LATVIJAS UNIVERSITĀTE

MAĢISTRA DARBS

RĪGA 2015

LATVIJAS UNIVERSITĀTE
EKONOMIKAS UN VADĪBAS FAKULTĀTE
Ekonometrijas un biznesa informātikas katedra

UZŅĒMUMA INFORMĀCIJAS SISTĒMU DATU ZUDUMU UN NOPLŪDES NOVĒRŠANA

Data loss and leakage prevention of enterprise information systems

MAĢISTRA DARBS

Autors: Vadības zinību maģistra studiju programmas
Vadības informācijas sistēmas
studiju virziena
2. kursa students
Edgars Teteris
Stud. apl. et09032

Darba vadītājs:
asoc.prof., Uldis Rozevskis

Rīga 2015

ANOTĀCIJA

Maģistra darba tēma ir „Uzņēmuma informācijas sistēmu datu zudumu un noplūdes novēršana”.

Izpētītā problēma ir informācijas tehnoloģu un informācijas sistēmu (turpmāk IT/IS) drošības riska mazināšana uzņēmumā, lai spētu saglabāt kvalitatīvu informāciju. Maģistra darbā tiek apzināta informācijas sistēmu drošība uzņēmumā, vadoties pēc esošā normatīvā regulējuma par informācijas sistēmu drošības nepieciešamību, kā arī veikta IS drošības standartu izpēte. Autors maģistra darbā ir izvirzījis sekojošu mērķi: novērtēt uzņēmuma informācijas tehnoloģiju un informācijas sistēmu riskus, un izstrādāt pasākumu plānu to mazināšanā.

Darbs sastāv no 81 lapaspuses. Darbā iekļauti 20 attēli, 5 tabulas, 2 pielikumi.

Atslēgas vārdi: Drošība, dokumentācija, biznesa modelis, riski.

ABSTRACT

Master's thesis: "Data loss and leakage prevention of enterprise information system".

The problem investigation is the information technology and information system (hereinafter referred to as IT/IS) security risk mitigation an undertaking to be able to maintain the high quality information. Master's work is to deliberate information systems security in company, according to the current regulatory framework for the security of information systems need, as well as carried out the IS security standards research. Author Master's work has set the following objectives: to assess the company's information technology and information systems risks, and develop an action plan for their reduction.

The work consists of 81 pages. Work includes 20 pictures, 5 tables, 2 annexes.

Keywords: Security, documentation, business model risks.

SATURS

APZĪMĒJUMU SARAKSTS

BCP- (*Business Continuity Plan*) biznesa nepārtrauktības plāns. Tiek izstrādātas, ieviestas un dokumentētas procedūras, kuras nodrošina biznesam svarīgāko funkciju pieejamību pēc iespējas mazākām dīkstāvēm.

DRP-(*Disaster Recowery Plan*) biznesa atjaunošanas plāns incidentu gadījumā. Tiek izstrādātas, ieviestas un dokumentētas procedūras un atbildības, pēc kurām vadoties tiek veiktas darbības biznesam svarīgāko funkciju atjaunošanu, incidentu gadījumā.

Discoverer objekti - discoverer atskaišu šabloni.

JAVA - objektu orientēta programmēšanas valoda.

JavaScript skriptēšanas valoda interaktīvo tīmekļa lapu izstādei.

IT/IS – informāciju tehnoloģijas/informāciju sistēmas

IS - informācijas sistēmas.

IT - informācijas tehnoloģijas.

Integritāte - īpašība, kas norāda, ka informācijas resursi saglabā savu sākotnējo precizitāti un pilnīgumu, kā arī informācijas apstrādes metožu aizsargātību.

OAS – (*Oracle Application Server*) oracle lietojumprogrammu serveris.

KPI – (*Key performance indicator*) svarīgākā darba izpildes rādītāji.

KRI – (*Key Risk Indicator*) svarīgākie riska identifikatori

ITSM - (*IT Service Management*) – IT pakalpojumu vadība

Pikšķerēšana jeb fišings – (*phishing*) nelikumīgs veids, kurā ar viltu tiek iegūts no interneta lietotāja slepena informācija, piemēram, lietotāju vārdus, paroles, kredītkaršu numurus.

RSA - (*RSA encryption*) RSA šifrēšana. Patentēts publiskās atslēgšifrēšanas algoritms, ko izstrādājuši RSA Data Security, Inc. darbinieki Rivest, Shamir un Adelman 1978. gadā. Šis algoritms ir šifrēšanas tehnikas PGP pamatā.

TLS - (*Transport Layer Security*) kriptogrāfijas protokola daļa, kas nodrošina drošu komunikāciju Internetā.

Tīmekļa servisi (*Web services*) - metode, komunikācijai starp divām informācijas sistēmām, izmantojot tīkla.

SLA - (Service level agreement**)** vienošanās par pakalpojuma līmeni – dokuments, kurš formulē divu vai vairāku pušu tiesības un pienākumus, līguma par pakalpojumu sniegšanu veidā. SLA galvenā nozīme ir noteikt sniedzamu klientam piegādātāja pakalpojumu līmeni saskaņā ar abpusīgu vienošanos. SLA ir pamata instruments IT pakalpojumu kvalitātes nodrošināšanas jautājumu regulēšanai.

Migrācijas testa vide - testa vide, kurā projekta ietvaros tika secīgi migrēta datubāze uz Oracle 12c un pēc tam lietojumprogramma uz 11g.

IEVADS

Mūsdienās informācijas tehnoloģijas un informācijas sistēmu izmantošana sniedz būtiskus atvieglojumus un uzlabojumus dažādās dzīves jomās, tomēr līdz ar IT/IS attīstību un tās priekšrocībām parādās arvien jaunas problēmas un riski. Lai šos riskus un problēmas būtu iespējams kontrolēt, ir nepieciešams pievērst papildu uzmanību IS drošībai. Viena no būtiskākajām problēmām šobrīd ir - vairums uzņēmumu, kuriem ir izstrādātas specializētas IT sistēmas biznesa funkciju veikšanai, neveic pietiekami lielas investīcijas to drošībā. Valda uzskats, ja reiz par tās izstrādi ir samaksāts, tad par tālāku sistēmas attīstību var nedomāt, kas nav korekti. Otra būtiska problēma ir, ka sistēmas izmaiņu veikšanā nav izveidota pilnvērtīga dokumentācija. Tādēļ veicot katras nākamās izmaiņas, sistēma lēnām tiek sagrauta līdz līmenim, ka rezultātā ekonomiski izdevīgāk ir investēt jaunas sistēmas izstrādē un ieviešanā, ne kā mēģināt glābt esošo situāciju.

IT uzņēmumā ir jāattīstās līdz ar biznesa procesu attīstību. Nav ieteicams piekopt praksi, ka sistēmas kļūdas tiek labotas, vai izmaiņas tiek ieviestas uzreiz, tiklīdz sistēma ir izstrādāta un ieviesta uzņēmumā. Lai neveidotos tādas situācijas, ir jābūt pilnvērtīgi izstrādātai sistēmas prasību specifikācijai, programmatūras prasību aprakstam un sistēmas dokumentācijai, kurā tiek atrunātas visas nepieciešamās sistēmas drošības prasības.

Autora darba tēma ir „Uzņēmuma informācijas sistēmu datu zudumu un noplūdes novēršana". Šī tēma ir ļoti aktuāla, jo katru dienu informācijas sistēmās tiek ievadīta arvien jauna informācija, un gan uzņēmumu, gan cilvēku interesēs ir to saglabāt pēc iespējas ilgāk kvalitatīvu un nosargāt tās konfidencialitāti. Tiesa, uzņēmumi nereti neapzinās visus riskus, kādi var rasties IT, un uztic visas informācijas sistēmu drošības prasības sistēmu administratoriem, kas nav korekti, jo bieži uzņēmuma IT personālam nav zināms, kas ir vairāk vai mazāk svarīgs biznesam, kā arī informācijas sistēmu atbildīgajiem cilvēkiem nav tiesību pieņemt nepieciešamos lēmumus.

No iepriekšminētā izriet arī pētāmā problēma par to, kam uzticēt uzņēmumā IS un IT drošību, kas var pieņemt nepieciešamos lēmumus, kā arī kā pasargāt informāciju no tīšas vai netīšas bojāšanas tieši uzņēmuma iekšienē, ja, piemēram, informācijas sistēma to pieļauj dēļ tā, ka nav veikts lietotājiem piešķirto tiesību audits.

Maģistra darba mērķis ir novērtēt uzņēmuma informācijas tehnoloģiju un informācijas sistēmu riskus, un izstrādāt pasākumu plānu to mazināšanā.

Lai sasniegtu izvirzīto mērķi, tika izvirzīti šādi uzdevumi:

- izpētīt esošo praksi IT/IS drošības jautājumos;
- izpētīt, kādi var būt IS drošības riski;

- izpētīt Valsts informācijas sistēmu vispārējās drošības prasības.
- izpētīt biznesa modeli IS drošībai, kas nodrošina sasaisti starp biznesa un IT procesiem;
- izdarīt secinājumus par IS drošības problēmām uzņēmumā.
- izdarīt secinājumus par uzņēmuma IT infrastruktūras drošības riskiem.
- izdarīt secinājumus par uzņēmumā īstenoto informācijas sistēmas atjaunināšanas projektu.

Darbs sastāv no 3 nodaļām.

- Informācijas sistēmu drošība – tiek paskaidrots par informācijas sistēmu drošības organizāciju, kāpēc nepieciešama IS drošība, kādi var būt apdraudējumi. Izklāstīts, kādas ir nepieciešamās drošības prasības, ar ko sākt IS drošības ieviešanai un kādi ir nepieciešamie pasākumi tās īstenošanai. Tiek ietverts jautājums par iespējamiem datu zuduma un noplūdes ceļiem uzņēmumā. Nodaļā veikta izpēte šobrīd aktuālākiem informācijas sistēmas drošības standartiem un LR normatīvam regulējumam, jo labi pārdomāts pamats drošībai ir viens no veidiem, kā uzņēmums labo praksi var ieviest visās struktūrās.
- Drošības organizācijas metodes – sniegti secinājumi par informācijas sistēmu drošības biznesa modeli, kas atbilst Cobit standartam, kādas ir tā priekšrocības attiecībā pret lineāri secīgu modeli. Izklāstīts jautājums par informācijas sistēmu drošības politikas nepieciešamību un jautājumiem, kuriem ir jābūt atrunātiem politikas dokumentā, kādi vēl dokumenti līdz ar drošības politiku uzņēmumā ir jāievieš. Sniegts izklāsts par datu zudumu un noplūdes novēršanas programmatūru. Tiek paskaidrots, kāpēc uzņēmumā svarīgi ir ieviest riska pārvaldības plānu, kādēļ to ir svarīgi aktualizēt regulāri
- Informācijas sistēmas drošības riska mazināšana uzņēmumā – nodaļā veikts IT infrastruktūras raksturojums. Izveidots riska novērtēšanas plāns izmantojot kvantitatīvo metodi atbilstoši ISO standartam. Atbilstoši riska plānam nodaļā veikti secinājumi par uzņēmuma IT/IS drošības riskiem. Veikta uzņēmuma izpēte un aprakstītas konstatētās problēmas, apzināts IS drošības risku mazināšanas plāns un soļi, kurus nepieciešams veikt primāri, lai varētu virzīties uz uzņēmuma vadības izvirzīto mērķi. Veikta analīze sistēmas

datubāzes un lietojumprogrammas atjaunināšanas projektam, kā rezultātā tika samazināts drošības risks sistēmas ievainojamībai un datu integritātei.

Darba izstrādes gaitā ir izmantotas sekojošas pētījuma metodes:

- zinātniskās literatūras pētīšana;
- kontentanalīze;
- kvantitatīvā,
- praktiskā.

Riska pārvaldības plānu var izmantot arī turpmāk uzņēmumi ar līdzīgu daudzumu datiem un sistēmām, attiecīgi to ir iespējams pielāgot. Maģistra darbā ir izdarīti secinājumi par situāciju, kad uzņēmums vēlas ieviest starptautiski atzītu standartu, bet, lai to paveiktu, ir jāanalizē esošā situācija un problēmas, kas pastāv uzņēmumā.

Maģistra darba izstrādē tika izmantoti sekojoši informācijas avoti:

- uzņēmuma, kurā autors strādā, iekšējie, nepublicētie materiāli;
- normatīvie un tiesību akti;
- jaunākā informācija no interneta resursiem, kas saistīta ar IS drošību un datu zudumu, to noplūdes novēršanu;
- autora 2013. gadā izstrādātais diplomdarbs „Datu zuduma un noplūdes novēršana".

1. INFORMĀCIJAS SISTĒMU DROŠĪBA

1.1 Informācijas sistēmu drošības organizācija

Drošībai ir nozīmīga loma sabiedrībā. Visiem uzņēmumiem, kas izmanto IT sistēmas, lai piegādātu vai atbalstītu pakalpojumus klientiem un pārvaldītu to kritiskos datus, ir nepieciešams nodrošināt datu un informācijas sistēmu drošību. Informācijas sistēmu drošību un uzticamību var formulēt vairākās nozīmīgās prasībās:

- konfidencialitāte - piekļuve informācijai, atļauta tikai pilnvarotām personām atkarībā no piešķirtajām tiesībām;
- integritāte - novērst kritisko datu apdraudējumu vai rediģēšanu bez pienācīgas atļaujas;
- piešķirt pieejamību - pilnvarotām personām pēc definētiem kritērijiem piešķirt pieeju pie datiem vai pakalpojumiem;
- sistēmas konfigurācija - nodrošināt to, ka sistēmas vai tīkla konfigurācija tiek mainīta tikai saskaņā ar noteiktajām drošības vadlīnijām un izmaiņas veic pilnvarotie lietotāji.

Parasti drošības prasību izpilde ietver jautājumus, kas saistīti ar personāla vadību, tomēr pieaugošas drošības prasības ir tieši aparatūras un programmatūras nodrošinājumam. Papildus 4 minētajām drošības prasībām ir jābūt pieejamai informācijai par to, kuram ir piekļuve pie informācijas resursiem. (7, 74-75)

No iepriekšminētā izriet, ka drošība ir vairāk nekā aizsargāt klasificētu informāciju no atklāšanas. Klasificēta informācija var būt - komercnoslēpums, loģistikas piegādes ķēdes, darbinieku algu saraksti u.c. Lai nodrošinātu minētās drošības prasības ir nepieciešama virkne drošības pasākumu:

- autentifikācija – process, kurā veic subjekta (*lietotāja*) identitātes pārbaudi datorsistēmā. Tās pamatā ir informācija, ko zina lietotājs - lietotājvārds, parole, pin kods – marķiera (*token*) kods, vai pirkstu nospiedums;
- autorizācija - process, kurā datorsistēma lietotājam nosaka noteiktās pilnvaras un resursus sistēmā, vai veicamo darbību kopumu;
- auditēšana – process, kas veic fiksēšanu katrai darbībai, ko veic lietotājs, pēc nepieciešamības sistēmas administrators var veikt šo ierakstu izskatīšanu;
- nenoliegšana – digitālā paraksta procedūras izmantošana, kas apliecina integritāti dotajos ziņojumos, gan aizsardzību pret nākamajiem mēģinājumiem noliegt autentiskumu. (8, 136)

Līdz ar to drošības pasākumu nodrošināšanā var minēt kriptogrāfiju. Kriptogrāfija nodrošina informācijas šifrēšanu pārraidīšanas laikā pret neatļautu izpaušanu vai viltošanu. Būtisks uzdevums ir arī informācijas aizsardzībai tās glabāšanas laikā, vai kamēr tā tiek apstrādāta. Informācija ir jāaizsargā ne tikai pret nesankcionētu atklāšanu, bet arī pret nesankcionētu modifikāciju, viltošanu un uzbrukumiem, kas cenšas noliegt autorizētu lietotāju piekļuvi tai. Kriptogrāfija spēj nodrošināt vairākas noderīgas iespējas informācijas sistēmu drošībai:

- konfidencialitātes drošību - īpašība, ka informācija tiek aizsargāta no izpaušanas, kas tiek pārraidīta elektroniskajā komunikācijā. Konfidencialitātes drošības prasības ir vistiešākajā veidā saistītas ar datu šifrēšanu;
- autentifikācijas drošību – ar kriptogrāfiju balstīta pārliecība, ka saņemtā identitāte ir spēkā izmantotai informācijas sistēmai, vai personai;
- integritātes pārbaudes – ar kriptogrāfiju balstīta pārliecība, ka ziņa vai fails nav bojāts mainīts, vai viltots;
- elektroniskais paraksts – elektroniski dati, kas pievienoti elektroniskajam dokumentam vai loģiski saistīti ar šo dokumentu, nodrošina elektroniskā dokumenta autentiskumu un apstiprina parakstītāja identitāti. (17)

Svarīgi atcerēties, ka ar informācijas šifrēšanu nerisina sistēmas ievainojamības problēmas, kas ir radušās programmatūras kļūdu rezultātā, tai skaitā tīkla konfigurācijas kļūdas, vai kļūdas pašā kriptogrāfijas programmā. Šifrēšana ir tikai kā metode, kas spēj palielināt informācijas sistēmu drošību. Līdz ar to šifrēšana var būt nepieciešama sastāvdaļa, iepriekš minētajiem, aizsardzības mehānismiem, bet ar pašu šifrēšanu informācijas sistēmu drošībā vien nepietiek.

1.2 IS drošības prasības un pasākumi gala iekārtu drošības nodrošināšanai

Informācijas sistēmu drošība nebeidzas ar informācijas sistēmām, līdz ar to ir nepieciešams saprast kāpēc un kādā veidā ir iespējams nosargāt informāciju.

Autors uzskata, ka eksistē trīs svarīgākās lietas, kas jāievēro:

- datu rezerves kopēšana;
- regulāra programmatūras atjaunošana;
- gala iekārtu drošība (datori, planšetes, viedtālruņi u.c.).

Datu rezerves kopiju veidošanai ir trīs galvenās stratēģijas failu izvēlei, veidojot rezerves kopijas. Kādu stratēģiju izvēlēties ir atkarīgs no tā kā tiek izmantota gala iekārta, cik bieži informācija mainās no izvēlētās rezerves kopēšanas metodes:

- pilna kopija (*full backup*)
- izvēles vai diferenciālā kopija (*selective, differential*);
- papildinošā kopija (*incremental*) (15)

Jāatceras, ka datu kopijas jāaizsargā tāpat kā paši dati, neaizmirstot par mobilo iekārtu drošību, jo uz tām attiecas tie paši drošības noteikumi, kas uz stacionārām iekārtām. Pēc labās prakses piemēriem nepieciešams regulāri pārliecināties, ka no izveidotajām datu rezerves kopijām ir iespējams atjaunot datus. Jo nereti gadās situācijas, ka datu rezerves kopēšana ir veikta, bet, veicot datu atjaunošanu no kopijas procesa vidū var parādīties kļūdas ziņojumi, ka datus nevar nolasīt un tādā gadījumā kopija ir nederīga.

Efektīvai datu rezerves kopēšanai nepieciešams izmantot automatizētos procesus, piemēram, kā vienu no automatizētajiem rīkiem var minēt Windows backup, kas jau ir iebūvēts operētājsistēmā. Eksistē arī speciāla programmatūra, kas labi pilda rezerves kopiju veidošanas procesu operētājsistēmā Windows – Time machine. Otrs veids rezerves kopiju veidošanai ir attālināta datu rezerves kopiju veidošana, kur datņu kopijas tiek glabātas attālināti „mākonī". Pēc autora domām tiešsaistes rezerves kopiju veidošana šobrīd ir ļoti izplatīta tieši mobilām ierīcēm, Bet, ja rezerves kopija tiek glabāta lokāli iekārtā, tā aizņem atmiņu, kas mūsdienās viedtālruņiem ir svarīga un, ja tā tiek sabojāta, vai nozagta, tad no datu rezerves kopijas nav lietderības. Ir izstrādātas dažādas programmatūras, kas veic attālināto tiešsaistes rezerves kopēšanu. Datoriem – JustCloud.com, ZIPCloud, BackuGENIE, SugarSync u.c. Viedierīcēm – iCloud, iTunes, TitaniumBackup, GCloudbackup, CMBackup u.c. Svarīgi atcerēties, ka RAID tehnoloģija, Dropbox, E-dati vai OneDrive nav datu rezerves kopēšana, tās ir datu glabāšanas iespējas.

Lietojuma programmatūras atjaunināšana jāveic regulāri, jo neatjaunināta programmatūra ir vienkāršākais veids kā „uzlauzt" vai piekļūt sistēmas datiem. Ja lietojumprogrammai ir pieejams atjauninājums, tad to nepieciešams uzstādīt iespējami ātri. Windows operētājsistēmas gadījumā tas notiek katra mēneša otrajā otrdienā. Riskantākās lietojumprogrammas, kuras regulāri nepieciešams atjaunināt līdz ko pieejami atjauninājumi ir interneta pārlūki, Java, biroja programmatūra, Acrobat Reader un Adobe Flash.

Gala iekārtu drošība nepieciešama, jo ne vienmēr programmatūras atjaunināšana nozīmē, ka lietojumprogrammas nav „cauras" un tās ir drošas. Biežākie uzbrukuma mērķi parasti ir personīgais dators vai mobilā iekārta, jo uzbrukumu šajās ierīcēs ir grūti konstatēt un nereti tajās ir pieejama hakeriem noderīga informācija – e-pasta autorizācijas dati, maksājumu karšu dati vai kompromitējoši fotoattēli.

Lai novērstu iespējamos draudus, tad datoriem un serveriem nepieciešams obligāti izmantot antivīrusa programmatūru. Tāpat nedrīkst aizmirst par antivīrusa programmatūru E-

pasta serveros un koplietošanas failu serveros. Bet ne vienmēr antivīrusa programmatūra ir efektīva pret iekārtas drošību, tādēļ datoros nedrīkst izmantot nelicencētas programmatūras, kuras ir atkodētas, izmantojot nelegāli iegūtas koda atslēgas, jo bieži ļaunatūra glabājas tieši pašās atslēgās. Nav ieteicams apmeklēt aizdomīgas tīmekļa vietnes, jo nereti tajās var būt ievietoti Adobe Flash reklāmkarogi, kas prasa spraudņu atjaunināšanu un, veicot atjaunināšanu, lietotājs neapzinoties inficē datoru ar ļaunatūru. Datoru un mobilās ierīces ar ļaunatūru var inficēt, atverot speciāli, bojātu biroja dokumentu, PDF, bildi vai video.

Kā piemēru var minēt 2015. gada sākumā izsūtītos e-pastus sk. 1.1 att. vairākiem Latvijas uzņēmumiem saistībā ar neapmaksātu rēķinu, kurā bija pievienota saite uz it kā pašu rēķinu. Saitē atradās saarhivēts fails, kas vizuāli izskatījās pēc PDF faila, lai gan tam bija pievienots izpildāmā (*exe*) faila paplašinājums. Atverot šo failu, darbstacija tiek inficēta ar šifrēšanas ļaunatūru (*Crypto locker*), kuru antivīrusa programmas neuzskatīja par draudu sistēmas drošībai. (37)


Steidzami apmaksājiet rēķinu!

