LATVIJAS UNIVERSITĀTE
EKONOMIKAS UN VADĪBAS FAKULTĀTE
TIRGZINĪBU KATEDRA

VALSTS UN PAŠVALDĪBAS IESTĀŽU DATU CENTRU NEPĀRTRAUKTAS DARBĪBAS NODROŠINĀŠANAS KVALITĀTE

THE QUALITY ASSURANCE FOR CONTINUOUS OPERATION OF PUBLIC DATA CENTERS

BAKALAURA DARBS

Autors: Vadības zinību bakalaura
studiju programmas
Kvalitātes vadības
studiju virziena
5.kursa students
Viesturs Šķila
(VadZ030660)

Darba vadītāja:
Dr. sc. eng., doc.Ilga Karlsone

RĪGA 2007

Saturs

Anotācija

Ikkatrs no mums, strādājot uzņēmumos un organizācijās, ikdienā saskaras ar dažāda rakstura daudzveidīgu informāciju. Tā tiek saņemta, reģistrēta, uzkrāta, analizēta, apstrādāta, lietota un izplatīta. Pamatojoties uz šo informāciju, tiek pieņemti lēmumi, veiktas noteiktas darbības izvirzīto mērķu sasniegšanai. Straujais informācijas tehnoloģiju progress ir radījis apstākļus, ka mūsdienīgs un attīstīts uzņēmums vai organizācija nevar iztikt bez specifiska informācijas tehnoloģiju atbalsta. Pieņemot, ka lielākā lietotās informācijas daļa tiek uzkrāta un apstrādāta informācijas sistēmās, informācijas sistēma/programmatūra ir pamats veiksmīga uzņēmuma iekšējās darbības efektivitātes paaugstināšanai, sadarbības uzlabošanai ar klientiem un sadarbības partneriem, kā arī pamats jaunu produktu izstrādei un virzībai tirgū. Tā ir neapšaubāma nepieciešamība gan šodien, gan attīstībai paredzamā nākotnē.

Informācijas sistēmu nepārtrauktas darbības un pieejamības garants ir stabila organizācijas datu centra darbība. Neskatoties uz datu centru attīstības perspektīvu pasaules skatījumā, darba autors ikdienā ir saskāries ar būtisku problēmu – valsts pārvaldes iestāžu vadība nepievērš lielu vērību atbilstošas serveru telpas elektroapgādes un mikroklimata nodrošināšanai. Bieži vien informācijas tehnoloģiju ekspertu centieni panāk lielāku finansējumu serveru telpu modernizēšanai, atduras pret organizācijas vadības neizpratni un norobežošanos.

Bakalaura darbā „Valsts un pašvaldības iestāžu datu centru nepārtrauktas darbības nodrošināšanas kvalitāte" tiek pētīti spēkā esošo Latvijas normatīvo aktu un standartu prasības informācijas sistēmu aizsardzībai valsts pārvaldes iestādēs un pašvaldībās, raksturota organizācijas „N" datu centru atbilstība normatīvo aktu prasībām. Izstrādāta datu centra pakalpojuma kvalitātes līmeņa klasifikācija un noteikta organizācijas „N" datu centra esošā situācija un nepieciešamā atbilstība autora piedāvātajam datu centru pakalpojuma kvalitātes līmenim.

Bakalaura darbā izmantotās metodes ir literatūras pētījumi, autora pieredze, anketēšana, iegūto rezultātu statistiskā analīze un grafiskā metode. Pētījums veikts 2007.gadā.

Darba rezultāti var tikt izmantoti kā vadlīnijas citu valsts iestāžu organizācijas datu centru nepārtrauktas darbības kvalitātes līmeņa atbilstības noteikšanai.

Darbs sastāv no 3 nodaļām un 18 apakšnodaļām. Darba apjoms ir 72 lpp, t.sk. 13 attēli un 2 tabulas. Izmantotās literatūras sarakstā ir 31 pozīcijas latviešu un angļu valodā.

Annotation

In a daily work everybody has to deal with a huge amount of multiple types of information. Usually this information is received, stored, analyzed, processed, used and redistributed. Based on this information all kinds of specific decisions are made to reach defined business targets. Recent fast growth of information technology caused a circumstance that a modern organization cannot properly function without information systems support. Assuming that the largest part of used data is collected and updated in information systems, program supply is the basis for a successful operational efficiency improvement. This is, however, also a foundation for improvement of client relationships and fruitful business partnerships. Beside that it is important for development of new products and prediction of new market tendencies. Doubtlessly up to date information systems are a necessity for today and will be a necessity also in a future.

A warranty for steady and continuous operation and accessibility of information systems is a stable work of organization's data center. Despite of broad spectra of development perspectives of data centers worldwide, the author of the present study concentrated on a topic of supply deficiencies of electricity and microclimate environment within rooms generally dedicated data centers. This is especially a case within state's organizations where adequate attention for an existing problem is not paid from the side of management. Often an effort for gaining finances with a purpose to modernize organization's server rooms meets a resistance and incomprehension form the part of organizations leadership.

Within the present study "The quality assurance for continuous operation of public data centers research has been done regarding Latvian laws and regulations concerning quality and protection of public information systems. Existing situation of a given organization's data center was analyzed and estimated its compliance with present governmental regulations. A classification was developed for quality level estimation. Furthermore, an evaluation of service quality of a given organization's data center was performed according to the developed classification.

Methods used within the present study are: literature, personal experience of author's daily work, questionnaire, interviews, statistical analysis of results and the graphical method. Research was performed in year 2007.

Results of the present study can be used as guidelines for estimation of quality assurance for continuous operation of public data centers within other governmental organizations.

A study consists of 3 parts and 18 sections. It includes 72 pages, 13 figures, 12 tables, and 31 literature citations in Latvian and English languages.

Saīsinājumu un nosacīto apzīmējumu saraksts

BSI	-	Lielbritānijas Standartizācijas organizācija
CPU	-	Centrālā procesora vienība *(Central processing unit)*
I/O	-	Ievades/Izvades operācijas *(Input/output)*
IBM	-	*International Business Machines corporation*
IEC	-	Starptautiskā Elektrotehnikas komisija
IS	-	Informācijas sistēma
ISO	-	Starptautiskā Standartizācijas organizācija
LAN	-	Lokālais datortīkls *(Local area network)*
LV	-	laikraksts Latvijas Vēstnesis
LVS	-	Latvijas Valsts Standarti
MK	-	Ministru Kabinets
PDU	-	Strāvas sadales vienība (*Power Distribution Unit*)
R/W	-	Lasīšanas/Rakstīšanas operācijas *(Read/Write)*
RAM	-	Datortehnikas operatīvās atmiņas modulis *(random access module)*
SAN	-	Disku iekārtu tīkls *(Storage Area Network)*
SUN		*SUN Microsystems corporation*
TIA	-	Telekomunikācijas nozares asociācija (*Telecommunication Industry Association)*
UPS	-	Nepārtrauktas barošanas avots *(Uninterruptible power supply)*
WAN	-	Korporatīvais datortīkls *(Wild area network)*

Ievads

Datu centru pirmsākumi ir meklējami informācijas tehnoloģiju ēras sākumā. Agrāk skaitļošanas sistēmas bija sarežģītas un grūti apkalpojamas. Lai sistēmas darbotos nevainojami, to uzturēšanai un darbināšanai bija nepieciešamas speciālas telpas (*computer rooms*), skaitļošanas iekārtu izvietošanai tika projektētas un būvētas speciālas ēkas. Pirmo paaudžu skaitļotājus raksturoja liels komponenšu savienojošo kabeļu zarojums un milzīgs strāvas patēriņš komponenšu pārkaršanas novēršanai. Skaitļošanas iekārtas bija ļoti dārgas, tāpēc drošības aspekts bija nozīmīgs, jo jaunās tehnoloģijas pārsvarā tika izmantotas militāristu vajadzībām. Tika ieviestas serveru telpu fiziskās pieejas kontroles iekārtas. Tādi datu centriem raksturīgi aprīkojumi, kā iekārtu statnes (*rack*), kas radīja iespēju iekārtas izvietot kompaktāk, dubultās grīdas (*elevated floor*) un kabeļu vadotnes (*cable trays*), kas ļāva komunikācijas izvietot pie griestiem vai zem dubultās grīdas, tika izgudrotas un ieviestas skaitļotāju ēras sākumā (pagājušā gadsimta 50 – 60 gados).

Strauji attīstoties procesoru tehnoloģijām, it īpaši pagājušā gadsimta 80os gados, datori (*microcomputers*) kļuva lētāki un pieejamāki plašākai sabiedrībai. Datoru pielietojums strauji kļuva populārs un sāka parādīties organizāciju birojos, bet lietotāji maz vērības pievērsa datora ekspluatācijas noteikumiem. Tomēr, mikroprocesoru tehnoloģijām kļūstot sarežģītākām, organizācijas sāka just arvien lielāku nepieciešamību pēc kontrolētas informācijas tehnoloģiju vides. Jaunākie zinātniski tehnoloģiskie sasniegumi (klientu-serveru arhitektūra, lēti komunikāciju tīklu risinājumi u.tml.) ļāva organizācijām izvietot nepieciešamo datortehniku pašu organizāciju iekšienē, tā sauktajās serveru telpās (*server rooms*). Šajā laikā arī plašāk pazīstamāks kļuva termins - „datu centrs" (*data center*), ar ko tika apzīmētas speciāli projektētas serveru telpas.

Straujš datu centru attīstības bums pasaulē sākās ar interneta pakalpojumu sfēras straujo attīstību, jeb tā saucamo *dot-com* mājas lapu bumu. Kompānijām bija nepieciešams ātrs pieslēgums pie pasaules tīmekļa (interneta) un nepārtrauktas darbības (*non-stop operational*) datortehnikas un programmatūras risinājumu nodrošinājums, jo interneta pakalpojumi bija kļuvuši internacionāli un klientu loks bija visā pasaulē. Pieprasījums pēc pakalpojuma bija visu diennakti un katra dīkstāves stunda nozīmēja līdz pat vairākiem miljoniem dolāru lielu negūto peļņu.

Mazas kompānijas nevarēja atļauties iegādāties datu centra aprīkojumu un apkalpošanu, tādēļ pagājušā gadsimta 90 gadu beigās parādījās specializētas kompānijas, kas būvēja

atsevišķus ēku kompleksus, sauktus par interneta datu centriem (*internet data centers*), kas sāka sniegt dažāda līmeņa datu centru pakalpojumus. Tika izgudrotas jaunas tehnoloģijas un izstrādāti standarti dažādiem datu centriem, kas nodrošināja lielu un tehnoloģiski sarežģītu informācijas sistēmu darbību dažādos pasaules reģionos. Galu galā arī citas kompānijas sāka attiecināt uz savu datu centru darbības kvalitātes nodrošināšanu ar jaunajā nozarē aprobētajiem standartiem.

Šajā gadsimtā, datu centru plānojums, tehnoloģijas un darbināšana ir pasaulē labi pazīstams process. Dažādu profesionāļu grupas – labāk pazīstamākie ir Telekomunikāciju nozares asociācija (*Telecommunications Industry Association*), informācijas tehnoloģiju giganti *IBM* un *Sun Microsystems* u.c., ir izstrādājušas datu centru kvalitatīvai darbības nodrošināšanai nepieciešamās vadlīnijas. Tomēr vēl daudz ir nepieciešams veikt, lai uzlabotu datu centru pieejamību, samazinātu resursu pašizmaksas un padarītu tos videi draudzīgākus.

Neskatoties uz datu centru perspektīvu pasaules skatījumā, darba autors ikdienā ir saskāries ar būtisku problēmu – valsts pārvaldes iestāžu vadība nepievērš lielu vērību atbilstošas serveru telpas elektroapgādes un mikroklimata nodrošināšanai. Bieži vien informācijas tehnoloģiju ekspertu centieni panākt lielāku finansējumu serveru telpu modernizēšanai atduras pret organizācijas vadības neizpratni un norobežošanos.

Savā darbvietā darba autors konstatējis, ka Latvijā spēkā esošie normatīvie akti nosaka, ka valsts informācijas sistēmas ir jāaizsargā pret apdraudējumiem, bet nav noteikta kārtība vai metodika, kā nodrošināt šādas informācijas aizsardzību. Izņēmums ir valsts finanšu nozare un ar valsts noslēpumu saistītās organizācijas, kuru pārraudzības iestādes ir izdevušas ierobežotas pieejamības noteikumus, kas uzliek par pienākumu veikt atbilstošus tehniskus soļus informācijas aizsardzībai.

Tēmas aktualitāti nosaka fakts, ka, attīstoties informācijas tehnoloģijām un Latvijas valstij realizējot e-pārvaldes projektus, arvien aktuālāks kļūst jautājums par valsts informācijas sistēmu darbību uzturošo datu centru darbības kvalitātes vienotu prasību izveidi. Šobrīd valsts pārvaldes iestāžu vadība pienācīgi nenovērtē vajadzību pēc datu centru (tajā skaitā, serveru telpu) vienotas vides prasībām – elektrības padevi, mikroklimata kontroli, fizisko un loģisko pieejas drošību, kas bieži vien ir par iemeslu neplānotām informācijas sistēmas nepieejamībām, nekvalitatīvu iedzīvotājiem sniegtu pakalpojumu, līdz pat iestādes dīkstāvei, kas negatīvi ietekmē valsts pārvaldes iestāžu pamatfunkciju veikšanu.

Bakalaura darba **mērķis** ir izpētīt Latvijā spēkā esošos normatīvos aktus un analizēt tajos izvirzītos nosacījumus valsts iestāžu datu centru darbības kvalitātei, noskaidrot un analizēt ar organizācijas „N" datu centra darbības kvalitāti saistītās problēmas, izstrādāt priekšlikumus

datu centru klasifikācijai un vadlīnijas nepārtrauktas datu centra darbības nodrošināšanas kvalitātei.

Pamatojoties uz bakalaura darba mērķi, tiek izstrādāti **darba uzdevumi**:

- analizēt spēkā esošos Latvijas normatīvos aktus un standartus par prasībām informācijas sistēmu aizsardzībai valsts pārvaldes iestādēs un pašvaldībās;
- raksturot organizācijas „N" datu centru un tā darbības problēmu izraisītās sekas informācijas sistēmas nepārtrauktā pieejamībā, informācijas uzglabāšanā un datu aizsargāšanā;
- izstrādāt vienotu sistēmu datu centra pakalpojuma kvalitātes līmeņa klasifikācijai un ieteikumus organizācijas „N" datu centram izvirzāmajām kvalitātes prasībām.

Pētījumu objekts ir Latvijas normatīvajos aktos un standartos noteiktie nosacījumi informācijas uzglabāšanai informācijas sistēmās un informācijas sistēmu fiziskajai aizsardzībai.

Pētījuma priekšmets ir datu centru klasifikācija, prasības nepārtrauktas darbības kvalitātes nodrošināšanai atbilstoši normatīvo aktu prasībām.

Pētījuma bāze ir normatīvie akti, speciālā literatūra un informācija no interneta.

Pētījuma hipotēze, kamēr organizācijā „N" nebūs noteikti vienoti principi datu centra darbības kvalitātei, tikmēr netiks apzināti un mazināti riski informācijas sistēmu nepārtrauktā pieejamībā un datu aizsargāšanā no fiziskiem apdraudējumiem.

Darba struktūra veidota pēc bakalaura darbā izvirzīto uzdevumu secības, nodrošinot problēmas izpētes veselumu.

Bakalaura darba ierobežotā apjoma dēļ netiks apskatīti normatīvie akti, kas regulē ar valsts, NATO un Eiropas Savienības noslēpumu aizsargātus objektus un pētījumā galvenokārt tiks analizētas organizācijas „N" prasības pret datu centru.

1. Likumdošana informācijas sistēmu drošības prasību jomā

Ja 20.gadsimts tika dēvēts par tehnoloģiju gadsimtu, tad 21.gadsimts tiek dēvēts par informācijas sabiedrības gadsimtu. Mūsdienās grūti iedomāties tādu valsts pārvaldes institūcijas darbības vai uzņēmējdarbības jomu, kas tieši vai netieši nebūtu atkarīga no dažādiem informācijas tehnoloģiju resursiem. Turklāt pastāvīgi vērojama aizvien pieaugoša tendence gan valsts pārvaldi, gan uzņēmējdarbību sistēmiski saistīt ar elektroniskas informācijas apstrādi, pārraidi un uzglabāšanu. Daudzās organizācijās un uzņēmumos tiek uzturētas datorizētas informācijas sistēmas elektroniskas informācijas apstrādei, notiek elektroniska saziņa gan uzņēmuma iekšienē, gan arī ar sadarbības partneriem, tajā skaitā arī ārvalstīs. Tas nozīmē, ka uzņēmuma darbības netraucēta efektīva darbība (kas nosaka arī peļņu) būtiski atkarīga no tā, cik stabili, kvalitatīvi un droši ir lietotie informācijas tehnoloģiju risinājumi.

Pēc Latvijas neatkarības atgūšanas uz padomju iekārtas organizāciju materiāltehniskās bāzes tika veidotas jaunās valsts pārvaldes iestādes. Pagājušā gadsimta 90os gados organizāciju funkciju veiksmīgākai veikšanai sāka izstrādāt un ieviest specifiskas datu bāzes, kuru primārais uzdevums bija uzkrāt informāciju par jaunās valsts iedzīvotājiem, iedzīvotāju veiktajiem maksājumiem nodokļu un nodevu veidā valsts budžetā u.c. funkcijām. Tādās valsts pārvaldes iestādēs, kā Valsts ieņēmumu dienests, Iekšlietu ministrija, Valsts zemes dienests u.c., sāka veidoties informācijas ziņā apjomīgas sistēmas, kas saturēja sensitīvus datus par fiziskajām un juridiskajām personām, to īpašumiem, nodokļu nomaksu, naudas plūsmām u.tml.

Pagājušā gadsimta beigās valsts pieņēma lēmumu veikt nepieciešamos pirmsiestāšanās darbus un iestāties tādās starptautiskajās organizācijās, kā NATO un Eiropas Savienība. Lai to veiktu, bija nepieciešams harmonizēt likumdošanu, ieviešot Eiropas Savienības regulu prasības Latvijas likumdošanā, un veikt esošo valsts informācijas sistēmu integrēšanu ar Eiropas Komisijas uzturētajām centrālajām informācijas sistēmām.

Pieaugot sistēmās uzkrātajam informācijas apjomam, pieaug arī nepieciešamība pēc informācijas sistēmu uzturēšanas, izmantošanas un drošības prasību regulējuma. Tāpēc valsts ir uzlikusi konkrētu atbildību, pienākumus un ierobežojumus informācijas sistēmu īpašniekiem.

Latvijā likumdevējs 22.05.2002. ir izdevis *Valsts informācijas sistēmu likumu* (1) un MK 02.08.2005. ir apstiprinājis noteikumus Nr.572 *Valsts informācijas sistēmu reģistrācijas noteikumi* (2). Saskaņā ar likuma 13.pantu valsts informācijas sistēmas turētājam pienākums ir reģistrēt informācijas sistēmu Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta uzturētajā *Valsts informācijas sistēmu reģistrā* (3), iekļaujot likuma 13.panta 1.daļā norādīto informāciju, saskaņā ar kuru valsts informācijas sistēmas turētājam ir arī jānorāda fiziskās aizsardzības līdzekļi tehnisko iekārtu aizsardzībai pret fiziskas iedarbības radītu valsts informācijas sistēmas apdraudējumu (13.panta 1.daļas 6.punkts). *Valsts informācijas sistēmu reģistrs*, kura pārzinis ir Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāts, ir publiski pieejams.

Analizējot *Valsts informācijas sistēmu reģistrā* pieejamo informāciju, darba autors konstatēja, ka valsts informāciju sistēmu pārziņi savu informācijas sistēmu fizisko aizsardzību nodrošina, ievērojot sekojošu normatīvo aktu prasības:

- *Valsts informācijas sistēmu likums*;
- 11.10.2005. MK noteikumu Nr.764 *Valsts informācijas sistēmu vispārējās tehniskās prasības* (4);
- 11.10.2005. MK noteikumu Nr.765 *Valsts informācijas sistēmu vispārējās drošības prasības* (5);
- *Fizisko personu datu aizsardzības likums* (6);
- 30.01.2001. MK noteikumu Nr.40 *Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības* (7, 8);
- LVS ISO/IEC 17799:2005 *Informācijas tehnoloģija - Drošības paņēmieni - Prakses kodekss informācijas drošības pārvaldībai* (9);
- LVS EN 1047-1:2005 un LVS EN 1047-2:2000 *Drošas uzglabāšanas telpas – Klasifikācija un ugunsdrošības testa metodes* (10, 11);
- BS 7799-2:2002 *Information security management systems – Specification with guidance for use* (12).

Saskaņā ar ISO mājas lapā (13) publicēto informāciju standarts BS 7799-2:2002 ir aizstāts ar ISO/IEC 27001 (14) (atbilstoši BS 7799-2:2002 standartam sertificētās sistēmas ir jāpārsertificē ne vēlāk kā līdz 15.04.2007.) un ISO/IEC 17799 (14) tiek aizstāts ar ISO/IEC 27002 (14). Standartu ISO/IEC 27001 un ISO/IEC 27002 prasības autors apskatīs turpmākajās apakšnodaļās.

Ņemot vērā, ka datu centra uzdevums ir nodrošināt informācijas sistēmu uzturošās datortehnikas nepārtrauktu darbību un fizisko aizsardzību, tad turpmākajās apakšnodaļās

autors analizēs minētajos normatīvos aktos izvirzītos nosacījumus valsts iestāžu un pašvaldības datu centru darbības kvalitātei.

1.1. Valsts informācijas sistēmu likums

Saskaņā ar *Valsts informācijas sistēmu likuma* (Saeimā pieņemts 2002.gada 2.maijā, ar grozījumiem 09.06.2005. un 31.05.2007.) 2.pantu, likuma mērķis ir nodrošināt valsts un pašvaldību institūciju sniedzamās informācijas pieejamību un kvalitāti valsts informācijas sistēmās. Likuma uzdevumi ir noteikt vienotu kārtību, kādā veido, reģistrē, uztur, lieto, reorganizē vai likvidē valsts informācijas sistēmas, regulēt valsts informācijas sistēmu pārziņu (valsts institūciju, kas normatīvajos aktos noteiktajā kārtībā organizē un vada valsts informācijas sistēmas darbību) sadarbību un noteikt valsts informācijas sistēmas turētāja (valsts informācijas sistēmas pārzinis vai tā pilnvarota institūcija, kas uztur šīs sistēmas informācijas un tehnisko resursu funkcionalitāti un nodrošina informācijas apriti) funkcijas un valsts informācijas sistēmas datu subjekta (juridiskā vai fiziskā persona, kura normatīvajos aktos noteiktajā kārtībā sniedz datus par sevi un sev piekritīgajiem reģistrējamiem juridiski dokumentētiem objektiem) tiesības un pienākumus.

Likuma izpratnē, saskaņā ar 1.panta 1.daļu, valsts informācijas sistēma ir strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

Saskaņā ar likuma 3.pantu, tas attiecināms valsts informācijas sistēmām, kuras lietojot tiek nodrošināta informācijas aprite normatīvajos aktos un Latvijai saistošos starptautiskajos līgumos noteikto funkciju izpildei, un uz informācijas sistēmām, ko pašvaldību institūcijas veido un uztur kā valsts informācijas sistēmas sastāvdaļu. *Valsts informācijas sistēmu* likuma normas neattiecas uz tām informācijas sistēmām, kuras veido un uztur saskaņā ar likumu *Par valsts noslēpumu* – par valsts noslēpuma objektu atzītas informācijas apritei, informācijas apritei saskaņā ar Operatīvās darbības likumu, kā arī šis likums neattiecas uz informācijas sistēmām, ko valsts un pašvaldību institūcijas veido un uztur iekšējās lietošanas informācijas apritei.

Valsts informācijas sistēmas turētājs saskaņā ar likuma 8.pantu:

- **nodrošina un atbild** par datu vākšanu, reģistrēšanu, ievadīšanu, apstrādi, glabāšanu, izmantošanu, pārraidīšanu, publicēšanu, atbilstību iesniegtajiem

datiem, aktualizēšanu, labošanu, kā arī datu kvalitāti valsts informācijas sistēmā (8.panta 1.daļa);

- **piekļūšanu** apritē esošajai **informācijai elektroniskā veidā** (8.panta 4.daļa);
- **iespēju** valsts informācijas sistēmas **lietotājiem** pieejamos informatīvos pakalpojumus **saņemt elektroniskā veidā**, izmantojot informācijas tehnoloģijas (8.panta 5.daļa);
- datu rezerves kopiju sagatavošanu, **datu drošību un aizsardzību** (8.panta 6.daļa).

