KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
PROGRAMŲ INŽINERIJOS KATEDRA

Kęstutis Morkūnas

# LOKALAUS TINKLO INCIDENTŲ MONITORINGO PROGRAMINĖS ĮRANGOS PROJEKTAVIMAS IR TYRIMAS

Magistro darbas

Darbo vadovas:
dr. E. Bareiša

KAUNAS, 2006

**KAUNO TECHNOLOGIJOS UNIVERSITETAS**
**INFORMATIKOS FAKULTETAS**
**PROGRAMŲ INŽINERIJOS KATEDRA**

Kęstutis Morkūnas

# LOKALAUS TINKLO INCIDENTŲ MONITORINGO PROGRAMINĖS ĮRANGOS PROJEKTAVIMAS IR TYRIMAS

MAGISTRO DARBAS

Kalbos konsultantė
Lietuvių k. katedros lekt.
dr. J. Mikelionienė
2006–05

Mokslinis vadovas
dr. E. Bareiša
2006–05

Recenzentas
doc. dr. Antanas Lenkevičius
2006–05

Atliko
IFM 0/2 gr. stud.
Kęstutis Morkūnas
2006–05–25

KAUNAS, 2006

# Lokalaus tinklo incidentų monitoringo programinės įrangos projektavimas ir tyrimas

# Local Area Networks Accident Monitoring Software Design and Research

*Summary*

Monitoring is an important activity in daily local area network maintance routine. To be able to run the network efficiently and without incidents that run into problems, networks must be monitored. This way it is possible to detect and remove serious problems at early stages. Various techniques are employed, including monitoring and checking users actions, data traffic, active running processes, open ports and system log analysis.

This thesis describes a method for engineering and implementing local area networks software and using it for field data analysis. In the process of writing this thesis such sample of software was created and aimed at the processes and event logs of Kaunas University of Technology Software Engineering Department.

In the conclusion methods and ways that will help solve current problems were suggested. Most alarming thing to notice was constant port scans and illegal attempts to log into the system without permission.

# Turinys

# Paveikslų sąrašas



# Lentelių sąrašas

# 1. Įvadas

Sukūrus kompiuterius atsirado poreikis jungti juos į bendrą tinklą ir keistis informacija. ARPANET projekto, kuris tapo kompiuterių tinklų ir interneto ištakomis, metu taip buvo užtikrinta kompiuterinio susisiekimo garantija karo atveju. Kuriantis įvairaus dydžio tinklams iškilo poreikis juos tinkamai prižiūrėti ir tinkamai išnaudoti. Daug programinės įrangos paketų yra skirti padėti vartotojams dirbti tinkle. Juos naudojant greičiau aptinkamos atsiradusios problemos, užtikrinamas esamo tinklo sklandus veikimas, siūlomos naujos paslaugos ir galimybės. Dauguma šių programų labai gerai atlieka vieną ar kelis veiksmus, tačiau nėra apjungtos į bendrą visumą. Vartotojai dažnai neturi laiko naudoti kelias ar keliolika programų vienu metu, todėl patogios naudoti programos apjungia įvairių įrankių galimybes į vieną bendrą visumą.

Tinklo stebėjimo priemonės teikia naujų idėjų kaip būtų galima organizuoti darbo optimizavimą bei galimų problemų išankstinį aptikimą ir išvengimą. Pavyzdžiui:

- Serveryje veikiančių procesų, susijusių su darbu tinkle, stebėjimas (HTTP, FTP, SSH, SMTP servisai, jų gyvybingumas ir panaudojamumas esamu laiko momentu).
- Duomenų srauto, keliaujančio per serverį, stebėjimas (elektroninių virusų ar kirminų protrūkio pastebėjimas, Ping of Death ir kitos atakos ir pan.).
- Vietinio tinklo vartotojų veiklos tinkle stebėjimas (atverti susijungimo taškai, užkrėsti virusais laiškai, šnipinėjimo programos)
- Servisų veiklos įrašų peržiūra ir analizė (nepavykusių susijungimų, nerastų failų, suklastotų antraščių (angl. *headers*) stebėjimas) [1].

# 2. Lokalaus tinklo incidentų monitoringo problemos analizė

## *2.1 Tikslas*

Šiame darbe egzistuoja trys dideli skyriai: problemos analizė, programinės įrangos problemai spręsti projektavimas ir kūrimas, eksperimentinis programinės įrangos patikrinimas ir panaudojimas realių Programų inžinerijos katedros serverių įrašų analizei.

Problemos analizės skyriaus tikslas yra išanalizuoti egzistuojančioms srities problemoms, apsibrėžti darbo tikslus ir kryptis, nustatyti laukiamus rezultatus. Apžvelgti panašius projektus, sprendimus ir vystymo kryptis pasaulyje. Išnagrinėti įstatymų nustatytas taisykles darbui su duomenimis ir vartotojų veiklos stebėjimui.

Programinės įrangos projektavimo ir realizavimo skyriaus tikslas yra skirtas suprojektuoti ir įgyvendinti lokalaus tinklo stebėjimo programinę įrangą, kuri bus naudojama eksperimente.

Tiriamojoje ir eksperimentinėje dalyje eksperimentuojama naudojant sukurtą programinę įrangą ir realius Programų inžinerijos katedros serverių veiklos įrašus. Ši informacija naudojama bandant aptikti esmines vietinio kompiuterių tinklo ir serverių problemas, formuluojant galutines išvadas ir siūlant pastebėtų problemų sprendimo būdus.

## *2.2. Pagrindinės sąvokos*

### 2.2.1. Incidento apibrėžimas.

Incidentas – žmogaus veiklos įtakotas ar natūraliai susidaręs įvykis kuriam nutikus reikia avarinės tarnybos įsikišimo siekiant sumažinti nuostolius gyvybei, nuosavybei ar gamtai.

Kompiuterijoje incidento apibrėžimas toks:

Tai įvykiai, kurie pažeidžia normalų kompiuterių/tinklo veikimą, prieštarauja tinklo saugumo taisyklėms, galiojantiems įstatymams. Visi tokie nepageidautini reiškiniai apibrėžiami kaip kompiuterinis saugumo incidentas. Formalus kompiuterinio incidento apibrėžimas yra toks:

Kompiuterinis incidentas – realų ar potencialiai nepageidaujamą poveikį kompiuterio ar kompiuterių tinklo veiklai turintis įvykis, kurio rezultatas – apgaulė, nuostoliai ar piktnaudžiavimas, grėsmė informacijai, informacijos nuosavybės praradimas ar žala jai. Pavyzdžiui, skverbimasis į kompiuterines sistemas, techninių pažeidžiamumų išnaudojimas, kompiuterinių virusų ar kitokios nepageidaujamos programinės įrangos įdiegimas.

Kompiuteriniai saugumo incidentais dažnai laikomi tokie įvykiai:

- įsilaužimai į sistemą
- bandymai įsilaužti į sistemą
- servisų darbo trikdymas, DoS ataka
- sistemos, programinės įrangos, informacijos pakeitimas be savininko žinios ar leidimo
- įstatymus pažeidžiantys veiksmai
- vagystės
- apgavystės
- grėsmė žmonių saugumui
- vaikų pornografija
- kita neleistina veikla
- tinklo skenavimas
- paslaugų skenavimai
- TNP pažeidimai (etikos pažeidimai, kt.)
- Intelektinės nuosavybės vagystės [18].

Paprastai, tiriant kompiuterinius incidentus, didesnis prioritetas yra suteikiamas atakoms, nukreiptoms prieš (išvardinta prioriteto mažėjimo tvarka)

- Žmogaus gyvybę, asmens saugumą
- Tinklo infrastruktūrą (*backbone* maršrutizatoriai, vardų (DNS) serveriai, archyvų serveriai, tinklo prieiga)
- Didelius viešo naudojimo serverius, daugiavartotojiškas sistemas, specialios paskirties sistemas
- Asmeninius kompiuterius
- Pavienius vartotojus (el. pašto dėžutes) [18].

### 2.2.2. Monitoringo apibrėžimas

Monitoringas apibrėžiamas taip: nuolatinis būsenos stebėjimas naudojamas norint aptikti ir įspėti apie pokyčius.

Šiame darbe monitoringas nusako veiksmus, kuriais stebimas vietinis kompiuterių tinklas bei serveriuose ir kompiuteriuose esanti informacija. Tai atliekama siekiant lengviau išspręsti esamas problemas bei formuoti išankstinio įspėjimo apie galimas problemas galimybę.

### 2.2.3. Kiti terminai

**Filtravimo priemonės** – programinė įranga, išskirianti pageidaujamą arba ribojanti nepageidaujamą kompiuterių tinklų informaciją pagal vartotojo nustatytus parametrus [19].

**Informacijos platinimas kompiuterių tinkluose** – informacijos pateikimas elektroninėse visuomenės informavimo priemonėse arba kituose interneto tinklalapiuose, siuntimas elektroniniu paštu neapibrėžtam gavėjų skaičiui arba pagal iš anksto sudarytus sąrašus, skleidimas elektroninėse konferencijose arba pateikimas visuomenei kitokiu viešai prieinamu būdu viešo naudojimo kompiuterių tinkluose, nesvarbu, ar paslauga mokama [19].

**Informacijos prieglobos paslaugų teikėjas** – asmuo, faktiškai teikiantis interneto tinklalapių prieglobos (angl. *hosting*) viešo naudojimo kompiuterių tinkluose paslaugas [19].

**Sisteminių įrašų byla (angl. *log file*)–** automatiškai generuojama byla, kurioje įrašyta informacija apie veiklą tarnybinėje stotyje [19].

**Neskelbtina informacija** – informacija, kurią paviešinti ir (ar) platinti draudžia Lietuvos Respublikos įstatymai [19].

**Protokolas** – duomenų formatą ir perdavimą apibrėžiančios taisyklės [19].

**Tinklo paslaugų teikėjas** – Lietuvos Respublikoje įregistruotas juridinis asmuo, teikiantis informacijos perdavimo viešo naudojimo kompiuterių tinklais arba prieigos prie šių tinklų paslaugas [19].

### 2.2.4. Egzistuojantys sprendimai.

Yra programinės įrangos realizacijų, kurios įgyvendina panašias galimybes. Apžvelgiau keletą pagrindinių mokamų ir nemokamų programų, apie kurias informacija laisvai prieinama internete.

## Castle Rock Computing. SNMP programinė įranga.

Ši kompanija siūlo tik mokamas programos versijas: pilna, skirta labai dideliems tinklams ir riboto funkcionalumo, skirta mažoms ir vidutinėms įmonėms, kurioms pilno programos funkcionalumo gali neprireikti ir/ar kurios nėra linkę mokėti kūrėjų prašomos

sumos už programinę įrangą. Nuo mano kurtos programinės įrangos tuo, kad neturi klientinės programos atskirų vartotojų veiklos tinkle stebėjimui.

Pagrindinis dėmesys skiriamas įvairių vartotojų grupių kūrimui bei administravimui. Daug programos modulių skirta skirtingų architektūrų tinklų palaikymui bei įvairių protokolų panaudojimui [2].

Pasirinkti sprendimai ir sukurtas funkcionalumas: WAN tinklų, serverių bei programų veiklos stebėjimas, per atstumą prieinamas valdymo punktas, internetu pateikiamos ataskaitos apie tinklo būseną, tinklo aptikimas ir jame esančių įrenginių analizė, veikia kaip Windows servisas.

Projektą realizuojant buvo pasirinkta naudoti Microsoft Windows šeimos operacines sistemas, nes produktą ketinta parduoti rinkoje, kurioje dominuoja Microsoft produkcija. Taip pat stengtasi pritaikyti paprastą programos versiją mažiau patyrusiems administratoriams.

## „Kimono" programinė įranga

Ši programinė įranga yra nemokama. Kaip ir daugelis OpenSource tipo programų, yra besitęsiančios kūrybos stadijoje. Galimybių plėtojimas ir palaikymas retai būna reguliarus, kadangi visas kūrimo procesas vyksta kelių ar keliolikos entuziastų dėka. Taip pat nėra garantuojamas bent jau minimalus tęstinis programinės įrangos palaikymas [3]. „Kimono'' programa skirta paties serverio, o ne tinklo veiklos stebėjimui, tačiau ji stebi ir su darbo tinkle ar tinklo palaikymu susijusius sistemos procesus.

Šios programos autorius pasirinko objektinę programavimo kalbą – PHP, kadangi programas, rašytas šio tipo kalbomis paprasčiau plėsti ir palaikyti [4].

Ši programa veikia UNIX šeimos operacinėse sistemose su instaliuotu *Apache* serveriu, palaikančiu *MySql* duomenų bazes ir *PHP* programavimo kalbą. Pasiekiama naudojant naršyklę [15].

Realizuotos galimybės: serverio servisų gyvybingumo, pasiekiamumo bei panaudojamumo stebėjimas, veiklos analizė, pasiekiama tiek per naršyklę tiek ir per komandinę eilutę, naujų servisų įtraukimas, senų šalinimas, parametrų keitimas, galimybė stebėti resursų išnaudojimą bei užklausų įvykdymo greitį [4].

## AdRem NetCrunch.

AdRem kompanija sukūrė NetCrunch. Programinė įranga yra mokama ir skirta didesnės apimties tinklams. Veikia Windows aplinkoje. Kuriant programą įgyvendintas

įdomus tinklų kelių aptikimo modulis, nestandartinių tinklų aptikimo, analizės ir atvaizdavimo galimybė, išvystyta pranešimų apie atsiradusias problemas idėja [5].

Programinė įranga teikia tokias galimybes: įvairių tinklų stebėjimas ir veiklos analizė, aptiktų tinklų žemėlapio sudarymas, atsiradusių problemų automatinis taisymas be administratoriaus įsikišimo [5].

## *2.3. Darbuotojai susiję su kompiuterinio tinklo priežiūra ir monitoringu*

Kompiuterinių tinklų bei sistemų priežiūrą ir monitoringą dažniausiai atlieka šie darbuotojai:

- Sistemų administratorius – kompiuterinių sistemų bei programinės įrangos techninė priežiūra ir aptarnavimas. Tiesioginis bendravimas su klientais. Bendradarbiavimas su darbuotojais, vystančiais, diegiančiais ir prižiūrinčiais organizacijos sistemas ir infrastruktūrą.
- Tinklo administratorius – užtikrinti organizacijos ar organizacijų grupės kompiuterių tinklo veikimą ir vystymą.
- Duomenų bazių administratorius – Duomenų bazių priežiūra ir aptarnavimas.
- Incidentų sprendėjas – Spręsti vartotojų užklausas, teikti pirminę pagalbą vartotojams, nustatant problemos pobūdį ir suteikiant informaciją apie sprendimo kelius. Užtikrinti incidentų išsprendimą per nustatytą laiką.

## *2.4. Monitoringo panaudojimas darbiniuose procesuose*

Monitoringas gali būti naudingas kai naudojamas šiuose darbo procesuose:

- Org. technikos įrengimas ir aptarnavimas
- Vartotojų kompiuterinių darbo vietų priežiūra
- Serverių priežiūra
- Duomenų bazių priežiūra

## *2.5. Įrašų failai ir jų palyginimas*

Įrašų failuose sistema kaupia informaciją apie įvairius įvykius sistemoje. Dauguma šios informacijos yra įprastinė ir incidentų požiūriu nesvarbi. Šie duomenys gali būti kaupiami labai įvairiai: tekstiniuose failuose, duomenų bazėse ir pan.

Šiame darbe nagrinėjami dviejų protokolų (Linux ir HTTP) įrašų kaupimo būdai. Analizės metu atrenkami tik tie įrašai kurie yra susiję su incidentais ir problemomis.