From: ieva meinerte
To: ieva.meinerte@mail.ru
otrdiena, 2015. gada 3. februāris 14:22

Labdien,

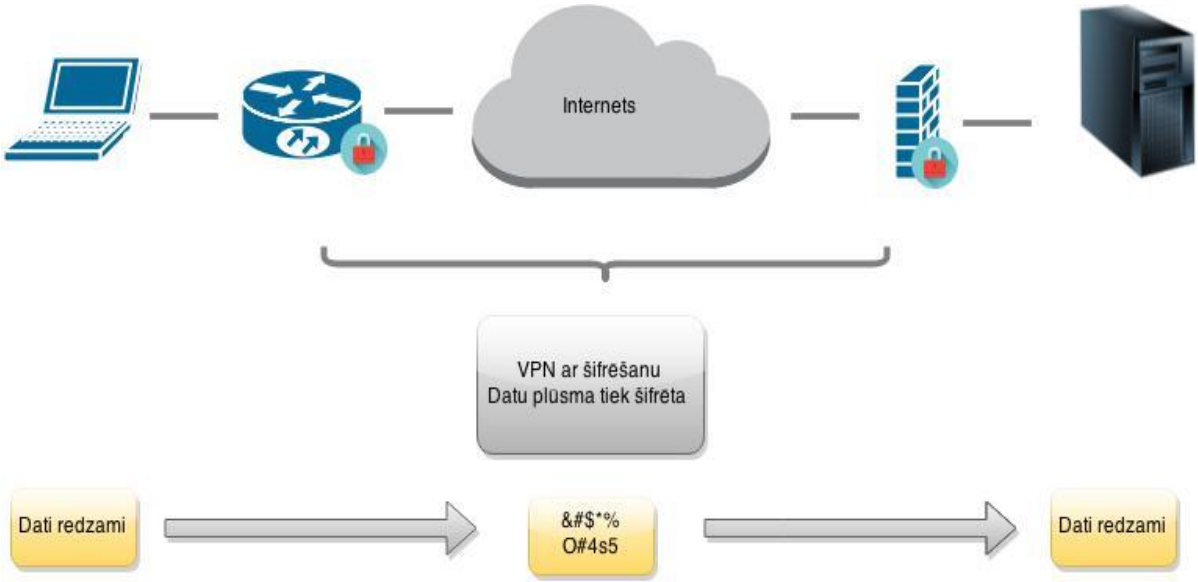
Šis rēķins nav apmaksāts jau 2 mēnešus, lūdzu pārbaudiet to un veiciet maksājumu! Paldies!
Rēķina kopija
http://dokumenti.su/klienti/rekini/pdf.php?id=43bdbef10790

Ar cieņu,
galvenā grāmatvede
+371 26812952
A/S "Elfasar"

1.1 att. **Ekrānšāviņš ar e-pasta ziņojumu ar hipersaiti uz inficētu failu (37)**

Domājot par gala iekārtu ārējo drošību, nav ieteicams pie datora pieslēgt nezināmas izcelsmes iekārtas (zibatmiņas, bezvadu peles, karšu lasītājus u.c.), jo pastāv risks, ka iekārta ir inficēta ar nezināmas izcelsmes programmatūru. Tāpat ja ārpus mājām vai darbavietas nepieciešams izmantot publiskā interneta tīklu, tad bez VPN vai šifrēšanas to nav ieteicams darīt, jo, ja netiek veikta šifrēšana, tad persona, kas ļaunprātīgi izveidojusi tīklu, maršrutēšanas iekārtā var nolasīt visus datus, kas tiek pārsūtīti, piemēram, autorizācijas dati, e-pasta sarakste, vai reāllaika sarakste. (17) Autors 1.2 att. vizuāli ir attēlojis, kā darbojas VPN ar iespējotu šifrēšanu. Nešifrētais teksts tiek kodēts un tad nosūtīts uz serveri vai datoru,

kur savukārt tas tiek atkodēts un ir pieejams. Līdz ar to informācijas pārsūtīšanas laikā tā nav redzama trešajām pusēm, kas var atrasties starp datora un servera savienojumu.

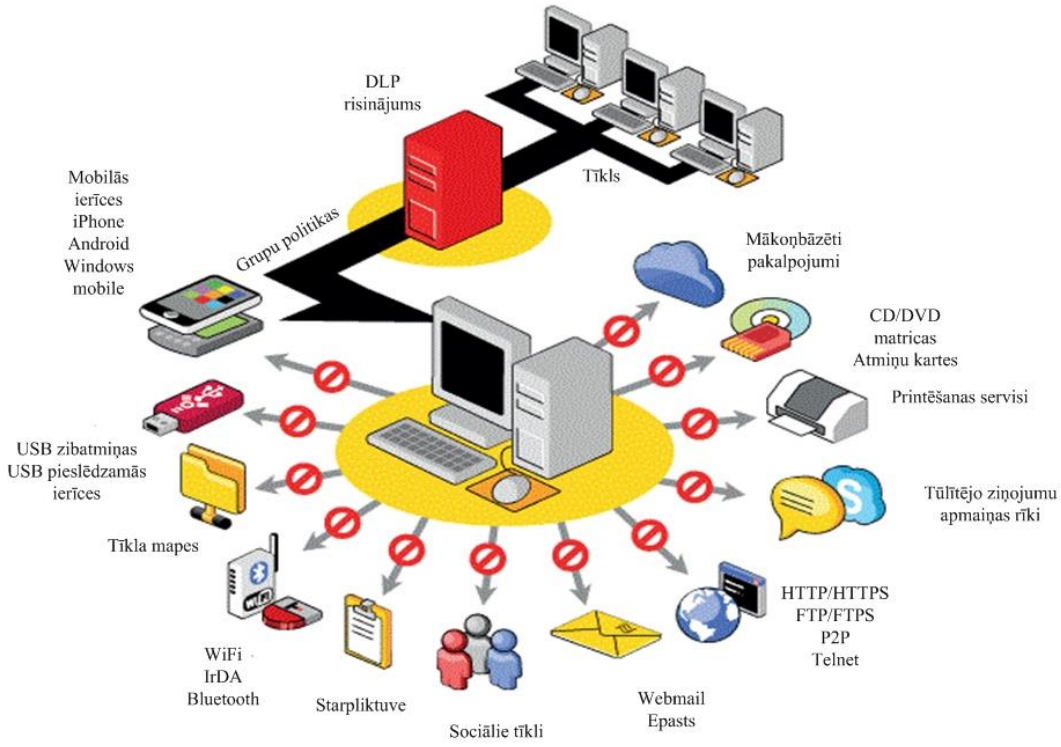


1.2 att. **Shematiski attēlots VPN savienojums ar iespējotu šifrēšanu**

1.3 Datu zuduma un noplūdes iespējamie ceļi uzņēmumā

Ne vienmēr pie datu zudumu un noplūdes uzņēmumā ir vainojamas sistēmas nepilnības. Uzņēmumā var būt ieviesti sarežģīti risinājumi pret neautorizētu piekļuvi pie resursiem no ārpuses, bet uzņēmuma iekšējā tīklā darbiniekiem ir piekļuve pie darbam nepieciešamās informācijas. Mēdz būt gadījumi, ka informācija no uzņēmuma tiek iznesta darbinieku neapzinīgas rīcības dēļ vai ļaunprātīgos nolūkos.

Sensitīvo datu zādzību no uzņēmuma var paveikt dažādos veidos. IT drošības ekspertu vai drošības pārvaldnieka galvenais uzdevums ir izzināt uzņēmuma drošības problēmas, un tā mērķis ir nodrošināt informācijas tehnoloģiju drošību, kā arī pilnveidot esošos aizsardzības mehānismus, samazinot cilvēciskā faktora radītos riskus informācijas tehnoloģiju izmantošanā. 1.3 att. ir attēloti iespējamie drošības trūkumi uzņēmuma IT infrastruktūrā, kurus var izmantot negodprātīgs vai neapzinīgs darbinieks, lai piesavinātos vai iznestu no uzņēmuma svarīgu informāciju. (15)



1.3 att. **Iespējamie drošības riski uzņēmumā datu noplūdei (15)**

Viens no ātrākajiem veidiem, kā nopludināt datus no uzņēmuma, ir, tieši izmantojot iekšējos un ārējos datu nesējus.

Lai novērstu vai mazinātu risku, ka darbinieki apzināti vai neapzināti no uzņēmuma iznes datus, ir radīta specializēta programmatūra Data Loss Prevention, kurai ir spēja aizsargāties pret ārējiem un iekšējiem datu nesējiem, kas zināma kā gala drošība (*endpoint security*). Gala drošība ir viena no primārajām aizsargfunkcijām, jo ārējie un iekšējie datu nesēji, atšķirībā no e-pasta ir daudz ietilpīgāki Risks, ka datu zādzībā, tiks izmantots iekšējais datu nesējs ir mazāks, jo to aizsargā korpuss, lai iegūtu datu nesēju, no sākuma nepieciešams izjaukt gala iekārtu.(41)

Ja uzņēmumā tiek ierobežota piekļuve gala iekārtām pievienot ārējos datu nesējus, tad, vēl joprojām pastāv iespējas nopludināt datus, izmantojot internetā bāzētas metodes, kas ir:

- e-pasts - internetā bāzētu sakaru kanāls, lai nosūtītu informāciju gan pa iekšējo, gan ārējo tīklu. Tomēr datu apjoms, ko var nosūtīt pa e-pastu, ir drauds uzņēmumiem. Reizēm uzņēmumi mēdz ierobežot ziņojumu sūtīšanu uz ārpusi, bet to var piemērot

tikai atsevišķiem darbiniekiem, kuriem darba uzdevumu veikšanai tas nav nepieciešams;

- tūlītējo ziņojumu programmatūra (*Instant Messenger*) - līdzīgi kā e-pasti, arī tūlītējo ziņojumu sūtīšanas programmatūra ir populāra, caur kuru var tikt nopludināta uzņēmumam svarīga informācija. Lielākā daļa programmu atļauj failu apmaiņu starp lietotājiem, tāpēc tam ir jāpievērš papildu uzmanība. Šo programmatūru ir ļoti viegli lietot vidēja līmeņa datora lietotājam. Uzņēmumi sāk aizliegt lietotājiem uzstādīt tādas programmas kā Skype, jo caur to klejo dažāda ļaunatūra, kas var kaitēt gan pašam lietotājam, gan uzņēmumam. Tādēļ sistēmu administratora darbs ir liegt lietotājiem uzstādīt šāda vai cita veida programmatūru;
- P2P (*torrent*) - viens no augstākajiem datu plūsmu kanāliem internetā. Šobrīd šo protokolu izmanto tādas programmas kā µTorrent, BitTorent, eDonkey u.c. Tiesa, šo paņēmienu datu nopludināšanai no uzņēmuma izmanto reti, ja tas ir daudz grūtāk nekā izmantojot e-pastu vai tūlītējo ziņošanas programmatūru. Vairāk tas tiek izmantots, lai iegūtu nelicencētu programmatūru vai ar autortiesībām saistītus, jo bieži saturs tiek izplatīts kopā ar vīrusiem.Ja šāds saturs ir darbinieka datorā, Ekonomikas policijas pārbaudes reizēs uzņēmums var saņemt Administratīvā pārkāpuma protokolus - par autortiesību nemaksāšanu vai pirātisku programmatūru izmantošanu. Šāda pārkāpuma konstatēšana uzņēmumam var radīt nepatīkamu pieredzi un zaudējumus, jo tiek konfiscētas visas atmiņas ierīces, uz kurām ir konstatējama ar autortiesību pārkāpumiem saistīta informācija;
- HTTP/HTTPS- protokols tiek izmantots, galvenokārt, lai lejupielādētu saturu no interneta mājaslapām. Bet tas nodrošina arī iespēju datus nosūtīt uz e-mākoņiem, izmantojot Dropbox vai iCloud servisu. Mākoņpakalpojumu galvenais mērķis un biznesa funkcijas ir uzturēt lietotāju failus pieejamus no dažādām vietām, izmantojot dažādas ierīces, kurām ir interneta savienojums. Līdzīgi kā e-pasta servisu arī HTTP servisu nevar lietotājiem aizliegt, jo darbiniekiem tas ir vajadzīgs, lai iegūtu informāciju veicamajam darbam;
- FTP, SCP – protokoli, kuriem ir jāpievērš tikpat pastiprināta uzmanība kā HTTP/HTTPS protokoliem, jo caur tiem darbinieks var izplatīt uzņēmumam ļoti svarīgu informāciju. Šos protokolus darbiniekiem, līdzīgi kā HTTP nevar aizliegt, jo, veicot darba pienākumus, tie dažkārt mēdz būt nepieciešami. (40)

DLP programmatūras ieviešana uzņēmuma infrastruktūrā ir sarežģīts process, bet tas ir viens no vislabākajiem risinājumiem, kā veikt darbinieku uzraudzību sensitīvas informācijas izplatīšanā. Šāda veida programmatūras ieviešana ekonomiski izdevīga ir lieliem

uzņēmumiem, kas strādā ar ierobežotas piekļuves informāciju, piemēram, bankas. Maziem un vidējiem uzņēmumiem, piemēram, kas darbojas pakalpojumu sniegšanas sfērā, kā alternatīvu datu zudumu un noplūdes novēršanas risinājumiem var minēt sakārtotu pieejas tiesību pārraudzību IT resursos. Bet lai ierobežotu piekļuvi pie nevēlamām interneta vietnēm, ir iespējams veikt uzņēmuma datu plūsmu pārraudzību, iestatot uzņēmuma tīkla maršrutētājā pārraudzīšanas un filtrēšanas funkciju.

Ar jautājumu, kas tad īsti ir svarīgu datu un informācijas aizsardzība, katram uzņēmumam izpratne par to ir atšķirīga, tomēr parasti par svarīgiem un sensitīviem datiem tiek uzskatīta personiskā un darba informācija - kredītkaršu, personas kodi vai bankas kontu numuri, un lielākajā daļā uzņēmumu arī intelektuālais īpašums un ar komercnoslēpumiem saistīta informācija. To visu kontrolē fiziskām personām Fizisko personu datu aizsardzības likums (2) un juridiskām personām Komerclikums. (1)

Konfidenciālas informācijas un datu zudums var radīt kaitējumu ne vien pašam uzņēmumam un tā darbiniekiem, bet arī klientiem. B2B International pēc Kaspersky Lab pasūtījuma veiktā pētījuma rezultāti liecina, ka visbiežāk tiek zaudēta informācija, kas satur ziņas par klientiem, kā arī finanšu datiem kopā 36% gadījumu. Tam ar nelielu intervālu seko darbinieku dati, kuru zādzība vai zudums novērots 31% gadījumu.

Svarīgas informācijas un datu noplūdi var izraisīt gan ārējie, gan iekšējie faktori. 35% IT speciālistu apstiprināja, ka viņu uzņēmumā datu zudums noticis, inficējoties ar kaitīgām programmām — tas ir viens no visbiežāk sastopamajiem ārējiem apdraudējumiem. Visizplatītāko noplūdes cēloņu saraksta otrajā vietā atrodas uzbrukumi ar e-pasta izmantošanu 21%, bet trešajā — pikšķerēšana 17%. Apskatot jautājumu par iekšējiem draudiem, svarīgu datu un informācijas zudumu visbiežāk izraisa ievainojamību klātbūtne uzņēmuma izmantotajā programmnodrošinājumā, tas sastāda 25%. Pēc pētījuma 23% aptaujāto norādīja, ka noplūdes cēlonis ir bijusi arī darbinieka tālruņa vai planšetdatora nozaudēšana, bet 15% — mobilās ierīces zādzība. 13% gadījumu svarīga informācija ir nonākusi svešās rokās neuzmanības dēļ, piemēram, nosūtot e-pastu vai īsziņas uz nepareizām e-pasta adresēm un numuriem.(39)

Veiktais pētījums spilgti demonstrē, ka, attīstoties informācijas tehnoloģijām, kā arī, nodrošinot lietotājiem, nepārtrauktu piekļuvi informācijas sistēmām, ir būtiski pieaudzis informācijas drošības apdraudējums, līdz ar to uzņēmumiem ir ļoti svarīgi nosargāt informācijas sistēmu un datu drošību.

1.4 LR normatīvais regulējums un standarti informācijas sistēmu drošībai

Lai nodrošinātu uzņēmuma informācijas sistēmu drošību un mazinātu riskus datu zudumu un noplūdes iespējamībai ir izstrādāti vairāki rekomendējoši standarti, kas nosaka, kā organizēt IT drošību uzņēmumā. Standarti un vadlīnijas ir radītas arī tādēļ, ka mūsdienās ir neiespējami iegādāties no viena ražotāja uzņēmumam visas IT infrastruktūrā nepieciešamās iekārtas un programmatūru. Ir daudz dažādu ražotāju un izstrādātāju, kas piedāvā IT risinājumus uzņēmumiem. Standarti ir nepieciešami, lai radītu konkurenci programmatūras ražotāju un iekārtu ražotāju tirgū, kā arī tie nodrošina tehnoloģiju mijiedarbību savā starpā. **Standarts** ir starptautiski atzītu institūciju izstrādāts un apstiprināts dokuments, kas ietver vispārējus noteikumus vai norādījumus dažāda veida darbībām, un ir vērsts uz optimālas sakārtotības pakāpi noteiktā jomā. (25)

Lai IT sniegtu ieguldījumu uzņēmuma biznesa mērķu sasniegšanā, tad svarīgi ir sakārtot un optimizēt biznesa procesus uzņēmumā. Tas nozīmē, ka uzņēmumā, attīstoties biznesam, ir jāattīstās arī IT/IS risinājumiem un pārvaldībai. IT pakalpojumu pārvaldības un biznesa savstarpējās attiecības ir plaši aprakstījis Robs Addijs (*Rob Addy*) savā grāmatā, kurā viņš ir teicis:

"IT Service Management is the planned and controlled utilisation of IT assets (including systems, infrastructure and tools), people and processes to support the operational needs of the business as efficiently as possible whilst ensuring that the organisation has the ability to quickly and effectively react to unplanned events, changing circumstances and new business requirements as well as continuously evaluating its processes and performance in order to identify and implement opportunities for improvement." („IT pakalpojumu vadība ir plānota un pārraudzīta IT resursu (iekļaujot sistēmas, infrastruktūru un tās rīkus) cilvēku un procesu atbalstīšana, lai radītu pēc iespējas efektīvāku atbalstu biznesa attīstībai, tai pašā laikā rūpējoties par organizācijas spēju ātri un efektīvi reaģēt uz neparedzētiem notikumiem, mainīgiem apstākļiem un jaunām biznesa prasībām, kā arī nepārtraukti novērtēt tās procesus un sniegumu ar mērķi identificēt un radīt izaugsmes iespējas"). (5, 46)

Savukārt, kas attiecas uz LR normatīvo regulējumu, tad vidējiem un mazajiem uzņēmumiem, kā arī valsts un pašvaldību iestādēm, ja vien tie nav finanšu un kapitāla tirgus dalībnieki vai arī to pārraudzībā nav valsts informācijas sistēmas drošības nepieciešamību nosaka nozares standarti, rekomendācijas un vadlīnijas. No tā izriet, ka IS drošību uzņēmumā vai valsts iestādē tiek reglamentēta ar:

- finanšu un kapitāla tirgus komisijas (FKTK) informācijas sistēmu drošības normatīviem noteikumiem (ja tie ir finanšu un kapitāla tirgus dalībnieki);

- valsts informāciju sistēmu vispārējās drošības prasībām;
- fizisko personu datu aizsardzības likumu.

Finanšu un kapitāla tirgus komisijas informācijas sistēmu drošības noteikumi nosaka, prasību minimumu IS drošībai tirgus dalībniekiem ar mērķi ierobežot tirgus dalībnieku darbību, klientiem nodrošināto pakalpojumu izmantojamo informācijas sistēmu riskus, tiecoties uz piesardzīgu risku pārvaldības līmeni, nosakot vienotas un strukturētas prasības tā dalībnieku IS drošībai. Noteikumi reglamentē un tirgus dalībniekiem ir jāievēro:

- informācijas sistēmu drošības organizēšana;
- informācijas sistēmu resursu pārvaldība;
- risku analīze un pārvaldība;
- personāla loma informācijas sistēmu drošībā;
- fiziskās un vides drošības pārvaldība;
- informācijas sistēmu pieejas tiesību pārvaldība;
- komunikāciju un operāciju pārvaldība;
- attālināto pakalpojumu drošības pārvaldība;
- informācijas sistēmu izstrāde un izmaiņu pārvaldība;
- incidentu pārvaldība.

Noteikumos ir minēts, ka tirgus dalībnieks var ieviest arī papildu aizsardzības pasākumus atkarībā no informācijas resursu klasifikācijas līmeņa un veiktās risku analīzes, ņemot vērā uzņēmuma sniegtos pakalpojumus, darbinieku skaitu un informācijas tehnoloģiju izmantošanas līmeni. (4)

Kopumā drošības noteikumi detalizēti apraksta FKTK dalībnieku IS drošības sfēras organizēšanu uzņēmumā, ņemot vērā uzņēmuma sniegtos pakalpojumus un IT tehnoloģiju izmantošanas līmeni.

Izpētot **Ministru kabineta noteikumus Nr. 765 (Valsts informāciju sistēmu vispārējās drošības prasības)** informācijas sistēmu drošību nepieciešams organizēt, sākot ar IS drošības politikas izveidi, risku analīzi, informācijas klasifikāciju, IS drošības un lietošanas noteikumu izveidi, darbības atjaunošanas un nepārtrauktības plāna izstrādi, kā arī darbinieku informēšanu un regulārām apmācībām drošības jautājumos. Noteikumi reglamentē vispārējās drošības prasības valstiskās nozīmes informācijas sistēmu pārvaldībai. (3)

Salīdzinot ar FKTK informācijas sistēmu drošības noteikumiem, šie noteikumi nav detalizēti, bet tie pieprasa IS drošības apdraudējumu tuvošanās pazīmju detalizētu uzskaitījumu.

Pateicoties informācijas tehnoloģiju attīstībai, ir mainījušās iespējas sniegt un saņemt dažādus pakalpojumus, turklāt palielinājušās iespējas sniegt un saņemt dažādus pakalpojumus virtuālā vidē. Tas savukārt uzņēmumiem un valsts iestādēm ir radījis izaicinājumu nodrošināt drošību sniegto pakalpojumu ietvaros, kas attiecas uz fizisko personu datu apstrādi un aizsardzību.

Fizisko personu datu drošību nosaka **Fizisko personu datu aizsardzības likums**, kura uzraudzību veic Datu valsts inspekcija. Par fizisko personu datu aizsardzību ir atbildīgs personas datu aizsardzības speciālists. Personas datu speciālists var būt uzņēmumā konkrēti norīkots darbinieks, kas ir atbildīgs par personu datu aizsardzību, vai uzņēmums var izmantot ārpakalpojumu sniegtos pakalpojumus attiecībā uz personas datu aizsardzību un apstrādi. Datu aizsardzības speciālista kvalifikāciju piešķir Datu valsts inspekcija, kad konkrētā persona ir nokārtojusi pārbaudījumu. Personas datu aizsardzības speciālists nav obligāta normatīvajos aktos noteikta prasība, bet par veikto personas datu apstrādi ir atbildīgs katrs uzņēmuma vadītājs. (38)

Ja uzņēmuma rīcībā ir informācija par darbiniekiem, klientiem, kas ir fiziskas personas, tad ir jānodrošina, ka informācija tiek aizsargāta ievērojot likumā noteiktās normas:

- apstrādāt tikai tādu informāciju, kas ir nepieciešama kādam konkrētam mērķim;
- nodrošināt drošību;
- pārliecināties, ka informācija ir aktuāla un saistoša;
- nodrošināt datu subjekta tiesības, nodrošinot piekļuvi personas datiem;
- saglabāt tikai tik daudz informācijas, cik nepieciešams, un tik ilgu laiku posmu, cik nepieciešams konkrētā mērķa sasniegšanai. (2)

FKTK informācijas sistēmu drošības noteikumos ir teikts, ka uzņēmums vai iestāde, kas ir tās tirgus dalībnieki var ieviest arī papildus drošības prasība, tas pats attiecas arī uzņēmumiem un valsts iestādēm. Līdz ar to papildus drošības prasības, kādas uzņēmums vai iestāde var ieviest, ir starptautiski atzīti standarti vai labā prakse, kas ir cieši saistītas. Veicot standartu izpēti, tika secināts, ka uz IT drošību attiecas vairākas metodes un vadlīnijas:

- ISO/IEC standarti (27001, 27002, 13335, 2000);
- IT Infrastructure Library (ITIL);
- Control Objectives for Information and related Technology (CobiT) (31)

Standarts **ISO/IEC 27002:2013** attiecas uz labas prakses kodeksu informācijas sistēmu drošības pārvaldībai un ir paredzēts kā kopīgs pamats un praktiskas vadlīnijas, lai attīstītu organizatorisko nodrošinājumu standartus un efektīvu pārvaldības praksi. Standarts nosaka pamatnostādnes un labās prakses ieteikumus 14 drošības jomās:

- informācijas drošības politika;
- informācijas drošības organizēšana;
- cilvēku resursu drošība;
- aktīvu pārvaldība;
- piekļuves kontrole;
- kriptogrāfija;
- fiziskā un vides drošība;
- darbības ar drošības procedūrām un pienākumi, aizsardzība pret ļaunprātīgu programmatūru, rezerves kopēšana, žurnālfailu sagatavošana un žurnalēšanas uzraudzība, tehniskās ievainojamības vadība un IS audita koordinēšana;
- komunikācijas drošība – tīkla drošības pārvaldība un informācijas nodošana;
- sistēmas iegāde, uzturēšana un izstrāde – drošības prasības informācijas sistēmās, drošības attīstība un atbalsta procesu testēšana;
- informācijas sistēmu izstrādātāja/piegādātāja attiecības un pakalpojumu sniegšanas vadība;
- informācijas drošības incidentu pārvaldība – IS drošības incidentu vadība un uzlabošana;
- informācijas drošības aspekti biznesa nepārtrauktības pārvaldība, IS drošības nepārtrauktība, darbinieku atbrīvošana no darba;
- atbilstība – atbilstība tiesību aktiem un līgumu prasībām atbilstoši informācijas drošības pārskatiem. (19)

Kopumā standarts nosaka un izklāsta ieteicamos drošības kontroles pasākumus katrā jomā. Kā labo praksi nosakot tieši informācijas drošības kontroli. Standartā skaidrotā labā prakse sniedz norādījumus un ieteikumus, lai īstenotu drošības pasākumu ieviešanu uzņēmumā.

