KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Laimonas Žakevičius

Asmens duomenų apsaugos metodų tyrimas ir pritaikymas personalo valdymo informacinėje sistemoje

Magistro darbas

Darbo vadovas
dr. Audronė Janavičiūtė

KAUNAS, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Asmens duomenų apsaugos metodų tyrimas ir pritaikymas personalo valdymo informacinėje sistemoje

Magistro darbas

Recenzentas

doc.dr. Jevgenijus Toldinas
2011-05-27

Vadovas

dr. Audronė Janavičiūtė
2011-05-27

Atliko
IFN 9/3 gr. stud.
Laimonas Žakevičius
2011-05-27

KAUNAS, 2011

Turinys

Pratarmė

Autorius: Laimonas Žakevičius

Tema: Asmens duomenų apsaugos metodų tyrimas ir pritaikymas personalo valdymo informacinėje sistemoje

Šio tyrimo tikslas – išanalizuoti asmens duomenų šifravimo metodus ir pritaikyti optimaliausią metodą personalo valdymo informacinėje sistemoje. Tyrimui atlikti buvo panaudota autoriaus suprojektuota ir sukurta personalo valdymo informacinė sistema, kuri yra įdiegta ir naudojama UAB „Teledema“.

Sukūrus personalo valdymo informacinės sistemos programinį modulį (servisą, kurio paskirtis įvestus į personalo valdymo informacinę sistemą duomenis užšifruoti ir užšifruotus persiųsti į duomenų bazių valdymo sistemą, arba gautus užšifruotus duomenis iš duomenų bazių valdymo sistemos, iššifruoti ir pateikti vartotojui, pageidauta forma), personalo valdymo informacinė sistema taps saugia ir patikima sistema, kuri leistų kaupti išsamius, tikslius duomenis realiu laiku, juos sistemintų ir pateiktų sistemos vartotojams, kuriems yra suteiktos teisės susipažinti, valdyti ir tvarkyti tokią informaciją, taip pat užtikrintų, kad saugomi asmens duomenys yra laikomi šifruotu pavidalu, todėl duomenis galės peržiūrėti, valdyti ir tvarkyti tik tie asmenys, kuriems leidimą yra davęs duomenų valdytojas.

Įvadas

Lietuvos įmonėse plečiantis informacinių technologijų skvarbai atsiranda daug naujų galimybių. Viena iš didesnių ir bendra visoms įmonėms bei įstaigoms problema yra personalo valdymas. Įvairios įmonės ir įstaigos renkasi skirtingus šios problemos sprendimo būdus. Tačiau dabartiniu metu galima išskirti tokias problemas, su kuriomis susiduria įmonės ir įstaigos, norinčios turėti personalo valdymo informacinę sistemą:

- Sistema privalo būti saugi ir patikima, nes sistema saugo asmens duomenis.
- Asmens duomenys privalo būti saugomi saugia forma, kad duomenis galėtų peržiūrėti, valdyti ir tvarkyti tik tie asmenys, kuriems leidimą davė duomenų valdytojas.

Atlikus tyrimą gautume tokią naudą:

- Turėtume sistemą, kuri būtų saugi ir patikima.
- Asmens duomenys būtų saugomi šifruotame pavidale, kas užtikrintų, kad duomenis galėtų peržiūrėti, valdyti ir tvarkyti tik tie asmenys, kuriems leidimą davė duomenų valdytojas.

Tyrimo tikslas – Išanalizuoti asmens duomenų šifravimo metodus ir pritaikyti optimaliausią metodą personalo valdymo informacinėje sistemoje. Tyrimui atlikti buvo panaudota autoriaus suprojektuota ir sukurta personalo valdymo informacinė sistema, kuri yra įdiegta ir naudojama UAB „Teledema“. UAB „Teledema“ yra vidutinio kapitalo įmonė, joje dirba apie 60 žmonių. Personalo valdymo informacinę sistemą naudoja įmonės vadovas, įmonės skyrių vadovai, įmonės personalo vadovas. Jie nuolat įveda į sistemą ir gauna iš sistemos įvairius jiems reikalingus duomenis, todėl yra poreikis turėti saugią sistemą.

Tikslui pasiekti buvo iškelti šie uždaviniai:

- Išanalizuoti, kurie asmens duomenys privalo būti apsaugoti;
- Išanalizuoti asmens duomenų apsaugos metodus;
- Išanalizuoti duomenų šifravimo metodus;
- Praplėsti personalo valdymo informacinę sistemą duomenų šifravimo moduliu, duomenims šifruoti;
- Atlikti duomenų šifravimo metodų pritaikymo tyrimą, naudojant metodus taikomųjų uždavinių serveryje ir duomenų bazių valdymo sistemos serveryje;
- Ištirti realioje aplinkoje duomenų šifravimo metodų efektyvumą.

Tyrimo tikslo sprendimo metodas, priemonės ir rezultatai: sukurtas sprendimas eksploatuojamos personalo valdymo informacinės sistemos duomenims šifruoti. Projektui realizuoti naudota PHP programavimo kalba, Microsoft .NET Framework ir MySQL duomenų

bazių valdymo sistema, priemonių pasirinkimą ribojo eksploatuojama sistema. Sukurti personalo valdymo informacinės sistemos programinis modulis leidžiantis apsaugoti asmens duomenis eksploatuojamoje sistemoje ir ištirtas šios sistemos darbas, kai :

- duomenys nėra šifruojami ir iššifruojami;
- duomenims šifruojami ir iššifruojami duomenų bazių valdymo sistemos serveryje naudojant standartines MySQL priemones;
- duomenis šifruos ir iššifruos DSM (programinis sistemos modulis (servisas) leidžiantis atlikti duomenų šifravimą ir iššifravimą ir integruojamas į eksploatuojamą sistemą) suteiksiantis galimybę naudotis simetriniais-blokiniais ir simetriniu – srautiniu duomenų šifravimo algoritmais.

Tyrimo rezultatai buvo publikuoti Informacinės Technologijos, XVI tarpuniversitetinė magistrantų ir doktorantų konferencija, Konferencijos pranešimų medžiaga Psl. 41-44 ; ISSN 2029-249X, 2011-04-22 (Konferencijos pranešimų medžiaga pateikta 1 priede). Sukurtas programinis sistemos modulis yra įdiegtas ir eksploatuojamas UAB „Teledema“ personalo valdymo informacinėje sistemoje (Įdiegimo raštas pateiktas 2 priede).

I. Asmens duomenų apsaugos metodų apžvalga ir analizė

1.1. Asmens duomenų apsauga Lietuvos Respublikoje

Statistikos departamento atlikto tyrimo duomenimis Lietuvoje nuolat didėja įmonių skaičius nuo 56176 (2005 m. sausio mėn.) iki 65526 (2009 m. sausio mėn.) [1]. 2008 m. pradžioje 94,8 % gamybos ir paslaugų įmonių, kuriose dirbo 10 ir daugiau darbuotojų darbe naudojosi kompiuteriais, 92,7 % – internetu. 2007 m. pradžioje kompiuteriais ir internetu atitinkamai naudojosi 90,5 % ir 88,4 % įmonių. Kompiuterius kasdieniniame darbe bent kartą per savaitę naudojo 32,2 %, internetą – 28,9 % gamybos ir paslaugų įmonių darbuotojų (2007 m. – atitinkamai 29,1 % ir 25,5 %), todėl daugėja įmonių, kurios verslo procesus siekia automatizuoti maksimaliai [2].

Vienas iš aktualiausių įmonės ir įstaigos valdymo procesų yra personalo valdymas. Lietuvos įmonėse ir įstaigose didėja poreikis turėti personalo valdymo informacines sistemas. Vienos įmonės ir įstaigos („Senukai“, „Mažeikių Nafta“, Švietimo ir Mokslo Ministerija) tokias sistemas perka iš IT sprendimus kuriančių bendrovių (UAB „Proringas“, UAB „Kibernetinė erdvė“), kitos didesnės įmonės, turinčios savo informacinių technologijų poskyrius, pačios kuria tokias sistemas. Tačiau visos įmonės ir įstaigos susiduria su esmine problema, kaip išspręsti asmens duomenų saugumo klausimus naudojantis informacinėmis sistemomis.

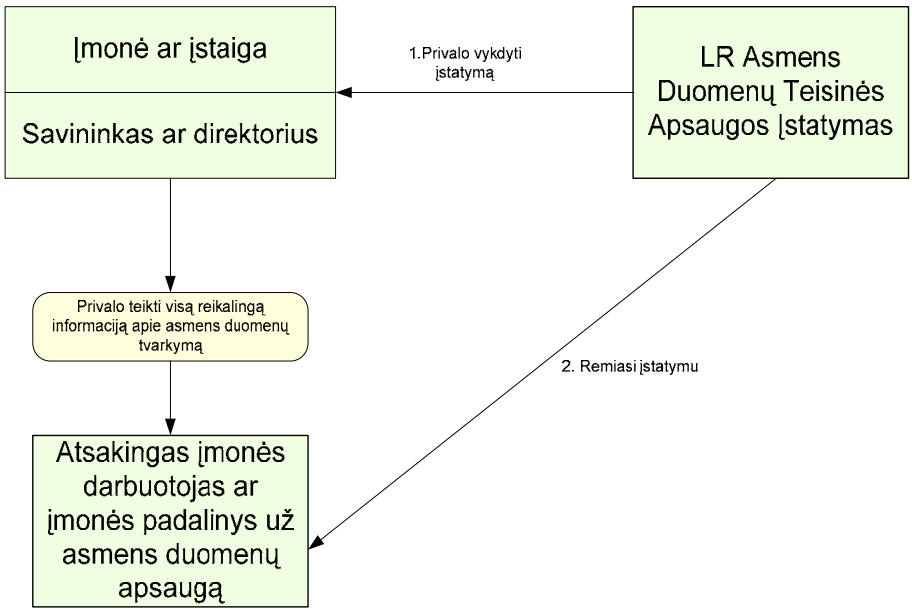
Kaip apibrėžia Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas [3] „**Asmens duomenys - duomenys apie konkretų arba iš duomenų nustatomą fizinį asmenį, jo dalykinius santykius ir išvados apie asmenį, padarytos remiantis šiais duomenimis.** Ypatingi asmens duomenys – asmens duomenys apie jo rasinę kilmę, tautinį ir etninį priklausomumą, politinius, religinius ir kitus įsitikinimus, partiškumą, teistumą, sveikatą, patologinius defektus ir intymų gyvenimą (privatų asmens gyvenimą).“ Tokie duomenys remiantis aukščiau minėtojo įstatymo 4 str. 1 dalimi turi būti saugomi visą fizinio asmens gyvenimą.

Visos įmonės ir įstaigos, kurios atitinka Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo 2 str. 8 dalies aprašymą „**Duomenų valdytojas – fizinis arba juridinis asmuo, kuris teisėtai tvarko duomenis**“ privalo tinkamai pasirūpinti asmens duomenų apsauga, nes įmones ir įstaigas įpareigoja minėtojo įstatymo 5 str. 1 dalis, kuri teigia, kad “Asmens duomenys yra kaupiami ir saugomi duomenų įrašuose, už kurių apsaugą ir tvarkymą yra atsakingas duomenų valdytojas.“

Ypatingas dėmesys turi būti skiriamas ypatingų asmens duomenų tvarkymui, nes minėti duomenys gali būti tvarkomi, tik išimtinais atvejais, kaip „toks tvarkymas yra būtinas darbo ar

valstybės tarnybos tikslu duomenų valdytojo teisėms ir prievolėms darbo teisės srityje įgyvendinti įstatymų nustatytais atvejais“ [4].

Įmonės ar įstaigos asmens duomenis tvarko įprastinės raštvedybos būdu arba duomenys tvarkomi automatiniu būdu, tai yra asmens duomenims tvarkyti naudojama verslo valdymo informacinė sistema su integruotu personalo valdymo sistemos moduliu arba personalo valdymo informacinė sistema. Jei įmonė ar įstaiga naudoja įprastinę raštvedybą, tada turi būti paskirtas asmuo arba padalinys atsakingas už duomenų apsaugą. Toks asmuo ar padalinys nėra laikomas duomenų tvarkytoju [5]. Atsakingas asmuo ar padalinys prižiūri (1 pav.), kad asmens duomenys būtų tvarkomi laikantis Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, reglamentuojančių asmens duomenų apsaugos tvarką. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas įpareigoja duomenų valdytoją (įmonę ar įstaigą) suteikti atsakingam asmeniui ar padaliniui už asmens duomenų apsaugą visą reikalingą informaciją apie asmens duomenų tvarkymą arba numatomą asmens duomenų tvarkymo automatizavimą.



1 pav. Duomenų valdytojo atsakomybės už asmens duomenis schema

Todėl personalo valdymo informacinė sistema turi būti saugi sistema, nes pagrindinė tokios sistemos paskirtis yra asmens duomenų (vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, telefono numeris, Socialinio draudimo pažymėjimo numeris, lytis, šeimyninė padėtis ir kita informacija apie asmenį) tvarkymas – duomenų rinkimas, kaupimas, apdorojimas ir saugojimas.

1.2. Asmens duomenų apsaugos elektroninėje erdvėje metodų apžvalga ir analizė

Lietuvoje nuolat auga aktyvių interneto vartotojų skaičius, 2009 m. vasarą atlikto tyrimo duomenis net 76,1% vartotojų naudojasi elektroniniu paštu, daugiau kaip 49,8% naudojasi internetinio banko paslaugomis, ir net 12,7% perka prekes ir paslaugas elektroninėse parduotuvėse [6]. Tačiau daugelis vartotojų nenutuokia apie rizikas jų asmens duomenų privatumui naudojantis interneto ryšiu. Apžvelgsime privatumui iškylančias rizikas naudojantis elektroniniu paštu, tiesiog naršant internete, perkant elektroninėse parduotuvėse ir išanalizuosime siūlomus Europos Komisijos ir valstybinės duomenų apsaugos inspekcijos asmens duomenų apsaugos metodus [7, 8].

1.2.1. Privatumui iškylančios rizikos naudojantis elektroniniu paštu

Elektroninio pašto adresas yra reikalingas norint išsiųsti arba gauti elektroninį laišką, tačiau jis tuo pačiu tampa svarbiu informacijos šaltiniu, kuris gali turėti asmeninės informacijos apie vartotoją. Atsiranda įvairios privatumo rizikos, kaip:

- Naudojantis neatnaujinta interneto naršykle ir lankantis nesaugiose svetainėse „palikti“ savo elektroninio pašto adresą.
- Elektroninio pašto adresas gali būti užklausiamas įvairių svetainių (dažniausiai elektroninės parduotuvės) įvairiais tikslais.
- Naudojantis elektroniniu paštu, kai kurie vartotojai nesugeba lengvai ir teisingai panaikinti elektroninio pašto žinutę, kai ji nusiunčiama arba gaunama, kadangi pasinaudojus ištrynimo funkcija, žinutė ne visais atvejais bus ištrinta.
- Speciali techninė ir programinė įranga gali būti naudojama duomenų stebėjimui tinkle. Ši įranga gali nešifruotus duomenų srautus pateikti aiškiu tekstu.

Visos šios išvardintos situacijos gali sukelti tokias problemas, kaip „brukalų“ laiškai, patekimas į elektroninio pašto žinynus, nepageidaujamų ir kenkėjiškų (virusai,“trojos arkliai“) laiškų gavimas. Norint išvengti tokių problemų yra siūlomi šie metodai [7, 8]:

- Vartotojas turi atsakingai naudotis elektroniniu paštu, [9] todėl registruodamasis ar pildydamas įvairias formas ar anketas turi būti įsitikinęs, kad svetainė atitinka rekomenduojamus saugumo standartus – ji naudoja SSL, SET protokolus [10, 11] turi saugumo žymes [12, 13].
- Elektroninio laiško turinio šifravimas ir iššifravimas. Šifravimas ir iššifravimas remiasi programine įranga, kuri papildo įprastas elektroninio pašto programas. Šio metodo patikimumas priklauso nuo pasirinkto algoritmo ir raktažodžių ilgio.

- Vientisumas. Tokio metodo principas yra, kai teksto pagrindu sukuriamas specialus kodas ir persiuntus šį kodą kartu su užkoduotu tekstu, iškodavus tekstą galima patikrinti ar nebuvo atlikta pakeitimų.
- Autentifikavimas. Norint tai atlikti reikalinga pasikeisti skaitmeniniais parašais, jie garantuoja, kad vartotojas yra tas kuris tvirtina esąs.

1.2.2. Privatumui iškylančios rizikos naršant internete

Pagrindinis naršymo internete tikslas yra rasti reikalingą informaciją, tai yra susiję su įvairiausių interneto svetainių peržiūra. Naršant vartotojas dažnai spaudžia ant įvairiausių nuorodų, kurios jį perkelia į kitas svetaines. Vienas iš svarbiausių rūpimų klausimų yra kokios informacijos iš vartotojo reikia interneto svetainėms, kad jos galėtų teikti vartotojams paslaugas. Paprastai, tai būna:

- Operacinė sistema.
- Interneto naršyklės tipas ir versija.
- Protokolai naudojami naršymui.
- Kalbos nustatymai.
- Slapukai.

Paskutinis punktas ir kelia didžiausią pavojų asmens duomenų privatumui. Slapukai leidžia suasmeninti svetainę, palengvina naršymą vartotojui, tačiau slapukai neretai naudojami vartotojo identifikavimui ir netgi pakartotinio registravimosi išvengimui. Ypač slapukus naudoja įvairūs interneto portalai. Interneto portaluose galima rasti daug įvairiausių nuorodų į kitas svetaines. Interneto portalai duomenis apie vartotoją renka kaip ir įprastos svetainės, tačiau jos informaciją gali saugoti „už“ portalo ribų. Tokia informacija gana dažnai būna parduodama trečioms suinteresuotoms šalims, kaip kompanijoms tiriančioms interneto vartotojų pomėgius. Todėl interneto vartotojas gali net nežinoti, kad jo asmeniniai duomenys buvo renkami ir apdorojami bei galėjo būti panaudoti jam nežinomiems tikslams. Todėl yra siūloma prisijungti, naršyti ir ieškoti internete anonimiškai.

1.2.3. Privatumui iškylančios rizikos perkant elektroninėse parduotuvėse

Elektroninė prekyba gali būti nusakoma, kad tai, bet kokia sandorio forma, kurio dalyviai sąveikauja išvengdami fizinio kontakto ir naudodami tik elektroninį būdą. Tokio tipo sandoriai leidžia prekybininkams tapti lankstesniems ir efektyvesniems, tačiau norint užtikrinti saugią prekybą internetinėse parduotuvėse reikia daug asmeninių duomenų, o tai gali kelti pavojų konfidencialumui. Žemiau pateiksiu apžvelgtus didžiausius pavojus asmens duomenų saugumui:

- Asmens duomenys gali būti renkami ir tvarkomi, ne tik teisėtiems tikslams - vienas iš dažniausių antrinių panaudojimų yra reklama. Reklama gali būti pritaikoma pasinaudojus asmenine informacija apie vartotoją.
- Dar vieną riziką sudaro persiunčiamos informacijos, kurios reikia įvykdyti sandorį, saugus perdavimas, nes jei nėra naudojami saugus protokolai, kaip SSL [10] ar SET [11] yra ganėtinai nesudėtinga perimti asmeninius duomenis.
- Ir naujausia problema atsirado išplitus 3G ir 3,5G ryšio telefonams, kurie įgalino padaryti elektroninę prekybą visiškai mobilia, tačiau mobiliojo telefono pagalba telekomunikacijų kompanijos gali nustatyti vartotojo buvimo vietą, kas suteiktų dar daugiau asmeninės informacijos apie vartotoją. Tai gali būti naudojama reklamai SMS žinutėmis.

Todėl norint užtikrinti saugią elektroninę prekybą reikia, kad svetainės tinkamai save autentifikuotų, kad pirkėjas žinotų, kad pardavėjas yra tas, kas tvirtina esąs. Pardavėjai turi rinkti tik tokius duomenis, kurių jiems tikrai reikia įvykdyti sandoriui, pačio sandorio atliekama elektroninė tranzakcija turi būti šifruojama, kad būtų užtikrinamas vientisumas.