Linux OS sistemos įvykių registravimo sistema informacijos kaupimui naudoja tokią struktūrą:

*1 lentelė. Prisijungimo Linux sistemoje įrašo pavyzdys*

| Įvykio data | Serverio vardas | Įvykį sąlygojęs procesas | Įvykis | Susijęs tinklo šaltinis (IP) |
|---|---|---|---|---|
| Jan 15 06:07:38 | diedas | sshd[16359]: | Illegal user rpc | ::ffff:161.53.131.204 |

*Apache* žiniatinklio serveris naudoja:

access.log – įrašams apie visus prisijungimus

error.log – įrašams apie klaidas

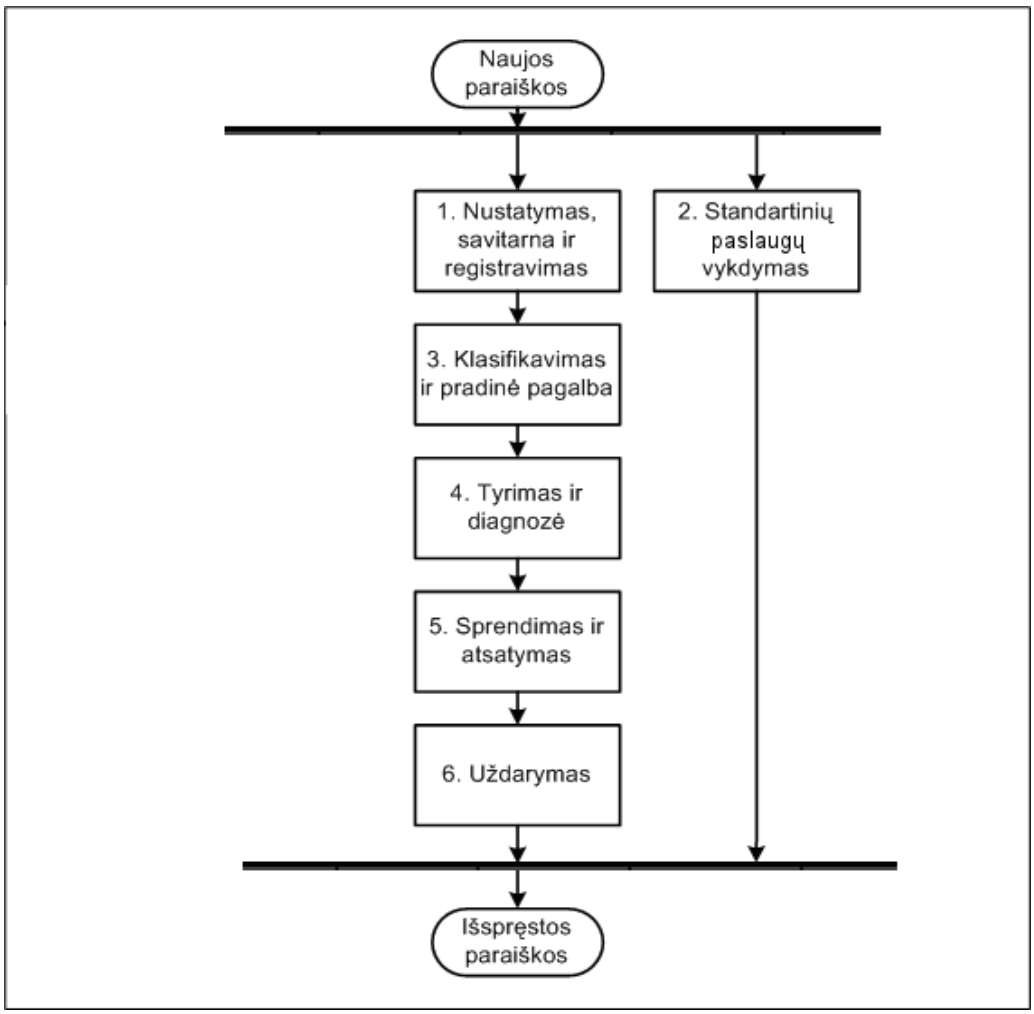
suexec.log – informacija apie CGI naudojimą.

*2 lentelė. Paslaugų (servisų) pokyčių įrašo pavyzdys*

| Įvykio data | Įvykio tipas | Serverio ir žiniatinklio serverio vardai | Įvykis |
|---|---|---|---|
| Jan 15 06:07:38 | diedas | sshd[16359]: | configured -- resuming normal operations |

## *2.6. Incidentų valdymas*

Šis procesas apima visus veiksmus, susijusius su klientų užsakymų paraiškų valdymu: poreikių (tame tarpe ir incidentų registravimą) identifikavimą, klasifikavimą, prioriteto suteikimą, paskirstymą, pradinės pagalbos suteikimą, išsprendimą bei eskalavimą, kai servisas nesuteikiamas per nustatytą laiką.




*1 pav. Bendra incidentų sprendimo schema*

Šiame dokumente aptariami rekomenduojami darbo organizavimo principai išskiriant pagal IT veiklos sritis.

Programų inžinerijos katedros incidentų valdymo padalinys organizuojamas remiantis pagrindiniais užklausų tipais:

- Vidinis katedros tinklas ir ryšys jame.
- Serverių ir servisų veikimo užtikrinimas. Elektroninis paštas, SSH ir HTTP protokolai.
- Išorinis tinklas (LITNET klausimai) [21]
- Kompiuterinė įranga (PC, organizacinė technika)
- Programinė įranga
- Infrastruktūra (tarnybinės stotys, vidinis tinklas, telefonija)

Sąrašas nėra baigtinis ir vystantis katedrai gali būti papildytas, skaidomas į smulkesnius tipus.

Aptarnavimo tikslas (remiantis pasauline praktika) – 80% užklausų išsprendžiamos pirmame aptarnavimo lygyje. Tai pasiekiama: pirmame lygyje neišspręsti incidentai,

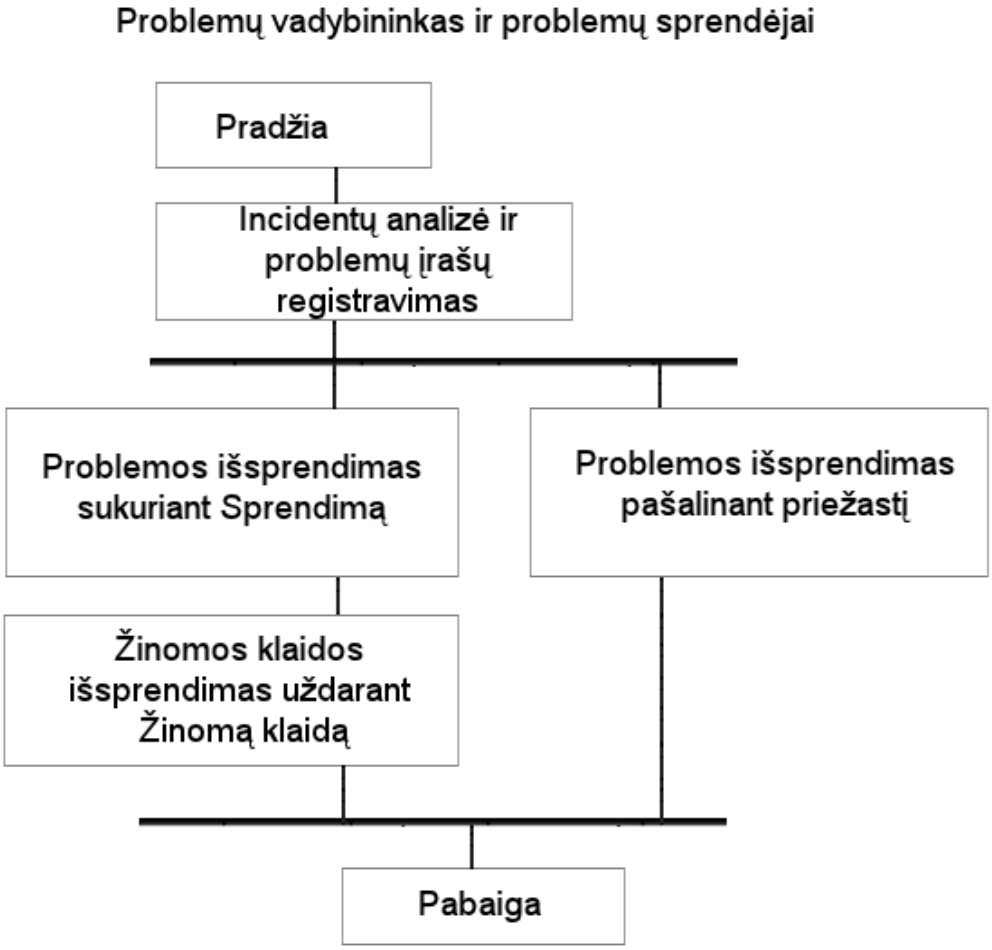
priklausomai nuo tipo, perduodami antro lygio sprendėjams vietoje (išorinė pagalba). Trečio lygio aptarnavimą teikia programinės ir techninės įrangos tiekėjai.

## *2.7. Problemų valdymas*

Procesas, skirtas registruoti ir spręsti Problemas (nežinomas priežastis, dėl kurių kyla Incidentai).

**Pastaba 1:** Neuždarytais incidentais šiame procese vadiname incidentus kurių „Būsena“ reikšmė „Atidaryti“ ir „Aptarnavimo būsena“ reikšmė ne „Išspręsta“ ir ne „Atmesta“;

**Pastaba 2:** Nesusietais incidentais šiame procese vadiname incidentus kurių „Žinoma klaida“ laukas yra tuščias




*2 pav. Problemų valdymo proceso scenarijus*

## *2.8. Detalus pasirinkto metodo įrankių pagrindimas*

### 2.8.1. Sistemos tikslai

Projekto tikslas ištirti lokalaus tinklo srautų ir veikimo stebėjimo galimybes, bei sukurti programinę įrangą tinklų administratoriams. Jiems skirta programinė įranga leis lengvai ir greitai pasiekti norimus įrašus apie veiklą bei duomenų srautus tinkle. Greitai reaguoti į atsiradusias problemas ar vykdyti jų prevenciją. Šitaip galima efektyviai sumažinti įmonės ar organizacijos IT departamento veiklos kaštus, kadangi sutaupius laiko specialistams gali būti skirtos kitos užduotys. Pagrindinis sistemos kūrimo tikslas – sukurti lengvai naudojamą ir naudingą PĮ.

Sukurtos tinklo stebėjimo bei srautų valdymo priemonės galės būt pakartotinai panaudojamos kituose projektuose, kuriuose gali kilti toks poreikis. Panaudojus jau sukurtą funkcionalumą nebereikės iš naujo kurti tų pačių galimybių, o esamas pritaikyti naujiems poreikiams. Toks kūrimo principas daug efektyvesnis, be to, užima žymiai mažiau laiko. Jau esamų metodų pritaikymas leis administratoriams panaudoti programos dalis savo projektuose ar pritaikyti ją specialiems poreikiams ar ypatingam funkcionalumas.

Yra keletas reikalavimų ir apribojimų, kurie turi įtaką sistemos architektūrai:

- Sistema turi būti realizuojama, remiantis Linux Debian sistemos įvykių kaupimo duomenų bazę (įrašų bylas), nes tokia DB yra įdiegta užsakovo serveriuose. Naudojant šią duomenų bazę žymiai palengvėja sistemos pernešimas į kitus serverius.
- Sistema pasižymi pernešamumu, kadangi tiek realizuojama duomenų bazės duomenys, tiek procedūros saugomos duomenų bazėje;
- Sistemos paskirstymas nulinis, kadangi visa sistema talpinama serveryje, o klientai per interneto naršyklę tik dirba su ja (siunčia jai užklausas ir gauna jau suformuotus rezultatus, kuriuos naršyklė tik atvaizduoja)
- Sistemos projektavimui gali rinktis iš daugybės UML įrankių. Autoriaus patirtis įtakojo Rational Rose 2003 projektavimo įrankio pasirinkimą.

### 2.8.2. Architektūros pateikimas UML kalba.

Architektūros vaizdavimui bus naudojama UML kalba. Sistemos architektūrinis vaizdas pateikiamas 5 brėžinių grupėmis:

- Panaudojimo atvejų vaizdas – aktoriai ir jų panaudojimo atvejai;

- Loginis vaizdas – sistemos posistemės ir jas sudarančios klasės;
- Procesų vaizdas – sąveikos ir veiksmų eiliškumo diagramos;
- Išdėstymo vaizdas – remiasi sistemos komponenčių išdėstymu fiziniuose kompiuteriuose;
- Duomenų vaizdas – duomenų bazės modelis;

### 2.8.3. Sąsajų pasirinkimas: interneto puslapio ir integruota sąsajos

Vartotojo sąsajai kurti interneto puslapiai dažniausiai vertinami dėl:

- Lengvas įdiegimas ir lengvas programos palaikymas vartotojo pusėje [9].
- Vartotojui įprasta naršyklės aplinka. Trumpesnis išmokimo dirbti sistema laikas.
- Naršyklės palaikymą ir atnaujinimus teikia naršyklės gamintojai.
- Nesunku integruoti su kitomis svetainėmis.
- Darbo įrankių gausos bei nesudėtingo kodo.

Realizacija interneto puslapiais turi trūkumų:

- Reikalingas nuolatinis prisijungimas prie tinklo. Visi veiksmai atliekami serveryje, todėl kas kart tenka į jį kreiptis norint ką nors atlikti. Apkraunamas aptarnaujantis kompiuteris.
- Ne visos naršyklės vienodai atvaizduoja HTML dokumentus. Taip pat gali iškilti problemų su DHTML, JavaScript ir kitų programavimo kalbų palaikymu [11, 14].
- Ribotos vartotojo sąsajos kūrimo galimybės.
- Klaidų apdorojimas vyksta serveryje. Atsiranda daugiau saugumo problemų [1].
- Svarbūs duomenys perduodami tinklu. Dėl to juos būtina papildomai šifruoti.

Sąsajos kūrimas kaip neatsiejama programos dalis suteikia šiuos privalumus.

- Daugiau sąsajos kūrimo galimybių.
- Greitas veikimas, kadangi kompiliuotas kodas vykdomas greičiau nei interpretuojamas. Nebūtina persiųsti pradinių duomenų ir rezultatų tinklu.
- Nebūtinas nuolatinis prisijungimas prie tinklo [9].

Tačiau kompiliuotų programų kūrimas turi ir trūkumų:

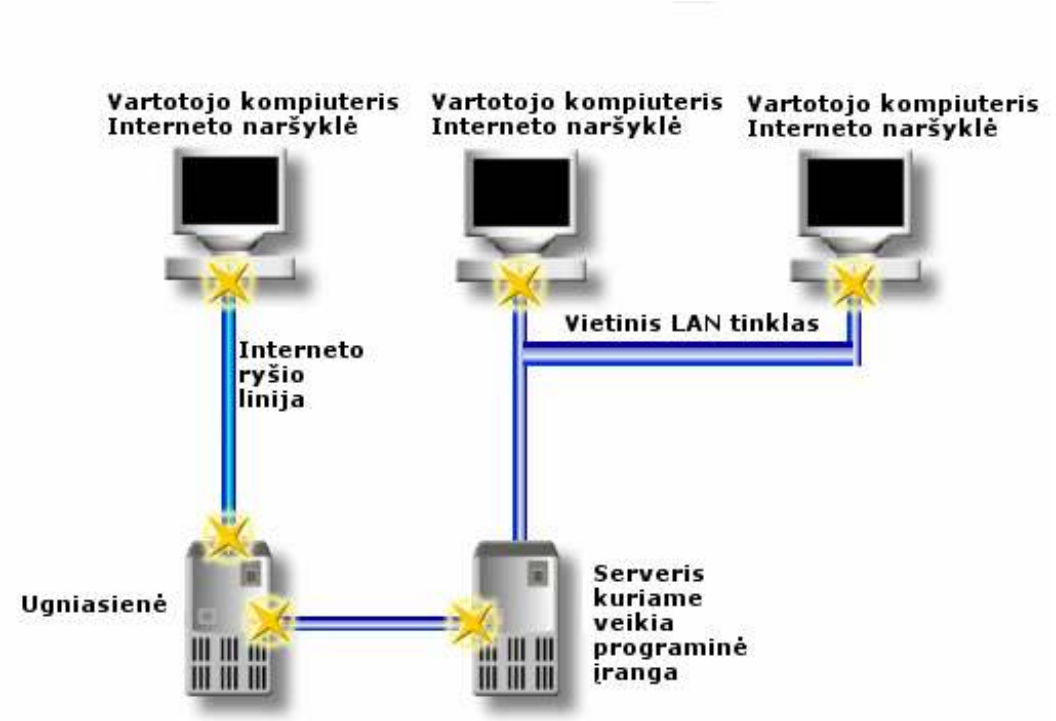
- Sudėtingas diegimas, palaikymas, tobulinimas ir atnaujinimas. Pakeistas programas būtina iš naujo įdiegti vartotojų kompiuteriuose.

- Skirtingų architektūrų kompiuteriuose būtina spręsti nesuderinamumo problemą. Tokiu atveju reikia perkompiliuoti kodą ir pritaikyti jį specialioms sistemoms arba diegti ir naudoti virtualias mašinas [9].

Šias problemas galima spręsti įgyvendinus automatinį programos atsinaujinimą iš nurodytų serverių, taip pat prašant vartotojų patiems atsisiųsti ir įdiegti norimas pataisas. Kiekvieną kartą paleidžiama programa galėtų pasitikrinti atnaujinimo galimybę bei pasiūlyti vartotojui tai atlikti savarankiškai ar automatiškai.

### 2.8.4. Architektūros pasirinkimas ir panaudojimas

Programinę įrangą galima realizuoti kelių lygių architektūroje. Programinės įrangos struktūra atrodytų taip [9]:




*3 pav. Programinės įrangos architektūra*

1 lygis – duomenų bazė. Jei sistemos veikimui būtina duomenų bazė, ji gali veikti tame pačiame serveryje kuriame veikia ir sistema. Duomenų bazė taip pat gali veikti ir kitame serveryje, tačiau esant nedideliam apkrovimui pirmu atveju daug racionaliau išnaudojami kompiuteriniai resursai. Tokiu atveju 1 ir antras lygiai tampa vienu.

2 lygis – serveris. Jame realizuota visa veikla susijusi su sistema. Čia atliekami visi veiksmai ir generuojami puslapiai bei ataskaitos vartotojui.

3 lygis – vaizdavimo lygis, naudojant antro lygio funkcijas galima lengvai realizuoti ploną klientą (žiniatinklio sąsaja), stalinio kompiuterio programinę įranga ar kt.

Kadangi visos darbinės funkcijos realizuotos 2 lygyje, trečią lygį realizuoti nėra sunku.

### 2.8.5. Programinės įrangos diegimas

Programinę įrangą reikia diegti tik serveryje. Šiuo atveju būtina įsitikinti, kad ji pakankamai gerai veikia su *Apache* serveriu, taip galima sėkmingai generuoti puslapius vartotojams. Taip pat – suderinti veikimą su duomenų baze, kad išeitų sėkmingai saugoti įrašus. Vartotojo pusėje užtenka įsitikinti tinkamos interneto naršyklės buvimu. Esant skirtumams tarp naršyklių galima identifikuoti besijungiančio vartotojo programinės įrangos tipą ir atitinkamai pakoreguoti generuojamus puslapius.