Lai aizsargātu valsts informācijas sistēmu no nesankcionētas pieejas, valsts informācijas sistēmas turētājam saskaņā ar 10.panta 2.daļu jānodrošina valsts informācijas sistēmas lietotāju identitātes un piekļuves tiesību pārbaudi. Šī panta prasības var arī tikt attiecinātas uz fiziskās pieejas drošības līmeņa nodrošināšanas pie informācijas sistēmas uzturošās datortehnikas.

Valsts informācijas sistēmas turētājam saskaņā ar 11.panta 1.daļu, lai nodrošinātu informācijas pieejamību, **jānodrošina piekļūšana valsts informācijas sistēmas vispārpieejamai informācijai globālajā datoru tīklā**.

Sākotnēji var norādīt, ka ar *Valsts informācijas sistēmu likuma* pārejas noteikumu nosacījumiem no 2002. gada 1. novembra spēku zaudēja MK noteikumi Nr. 106 *Informācijas sistēmu drošības noteikumi*. Šie noteikumi tika pieņemti saskaņā ar *Krimināllikuma* (15) pārejas noteikumu 3.panta 1.apakšpunktu tādēļ, lai nodrošinātu *Krimināllikuma* 245.panta piemērošanu. Saskaņā ar minētajiem noteikumiem, kriminālatbildību par *Krimināllikuma* 245.panta pārkāpumu var piemērot, ja MK noteikumiem Nr. 106 atbilstīgas informācijas sistēmas organizācijas amatpersona, kas ir atbildīga par informācijas sistēmas drošības noteikumu ieviešanu un nodrošināšanu, tīši vai netīši pieļāvis tādu informācijas sistēmas drošības noteikumu pārkāpumu (vai vispār nav ieviesis atbilstīgus drošības noteikumus), kā dēļ šim uzņēmumam vai organizācijai nodarīts būtisks kaitējums (16).

Saskaņā ar *Valsts informācijas sistēmu likuma* 4. panta 2.daļas normu nepieciešamie MK noteikumi *Valsts informācijas sistēmu vispārējās drošības prasības* pieņemti 11.10.2005. un stājās spēkā 15.10.2005. Vienlaikus ar tiem tika pieņemti arī MK noteikumi Nr.764 *Valsts informācijas sistēmu vispārējās tehniskās prasības*. Minēto noteikumu prasības arī tiks apskatītas nākošajās apakšnodaļās.

1.1.1 Valsts informācijas sistēmu vispārējās tehniskās prasības

11.10.2005. apstiprināto MK noteikumu Nr.764 *Valsts informācijas sistēmu vispārējās tehniskās prasības* (4) 2.punkts nosaka valsts informācijas sistēmu vispārējās tehniskās prasības, kas ievēro sistēmas informācijas un tehnisko resursu pārvaldībā un saskaņā ar 2.punkta 2.apakšpunktu, tajā skaitā arī sistēmas drošību un attīstību.

Noteikumu 10.punkts nosaka, ka sistēmas pārzinis nodrošina šajos noteikumos noteikto prasību izpildi atbilstoši tam piešķirtajiem valsts budžeta līdzekļiem.

Sistēmas pārzinim, saskaņā ar noteikumu 5.punktu, lietojot sistēmas tehniskos resursus (datorus, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību), jāievēro šādas prasības:

- tos jāizmanto atbilstoši **ražotāja noteiktajām prasībām**;
- tiem jābūt aizvietojamiem ar citu ražotāju piedāvātajiem tehniskajiem resursiem;
- to lietošanai jānodrošina **sistēmas drošība un sistēmas darbība integrētā** valsts informācijas sistēmā.

Ņemot vērā, ka organizācija „N" informācijas sistēmu darbināšanai pārsvarā izmanto korporācijas *International Business Machines corp.* (IBM) ražotos serverus un disku masīva iekārtas, tad saskaņā ar noteikumu 5.punktu organizācijai ir jāizpilda datortehnikas ražotāja IBM izvirzītās prasības pret datortehnikas ekspluatācijas mikroklimatu. Ražotāja izvirzītās prasības ir sekojošas (7; 67.lp.):

- gaisa temperatūrai jābūt 22 °C (+/-1 °C);
- relatīvajam gaisa mitrumam 45–50%;
- dzesējošajā gaisā nedrīkst atrasties putekļu daļiņas vai citas mazas daļiņas.

Pieļaujamie ekstremālie serveru telpas mikroklimata apstākļi (īstermiņā) ir sekojoši:

- gaisa temperatūra 16–29 °C (+/-1 °C);
- relatīvais gaisa mitrums 20–80%.

Tātad no šo noteikumu prasībām autors var secināt, ka organizācijas „N" vadībai, piešķirtā valsts budžeta iespēju robežās un ievērojot samērīgumu, pienākums ir aprīkot organizācijas datu centru ar visu nepieciešamo, lai nodrošinātu normatīvo aktu, tajā skaitā, ražotāju, izvirzītās prasības.

Nākošajā apakšnodaļā tiks apskatītas 11.10.2005. MK noteikumu *Valsts informācijas sistēmu vispārējās drošības prasības*.

1.1.2 Valsts informācijas sistēmu vispārējās drošības prasības

2005.gada 11.oktobrī apstiprinātie Ministru kabineta noteikumi Nr.765 *Valsts informācijas sistēmu vispārējās drošības prasības* (5) nosaka valsts informācijas sistēmas drošības pasākumu kopumu, kurus īsteno, lai:

- nodrošinātu **sistēmas darbību** atbilstoši normatīvajos aktos noteiktajām funkcijām;
- **informācijas pieejamību** (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);
- nodrošinātu **informācijas veselumu** (pilnīgas un nemainītas informācijas saglabāšanu);
- nodrošinātu **informācijas slepenību** (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);
- aizsargātu sistēmas **informācijas resursus** (programmatūru, datnes (arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju) un sistēmas dokumentāciju);
- aizsargātu **sistēmas tehniskos resursus** (datorus, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību);
- noteiktu **sistēmas drošības apdraudējumu** (ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama);
- novērtētu **sistēmas drošības risku** (iespēju, ka, īstenojoties drošības apdraudējumam, sistēmas informācija vai tehniskie resursi varētu mainīties, sabojāties, tikt iznīcināti vai nonākt tādu personu rīcībā, kuras nav tam pilnvarotas, vai piekļūšana sistēmas informācijas resursiem varētu būt traucēta vai neiespējama);
- **atklātu sistēmas drošības incidentu** (ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas izraisījis sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem ir traucēta vai neiespējama);

- **atjaunotu sistēmas darbību** pēc sistēmas drošības incidenta.

Ja sistēma saskaņā ar *Fizisko personu datu aizsardzības* likumu ir atzīta par **personu datu apstrādes sistēmu**, sistēmas pārzinis nodrošina noteikumu 5.pantā noteikto prasību izpildi, ciktāl tas nav pretrunā ar normatīvajiem aktiem par personas datu apstrādes sistēmas aizsardzības obligātajām tehniskajām un organizatoriskajām prasībām.

Tātad noteikumi uzliek par **pienākumu organizācijas vadībai izstrādāt informācijas sistēmas drošības noteikumus** un veikt informācijas sistēmas drošības nodrošināšu, kuras viens no organizatoriskajiem pamatprincipiem ir kontroles un funkcionalitātes līdzsvars (var arī teikt – kompromiss). Tas attiecās gan uz organizācijas vadības mijiedarbību ar IT speciālistiem, gan arī uz pašas informācijas sistēmas veidošanu un uzturēšanu. Uzņēmuma vadītājam vai tās drošības speciālistam nepieciešams vienlaikus, no vienas puses, pārraudzīt IT speciālistu darbu, lai novērstu viņu nolaidību vai pat konstatētu iespējamas ļaunprātības, no otras puses, nepieciešams deleģēt IT speciālistiem atbildību par informācijas sistēmas veidošanu un uzturēšanu, lai viņi būtu motivēti un arī varētu pastāvīgi gan uzturēt informācijas sistēmas drošības sistēmu adekvātu darbību no iespējamiem apdraudējumiem. Bez tam vienlaikus nepieciešams rūpēties gan par informācijas sistēmas drošību, gan par tās funkcionalitāti un lietošanas ērtumu. Nav vēlamas galējības nedz vienā, nedz otrā virzienā.

Nepieciešamību pastiprināti pievērst uzmanību informācijas sistēmu drošībai mūsdienās nosaka praktiskā situācija valsts pārvaldes institūciju, privātuzņēmumu, kā arī fizisko personu tiesisko un ekonomisko interešu aizsardzībā gan globālā mērogā, gan Latvijā. Vairākas informācijas sistēmas apdraudējumu formas mūsdienās tiek pielīdzinātas terorismam, IT drošības eksperti un politiķi runā arī par kiberkaru (*cyberwar*) jeb 4GW (ceturtās paaudzes karu), kam zūd robežlīnija starp karu un mieru un kuram raksturīgi tā sauktie asimetriskie uzbrukumi, kad lielu kaitējumu var nodarīt personu grupas vai pat atsevišķs cilvēks ar nesalīdzināmi mazākiem resursiem, nekā ir apdraudētajai valstij. Teroristi, tajā skaitā islāma ekstrēmistu organizācijas, kā arī vairāku valstu specdienesti šajā nolūkā izmanto Internet tāpēc, ka tās sniedz ārkārtīgi lielas organizatoriskās un uzbrukuma iespējas, kas var būt vērstas pret visu pārvaldes sistēmu, padarot mūsdienu sabiedrību ļoti viegli ievainojamu (*vulnerable society*). Terorismam un kriminālām darbībām radušies virkne jaunu mērķu – telekomunikāciju tīkli, energoapgādes sistēmu vadība, dispečeru un aizsardzības sistēmas, ražošanas un apgādes ķēdes, finanšu transakcijas utt. Mūsdienās iespējams nodarīt milzīgu kaitējumu, neizejot no savas istabas. (18).

Vienmēr jāatceras, ka galvenais apdraudējuma avots praktiski ir nevis informācijas sistēmu tehnisko un informācijas resursu darbības īpatnības, bet gan cilvēki – informācijas

sistēmu lietotāji un personāls, kuri var pieļaut paviršības, kļūdas vai pat ļaunprātību. Informācijas drošības pārvaldība atbilstīgi starptautisko standartu prasībām nozīmē, ka uzņēmums, kas to īsteno, izvirzījusi informācijas sistēmu drošību kā vienu no augstākajām prioritātēm. Līdz ar to informācijas sistēmu drošības noteikumu un standartu ieviešana ļauj iegūt gan uzņēmuma sadarbības partneru un klientu uzticību, gan daudz augstākā ticamības pakāpē prognozējamu uzņēmuma attīstību (19).

Nākošajā apakšnodaļā tiks apskatītas *Fizisko personu datu aizsardzības likuma* izvirzītās prasības.

1.2. Fizisko personu datu aizsardzības likums

Fizisko personu datu aizsardzības likuma (Saeimā pieņemts 23.03.2000., ar grozījumiem 24.10.2002, 19.12.2006 un 01.03.2007) 1.pants nosaka, ka mērķis ir aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību, attiecībā uz fiziskās personas datu apstrādi (6).

Likuma izpratnē, saskaņā ar 2.panta 4.daļu, personas datu apstrāde ir jebkuras ar personas datiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu, un personas datu apstrādes sistēma ir jebkādā formā fiksēta strukturizēta personas datu kopa, kas ir pieejama, ievērojot attiecīgus personu identificējošus kritērijus, piemēram, personas kods, dzīves vietas adrese u.tml.

Informāciju sistēmu, kas satur personas datus, izveides un uzturēšanas pamatotība valsts pārvaldē ir balstīta uz *Fizisko personu datu aizsardzības likuma* 7.panta 3.daļu, kas nosaka, ka datu apstrāde nepieciešama informācijas sistēmas pārzinim likumā noteikto pienākumu veikšanai, vai 7.panta 5.daļu – datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ievērošanu vai realizētu publiskās varas uzdevumus, kuru veikšanai personas dati ir nodoti pārzinim vai pārraidīti trešajai personai.

Datu valsts inspekcija savā mājas lapā ir publicējusi uzziņai astoņus labas prakses principus personu datu apstrādē:

- dati tiek godīgi un likumīgi apstrādāti;
- datu apstrāde tiek veikta konkrētiem mērķiem un tikai saskaņā ar tiem;
- dati ir adekvāti (nevis pārmērīgi);
- dati ir precīzi;

- dati netiek glabāti ilgāk, nekā nepieciešams;
- dati tiek apstrādāti saskaņā ar jūsu tiesībām;
- dati ir drošībā;
- dati netiek pārsūtīti uz citām organizācijām, iestādēm vai ārvalstīm bez drošas adekvātas aizsardzības. (20)

Likuma 21.panta 1.daļa nosaka, ka informācijas sistēmas pārzinim personas datu apstrādes sistēma ir jāreģistrē Datu valsts inspekcijā.

Bez tam jānorāda, ka arī *Fizisko personu datu aizsardzības likums* paredz informācijas sistēmas drošības noteikumu izstrādi. Šā likuma 21. un 22.pants noteic, ka visas valsts un pašvaldību institūcijas, citas fiziskās un juridiskās personas, kas veic vai vēlas uzsākt personas datu apstrādi un veido personas datu apstrādes sistēmas, reģistrē tās šā likuma noteiktajā kārtībā (izņēmumi ir attiecībā uz tādām informācijas sistēmām, kurās informācijas reģistrēšanu veic sabiedriskās drošības, noziedzības apkarošanas vai valsts drošības un aizsardzības jomās). Vienlaikus ar reģistrācijas pieteikumu attiecīgas informācijas sistēmas īpašnieks (valdītājs) iesniedz Datu valsts inspekcijai arī informāciju par tehniskiem un organizatoriskiem pasākumiem, kas nodrošina personas datu aizsardzību.

Saskaņā ar *Fizisko personu datu aizsardzības likuma* 26.pantu 1.daļu, MK ir izstrādājis un 30.01.2001. apstiprinājis noteikumus Nr.40 *Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības*, kuru apskatīsim nākošajā nodaļā.

1.3. Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības

30.01.2001. MK noteikumu Nr.40 *Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības* un ar 28.08.2007. MK noteikumu Nr.574 *Grozījumi Ministru kabineta 2001.gada 30.janvāra noteikumos Nr.40 Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības"*, izdoti saskaņā ar *Fizisko personu datu aizsardzības likuma* 26.panta 1.daļu un, saskaņā ar noteikumu 1.punktu, nosaka personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības (7, 8) .

Saskaņā ar noteikumu 3.punktu, personas datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot:

- **aizsardzību pret fiziskās iedarbības** radītu personas datu apdraudējumu;
- **aizsardzību**, kuru realizē **ar programmatūras līdzekļiem**, parolēm, šifrēšanu, kriptēšanu un citiem loģiskās aizsardzības līdzekļiem.

Saskaņā ar noteikumu 5.punktu, sistēmas pārzinis, apstrādājot personas datus, izstrādā iekšējos datu apstrādes aizsardzības noteikumus, kuros nosaka:

- **personas datu aizsardzības klasifikāciju** atbilstoši to vērtības un konfidencialitātes pakāpei;
- **tehniskos resursus**, ar kādiem tiek nodrošināta personas datu apstrāde;
- **pasākumus**, kas veicami tehnisko resursu aizsardzībai pret ārkārtas apstākļiem (piemēram, ugunsgrēks, plūdi);
- **līdzekļus**, ar kādiem nodrošina tehniskos resursus pret tīšu bojāšanu un neatļautu iegūšanu

Pēc autora domām, MK noteikumu Nr.40 prasības korelē ar MK noteikumu Nr.764 un Nr.765 prasībām. Tas varētu būt arī saistīts ar to, ka MK noteikumi Nr.40 ir vispārīgāki un izstrādāti piecus gadus pirms MK noteikumu Nr.764 un Nr.765 apstiprināšanas, bet pēc būtības šie noteikumi viens otru tikai papildina. Personas datu apstrādes sistēmas pārziņa, līdzīgi kā valsts informācijas sistēmas pārziņa pienākums ir izstrādāt iekšējās kārtības noteikumus, kas nosaka piemērojamos fiziskos un loģiskos aizsardzības gan proaktīvos (riska analīzes veidā), gan reaktīvos (nosakot konkrētus un neatliekamus pasākumus) pasākumu un līdzekļu kopumu informācijas sistēmas uzturēšanas un darbināšanas laikā. Minētie pasākumi var būt arī iekļauti iestādes informācijas sistēmu drošības noteikumos.

Jāņem vērā, ka iespējamie apdraudējumi informācijas sistēmas drošībai ir viens no pamatfaktoriem, kas jāievēro ne vien tādu informācijas sistēmu izveidē un uzturēšanā, kurās tiek apstrādāta valsts interesēm svarīga un ar likumiem un citiem normatīvajiem aktiem aizsargāta informācija, bet arī tādu informācijas sistēmu izveidē un uzturēšanā, kur tiek apstrādāta uzņēmumu vai organizāciju sekmīgai darbībai nozīmīga informācija. Kaut arī pilnīga informācijas sistēmas drošība praktiski nav iespējama, tomēr maksimāli daudz pūles jāveltī aizsardzībai pret informācijas sistēmas apdraudējumiem jebkādu informācijas tehnoloģiju projektu īstenošanā gan valsts pārvaldes jomā, gan arī uzņēmējdarbībā. Arī lielākai daļai privātpersonu ir svarīga viņu īpašumā vai valdījumā esošo datorsistēmu un tajā apstrādātās, uzglabātās un pārraidītās informācijas drošība (16).

Tālāk tiks apskatīti standarti, kas reglamentē organizācijas informācijas sistēmas drošības prasības.

1.4. Standarti, kas reglamentē informācijas sistēmas drošības prasības

2007.gada jūlijā *Starptautiskā Standartizācijas organizācija* (ISO) un *Starptautiskā Elektrotehnikas komisija* (IEC) publicēja pirmos divus jaunās informācijas drošības standartu ISO/IEC 27000 saimes standartus – ISO/IEC 27001 un ISO/IEC 27002 (13, 14).

ISO/IEC 27001 standarts ir informācijas drošības pārvaldības standarts, kura mērķis ir palīdzēt organizācijai ieviest un uzturēt **Informācijas drošības vadības sistēmu**, un ISO/IEC 27002 standarts ir mūsdienām atbilstoši adaptēts standarts ISO/IEC 17799:2005 (Informācijas tehnoloģija – Drošības paņēmieni – Prakses kodekss informācijas drošības pārvaldībai), savukārt kurš 2000.gadā tika pārņemts no britu standarta BS 7799–1:1999 (9, 12).

ISO/IEC 27001 standarts apraksta sekojošus Informācijas drošības vadības sistēmas ieviešanas un uzturēšanas soļus:

- izveide (personāla apmācība, sistēmas izstrāde, sistēmas dokumentēšana);
- pārvaldība (politikas dokumentu izstrāde, nepieciešamo resursu vadība);
- audits (audita procedūru izstrāde, iekšējo auditu plānošana un veikšana, korektīvu pasākumu veikšana);
- sistēmas efektivitātes novērtēšana (veikt procesu pārskatīšanu, veikto pasākumu un gūto rezultātu efektivitātes novērtēšanu);
- sistēmas nepārtraukta pilnveidošana (labot un preventīvi novērst nepilnības).

Saskaņā ar šo standartu tiek sertificētas organizācijā ieviestās informācijas drošības vadības sistēmas. Citiem vārdiem sakot, ja organizācija ir ieviesusi ISO/IEC 27001 standarta prasības un sasniegusi izvirzītos mērķus, var tik uzaicināta auditora firma, lai veiktu organizācijas *Informācijas drošības vadības sistēmas* novērtējumu un, atbilstības gadījumā, sertificētu ISO/IEC 27001 standartam.

ISO/IEC 27002 ietver kompleksus praktiskus nosacījumus informācijas drošības vadībai, tāpēc tas var būt pielietots arī kā novērtējuma kritērijs informācijas sistēmas drošības risinājumam organizatoriskā līmenī, tajā skaitā administratīvajiem, procedūras un tehniskiem aspektiem. Standartā informācijas drošības aspekti ir definēti C-I-A triādes kontekstā: **konfidencialitāte, integritāte un pieejamība**.

Standarts palīdz identificēt, vadīt un mazināt organizācijas informāciju sistēmu drošības riskus, kuriem regulāri tiek pakļauta konfidenciāla informācija, un ieviestu organizācijai piemērotākās drošības kontroles, kas palīdzētu maksimāli aizsargāt informācijas drošību, tajā pašā laikā ļaujot nodrošināt organizācijas iekšējo un ārējo informācijas sistēmas lietotāju vajadzības.

Standarts ir piemērojams dažādu nozaru organizāciju lietojumam un apraksta tādas informācijas drošības vadības jomas kā:

- drošības politika;
- informācijas drošības nodrošināšanas organizatoriskās metodes;
- resursu un risku vadība;
- informācijas sistēmas lietotāji;
- fiziskā drošība;
- procesu un komunikāciju vadība;
- piekļuves kontrole;
- informāciju sistēmu iegāde, izstrāde un atbalsts;
- informācijas drošības incidentu vadība;
- nepārtraukta biznesa procesa vadība;
- sistēmas atbilstību organizācijas drošības prasībām.

ISO/IEC 27000 standarts neizvirza nosacījumus informācijas sistēmās pielietotajām tehnoloģijām, iekārtām un nesniedz informācijas tehnoloģiju pārvaldības konceptuālu struktūru, bet tas aplūko informāciju kā kopumu, kas var būt apstrādāta un uzglabāta visdažādākajos veidos. Tas, ka standarts nav atkarīgs no konkrētiem tehniskiem līdzekļiem un risinājumiem, no vienas puses, nedod skaidru priekšstatu, kā praktiski īstenot tā vai cita informācijas sistēmas elementa aizsardzību, taču, no otras puses, dod brīvību izvēlēties informācijas sistēmas tehniskos un informācijas resursus.

Te gan jāuzsver, ka jebkurā gadījumā atbildību par informācijas sistēmas drošību, ja tas saistīts ar likumos noteikto fizisko un juridisko personu tiesību un interešu aizsardzību, kopumā jāuzņemas uzņēmuma vadītājam.

1.5. Likumdošanas prasību informācijas sistēmu drošības jomā izvērtējums

Izanalizējot pirmajā nodaļā apskatīto literatūru un normatīvos aktus, var secināt, ka organizācijas vadītāju (sistēmas pārziņa) pienākums ir veikt valsts informācijas sistēmās un/vai personas datu apstrādes informācijas sistēmās esošās informācijas loģisko un fizisko aizsardzību.

Šāda mērķa sasniegšanai jāveic noteiktu **tiesisko, organizatorisko un tehnisko pasākumu komplekss**, ko apzīmē kā **informācijas sistēmas drošības politika**, kurai jāiekļaujas attiecīgās iestādes kopējā drošības politikā. Informācijas sistēmas drošības politika jānosaka pamatnostādnes informācijas sistēmas drošības pārvaldības izveidei un uzturēšanai, tajā skaitā konceptuālu informācijas sistēmas drošības pārvaldības principu, nosacījumu un pamatmērķu aprakstu. Citiem vārdiem sakot, informācijas sistēmas drošības politikai jāsatur prasības, kuras noteicis informācijas īpašnieks (turētājs), un jāapraksta pasākumus šo prasību nodrošināšanai. Informācijas sistēmas drošības politika jānostiprina ar uzņēmuma normatīvajiem dokumentiem.

Ar uzņēmuma informācijas sistēmas drošības noteikumiem jāreglamentē informācijas sistēmas informācijas un tehnisko resursu pārvaldi (administrēšanu), atbildīgos darbiniekus un informācijas sistēmas lietotāju tiesības, pienākumus un atbildību, informācijas klasifikāciju, informācijas un tehnisko resursu aizsardzības organizatoriski tehniskos u.c. nepieciešamos pasākumus.

Katram jaunam ar informācijas resursiem un tehniskajiem resursiem saistītam projektam jāveic **riska analīze**. Tā vajadzīga arī tad, ja informācijas sistēmās notikušas izmaiņas, kas var ietekmēt informācijas sistēmas drošību, kā arī riska analīzi veic periodisko drošības auditu ietvaros.

Ar **informācijas sistēmas loģisko aizsardzību** normatīvo aktu izpratnē tiek saprasta informācijas resursu aizsardzība, ko īsteno ar programmatūras līdzekļiem (piemēram, identificējot informācijas sistēmas lietotāju, pārbaudot viņa pilnvaru atbilstību noteiktām darbībām informācijas sistēmā, pasargājot informāciju no tīšas vai nejaušas nevēlamas izmainīšanas, dzēšanas vai izpaušanas, novēršot patvaļīgu piekļūšanu informācijas resursiem, novēršot informācijas sistēmas pārslogošanu, kas var izsaukt tās darbības pārtraukumus u.c.).

