KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Arvydas Bubnys

ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ PRIEIGAI PRIE ĮMONĖS INFORMACIJOS, SAUGOS PROBLEMŲ TYRIMAS

Baigiamasis magistro darbas

Vadovas
Doc. dr. J. Toldinas

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ PRIEIGAI PRIE ĮMONĖS INFORMACIJOS, SAUGOS PROBLEMŲ TYRIMAS

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

Vadovas
(parašas) Doc. dr. J. Toldinas
(data)

Recenzentas
(parašas) Doc. dr. S. Maciulevičius
(data)

Projektą atliko
(parašas) Arvydas Bubnys
(data)

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos fakultetas

(Fakultetas)

Arvydas Bubnys

(Studento vardas, pavardė)

M4096N21 Informacijos ir informacinių technologijų sauga (kodas 621E10003)

(Studijų programos pavadinimas, kodas)

„Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos problemų tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 17 m. gegužės 22 d.

Kaunas

Patvirtinu, kad mano **Arvydo Bubnio** baigiamasis projektas tema „Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos problemų tyrimas“ 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)*

Bubnys, A. „ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ PRIEIGAI PRIE ĮMONĖS INFORMACIJOS, SAUGOS PROBLEMŲ TYRIMAS“. Magistro baigiamasis projektas / vadovas doc. dr. Jevgenijus Toldinas; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra. Kaunas, 2017. 54 p.

SANTRAUKA

Dabartinės skaitmeninių įrenginių technologijos leidžia lanksčiai taikyti įmonės ir asmeninių įrenginių naudojimą darbe ir asmeniniams poreikiams. Šiuo metu vis labiau plintanti metodika BYOD (angl. Bring Your Own Device arba atsinešti savo įrenginį į darbo vietą) yra viena iš populiariausių modelių, teikiant įmonėms mobilumą ir lankstumą darbo vietose. Atsiradus naujoms technologijoms ir mobiliųjų įrenginių funkcijoms, jų saugus naudojimas tampa labai svarbus kasdieninėje veikloje. Naudojant asmeninius įrenginius darbo vietoje mobiliųjų įrenginių saugumas tampa ypač svarbus, kadangi vis daugiau darbuotojų naudoja savo mobiliuosius įrenginius norėdami prieiti prie organizacijos duomenų ir sistemų.

Asmeninių įrenginių naudojimas darbo vietoje leidžia darbuotojams atsinešti savo įrenginius, pavyzdžiui, nešiojamuosius kompiuterius, išmaniuosius telefonus ir/ar planšetinius kompiuterius darbui ir prijungti juos į organizacijos tinklą, nenaudojant įmonei priklausančių įrenginių. Darbuotojams yra nepatogu, kai jie darbui turi naudoti įmonės skirtus, o ne asmeninius mobiliuosius įrenginius. Asmeninių įrenginių naudojimo įmonėje reikšmė - darbuotojai yra labiau susipažinę su konkrečiu asmeniniu įrenginiu ir patenkinti naudodami savo įrenginį (-ius), o darbdaviai sutaupo pinigų nemokėdami už brangius įrenginius.

Magistrinio darbo objektas - asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistema.

Šio darbo struktūra:

- Pirmoje darbo dalyje pateikiama asmeninių įrenginių, naudojamų įmonėse, saugos modelių analizė, asmeninių įrenginių, naudojamų įmonėse, rizikos analizė. Taip pat šioje dalyje pateikiama asmeninių įrenginių, naudojamų įmonėse, saugumo modelių funkcijų analizė.
- Antroje darbo dalyje pateikiama asmeninių įrenginių, naudojamų prieigai prie įmonės dokumentų failų, saugos sistemos vizija, modelis, architektūra, veikimo principai ir sistemos prototipas.
- Trečioje darbo dalyje pateikiamas eksperimento tyrimas ir jo rezultatai.
- Darbo pabaigoje pateiktos išvados.

Surname, Name. *Title of the Project (Each Word of the Title is Written in Capital Letters)*: *Master's* thesis in PERSONAL DEVICES USED TO ACCESS THE COMPANY'S INFORMATION SAFETY PROBLEM research / supervisor assoc. prof. Jevgenijus Toldinas. The Faculty of Informatics, Kaunas University of Technology.

Research area and field:

Key words:

Kaunas, 2017. 54 p.

SUMMARY

Current digital device technology allows flexibility for companies and personal devices for work and personal needs. Currently, the increasingly pervasive methodology BYOD or bring your own device to work place is one of the most popular models, providing businesses the mobility and flexibility in the workplace. The emergence of new technologies and mobile devices, their safe use becomes very important in everyday activities. The use of personal devices in the workplace mobile device security becomes especially important, since more and more employees use their mobile devices to access the organization's data and systems.

The use of personal devices in the workplace allows employees to bring their own devices, such as laptops, smartphones and / or tablet computers at work and connect them to the organization's network, without the use of company-owned facilities. Workers are uncomfortable when their work must be done using the organization device, not private mobile devices. Personal devices in the enterprise value is that the staff are more familiar with the specific personal devices and satisfied using your device (s), while employers save money by not paying for expensive equipment.

The Object - personal devices used to access the company's information security system.

The structure of this work:

- The first work part is the Analysis of personal devices used by businesses, Safety Model Analysis of personal devices used in enterprises and Risk Analysis. Also in this part is the analysis of the personal devices used in enterprises and security model functions.
- The second work part is the personal devices used for access to the company's document files, security systems Vision, Model, Architecture, principles and system prototype.
- The third part is the experimental research and its results.
- In the end, the conclusion.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

DFSS	Dokumentų failų saugos sistema
MDM	Mobiliųjų įrenginių valdymas (*angl. Mobile Device Management*)
MAM	Mobiliųjų programėlių valdymas (*angl. Mobile Application Management*)
MIM	Mobiliosios informacijos valdymas (*angl. Mobile Information Management*)
BYOD	Atsinešk savo asmeninį įrenginį (*angl. Bring Your Own Device*)
AĮ	Asmeninis įrenginys
NFC	Ryšių mažame lauke technologija (*angl. Near Field Communication*)
TCP	Standartinis duomenų perdavimo protokolas (*angl. Transmission Control Protocol*)
HTTP	Tai užklausimo - atsakymo protokolas, jungiantis klientą ir serverį (*angl. Hypertext Transfer Protocol*)
HTTPS	Apsaugotas HTTP protokolas (*angl. Hypertext Transfer Protocol Secure*)
PLM	Produkto gyvavimo ciklo valdymas (*angl. Product Line Management*)
IT	Informacinės technologijos
ASĮ	Atsinešk savo įrenginį
EMM	Įmonių mobilus valdymo modelis (*angl. Enterprise Management Model*)
OS	Operacinė sistema
DoD	Amerikos apsaugos departamentas (*angl. Department of Defense*)

ĮVADAS

Dabartinės skaitmeninių įrenginių technologijos leidžia lanksčiai taikyti įmonės ir asmeninių įrenginių naudojimą darbe ir asmeniniams poreikiams. Lankstumas įgalina gauti tiek ekonominės naudos, tiek taupyti laiką atliekant įvairius darbus. Šiuo metu vis labiau plintanti metodika BYOD (angl. BringYourOwnDevics arba atsinešti savo įrenginį į darbo vietą) yra viena iš populiariausių modelių, teikiant įmonėms mobilumą ir lankstumą darbo vietose. Atsiradus naujoms technologijoms ir mobiliųjų įrenginių funkcijoms, jų saugus naudojimas kasdieninėje veikloje tampa labai svarbus. Mobilūs įrenginiai nėra gerai apsaugoti, lyginant su kompiuteriais ir kompiuterių tinklais, ir vartotojai mažiau dėmesio kreipia į saugumo atnaujinimus ir saugumo sprendimus. Naudojant asmeninius įrenginius darbo vietoje mobiliųjų įrenginių saugumas tampa ypač svarbus,[1] kadangi vis daugiau darbuotojų naudoja savo mobiliuosius įrenginius norėdami prieiti prie organizacijos duomenų ir sistemų. Šioje dalyje pateikiama dabartinė BYOD saugumo apžvalga.

Asmeninių įrenginių naudojimas darbo vietoje leidžia darbuotojams atsinešti savo įrenginius, pavyzdžiui, nešiojamuosius kompiuterius, išmaniuosius telefonus ir/ar planšetinius kompiuterius darbui ir prijungti juos į organizacijos tinklą, nenaudojant įmonei priklausančių įrenginių. Daugybė kompanijų ir organizacijų ėmėsi iniciatyvos priimdami naudoti asmeninius įrenginius įmonėse: „Intel“, „CitrixSystems“, „Unisys“, JAV Baltieji rūmai, „Apple“ [1].

Asmeninių įrenginių naudojimo įmonėje reikšmė - darbuotojai yra labiau susipažinę su konkrečiu asmeniniu įrenginiu ir patenkinti naudodami savo įrenginį (-ius), o darbdaviai sutaupo pinigų nemokėdami už brangius įrenginius. Įmonių, kurios darbui taiko ASĮ, tikslai: padidinti prietaisų lankstumą, patogumą ir mobilumą siekiant patenkinti savo darbuotojų profesinius poreikius, kurie didina įmonių produktyvumą ir moralę [1].

Perėjimas prie asmeninių įrenginių naudojimo organizacijose pagerina tris pagrindinius veiksnius: darbuotojų elgesio kodeksą, apsaugos programų diegimą ir efektyvų taisyklių valdymą [1]. Visi šie veiksniai yra atsakingi už bendrą efektyvumą naudojant asmeninius įrenginius.

1. ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE, SAUGOS PROBLEMŲ ANALIZĖ

Šiandien esant daugybei saugumo grėsmių mobilieji įrenginiai vis dar turi saugumo spragų, kurias gali išnaudoti piktavaliai. Tačiau organizacijose, kuriose tai leidžiama, darbuotojai gali atsinešti ir naudoti darbo uždaviniams spręsti asmeninius mobiliuosius įrenginius (*angl. Bring Your Own Device* (BYOD)). Kaip mobiliųjų įrenginių pažeidžiamumo atvejus, galima paminėti šiuos: pavogti ar pamesti įrenginiai, neteisinga vartotojų elgsena [1]. Todėl iškyla konfidencialios informacijos praradimo ar vagystės grėsmės.

Magistro darbo tyrimo objektas – organizacijos dokumentų failai, kurie saugomi organizacijos serveriuose, ir kuriems priskirti įvairūs slaptumo lygiai.

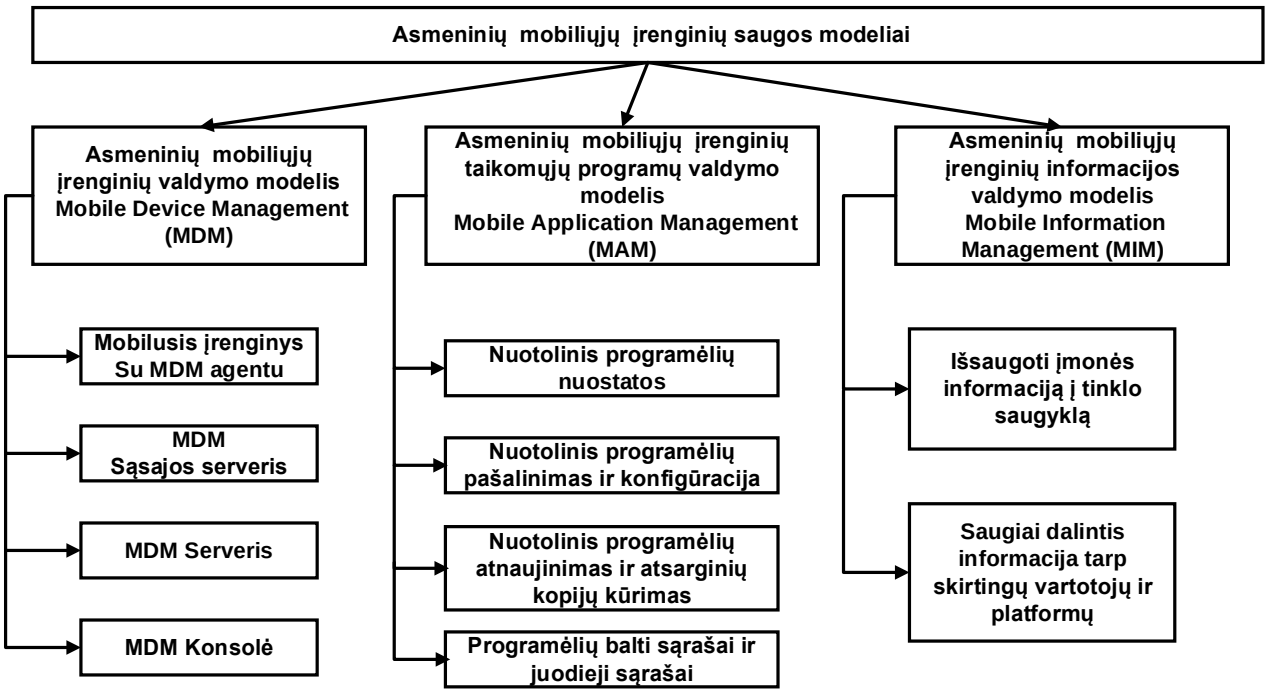
Magistro darbo tyrimo sritis – saugus dokumentų valdymas organizacijose priklausomai nuo slaptumo lygio.

Saugos problemos apibrėžimas – situacija, kai leidžiama naudotis asmeniniais įrenginiais ir dirbti organizacijos viduje, tuomet asmeninių įrenginių naudotojai parsisiunčia ir išsaugo savo įrenginiuose įvairius organizacijos dokumentus, kurie būdami tam tikro slaptumo lygio negali būti naudojami už organizacijos ribų.

1.1. Asmeninių įrenginių, naudojamų įmonėse, saugos modeliai

Šiuo metu yra trys pagrindiniai asmeninių įrenginių organizacijose saugumo modeliai (1.1 pav.):

- Mobile Device Management (MDM) – mobiliųjų įrenginių valdymas:
  - Mobilusis įrenginys su mobiliųjų įrenginių valdymo agentu;
  - Mobiliųjų įrenginių valdymo sąsajos serveris;
  - Mobiliųjų įrenginių valdymo konsolė arba valdymo skydas.
- Mobile Application Management (MAM) – mobiliųjų programėlių valdymas:
  - Nuotolinis programėlių valdymas;
  - Nuotolinė programėlių konfigūracija ir pašalinimas;
  - Nuotolinis programėlių atnaujinimas ir atsarginių kopijų kūrimas;
  - Programėlių baltieji ir juodieji sąrašai.
- Mobile Information Management (MIM) – mobiliosios informacijos valdymas:
  - Įmonės informacijos išsaugojimas tinklo saugykloje;
  - Saugus dalinimasis informacija tarp skirtingų vartotojų ir platformų.

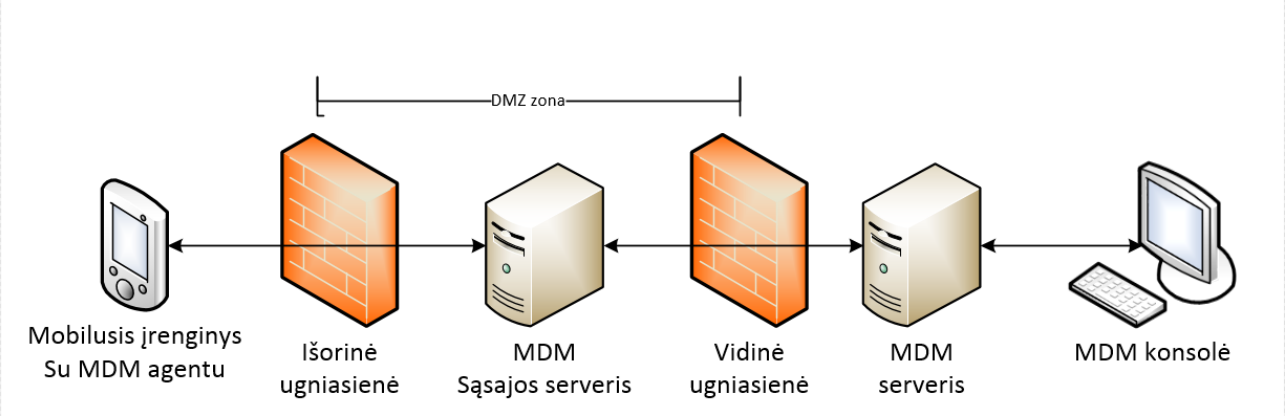


1.1 pav. Asmeninių įrenginių, naudojamų įmonėse, saugumo modeliai

1.2. Asmeninių įrenginių, naudojamų įmonėse, valdymas

MDM sistemos nuotoliniu būdu stebi mobiliųjų įrenginių būseną, siekdamos kontroliuoti įrenginių funkcijas. MDM sudarytas iš dviejų pagrindinių komponentų: MDM agento ir MDM serverio. MDM agentas yra programa, kuri yra įdiegiama į mobiliuosius prietaisus ir siunčia savo statusą ir duomenis į MDM serverį [1]. MDM serveris valdo gautus duomenis ir pagal juos vykdo komandas registruotuose mobiliuose įrenginiuose - užrakinimą, kontrolę, šifravimą ir vykdymo politiką [2].

MDM sistemos susideda iš keleto komponentų: MDM serverio, sąsajos serverio, MDM konsolės ir mobiliojo prietaiso su valdymo agentu. Valdymo agentas yra programinės įrangos valdymo agentas, kuris gali būti įdiegtas į mobiliuosius įtaisus [3, 4]. 2 pav. pavaizduota bendrinė MDM architektūros schema įmonės tinkle.



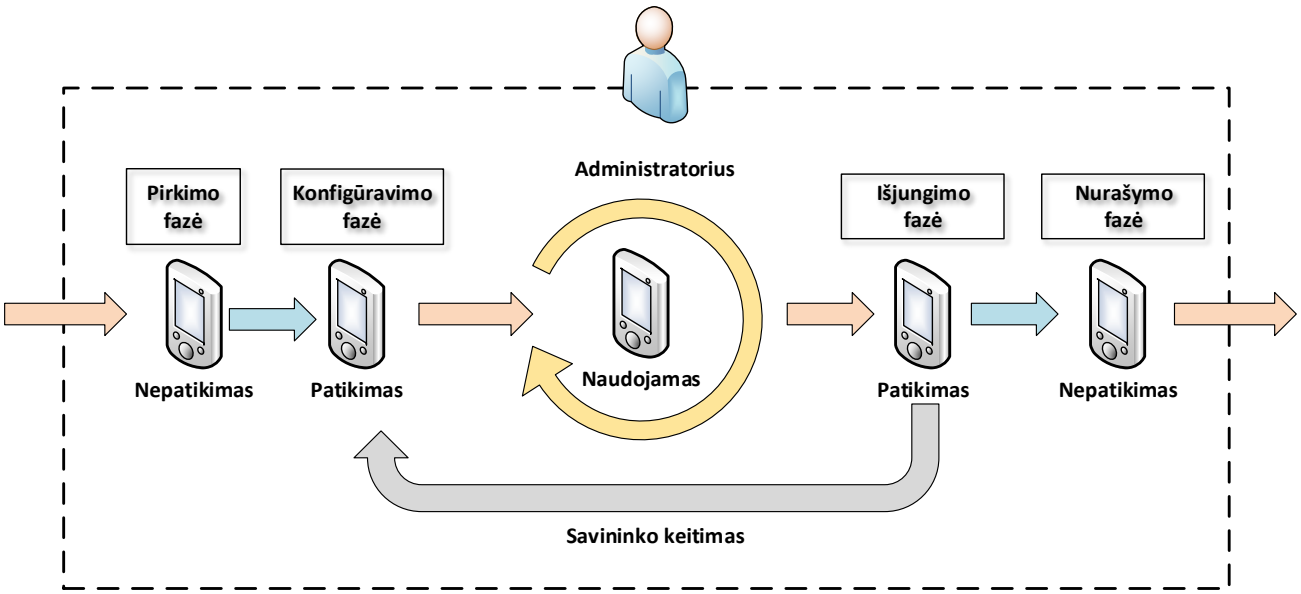
1.2 pav. Bendrinė MDM architektūros schema

Minėtoje architektūroje programinė įranga, vadinama agentu, yra platinama per trečiosios šalies terpę - programėlių parduotuvę arba kitas programėles, ir įdiegiama į mobilųjį prietaisą [3]. Pagrindinis agento tikslas yra pervesti mobiliojo prietaiso duomenis ir vartotojo informaciją į MDM serverį ir taikyti atitinkamas politikos taisykles ir administracinius veiksmus, kaip, pavyzdžiui, nuotolinis ištrynimas [5].