Internetinis įgyvendinimas yra geras, tačiau atsiranda papildomos problemos:

- Naudojami serverio resursai. Beveik nenaudojami vartotojo resursai. Apkrova serveriui gali tapti per didelė.
- Dažnai naudojant – pastovus tinklo apkrovimas.
- Prastesnė klaidų aptikimo ir apdorojimo galimybė.

Kliento programinę įrangą realizavus kaip atskirą programą, ją tektų įdiegti kiekviename kompiuteryje atskirai. Tokiu atveju pasunkėtų atnaujinimo ir palaikymo procesai. Tai galima spręsti savaiminio atsinaujinimo būdu, arba aptikus naują programos versiją pasiūlant vartotojui pačiam tai padaryti rankiniu būdu.

## *2.9. Įrašų analizės metodai*

Įrašų failai bei jų struktūra aptarti darbo 2.3 skyriuje.

Įrašuose esančiai informacijai analizuoti pasitelkiami įvairūs metodai ir esminės informacijos išgavimo būdai. Svarbią informaciją atrinkinėti būtina, nes dažniausiai sistemos įvykių kaupimo duomenys užima ne vieną dešimtį megabaitų, dėl ko nėra paprasta nei reikalinga nagrinėti visus įrašus, kurių dauguma – įprastiniai sistemos veiklos signalai.

Analizės metu naudojami tokie metodai informacijai atrinkti:

- Įrašų pagal užduotus specifinius raktinius žodžius atrinkimas (pvz., nesėkmingas prisijungimas).

- Žinomo potencialiai kenksmingos informacijos IP šaltinio veiksmų atrinkimas.
- Užklausos sistemai ieškant žinomai kenksmingų programų
- Neleistinų programų bei komandų naudojimas.
- Problemas keliančių vartotojų veiksmai sistemoje.

Sistemoje veikiantiems procesams stebėti taikomi tokie metodai:

- Stebimas resursų išnaudojimas. Nuolatinis padidėjęs ar sumažėjęs resursų išnaudojimas gali signalizuoti problemas.
- Procesų sąrašo lyginimas su žinomu kenksmingų programų sąrašu. Šis būdas nėra visiškai patikimas, tačiau gali pasiūlyti išankstinę problemų aptikimo galimybę.
- Problemas keliančių vartotojų procesų peržiūra.

Toks atrinkimas gali būti taikomas ir sisteminiams klaidų failams, kuriuose kaupiama informacija apie sistemos veiklos metu įvykusias klaidas. Tokiu atveju monitoringo programą galima panaudoti klaidų prevencijai ir tolerancijai užtikrinti.

## *2.10. Analizės išvados ir galimos problemos*

Analizės metu dažniausiai aptinkamos tokios problemos:

- Veikiantys kenksmingi, nelegalūs ir neleistini procesai
- Kenksmingi, nelegalūs ir neleistini vartotojų veiksmai.
- Padidėjęs resursų sunaudojimas sistemoje dėl neleistinų atskirų vartotojų veiklos ar vartotojų kompetencijos trūkumo.
- Bandymai nelegaliai prisijungti prie sistemos paskyrų
- Bandymai nelegaliai prisijungti prie sistemos pasinaudojant žiniatinklio puslapiais ir programomis.

## *2.11. Būtinos funkcijos monitoringui užtikrinti*

Norint sėkmingai realizuoti kompiuterių tinklo monitoringą, būtina stebėti, kaupti, analizuoti informaciją bei formuoti išvadas. Tai atlikti galima pasitelkus tokius metodus (smulkesnis metodų aprašymas pateiktas 2 darbo skyriuje, kuriame aprašomas programinės įrangos projektavimas):

- Duomenų srauto stebėjimas.
- Servisų veiklos stebėjimas.
- Potencialiai kenksmingos veiklos įrašų peržiūra.

- Potencialiai kenksmingų įrašų analizė.
- Reagavimas į servisų veiklos sutrikimus.
- Vartotojų administravimas.
- Kompiuterių vietiniame tinkle veiklos stebėjimas.
- Ataskaitų pateikimas.

## *2.12. Monitoringas Lietuvos Respublikos teisės aktuose.*

Lietuvos Respublikos teisės aktuose rašoma apie kompiuterius, vartotojų veiklą bei tinklus ir jų monitoringą [19, 20].

Konstitucijos 25 straipsnyje nustatyta:

„Žmogus turi teisę turėti savo įsitikinimus ir juos laisvai reikšti.

Žmogui neturi būti kliudoma ieškoti, gauti ir skleisti informaciją bei idėjas.

Laisvė reikšti įsitikinimus, gauti ir skleisti informaciją negali būti ribojama kitaip, kaip tik įstatymu, jei tai būtina apsaugoti žmogaus sveikatai, garbei ir orumui, privačiam gyvenimui, dorovei ar ginti konstitucinei santvarkai.

Laisvė reikšti įsitikinimus ir skleisti informaciją nesuderinama su nusikalstamais veiksmais – tautinės, rasinės, religinės ar socialinės neapykantos, prievartos bei diskriminacijos kurstymu, šmeižtu ir dezinformacija.

Pilietis turi teisę įstatymo nustatyta tvarka gauti valstybės įstaigų turimą informaciją apie jį“ [20].

LITNET tiekia interneto ryšį Kauno technologijos universitetui. Pasak LR Švietimo ir mokslo ministro įsakymo dėl LITNET kompiuterių tinklo [21]:

- Tinklo naudojimosi taisyklės yra privalomos visoms organizacijoms bei vartotojams, kurie naudojasi Lietuvos mokslo ir studijų kompiuterių tinklo LITNET (toliau – LITNET) resursais.
- LITNET tinkle draudžiama atlikti bet kokio pobūdžio veiksmus, kurie gali sukelti incidentą kompiuteriuose ar kompiuterių tinkluose (neautorizuotas servisų naudojimas, konfidencialios informacijos atskleidimas ar pakeitimas, servisų darbo sutrikdymas, portų skanavimas ir kt.);
- LITNET tinkle draudžiama talpinti ir platinti kompiuterių programas ir kitus autorinius produktus nesilaikant licencijose nustatytų reikalavimų ar kitaip pažeidžiant autorių teises;
- LITNET tinkle draudžiama: talpinti pornografinę, rasinę, tautinę neapykantą ar smurtą propaguojančią medžiagą, akademinės organizacijos vardą diskredituojančią medžiagą, kitus asmenis, organizacijas, firmas ar valstybes įžeidžiančią informaciją [21];

Keletas svarbių su monitoringu susijusių punktų iš ministro įsakymo:

10. Jeigu iš institucijos kompiuterių tinklo vyksta tęstiniai ar pakartotiniai incidentai arba institucijos kompiuteriai platina virusus, LITNET paslaugų teikimas gali būti sustabdytas, kol bus pašalintos incidentų priežastys.

11. LITNET paslaugų teikimas gali būti visiškai nutrauktas, jei institucija pažeidžia švietimo ir mokslo ministro patvirtintas Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisykles (toliau – LITNET tinklo naudojimo taisykles) ar sutarties sąlygas.

**16. Institucija privalo:**

16.3. užtikrinti saugų ir incidentų nesukeliantį lokalaus tinklo veikimą naudojantis LITNET paslaugomis;

16.4. bendradarbiauti su LITNET Tinklo incidentų tyrimo tarnyba CERT išaiškinant incidentus, sukeltus iš institucijos kompiuterių tinklo, ir nedelsiant likviduoti incidentus sukėlusias priežastis;

16.5. įdiegti ir eksploatuoti Lietuvos Respublikos teisės aktais bei LITNET valdybos sprendimais nustatytas LITNET tinkle privalomas saugumo ir įvykių registravimo priemones;

16.6. paskirti asmenį, atsakingą už institucijos tinklo veikimo ir vartotojų darbo LITNET tinkle priežiūrą [21].

Kaip ir įvardinta ministro įsakyme, institucijoje būtina paskirti asmenį kuris būtų atsakingas už tinklo monitoringą, koordinuotų veiksmus tarp LITNET CERT padalinio bei užtikrintų saugų bei incidentų nesukeliantį lokalaus tinklo veikimą.

## *2.13. Išvados*

Atlikus lokalaus tinklo incidentų monitoringo programinės įrangos projektavimo ir duomenų šia programinę įranga analizę galima teigti, kad:

- Egzistuoja alternatyvūs įrankiai atskiriems veiksmams atlikti, tačiau nė vienas jų neapima pilno funkcionalumo, kurį siūlo kuriama programinė įranga.
- Veiklas katedros serveriuose ir darbo kompiuteriuose būtina stebėti, kad būtų iš anksto pastebėtos ir pašalintos atsiradusios problemos ir sutrikimai.
- LR įstatymai ir LitNET tinklo naudojimosi taisyklės nurodo, kad paskirti katedros darbuotojai atsako už tinkle ir serveriuose esančių duomenų neprieštaravimą LR įstatymams bei LitNET darbo tinkle taisyklėms ir įgalina imtis veiksmų šiems nurodymams įgyvendinti.

- Incidentai – tai įvykiai, kurie pažeidžia normalų kompiuterių/tinklo veikimą, prieštarauja tinklo saugumo taisyklėms, galiojantiems įstatymams.

# 3. Lokalaus tinklo monitoringo programinės įrangos projektavimas

## *3.1. Programų inžinerijos katedros kompiuterių tinklas*

Šiuo metu, 2006 metų gegužės mėnesį Programų inžinerijos katedros kompiuterių tinklas išsidėstęs 3 pastatuose.

Pagrindiniai tinklo vartotojai (pagal užklausų skaičių): studentai, dėstytojai, kiti katedros darbuotojai, LitNET CERT padalinys.

Duomenų perdavimu kabeliais rūpinasi LitNET organizacija.

Studentų mokymui yra skirtos 3 kompiuterių klasės, kuriose yra apie 60 mokymo ir darbo vietų:

Skaičiavimo centro (SC, ITPI) 206 kompiuterių klasė – 12 darbo vietų

Skaičiavimo centro (SC, ITPI) 105 kompiuterių klasė – 24 darbo vietos

Informatikos fakulteto antras korpusas – 305 kompiuterių klasė – 24 darbo vietos

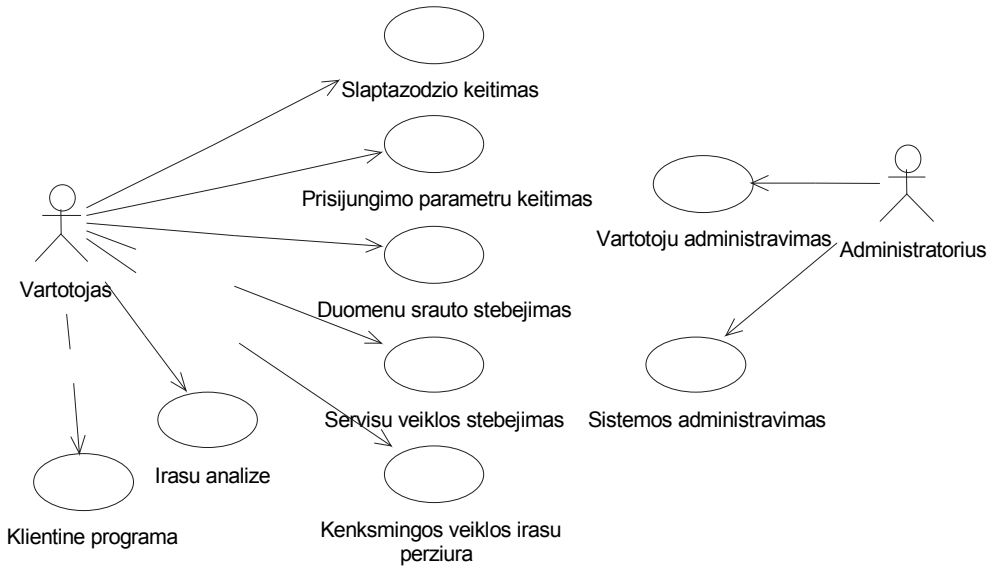
Be šių kompiuterių apie 28 kompiuteriai yra skirti dėstytojų bei katedros personalo reikmėms.

Katedros kompiuterių tinklo veikimui bei vartotojų poreikiams užtikrinti yra naudojami du serveriai:

Diedas.soften.ktu.lt – saugomos vartotojų paskyros, sisteminiai įrašų failai, taikomosios programos,

Bosas.soften.ktu.lt – saugomas ir vartotojams perduodamas elektroninis paštas, taip pat saugomos atsarginės duomenų kopijos.

## *3.2. Panaudos atvejų modelis*




*4 pav. Lokalaus tinklo incidentų monitoringo programinės įrangos panaudos atvejai..*

### 3.2.1. Duomenų srauto stebėjimas

Šis stebėjimas vykdomas ne realiu laiku bet analizuojant įrašų failus. Vartotojas naudodamas kompiuterį su interneto ryšiu ir naršykle gali nesunkiai prisijungti prie sistemos. Taip įvairių administravimo užduočių atlikimas žymiai palengvėja [2]. Vartotojas stebėdamas per serverį ar kitus tinklo įrenginius keliaujantį duomenų srautą gali realiu laiku stebėti tinklo veiklos kokybę. Tai gali padėti išvengti problemų bei sutaupyti laiko [4]. Apdorojamus duomenis sistema pati pasiima iš tinklo, o rezultatai pateikiami vartotojui tinkama forma.

### 3.2.2. Servisų veiklos stebėjimas

Kuriant tinklo stebėjimo sistemą pravartu matyti, kaip veikia sisteminiai procesai, susiję su darbu tinkle arba jo palaikymu. Tai matydamas vartotojas gali greičiau aptikti atsiradusias bėdas ir jas spręsti. Duomenis šiai programos daliai teiktų pati operacinė sistema, rezultatai būtų pateikiami vartotojui tinkama elektronine forma. Panašų stebėjimą įdiegus visame tinkle galima nesunkiai matyti, kaip veikia norimi procesai kiekviename iš serverių [4].

### 3.2.3. Potencialiai kenksmingos veiklos įrašų peržiūra

Stebėti žalingą ar kenksmingą veiklą yra naudinga, tai leidžia daug greičiau suprasti problemų priežastį ir žalos dydį. Kaip ir kiti moduliai, šis pasiekiamas per internetą naudojant naršyklę. „Kimono‘‘ įrankyje realizuotas informacijos pateikimas ir komandinėje eilutėje [4]. Šiuos įrašus būtina kaupti, neleisti redaguoti bet kam, kad nebūtų prarasta svarbi informacija

apie problemų šaltinius, priežastis bei atsiradimo laiką. Vėliau, atsiradus poreikiui, šie įrašai gali būti analizuojami ir atitinkamai keičiama saugumo tvarka ir nustatymai tinkle ar serveryje. Dideliuose tinkluose net ir trumpalaikiai sutrikimai gali smarkiai sutrikdyti bendrą organizacijos darbą [6].

### 3.2.4. Potencialiai kenksmingų įrašų analizė

Sistemos vartotojai, pastebėję nesklandumus, gali nesunkiai pasiekti įrašus apie pastebėtą kenksmingą/klaidingą veiklą tinkle, jei turi tam pakankamai teisių sistemoje. Sistema, išanalizavusi sukauptus įrašus, nustato pavojaus laipsnį. Taip labai palengvėja darbas, kadangi nebereikia peržiūrėti daug neesminės informacijos. Šiame darbe apžvelgtose šio tipo programose įrašai kaupiami apie daugelį procesų vykstančių tinkluose, tinklo įrenginiuose bei serveriuose [1, 2, 5].

### 3.2.5. Reagavimas į servisų veiklos sutrikimus

Kartais sistema gali automatiškai reaguoti į susidariusias problemas be papildomo vartotojo įsikišimo. Pavyzdžiui, ugniasienės pačios ima blokuoti kenksmingos informacijos šaltinius. Apie tokios veiklos aptikimą iškart gali būti įspėjamas tinklo administratorius [2]. Tuo pačiu gali būti atliekamas papildomas vietinio tinklo aptikimas, skenavimas bei analizė bandant nustatyti kitas galimas tokio pats sutrikimo vietas [1]. Tą patį galima atlikti ir su serveriuose veikiančiomis paslaugomis bei jas naudojančiais vartotojais [2]. Sistemos vartotojas vėliau gali nuspręsti, kuriems pranešimams verta skirti daugiau dėmesio.

### 3.2.6. Vartotojų administravimas

Daugelyje sistemų kuriamos kelių lygių prieigos. Vienos skirtos sistemų administratoriams, atsakingiems asmenims ir turi daugiau teisių sistemoje. Kitos paskyros yra skirtos paprastiems vartotojams. Pastarosios neleidžia naudoti daugelio administracinių ar potencialiai pavojingų komandų, tačiau leidžia pilnavertiškai dirbti sistemoje [8]. Kai vartotojams suteikiama pernelyg daug teisių sistemoje, padidėja saugumo pažeidimo galimybė, o tai gali baigtis rimtais gedimais. Atsižvelgiant į visų vartotojų poreikius sudaroma tokia saugumo politika, kuri mažiausiai trukdytų naudotis sistema, bet tuo pačiu ir užtikrintų pakankamą saugumą [7]. Daug didesnės apimties tinkluose iškyla visai kito tipo saugos ir vartotojų teisių problemos nei mažuose. Kuriant saugumo nuostatas reikia viską pilnai numatyti [8].