Ar **informācijas sistēmas fiziskā aizsardzību** normatīvo aktu izpratnē tiek saprasta ir tehnisko resursu aizsardzība pret fiziskas iedarbības radītu informācijas sistēmas apdraudējumu (piemēram, ugunsgrēks, applūšana, elektriskā sprieguma pazemināšanās vai

pārspriegums elektroenerģijas pievades datortīklā, tehnisko resursu zādzība vai personas veikta to sabojāšana, ekspluatācijas noteikumiem neatbilstīgs mitrums, gaisa temperatūra, putekļi, dūmi telpā, vibrācija, ārējs spēcīgs elektromagnētiskais lauks u.c.).

Normatīvie akti neuzliek par pienākumu organizācijas vadītājam, izstrādājot un ieviešot informācijas sistēmas drošības noteikumus, vadīties no konkrētiem starptautiski atzītiem vai Latvijas republikā apstiprinātiem standartiem.

Tas, ka normatīvajos aktos un standartos nav noteiktas atkarības no konkrētiem tehniskiem līdzekļiem un risinājumiem, no vienas puses, nedod skaidru priekšstatu, kā praktiski īstenot tā vai cita informācijas sistēmas elementa aizsardzību, taču, no otras puses, dod brīvību organizācijai izvēlēties informācijas sistēmas tehniskos un informācijas resursus. Tomēr, šāda rīcības brīvība var radīt draudus informācijas sistēmu drošībai organizācijas vadības un IT speciālistu nekompetences gadījumā, jo valstī nav izstrādātas nepieciešamo minimālo loģiskās un fiziskās drošības prasību vadlīnijas.

Nākošajā nodaļā autors noskaidros un analizēs organizācijas „N" datu centra darbības kvalitāti, jo informācijas sistēmu fiziskā aizsardzība galvenokārt tiek realizēta ar automatizētu organizācijas datu centra servisu kvalitatīvu un nepārtrauktu darbību.

2. Organizācijas „N" datu centra raksturojums

Sākumā ļaujiet kliedēt plaši izplatīto mītu, ka informācijas tehnoloģijas ir programmētāju entuziastu grupiņa, kas caurām dienām *kodē* ar datortehniku pārpildītā tumšā, zilo ekrānu izgaismotā telpā. Diemžēl, šis mīts ir tālu no patiesības. Tehnoloģijas strauji attīstās un informācijas tehnoloģiju loma un nozīme ikdienā kļūst arvien nozīmīgāka. Autora teiktais nav tukšu salmu malšana – saskaņā ar *MIT Sloan Managment* pētījumu – *informācijas un informācijas tehnoloģijas kļūst par vadītāju piekto lielāko pieejamo resursu organizācijas veidošanā, līdzās darbiniekiem, finansēm, resursiem un tehnoloģijām* (21). Faktiski mēs sākotnēji esam pakļāvuši visu organizāciju un uzņēmumu, neatkarīgi no to lieluma, biznesa procesus informācijas tehnoloģijām. *Informācijas Sistēmas* drošība tagad ir kļuvusi par korporatīvu atbildību. Šī jaunā *Informācijas Sistēmas* paradigma ir atbildīga par biznesa procesu attīstību un ieviešanu ikvienā organizācijas struktūrvienībā. Mūsdienās biznesa procesi pārsvarā tiek balstīti uz informācijas tehnoloģijām, tādēļ kļuvuši par organizācijas iekšējo procesu tehnoloģiskajiem līderiem.

Informācijas tehnoloģijas, precīzāk būtu teikt – *Informācijas Sistēmas*, ir atbildīgas par daudz vairāk nekā tikai personālo datoru darbības nodrošināšanu. Informācijas sistēmu tiek saprasta visa infrastruktūras lietošana, tajā skaitā, personālo datoru, serveru, disku masīvu, telekomunikāciju tīkla, drošības, datu apmaiņas un citas saistītās programmatūras, lai varētu droši apstrādāt, glabāt, aizsargāt, pārraidīt un saņemt organizācijai nepieciešamo informāciju. Šodien, informācijas tehnoloģiju pielietojums kļuvis daudzpusīgs un tiek pielietots visdažādākajās jomās, sākot no pilsētas satiksmes regulēšanas līdz pat kosmosa izpētei. Informācijas tehnoloģiju speciālisti veic dažādus darbus sākot no programmatūras uzstādīšanas, LAN/WAN telekomunikāciju tīklu ierīkošanas un beidzot ar datu bāzu, datu centru projektēšanu līdz pat visu informācijas tehnoloģiju kopuma pārvaldīšanai. Informācijas tehnoloģiju speciālistu pienākumi ir daudzveidīgi un ietver gan organizācijas informācijas, tīklu un drošības pārvaldīšana, gan datortehnikas izvietošana, gan datu bāzu un programmatūras prasību analīze, izstrāde un ieviešana, līdz pat pašas *Informācijas Sistēmas* uzturēšanai un pārraudzībai. (22)

Nākošajās apakšnodaļās autors apskatīs organizācijas „N" informācijas sistēmas, lai varētu analizēt informācijas sistēmu lomu organizācijas „N" biznesa procesos un, sekojoši, nepieciešamās prasības pret datu centru darbības kvalitāti.

2.1. Organizācijas „N" informācijas sistēmas

Pēc Latvijas neatkarības atgūšanas tika izveidotas divas organizācijas, kuru uzdevums bija ieņēmumu iekasēšana:

- Valsts finansu inspekcija, kas atbildēja par nodokļu iekasēšanu;
- Muitas departaments, kas atbildēja par muitas nodevām un nodokļiem par starptautisko tirdzniecību.

Par organizācijas „N" dibināšanas brīdi var uzskatīt 1993.gada 28.oktobri, kad tika pieņemts likums *Par Valsts ieņēmumu dienestu*. Šis likums un nepieciešamība uzlabot ieņēmumu iekasēšanu un ekonomēt administratīvās izmaksas bija par pamatu tam, ka divas minētās organizācijas tika apvienotas, izveidojot organizāciju „N", kas ir tieši pakļauta Finanšu ministrijai.

1998. gadā organizācijā „N" tika izstrādāta misija un apstiprināts Stratēģiskais plāns (laikposmam no 1999. gada līdz 2003. gadam), kurā noteikts organizācijas nākotnes redzējums un svarīgākie stratēģiskie mērķi. Bija noteikts, ka jāpanāk organizācijas „N" sniegto pakalpojumu un nodokļu kontroles līdzsvars, lai nodokļu maksātāji godīgi pildītu nodokļu saistības un izvēlētos brīvprātīgu pakļaušanos nodokļu likumu prasībām, uztverot organizāciju „N" kā uzņēmuma partneri nodokļu saistību izpildē. Stratēģijā arī tika paredzēta organizācijas informācijas sistēmu un sistēmu darbības nodrošināšanai nepieciešamā infrastruktūra (23).

Šajā laika posmā līdz 2000.gadam, organizācijas rīcībā bija neliels skaits serveru, bet modernizācijas ietvaros to skaits palielinājās līdz piecdesmit. Informācijas sistēmu uzturošā datortehnika tika izvietota pielāgotā serveru telpā. Katra serveru vienība tika aprīkota ar mazjaudīgu nepārtrauktas elektrobarošanas avotu (UPS) un telpā ierīkotas birojiem paredzētās mobilās kondicionēšanas iekārtas.

Organizācija „N" uztur un nepārtraukti pilnveido nosacīti trīs lielas valsts informācijas sistēmas: *Nodokļu informācijas sistēma*, *Muitas informācijas sistēma* un *Datu noliktavas sistēma*, kuras sastāv no daudzām apakšsistēmām. Minēto **informācijas sistēmu darbības kvalitāte, stabilitāte, integritāte un nepārtraukta pieejamība ir būtisks faktors izvirzīto organizācijas stratēģisko mērķu sasniegšanā un galveno uzdevumu veiksmīgā izpildē**.

Nodokļu informācijas sistēmas uzdevums ir nodrošināt nodokļu administrēšanas funkciju automatizēšanu, tai skaitā riska analīzes un kontroles darba plānošanas iespējas. Papildus tam, NIS jānodrošina tādas papildus funkcijas kā licenču reģistrēšana (licences un atļaujas, kuras izsniedz organizācija un citas institūcijas), dažāda veida tirgus regulējošu aizsardzības

mehānismu atbalsta funkcijas, kas saistītas ar specifisku marķējumu ieviešanu noteiktām preču grupām un elementiem, kuros uzglabā noteiktas preces. Nodokļu informācijas sistēmai ir jāsniedz darbiniekiem atbalsts ļoti daudzu funkcionāli visai atšķirīgu, bet savstarpēji saistītu uzdevumu izpildē

Muitas informācijas sistēmas uzdevums ir sniegt palīdzību muitas funkciju sekmīgai izpildei, nodrošināt muitas darbam nepieciešamās informācijas saņemšanu, uzglabāšanu un automatizētu izmantošanu. Šai nolūkā līdztekus tādu muitas pamatdokumentu, kā muitas kravas deklarāciju jeb *Vienoto Administratīvo Dokumentu* un TIR karnešu noformēšanai un uzskaitei Muitas informācijas sistēmai jārealizē virkne palīgfunkciju informācijas ieguvei un aktualizācijai par: muitas procedūru veicējiem; preču ievešanas, izvešanas, pārstrādes un cita veida atļaujām; muitas tarifiem; aprēķinātajiem un faktiskajiem muitas maksājumiem; identificētajiem muitas noteikumu pārkāpumiem un riska situācijām; kravu plūsmām un citiem faktoriem. Muitas informācijas sistēmas izveidošanas un attīstības ietvaros pirmkārt tiek veidota muitas deklarāciju datu apstrādes sistēma. Liela Muitas informācijas sistēmas sastāvdaļa ir integrētā muitas tarifa uzturēšanas automatizēta sistēma. Specifiska muitas darba joma ir saistīta ar analītisko darbu riska faktoru identificēšanai un muitas likumpārkāpumu novēršanai. Citas vairāk vai mazāk autonomas Muitas informācijas sistēmas sastāvdaļas ir kravu (īpaši tranzīta) kustības kontrole, ārējās tirdzniecības un muitas statistikas uzskaite, muitas maksājumu, klientu, dažādu atļauju uzskaite.

Datu noliktavas sistēma ir izveidota veidota kā centralizēta sistēma ar kopēju datu bāzi, kurā tiek integrēta un aktualizēta informācija no galvenajām organizācijas informācijas sistēmām. Tās mērķis ir nodrošināt organizācijas centrālo aparātu un teritoriālās iestādes, kā arī ieinteresēto valsts institūciju amatpersonas ar operatīviem analītiskiem pārskatiem par organizācijas darbu. Datu noliktavas sistēma kalpo par analīzes instrumentu, analītiķiem sagatavojot un vadībai pieņemot atbildīgus lēmumus. Sistēmā pakāpeniski tiek apkopota informācija par organizācijas darbību, kura tiešā vai netiešā veidā ietekmē lēmumu pieņemšanu.

2002. – 2004.gadā Eiropas Savienības kandidātvalstij Latvijai, tajā skaitā organizācijai „N", tika izvirzīti, tā saucamie, „mājas darbi" – bija nepieciešams veikt nacionālajās informācijas sistēmās izmaiņas un izstrādāt jaunas informācijas sistēmas datu apmaiņai ar Eiropas Komisijas centralizēti pārvaldītajām un uzturētajām tranzīta kontroles, akcīzes preču kontroles un integrētā tarifa informācijas sistēmām. Minēto informācijas sistēmu uzturēšanas un nepārtrauktas darbības nodrošināšanas vajadzībām tika iegādāti papildus tehniskie resursi.

Līdz 2007.gadam organizācijas vajadzībām tika izstrādātas un ieviestas jaunas informācijas sistēmas audita un tematisko pārbaužu struktūrvienību atbalstam. Modernizēta esošo informācijas sistēmu infrastruktūra, kurās darbības nodrošināšanai tiek izmantoti augstas veiktspējas serveri augstas pieejamības slēgumā pie SAN tipa ārējiem disku masīviem, kuros tiek uzglabāta vairāku terabaitu (informācijas vienība) liela konfidenciāla informācija par fiziskajām un juridiskajām personām.

Lai nodrošinātu augstu un nepārtrauktu organizācijas informācijas sistēmu pieejamību citu iestāžu un organizācijas klientu lietotāju vajadzībām, izveidotas tā saucamās tīmekļa serveru fermas, jeb serveru klasteri, kas apvieno atsevišķu serveru resursus. Tādējādi tiek panākta augsta kopējā informācijas sistēmu veiktspēja (24).

Šobrīd apstiprināšanā ir stratēģiski likumprojekti, kas nosaka, ka visām valsts pārvaldes iestādēm ar 01.01.2009. obligāti ir jāsniedz visa normatīvajos aktos noteiktā informācija (deklarācijas) elektroniskā formā, izmantojot organizācijas Elektronisko deklarēšanas sistēmu. Ar 2010.gadu šī informācija elektroniski ir jāsniedz arī normatīvajos aktos noteiktajām pārējām juridiskajām un fiziskajām personām. Papildus minētajam, ir uzsākti izstrādes darbi esošajās informācijas sistēmās, lai ar 2009.gadu iedzīvotāji varētu veikt tā saucamo *nulles deklarāciju* iesniegšanu. **Minēto pasākumu rezultātā visas juridiskās un fiziskās personas iesniegs deklarācijas, izmantojot organizācijas informācijas sistēmu piedāvātās iespējas.**

Saskaņā ar Eiropas Komisijā apstiprināto e-muitas stratēģiju līdz 2010.gadam organizācijas Muitas informācijas sistēma jāpapildina ar Eiropas Komisijas standartos noteikto eksporta un importa procedūru funkcionalitāte. Līdz 2013.gadam jāievieš vienas pieturas stratēģija, kuras pamatprincips ir, ka jebkurš Eiropas Savienības pilsonis, neierodoties Latvijā, var deklarēt muitas preces no jebkuras Eiropas Savienības dalībvalsts, izmantojot organizācijas E-muitas sistēmas portālu.

Rezumējot, autors var secināt, ka nepārtrauktas organizācijas nodokļu un muitas informācijas sistēmu, datu noliktavas un audita atbalsta sistēmu pilnveidošanas rezultātā tiek paaugstināta iekšzemes un starptautiskās tirdzniecības drošības līmenis, atvieglota muitas un nodokļu formalitāšu kārtošana, paātrināta preču aprite pāri Eiropas Savienības robežām un samazinātas organizācijas administratīvās izmaksas. Jāatzīmē, ka **šobrīd informācijas sistēmas ir kļuvušas par organizācijas „N" biznesa procesu neatņemamu sastāvdaļu**. Organizācijas mērķu sasniegšana nav iedomājama bez informāciju sistēmu nepārtrauktas pieejamības un tajās esošo datu integritātes un uzticamības. Būtisks faktors šādu organizācijai nepieciešamo garantiju sniegšanai ir informācijas sistēmu infrastruktūras, tajā skaitā datu centra, droša, nevainojamai un stabilai darbībai, kas arī tiks apskatīta nākošajā apakšnodaļā.

2.2. Organizācijas „N" informācijas sistēmu fiziskās drošības atbilstība normatīvo aktu prasībām

Atbilstoši normatīvo aktu **prasībām ar organizācijas vadības rīkojumu ir apstiprināti organizācijas informācijas sistēmu drošības noteikumi** (Noteikumi), kas nosaka organizācijas informācijas sistēmas drošības sistēmas organizatoriskos pamatprincipus un darbību kārtību, lai regulētu organizācijas informācijas pieejamību un klasifikāciju. Papildus informācijas sistēmas drošības noteikumiem ar vadības rīkojumu ir apstiprināts organizācijas informācijas sistēmas resursa īpašnieku (sistēmas pārziņi), resursa īpašnieku pilnvaroto personu un aizbildņu saraksts, kas nosaka, par kuriem informācijas sistēmas resursiem ir atbildīgi konkrētu struktūrvienību ierēdņi vai darbinieki, atbilstoši Noteikumos definētajām kategorijām (24).

Saskaņā ar Noteikumu prasībām, **organizācijā ir veikta risku analīze informāciju sistēmu nepieejamības ietekmei uz biznesa procesiem**. Veiktās risku analīzes rezultātā, iespēju robežās tika identificēti visi iespējamie riski, to ietekme un nepieciešamie pasākumi šo risku novēršanai. Tika identificēti sekojoši organizācijas biznesa procesus ietekmējoši informācijas sistēmu nepieejamības laiki:

- Datu noliktavas sistēmai līdz 24 stundām (72 stundas - kritiskas);
- Nodokļu informācijas sistēmai līdz 3 stundām (24 stundas);
- Muitas informācijas sistēmai līdz 1 stundai (3 stundas);
- Elektroniskās deklarēšanas sistēmai līdz 1 stundai (3 stundas);
- Risku analīzes, audita un tematisko pārbaužu atbalsta sistēmām līdz 24 stundām (72 stundas);
- Aktīvās direktorijas infrastruktūrai un e-pasta sistēmai līdz 1 stundai (3 stundas).

Tātad organizācijas nepieciešamība nosaka, ka informācijas sistēmu infrastruktūrai, tajā skaitā datu centram, jāizvirza tādas kvalitātes prasības, kas plānotu tehnisko apkopju un incidentu gadījumos nodrošina **informācijas sistēmas darbības atjaunošanu 1 stundas laikā**.

Atbilstoši normatīvo aktu prasībām, **organizācijā ir izstrādāti informācijas sistēmu nepārtrauktas darbības nodrošināšanas plāni**, kuros ir noteikti organizatorisko un tehnisko pasākumu kompleksi preventīvu pasākumu veikšanai, lai iespēju robežās izvairītos no

cilvēciska faktora izraisītām informācijas sistēmu nepieejamībām, un konkrētas darbinieku lomas un rīcība, incidentu gadījumos.

Atbilstošas fiziskās drošības prasības organizācija arī izvirza, iegādājoties informācijas sistēmas infrastruktūrai nepieciešamo datortehniku un komunikāciju tīklu aktīvo aparatūru. Visām aparatūras darbību nodrošinošajām kritiskajām komponentēm jābūt dublētām un karsti maināmām, lai, komponenšu bojājumu gadījumā, tās būtu iespējams nomainīt, neapstādinot datortehnikas vai iekārtas darbību.

Attiecīgas prasības tiek izvirzītas plānojot informācijas sistēmu tehnisko infrastruktūru un realizējot tehnisko pasākumu kopumu, lai, iespēju robežās, fiziski izvietotu informācijas sistēmas loģiskās komponentes uz dažādiem neatkarīgiem datortehnikas resursiem, izslēdzot *single–point–of–failure* faktora ietekmi uz sistēmas kopējo pieejamību.

Mūsdienās informācijas sistēmu infrastruktūras tehnoloģiskie risinājumi izmanto augstas veiktspējas serverus un disku masīvus, kuri ātrdarbības nodrošināšanai izmanto lielus serveru un disku kontrolieru operatīvās atmiņas (RAM), procesoru (CPU) un disku tiešās pieejas atmiņas (*cache*) apjomus. Šajos moduļos zemākā līmeņa sīkprogrammas (*firmware*) izvieto informācijas apgabalus, kuri nepieciešami operatīvai un nepārtrauktai operētājsistēmas un programmatūras darbības nodrošināšanai, lai būtiski palielinātu sistēmas kopējo ātrdarbību.

Organizācijā „N" ieviesti augstas veiktspējas serveri un disku masīvi, lai samazinātu nepieciešamību pēc nepārtrauktas datu nolasīšanas no fiziskajiem diskiem (samazinātu I/O un R/W operācijas), palielinot vairākkārtīgi operētājsistēmu un datu bāzu ātrdarbību. Datu bāzu pārvaldības sistēmas biežāk izmantotās darba tabulas un indeksu masīvus var turēt serveru un/vai disku masīvu kontrolieru operatīvajās atmiņās, informāciju operatīvajā atmiņā noteiktā laika vienībā sinhronizējot ar informāciju uz fiziskajiem disku atmiņas apgabaliem. Tādējādi tiek sasniegta būtiska disku masīvuakopējā veiktspēja un ātrdarbība – *enterprise* tipa disku masīviem līdz pat 1 000 000 I/O operācijām sekundē (24).

Lai nodrošinātu organizācijas „N" informācijas sistēmās uzkrāto datu integritāti minēto organizācijā ieviesto tehnoloģisko risinājumu gadījumos, **būtisks faktors ir nepārtraukta un kvalitatīva organizācijas „N" datu centra darbība**, nodrošinot augsto tehnoloģiju nevainojamai darbībai tik ļoti nepieciešamo stabilu strāvas padevi un atbilstošus mikroklimata apstākļus.

Lai noskaidrotu organizācijas „N" informācijas tehnoloģiju speciālistu un vadošo darbinieku viedokli par organizācijas datu centra darbības kvalitāti un tā kvalitātes atbilstību normatīvo aktu un organizācijas izvirzītajām fiziskās drošības prasībām, darba autors veica aptauju, kas tiks apskatīta nākošajās apakšnodaļās.

2.3. Aptauja par datu centra pakalpojuma kvalitāti

Katram pētniekam, kurš ir iecerējis izmantot savā pētījumā anketēšanas metodi ir vispirms jāpieņem lēmums par to, ko tieši ir nepieciešams uzzināt, kas ir anketas mērķa auditorija un kādā veidā izdarīt aptauju.

Anketēšana ir pirmreizēju datu vākšanas veids, tā sastāv no jautājumiem, kas adresēti respondentiem atbildēšanai uz tiem.

Neviens pētījums nevar notikt bez labi izveidotas anketas. Diemžēl nav izstrādāta teorētiska bāze aptaujas lapas veidošanai. Viss, pēc kā pētnieks var vadīties, ir viņa vai citu pētnieku iepriekšējā pieredze. Tāpēc var teikt, ka anketas izstrādāšana ir vairāk māksla nekā zinātne.

Sākotnēji darba autors plānoja veikt anketēšanu pašvaldības un valsts iestādēs. Anketas elektroniski tika aizsūtītas 15 valsts iestādēm un 50 pašvaldībām. Diemžēl, uz autora nosūtītajiem e-pastiem atbildēja tikai 2 valsts iestādes un 1 pašvaldība. Tāpēc anketēšana tika veikta tikai organizācijā „N" un tika aptaujāti 50 respondenti, no kuriem 28 respondenti bija informācijas tehnoloģiju eksperti un 22 – organizācijas „N" dažādu līmeņu vadītāji. Respondentu vecums un dzimums netika ņemts vērā. Aptaujāto cilvēku darba pienākumi saistīti ne tikai ar informāciju sistēmu uzturošās datortehnikas un programmatūras administrēšanu, uzraudzību un attīstību, bet arī ar informācijas tehnoloģiju pakalpojumu izmantošanu, tāpēc darba autors uzskata, ka pēc respondentu sniegtajām atbildēm var noteikt arī kopējās tendences valstī.