MDM sprendimas susideda iš pagrindinių komponentų, kurie valdo protokolus, teikia nuolatinę kontrolę ir stebėseną. Sprendimas priklausomas nuo įmonės tinklo ir remiasi sertifikatų apsikeitimu autentifikuoti ir bendrauti su MDM agentais, kurie yra įdiegti į mobiliuosius įrenginius. MDM naudojama taikant ASĮ įmonės ir verslo įgyvendinimo strategiją, kuri reikalauja centralizuoto supaprastinto sprendimo, leidžiančio įmonėms ir organizacijoms griežtai kontroliuoti mobiliuosius įrenginius [17]. MDM pagrindiniai komponentai yra bendrauti su MDM agentu mobiliuosiuose įrenginiuose, vykdyti prieigos teises, atnaujinimus, sinchronizuoti failus, suteikti nuotolinį valymą, leisti VPN atlikti kenkėjiškų programų valymą ir teikti veiklos ataskaitas [17]. MDM yra geras sprendimas darbuotojui priklausantiems įrenginiams, jeigu darbuotojai sutinka su sąlygomis, susijusiomis su šia technologija. Kadangi dabar vartotojai naudoja savo prietaisus, jie nori turėti asmeninių programėlių ir daryti daug asmeninių dalykų, dėl kurių yra būtina taikyti ASĮ. Su MDM programinė įranga yra šiek tiek sunkiau modifikuojama ir apribota vartotojams.

Produkto gyvavimo ciklo valdymas (PLM) [29] yra išsami informacijos sistema, kuri koordinuoja visus produkto aspektus nuo pradinio projektavimo iki galutinio pašalinimo (1.3 pav.). Produkto gyvavimo ciklas yra gerai apibrėžtas produktų, procesų ir paslaugų, bet jo standartizacijos daugelyje saugumo procesų, kur yra naudojami mobilieji įrenginiai, vis dar neapibrėžtos. Organizacijos negali dalyvauti kiekviename mobiliojo prietaiso valdymo gyvavimo cikle; įgyvendinimo laikotarpis prasideda nuo OEM (Original Equipment Manufacturer) pirkimo ir tęsiasi iki galutinio nurašymo. Mobiliojo prietaiso saugus gyvavimo ciklo valdymas skirstomas į penkis etapus:

1. Pirkimo etapas;
2. Konfigūracijos etapas;
3. Naudojimosi etapas;
4. Išjungimo etapas;
5. Nurašymo etapas.



1.3 pav. Produkto gyvavimo ciklo valdymas

Gyvavimo cikle mobilus įrenginys gali būti vienos iš trijų skirtingų būsenų: nepatikima, patikima ir naudojama nuosavybė.

Kai prietaisas yra nepatikimos būsenos, nei organizacija, nei kas nors iš jos darbuotojų negali būti laikomi atsakingi už tą įrenginį. Kai prietaisas yra pažymimas nepatikimu, jokie svarbūs organizacijos duomenys negali būti saugomi ir prietaisas negali būti prijungtas prie verslo tinklų. Kai prietaisas yra patikimos būsenos, tik organizacija yra atsakinga už tą įrenginį. Šios būsenos prietaisas gali saugoti jautrius verslo duomenis (pvz.: įmonių kontaktų knygos, verslo tinklo profiliai). Nors prietaisas yra patikimas, jokie asmeniniai duomenys negali būti saugomi įrenginio atmintyje. Pati sudėtingiausia būsena yra priklausančių naudojamų įrenginių būsena. Toks mobilusis įrenginys yra duodamas organizacijos darbuotojui, kuris yra atsakingas už šį įrenginį. Naudojamas įrenginys paprastai gali saugoti tiek verslo, tiek ir asmeninę informaciją, jeigu priklausantis prietaisas atitinka pageidaujamus saugumo ir privatumo tikslus siekiant apsaugoti bendrovės turtą.

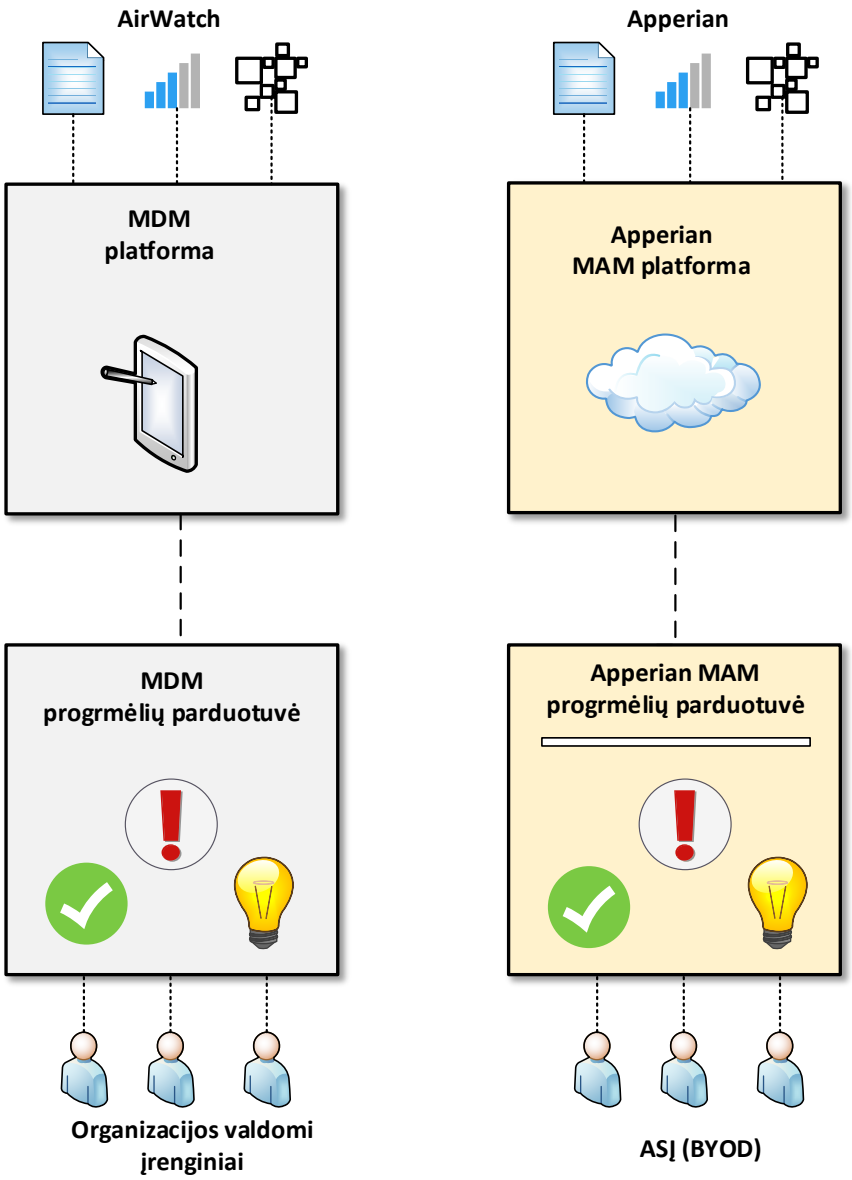
1.3. Asmeninių įrenginių, naudojamų įmonėse, mobiliųjų programėlių valdymas

MAM sistema yra sprendimas, naudojamas IT administratorių, siekiant nuotoliniu būdu įdiegti, atnaujinti, ištrinti, vesti auditą ir stebėti su įmone susijusias programėles mobiliuosiuose įrenginiuose, todėl MAM funkcijos gali būti apibendrintos taip [6]:

- Nuotolinės programėlių nuostatos;
- Nuotolinis programėlių pašalinimas ir konfigūracija;
- Nuotolinis programėlių atnaujinimas ir atsarginių kopijų kūrimas;
- Programėlių baltieji ir juodieji sąrašai.

Skirtingai nei MDM, kuris kontroliuoja mobiliuosius prietaisus aparatūros lygyje, mobiliųjų programėlių valdymo sistemos stebi ir kontroliuoja tam tikras programas siekdamos, kad būtų laikomasi organizacijos politikos ir reikalavimų. Pavyzdžiui, organizacijos gali naudoti MAM siekdamos apriboti programėles, susijusias su įmone, palikdamos kitą informaciją atvirai naudoti kitiems vartotojams [7].

MAM yra mobiliųjų programėlių valdymas, kuris yra alternatyva MDM (mobiliųjų įrenginių valdymui), tačiau jis skirtas riboti mobiliųjų įrenginių naudotojų prieigą prie programų ir apsaugoti leidžiamas programas ir duomenis, kurie naudojami mobiliajame įrenginyje [21]. MAM leidžia organizacijoms taikyti saugumo politiką, užrakinti, nustatyti prieigos kontrolės taisykles, konfigūruoti programinės įrangos veikimą, nuotoliniu būdu trinti programėles pagal savo kontrolę, riboti prieigą prie neleistinų programų ir įdiegti leidžiamas programėles [17]. Vienas iš MAM programėlių saugumo metodų, padedančių valdyti duomenų nutekėjimą pašaliniams žmonėms yra juodojo sąrašo politika mobiliųjų programėlėms, kuri leidžia prietaiso programėlių ištrynimą arba užblokavimą, kai sistema aptinka juodajame sąraše esančią programą [22].



1.4 pav. AirWatch ir Apperian valdymo metodų pavyzdys

Organizacijų Mobilus valdymas (1.4 pav.) remiasi dviem metodais. Pirmasis yra organizacijai priklausančiais įrenginiais naudojamas AirWatch sprendimas valdyti įrenginius ir programas. Bet taikant ASĮ vartotojai naudoja Apperian sprendimą, kuris reikalingas parsisiųsti saugos politikos valdomas programėles ar įrenginius, kurie nėra įtraukti į MDM profilį. Abu sprendimai veikia nepriklausomai vienas nuo kito. Bet turi nuoseklią saugumo savybę - suteikia organizacijoms galimybę lanksčiai palaikyti įvairių tipų įrenginius toje pačioje darbo aplinkoje, nepriklausomai nuo to, kam priklauso įrenginys [23]. Aukščiau pateiktas paveikslėlis parodo, kodėl reikia naudoti atskirą MAM modelį, nes nepakanka vien tik MDM modelio įdiegti mobiliąsias programas, kad apsaugotume darbuotojus.

MAM modelis yra naudojamas IT administratorių tikslu nuotoliniu būdu įdiegti, atnaujinti, vesti auditą ir stebėti organizacijos programėles mobiliuosiuose įrenginiuose [1]. Kitos programėlės išsiskiria iš MAM modelio programėlių ribos, nes yra asmeninės ir priklauso nuo vartotojo kontrolės. MAM modelis yra efektyvesnis, kai yra derinama su konteinerių modeliu. Atliekant nuotolinį trynimą, organizacija gali tiesiog ištrinti organizacijos programas ir duomenis, tačiau vartotojo asmeniniai duomenys ir programos lieka. Naudojant MAM, organizacija neturi jokių teisių stebėti vartotojo įrenginio veiklos už jų programėlės ribų [1, 22].

1.4. Asmeninių įrenginių, naudojamų įmonėse, informacijos valdymas

Įmonės gali pasinaudoti nauju saugumo modeliu, vadinamu MIM. Kritinė įmonių informacija yra nesaugojama mobiliuosiuose įrenginiuose. Pagrindinis MIM tikslas yra išsaugoti įmonės informaciją tinklo saugykloje (pvz: privatus debesis) ir saugiai dalintis informacija tarp skirtingų vartotojų ir platformų. MIM leidžia kontroliuoti ir valdyti tik ribotą patikimų programų kiekį ir šifruotus įmonių duomenis [2].

Nepriklausomai nuo privalumų ir trūkumų minėti saugumo modeliai orientuojasi tik į ribotus sprendimus ir apsaugą ir tik į įrenginių valdymą (MDM), programėles (MAM) ir informaciją (MIP), remiantis tam tikra politika [8].

MIM reiškia Mobiliosios informacijos valdymą, kuris suteikia galimybę sinchronizuoti failus ir dokumentus tarp įvairių prietaisų serveryje ir tuo pačiu metu administruoti saugumo procedūras, tokias kaip kenkėjiškų programų skenavimas [17]. Duomenys saugomi paslaugų teikėjo serveryje (debesyje) ir klientas gali prisijungti tiesiogiai arba per prieigą vieno iš prietaisų su programine įranga. MIM negali pritaikyti kliento programėlių prietaisui, todėl MIM veikia su MDM arba MAM, kad pritaikytų programėles mobiliajame įrenginyje. Taikant ASĮ modelius, tokius kaip MDM, MAM ir MIM, kurie teikia esminius sprendimus, kaip gali būti panaudojami mobilūs prietaisai ir kaip gali būti pasiekiami duomenys, skiriamos keturios pagrindinės kategorijos:

- Identifikavimas ir prieigos kontrolė
- Duomenų apsauga
- Programėlių saugumas ir vientisumas
- Atitiktis

Aukščiau pateiktos technikos, atsakingos už mobiliųjų įrenginių, programų ir informacijos valdymą, nepakanka, nes mobiliųjų įrenginių tinklai yra taikiniai, todėl yra daugiau technikų imtis kontroliuoti mobiliojo prietaiso saugumą.

Naudojimasis asmeniniu įrenginiu darbo vietoje apima daug funkcinių sričių organizacijos viduje, įtraukiant žmogiškuosius išteklius, teisę, IT, finansus ir jų operacijas [1, 6]. Asmeninių įrenginių naudojimo organizacijose iššūkiai gali būti vertinami iš įvairių perspektyvų, imant tiek organizacines, tiek technines. Tai duoda keletą kontrolės savybių taikant asmeninius įrenginius, kurie susiję su duomenų kontroliavimu, prieigos kontrole, tinklų kontroliavimu ir įrenginių valdymu, taip pat sukurti saugos politiką ir procedūras [11, 12]. Nors daugelis gamintojų taiko techninius sprendimus norėdami valdyti asmeninius įrenginius įmonėse, tačiau šie techniniai sprendimai negali išspręsti saugumo ir privatumo problemų [11, 13].

Informacijos saugumo ir privatumo politikos įgyvendinimas yra pagrindinė kontrolė, kurios reikalaujama naudojant asmeninius įrenginius įmonės aplinkoje, nes ji taip pat gali įtraukti arba palaikyti kitas kontroles [10].

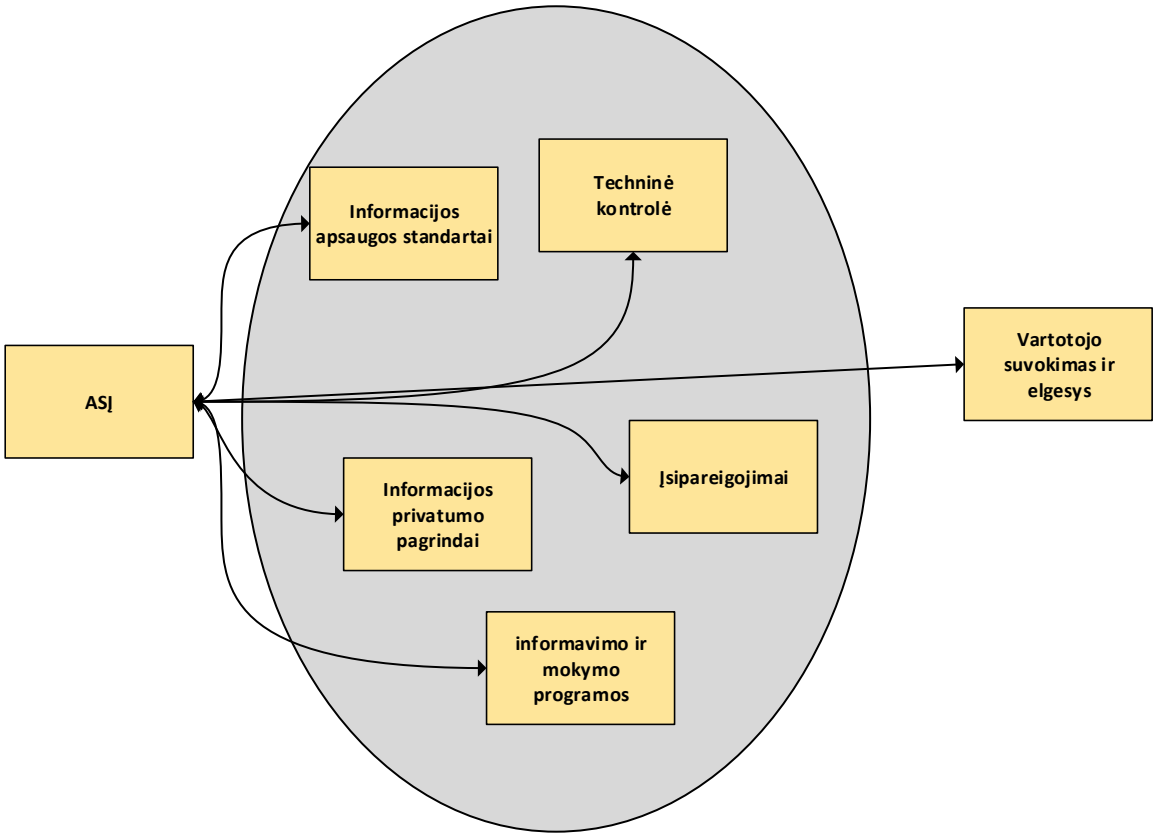
Tačiau prieš kuriant ir taikant asmeninių įrenginių įmonėse politiką, turi būti apsvarstyti keli klausimai, susiję su juridiniais ir atsakomybės aspektais, procedūromis ir techninės kontrolės priemonėmis, kurių reikia įdarbinant.

Sprendžiant šias problemas, siūloma taikyti valdymo modelį, pagrįstą asmeninių įrenginių įmonėse politika, kuris rekomenduoja šešis kontrolės komponentus, kurių turėtų būti laikomasi:

- Informacijos saugumo standartai ir procedūros;
- Informacijos privatumo principai;
- Informacijos saugumo ir privatumo techninė kontrolė;
- Įsipareigojimai;
- Supratimas ir mokymo programa;
- Asmeninių įrenginių vartotojo suvokimas ir elgesys.