Sistemos dalis, padedanti atlikti vartotojų administravimą, gali būti pasiekiama internetu iš bet kurio kompiuterio prijungto prie tinklo.

### 3.2.7. Kompiuterių vietiniame tinkle veiklos stebėjimas

Kuriant sistemą galima realizuoti papildomą klientinę programą. Ši programa veiktų vartotojo kompiuteryje, stebėtų su darbu tinkle susijusius procesus ir apie tai informuotų serverį [9]. Programa stebėtų esamus susijungimus ir atviras jungtis. Atidaryti priėjimai dažnai įspėja apie galimą žalingą veiklą tinkle. Dažnai savavališkai jungtis atveria įvairios kenkėjiškos programos – interneto kirminai, virusai, šnipai ir kt. [10]. Stebint atviras jungtis galima nuspėti, kokios programos šiuo metu veikia kompiuteryje, kokia jų paskirtis ir kokia jų įtaka bendram tinklui [1]. Analogiškose nagrinėtose sistemose šio tipo funkcionalumas nebuvo realizuotas, todėl tektų naudotis papildomomis programomis norint pasiekti tokį patį efektą.

### 3.2.8. Ataskaitų pateikimas.

Ataskaitos generuojamos serveryje, kuriame veikia kuriama sistema. Jos pateikiamos vartotojui priimtinu formatu, paprastai HTML kodo eilutėmis, kurias supranta ir atvaizduoja interneto naršyklės [4, 14]. Apžvelgtose tokio tipo programose taip pat siūloma ataskaitas pateikti el. pašto pavidalu [2], taip pat SMS ar ICQ žinutėmis [5].

Realizuota ataskaitų, pranešimų ar įspėjimų galimybė leidžia greitai pasiekti sistemos vartotojus ir administratorius. Tai leidžia greitai reaguoti į iškilusias problemas, arba jų išvengti gavus išankstinį įspėjimą [2].

### *3.2.9. Nefunkciniai reikalavimai sistemai*

Projektuojamai sistemai keliami tokie nefunkciniai reikalavimai:

- Paprasta, lengvai suprantama sąsaja [13].
- Sistema turi padėti vartotojui išvengti klaidų.
- Turi būti nesunku apsimokyti dirbti sistema.
- Tiek sistemos serveris, tiek ir vartotojų darbo vietos turi būti prijungtos prie tinklo.
- Duomenys vaizduojami ir saugomi iš anksto apibrėžtais formatais.
- Produktas turi veikti turimuose kompiuteriuose.
- Produkto klientinė dalis turi veikti bet kurioje OS su naršykle. Produkto serverinė dalis turi veikti Linux šeimos OS.
- Produktas turi neleisti neautorizuotiems vartotojams prisijungti prie sistemos ir ja naudotis.
- Sistema neturi būti įrankis pažeisti kompiuterinį etiketą, atlikti nelegalius ir/ar žalingus veiksmus, rinkti neleistiną informaciją.

- Produktas turi nepažeisti galiojančių LR įstatymų bei LitNet tinklo taisyklių.
- Produktas turi neleisti keisti svarbios informacijos sistemoje.

## *3.3. Monitoringo pritaikymas egzistuojančioms veikloms*

Kuriant programinę įrangą būtiną pritaikyti ją egzistuojančioms veikloms, kad programa savo buvimu palengvintų dabar esamų užduočių atlikimą.

### 3.3.1. Vietinio kompiuterių tinklo priežiūra

*3 lentelė. Vietinio kompiuterių tinklo priežiūros veikla.*

| Pagrindinė informacija | |
|---|---|
| Trumpas apibūdinimas | Vidinio kompiuterinio tinklo aktyviosios (komutatoriai, koncentratoriai) ir pasyviosios dalies (komutuojami laidai, jungtys) priežiūra |
| Pagrindiniai Paslaugos teikimo parametrai | |
| Pagrindinė informacija apie paslaugą | Kompiuterinio tinklo suteikimas vidiniams vartotojams ryšiui su serveriais, su internetu ir tarpusavyje. |
| Kliento apibūdinimas | Ši paslauga teikiama visiems katedros vidinio kompiuterinio tinklo vartotojams. |
| Paslaugos tiekėjo apibūdinimas | PĮ katedros kompiuterių administratoriai yra atsakingi už šios paslaugos teikimą ir apskaitą.<br>Paslaugą teikia:<br>• Smulkiems pakeitimams: Programų inžinerijos katetros kompiuterių tinklo administratoriai.<br>• Esant esminiams pakeitimams: Šiuo metu šią paslaugą teikia KTU ITPI KAC ir KTC<br>Paslaugos užsakymo būdai:<br>• Užregistravus užklausą administratorių darbo vietoje;<br>• El. pašto adresu support@soften.ktu.lt išsiuntus pranešimą;<br>• Paskambinus budinčiam kompiuterių administratoriui vietinio ryšio arba mobiliu telefonijos tinklu.<br>• Atsiuntus užklausą kitais ryšio kanalais (SMS, ICQ, MSN)<br>• Papildomai gali būti užsakoma tiesiogiai kreipiantis į ITPI darbuotoją; |

| | |
|---|---|
| | Papildoma kontaktinė informacija pateikiama prieduose. |
| Paslaugos teikimo gyvavimo ciklas/ Pateikimo laikas | Paslauga sukurta ir pradėta teikti 2001 metais pertvarkius Programinės įrangos katedrą į Programų inžinerijos, Kompiuterinių tinklų ir Sisteminės analizės katedras.<br>Paslaugos atnaujinimo tvarka:<br>• periodiškai kiekvienų metų sausio ir rugpjūčio mėn. (paruošimas mokslo semestrams);<br>• pastoviai priklausomai nuo poreikio ir naujų funkcionalumų įtraukimo. |
| Kiti parametrai | |
| Detalus paslaugos aprašymas | Paslauga apima:<br>1. Vidinio kompiuterinio tinklo teikimo atstatymą nustačius sutrikimus (savo kompetencijos ribose);<br>Pastaba: į šią paslaugą neįtraukiami vidinio tinklo kūrimas ir atnaujinimas, jis priskiriamas prie infrastruktūros valdymo paslaugos: IT kompiuterinio tinklo vystymas.<br>2. Vidinio kompiuterinio tinklo aktyviosios dalies (komutatoriai, koncentratoriai, šakotuvai, optiniai keitikliai, bevielio tinklo stotelės) (Incidentų sprendimą) suderinimą ir priežiūrą;<br>3. Vidinio kompiuterinio tinklo pasyviosios dalies (komutuojami laidai, jungtys) (Incidentų sprendimą) priežiūrą;<br>4. Kompiuterinio tinklo ryšio su išorinio kompiuterinio tinklo (WAN) aktyviąja dalimi (maršrutizatoriai) ir priemonių reikalingų tinklo saugumui užtikrinti (ugniasienių) diegimą, palaikymą ir (Incidentų sprendimą) priežiūrą;<br>5. tinklo plėtros darbų (pastato ar patalpų remonto metu) konsultacijos, įvertinant perspektyvą; |
| Priklausomybės | Ši paslauga gali būti susijusi su:<br>• PĮ katedros duomenų perdavimo paslauga (LITNET):<br>• Elektros tiekimo paslauga (įtampos svyravimai ir kt.);<br>• Tinklinės įrangos garantiniu aptarnavimu;<br>• Kai kuriais aptarnavimo darbais: remonto (nukarpo telefono, tinklo |

| | |
|---|---|
| | laidus, pajungia savo aparatus i pc elektros tiekimui skirtas sroves...), valytojų;<br>• Kitos sutartys pasirašytos tarp PĮ katedros bei kompiuterinio tinklo bei interneto ryšio duomenų tiekėjų. |
| Priskirti resursai | 1. Paslaugą teikiančių darbuotojų rolės ir reikalavimai:<br>• Paslaugą teikianti rolė: katedroje dirbantis laborantas ar inžinierius.<br>• Paslauga teikiama (KTU atveju) ITPI, ITCR darbuotojų;<br>• IT tinklo inžinieriaus resursas nustatomas – vienas darbuotojas tinklo įrangai nuo lokalizuoto tinklo įvadinio įrenginio;<br>2. Biudžetas:<br>Etatinio darbuotojo darbas standartinėmis darbo valandomis apmokamas iš katedros ir fakulteto lėšų. |
| Paslaugos lygio kriterijai | Nustatomi paslaugos lygio kriterijai:<br>• Paslaugos teikimo laikas;<br>• Darbo laiko lygiai;<br>• Paslaugos lygiai;<br>• Kiekvienas lygis matuojamas pagal:<br>o Reagavimo laiką;<br>o Sprendimo laiką;<br>o Aptarnavimo lygį. |
| Paslaugos lygiai | Nustatomi paslaugos aptarnavimo parametrai:<br>• Paslaugos teikimo laikas:<br>o I–V: nuo 8:00 iki 17:00;<br>o VI, VII: dirbama tik esant atskiram pareikalavimui.<br>• Darbo laiko lygiai:<br>o Normalus – I–IV: nuo 8:00 iki 17:00; V: nuo 8:00 iki 15:45;<br>o Papildomas1 – I –IV: nuo 17:00 iki 21:00, V: nuo 15:45 iki 21:00 ir VI: nuo 8:00 iki 17:00;<br>o Papildomas 2 – VII nuo 8:00 iki 17:00<br>Pastaba:<br>Papildomas1 laikas taikomas tik mokymo procesui kompiuterių klasėse užtikrinti.<br>Papildomas2 laikas taikomas tik pagal patvirtintą administracijos |

<table>
<tr><td></td><td>grafiką.<br>• Paslaugos aptarnavimo lygis ir sąlygos (SLA):<table><tr><td>Darbo laiko lygis</td><td>Visų aptarnautų paraiškų vidutinis sprendimo laikas (val./ paraiškai)</td><td>Aptarnavimo lygis (%)</td></tr><tr><td>Normalus</td><td><2 val.</td><td>80</td></tr><tr><td>Papildomas</td><td><8 val.</td><td>80</td></tr></table></td></tr>
</table>

### 3.3.2. Serverių priežiūra

*4 lentelė. Serverių priežiūros veikla.*

| **Pagrindinė informacija** | |
|---|---|
| Trumpas apibūdinimas | Serverių kompiuterinės įrangos resursų (CPU, HDD, RAM), operacinės sistemos (Windows, Unix, Linux, Novell Netware ir kt.), IT duomenų failų sistemos priežiūra |
| Pagrindiniai Paslaugos teikimo parametrai | |
| Pagrindinė informacija apie paslaugą | Bendros paskirties ir specializuotų serverių diegimas ir priežiūra. |
| Kliento apibūdinimas | Ši paslauga teikiama Programų inžinerijos katedros serveriams. |
| Paslaugos tiekėjo apibūdinimas | PĮ administratoriai yra atsakingi teikimą ir apskaitą.<br>Paslaugą teikia:<br>• PĮ administratoriai;<br>Paslaugos užsakymo būdai:<br>• Serverių priežiūra atliekama periodiškai.<br>Papildomi darbai užsakomi:<br>• El. pašto adresu support@soften.ktu.lt išsiuntus pranešimą;<br>• Paskambinus budinčiam kompiuterių administratoriui vietinio ryšio arba mobiliu telefonijos tinklu.<br>• Atsiuntus užklausą kitais ryšio kanalais (SMS, ICQ, MSN) |
| Paslaugos teikimo | Paslauga sukurta ir pradėta teikti 2001 metais pertvarkius Programinės įrangos katedrą į Programų inžinerijos, Kompiuterinių tinklų ir Sisteminės |

| | |
|---|---|
| gyvavimo ciklas/ Pateikimo laikas | analizės katedras.<br><br>Paslaugos atnaujinimo tvarka:<br>• periodiškai kiekvieną dieną priklausomai nuo iškilusių problemų ir kuriant atsargines duomenų kopijas;<br>• pastoviai priklausomai nuo naujų funkcionalumų įtraukimo. |
| Kiti parametrai | |
| Detalus paslaugos aprašymas | Paslauga apima:<br>6. Serverių diegimą ir priežiūrą:<br>a. Linux serveris<br>Linux įdiegimas, branduolio kompiliavimas, atnaujinimas<br>FTP, SMB, SSH, DHCP, DNS serverių konfigūravimas<br>Srautų valdymas,<br>vykstančių įvykių stebėjimas ir savalaikis reagavimas į sistemos perspėjančius pranešimus apie gręsiančius sutrikimus<br>Linux saugumo, ugniasienių konfigūravimas<br>Maršrutizavimas<br>Administravimas (vartotojų sąrašų kūrimas bei naikinimas, atributų bei vartotojų teisių nustatymas ir kt.).<br>Atsarginės kopijos, kasdieniniai arba periodiniai duomenų archyvavimo darbai (Back up).<br>Problemų analizė ir sprendimas (troubleshoot) sutrikimo atveju<br>b. Windows serveris<br>Operacinės sistemos diegimas, atnaujinimas<br>Windows 2003 aplinkos konfigūravimas. DNS, IIS ir kt. servisų diegimas, konfigūravimas, palaikymas, saugumo priemonių diegimas<br>Active Directory serviso diegimas<br>Vartotojų ir grupių sąrašų kūrimas ir administravimas<br>Grupių politikos diegimas ir palaikymas<br>Spausdinimo įrenginių diegimas ir palaikymas<br>Resursų valdymas, naudojant Actine Directory ir Group policy<br>vykstančių įvykių stebėjimas ir savalaikis reagavimas į sistemos perspėjančius pranešimus apie gręsiančius sutrikimus |

| | |
|---|---|
| | Atsarginės kopijos, kasdieniniai arba periodiniai duomenų archyvavimo darbai (Back up).<br>Problemų analizė ir sprendimas sutrikimo (troubleshoot) atveju<br>7. Kasdieninius duomenų atnaujinimo darbus (daily load). |
| Priklausomybės | Ši paslauga gali būti susijusi:<br>1. Serverių garantinio aptarnavimo paslauga.<br>2. Vidinio kompiuterinio tinklo (LAN) priežiūros paslauga<br>3. Elektros tiekimo paslauga (sutarties su Elektros tinklais, elektros energijos rezervavimo sistema: UPS, dyzelinis generatorius, įtampa).<br>4. KTU IF PĮ ir išorinio paslaugų tiekėjo pasirašytomis sutartimis. |
| Priskirti resursai | 2. Paslaugą teikiančių darbuotojų rolės ir reikalavimai:<br>• Paslaugą teikianti rolė: IT administratorius (laborantas arba inžinierius)<br>IT administratoriaus resursas nustatomas – vienas darbuotojas vienam serverių tipui lokalizuotame tinkle.<br>3. Paslaugą teikiančių darbuotojų rolės ir reikalavimai:<br>• Paslaugą teikianti rolė: IT serverių administratorių darbo grupė<br>• IT administratorių darbo grupės resursas nustatomas pagal serverių atliekamas funkcijas (failų kontroleris, žiniatinklio serveris, duomenų bazių serveris, pašto serveris, FTP serveris, spausdinimo serveris .....).<br><br>3. Biudžetas:<br>Darbai apmokami pagal etatinio darbuotojo apmokėjimo tvarką. |
| Paslaugos lygio kriterijai | Nustatomi paslaugos lygio kriterijai:<br>• Paslaugos teikimo laikas;<br>• Darbo laiko lygiai;<br>• Paslaugos lygiai;<br>• Kiekvienas lygis matuojamas pagal:<br>o Reagavimo laiką;<br>o Sprendimo laiką;<br>o Aptarnavimo lygį. |

<table>
<tr><td>Paslaugos lygiai</td><td>Nustatomi paslaugos aptarnavimo parametrai:<ul><li>Paslaugos teikimo laikas:<ul><li>I–V: nuo 8:00 iki 17:00;</li><li>VI, VII: dirbama tik esant atskiram pareikalavimui.</li></ul></li><li>Darbo laiko lygiai:<ul><li>Normalus – I–IV: nuo 8:00 iki 17:00; V: nuo 8:00 iki 15:45;</li><li>Papildomas1 – I –IV: nuo 17:00 iki 21:00, V: nuo 15:45 iki 21:00 ir VI: nuo 8:00 iki 17:00;</li><li>Papildomas 2 – VII nuo 8:00 iki 17:00</li></ul>Pastaba:<br>Papildomas1 laikas taikomas tik mokymo procesui kompiuterių klasėse užtikrinti.<br>Papildomas2 laikas taikomas tik pagal patvirtintą administracijos grafiką.</li><li>Paslaugos aptarnavimo lygis ir sąlygos (SLA):</li></ul>
<table>
<tr><td rowspan="2">Paslaugos lygis</td><td colspan="2">Visų aptarnautų paraiškų vidutinis sprendimo laikas (val./paraiškai)</td><td colspan="2">Aptarnavimo lygis (%)</td></tr>
<tr><td>Normaliu laiku</td><td>Papildomu1 ir papildomu 2 laiku</td><td>Normaliu laiku</td><td>Papildomu1 ir papildomu 2 laiku</td></tr>
<tr><td>Svarbus</td><td><2 val.</td><td><4 val.</td><td>80</td><td>80</td></tr>
<tr><td>Standartinis</td><td><8val.</td><td><8 val.</td><td>80</td><td>80</td></tr>
<tr><td>Planuojamas</td><td>Planuojamas</td><td>Planuojamas</td><td>80</td><td>80</td></tr>
</table>
Pastaba 1: Planuojamas gali būti naudojamas tik techninio gedimo ir planinių pakeitimų atvejais;</td></tr>
</table>