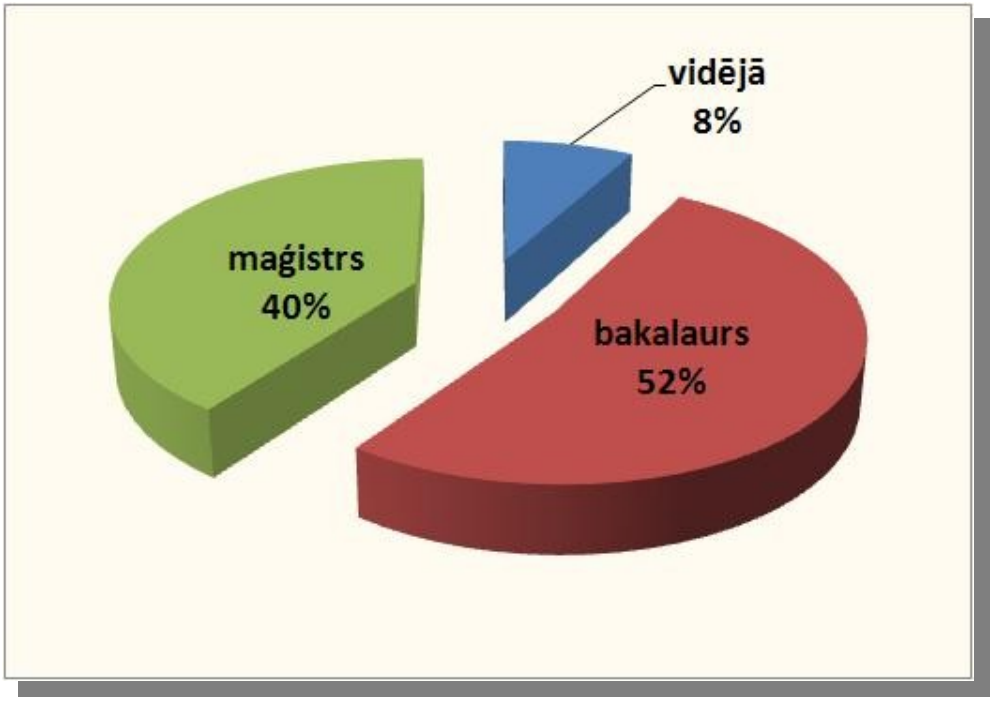
Lai iegūtu nepieciešamos rezultātus, aprēķinos tika izmantotas statistiskās analīzes metodes. Lai iegūtu procentuālo sadalījumu attiecīgo anketas jautājumu atbilžu analīzē, tika izmantota grupēšanas un vidējo aritmētisko lielumu aprēķināšana. Tika izveidota anketa (skat. 1.pielikumu), kurā autors par anketēšanas un intervēšanas mērķi izvirzīja sekojošo:

- noskaidrot respondentu zināšanas par normatīvo aktu prasībām;
- par organizācijā veikto informācijas sistēmas nepieejamības riska ietekmi uz organizācijas biznesa procesiem analīzi;
- noskaidrot organizācijas IT ekspertu un vadītāju viedokli par organizācijas izmantotā datu centra atbilstību organizācijas vajadzībām;
- datu centra komponenšu lomu kvalitatīva pakalpojuma nodrošināšanā.

Nākošajā apakšnodaļā autors analizēs aptaujā iegūtos datus.

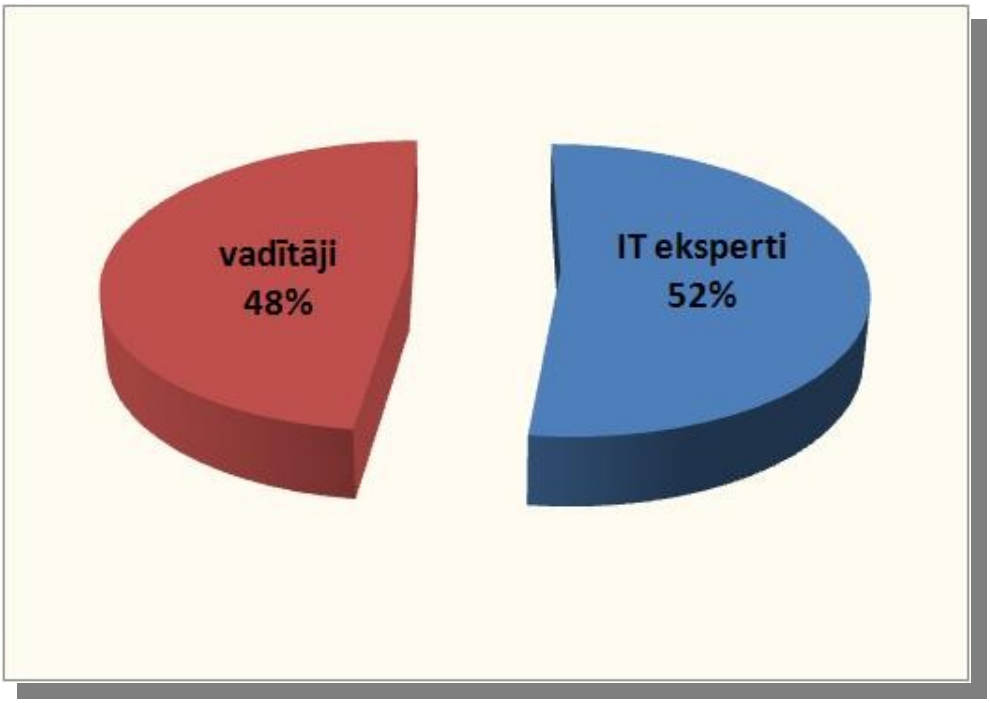
2.4. Aptaujas datu analīze

Uz jautājumu „*Jūsu izglītība: vidējā, bakalaurs vai maģistrs?*" respondenti sniedza sekojošas atbildes: 40% respondentiem bija maģistra grāds, 52% – bakalaura grāds, 8% attiecīgi vidējā izglītība (skat. 2.1.att.). Attiecīgi 92% respondenti ir ieguvuši augstāko izglītību, bet, veicot pārrunas ar respondentiem, kuriem ir vidējā izglītība, autors guva informāciju, ka respondenti aptaujas brīdī mācās augstskolā. Kopumā, var secināt, organizācijā „N" nodarbināto darbinieku izglītības līmenis ir atbilstošs.



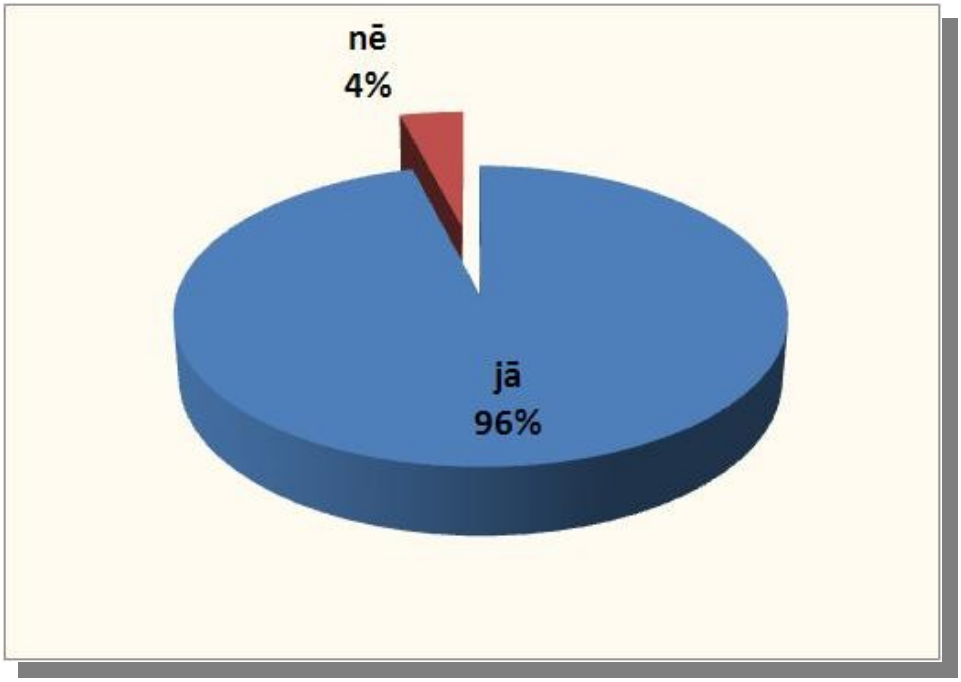
2.1. att., Respondentu izglītība

Uz jautājumu „*Jūsu ieņemamais stāvoklis organizācijā: informācijas tehnoloģiju eksperts vai vadītājs?*" respondenti sniedza sekojošas atbildes: 52% respondenti bija informācijas tehnoloģiju eksperti un 48% bija organizācijā par informācijas tehnoloģijām atbildīgie vadošie darbinieki (skat. 2.2.att.). Analizējot šādu procentuālo attiecību, autors konstatēja, ka ne visu respondentu darba pienākumi ir tiešā veidā saitīti ar informācijas tehnoloģiju uzturēšanu un attīstību. Daļa no respondentiem pārstāv arī tos darbiniekus, kas izmanto informācijas sistēmas darba pienākumu veikšanai. Autors uzskata, ka tādējādi uz anketā uzdotajiem jautājumiem tika saņemti daudzpusīgāki dažādu organizācijas „N" jomu pārstāvošo darbinieku viedokļi, kas nav mazsvarīgi pētījumam kopumā.



2.2. att., Respondentu ieņemamais stāvoklis organizācijā

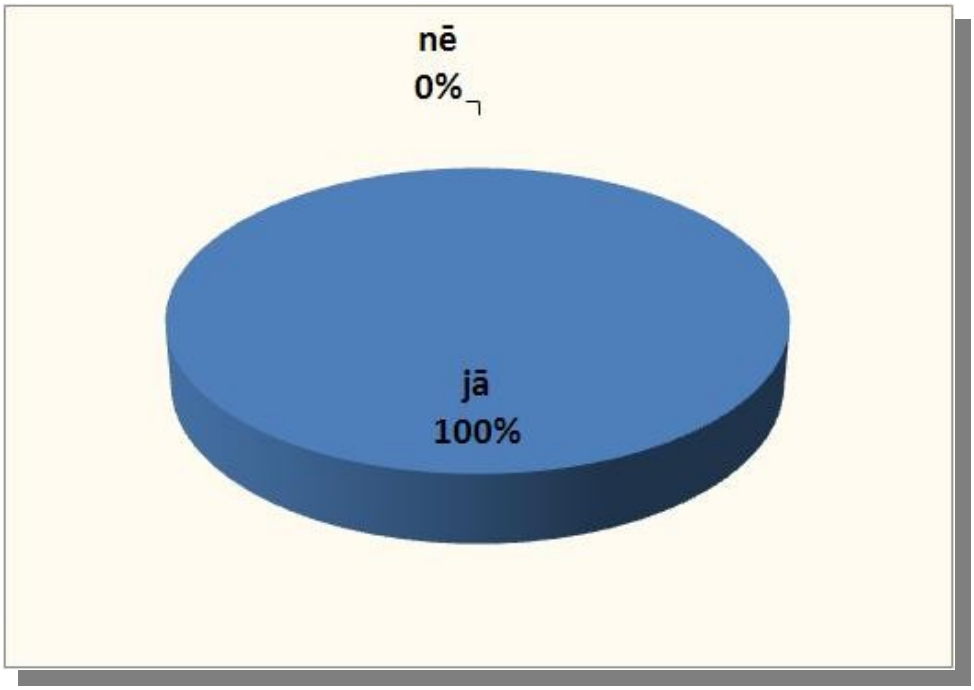
Uz jautājumu „*Vai Jūsu organizācijas pamatfunkciju veikšanai ir nepieciešama pieeja pie ārējiem informācijas resursiem, interneta?*" respondenti sniedza sekojošas atbildes: ar „Nē" atbildēja 4% respondenti un „Jā" atbildēja atlikušie 96% respondenti (skat. 2.3.att.).



2.3. att., Respondentu atbildes uz jautājumu „Vai Jūsu organizācijas pamatfunkciju veikšanai ir nepieciešama pieeja pie ārējiem informācijas resursiem, interneta?"

No atbildēm ir secināms, ka Interneta sniegtās iespējas – elektroniskais pasts, citu organizāciju mājas lapas un informācijas sistēmas, ir kļuvušas par organizācijas ikdienas nepieciešamību un šīs piedāvātās iespējas tiek aktīvi gan organizāciju, gan darbinieku savstarpējā komunikācijā. Organizācijas „N" pati uztur savu mājas lapu un vairākas publiskas (piemēram, *Publiskojamo datu bāze u.c.*) un uz lietotāju autentifikāciju balstītas datu bāzes (piemēram, *Elektroniskās deklarēšanas sistēma, Jaunā datorizētā tranzīta kontroles sistēma u.c.*). Šie publiski sniegtie pakalpojumi ir iestādes sabiedriskais tēls virtuālajā e-pasaules vidē, kas mūsdienās jau ir kļuvusi par neatņemamu organizācijas vizītkarti.

Uz jautājumu „*Vai Jūsu organizācijas pamatfunkciju vajadzībām ir izstrādāta(as) informācijas sistēma(as)*?" visi respondenti 100% atbildēja apstiprinoši (skat. 2.4.att.).

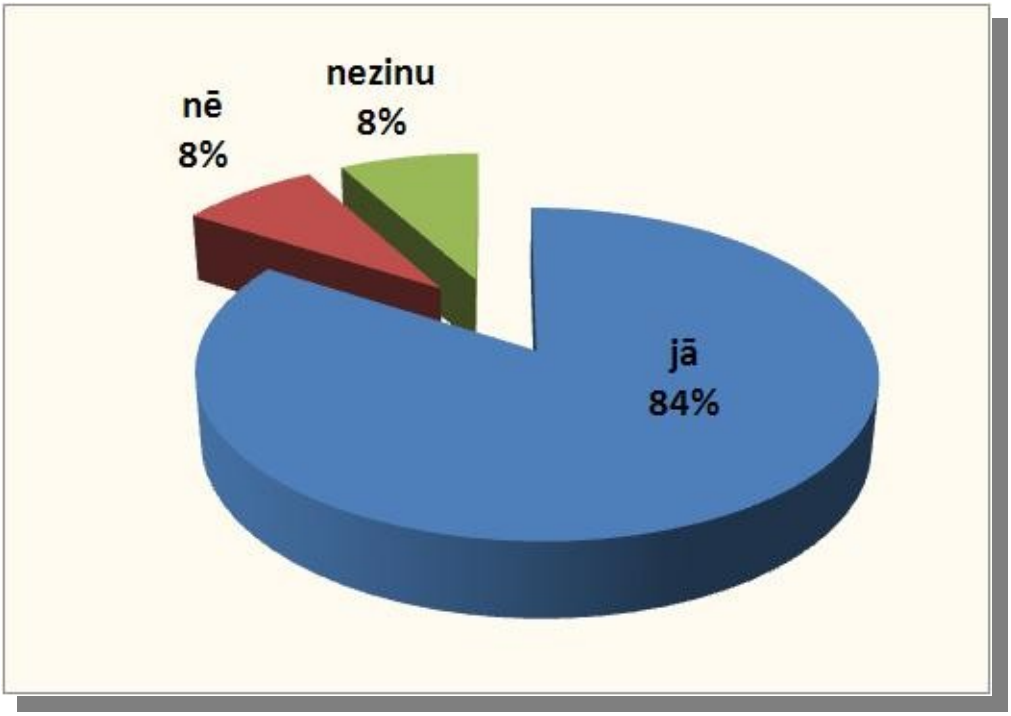


2.4. att., Respondentu atbildes uz jautājumu „Vai Jūsu organizācijas pamatfunkciju vajadzībām ir izstrādātas informācijas sistēmas?"

Minētais jautājums tika uzdots, lai pārliecinātos par respondentu godprātību un informētību. Respondentu sniegtā viennozīmīgā atbilde liecina, ka organizācijas darbinieki apzinās informācijas tehnoloģiju lomu organizācijas biznesa procesos.

Darba autors nākošos divus jautājumus anketā iekļāva, lai netiešā veidā noskaidrotu respondentu viedokli par viņu uzturēto vai izmantoto informācijas sistēmu statusiem normatīvo aktu izpratnē.

Uz jautājumu „*Vai Jūsu organizācijas uzturētā(ās) informācijas sistēma(as) ir reģistrētas Datu valsts inspekcijā?*” respondenti sniedza sekojošas atbildes: ar „Jā” atbildēja 84% aptaujātie, ar „Nē” – 8% un „Nezinu” – 8% (skat. 2.5.att.).

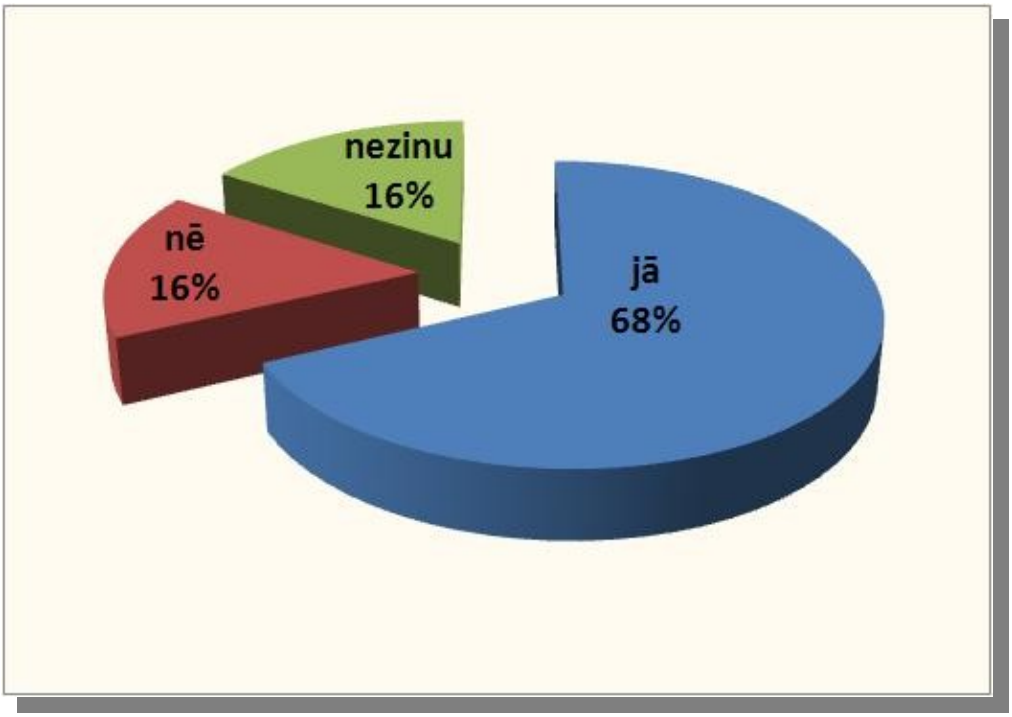


2.5. att., Respondentu atbildes uz jautājumu „Vai Jūsu organizācijas uzturētās informācijas sistēmas ir reģistrētas Datu valsts inspekcijā?”

Pēc saņemtajām atbildēm ir skaidri redzams, ka 84% respondentu ir informēti, ka viņu uzturētā vai izmantotā informācijas sistēmā tiek uzkrāti dati par fiziskajām un juridiskajām personām. Pārrunās autors noskaidroja, ka visi respondenti ir informēti par *Fiziskas personas datu aizsardzības likumu* un likuma izvirzītās prasības personas datu apstrādes informācijas sistēmām.

Autors konstatēja, ka intervijās, aicinot respondentus nosaukt izvirzītās prasības, vairākums minēja likuma izvirzītās loģiskās aizsardzības prasības – lietotāju autentifikāciju un autorizāciju, lietotāju veikto darbību auditu, ugunsmūrus un pretvīrusu ķeršanas programmatūru. Neliels skaits respondentu minēja tādus pasākumus, kā informācijas sistēmu administratoru un lietotāju izglītošanu informācijas sistēmu drošības jautājumos, riska analīzes veikšanu, serveru telpas fiziskās pieejas kontroli un atbilstoša mikroklimata nodrošināšanu.

Uz jautājumu „*Vai Jūsu organizācijas uzturētajai(ām) informācijas sistēmai(ām) ir piešķirts valsts informācijas sistēmas statuss?*" respondenti sniedza sekojošas atbildes: ar „Jā" atbildēja 68%, „Nē" – 16% un „nezinu" – 16% respondentu (skat. 2.6.att.).



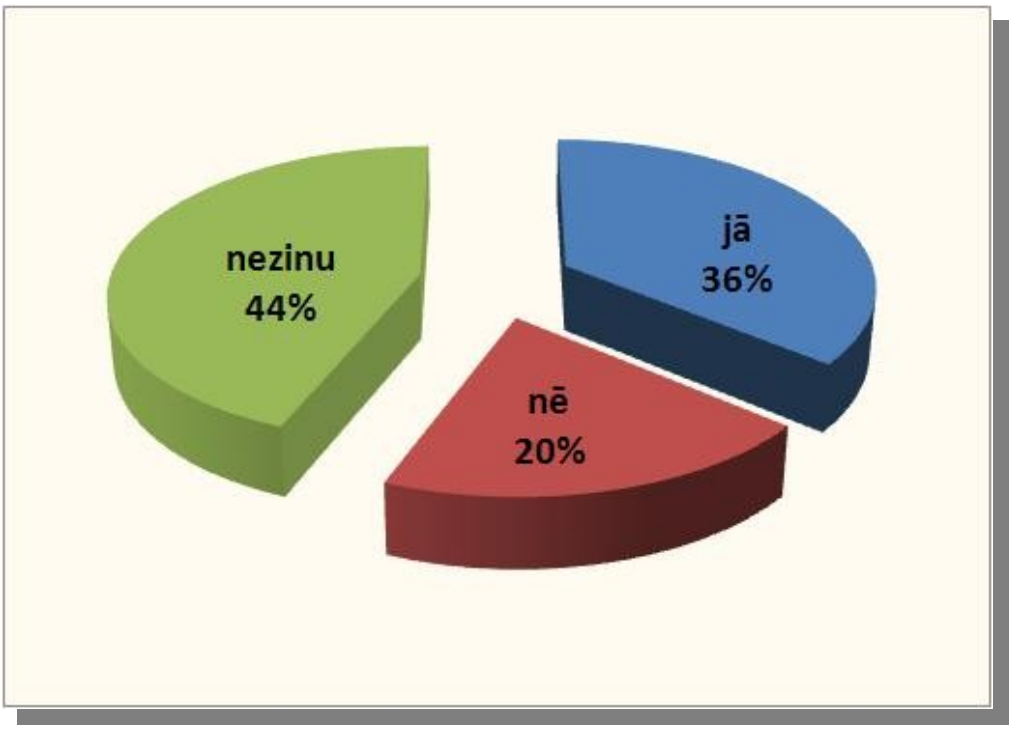
2.6. att., Respondentu atbildes uz jautājumu „Vai Jūsu organizācijas uzturētajai informācijas sistēmai ir piešķirts valsts informācijas sistēmas statuss?"

Lielāks negatīvi atbildējušo respondentu īpatsvars (32%), skaidrojams ar to, ka valsts informācijas sistēmas statuss ir juridiski specifisks jēdziens, un organizācijas darbiniekiem, it sevišķi tiem, kas informācijas sistēmas izmanto ikdienas darbā, šīs normatīvā akta izvirzīts jēdziens ir neskaidrs. Un otrs aspekts ir tas, ka organizācijā IT eksperti specializējas konkrētu informācijas sistēmu uzturēšanā, kurām šis statuss nav piešķirams, piemēram, organizācijas finanšu vadības un grāmatvedības sistēma, lietvedības un dokumentu vadības sistēma u.c.

Kā jau tika noskaidrots darba pirmajā nodaļā, tad saskaņā ar *Valsts informācijas sistēmas likumu* valsts informācijas sistēmas statuss tiek piešķirts organizācijas informācijas sistēmām, kurās tiek uzkrāta valsts pārvaldes funkciju veikšanai kritiski nepieciešama informācija, piemēram, LR Iekšlietu ministrijas Iedzīvotāju reģistrs, LR Uzņēmumu reģistra Komercuzņēmumu reģistrs, Valsts ieņēmumu dienesta Nodokļu informācijas sistēma un Muitas informācijas sistēma u.c. organizāciju informācijas sistēmas. Šo informācijas sistēmu nepieejamības gadījumā, būtiski ir apdraudēta gan organizācijas, gan valsts spēja atbilstošajās jomās veikt savas funkcijas.

Valsts informācijas sistēmu un personas datu apstrādes sistēmu uzturēšanā īpaši jāņem vērā iespējamie fiziskie un loģiskie apdraudējumi, tajā skaitā arī pret datu centriem. Lai varētu novērtēt iespējamos riskus un tos iespēju robežās vadīt, viens no obligātajiem pasākumu kompleksiem ir veikt informācijas sistēmas un to komponenšu pieejamības riska analīzi, ko arī darba autors centās noskaidrot ar nākamā anketas jautājuma palīdzību.

Uz jautājumu „*Vai Jūsu organizācijā ir veikta informācijas sistēmas(u) un ārējo informācijas resursu pieejamības riska analīze, lai noteiktu ietekmi uz organizācijas spēju nodrošināt pamatfunkciju izpildi datu centra nepieejamības gadījumā?*" respondenti sniedza sekojošas atbildes: ar „Jā" atbildēja 36%, „Nē" – 20% un „Nezinu" – 44% respondentu (skat. 2.7.att.).

