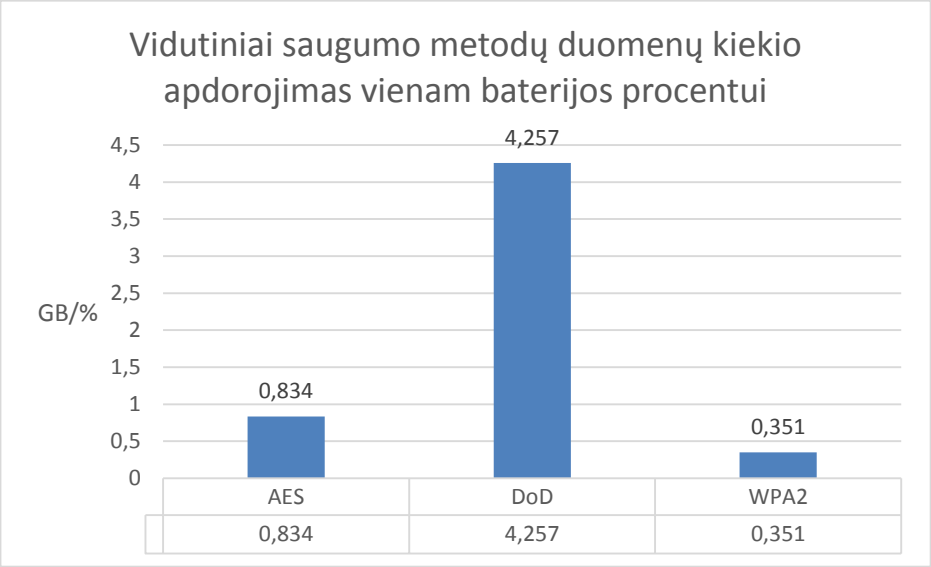


3.6 pav. WPA2-AES saugumo protokolą energijos sąnaudų priklausomybė nuo laiko.

Norint apskaičiuoti kiek energijos bus sunaudota panaudojant AES šifravimo arba DoD trynimo algoritmą, užtenka norimo failo dydį padalinti iš vidutinio apdorotų duomenų kiekio vienam procentui energijos. Tuo tarpu, norint sužinoti kiek energijos reikia sunaudoti norint išsiusti tam tikro dydžio dokumentą, reikia apskaičiuoti numatomo siuntimo laiką ir jį padauginti iš vidutinių energijos sąnaudų per 1 sekundę.

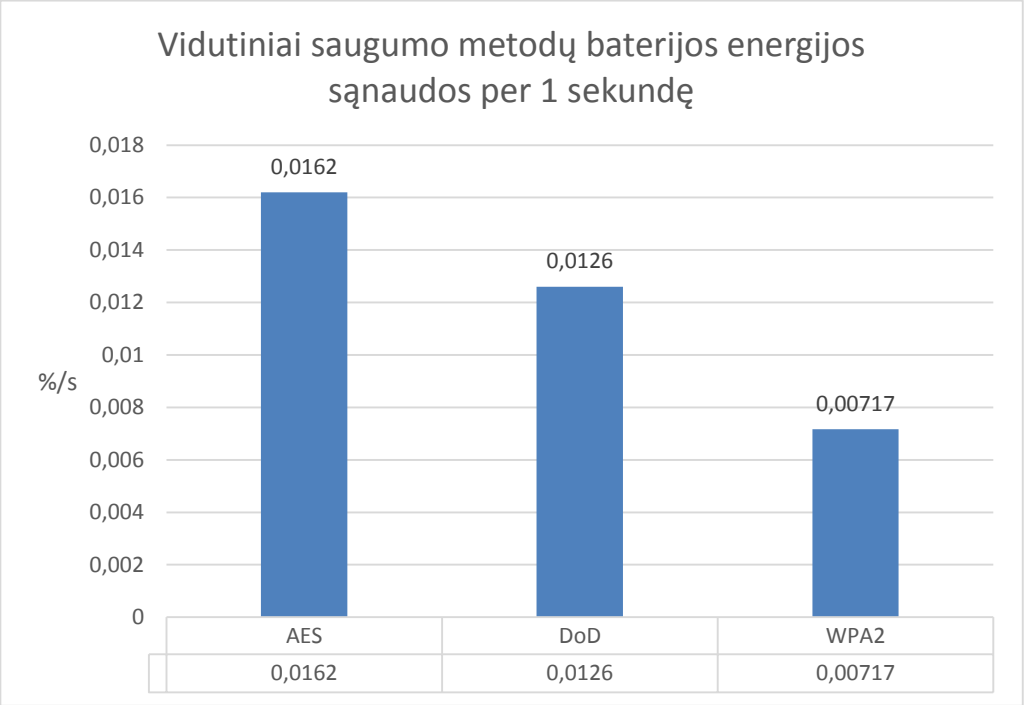
3.3. Eksperimento rezultatų apibendrinimas