### 3.3.3. Vartotojų kompiuterinių darbo vietų priežiūra

*5 lentelė. Vartotojų kompiuterinių darbo vietų aptarnavimo veikla.*

| Pagrindinė informacija | |
|---|---|
| Trumpas apibūdinimas | Paslauga apima Programinės inžinerijos katedros kompiuterių techninės ir programinės dalies aptarnavimą, įskaitant standartinės ir nestandartinės (pagal |

| | |
|---|---|
| | galimybes) kompiuterinės ir programinės įrangos valdymą vartotojo darbo vietoje. |
| Pagrindiniai Paslaugos teikimo parametrai | |
| Pagrindinė informacija apie paslaugą | Centralizuotas vartotojų kompiuterinės ir programinės įrangos valdymas siekiant užtikrinti kokybišką vartotojų kompiuterinės darbo vietos įrengimą ir optimalų kompiuterinių resursų panaudojimą.<br>Siekiant šio tikslo taikomos priemonės:<br>• Kompiuterinės įrangos naudojamos vartotojų darbo vietose standartizavimas;<br>• Programinės įrangos naudojamos vartotojų darbo vietose standartizavimas;<br>• Optimalus vartotojų poreikių užtikrinimas centralizuotomis priemonėmis. |
| Kliento apibūdinimas | Ši paslauga teikiama visiems katedros pastoviems darbuotojams, taip pat kompiuterių klasėse esančioms kompiuterinėms darbo vietoms. |
| Paslaugos tiekėjo apibūdinimas | PĮ katedros kompiuterių administratoriai yra atsakingi už šios paslaugos teikimą ir apskaitą.<br>Šią paslaugą gali teikti:<br>• KTU IF PĮ kompiuterių tinklo administratoriai.<br>Paslaugos užsakymo būdai:<br>• Užregistravus užklausą administratorių darbo vietoje;<br>• El. pašto adresu support@soften.ktu.lt išsiuntus pranešimą;<br>• Paskambinus budinčiam kompiuterių administratoriui vietinio ryšio arba mobiliu telefonijos tinklu.<br>• Atsiuntus užklausą kitais ryšio kanalais (SMS, ICQ, MSN)<br>• Esant smulkiems gedimams papildomai gali būti užsakoma tiesiogiai kreipiantis į ITPI darbuotoją;<br><br>Papildoma kontaktinė informacija pateikiama prieduose. |
| Paslaugos teikimo gyvavimo ciklas/ Pateikimo laikas | Paslauga sukurta ir pradėta teikti 2001 metais pertvarkius Programinės įrangos katedrą į Programų inžinerijos, Kompiuterinių tinklų ir Sisteminės analizės katedras.<br>Paslaugos atnaujinimo tvarka:<br>• periodiškai kiekvienų metų sausio ir rugpjūčio mėn. (paruošimas mokslo semestrams); |

| | |
|---|---|
| | pastoviai priklausomai nuo poreikio ir naujų funkcionalumų įtraukimo. |
| Kiti parametrai | |
| Detalus paslaugos aprašymas | Paslauga apima:<br>• darbo vietos techninė priežiūrą įskaitant:<br>o įrengimą darbo vietoje;<br>o vidinių ir išorinių įrenginių diegimą ir suderinimą;<br>o sugedusios įrangos keitimą;<br>o apskaitą;<br>o nestandartinės įrangos diegimą ir aptarnavimą, kuris gali būti vykdomas tik pagal galimybes;<br>• programinės įrangos priežiūrą<br>o operacinės sistemos diegimą, suderinimą (konfigūravimą) ir priežiūrą;<br>o standartinės programinės įrangos diegimą ir suderinimą;<br>o saugumo priemonių diegimą, atnaujinimą, priežiūrą ir profilaktiką;<br>o kompiuterinės technikos darbingumo atstatymą;<br>o licencijuotos arba laisvai platinamos vartotojiškos programinės įrangos diegimą ir priežiūrą;<br>o konsultacijas;<br>o apskaitą.<br>• vietinio ir tinklinio spausdinimo suderinimą;<br>• kompiuterio programinės ir aparatūrinės dalies gedimų diagnostiką ir analizę;<br>• profesionalius patarimus ar konsultacijas;<br>• naujų programinės įrangos versijų diegimą, pakeitimų ir papildymų įdiegimą;<br>• duomenų išsaugojimą ir atstatymą, šalinant gedimus (esant techninėms galimybėms);<br>• vartotojų kompiuterių konfigūravimą darbui su mobilia įrangą, kuri pastoviai naudojama mokymo organizacijoje. |
| Priklausomybės | Dėl bet kokio poreikio susijusio su įstaigos kompiuterine įranga vartotojas privalo kreiptis į Programų inžinerijos katedros tinklo administratorius.<br>PĮ tinklo administratoriai savo jėgomis arba pagal poreikį pasitelkiant kitus |

| | |
|---|---|
| | katedros ar KTU darbuotojus pateikia vartotojui sprendimą.<br>Ši paslauga susijusi su:<br>1. Pagalbos vartotojui dirbant katedros kompiuteriais teikimu<br>2. Vartotojų teisių valdymo paslauga;<br>3. PĮ garantinio aptarnavimo paslauga;<br>4. Negarantinio remonto paslauga<br>5. Elektros tiekimo paslauga;<br>6. Vidinio kompiuterinio tinklo (LAN) priežiūros paslauga;<br>7. Serverių priežiūros paslauga;<br>8. Programų inžinerijos katedros ir išorinio paslaugų tiekėjo pasirašytomis sutartimis. |
| Priskirti resursai | Paslaugą teikiančių darbuotojų rolės ir reikalavimai:<br>• Paslaugą teikia IT administratorius (specialistas);<br>• Vieno darbuotojo išdirbio norma nustatoma ~ 50–70 aptarnaujamos kompiuterinės įrangos vienetų;<br>• Darbuotojų skaičius nustatomas pagal formulę: Nkomp/Aptarnaujamų kompiuterių skaičiaus ; |
| Paslaugos lygio kriterijai | Nustatomi paslaugos lygio kriterijai:<br>• Paslaugos teikimo laikas:<br>• Darbo laiko lygiai:<br>• Paslaugos lygiai;<br>• Kiekvienas lygis matuojamas pagal:<br>o Reagavimo laiką;<br>o Sprendimo laiką;<br>o Aptarnavimo lygį. |
| Paslaugos lygiai | Nustatomi paslaugos aptarnavimo parametrai:<br>• Paslaugos teikimo laikas:<br>o I–IV: nuo 8:00 iki 17:00; V: nuo 8:00 iki 15:45;<br>• Darbo laiko lygiai:<br>o Normalus – I–IV: nuo 8:00 iki 17:00; V: nuo 8:00 iki 15:45;<br>Papildomas –taikomas tik papildomą patvirtintą grafiką.<br>Įvertinant darbą papildomu laiku turi būti taikomas koeficientas 2.0. |

| Vertinimo rodikliai | Aptarnavimo lygio svarba | | |
|---|---|---|---|
| | Skubi | Standartinė | Planuojama |
| Įtaka darbo procesui | Darbas neįmanomas | Dalinis arba sulėtėjęs funkcionalumas | Planuojamas gali būti naudojamas tik techninio gedimo ir planinių pakeitimų atvejais. |
| | | | |

Aptarnavimo lygio svarba nustatoma iš lentelės:

| Lygio pavadinimas | Reagavimo laikas | | Sprendimo laikas | | Aptarnavimo lygis % |
|---|---|---|---|---|---|
| | Normaliu laiku | Papildomu laiku | Normaliu laiku | Papildomu laiku | |
| 1. Skubus | 30 min. | 1val. | 4 val. | 6 val. | 80 |
| 2. Standartinis | 1 val. | | 8 val. | | 80 |
| 3.Planuojamas | | | 30 d. | | 80 |

Pastaba: Nukrypimui nuo aptarnavimo lygio matuoti taikomas 3% intervalas. Ši reikšmė yra naudojama nustatant baudų skaičiavimo taisykles.

### 3.3.4. Organizacinės technikos įrengimas ir aptarnavimas

*6 lentelė. Org. techikos įrengimas ir aptarnavimas*

| Pagrindinė informacija | |
|---|---|
| Trumpas apibūdinimas | Paslauga apima visos katedros org. techninės įrangos (spausdintuvų, kopijavimo įrenginių, faksų, skenerių ir daugiafunkcinių įrengimų) aptarnavimą, įskaitant org. techninės įrangos įrengimą, atnaujinimą, gedimų šalinimą, konfigūravimą ir priežiūrą bei dažiklių keitimą.<br>Paslauga apima standartinės org. techninės įrangos bei su ja susijusių priedų aptarnavimą tame tarpe pagalbos suteikimą vartotojams |
| Pagrindiniai Paslaugos teikimo parametrai | |
| Pagrindinė informacija apie paslaugą | Orgtechninės įrangos valdymas siekiant užtikrinti kokybišką jos funkcionavimą ir optimalų šių resursų panaudojimą.<br>Todėl vykdomas:<br>• Org. techninės įrangos standartizavimas; |

| | |
|---|---|
| | • Org. technikos optimizavimas (stebimas: resursų naudojamo; pajėgumų atitikimas vartotojų poreikiams) |
| Kliento apibūdinimas | Ši paslauga teikiama:<br>• aptarnaujami visi katedrai priklausantys org. technikos įrengimai.<br>• visiems įstaigos pastoviems ir laikiniems darbuotojams. |
| Paslaugos tiekėjo apibūdinimas | PĮ tinklo administratoriai yra atsakingas už šios paslaugos teikimą ir apskaitą.<br>Šią paslaugą gali teikti:<br>• PĮ katedros tinklo administratoriai;<br>• PĮ katedros vidiniai ir išoriniai partneriai (pavyzdžiui, kopijavimo aparatų ar spausdintuvų nuomos atveju).<br>Paslaugos užsakymo būdai:<br>• Užregistravus užklausą administratorių darbo vietoje;<br>• El. pašto adresu support@soften.ktu.lt išsiuntus pranešimą;<br>• Paskambinus budinčiam kompiuterių administratoriui vietinio ryšio arba mobiliu telefonijos tinklu.<br>• Atsiuntus užklausą kitais ryšio kanalais (SMS, ICQ, MSN)<br>• Esant smulkiems gedimams papildomai gali būti užsakoma tiesiogiai kreipiantis į ITPI darbuotoją;<br><br>Papildoma kontaktinė informacija pateikiama prieduose. |
| Paslaugos teikimo gyvavimo ciklas/ Pateikimo laikas | Paslauga sukurta ir pradėta teikti 2001 metais pertvarkius Programinės įrangos katedrą į Programų inžinerijos, Kompiuterinių tinklų ir Sisteminės analizės katedras.<br>Paslaugos atnaujinimo tvarka:<br>• Esant atnaujinimų, užpildymų (spausdintuvai) ar kitokiems poreikiams (personalinės vartotojų užklausos) |
| Kiti parametrai | |
| Detalus paslaugos aprašymas | Paslauga apima:<br>• spausdintuvų, kopijavimo įrenginių, faksų, skenerių ir daugiafunkcinių įrengimų instaliavimą ir priežiūrą įskaitant:<br>o įrengimą ir pasenusios įrangos atnaujinimą/keitimą;<br>o sugedusios įrangos diagnozę ir remontą (jei naudingas remonto |

| | |
|---|---|
| | pasiūlymas);<br>o apskaitą;<br>o Dažiklio keitimas;<br>• vartotojų mokymą ir darbo su org. technika pagalbos dokumentacijos pateikimą.<br>• vartotojų teisių susijusių su org. technika administravimą. |
| Priklausomybės | Dėl bet kokio poreikio susijusio su bendrovės org. technika vartotojas privalo kreiptis į Programų inžinerijos tinklo administratorius.<br>Administratoriai savo jėgomis arba pagal poreikį pasitelkiant kitus administratorius, katedros personalą ar KTU darbuotojus pateikia vartotojui sprendimą.<br>Ši paslauga susijusi su:<br>9. Bendro pobūdžio pagalba vartotojams;<br>10. Elektros tiekimo paslauga;<br>11. Org. technikos įrangos garantinio aptarnavimo paslauga;<br>12. Vartotojų teisių valdymo paslauga;<br>13. Standartinės vartotojo darbo vietos įrengimo paslauga;<br>14. katedros ir išorinio paslaugų tiekėjo pasirašytomis sutartimis. |
| Priskirti resursai | Paslaugą teikiančių darbuotojų rolės ir reikalavimai:<br>• Paslaugą teikianti rolės:<br>o PĮ tinklo administratorius<br>• Vieno darbuotojo išdirbio norma nustatoma ~ 150 aptarnaujamos KĮ vienetų;<br>• Darbuotojų skaičius nustatomas pagal formulę: Norg/150;<br>• Išdirbio norma nustatyta pilnam šios paslaugos suteikimui, įskaitant ir įrangos darbo vietoje įrengimą. |
| Paslaugos lygio kriterijai | Nustatomi paslaugos lygio kriterijai:<br>• Paslaugos teikimo laikas:<br>• Darbo laiko lygiai:<br>• Paslaugos lygiai;<br>• Kiekvienas lygis matuojamas pagal:<br>o Reagavimo laiką;<br>o Sprendimo laiką;<br>o Aptarnavimo lygį. |

<table>
<tr><td>Paslaugos lygiai</td><td>Nustatomi paslaugos aptarnavimo parametrai:<ul><li>Paslaugos teikimo laikas:<ul><li>I–V: nuo 8:00 iki 17:00;</li></ul></li><li>Darbo laiko lygiai:<ul><li>Normalus – I–IV: nuo 8:00 iki 17:00; V: nuo 8:00 iki 15:45;</li></ul></li></ul>Paslaugos aptarnavimo lygis ir sąlygos:<table>
<tr><td rowspan="2">Vertinimo rodikliai</td><td colspan="4">Aptarnavimo lygio svarba</td></tr>
<tr><td>Kritinė</td><td>Didelė</td><td>Vidutinė</td><td>Planuojama</td></tr>
<tr><td>Darbuotojų grupė</td><td>Rektoratas</td><td>Dekanatas; Katedros</td><td>Kiti MĮ darbuotojai</td><td rowspan="2">naudojama įrangos užsakymo atveju</td></tr>
<tr><td>Paveiktų vartotojų skaičius, vnt.</td><td>>50</td><td>>25</td><td><=10</td></tr>
</table>Aptarnavimo lygio svarba nustatoma įvertinus kiekvieną rodiklį atskirai. Sprendimas priimamas imant didžiausią reikšmę.<table>
<tr><td rowspan="2">Lygio pavadinimas</td><td colspan="2">Reagavimo laikas</td><td colspan="2">Sprendimo laikas</td><td rowspan="2">Aptarnavimo lygis %</td></tr>
<tr><td>Normaliu laiku</td><td>Papildomu laiku</td><td>Normaliu laiku</td><td>Papildomu laiku</td></tr>
<tr><td>1.Kritinis</td><td>15 min.</td><td>15 min.</td><td>2 val.</td><td>2 val.</td><td>60</td></tr>
<tr><td>2.Didelis</td><td>1 val.</td><td>2 val.</td><td>6 val.</td><td>6 val.</td><td>60</td></tr>
<tr><td>3.Vidutinis</td><td>2 val.</td><td></td><td>24 val.</td><td></td><td>60</td></tr>
<tr><td>4.Planuojamas</td><td>3 d.</td><td></td><td>30 d.</td><td></td><td>60</td></tr>
</table></td></tr>
</table>

Šiose aukščiau išvardintose veiklose monitoringo sistema gali:

- Padėti patikti susidariusias problemas.
- Pasiūlyti sprendimą.
- Iš anksto įspėti apie galima problemų susidarymą.
- Pagreitinti problemų sprendimą bei vartotojų užklausų aptarnavimą.
- Padėti įvardinti problemines sritis bei vartotojus.

## *3.4. Monitoringą naudojantys darbuotojai*

Kompiuterinių tinklų bei sistemų priežiūrą ir monitoringą Programų inžinerijos katedroje atlieka šie darbuotojai:

- Sistemų administratorius – kompiuterinių sistemų bei programinės įrangos techninė priežiūra ir aptarnavimas. Tiesioginis bendravimas su klientais. Bendradarbiavimas su darbuotojais, vystančiais, diegiančiais ir prižiūrinčiais organizacijos sistemas ir infrastruktūrą.
- Tinklo administratorius – užtikrinti organizacijos ar organizacijų grupės kompiuterių tinklo veikimą ir vystymą.
- Duomenų bazių administratorius – Duomenų bazių priežiūra ir aptarnavimas.
- Incidentų sprendėjas – Sprendžia vartotojų užklausas, teikia pirminę pagalbą vartotojams, nustatant problemos pobūdį ir suteikiant informaciją apie sprendimo kelius. Užtikrinti incidentų išsprendimą per nustatytą laiką.

Visų šių darbuotojų veikla yra tiesiogiai susijusi su sistemos veiksmų monitoringu užtikrinat pakankamą ir tinkamą aparatūrinės įrangos, tinklo bei vartotojų užklausų aptarnavimą.

## *3.5. HTTP ir Linux Debian įrašų analizė*

Įrašų failai bei jų palyginimas pateikti 1.4. šio darbo skyriuje.