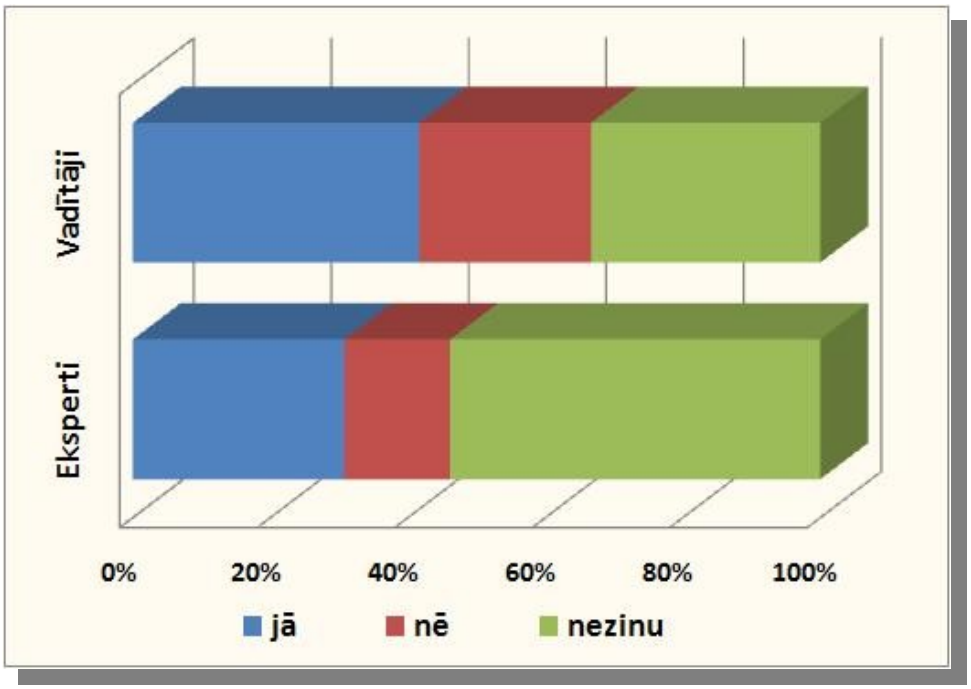


2.7. att., Respondentu atbildes uz jautājumu" Vai Jūsu organizācijā ir veikta informācijas sistēmas(u) un ārējo informācijas resursu pieejamības riska analīze?"

Sniegtās respondentu atbildes par veikto risku analīzi un risku iestāšanās ietekmi uz organizācijas biznesa procesiem, autoram radīja izbrīnu! Ja no informācijas tehnoloģiju speciālistu un vadības puses 64% respondenti atbild negatīvi, tad tas liecina par organizācijas un tās vadības neizpratni par informācijas sistēmu lomu organizācijas biznesa procesu kvalitātes nodrošināšanā. It sevišķi, ja ņem vērā iepriekšējos jautājumos organizācijas ekspertu sniegtās atbildes par informācijas sistēmu valstisko statusu un normatīvajos aktos noteiktajiem pienākumiem, saskaņā ar kuriem organizācijas vadībai kā personas datu

apstrādes sistēmas pārzinim ir jāatbild par personas datu apstrādi saskaņā ar Fizisko personu datu aizsardzības likuma prasībām.

Atsevišķi analizējot respondentu grupu (IT eksperti un vadība) sniegtās atbildes, autors secina, ka 40% vadītāju ir atbildējuši apstiprinoši, nevarēja atbildēt uz jautājumu – 28% un viennozīmīgu ,,Nē" teica ap 12% vadītāju. Savukārt 22% ekspertu atbildēja ar „Jā", ar ,,Nē" – 18% un ar ,,Nezinu" atbildēja 60%.. (skat. 2.8.att.).



2.8.att., Respondentu atbildes uz jautājumu" Vai Jūsu organizācijā ir veikta informācijas sistēmas un ārējo informācijas resursu pieejamības riska analīze?"

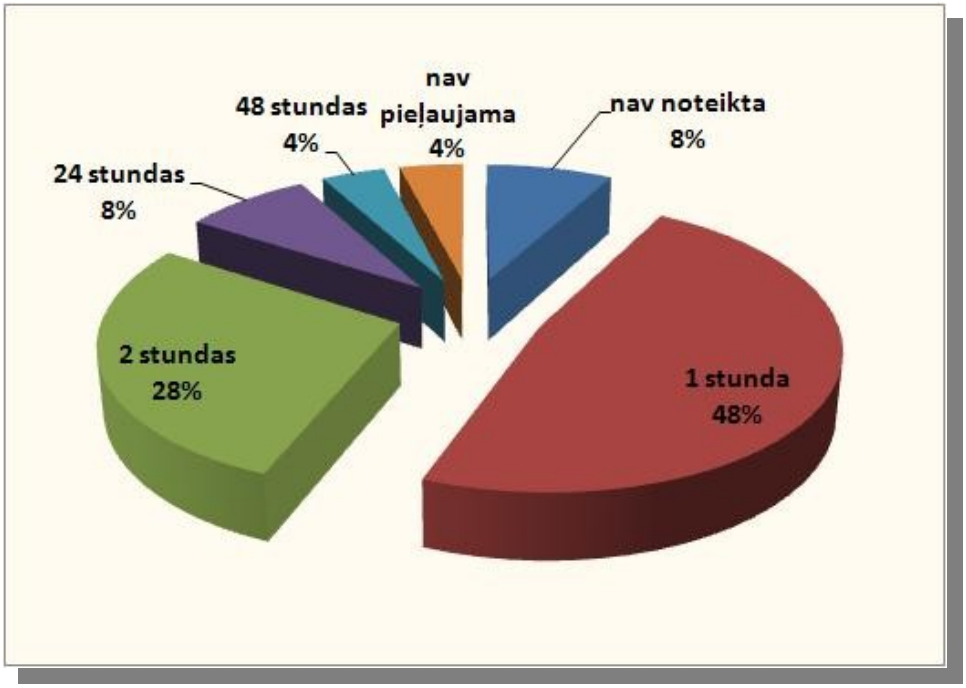
Respondentu grupu sniegtās atbildes uz jautājumu par risku analīzi, varētu skaidrot ar vadītāju un ekspertu atšķirīgajiem darba stāžiem organizācijā. Autors noskaidroja, ka vidējais organizācijas eksperta (saprast arī, kā galvenais speciālists) darba stāžs organizācijā ir pusotrs gads. Diemžēl, daļai no darbiniekiem šis ir arī kopējais darba stāžs informācijas tehnoloģiju jomā.

IS drošības politikas pamatu lietderīgi saistīt ar uzņēmuma pārvaldes formu – ja uzņēmumam ir vertikāla pārvaldes struktūra, turklāt zemāka ranga darbinieki, tostarp arī datorspeciālisti saņem noteiktu nemainīgu (turklāt ne pārāk lielu) darba algu, tad vadītājam pašam ļoti lielā mērā jāuzņemas atbildība par IS drošības sistēmas veidošanas un uzturēšanas principiem un kontroli, jo zemāka ranga darbinieki var nebūt īpaši motivēti pēc savas iniciatīvas rūpēties par uzņēmuma drošības pastāvīgu nodrošināšanu un pilnveidošanu. Savukārt, ja uzņēmuma vadītājs nevēlas vai zināšanu trūkuma dēļ nespēj pats pilnvērtīgi

uzņemties atbildību par šo jomu, tad uzņēmumā lietderīgi veidot horizontālu pārvaldes struktūru, kur liela daļa atbildības un rīcības brīvības deleģēta vidēja ranga struktūrvienību (tajā skaitā arī Informācijas sistēmu daļas) vadītājiem, un viņi tiek motivēti censties pastāvīgi pilnveidot viņu struktūrvienības darbību – gan ar elastīgu darba apmaksas sistēmu, kas ir atbilstīga viņu ieguldījumam un pozitīvai iniciatīvai, gan ar citiem motivēšanas paņēmieniem, kas vērsti uz iespēju viņiem paaugstināt savu kompetenci un to pilnvērtīgi arī īstenot (tā sauktā ārējās un iekšējās motivācijas sistēma) (18).

Te gan jāuzsver, ka jebkurā gadījumā atbildību par IS drošību, ja tas saistīts ar likumos noteikto fizisko un juridisko personu tiesību un interešu aizsardzību, kopumā jāuzņemas organizācijas vadītājam.

Uz jautājumu „*Kāds ir pieļaujamais organizācijas visu informācijas sistēmu maksimālais nepieejamības laiks?*" respondenti sniedza sekojošas atbildes: ar „1 stundu" atbildēja 48%, ar „2 stundām" – 28%, „24 stundas" – 8%, „nav noteikta" – 8% un 4% attiecīgi „48 stundas" un „nav pieļaujama" (skat. 2.9.att.).



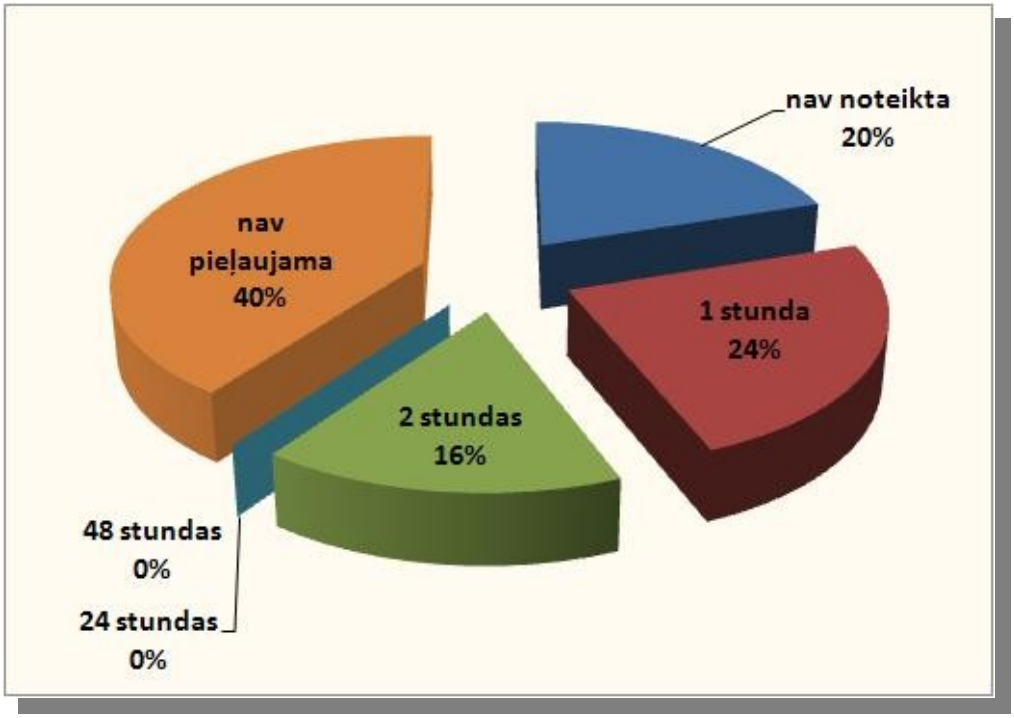
2.9.att., Respondentu atbildes uz jautājumu "Kāds ir pieļaujamais organizācijas visu informācijas sistēmu maksimālais nepieejamības laiks?"

Ņemot vērā iepriekšējā jautājumā respondentu sniegtās atbildes par veikto risku analīzi, autoram rodas šaubas par 80% respondentu novērtētās 0 līdz 2 stundu maksimālās pieļaujamās informācijas sistēmu nepieejamību laikiem.

Ņemot vērā, ka lielākā daļa no respondentiem ir tiešā veidā saistīti ar informācijas sistēmu kvalitatīvas un nepārtrauktas darbības nodrošināšanu, tad intervijās autors konstatēja, ka atbildēs darbinieki minējuši informācijas sistēmu uzturēšanas labās prakses laikus. Minētie termiņi vairāk domāti, kā darbiniekiem stresu nepaaugstinošie laiki, nevis ar organizācijai tiešiem vai netiešiem finansiāliem zaudējumiem saistītajiem riskiem.

Uz šo jautājumu sniegtās atbildes, atkārtoti apstiprina nepieciešamību veikt objektīvu informācijas sistēmu drošības risku un incidentu ietekmes analīzi uz organizācijas biznesa procesiem kopumā. Pārāk augstas izvirzītās pieejamības prasības nepamatoti sadārdzina prasības pret informācijas sistēmu uzturēšanai nepieciešamajiem tehniskiem un tehnoloģiskiem risinājumiem.

Uz jautājumu: „*Kāda ir organizācijas noteiktā maksimāli pieļaujamā datu centra nepieejamība, kura laikā nav pieejama neviena no organizācijai nepieciešamajām informācijas sistēmām?*" respondenti atbildēja ar „1 stunda" 24% gadījumos, 2 stundas – 16%, „nav noteikta" – 20% un „nav pieļaujama" – 40% (skat. 2.10.att.).

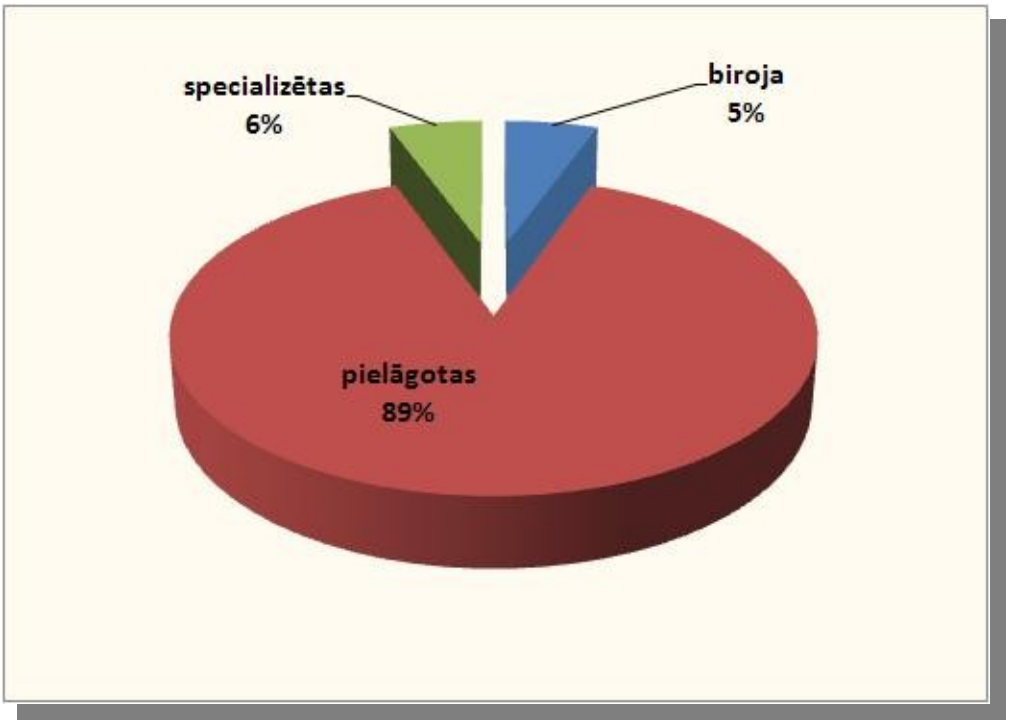


2.10.att., Respondentu atbildes uz jautājumu "Kāda ir organizācijas noteiktā maksimāli pieļaujamā datu centra nepieejamība, kura laikā nav pieejama neviena no organizācijai nepieciešamajām informācijas sistēmām?"

Analizējot uz jautājumu sniegtās respondentu atbildes un ņemot vērā, ka organizācijās nav veikta risku ietekmes uz organizācijas biznesa procesiem analīze, darba autors secina, ka

respondenti atbildes snieguši, vadoties no labās prakses vai dzīves pieredzes. **Informāciju sistēmas kritiskos nepieejamības laikus un to pamatotību objektīvi var noteikt tikai ar riska analīzes palīdzību**, savukārt, **izvirzot nepamatoti augstas prasības pret datu centru pieejamību, var tikt nepamatoti sadārdzinātas datu centra modernizācijas un uzturēšanas izmaksas**. Protams, ka datu centru nepieejamības laiks nedrīkst būt augstāks par organizācijas definēto mazāko informācijas sistēmas nepieejamības laiku, kas respondentu gadījumā ir 1 līdz 2 stundas.

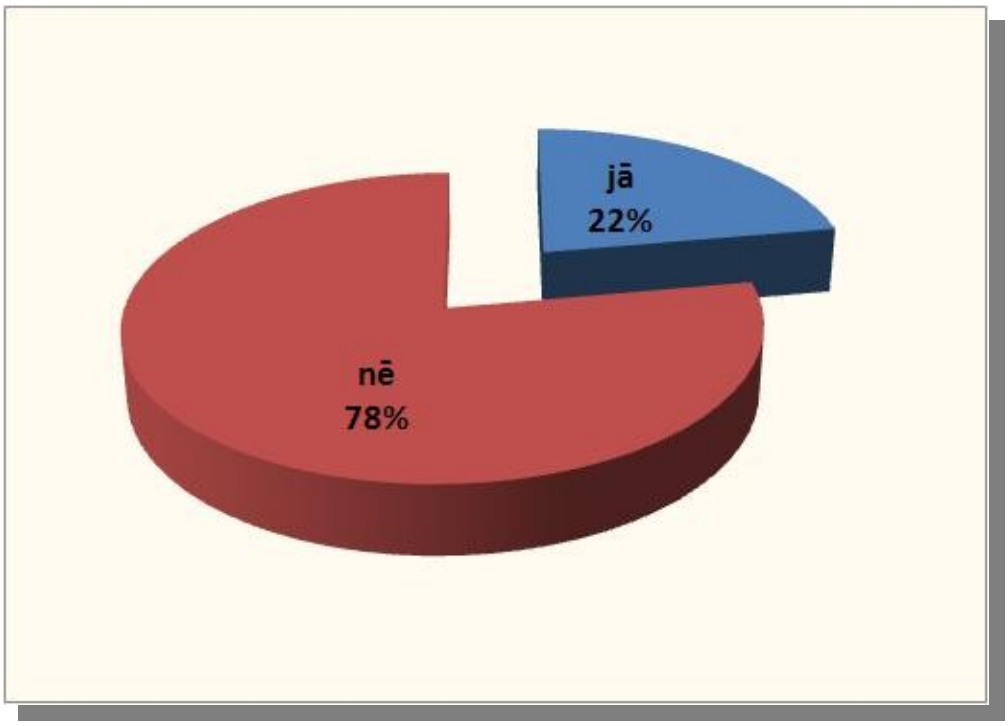
Uz jautājumu „*Vai organizācijas datu centrs ir izvietots biroja telpās, pielāgotās vai speciāli datu centra vajadzībām projektētās telpās?*" 84% respondenti atbildēja, ka organizācijas datu centrs izvietots pielāgotās telpās, 12% respondenti –speciāli projektētās telpās, bet 4% – serveri izvietoti biroja telpās (skat. 2.11.att.).



2.11.att., Respondentu atbildes uz jautājumu „Vai organizācijas datu centrs ir izvietots biroja telpās, pielāgotās vai speciāli datu centra vajadzībām projektētās telpās?"

Analizējot atbildes pa respondentu grupām, autors secināja, ka visi organizācijas eksperti viennozīmīgi norādījuši, ka serveru telpas ir ierīkotas pielāgotās telpās. 5% vadītāju sniegtās atbildes par biroja telpām intervijas laikā tika skaidrotas kā pielāgotas organizācijas biroja telpas, kas, autora skatījumā, arī nav tālu no taisnības organizācijas „N" gadījumā. Savukārt 6% vadītāju sniegtās atbildes par specializētajām telpām uzskatāmas, kā kļūdainas un, visdrīzāk, izraisītas nezināšanas dēļ, kas arī guva apstiprinājumu autora veikto interviju laikā.

Uz jautājumu „*Vai organizācijas datu centrs spēs atbilstošā kvalitātē nodrošināt Jūsu organizācijas esošās un nākotnes prasības arī tuvāko piecu gadu laikā?*” 78% respondenti sniedza negatīvu atbildi un tikai 22% respondentu – pozitīvu (skat. 2.12.att.).



2.12.att., Respondentu atbildes uz jautājumu „Vai organizācijas datu centrs spēs atbilstošā kvalitātē nodrošināt Jūsu organizācijas esošās un nākotnes prasības arī tuvāko piecu gadu laikā?”

Ņemot vērā iepriekšējā jautājumā un darba 2.1.apakšnodaļā aprakstītās organizācijas „N” plānoto informācijas sistēmu modernizācijas un jauno ieviešanas plānus, darba autoram atliek tikai piekrist 78% skeptisko respondentu viedoklim par organizācijas pielāgotā datu centra spējām atbilstošā kvalitātē nodrošināt organizācijas augošās prasības ne tikai tuvāko piecu, bet arī tuvāko divu gadu laikā.

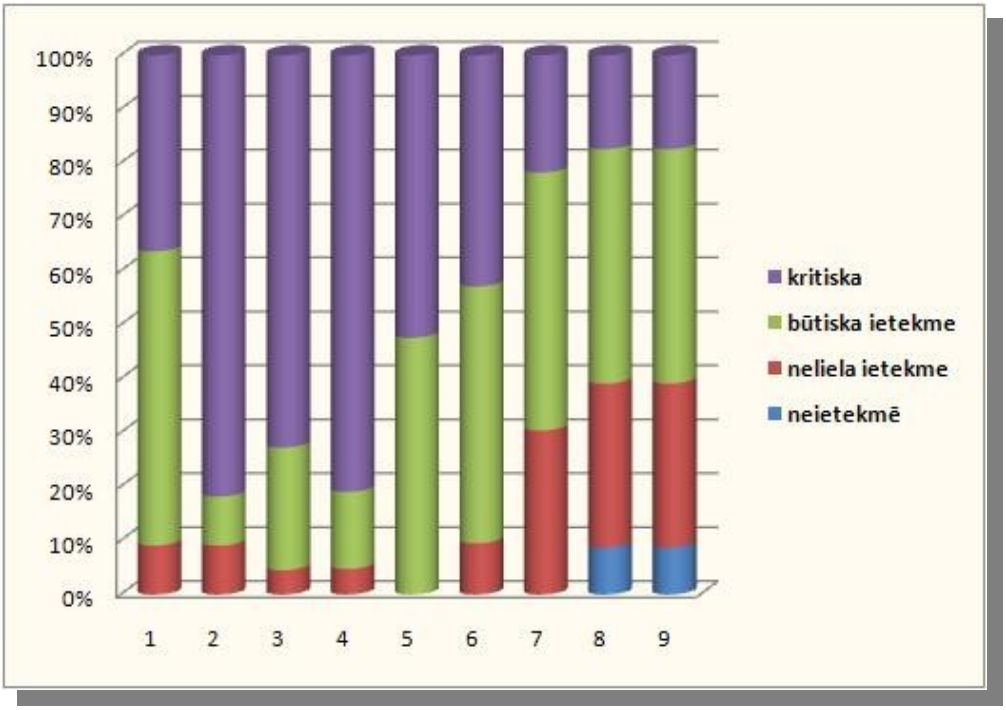
Intervijās respondenti savu vērtējumu pamatoja ar tādiem ierobežojumiem, kā pastāvošās problēmas ar datortehnikas izvietojumu, lai optimāli varētu organizēt kondicionieru sistēmas virzītās augstā gaisa plūsmas pa datortehnikas vienībām un serveru telpas platības un grīdas nestspējas neatbilstību. Esošā serveru telpa uz doto brīdi ir aizpildīta un jaunas aparatūras uzstādīšana un darbināšana būs apgrūtināta. Lielākā daļa no darbiniekiem izteica viedokli, ka organizācijas „N” informācijas sistēmu nepārtrauktas darbināšanas vajadzībām ir nepieciešams jauns un moderns datu centrs.

Anketas pēdējā jautājumā „*Lūdzu, norādiet, Jūsuprāt, nepieciešamo datu centra darbības kvalitātes nodrošināšanai nepieciešamo aprīkojumu*” respondentiem tika piedāvāts novērtēt deviņas datu centra kvalitatīvai darbībai nepieciešamās komponentes (skat. 2.13.att.):

1) ēkas konstrukciju un platības atbilstība;
2) elektroapgāde;
3) avārijas strāvas ģenerators;
4) nepārtrauktas elektrobarošanas avots (UPS);
5) mikroklimata sistēma;
6) automatizēta ugunsdzēsības sistēma;
7) signalizācijas un video novērošanas sistēma;
8) fiziskā apsardze;
9) diennakts uzraudzība.

Respondentiem bija jānovērtē komponenšu kvalitātes ietekmi uz kopējo datu centra kvalitāti pēc 4 punktu skalas:

- 1 punkts, ja aprīkojuma esamība neietekmē datu centra pakalpojuma kvalitāti;
- 2 punkti – ar nelielu ietekmi,
- 3 punkti – būtiska ietekme,
- 4 punkti – kritiska – bez šīs komponentes datu centra darbības kvalitāte nav iedomājama.