Standarts **ISO/IEC 27001:2013** precizē prasību specifikāciju izveidi, ieviešanu, darbību, uzraudzību, pārskatīšanu un uzlabotu dokumentētu informācijas drošības pārvaldību uzņēmumā. Tā mērķis ir nodrošināt, ka tiek atlasīta atbilstoša un samērīgi laba drošības kontrole, lai aizsargātu informāciju. Šis standarts parasti ir piemērojams visiem organizāciju veidiem, arī valsts iestādēm. Dokuments satur desmit īsas klauzulas, kurās ietverta:

- standarta darbības jomas;
- dokumenta atsauces;
- atkārtojums noteikumiem un definīcijām ISO / IEC 27000;
- organizatoriskā struktūra un ieinteresētās personas;

- informācijas drošības vadība un augsta līmeņa atbalsts drošības politikai;
- informācijas drošības vadības sistēmu plānošana, risku novērtēšana, risku mazināšana;
- informācijas drošības sistēmu atbalsts;
- padarīt informācijas drošības sistēmas funkcionēt spējīgas;
- sistēmas veiktspējas pārskats;
- koriģējoši pasākumi. (20)

Izstrādājot Valsts informācijas sistēmu drošības noteikumus, tajos ir netieši ietvertas standarta klauzulas, līdz ar to uzņēmums, plānojot ieviest standartu, par pamatu var ņemt MK noteikumus neiegādājoties standarta dokumentu. Standarts galvenokārt ietver prasības loģiskas un saprotamas informācijas drošības vadības sistēmas izveidošanai, kurā ir ietverta gan informācijas aktīvu aizsardzība gan tehniskos, gan organizatoriskos un administratīvos aspektos.

Par pamatu standarta ieviešanai tiek ņemts risku analīzes rezultātā izveidots risku pārvaldības plāns. Ieviešot šo standartu, uzņēmumā galvenokārt tiek nodrošināta darbības pamatprocesu pilnveidošana, nodrošinot informācijas konfidencialitāti, integritāti un pieejamību. Standarts nodrošina sadarbības partneriem un klientiem uzņēmuma nopietno pieeju biznesam, kā arī neatkarīgas trešās puses (auditoru) apliecinājumu, ka uzņēmumā ieviestā informācijas drošības vadības sistēmas atbilst starptautiskā standarta prasībām.

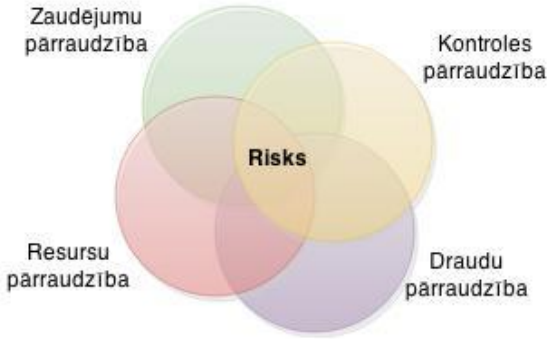
Standarts **ISO/IEC 27005:2011** nosaka jēdzienus un modeļus kā panākt pamata izpratni par IKT drošību, kā arī nosaka vispārējos vadības jautājumus, kas ir būtiski, lai veiksmīgi plānotu un īstenotu IKT drošību organizācijā.

Izpētot standartu, tapa skaidrs, ka tas balstās uz 27001 un 27002 izstrādātajām norādēm saistībā ar IS drošību, bet pievēršot uzmanību padziļinātiem riska vadības aspektiem att.1.4., kuros ietverta – zaudējumu, kontroles, draudu un resursu pārraudzība. Drošības pārvaldība uzņēmumiem ļauj novērtēt informācijas apdraudējuma riskus.

Standarts palīdz izveidot, un ieviest atbilstošu kontroli pār konfidenciālu informāciju uzņēmumā saglabājot tās integritāti un pieejamību. Standarts neprecizē un neiesaka izmantot kādu konkrētu riska vadības metodi, tomēr tas nosaka nepārtrauktu procesu, kas sastāv no strukturētām secīgām darbībām:

- izveidot riska pārvaldības modeli ietverot darbības jomu, pieejas un metodes, kuras jāizmanto;

- kvantitatīvi un kvalitatīvi novērtēt saistītos riskus, ņemot vērā informācijas kopumu, draudus un ievainojamību, lai noteiktu varbūtību incidentiem un ietekmi uz uzņēmuma biznesa darbību;
- draudu noteikšana informācijas un datu integritātes saglabāšanai;
- risku uzraudzība un risku mazināšana, atbilstoša riska identificēšanai un darbībai. (21)



1.4 att. **Riska vadības aspekti pēc ISO 27000(42)**

Viens no populārākiem standartiem uz kura pamata daudzi uzņēmi veido IT organizācijas attīstību ir **ITIL (*Information Technology Infrastructure Library*) vai ISO/IEC 20000 series** pakalpojumu pārvaldības labākās prakses ieteikumi un apkopojums. Standarts plaši tiek izmantots visā pasaulē, jo augstas kvalitātes IT pakalpojumu nodrošināšana balstīta uz integrētu procesu kopas izveidi.

Pēc būtības ITIL ir dokumentu kopums, kas apraksta labas prakses veidus IT pakalpojumu sniegšanas jomā. Svarīgākie ir desmit galvenie procesi, kas nodrošina IT pakalpojumus:

- incidentu pārvaldības process;
- problēmu pārvaldības process;
- konfigurācijas pārvaldības process;
- izmaiņu vadības process;
- darbinieku atbrīvošanas vadība;
- pakalpojumu līmeņa pārvaldības process;
- jaudas jeb resursu pārvaldība;
- pieejamības pārvaldība;
- nepārtrauktības pārvaldība;
- finanšu vadības procesi.

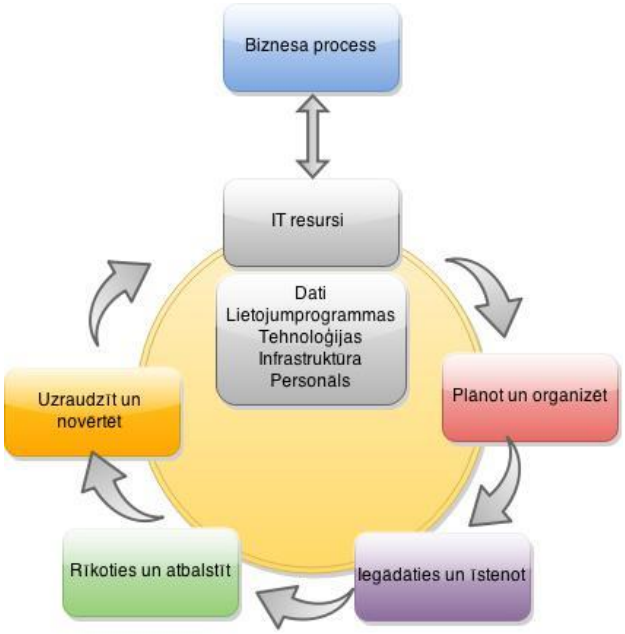
ITIL un ITSM (*IT Service Management*) procesos svarīgu lomu spēlē IT palīdzības dienests.(22) ITSM iesaka koncentrēties uz klienta vajadzībām un biznesa procesiem, nevis uz tehnoloģiju sniegtajiem pakalpojumiem. Šajā gadījumā organizācijas procesu pakalpojumu sniegšanai un pieejamībai iepriekš tiek definēts SLA (*Service Level Agreement*) un veiktspējas parametriem KPI (*Key performance indicator*), kas ļauj IT departamentam sniegt augsta līmeņa pakalpojumus, nosakot to kvalitāti un uzlabojot to. (22)

ITIL ieviešanu uzņēmumā ir iespējams attēlot, kā uzrādīts att. 1.5, kurā redzams, ka no sākuma uzņēmumam ir nepieciešams definēt mērķi, tālāk tiek īstenota stratēģija biznesa procesu izvērtēšanai un pielāgošanai IT. Kad konkrētie soļi ir paveikti, tikai tad var sākties ieviešanas taktikas izvēle un IT servisa nodrošināšana darbiniekiem atbilstoši ITIL standartiem. (26)

1.5 att. **ITIL ieviešana uzņēmumā stratēģija(26)**

Standartus ne vienmēr vajag aprakstīt dokumentos, tos var arī ilustrēt, to pierāda **COBIT (*Control Objectives for Information and Related Technology*)**, kuru plaši izmanto tieši IT auditori. Tas ir augsta līmeņa procesu modelis, kas IT/IS aktivitāšu spektru apraksta ar procesiem. Procesu modelis sevi ir pierādījis, kā teicams audita rīks, jo tas spēj piedāvāt procesa unificētu struktūru, kura ļauj novērtēt IT kapacitāti.

Biznesa orientācija tiek veidota saistot biznesa mērķus ar IT mērķiem, nodrošinot metriku un termiņus, lai novērtētu to sasniegšanu, un nosakot saistītos pienākumus biznesam un IT procesa īpašniekiem. COBIT tiek ilustrēts ar procesa modeli, kā redzams attēlā 1.6, kas sadala IT četrās jomās - plānot un organizēt, iegādāties un īstenot, rīkoties un atbalstīt, uzraudzīt un novērtēt, un 34 apakšprocesi, kas sakrīt ar atbildības lomām: plānot, būvēt, vadīt un uzraudzīt. COBIT darbojas kā integrācija visu minēto vadības materiālu apkopošanai, kurā galvenie mērķi ir zem viena jumta, kas sasaista labās prakses modeļus ar pārvaldības un biznesa prasībām. (27)



1.6 att. **COBIT ilustrācija (27)**

Izpētot standarta procesa shēmas, tik secināts, ka Cobit standarts savā ziņā ir unikāls, jo tas der un ir paredzēts gan uzņēmuma vadībai, gan lietotājiem, gan IS drošības auditoriem. Standarta pamatā ir sniegt uzņēmuma vadībai pārliecību par IT ieguldījumu lietderību biznesā. Lietotājiem tas sniedz iespēju pārliecināties par izmantoto IT resursu drošību savukārt auditoriem tas piedāvā rīkus kontroles mehānismu pārbaudei un uzņēmuma vadības informēšanai.

Lai nodrošinātu biznesa sasaisti ar IT, tad standartā galvenais priekšnosacījums ir izvirzīts, ka biznesa un IT puses vienādā mērā jānodrošina ar informāciju, balstoties uz savstarpēju komunikāciju.

Lai gan Cobit standartā tieši ir izteikta galvenā prasība, ka starp biznesu un IT pusēm ir jābūt informācijas apmaiņai, tad ISO standartos tas tiek pieņemts par pašsaprotamu, jo standarta ieviešanas pamatā ir izstrādāt pilnvērtīgu riska pārraudzību.

2. DROŠĪBAS ORGANIZĀCIJAS METODES

Tālākajā maģistra darba nodaļā ir izpētītas metodes un izdarīti secinājumi, ar ko sākt, lai uzņēmumā būtu iespēja veikt informācijas sistēmu drošības riska mazināšanu, vadoties pēc, IS drošības standartiem, tādējādi mēģinot identificēt, kādi nepieciešamie pasākumi būs nepieciešami ISO 27001 standarta ieviešanai uzņēmumā. Nodaļā apskatīta informācija saistībā ar biznesa modeļa pielāgošanu IS drošības prasībām IS drošības politikas, noteikumu un biznesa nepārtrauktības un atjaunošanas plāna izstrādei. Nodaļā iekļauta papildus risinājuma analīze, kas neļauj no organizācijas iznest uzņēmumam piederošu informāciju, kas ir uzskatāms, kā papildus drošības pasākums datu zudumu un noplūdes novēršanai tieši no uzņēmuma darbinieku. Risinājums iekļauts nodaļā, jo, vadoties pēc autora pieredzes, bieži risku analīzēs pieminēts datu zudumu un noplūdes ceļš, par kuru atbildība jāuzņemas galvenokārt uzņēmuma darbiniekiem un sistēmas lietotājiem.

2.1 Biznesa modelis informācijas sistēmu drošībai

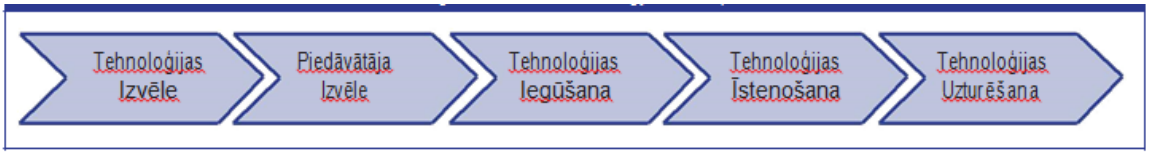
Svarīgākais, lai veicinātu un radītu dinamiski sasaistītu sistēmu ar biznesu, atgūtu veiktos ieguldījumus sistēmas izstrādē, un sasniegtu biznesa mērķus, ir veikt biznesa procesu pārskatīšanu un atbilstības izvērtējumu. Tas nozīmē, ka uzņēmumā vispirms ir jāsaprot attiecības starp biznesa procesu un tehnoloģijas elementiem. Dinamiska sasaiste starp biznesu un IT ir pamats uzņēmuma attīstībai. Ieviešot jaunus IT risinājumus, tie ir jāizvēlas, jānovērtē, jāīsteno un jākontrolē. Tas pats attiecas uz biznesa procesiem. Tos nepieciešams projektēt, izstrādāt, ieviest un izmantot. Mūsdienās vairums uzņēmumu daudz pūļu velta tieši IT risinājumu pielāgošanai biznesam, jo sākotnēji nav veikts izpētes darbs un uzņēmuma vadība vaino IT, ka pietrūkst risinājumu tehnoloģiju. Lai gan realitātē ir gluži pretēji - uzņēmumā ir pietiekoši tehnoloģiskie resursi, bet pats bizness nepietiekamai atbalsta esošos procesus. (43) Kā piemēru minētajiem apgalvojumiem var minēt uzņēmumu, kurā autors strādā. Izstrādājot un ieviešot sistēmu, netika ņemts vērā LR normatīvais regulējums un pārvalžu prasības, līdz ar to sistēma pašā saknē bija izveidota nepareizi. Sistēmai ir izstrādāta nepilnvērtīga lietotājiem grūti saprotama saskarne, kā arī nepilnvērtīga sistēmas integrācija ar grāmatvedības sistēmu. Šāda situācija radās, jo sistēmas izstrādātājs neveica savstarpējo komunikāciju ar uzņēmumu, un ar grāmatvedības sistēmas uzturētāju.

Vadoties pēc COBIT standarta metodoloģijām, tad to pamatā ir biznesa sasaiste ar IT. Lai to nodrošinātu, tad uzņēmumā ir jābūt stratēģiskās vadības mehānismam, kurš nosaka:

- uzņēmumā ir izstrādāti stratēģiskie plāni, kuros ir novērtēta uzņēmuma pašreizējā situācija un noteikti uzņēmuma darbības mērķi noteikto funkciju veikšanai;

- atbilstoši uzņēmuma stratēģiskajā plānā noteiktām attīstības vajadzībām ir izveidota IS stratēģija, kurā noteikta informācijas tehnoloģiju attīstības vajadzības;
- informācijas tehnoloģiju stratēģijas īstenošanai uzņēmumā ir izstrādāts stratēģijas ieviešanas plāns. Tajā noteikti plānotie darbi, iesaistītās uzņēmuma struktūrvienības, un paredzētas regulāras progresa ziņojumu izstrādes par darbu izpildes gaitu.

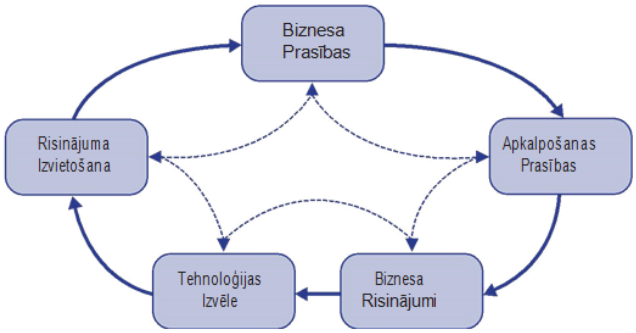
Pēc ISACA veiktā pētījuma liela daļa uzņēmumu koncentrējas tieši uz tehnoloģijām, nevis uz sapratni par biznesu, kur konkrēta tehnoloģija būtu vispiemērotākā. Uzņēmumu skatījums uz tehnoloģiju piedāvājumu tirgū ir lineārs, kā uzrādīts attēlā 2.1. (43)



2.1 att. **Lineārais tehnoloģiju ieviešanas process uzņēmumā(29)**

Šī procesa karte ir secīga un taisna bez atgriezeniskās saites. Kad risinājums ir iegūts uzņēmumi izmanto pārdevēja atbalstu tās īstenošanai. Reizēm uzņēmumi samazina vai pat vispār atsakās no pārdevēja atbalsta. Zināšanu un dokumentu apmaiņa tiek ignorēta, nosakot problēmas tehnoloģijā un tās labojot atbilstoši tiem biznesa procesiem, kas ir dzīvē. Sistemātiskās domāšanas lineārais modelis neatrisina nevienu no problēmām, kas rodas no secīgu tehnoloģisku risinājumu ieviešanas un uzturēšanas.

IS biznesa drošības modelim ir jāsniedz atgriezeniskā saite, kā rezultātā IT spēj pielāgoties biznesa prasībām, jo katrā no posmiem notiek savstarpēja komunikācija. Attēlā 2.2 ir attēlots process, kā tiek veikta IT risinājumu ieviešana uzņēmumā, viss sākas ar prasību specifikācijas izstrādi, kurā tiek definētas biznesa prasības. Nākamajos procesa etapos tiek veikta apkalpošanas prasību un biznesa risinājumu specifikācija. Pēc šo soļu paveikšanas tikai tad tiek veikta tehnoloģijas izvēle un risinājuma izstrāde.



2.2 att. **Sistemātiska procesa cikla darbība uzņēmumā(29)**

Papildus biznesa modelī tiek nodrošināta cilpa, kas ļauj atgriezties pie iepriekšējiem posmiem, kas vajadzīgi, lai sistemātiski varētu pielāgot, kādu no soļiem IS izstrādes ciklā. Piemēram, ja tehnoloģijas risinājums šķiet neskaidrs vai nepietiekami definēts, biznesa risinājums ir jāpārskata, lai nodrošinātu saskaņošanu. Ja biznesa risinājums ir nesaprotams vai rada jautājumus var būt nepieciešams doties atpakaļ uz sākotnējo pakalpojuma prasību formulējumu, vai pat visaptverošām biznesa prasībām. Biznesa modeļa diagramma nav pakāpeniska risinājuma ieviešanas secība, kas uzrādīta attēlā 2.1. Šī ir sistemātiska cikla darbība, kurā neviens solis vai cilpa nebeidzas, jo visi pasākumi mijiedarbojas kopējā ķēdē, kurā var mainīt tehnoloģiju risinājumus to ieviešanai dzīvē. (6)

Tehnoloģijas izvēle un īstenošana ir daļa no biznesa risinājuma, jo process ir ciklisks, kas ļauj nodrošināt atbilstošu risinājumu komponentu pielāgošanu procesā. Process palīdz nodrošināt visaptverošu un līdzsvarotu viedokli par tehnoloģiju iespējām paplašināties. Modelis nav tendēts uz pilnīgu automatizāciju, bet gan koncentrēšanos uz iespēju pilnveidoties, attīstīties izmantojot tehnoloģiskos risinājumus. (12)

Secinājumi

Procesu plānošana ir veids, kā pilnveidot biznesa mērķus un īstenot izvēlēto stratēģiju, jo bez mērķiem procesi ir maz noderīgi. Tas pats attiecas uz tehnoloģijām, kurām nav vērtības, ja tās neļauj uzņēmumam sasniegt mērķus un īstenot stratēģiju. No visa minētā izriet, ka pastāv sadarbības atkarība starp procesu un tehnoloģijas elementiem, kas padara to grūti izolējamu vienu no otra. Iespējošana un atbalsts starp sistēmu risinājumiem ir cieši saistītas divvirzienu attiecības, kuras var saprast tikai tad, kad tiek piemēroti trīs sistēmu domāšanas bloki - atgriezeniskā saite, līdzsvars un kavēšanās.

Lai veiktu uzņēmuma biznesa procesu pielāgošanu IS drošībai att. 2.2, tad par pamatu būtu nepieciešams ņemt COBIT standartus, jo tie ir grafiski attēloti ar procesu shēmām, kur katram apvienotajam procesam tiek noteikti atbilstoši kontroles mērķi. Biznesa prasībās definējot uzņēmuma vadības atbildību par uzņēmuma politiku. Apkalpošanas prasībās definējot ekspluatācijas personāla darba uzdevumus. Biznesa risinājumos definējot informācijas prasību specifikācijas definīcijas. Tehnoloģijas izvēlē definējot tehnoloģiskās infrastruktūras plānu. Risinājuma izvietošanā definējot galvenās esošo sistēmu izmaiņas.

2.2 IS drošības politika

Kā vienu no pamatiem uzņēmuma IS drošības organizēšanā var minēt drošības politikas izveidi, kas ir iekļauta ISO 27000 drošības standartu dokumentos. Drošības politika ir kā noteikumi IS pārvaldei, kurā atrunātas prasības, kā uzņēmumā tiek organizēta IS/IT drošība.

Būtiskas kļūdas IS drošības ieviešanā ir darbinieku neinformēšana par drošības politiku un noteikumiem un uzņēmumā nav nozīmēta atbildīgā persona/s par IS drošību. Līdz ar to var veidoties situācijas, ka IS pārvaldes cilvēki nezina, kas ir vairāk vai mazāk svarīgs biznesam, kā arī viņiem nav tiesību pieņemt nepieciešamos lēmumus. Tādēļ ir jānodala drošības kontroles funkcijas no izpildes funkcijām.

Drošības politikai ir jānosaka:

- IS drošības pārvaldības principus;
- kas ir atbildīgs par IS drošību uzņēmumā;
- uz ko attiecas IS drošība;
- kādi dokumenti reglamentē IS drošību uzņēmumā;
- kā jāveic risku analīze uzņēmumā;
- kā nepieciešams klasificēt informāciju;
- kā nepieciešams veikt pārbaudes, auditus vai testus.

Drošības politikas mērķi un pamatnostādnes ir noteikt drošības politikas vadlīnijas informācijas sistēmā, samazinot drošības ievainojamību un incidentu ietekmi uz uzņēmuma darbību. Tāpat, kā riska plānu arī drošības politiku un ar to saistītos iekšējos dokumentus nepieciešams regulāri pārskatīt, ja:

- mainās uzņēmuma IS iekļautās informācijas apjoms un nozīmīgums vai informācijas sistēmā tiek veiktas būtiskas izmaiņas;
- tiek konstatēti drošības incidenti, kuri nav iekļauti drošības politikā ietvertajā darbības apjomā.

Informācijas sistēmas drošības politika attiecas uz visu uzņēmuma personālu, kam ir dota pieeja informācijas sistēmai, resursiem un informācijai, kā arī ārējiem pakalpojumu sniedzējiem, kas ir iesaistītas uzņēmuma IS darbībā, uzturēšanā vai informācijas apstrādē.