1.2.4. Išvados

Siekiant saugiai naudotis interneto ryšio teikiamomis paslaugomis, kaip informacijos paieška, elektroninis paštas ar elektroninė prekyba ir visomis su ja susijusiomis paslaugomis, reikėtų taikyti šiuos asmens duomenų saugos metodus:

- Slapukų filtrai ir jų filtravimo priemonės įdiegtos naršyklėse, jei jų teikiamų funkcijų nepakanka galima naudoti trečių šalių pagamintas priemones.
- Proxy serveriai ir jų teikiamos paslaugos sudaro galimybę paslėpti savo IP adresą ir gali nufiltruoti svetainės siunčiamus sisteminius pranešimus.
- Elektroninio pašto filtrai leidžiantys gauti tik pageidaujamus elektroninio pašto laiškus.
- Konfidencialumo lygio žymėjimas. Tokia žymė suteikiama tik svetainėms, kurios atitinka aukštus saugos reikalavimus, keliamus žymėjimą atliekančių organizacijų. Vienos žinomiausių organizacijų yra TRUSTe [12], Better Business Bureau [13]. Todėl lankytis svetainėse, turinčiose tokias žymes, yra saugu ir patikima.
- P3P [14]. Tai konfidencialumo nuostatų platforma, jos tikslas leisti svetainėms išreikšti savo konfidencialumo nuostatas, o vartotojai, pasinaudoję šiomis nuostatomis, galės lengviau priimti sprendimą ir kontroliuoti jų informacijos

panaudojimą. Ir svarbiausias dalykas ši platforma leis aiškiau standartizuoti konfidencialumo problemas ir padidinti konfidencialumo lygį.

- Tai pat yra būtinybė įdiegti antivirusinę programą su tikslu išvengti kenkėjiškų programų (virusai, „trojos arkliai“, „klaviatūros klavišų sekikai“). Visos išvardintos programos gali atnešti didelės žalos vartotojui, todėl antivirusines programas reikia savalaikiai atnaujinti.

Išanalizavus asmens duomenims iškylančias rizikas internetinėje erdvėje, galima teigti, kad asmens duomenys internete yra plačiai paplitę ir yra pažeidžiami. Rizikai sumažinti turi būti imtasi atitinkamų priemonių. Įmonės darbuotojai darbo metu, gali atsitiktinai išplatinti svarbius asmens duomenis, kurie gali būti panaudoti kenkėjiškiems tikslams. Personalo valdymo informacinės sistemos tikslas yra tvarkyti ir valdyti darbuotojų duomenis, jų platinimas internete yra draudžiamas teisės aktais, todėl atsitiktinis asmens duomenų, saugojamų personalo valdymo informacinėje sistemos, paplitimas internete yra duomenų valdytojo atsakomybės klausimas.

1.3. Informacinių sistemų duomenų keitimosi saugos metodų apžvalga

Informacinės sistemos yra sudarytos iš klientinės dalies ir serverinės dalies bei tarp jų nuolat vykstančio duomenų keitimosi. Norint saugiai keistis duomenimis galima naudotis žemesniuose OSI lygmenyse funkcionuojančius ir saugą garantuojančius SSL/TLS protokolais ar IPsec tarnyba veikiančia TCP/IP protokolų steko tinklo lygmenyje, tad ja gali pasinaudoti visi aukštesnio lygmens protokolai. IPsec suteikia galimybę apsaugoti komunikacijas tiek vietiniame tinkle, tiek vykstančias internete.

1.3.1. SSL protokolas

SSL (Secure Sockets Layer) – kriptografinis protokolas, skirtas informacijai, perduodamai tarp kliento ir serverio, apsaugoti ją šifruojant. SSL šifravimui naudoja tiek simetrinę, tiek ir asimetrinę kriptografiją.

SSL veikia TCP/IP modelio taikymo lygmenyje. Dėl šios priežasties SSL gali būti realizuotas beveik visose operacinėse sistemose, kurios suderintos su TCP/IP nekeičiant sistemos branduolio ar TCP/IP protokolų rinkinio.

Naudojant SSL, serverio sertifikatas yra privalomas. Sertifikatas – tai X.509 v3 struktūros skaitmeninis dokumentas. Svarbiausi sertifikato elementai: versija, serijos numeris, algoritmo identifikatorius, leidėjas, galiojimo terminas, subjektas (serveris arba klientas), subjekto viešojo rakto informacija, viešojo rakto algoritmas, subjekto viešasis raktas, leidėjo unikalus identifikatorius (neprivalomas), subjekto unikalus identifikatorius (neprivalomas), išplėtimai (neprivalomi), sertifikato parašo algoritmas, sertifikato parašas.

Kai serveris naršyklei pateikia sertifikatą, ji patikrina:

- Galiojimo datą – jei sertifikatas nebegalioja, parodomas klaidos pranešimas.
- Pasirašiusios organizacijos patikimumą – sertifikatą generuoti gali bet kas, tačiau jį turi patvirtinti patikima sertifikatų tarnyba. Šiuolaikinėse naršyklėse jau būna įdiegti patikimų ir pripažintų organizacijų šakniniai sertifikatai, pagal kuriuos atliekamas žemesnio lygmens sertifikatų patikrinimas. Jei sertifikatas neišsaugotas atmintyje, naršyklė jį pateikia vartotojui, kad jis pats patikrintų sertifikato patikimumą.
- Parašą – sertifikato vientisumui patikrinti.
- Serverio tapatybę – ar sertifikate nurodytas serverio vardas sutampa su sertifikatą pateikiančio serverio vardu.

Kliento sertifikatas yra neprivalomas ir naudojamas retai. Daugelis žiniatinklyje naršančių vartotojų neturi savo asmeninių sertifikatų. Kliento sertifikatai gali būti taikomi įmonių vidiniuose tinkluose darbuotojų prieigai prie informacijos valdyti. Ateityje daugiau dėmesio skiriant žiniatinklio saugai, jų naudojimas gali išaugti [15].

1.3.2. IPsec protokolas

Informacija yra perduodama tinklais – ji sudedama į IP paketus. Kadangi IP nėra saugus protokolas, todėl galima:

- suklastoti IP adresą,
- modifikuoti IP paketo turinį,
- paketo perdavimo metu peržiūrėti jo turinį.

IP paketo turinys apsaugomas jį šifruojant. IPsec yra IETF (Internet Engineering Task Force) standartas, kuris užtikrina IP paketų saugą. Į IP lygio apsaugą įeina:

- Prieinamumo (pasiekiamumo) kontrolė.
- Paketo konfidencialumas. Kadangi paketai yra šifruojami, tai tik autorizuoti asmenys gali juos perskaityti.
- Paketo vientisumas. Paketai apsaugomi taip, kad bet koks paketo pakeitimas būtų pastebėtas.
- Paketo šaltinio autentiškumas. Paketai apsaugomi taip, kad siuntėjais iš tikrųjų gali būti tie, kurių IP adresai yra nurodyti IP antraštėje.
- Pakartojimo apsauga – paketai yra apsaugomi nuo perėmimo ir vėlesnio persiuntimo.

IPsec – protokolų ir priemonių visuma, skirta IP paketo turinio konfidencialumui, vientisumui ir autentiškumui užtikrinti. IPsec plačiai įdiegta visose moderniose operacinėse sistemose. IPsec naudingas sudarant virtualiuosius privačiuosius tinklus VPN [15, 17].

IPsec – ne vienas protokolas, o jų grupė. IPsec naudoja du srauto saugą užtikrinančius protokolus: AH – IP autentifikacinės antraštės protokolą, ESP – saugaus IP paketo apkrovos įpakavimo protokolą. Įprastai konfidencialumui užtikrinti pasirenkamas ESP, o duomenų vientisumui – AH arba ESP protokolai [15, 16].

1.3.3. Išvados

Siekiant užtikrinti informacinės sistemos sudarytos iš klientinės dalies ir serverinės dalies saugią duomenų kaitą tarp klientinės ir serverinės dalies reikalinga naudotis SSL/TLS protokolais funkcionuojančiais ir saugą garantuojančiais žemesniuose OSI lygmenyse arba IPsec tarnyba veikiančia TCP/IP protokolų steko tinklo lygmenyje. SSL/TLS protokolas veikia TCP/IP modelio taikymo lygmenyje. Dėl šios priežasties SSL/TLS gali būti realizuotas beveik visose operacinėse sistemose.

1.4. Duomenų bazių saugos metodų apžvalga

Duomenų bazė – organizuotas (susistemintas, metodiškai sutvarkytas) duomenų rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu. Termino vartojimo prasmės ribas geriausiai apibrėžia Europos Parlamento priimta direktyva [18].

Taigi duomenų bazės sauga yra būtina rūpintis, ir ypač juridiniams asmenims, nes duomenų bazės saugomuose duomenyse galima rasti darbuotojų asmens duomenis, finansinę ir kitokią svarbią vertę įmonės ar įstaigos veiklai turinčią informaciją.

1.4.1. Fiziniai saugos metodai

Reikalinga tinkamai rūpintis infrastruktūros įranga, jai priklauso serveriai, tinklinė aparatūra, kabelinės sistemos, maitinimas, pagalbinės sistemos. Ši įranga gali sulaukti fizinio pavojaus ir dėl to tapti dalinai ar net visiškai nefunkcionali. Tokio pobūdžio rizikoms šalinti dažniausiai naudojami klasikiniai metodai:

- Leidimų sistemai ir personalo praėjimo kontrolei reikia turėti taisykles, kurios apibrėžia lankytojų elgesį, nustato tvarką kaip lankytojai identifikuojami ir registruojami.
- Videostebėjimas.
- Apsauginis perimetras.
- Įmonės ar įstaigos saugos tarnyba.

Dažniausiai pakanka šių fizinės apsaugos metodų, siekiant išvengti duomenų praradimo dėl fizinės grėsmės.

1.4.2. Programiniai saugos metodai

Jei nuo fizinės grėsmės apsisaugoti yra ganėtinai nesudėtinga, tai saugotis nuo programinės grėsmės yra kur kas sudėtingiau. Egzistuoja kelios programinės grėsmės. Jas gali sukelti piktavališkai nusiteikę žmonės, kurių motyvai gali būti patys įvairiausi: nuo taip vadinamų programišių iki darbdavio „nuskriausto“ darbuotojo. Tai pat pasitaiko atvejų, kai įmonės darbuotojas, turintis vartotojo teises su dideliais įgaliojimais, tam tikromis aplinkybėmis atlieka neteisingus ar net kenkėjiškus veiksmus, tai gali sąlygoti įvairūs faktoriai tokie, kaip kvalifikacijos stoka, neatidumas kylantis iš nuovargio. Ir viena svarbiausių grėsmių yra virusai, „kirminai“ ir „trojos arkliai“. Visos šios grėsmės sudaro didelį pavojų duomenų bazių saugumui, todėl yra būtina imtis saugos metodų [19, 20, 21], kurie pašalina ar sumažina šių grėsmių keliamą riziką.

- Praėjimo kontrolė – saugos metodas, leidžiantis nustatyti vartotojų identifikavimo ir autentifikavimo tvarką, kuri apibrėžia kokias teises gaus vartotojas dirbantis su duomenų baze.
- Auditas – saugos metodas, skirtas fiksuoti visas duomenų bazės operacijas. Tai apima visus įvykius (sukūrimas, pakeitimas, pašalinimas), kurie įvyko duomenų bazėje ir galėjo paveikti ar įtakoti duomenų bazės veikimą. Minimaliai reikėtų tikrinti ar operacijos duomenų bazėje atliekamos sėkmingai ir teisingai, bet visada yra rekomenduojamas atlikti detalesnis auditas, kuris galėtų atsakyti ar nėra kenkėjiškos veiklos, skirtos pakenkti duomenų bazėje saugomiems duomenims.
- Autentifikavimas – saugos metodas [22] skirtas patikrinti ar vartotojo ID yra tikras. Dažniausiai naudojamas autentifikavimo būdas kompiuterinėse sistemose yra vartotojo vardo ir slaptažodžio įvedimas ir po to sulyginimas su sistemoje esančiais duomenimis.
- Duomenų šifravimas – atviro teksto (duomenys, kurių neįtakojo kriptografijos sistemos) pavertimas šifruotu tekstu (duomenys, įtakoti kriptografijos sistemos) naudojant šifravimo algoritmą ar raktą.
- Vientisumo kontrolė – metodas [9] leidžiantis nustatyti ar duomenys yra korektiški (nekintami ir pasiekiami), tai pat suteikiantis galimybę kontroliuoti ar modifikavimas buvo atliktas teisėtai, tai yra atliktas vartotojo turinčio tam teisę.

Dažniausiai pakanka šių teorinių programinės saugos metodų, siekiant išvengti duomenų praradimo dėl programinės grėsmės.

1.4.3. MySQL serverio saugos metodai

UAB „Teledema“ naudoja MySQL duomenų bazių valdymo sistemą, todėl išanalizavau, kaip MySQL serverio kūrėjai pateikė vienuolika saugos žingsnių [23] skirtų apsaugoti serveryje esančius duomenis.

- MySQL serverį įdieginėti tik į Windows NT šeimos sistemas, rekomenduojama naudoti naujausią sistemą.
- MySQL serverį įdieginėti tik į NTFS failų sistemą.
- Geriausia MySQL serveriui skirti atskirą kompiuterį, tada būtų galima išjungti visus nereikalingus operacinės sistemos servisus, tai ne tik padidina serverio saugumą, bet ir suteikia daugiau resursų serverio veiklai. Prisijungti prie serverio turėtų būti leidžiama tik admnistratoriui.
- Rekomenduojama naudoti tik vėliausią MySQL serverio versiją, kad išvengti galimų saugumo spragų.
- Yra būtina apsaugoti visas MySQL serverio naudojamas vartotojų sąskaitas. Rekomenduojama „root“ sąskaitai naudoti tik „stiprų“ slaptažodį, išjungti galimybę prisijungti anonimiškiems vartotojams.
- Siekiant išvengti galimų neleistinų prisijungimų rekomenduojama išjungti galimybę naudotis TCP/IP prieigą.
- Kai nėra galimybės, išjungti TCP/IP prieigą siūloma susieti su „localhost“, tada serveris atsakys į užklausas tik iš „localhost“.
- Yra būtina naudoti ugniasienės programinę įrangą užkardai sukurti. Užkarda turi leisti jungti tik vietinio tinklo IP adresams ir tik patikimiems IP adresų ruožams, jei jie yra ne iš vietinio tinklo.
- Rekomenduojama kurti apribotų teisių vartotojus, jiems suteikiant tik tas teises, kurių jiems tikrai reikia atlikti kasdienines darbo užduotis.
- **Siekiant ypatingos saugos arba saugant ypatingai svarbius duomenis rekomenduojama naudoti duomenų šifravimą.**
- Siūloma nenaudoti standartinio administratoriaus vardo „root“ ir jį pakeisti kitu.

MySQL serverio kūrėjai, siekdami užtikrinti duomenų saugomų serveryje saugumą, sukūrė [24] galimybę šifruoti ir iššifruoti duomenis naudojant AES ir 3DES algoritmus, tai pat yra palaikomas SSL protokolas, kad būtų užtikrintas saugus duomenų apsikeitimas, jei yra naudojamas ne vietinis tinklas.

1.4.4. Išvados

Siekiant užtikrinti duomenų bazių valdymo sistemos serverio apsaugą išskiriami fiziniai ir programiniai apsaugos metodai. Vienas iš svarbiausių fizinės apsaugos metodų yra leidimų sistema ir personalo praėjimo kontrolė turinti taisykles, kurios apibrėžia lankytojų elgesį ir nustato tvarką kaip lankytojai identifikuojami ir registruojami. Programiniai duomenų bazių valdymo sistemos serverio apsaugai reikia taikyti:

- Praėjimo kontrolę;
- Auditą
- Autentifikavimą;
- Duomenų šifravimą;
- Vientisumo kontrolę.

Taikant šiuos saugos metodus galima užtikrinti duomenų bazių valdymo sistemos serverio apsaugą, tai pat reikalinga atsižvelgti į MySQL serverio kūrėjų pasiūlymus kaip apsaugoti duomenis. MySQL serverio kūrėjai rekomenduoja siekiant ypatingos saugos arba saugant ypatingai svarbius duomenis naudoti duomenų šifravimą. Kadangi personalo valdymo informacinė valdymo sistema saugo ypatingai svarbius duomenis, reikalinga duomenis saugoti šifruotu pavidalu, tai leistų užtikrinti duomenų konfidencialumą ir vientisumo kontrolę įsilaužimo į duomenų bazių valdymo sistemos serverį atveju. Tyrimas parodantis, ar duomenims šifruoti turi būti naudojamos standartinės duomenų bazių valdymo sistemos priemonės, atsižvelgiant į duomenų šifravimo greitį ir saugumo lygį, yra vienas iš šio darbo uždavinių.

1.5. Duomenų šifravimo algoritmų apžvalga

Duomenų šifravimo algoritmai skirstomi į simetrinio rakto ir asimetrinio rakto algoritmus [25]. Kriptografinėje sistemoje, naudojančioje simetrinę kriptografiją, šifravimui bei iššifravimui naudojamas tas pats raktas. Kriptografinėje sistemoje, naudojančioje asimetrinę kriptografiją, šifravimui ir iššifravimui naudojami du skirtingi raktai, jie yra matematiškai susieti.

Simetrinio rakto algoritmai skirstomi į srauto ir blokinius [26].

- Srauto algoritmai duomenis šifruoja po bitą. Labiausiai žinomi RC4 ir RC5.
- Blokiniai algoritmai duomenis šifruoja blokais. Labiausiai žinomi DES, 3DES, AES, Blowfish. Šiuos algoritmus plačiau apžvelgsime.

1.5.1. DES ir 3DES algoritmo apžvalga

DES (Data Encryption Standart – duomenų šifravimo standartas) – blokinis simetrinio rakto algoritmas, kurio blokų rakto ilgis 64 bitai, rakto ilgis 56 bitai. DES tapo duomenų šifravimo standartu 1977 m. [27].

Tačiau DES algoritmas yra pakankami nesaugus, dėl mažo rakto dydžio, tačiau jau 1999 m. distributed.net [28] paskelbė, kad jiems pavyko įveikti DES algoritmo raktą per rekordiškai trumpą laiką, todėl buvo pakeistas standartas ir atsirado 3DES (Triple DES) [29].

3DES – blokinis simetrinio rakto algoritmas, kurio blokų rakto ilgis 64 bitai, o rakto ilgis yra 56, 112 arba 168 bitai. 3DES standartas leidžia naudoti tris skirtingus duomenų šifravimo nustatymus, tai:

- Visi trys raktai yra skirtingi, ir tai yra pats stipriausias nustatymas, nes naudojamas 3*56=168 bitų raktas.
- Pirmas ir antras raktai skirtingi, o trečias yra lygus pirmajam raktui, todėl šis nustatymas yra mažiau saugus, nes yra naudojamas 2*56=112 bitų raktas. Tai yra pakankamai saugu, nes toks raktas apsaugo nuo „žmogaus viduryje“ atakos [30]. Tačiau šis variantas yra pasiduodantis „chosen-plaintext“ arba „known-plaintext atakoms“ [31, 32].
- Visi trys raktai yra vienodi, šis nustatymas palaiko suderinamumą su DES standartu, nes pirmas ir antras pasirinkimai nėra suderinami ir DES operacijas tiesiog panaikintų. Tai yra nerekomenduojama NIST [29] ir nėra palaikoma pagal ISO/IEC 18033-3.

1.5.2. AES algoritmo apžvalga

AES (Advanced Encryption Standart – pažangus šifravimo standartas) šifravimo algoritmas 2001 m. JAV vyriausybės buvo pripažintas standartu [33, 34]. Algoritmas dar vadinamas Rinjdael algoritmu, jo autoriai yra J. Daemen ir V.Rijmen. Algoritmo blokų rakto ilgis 128 bitai, o šifravimo raktų ilgis 128, 192, 256 bitai.

AES lyginant su DES algoritmu yra greitesnis ir programiniu, ir techniniu požiūriu [35]. Iki 2009 m. gegužės mėn. buvo pavykusi tik viena ataka „side-chanell attacks“, todėl 2003 m. birželio mėn. JAV vyriausybė paskelbė, kad AES gali būti naudojamas siekiant apsaugoti slaptą informaciją [36], tik buvo nurodyta, kad galima slaptiems dokumentams naudoti 128, 192, 256 bitų raktus, o ypatingai slaptiems dokumentams naudoti tik 192 ar 256 bitų raktus.