2.13.att., Respondentu atbildes uz jautājumu „Lūdzu, norādiet, Jūsuprāt, datu centra darbības kvalitātes nodrošināšanai nepieciešamāko aprīkojumu”

Ar „būtisku ietekmi" 53% respondenti un „kritisku" ietekmi 37% respondenti novērtēja datu centra ēkas konstrukciju un platības atbilstību (skat. 2.13.att. 1.pozīciju), tāpēc, ka esošā serveru telpa ir izvietota pielāgotās ēkas telpās, kas būvētas pagājušā gadsimta 30 gados un tika plānotas dzīvojamā fonda vajadzībām. Intervijās darbinieki norādīja, ka šī datu centra komponente ir problemātiskākā esošajam organizācijas datu centram, tuvākās nākotnes perspektīvā.

Kā **viskritiskāko** no visām datu centra komponentēm pretendenti atzīmēja elektroapgādes sistēmas (skat. 2.13.att. 2.pozīciju), tajā skaitā, strāvas ģeneratoru un nepārtrauktas elektrobarošanas avota sistēmas (skat. 2.13.att. 3 un 4.pozīciju), nepārtrauktu un nevainojamu darbību. 84% no respondentiem norādīja ka kritisku datu centram atbilstošas kapacitātes jaudas un nepārtrauktas strāvas piegādi, 83% – nepārtrauktas elektrobarošanas avota sistēmas un 73% – avārijas strāvas ģeneratorus. Intervijās autors noskaidroja, ka 2004.gadā veiktā serveru telpas jaudas palielināšana līdz 120kW šobrīd ir nepietiekama. Datu centra prasības pēc strāvas jaudas ir dramatiski augušas. Šobrīd esošā 120kW jauda spēj nodrošināt esošās datortehnikas un mikroklimata sistēmas patēriņu, bet 2008.gada iepirkumos plānotās datortehnikas darbināšanu vairs nespēs nodrošināt.

Likumsakarīgi, ka respondenti kā **nākošo kritiskāko** no visām datu centra komponentēm atzina mikroklimata sistēmu (skat. 2.13.att. 5.pozīciju). 53% respondentu atzīmēja šo komponenti ar „kritisku" un 47% – ar „būtisku ietekmi",. Intervijās ar respondentiem, autors konstatēja, ka esošajai organizācijas datu centra mikroklimata sistēmai, kas ir būvēta izmantojot stacionāros kondicionierus, ir regulāras problēmas ar optimālas temperatūras nodrošināšanu. Datortehnikas dzesēšana serveru telpā nav pārdomāta un siltajos gada laika mēnešos dzesēšanas problēma sevišķi aktualizējas. Problēmas kritiskumu pastiprina apstāklis, ka modernā datortehnika ir apgādāta ar pret-pārkaršanas aizsardzību, kas automātiski pārtrauc strāvas piegādi serveru un disku masīvu kontrolieru procesoriem, gaisa temperatūrai datortehnikas korpusos pārsniedzot ražotāju iestatītos parametrus. Bieži vien pēc šāda rakstura incidentiem datu bāzu administratoriem bija jāveic informācijas atjaunošana no rezerves kopijām, dēļ datu integritātes problēmām informācijas sistēmās.

Respondenti sekojoši novērtēja nepieciešamību pēc automatizētas datu centra ugunsdzēsības sistēmas (skat. 2.13.att. 6.pozīciju): 46% respondenti to novērtēja ar „kritiska", 47% – „būtiska ietekme" un 7% – „neliela ietekme". Efektīvas automatizētas ugunsdzēsības sistēmas esamību, respondenti vērtēja, kā būtisku faktoru ar lielu ietekmi datu centra spējā nodrošināt kopējo pakalpojuma kvalitāti tādos ārkārtas gadījumos, kā ugunsgrēks.

Ar būtisku un nelielu ietekmi uz datu centra pakalpojuma kvalitāti aptuveni 63% respondenti novērtēja datu centra automatizētu signalizācijas un video novērošanas sistēmas, fiziskās apsardzes un datu centra komponenšu diennakts uzraudzības esamību (skat. 2.13.att. 7., 8. un 9..pozīciju). Autors uzskata, ka 34% respondentu paustais viedoklis, ka fiziskās drošības nodrošināšanas preventīvie pasākumi nav būtiski informācijas sistēmu nepārtrauktas darbības un, atbilstoši normatīvo aktu prasībām, drošības nodrošināšanai, ir respondentu nezināšana un, iespējams, precedenta neesamības apliecinājums.

Katrā ziņā, datu centra kritisko mezglu automatizēta un attālināta pārraudzība, vizuālā uzraudzība un fiziskā drošība, ir viens no primārajiem garantiem, augstas pieejamības datu centra kvalitātes nodrošināšanā. Kā piemēru varu citēt tautas sakāmvārdu: „Pret zagļiem nelīdzēs modernas un dārgas dzelzs durvis, ja saimnieks ierīkos slēdzeni viena lata vērtībā."

2.5. Organizācijas „N" datu centra pakalpojuma kvalitātes izvērtējums

Šajā nodaļā autors noskaidroja, ka nepārtrauktas organizācijas nodokļu un muitas informācijas sistēmu, datu noliktavas un audita atbalsta sistēmu pilnveidošanas rezultātā tiek paaugstināta iekšzemes un starptautiskās tirdzniecības drošības līmenis, atvieglota muitas un nodokļu formalitāšu kārtošana, paātrināta preču aprite pāri Eiropas Savienības robežām un samazinātas organizācijas administratīvās izmaksas. Organizācijas vajadzībām izstrādāto informācijas sistēmu darbības kvalitāte, stabilitāte, integritāte un nepārtraukta pieejamība ir būtisks faktors izvirzīto organizācijas stratēģisko mērķu sasniegšanā un galveno uzdevumu veiksmīgā izpildē.

Organizācijā ir izstrādāti un apstiprināti informācijas sistēmas drošības noteikumi un normatīvajos aktos noteiktajām valsts informācijas sistēmām un personas datu apstrādes sistēmām ir veikta risku analīze informāciju sistēmu nepieejamības ietekmei uz biznesa procesiem. Risku analīzes rezultātā ir noskaidrots, ka kritiskākās organizācijas informācijas sistēmas darbības atjaunošanai jābūt veiktai 1 stundas laikā, lai būtiski neietekmētu organizācijas „N" spēju veikt likumos noteikto funkciju izpildi.

Organizācijā ir izstrādāti kritisko informācijas sistēmu nepārtrauktas darbības nodrošināšanas plāni, kuros ir noteikti organizatorisko un tehnisko pasākumu kompleksi preventīvu pasākumu veikšanai, lai, iespēju robežās, izvairītos no cilvēciska faktora izraisītām informācijas sistēmu nepieejamībām, un konkrētas darbinieku lomas un rīcība, incidentu gadījumos.

Autors secināja, ka organizācijas informācijas sistēmu darbināšanā, drošībā un pieejamībā būtisks faktors ir nepārtraukta un kvalitatīva organizācijas „N" datu centra darbība.

Organizācijas „N" esošā datu centra infrastruktūras iekārtu un topoloģijas raksturojums:

- izvietotās datortehnikas iekārtas kopā patērē aptuveni 60kW. Datortehnika ir aprīkota ar dubultu strāvas pieslēgumu (N+1);
- ierīkots primārais strāvas avots ar 120kW jaudu un alternatīvais – ar 50kW jaudu. Strāvas avotu sadales tīkli nenodrošina to darbu paralēlā režīmā;
- izvietots viens novecojis UPS ar 25kW jaudu un viens jauns UPS ar 50kW jaudu. Jaudīgākais UPS nodrošina rezervējamības prasības – 2 UPS vadības bloki (N+1 slēgumā), kas nodrošina rezervētu jaudas kapacitāti (N 100%);
- ierīkots viens strāvas ģenerators ar 120kW jaudu, kas automatizētā režīmā nodrošina datu centra infrastruktūru ar elektroenerģiju, ilgstošas strāvas padeves traucējumu gadījumā;
- izvietotas gaisa dzesēšanas iekārtu stacionārās vienības, kas kopā nodrošina 45-50kW dzesēšanas jaudu. Dzesēšanas iekārtas nenodrošina rezervējamības prasības;
- nav ierīkota sensoru sistēma datu centra mikroklimata vai iekārtu darbības parametru uzraudzībai un preventīvai problēmu konstatēšanai;
- ierīkota signalizācijas sistēma, bet nav automatizēta ugunsgrēka dzēšanas sistēma;
- nodrošināta bruņota apsardze un pieejas kontroles sistēma (24).

Autors konstatē, ka esošās organizācijas vajadzības tiek nodrošinātas pietiekošā līmenī, bet problēmas var rasties nākotnē, ņemot vērā organizācijas informācijas sistēmu straujo attīstību un organizācijas prasībām pret jaunu informācijas sistēmu izveidi.

Analizējot anketēšanā un intervijās iegūto informāciju, autors konstatēja, ka esošais organizācijas datu centrs ir izvietots pielāgotās telpās un tuvākajā nākotnē organizācijai var rasties problēmas ar jaunās datortehnikas izvietošanu, jo esošās ēkas konstrukcijas tika projektētas atbilstoši dzīvojamā fonda vai biroju būvnormatīvu prasībām. Datu centrā izvietotajai datortehnikai un mikroklimata sistēmai tuvākajā nākotnē var arī nepietikt ar pašreizējās elektroapgādes sistēmas nodrošinātās jaudas kapacitāti.

Organizācijas vadības un darbinieki nepietiekami novērtē nepieciešamību pēc datu centra kritisko mezglu automatizētas un attālinātas pārraudzības, vizuālās uzraudzības un fiziskās apsardzes nepieciešamību, kas pēc autora uzskatiem ir viens no normatīvo aktu izvirzītajām prasībām pret valsts informācijas sistēmu un personas datu apstrādes sistēmu fizisko drošību.

Nākošajā nodaļā autors klasificēs datu centra nepārtrauktas darbības līmeņus un analizēs organizācijas „N" datu centra darbības kvalitātes atbilstību standarta klasifikācijas līmeņiem

3. Datu centru darbības kvalitātes līmeņu klasifikācija

Par spīti pastāvošai dzīvības formu komplicētībai un dažādībai, visi dzīvie organismi sastāv no pamata blokiem vai fundamentālās dzīvo organismu pamatvienības – šūnas. Kopīgi darbojoties uz bioloģiskās eksistences pamata, šīs mazās vienības pilda savu uzdevumu standartizētas struktūras, kurai tā pieder, kopumā.

Līdzīgi, informācijas sistēmu arhitektūra izmanto pamata blokus vai ekspluatācijas vidi, lai radītu, sagatavotu un pārveidotu organizācijas biznesa procesiem nepieciešamo informāciju. Šādus principus ir pārņēmusi arī datu centru nepārtrauktas darbības nodrošināšanas un optimizācijas koncepcija – standartizēta un pārvaldīta ekspluatācijas vide (25).

3.1. Datu centra infrastruktūras komponentes

Datu centrs ir viss nepieciešamais infrastruktūras tehnoloģiskais aprīkojums, palīgtelpas un serveru telpa, kurās izvietota organizācijas informācijas sistēmu uzturošā datortehnika un infrastruktūras komponentes, lai nodrošinātu nepārtrauktu datortehnikas darbināšanu saskaņā ar darba pirmajā nodaļā autora analizēto normatīvo aktu un ražotāju noteiktajiem datortehnikas ekspluatācijas noteikumu prasībām (26).

Saskaņā ar normatīvo aktu prasībām, organizācijas „N" datu centra galvenais uzdevums ir nodrošināt drošu, stabilu un garantētu informācijas sistēmām nepieciešamo resursu nepārtrauktu pieejamību. Tas var tikt nodrošināts ar sekojošu pasākumu kopumu:

- **garantētu (stabilu un nepārtrauktu) strāvas apgādi** ar nepārtrauktas barošanas avotu (UPS) sistēmu, kas nodrošina elektrosistēmas darbību īslaicīgu elektrotīkla darbības traucējumu laikā, un ar dīzeļģeneratoru sistēmu, kas nodrošina elektrību ilgstošu bojājumu gadījumā, palīdzību;
- **garantētus mikoklimatiskos apstākļus,** atbilstoši datortehnikas ražotāju noteiktajiem ekspluatācijas noteikumiem (temperatūras un mitruma režīms),
- **fizisko apdraudējumu novēršana** pret datu centra darbību uzturošo servisa iekārtu un izvietotās datortehnikas iekārtu stabilu un nepārtrauktu darbību ar automatizētu rīku palīdzību:

- **integrēta pārraudzības sistēma**, kuras uzdevums ir nepārtraukti pārraudzīt dažādo datu centra komponenšu darbību un savlaicīgi () brīdināt apkalpojošo personālu par iespējamām

Ideālais datu centra topoloģijas modelis sastāv no sekojošiem blokiem, jeb komponentēm (26, 27, 28):

- centralizēta strāvas apgādes sistēmas infrastruktūra, kas sastāva no:
  - UPS un akumulatoru sistēmas;
  - strāvas sadales sistēmas (PDU);
  - strāvas ģeneratoru sistēmas;
  - kabeļu vadotnes (*cable pathway*),
- centralizēta mikroklimata sistēmas infrastruktūra, kas sastāv no:
  - gaisa dzesēšanas iekārtu sistēmas;
  - augstā gaisa izplatīšanas sistēmas (*cooling distribution*);
  - gaisa filtrēšanas iekārtas;
  - paceltās grīdas (*raised flooring*),
- centralizēta drošības sistēma, kas sastāv no:
  - automatizētā durvju atvēršanas/aizvēršanas mehānisma;
  - pieejas kontroles sistēmas;
  - video novērošanas sistēmas,
- centralizēta ugunsdzēsības sistēma, kas sastāv no:
  - signalizācijas sistēmas;
  - preventīvās izsmidzināšanas sistēmas (*pre-action sprinkler systems*);
  - uguns slāpēšanas sistēmas;
  - kondensāta un ūdens izvadīšanas sistēmas,
- centralizēta pārraudzības sistēma, kas sastāv no:
  - patērētās strāvas jaudas sensoru sistēmas;
  - mikroklimata sensoru sistēmas;
  - kabeļu pārvaldības (*cable management*),
- tehniskais aprīkojums:
  - statnes, skapji, KVM un piederumi (*racks, cabinets & accessories*);
  - tehniskās iekārtas (*NOC, Console & Technical Furniture*);
  - standartizēta kabeļu sistēma (*structured cabling*).

Nākošajā apakšnodaļā autors apskatīs standarta TIA-942 izvirzītās prasības definētajām četriem datu centru pieejamības klasifikācijas līmeņiem.

3.2. Standarta TIA-942 apraksts

Ņemot vērā straujo informācijas sistēmu, telekomunikāciju un datortehnikas attīstību, Telekomunikācijas Nozares asociācija (*Telecommunication Industry Association*) 2005.gada aprīlī publicēja standartu TIA-942 *Datu centru komunikāciju infrastruktūras standarts* (*Telecommunication Infrastructure Standards for Data Center*). Standarts TIA-942, balstoties uz *The Uptime* institūta publicēto dokumentu TUI-705C *Datu centru infrastruktūras līmeņi* (*Tier Classifications Define Site Infrastructure Performance*) (29), nosaka četrus galvenos datu centru raksturojošos pieejamības līmeņus (30), kuri arī tiks apskatīti šajā apakšnodaļā.

3.2.1 Ieskats standarta izveides vēsturē

Pēdējo četrdesmit gadu laikā, datu centru infrastruktūras projekti attīstījās četros posmos. Vēsturiski, pirmais *(Tier I)* datu centra infrastruktūras līmenis tika definēts pagājušā gadsimta 60 gadu sākumā, otrais *(Tier II)* līmenis – 1970, trešais *(Tier III)* līmenis – pagājušā gadsimta 80 gadu beigās un 90 gadu sākumā, bet ceturtais *(Tier IV)* – 1994.gadā.

The Uptime Institute standarta ceturtā līmeņa prasībās noteica, ka datu centra infrastruktūrai jānodrošina vismaz divu pilnīgi neatkarīgu elektropadeves sistēmu vienlaicīgu darbību, jo nozares vadošo institūtu pētījumi par elektroapgādes problēmas ietekmi uz datu centra kopējo pieejamību ir pierādījuši, ka visbiežāk elektroapgādes incidenti rodas tieši posmā no UPS sistēmām līdz datortehnikas iekārtai. Tādējādi, datu centra dublējošai elektrības padeves sistēmai ir jānodrošina tiešā strāvas padeve datortehnikas iekārtām, kuru barošanas bloki strādā savstarpējā slodzes līdzsvarošanas režīmā un spēj aizvietot viens otru problēmu gadījumos.

No 1994.gada pasaules tirgū kļuva pieejama ar dubultu strāvas pieslēgumu aprīkota datortehnika un guva strauju popularitāti. Jaunās tehnoloģija ļāva efektīvi pārvietot datu centru elektrības avotu dublēšanu no UPS sistēmām uz pašām datortehnikas iekārtām. Tāpēc ar duālās barošanas avotiem aprīkoti serveri tandēmā ar ceturtajam līmenim atbilstošu datu centra strāvas padeves infrastruktūru, spēj sniegt visaugstāko iespējamo drošības pakāpi informācijas sistēmu nepārtrauktā pieejamībā (31).

3.2.2 Standartā pielietotie termini

Šajā apakšnodaļā darba autors aprakstīs standartā pielietoto terminu skaidrojumu.

Datortehnikas iekārta (*computer equipment*) – termins ietver plašu nepieciešamo informācijas tehnoloģiju aprīkojumu klāstu datu centra darbības uzturēšanai. Tas ietver sevī serverus, disku masīvus, komunikāciju tīklus u.c. informācijas tehnoloģijas komponentes.

Rezerves jaudas komponentes (*redundant capacity components*) ir visas tās komponentes, kuru skaits pārsniedz iekārtas darbībai nepieciešamo komponenšu skaitu. Gadījumā, ja kāda no datortehnikas iekārtas komponentēm tiek bojāta, tad to darbību automātiski pārņem kāda no atbilstošajām rezerves komponentēm. Šajā sakarā termini „N+1" vai „N+2" ir pielietojami, lai raksturotu esošo rezerves komponenšu skaitu.

Lietojamās jaudas kapacitāte (*usable capacity*) ir maksimāli pieļaujamā slodze, kas var tikt izmatota N-tajam līmenim bez rezerves jaudas komponentēm. Parasti N-tajā līmenī papildus ņemt vērā faktorus, kas saistīti ar datortehnikas iekārtu novecošanu un iekārtas komponenšu kļūdām, lai, neskatoties uz tām, nodrošinātu iekārtas darbības nepārtrauktību.

Infrastruktūra (*site infrastructure*) – tā sevī ietver datu centra centrālo strāvas padevi un serveru telpā izvietotā aprīkojuma un dzesēšanas iekārtu strāvas apgādi. Parasti datu centrs ietver sevī vismaz 20 dažādas sistēmas, kā piemēru var minēt, mehāniskās, elektriskās, ugunsdrošības, aizsardzības u.tml. Katra no minētajām sistēmām var sastāvēt no apakšsistēmām un papildus komponentēm.

Nepārtraukta darbība (*fault tolerance*) nozīmē, ka datu centra strāvas apgādes sistēma spēj nodrošināt nepārtrauktu darbību pat ārkārtas situācijās. Šim risinājumam ir nepieciešami vairāki strāvas avoti un vairāki sadales tīkli. Gadījumā, ja kāds no avotiem vai sadales tīkliem tiek bojāts, tas neietekmē normālu iekārtu apgādi ar elektrību, nodrošinot ierasto darba režīmu. Tas ietver sevī arī prasību pēc datortehnikas aprīkošanu ar dubultu strāvas pieslēgumu.

Paralēlais apkalpes serviss (*concurrent maintainability*) nozīmē, ka jebkurš tehniskās apkalpes darbs var tikt veikts neizslēdzot iekārtas. Informācijas tehnoloģiju jomā šis termins nozīmē, ka jebkura no jaudas komponentēm vai jebkurš sadales tīkla elements var tikt labots, apmainīts, testēts u.tml., bez jebkādas ietekmes uz iekārtu nepārtrauktu darbību.

3.2.3 Standartā definētie datu centru pieejamības līmeņi

Pirmais līmenis: Pamata infrastruktūra

Raksturojums:

- datu centram nav rezervējamības pakāpe. Iekārtu kritiskie mezgli netiek dublēti un netiek nodrošinātas jaudas rezervējamības prasības. Iekārtas apkalpo tikai viens strāvas avots (skat. 2.pielikumu).

Pieejamības standartatbilstības tests:

- jebkura infrastruktūras mezgla vai strāvas avota bojājums tieši ietekmē iekārtu pieejamību.

Ietekme uz ekspluatācijas procesiem:

- infrastruktūras darbības pārtraukums ir nepieciešams gan plānotu aktivitāšu veikšanai, gan neplānotu situāciju novēršanai;
- infrastruktūras pilnīga izslēgšana ir nepieciešama plānoto tehnisko apkopju un iekārtu mezglu nomaiņas laikā. Ārkārtas situācijās iespējamas vairākkārtīgi infrastruktūras darbības pārtraukumi. Regulāra tehnisko apkopju neveikšana krasi palielina neprognozējamu datu centra infrastruktūras darbības traucējumu risku, kas var izraisīt pilnīgu datu centra nepieejamību;
- ekspluatācijas gaitā pieļautās kļūdas vai spontāni infrastruktūras iekārtu bojājumi var izraisīt datu centra nepieejamību.

Otrais līmenis: Infrastruktūras rezervējamība

Raksturojums:

- datu centra infrastruktūrai piemīt rezervējamības pakāpe. Iekārtu kritiskie mezgli tiek dublēti, nodrošinot jaudas rezervējamības prasības. Infrastruktūru apkalpo tikai viens strāvas avots (skat. 3.pielikumu);

Pieejamības standartatbilstības tests:

- kritiskā datu centra mezgla bojājumi var iespaidot datu centra pieejamību;
- strāvas apgādes tīkla kļūda izraisa datu centra nepieejamību.

Ietekme uz ekspluatācijas procesiem:

- infrastruktūras nepārtraukta darbība ir atkarīga no traucējumiem gan plānotu aktivitāšu, gan neplānotu incidentu gadījumos;
- ir nepieciešams uzstādīt papildus UPS un rezerves strāvas apgādes ģeneratorus;
- ir jāparedz infrastruktūrai pilnīga izslēgšana ne retāk kā reizi gadā, lai veiktu ikgadēju plānotās apkopes un labošanas darbus. Incidenti var izraisīt arī biežāku sistēmu izslēgšanas nepieciešamību. Gadījumā, ja netiek ievērotas regulārās apkopes prasības, paaugstināts infrastruktūras neplānotu pārtraukuma iestāšanās risks un sistēmas darbības traucējumu izraisīto seku smaguma pakāpe;
- kritisko mezglu darbības kļūdas vai spontāni darbības traucējumi var izsaukt datu centra nepieejamību.

Trešais līmenis: Paralēlās apkalpojamības infrastruktūras serviss

Raksturojums:

- datu centra iekārtu kritiskie mezgli tiek dublēti un iekārtas apkalpo vairāki neatkarīgi komunikāciju sadales tīkli, taču tikai viens no sadales tīkliem vienlaicīgi apkalpo iekārtas (skat. 4.pielikumu).

Pieejamības standartatbilstības tests:

- jebkurai no kritiskā mezgla komponentēm un jebkuram sadales tīkla elementam var tikt veikta plānota tehniskā apkope. Apkopes gaitā uz laiku var tikt izslēgtas komponentes vai elementi, taču tas neietekmē kopējo datu centra infrastruktūras pieejamību.

Ietekme uz ekspluatācijas procesiem:

- tikai neplānotas aktivitātes var ietekmēt datu centra infrastruktūras nepārtrauktu darbību;
- datu centra infrastruktūras plānota apkope tiek veikta, izmantojot kritisko mezglu un alternatīvo komunikāciju sadales tīklu rezervējamību, proti, izmantojot esošo rezerves infrastruktūru;
- lai nodrošinātu vienlaicīgu uzturamību strāvas padeves posmā starp UPS un datortehniku, visai informācijas sistēmu uzturošajai datortehnikai jābūt aprīkotai ar dubultu strāvas pieslēgumu (rezerves barošanas bloki slēgumā N+1);
- datu centra darbības pārtraukuma risks paaugstinās plānoto tehnisko apkopju laikā;

- ekspluatācijas kļūdas vai spontānas kļūmes sadales tīklos var izraisīt datu centra darbības traucējumus.

Ceturtais līmenis: Augsta pieejamības infrastruktūra

Raksturojums:

- augstas pieejamības datu centram ir vairākas rezervējamas kapacitātes kritisko mezglu sistēmas un vairāki neatkarīgi un vienlaicīgi aktīvi sadales tīkli, kuri apkalpo datortehnikas iekārtas;
- visas IT iekārtas ir aprīkotas ar dubultu strāvas pieslēgumu barošanas blokiem, lai atbilstu datu centra infrastruktūras topoloģijai un arhitektūrai (skat. 5.pielikumu).