Analizuojant prisijungimo įrašus, dažniausiai esančius auth.log faile, ieškomos eilutės, kuriose yra žodžių:

- authentication,
- failed,
- failure,
- login,
- Illegal,

Taip pat gali būti ieškoma neįprastų prisijungimo laikų (pvz., tarp 24 ir 5 valandos nakties).

Prisijungimų iš užsienio, kur katedros kompiuterių vartotojų turėtų nebūti, arba būti vos keletas.

HTTP įrašų analizei gali būti taikomi panašūs atrankos kriterijai, tačiau reikia atsižvelgti į tai, kad interneto puslapiai Programų inžinerijos katedros serveriuose gali būti atversti bet kuriuo paros metu iš bet kurios pasaulio vietos. Sutrumpintas ieškomų žodžių sąrašas pateikiamas prieduose.

## *3.6. Serverio ir tinklo kompiuterių procesų analizė*

Analizuojant serverio ir tinklo kompiuteriuose vykstančius procesus yra stebima jų išnaudojama atminties apimtis, procesoriaus skaičiavimų poreikiais, taip pat galimi neleistini

veiksmai. Tam atlikti yra pasitelkiama kompanijos „Uniblue Systems“ dažniausiai pasitaikančių kenkėjų sąrašas. Jis lyginamas su kompiuteriuose veikiančiais procesais. Apie pastebėtas problemas pranešama administratoriui [22].

## *3.7. Realizacijos ypatumai*

Realizuojant programinę įrangą įgyvendinti tokie ypatumai:

- Sistema veikia dviejuose lygiuose:
  - Serverio lygis. Šiame lygyje veikia pati programa, čia ji generuoja vartotojo sąsają, saugo duomenis, atlieka skaičiavimus.
  - Vartotojo lygis, kuriame informacija atvaizduojama. Šiame lygyje vartotojas taip pat gali įvesti informaciją.
- Naudojant tokią architektūra tampa žymiai lengviau plėsti, atnaujinti ir palaikyti jau esamą sistemą, kadangi galima vystyti atskirų lygių komponentus.
- Žiniatinklio svetainės vartotojo sąsaja pasirinkta nes:
  - Lengvai keičiama ir palaikoma.
  - Neapkrauna vartotojo kompiuterio.
  - Prieinama iš bet kurio kompiuterio turinčio prisijungimą prie interneto ir naršyklę.
  - Naršyklės atnaujinimu ir palaikymu rūpinasi jos kūrėjai. Šio darbo nereikia atlikti programinės įrangos kūrėjams. Jiems lieka daugiau laiko ir resursų kitiems darbams atlikti.
- *Apache* žiniatiklio paslauga ir MySql duomenų bazių programa pasirinkta nes:
  - Yra nemokamos.
  - Gali patikimai aptarnauti didelius duomenų ir užklausų srautus.
  - Nuolat išleidžiamos pataisos ir patobulinimai.
  - Lengvai administruojama, yra pritaikyta Linux OS.
- Linux OS pasirinkta nes:
  - Yra nemokama.
  - Greita OS. Spartesni skaičiavimai nei Windows operacinėse sistemose, turi daug įrankių ir bibliotekų skirtų darbui tinkle.
  - Galimybė naudotis įvairių kalbų kompiliatoriais ir interpretatoriais.
  - Nuolat atnaujinama ir tobulinama.

# 4. Tiriamoji ir eksperimentinė dalis

Šioje darbo dalyje eksperimentiškai tirta sukurta programinė įranga, kuri analizuoja realius 3 mėnesių laikotarpio duomenys. Šie duomenys, rodantys interneto vartotojų prisijungimą prie pagrindinio kompiuterio, buvo kaupiami katedros serveriuose.

## *4.1. Įrašų analizės rezultatų tyrimas*

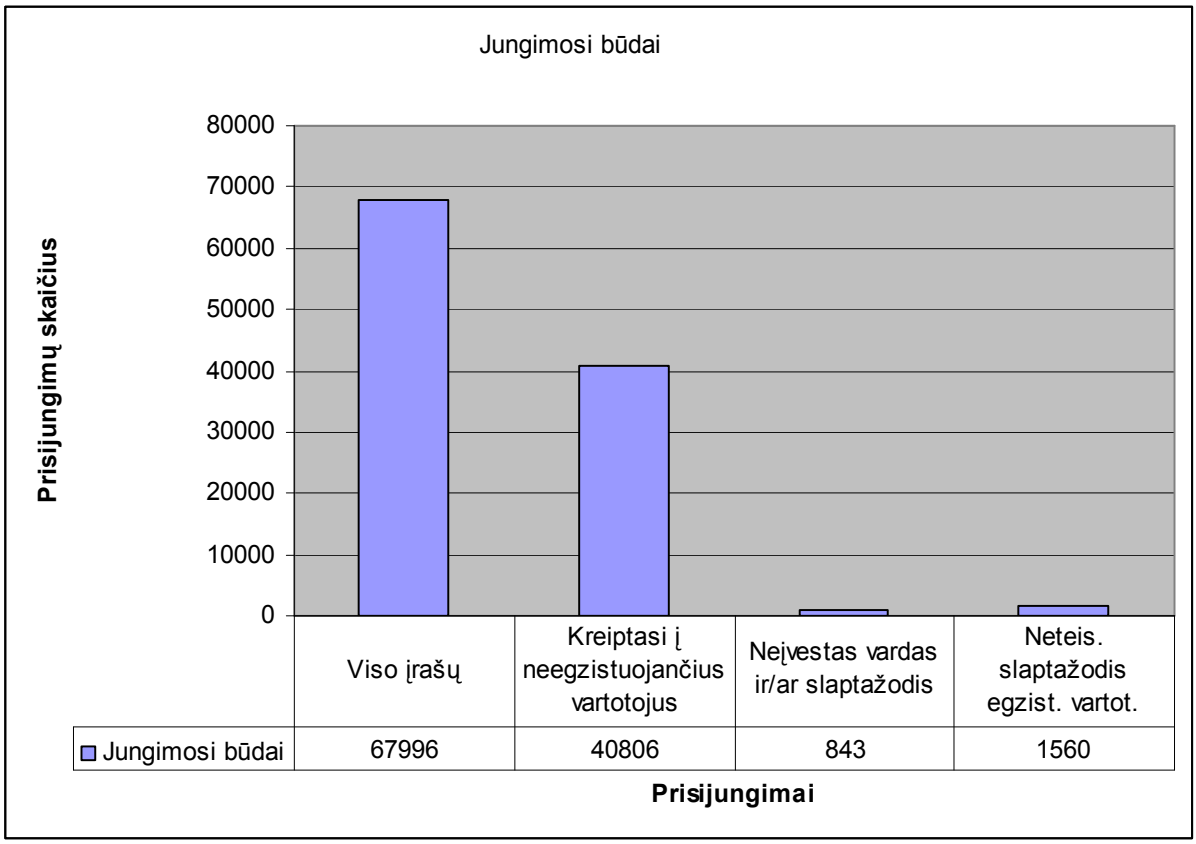
Analizuojant įrašų failus buvo pasitelktas taisyklių sąrašas, pagal kurį iš šimtų tūkstančių įrašų buvo atrinkti dominantys ir informuojantys apie galimas problemas tinkle.

Taisyklių sąrašą sudaro:

- Raktiniai žodžiai.
- Pavojinga informacija užklausose serveriams.
- Tuščias prisijungimo vardas ar/ir slaptažodis prisijungimo informacijoje.
- Žinomai pavojingos užklausos serveriams.
- Kenksmingų procesų sąrašai [17].

Tiriami 3 mėnesių prisijungimo įrašai, nuo 2006 m. kovo 19 d. iki 2006 m. gegužės 14 d. imtinai.

Iš viso analizės metų buvo tirti 67996 įrašų (apie 1759 *MS Word* puslapiai 10 dydžio šriftu).

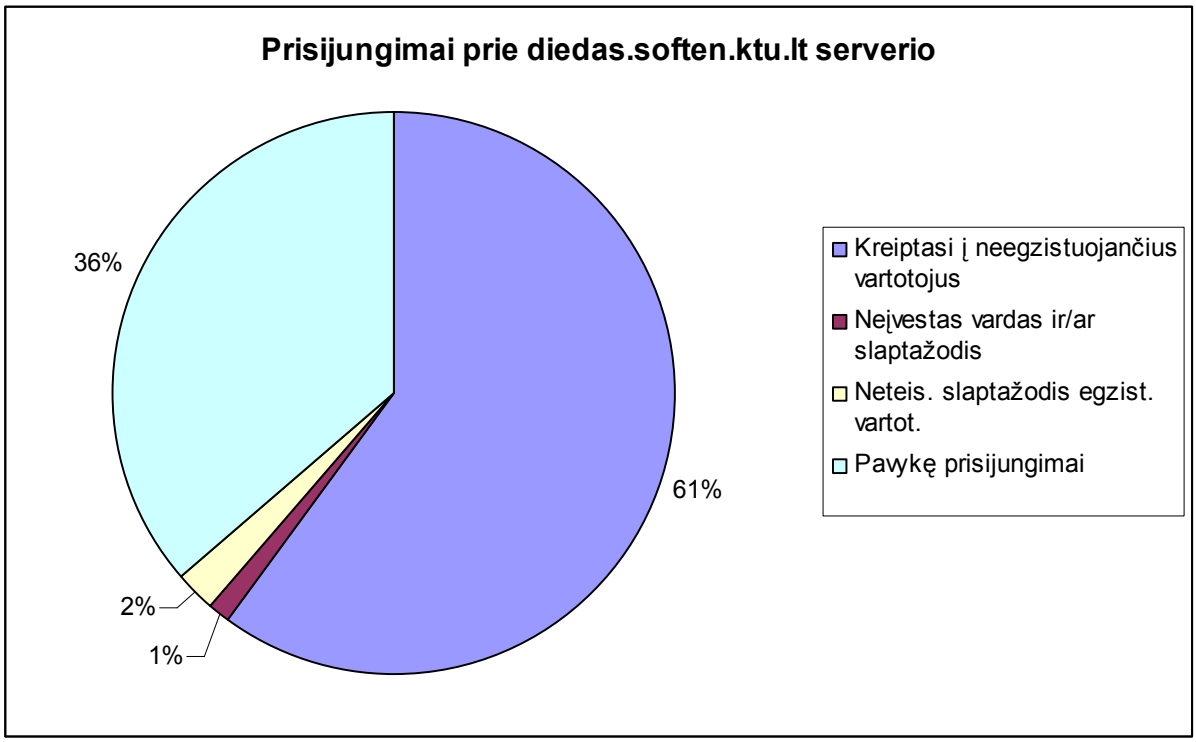



*5 pav. Prisijungimų skaičius ir būdai stebėtu laikotarpiu*

### 4.1.1. SSH protokolas

Analizuojant SSH protokolą pastebėta, kad daugiausia problemų sukėlė išoriniai vartotojai ne iš Lietuvos daug kartų bandę prisijungti prie sistemos įvesdami neegzistuojančių vartotojų prisijungimo vardus ir slaptažodžius. Tai dažniausiai atliekama pasitelkiant specialią programinę įrangą tikintis, kad bus atsitiktinai atspėta vienos iš daugelio paskyrų prisijungimo informacija.

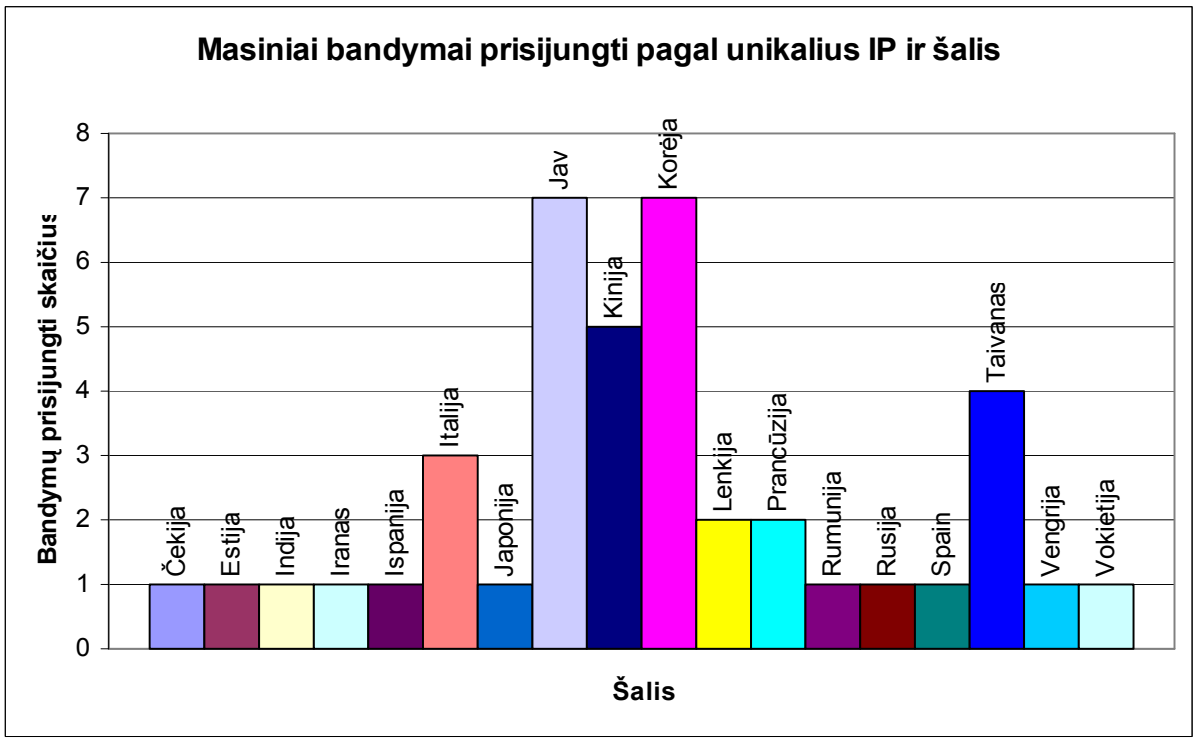
Detalesnė informacijos analizė:



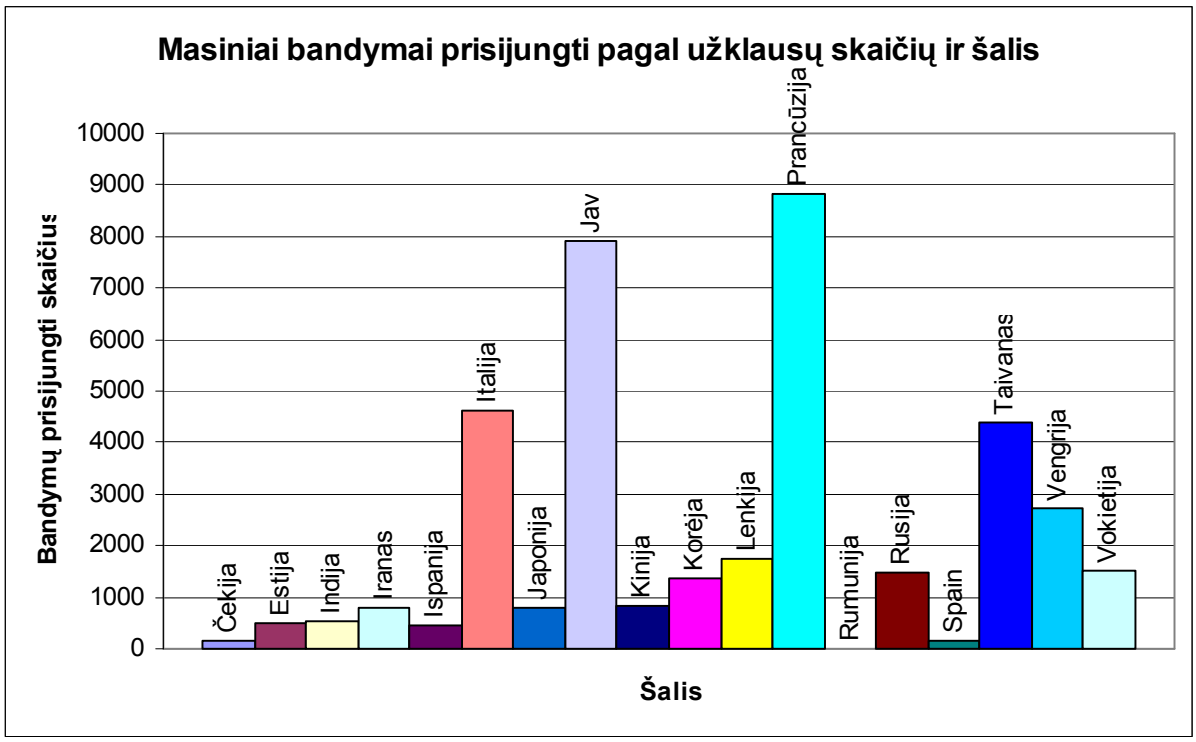

*6 pav. Prisijungimai prie diedas.soften.ktu.lt serverio*

Absoliuti dauguma kreipimųsi į neegzistuojančius vartotojus buvo atlikta SSH protokolu (38820 įrašai iš 40806, t.y. 95,13% visų kreipimųsi į neegzistuojančius vartotojus).