Šie komponentai yra atrinkti remiantis indikacijomis iš informacijos saugumo ir privatumo srities[14, 15], todėl jie yra svarbūs bandant pasiekti aukštą duomenų apsaugos lygį organizacijose. Asmeninių įrenginių įmonėse politika pagrįstas valdymo modelis(1.5 pav.), patikrina kiekvieną komponentą nustatant tinkamas kontrolės priemones, kurios gali būti naudojamos taikant asmeninių

įrenginių įmonėse politiką. Ryšių analizė tarp komponentų yra skirta išlaikyti pusiausvyrą tarp saugumo ir privatumo, todėl siekiama nustatyti tokias kontrolės priemones, kurios nepaveiktų organizacijų ir darbuotojų naudojimosi patirties taikant asmeninius įrenginius.

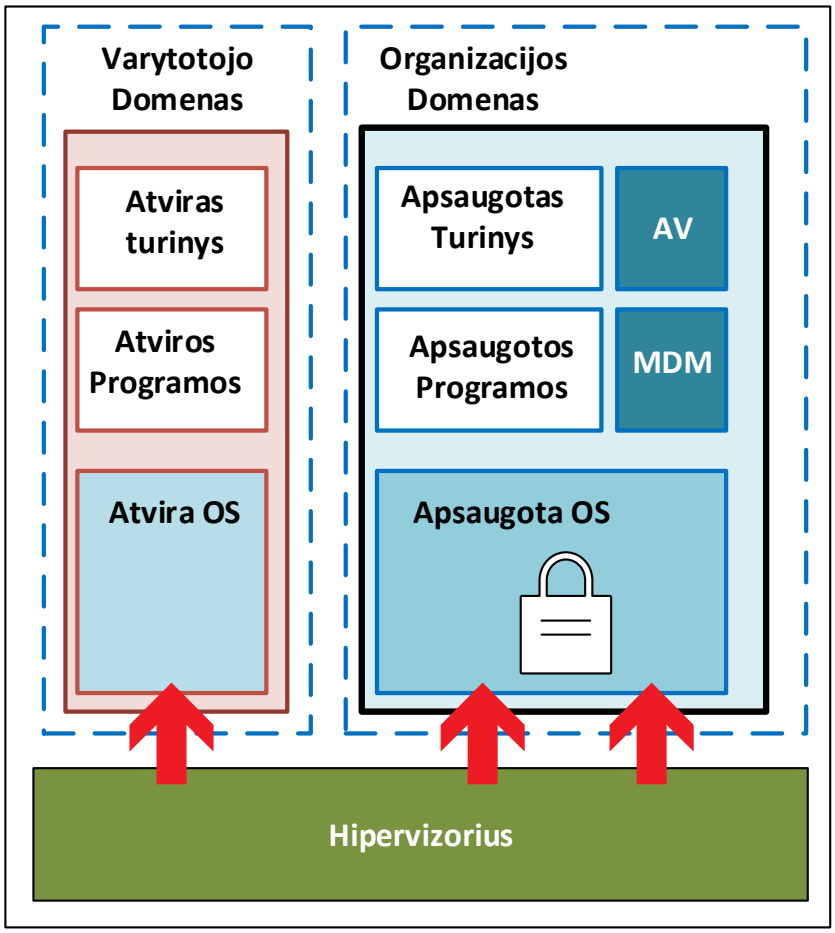


1.5 pav. Asmeninių įrenginių įmonėse politika pagrįstas valdymo modelis

1.5. Mobilios virtualizacijos modelis

Virtualizacija yra sukurti virtualią kopiją, įskaitant OS, aparatūros platformą, saugojimo ir kompiuterių tinklo įrenginius ir pritaikyti juos prie stalinio, nešiojamo, planšetinio kompiuterio arba prie išmaniojo telefono. Kompiuterių ir programų virtualizacija yra auganti tendencija, kylanti iš poreikio sumažinti išlaidas ir pagerinti saugumą bei IT paslaugų prieinamumą [19], o dažniausia virtualizacijos naudojimo priežastis – suteikti galimybę vartotojams paleisti kitų operacinių sistemų programėles vienu kompiuteriu [24].

Su mobiliąja virtualizacija vartotojai saugiai paleidžia programas ir operacines sistemas prisijungdami prie apsaugotų namuose kompiuterių, serverių, kurie yra įsteigti šiam tikslui [25] [19].



1.6 pav. Mobilusis virtualizacijos modelis.

Paveikslėlyje 1.6 pav. pavaizduota mobilusis virtualizacijos modelis, hipervizorius "Android" telefone. Mobilioji virtualizacija yra paremta konteinerių natūra, kurią kiekvienas vartotojas naudoja mobiliajame įrenginyje, turinčiame virtualią dalį konteineryje laikyti įmonių duomenis..

Mobilioji virtualizacija yra dvejopos personos technologija arba konteinerių technologija. Kiekvieno vartotojo mobilusis prietaisas, dalyvaujantis mobilioje virtualizacijoje, turi virtualią dalį konteinerio, skirto saugoti įmonės duomenis. Kai kuriais atvejais yra dvi virtualios konteinerio dalys – viena skirta darbo duomenims, o kita - asmeniniams. Mobilioji virtualizacija leidžia įrenginį valdyti lengviau, nes prietaise reikia valdyti tik virtualiąją naudotojo dalį [25].

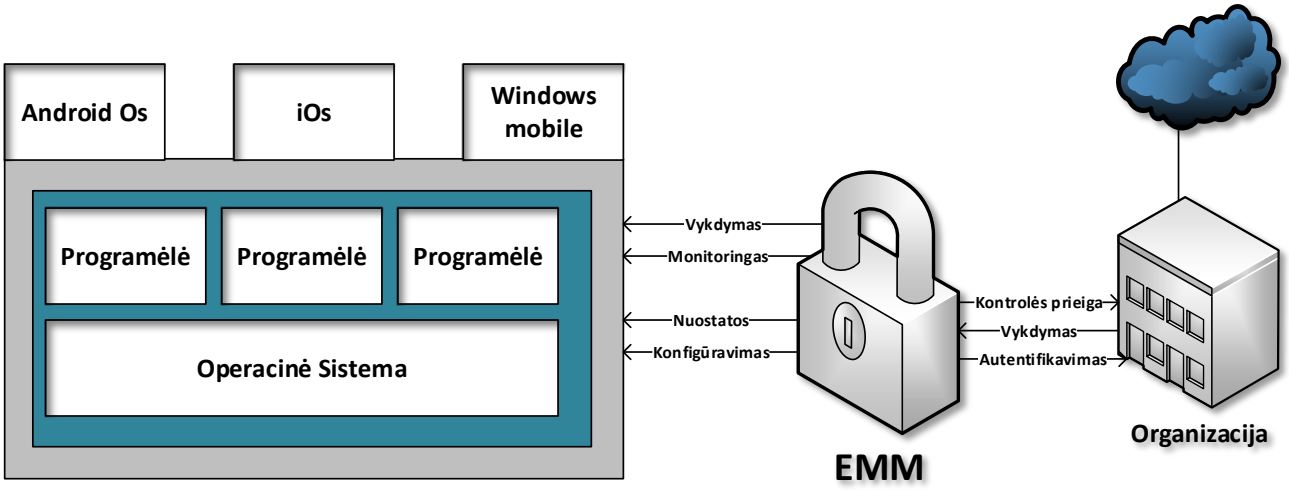
Nuotolinės prieigos paslaugos yra palaikyti mobiliąją virtualizaciją ir pasiekti bei paleisti nuotolinio darbalaukio paslaugas ir taikomąsias programas. Didžiausias virtualizacijos privalumas - tai neskelbtinų organizacijų duomenų saugumas, kurie lieka organizacijos viduje ir niekada nebus saugomi pačiame prietaise. Failas bus perkeliamas tik tada, kai nuotolinės prieigos paslauga palaikys persiuntimą ir leis persiųsti ateityje.

1.6. Asmeninių įrenginių, naudojamų įmonėse, mobilus valdymo modelis

Įmonių valdymo tikslas yra įgyvendinti tinkamą technologiją, kuri užtikrintų darbuotojų galimybes ir jų darbo produktyvumą keliaujant. Užtikrinti mobiluįį našumą yra vienas iš įmonių prioritetų, kuris skatina organizacijas priimti mobiliąsias technologijas. Turint tinkamas naujausias programėles tinkamame įrenginyje galima padidinti darbuotojų produktyvumą ir sumažinti prarandamą laiką [16, 26].

Svarbu, kad organizacijos turėtų galimybes mokyti darbuotojus teikiamų mobilumo privalumų [26].

Atsižvelgdamos į tinkamas žinias ir tinkamą technologiją darbo vietose, įmonės gali matyti mobilumo naudą ir produktyvumą. Šis įmonių mobilumas atneša joms keletą saugumo problemų. Todėl kompanijos ar įmonės turi naudoti tinkamas technologijas ir saugumo sprendimus, siekdamos užtikrinti mobiliojo ryšio saugumą ir darbuotojų produktyvumą [16].



1.7 pav. Asmeninių įrenginių, naudojamų įmonėse, mobilaus valdymo modelis

Paveikslėlyje yra įmonių mobilaus valdymo (EMM) pavyzdys, siekiant užtikrinti jų saugumą, vartotojų prijungimo prieigą prie duomenų ir autentifikuoto naudotojo identifikavimą.

Moderni EMM platforma gali daug gauti iš šiuolaikinių mobiliųjų įrenginių ir MDM technologijos, tačiau daugelis darbuotojų reikalauja atskirų mobiliųjų programėlių be MDM. Bet EFSS (įmonių failų sinchronizavimas ir dalinimasis) dabar yra pakeičiamas kitų mobiliųjų technologijų [28]. Nauji mobilūs įrenginiai turi savo elektroninio pašto programėles ir interneto naršykles. Bet EFSS gali saugiai bendrinti failus, pavyzdžiui, dokumentus, nuotraukas ir vaizdo įrašus keliuose prietaisuose ir su keliais žmonėmis (viršutinis paveikslas). Sinchronizacijos ar kopijavimo gebėjimas leidžia failus saugoti patvirtintose duomenų saugyklose, kurios pasiekiamos darbuotojų nuotoliniu būdu iš kompiuterių, planšetinių kompiuterių arba išmaniųjų telefonų, palaikančių EFSS sistemą.

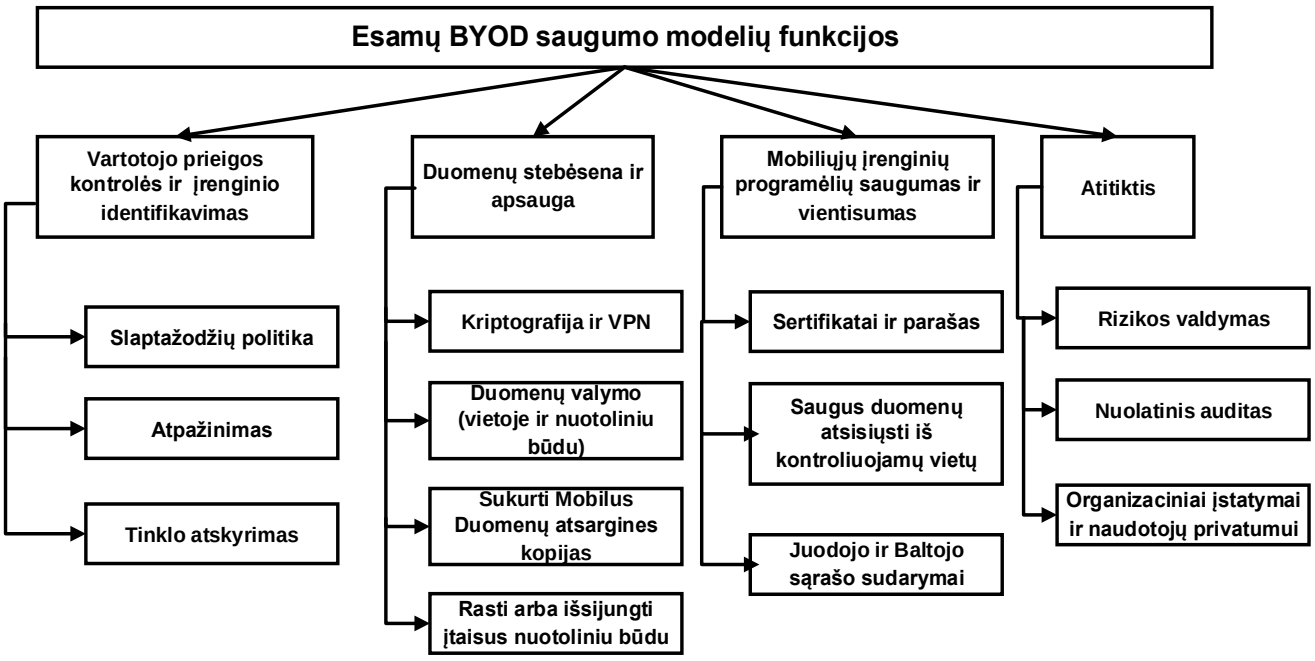
Daugelis EMM platformų dabar gali būti integruotos su tapatybės ir saugumo produktais. Pavyzdžiui, tapatybės teikėjai galėtų atlikti prieigos sprendimus ir remdamiesi prietaiso būsena ir saugumo produktais, vykdyti EMM politiką arba pašalinti rastas grėsmes [28].

1.7. Asmeninių įrenginių, naudojamų įmonėse, saugumo modelių funkcijų analizė

Asmeninių įrenginių, naudojamų įmonėse, modeliai MDM, MAM ir MIM teikia pagrindinius sprendimus, kaip mobilieji įrenginiai gali būti naudojami arba kaip duomenys gali būti pasiekiami. Skiriamos keturiomis pagrindinės kategorijos:

- Identifikavimas ir prieigos kontrolė
- Duomenų apsauga
- Programos saugumas ir vientisumas
- Atitikimas

3 paveikslėlyje parodyti šių galimybių pavyzdžiai [9].



1.8 pav. Asmeninių įrenginių, naudojamų įmonėse, saugumo modelių funkcijos

Vartotojo prieigos kontrolės ir įrenginio identifikavimo tikslai siekiant užkirsti kelią nesankcionuotai prieigai prie asmeninių įrenginių, naudojamų įmonėse, tinklo:

• Identifikuoti ir patikrinti mobiliuosius prietaisus ir vartotojus;
• Plėtoti ir įgyvendinti tarptinklinio ryšio mobiliųjų prietaisų lygio politiką siekiant kontroliuoti prieigą prie duomenų.

Duomenų stebėsenos ir apsaugos tikslai siekiant apsaugoti jautrius verslo duomenis:

• Šifruoti komunikacijų ir mobiliųjų įrenginių duomenis;
• Ištrinti duomenis iš mobiliųjų įrenginių, jei jie yra pamesti arba pavogti;
• Atstatyti duomenis kritiniu duomenų atkūrimu;
• Sekti ir užrakinti mobiliuosius įrenginius, jeigu jie yra pamesti arba pavogti.

Mobiliųjų įrenginių programėlių saugumo ir vientisumo tikslai siekiant sumažinti nepatikimų programėlių naudojimą:

• Patikrinti sertifikatus ir programėlių vientisumą;
• Kontroliuoti programų parsisiuntimus;
• Laikyti programėles patikimuose serveriuose;
• Sudaryti kenksmingų programų juodąjį sąrašą.

Atitikties tikslai siekiant patenkinti organizacinius reikalavimus:

• Atnaujinti apsaugos politiką;
• Patikrinti mobiliuosius įrenginius;
• Laikytis organizacijos įstatymų atsižvelgiant į darbuotojų privatumą.

1.8. Prieigos kontrolė ir autentifikavimas

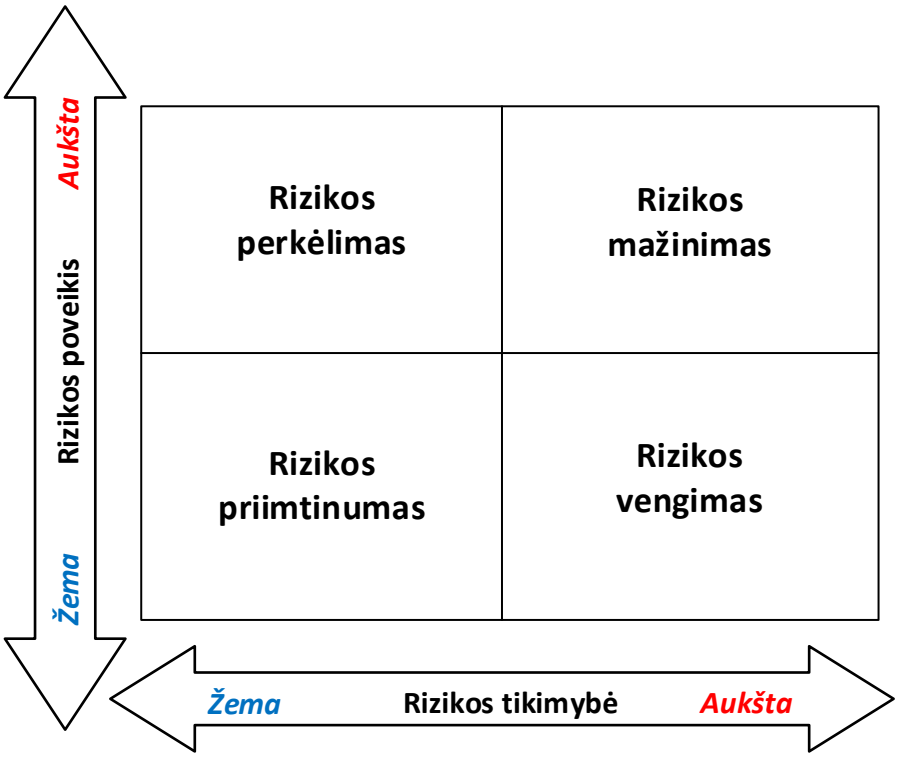
Prieigos kontrolė yra būtinas tinklo mechanizmas. Autentifikavimo sistema yra pirmasis prieigos kontrolės žingsnis. Prieigos kontrolė gali būti netyčia užmiršta, kai kritinės sistemos yra izoliuotos nuo įmonės tinklo. Kritinės sistemos gali būti izoliuotos, bet vartotojai gali rasti sprendimą, kaip prieiti prie sistemos per specialų kanalą. Todėl turi būti įdiegta autentiškumo patvirtinimo ir leidimų išdavimo sistema. Kaip ASĮ skiriasi nuo asmeninio kompiuterio perkeliamumo požiūriu, jei mobilusis įrenginys pametamas? Jis gali užpuolikui suteikti galimybę pavogti vartotojo tapatybę ir gauti prieigą prie sistemos. Taikant ASĮ siūloma naudoti vieno prisijungimo ir atsijungimo funkcija. Prisijungimo funkcija yra galimybė vartotojui prisijungti bet kur ir su bet kokiais įrenginiais, o atsijungimo funkcija naudojama norint priversti sistemą atjungti visus prisijungusius įrenginius. Atsijungimo funkcijos naudojimas yra labai svarbus taikant ASĮ, nes kai kuriose neįprastose situacijose (pavyzdžiui, vagystės ir prietaisų praradimas) visi mobilieji įrenginiai, prisijungę prie kritinės sistemos, gali būti atjungti nuo tinklo, kai prašo teisėtas naudotojas. [30]

Dviejų veiksnių autentifikavimas visada reikalingas. Be klasikinio autentifikavimo metodo, svarbus yra vietos nustatymu grindžiamas mechanizmas, kurio vartotojui gali prireikti naudojant mobilųjį įrenginį arba gaunat prieigą prie labai kritiškos sistemos. Šis mechanizmas gali būti naudojamas siekiant aptikti neįprastą veiklą. Pavyzdžiui, prieiti iš neįprastos vietos, kurioje vartotojas negali būti apribojamas. Fizinės kontrolės požiūriu, ASĮ naudojimas gali būti apribotas kai kuriose vietose.