Pieejamības standartatbilstības tests:

- jebkuras vienas sistēmas kapacitātes komponentes bojājumu gadījumā, neietekmē kopējo infrastruktūras darbību;
- jebkuras sistēmas komponentes un sadales tīkla elementi var tikt izslēgti tehnisko apkopju laikā bez ietekmes uz datortehnikas iekārtu darbību;
- lai nodrošinātu augstu pieejamību un paralēlu apkopi, neizslēdzot sistēmas, visai datortehnikai ir jābūt nodrošinātai ar dubultu strāvas apgādi;
- lai nodrošinātu datu centra augstu pieejamību un vienlaicīgu uzturamību strāvas padeves posmā starp UPS un datortehniku, visai informācijas sistēmu uzturošajai datortehnikai jābūt aprīkotai ar dubultu strāvas pieslēgumu (rezerves barošanas bloki slēgumā N+1);
- papildus minētajām prasībām, sistēmām un sadales tīkliem fiziski ir jāatrodas nošķirtās vietās, lai novērtu vienlaicīgu ārējo fizikālo faktoru izraisītu bojājumu iespējamību.

Ietekme uz ekspluatācijas procesiem:

- datu centra pieejamību neietekmē jebkura viena kritiskā mezgla ārkārtas bojājums;
- datu centru pieejamību neietekmē jebkuras plānoto apkopju aktivitātes;
- datu centra infrastruktūras plānota apkope tiek veikta, izmantojot kritisko mezglu un alternatīvo komunikāciju sadales tīklu rezervējamību, proti, izmantojot esošo rezerves infrastruktūru
- datu centra darbības pārtraukuma risks var būt paaugstināts plānoto tehnisko apkopju laikā un ārkārtas specifiskos gadījumos, piemēram, ugunsgrēks;

- ugunsgrēka trauksmes, ugunsgrēka dzēšanas laikā vai ārkārtas strāvas padeves atslēgšana var izsaukt datu centra darbības traucējumus.

3.2.4 Datu centra pieejamības līmeņu salīdzinājums

Darba autors veiks standarta piedāvāto datu centru pieejamības līmeņu salīdzinājumu (skat. 3.1.tabulu) un analīzi, kā piemēros minēs, kādos gadījumos organizācijas vai uzņēmumi izvēlas atbilstošo datu centru pieejamības līmeni.

Parasti pirmā līmeņa datu centru risinājumu izvēlas uzņēmumu vadītāji, kas sāk apzināties nepieciešamību uzlabot savas informācijas sistēmas uzturošās datortehnikas drošību un mikroklimatu, kuru nav iespējams nodrošināt publiski pieejamās biroja telpās. Minētā līmeņa risinājums, atšķirībā no biroja telpu aprīkojuma, nodrošina:

- izdalītas un ierobežotas pieejamības telpas datortehnikas izvietošanai;
- nepārtrauktas strāvas avotu (UPS), kas pasargā iekārtas no elektrotīkla strāvas pārslodzēm, kritumiem un īslaicīgiem pārtraukumiem;
- lokālu gaisa kondicionieri, telpas mikroklimata normalizēšanai;
- strāvas ģeneratoru, lai nodrošinātu iekārtu darbību ilgstošas elektroapgādes traucējumu gadījumos.

Šī līmeņa datu centra risinājumu parasti izvēlas un tas ir pietiekošs mazām un jaunām firmām un uzņēmumiem, kuru prasības pret informācijas sistēmu pieejamību ir nelielas – pieļaujams iekārtas izslēgt ārpus darba laika.

Otrais datu centra pieejamības līmenis papildina pirmā līmeņa prasības ar infrastruktūras kritisko mezglu jaudas un dzesēšanas iekārtu rezervējamības komponentēm, lai palielinātu informācijas sistēmu iekārtu drošību infrastruktūras aprīkojuma bojājumu gadījumos. Rezervējamības komponentes parasti ir papildus UPS vadības un akumulatoru moduļi, papildus dzesēšanas iekārtas, strāvas ģeneratori, u.tml. Minētās komponentes paaugstina datu centra iekārtu drošību, jo rezervējamības zaudēšanas gadījumā (piemēram, kādā no UPS moduļiem rodas darbības traucējumi) iekārtas funkcionalitāte saglabājas vai tikai daļēji tiek traucēta.

Otrā līmeņa datu centra risinājumu parasti izvēlas valsts vai izglītības iestādes, jo to pakalpojumu procesi vai funkciju sniegšana tiešā veidā neietekmē datu centra vai informācijas sistēmas nepieejamība. Minēto līmeni var izmantot arī organizācijas un uzņēmumi, kuru informācijas sistēmas (piemēram, finanšu vadības un grāmatvedības uzskaite, dažādas

uzskaites sistēmas u.tml.) nodrošina tikai iestādes iekšējos procesus, kuri pieļauj plānotās tehniskās apkopes veikt arī darba laikā. Parasti šādiem uzņēmumiem vai organizācijām nav noteikta reālā laika (*on-line*) pakalpojumu nodrošināšana klientiem un datu centra nepieejamības gadījumi nerada tiešus vai netiešus finansiāla rakstura zaudējumus.

Uzņēmumi, kas izvēlas pirmo vai otro datu centra pieejamības līmeni, parasti meklē īstermiņa risinājumus, lai nodrošinātu esošo informācijas tehnoloģiju darbību. Gan pirmais, gan otrais līmenis ir tikai taktiskie risinājumi, kuri pamatā tiek izvēlēti pateicoties to lētākām sākotnējam izmaksām. Šādos gadījumos netiek ņemti vērā datu centra ilgtermiņa darbība un nepārtrauktas pieejamības nodrošināšanas slēptās izmaksas, kas uzturēšanā var pārsniegt sākotnējās datu centra ierīkošanas izmaksas.

Trešā datu centru pieejamības līmeņa prasības papildina pirmā un otrā līmeņa prasības pret tehnoloģijām, lai būtu iespējams veikt paralēlās apkalpojamības infrastruktūras servisa apkopes. Tas nozīmē, ka jebkura infrastruktūras kritiskā mezgla komponentei jābūt nomaināmai bez nozīmīga datu centra darbības traucējuma. Tas tiek panākts ar datu centra infrastruktūras kritisko mezglu komponenšu dublēšanu, tajā skaitā arī dzesēšanas iekārtām, un iekārtas apkalpo vairāki neatkarīgi komunikāciju sadales tīkli, taču tikai viens no sadales tīkliem vienlaicīgi apkalpo iekārtas. Tādējādi tiek panākts, ka regulārā infrastruktūras apkope ļauj modernizēt vai plānoti nomainīt infrastruktūras komponentes, tā palielinot kopējo sistēmu drošību un datu centra darbības nepārtrauktības paredzamību.

Trešā līmeņa datu centra risinājumu parasti izvēlas kompānijas, kuras sniedz pakalpojumus nepārtrauktā diennakts režīmā visu gadu iekšējiem un ārējiem klientiem, kā piemēram, servisu centri, diennakts palīdzības dienesti u.c. Šeit var minēt arī tās kompānijas, kuru filiāles atrodas atšķirīgās laika zonās un kompāniju darbinieki apkalpo dažādus reģionus un kuru informācijas tehnoloģiju resursi atbalsta automatizētus biznesa procesus. Parasti minētie uzņēmumi un to klienti var atļauties datu centra servisa īslaicīgus darbības pārtraukumus, kuros informācijas sistēmu pieejamība var tikt ierobežota.

Informācijas drošības aspektu un investīciju aizsardzības dēļ trešā līmeņa vai augstāka datu centra risinājumus izvēlas arī lielas valsts organizācijas vai kompānijas, kuras informācijas sistēmu uzturošajās tehnoloģiskajos risinājumos ir investējušās lielus finanšu līdzekļus. Parasti organizācijām un to izmantotajiem tehnoloģiskajiem risinājumiem ir izvirzītas augstas prasības pret datu centru drošu un nepārtrauktu darbību. Šādas iestādes vadības var akceptēt traucējumu risku no neparedzētiem notikumiem. Dažkārt šīs kompānijas izvēlas sākotnēji izveidot trešā līmeņa datu centrus, lai nākotnē varētu tos modernizējot nodrošināt atbilstību ceturtajam līmenim.

3.1.tabula

Datu centra pieejamības līmeņu definētās prasības*

Līmeņa vajadzības	1.līmenis	2.līmenis	3.līmenis	4.līmenis
Strāvas avots	1	1	1	1+1
Rezervējamība	N	1+1	N+1	vismaz N+1
Lietojamās jaudas kapacitāte	100% N	100% N	90% N	90% N
Sadales tīkli	1	1	1 aktīvs un 2 rezerves	2 paralēli strādājoši
Neatkarīgi avoti	-	-	-	X
Paralēlais apkalpes serviss	-	-	X	X
Augsta pieejamība	-	-	-	X
Telpu statuss	Biroja telpas	Pielāgotas	Pielāgotas vai projektētas	Projektētas
Personāls	-	1 maiņa (darba dienās)	2 maiņas (24x7)	3 maiņas (24x 365)
Nepieejamības riski	Daudz + cilvēka faktora kļūdas	Daudz + cilvēka faktora kļūdas	Dažas + cilvēka faktora kļūdas	Neviena + ugunsgrēks
Līmeni raksturojoša pieejamība	99,67%	99,75%	99,98%	99,99%

*Autora izveidotā tabula, apkopojot 3.2.3.apakšnodaļā definētās datu centru līmeņu prasības

Ceturtā datu centru pieejamības līmeņa prasības ir bāzētas uz trešā līmeņa prasībām, papildus izvirzot prasības infrastruktūras noturībai pret kritisko mezglu bojājumiem, ieviešot vairākus neatkarīgus un vienlaicīgi aktīvus strāvas avotus un sadales tīklus, kas paralēli apkalpo datortehnikas iekārtas. Paralēlā apkalpojamība tiek attiecināta pilnīgi uz visām infrastruktūras daļām un komponentēm. Minētais līmenis paredz, ka jebkura no

infrastruktūras komponentēm vai sadales tīklu elementiem var kļūt nepieejami jebkurā laika vienībā, neatstājot iespaidu uz datu centra infrastruktūras kopējo funkcionalitāti.

Ceturto līmeni izvēlas organizācijas, kuras ir identificējušas lielus finansiālus zaudējumus, ja datu centram ir novērojami spontāni darbības traucējumi. Šāda līmeņa datu centrs attaisno savas izmaksas valsts organizācijām vai internacionālām institūcijām vai kompānijām, kurām jānodrošina informācijas sistēmu servisa pakalpojums režīmā 24 stundas 7 dienas nedēļā un 365 dienas gadā vai augsta informācijas drošība un pieejamība. Kompānijas, kuru bizness ir balstīts uz starptautisko elektronisko tirgu un finanšu apkalpes procesiem, darbojas augstas konkurences apstākļos, datu centru pieejamība ir būtisks konkurent spējas faktors. Tāpēc tās ir motivētas veikt investīcijas augstas pieejamības datu centrā.

Nākošajā apakšnodaļā autors noteiks organizācijas „N" datu centra infrastruktūras atbilstību standartā klasificētajiem datu centra pieejamības līmeņiem.

3.3. Organizācijas „N" prasībām nepieciešamā datu centra darbības kvalitāte atbilstoši standarta noteiktajai klasifikācijai

Ņemot vērā darba pirmajā nodaļā izvirzītās valsts normatīvo aktu prasības un otrajā nodaļā organizācijas „N" izvirzītās prasības pret informācijas sistēmu pieejamību, autors konstatē, ka organizācijas „N" datu centra infrastruktūrai **jāatbilst standarta 3.līmenim**, lai nodrošinātu organizācijai atbilstošu darbības kvalitāti.

Autors konstatēja, ka organizācijas „N" datu centra infrastruktūras topoloģija **atbilst standarta 1.līmenim** (skat. 3.2.tabulu un 2.pielikumu), jo:

- strāvas avoti nenodrošina rezervējamību vai to darbu paralēlā režīmā;
- esošie UPS nenodrošina rezervējamību un strāvas avotam atbilstošu jaudas kapacitāti;
- ierīkots viens strāvas ģenerators;
- nav centralizētas gaisa dzesēšanas iekārtas sistēmas. Stacionārās nenodrošina rezervējamības prasības, kā arī visas kopā – jaudas kapacitātes prasības;
- datu centrā izvietotās datortehnikas ir aprīkota ar dubultu strāvas pieslēgumu (N+1).

Autora bakalaura darba pētījuma **hipotēze ir pierādīta**.

3.2.tabula

Organizācijas „N" datu centra komponenšu atbilstība standarta prasībām*

Komponentes	N+1	Rezervējamība	Jaudas kapacitāte**	Neatkarīgi avoti
Strāvas avots	Daļēji	Nav	Neatbilst (50kW/120kW)	Nav
Datortehnika	Atbilst	Atbilst	Atbilst (120kW/60kW)	-
UPS un akumulatoru sistēma	Neatbilst	Daļēji***	Neatbilst (50kW/120kW)	Nav
strāvas ģenerators	Neatbilst	Nav	Atbilst (120kW/120kW)	Nav
gaisa dzesēšanas sistēma	Neatbilst****	Nav	Neatbilst (50kW/120kW)	Nav

* autora izveidotā tabula, apkopojot 3.2.3.apakšnodaļā definētās datu centru līmeņu prasības.

** iekavās: iekārtas vai avota nodrošinātā jauda/nepieciešamā jauda.

*** jaunais UPS nodrošina rezervējamību līdz 50kW.

**** gaisa dzesēšanai tiek izmantotas neatkarīgas stacionārās iekārtas.

Lai organizācijas datu centrs atbilstu 3.līmeņa prasībām, ir jāveic sekojošs esošā datu centra modernizācijas pasākumu komplekss:

1) alternatīvā strāvas avota jauda jāpalielina līdz 120kW;
2) esošā UPS akumulatoru jauda jāpalielina līdz 120kW;
3) jāuzstāda neatkarīgs 120kW UPS (N+1 slēgumā ar esošo);
4) jāuzstāda rezerves 120kW strāvas ģenerators (N+1 slēgumā ar esošo);
5) jāuzstāda divas neatkarīgas gaisa dzesēšanas sistēmas (N+1 slēgumā) ar 100kW dzesēšanas jaudu ;
6) jāpārkārto serveru statņu izvietojums, atbilstoši jaunās dzesēšanas sistēmas prasībām;
7) jāuzstāda centralizēta pārraudzības sistēma, kas pārraudzītu ekspluatācijas vides mikroklimata un strāvas patēriņa izmaiņas.

Secinājumi un priekšlikumi

Pētījuma gaitā, izstrādājot bakalaura darbu, autors ir nonācis pie **secinājumiem**.

1. Latvijā informācijas sistēmu drošības prasības reglamentē *Valsts informācijas sistēmu likums, Fizisko personu datu aizsardzības likums* un uz šo likumu pamata izdotie MK noteikumi.

2. MK noteikumu Nr.40 izvirzītās prasības korelē ar MK noteikumu Nr.764 un Nr.765 prasībām. Tas varētu būt saistīts ar to, ka MK noteikumi Nr.40 ir vispārīgāki un izstrādāti piecus gadus pirms MK noteikumu Nr.764 un Nr.765 apstiprināšanas, bet pēc būtības šie noteikumi viens otru tikai papildina.

3. Valsts informācijas sistēmas statuss tiek piešķirts informācijas sistēmām, kuras lietojot, tiek nodrošināta informācijas aprite normatīvajos aktos un Latvijai saistošos starptautiskajos līgumos noteikto funkciju izpildei.

4. Personas datu apstrādes sistēmas statuss tiek piešķirts informācijas sistēmām, kurās tiek veiktas jebkādas darbības ar personas datiem un jebkādā formā tiek uzturēta fiksēta strukturizēta personas datu kopa.

5. Valsts ir uzlikusi konkrētu atbildību, pienākumus un ierobežojumus informācijas sistēmu īpašniekiem, kuru pienākums ir veikt valsts informācijas sistēmās un/vai personas datu apstrādes informācijas sistēmās esošās informācijas loģisko un fizisko aizsardzību. Šāda mērķa sasniegšanai jāveic noteiktu tiesisko, organizatorisko un tehnisko pasākumu komplekss, ko apzīmē kā informācijas sistēmas drošības politika, kurai jāiekļaujas attiecīgās iestādes kopējā drošības politikā.

6. Valsts informācijas sistēmas un/vai datu apstrādes sistēmas turētājs nodrošina un atbild par:

- informācijas valsts sistēmās veikto datu apstrādi;
- datu drošību ar loģiskiem līdzekļiem;
- aizsardzību pret fiziskās iedarbības radītu datu apdraudējumu;
- datu pieejamību no globālā datoru tīkla.

7. Valsts informācijas sistēmas turētājam, lietojot sistēmas tehniskos resursus, jānodrošina resursu izmantošana atbilstoši ražotāja noteiktajām ekspluatācijas vides prasībām.

8. Piešķirtā valsts budžeta iespēju robežās un, ievērojot samērīgumu, organizācijas pienākums ir aprīkot organizācijas datu centru ar visu nepieciešamo, lai nodrošinātu normatīvo aktu, tajā skaitā, ražotāju izvirzītās prasības.

9. Informācijas sistēmas turētāja pienākums ir izstrādāt un ar iekšējiem normatīviem aktiem nostiprināt informācijas sistēmas drošības noteikumus, kuri reglamentē informācijas

sistēmas informācijas un tehnisko resursu pasākumu kompleksu realizāciju un pārvaldi organizācijā.

10. Katram jaunam ar informācijas resursiem un tehniskajiem resursiem saistītam projektam jāveic riska analīze, lai noteiktu draudu cēloņus, veiktu seku analīzi un nepieciešamos loģiskās un fiziskās aizsardzības pasākumus.

11. Normatīvie akti neuzliek par pienākumu organizācijas vadītājam, izstrādājot un ieviešot informācijas sistēmas drošības noteikumus, vadīties no konkrētiem starptautiski atzītiem vai Latvijas republikā apstiprinātiem standartiem.

12. Tas, ka normatīvajos aktos un standartos nav noteiktas atkarības no konkrētiem tehniskiem līdzekļiem un risinājumiem, no vienas puses, nedod skaidru priekšstatu, kā praktiski īstenot tā vai cita informācijas sistēmas elementa aizsardzību, taču, no otras puses, dod brīvību organizācijai izvēlēties informācijas sistēmas tehniskos un informācijas resursus, tomēr šāda rīcības brīvība var radīt draudus informācijas sistēmu drošībai organizācijas vadības un IT speciālistu nekompetences gadījumā, jo valstī nav izstrādātas nepieciešamo minimālo loģiskās un fiziskās drošības prasību vadlīnijas.

13. Organizācijas „N" vajadzībām izstrādāto informācijas sistēmu darbības kvalitāte, stabilitāte, integritāte un nepārtraukta pieejamība ir būtisks faktors izvirzīto organizācijas stratēģisko mērķu sasniegšanā un galveno uzdevumu veiksmīgā izpildē.

14. Organizācijas „N" informācijas sistēmas atbilst valsts informācijas sistēmu un personas datu apstrādes informācijas sistēmu prasībām, un to darbības nodrošināšanas un aizsardzības pasākumu kompleksus pilnā mērā reglamentē normatīvie akti.

15. Organizācijā „N" ir izstrādāti un apstiprināti:

- informācijas sistēmas drošības noteikumi;
- nepārtrauktas darbības nodrošināšanas plāni un
- veikta risku analīze informāciju sistēmu nepieejamības ietekmei uz biznesa procesiem.

16. Organizācijas „N" vajadzības tiek nodrošinātas pietiekošā līmenī, bet problēmas var rasties tuvākajās nākotnē, ņemot vērā organizācijas informācijas sistēmu straujo attīstību un organizācijas prasībām pret jaunu informācijas sistēmu izveidi.

17. Balstoties uz aptaujas rezultātiem var secināt, ka organizācijas „N" vadība un darbinieki nepietiekami novērtē nepieciešamību pēc datu centra kritisko mezglu automatizētas un attālinātas pārraudzības, vizuālās uzraudzības un fiziskās apsardzes nepieciešamību. Vadība ir apstiprinājusi iekšējos normatīvos noteikumus, kas administratīvā kārtā reglamentē darbinieku pienākumus ievērot drošības prasības, bet neievieš automatizētus tehniskos

līdzekļus, kā preventīvu līdzekli. Savukārt, darbiniekiem minēto noteiktumu ievērošana rada papildus birokrātiju un neērtību, kas bieži vien ir par iemeslu drošības prasību neievērošanai.

18. Organizācijas „N" datu centrā izvietotajai datortehnikai un mikroklimata sistēmai tuvākajā nākotnē var arī nepietikt ar pašreizējās elektroapgādes sistēmas nodrošinātās jaudas kapacitāti, jo strāvas avota jauda ir 120kW, datortehnikas šobrīd patērē 60-70kW, savukārt stabilizētā UPS rezervējamības jaudas kapacitāte ir tikai 50kW.

19. Organizācijas „N" izvirzītās prasības pret informācijas sistēmu drošību un pieejamību, atbilstoši risku analīzei, tika definēta 1 stunda, kas **atbilst standarta 3.līmeņa** izvirzītajām prasībām, organizācijas „N" datu centra infrastruktūras topoloģija atbilst tikai **standarta 1.līmenim**, jo:

- strāvas avoti nenodrošina rezervējamību vai to darbu paralēlā režīmā;
- esošais UPS (50kW) nenodrošina rezervējamību un strāvas avotam (120kW) atbilstošu jaudas kapacitāti;
- ir uzstādīts viens avārijas strāvas ģenerators, kas nenodrošina rezervējamības prasības;
- nav centralizētas gaisa dzesēšanas iekārtas sistēmas. Stacionārās nenodrošina rezervējamības prasības, kā arī visas kopā – datortehnikas izdalītā siltuma kompensēšanai nepieciešamās jaudas kapacitātes prasības (ne mazāk kā 70kW).

20. Organizācijas „N" datu centrā izvietotās datortehnikas ir aprīkota ar dubultu strāvas pieslēgumu (N+1) un datortehnikas kritisko mezglu (CPU, RAM u.c.) rezervējamību, kas nākotnē bez papildus ieguldījumiem datortehnikas iekārtu modernizēšanā ļautu palielināt informācijas sistēmas kopējo drošību apvienojumā ar 3.līmenim atbilstīgu datu centra pakalpojuma kvalitāti.

Pamatojoties uz zinātniskajā darbā veikto analīzi un izdarītajiem secinājumiem, autors ir izvirzījis **priekšlikumus**:

1. Organizācijā „N" nepieciešams izstrādāt, apstiprināt un realizēt ilgtermiņa stratēģiju datu centra infrastruktūras izveidei, lai, sasniedzot šodien izvirzītos mērķus, tie būtu vēl aktuāli pēc pieciem vai desmit gadiem.

2. Lai organizācijas „N" datu centrs atbilstu 3.līmeņa prasībām, ir jāveic sekojošs esošā datu centra modernizācijas pasākumu komplekss:

- alternatīvā strāvas avota jauda jāpalielina līdz 120kW;
- esošā UPS akumulatoru jauda jāpalielina līdz 120kW;
- jāuzstāda neatkarīgs 120kW UPS (N+1 slēgumā ar esošo);

- jāuzstāda rezerves 120kW strāvas ģenerators (N+1 slēgumā ar esošo);
- jāuzstāda divas neatkarīgas gaisa dzesēšanas sistēmas (N+1 slēgumā) ar 100kW dzesēšanas jaudu ;
- jāpārkārto serveru statņu izvietojums, atbilstoši jaunās dzesēšanas sistēmas prasībām;
- jāuzstāda centralizēta pārraudzības sistēma, kas pārraudzītu ekspluatācijas vides mikroklimata un strāvas patēriņa izmaiņas.

3. Organizācijas „N" augstākai vadībai ir jāveic aktīvāka vidēja līmeņa vadītāju un darbinieku izglītošana informācijas sistēmu drošības prasību jomā, lai veicinātu organizācijas visu līmeņu darbinieku vienotu izpratni par drošības prasību izpildes nepieciešamību un draudošo disciplināro, administratīvo vai krimināLo atbildību.

4. Autora darbā aprakstītās standarta datu centra darbības kvalitātes noteikšanas vadlīnijas, izmantojot standarta TIA-942 klasifikāciju, ieteicams piemērot arī citu valsts un pašvaldības vai privāto uzņēmumu datu centru nepārtrauktas darbības nodrošināšanas kvalitātes atbilstības noteikšanai.