Kaip matyti 3.7 paveikslėlyje daugiausiai duomenų apdoroja iškraunant 1 baterijos energijos procentą DoD trynimo algoritmas 4,257 GB/%, mažiausiai – duomenų siuntimas naudojant WPA2-AES protokolą, kuris apdoroja 0.351 GB/%. AES apdoroja 0.834 GB/%.



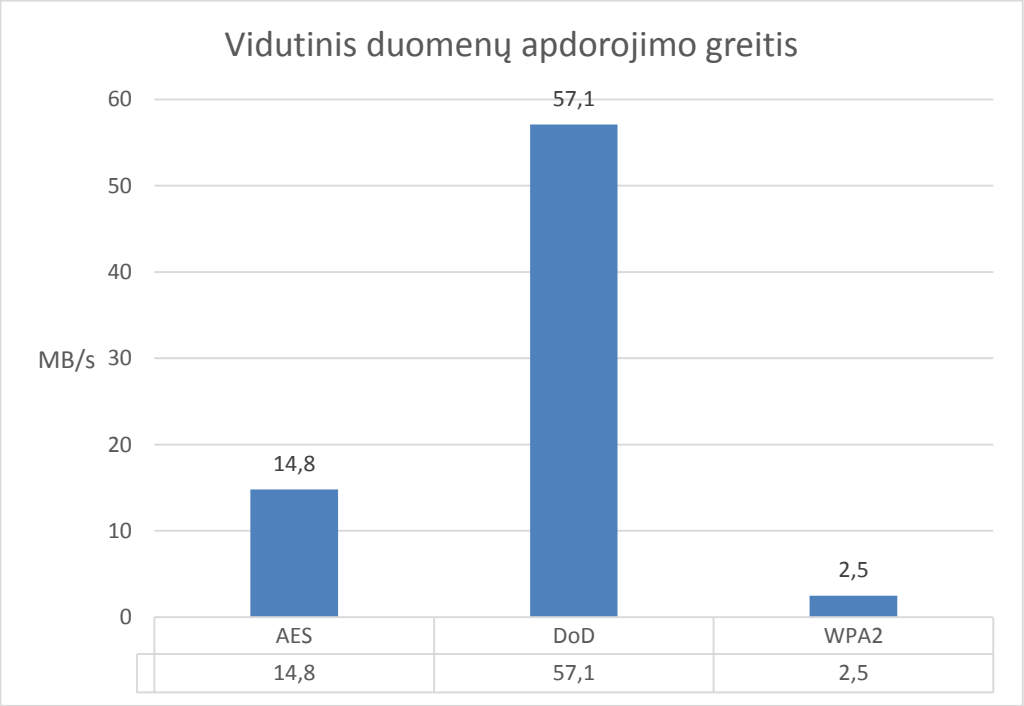
3.7 pav. Vidutiniai saugumo metodų duomenų kiekio apdorojimas vienam baterijos procentui.

3.8 paveikslėlyje pavaizduoti vidutiniai saugumo metodų baterijos energijos sąnaudos per 1 sekundę. Daugiausiai energijos reikalaujantis saugumo metodas yra AES šifravimo algoritmas, kuris sunaudoja 0,0162 %/s. Mažiausiai energijos suvartoja duomenų siuntimas belaidžiu ryšiu panaudojant WPA2-AES saugumo protokolą 0.00717 %/s, o tai 2,26 mažiau nei AES algoritmas. DoD trynimo algoritmas sunaudoja 0.0126 %/s.