Norėdama įsitikinti, kad tik autorizuoti vartotojai gali naudotis organizacijos kompiuterių ištekliais [12], ir siekdama užtikrinti, kad prieiga yra tinkamai apribota, organizacija, prieš suteikdama bet kokią prieigą prie organizacijos išteklių, turėtų patvirtinti kiekvieną prisijungimą. Įprastai įmonė nustato ribą, kad vidinis tinklas yra patikimas, o išorinis tinklas - laikomas nepatikimu [18] [20]. Yra daug būdų, kaip autentifikuoti nuotolinės prieigos vartotojus, pavyzdžiui, su slaptažodžiais, skaitmeninio sertifikato arba aparatūros autentifikacijos žymėm [18]. Šie mechanizmai suteikia didesnį pasitikėjimą įrenginiais, kurie apsaugo duomenis ir užtikrina prieigą prie įrenginių. Jeigu slaptažodis yra vienintelis nuotolinės prieigos autentifikavimo mechanizmas dėl autentiškumo, tada organizacijos autentifikavimo mechanizmas turėtų skirtis nuo nuotolinės prieigos autentifikavimo mechanizmo [12]. Gali būti daroma prielaida, kad kartais kai kurie vartotojai naudos tą patį slaptažodį, bet turėdami skirtingus slaptažodžius padidintų saugumo garantiją, jeigu būtų pažeistas vienos sistemos saugumas (kita liktų saugi). Todėl slaptažodis turi būti privalomas. Organizacijos, siekdamos aukštesnio saugumo, turėtų remtis ne tik slaptažodžių mechanizmu, bet naudoti ir kitokius autentifikavimo faktorius [12].

1.9. Asmeninių įrenginių, naudojamų įmonėse, rizikos analizė

Rizikos analizė buvo atlikta rizikos matricos metodu, kuris yra bendrasis metodas rizikos valdymo srityje. Rizikos yra klasifikuojamos pagal rizikos poveikį ir rizikos tikimybę. Rizikos veiksnių 1.1 lentelėje, kaip parodyta 1.9 pav., šis metodas klasifikuoja atsakomąsias priemones į keturias rūšis pagal jų rizikos tikimybes ir rizikos poveikį: rizikos perkėlimas, rizikos mažinimas, rizikos priėmimas ir rizikos vengimas. Rezultatai pateikti 1.1 lentelėje. Taigi, rizika naudojant asmeninius įrenginius skirstoma į rizikos vengimo (2 rizikos veiksniai), rizikos mažinimo (4 rizikos veiksniai), pavojaus priimtinumo (4 rizikos veiksniai) ir rizikos perkėlimo (10 rizikos veiksnių).



1.9 pav. 1.9. Asmeninių įrenginių, naudojamų įmonėse, rizikos matrica

Rizikos vengimas: yra vengti rizikos ir rodyti alternatyvas.
Rizikos mažinimas: Sumažinti riziką iki priimtino lygio.
Rizikos perkėlimas: Perduoti riziką trečiosioms šalims.
Rizikos priėmimas: Priimti pavojų besąlygiškai.

1.1 lentelė. Rizikos analizės rezultatai pagal rizikos matricą.

Nr.	Aukštasis skyrius	Vidurinysis skyrius	Žemasis skyrius (=rizikos faktorius)	Rizikos klasifikacija
1	1. Įmonės pusėje	1.1 Operacijų	Valdymas ne darbo metu	Rizikos perkėlimas
2			Išorinis valdymas	Rizikos perkėlimas
3			Asmeninių įrenginių terminalas, paremtas ryšiu	Rizikos perkėlimas
4			Darbuotojų darbo valandų valdymas	Rizikos vengimas
5			Darbuotojo asmeninės informacijos valdymas	Rizikos perkėlimas
6		1.2 Sistemos	Neautorizuotas priėjimas per asmeninius įrenginius	Rizikos mažinimas
7			Darbuotojo sumaišyti privatūs duomenys asmeninių įrenginių terminale	Pavojaus priimtinumas
8			Konfidencialios informacijos, susijusios su įmone, praradimas	Rizikos perkėlimas
9			Įrenginio užkrėtimas virusu per nepageidaujamą programinę įrangą.	Rizikos perkėlimas

10			Saugos politikos edukacija ir supažindinimas su asmeninių įrenginių įmonėse politika	Rizikos mažinimas
11			Ribojimas prisijungti prie nepageidaujamų svetainių per asmeninius įrenginius	Rizikos mažinimas
12	2. Darbuotojo pusėje	2.1 Operacijų	Nepageidaujamų programų įdiegimo rizika į asmeninį įrenginį	Rizikos mažinimas
13			Darbo valandų nesilaikymas	Rizikos vengimas
14			Asmeninio įrenginio praradimas arba vagystė	Rizikos perkėlimas
15			Priėjimas prie neleistinų svetainių naudojantis asmeniniu įrenginiu	Rizikos perkėlimas
16		2.2 Sistemos	Duomenų praradimas iš asmeninio įrenginio naudojantis debesų paslaugomis	Rizikos perkėlimas
17			Įsilaužimas į asmeninį įrenginį naudojantis slaptažodžiu	Pavojaus priimtinumas
18			Informacijos praradimas prisijungus prie viešo wifi	Rizikos perkėlimas
19			Nenustatytas prisijungimo slaptažodis asmeniniame įrenginyje	Pavojaus priimtinumas
20			Šeimos narių naudojimasis asmeniniu įrenginiu	Pavojaus priimtinumas

1.10. Asmeninių įrenginių, naudojamų įmonėse, analizės išvados

Išanalizuoti trys pagrindiniai asmeninių įrenginių organizacijose saugumo modeliai - mobiliųjų įrenginių valdymo modelis, mobiliųjų programėlių valdymo modelis, mobiliosios informacijos valdymo modelis.

Nustatyta, kad taikant mobiliųjų įrenginių valdymo modelį asmeninis įrenginys, naudojamas įmonėse, gyvavimo cikle gali būti vienos iš trijų skirtingų būsenų: nepatikima, patikima ir naudojama nuosavybė. Kai prietaisas yra nepatikimos būsenos, nei organizacija, nei kas nors iš jos darbuotojų negali būti laikomi atsakingi už tą įrenginį. Kai prietaisas yra pažymimas nepatikimu, jokie svarbūs organizacijos duomenys negali būti saugomi ir prietaisas negali būti prijungtas prie verslo tinklų. Kai prietaisas yra patikimos būsenos, tik organizacija yra atsakinga už tą įrenginį. Šios būsenos prietaisas gali saugoti jautrius verslo duomenis.

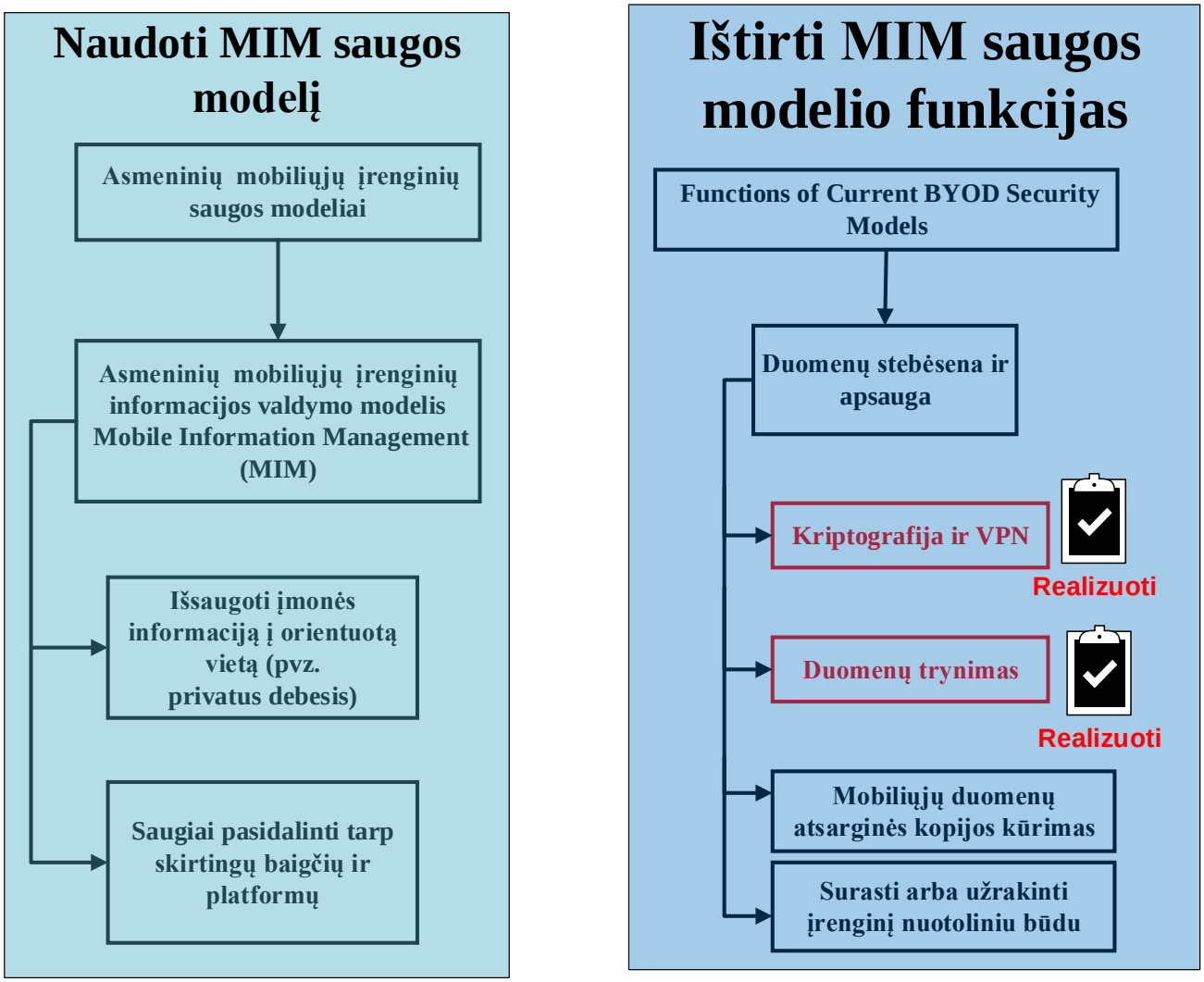
Nustatyta, kad asmeninių įrenginių, naudojamų įmonėse, mobiliųjų programėlių valdymo modelis yra sprendimas, naudojamas IT administratorių, siekiant nuotoliniu būdu įdiegti, atnaujinti, ištrinti, vesti auditą ir stebėti su įmone susijusias programėles mobiliuosiuose įrenginiuose. Skirtingai nei MDM, kuris kontroliuoja mobiliuosius prietaisus aparatūros lygyje, mobiliųjų programėlių valdymo sistemos stebi ir kontroliuoja tam tikras programas siekdamos, kad būtų laikomasi organizacijos politikos ir reikalavimų.

Nustatyta kad, asmeninių įrenginių, naudojamų įmonėse, informacijos valdymo modelio pagrindas - kritinę įmonių informaciją nesaugoti mobiliuosiuose įrenginiuose. Pagrindinis MIM tikslas yra išsaugoti įmonės informaciją tinklo saugykloje ir saugiai dalintis informacija tarp skirtingų vartotojų ir platformų. MIM leidžia kontroliuoti ir valdyti tik ribotą patikimų programų kiekį ir šifruotus įmonių duomenis.

Nepriklausomai nuo privalumų ir trūkumų minėti saugumo modeliai orientuojasi tik į ribotus sprendimus ir apsaugą ir tik į įrenginių valdymą (MDM), programėles (MAM) ir informaciją (MIP), remiantis tam tikra politika.

2. ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ PRIEIGAI PRIE ĮMONĖS INFORMACIJOS, SAUGOS SISTEMA

Magistro darbe pasiūlyta asmeninių įrenginių (AĮ), naudojamų prieigai prie įmonės informacijos, dokumentų failų saugos sistema (DFSS). Darbe panaudotas MIM saugos modelis, kuris praplėstas papildomu funkcionalumu. Magistro darbe ištirtos MIM modelio šifravimo ir saugaus trynimo funkcijos (2.1 pav.). Kitame skyriuje apžvelgsime siūlomos sistemos struktūrą.

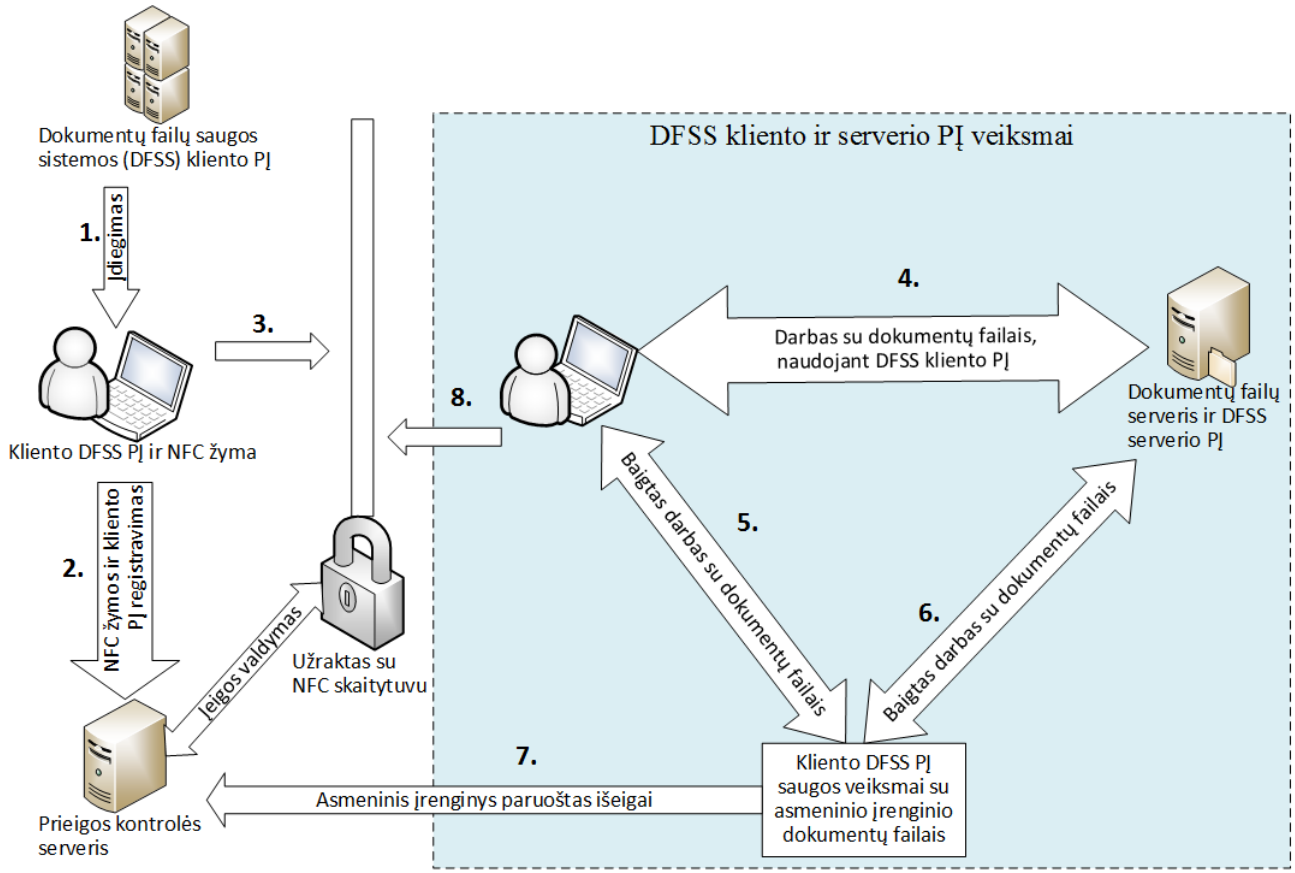


a) MIM saugos modelis b) MIM saugos modelio funkcijos

2.1 pav. MIM saugos modelis ir jo funkcijos

2.1. Asmeninių įrenginių, naudojamų prieigai prie įmonės dokumentų failų, saugos sistemos vizija

AĮ, naudojamų prieigai prie įmonės informacijos, DFSS modelis pateiktas paveiksle 2.2. DFSS sudaryta iš dviejų dalių kliento PĮ ir serverio PĮ. Kliento PĮ patalpinta organizacijos programėlių serveryje.



2.2 pav. Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, dokumentų failų saugos sistemos modelis

Kliento PĮ organizacijos darbuotojai, kurie pradeda dirbti organizacijoje, į savo įrenginius įdiegia iš šio serverio (2.2 pav. žingsnis 1). Taip pat AĮ naudotojas privalo gauti NFC žymą. Įdiegus kliento PĮ ir gavus NFC žymą įmonės darbuotojas užregistruoja jas prieigos kontrolės serveryje (2.2 pav. žingsnis 2). Užregistravus PĮ ir AĮ NFC žymą darbuotojas gali įeiti į įmonės darbo su apsaugotais dokumentais pastatą, kuriame įrengtas užraktas su NFC skaitytuvu (2.2 pav. žingsnis 3).

Su AĮ darbuotojas atlieka darbą ir parsiunčia reikalingus jam failus su kliento PĮ, kuri failų gavimui naudoja serverio PĮ (2.2 pav. žingsnis 4). Baigęs darbą, darbuotojas informuoja kliento PĮ apie darbo su dokumentais pabaigą (2.2 pav. žingsnis 5). Kliento PĮ atlieka saugos veiksmus su AĮ dokumentų failais (failai užšifruojami ir išsiunčiami į serverį, o failų kopijos įrenginyje saugiai ištrinamos - 2.2 pav. žingsnis 6) ir pabaigus veiksmus apie tai informuoja prieigos kontrolės serverį (2.2 pav. žingsnis 7). Darbuotojas informuojamas ir gali išeiti iš įmonės pastato su apsaugotais dokumentais ir išsinešti savo AĮ (2.2 pav. žingsnis 8).

2.2. Asmeninių įrenginių, naudojamų prieigai prie įmonės dokumentų failų, saugos sistema

Pagrindinė funkcija yra dokumentų failų, kurie buvo parsiųsti į darbuotojo AĮ, registravimas, kad baigus darbą su jais, būtų galimą dokumentų failus užšifruoti, persiųsti į serverį ir po to saugiai ištrinti iš darbuotojo AĮ. Lentelėje 2.1 pateikiame dokumentų failų požymius, naudojamus serverio PĮ, registruojant parsiųstus dokumentų failus į darbuotojo AĮ. Taip pat pateikiame kliento PĮ veiksmus, kurie bus atlikti darbuotojui užbaigus darbą su dokumentų failais.