Pateicības

Vēlos pateikties bakalaura darba vadītājai, dr. sc. eng. Ilgai Karlsonei par izsmeļošu metodisko ieteikumu sniegšanu, organizatorisko un morālo atbalstu bakalaura darba izstrādē. Paldies par laipnību un sapratni!

Autors vēlas pateikties godājamai recenzentei, dr. oec. Inesei Spīčai, par sniegto darba recenziju.

Izmantotās literatūras un avotu saraksts

1. *Valsts informācijas sistēmu likums* [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?mode=DOC&id=62324 .

2. 02.08.2005. MK noteikumi Nr. 572 *Valsts informācijas sistēmu reģistrācijas noteikumi* [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?id=113829&mode=DOC.

3. *Valsts informāciju sistēmu reģistrs* [tiešsaiste]. Pieejams internetā: https://www.visr.eps.gov.lv/visr/.

4. 11.10.2005. MK noteikumi Nr.765 *Valsts informācijas sistēmu vispārējās tehniskās prasības* („LV" 164 (3322), 14.10.2005) [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?mode=DOC&id=118986.

5. 11.10.2005. MK noteikumi Nr.765 *Valsts informācijas sistēmu vispārējās drošības prasības* („LV" 164 (3322), 14.10.2005) [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?mode=DOC&id=118990.

6. *Fizisko personu datu aizsardzības likums* [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?id=4042 .

7. 30.01.2001. MK noteikumi Nr.40 *Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības* [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?id=2697&mode=KDOC.

8. 28.08.2007. MK noteikumi Nr.574 *Grozījumi Ministru kabineta 2001.gada 30.janvāra noteikumos Nr.40 "Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības"* [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?mode=DOC&id=162385.

9. Standarts LVS ISO/IEC 17799:2005 [tiešsaiste]. Pieejams internetā: http://www.praxiom.com/iso-17799-2005.htm.

10. Standarts BSI EN 1047-1:2005 [tiešsaiste]. Pieejams internetā: http://www.bsi-global.com/en/Standards-and-Publications/.

11. Standarts BSI EN 1047-2:2000 [tiešsaiste]. Pieejams internetā: http://www.bsi-global.com/en/Standards-and-Publications/.

12. Standarts BS 7799-2:2002 [tiešsaiste]. Pieejams internetā: http://www.noweco.com/wp_ismse.htm.

13. Starptautiskās Standartizācijas organizācijas mājas lapa [tiešsaiste]. Pieejams internetā: http://www.iso.org

14. Standartu ISO/IEC 2700 saimes mājas lapa [tiešsaiste]. Pieejams internetā: http://www.27000.org/index.htm.

15. *Krimināllikums* [tiešsaiste]. Pieejams internetā: http://www.likumi.lv/doc.php?id=88966&mode=DOC.

16. **Miķelsons Uldis** *Informācijas tehnoloģiju noziegumu izmeklēšanas īpatnības* (ISBN 9984-7286-1-7). Rīga : Biznesa augstskola "Turība", 2003. - 387 lpp.

17. **IBM korporācija** *System i and System pSite Preparation and Physical Planning Guide, Second Edition.* IBM: September 2007 – 120.p.

18. **Autoru kolektīvs, U.Ķiņa juridiskajā redakcijā** *Uzņēmumu drošība* (ISBN 9984766691). Rīga : Biznesa augstskola "Turība", 2006. - 422 lpp.

19. **Jordan E., Silrock L.** *Beating IT Risks*. John Wiley & Sons, Ltd: 2005. – 278 p.

20. Datu valsts inspekcijas mājas lapa [tiešsaiste]. Pieejams internetā: http://www.dvi.gov.lv/fpda/principi/.

21. **Al Rockart** *Eight imperatives for the new IT organization*, Sloan Management: 1996. – 56 p.

22. **Pete Sacco** *Embracing the Expanding Role of IT in Business*. E-žurnāls *Data Center Design*, 12.2007. [tiešsaiste]. Pieejams internetā: http://datacenterdesign.blogspot.com/2007/12/embracing-expanding-role-of-it-in.html.

23. Organizācijas „N" mājas lapā publicētie stratēģiskie mērķi [tiešsaiste]. Pieejams internetā: http://www.vid.gov.lv/default.aspx?tabid=4&id=684&hl=1;

24. Organizācijas „N" nepublicētie materiāli.

25. **Pedro Gómez** *A Route to Standardized Operating Environments/SUN blueprints*, SUN: 2007 – 127 p.

26. **Mauricio Arregoces,Maurizio Portolani** *Data Center Fundamentals*. Cisco systems: 2003 – 306 p..

27. **Rob Snevely** *Enterprise Data Center Design and Methodology/SUN Blueprints.* SUN: 2002 – 189 p.

28. **William Tschudi** Best practices for energy-efficient data centers identified through case studies and demonstration projects. *ASHRAE Transactions*, 2007, vol. 113, p.450 – 457.

29. The Uptime institūta mājas lapa [tiešsaiste]. Pieejams internetā: http://uptimeinstitute.org.

30. *TIA-942 Data Center Standards Overview* [tiešsaiste]. Pieejams internetā: www.adc.com/Library/Literature/102264AE.pdf.

31. **W.Pitt Turner IV, John H.Seader, Kenneth G.Brill** *Tier Classifications Define Site Infrastructure Performance/The Uptime Institute white paper*. The Uptime Institute: 2006 – 17 p.

Pielikumi

1.pielikums

Anketa

Pirms aizpildīt anketu, autors vēlas paskaidrot par anketā bieži pieminētā apzīmējuma *datu centrs* definīciju. Ar *datu centrs* (tajā skaitā *serveru telpa*) tiek saprasts viss nepieciešamais aprīkojums (piemēram, kondicionieri, komutatori, strāvas avoti u.tml.) un telpas, kurās izvietota organizācijas informācijas sistēmu uzturošā datortehnika un infrastruktūra, lai nodrošinātu datortehnikas nepārtrauktu darbināšanu saskaņā ar ražotāju noteiktajiem datortehnikas ekspluatācijas noteikumiem.

Lūgums – atbildēt uz jautājumiem godprātīgi un, ja anketas aizpildīšanas laikā rodas kaut mazākās šaubas par atbildi Jūsu pārstāvētās organizācijas gadījumā, atbildiet negatīvi (noliedzoši).

1. Jūsu izglītība (*šeit un turpmāk atbilstošo jautājuma atbildi pasvītrojiet vai izceliet*):

   ☐ Vidējā ☐ Bakalaurs ☐ Maģistrs

2. Jūsu ieņemamais stāvoklis organizācijā:

   ☐ IT eksperts ☐ Vadība

3. Vai Jūsu organizācijas pamatfunkciju veikšanai ir nepieciešama pieeja pie ārējiem informācijas resursiem, interneta?

   ☐ Jā ☐ Nē

4. Vai Jūsu organizācijas pamatfunkciju vajadzībām ir izstrādāta(as) informācijas sistēma(as) (*Ja uz 4.jautājumu atbildēts noliedzoši, uz 5. un 6.jautājumu nav jāatbild.*)?

   ☐ Jā ☐ Nē

5. Vai Jūsu organizācijas uzturētā(ās) informācijas sistēma(as) ir reģistrētas Datu valsts inspekcijā?

   ☐ Jā ☐ Nē ☐ Nezinu

6. Vai Jūsu organizācijas uzturētajai(ām) informācijas sistēmai(ām) ir piešķirts valsts informācijas sistēmas statuss?

   ☐ Jā ☐ Nē ☐ Nezinu

7. Vai Jūsu organizācijā ir veikta informācijas sistēmas(u) un ārējo informācijas resursu pieejamības riska analīze, lai noteiktu ietekmi uz organizācijas spēju nodrošināt pamatfunkciju izpildi datu centra nepieejamības gadījumā? (*Ja uz 7.jautājumu atbildēts noliedzoši („Nē" vai „Nezinu"), uz 8.jautājumu nav jāatbild.*)

   ☐ Jā ☐ Nē ☐ Nezinu

8. Kāds ir pieļaujamais organizācijas visu informācijas sistēmu maksimālais nepieejamības laiks? (*Ja norādījāt atbildes variantu "cits", tad norādiet laiku.*)

   ☐ 1 stunda; ☐ 48 stundas;

   ☐ 2 stundas; ☐ Cits

   ☐ 24 stundas; _____

9. Kāda ir organizācijas noteiktā maksimāli pieļaujamā datu centra nepieejamība, kura laikā nav pieejama neviena no organizācijai nepieciešamajām informācijas sistēmām?

☐	Nav noteikta;	☐	2 stundas;
☐	48 stundas;	☐	1 stunda;
☐	24 stundas;	☐	Nav pieļaujama.

10. Vai organizācijas datu centrs ir izvietots biroja telpās, pielāgotās vai speciāli datu centra vajadzībām projektētās telpās?

☐ Biroja ☐ Pielāgotās ☐ Speciāli projektētās

11. Vai organizācijas datu centrs spēs atbilstošā kvalitātē nodrošināt Jūsu organizācijas esošās un nākotnes prasības arī tuvāko piecu gadu laikā?

☐ Jā ☐ Nē

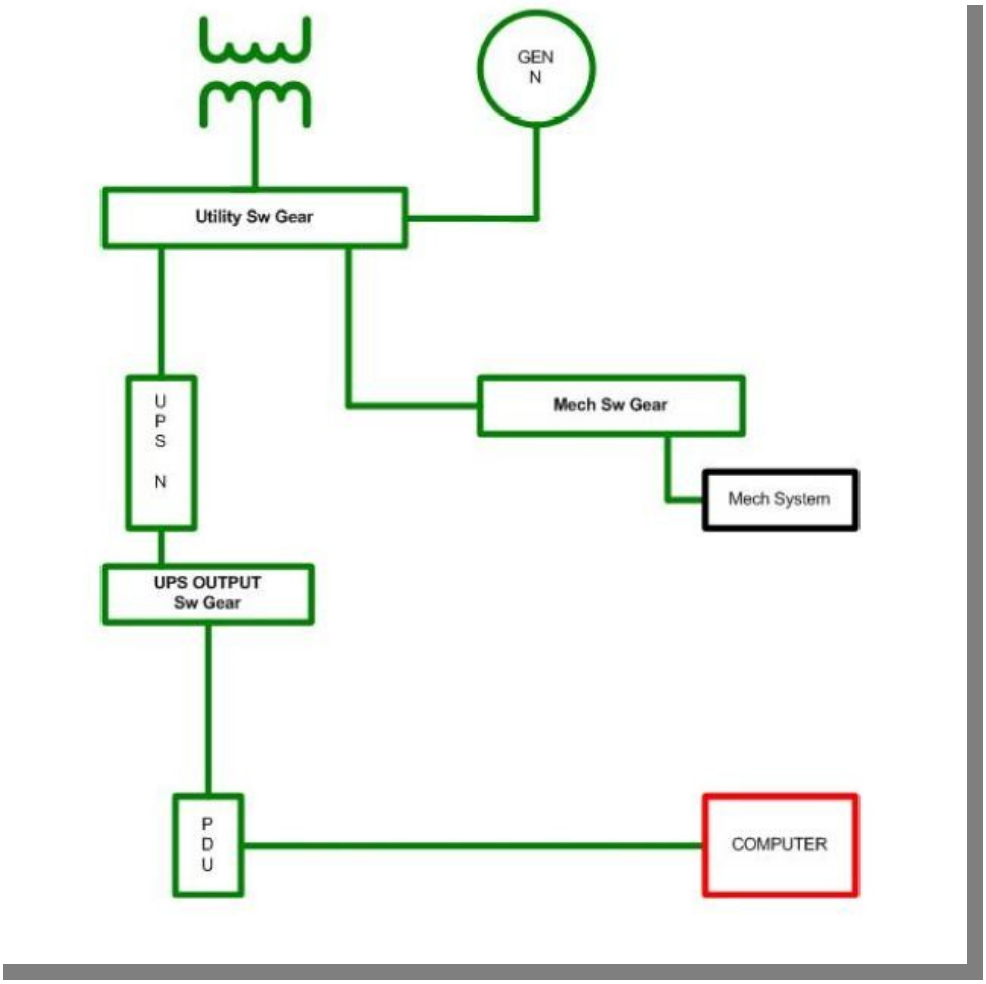
12. Lūdzu, norādiet, Jūsuprāt, datu centra darbības kvalitātes nodrošināšanai nepieciešamāko aprīkojumu: (*1 – neietekmē, 2 – neliela ietekme, 3 – būtiska ietekme, 4 – kritiska*)

1)	Ēkas konstrukciju un platības atbilstība	☐1	☐2	☐3	☐4
2)	Elektroapgāde	☐1	☐2	☐3	☐4
3)	Strāvas ģenerators	☐1	☐2	☐3	☐4
4)	Nepārtrauktas elektrobarošanas avots (UPS)	☐1	☐2	☐3	☐4
5)	Mikroklimata sistēma	☐1	☐2	☐3	☐4
6)	Ugunsdzēsības sistēma	☐1	☐2	☐3	☐4
7)	Signalizācijas un video novērošanas sistēma	☐1	☐2	☐3	☐4
8)	Fiziskā apsardze	☐1	☐2	☐3	☐4
9)	Diennakts uzraudzība	☐1	☐2	☐3	☐4

Paldies!

2.pielikums

Pirmā līmeņa datu centra strāvas apgādes topoloģijas shēma



Izmantotie apzīmējumi:

Switch gear – slēdžu iekārta

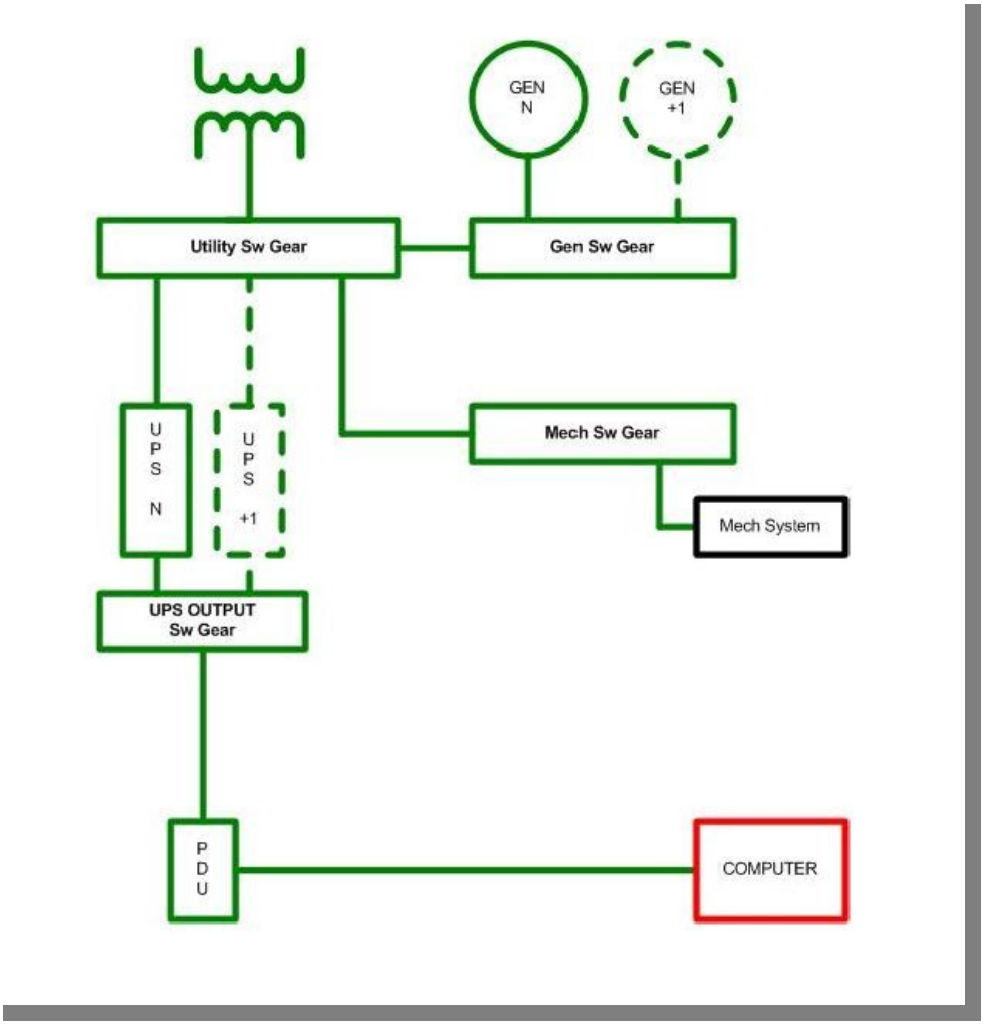
UPS – nepārtrauktas barošanas avots

PDU – strāvas sadale

GEN – strāvas ģeneratori

3.pielikums

Otrā līmeņa datu centra strāvas apgādes topoloģijas shēma



Izmantotie apzīmējumi:

Switch gear – slēdžu iekārta

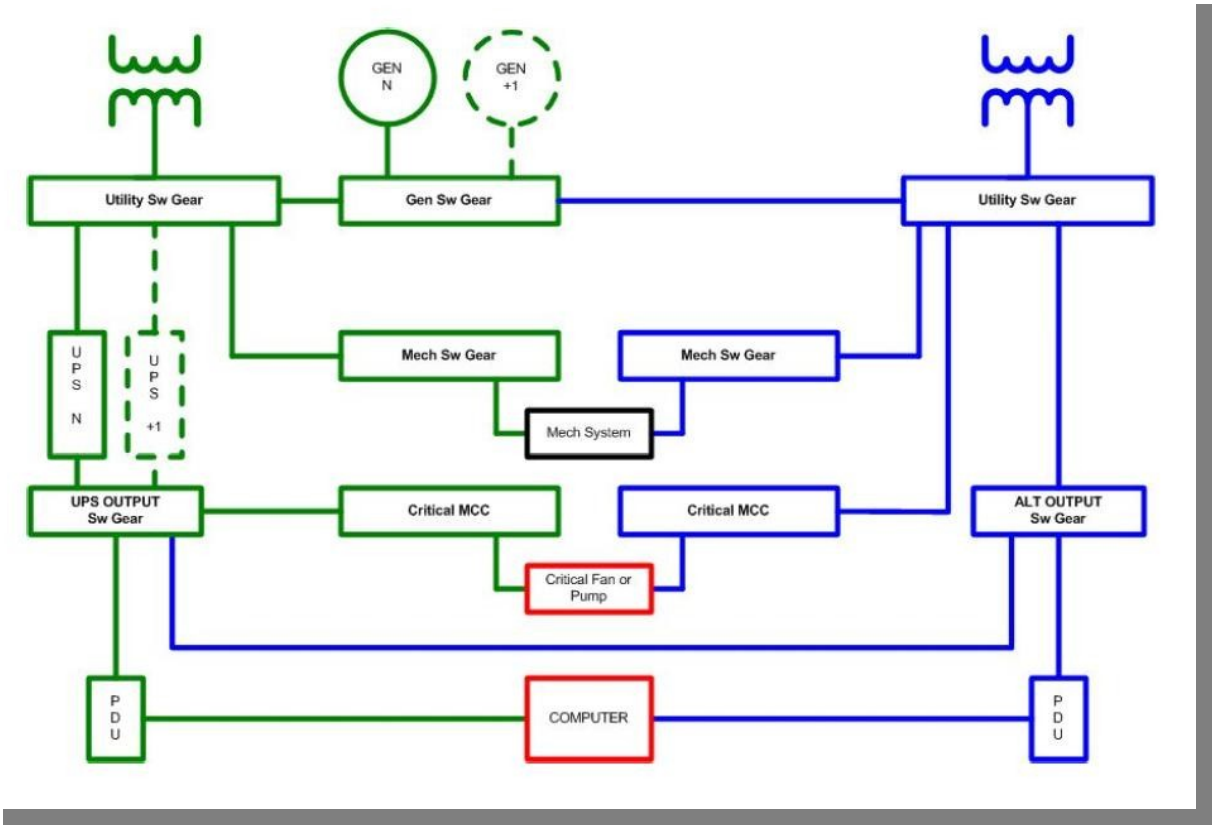
UPS – nepārtrauktas barošanas avots

PDU – strāvas sadale

GEN – strāvas ģeneratori

4.pielikums

Trešā līmeņa datu centra strāvas apgādes topoloģijas shēma



Izmantotie apzīmējumi:

Switch gear – slēdžu iekārta

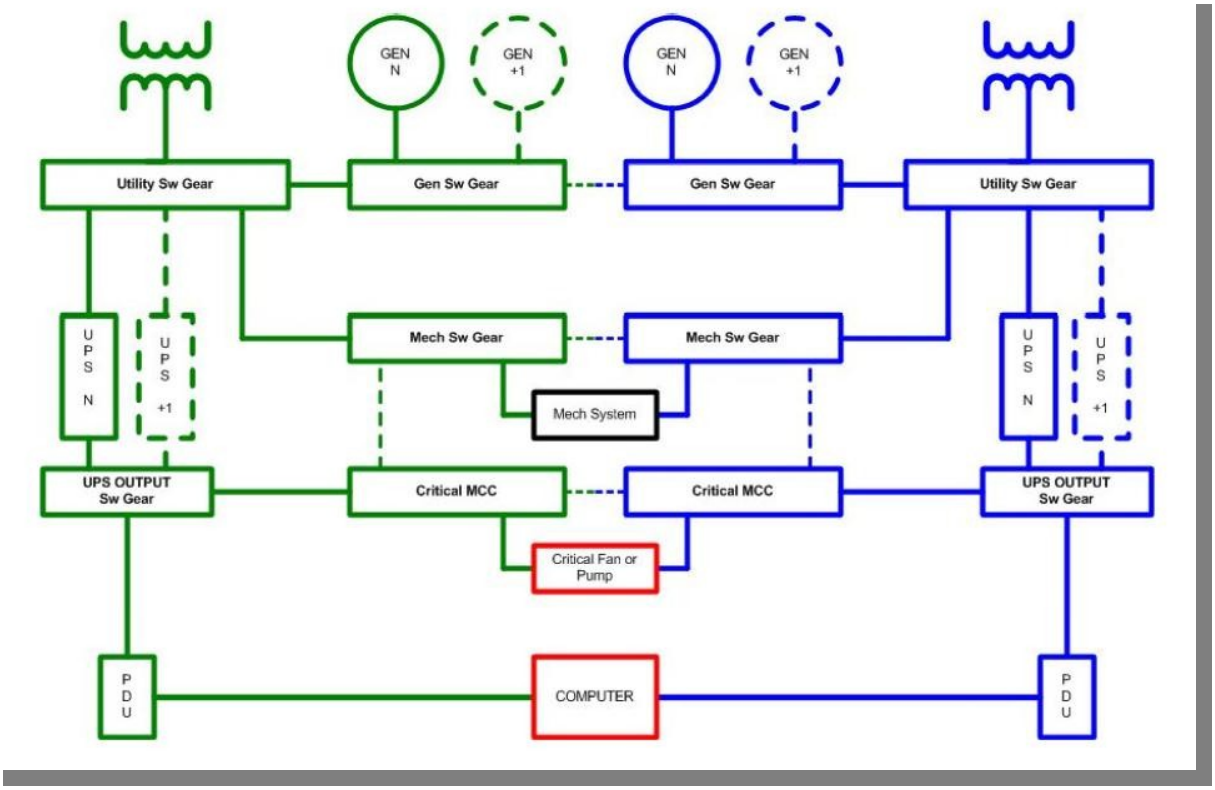
UPS – nepārtrauktas barošanas avots

PDU – strāvas sadale

GEN – strāvas ģeneratori

5.pielikums

Ceturtā līmeņa datu centra strāvas apgādes topoloģijas shēma



Izmantotie apzīmējumi:

Switch gear – slēdžu iekārta

UPS – nepārtrauktas barošanas avots

PDU – strāvas sadale

GEN – strāvas ģeneratori

Bakalaura darbs „Valsts un pašvaldību iestāžu datu centru nepārtrauktas darbības nodrošināšanas kvalitāte” izstrādāts LU Ekonomikas un vadības fakultātē.

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

Autors: Viesturs Šķila

Rekomendēju darbu aizstāvēšanai
Vadītāja: Dr. sc. eng., doc. Ilga Karlsone

Recenzents: Dr. oec., doc. Inese Spīča

Darbs iesniegts Tirgzinību katedrā

_____
(darba pieņēmēja paraksts, datums)

Darbs aizstāvēts bakalaura gala pārbaudījuma komisijas sēdē

_____2007. prot. Nr. _____, vērtējums _____

Komisijas sekretāre: _____
(paraksts, datums)