3.8 pav. Vidutiniai saugumo metodų baterijos energijos sąnaudos per 1 sekundę.

Nors DoD trynimo algoritmas apdoroja 5,1 karto daugiau duomenų nei AES algoritmas tačiau, jis sunaudoja 1,29 kartus mažiau energijos per 1 sekundę ir 1,76 kartus daugiau nei duomenų siuntimas belaidžiu tinklu naudojant WPA2-AES protokolą.



3.9 pav. Vidutinis duomenų apdorojimo greitis (MB/s).

3.9 paveikslėlyje pavaizduotas vidutiniai duomenų apdorojimo greičiai per 1 sekundę. Sparčiausiais algoritmas DoD (57.1 MB/s) – 3,9 kartus spartesnis nei AES (14.8 MB/s) ir 22,8 kartus spartesnis nei duomenų siuntimas su WPA2-AES (2.5 MB/s) protokolu. AES šifravimo algoritmas 6 kartus spartesnis nei WPA2-AES protokolas.

Pagal gautą duomenų apdorojimo kiekį vienam baterijos energijos procentui galima apskaičiuoti kiek baterijos energijos prireiks apdoroti tam tikram duomenų kiekiui naudojant AES arba DoD algoritmą. Lentelė 3.10 parodo kiekvieno pasirinkto saugumo metodų energijos sąnaudas tam tikram duomenų kiekiui. Šviesiai žaliai pažymėti variantai įmanomi esant 20 % baterijos energijos.

Lentelė 3.10. AES ir DoD algoritmų energijos sąnaudos tam tikram kiekiui duomenų.

	20% baterijos įkrovimas				
	1GB	5 GB	10 GB	15 GB	20 GB
AES	1,2 %	6,0 %	12,0 %	18,0 %	24,0 %
DoD	0,2 %	1,2 %	2,3 %	3,5 %	4,7 %

Norint tiksliai apskaičiuoti duomenų siuntimo belaidžiu tinklu, naudojant WPA2 protokolą, energijos sąnaudas, reikia atsižvelgti į siuntimo greitį, apskaičiuojant visą siuntimo laiką ir jį padalinti iš siunčiamo dokumento dydžio. Lentelė 3.11 rodo duomenų siuntimo belaidžiu ryšiu su WPA2 saugos protokolu energijos sąnaudos tam tikram kiekiui duomenų, siunčiant duomenis tam tikru greičiu. Šviesiai žaliai pažymėti variantai įmanomi esant 20 % baterijos energijos.

Lentelė 3.11. Duomenų siuntimo belaidžiu ryšiu, naudojant WPA2-AES, energijos sąnaudos.

	20% baterijos įkrovimas				
	1 GB	**5 GB**	**10 GB**	**15 GB**	**20 GB**
1 MB/s	7,2	35,9	71,7	107,6	143.4
5 MB/s	1,4	7,2	14,3	21,5	28,7
10 MB/s	0,7	3,6	7,2	10,8	14,3

Tačiau reikia nepamiršti, kad esant tam tikram mobiliojo įrenginio baterijos energijos lygiui, kai kurios operacinės sistemos užmigdo įrenginį.

3.4. Eksperimentinio tyrimo išvados

Eksperimentui, su pasirinktais informacijos saugos metodais, parsisiųstas standartizuotas testavimui skirtas paveikslėlis „San Diego“ iš „University of Southern California“ svetainės (http://sipi.usc.edu/database/). Eksperimento metu energijos sąnaudų matavimai pakartoti tris kartus, visiškai iškraunat pilnai pakrautą bateriją.

Gauti eksperimento rezultatai parodė, daugiausiai duomenų apdoroja, iškraunant 1 % baterijos energijos, DoD trynimo algoritmas - 4,257 GB/%. Tuo tarpu AES apdoroja 5,2 kartus mažiau duomenų (0.834 GB/%) nei DoD, o duomenų siuntimas su WPA2-AES saugos protokolu – 12,1 karto mažiau (0.351 GB/%) nei DoD algoritmas.