2.1 lentelė. Kliento PĮ dokumentų failų registravimo požymiai ir saugumo veiksmai

Požymis	Saugumo lygis	DFSS kliento PĮ veiksmai darbuotojui užbaigus darbą su dokumentų failais		
		Šifravimo algoritmas	**Trynimas**	**Kliento PĮ modulis**
YS	Ypač slaptas,	RC2	DoD ištrynimas	„Šifratorius RC2“
VS	Vidutiniškai slaptas	AES	DoD ištrynimas	„Šifratorius AES“
S	Slaptas	3DES	DoD ištrynimas	„Šifratorius 3DES“
P	Bendram naudojimui	DES	Ištrinti naudojant OS komandą „Delete“	„Komandų OS vykdymo procesas“
L	Laisvos formos	Jokio šifravimo	Ištrinti naudojant OS komandą „Delete“	Nėra

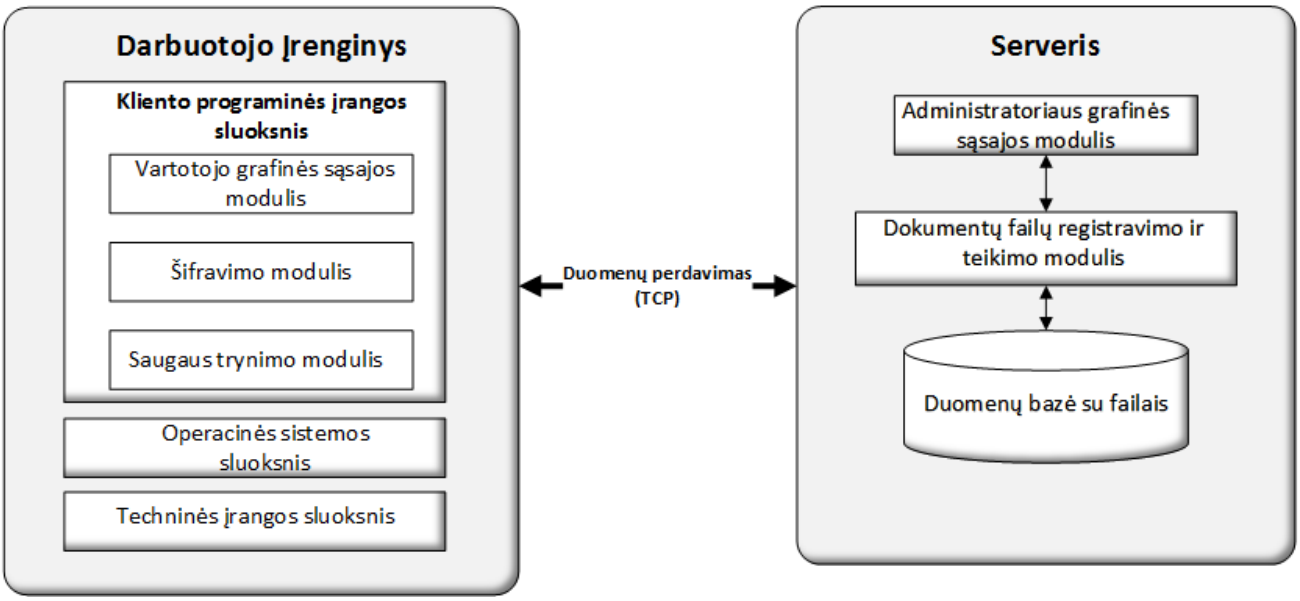
Lentelė formuojama ir pildoma serverio PĮ. Kliento PĮ nuskaito registravimo informaciją, pagal numatytus požymius atlieka šifravimą ir saugų ištrynimą.

2.2 lentelė. Dokumentų failų registravimo lentelė

ID	Data	Laikas	Pavadinimas	Failo dydis	Vieta	Saugumo lygis	Įrenginio pavadinimas
1	05-20	15:10	Failas1.doc	20 MB	C:\workfiles	YS	DESKTOP-RM251IM
2	05-20	16:00	Paveiklelis1.bmp	10 MB	C:\ workfiles	VS	DESKTOP-RM251IM
3	05-22	10:00	Failas3.txt	1 MB	C:\ workfiles	L	DESKTOP-RM251IM

Kaip matome lentelėje, kiekvienas failas lentelėje turi savo ID datą ir laiką, kada buvo sukurtas failas, failo pavadinimą, dydį, vietą, įrenginio pavadinimą, kur yra saugomas failas, ir saugumo lygio požymį, pagal kurį kliento PĮ atliks veiksmus, kai darbuotojas užbaigs darbą su dokumentų failais.

Kliento ir serverio PĮ siūlomos DFSS architektūra parodyta paveiksle 2.3.

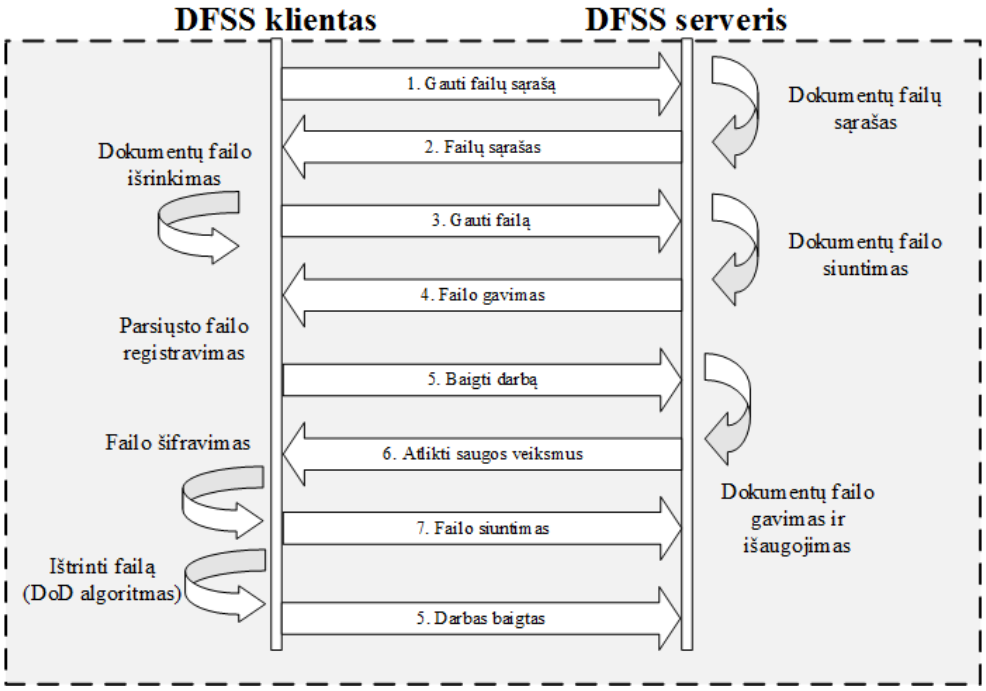


2.3 pav. Pasiūlytos dokumentų failų saugos sistemos architektūra

Kiekviena sistemos dalis yra sudaryta iš modulių, kurie atlieka tokias funkcijas:

- **Vartotojo grafinės sąsajos modulis –** skirtas darbuotojo dokumentų failų parsiuntimo, darbo pabaigos komandų įvesčiai ir informacijos atvaizdavimui.
- **Šifravimo modulis** – šis modulis atlieka dokumentų failų šifravimą.
- **Saugaus trynimo modulis** – ištrina dokumentų failų informaciją iš darbuotojo AĮ taikant DoD algoritmą.
- **Duomenų bazė su failais** – tai duomenų bazė, kurioje yra laikomi įmonės dokumentų failai ir priskirto saugumo požymiai, ši duomenų bazė šifruojama.
- **Dokumentų failų registravimo ir teikimo modulis** – yra atsakingas už failų teikimą ir pateiktų dokumentų failų registravimą.
- **Administratoriaus grafinės sąsajos modulis –** skirtas administratoriui serverio PĮ valdymo tikslams.

DFSS kliento ir serverio PĮ vykdomos komandos parodytos paveiksle 2.4.

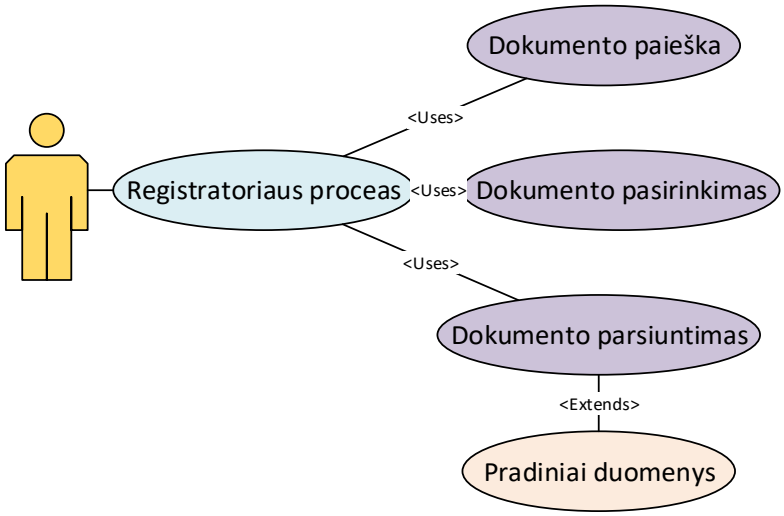


2.4 pav. DFSS kliento ir serverio PĮ vykdomos komandos

Darbuotojas įsidiegęs į savo įrenginį kliento PĮ gali dirbti įmonės su apsaugotais darbo dokumentais. Prieš keliaudamas namo iš organizacijos vartotojas turi pranešti kliento PĮ apie išvyką. Kai vartotojas nori išeiti iš organizacijos, kliento PĮ gauna iš serverio PĮ registracijos žurnalo informaciją, nustato, kokie failai yra įrenginyje ir taikant požymius atlieka atitinkamus veiksmus.

2.3. Asmeninių įrenginių, naudojamų prieigai prie įmonės dokumentų failų, saugos sistemos prototipas

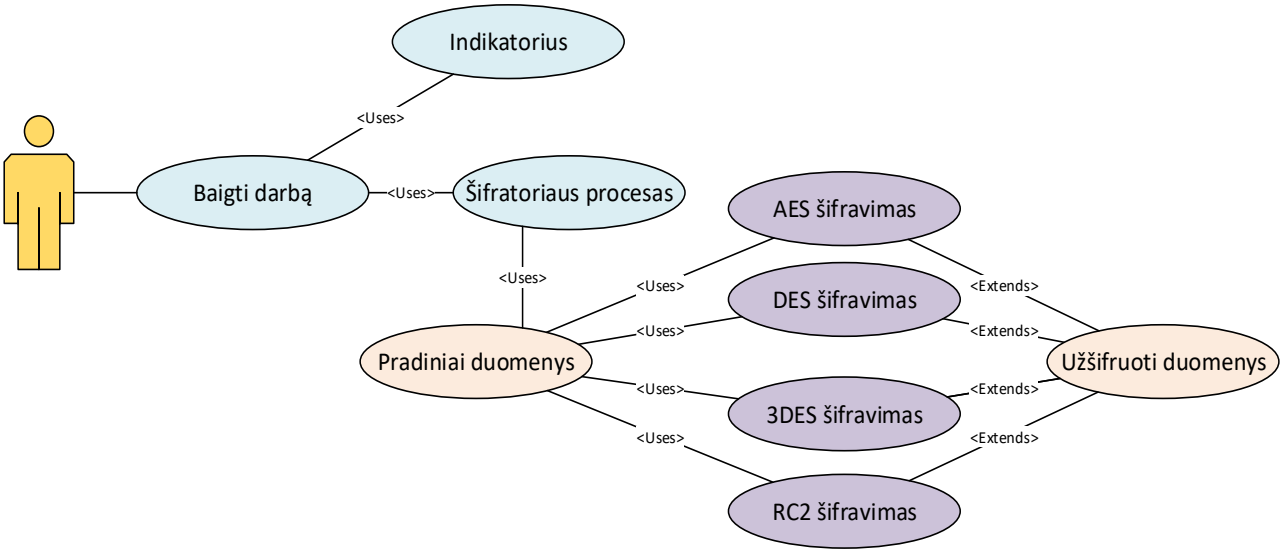
Paveiksluose 2.5 – 2.8 parodytos DFSS panaudos atvejų diagramos. Lentelėse 2.3 – 2.5 aprašyti panaudos atvejai.



2.5 pav. Registravimo modulio panaudos atvejų diagrama2.3 lentelė. Registravimo modulio panaudos atvejai.

Panaudos atvejis	Aprašymas
Registravimo modulis	
Dokumento paieška	Atlieka dokumento paiešką
Dokumento parsiuntimas	Parsiunčia rastą dokumentą

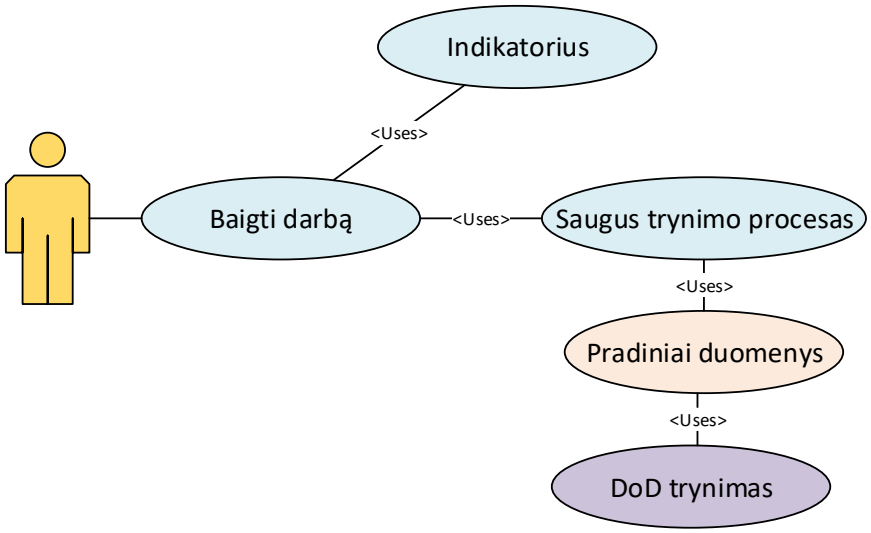
Panaudos atvejis	Aprašymas
Dokumento pasirinkimas	Pasirenkamas norimas parsisiųsti dokumentas
Pradiniai duomenys	Parsiųsti dokumentai, su kuriais darbuotojas dirbs
Indikatorius	Parodo, ar darbuotojas gali išeiti iš įmonės



2.6 pav. Darbo baigimo ir šifravimo modulio panaudos atvejų diagrama

2.4 lentelė. Darbo baigimo ir šifravimo modulio panaudos atvejai

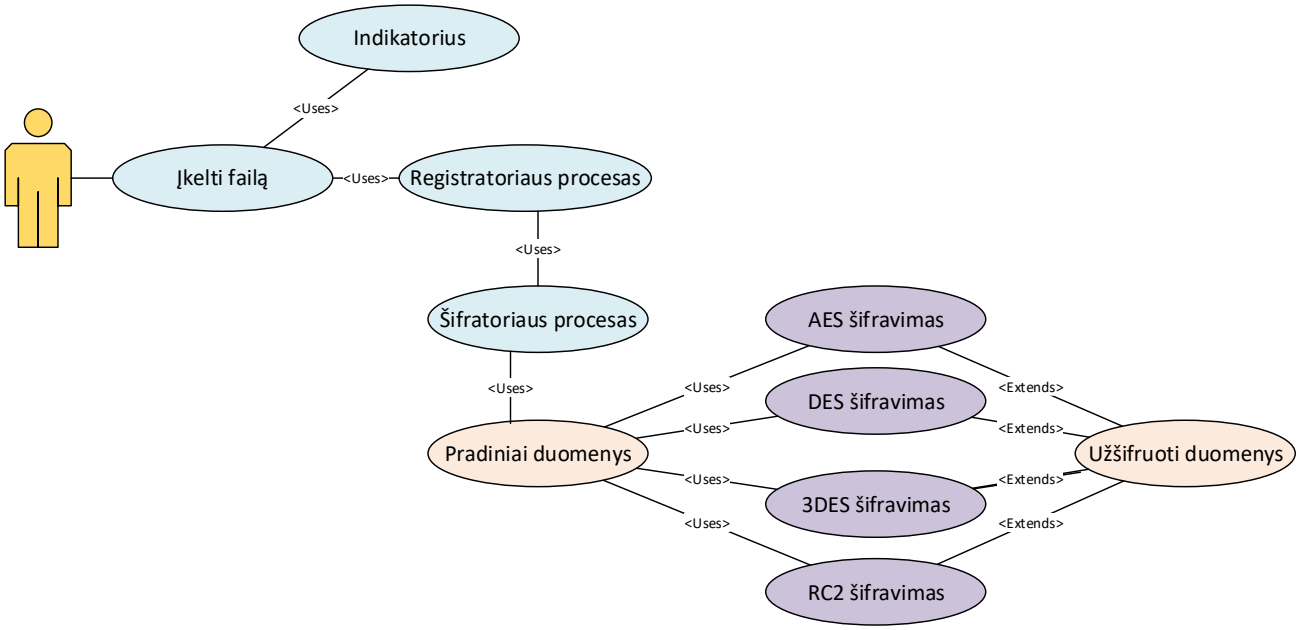
Panaudos atvejis	Aprašymas
Pradiniai duomenys	Parsiųsti dokumentai, su kuriais darbuotojas dirbs
Baigti darbą	Paspaudus „Baigti darbą“ iškviečiami šifratoriaus procesas ir saugus trynimas.
Šifratoriaus procesas	Užšifruoja failą pagal parinktą šifravimo būdą
AES šifravimas	Užšifruojamas failas AES šifravimu
DES šifravimas	Užšifruojamas failas DES šifravimu
3DES šifravimas	Užšifruojamas failas 3DES šifravimu
RC2 šifravimas	Užšifruojamas failas RC2 šifravimu
Užšifruoti duomenys	Po šifravimo yra užšifruoti failai
Indikatorius	Parodo, ar darbuotojas gali išeiti iš įmonės



2.7 pav. Darbo baigimo ir saugaus trynimo modulio panaudos atvejų diagrama

2.5 lentelė. Darbo baigimo ir saugaus trynimo modulio panaudos atvejai

Panaudos atvejis	**Aprašymas**
Pradiniai duomenys	Dokumentai, su kuriais bus atlikti veiksmai.
Baigti darbą	Paspaudus „Baigti darbą“ iškviečiami procesas šifratorius ir saugus trynimas.
Saugaus trynimo procesas	Saugaus trynimo procesas ištrina dokumentą DoD trynimu.
DoD trynimas	Ištrina failą naudojant DoD trynimą.
Indikatorius	Parodo, ar darbuotojas gali išeiti iš įmonės.