Uzņēmumā nepieciešams iecelt atbildīgo, kas nodrošina regulāru risku analīzi un pārvaldības plāna atjaunināšanu, informācijas resursu klasificēšanu un risku pārvaldības plāna efektivitātes izvērtēšanu. Svarīga drošības politikas dokumenta sastāvdaļa ir izskaidrot, ko nozīmē minētās definīcijas politikas dokumentā.

Piemēram:

- uzņēmuma IS – vairāku informācijas sistēmu un tajās uzglabātās informācijas kopums, kas nodrošina pamatfunkciju veikšanu;

- informācijas resurss - tehniskais resurss, dokumentācija, dati vai cita veida informācija, datu nesēji vai apstrādes sistēmas, kas ir iesaistītas uzņēmuma IS vai IT resursu nodrošināšanā;
- komponente - daļa no uzņēmuma informācijas sistēmas;
- drošības incidents - notikums, kas skar informācijas vai informācijas sistēmas drošību. Incidents var būt konfidencialitātes, informācijas veseluma vai pieejamības zudums, kas izraisījis sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai kura dēļ piekļūšana IS ir traucēta vai neiespējama;
- informācijas lietotājs - personāls, kuram ir piekļuve IS vai IT resursiem un tajā glabātajai informācijai.(34)

Uzņēmuma informācijas resursiem jābūt pieejamiem lietotājiem tikai atbilstoši nepieciešamo darba vai citu uzdoto pienākumu veikšanai. Gadījumā, kad lietotājam ir pieejama informācija, kas tam nav nepieciešama pienākumu veikšanai tas, ir uzskatāms par drošības incidentu.

Par uzņēmuma IS darbības nodrošināšanu un drošības prasību ievērošanu parasti atbild drošības pārvaldnieks, kuram nepieciešams nodrošināt ar informācijas drošību saistīto iekšējo dokumentu uzturēšanu, kā arī organizēt ar sistēmas lietošanu saistīto pasākumu izpildi un lēmumu pieņemšanu par nepieciešamajām darbībām risku pārvaldības plānā minēto pasākumu īstenošanai. Par drošību atbildīgajai personai nepieciešams nodrošināt skaidras prasības informācijas sistēmas resursu izmantošanā, lai samazinātu drošības incidentu iestāšanās varbūtību un to atstātās sekas uz uzņēmuma IS un darbiniekiem. Papildus tiek koordinētas piekļuves tiesības, informācijas saturs un klasifikācija informācijas resursa ietvaros, incidentu un problēmu pārvaldības procedūras, izmaiņu pārvaldības procedūras, komunikācija ar trešajām pusēm saistībā ar informācijas resursiem un ar resursu uzturēšanu un attīstību saistītie jautājumi. Atbildīgajam par Drošību ir jāidentificē drošības incidenti un jānodrošina to izmeklēšana. Papildus par IS drošību ir atbildīgi IS lietotāji, kuri tiešo darba pienākumu veikšanā ievēro ar IS darbību saistītos noteikumus, un viņiem ir pienākums informēt IS drošības pārvaldnieku par identificētajiem drošības incidentiem, kā arī ir jāsniedz visa nepieciešamā informācija negadījumu izmeklēšanā.

Informācijas sistēmas drošības politika nosaka drošības uzņēmuma pamatprincipus, kas saistīti ar:

- regulāru, ar drošību saistīto dokumentu, informācijas resursu un tehnisko resursu testēšanu un pārbaudi;

- drošības prasību ievērošanu pievienojot IS jaunus resursus un citas informācijas sistēmas, ja tādas ir radušās;
- ar informācijas drošību saistīto risku identificēšanu, izvērtēšanu un darbību veikšanu risku iestāšanās atstāto seku novēršanā.

Uzņēmumos informācijas sistēmu saistītie iekšējie dokumenti parasti ir - informācijas sistēmas drošības un lietošanas noteikumi, informācijas sistēmas drošības risku pārvaldības plāns un darbības nepārtrauktības un atjaunošanas plāns. (18)

Secinājumi

Pēc iepriekš minētā, mēģinot attēlot drošības politikas hierarhiju, tai būtu nepieciešams izskatīties, kā ir norādīts attēlā 2.3. Diagramma ir izveidota atbilstoši saistošām uzņēmuma prasībām, kas vēlas ieviest ISO 27001 standartu IS drošības pārvaldībai. Diagramma uzrāda sākotnējos soļus, ar ko nepieciešams sākt, lai izveidotu veiksmīgu drošības politiku uzņēmumā, kas kalpotu kā pamats turpmākai IS/IT drošības organizēšanai uzņēmumā.

2.3 att. **Drošības politikas diagrammas attēlojums**

2.3 IS drošības noteikumi

Uzņēmumā, lai aizsargātu tās esošās informācijas sistēmas nepieciešams izstrādāt IS drošības noteikumus, kas nosaka pasākumus drošības risku mazināšanai. To mērķis ir definēt uzņēmuma IS fiziskās un loģiskās aizsardzības, informācijas pieejamības, kā arī informācijas uzglabāšanas prasības, lai izvairītos no tehniskajiem, cilvēciskajiem un apkārtējās vides faktoriem. Ja uzņēmumā ir IS drošības pārvaldnieks, tad noteikumu izstrādi veic viņš, sadarbojoties ar tehnoloģisko resursu turētājiem. Ja uzņēmumā nav atbildīgā par IS drošību, tad par drošības noteikumiem atbildību ir jāuzņemas IS pārvaldes vadītājam. Tāpat noteikumu izstrāde ir saistīta ar darbības nepārtrauktības un atjaunošanas plānu, jo noteikumos vēlams attēlot informāciju par konkrētā resursa dīkstāves atļauto ilgumu, kā arī ietekmi uz lietotājiem.

Pēc autora domām, IS drošības noteikumiem ir jāsatur informācija par IS informācijas resursu izveidošanu, papildināšanu, apstrādi, glabāšanu, atjaunošanu un iznīcināšanu. Atsevišķās sadaļās jāiekļauj punkti par IS informācijas un tehnisko resursu lietošanu un kontroli, piekļuve uzņēmuma IS informācijas un tehniskajiem resursiem, IS rezerves kopiju izgatavošanas un uzglabāšanas nosacījumiem, datu nesēju lietošanu, IS informācijas resursu aizsardzību, papildus jāiekļauj informāciju par drošības pārvaldību. Papildus noteikumos var iekļaut informāciju par biznesa nepārtrauktības plānu un informāciju, kas jādara, ja uzņēmumā ir ierobežota piekļuve IS resursiem, vai tie nav vispār pieejami. (18)

Lai sāktu drošības noteikumu izveidi no sākuma nepieciešams klasificēt informāciju pēc:

- konfidencialitātes – publiska / iekšējas lietošanas/ konfidenciāla;
- pieejamības - kad pieejama / cik ilgi var būt nepieejama;
- vērtības - kādi zaudējumi ir ja informācija tiek pazaudēta / sagrozīta / nopludināta.

Noteikumos jābūt atrunātām procedūrām, kā tiek veiktas IS/IT izmaiņas un, kādai dokumentācijai ir obligāti jābūt. Piemēram, tas var būt sistēmas projektējuma apraksts, risku pārvaldības plāns, vai darbības nepārtrauktības plāns. Noteikumu pielikumā vēlams uzrādīt riska pārvaldības un darbības nepārtrauktības plāna atsauces uz resursa dokumentu. Svarīgi ir minēt IS informācijas un tehnisko resursu lietošanas un kontroles noteikumus, ka konkrēto sistēmu ir atļauts lietot tikai tiem paredzētajiem mērķiem un lietotājiem veicamajiem darba pienākumiem. Noteikumos obligāti ir jāiekļauj sadaļa par lietotāja tiesību piešķiršanu attiecīgajam resursam, kā arī procedūru, kas uzņēmumā drīkst pieprasīt lietotājiem piešķirt tiesības. Noteikumu neatņemama sastāvdaļa ir incidentu pārvaldības sadaļai, kurā tiek norādīti resursa adrese vai e-pasta adrese, uz kuru ir iespējams ziņot, ja tiek konstatētas problēmas resursu darbībā. Tāpat nedrīkst aizmirst minēt noteikumus, kas jāievēro attiecībā uz IT/IS resursu fizisko drošību, piemēram, resursi ir izvietoti speciālās telpās, kurās ir nodrošināta aizsardzība un brīdināšanas sistēma par šādiem apdraudējumiem - dūmi, īpaši paaugstināta vai pazemināta temperatūra, neautorizēta fiziska piekļuve vai resursu zādzība, kā arī tehniskie resursi ir aizsargāti no elektroenerģijas padeves zudumiem vai pārsprieguma/ zemsprieguma ar atbilstošu tehnoloģiju. (34)

Secinājumi

Lai IS drošības noteikumi būtu pilnvērtīgi un aktuāli, tad tajos noteikti jābūt atsaucēm uz sistēmas lietošanas noteikumiem, ja tādu nav, vai tie neatbilst pastāvošajai situācijai, tad tie ir jāaktualizē. Sistēmas lietošanas noteikumi tiek veidoti pamatā no sistēmas projektējuma

apraksta. IS drošības noteikumi ir kā pamats IS pārvaldes darbam, jo tajos tiek atrunātas problēmu pieteikšanas procedūras un lietotāju atbildība. Kopumā noteikumi nodala uzņēmuma lietotāju atbildību no IS pārvaldes atbildības.

2.4 Biznesa nepārtrauktības un atjaunošanas plāns, IS uzskaitījums

BCP (*Business continuity plan*) un DRP (*Disaster recovery plan*) plānam jāsatur pasākumu kopums problēmu novēršanai vai preventīvas darbības, kuras samazina iespējamos riskus IT dīkstāvei. Bez uzņēmuma izvirzītām prioritātēm par IS drošību atbildīgajiem ir neiespējams plānot IT sistēmu darbības nepārtrauktību, tādēļ plāna izstrādē ir nepieciešama cieša uzņēmuma darbinieku un IT personāla sadarbība. Biznesa nepārtrauktības un atjaunošanas plānā ir jānosaka:

- informācijas sistēmu informācijas un tehnisko resursu atjaunošanas pasākumi, kas veicami pēc sistēmas incidenta, kā arī jānorāda kontrollaiki, cik ilgi resurss var būt nepieejams;
- informācijas sistēmu atjaunošanas pasākumu procedūru soļi, kurus nepieciešams veikt, resursa pieejamības atjaunošanai;
- informācijas sistēmu atjaunošanas pasākumos iesaistīto atbildīgo personu darbības instrukcijas, ja resursu uztur ārpakalpojuma sniedzēji. (34)

Ilustrējot plāna izstrādi, kā redzams attēlā 2.4 pirmajā daļā, ir veicama analīze, kurā tiek uzskaitīti tehniskie resursi un informācijas sistēmas, kuras uzņēmumā ir apzinātas un detalizēti raksturotas. Otrajā daļā tiek minēts tehnisko resursu un informācijas sistēmu darbības atjaunošanas plāna procedūras, ar kurām var veikt resursa pieejamības atjaunošanu. Trešajā un ceturtajā daļā tiek ieviests risinājums un veikta tā testēšana. Piektajā daļā plāns ir sagatavots un tiek veikta tā uzturēšana atbilstoši aktuālai informācijai uzņēmumā.

2.4 att. **Biznesa nepārtrauktības plāns uzņēmumā(35)**

Veicot IS resursu uzskaitījumu, ko nepieciešams iekļaut biznesa nepārtrauktības plānā, var izmantot valsts informācijas sistēmu drošības standartu, jo Ministru kabineta noteikumi Nr.765 par Valsts informācijas sistēmu vispārējās drošības prasībām netieši ietver ISO 27001 standarta prasības. Pēc valsts informācijas sistēmu drošības prasībām, biznesa nepārtrauktības plānā tehnoloģiskajām iekārtām jābūt norādītam iekārtas nosaukumam un atrašanās vietai. Tāpat ir jābūt informācijai par interneta pieslēgumu, kā arī par atjaunošanas laiku. Papildus nepieciešams uzskaitījums par uzņēmuma pārvaldībā esošajiem serveriem, un vēlams iekļaut informāciju par lietotāju darbstacijām. Sk. Tab. Nr. 2.1. Papildus plānā nepieciešams norādīt datu apstrādi, uzglabāšanu un rezerves kopēšanu, piemēram, uzņēmuma dati tiek uzglabāti un apstrādāti disku masīva iekārtā, un datu rezerves kopēšana tiek veikta uz lentām, attiecīgi norādot iekārtas nosaukumu un rezerves kopiju veidošanas biežumu, kā arī uzglabāšanas laiku.

2.1. tabula

Biznesa nepārtrauktības plāna tehnoloģisko iekārtu uzskaitījums uzņēmuma biznesa nepārtrauktības plānā

Modelis	**Procesors (CPU)**	**Atmiņa (RAM)**	**Cietie diski (HDD) un RAID**	**Operētāj-sistēma**	**Iekārtas kods**	**Garantijas saistības līdz**
IBM x3850 X5	2xXeon 4C E7520 95W 1.86GHz/18 MB	64 GB DDR3-SDRAM	Dinamiski – kopējais disku masīvs 4TB	Windows Server 2008 R2	7145-2RG	

Tehnoloģisko resursu un informācijas sistēmu darbības atjaunošana sadaļā tab. Nr. 2.2. tiek aprakstīti infrastruktūras atjaunošanas soļi, kā rīkoties, ja iestājās kāds no uzskaitītajiem negadījumiem:

- iekārta pilnībā iziet no ierindas;
- informācijas sistēma nav pieejama;
- informācijas sistēmas dati ir izdzēsti vai sabojāti;
- atjaunošanas procedūru testēšana.

Uzskaitījuma tabulā Nr.2.2 tiek norādīts attiecīgais resurss, tā atjaunošanas soļi, atbildīgā persona un atjaunošanas laiks. (3)

2.2. tabula

Informācijas resursu uzskaitījumu tabula un to atjaunošanas veicamie soļi uzņēmuma biznesa nepārtrauktības plānā

Atjaunošanas soļi	**Atbildīgais**	**Atjaunošanas laiks**
1. Bojājums tiek reģistrēts incidentu pieteikšanas sistēmā 2. Atbildīgais sazinās ar ārpakalpojumu sniedzēju pa telefonu vai e-pastu.		

Secinājumi

Izstrādājot biznesa nepārtrauktības un atjaunošanas plānu par pamatu nepieciešams ņemt uzņēmumā visu informācijas sistēmu un tehnoloģisko iekārtu uzskaitījumu. Ja tāds uzskaitījums nav izveidots, tad BCP un DRP plānu nav iespējams sastādīt kvalitatīvu. Līdz ar to, kā pamatu tehnoloģisko un informācijas sistēmu uzskaitījumam var minēt pilnvērtīgu IS/IT audita veikšanu uzņēmumā, kas sniegs informāciju par tehnoloģiskajām iekārtām un to sasaisti. Ja auditā ir paredzēts noskaidrot informācijas sistēmu savstarpējo sasaisti un uzskaitījumu, tad, ja nav pieejama sistēmu dokumentācija tas ir laikietilpīgs darbs, jo ir nepieciešams veikt sistēmas pamatfunkciju izpēti, kā arī apzināt lietotājus uzņēmumā, kas strādā ar šo sistēmu.

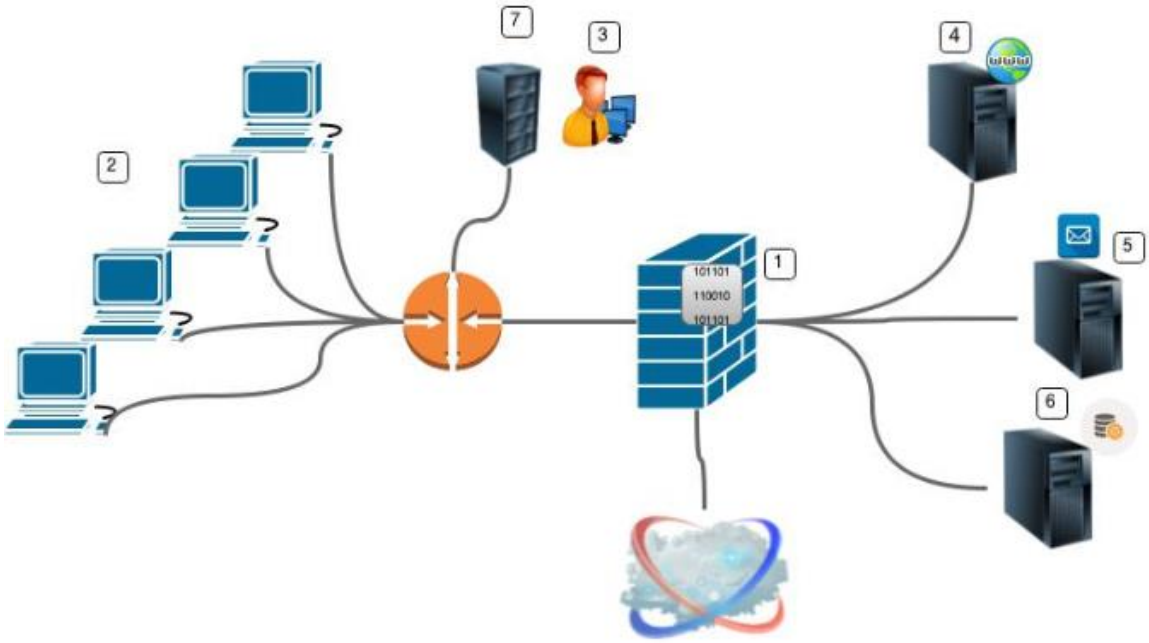
2.5 DLP programmatūra

Ja uzņēmumā ir ieviesti visi drošības standarti un sistēmas ir nodrošinātas, tāpat pastāv risks, ka no uzņēmuma var tikt nopludināta svarīga informācija. Līdz ar to ir izstrādāta specializēta programmatūra, kas spēj noteikt potenciālos datu aizsardzības pasākumus.

Termini "datu zudums" un "datu noplūde" ir cieši saistīti, un bieži tiek izmantoti pamīšus, lai gan pēc būtības tie ir nedaudz atšķirīgi. Datu zudumu incidenti pārvērtīsies datu noplūdes incidentu gadījumā, kad resursi, kas satur konfidenciālu informāciju, ir zaudēti un tie ir nonākuši trešo personu rīcībā. Tomēr datu noplūde ir iespējama arī tad, ja dati netiek zaudēti datu izcelsmes, rašanās pusē. Ir izstrādātas arī citas programmas, kas saistītas ar datu noplūdes novēršanu un informācijas noplūdes atklāšanu un novēršanu - IDLP (*Information Leak Detection and Prevention*), informācijas noplūdes novēršana ILP (*Information Leak Prevention*), satura uzraudzība un filtrēšana CMF (*Content Monitoring and Filtering*), informācijas aizsardzība un kontrole IPC (*Information Protection and Control*) un

štancēšanas novēršanas sistēma EPS (*Extrusion Prevention System*). Apakšnodaļā izdarīsim secinājumus par datu zuduma un noplūdes programmu, jo tā ietver datu skenēšanas un aizsardzības funkcijas attiecībā uz ievadītajiem kritērijiem, kurus definē sistēmas administrators. (17)

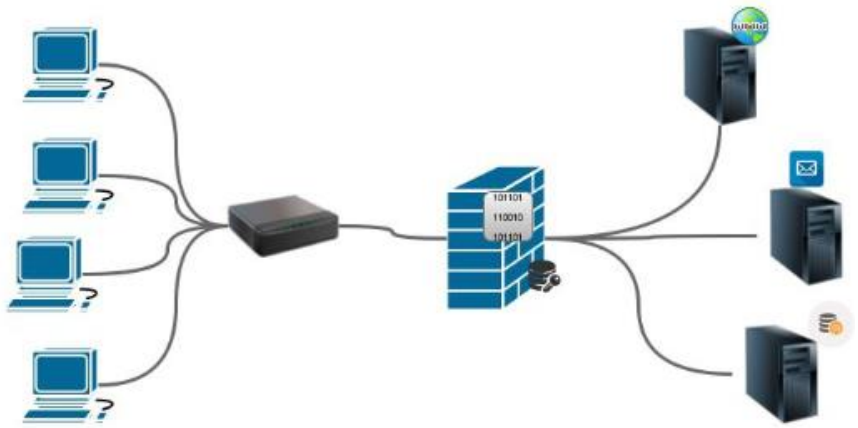
Standarta shēma, lai gūtu izpratni kā darbojas DLP programmatūra datortīklā skat. 2.5 att.



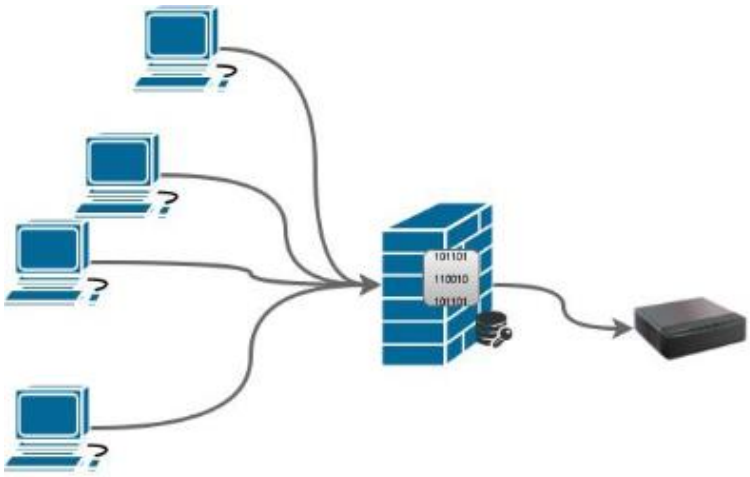
*2.5 att.***DLP programmatūras iespējamais novietojums uzņēmumā(9)**

- Skat. Att. 2.5 datu zudumu novēršanas programmatūra ir iespējota uz drošības vārtiem **1**(*security gateway*). Tas padara to par DLP vārteju;
- Izmantojot drošības pārvaldes serveri **3**, lai uzstādītu un konfigurētu DLP vārtejas politiku;
- DLP vārteja **1** izmanto iestatītos datu veidus un noteikumus, kas nodrošina datu zuduma novēršanu. To var izmantot AD vai LDAP serveri **6,** lai noteiktu iekšējo organizāciju. Tas pārauga tīkla datu plūsmu un pārtver datus vai informāciju, kura ir iestatīta DLP vārtejas politikā kā slepena. Tādējādi dati, kas iet uz HTTP **4** vai pasta serveri **5** tiek pārtverti. DLP programmatūra var skenēt arī tīkla iekšējo datu plūsmu starp lietotājiem skat. 2.6 un 2.7 att., kā arī sūtīto e-pastu pielikumus. Ja dati neatbilst nevienai no iestatītajām politikām DLP programmatūrā tiem tiek atļauts atstāt organizācijas tīklu.
- DLP programmatūras monitorings, kurā var redzēt visu notikumu izsekošanu un iegūt atskaites par incidentiem par katru lietotāju notiek uz DLP sistēmas administratora

darba stacijas **7**, uz kuras ir uzstādīts konkrētās DLP programmatūras vadības panelis.(9, 147)



*2.6 att.***DLP sistēma aizsargā datu zudumus starp uzņēmuma departamentiem (9)**



*2.7 att.***DLP programmatūra uzstādīta starp lietotājiem un Switch aizsargājot apakštīklu (9)**

DLP programmatūra nepārtraukti skenē un pārbauda tīkla datu plūsmu pret datu zudumiem, un vai tas sakrīt ar noteikto politiku:

1) Starpgadījums tiek piefiksēts, un konkrētie dati tiek uzglabāti speciāli tam atvēlētā krātuvē, kurā tiek uzglabāti DLP sistēmas žurnālfaili;
2) Drošības noteikumi - ja tie ir iestatīti uz to, lai tikai piefiksētu starpgadījumu, tad lietotājs, kurš veicis pārkāpumu e-pastā parasti saņem ziņojumu, ka konkrētā darbība ir piefiksēta un ierakstīta. Ja drošības noteikumos ir noteikts, ka lietotājs ir tikai jāinformē, tad elektroniskajā pastā tiek saņemts ziņojums un dati, kas sūtīti ir atstājuši uzņēmumu. Ja drošības politikā ir noteikts, ka lietotājam ir jājautā vai viņš vēlas, lai piefiksētie dati atstāj uzņēmumu un tas tiek piefiksēts žurnālfailos, vai atceļot faili netiek nosūtīti un paliek uzņēmumā. (9, 147)

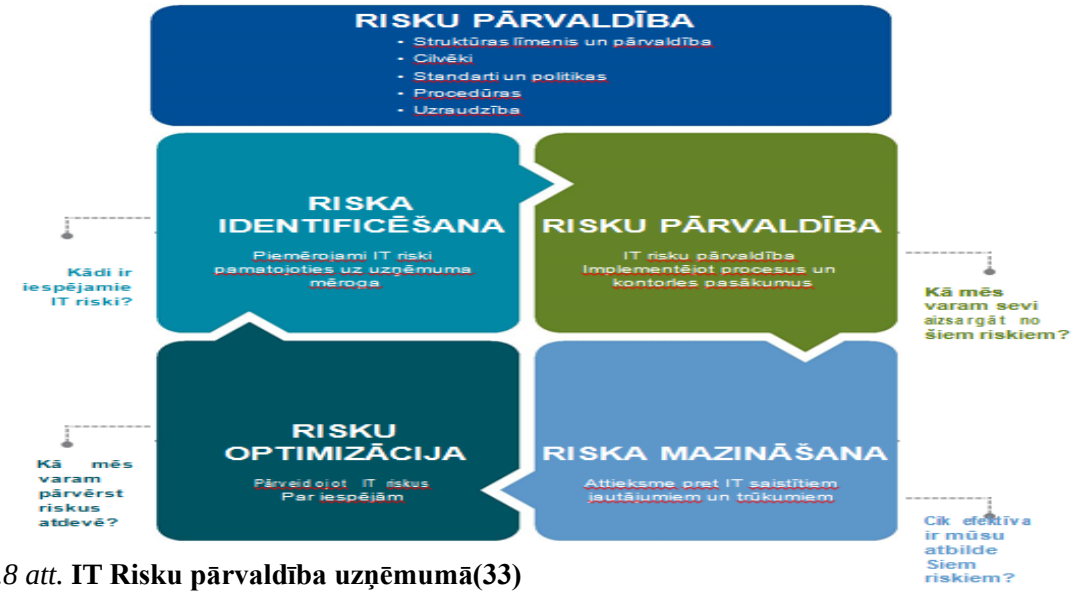
Secinājumi

Ieviešot DLP programmatūru uzņēmuma tīklā, kā labo praksi var minēt lietotāju informēšanu, ka informācija var saturēt uzņēmuma konfidenciālus datus. DLP sistēmas drošības noteikumos tiek iestatīti tikai informatīvi paziņojumi darbiniekiem. Tādā veidā tiek panākts, ka lietotāji laika gaitā sāk piedomāt, vai konkrēto materiālu ir nepieciešams sūtīt, vai darba materiālus ņemt uz mājām. Iestatot sistēmu uz šādiem parametriem lietotājiem, tiek nodrošināts pārejas periods. Jo ja tiks ieviesta sistēma un uzreiz aizliegts konkrētus datus iznest ārpus uzņēmuma, tad pieaugs neapmierinātība, un IS pārvalde uzņēmumā tiks uzskatīta kā traucēklis uzņēmuma darbiniekiem konkrēto darba pienākumu veikšanai.