Sparčiausiai iškraunantis bateriją saugumo metodas yra AES šifravimo algoritmas (0,0162 %/s), o tai yra 1,29 kartus daugiau nei DoD trynimo algoritmas (0.0126 %/s) ir 2,26 daugiau nei duomenų siuntimas naudojant WPA2-AES protokolą (0.00717 %/s).

Daugiausiai duomenų per 1 sekundę apdoroja DoD trynimo algoritmas, kuris 3,9 kartus spartesnis nei AES ir 22,8 kartus spartesnis nei duomenų siuntimas su WPA2-AES protokolu. AES šifravimo algoritmas 6 kartus spartesnis nei WPA2-AES protokolas.

Duomenų siuntimo belaidžiu ryšiu energijos sąnaudos nėra tiesiškai priklausomos nuo apdorotų (išsiųstų) duomenų. Be to skirtingų tyrimų metu gauti skirtingi rezultatai. Tačiau siunčiant duomenis gauta tiesinė energijos sąnaudų priklausomybė nuo siuntimo laiko. Taigi siunčiant duomenis, energijos sąnaudos gali būti apskaičiuotos žinant siuntimo laiką. O AES ir DoD algoritmų

energijos sąnaudas galima paskaičiuoti padauginus dokumento dydį iš vidutinio apdorotų duomenų kiekiui 1 % baterijos energijos.

Turint 20 GB duomenų ir esant 20% baterijos įkrovimui, galimas tik duomenų trynimi ir duomenų išsiuntimas į išorinę talpyklą esant 10 MB/s siuntimo greičiui.

4. IŠVADOS

- Populiarėjant asmeninių įrenginių naudojimui įmonėse, daug dėmesio skiriama duomenų saugumui. Tačiau duomenų užtikrinimo algoritmai sutrumpina ir taip jau trumpą baterijos iškrovimo laiką.
- Atlikus saugumo metodų analizę buvo pasirinktas AES šifravimo algoritmas, WPA2-AES belaidžio tinklo saugumo protokolas ir DoD 3 ciklų trynimo algoritmas. Šie variantai pasirinkti dėl patenkinamo saugumo lygio ir vidutinių energijos sąnaudų.
- Pasiūlytas asmeniniuose įrenginiuose duomenų saugumą užtikrinantis metodas, suteikiantis vartotojui galimybę saugiai apdoroti duomenis: užšifruojant AES algoritmu, talpinant nuotoliniame serveryje, siunčiant duomenis naudojant WPA2-AES saugumo protokolą; saugiai ištrinant iš kietojo disko panaudojant DoD 3 ciklų algoritmą.
- Atlikus eksperimentą su pasirinktais saugumo metodais paaiškėjo, jog daugiausiai duomenų apdoroja, iškrovus 1 % baterijos energijos, DoD trynimo algoritmas - 4,257 GB/%, AES apdoroja 5,2 kartus mažiau duomenų (0.834 GB/%), o duomenų siuntimas su WPA2-AES saugos protokolu – 12,1 karto mažiau (0.351 GB/%). Tuo tarpu sparčiausiai iškraunantis bateriją saugumo metodas yra AES šifravimo algoritmas (0,0162 %/s), o tai yra 1,29 kartus daugiau nei DoD trynimo algoritmas (0.0126 %/s) ir 2,26 daugiau nei duomenų siuntimas naudojant WPA2-AES protokolą (0.00717 %/s).
- Pagal pasiūlytą metodiką, turint 20 GB duomenų ir esant 20% baterijos įkrovimui, galimi tik duomenų trynimas ir duomenų išsiuntimas į išorinę talpyklą esant 10 MB/s siuntimo greičiui.

5. LITERATŪRA

[1] B. Danyl, „Mobile Internet trends 2014 by Mary Meeker,“ [Tinkle]. Available: http://www.smartinsights.com/digital-marketing-strategy/internet-trends-2014-mary-meeker/. [Kreiptasi 11 3 2016].

[2] Statista, „Shipment forecast of tablets, laptops and desktop PCs worldwide from 2010 to 2019 (in million units),“ [Tinkle]. Available: http://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/. [Kreiptasi 11 3 2016].