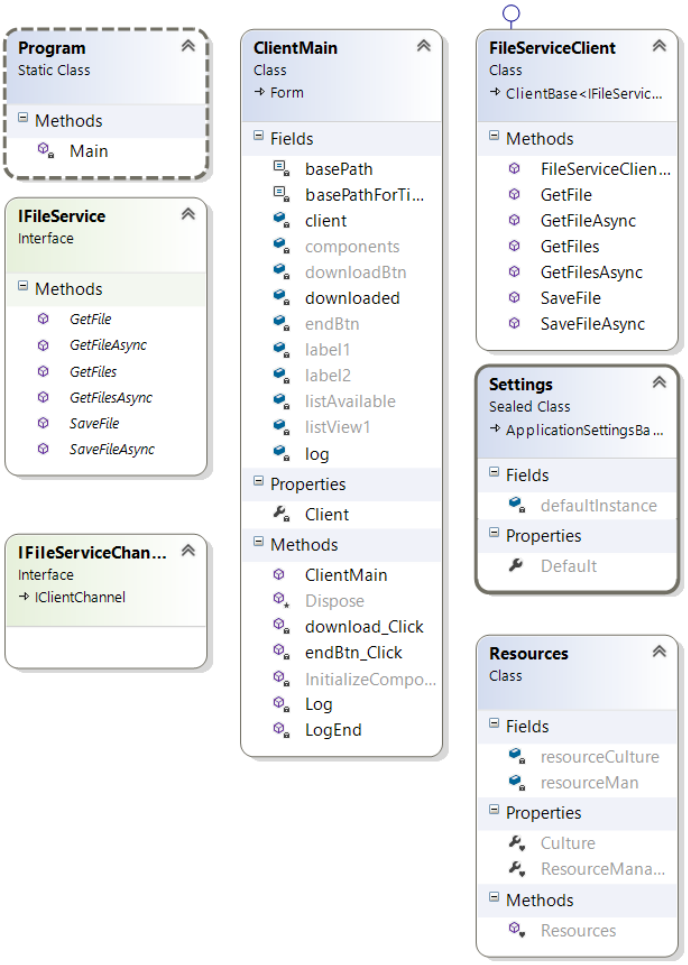


2.8 pav. Failo įkėlimo panaudos atvejų diagrama

2.6 lentelė. Failo įkėlimo panaudos atvejai

Panaudos atvejis	**Aprašymas**
Įkelti failą	Pasirinktas įkėlimui dokumentas.
Registratoriaus procesas	Registratoriaus procesas parinks reikalingus atlikti procesus.
Pradiniai duomenys	Dokumentai, su kuriais bus atlikti veiksmai.
Baigti darbą	Paspaudus „Baigti darbą“ iškviečiamas šifratoriaus procesas ir saugus trynimas.
Šifratoriaus procesas	Užšifruoja failą pagal parinktą šifravimo būdą
AES šifravimas	Užšifruojamas failas AES šifravimu
DES šifravimas	Užšifruojamas failas DES šifravimu
3DES šifravimas	Užšifruojamas failas 3DES šifravimu
RC2 šifravimas	Užšifruojamas failas RC2 šifravimu
Užšifruoti duomenys	Po šifravimo yra užšifruoti failai
Indikatorius	Parodo, ar darbuotojas gali išeiti iš įmonės

DFSS sistemos prototipo kliento PĮ klasių diagramos parodytos paveiksle 2.9 ir pagrindinės klasės aprašytos lentelėje 2.7.

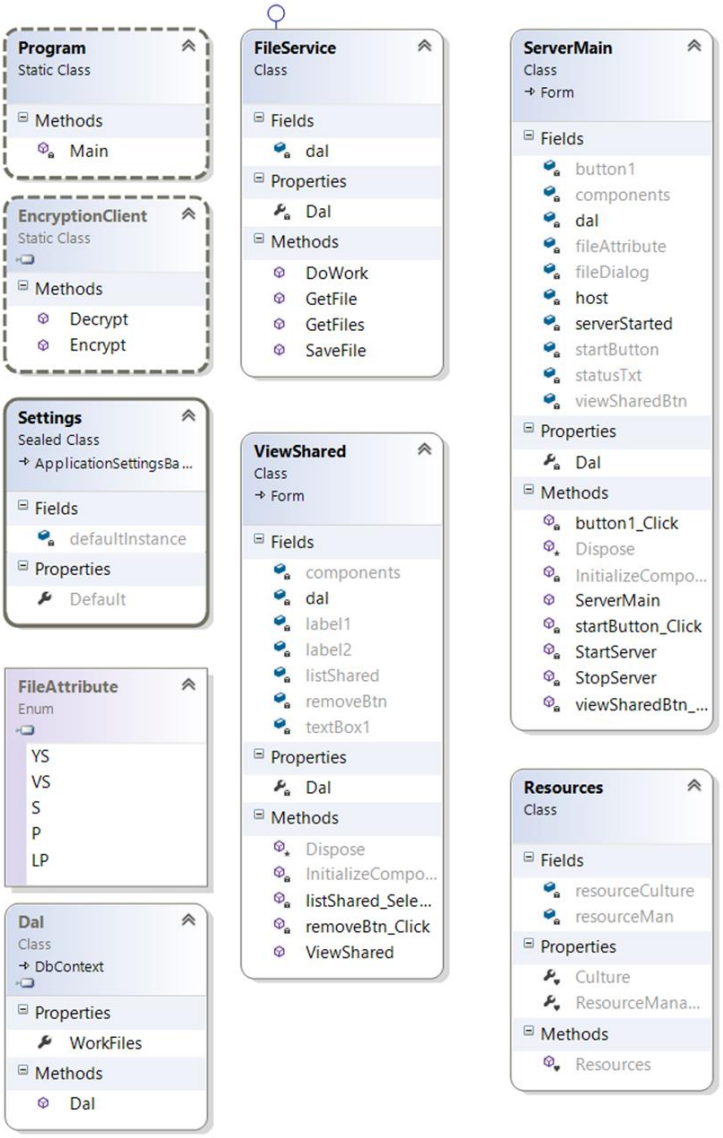


2.9 pav. Kliento PĮ klasių diagrama

2.7 lentelė. Pagrindinių kliento PĮ klasių aprašymas

Klasės pavadinimas	Objektas	Aprašymas
Program	Main	Pagrindinė programa
ClientMain	BasePath	Šioje klasėje aprašomas pagrindinio kliento programos grafinės sąsajos išdėstymas ir sąsajoje atliekamų veiksmų funkcijos.
	BasePathFor	
	client	
	components	
	downloadBtn	
	Downloaded	
	endbtn	
	Lable1	
	Lable2	
	ListAvalable	
	ListViev1	
	log	
Settings	DefaultInstance	Šioje klasėje saugomi SQLExpress duomenų bazės nustatymų parametrai.
	Default	

DFSS sistemos prototipo serverio PĮ klasių diagrama parodyta paveiksle 2.10 ir pagrindinės klasės aprašytos lentelėje 2.8.

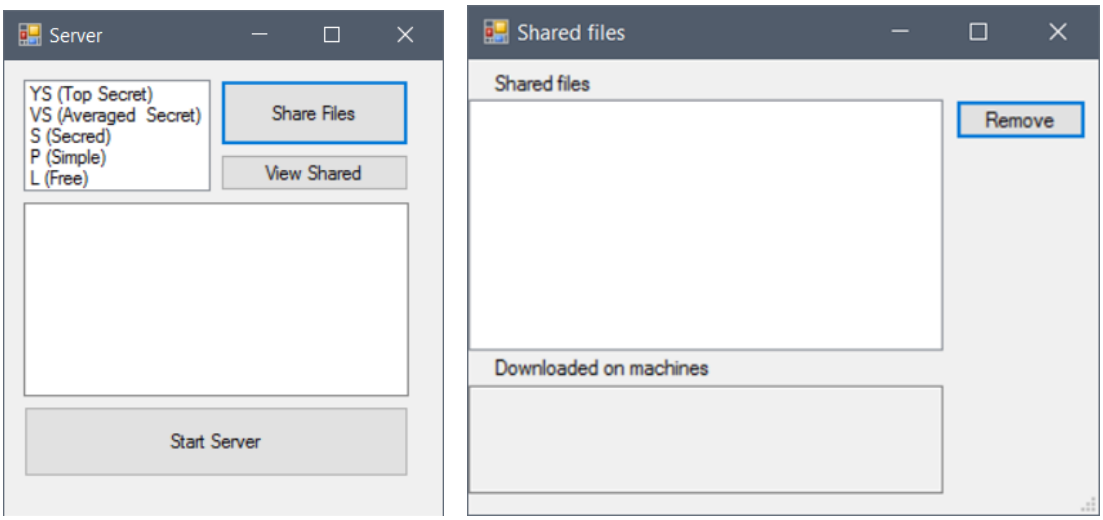


2.10 pav. Serverio PĮ klasių diagrama

Pagrindinių serverio programos klasių lentelė

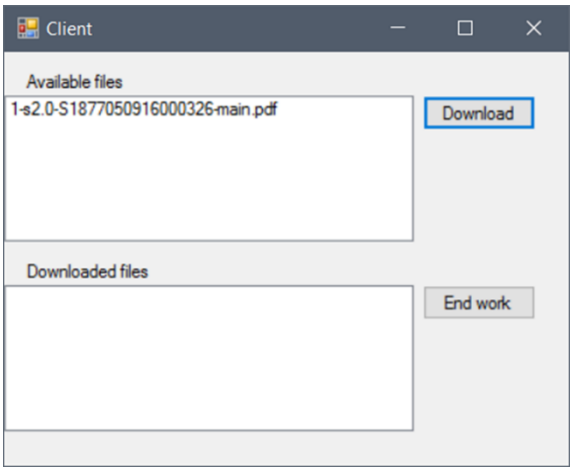
Klasės pavadinimas	Objektas	Aprašymas
Program	Main	Pagrindinė programa.
EncryptionClient	Decrypt	Šios klasės objektai yra Šifravimo ir dešifravimo bibliotekos.
	Encrypt	
Settings	DefaultInstance	Šioje klasėje saugomi SQLExpress duomenų bazėje nustatymų parametrai.
	Default	
Dal	WorkFiles	Duomenų prieigos lygio klasė.
	Dal	
FileService	dal	Šios klasės objektai atlieka veiksmus su failais.
	Dal	
	DoWork	
	GetFile	
	GetFiles	
	SaveFile	
ViewShared	Components	Šioje klasėje aprašomas serverio programos įkeltų failų peržiūros lango elementų išdėstymas ir atliekamos funkcijos.
	Dal	
	Label1	
	Label2	
	ListShared	
	removeBtn	
	TextBox	
	Dal	
	Dispose	
	InitalizeComponent	
	ListShared_Select	
	removeBtn_click	
	ViewShared	
ServerMain	Button1	Šioje klasėje aprašomi serverio programos grafinės sąsajos objektai ir metodai, su kuriais bus atlikti tokie veiksmai: serverio paleidimas ir sustabdymas, failų atributų pasirinkimas įkeliant failus, parodomas failų statusas.
	Components	
	dal	
	FileAtribute	
	FileDialog	
	Host	
	ServerStarted	
	StartButton	
	StatusTxt	
	ViewSharedBtn	
	Dal	
	Button1Click	
	Dispose	
	InitializeComponent	
	ServerMain	
	StartBtnClick	
	StartServer	
	StopServer	
	ViewShrdBtn	

Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, dokumentų failų saugos sistemos (DFSS) serverio ir kliento PĮ prototipas realizuoti naudojant Microsoft .NET Framework C# programavimo kalbą ir Visual Studio 2015 programų projektavimo įrankį. Serverio PĮ grafinės sąsajos langai parodyti paveiksle 2.11.



2.11 pav. Serverio PĮ grafinės sąsajos langai

Kliento PĮ grafinė sąsaja parodyta paveiksle 2.12.



2.12 pav. Kliento PĮ grafinė sąsaja

2.4. Išvados

Pasiūlytas AĮ, naudojamų prieigai prie įmonės informacijos, DFSS modelis sudarytas iš dviejų dalių PĮ - kliento ir serverio. Suprojektuota dokumentų failų saugos sistemos architektūra ir kliento bei serverio PĮ vykdomos komandos.

Aprašyti darbuotojo, naudojančio AĮ įmonės pastate darbui su apsaugotais dokumentais, žingsniai ir sąveika su kliento PĮ.

Pasiūlyti kliento PĮ dokumentų failų registravimo požymiai ir saugumo veiksmai.

Sukurtas AĮ, naudojamų prieigai prie įmonės informacijos, DFSS sistemos prototipas.

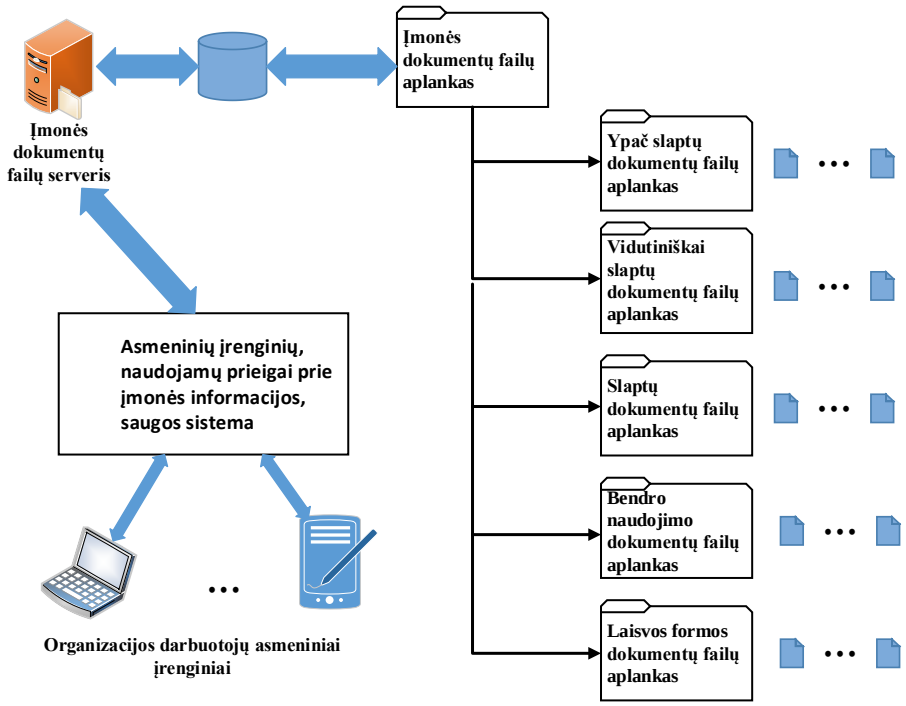
Prototipas sukurtas naudojant Microsoft.NET Framework C# programavimo kalbą ir Visual Studio 2015 programų projektavimo įrankį.

3. ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ PRIEIGAI PRIE ĮMONĖS INFORMACIJOS, SAUGOS SISTEMOS PROTOTIPO EKSPERIMENTINIS TYRIMAS

Magistro darbe pasiūlyta asmeninių įrenginių (AĮ), naudojamų prieigai prie įmonės informacijos, dokumentų failų saugos sistema (DFSS). Sukurto prototipo tyrimui reikia sukurti aplinką, parašyti tyrimo scenarijų ir atlikti eksperimentinį tyrimą.

3.1. Asmeninių įrenginių, naudojamų prieigai prie įmonės dokumentų failų, saugos sistemos prototipo tyrimo aplinka ir scenarijus

Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos prototipo eksperimentinio tyrimo aplinka parodyta paveiksle 3.1 pav.



3.1 pav. Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos prototipo tyrimo aplinka

Tyrime organizacijos dokumentai simuliuojami panaudojant etaloninių failų rinkinį iš 16 spalvotų ir 28 nespalvotų vaizdų [31]. Eksperimente naudojami failai, įkelti į įmonės dokumentų failų serverio atitinkamus saugumo lygiams aplankus - „Įmonės dokumentų failų aplankas“ . Eksperimento rezultatų palyginimui į kiekvieną saugumo lygio aplanką įkelti visi etaloninių failų rinkinio failai. Etaloninių failų parametrai pateikiami lentelėje 3.1.

3.1 lentelė. Etaloniniai failai ir jų parametrai

Failo vardas	Aprašymas	Failo dydis baitais	Vaizdo taškų skaičius	Failo tipas	Bitų kiekis vienam taškui bits/pixel
4.1.01	Girl	196744	256x256	Color	24
4.1.02	Couple	196744	256x256	Color	24
4.1.03	Girl	196744	256x256	Color	24
4.1.04	Girl	196744	256x256	Color	24
4.1.05	House	196744	256x256	Color	24

Failo vardas	Aprašymas	Failo dydis baitais	Vaizdo taškų skaičius	Failo tipas	Bitų kiekis vienam taškui bits/pixel
4.1.06	Tree	196744	256x256	Color	24
4.1.07	Jelly beans	196744	256x256	Color	24
4.1.08	Jelly beans	196744	256x256	Color	24
4.2.01	Splash	786568	512x512	Color	24
4.2.02	Girl (Tiffany)	786568	512x512	Color	24
4.2.03	Mandrill (Baboon)	786568	512x512	Color	24
4.2.04	Girl (Lena, or Lenna)	786568	512x512	Color	24
4.2.05	Airplane (F-16)	786568	512x512	Color	24
4.2.06	Sailboat on lake	786568	512x512	Color	24
4.2.07	Peppers	786568	512x512	Color	24
5.1.09	Moon surface	65664	256x256	Gray	8
5.1.10	Aerial	65664	256x256	Gray	8
5.1.11	Airplane	65664	256x256	Gray	8
5.1.12	Clock	65664	256x256	Gray	8
5.1.13	Resolution chart	65664	256x256	Gray	8
5.1.14	Chemical plant	65664	256x256	Gray	8
5.2.08	Couple	262272	512x512	Gray	8
5.2.09	Aerial	262272	512x512	Gray	8
5.2.10	Stream and bridge	262272	512x512	Gray	8
5.3.01	Man	1048704	1024x1024	Gray	8
5.3.02	Airport	1048704	1024x1024	Gray	8
7.1.01	Truck	262272	512x512	Gray	8
7.1.02	Airplane	262272	512x512	Gray	8
7.1.03	Tank	262272	512x512	Gray	8
7.1.04	Car and APCs	262272	512x512	Gray	8
7.1.05	Truck and APCs	262272	512x512	Gray	8
7.1.06	Truck and APCs	262272	512x512	Gray	8
7.1.07	Tank	262272	512x512	Gray	8
7.1.08	APC	262272	512x512	Gray	8
7.1.09	Tank	262272	512x512	Gray	8
7.1.10	Car and APCs	262272	512x512	Gray	8
7.2.01	Airplane (U-2)	1048704	1024x1024	Gray	8
boat.512	Fishing Boat	262272	512x512	Gray	8
elaine.512	Girl (Elaine)	262272	512x512	Gray	8
house	House	262272	512x512	Color	8
gray21.512	21 level step wedge	786568	512x512	Gray	8
numbers.512	256 level test pattern	262272	512x512	Gray	8
ruler.512	Pixel ruler	262272	512x512	Gray	8
testpat.1k	General test pattern	1048704	1024x1024	Gray	8
	IŠ VISO	17176192			

Iš viso tyrimui pasirinkti 44 failai, kurių dydžiai yra: 14 failai - 256x256 taškų, 26 failai 512x512 taškų ir 4 failai 1024x1024 taškų. Bendras kiekvieno aplanko dydis - 17176192 baitai.