2.6 IT risku pārvaldība

IT loma pēdējos gados organizācijās ir pārveidojusies un tā vairs nesniedz tikai atbalstu uzņēmējdarbībā. IT uzņēmumiem nodrošina daudzas konkurētspējīgas priekšrocības. Tā rezultātā IT ir stratēģisks biznesa attīstības veicinātājs nevis izmaksu centrs. Līdz ar to skats uz IT risku uzņēmumā ir attīstījies, jo tehnoloģiju risks aptver daudzus organizatoriskos aspektus. Līdz ar to, lai mazinātu riskus, ir nepieciešams iekšējais audits uzņēmējdarbībai un tehnoloģijas darbībai, lai spētu identificēt riskus un izstrādātu risku mazināšanas plānu.

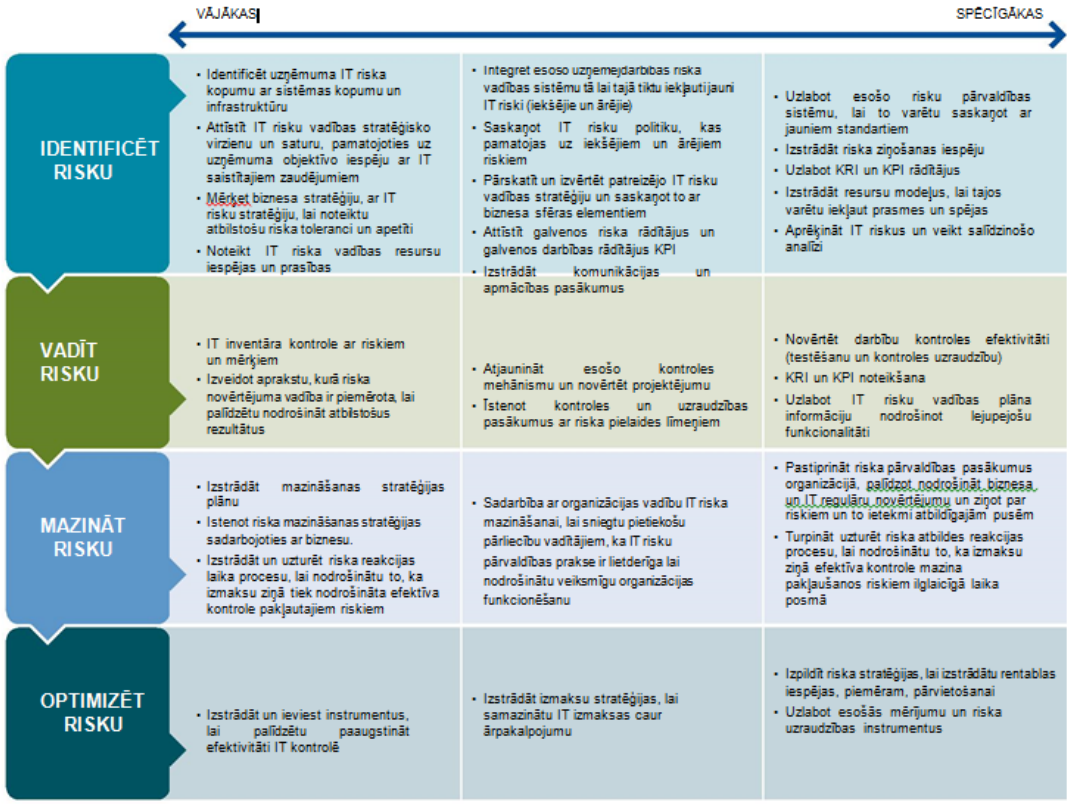
IT risku pārvaldība uzņēmuma ietvaros darbojas kā atsevišķa, bet integrēta funkcija tajā. Attēlā 2.8 vizuāli attēlota IT risku pārvaldības shēma. Tā atbalsta uzņēmumu kopumā un virza to uz vienotu stratēģisko mērķi, misiju un biznesa modeli. IT riska pārvaldības funkcijas pārvalda galvenos IT apdraudējumus ar, ko uzņēmums var, vai saskaras un vada preventīvu reakciju, lai apkarotu vai mazinātu šos draudus. Efektīva riska pārvaldība nodrošina stabilu un efektīvu sadarbību ar regulatīvām iestādēm, lai noteiktu atbilstību prioritātes katrā jurisdikcijā. (14)



2.8 att. **IT Risku pārvaldība uzņēmumā(33)**

IT risku pārvaldības funkciju izlīdzināšana ar citām riska uzraudzības funkcijām, piemēram, iekšējā audita, uzņēmuma riska pārvaldība un atbilstību ir svarīgs elements, lai efektīvāk nodrošinātu, ka riski tiek optimizēti.

Koordinēta risku pārvaldība ļauj plūst skaidrai un saprotamai informācijas plūsmai IT jautājumos. Uzņēmumiem ir jānovērtē riski un jāizstrādā risku optimizācijas stratēģijas, nosakot un nodrošinot plaša riska optimizācijas programmas att. 2.9. Tās nepieciešamas, lai izstrādātu mērījumu rīkus, kas spētu novērtēt IT riskus, bet tas nav tikai noteikt risku skaitliskā lielumā un ziņot par to, tas attiecas arī uz resursu optimizēšanu, kas veltītu risku vadībai saistībā ar biznesa procesu ietekmes prioritātēm.(33)



2.9 att. **IT Risku identificēšana uzņēmumā(33)**

Katru gadu mainoties drošības risku sarakstam, ar kuriem nākas saskarties uzņēmumiem, lielākie būtiskākie draudi IS drošībai 2014. un 2015. gadā Pēc KPMG datiem ir:

- darbiniekiem tendence lietot savas iekārtas. Darbinieki arvien vairāk darbā izmanto personīgos viedtālruņus planšetdatorus un tas ievērojami palielina risku, ka ierīces tiek inficētas ar dažādām ļaunatūrām un spiegprogrammām vai no tām tiek nozagti dati, kas parasti nav šifrēti;
- internetam pieslēgto ierīču un tehnoloģiju paplašināšanās - jaunu tehnoloģiju ieviešana var pakļaut ierīces draudiem, jo jaunu drošības risinājumu izstrādei ir nepieciešams ilgāks laiks nekā jaunu ierīču sagatavošanai. Uzņēmumu pieejas

sistēmas un u.c. līdzīgas sistēmas var sniegt urķiem vērtīgu informāciju un neskaitāmas iespējas veikt uzbrukumus pret uzņēmumu. Mērķu sasniegšanai kibernoziedznieki izmanto jaunās tehnoloģijas un IT ievainojamības;

- mākoņskaitļošanas pakalpojumu datu privātums un aizsardzība - kļūst arvien svarīgāk nodrošināt mākonī saglabātās informācijas aizsardzību, jo kibernoziedznieki meklē dažādas ievainojamības pakalpojumu sniedzēju tīklos un cenšas izmantot drošības nepilnības, lai iegūtu svarīgus datus;
- Java un citas programmatūras ievainojamības - Java vēljoprojām ir nedroša programmatūra, un tās drošības nepilnības ir viegli izmantot. Lielākā daļa uzņēmumi apzinās nepilnības, tomēr ir tādi, kas neuzstāda jaunākās programmu versijas vai jauninājumus, kas tās novērstu. Kā piemēru var minēt, ka Oracle BI Discoverer V10 neatbalsta pēdējo Javas atjauninājumu uz 8. versiju, un atjaunināt Discoverer versiju uz 11g nav iespējams iekams uzņēmums neveic IS datubāzes un lietojumprogrammas atjaunināšanu;
- datu apmaiņas risks - kibernoziedznieki parasti uzbrūk vājākajam ķēdes posmam uzņēmumā. Parasti korporatīvās IT sistēmas ir labi nodrošinātas, tomēr to vai datu drošību ir iespējams nodrošināt ārpus uzņēmuma ir grūti uzraudzīt. Līdz ar to urķi izmanto šo situāciju tā vietā, lai uzbruktu uzņēmumam tie izvēlas uzbrukt uzņēmuma darbiniekiem, izmantojot sociālās inženierijas paņēmienus;
- uzbrukumi izmantojot sociālos tīklus - urķi cenšas gūt pieeju uzņēmumiem, izmantojot biznesa sociālo tīklu vietnes, kurās uzņēmuma vadītājus mudina pievienoties sociāliem tīkliem un izmantot inficētas vietnes. (30)

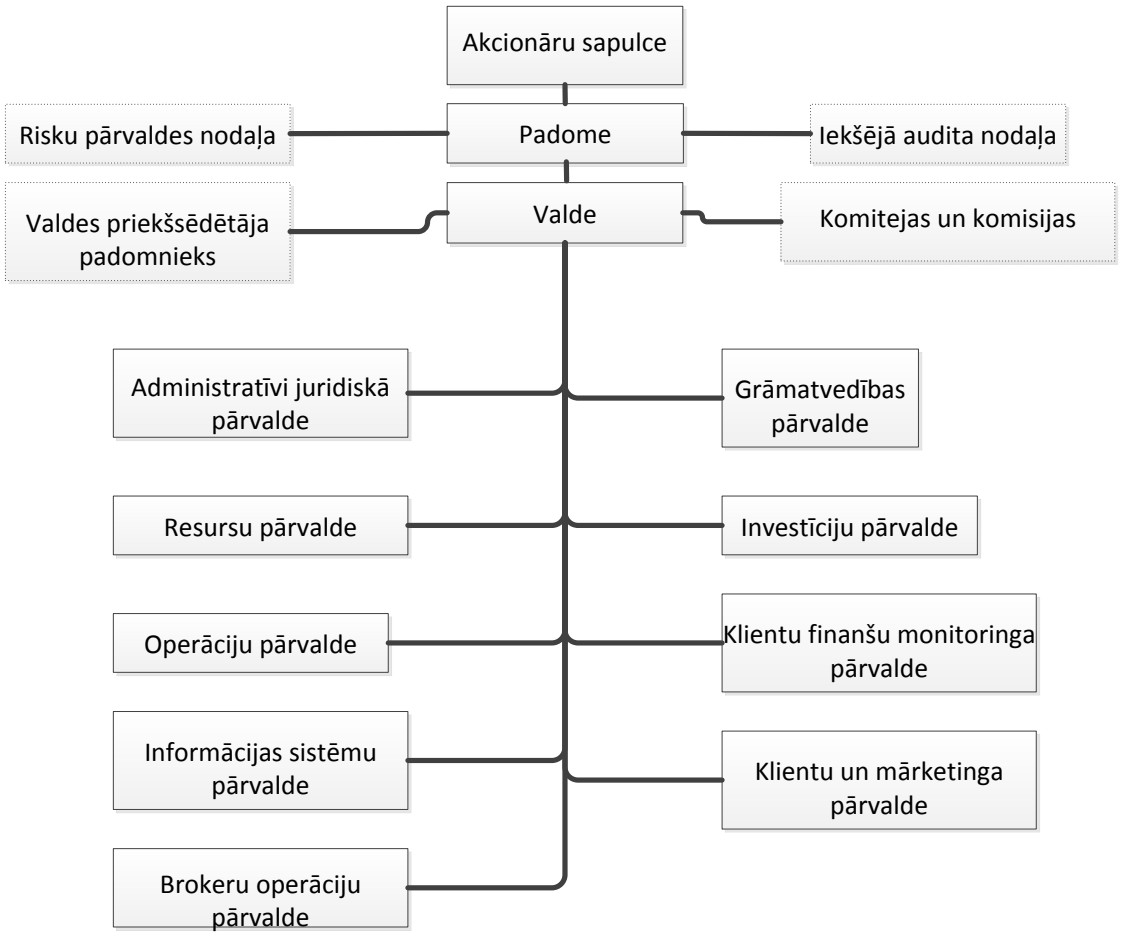
Secinājumi

Uzņēmumiem būtu jāseko līdzi jaunākajām tendencēm un risku pārvaldības plāna dokumentācijā jāaktualizē riski, kas var būt saistīti ar darbinieku drošību ārpus uzņēmuma, jo uzņēmumi koncentrējas uz iekšējiem riskiem nevis uz ārējiem. Lai mazinātu šo risku, tad IT drošības apmācībās būtu nepieciešams pieaicināt speciālistu, kas var nodemonstrēt, kādas var būt iespējamās sekas, ja darbinieks neievēro visus atrunātos IS drošības noteikumus ārpus uzņēmuma. Pēc KPMG veiktā pētījuma tas spilgti pierāda, ka, attīstoties tehnoloģijām, mainās uzņēmumam IS drošības draudi, līdz ar to ir svarīgi sekot līdzi jaunākajām tendencēm, piemēram, apmeklējot dažādus ražotāju un izstrādātāju seminārus, kurus uzņēmumiem piedāvā apmeklēt bez maksas.

3. IS DROŠĪBAS RISKA MAZINĀŠANA UZŅĒMUMĀ

Tālākajā maģistra darbā tiek atspoguļota informācija par uzņēmuma raksturojumu un struktūru. Raksturota uzņēmuma IT arhitektūra. Veikta uzņēmuma IT risku analīze informācijas sistēmām, kurām uzņēmumā ir konstatētas ar drošības riskiem saistītas problēmas. papildus riskos tiks iekļauta iepriekšējās IS pārvaldes darbinieku piekoptā prakse sistēmas uzturēšanā un sadarbība ar uzņēmuma citām pārvaldēm. Risku analīzes ietvaros tiek sniegtas rekomendācijas turpmāko pasākumu plānošanai, kas ļaus mazināt riskus un nākotnē samazināt riska vērtību uzņēmumā. Riska analīzē ietverta informācija, kas ir konstatētā uzņēmumā uz maģistra darba izstrādes brīdi. Vadoties pēc risku analīzes, tiek izdarīti secinājumi par sistēmas datubāzes un lietojumprogrammas atjaunināšanu uz jaunāku versiju.

Uzņēmuma pamatdarbība ir apdrošināšanas pakalpojumu sniegšana. Uzņēmuma veids ir akciju sabiedrība (AS) Iestādes struktūra att. 3.1 ir izveidota pēc funkcionālā principa, tajā ir deviņas pārvaldes, un katra no tām ir noteikta valdes locekļa pakļautībā. Darbības plāns paredz biznesa sadarbības attiecību attīstību ar esošiem un jauniem klientiem.



3.1 att. **Apdrošināšanas uzņēmuma struktūra (44)**

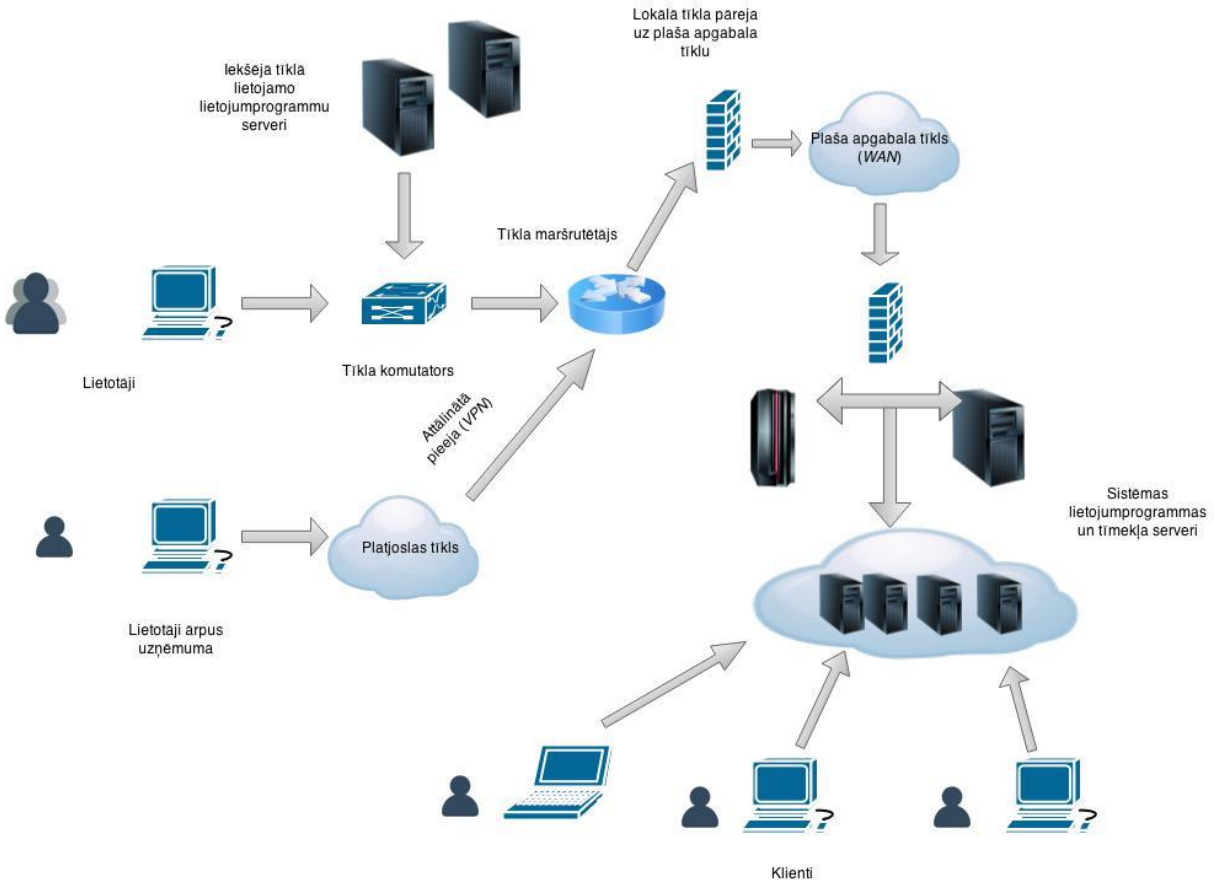
3.1 Uzņēmuma IT arhitektūras raksturojums

Uzņēmuma IT infrastruktūra tikusi veidota, piesaistot vietējos un ārzemju pakalpojumu sniedzēju uzņēmumus, balstoties uz to izstrādātajiem risinājumiem un procedūrām. Vienas no būtiskām izmaiņām, kas ieviestas uzņēmuma IT infrastruktūrā, ir divu faktoru autentifikācijas risinājums un Data Loss Prevention programmatūras ieviešana, kas veic preventīvus pasākumus pret datu noplūdi uzņēmumā. Šobrīd minētos risinājumus var nosaukt kā vienīgās veiksmīgi realizētās izmaiņas saistībā ar iespējamo datu noplūdi. Uzņēmuma infrastruktūras attīstība notikusi pakāpeniski, pievienojot pie esošās sistēmas jaunas funkcijas un to nodrošināšanai nepieciešamās tīkla iekārtas un serverus. Pievienojot jaunas iekārtas esošā infrastruktūrā, nav analizēta iespēja kopējās infrastruktūras optimizēšanai un standartizēšanai.

Uzņēmumā kopumā ir 11 informācijas sistēmas, kur daļu no biznesa procesiem izpilda sistēmu kopums, kas uzņēmumā nav aprakstīts. Līdz ar to šobrīd ir zināms, ka savstarpēji ir sasaistītas polišu sistēmas ar grāmatvedības un dokumentu pārvaldības sistēmām. Sistēmu savstarpējo sasaisti nodrošina tīmekļa servisi (*web services*), kuru integrācija notiek reizi stundā dokumentu pārvaldības sistēmai un reizi diennaktī grāmatvedības sistēmai. Līdz ar dokumentācijas trūkumu uzņēmumā tiek veikts IT audits, kura noslēgumā paredzēts izstrādāt infrastruktūras dokumentāciju, kā arī pilnu audita ziņojumu ar konstatētajām problēmām uzņēmuma IT infrastruktūrā.

Aptuvena vispārējā uzņēmuma tīkla infrastruktūras arhitektūras shēma sk. att. 3.2. IT infrastruktūra sastāv no 7 sfērām:

- lietotājiem;
- darbstacijām;
- lokālā tīkla (*LAN*);
- plaša apgabala tīkla (*WAN*);
- attālinātās piekļuves;
- sistēmas / lietojumprogrammas serveriem;
- lokā tīkla pārejas uz plaša apgabala tīklu.



3.2 att. **Uzņēmuma IT infrastruktūras shēma(44)**

3.2 Risku novērtēšana atbilstoši ISO 27000 uzņēmumā

Uzņēmuma mērķis ir ieviest informācijas sistēmu drošības standartu atbilstoši ISO 27000, līdz ar to tika veiktas vairākkārtējas padomes un valdes sēdes, kurā piedalījās uzņēmuma pārvalžu vadītāji. Sēdēs tika nolemts pieaicināt neatkarīgu konsultantu komandu, kas veiks uzņēmuma biznesa procesu auditu un veiks izvērtējumu, kuru no ISO standartiem uzņēmumā būtu nepieciešams ieviest.