[3] D. Jevans, „(BYOD), The Beginners Guide to Bring Your Own Device,“ [Tinkle]. Available: http://www.marblesecurity.com/2014/04/29/byod-best-practices/. [Kreiptasi 11 03 2016].

[4] T. Kaneshige, „BYOD Users Work Longer and Earlier,“ [Tinkle]. Available: http://www.cio.com/article/2449817/byod/byod-users-work-longer-and-earlier.html. [Kreiptasi 11 03 2016].

[5] „iPhone,“ [Tinkle]. Available: https://en.wikipedia.org/wiki/IPhone. [Kreiptasi 11 03 2016].

[6] D. P. H. i. D. H. Zervos, „Batteries, Supercapacitors, Alternative Storage for Portable Devices 2009-2019,“ [Tinkle]. Available: http://www.idtechex.com/users/action/dl.asp?documentid=3825#sthash.NDTqNldZ.dpuf. [Kreiptasi 11 03 2016].

[7] D. S. D. T. A. Penrig, „ELK, a new protocol for efficient large-group key distribution,“ [Tinkle]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=924302. [Kreiptasi 11 03 2016].

[8] N. M. T. M. Jun Anzai, „A Quick Group Key Distribution Scheme with “Entity Revocation”,“ [Tinkle]. Available: http://link.springer.com/chapter/10.1007/978-3-540-48000-6_27. [Kreiptasi 11 03 2016].

[9] E. Neidhardt, „Asymmetric Cryptography for Mobile Devices,“ [Tinkle]. Available: https://www.snet.tu-berlin.de/fileadmin/fg220/courses/WS1112/snet-project/asymmetric-cryptography_neidhardt.pdf. [Kreiptasi 11 03 2016].

[10] Scott Fluhrer, Itsik Mantin, Adi Shamir., „Weaknesses in the Key Scheduling Algorithm of RC4,“ [Tinkle]. Available: https://www.cs.cornell.edu/people/egs/615/rc4_ksaproc.pdf. [Kreiptasi 11 03 2016].

[11] G. Lehembre, „Wi-Fi security – WEP, WPA,“ *Hervé Schauer Consultants,* pp. 1-15, 2005.

[12] Swati Sukhija, Shilpi Gupta, „Wireless Network Security Protocols,“ *International Journal of Emerging Technology and Advanced Engineering,* t. 3, nr. 2, pp. 357-364, 2012.

[13] F. H. Katz, „WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?,“ [Tinkle]. Available: http://infotech.armstrong.edu/katz/katz/Frank_Katz_CSC2010.pdf. [Kreiptasi 12 03 2016].

[14] P. Arana, „Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2),“ [Tinkle]. Available: http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf. [Kreiptasi 12 03 2016].

[15] L. M. G. F. E. S. S. S. Michael Wei, „Reliably Erasing Data From Flash-Based Solid State Drives,“ [Tinkle]. Available: https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf. [Kreiptasi 11 03 2016].

[16] D. Naunikas, „Energijos suvartojimo naudojant kriptografinius servisus delniniuose kompiuteriuose tyrimas,“ [Tinkle]. Available: http://vddb.library.lt/fedora/get/LT-eLABa-0001:E.02~2010~D_20100813_142604-69566/DS.005.0.02.ETD. [Kreiptasi 11 03 2016].

[17] I. Gudaitytė, „Delninukų bevielio ryšio saugos protokolų tyrimas,“ [Tinkle]. Available: https://oatd.org/oatd/record?record=oai%5C%3Aelaba.lt%5C%3ALT-eLABa-0001%5C%3AE.02%5C~2011%5C~D_20110831_115317-95358. [Kreiptasi 11 03 2016].

[18] „Softonic,“ [Tinkle]. Available: http://virtualrouter-plus.en.softonic.com/. [Kreiptasi 2 4 2016].

[19] V. Neverdauskaitė, „LABA,“ 27 05 2013. [Tinkle]. Available: http://vddb.laba.lt/fedora/get/LT-eLABa-0001:E.02~2013~D_20130821_153046-89372/DS.005.0.01.ETD. [Kreiptasi 06 04 2016].