Atlikus detalesnę analizę pagal problemų šaltinius, gautas toks atakų pasiskirstymas pagal šalis:

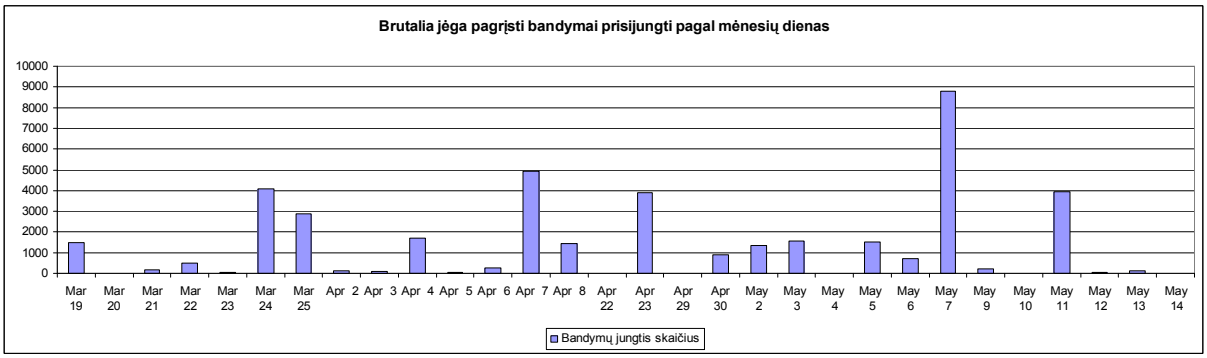



*7 pav. Prisijungimo bandymai pagal unikalių IP adresų skaičių ir šalį.*




*8 pav. Prisijungimo bandymai pagal užklausų skaičių ir šalis*

Atlikus detalesnę analizę pagal problemų šaltinius, gautas toks atakų pasiskirstymas pagal mėnesių dienas:




*9 pav. Brutalia jėga pagrįsti bandymai nelegaliai prisijungti*

### 4.1.2. Pop3 protokolas

Analizuojant pop3 (el. pašto prisijungimo) informaciją paaiškėjo, kad dažniausia problema – bandymas prisijungti nepateikiant nei prisijungimo vardo nei slaptažodžio. Tokios problemos gali atsirasti dėl pažeidžiamų serverių paieškos programinės įrangos arba vartotojų, kurie neįvedę šių duomenų bando jungtis prie serverio, kaltės. Fiksuoti 1306 tokie atvejai.

### 4.1.3. FTP protokolas

Analizuojant FTP paslaugos (failų siuntimo) informaciją paaiškėjo, kad dažniausia problema – bandymas prisijungti nepateikiant nei prisijungimo vardo nei slaptažodžio. Tokios

problemos gali atsirasti dėl pažeidžiamų serverių paieškos programinės įrangos arba vartotojų, kurie neįvedę šių duomenų bando jungtis prie serverio, kaltės. Fiksuoti 1959 tokie atvejai.

### 4.1.3. HTTP protokolas

Šio protokolo įrašai buvo analizuojami ieškant 6557 žinomų problemų ir pažeidžiamumų. Buvo aptikti vos keli nesusiję incidentai. Masinių puolimo atvejų nerasta. Taip gali būti dėl serveriuose veikiančios programinės įrangos versijų. Linux Debian operacinė sistema skiria ypatingą dėmesį sistemos saugumui. Visos užklausos *Apache* paslaugai (servisui) yra vykdomos specialaus vartotojo „nobody“, turinčio itin žemas veiklos teises Linux Debian sistemoje, kas žymiai sumažina pažeidžiamumo galimybę.

### 4.1.4 Prievadų skenavimas

Prievadų skenavimas (angl. port scanning) pastebėtas prisijungimo įrašuose. 85% šių bandymų aptikti atviras jungtis atkeliavo iš jau anksčiau pastebėtų problemų šaltinių JAV, Kinijoje ir Vengrijoje. Viso aptikta 4476 prievadų skenavimo užklausos. Skirtingai nei prieš tai buvusiuose rezultatuose, šiuose rezultatuose matomi ir Lietuvoje esančių kompiuterių IP adresai.

## 4.2. Incidentų klasifikacija

Įsilaužimo incidentai kartais klasifikuojami taip:

- Socialinė inžinerija – manipuliavimas personalu bandant apeiti apsaugas. Katedros darbuotojai studentus aptarnauja tik pateikus studento pažymėjimą, kas labai apsunkina tokio tipo incidentų atsiradimą.
- Trojos arkliai – speciali programinė įranga instaliuojama vartotojų kompiuteriuose ir sukurianti pilnavertį priėjimą prie kompiuterio šios programinės įrangos savininkui. Mokymo klasėse studentai jungiasi prie ribotų teisių paskyrų, kas riboja panašios programinės įrangos įdiegimą. Kompiuteriai yra nuolat tikrinami siekiant aptikti panašias programas.
- Virusai ir kirminai – šiais laikais dažniausiai plinta elektroniniu paštu. Administratoriai šviečia katedros personalą. Esant reikalui blokuojami kompiuterio duomenų srautai tinkle siekiant sustabdyti virusų plitimą. Papildomai yra įdiegtas elektroninio pašto filtras *SpamAssasin* kuris automatiškai atrenka nepageidaujamus laiškus, o esant reikalui gali būti konfigūruojamas specifinių virusų plitimo stabdymui.
- Fizinės atakos – vyksta turint fizinį priėjimą prie kompiuterio. Serveriai yra užrakinti Elektronikos fakulteto serverių patalpoje, todėl fizinį patekimą prie jų turi tik už

serverius atsakingi administratoriai. Personalinius kompiuterius nuo to apsaugoti žymiai sunkiau, tačiau tokios atakos pasitaiko itin retai.

- Nelegalus prisijungimas prie tinklo – be tinkamos formos prašymo katedros turimi IP adresai nėra išduodami. Papildomu saugumu rūpinasi LITNET.
- Gamykliniai slaptažodžiai – visi slaptažodžiai katedroje pakeičiami pirmą kartą pristačius kompiuterius, taip žymiai sumažinant galimybę rasti tokį pažeidžiamumą.
- Srauto šnipinėjimas – sunkiai realizuojamas dėl tinklo tipologijos.
- Slaptažodžių spėliojimas – pastebėta nuolatiniai bandymai įrašų analizės metu. Sprendimo būdas pasiūlytas išvadose.
- Pažeidžiamumai – programinė serverių įranga yra nuolat atnaujinama ištaisant naujai atsiradusius pažeidžiamumus. Reaguojama į LITNET CERT pastabas
- Nereikalingi servisai – veikia tik mokslo procesams ir operacinės sistemos gyvavimui reikalingi procesai. Procesų sąrašas nuolat tikrinamas, išjungiant nereikalingus.
- Prievadų skenavimas – pastebėtas nuolatinis kompiuterio prievadų skenavimas tiriant sisteminius įrašus. Sprendimas pasiūlytas šio darbo išvadose.
- Žmogus–viduryje atakos – sunkiai realizuojamos, egzistuoja papildomos apsaugos.
- Paslaugų nutraukimo atakos – aptikti sunku, įrašų analizės metu nepastebėta.
- Nelegalūs vartotojų veiksmai – nelegali programinė įranga kenkti tinklo saugumui. Nelegali informacija.
- Vartotojų teisių eskalavimas – įrašų analizės metu neaptikta [16].

Pagal incidentų klasifikaciją stebėtu kovo–gegužės laikotarpiu buvo stebimi tokie incidentai (+ reiškia buvus incidentų, – incidentų nepastebėta):

*7 lentelė. Incidentai tyrimo mėnesiais.*

| Incidento pavadinimas | Mėnuo | | |
|---|---|---|---|
| | 2006 kovas | 2006 balandis | 2006 gegužė |
| Socialinė inžinerija | – | + | – |
| Trojos arkliai | + | – | – |
| Virusai ir kirminai | +– (ieškota spragų) | +– (ieškota spragų) | – |
| Fizinės atakos | – | – | – |
| Nelegalus prisijungimas | – | – | – |
| Gamykliniai slaptažodžiai | – | – | – |
| Srauto šnipinėjimas | – | – | – |
| Slaptažodžių spėjimai | + | + | + |
| Pažeidžiamumai | + | – | + |
| Nereikalingi servisai | +– (studentų) | +– | +– |
| Prievadų skenavimas | + | + | + |
| Žmogus-viduryje atakos | – | – | – |
| Paslaugų nutraukimas | – | – | – |
| Nelegalūs vart. veiksmai | + | + | – |
| Teisių eskalavimas | +– (su komanda) | +– | +– |

## *4.3. Ugniasienės taisyklių generavimas*

Aptikus pasikartojančių problemų šaltinius yra patartina juos blokuoti, kad daugiau iš šių taškų nebūtų jungimųsi. Tai atlikti padeda ugniasienės. Linux operacinėje sistemoje dažniausiai siūloma keletas šio tipo programinės įrangos paketų, tarp jų populiariausi yra *IPtables* ir *IPchains*.

Internete yra siūlomas automatinis įrankis ugniasienės taisyklių sąrašo generavimui (*PHP Firewall Generator* http://phpfwgen.sourceforge.net/demo/). Jis patogus tuo, kad parašytas PHP kalba, kaip ir suprojektuota programinė įranga. Tokiu atveju būtų lengva abi šias programas integruoti.

## *4.4. Pastebėtos problemos ir įgyvendinti patobulinimai*

Analizuojant realius serverių įrašus buvo pastebėta nuolatiniai bandymai įsibrauti, kas nėra netikėta, ir ko reikia tikėtis administruojant nuolat tinkle veikiančius serverius.

gyvendinus projektą ir jo metu sukurta programine įranga analizuojant įrašų failus iškilo poreikis papildomai analizuoti IP adresus ir informacija apie juos. Tame pačiame skyriuje kaip ir analizės išvados buvo sukurtas modelis „Papildoma IP adresų analizė“. Šis papildymas apima tokį papildomą funkcionalumą:

- IP adreso išrišimą į tekstinį vardą
- informacijos paieška DNS įrašuose
- informacijos apie IP adreso savininką paieška
- pasirinktos jungties atvirumo tikrinimas
- atsakymo (angl. ping) prašymas

# 5. Išvados

Atlikus srities analizę, projektavimą, eksperimentinės programos panaudojimą realių serverių duomenų analizei galima daryti tokias išvadas:

- Egzistuoja veiklos kurias būtina realizuoti projektuojant monitoringo programinę įrangą.
- Analizuojant panašią programinę įrangą, nemokamos tinkamos neradau. Tinkamos alternatyvos šioje srityje kainuoja brangiai.
- Norint išgauti tą patį funkcionalumą būtų tekę diegti ir derinti bent porą naujų programų.
- Projektavimo metu kurta programinė įranga pritaikyta Programų inžinerijos katedros reikmėms, esančiam kompiuterių tinklui ir veikloms.
- Realizuota programinė įranga leidžia stebėti serverių ir kompiuterių mokymo klasėse veiklos parametrus. Tai patogu, nes viską galima atlikti naudojant vieną kompiuterį su prisijungimu prie interneto bei naršykle. Kompiuterius prižiūrinčio personalo darbo vieta tampa mobilesnė.
- Projektuojant programinę įrangą pasirinkta *Apache* ir *MySql* programinė įranga. Už šios programinės įrangos naudojimą ir licenzijas mokėti nereikia. Tai sumažina programinės įrangos kūrimo kaštus.
- Projektuojant pasirinkta plono kliento–serverio architektūra, dėl to, kad dauguma duomenų saugoma serveryje.
- Realizavus vartotojo sąsają kaip žiniatinklio svetainę žymiai palengvėja sistemos atnaujinimas ir palaikymas, kadangi programinį kodą ir duomenis užtenka atnaujinti serveryje. To nereikia daryti kiekviename iš kompiuterių kuriuose naudojama programinė įranga.
- Sukurta programine įranga analizuojant serverių veiklos įrašus išaiškėjo, kad:
    - Pastebimi nuolatiniai bandymai atspėti prisijungimo slaptažodžius įvairiems vartotojams įvairiais protokolais, SSH, POP3, FTP ir kitais (išvardinti pagal dažnumą).
    - Pastebimi nuolatiniai prievadų skenavimo incidentai.
- Tiriant 3 mėnesių prisijungimo įrašus, nuo 2006 m. kovo 19 d. iki 2006 m. gegužės 14 d. imtinai paaiškėjo, kad dažniausiai kreipiamasi norint prisijungti prie neegzistuojančių vartotojų paskyrų (61% visų bandymų susijungti)
- Pagrindiniai problemų šaltiniai užsienyje – JAV, Korėja, Taivanas, Kinija. Panašių incidentų iš Lietuvos IP adresų nepastebėta.

- Siūlomas sprendimo būdas – blokuoti visus prisijungimus prie Programų inžinerijos katedros serverių iš užsienio SSH ir POP3 ir kitais protokolais, HTTP ir FTP paliekant atvirus. Absoliuti dauguma katedros serverių vartotojų gyvena Lietuvoje, tuo tarpu susijungimus į užsienį leisti tik pagal asmeninį prašymą ir fiksuotą IP adresą. Taip pat galima konfigūruoti sistemą, kad ši neleistų pakeisti slaptažodžio į lengvai nuspėjamą.
- Problemoms kartojantis galima pakeisti standartinių paslaugų tiekimo prievadus.

# 6. Terminų ir santraukų žodynas

**DB** – duomenų bazė.

**HTML** *(angl. Hyper Text Markup Language)* – žiniatinklio programavimo kalba.

**FTP** *(angl. File Transfer Protocol)* – bylų persiuntimo protokolas

**HTTP** *(angl. Hyper Text Transfer Protocol)* – duomenų perdavimo protokolas.

**PĮ** – programinė įranga

**SSH** *(angl. Super Secure Shell)* – saugus duomenų perdavimo protokolas tinkle.

**PHP** *(angl. Hypertext Preprocessor)*– programavimo kalba.

**LTS** – lokalaus tinklo stebėjimas

**LAN** *(angl. Local Area Network)* – vietinis tinklas.

**WI–FI** – bevielio tinklo technologija

**ODBC** *(angl. Open Database Connectivity)* – sąsaja, leidžianti jungtis ir bendrauti su reliacinėmis duomenų bazėmis. Praktiškai kiekvienai DBVS egzistuoja atskiros ODBC tvarkyklės. Įdiegus ODBC tvarkyklę ir nurodžius ODBC duomenų šaltinį, SQL užklausų pagalba galima bendrauti tiek su vietinėmis, tiek su nutolusiomis duomenų bazėmis.

**RUP** *(angl. Rational Unified Process*) – Rational unifikuotas procesas, apibendrintas projektavimo metodas.

**SQL** *(angl. Structural Query Language)* – struktūrizuota užklausų kalba, skirta duomenų, esančių kompiuterinėje duomenų bazėje, nuskaitymui ir apdorojimui.

**TCP/IP** (*angl. Transmission Control Protoco/Internet Protocol*) – transporto valdymo protokolas/interneto protokolas, leidžia programuotojui realizuoti ryšį tarp dviejų kompiuterių bei siųsti duomenis abiem kryptimis.

**UML** (*angl. Unified Modeling Language*) – unifikuota modeliavimo kalba.

**DOS** (*angl. Denial of Service*) **–** paslaugų nutraukimo ataka.

# 7. Literatūra


[1] BRENTON, C. *Mastering Network Security*, Sybex, 2002, 520 p.

[2] *Finally, an easily installed networking monitor application that delivers* [interaktyvus]. [Žiūrėta 2006 05 21], prieiga internete <http://www.castlerock.com/pdf/SNMPc%207%20review.pdf>

[3] WHEATLEY, M. *The Myths of Open Source*, CIO magazine [interaktyvus]. 2004, nr. 3 [žiūrėta 2006 05 21], Prieiga per internetą <http://www.cio.com/archive/030104/open.html>

[4] *„Kimono'' – flexible network monitor* [interaktyvus]. [Žiūrėta 2006 05 21], Prieiga per internetą <http://downshift.org/kimono/about.php>

[5] *Network diagnosis and report tool* [interaktyvus]. [Žiūrėta 2006 05 21]. Prieiga per internetą : <http://www.adremsoft.com/netcrunch/index.php>

[6] BROOKS, K. *Networking Complete*. Sybex Network Press, 2001, 877 psl.

[7] GALVIN, P. *Role–Based Access Control*, Sys Admin magazine [interaktyvus] 2001 rugpjūtis [žiūrėta 2006 05 21]. Prieiga per internetą: <http://www.samag.com/documents/s=1147/sam0108p/0108p.htm>

[8] STANFIELD, V., *Linux sistemos administravimas*, Kaunas, Smaltija, 2003, 629 psl.

[9] *Client–server architecture* [interaktyvus]. Iš Britannica Encyclopedia Online. [Žiūrėta 2006 05 21]. Prieiga per internetą: <http://www.britannica.com/ebc/article?tocId=9360963&query=database&ct=gen1>

[10] JANG, M. Linux *Annoyances for Geeks*, 2006, 502 psl.

[11] CASTRO, E. *HTML for the World Wide Web with XHTML and CSS: Visual QuickStart Guide, Fifth Editon*. Elizabeth Castro . Peachpit Press; 5 edition (September 17, 2002) 480 psl.

[12] MCCLURE, S. *Hacking Exposed: Network Security Secrets & Solutions*, 2003, 737 psl.

[13] PHILLIPS, A. *Requirements for the Internationalization of Web Servines* [interaktyvus]. [Žiūrėta 2006 05 11]. Prieiga per internetą: <http://www.w3.org/TR/ws-i18n-req/>

[14] LADD, E. *Using HTML4, Java 1.1 and JavaScript 1.2*., 1998, 1395 psl.

[15] ALLEN, J. *PHP4*, Smaltijos leidykla, Kaunas 2003, 708 psl.