1.5.3. RC2 algoritmo apžvalga

RC2 (RC2 – Rivest Cipher) yra blokinis simetrinio rakto algoritmas sukurtas 1987 m. Rono Rivesto, jis tai pat sukūrė RC4, RC5, RC6 algoritmus [37, 38].

RC2 algoritmo plėtojimą rėmė Lotus, nes jiems vykdant JAV NSA agentūros užsakymą buvo siekiama apsaugoti Lotus Notes kuriamą programinę įrangą. 1989 m. RC2 buvo priimtas, kaip standartas.

Nuo sūkurimo RC2 buvo laikomas uždaru algoritmu, kol 1996 m. buvo anonimiškai UseNet tinkle atskleistas, kas leido matyti,kad algoritmas rėmėsi atvirkštinės inžinerijos principu.

RC2 naudojant 128 bitų raktą užtikrina tokį pat saugumo lygį, kaip ir 3DES.

1.5.4. Blowfish algoritmo apžvalga

Blowfish – blokinis simetrinio rakto algoritmas, sukurtas 1993 m. B.Schneier [39] ir naudojamas daugelyje šifravimo produktų. Blowfish blokų rakto ilgis 64 bitai, o šifravimo raktų ilgis gali būti kintamas nuo 32 iki 448 bitų, naudojant 8 bitų žingsnį, standartinis ilgis yra 128 bitai.

B.Schneier šį algoritmą kūrė siekdamas pakeisti pasenusį DES [27] ir dėl esančių įvairių ribojimų (patentai ar komercinės-valstybinės paslaptys) susijusių su kitais žinomais algoritmais (kaip IDEA). Remiantis B.Schneier, galima teigti Blowfish yra nepatentuotas, ir jį galima naudoti visoms valstybėms. Algoritmą kūrėjas pateikė viešai ir algoritmas gali būti laisvai naudojamas [39].

Blowfish yra greitas šifravimo algoritmas, išskyrus atvejus, kai keičiamas raktas. Kiekvienam naujam raktui reikalingas apdorojimas, kuris yra ganėtinai lėtas, tai neleidžia jo naudoti tam tikruose taikomuosiuose procesuose. AES naudojantis 128 bitų raktą yra apie 50% greitesnis už Blowfish juos realizuojant kriptografinėse bibliotekose (kaip OpenSSL) [40]. Tačiau CPU architektūros tobulėjimo dėka Blowfish veikia daug greičiau negu AES naudojantis 128 bitų raktą [41].

Entuziastai rado saugumo spraga algoritme [42]. Galutinai realizuotas algoritmas šios spragos neturi. Buvo ir daugiau tyrusių šį algoritmą, tai Serge Vaudenay [43], kuriam pavyko rasti silpnas algoritmo raktų klases. V.Rijmen [39] pavyko dalinai pertraukti algoritmo ciklus, bet ne iki galo. Todėl B.Schneier vietoj naudojamo Blowfish siūlo naudoti naujesnį Twofish algoritmą [44, 45].

1.5.5. Twofish algoritmo apžvalga

Twofish – blokinis simetrinio rakto algoritmas, [44, 45] sukurtas B.Schneier, J.Kelsey, D.Whiting, D.Wagner, Ch. Hall, N.Ferguson, toliau prie jų prisijungė ir tolimesnę analizę atlikinėjo S.Lucks, T.Kohno ir M.Stay. Pirmą sykį buvo paskelbtas 1998 metais. Algoritmo blokų rakto ilgis 128 bitai, o šifravimo raktų ilgis nuo 128 iki 256 bitų. Twofish algoritmas buvo vienas iš penkių finalininkų renkant AES standartą, [46] tačiau jis buvo nepasirinktas dėl standartizavimo, nes naudojant 128 bitų raktą dauguma programinės įrangos veikė truputį lėčiau, nei pasirinktasis Rinjdael, tačiau naudojant 256 bitų raktą Twofish buvo greitesnis.

Twofish algoritmas, kaip ir Blowfish nebuvo patentuotas ir buvo pristatytas viešai, jis yra visiškai nemokamas, jam naudoti nėra taikomi jokie apribojimai. Jis yra vienas iš nedaugelio įtrauktas į OpenPGP [47] standartą.

Twofish algoritmo kriptologinę analizę atliko S.Moriai ir Y.L.Yin dar 2000 metais ir visi bandymai buvo tik teoriniai ir jokių praktinių veiksmų nebuvo atlikta [48]. B.Schneier savo internetiniame dienoraštyje teigė, kad algoritmo kriptanalizę praktiškai įgyvendinti nėra įmanoma [49].

1.5.6. Išvados

Išsiaiškinome, kad duomenų šifravimo algoritmai skirstomi į simetrinio rakto ir asimetrinio rakto algoritmus [25]. Simetrinio rakto galima suskirstyti į srautinius ir blokinius. Plačiau buvo apžvelgti žinomiausiai simetrinio rakto blokiniai algoritmai: DES, 3DES, AES, RC2, Blowfish, Twofish. 1 lentelėje pateiktas palyginimas algoritmų rakto dydžiu ir žinomomis saugos problemomis.

1 lentelė. Duomenų šifravimo algoritmų palyginimas

	DES	3DES	AES	RC2	Blowfish	Twofish
Rakto ilgis (bitais)	56	56-168	128-256	kintamas	32-448	128-256
Patikimumas	pasenęs	pakankamas	patikimas	pakankamas	pasenęs	patikimas

Apžvelgti šifravimo algoritmai gali būti naudojami duomenims šifruoti personalo valdymo informacinėje sistemoje, nenaudojant duomenų bazių valdymo sistemos standartinių šifravimo funkcijų. Tuo tikslu turi būti sukurtas atskiras duomenų šifravimo modulis. Modulio darbo rezultatų tyrimas, įvertinant duomenų šifravimo greitį ir saugumo lygį, yra vienas iš šio darbo uždavinių ir jo rezultatai pateikiami kituose skyriuose.

1.6. Personalo valdymo informacinių sistemų saugos sprendimų analizė

Personalo valdymo informacinė sistemos pagrindinė paskirtis yra asmens duomenų tvarkymas – duomenų rinkimas, kaupimas, apdorojimas ir saugojimas. Dėl personalo valdymo informacinės sistemos tiesioginės paskirties, tokios sistemos susiduria su įvairiomis saugumo problemomis, pagrindinė saugos problema kaip apsaugoti asmens duomenis, kuriuos saugo sistema. Personalo valdymo informacines sistemas ar verslo valdymo informacines sistemas, kurių sudėtinė dalis yra personalo valdymo informacinės sistemos modulis, kuria daug įvairių programinės įrangos gamintojų nuo Microsoft Dynamics [50] iki atvirojo kodo OrangeHRM [51] iš užsienio kompanijų, tarp lietuviškųjų gamintojų išsiskiria UAB „Proringas“ [52] gaminantis verslo valdymo sistemą „Pragma“ ir UAB „Kibernetinė erdvė“ [53] kurianti verslo valdymo sistemą „Tėja“.

1.6.1. Programinės įrangos gamintojų sukurtų personalo valdymo informacinių sistemų saugos sprendimų analizė

Microsoft atnaujintoje verslo valdymo sistemoje „Microsoft Dynamics AX“ (anksčiau Microsoft Axapta) [54] pasirūpino padidintu saugumu:

- „Windows“ autentifikavimas ir „Active Directory“ vieno prisijungimo funkcija leidžia padidinti saugumą ir privatumą bei siūlo administratoriui geresnį slaptų duomenų valdymą. Vieno prisijungimo funkcija taip pat gali padidinti našumą ir patogumą, nes vartotojams reikia tik vieną kartą prisijungti („Microsoft Windows“ registracijoje), norint pasiekti „Microsoft Dynamics AX“.
- Patobulinimai visose „Microsoft Dynamics AX“ programose bei patobulinimai duomenų bazių technologijoje, naudojamoje „Microsoft SQL Server 2005“, pvz., vidinių duomenų šifravimas, saugūs numatytieji nustatymai ir slaptažodžių strategijos priežiūra, sudaro sistemą, kurią galima pasitikėti.

OrangeHRM [51] pasaulyje pirmaujanti atvirojo kodo žmogiškųjų išteklių valdymo sistemos kūrėja sistemos administratoriui suteikė galimybę OrangeHRM sistemos administraciniame modulyje [55] nustatyti saugumo parametrus. Sistemos administratorius gali suskirstyti vartotojus pagal grupes, kiekvienai grupei suteikti tik tas teises kurių reikia atlikti kasdieninėms darbo užduotims. OrangeHRM sistema vidinių duomenų nešifruoja, norint užtikrinti saugų duomenų apsikeitimą tarp klientinės dalies ir serverinės dalies, gamintojas rekomenduoja naudoti SSL protokolą, jei duomenų apsikeitimas vyksta už vietinio tinklo ribų.

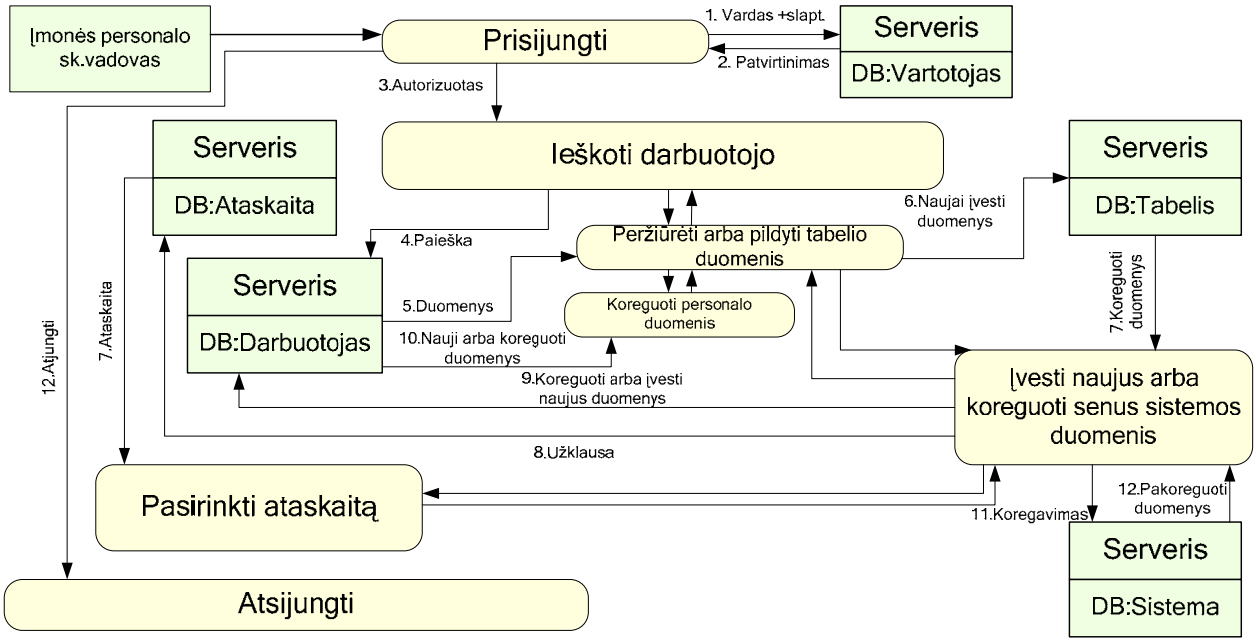
Lietuviškos programinės įrangos gamintojas UAB „Proringas“, kuriantis verslo valdymo informacinę sistemą „Pragma“, jos saugumui užtikrinti naudoja [56] Sentinel apsaugos raktus,

kurie yra skirti apsaugoti programinę įrangą nuo nelegalaus kopijavimo. Sentinel raktų veikimas paremtas principu: apsaugota programa kreipiasi į raktą, siųsdama jam paklausimą, į kurį rakte esantis mikroprocesorius generuoja atsakymą. Iš gauto atsakymo programa sprendžia ar ji yra naudojama legaliai, ar ne. Programa Pragma v4.0 yra apsaugota SentinelSuperProNet apsaugos raktais, kurie skirti kontroliuoti vartotojų, vienu metu dirbančių su apsaugota programa tinkle, skaičių. Prie kompiuterio raktai jungiami USB jungtimi.

UAB „Kibernetinė erdvė“ gaminanti verslo valdymo sistemą „Tėja“ duomenų saugumui [57] užtikrinti prieš persiunčiant duomenis tarp nutolusių kompiuterių, juos supakuoja. Toks siuntimo būdas padidina duomenų saugumą, tačiau padidina ir procesoriaus resursų panaudojimą. Taip pat verslo valdymo sistemos „Tėja“ gamintojas duomenų bazės administravimo lange pateikė įrankį, kuris leidžia prižiūrėti duomenų esančių duomenų bazėje korektiškumą ir vientisumą.

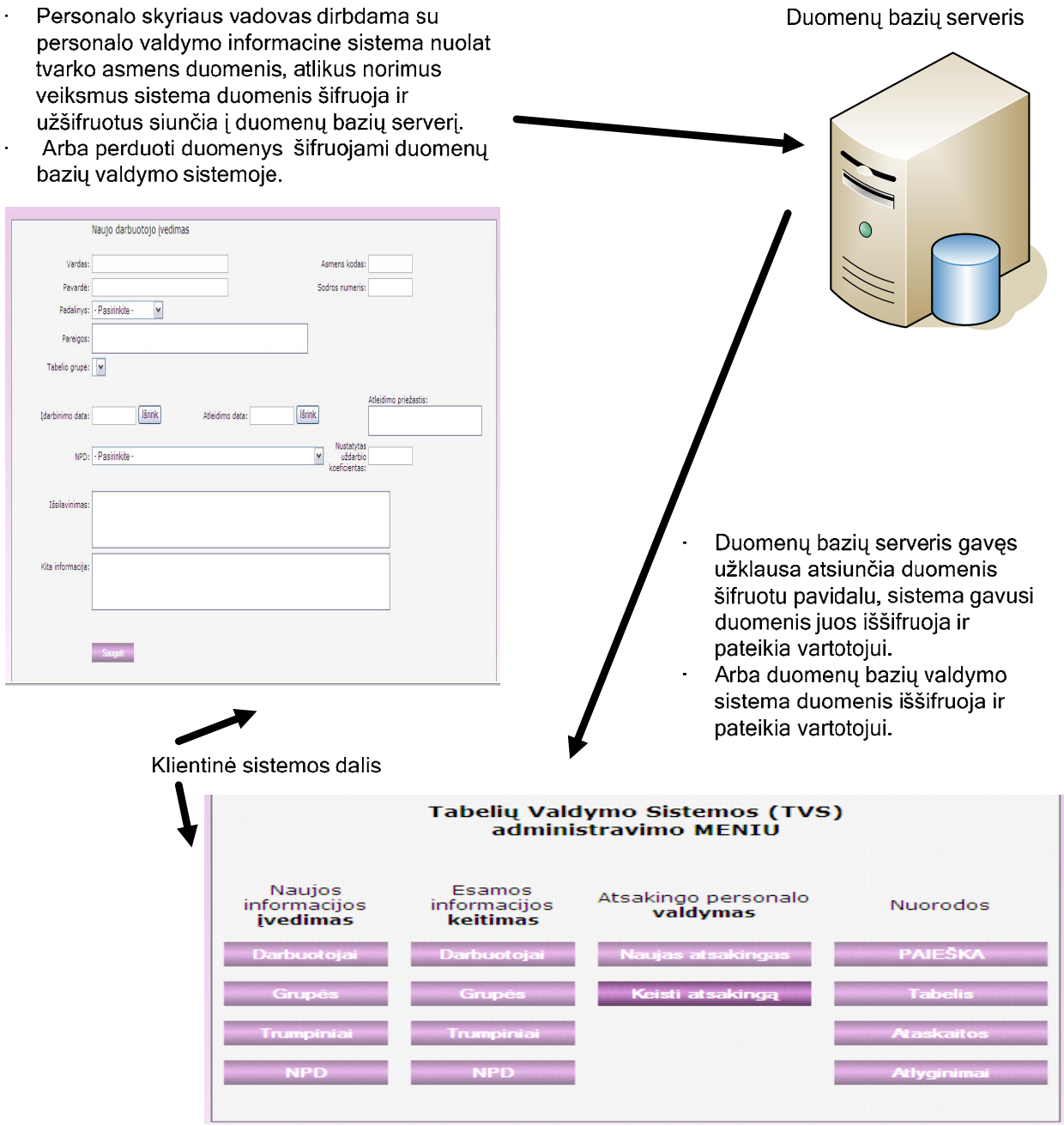
1.6.2. UAB „Teledema“ personalo valdymo informacinės sistemos saugos problemų analizė

UAB „Teledema“ naudoja personalo valdymo informacinę sistemą. Sistemą savo kasdieninėms darbo užduotims atlikti naudoja įmonės vadovas, įmonės skyriaus vadovai ir įmonės personalo vadovas. Visi dirbantys su sistema įveda duomenis arba pateikia užklausą gauna duomenis iš duomenų bazės. Diagramoje (2 pav.) vaizduojamas daugiausiai atvejų apimantis personalo skyriaus vadovo darbas su sistema, tai galimybė atlikti paiešką sistemoje ieškant darbuotojo duomenų, gavus duomenis juos tvarkyti, tai pat įvesti naujus arba koreguoti senus sistemos duomenis.



2 pav. Įmonės personalo vadovo darbo su sistema kontekstinė diagrama

Taigi, kaip matome iš diagramos (2 pav.), dirbant su sistema nuolat vyksta duomenų kaita - įvedami, koreguojami duomenys, o visi sistemoje esantys duomenys atitinka asmens duomenų apibrėžimą pagal LR Asmens duomenų teisinės apsaugos įstatymą [3], todėl tokius duomenis privalu apsaugoti, nes duomenų valdytoją įpareigoja LR Asmens duomenų teisinės apsaugos įstatymo 5 str. 1 dalis, kuri teigia, kad "Asmens duomenys yra kaupiami ir saugomi duomenų įrašuose, už kurių apsaugą ir tvarkymą yra atsakingas duomenų valdytojas".



3 pav. Personalo valdymo informacinės sistemos duomenų apsikeitimo paveikslas įdiegus duomenų šifravimo modulį

Todėl sieksime nustatyti, ar yra tikslinga įvedamus duomenis šifruoti ir į duomenų bazę perduoti užšifruotus, ar duomenis perduoti į duomenų bazę ir duomenų bazių valdymo sistemoje

juos šifruoti. Visus duomenis, esančius duomenų bazėje, reikalinga saugoti šifruotame pavidale, esant asmens duomenims šifruotiems bus užkirsta galimybė piktavaliams įmonės darbuotojams juos sužinoti ir atskleisti trečiajai šaliai.

Paveiksle (3 pav.) vaizduojamas personalo skyriaus vadovo darbas naudojantis personalo valdymo informacinę sistemą. Personalo skyriaus vadovui atlikus norimus veiksmus sistema duomenis šifruoja ir užšifruotus siunčia į duomenų bazių valdymo serverį, tai pat atlikus užklausą duomenų bazių valdymo sistemos serveris atsiunčia duomenis šifruotu pavidalu, sistema duomenis iššifruoja ir pateikia vartotojui.

1.7. Išvados

Išanalizavus Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymą [3] išsiaiškinome, kaip įstatymas apibrėžia asmens duomenų sąvoką, ir kas yra laikomi asmens duomenų valdytojais ir kokios jų pareigos. Personalo valdymo informacinės sistemos tvarkomi ir valdomi duomenys yra asmens duomenys, kurių saugumas turi būti užtikrintas. Tiriamoje personalo valdymo sistemoje duomenų saugumui užtikrinti naudojamos minimalios priemonės: saugus interneto ryšys ir vartotojo identifikacija, duomenų šifravimo priemonės nėra naudojamos, šio darbo tikslas buvo sukurti programinį modulį duomenims šifruoti ir ištirti jo įtaką eksploatuojamos sistemos darbui.