Pēc sākotnējo audita rezultātu apkopošanas lielākie darbi, kurus nepieciešams veikt, ir:

- dokumentācijas atjaunošana atbilstoši ISO 27000 prasībām (drošības politika, risku pārvaldes plāns, IS lietošanas noteikumi);
- pēc visas nepieciešamās dokumentācijas izstrādāšanas un apstiprināšanas būs nepieciešams izvest darbinieku apmācības;
- veikt atkārtotu iekšējo auditu;
- ārējo auditoru piesaistīšana (kas nav sertifikācijas auditori), lai gūtu pārliecību, ka uzņēmums ir gatavs sertifikācijas auditam, tas tiks darīts ar mērķi, lai gūtu pārliecību par to, ka viss ir kārtībā, vai ir konstatētas nebūtiskas neatbilstības, kuras līdz sertifikācijas auditam nepieciešams novērst.

Pēc dokumentu izpētes tika noskaidrots, ka no ISO standarta ir iespējams izslēgt punktus, kas ISO 27001 gadījumā sākas no 8. punkta, bet tas ir argumentēti jāpamato. Standarta 8. Punkts satur rekomendācijas par informācijas drošības vadības sistēmām, kurā ietvertas rekomendācijas par sistēmas patstāvīgu uzlabošanu un korektīvām darbībām. Līdz ar to, ja ISO standarta ieviešana uzņēmumā var tikt aizkavēta dēļ IS aktuālās dokumentācijas trūkuma, tad, sertifikācijas auditoriem uzrādot pasākumu plānu, kurā tiek norādīts konkrēto pasākumu veikšanas termiņš, uzņēmumam var nebūt šķēršļi ISO 27001 standarta sertifikācijas iegūšanai.

Vadoties pēc ISO standarta pieejas risku novērtēšanai, risku novērtējums tiks veikts skalā pēc kvantitatīvās metodes. Šāda pieeja ļauj apskatīt ietekmes vērtējumu konfidencialitātei, integritātei, pieejamībai un iestāšanās varbūtības vērtējumu. Riska vērtēšana tiek veikta katram identificētajam apdraudējumam. Risks tiks izteikts kā varbūtības un ietekmes reizinājums.

Riska noteikšana formula: **Riska vērtība** vai **Riska atlikusī vērtība** = (**Ietekmes vērtējums konfidencialitātei + Ietekmes vērtējums integritātei + Ietekmes vērtējums pieejamībai**) * **Iestāšanās varbūtības vērtējums**

Uzņēmumā pieļaujamais risku kopējais līmenis ir noteikts 4 vai zemāks. Tab. Nr. 3.1.

Risku vērtību diapazona apzīmējuma tabula *3.1. tabula*

Krāsa	Riska vērtības diapazons	Lēmums par tālāko rīcību
Zaļa	<=4*	Apdraudējuma līmenis ir **zems**, tālākā rīcība nav nepieciešama.
Dzeltena	=>5<7*	Apdraudējuma līmenis ir **vidējs**, par tālāko rīcību lemj atkarībā no apdraudējuma veida un pieejamiem resursiem
Sarkana	=>7*	Apdraudējuma līmenis ir **augsts**, ir nepieciešams pieņemt lēmumu par tālāko rīcību riska ietekmes mazināšanai.

Riska analīze tika veikta uzņēmuma informācijas sistēmām, kurās pēc pieejamās informācijas un apskates ir konstatēti IS drošības draudi, papildus riskos tiks iekļauta iepriekšējās IS pārvaldes darbinieku piekoptā prakse sistēmas uzturēšanā un sadarbība ar uzņēmuma citām pārvaldēm, jo lai būtu iespēja sakārtot IS drošību ir nepieciešama visu nodaļu savstarpējā sadarbība un informācijas apmaiņa. Informācijas sistēmas, kurās ir konstatēti IS drošības draudi:

- **polišu sistēma** – sistēma, kurā tiek uzkrāta informācija par klientiem un to veiktajiem maksājumiem un iegādātajām polisēm;
- **polišu sistēma 2** – sistēma, kurā tiek uzskaitīti nelaimes gadījumi attiecīgi pēc klientiem;
- **dokumentu pārvaldības sistēma** - dokumentu pārvaldības sistēma, kurā tiek veikta elektronisko dokumentu reģistrācija, parakstīšana, uzglabāšana un arhivēšana;
- **e-pasts** - sistēma elektronisku ziņojumu sastādīšanai, nosūtīšanai un saņemšanai;
- **IT atbalsta programma** – sistēma, ar kuras palīdzību uzņēmuma lietotāji var izveidot problēmu pieteikumus (*helpdesk*);
- **uzņēmuma mājaslapa** – informācija par uzņēmumu ar iespēju autorizēties uzņēmuma IS;
- **uzņēmuma iekšējais portāls** – sistēma, kurā tiek nodrošināta aktuālo dokumentu, likumu projektu izmaiņas, iekšējās uzņēmuma ziņas un jaunumi;
- **sistēmu testa vides** – sistēmu vides, uz kurām ir iespējams pārbaudīt un notestēt sistēmas jauninājumu ieviešanu.

Riska analīzes rezultātā tiks izveidots saraksts ar konkrētajā risku analīzē aktuāliem apdraudējumiem. Apdraudējumi tika identificēti ārpus maģistra darba ietvara pēc iepriekš:

- analizētiem drošības incidentiem;
- veiktām tehniskās drošības pārbaudēm;
- analizētas izmaiņu vēstures un veikto izmaiņu atstātās ietekmes;
- analizētām apkārtējās vides izmaiņām pamatojoties uz informāciju par apdraudējumiem;
- esošo kontroles risku mehānismu identifikācijas;
- katram apdraudējumam fiksējot jau esošos apdraudējumus;
- kontroles mehānismi tiks balstīti uz iepriekš atbilstošām intervijām ar atbilstošajiem lietotājiem, kas var būt iesaistīti risku kontroles pasākumu ieviešanā;
- faktisku situācijas izpēti;
- ievainojamību identifikāciju;

Ievainojamības uzņēmumā tika identificētas pēc:

- personālu saistītām ievainojamībām;
- fiziskās vides ietekmes;
- informācijas sistēmas, programmatūras, aparatūras un tās konfigurācijas;

- trešo pušu saistības vai iesaistes informācijas resursu pārvaldībā.

Katram apdraudējumam risku analīzes procesa laikā tiks piešķirts tā ietekmes kvantitatīvs vērtējums pēc šādiem kritērijiem.

Ietekmes vērtējums konfidencialitātei, kur**:**

3	apdraudējums rada tiešas tiesiskas sekas uzņēmumam (saistīts ar spēkā esošo normatīvo aktu neievērošanu un krimināLatbildību)
2	apdraudējumam ir administratīva rakstura sekas
1	informācijai nonākot neautorizētu personu rīcībā ir iespējamas nebūtiskas, ar reputāciju saistītas sekas
0	informācija ir publiski pieejama, un uz to nav attiecināmi konfidencialitātes zuduma riski

Kā viena no uzņēmuma pamatvērtībām ir individuāla pieeja katram klientam, nodrošinot privātuma aizsardzību un uzticamību. Līdz ar to tika noteiktas vērtības, vadoties pēc tiesiskā un administratīvā regulējuma un uzņēmuma atpazīstamības Latvijā un Baltijas valstīs.

Ietekmes vērtējums integritātei, kur:

3	integritātes zudums kritiski traucē uzņēmuma informācijas resursu darbību
2	apdraudējums rada netiešus finansiālos zaudējumus (piemēram: datu atjaunošanai nepieciešams veltīt papildus darba laiku). Pat ja integritātes zudums ir grūti konstatējams, ir iespējams ar pilnu pārliecību par informācijas integritāti atjaunot visu informāciju.
1	apdraudējums nerada finansiālus zaudējumus uzņēmumam, integritātes zudums ir viegli konstatējams un tā sekas netraucē kopējiem biznesa procesiem. Ir iespējams ar pilnu pārliecību par informācijas integritāti atjaunot visu informāciju

Uzņēmuma pamatdarbība ir balstīta uz IS un to savstarpējo datu apmaiņu, tādēļ, ja kādā no sistēmām tiek konstatētas problēmas ar datu integritāti, tās ir nepieciešams atrisināt pēc iespējas ātrāk, jo nekorekti dati nozīmē informācijas veseluma zudumu un problēmas nākotnē.

Ietekmes vērtējums pieejamībai, kur:

3	apdraudējums rada tiešus/ nozīmīgus finansiālus un/vai reputācijas zaudējumus. Šajā kategorijā ietilpst arī jebkurš risks, kas rada tiešus riskus cilvēka dzīvībai vai veselībai

2 apdraudējums rada netiešus vai nenozīmīgus finansiālus zaudējumus, piemēram, nepieciešama darbinieku vai ārpakalpojuma papildus laika ieguldījums ārpus darba laika un tiešajiem pienākumiem pieejamības atjaunošanai.

1 apdraudējums nerada vērā ņemamus zaudējumus. Ir iespējams atjaunot pieejamību darba laikā, netērējot papildus cilvēkresursus vai finansiālos resursus

Svarīga loma uzņēmumā ir ārpakalpojumu izmantošana IS uzturēšanā un izmaiņu ieviešanā. Līdz ar to ir būtiska to sniegtā pakalpojuma kvalitāte un laiks.

Iestāšanās varbūtības vērtējums, kur:

3 apdraudējumam ir augsta iestāšanās varbūtība, apdraudējums var iestāties vairākas reizes gadā vai tas jau ir noticis, piemēram, tehniskās ievainojamības, kurām ir plaši zināmi izmantošanas rīki, jau noticis drošības incidents; ir interešu grupa, kurai ir interese par atbilstošo informāciju un kapacitāte šīs informācijas iegūšanā.

2 apdraudējumam ir vidēja iestāšanās varbūtība, apdraudējums var **iestāties 1 reizi** gadā vai tas noteikti vēl nav noticis, piemēram, ir identificējamas tehniskās ievainojamības, kas, iespējams, ļauj piekļūt informācijai, bet nav identificējami šo ievainojamību lietojumi.

1 apdraudējumam ir zema iestāšanās varbūtība, apdraudējums var iestāties 1 reizi 3 gados vai ir maza varbūtība, ka tas notiks (piem.: ir informācija par iespējamo interešu grupu, kas varētu gribēt iegūt noteiktu informāciju, bet ir veikts vairums aizsardzības pasākumu, lai šo informāciju aizsargātu un identificējamie apdraudējumi prasa papildus zināšanas par uzņēmuma informācijas aizsardzības procesiem vai papildus piekļuves).

Ir svarīgi apzināt esošo situāciju uzņēmumā un saprast kādi ir IS drošības draudi, cik bieži uzņēmumā tiek konstatēti incidenti, kas saistīti ar sistēmas drošību uzņēmumā un klientu ziņotās problēmas ar sistēmas funkcionalitāti un drošību saistītos jautājumos.

Riska novērtēšanas pārskata tabula *3.2. tabula*

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
1	Dokumentu pārvaldības sistēma	Sagatavoto e-dokumentu tehnisko iemeslu dēļ nav iespējams parakstīt.	E-dokuments nav izveidojies.	Iztērēti resursi	0	1	3	3	**12**	Iegādāties papildus licences atkarībā no parakstītāja skaita.
2	Dokumentu pārvaldības sistēma	Tehnisko vai citu iemeslu dēļ informācija nav sasniegusi adresātus	No saņēmēja nav apliecinājuma par saņemšanu pēc 24.st.	saņēmējs nesaņem informāciju	0	1	2	2	**6**	Izveidot speciālu e-pasta ziņojumu, kas veic pārbaudi reizi stundā par nosūtāmo dokumentu statusu.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
3	Dokumentu pārvaldības sistēma	E-dokumentus nav iespējams pievienot visiem sistēmas moduļiem	Nav izveidoti lauki, kuriem var pievienot e-dokumentus	Dokumenti tiek uzglabāti atšķirīgās vietās; veicot atlasi, grūti tos atrast, jo nav vienotas sistēmas	0	1	1	3	**6**	Paredzēt iespēju pievienot e-dokumentus pie sistēmas moduļiem. Izveidot kopējo lietvedības sistēmu.
4	Grāmatvedības sistēma	Sinhronizācijas trūkums starp Grāmatvedības sistēmu un Polišu sistēmu	Dati netiek piegādāti	Integritātes zudums	0	3	1	2	**8**	Sistēmas sinhronizācijas darbības pārtraukuma rezultātā tiek ģenerēta automātiska atskaite sistēmas administratoram
5	Grāmatvedības sistēma	Atkarība no sistēmas uzturētāja un izmaiņu izstrādātāja	Ar piegādātāju netiek pagarināts līgums	Sistēma netiek atbilstoši uzturēta.					**0**	Apzināt alternatīvus piegādātājus.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
6	Grāmatvedības sistēma	Ievadīta nekorekta informācija.	Manuāli pārbaudot informāciju.	Nepieciešami papildus resursi informācijas labošanai.	0	2	1	2	**6**	Izstrādāt lomu, kas grāmatvedībai nodrošinās datu labošanu no lietojumprogrammas.
7	IT atbalsta programma	Cilvēciskais faktors (nolaidība, darbinieku prombūtne).	Lietotāji informē par pieteikto uzdevumu neizpildi.	Netiek izpildīti uzdevumi, netiek nodrošināts lietotāju atbalsts.	0	2	1	3	**9**	Nodrošināt sistēmā automātisko ziņošana par jauniem reģistrētiem IT pieprasījumiem vairākiem pārvaldes darbiniekiem.
8	IT atbalsta programma	Sistēma nav pieejama, incidentu pieņemšana notiek caur e-pastu IS pārvaldei vai zvanot pa tālruni.	Lietotāji informē par pieteikto uzdevumu neizpildi.	Netiek reģistrēti pieteikumi sistēmā.	0	1	3	1	**4**	Tiek regulāri atgādināts par IT atbalsta sistēmas izmantošanu.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
9	Polišu sistēma 2	Pēc piekļuves tiesību izbeigšanās ārējam lietotājam nav noņemtas piekļuves tiesības.	Problēmu pamana darbinieki.	Lietotājam ir pieejama informācija bez maksas.	1	1	1	3	**9**	Datu bāzei paredzēt funkciju, kas pēc lietotāju tiesību izbeigšanos, automātiski noņem pieejas tiesības.
10	Polišu sistēma	Sistēmas ārējais lietotājs, aizpildot informāciju par polišu iegādi, norāda neprecīzu informāciju.	Par problēmu paziņo ārējais lietotājs, vai kļūda tiek atklāta ekspluatācijas un tehniskās uzraudzības laikā.	Iegūtie dati par polišu iegādi ir neprecīzi.	0	2	1	1	**3**	Izstrādāt ārējo lietotāju atjauninātu sistēmas instrukciju.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
11	Polišu sistēma	Atkarība no sistēmas uzturētāja un izmaiņu izstrādātāja.	Kompetences trūkums sistēmas koda kļūdainas darbības novēršanai.	Daļējas sistēmas vai pilnīgas sistēmas nestrādāšana.	0	2	2	2	**8**	Apzināt iespējas piesaistīt uzņēmumam kvalificētu darbiniekus.
12	E-pasts	Nesankcionēta informācijas nosūtīšana no uzņēmuma darbinieka puses.	Informācija par šādu gadījumu ienāk no ārējiem avotiem.	Konfidenciālas informācijas noplūde, tiešais finansiālais zaudējums trešajai personai.	2	1	1	1	**4**	Iestāšanas varbūtības koeficients mainās atkarībā no saņemtās informācijas. Papildus risinājums specializēta programmatūra, kas filtrē nosūtāmo informāciju.
13	E-pasts	Darba e-pasts netiek izmantots tiešo darba pienākumu izpildei.	Uzglabājamo datu apjoma palielināšanās.	Nelietderīgi izmantoti resursi.	0	1	1	2	**4**	Izskatīt iespējas pievienot papildus atmiņu e-pasta serverim.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
14	Dokumentu pārvaldības sistēma	Ievadīta nepareiza vai neievadīta informācija sistēmā, informācija nonāk pie nepareiza lietotāja.	Pamanīta kļūda no darbinieku puses.	Informācija nonāk vai nenonāk pie izpildītāja, nokavēti termiņi, nesavlaicīgi sniegta atbilde.	0	2	1	3	**9**	Jāveic papildus apmācības darbiniekiem, gan kopējās, gan individuālās.
15	Risku pārvaldības plāns	Nav iekļauti, vai nepilnvērtīgi novērtēti riski IS/IT resursiem.	Nav pieejama aktuālā informācija.	Nav iespējams atjaunot sistēmas darbību vadoties pēc darbības atjaunošanas plāna.	1	3	1	2	**10**	Veikt IT/IS auditu atjaunot sistēmas dokumentāciju. Atjaunot IS drošības noteikumus, drošības politikas dokumentus u.c. atbilstoši aktuālajai situācijai.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
16	Dokumentu pārvaldības sistēma	Ievadīta nepareiza vai neievadīta informācija sistēmā.	Pamanīta kļūda no darbinieku puses	Informācija nonāk vai nenonāk pie izpildītāja, nokavēti termiņi, nesavlaicīgi sniegta atbilde	2	1	1	1	**4**	Papildus pārbaudes informācijas ievadīšanai sistēmā.
17	Dokumentu pārvaldības sistēma	Izpildītājs nereaģē uz sistēmas paziņojumu.	Sistēma ziņo par dokumentiem, kuriem termiņš beigsies, vai ir pārsniegts un nav atzīmes par izpildi.	Nokavēti termiņi, dokumenti nav izpildīti	0	1	1	3	**6**	Nodrošināt e-pastu sūtīšanu no sistēmas, ja dokumenta izpildes termiņš tuvojas beigām.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
18	Uzņēmuma iekšējais portāls	Nav uzņēmuma iekšienē pieejama publiska informācija.	Sistēma nav pieejama.	Tiek traucēta organizatoriskā darbība, jāpatērē papildus laiks informācijas atrašanai.	0	1	2	1	**3**	Izstrādāt procedūru, kas tiek darīts, ja informācija lapā nav pieejama.
19	Starp pārvaldēm nav kopējas vīzijas saistībā ar uzņēmuma nospraustajiem mērķiem.	Pārvaldes savā starpā neveic komunikāciju, netiek saņemta atgriezeniskā saite.	Sistēmas nekorektas funkcionēšanas gadījumā tiek norādīta IS pārvalde.	Sistēma neveic visas tai paredzētās biznesa funkcijas.	0	3	2	2	**10**	Veikt pārvalžu savstarpējo sanāksmi, noskaidrot kuras ir tās lietas, kas ir prioritāras.
20	IS pārvaldes sistēmas kļūdu labošanas prakse.	Sistēmā tiek piefiksētas kļūdas, kas radušās ievadot nekorektu informāciju.	Kļūdas ar datiem ir iespējams labot tikai datubāzē.	Rēķins tiek izrakstīts nekorektam klientam.	1	3	1	1	**5**	Ir veikti sākotnēji uzlabojumi rēķinu integrācijā, kas ir samazinājis kļūdu iespējamību. Laika gaitā vēsturiskajos datos kļūdas var parādīties.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
21	Polišu sistēma 2	Atkarība no sistēmas uzturētāja un izmaiņu izstrādātāja.	Kompetences trūkums sistēmas koda kļūdainas darbības novēršanai.	Daļējas sistēmas vai pilnīgas sistēmas nestrādāšana.	0	2	2	2	**8**	Apzināt iespējas piesaistīt uzņēmumam kvalificētu darbaspēku.
22	Polišu sistēma	Sistēmas uzturēšanas līguma termiņš.	Uzturēšanas līguma termiņš - 1 gads.	Īsa termiņa gadījumā jaunā sistēmas izstrādātājam nepieciešams laiks, lai iepazītu sistēmas darbību, tādējādi pagarinot sistēmas kļūdu novēršanas un jaunu pieprasījumu izstrādes piegādes laiku.	0	2	2	2	**8**	Paredzēt līguma termiņa noslēgšanu vismaz līdz 3 gadiem vai neierobežotu laiku.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
23	Polišu sistēma 2	Sistēmā ir veiktas izmaiņas, kuras nav dokumentētas. Izmaiņām nav izstrādāta programmatūras prasību specifikācija.	Sistēmas kļūdaina darbība.	Sistēma ir daļēji vai pilnībā nav pieejama.	0	2	2	2	**8**	Kvalitatīvākā testēšana izstrādes gaitā, kļūdu kvalitatīva novēršana. Kontroles metožu izstrāde. Izmaiņu vadības procedūras izstrāde.
24	Polišu sistēma 1 un 2	Lietotāji autentifikācijas datus pieraksta uz papīra.	Iespējama nesankcionēta piekļuve pie lietotāju datiem.	Konfidenciālas informācijas noplūde, tiešais finansiālais zaudējums trešajai personai.	2	2	2	1	**6**	Ieviest divu faktoru autentifikācijas risinājumu, izmantojot (*token*).

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
25	Polišu sistēma 2	Informācija ir pieejama administrēšanas nolūkos konkrētai trešajai personai, kuru to var ļaunprātīgi izmantot.	Informācija par šādu gadījumu ienāk no ārējiem avotiem.	Konfidenciālas informācijas noplūde, tiešais finansiālais zaudējums trešajai personai.	3	2	1	1	**6**	Atbildīgais par drošības pārvaldību regulāri veic auditācijas pierakstu pārbaudi. Datu bāzes satura kriptēšana.
26	Polišu sistēma 2	IS uzturētāju pieeja produkcijas datiem.	Ikdienas darbā pieejama sensitīva informācija.	Informācijas noplūde.	3	1	1	1	**5**	Veikt datubāzu datu miksēšanu.
27	Uzņēmuma mājaslapa	Tiek pārsniegts vienlaicīgo lietotāju skaits	Sistēma lēni darbojas vai nestrādā vispār	Mājaslapa lēni atveras vai nav pieejama	0	1	3	1	**4**	Izskatīt iespēju par servera resursu papildināšanu.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
28	Drošības pārvaldnieks	Ierobežotu resursu dēļ nav izveidots amats vai tiek daļēji - formāli pildīts	Uzņēmuma IS drošību daļēji veic IS pārvaldes vadītājs.	Netiek pildītas funkcijas, kas paredzētas likumdošanā.	2	2	3	2	**14**	Rast resursus jauna vai esoša amata apvienošanai, lai nākotnē būtu iespēja pildīt ISO 27001 standarta prasības.
29	Uzņēmuma mājaslapas ievainojamība	Iespējama lietotāju piekļuves identifikatoru noplūde.	Sistēma atbalsta novecojušas kriptogrāfijas aizsardzības metodes.	Iespējama lietotāju piekļuves identifikatoru noplūde.	2	2	2	3	**18**	Veikt konfigurācijas izmaiņas, lai nepieļautu novecojušu kriptogrāfijas algoritmu izmantošanu.
30	Uzņēmuma mājaslapas ievainojamība	Iespējama neautorizēta piekļuve pie informācijas resursiem.	Sistēmas moduļi nepārbauda HTML tagus. Iespējams veikt XSS/CSFR veida uzbrukumus pret autorizētiem sistēmas lietotājiem.	Iespējama neautorizēta piekļuve pie informācijas resursiem.	2	3	2	3	**21**	Veikt programmatūras uzlabojumus, lai novērstu nepilnīgu lietotāju ievadīto datu apstrādi.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
31	Polišu sistēma (*Oracle Application Server*)	Iespējama sistēmas pakalpojuma atteice, informācijas noplūde. Iepriekšējā IS pārvaldes komanda vairākkārtīgi ir skatījusi un pilnveidojusi uzturētāja piedāvājumu saistībā ar sistēmas migrāciju uz jaunāku Oracle versiju, taču realizācija ir atlikta, saistībā ar resursu trūkumu	Sistēma izmanto neatbalstītu (novecojušu) programmatūras komponenti, kurai netiek sniegti jauninājumi no izstrādātāja, kā arī netiek sniegts atbalsts. Lietojumprogramma neatbalsta jaunāka SSL sertifikāta uzstādīšanu ar TLS versiju virs 1.0	Iespējama sistēmas pakalpojuma atteice, informācijas noplūde. Sistēma nav pieejama klientiem, kas izmanto pārlūkprogrammas ar pēdējiem atjauninājumiem.	3	2	3	3	**24**	Veikt pakalpojuma migrāciju uz jaunāku programmatūras komponenti.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
32	Polišu sistēma (*Oracle Database Server*)	Iespējama sistēmas pakalpojuma atteice, informācijas noplūde. Iepriekšējā IS pārvaldes komanda vairākkārtīgi ir skatījusi un pilnveidojusi uzturētāja piedāvājumu saistībā ar sistēmas migrāciju uz jaunāku Oracle versiju, taču realizācija ir atlikta, saistībā ar resursu trūkumu.	Sistēma izmanto neatbalstītu (novecojušu) programmatūras komponenti, kurai netiek sniegti jauninājumi no izstrādātāja, kā arī netiek sniegts atbalsts.	Iespējama sistēmas pakalpojuma atteice, informācijas noplūde, neatgriezenisks datu zudums.	3	3	3	3	**27**	Veikt pakalpojuma migrāciju uz jaunāku programmatūras komponenti.