[16] HATCH, B. *Hacking Linux exposed: Linux Security Secrets & Solutions*. ISBN 0–07–212773–2 McGraw–Hill Osborne Media; 2002 566 psl.

[17] SCAMBRAY, J. *Hacking Exposed (Second edition,* McGraw–Hill Osborne Media; 2002 843 psl.*)*

[18] LitNET CERT. *Kaip pranešti apie kompiuterinę ataką?* [interaktyvus]. [Žiūrėta 2006 05 21] Prieiga per internetą: <http://cert.litnet.lt/pranesti/kaip_raportuoti.html>

[19] *Nutarimas: Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo* [interaktyvus]. Vilnius, 2003 [žiūrėta 2006 05 21]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=206198&p_query=kompiuteri%F8%20tinkl%F8&p_tr2=1>

[20] *Lietuvos Respublikos Konstitucinio teismo nutarimas* [interaktyvus]. Vilnius, 2005 [žiūrėta 2006 05 21]. Prieiga per internetą: <http://www3.lrs.lt/cgi–bin/getfmt?C1=e&C2=262264>

[21] *Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LitNET naudojimo taisyklės* [interaktyvus]. [Žiūrėta 2006 05 21]. Prieiga per internetą: <http://www.litnet.lt/index.php?option=com_content&task=view&id=23&Itemid=47>

[22] *WinTask procesų biblioteka* [interaktyvus]. [Žiūrėta 2006 05 21]. Prieiga per internetą: http://www.liutilities.com/products/wintaskspro/processlibrary/

# 8. Priedai

## *8.1 Priedas. Programų inžinerijos katedrai priklausantys serveriai.*

*8 lentelė. Serveriai*

| **Serverio tipas** | **Serverių skaičius** | **Aprašymas** |
|---|---|---|
| PĮ katedros aptarnaujami serveriai | | |
| Windows | 1 | Serveris administratoriaus darbo vietoje. Naudojamas kompiuterių priežiūrai ir diagnostikai. |
| Linux | 2 | Serveris vartotojų informacijai ir kopijoms<br>Serveris vartotojų paštui |

## *8.2. priedas. Katedros darbuotojai prižiūrintys kompiuterius.*

### 8.2.1. Sistemų administratorius

*9 lentelė. Sistemų administratorius.*

| | |
|---|---|
| **Pareigybės pavadinimas** | Sistemų administratorius |
| Sritis | Technologijų |
| Departamentas | IT departamentas |
| **Skyrius** | Paslaugų tarnyba |
| **Pareigybės darbo tikslas** | Kompiuterinių sistemų bei programinės įrangos techninė priežiūra ir aptarnavimas. Tiesioginis bendravimas su klientais. Bendradarbiavimas su darbuotojais, vystančiais, diegiančiais ir prižiūrinčiais organizacijos sistemas ir infrastruktūrą. |

| | |
|---|---|
| **Pareigybės funkcijos** | **Serviso tarnybos funkcijos (40%):**<br>❑ Gaunamų incidentų valdymas.<br>❑ Incidentų ir problemų tyrimas bei diagnostika.<br>❑ Galimų problemų nustatymas ir valdymo problemų įvardijimas.<br>❑ Priskirto incidento sprendimas ir rezultato registravimas sistemoje.<br>❑ Veiksmų, kurie ištaisytų žinomas klaidas vykdymas.<br>❑ Sprendimų paieška techninėje dokumentacijoje.<br>❑ Sprendžiamų incidentų susiejimas su problemomis.<br>❑ Galimų problemų nustatymas ir valdymo problemų įvardijimas.<br>❑ Veiksmų, kurie ištaisytų žinomas klaidas vykdymas.<br>❑ Bendravimas su klientais.<br>**Sistemų administravimas (60%):**<br>❑ Serverių administravimas ir priežiūra.<br>❑ Klaidų prevencija ir šalinimas.<br>❑ Kompiuterinės ir programinės įrangos diegimas.<br>❑ Sistemos saugumo ir veiklos stabilumo užtikrinimas.<br>❑ Duomenų archyvavimas, atstatymas.<br>❑ Duomenų saugumo užtikrinimas.<br>❑ Dalyvavimas integruojant sistemas.<br>❑ Infrastruktūros projektavimas.<br>❑ Sistemos techninių galimybių stebėjimas ir rezervų planavimas.<br>❑ Kitų techninių darbuotojų vykdomos veiklos priežiūra.<br>❑ Dalyvavimas pojektuose. |
| **Kita** | ❑ Kiti, tiesioginio vadovo deleguoti darbai.<br>❑ Sprendimų komandos narys per pagrindinius incidentus. |
| **Žinios ir įgūdžiai** | ❑ Ne mažesnė kaip 2 m. panašaus darbo patirtis<br>❑ Geras kompiuterinių sistemų ir programinės įrangos išmanymas<br>❑ Darbo su duomenų bazėmis patirtis<br>❑ Programavimo patirtis (MS SQL, Oracle)<br>❑ Unix/Windows žinios<br>❑ Infrastruktūros vystymo projektų patirtis<br>❑ Geros techninės anglų k. žinios<br>❑ Vadovavimo projektams patirtis |
| **Gebėjimai** | ❑ Greitas sudėtingų techninių problemų sprendimas<br>❑ Darbas komandoje<br>❑ Iniciatyvumas, noras mokytis ir tobulėti<br>❑ Gebėjimas dirbti savarankiškai, atsakingumas |
| **Išsilavinimas** | ❑ Aukštasis (informatika, elektronika, programavimas) |
| **Monitoringas** | Aktyviai stebi esamo kompiuterių klasių, personalo kompiuterių, organizacinės technikos būklę, ieško galimų problemų ir užtikrina išankstinę gedimų profilaktiką. Stebi esamų problemų lygį ir būseną. Atrenka kritines užduotis. |

## 8.2.2. Tinklo administratorius

*10 lentelė. Tinklo administratorius.*

| | |
|---|---|
| **Pareigybės pavadinimas** | Tinklo administratorius |
| Sritis | Technologijų |
| Departamentas | IT departamentas |
| **Skyrius** | Paslaugų tarnyba |
| **Pareigybės darbo tikslas** | Užtikrinti organizacijos ar organizacijų grupės kompiuterių tinklo veikimą ir vystymą. |
| **Pareigybės funkcijos** | **Serviso tarnybos funkcijos (40%):**<br>❑ Gaunamų incidentų valdymas.<br>❑ Incidentų ir problemų tyrimas bei diagnostika.<br>❑ Galimų problemų nustatymas ir valdymo problemų įvardijimas.<br>❑ Priskirto incidento sprendimas ir rezultato registravimas sistemoje.<br>❑ Veiksmų, kurie ištaisytų žinomas klaidas vykdymas.<br>❑ Sprendimų paieška techninėje dokumentacijoje.<br>❑ Sprendžiamų incidentų susiejimas su problemomis.<br>❑ Galimų problemų nustatymas ir valdymo problemų įvardijimas.<br>❑ Veiksmų, kurie ištaisytų žinomas klaidas vykdymas.<br>❑ Bendravimas su klientais.<br>❑ SD konsultavimas tinklo klausimais.<br>**Tinklo administravimas (60%):**<br>❑ Vartotojų teisių administravimas.<br>❑ Naujų darbo vietų rengimas.<br>❑ Periferinės tinklinės įrangos diegimas.<br>❑ Naujos programinės įrangos diegimas.<br>❑ Vartotojų prijungimo prie interneto ar organizacijos vidinio tinklo administravimas.<br>❑ Duomenų saugumo užtikrinimas.<br>❑ Atsarginių duomenų kopijų darymas.<br>❑ Saugumo sistemų stebėjimas, apsaugos nuo įsilaužimo į tinklą užtikrinimas.<br>❑ Tinklo pritaikymas vartotojų poreikiams ir optimizavimas.<br>❑ Vidinio tinklo resursų valdymas (IP adresai ir kt.).<br>❑ Vartotojų mokymas.<br>❑ Tinklo resursų panaudojimo stebėjimas.<br>❑ Tinklo vystymo ir tobulinimo klausimų inicijavimas.<br>❑ Nelegalios programinės įrangos naudojimo prevencija.<br>❑ Vartotojų, pažeidžiančių naudojimosi tinklu taisykles apribojimas.<br>❑ Dalyvavimas projektuojant infrastruktūrą.<br>❑ Dalyvavimas integruojant sistemas. |
| **Kita** | ❑ Kiti, tiesioginio vadovo deleguoti darbai.<br>❑ Sprendimų komandos narys per pagrindinius incidentus. |
| **Žinios ir įgūdžiai** | ❑ Ne mažesnė kaip 2 m. kompiuterinio tinklo priežiūros (LAN) patirtis (IP, DNS, Mail, Web server, FTP ir kt.)<br>❑ Tinklo įrangos ir infrastruktūros išmanymas<br>❑ Geras kompiuterinių sistemų ir programinės įrangos išmanymas<br>❑ Tinklo saugumo reikalavimų išmanymas |

| | |
|---|---|
| | ❑ Programavimo patirtis<br>❑ Unix/Windows žinios<br>❑ Geros techninės anglų k. žinios |
| **Gebėjimai** | ❑ Greitas sudėtingų techninių problemų sprendimas<br>❑ Darbas komandoje<br>❑ Iniciatyvumas, noras mokytis ir tobulėti<br>❑ Gebėjimas dirbti savarankiškai, nuolatinės priežiūros<br>❑ Atsakingumas |
| **Išsilavinimas** | ❑ Aukštasis techninis |
| **Monitoringas** | Aktyviai stebi esamo kompiuterių tinklo būklę, ieško galimų problemų ir užtikrina išankstinę gedimų profilaktiką. Stebi esamų problemų lygį ir būseną. Atrenka kritines užduotis. |

## 8.2.3. Duomenų bazių administratorius

*11 lentelė. Duomenų bazių administratorius.*

| | |
|---|---|
| **Pareigybės pavadinimas** | Duomenų bazių administratorius |
| Sritis | Technologijų |
| Departamentas | IT departamentas |
| **Skyrius** | Paslaugų tarnyba |
| **Pareigybės darbo tikslas** | Duomenų bazių priežiūra ir aptarnavimas. |

| | |
|---|---|
| **Pareigybės funkcijos** | **Serviso tarnybos funkcijos (25%):**<br>❑ Gaunamų incidentų valdymas.<br>❑ Incidentų ir problemų tyrimas bei diagnostika.<br>❑ Galimų problemų nustatymas ir valdymo problemų įvardijimas.<br>❑ Priskirto incidento sprendimas ir rezultato registravimas sistemoje.<br>❑ Veiksmų, kurie ištaisytų žinomas klaidas vykdymas.<br>❑ Sprendimų paieška techninėje dokumentacijoje.<br>❑ Sprendžiamų incidentų susiejimas su problemomis.<br>❑ Galimų problemų nustatymas ir valdymo problemų įvardijimas.<br>❑ Veiksmų, kurie ištaisytų žinomas klaidas vykdymas.<br>**Duomenų bazių administravimas (75%):**<br>❑ Serverių administravimas ir priežiūra.<br>❑ Greitas reagavimas į duomenų bazių klaidas.<br>❑ Duomenų bazės instaliavimas, atnaujinimas, migravimas, pakeitimų testavimas.<br>❑ Duomenų archyvavimas, atstatymas.<br>❑ Duomenų saugumo užtikrinimas.<br>❑ Dalyvavimas integruojant sistemas.<br>❑ Duomenų rinkimo, kodavimo, sąsajų, keitimo procedūrų kūrimas ir įgyvendinimas.<br>❑ Duomenų bazių veiklos stebėjimas ir optimizavimas.<br>❑ Duomenų pilnumo ir suderinamumo užtikrinimas.<br>❑ Siūlymai, kaip tobulinti duomenų bazes ir duomenų kaupimą.<br>❑ Kompiuterinės įrangos atranka ir pirkimas.<br>❑ Tinkamo sistemos funkcionavimo ir veikimo patikra.<br>❑ Infrastruktūros projektavimas.<br>❑ Pakeitimų dokumentavimas. |
| **Kita** | ❑ Kiti, tiesioginio vadovo deleguoti darbai.<br>❑ Sprendimų komandos narys per pagrindinius incidentus. |
| **Kvalifikacija:** | |
| **Žinios ir įgūdžiai** | ❑ Geras kompiuterinių sistemų ir programinės įrangos išmanymas<br>❑ Ne mažesnė kaip 2m. darbo su duomenų bazėmis patirtis<br>❑ Programavimo patirtis (MS SQL, Oracle)<br>❑ Unix/Windows žinios<br>❑ Serverių administravimo patirtis<br>❑ Infrastruktūros vystymo projektų patirtis<br>❑ Geros techninės anglų k. žinios<br>❑ Vadovavimo projektams patirtis |
| **Gebėjimai** | ❑ Greitas sudėtingų techninių problemų sprendimas<br>❑ Gebėjimas dirbti savarankiškai ir komandoje<br>❑ Laiko planavimas ir užduočių prioritetizavimas<br>❑ Iniciatyvumas, noras mokytis ir tobulėti<br>❑ Atsakingumas |
| **Išsilavinimas** | ❑ Aukštasis techninis (informatika, programavimas) |
| **Monitoringas** | Aktyviai stebi esamų duomenų bazių būklę, ieško galimų problemų ir užtikrina išankstinę gedimų profilaktiką. Stebi esamų problemų lygį ir būseną. Atrenka kritines užduotis. |

## 8.2.4. Incidentų sprendėjas

*12 lentelė. Incidentų sprendėjas.*

| | |
|---|---|
| **Pareigybės pavadinimas** | Incidentų sprendėjas |
| Sritis | Technologijų |
| Departamentas | IT departamentas |
| **Skyrius** | Paslaugų tarnyba |
| **Tiesioginio vadovo pareigybė** | Paslaugų tarnybos vadovas |
| **Pareigybės darbo tikslas** | Spręsti vartotojų užklausas, teikti pirminę pagalbą vartotojams, nustatant problemos pobūdį ir suteikiant informaciją apie sprendimo kelius. Užtikrinti incidentų išsprendimą per nustatytą laiką. |
| **Pareigybės funkcijos** | **Serviso tarnybos funkcijos (100%):**<br>❑ Užregistruotų užklausų sprendimas.<br>❑ Užklausos informacijos papildymas.<br>❑ Neišspręstų užklausų persiuntimas antro lygio sprendėjams.<br>❑ Incidentų diagnozavimas, registravimas, detalizavimas, sprendimas.<br>❑ Kliento informavimas apie sprendžiamo incidentų būseną.<br>❑ Sprendimų atitikimo SLA susitarimams užtikrinimas.<br>❑ Nepriskirtų ir pradinės pagalbos būdu neišspręstų užklausų/incidentų eskalavimas<br>❑ Bendradarbiavimas su kitų padalinių darbuotojais, užtikrinant greitą ir efektyvų sprendimą.<br>❑ Potencialių problemų išaiškinimas ir eskalavimas.<br>❑ Kritinių incidentų identifikavimas ir reikiamų sprendimo procesų inicijavimas.<br>❑ Vadovybės informavimas apie problemas, kurios įtakoja masinius sutrikimus. |
| **Kita** | ❑ Kiti, tiesioginio vadovo deleguoti darbai.<br>❑ Nuolatinis naujų žinių įgijimas (vartotojo instrukcijos, sprendimų bazė, mokymai). |
| **Kvalifikacija:** | |
| **Žinios ir įgūdžiai** | ❑ Patirtis klientų aptarnavimo srityje (aptarnavimo tarnyba, techninio aptarnavimo padalinys)<br>❑ Žinios, apimančios Microsoft Windows ir Linux operacines sistemas, vartotojiškas programas, tinklo, techninės ir programinės įrangų galimus sutrikimus<br>❑ Geras anglų kalbos mokėjimas (rusų k. būtų privalumas)<br>❑ Greitas spausdinimas.<br>❑ Derybų įgūdžiai. |
| **Gebėjimai** | ❑ Orientacija į klientą.<br>❑ Atsakingumas.<br>❑ Iškalba formuojant mintis tiek žodžiu, tiek raštu.<br>❑ Greitas analitinis mąstymas, leidžiantis tiksliai numatyti ir įvertinti problemas.<br>❑ Organizuotumas, mokėjimas valdyti daugelio užduočių sprendimą vienu metu.<br>❑ Gebėjimas dirbti individualiai ir komandoje. |
| **Išsilavinimas** | ❑ Aukštasis techninis |
| **Monitoringas** | Aktyviai sprendžia susidariusias problemas, jas stebi, bendrauja ir informuoja vartotojus. |

### 8.2.5. Pažyma apie programinės įrangos įdiegimą katedros kompiuteriuose

Kauno technologijos universiteto
Informatikos fakulteto
Programų inžinerijos katedros
Vedėjo E. Bareišos

**PAŽYMA**

Šiuo raštu pažymima, kad magistranto Kęstučio Morkūno sukurta „Lokalaus tinklo incidentų monitoringo“ programinė įranga yra įdiegta Programų inžinerijos katedros serveriuose. Bandomasis diegimas yra atliktas mokymo klasių kompiuteriuose.

Programinė įranga buvo kuriama Programų inžinerijos katedros užsakymu. Šiuo metu įdiegta programos versija pilnai tenkina poreikius ir atitinka kūrimo pradžioje iškeltus ir eigoje papildytus reikalavimus.

Programų inžinerijos katedros vedėjas

prof. dr. E. Bareiša _____