Duomenims apsaugoti duomenų bazių valdymo sistemose gali būti naudojami tiek fizinės, tiek programinės saugos priemonės. Fizinių saugos priemonių naudojimas, įtakai į eksploatuojamos sistemos darbą neturi, šių priemonių naudojimas yra įmonės organizacinis klausimas. Programinių priemonių – duomenų bazės valdymo sistemos standartinių šifravimo funkcijų naudojimas gali įtakoti sistemos darbą, jų naudojimas turi būti ištirtas. Tačiau tokių priemonių naudojimas, nepilnai užtikrina duomenų saugumą (konfidencialumą ir vientisumą) įsilaužimo į duomenų bazės valdymo sistemos serverį atveju.

Apžvelgti duomenų šifravimo algoritmai gali būti naudojami kaip papildomos duomenų saugos priemonės. Personalo valdymo informacinės sistemos duomenims šifruoti naudojami šifravimo algoritmai apsaugotų duomenis konfidencialumo ir vientisumo atžvilgiu juos saugant duomenų bazių valdymo sistemoje.

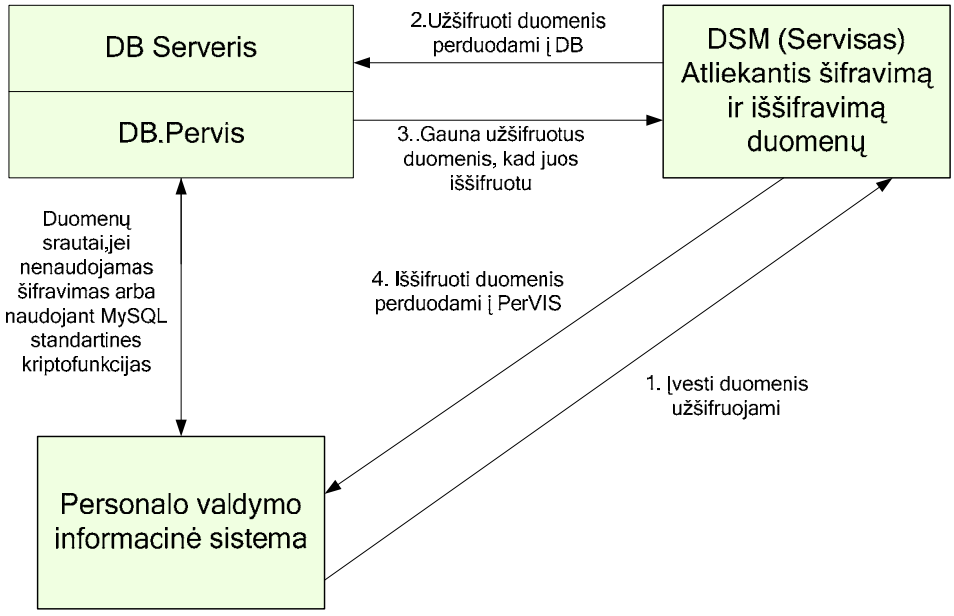
Kadangi duomenis gali būti šifruojami tiek programoje, tiek duomenų bazių valdymo sistemoje, tikslinga kurti programinį sistemos modulį – servisą, kurio paskirtis įvestus į sistemą duomenis užšifruoti ir užšifruotus persiųsti į duomenų bazių valdymo sistemą, arba gautus užšifruotus duomenis iš duomenų bazių valdymo sistemos, duomenis iššifruoti ir pateikti vartotojui, vartotojo pageidauta forma arba nurodyti, kad šifravimui ir iššifravimui turi būti naudojamos standartinės duomenų bazių valdymo sistemos funkcijos.

Tyrimo būtinybę nusako Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas, įmonei reikalinga saugi ir patikima personalo valdymo informacinė sistema, kuri leistų kaupti išsamius, tikslius duomenis realiu laiku, juos sistemintų ir pateiktų sistemos vartotojams, kuriems yra suteiktos teisės susipažinti, valdyti ir tvarkyti tokią informaciją, taip pat užtikrintų, kad saugomi asmens duomenys yra laikomi šifruotu pavidalu, kas leistų užtikrinti, kad duomenis galės peržiūrėti, valdyti ir tvarkyti tik tie asmenys, kuriems leidimą yra davęs duomenų valdytojas.

II. Personalo valdymo informacinės sistemos duomenų šifravimo modulio specifikacija

2.1. Programinio sistemos modulio paskirtis

DSM – tai programinis sistemos modulis (servisas) leidžiantis atlikti duomenų šifravimą ir iššifravimą ir integruojamas į eksploatuojamą sistemą. DSM leis vartotojui, turinčiam teises, nustatyti norimą šifravimo algoritmą. Duomenų šifravimo modulis, naudodamas vartotojo nustatytą šifravimo algoritmą, atlieka duomenų šifravimą ir iššifravimą eksploatuojamoje sistemoje. Vartotojui įvedus naujus duomenis į sistemą ir norint juos įrašyti į duomenų bazių valdymo sistemą, DSM šiuos duomenis užšifruos ir perduos duomenų bazių valdymo sistemai. Vartotojui atlikus užklausą duomenų bazių valdymo sistemoje, DSM reikalingus duomenis iššifruos ir perduos į eksploatuojamą sistemą vartotojo pageidauta forma, arba bus galima duomenis šifruoti ir iššifruoti naudojantis standartinėmis MySQL duomenų bazių valdymo sistemos funkcijomis (4 pav.). Atlikdami tyrimą nustatysime ir parinksime, jau eksploatuojamai personalo valdymo informacinei sistemai optimaliausią (parenkant atsižvelgsime, kad sistema turi ne tik saugiai veikti, bet dėl to neturi sutrikti sistemos darbas) duomenų šifravimo algoritmą.



4 pav. DSM veikimo schema

2.2. Programinio sistemos modulio funkcijos

- **Saugumo lygio nustatymas:** Galimybė pasirinkti norimą duomenų šifravimo algoritmą (simetrinis-blokinis arba simetrinis-srautinis). Skirtingi algoritmai naudoja skirtingo bitų dydžio raktus, nuo ko priklauso saugumo lygis ir sistemos darbo greitis.
- **Duomenų šifravimas atliekamas eksploatuojamoje sistemoje:** Įvedus duomenis arba pakoregavus, jau esamus duomenis ir nurodžius, kad sistema duomenis siųstų į duomenų bazių valdymo sistemos serverį, duomenys yra šifruojami nustatytu duomenų šifravimo algoritmu, ir išsiunčiami, jau užšifruotu pavidalu.
- **Duomenų iššifravimas atliekamas eksploatuojamoje sistemoje:** Įvedus užklausą gauti ataskaitą ar kitą informaciją, duomenų bazių valdymo sistemos serveris atsiunčia duomenis šifruotu pavidalu. Gavus duomenis eksploatuojama sistema, naudodama pasirinktą duomenų šifravimo algoritmą, duomenis iššifruoja ir pateikia vartotojui ataskaitą ar kitą norimą gauti informaciją.
- **Duomenų šifravimas atliekamas duomenų bazių valdymo sistemoje:** Įvedus duomenis arba pakoregavus, jau esamus duomenis ir nurodžius, kad sistema duomenis siųstų į duomenų bazių valdymo sistemos serverį, nešifruotu pavidalu duomenys yra siunčiami į duomenų bazių valdymo sistemos serverį, ir gavus duomenis duomenų bazių valdymo sistemos serveris užšifruoja.
- **Duomenų iššifravimas atliekamas duomenų bazių valdymo sistemoje:** Įvedus užklausą gauti ataskaitą ar kitą informaciją, duomenų bazių valdymo sistemos serveris duomenis iššifruoja ir atsiunčia duomenis nešifruotu pavidalu. Gavus duomenis eksploatuojama sistema pateikia vartotojui ataskaitą ar kitą norimą gauti informaciją.

2.3. Programinio sistemos modulio reikalavimai

2.3.1. Funkciniai reikalavimai

- DSM turi šifruoti ir iššifruoti duomenis, taip užtikrinant duomenų saugumą. Duomenų šifravimas – atviro teksto (duomenys, kurių neįtakojo kriptografijos sistemos) pavertimas šifruotu tekstu (duomenys, įtakoti kriptografijos sistemos) naudojant šifravimo algoritmą ar raktą. Duomenų iššifravimas – šifruoto teksto (duomenys, įtakoti kriptografijos sistemos) pavertimas atviru tekstu (duomenys, kurių neįtakojo kriptografijos sistemos) naudojant šifravimo algoritmą ar raktą;

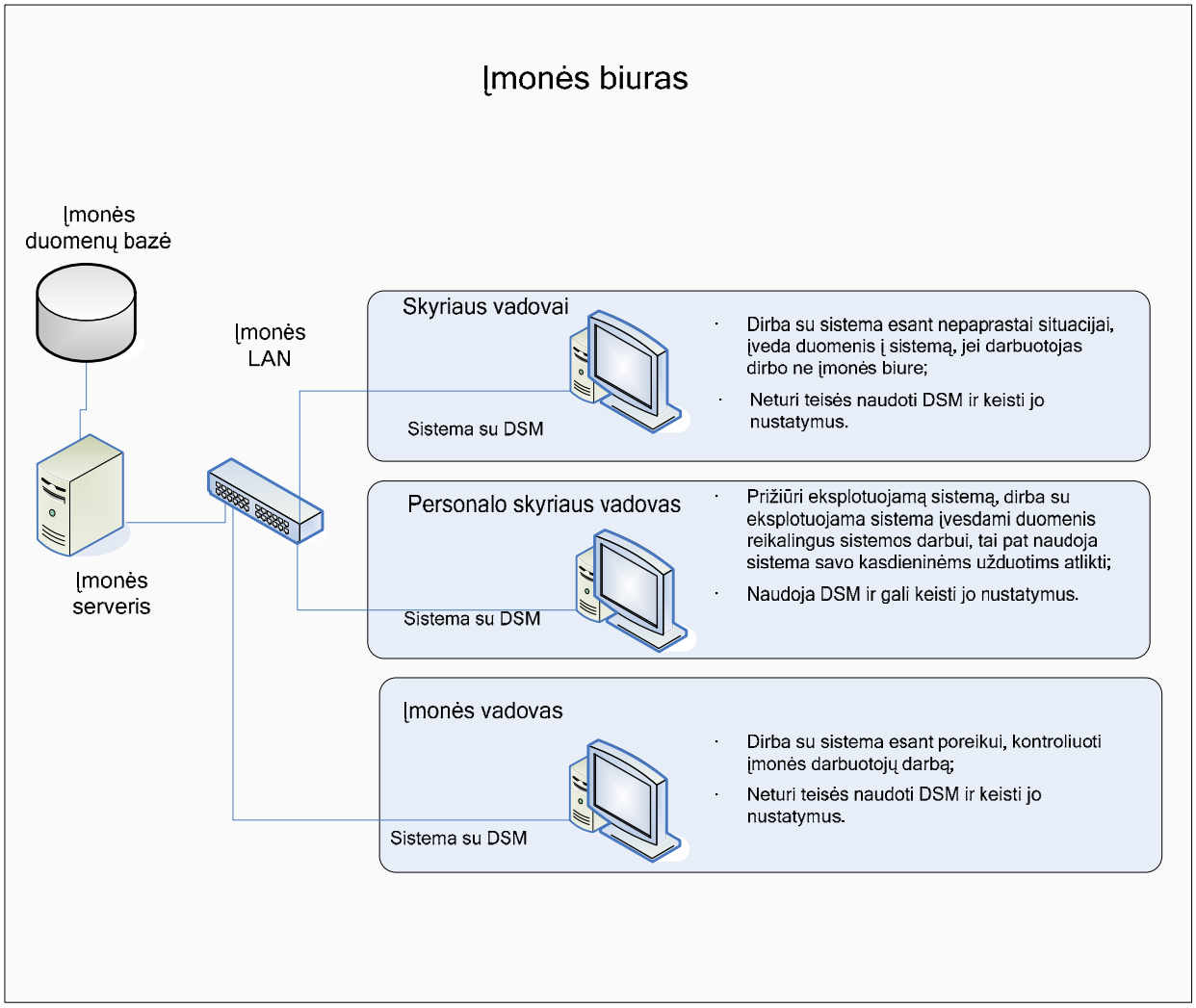
- DSM turi leisti vartotojui turinčiam teises (tai toks vartotojas kuriam sistemos hierarchijoje numatyta prieiga prie programinio sistemos modulio skirto užtikrinti duomenų saugumą) pasirinkti norimą saugumo lygį, tai įgyvendinama pasirenkant pageidaujamą duomenų šifravimo algoritmą iš sistemos pasiūlytų duomenų šifravimo algoritmų, nes duomenų saugumo lygis priklauso nuo algoritmo naudojamo rakto ilgio, ir paties algoritmo patikimumo;
- DSM turi gauti duomenis iš eksploatuojamos sistemos, kad galėtų duomenis užšifruoti naudodama vartotojo pasirinktą duomenų šifravimo algoritmą;
- DSM turi perduoti užšifruotus duomenis į duomenų bazių valdymo sistemos serverį;
- DSM turi gauti užšifruotus duomenis iš duomenų bazių valdymo sistemos serverio, kai vartotojas atlieka užklausą norėdamas gauti informaciją, kad galėtų duomenis iššifruoti naudodamas vartotojo nustatytą duomenų šifravimo algoritmą;
- DSM turi perduoti iššifruotus duomenis eksploatuojamai sistemai;

2.3.2. Nefunkciniai reikalavimai

- DSM turi būti pritaikytas Windows šeimos operacinei sistemai. Optimaliai DSM turi veikti su Windows XP,Vista, 7 operacinės šeimos versijomis;
- DSM turi užtikrinti, kad duomenis būtų korektiškai teisingai užšifruoti arba iššifruoti, kad būtų išvengta duomenų praradimo, dėl šifravimo arba iššifravimo;
- DSM turi dirbti patikimai ir optimaliai, nes dėl sistemos duomenų saugumo neturi sutrikti sistemos patikimas darbas;
- DSM turi užtikrinti, kad jokiems asmenims, kurie neturi tam teisės, eksploatuojama sistema neatskleis jokios informacijos apie įmonės darbuotojus ir kitokios informacijos susijusios su asmens duomenimis;
- DSM turi būti teisingas lietuviškų simbolių apdorojimas, kadangi įvedamuose ar gaunamuose duomenyse gali būti lietuviškų simbolių;
- DSM, kaip ir eksploatuojama sistema gali būti prieinama tik iš įmonės vidaus tinklo, dėl saugumo reikalavimų;
- DSM vartotojo sąsaja turi būti intuityvi, paprasta, aiški;
- DSM saugumo lygio nustatymo laukai turi būti patogiai išdėstyti;
- DSM klaidų pranešimai turi būti informatyvūs ir neapsunkinti technine informacija.

III. Personalo valdymo informacinės sistemos duomenų šifravimo modulio projektas

3.1. Programinio sistemos modulio koncepcija



5 pav. Sistemos koncepcinė schema

Įmonė naudoja personalo valdymo informacinę sistemą (5 pav.). Eksploatuojama sistema nėra apsaugota papildomomis saugos priemonėmis, kadangi sistema saugo asmens duomenis yra būtina įdiegti papildomas saugos priemones siekiant apsaugoti duomenis. Tam tikslui reikia personalo valdymo informacinėje sistema apsaugoti sukuriant duomenų šifravimo modulį, tai programinis sistemos modulis leidžiantis atlikti duomenų šifravimą eksploatuojamoje sistemoje (toliau vadinamas DSM), kurio tikslas užtikrinti duomenų apsaugą naudojant duomenų šifravimą ir iššifravimą. Duomenų šifravimas – atviro teksto (duomenys, kurių neįtakojo kriptografijos sistemos) pavertimas šifruotu tekstu (duomenys, įtakoti kriptografijos sistemos) naudojant šifravimo algoritmą ar raktą. Duomenų iššifravimas – šifruoto teksto (duomenys, įtakoti

kriptografijos sistemos) pavertimas atviru tekstu (duomenys, kurių neįtakojo kriptografijos sistemos) naudojant šifravimo algoritmą ar raktą. Taip pat DSM turi leisti tik vartotojui turinčiam teises (tai toks vartotojas kuriam sistemos hierarchijoje numatyta prieiga prie programinio sistemos modulio skirto užtikrinti duomenų saugumą) nustatyti norimą simetrinį-blokinį šifravimo algoritmą.

DSM veikimo aplinka

Duomenų šifravimo modulis – servisas veikia įmonės vietiniame tinkle, atlieka duomenų šifravimą ir iššifravimą ir yra integruotas į įmonės eksploatuojamą personalo valdymo informacinę sistemą.

DSM veikimo principai

Pagal nusistovėjusias taisykles ar pareigybes, kiekvienas darbuotojas turi savo funkcijas ir atsakomybės ribas, todėl ir priklausomai nuo pareigybės skirtingi vartotojai galės naudotis skirtingomis duomenų šifravimo modulio funkcijomis:

Skyriaus vadovai - turi galimybę prisijungti prie eksploatuojamos sistemos esant neįprastai situacijai, tačiau neturi teisės naudotis DSM ir keisti jo nustatymus ar kitaip įtakoti eksploatuojamos sistemos duomenų saugumą;

Personalo skyriaus vadovas - prižiūri eksploatuojamos sistemos darbą. Dirba su eksploatuojama sistema, įvesdami visus papildomus duomenis reikalingus korektiškam sistemos funkcionavimui. Nustato DSM nustatymus reikalingus užtikrinti asmens duomenų saugumui, kad būtų garantuotas asmens duomenų saugumas ir patikimas sistemos darbas. Naudoja eksploatuojamą sistemą savo darbo užduotimis atlikti;

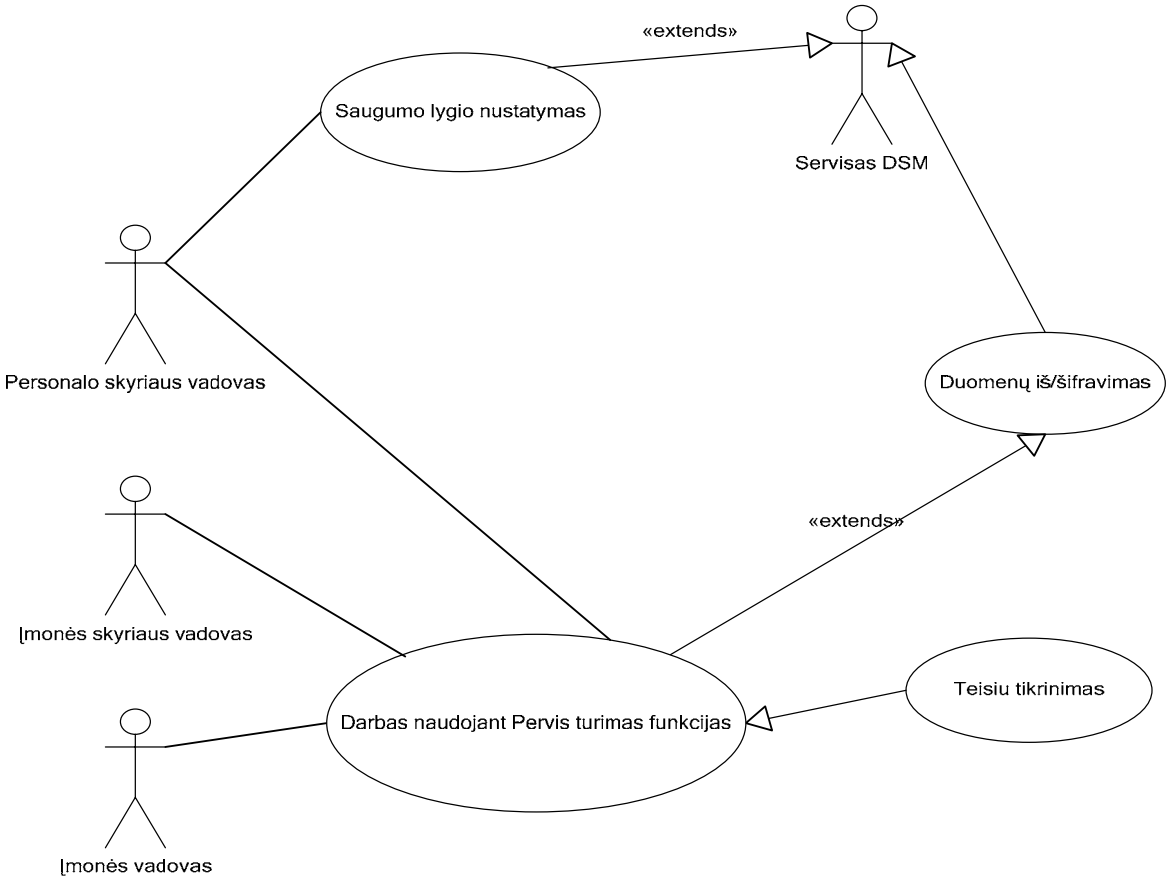
Direktorius - esant reikalui gali naudotis eksploatuojamos sistemos resursais, kad kontroliuotų įmonės darbuotojų darbą, tačiau neturi teisės naudotis DSM ir keisti jo nustatymus ar kitaip įtakoti eksploatuojamos sistemos duomenų saugumą.