AĮ, naudojamų prieigai prie įmonės informacijos, DFSS prototipo tyrimo scenarijus

1. Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, DFSS tyrimui sukurtas sistemos prototipas, susidedantis iš dviejų dalių: serverio PĮ ir kliento PĮ.
2. Serverio ir kliento dalių realizacijos tyrimas atliktas Asus N56V kompiuteryje su parametrais: Intel Core i5 3230m, veikiantis 2,6 Ghz dažniu, 4 branduolių procesorius, 8 Gb operatyvioji atmintis, 480 Gb SSD tipo diskas, Windows 10 operacine sistema, .NET Framework CLR 4.0 versija.
3. Asmeninio įrenginio naudotojas atsisiunčia į savo įrenginį visus failus iš serverio.
4. Imituojamas veiksmas „Baigti darbą“.
5. Matuojamas laikas iki asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos leidimo „Galima išnešti įrenginį už organizacijos ribų“.
6. Asmeninio įrenginio naudotojas atsisiunčia į savo įrenginį visus failus iš aplanko „Vidutiniškai slaptų dokumentų failų aplankas“.
7. Imituojamas veiksmas „Baigti darbą“.
8. Matuojamas laikas iki asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos leidimo „Galima išnešti įrenginį už organizacijos ribų“.
9. Asmeninio įrenginio naudotojas atsisiunčia į savo įrenginį visus failus iš aplanko „Slaptų dokumentų failų aplankas“.
10. Imituojamas veiksmas „Baigti darbą“.
11. Matuojamas laikas iki asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos leidimo „Galima išnešti įrenginį už organizacijos ribų“.
12. Asmeninio įrenginio naudotojas atsisiunčia į savo įrenginį visus failus iš aplanko „Bendro naudojimo dokumentų failų aplankas“.
13. Imituojamas veiksmas „Baigti darbą“.
14. Matuojamas laikas iki asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos leidimo „Galima išnešti įrenginį už organizacijos ribų“.
15. Asmeninio įrenginio naudotojas atsisiunčia į savo įrenginį visus failus iš aplanko „Laisvos formos dokumentų failų aplankas“.
16. Imituojamas veiksmas „Baigti darbą“.
17. Matuojamas laikas iki asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos leidimo „Galima išnešti įrenginį už organizacijos ribų“.
18. Apibendrinami gauti eksperimentinio tyrimo rezultatai.

3.2. Asmeninių įrenginių, naudojamų prieigai prie įmonės dokumentų failų, saugos sistemos prototipo eksperimentinio tyrimo rezultatai

Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos prototipo (DFSS) eksperimentinis tyrimas atliktas kartojant eksperimentą 3 kartus. Pirmojo eksperimentinio tyrimo metu gauti rezultatai pateikti 3.2 lentelėje.

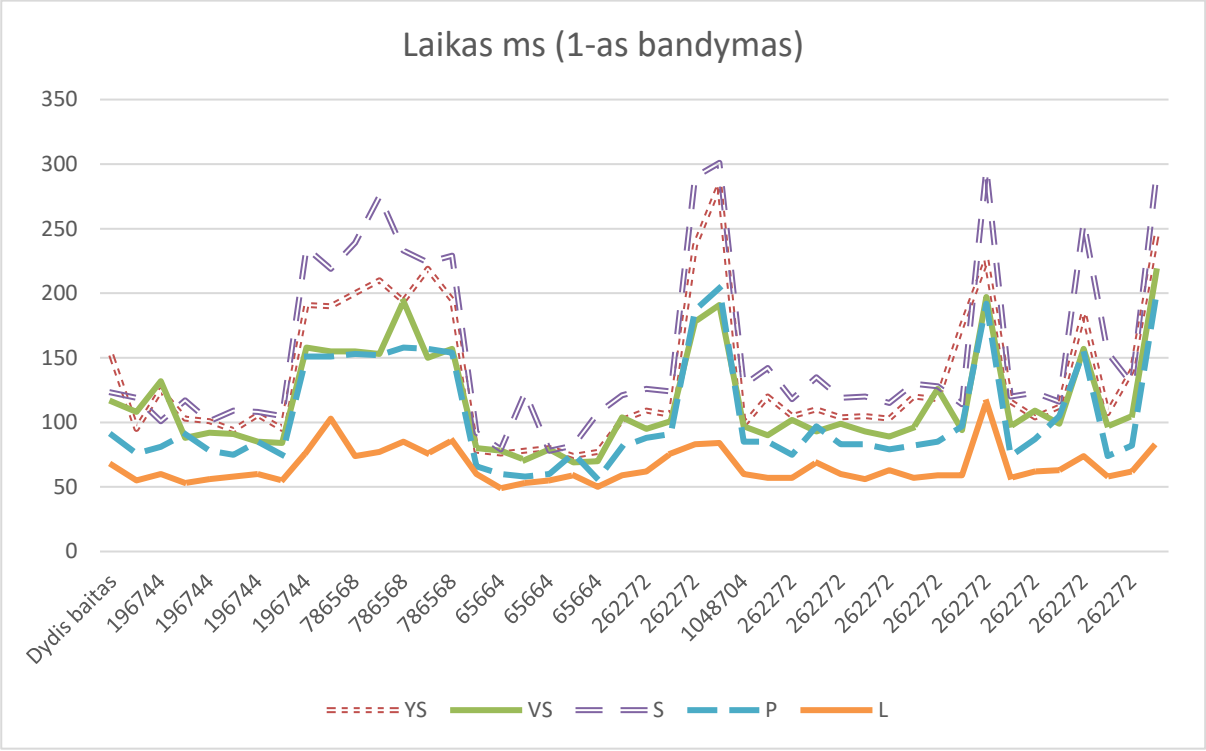
3.2 lentelė. Pirmojo bandymo metu gauti rezultatai

1-as bandymas						
	Dydis baitas	Laikas ms	Laikas ms	Laikas ms	Laikas ms	Laikas ms
Nr.		**YS**	**VS**	**S**	**P**	**L**
1	196744	150	116	123	90	67
2	196744	95	108	119	76	55

1-as bandymas						
	Dydis baitas	Laikas ms	Laikas ms	Laikas ms	Laikas ms	Laikas ms
Nr.		**YS**	**VS**	**S**	**P**	**L**
3	196744	125	132	101	81	60
4	196744	103	88	117	91	53
5	196744	101	92	101	78	56
6	196744	94	91	109	75	58
7	196744	106	85	108	85	60
8	196744	95	84	105	75	55
9	786568	191	158	235	151	77
10	786568	190	155	219	151	103
11	786568	200	155	239	153	74
12	786568	210	153	275	152	77
13	786568	194	194	233	158	85
14	786568	219	150	224	157	76
15	786568	195	157	229	154	86
16	65664	78	80	92	66	60
17	65664	76	78	79	60	49
18	65664	78	71	123	58	53
19	65664	80	79	78	60	55
20	65664	74	69	82	76	59
21	65664	77	70	107	56	50
22	262272	102	104	121	81	59
23	262272	109	95	126	88	62
24	262272	106	101	124	91	76
25	1048704	237	178	290	187	83
26	1048704	284	191	301	204	84
27	262272	98	97	129	85	60
28	262272	120	90	142	85	57
29	262272	105	102	118	75	57
30	262272	110	93	135	97	69
31	262272	104	99	119	83	60
32	262272	105	93	120	83	56
33	262272	103	89	115	79	63
34	262272	120	96	130	82	57
35	262272	118	126	128	85	59
36	262272	175	94	114	97	59
37	1048704	226	197	296	192	116
38	262272	116	97	120	74	57
39	262272	104	109	123	87	62
40	262272	112	99	116	105	63
41	786568	185	157	255	155	74
42	262272	107	97	154	74	58
43	262272	140	105	130	82	62
44	1048704	244	217	291	199	84

1-as bandymas						
Nr.	Dydis baitas	Laikas ms	Laikas ms	Laikas ms	Laikas ms	Laikas ms
		YS	**VS**	**S**	**P**	**L**
VISO		5961	5091	6795	4573	2905

Pirmojo bandymo tyrimo rezultatai grafiškai parodyti paveiksle 3.2.



3.2 pav. DFSS pirmojo eksperimentinio tyrimo rezultatai

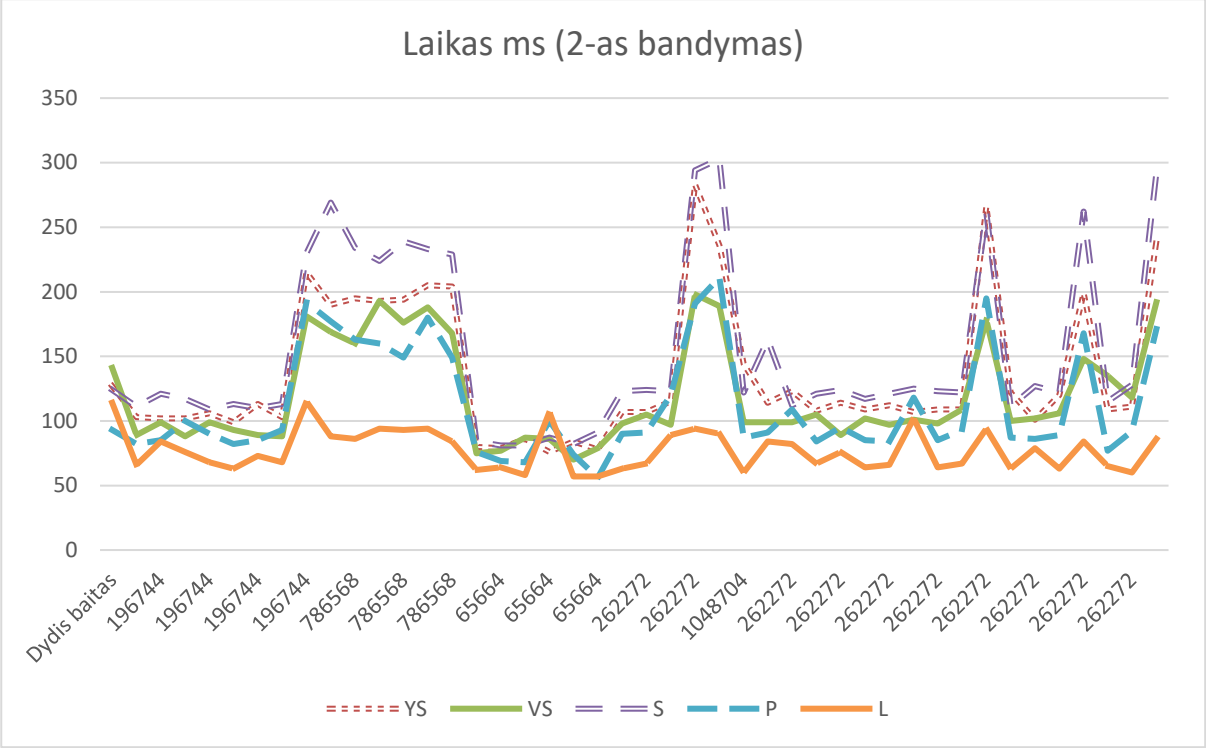
Antrojo eksperimentinio tyrimo metu gauti rezultatai pateikti 3.3 lentelėje.

3.3 lentelė. Antrojo eksperimentinio tyrimo metu gauti rezultatai

2-as bandymas						
Nr.	Dydis baitas	Laikas ms	Laikas ms	Laikas ms	Laikas ms	Laikas ms
		YS	**VS**	**S**	**P**	**L**
1	196744	127	141	124	93	114
2	196744	103	89	111	82	66
3	196744	102	99	121	85	84
4	196744	102	88	117	100	76
5	196744	106	99	109	90	68
6	196744	99	93	113	82	63
7	196744	113	89	110	85	73
8	196744	103	88	113	93	68
9	786568	215	181	230	192	115
10	786568	190	169	269	177	88

2-as bandymas						
	Dydis baitas	Laikas ms	Laikas ms	Laikas ms	Laikas ms	Laikas ms
Nr.		**YS**	**VS**	**S**	**P**	**L**
11	786568	195	160	234	163	86
12	786568	193	193	224	160	94
13	786568	194	176	239	149	93
14	786568	205	188	233	180	94
15	786568	204	168	229	149	84
16	65664	80	75	84	76	62
17	65664	79	77	81	69	64
18	65664	86	87	81	68	58
19	65664	76	86	87	100	107
20	65664	84	70	82	74	57
21	65664	78	79	91	56	57
22	262272	107	98	123	90	63
23	262272	107	105	124	91	67
24	262272	115	97	123	120	89
25	1048704	283	198	294	191	94
26	1048704	236	189	303	211	90
27	262272	144	99	122	87	60
28	262272	114	99	163	91	84
29	262272	123	99	112	109	82
30	262272	108	105	121	84	67
31	262272	114	89	124	95	76
32	262272	109	102	117	85	64
33	262272	112	97	121	84	66
34	262272	107	101	125	118	102
35	262272	109	98	123	85	64
36	262272	109	109	122	93	67
37	1048704	266	178	261	195	94
38	262272	122	100	111	87	63
39	262272	101	102	127	86	79
40	262272	120	106	122	89	63
41	786568	199	148	262	168	84
42	262272	109	135	115	77	65
43	262272	111	118	128	92	60
44	1048704	239	192	292	171	86
VISO		5998	5259	6717	4922	3400

Antrojo bandymo tyrimo rezultatai grafiškai parodyti paveiksle 3.3.



3.3 pav. DFSS antrojo eksperimentinio tyrimo rezultatai

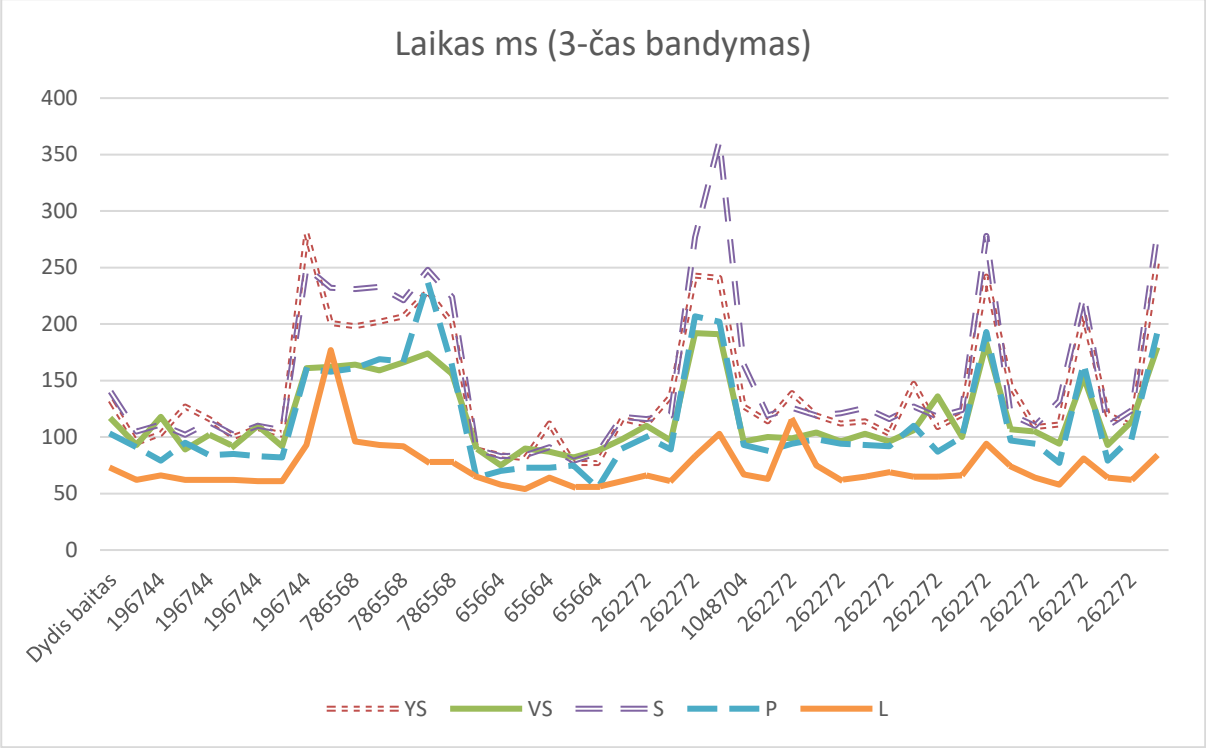
Trečiojo eksperimentinio tyrimo metu gauti rezultatai pateikti 3.4 lentelėje.

3.4 lentelė. Trečiojo eksperimentinio tyrimo metu gauti rezultatai

3-čas bandymas						
Nr.	Dydis baitas	Laikas ms **YS**	Laikas ms **VS**	Laikas ms **S**	Laikas ms **P**	Laikas ms **L**
1	196744	130	115	138	102	72
2	196744	95	93	105	91	62
3	196744	103	118	111	79	66
4	196744	127	89	102	95	62
5	196744	116	102	113	84	62
6	196744	100	92	102	85	62
7	196744	108	110	110	83	61
8	196744	102	92	106	82	61
9	786568	280	161	250	160	93
10	786568	201	162	232	158	177
11	786568	198	164	231	161	96
12	786568	202	159	233	169	93
13	786568	207	166	221	167	92
14	786568	229	174	248	237	78
15	786568	201	156	224	163	78
16	65664	89	90	89	64	65
17	65664	84	75	83	70	58
18	65664	81	90	84	73	54
19	65664	112	87	91	73	64

3-čas bandymas						
	Dydis baitas	Laikas ms	Laikas ms	Laikas ms	Laikas ms	Laikas ms
Nr.		**YS**	**VS**	**S**	**P**	**L**
20	65664	77	82	79	75	56
21	65664	77	88	86	55	56
22	262272	116	98	118	90	61
23	262272	111	110	116	100	66
24	262272	136	97	119	89	61
25	1048704	243	192	277	207	83
26	1048704	241	191	362	202	103
27	262272	127	96	164	93	67
28	262272	114	100	119	88	63
29	262272	139	99	126	94	116
30	262272	119	104	119	98	75
31	262272	112	96	121	94	62
32	262272	114	103	126	93	65
33	262272	103	96	116	92	69
34	262272	147	106	127	110	65
35	262272	109	136	118	87	65
36	262272	120	100	124	100	66
37	1048704	242	183	278	193	94
38	262272	145	107	120	97	74
39	262272	109	105	110	94	64
40	262272	111	94	132	77	58
41	786568	208	153	225	165	81
42	262272	120	93	110	79	64
43	262272	110	114	124	100	62
44	1048704	251	177	275	189	83
VISO		6266	5215	6664	4957	3235

Trečiojo bandymo tyrimo rezultatai grafiškai parodyti paveiksle 3.4.



3.4 pav. DFSS trečiojo eksperimentinio tyrimo rezultatai

DFSS prototipo eksperimentinio tyrimo rezultatų suvestinė pateikta 3.5 lentelėje. Joje pateikiama, kiek vidutiniškai laiko užtrunka atlikti procedūras pagal pasirinktą požymį su kiekvienu failu.