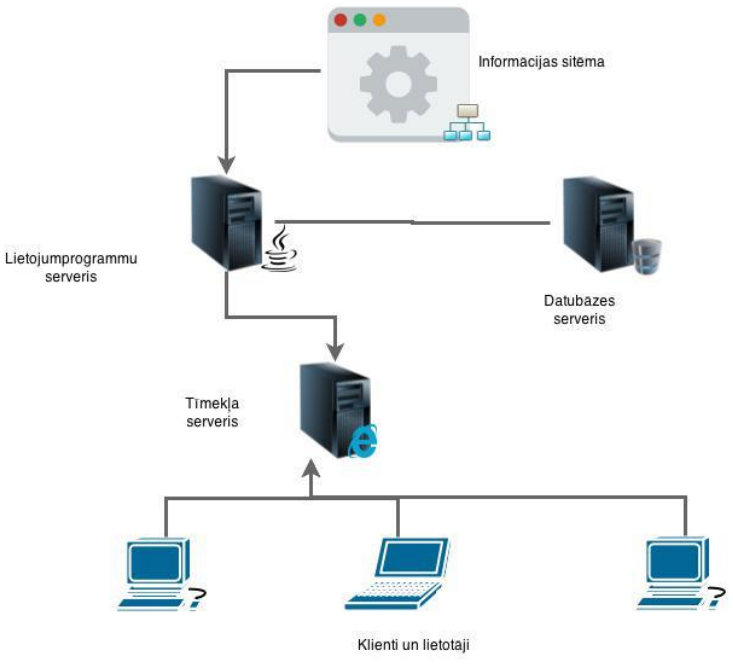
Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
33	Polišu sistēma (Oracle Discoverer Lietojumprogr amma)	Iespējama neautorizēta piekļuve pie informācijas resursiem.	Sistēmas noklusētājā konfigurācijā izvietotajām lietojumprogram mām ir iespējams izpildīt XSS uzbrukumus no uzņēmuma lokālā lietotāju tīkla.	Iespējama neautorizēta piekļuve pie informācijas resursiem.	2	1	1	3	**12**	Novērst piekļuvi no publiskā tīkla, vai arī veikt versijas atjaunināšanu.
34	Polišu sistēma (Oracle TNS komponente)	Iespējama pakalpojuma atteice.	Var tikt izmantota pakalpojuma atteicei vai arī neautorizētas sistēmas piekļuves ieguvei	Iespējama pakalpojuma atteice.	2	2	2	3	**18**	Veikt sistēmas konfigurāciju atbilstoši ražotāja rekomendācijām.

Nr. p.k.	IR - Informācijas resurss	Apdraudējuma apraksts	Ievainojamības pazīmes, kas liecina par iespējamo apdraudējuma iestāšanos	Ievainojamības iestāšanās gadījumā identificētās sekas	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Riska vērtība	Rekomendācijas riska vērtības mazināšanai
35	E-pasts, polišu sistēmas (aizsardzību pret L2 „tīkla līmeņa" uzbrukumiem)	Iespējama neautorizēta piekļuve pie IS resursiem.	Pieļauj MITM (*Man-In-The-Middle*) uzbrukumus.	Iespējama neautorizēta piekļuve pie IS resursiem.	2	2	2	3	**18**	Veikt tīkla iekārtu vai to konfigurācijas maiņu.
36	Sistēu testu vides (polišu / dokumentu pārvaldības)	Iespējama lietotāju piekļuves identifikatoru noplūde.	Ļauj veidot savienojumus neizmantojot šifrēšanu datu pārraidei.	Iespējama lietotāju piekļuves identifikatoru noplūde.	2	1	2	3	**15**	Nodrošināt piekļuvi pie pakalpojuma izmantojot drošu HTTPS risinājumu.

Pēc veiktās risku analīzes Tab. 3.2 ir redzams, ka uzņēmumā vairākām sistēmām vai tās komponentēm riska apdraudējuma līmenis ir virs pieļaujamā līmeņa uzņēmumā. Viens no nopietnākajiem draudiem ir Polišu sistēmas datubāzu un lietojumprogrammu serveru programmatūras komponentes, kurām netiek sniegti jauninājumi no ražotāja, kā arī netiek sniegts atbalsts. Konkrētā situācija ir radusies, jo vairākkārtēji mainoties Informācijas sistēmu pārvaldes darbiniekiem un vadītājam, uzņēmumā nav veikta pilnvērtīga risku analīze, kurā būtu iekļautas uzņēmuma biznesam primārās sistēmas.

Oracle 10.2 versijai standarta atbalsts ir beidzies 2010. gada jūlijā, bet paplašinātais atbalsts ir beidzies 2013. gada jūlijā. (36) Līdz ar to, Polišu sistēmas kļūdas vai avārijas gadījumā nav pieejams ražotāja atbalsts un padoms vai palīdzība sistēmas normālas darbības atjaunošanai. Pēc pieejamās informācijas iepriekšējā IS pārvaldes komanda vairākkārtīgi ir skatījusi un pilnveidojusi uzturētāja piedāvājumu saistībā ar sistēmas migrāciju uz jaunāku Oracle versiju, taču realizācija ir atlikta, saistībā ar resursu trūkumu.

Pēc dokumentācijas, kurā ir būtiski trūkumi, aptuvenā IS arhitektūras shēma izskatās kā redzams attēlā 3.3. Sistēma ir saistīta ar Uzņēmuma informācijas sistēmu, un darbs ar sistēmu tiek veikts tīmekļa pārlūkā. Tas nozīmē, ka uzņēmuma informācijas sistēmas līmenī tiek ietvertas trīs sastāvdaļas: Tīmekļa (*Web*) serveris, kur tiek veikti lietotāju pieprasījumi, lietojumprogrammu serveris un datubāzes serveris, kur tiek veikta datu apstrāde. Darbības tiek realizētas, izmantojot HTTP protokolu, kurš strādā caur transporta slāņa šifrēšanas mehānismiem TLS/SSL, tādējādi papildinot standarta HTTP sakarus ar TLS/SSL drošības iespējām.



*3.3 att.***Uzņēmuma Polišu sistēmas arhitektūras shēma (44)**

Veicot sistēmas sākotnējo analīzi un izpēti, tika secināts, ka sistēmas darbība vairs neatbilst dokumentācijā norādītajai IS arhitektūras shēmai. Tādēļ, vadoties pēc risku analīzes, sistēmai ir nepieciešama lietojumprogrammas un datubāzes atjaunināšana uz jaunāku versiju. Bet, lai veiktu atjaunināšanu, nepieciešams izveidot atjaunināto IS arhitektūras shēmu, un atjaunināt sistēmas dokumentāciju.

Uzņēmumā tika izveidota jauna komanda IS pārvaldē, kurā autors pilda IS administratora pienākumus. IS pārvaldei ir nodots tai prioritāro lietu saraksts, kuras nepieciešams veikt 2 gadu laikā. Viens no uzņēmuma darbības mērķiem ir ieviest IS drošības standartu atbilstoši ISO 27001, jo tas izstrādāts, lai identificētu un novērstu iespējamos draudus informācijas uzturēšanā un glabāšanā. Atbilstība šim standartam apliecina, ka uzņēmuma informācijas drošības sistēmai un uzņēmumam kā sadarbības partnerim var uzticēties. Viens no pirmajiem soļiem, kas tika veikts, lai apzinātu esošo sistēmas darbību, tika pieaicināta sistēmas izstrādātāju komanda ar kvalificētiem programmētājiem, jo, lai aktualizētu sistēmas dokumentāciju, nepieciešams iepazīties ar sistēmas kodā veiktajām izmaiņām, ko iepriekš bez dokumentēšanas veikuši IS pārvaldes programmētāji, kas iekļauta riska analīzē. Sistēmas uzturēšanu veica IS pārvaldes programmētāji, daļēji sadarbojoties ar izstrādātāju, kuri izmaiņas sistēmā veica, saņemot lietotāju pieprasījumus, neizvērtējot to kā šīs konkrētās izmaiņas ietekmēs citu pārvalžu darbu un datu kvalitāti sistēmā. Veicot izmaiņas sistēmā, netika veidot programmatūras prasību specifikācija. Līdz ar to sistēmas dokumentācijas versijas šobrīd ir neaktuālas, jo tās neatbilst pašreizējai situācijai.

Lai uzņēmumā būtu iespēja ieviest ISO 27001 standartu, tika izveidota speciāla komisija, kurā tika pieaicināti ārējie konsultanti, lai iepazītos ar uzņēmumā esošo situāciju un nākotnes plāniem. Viens no būtiskiem trūkumiem ir esošās sistēmas novecojušās datubāzes un lietojumprogrammas lietošana, kā arī sistēmas tehniskās dokumentācijas nepilnības. Līdz ar to viens no IS pārvaldes prioritāriem uzdevumiem ir veikt sistēmas datubāzes un lietojumprogrammas migrāciju uz jaunāku versiju. Kā pamatojums šī uzdevuma prioritātēm tika minēts ne tikai atbalsta beigas, bet arī iespējamais drošības risks datu noplūdes novēršanai un IS drošībai. Vadoties pēc risku analīzes, tad Polišu sistēmas riska vērtība ir viena no augstākajām, kas pārsniedz uzņēmumā pieļaujamo riska līmeni gandrīz septiņas reizes. Šobrīd daļa klientu pieslēdzas pie sistēmas ārējās lietojumprogrammas, bet daļa veic pieslēgumus arī pie iekšējās sistēmas, kas ir liels drošības risks. Ja klienti pieslēdzas pie sistēmas iekšējās lietojumprogrammas, kur ierobežojumi uz formu attēlošanu ir ierobežotas

tikai ar tiesībām, pastāv iespējamība, ka klientam var būt pieeja pie uzņēmuma darbiniekiem paredzētas sistēmas funkcionalitātes.

Vadoties pēc risku analīzes, tad šobrīd svarīgi ir mazināt risku iespējamību, ka sistēma var pārstāt darboties un problēmas risināšanai nebūs iespējams pieaicināt ražotāju. Tas ir viens no svarīgākajiem punktiem biznesa nepārtrauktības plānā, jo uz sistēmas darbību balstās viss uzņēmuma darbs. Autors uzskata, ka pie šādas situācijas uzņēmums ir nonācis, jo risku pārvaldes nodaļā un iekšējā audita nodaļā nav pieejami cilvēkresursi, kas pārzinātu IT un ar tām saistītos riskus, jo šīs nodaļas veic risku izvērtēšanu un auditu saistībā tikai ar uzņēmuma pamatdarbību un klientiem, līdz ar to risku pārvaldības plānā ir iekļauts papildu risks saistībā ar to, ka uzņēmumā nav IS drošības pārvaldnieka amats. Līdz ar to uzņēmumā ir izstrādāts nepilnvērtīgs risku pārvaldības plāns un IS drošības politika. Dokumenti ir izstrādāti neiepazīstoties ar jaunākajām tendencēm un likumdošanu, kas attiecas uz IS drošību.

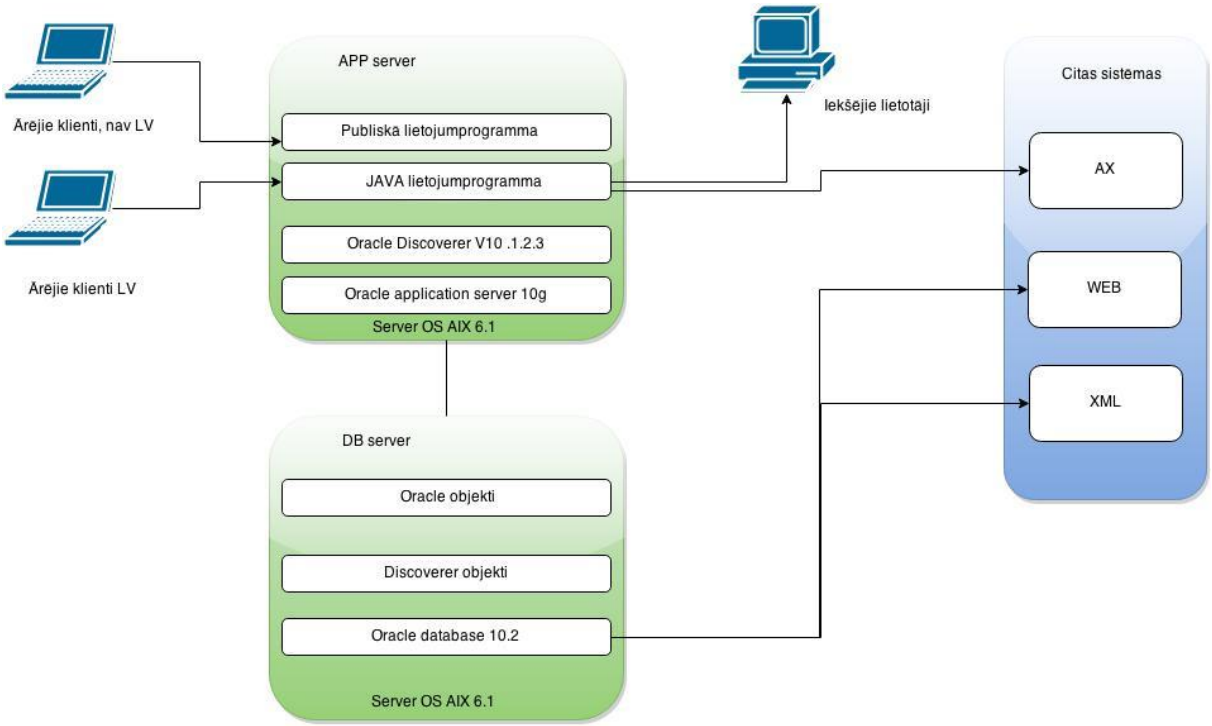
Viens no būtiskiem riskiem ir, ka iepriekš IS izstrādes pārvaldei nebija kopējas vīzijas saistībā ar uzņēmuma nospraustajiem mērķiem. Uzņēmuma pārvaldes savā starpā neuzturēja komunikāciju. Uzņēmumā IS pārvaldes un Grāmatvedības pārvaldes starpā valdīja nesaskaņas un komunikācijas trūkums, jo sistēma nespēja nodrošināt esošā biznesa prasības Kā piemēru, var minēt rēķinu izrakstīšanas nekorektiem klientiem, kā arī nereti rēķinos uzrādītās summas nesakrita ar grāmatvedības sistēmām uzrādītajām summām. Lai novērstu kļūdas, iepriekš netika analizēta situācija, kāpēc tā notiek, bet gan veikta datu labošana datubāzē. Šāda prakses piekopšana ir nekorekta un no sistēmas viedokļa bīstama, jo ar laiku var tikt sabojāta datu integritāte sistēmā.

3.3 Sistēmas drošības riska mazināšana

Uzņēmumā lielākais drauds pēc riska analīzes tika konstatēts, ka tā ir Polišu sistēma, kura darbojas uz izstrādātāja neatbalstītas lietojumprogrammas un datubāzes versijas. Līdz ar to, lai mazinātu draudus IS drošībai uzņēmumā un būtu iespējams nākotnē veikt citus ar sistēmas drošības uzlabošanu saistītus pasākumus ir nepieciešams veikt sistēmas migrāciju uz izstrādātāja atbalstītu programmatūras un datubāzes versiju. Lai veiktu sistēmas atjaunināšanu nepieciešams izstrādāt projektu, lai saprastu katras atbildīgās personas lomu veicamajās darbībās. Projekta izstrādē piedalījās uzņēmuma 2 IS administratori un viens IT administrators, kura pienākumos projekta ietvaros bija veikt serveru atjaunināšanu un tīkla konfigurēšanu atbilstoši funkcionalitātei. No izstrādātāja puses projektā piedalījās sistēmas izstrādes vadītājs, 3 programmētāji un 2 sistēmanalītiķi. Autors projekta realizācijas laikā pildīja IS administratora un projekta vadītāja pienākumus.

Projekta realizācija tika sadalīta 3 etapos. 1. etapā tika veikta datubāzes versijas maiņa, 2. etapā ārējās lietojamās programmatūras versijas maiņa, un 3. etapā iekšēji lietojamās programmatūras versijas maiņa. Tas tika darīts ar mērķi, jo tad būtiski samazinājās iespējamība, ka sistēmai, veicot atjaunināšanu, var tikt konstatētas kļūdas un tā rezultātā var tikt sabojāti dati, kurus būtu nepieciešams atgūt no rezerves kopijām. Sākotnējā projekta plānojumā bija paredzēts atjaunināšanu veikt divos etapos no sākuma, veicot datubāzes atjaunināšanu un tad veicot lietojumprogrammu atjaunināšanu. Tas būtiski palielinātu risku, ka sistēma klientiem var būt nepieejama vienu dienu, kas uzņēmumam radītu ievērojamus zaudējumus un klientu neapmierinātību.

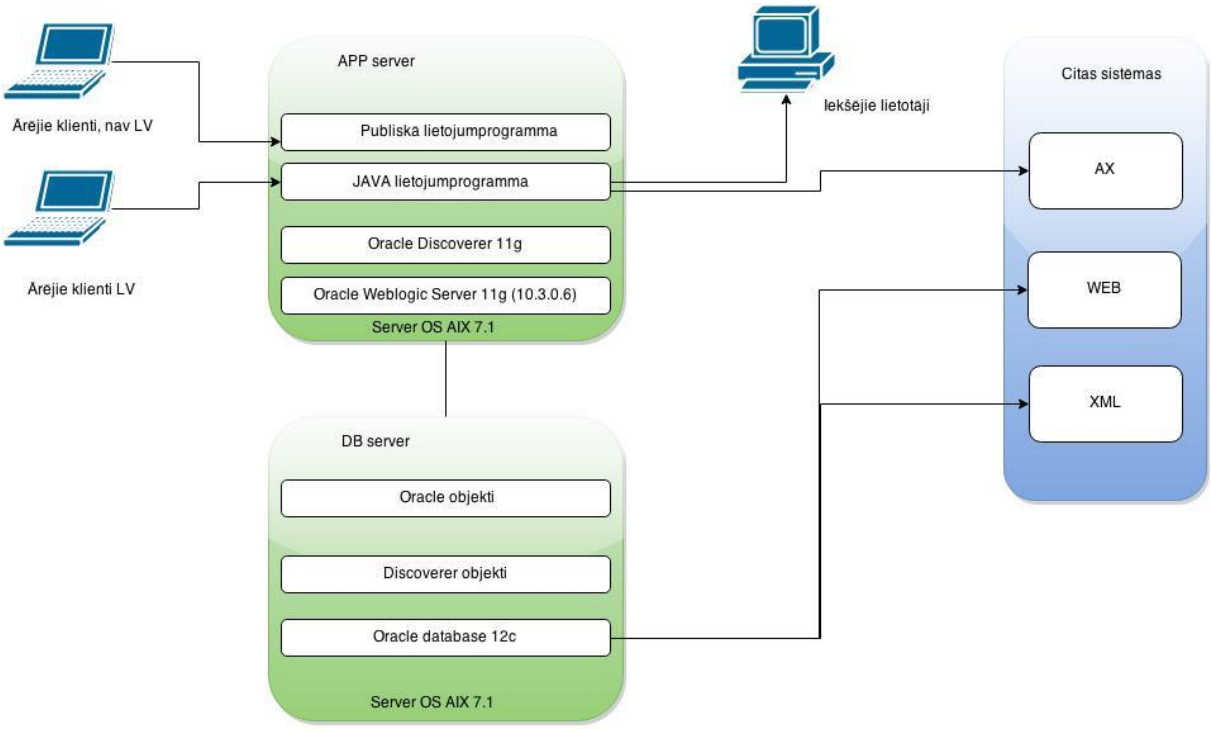
Projekta ietvaros tika atjauninātas IS arhitektūras shēmas. Esošā IS arhitektūrā att. 3.4 redzams, ka sistēmai ir divas lietojumprogrammas. Pie publiskās lietojumprogrammas slēdzas lietotāji, kas nav Latvijas klienti, lietojumprogramma tika izveidota un piesaistīta esošai sistēmai, kad uzņēmums sāka orientēties uz tirgu ārpus Latvijas.



3.4 att. **Iepriekšējā Polišu sistēmas arhitektūras shēma uzņēmumā 2014. gadā (44)**

JAVA lietojumprogrammai ir iekšēja un ārēja piekļuve. Iekšējā piekļuve tiek nodrošināta lietotājiem izmantojot SSO, savukārt ārējiem lietotājiem izmantojot lietotājvārdu un paroli. Sistēmai tiek nodrošināta integrācija ar grāmatvedības un uzskaites sistēmu Microsoft Dynamics AX. Integrācija tiek veikta ar tīmekļa servisu palīdzību. Sistēmai ir izveidota sasaiste ar tīmekļa vietni, kurās tiek norādītas OCTA un KASKO polišu cenas. Datu nosūtīšanai tiek izmantots tīmekļa serviss vai XML fails.

Attēlā 3.5 ir redzama IS arhitektūras shēma, kurā izmaiņas ir veiktas lietojumprogrammas servera versijas nomaiņā uz WebLogic 11g serveri, jo pēc Oracle dokumentācijas migrāciju uz WLS tiek piedāvāta kā vienīgā iespēja, Oracle lietojumprogrammu serveris (*OAS*) vairs netiek atbalstīts.(35) Datubāzes versija tiek atjaunināta no 10g uz 12c. Migrācijas laikā tika veikta lietojumprogrammas servera un datubāzes servera operētājsistēmas maiņa no AIX 6.1 uz AIX 7.1. Tas tika veikts, jo paredzēts, ka migrācijas 2. etapā publiskā lietojumprogramma uz laiku tiks izvietota uz datubāzes servera, kamēr aplikāciju serverim netiks veikta AIX migrācija, kuru var veikt tikai pēc Java lietojumprogrammas atjaunināšanas.



3.5 att. **Jaunā Polišu sistēmas arhitektūras shēma uzņēmumā, ieviesta 2015. gadā(44)**

Projekta realizācija kopējais darbības laiks bija 8 mēneši, bet plānošanas un sanāksmju organizēšana aizņēma 2 mēnešu. Projekta realizācijas termiņi pa etapiem ir redzami tabulā Nr. 3.7. Vienas no būtiskākajām problēmām projekta laikā bija uzņēmuma lietotāju iesaistīšana sistēmas migrācijas procesā, jo sistēmas akcepttestēšana bija jāveic lietotājiem. Migrācijas ietvaros tika veikta augsta līmeņa testa scenāriju izstrāde esošajai sistēmai. Ar scenāriju palīdzību laika gaitā tiks atjaunināta sistēmas funkcionalitātes dokumentācija. 1. Pielikumā ir

aplūkojama daļa no sistēmas funkcionālā testa scenārija. Izstrādājot sistēmas funkcionalitātes testus, svarīgi ir nodefinēt kvalitatīvus un pēc iespējas dažādākus testa scenārijus, kas nodrošinās sistēmas veiksmīgu migrāciju. Līdz ar projekta uzsākšanu tika konstatēts, ka esošā sistēmā netiek izmantota daļa sistēmas funkcionalitātes, ar ko tiek veiktas darba plūsmu uzskaites funkcijas.