3.2. Personalo valdymo informacinės sistemos duomenų šifravimo modulio informacinė posistemė

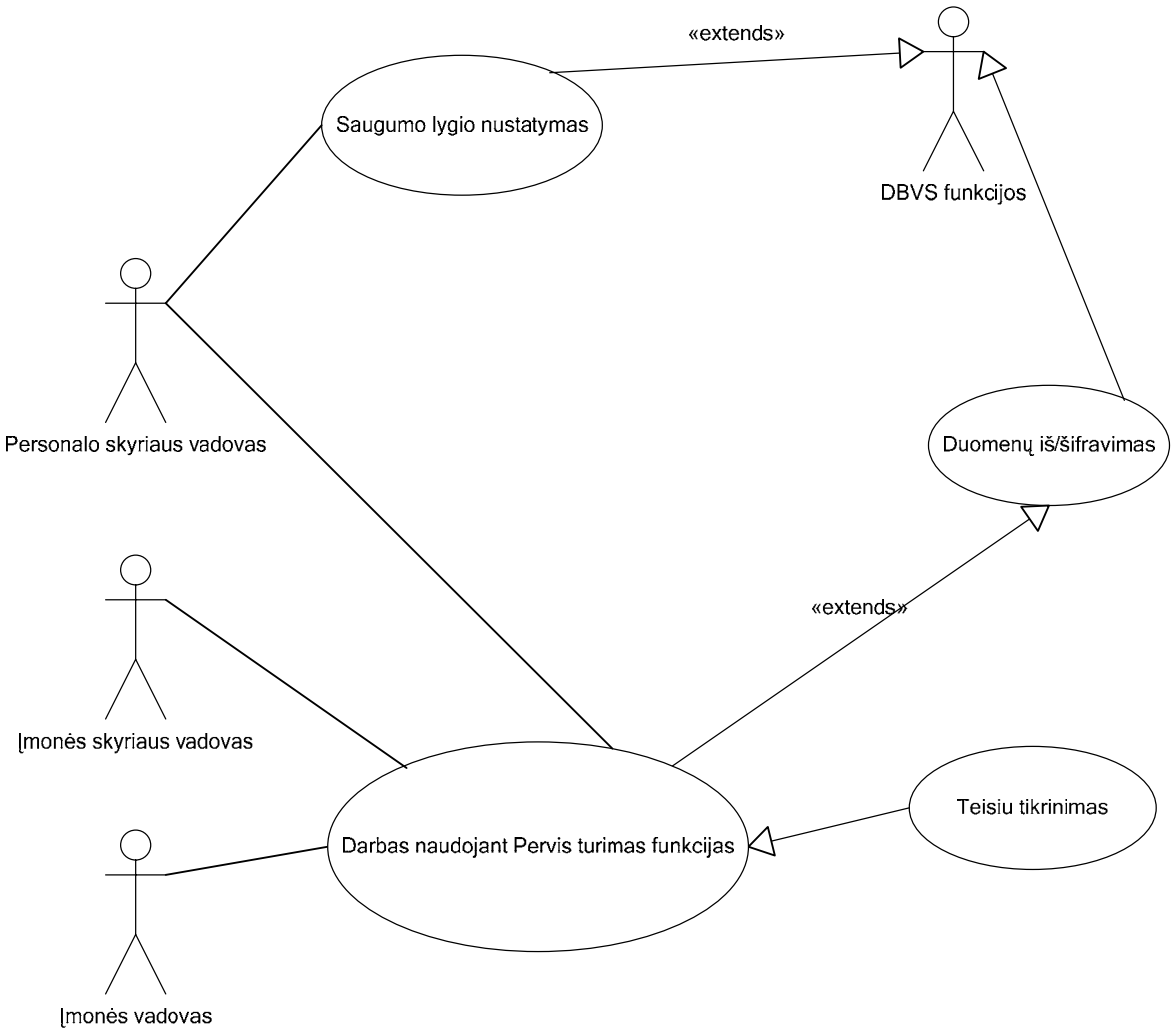
3.2.1. Panaudojimo diagrama

Tyrimui atlikti buvo naudojami du personalo valdymo informacinės sistemos asmens duomenų šifravimo atvejai: 1) naudojant duomenų šifravimo modulį integruotą į personalo valdymo informacinę sistemą (6 pav.) ir 2) naudojant duomenų bazių valdymo sistemos duomenų šifravimo funkcijas (7 pav.). Abejais atvejais saugumo lygio (galimybė nustatyti ar šifruoti, ar nešifruoti duomenis, jei pasirinkta šifruoti duomenis reikės pasirinkti, kaip šifruoti ar naudojantis duomenų bazių valdymo sistemos standartinėmis funkcijos ar naudotis duomenų šifravimo algoritmais) nustatymus galės keisti tik personalo skyriaus vadovas

Panaudojimo atvejų diagramose yra šie aktoriai: Personalo skyriaus vadovas, Įmonės skyriaus vadovas, Įmonės vadovas, Servisas DSM, DBVS funkcijos.



6 pav. Panaudojimo atvejų diagrama, kai duomenys iš/šifruoja DSM



7 pav. Panaudojimo atvejų diagrama, kai duomenys iš/šifruoja standartinės MySQL duomenų bazių valdymo sistemos funkcijos

Įmonės skyriaus vadovas

Prisijungęs prie sistemos galės įvesti ar koreguoti informaciją, susijusią su darbo apskaita (darbuotojas išsiųstas mokytis, komandiruotėje, dirba kitame pastate ar įmonėje), tik apie savo skyriaus darbuotojus. Neturi teisės valdyti, koreguoti DSM nustatymus.

Įmonės vadovas

Prisijungęs prie sistemos galės peržiūrėti apibendrintą informaciją, išdirbtų visų skyrių valandas, jų piniginę išraišką, palyginti su ankstesnių mėnesių duomenimis, spausdinti suvestines ir ataskaitas. Neturi teisės valdyti, koreguoti DSM nustatymus.

Personalo skyriaus vadovas

Prisijungęs prie sistemos galės atlikti bet kurio lygio duomenų pakeitimus, įvesti naujus, formuoti ataskaitas, analizuoti aktualią informaciją. Turi teisę valdyti, koreguoti DSM nustatymus.

Servisas DSM

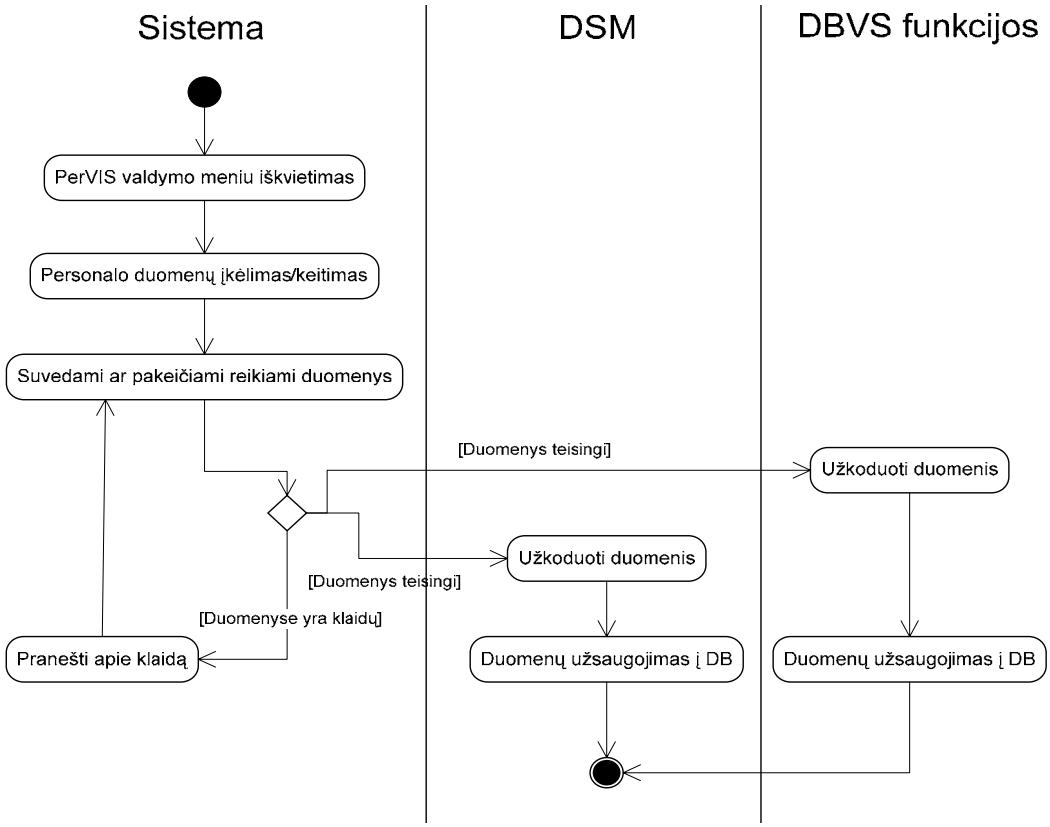
Sistemos servisas atliekantis duomenų šifravimą ir iššifravimą. Serviso nustatymus gali valdyti ir koreguoti, tik vartotojas kuriam skirtos teisės.

DBVS funkcijos

Duomenų bazių valdymo sistemos serverio funkcijos atliekančios duomenų šifravimą ir iššifravimą. Duomenų bazių valdymo sistemos serverio funkcijų nustatymus gali valdyti ir koreguoti, tik vartotojas kuriam skirtos teisės.

3.2.2. Veiklos diagrama

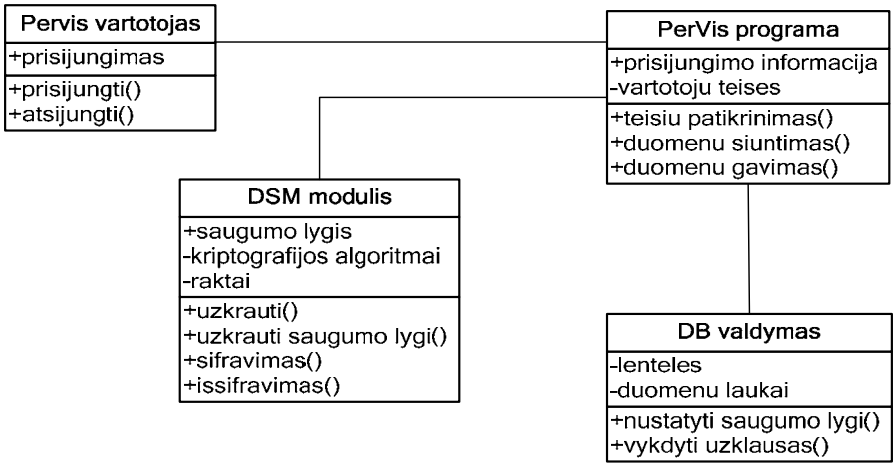
Veiklos diagramoje (8 pav.) atvaizduotas personalo valdymo informacinės sistemos darbo fragmentas, kai yra įvedami ar keičiami personalo duomenys ir parodyta DSM įtaka personalo valdymo informacinės sistemos darbui, ir kaip veikia personalo valdymo informacinė sistema, kai yra naudojamos duomenų bazių valdymo funkcijos.



8 pav. Veiklos diagrama atvaizduojanti DSM įtaka sistemos darbui

3.2.3. Klasių diagrama

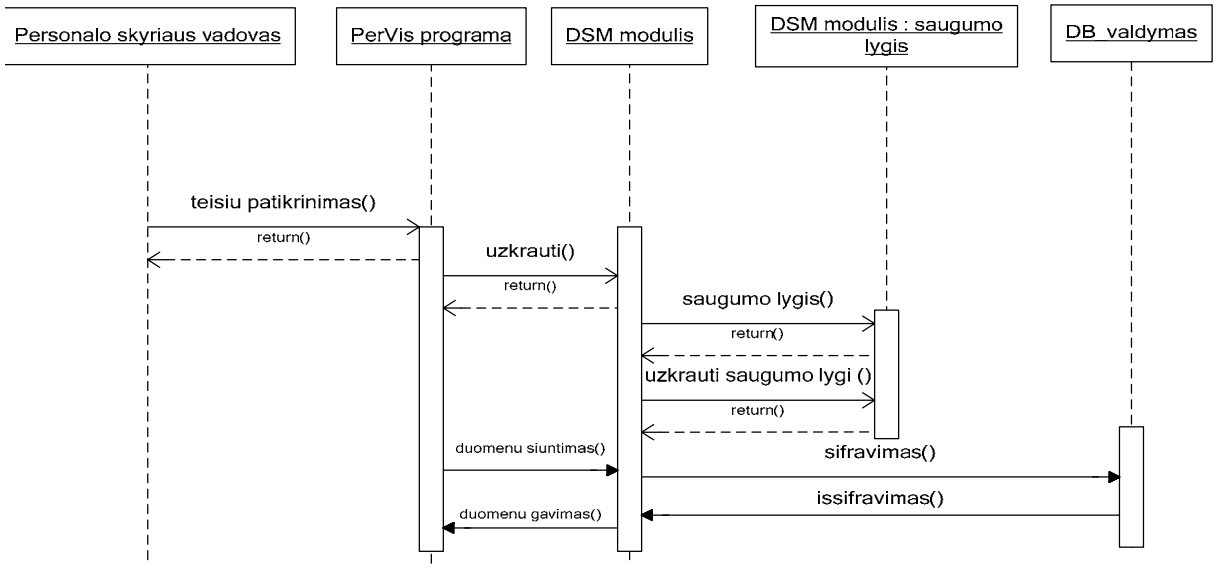
Pervis programa klasė skirta aprašyti eksploatuojamą personalo valdymo informacinę sistemą ir jos sudėtį. Pervis vartotojas klasė skirta galimiems vartotojo veiksmams sistemos atžvilgiu. DSM modulis klasė atspindi DSM modulio galimybes, tai užkrauti saugumo lygį, atlikti šifravimą ir iššifravimą, kiekvienu atveju vyksta kreipimasis į eksploatuojamą sistemą. DB valdymas klasė skirta valdyti duomenų bazei (9 pav.).



9 pav. Klasių diagrama

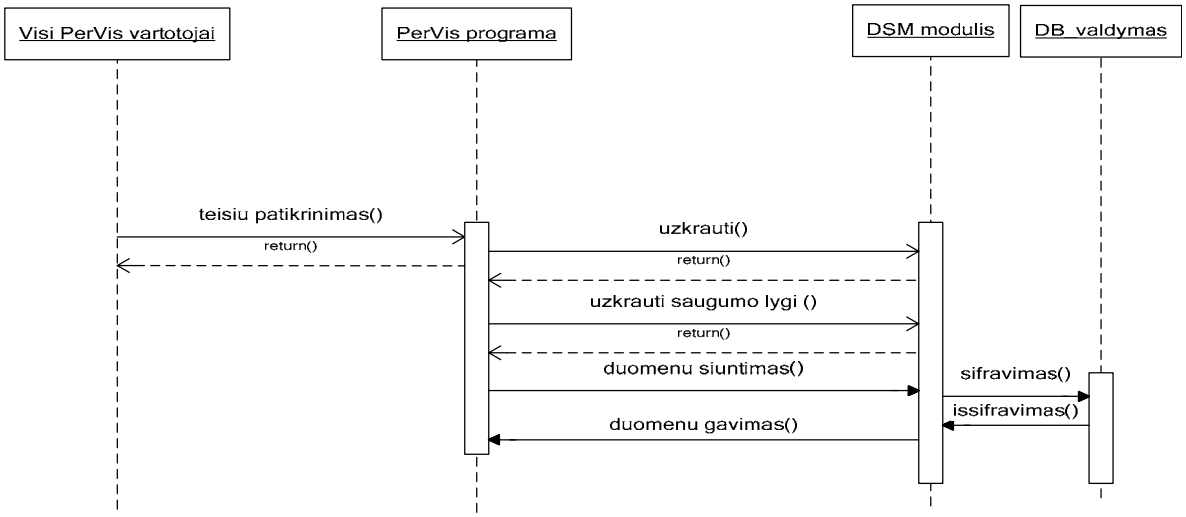
3.2.4. Sekos diagrama

Tobulinant personalo valdymo informacinę sistemą svarbu žinoti kaip sąveikauja tarpusavyje programa, DSM modulis ir duomenų bazių valdymo sistema.



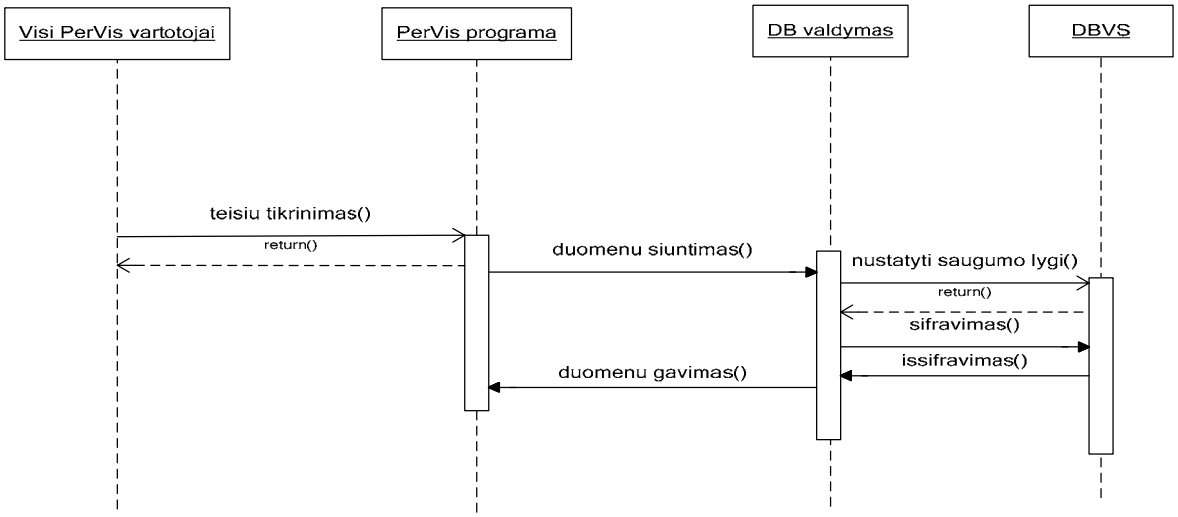
10 pav. Personalo skyriaus vadovas paruošia sistemą darbui sekos diagrama

Personalo valdymo informacinė sistema, prieš pradedant dirbti su ja, patikrina vartotojo teises ir tada startuoja DSM servisas ir leidžia parinkti norimą saugumo lygį. Kai tai atliekama, DSM užkrauna parinktą saugumo lygį ir galima pradėti dirbti su PerVIS, personalo valdymo informacinė sistema paruošta saugiam darbui (10 pav).



11 pav. Visų PerVis vartotojų sekos diagrama, kai duomenys iš/šifruoja DSM

Vartotojai dirbantys su personalo valdymo informacine sistema (11 pav.) turi prieš pradėdami darbą identifikuotis (vartotojo vardas ir slaptažodis), kad PerVIS galėtų patikrinti, kokios yra suteiktos teisės dirbti su PerVIS, tada startuoja DSM servisas ir užkraunamas personalo vadovo nustatytas saugumo lygis. Vartotojai gali pradėti dirbti su PerVIS, darbas yra saugus.