3.5 lentelė. DFSS prototipo eksperimentinio tyrimo rezultatų suvestinė

Eil. Nr.	Failo vardas	Aprašymas	Failo dydis baitais	Vaizdo taškų skaičius	Failo tipas	Bitų kiekis vienam taškui bits/pixel	Šifravimas RC2 ir DoD ištrynimas (YS)	Šifravimas AES ir DoD ištrynimas (VS)	Šifravimas 3DES ir DoD ištrynimas (S)	Šifravimas DES ir OS komanda „Delete“ (P)	Jokio šifravimo, OS komanda „Delete“ (L)
1	4.1.01	Girl	196744	256x256	Color	24	136	124	128	95	84
2	4.1.02	Couple	196744	256x256	Color	24	98	97	112	83	61
3	4.1.03	Girl	196744	256x256	Color	24	110	116	111	82	70
4	4.1.04	Girl	196744	256x256	Color	24	111	88	112	95	64
5	4.1.05	House	196744	256x256	Color	24	108	98	108	84	62
6	4.1.06	Tree	196744	256x256	Color	24	98	92	108	81	61
7	4.1.07	Jelly beans	196744	256x256	Color	24	109	95	109	84	65
8	4.1.08	Jelly beans	196744	256x256	Color	24	100	88	108	83	61
9	4.2.01	Splash	786568	512x512	Color	24	229	167	238	168	95
10	4.2.02	Girl (Tiffany)	786568	512x512	Color	24	194	162	240	162	123
11	4.2.03	Mandrill (a.k.a. Baboon)	786568	512x512	Color	24	198	160	235	159	85
12	4.2.04	Girl (Lena, or Lenna)	786568	512x512	Color	24	202	168	244	160	88
13	4.2.05	Airplane (F-16)	786568	512x512	Color	24	198	179	231	158	90
14	4.2.06	Sailboat on lake	786568	512x512	Color	24	218	171	235	191	83

Eil. Nr.	Failo vardas	Aprašymas	Failo dydis baitais	Vaizdo taškų skaičius	Failo tipas	Bitų kiekis vienam taškui bits/pixel	Šifravimas RC2 ir DoD ištrynimas (YS)	Šifravimas AES ir DoD ištrynimas (VS)	Šifravimas 3DES ir DoD ištrynimas (S)	Šifravimas DES ir OS komanda „Delete“ (P)	Jokio šifravimo, OS komanda „Delete“ (L)
15	4.2.07	Peppers	786568	512x512	Color	24	200	160	227	155	83
16	5.1.09	Moon surface	65664	256x256	Gray	8	82	82	88	69	62
17	5.1.10	Aerial	65664	256x256	Gray	8	80	77	81	66	57
18	5.1.11	Airplane	65664	256x256	Gray	8	82	83	96	66	55
19	5.1.12	Clock	65664	256x256	Gray	8	89	84	85	78	75
20	5.1.13	Resolution chart	65664	256x256	Gray	8	78	74	81	75	57
21	5.1.14	Chemical plant	65664	256x256	Gray	8	77	79	95	56	54
22	5.2.08	Couple	262272	512x512	Gray	8	108	100	121	87	61
23	5.2.09	Aerial	262272	512x512	Gray	8	109	103	122	93	65
24	5.2.10	Stream and bridge	262272	512x512	Gray	8	119	98	122	100	75
25	5.3.01	Man	1048704	1024x1024	Gray	8	254	189	287	195	87
26	5.3.02	Airport	1048704	1024x1024	Gray	8	254	190	322	206	92
27	7.1.01	Truck	262272	512x512	Gray	8	123	97	138	88	62
28	7.1.02	Airplane	262272	512x512	Gray	8	116	96	141	88	68
29	7.1.03	Tank	262272	512x512	Gray	8	122	100	119	93	85
30	7.1.04	Car and APCs	262272	512x512	Gray	8	112	101	125	93	70
31	7.1.05	Truck and APCs	262272	512x512	Gray	8	110	95	121	91	66

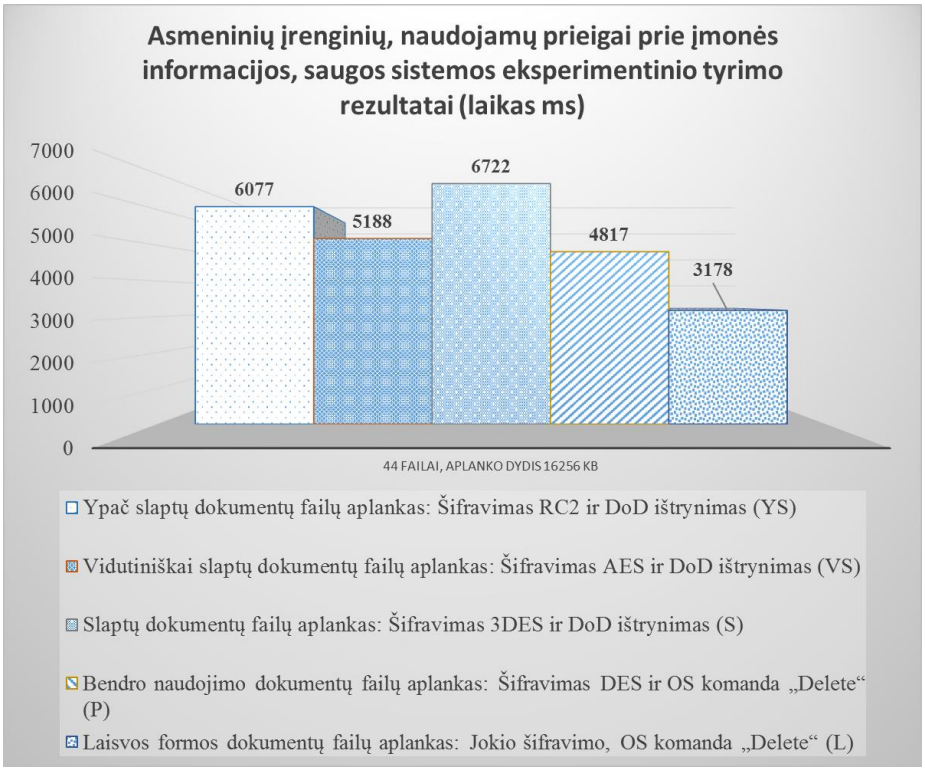
Eil. Nr.	Failo vardas	Aprašymas	Failo dydis baitais	Vaizdo taškų skaičius	Failo tipas	Bitų kiekis vienam taškui bits/pixel	Šifravimas RC2 ir DoD ištrynimas (YS)	Šifravimas AES ir DoD ištrynimas (VS)	Šifravimas 3DES ir DoD ištrynimas (S)	Šifravimas DES ir OS komanda „Delete“ (P)	Jokio šifravimo, OS komanda „Delete“ (L)
32	7.1.06	Truck and APCs	262272	512x512	Gray	8	109	99	121	87	62
33	7.1.07	Tank	262272	512x512	Gray	8	106	94	117	85	66
34	7.1.08	APC	262272	512x512	Gray	8	125	101	127	103	75
35	7.1.09	Tank	262272	512x512	Gray	8	112	120	123	86	63
36	7.1.10	Car and APCs	262272	512x512	Gray	8	135	101	120	97	64
37	7.2.01	Airplane (U-2)	1048704	1024x1024	Gray	8	245	186	278	193	101
38	boat.512	Fishing Boat	262272	512x512	Gray	8	128	101	117	86	65
39	elaine.512	Girl (Elaine)	262272	512x512	Gray	8	105	105	120	89	68
40	gray21.512	21 level step wedge	262272	512x512	Gray	8	114	100	123	90	61
41	house	House	786568	512x512	Color	8	197	153	247	163	80
42	numbers.512	256 level test pattern	262272	512x512	Gray	8	112	108	126	77	62
43	ruler.512	Pixel ruler	262272	512x512	Gray	8	120	112	127	91	61
44	testpat.1k	General test pattern	1048704	1024x1024	Gray	8	245	195	286	186	84
		IŠ VISO	17176192				6077	5188	6722	4817	3178

3.6 lentelėje pateikti apibendrinti eksperimentinio tyrimo metu užfiksuoti vidutiniai laikai atliekant pasirinktą metodą su visais failais.

3.6 lentelė. Apibendrinta DFSS prototipo eksperimentinio tyrimo rezultatų suvestinė

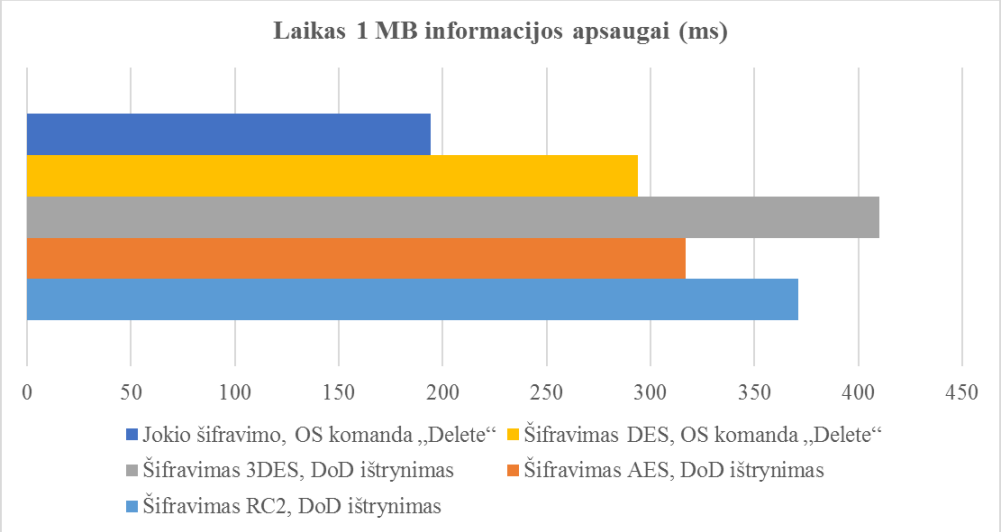
Įmonės dokumentų failų serverio aplankas	Aplanko failų skaičius	Aplanko dydis KB	Sistemos taikomas saugos metodas	Eksperimentinio tyrimo užfiksuotas laikas (ms)
Ypač slaptų dokumentų failų aplankas	44	16256	Šifravimas RC2 ir DoD ištrynimas	6077
Vidutiniškai slaptų dokumentų failų aplankas	44	16256	Šifravimas AES ir DoD ištrynimas	5188
Slaptų dokumentų failų aplankas	44	16256	Šifravimas 3DES ir DoD ištrynimas	6722
Bendro naudojimo dokumentų failų aplankas	44	16256	Šifravimas DES ir OS komanda „Delete“	4817
Laisvos formos dokumentų failų aplankas	44	16256	Jokio šifravimo, OS komanda „Delete“	3178

Asmeninių įrenginių, naudojamų prieigai prie įmonės informacijos, saugos sistemos prototipo eksperimentinio tyrimo rezultatai grafiškai parodyti paveiksle 3.5.



3.5 pav. Apibendrinti DFSS eksperimentinio tyrimo rezultatai

Apibendrinti atlikto eksperimentinio tyrimo rezultatai perskaičiuoti 1MB informacijos grafiškai parodyti paveiksle 3.6 pav.



3.6 pav. Apibendrinti DFSS eksperimentinio tyrimo rezultatai 1MB informacijos

3.3. Išvados

Eksperimentinio tyrimo metu nustatyta:

- Didėjant failų dydžiui matome, kad atlikti šifravimo ir saugaus trynimo procedūras užtrunka ilgiau;
- Ilgiausiai laiko užtrunka pasirinkus S (Slaptas) požymį, kuris naudoja 3DES šifravimą ir DoD trynimą.
- Trumpiausiai laiko užtrunka pasirinkus L (Laisvos formos) požymį, kuris nenaudoja šifravimo, bet naudoja OS ištrynimo komandą.

4. IŠVADOS

Išanalizuoti trys pagrindiniai asmeninių įrenginių organizacijose saugumo modeliai - mobiliųjų įrenginių valdymo modelis, mobiliųjų programėlių valdymo modelis, mobiliosios informacijos valdymo modelis.

Nustatyta, kad taikant mobiliųjų įrenginių valdymo modelį asmeninis įrenginys, naudojamas įmonėse, gyvavimo cikle gali būti vienos iš trijų skirtingų būsenų: nepatikima, patikima ir naudojama nuosavybė. Kai prietaisas yra nepatikimos būsenos, nei organizacija, nei kas nors iš jos darbuotojų negali būti laikomi atsakingi už tą įrenginį. Kai prietaisas yra pažymimas nepatikimu, jokie svarbūs organizacijos duomenys negali būti saugomi ir prietaisas negali būti prijungtas prie verslo tinklų. Kai prietaisas yra patikimos būsenos, tik organizacija yra atsakinga už tą įrenginį. Šios būsenos prietaisas gali saugoti jautrius verslo duomenis.

Nustatyta, kad asmeninių įrenginių, naudojamų įmonėse, mobiliųjų programėlių valdymo modelis yra sprendimas, naudojamas IT administratorių, siekiant nuotoliniu būdu įdiegti, atnaujinti, ištrinti, vesti auditą ir stebėti su įmone susijusias programėles mobiliuosiuose įrenginiuose. Skirtingai nei MDM, kuris kontroliuoja mobiliuosius prietaisus aparatūros lygyje, mobiliųjų programėlių valdymo sistemos stebi ir kontroliuoja tam tikras programas siekdamos, kad būtų laikomasi organizacijos politikos ir reikalavimų.

Nustatyta, kad asmeninių įrenginių, naudojamų įmonėse, informacijos valdymo modelio pagrindas - nesaugoti kritinės įmonių informacijos mobiliuosiuose įrenginiuose. Pagrindinis MIM tikslas yra išsaugoti įmonės informaciją tinklo saugykloje ir saugiai dalintis informacija tarp skirtingų vartotojų ir platformų. MIM leidžia kontroliuoti ir valdyti tik ribotą patikimų programų kiekį ir šifruotus įmonių duomenis.

Nepriklausomai nuo privalumų ir trūkumų minėti saugumo modeliai orientuojasi tik į ribotus sprendimus ir apsaugą ir tik į įrenginių valdymą (MDM), programėles (MAM) ir informaciją (MIP), remiantis tam tikra politika.

Pasiūlytas AĮ, naudojamų prieigai prie įmonės informacijos, DFSS modelis sudarytas iš dviejų dalių PĮ: kliento ir serverio. Suprojektuota dokumentų failų saugos sistemos architektūra ir kliento ir serverio PĮ vykdomos komandos. Pasiūlyti kliento PĮ dokumentų failų registravimo požymiai ir saugumo veiksmai.

Sukurtas AĮ, naudojamų prieigai prie įmonės informacijos, DFSS sistemos prototipas. Prototipas sukurtas naudojant Microsoft .NET Framework C# programavimo kalbą ir Visual Studio 2015 programų projektavimo įrankį.

Sukurtas DFSS prototipo eksperimentinio tyrimo scenarijus. Sukurta DFSS eksperimentinio tyrimo aplinka ir atliktas sukurto DFSS prototipo eksperimentinis tyrimas.

Eksperimentinio tyrimo metu nustatyta:

- Didėjant failų dydžiui matome, kad atlikti šifravimo ir saugaus trynimo procedūras užtrunka ilgiau;
- Ilgiausiai laiko užtrunka pasirinkus S (Slaptas) požymį, kuris naudoja 3DES šifravimą ir DoD trynimą;
- Trumpiausiai laiko užtrunka pasirinkus L (Laisvos formos) požymį, kuris nenaudoja šifravimo, bet naudoja OS ištrynimo komandą.

5. LITERATŪRA

[1] K. Rhee, D. Won, S.-W. Jang, S. Chae, and S. Park, "Threat modeling of a mobile device management system for secure smart work," Electronic Commerce Research, pp. 1-14, 2013.

[2] A. Scarfo, "New Security Perspectives around BYOD," in Proceedings of the Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012, pp. 446- 451.

[3] K. Rhee, W. Jeon, and D. Won, "Security Requirements of a Mobile Device Management System," International Journal of Security and Its Applications, vol. 6, pp. 353-358, 2012.

[4] H. Kwon and S.-H. Kim, "Efficient Mobile Device Management Scheme Using Security Events from Wireless Intrusion Prevention System," in Ubiquitous Information Technologies and Applications. vol. 214, ed: Springer Netherlands, 2013, pp. 815-822.

[5] H. Kwon and S.-H. Kim, "A Mobile Device Classification Mechanism for Efficient Prevention of Wireless Intrusion " presented at the The 2nd International Conference on Information Science and Industrial Applications (SERSC), Guam, USA, 2013.
[6] P. WINTHROP. (2009). UNIFYING MOBILE APPLICATION MANAGEMENT WITH MOBILE DEVICE MANAGEMENT. Galima parsisiųsti: http://theemf.org/2009/10/15/unifying-application-management-withdevice-management/

[7] C. Knight. (2013). Mobile Application Management. Galima pasiekti: http://forms.kony.com/rs/konysolutions/images/WP_Kony_MAM.pdf

[8] A. Armando, G. Costa, and A. Merlo, "Bring your own device, securely," presented at the 28th Annual ACM Symposium on Applied Computing, Coimbra, Portugal, 2013.

[9] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," Communications Surveys & Tutorials, IEEE, vol. PP, pp. 1-26, 2012.

[10] S. Donaldson, S. Siegel, C. Williams, and A. Aslam, “Enterprise Cybersecurity,” Apress, pp. 119–129, 2015.

[11] M. Souppaya and K. Scarfone, “NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise,” p. 30, 2013.

[12] “Publication Number : Title : Publication Date : NIST Special Publication (SP) 800-46 Rev . 2 Guide to Enterprise Telework , Remote Access , and Bring Your Own Device (BYOD) Security • Final Publication : http://dx.doi.org/10.6028/NIST.SP.800-46r2 (wh,” vol. 2, 2016.

[13] A. A. Morufu Olalere, Mohd Taufik Abdullah, Ramlan Mahmod, “Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication,” vol. 4, no. 1, pp. 21–32, 2016.

[14] W. . Zikmund, J. . Babin, and M. Griffin, Business Research Methods. 2012.

[15] A. R. Ommani, “Strengths, weaknesses, opportunities and threats (SWOT) analysis for farming system businesses management: Case of wheat farmers of Shadervan District , Shoushtar Township, Iran,” African J. Bus. Manag., vol. 5, no. 22, pp. 9448–9454, 2010.

[16] V. Samaras, S. Daskapan, R. Ahmad, and S. K. Ray, “An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD,” 11th Australas. Telecommun. Networks Appl. Conf., no. July, pp. 1–6, 2015.

[17] K. Downer and M. Bhattacharya, “BYOD Security : A New Business Challenge,” 5th Int. Symp. Cloud Serv. Comput. (SC2 2015), pp. 1128–1133, 2016.

[18] J. Viega and B. Michael, “Mobile Device Security,” IEEE Secur. Priv. Mag., vol. 8, no. 2, pp. 99–101, 2010.

[19] A. Scarfo, “New security perspectives around BYOD,” in Proceedings - 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2012, 2012, pp. 446–451.

[20] M. Souppaya and K. Scarfone, “User’s Guide to Telework and Bring Your own Device (BYOD) security,” NIST Spec. Publ. 800-114, 2016.

[21] N. Leavitt, “Today’s mobile security requires a new approach,” Computer (Long. Beach. Calif)., vol. 46, no. 11, pp. 16–19, 2013.

[22] R. Review, “Q4 Mobile Security and Risk Review,” pp. 1–13, 2016

[23] “Why mdm needs standalone mam,” p. 8740.

[24] K. Scarfone and P. Hoffman, “Guide to Security for Full Virtualization Technologies Recommendations of the National Institute of Standards and Technology,” Natl. Inst. Stand. Technol. Spec. Publ., no. 800–125, pp. 1–35, 2010.

[25] M. A. Delivery and T. N. Frontier, “1 2 3 4.”

[26] S. Butler, “Must-Have Capabilities to Optimise Enterprise Mobility,” pp. 1–7, 2014.

[28] Jack Madden, “In 2016, many of the tools and concepts for enterprise mobility are ready to go.”

[29] Research In Motion Ltd., BlackBerry Business Solutions, April 7, 2010, http://na.blackberry.com/eng/solutions.

[30] Igure, V. M., Laughter, S. A., and Williams, R. D. 2006. Security issues in SCADA networks. Computers & Security. 25, 7, 498-506.

[31] The USC-SIPI Image Database. Galima pasiekti: http://sipi.usc.edu/database/database.php?volume=misc