Projekta realizācijas termiņi pa etapiem (44) *3.7. tabula*

Atjauninašanas	**Sistēmas elements**	**Termiņš**	**Paveikts**
1.etaps	Datubāze tika migrēta no 10g uz 12c. Lietojumprogrammas versija paliek 10g.	14.11.14	**12.11.14**
2.etaps	Publiskā lietojumprogramma tika pielāgota darbam ar Oracle 12c datubāzi	15.12.14	**10.12.14**
3.etaps	JAVA lietojumprogramma tika migrēta uz WebLogic serveri 11g un pielāgota darbam ar Oracle 12c datubāzi.	7.04.2015	**06.04.15**

Veicot sistēmas datubāzes un lietojumprogrammas atjauninašanu, kopumā tika reģistrētas 28 migrācijas kļūdas, kuras vairumā gadījumu bija saistītas ar nekorekta teksta formatējuma attēlošanos un atskaišu datņu faila paplašinājuma problēmām. Viena no būtiskām kļūdām, kas šobrīd nav atrisināta, un kas ir drauds IS drošībai uzņēmumā ir SSO funkcionalitāte. Kļūdas iemesls ir WebLogic servera atšķirīgā java konfigurācijas faila interpretācija domēna kontrolierim. Sistēmai lietotāji var piekļūt, izmantojot lietotājvārdu un paroli. Projekta laikā, veicot intervijas ar lietotājiem, saistībā ar biznesa scenāriju un akcepttestu izveidi tika konstatēts, ka daļai lietotāju nav informācijas par sistēmas funkcionalitāti, jo lietotāji paļaujas uz kolēģu sniegtajām rekomendācijām sistēmas lietošanā. Līdz ar to tas ir drošības risks, ka sistēmā veiktās lietotāja darbības ir nekorektas, jo nav pieejama sistēmas lietošanas instrukcija.

SECINĀJUMI UN PRIEKŠLIKUMI

Maģistra darbā izvirzītie mērķi ir sasniegti, pētījuma rezultātā ir identificēti šādi turpmāk minētie secinājumi.

1. Šobrīd spēkā esošajā LR normatīvajā regulējumā, vidējiem un mazajiem uzņēmumiem, kā arī valsts un pašvaldību iestādēm, ja vien tie nav finanšu un kapitāla tirgus dalībnieki vai arī to pārraudzībā nav valsts informācijas sistēmas, drošības nepieciešamību nosaka nozares standarti, rekomendācijas un vadlīnijas.
2. Ieviešot uzņēmumā IS drošības standartus, par piemēru var ņemt Valsts informācijas sistēmu vispārējās drošības prasības MK noteikumus Nr. 765., jo tie netieši ietver ISO 27001 standarta prasības.
3. Konfidenciālas informācijas un datu zudums var radīt kaitējumu ne vien pašam uzņēmumam un tā darbiniekiem, bet arī klientiem. Līdz ar to ir svarīgi informēt darbiniekus par vispārējām drošības prasībām, jo nereti konfidenciālu informāciju no uzņēmuma iznes viņi to pat neapzinoties.
4. Veicot pieslēgumus publiski pieejamiem bezvadu tīkliem, ieteicams pieslēgumam izmantot VPN, kurā tiek nodrošināta datu šifrēšana. Tāpat nepieciešams veikt regulāri sistēmas lietojumprogrammu atjaunināšanu, pastiprinātu uzmanību pievēršot interneta pārlūku, Java un Adobe Flash atjauninājumiem, jo ne vienmēr antivīruss spēj aizsargāt gala iekārtu pret ļaunatūru.
5. Procesu plānošana ir veids, kā pilnveidot biznesa mērķus, un īstenot izvēlēto stratēģiju, jo bez mērķiem procesi ir maz noderīgi. Līdz ar to, lai veiktu uzņēmuma biznesa procesu pielāgošanu IS drošībai, par pamatu būtu nepieciešams ņemt COBIT standartu, jo tajā ir grafiski attēlotas procesu shēmas, kur katram apvienotajam procesam tiek noteikti atbilstoši kontroles mērķi.
6. Informācijas sistēmas drošības organizēšanu uzņēmumā nepieciešams organizēt, sākot ar IS drošības politikas, risku analīzi, informācijas klasifikāciju, IS drošības un lietošanas noteikumu izveidi, un darbības atjaunošanas un nepārtrauktības plāna izstrādi.
7. IS drošības noteikumi ir kā pamats IS pārvaldes darbam, jo tajos tiek atrunātas problēmu pieteikšanas procedūras un lietotāju pienākumi, tādā veidā nodalot lietotāju atbildību no IS pārvaldes atbildības.

8. Izstrādājot biznesa nepārtrauktības un atjaunošanas plānu par pamatu nepieciešams ņemt uzņēmuma informācijas sistēmu un tehnoloģisko iekārtu uzskaitījumu. Ja tāds uzskaitījums nav izveidots, tad plānu nav iespējams sastādīt kvalitatīvu. Līdz ar to, kā pamatu tehnoloģisko un informācijas sistēmu uzskaitījumam var minēt pilnvērtīgu IS/IT audita veikšanu uzņēmumā, kas sniegs informāciju par tehnoloģiskajām iekārtām un to sasaisti.
9. Ieviešot datu zudumu un noplūdes programmatūru uzņēmuma tīklā, kā labo praksi var minēt, ka programmatūras drošības politikā ir iestatīta lietotāju informēšana un izglītošana, ka pārkopētā vai nosūtītā informācija var saturēt uzņēmumam konfidenciālus datus.
10. Labi izstrādāta drošības politika nodrošina to, ka uzņēmums var veikt savas primārās biznesa funkcijas pat tādā gadījumā, ja notiek incidents, kura laikā nepieciešams rīkoties atbilstoši biznesa nepārtrauktības plānam vai atjaunošanas plānam, kopumā drošība uztur uzņēmuma dzīvotspēju un ļauj tam veikt biznesa primārās funkcijas
11. Uzņēmumā vienmēr pastāvēs risks, ka kāds no darbiniekiem var veikt datu nopludināšanu, ne vienmēr pie tā ir vainojamas ar sistēmu saistītas drošības problēmas. Jāatceras, ka uzņēmuma lielākais drošības drauds ir IT resursu lietotājs.
12. Uzņēmumiem būtu jāseko līdzi jaunākajām tendencēm un risku pārvaldības plāna dokumentācijā jāaktualizē riski, kas var būt saistīti ar darbinieku lietoto datu drošību ārpus uzņēmuma, jo uzņēmumi koncentrējas uz iekšējiem riskiem nevis uz ārējiem.
13. IT ir stratēģisks veicinātājs biznesa attīstībā, nevis izmaksu centrs, un savstarpējā komunikācija ir atslēga uz veiksmīgu risinājumu realizēšanu.
14. Maģistra darba ietvaros analizētā uzņēmuma būtiskākie šķēršļi ISO standarta ieviešanā ir dokumentācijas neatbilstība reālajai situācijai uzņēmumā.
15. Kā būtiskākie šķēršļi IS drošības nodrošināšanai uzņēmumā ir pārvalžu savstarpējās komunikācijas trūkums.
16. Veicot risku analīzi, tika konstatēts, ka vairākām informācijas sistēmām riska vērtība ir ievērojami augstāka, nekā uzņēmumā pieļaujamā.
17. Pēc riska analīzes tika konstatēts, ka uzņēmumā lielākais drauds IS drošībai ir Polišu sistēma, līdz ar to sistēmai tika veikta lietojumprogrammas un datubāzes versijas atjaunošana.

Balstoties uz secinājumiem un veiktajiem uzdevumiem, autors izteicis zemāk esošos priekšlikumus.

1. Izvēloties viena konkrēta IS drošības standarta ieviešanu uzņēmumā, būtu nepieciešams izpētīt, vai kāds no citiem standartiem nebūs atbilstošāks, piemēram ITIL, kura pamatā ir sakārtot incidentu pārvaldību.
2. Uzņēmuma darbiniekiem nepieciešams veikt regulāras apmācības, kurās tiek demonstrēti praktiski ieteikumi un padomi kā pasargāt savu privātumu.
3. Mazinot riskus IS drošībai, ieviešot tehnoloģiskus risinājumus, nedrīkst aizmirst par informācijas sistēmām, uz kurām balstās uzņēmuma pamatdarbība.
4. Vairāk izmantot COBIT standartu Latvijā, jo tas netieši ietver ITIL un ISO standarta nostādnes.

IZMANTOTĀ LITERATŪRA UN AVOTI

LR likumi

1. LR likums *Komerclikums.* Saeima un Valdības Ziņotājs, Nr. 11, 01.06.2000.
2. LR likums *Fizisko personu datu aizsardzības likums.* Saeima un Valdības Ziņotājs, Nr. 9, 04.05.2000.
3. LR MK noteikumi Nr. Nr.765 *Valsts informācijas sistēmu vispārējās drošības prasības.* Latvijas Vēstnesis, Nr. 164. 2005.
4. LR MK noteikumi *Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi*, Finanšu un kapitāla tirgus komisija, Nr.49, 01.04.2014.

Grāmatas

5. **Addy R.,** *Effective IT Service Management: To ITIL and Beyond!*, Berlin: Springer-Verlag Berlin Heidelberg, 2007. 46 p.
6. **Rolf M. von Roessing,** *The Business Model for Information Security*, Germany: ISACA, 2009.
7. **National Research Council of the National Academies**, *Information Assurance for Network-Centric Naval Forces,* Washington, D.C., 2010. 72 – 82 p.
8. **National Research Council**, *Realizing the Potential of C4I*, National Academy Press, Washington, D.C., 1996. 131 – 142 p
9. **Softwareblades,** *Data Loss Prevention Admin Guide. Check Point,* Israel Telaviv, 2011. 147 p.
10. **CLUSIF**, *Information Systems Threats and Security Practices in France,* France, 2008. 34 p par recovery plānu

Žurnāli

11. **Rich MogullIs** *DLP keeping your data where it should be?Information Security*, 2009. Nr. 4, 12-22 p
12. **Dr Pramath Raj Sinha,** *IT NEXT - Security will Shift from 'IT problem' to Executive Problem' in 2015,*2015 March, 6 p

Zinātniskie raksti

13. **T. Sommestad, M. Ekstedt, H. Holm, M. Afzal,** *Security mistakes in information system deployment projects,* 2011, www.emeraldinsight.com/0968-5227.htm (skatīts 20.04.2015.)

14. **G. Stoneburner, A. Goguen, A. Feringa**, *Risk Management Guide for Information Technology Systems*, 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (skatīts 22.04.2015.)
15. **E.Teteris**, *Datu zuduma un noplūdes novēršana,* Rīga, 2013, 31. – 37. lpp.

Elektroniskās informācijas avoti

16. *Policijas ieteikumi e-pasta un e-vides drošībai*. Pieejams: http://m.lvportals.lv/visi/likumi-prakse/167351-policijas-ieteikumi-e-pasta-un-e-vides-drosibai/ (skatīts 22.04.2015.)
17. *Data Security: Top Threats to Data Protection.* Pieejams: http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf (skatīts 20.04.2015.)
18. *IT drošības politika un normatīvie akti.* Pieejams:https://www.cert.lv/section/show/49 (skatīts 22.04.2015.)
19. *Information technology - Security techniques - Code of practice for information security controls.* Pieejams: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533 (skatīts 21.04.2015.)
20. *Information technology - Security techniques - Information security management systems – Requirements*. Pieejams: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534 (skatīts 21.04.2015.)
21. *Information technology - Security techniques - Information security risk management.* Pieejams: http://www.iso.org/iso/catalogue_detail?csnumber=56742 (skatīts 22.04.2015.)
22. *ITIL V3 Application Support.* Pieejams: http://www.itservicemanagement-itil.com/wp-content/downloads/ITIL-V3-Application-Support.pdf (skatīts 22.04.2015.)
23. *ITSM (IT Service Management) definition.* Pieejams: http://searchcio.techtarget.com/definition/ITSM (skatīts 23.04.2015.)
24. *Resursu klasifikācijas un risku analīzes piemērs virtuālai iestādei.* Pieejams:https://cert.lv/uploads/uploads/resursu_klasifikacija_risku_nov20111011web2.pdf (skatīts 22.04.2015.)
25. *Sertifikācija.*Pieejams:http://www.bureauveritas.lv/wps/wcm/connect/bv_lv/local/home/about-us/our-business/certification (skatīts 28.04.2015.)

26. *Informācijas tehnoloģiju Infrastruktūras bibliotēka (ITIL) metožu pielietošana un adaptēšana.* Pieejams: http://aict.itf.llu.lv/files/rakstkraj/2006/Tukris_LV_2006.pdf (skatīts 01.05.2015.)
27. *The comprehensive IT governance framework that addresses every aspect of IT and integrates all of the main global IT standards.* Pieejams: http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-4.1-Brochure.pdf (skatīts 06.05.2015.)
28. *Informācijas drošības sistēma.* Pieejams:https://www.lv.lv/?menu=par_mums&sid=51 (skatīts 28.04.2015.)
29. *A Business Model for Information Security.* Pieejams:http://www.nis-summer-school.eu/nis09/presentations/15-Le-Roux.pdf (skatīts 29.04.2015.)
30. *Drošas informācijas sistēmas – mīts vai realitāte?* Pieejams: https://www.kpmg.com/LV/lv/IssuesAndInsights/ArticlesPublications/Publicationseries/Documents/Forum%203%20-%20Junijs%202014/Dro%C5%A1as%20inform%C4%81cijas%20sist%C4%93mas%20%E2%80%93m%C4%ABts%20vai%20realit%C4%81te%20(12-14).pdf (skatīts 02.05.2015.)
31. *Kā integrēt IT sadaļu iekšējā audita plānā vai Integrētā auditēšana.* Pieejams: http://iai.lv/wp-content/uploads/2.4-Juris-Ziedins-Intergetais-audits.pdf (skatīts 29.04.2015.)
32. *An Overview of Information Security Standards.* Pieejams: http://www.infosec.gov.hk/english/technical/files/overview.pdf (skatīts 29.04.2015.)
33. *The transformation of IT Risk Management.* Pieejams: https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/transformating-it-risk-management.pdf (skatīts 04.05.2015.)
34. *Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas.* Pieejams: http://varam.gov.lv/lat/darbibas_veidi/e_parv/vis/?doc=12650 (skatīts 28.04.2015.)
35. *Information Systems Security Control Guidance Document.* Pieejams: http://www.selectagents.gov/resources/Information_Systems_Security_Control_Guidance_version_3_English.pdf (skatīts 18.04.2015.)
36. *Oracle JDeveloper and Application Development Framework 11g.* Pieejams: http://www.oracle.com/technetwork/developer-tools/jdev/index-091111.html (skatīts 10.05.2015.)

37. *Izplatās bīstams datorvīruss "CTB Locker".* Pieejams: https://cert.lv/resource/show/603 (skatīts 12.05.2015.)
38. *Rekomendācija "Personas datu aizsardzība darba vietās". (2013)* Pieejams: http://www.dvi.gov.lv/lv/jaunumi/publikacijas/ (skatīts 13.05.2015.)
39. *Uzņēmuma datu noplūdes dēļ var ciest klienti.* Pieejams: http://www.reitingi.lv/lv/news/zinatne/76480-uznemuma-datu-nopludes-del-var-ciest-klienti.html (skatīts 04.04.2015.)
40. *Understanding and Selecting aData Loss Prevention Solution.* Pieejams: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf (skatīts 09.05.2015.)
41. *Best Practices for PreventingEnterprise Data*. Loss. Pieejams: http://www.nascio.org/committees/security/securityVideo/whitepapers/emc.pdf
42. *FAIR–ISO/IEC27005 Cookbook.* Pieejams: http://www.businessofsecurity.com/docs/FAIR%20-%20ISO_IEC_27005%20Cookbook.pdf (skatīts 06.05.2015.)
43. *ISACÁs Business Model for Information Security (BMIS).* Pieejams: http://www.emi-tuv.hu/uploads/images/133715495692449312025 9/isaca-bmis-prezi-hgk.pdf (skatīts 12.05.2015.)
44. Uzņēmuma "X" nepublicētie materiāli.

PIELIKUMI

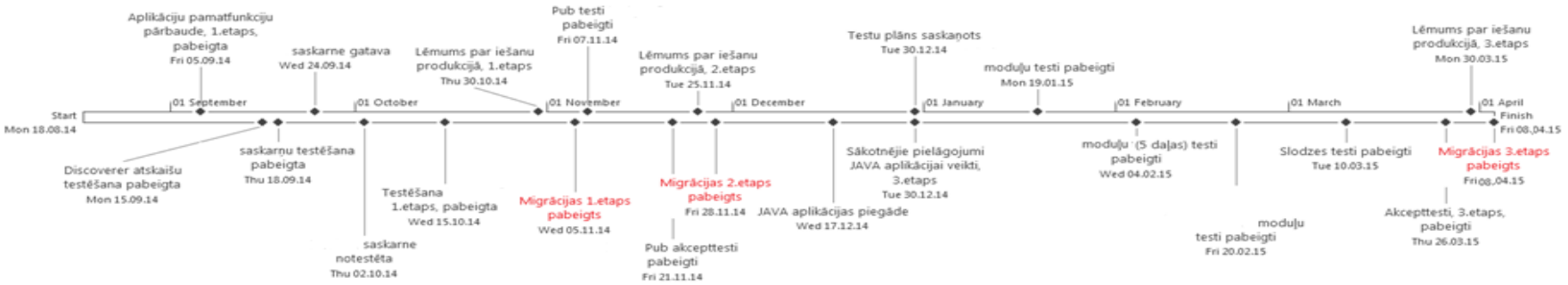
1. Pielikums. Sistēmas funkciju testpiemēri: modulis „Administrācija”

Biznesa scenārijs	Testu grupa	Priekšnosacījumi	Veicamās darbības	Sagaidāmais rezultāts	Lietotājs
1.1	**Lietotāju lomu un kontu administrēšana**				
1.1.1	**IP reģiona veidošana**				
1.1.1.1	ADMIN		Atver formu "Administrācija" → "IP reģioni"	Atveras forma ar pilnu sarakstu, pieejamas pogas [Atlasīt], 2x [Atcelt]	test_user (Admin)
1.1.1.2	ADMIN		Nospiež pogu [Atlasīt]	Atveras meklēšanas kritēriju sadaļa ar pogu [Meklēt]	test_user (Admin)
1.1.1.3	ADMIN		Ievada atlases parametrus un nospiež pogu [Meklēt]	Tiek atlasīts saraksts pēc ievadītajiem parametriem	test_user (Admin)
1.1.1.4	ADMIN		Nospiež pogu [Pievienot]	Atveras rediģēšanas forma ar pieejamām pogām [Saglabāt], [Atcelt], [Dzēst]	test_user (Admin)
1.1.1.5	ADMIN		Pārbauda formas pieejamo pogu darbību: [Izvēlēties no saraksta], [Izvēlēties no izkrītošā saraksta], [Kalendārs], [Ķekš rūtiņas], [Dzēst lauka vērtības] u.c.	Pogas darbojas: atver sarakstu, notīra lauka vērtību, atzīmē ķekšrūtiņu, atver kalendāru, krāsu izvēle utt.	test_user (Admin)
1.1.1.6	ADMIN		Formā veic datu izmaiņas un nospiež pogu [Saglabāt]	Izvada ziņojumu par veiksmīgu datu saglabāšanu, pieejama apakšforma	test_user (Admin)
1.1.2	**Lietotāja konta veidošana**				
1.1.2.1	ADMIN		Atver formu "Administrēšana" → "Lietotājs"	Atveras forma ar pilnu sarakstu, pieejamas pogas [Atlasīt], 2x [Atcelt]	test_user (Admin)
1.1.2.2	ADMIN		Nospiež pogu [Atlasīt]	Atveras meklēšanas kritēriju sadaļa ar pogu [Meklēt]	test_user (Admin)

1.1.2.3	ADMIN		Ievada atlases parametrus un nospiež pogu [Meklēt]	Tiek atlasīts saraksts pēc ievadītajiem parametriem	test_user (Admin)
1.1.2.4	ADMIN		Nospiež pogu [Pievienot]	Atveras rediģēšanas forma ar pieejamām pogām [Saglabāt], [Atcelt], [Dzēst]	test_user (Admin)
1.1.2.5	ADMIN		Pārbauda formas pieejamo pogu darbību: [Izvēlēties no saraksta], [Izvēlēties no izkrītošā saraksta], [Kalendārs], [Ķekš rūtiņas], [Dzēst lauka vērtības] u.c.	Pogas darbojas: atver sarakstu, notīra lauka vērtību, atzīmē ķekšrūtiņu, atver kalendāru, krāsu izvēle utt.	test_user (Admin)
1.1.2.6	ADMIN		Formā veic datu izmaņas un nospiež pogu [Saglabāt]	Izvada ziņojumu par veiksmīgu datu saglabāšanu un tiek uzrādītas 4 apakšformas: "Lomas", "IP reģioni", "Lietotāju grupas", "Pieejamība" un pieejamas pogas [Saglabāt], [Bloķēt], [Dzēst], [Atcelt]	test_user (Admin)
1.1.3	**IP reģiona pievienošana jaunam lietotāja kontam**				
1.1.3.1	ADMIN		Atver apakšformu "IP reģioni"	Formā atveras pilns saraksts ar pieejamām pogām [Pievienot]	test_user (Admin)
1.1.3.2	ADMIN		Nospiež pogu [Pievienot]	Atveras rediģēšanas forma ar pieejamām pogām [Saglabāt], [Atcelt], [Dzēst]	test_user (Admin)
1.1.3.3	ADMIN		Pārbauda formas pieejamo pogu darbību: [Izvēlēties no saraksta], [Izvēlēties no izkrītošā saraksta], [Kalendārs], [Ķekš rūtiņas], [Dzēst lauka vērtības] u.c.	Pogas darbojas: atver sarakstu, notīra lauka vērtību, atzīmē ķekšrūtiņu, atver kalendāru, krāsu izvēle utt.	test_user (Admin)
1.1.3.4	ADMIN		Formā veic datu izmaiņas un nospiež pogu [Saglabāt]	Izvada ziņojumu par veiksmīgu datu saglabāšanu	test_user (Admin)
1.1.4	**Lietotāja grupas pievienošana jaunam lietotāja kontam**				
1.1.4.1	ADMIN	ADMIN_022	Atver apakšformu "Lietotāju grupas"	Formā atveras pilns saraksts ar pieejamām pogām [Pievienot]	test_user (Admin)

1.1.4.2	ADMIN		Nospiež pogu [Pievienot]	Atveras rediģēšanas forma ar pieejamām pogām [Saglabāt], [Atcelt], [Dzēst]	test_user (Admin)
1.1.4.3	ADMIN		Pārbauda formas pieejamo pogu darbību: [Izvēlēties no saraksta], [Izvēlēties no izkrītošā saraksta], [Kalendārs], [Ķekš rūtiņas], [Dzēst lauka vērtības] u.c.	Pogas darbojas: atver sarakstu, notīra lauka vērtību, atzīmē ķekšrūtiņu, atver kalendāru, krāsu izvēle utt.	test_user (Admin)
1.1.4.4	ADMIN		Formā veic datu izmaiņas un nospiež pogu [Saglabāt]	Izvada ziņojumu par veiksmīgu datu saglabāšanu	test_user (Admin)
1.1.5	**Lietotāja lomas pievienošana jaunam lietotāja kontam**				
1.1.5.1	ADMIN	ADMIN_022	Atver apakšformu "Lomas"	Formā atveras pilns saraksts ar pieejamām pogām [Pievienot]	test_user (Admin)
1.1.5.2	ADMIN		Nospiež pogu [Pievienot]	Atveras rediģēšanas forma ar pieejamām pogām [Saglabāt], [Atcelt], [Dzēst]	test_user (Admin)
1.1.5.3	ADMIN		Pārbauda formas pieejamo pogu darbību: [Izvēlēties no saraksta], [Izvēlēties no izkrītošā saraksta], [Kalendārs], [Ķekš rūtiņas], [Dzēst lauka vērtības] u.c.	Pogas darbojas: atver sarakstu, notīra lauka vērtību, atzīmē ķekšrūtiņu, atver kalendāru, krāsu izvēle utt.	test_user (Admin)
1.1.5.4	ADMIN		Formā veic datu izmaiņas un nospiež pogu [Saglabāt]	Izvada ziņojumu par veiksmīgu datu saglabāšanu	test_user (Admin)

2. Pielikums. Kalendārais plāns



Maģistra darbs „Uzņēmuma informācijas sistēmu datu zudumu un noplūdes novēršana” izstrādāts LU Ekonomikas un vadības fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un darba elektroniskā kopija atbilst izdrukai.

Autors: Edgars Teteris _____

Rekomendēju darbu aizstāvēšanai

Vadītājs: asoc.prof. Uldis Rozevskis _____

Recenzents: lektore Ilze Baļčūne

Darbs iesniegts Akadēmisko studiju programmu dekanātā __.05.2015.

Metodiķe: Anita Rudāja _____

Darbs aizstāvēts maģistra gala pārbaudījuma komisijas sēdē

_____

Komisijas sekretāre: _____