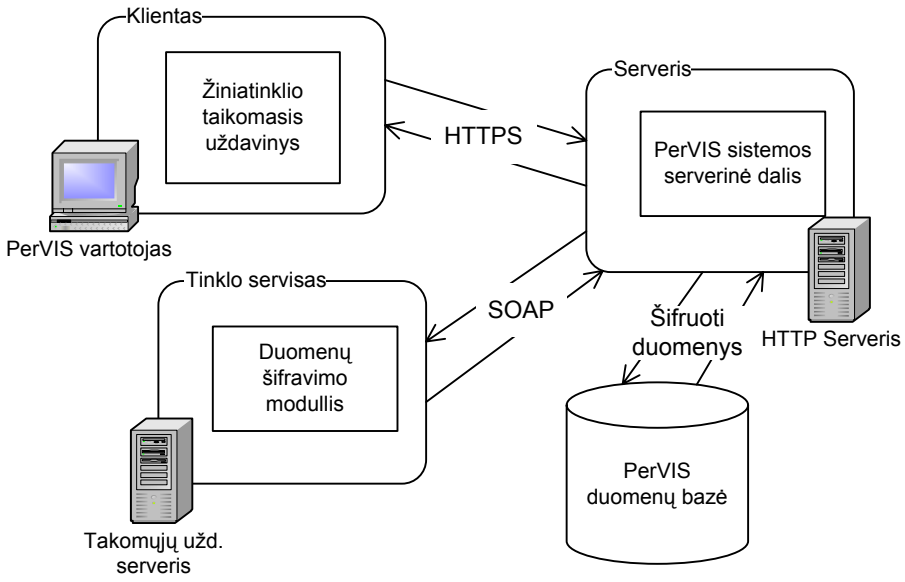
12 pav. Visų PerVis vartotojų sekos diagrama, kai duomenys iš/šifruoja standartinės MySQL duomenų bazių valdymo sistemos funkcijos

Vartotojai dirbantys su personalo valdymo informacine sistema turi prieš pradėdami darbą identifikuotis (vartotojo vardas ir slaptažodis), kad PerVIS galėtų patikrinti kokios yra suteiktos teisės dirbti su PerVIS. Identifikavus galima pradėti dirbti su PerVIS. Dirbant vyksta duomenų siuntimas ir duomenų gavimas, gavus duomenis duomenų bazių valdymo sistema šifruoja duomenis ir saugo duomenis šifruotam pavidale (12 pav.). Kai vartotojas atlieka užklausą duomenų bazių valdymo sistema iššifruoja duomenis ir atsiunčia atviram pavidale, tada sistema gali duomenis pateikti vartotojui pageidauta forma.

IV. Eksperimentas

Programavimui buvo naudota: PHP 5, C#, Microsoft .NET 2.0, MySQL 5. Pasirinktos šios programavimo kalbos ir duomenų bazės valdymo sistema, nes jomis sukurta, jau eksploatuoja personalo valdymo informacinė sistema ir jos pritaikytos internetinėms technologijom ir veikia daugumoje naudojamų operacinių sistemų aplinkose, todėl nereikalauja papildomos techninės įrangos. Yra nemokamos ir pilnai patikimos smulkioms ir vidutinėms įmonėms, naudojant tokio pobūdžio programas.

Programinis sistemos modulis veikia, kaip tinklo servisas (13 pav.). Pradėdamas veikti iškviečia metodą DESEncrypt sukuria objektą tada iškviečiamas jo metodas DESEncrypt, tada yra sukuriamas .NET objektas DESCryptoServiceProvider (kiekvieno algoritmo atveju yra analogiškai), jo pagalba užkoduojamas tekstas ir jis grąžinamas.



13 pav. Personalo valdymo sistemos ir duomenų šifravimo modulio sąsaja

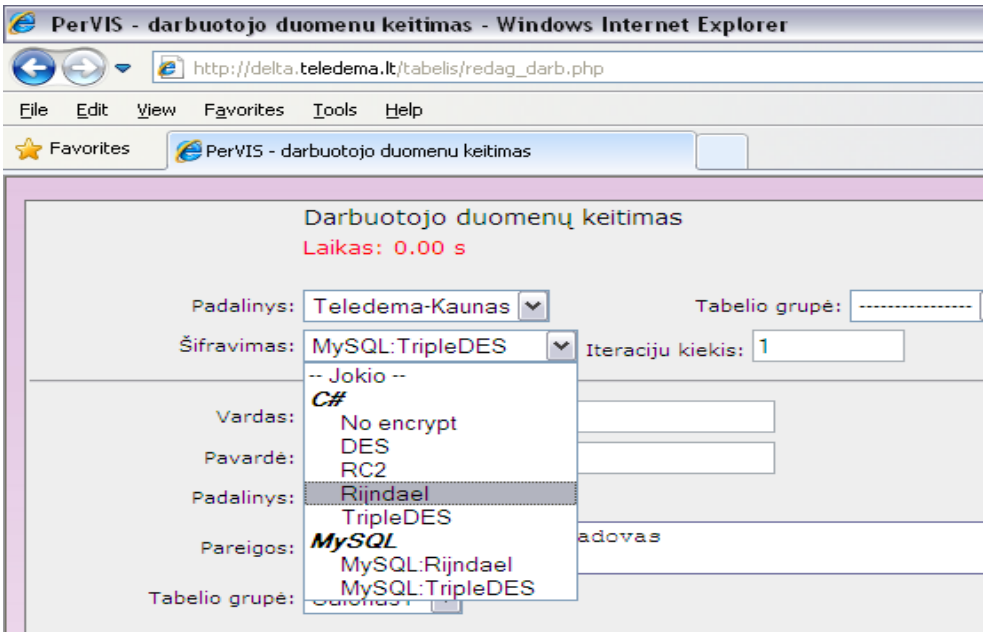
Įdiegus programinį sistemos modulį (tinklo servisą) reikėjo jį susieti su esama sistema komunikacijai buvo pasinaudota PHP CURL biblioteka [56], kad sėkmingai PerVIS veiktų reikėjo pakoreguoti esamos duomenų bazės laukų ilgius, kad tilptų koduota informacija. Pasikeitė duomenų atvaizdavimo bei saugojimo funkcionalumas. Programiniame sistemos modulyje (tinklo servise) po duomenų iš duomenų bazės gavimo juos reikėjo iškoduoti, prieš saugant duomenis į duomenų bazių valdymo sistemą reikėjo juos užkoduoti. Duomenų bazių valdymo sistemoje reikėjo koreguoti ir saugojimo, ir duomenų gavimo užklausas.

Naudojantis minėtomis programavimo technologijomis buvo sukurtas programinis sistemos modulis, kuris leidžia atlikti duomenų šifravimą eksploatuojamoje sistemoje. Ištyrus sukurto programinio sistemos modulio funkcijas buvo gauti rezultatai ir padarytos išvados.

4.1. Gauti rezultatai

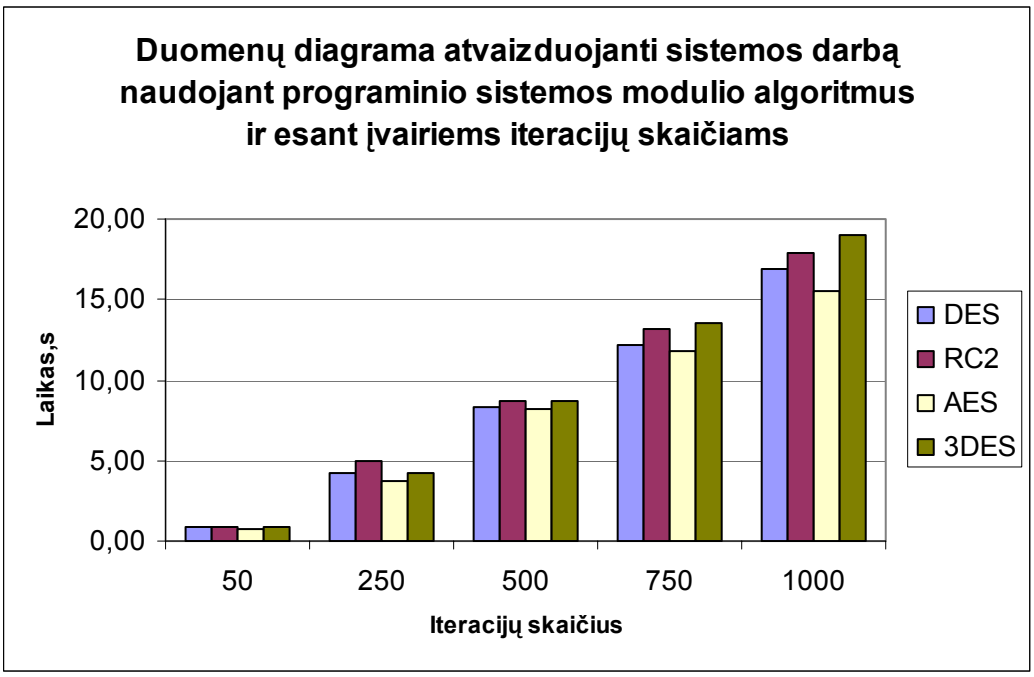
Taigi programinis sistemos modulis turi šias funkcijas, jis leidžia pasirinkti DES, RC2, AES, 3DES šifravimo algoritmus, tai pat suteikia galimybę atlikti šifravimą naudojantis standartinėmis MySQL duomenų bazių valdymo sistemos funkcijomis, tai pat leidžia nustatyti iteracijų kiekį atliekant šifravimą. Buvo atliktas tyrimas (14 pav.) siekiant nustatyti programinio sistemos modulio darbą, kai;

- pasirenkamas duomenų šifravimas naudojant duomenų šifravimo algoritmus ir keičiamas iteracijų skaičius;
- pasirenkamas duomenų šifravimas naudojant standartines duomenų bazių valdymo sistemos funkcijas ir keičiamas iteracijų skaičius;
- pasirenkama duomenų nešifruoti, o tik įvertinti tinklo vėlinimą.



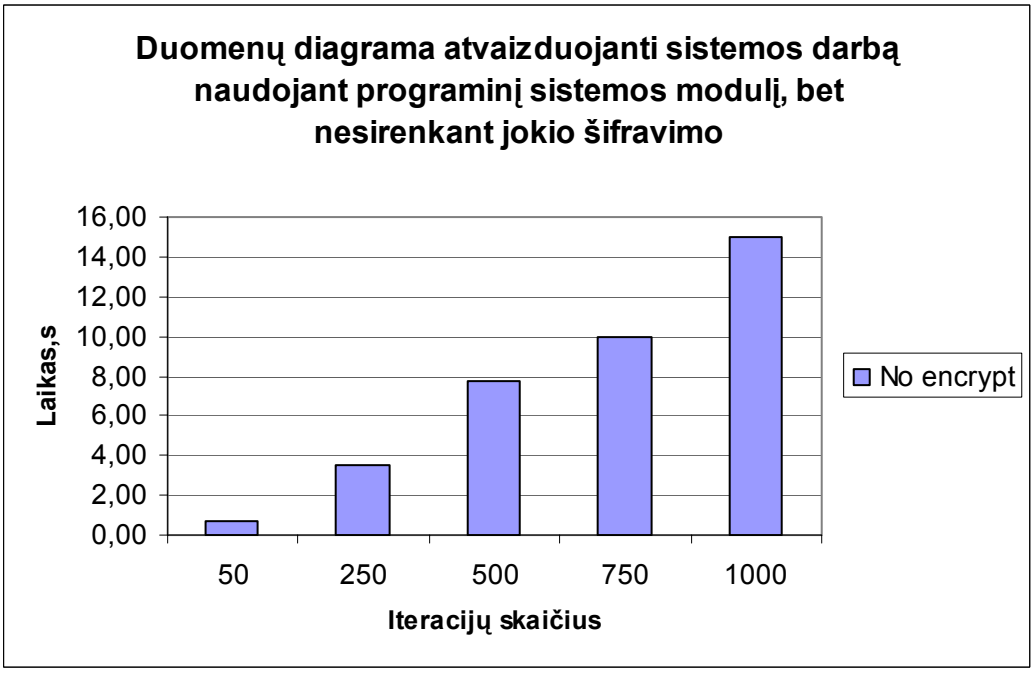
14 pav. Duomenų šifravimo modulio saugumo lygio nustatymo langas

Tyrimas atliktas vienodomis sąlygomis, dėl įrangos rezultatai gali skirtis, tačiau proporcija išliks ta pati vidiniame įmonės tinkle.



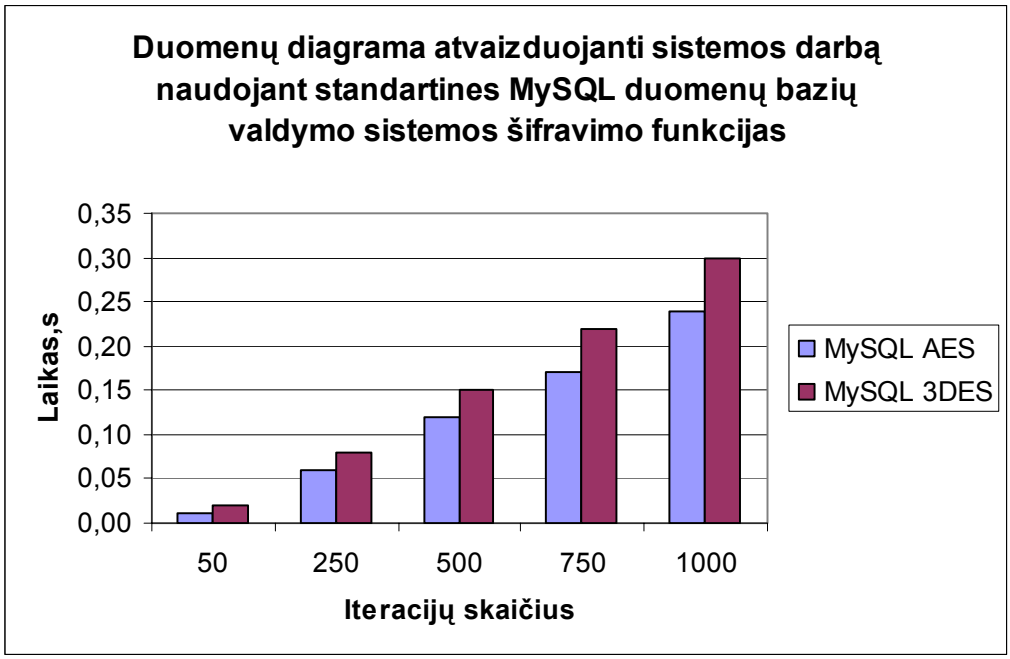
15 pav. Duomenų diagrama atvaizduojanti sistemos darbą naudojant programinio sistemos modulio algoritmus ir esant įvairiems iteracijų skaičiams

Duomenų diagramoje (15 pav.) atvaizduoti programinio sistemos modulio (tinklo serviso) algoritmai ir jų greitaveikos palyginimas vertinant juos pagal iteracijų skaičių. Akivaizdžiai matome iš diagramos AES algoritmas veikia greičiausiai visais atvejais.



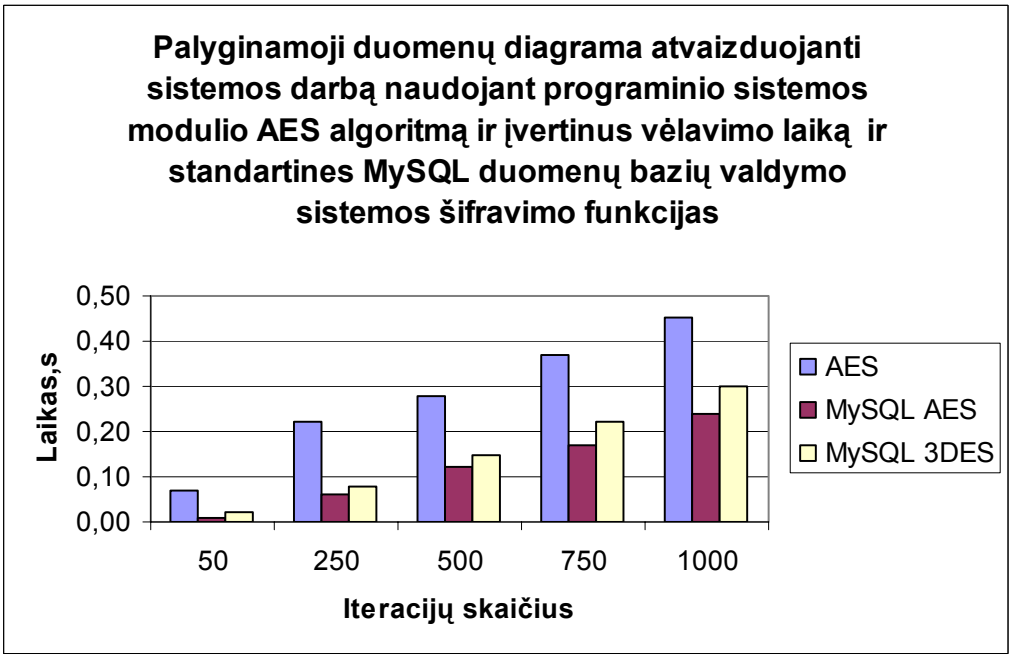
16 pav. Duomenų diagrama atvaizduojanti sistemos darbą naudojant programinį sistemos modulį, bet nesirenkant jokio šifravimo

Duomenų diagramoje (16 pav.) atvaizduotas programinio sistemos modulio (web service) veikimas, kai nenaudojami jokie algoritmai, kaip matome iš diagramos atsiranda vėlinimas, kurio priežastys gali būti įvairios (tinklo greitaveika, techninės įrangos našumas).



17 pav. Duomenų diagrama atvaizduojanti sistemos darbą naudojant standartines MySQL duomenų bazių valdymo sistemos šifravimo funkcijas

Duomenų diagramoje (17 pav.) atvaizduoti standartiniai duomenų bazių valdymo sistemos šifravimo algoritmai ir jų greitaveikos palyginimas vertinant juos pagal iteracijų skaičių. Akivaizdžiai matome iš diagramos AES algoritmas veikia greičiausiai visais atvejais.



18 pav. Palyginamoji duomenų diagrama atvaizduojanti sistemos darbą naudojant programinio sistemos modulio algoritmus ir standartines MySQL duomenų bazių valdymo sistemos šifravimo funkcijas

Duomenų diagramoje (18 pav.) atvaizduota programinio sistemos modulio (tinklo serviso) AES algoritmas ir jo greitaveika ir jo palyginimas su standartiniais duomenų bazių valdymo

sistemos šifravimo algoritmais vertinant juos pagal iteracijų skaičių. Akivaizdžiai matome iš diagramos AES algoritmas veikia greičiausiai visais atvejais,o programinio sistemos modulio (tinklo serviso) AES algoritmas įvertinant vėlinimą veikia tik nežymiai lėčiau už standartinį duomenų bazių valdymo sistemos AES šifravimo algoritmą.

4.2. Eksperimento išvados

Taigi atlikus tyrimą gavome tokius rezultatus, jie atvaizduoti paveiksluose nuo 15 iki 18 imtinai. Apibendrinus gautus rezultatus galima daryti išvadas, kad greičiausius rezultatus atliekant duomenų šifravimą davė AES duomenų šifravimo algoritmas, todėl remiantis, kad AES šifravimo algoritmas 2001 m. JAV vyriausybės buvo pripažintas standartu [33, 34] ir AES lyginant su DES algoritmu yra greitesnis ir programiniu, ir techniniu požiūriu [35], o iki 2009 m. gegužės mėn. buvo pavykusi tik viena ataka („side-chanell atacks“), ir todėl jau 2003 m. birželio mėn. JAV vyriausybės paskelbtas, kad gali būti naudojamas siekiant apsaugoti slaptą informaciją [36], manau tikslinga pasirinkti AES duomenų šifravimo algoritmą, kaip optimaliausią metodą personalo valdymo informacinei sistemai.

MySQL duomenų šifravimo funkcijos naudojančios AES ir 3DES algoritmus, tai pat buvo ištirtos ir pateikė labai greitus rezultatus, tačiau atsižvelgiant, kad atsirastų saugumo spraga, nes duomenys keliautų iš kliento iki serverio atviru tekstu yra nesiūloma rinktis naudoti šias duomenų šifravimo funkcijas.

Atlikus tyrimą gavome rezultatus, juos susisteminus ir palyginus galima teigti, AES šifravimo algoritmas duomenų šifravimą atliko nuo 12 % iki 18 % greičiau už kitus tirtus algoritmus, esant įvairiems iteracijų kiekiams. Didėjant iteracijų kiekiui atsiranda vėlinimas. Vėlinimas atsiranda dėl į personalo valdymo informacinę sistemą integruoto programinio sistemos modulio ir jo atliekamo komunikavimo tarp personalo valdymo informacinės sistemos ir duomenų bazių valdymo sistemos. Norint išvengti vėlinimo reikėtų naudotis standartinėmis MySQL duomenų bazių valdymo sistemos šifravimo funkcijomis. Tokiu atveju siekiant išvengti atviro duomenų formato keliavimo tarp klientinės ir serverinės dalies būtų galima naudoti komunikacijai SSL protokolą.

V. Išvados

1. Išanalizavus Lietuvos Respublikos įstatymus susijusius su asmens duomenimis, nustatyta, kad personalo valdymo informacinė sistema tvarko ir valdo ypatingos svarbos asmens duomenis. Šių duomenų tvarkymas yra reglamentuotas teisės aktais ir atsakomybę turi prisiimti duomenų valdytojas už netinkamą priežiūrą. Duomenų praradimo ar paviešinimo atvejais, atsakomybė tenka tų duomenų valdytojui, todėl įmonė privalo rūpintis asmens duomenų apsauga konfidencialumo atžvilgiu.

2. Išanalizavus duomenų apsaugos metodus, nustatyta, kad fizinės saugos priemonėmis turi pasirūpinti pati įmonė imantis atitinkamų organizacinių sprendimų, programinės saugos priemonių naudojimas gali pagerinti duomenų saugumą, nepriklausomai nuo įmonės vidinės politikos. Duomenų saugumui užtikrinti naudojant programines priemones, gali būti naudojamas duomenų šifravimas, kuris užtikrintų duomenų konfidencialumą ir integralumą.

3. Išanalizuotos rinkoje naudojamas personalo valdymo informacinės sistemos, naudoja duomenų apsaugą duomenų perdavimui arba nenaudoja papildomų duomenų saugos priemonių, todėl šio tyrimo rezultatai yra aktualus siekiant pritaikyti duomenų šifravimą, kaip saugos priemonę personalo valdymo informacinėms sistemoms.

4. Sukurtas personalo valdymo informacinei sistemai duomenų šifravimo modulis ir ištirtas su skirtingais duomenų šifravimo algoritmais ir duomenų srautais. Tyrimas parodė, kad duomenų šifravimas didelės įtakos personalo valdymo informacinės sistemos darbui neturi.

VI. Naudota literatūra

1. Statistikos departamentas | Veikiantys ūkio subjektai ir verslumas. Informacijos skelbimo kalendorius. [interaktyvus], 2009-07-07.
[Žiūrėta: 2009-11-06]. Prieiga per internetą:
http://www.stat.gov.lt/lt/news/view/?id=7628

2. Statistikos departamentas | IT naudojimas įmonėse. Informacijos skelbimo kalendorius [interaktyvus], 2008-07-30.
[Žiūrėta: 2009-11-06]. Prieiga per internetą:
http://www.stat.gov.lt/lt/news/view/?id=2885

3. Lietuvos Respublikos Seimas | Lietuvos Respublikos Asmens Duomenų Teisinės Apsaugos Įstatymas. [interaktyvus], 1996-06-11.
[Žiūrėta: 2009-11-06]. Prieiga per internetą:
http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=29193

4. Valstybinė duomenų apsaugos inspekcija | Svarbu žinoti vadovui. | [interaktyvus], 2005-11-04.
[Žiūrėta: 2009-11-07]. Prieiga per internetą:
http://www.ada.lt/index.php?lng=lt&action=page&id=90

5. Valstybinė duomenų apsaugos inspekcija | Už duomenų apsauga atsakingas asmuo ar padalinys – kas jis ?, 2009-04-17 [interaktyvus].
[Žiūrėta: 2009-11-07]. Prieiga per internetą:
http://www.ada.lt/index.php?lng=lt&action=page&id=615

6. Asociacija „Infobalt“. | Išaugo aktyvių interneto vartotojų skaičius Lietuvoje. [interaktyvus], 2009-10-09.
[Žiūrėta: 2009-11-07]. Prieiga per internetą:
http://www.infobalt.lt/main.php?&i=8019

7. Valstybinė duomenų apsaugos inspekcija | Rekomendacijos asmens duomenų apsaugai internete. [interaktyvus], 2001.
[Žiūrėta: 2009-11-07]. Prieiga per internetą:
http://www.ada.lt/images/cms/File/rekomendacijos%20asmens%20duomenu%20apsaugai%20internete.pdf

8. The European Commission | Privacy on the Internet - An integrated EU Approach to On-line Data Protection. [interaktyvus], 2000-11-21.
[Žiūrėta: 2009-11-07]. Prieiga per internetą:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf

9. Egidijus Kazanavičius, Algimantas Venčkauskas, Agnius Liutkevičius, Arūnas Vrubliauskas | Informacijos saugos vadyba. Kaunas, Vitae Litera, ISBN 978-9955-686-72-9, 2008.

10. Microsoft TechNet | SSL/TLS in Detail. [interaktyvus], 2003-07-31.
[Žiūrėta: 2009-11-08]. Prieiga per internetą:
http://technet.microsoft.com/en-us/library/cc785811(WS.10).aspx

11. Ganesh Ramakrishnan,CISA | Secure Electronic Transaction (SET) Protocol.; Information Systems Control Journal,Volume 6, 2000 [interaktyvus].
[Žiūrėta: 2009-11-08]. Prieiga per internetą:
http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=21545&TEMPLATE=/ContentManagement/ContentDisplay.cfm

12. FAQs on privacy practices, seals & programs | Leader in privacy services [interaktyvus].
[Žiūrėta: 2009-11-08]. Prieiga per internetą:
http://www.truste.com/about_TRUSTe/faqs.html

13. The Better Business Bureau Vision, Mission and Values – U.S. BBB [interaktyvus].
[Žiūrėta: 2009-11-08]. Prieiga per internetą:
http://www.bbb.org/us/BBB-Mission/

14. Lorrie Cranor (Chair) & Rigo Wenning (W3C) | P3P: The Platform for Privacy Preferences , 2007-11-20. [interaktyvus].
[Žiūrėta: 2009-11-08]. Prieiga per internetą:
http://www.w3.org/P3P/

15. Rimantas Plėštys, Dangis Rimkus, Rimantas Kavaliūnas, Ingrida Lagzdinytė, Nijolė Sarafinienė | Kompiuterių tinklų sauga. Kaunas, Vitae Litera, 2008.

16. Heng Yin; Haining Wang | Building an application-aware IPsec policy system; Proceedings of the 14th USENIX Security Symposium, USENIX Associationm, 2005, p. 315–329.

17. Vijay Bollapragada, Mohamed Khalid, Scott Wainner | IPSec VPN Design; Cisco Press, 2005, p. 352

18. European Parliament | Council Directive 96/9/EC; Official Journal L077, 27/03/1996 page(s) 0020-0028, 1996-03-11 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML

19. W. Ford, B.S. Kaliski Jr. | Server-Assisted Generation of a Strong Secret from a Password; 9th International Workshops on Enabling Technologies (WET-ICE 2000), IEEE, 2000.

20. J. Brainard, A. Juels, R. Rivest, M. Szydlo, M. Yung | Fourth Factor Authentication: Somebody You Know ; In ACM CCS , page(s) 168-178, 2006 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://www.rsa.com/rsalabs/node.asp?id=3156

21. Defense Information Systems Agency for Department of Defense | Database Security Technical Implementation Guide ; Version 7, Realese 1, 2004-10-29 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://www.databasesecurity.com/dbsec/database-stig-v7r1.pdf

22. R. E. Smith | Server Authentication: From Passwords to Public Keys First Edition; Boston, MA; London: Addison-Wesley, c2002.

23. Mike Hillyer | Securing a MySQL Server on Windows, 2005-02-01 [interaktyvus]. [Žiūrėta: 2009-11-18]. Prieiga per internetą: http://dev.mysql.com/tech-resources/articles/securing_mysql_windows.html

24. Sun Microsystem | MySQL 5.1 Reference Manual, 2009 [interaktyvus]. [Žiūrėta: 2009-11-18]. Prieiga per internetą: http://dev.mysql.com/doc/refman/5.1/en/index.html

25. Sarker, M.Z.H.; Parvez, M.S | A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data ; 9th International Multitopic Conference, IEEE INMIC 2005, 2005-12-24 Page(s): 1-6.

26. Bart Preneel | A introduction to modern cryptology ; The History of Information Security, 2007, Pages 565-592.

27. U.S Department of Commerce/ National Institute of Standarts and Technology | Data Encryption Standart (DES), 1999-10-25 [interaktyvus]. [Žiūrėta: 2009-11-18]. Prieiga per internetą: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

28. distributed.net: History & Timeline, 2004-11-01 [interaktyvus]. [Žiūrėta: 2009-11-18]. Prieiga per internetą: http://www.distributed.net/history.php

29. U.S Department of Commerce/ National Institute of Standarts and Technology | Recommendation for the Triple Data Encryption Algorithm, 2004-04-16 [interaktyvus]. [Žiūrėta: 2009-11-18]. Prieiga per internetą: http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

30. W.Diffie and M.E. Hellman | Exhaustive Cryptanalysis of the NBS Data Encryption Standart ; Computer 10(6), 1977-06 Page(s) 74-84.

31. Ralph Merkle, Martin Hellman | On the Security of Multiple Encryption; Communications of the ACM, Vol 24, No 7, 1981-07, Page(s) 465-467 [interaktyvus]. [Žiūrėta: 2009-11-18]. Prieiga per internetą: http://www.cs.purdue.edu/homes/ninghui/courses/Spring04/homeworks/p465-merkle.pdf

32. Paul van Oorschof, Michael J. Wiener | A known-plaintext attack on two-key triple encryption ; EUROCRYPT'90, LNCS 473, 1990 Page(s) 318-325 [interaktyvus]. [Žiūrėta: 2009-11-18]. Prieiga per internetą: http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E90/318.PDF

33. National Institute of Standarts and Technology | Specification for the Advanced Encryption Standart (AES) ; 2001-11-26 [interaktyvus]. [Žiūrėta: 2009-11-19]. Prieiga per internetą: http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

34. John Schwartz | Technology: U.S. Selects a New Encryption Technique; New York Times; 2000-10-03 [interaktyvus].
[Žiūrėta: 2009-11-19]. Prieiga per internetą:
http://www.nytimes.com/2000/10/03/business/technology-us-selects-a-new-encryption-technique.html

35. B.Schneier, J.Kelsey, D.Whiting, D.Wagner, Ch. Hall, N.Ferguson, T.Kohno, M.Stay | The Twofish Team's Final Comments on AES selection; 2000-05-15 [interaktyvus].
[Žiūrėta: 2009-11-19]. Prieiga per internetą:
http://www.schneier.com/paper-twofish-final.pdf

36. National Security Agency | National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information; CNSS Policy No.15, FS-1; 2003-06 [interaktyvus].
[Žiūrėta: 2009-11-19]. Prieiga per internetą:
http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

37. Lars R. Knudsen, Vincent Rijmen, Ronal L.Rivest, Matthew J.B. Robshaw: On in the Design and Security of RC2. Fast Software Encryption 1998: 206-221.

38. John Kelsey, Bruce Schneier, David Wagner: Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. ICICS 1997: 233–246

39. B.Schneier | Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish); Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag 1994 Pages(s) 191-204 ; 1993-12 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://www.schneier.com/paper-blowfish-fse.html

40. Anton | run OpenSSL speed benchmark ; 2008-02-23 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://lwn.net/Articles/270590/

41. Aamer Nadeem, Dr M. Younus Javed. | A Performance Comparison of Data Encryption Algorithms; Information and Communication Technologies, 2005.First International Conference Pages(s) 84-89 ; 2005-08-27 .

42. schneier.com/blowfish-bug.txt ; 1996-07-08 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://www.schneier.com/blowfish-bug.txt

43. Serge Vaudenay | On the Weak Keys of Blowfish; Fast Software Encryption, Cambridge, United Kingdom, Lecture Notes in Computer Science No.1039, Page(s) 27-32 , Springer-Verlag 1996 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://lasecwww.epfl.ch/pub/lasec/doc/liens-95-27.A4.ps

44. B.Schneier | Twofish ; 1998 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://www.schneier.com/twofish.html

45. B.Schneier, J.Kelsey, D.Whiting, D.Wagner, Ch. Hall, N.Ferguson | The Twofish Encryption Algorithm: A 128-bit Block Cipher ; New York City; John Willey & Sons. ISBN 0-471-35381-7. 1999-03-22.

46. B.Schneier, D.Whiting | A Performance Comparison of the Five AES Finalists, Third AES Candidate Conference, 2000 [interaktyvus].
[Žiūrėta: 2009-11-22]. Prieiga per internetą:
http://www.schneier.com/paper-aes-comparison.pdf

47. J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer | OpenPGP Message Format, 2007-11 [interaktyvus].
[Žiūrėta: 2009-12-02]. Prieiga per internetą:
http://tools.ietf.org/html/rfc4880

48. S. Moriai, Y. L. Yin | Cryptanalysis of Twofish Cryptanalysis (II); 2000 [interaktyvus].
[Žiūrėta: 2009-12-04]. Prieiga per internetą:
http://www.schneier.com/twofish-analysis-shiho.pdf

49. B.Schneier | Schneier on Security: Twofish Cryptanalysis Rumors; 2005-11-23 [interaktyvus].
[Žiūrėta: 2009-12-04]. Prieiga per internetą:
http://www.schneier.com/blog/archives/2005/11/twofish_cryptan.html

50. Human Resource Management Software – Microsoft Dynamics | Realize the potential of your workforce with human resource management software, 2009 [interaktyvus].
[Žiūrėta: 2009-12-07]. Prieiga per internetą:
http://www.microsoft.com/dynamics/en/us/hr-management.aspx

51. Product Features | Product Features - OrangeHRM , 2009 [interaktyvus].
[Žiūrėta: 2009-12-09]. Prieiga per internetą:
http://www.orangehrm.com/product-features.shtml

52. VVS 'Pragma' v. 4.0 modulis 'Personalo apskaita' | Informacija apie prekę , 2009 [interaktyvus].
[Žiūrėta: 2009-12-12]. Prieiga per internetą:
http://www.proringas.lt/PragPreke.aspx?PrekeID=1831

53. Personalo apskaita | Tėja – verslo procesų valdymas, rodikliai, apskaita, analizė, 2009 [interaktyvus].
[Žiūrėta: 2009-12-14]. Prieiga per internetą:
http://www.teja.lt/personalo_apskaita.html

54. Microsoft Corporation | Kas nauja programoje „Microsoft Dynamics AX 4.0", 2009 [interaktyvus].
[Žiūrėta: 2009-12-14]. Prieiga per internetą:
http://www.microsoft.com/lietuva/Dynamics/ax/whatsnew.mspx

55. OrangeHRM | Quick User Guide OrangeHRM 2.2.2 Document Version 1.0, 2005-2007 [interaktyvus].
[Žiūrėta: 2009-12-14]. Prieiga per internetą:
http://www.orangehrm.com/quickstart/QuickUse%20Guide_version%202_2_2.pdf

56. Avilura Pragma v. 4.0 | Naudojamos technologijos, 2004 [interaktyvus]. [Žiūrėta: 2009-12-14]. Prieiga per internetą: http://www.avilura.lt/index.php?lng=lt&content=pages&page_id=103

57. UAB „Kibernetinė erdvė“ | Tėja – verslo procesų valdymas, rodikliai, apskaita, analizė - Dokumentacija [interaktyvus]. [Žiūrėta: 2009-12-14]. Prieiga per internetą: http://www.teja.lt/media/TEJA_Administratoriaus_vadovas_1_0_4_0.pdf

58. PHP: cURL – Manual | Client URL Library [interaktyvus]. [Žiūrėta: 2010-10-04]. Prieiga per internetą: (http://php.net/manual/en/book.curl.php

Summary

Author: Laimonas Žakevičius

Subject: Research and application of methods for personal data protection in human resource management system

Purpose of this research – to analyze numbering methods of personal data and to adapt the most optimal method of staff management in the informative system. The research will be done using an informative system of personal management, which was created by me, and which now is succesfuly used by JSC „Teledema“.

After creation of informative system programmable model of staff management (service, the purpose of which is to encode the data, which were written in the informative system of staff management and to send the encoded data into the system of bases handling, or to decode the data, received from the system of data handling, and to provide them by the form required by a user, the system of staff management will become a safe and reliable informative system of staff management, which would allow to gather an exhaustive, exact data in real time, would allow to systemize them and provide for users of the system, who have rights to familiarize, manage and handle such information, also would ensure, that protected data of a person are kept in the encoded form, thus data could be reviewed, managed and handled not only by these people, who have permission from the manager of data.

VII. Priedai

1. Laimonas Žakevičius | Asmens duomenų šifravimo metodų naudojimas personalo valdymo informacinėje sistemoje; Informacinės Technologijos, XVI tarpuniversitetinė magistrantų ir doktorantų konferencija, Konferencijos pranešimų medžiaga Psl. 41-44 ; ISSN 2029-249X, 2011-04-22 .
2. UAB „Teledema“ | Oficialus duomenų šifravimo modulio skirto personalo valdymo informacinei sistemai įdiegimo raštas; 2011-05-23 Nr. 11-239.

ISSN 2029–249X

KAUNO TECHNOLOGIJOS UNIVERSITETAS
VYTAUTO DIDŽIOJO UNIVERSITETAS
VILNIAUS UNIVERSITETO KAUNO HUMANITARINIS FAKULTETAS

INFORMACINĖS TECHNOLOGIJOS

XVI tarpuniversitetinė magistrantų ir doktorantų konferencija

Konferencijos pranešimų medžiaga

TECHNOLOGIJA
KAUNAS • 2011

TURINYS

I sekcija. Programinės įrangos inžinerija

II sekcija. Informacinių technologijų taikymai

ASMENS DUOMENŲ ŠIFRAVIMO METODŲ NAUDOJIMAS PERSONALO VALDYMO INFORMACINĖJE SISTEMOJE *

Laimonas Žakevičius[1],

[1]KTU Informatikos fakultetas, Studentų g. 50, Kaunas, Lietuva,
laimonas.zakevicius@stud.ktu.lt

Santrauka. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas įpareigoja saugoti asmens duomenis, todėl atsiranda prievolė kiekvienam duomenų valdytojui juos saugoti. Šiame straipsnyje aprašomas asmens duomenų apsaugos metodų naudojimas, atliktų eksperimentų metodika bei rezultatai – blokinio simetrinio rakto algoritmo pasirinkimas, vertinant saugų ir stabilų sistemos darbą. Remiantis gautais rezultatais, pagrindžiamas sistemos duomenų šifravimo modulio sukūrimas ir taikymas.

Raktiniai žodžiai: asmuo, duomenys, šifravimas, metodas, personalas, valdymas.

1 Įvadas

Kaip apibrėžia Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas: [1] "Asmens duomenys - duomenys apie konkretų arba iš duomenų nustatomą fizinį asmenį, jo dalykinius santykius ir išvados apie asmenį, padarytos remiantis šiais duomenimis. Ypatingi asmens duomenys - asmens duomenys apie jo rasinę kilmę, tautinį ir etninį priklausomumą, politinius, religinius ir kitus įsitikinimus, partiškumą, teistumą, sveikatą, patologinius defektus ir intymų gyvenimą (privatų asmens gyvenimą)." Tokie duomenys, remiantis minėto įstatymo 4 str. 1 dalimi, turi būti saugomi visą fizinio asmens gyvenimą. Visos įmonės ir įstaigos, kurios atitinka Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 2 str. 8 dalies aprašymą: "duomenų valdytojas - fizinis arba juridinis asmuo, kuris teisėtai tvarko duomenis", privalo tinkamai pasirūpinti asmens duomenų apsauga, nes jas įpareigoja minėtojo įstatymo 5 str. 1 dalis, kuri teigia, kad "asmens duomenys yra kaupiami ir saugomi duomenų įrašuose, už kurių apsaugą ir tvarkymą yra atsakingas duomenų valdytojas." Ypatingas dėmesys turi būti skiriamas ypatingų asmens duomenų tvarkymui, nes minėti duomenys gali būti tvarkomi, tik išskirtiniais atvejais, kai "toks tvarkymas yra būtinas darbo ar valstybės tarnybos tikslu duomenų valdytojo teisėms ir prievolėms darbo teisės srityje įgyvendinti įstatymų nustatytais atvejais"[2].

Lietuvos įmonėse, sparčiai plečiantis informacinių technologijų skvarbai, atsiranda daug naujų galimybių. Viena iš didesnių ir bendra visoms įmonėms bei įstaigoms problema yra personalo valdymas. Lietuvos įmonėse ir įstaigose didėja poreikis turėti personalo valdymo informacines sistemas. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas įpareigoja saugoti asmens duomenis, todėl atsiranda prievolė kiekvienam duomenų valdytojui juos saugoti. Dėl šios priežasties, personalo valdymo informacinė sistema turi būti saugi sistema, nes pagrindinė tokios sistemos paskirtis yra asmens duomenų (vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, telefono numeris, Sodros pažymėjimo numeris, lytis, šeimyninė padėtis ir kita informacija apie asmenį) tvarkymas – duomenų rinkimas, kaupimas, apdorojimas ir saugojimas.

2 Personalo valdymo informacinių sistemų saugos problemų analizė

Personalo valdymo informacinės sistemos pagrindinė paskirtis yra asmens duomenų tvarkymas – duomenų rinkimas, kaupimas, apdorojimas ir saugojimas. Dėl personalo valdymo informacinės sistemos tiesioginės paskirties, tokios sistemos susiduria su įvairiomis saugumo problemomis. Pagrindinė saugos problema – kaip apsaugoti asmens duomenis, kuriuos saugo sistema. Personalo valdymo informacines sistemas ar verslo valdymo informacines sistemas, kurių sudėtinė dalis yra personalo valdymo informacinės sistemos modulis, kuria daug įvairių programinės įrangos gamintojų tiek užsienyje (nuo Microsoft Dynamics [3] iki atvirojo kodo OrangeHRM [4]), tiek Lietuvoje (tarp lietuviškųjų gamintojų išsiskiria UAB „Proringas" [5], gaminantis verslo valdymo sistemą „Pragma" ir UAB „Kibernetinė erdvė" [6], kurianti verslo valdymo sistemą „Tėja"). Visos šios kompanijos didelį dėmesį skyrė duomenų perdavimui tarp klientinės dalies ir serverinės dalies. Siekiant išvengti saugos incidentų, yra siūloma naudoti SSL protokolą [7] arba perduodamus/gaunamus duomenis siųsti užšifruotus.

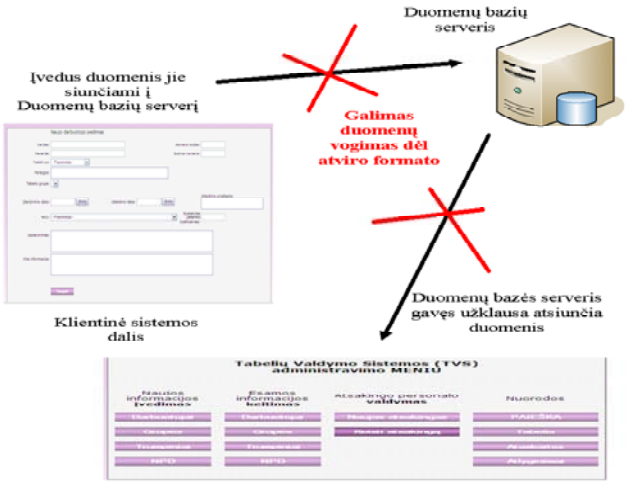
2.1 UAB „X" personalo valdymo informacinės sistemos saugos problemų analizė

UAB „X" naudoja personalo valdymo informacinę sistemą. Sistemą savo kasdieninėms darbo užduotims atlikti naudoja įmonės vadovas, įmonės skyriaus vadovai ir įmonės personalo vadovė. Asmenys, dirbantys su sistema, įveda duomenis arba pateikia užklausą, siekiant gauti duomenis iš duomenų bazės. Dirbant su sistema nuolat vyksta duomenų kaita - įvedami, koreguojami duomenys, o visi sistemoje esantys duomenys

* Asmens duomenų šifravimo metodų naudojimas personalo valdymo informacinėje sistemoje

atitinka asmens duomenų apibrėžimą pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą [1], todėl tokius duomenis privaloma apsaugoti. Saugoti duomenis duomenų valdytoją įpareigoja Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 5 str. 1 dalis, kuri teigia, kad "asmens duomenys yra kaupiami ir saugomi duomenų įrašuose, už kurių apsaugą ir tvarkymą yra atsakingas duomenų valdytojas. "

Dėl minėtos priežasties yra tikslinga įvedamus duomenis šifruoti ir į duomenų bazę perduoti užšifruotus. Visus duomenis, esančius duomenų bazėje, būtina taip pat saugoti šifruotame pavidale, siekiant išvengti asmens duomenų nesaugaus perdavimo vietiniu tinklu. Esant šifruotiems asmens duomenims, taip pat užkertama galimybė darbuotojams, neturintiems teisės naudotis minėta informacija, panaudoti ją netinkamiems tikslams bei atskleisti trečiajai šaliai.



1 pav. Personalo valdymo informacinės sistemos saugos problema

2.2 Duomenų šifravimo algoritmų apžvalga

Duomenų šifravimo algoritmai skirstomi į simetrinio rakto ir asimetrinio rakto algoritmus.[8]. Kriptografinėje sistemoje, naudojančioje simetrinę kriptografiją šifravimui ir iššifravimui, naudojamas tas pats raktas. Kriptografinėje sistemoje, naudojančioje asimetrinę kriptografiją šifravimui ir iššifravimui, naudojami du skirtingi raktai, kurie yra matematiškai susieti. Simetrinio rakto algoritmai skirstomi į srauto ir blokinius [9]. Srauto algoritmai duomenis šifruoja po bitą. Labiausiai žinomi RC4 ir RC5. Blokiniai algoritmai duomenis šifruoja blokais. Labiausiai žinomi DES, 3DES, AES, Blowfish. Šiuos algoritmus plačiau apžvelgsime.

2.2.1 DES ir 3DES algoritmų apžvalga

DES (Data Encryption Standart – duomenų šifravimo standartas) – blokinis simetrinio rakto algoritmas, kurio blokų rakto ilgis 64 bitai, rakto ilgis 56 bitai. DES tapo duomenų šifravimo standartu 1977 m. [10].

DES algoritmas yra pakankami nesaugus dėl mažo rakto dydžio, todėl jau 1999 m. distributed.net [11] paskelbė, kad jiems pavyko įveikti DES algoritmo raktą per rekordiškai trumpą laiką. Dėl šios priežasties buvo pakeistas standartas ir atsirado 3DES (Triple DES) [12].

3DES – blokinis simetrinio rakto algoritmas, kurio blokų rakto ilgis 64 bitai, o rakto ilgis yra 56 arba 112 arba 168 bitai. 3DES standartas leidžia naudoti tris skirtingus duomenų šifravimo nustatymus, tai :

- Visi trys raktai yra skirtingi ir tai yra pats stipriausias nustatymas, nes naudojamas 3*56=168 bitų raktas.
- Pirmas ir antras raktas yra skirtingi, o trečias yra lygus pirmajam raktui, todėl šis nustatymas yra mažiau saugus, nes yra naudojamas 2*56=112 bitų raktas. Tai yra pakankamai saugu, nes toks raktas apsaugo nuo meet-in-the-middle attacks (žmogaus viduryje atakos) [13], tačiau šis variantas yra pasiduodantis chosen-plaintext arba known-plaintext atakoms.[14,15].
- Visi trys raktai yra vienodi. Šis nustatymas palaiko suderinamumą su DES standartu, nes pirmas ir antras pasirinkimai nėra suderinami ir DES operacijas tiesiog panaikintų. Tai yra nerekomenduojama NIST [12] ir nėra palaikoma pagal ISO/IEC 18033-3.

2.2.2 AES algoritmo apžvalga

AES (Advanced Encryption Standart – pažangus šifravimo standartas) šifravimo algoritmas 2001 m. JAV vyriausybės buvo pripažintas standartu.[16,17]. Algoritmas dar vadinamas Rinjdael algoritmu, jo autoriai yra J. Daemen ir V.Rijmen. Algoritmo blokų rakto ilgis 128 bitai, o šifravimo raktų ilgis - 128, 192, 256 bitai.

AES lyginant su DES algoritmu yra greitesnis ir programiniu, ir techniniu požiūriu.[18]. Iki 2009 m. gegužės mėn. buvo pavykusi tik viena ataka (side-chanell atacks), todėl 2003 m. birželio mėn. JAV vyriausybė paskelbė, kad AES gali būti naudojamas, siekiant apsaugoti slaptą informaciją. [19]. Tik tada buvo nurodyta, kad galima slaptiems dokumentams (SECRET) naudoti 128, 192, 256 bitų raktus, o ypatingai slaptiems dokumentams (TOP SECRET) naudoti tik 192 ar 256 bitų raktus.

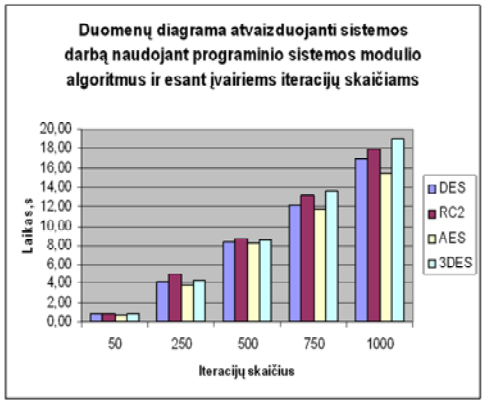
2.2.3 RC2 algoritmo apžvalga

RC2 (RC2 – Rivest Cipher) yra blokinis simetrinio rakto algoritmas sukurtas 1987 m. Rono Rivesto, kuris taip pat sukūrė RC4, RC5, RC6 algoritmus.[20,21]. RC2 algoritmo plėtojimą rėmė Lotus, nes jiems vykdant JAV NSA agentūros užsakymą buvo siekiama apsaugoti Lotus Notes kuriamą programinę įrangą. 1989 m. RC2 buvo priimta, kaip standartas. Nuo sukūrimo RC2 buvo laikomas uždaru algoritmu, kol 1996 m. buvo anonimiškai atskleistas UseNet tinkle. Dėl šios priežasties buvo manoma, kad algoritmas rėmėsi atvirkštinės inžinerijos principu. RC2 naudojant 128 bitų raktą užtikrina tokį pat saugumo lygį, kaip ir 3DES.

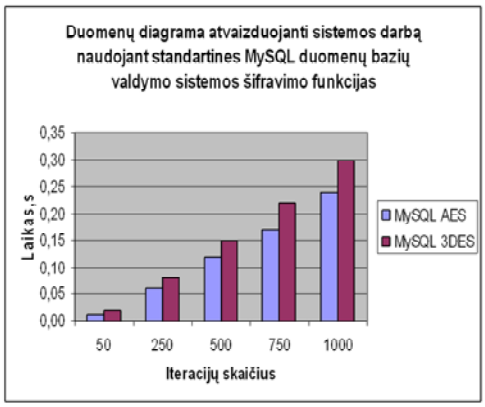
3 Eksperimentas ir jo rezultatai

Eksperimento tikslas – sukurtas programinis sistemos modulis, kuris leidžia atlikti duomenų šifravimą, UAB „X" eksploatuojamoje personalo valdymo informacinėje sistemoje. Eksperimento realizavimui naudota PHP programavimo kalba, Microsoft NET aplinka ir UAB „X" duomenų bazių serveryje naudojama MySQL duomenų bazių valdymo sistema. Atlikus tyrimą ir gavus rezultatus galima teigti, kad atliekamų iteracijų skaičius tiesiogiai įtakoja šifravimo laiką, ir iteracijų skaičiui viršijant 250 atsiranda vėlinimas.Vėlinimo atsiradimą įtakoja personalo valdymo informacinės sistemos ir programinio sistemos modulio komunikavimo laikas. Siekiant išvengti vėlinimo problemos galima naudoti standartines MySQL duomenų bazių valdymo sistemos šifravimo funkcijas.

Apibendrinus gautus rezultatus, galima daryti išvadą, kad greičiausi rezultatai, atliekant duomenų šifravimą, pasiekiami naudojant AES duomenų šifravimo algoritmą. Dėl šios priežasties, AES šifravimo algoritmas 2001 m. JAV vyriausybės buvo pripažintas standartu. [16,17] Manau, kad tikslinga pasirinkti AES duomenų šifravimo algoritmą, kaip optimaliausią metodą personalo valdymo informacinei sistemai.



2 pav. Algoritmų našumo palyginimas



3 pav. Algoritmų našumo palyginimas (duomenų bazių serveryje)

4 Išvados / Ateities darbai

Išanalizavus Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą [1], išsiaiškinome, kaip įstatymas apibrėžia asmens duomenų sąvoką, kas yra įvardijami asmens duomenų valdytojais bei kokios jų pareigos. Remiantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu yra būtina saugoti asmens duomenis. Įvairūs programinės įrangos gamintojai renkasi skirtingus saugos metodus. Duomenų šifravimas – atviro teksto (duomenys, kurių neįtakojo kriptografijos sistemos) pavertimas šifruotu tekstu (duomenys įtakoti kriptografijos sistemos), naudojant šifravimo algoritmą ar raktą, yra laikomas patikimu metodu siekiant apsaugoti asmens duomenis.

Personalo valdymo informacinėje sistemoje saugomi duomenys yra priskiriami asmens duomenims arba ypatingiesiems asmens duomenims, todėl apsaugai siūlome naudoti duomenų šifravimą. Atlikus tyrimą gavome rezultatus, juos susisteminus ir palyginus galima teigti, AES šifravimo algoritmas duomenų šifravimą atliko nuo 12 % iki 18 % greičiau už kitus tirtus algoritmus, esant įvairiems iteracijų kiekiams. Didėjant iteracijų kiekiui atsiranda vėlinimas. Vėlinimas atsiranda dėl į personalo valdymo informacinę sistemą integruoto programinio sistemos modulio ir jo atliekamo komunikavimo tarp personalo valdymo informacinės sistemos ir duomenų bazių valdymo sistemos. Norint išvengti vėlinimo reikėtų naudotis standartinėmis MySQL duomenų bazių

valdymo sistemos šifravimo funkcijomis. Tokiu atveju siekiant išvengti atviro duomenų formato keliavimo tarp klientinės ir serverinės dalies siūlyčiau naudoti komunikacijai SSL protokolą.[7].

Literatūros sąrašas:

[1] **Lietuvos Respublikos Seimas**. Lietuvos Respublikos Asmens Duomenų Teisinės Apsaugos Įstatymas. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=29193, 1996-06-11.Žiūrėta 2009-12-20.

[2] **Valstybinė duomenų apsaugos inspekcija**. Svarbu žinoti vadovui. http://www.ada.lt/index.php?lng=lt&action=page&id=90, 2005-11-04.Žiūrėta 2009-12-20.

[3] **Human Resource Management Software – Microsoft Dynamics**. Realize the potential of your workforce with human resource management software. http://www.microsoft.com/dynamics/en/us/hr-management.aspx, 2009.Žiūrėta 2009-12-20.

[4] **Product Features**. Product Features - OrangeHRM. http://www.orangehrm.com/product-features.shtml, 2009.Žiūrėta 2009-12-20.

[5] **VVS 'Pragma' v. 4.0 modulis 'Personalo apskaita'.** Informacija apie prekę . http://www.proringas.lt/PragPreke.aspx?PrekeID=1831, 2009.Žiūrėta 2009-12-20.

[6] **Personalo apskaita**. Tėja – verslo procesų valdymas, rodikliai, apskaita, analizė http://www.teja.lt/personalo_apskaita.html, 2009.Žiūrėta 2009-12-20.

[7] **Microsoft TechNet**. SSL/TLS in Detail http://technet.microsoft.com/en-us/library/cc785811(WS.10).aspx, 2003-07-31.Žiūrėta 2009-12-20.

[8] **Sarker, M.Z.H.; Parvez, M.S**. A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data , *9th International Multitopic Conference, IEEE INMIC 2005*. 2005-12-24, Page(s) 1-6

[9] **Bart Preneel**. A introduction to modern cryptology ; *The History of Information Security*, 2007, Pages 565-592.

[10] **U.S Department of Commerce/ National Institute of Standarts and Technology**. Data Encryption Standart (DES), http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf , 1999-10-25. Žiūrėta 2009-12-20.

[11] **distributed.net**. History & Timeline. http://www.distributed.net/history.php , 2004-11-01. Žiūrėta 2009-12-20.

[12] **U.S Department of Commerce/ National Institute of Standarts and Technology**. Recommendation for the Triple Data Encryption Algorithm, http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf , 2004-04-16. Žiūrėta 2009-12-20.

[13] **W.Diffie and M.E. Hellman**. Exhaustive Cryptanalysis of the NBS Data Encryption Standart, *Computer 10(6)*, 1977-06 Page(s) 74-84.

[14] **Ralph Merkle, Martin Hellman**. On the Security of Multiple Encryption; *Communications of the ACM, Vol 24, No 7*, 1981-07, Page(s) 465-467 http://www.cs.purdue.edu/homes/ninghui/courses/Spring04/homeworks/p465-merkle.pdf .Žiūrėta 2009-12-20.

[15] **Paul van Oorschof, Michael J. Wiener**. A known-plaintext attack on two-key triple encryption, *EUROCRYPT'90, LNCS 473*, 1990, Page(s) 318-325 , http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E90/318.PDF , Žiūrėta 2009-12-20.

[16] **U.S Department of Commerce/ National Institute of Standarts and Technology**. Specification for the Advanced Encryption Standart (AES) ; http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf , 2001-11-26. Žiūrėta 2009-12-20.

[17] **John Schwartz**. Technology: U.S. Selects a New Encryption Technique; *New York Times*; http://www.nytimes.com/2000/10/03/business/technology-us-selects-a-new-encryption-technique.html , 2000-10-03. Žiūrėta 2009-12-20.

[18] **B.Schneier, J.Kelsey, D.Whiting, D.Wagner, Ch. Hall, N.Ferguson, T.Kohno, M.Stay**. The Twofish Team's Final Comments on AES selection; http://www.schneier.com/paper-twofish-final.pdf , 2000-05-15. Žiūrėta 2009-12-20.

[19] **National Security Agency**. National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, *CNSS Policy No.15*, FS-1, http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf , 2003-06. Žiūrėta 2009-12-20.

[20] **Lars R. Knudsen, Vincent Rijmen, Ronal L.Rivest, Matthew J.B. Robshaw**: On in the Design and Security of RC2. *Fast Software Encryption 1998*, 206-221

[21] **John Kelsey, Bruce Schneier, David Wagner**: Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. *ICICS 1997*, 233–246

Usage of numbering methods of person's data in the human resource managament system

Legal security law of person's data of the Republic of Lithuania obligates to secure data of person, thus the duty to secure them is imposed on each possessor of the data. Usage of methods concerning security of person's data, methods and results of the experiments - choice of symmetrical key algorithm while evaluating safe and stabile work of the system, are described in this article. Creation and application of the numbering model of system data is based with reference to the received results.

teledema
mobiliojo ryšio operatorius

Vytauto pr. 32 LT-44328 Kaunas, tel. 8 37 42 45 22, faksas 8 37 22 13 13

el. paštas info@teledema.lt, www.teledema.lt

2011-05-23 Nr. 11-239

Kaunas

ĮDIEGIMO RAŠTAS

Laimonas Žakevičius, Kauno technologijos universiteto IFN 9/3 gr. magistrantas, atliko tyrimą, siekiant išanalizuoti asmens duomenų šifravimo metodus ir pritaikyti optimaliausią metodą personalo valdymo informacinėje sistemoje. Tyrimo tikslas įgyvendintas. Įmonės naudojamoje personalo valdymo informacinėje sistemoje įdiegtas programinis sistemos modulis, leidžiantis atlikti duomenų šifravimą ir iššifravimą bei užtikrinantis, kad duomenis galės peržiūrėti, valdyti ir tvarkyti tik tie asmenys, kuriems leidimą yra davęs duomenų valdytojas.

UAB „Teledema"
Direktorius Andrius Jankauskas

IT vadovas Giedrius Kaleckas