Darja Šmite
Dainis Dosbergs
Juris Borzovs

INFORMĀCIJAS UN KOMUNIKĀCIJAS TEHNOLOĢIJAS NOZARES TIESĪBU UN STANDARTU PAMATI

UDK 004(094)
Šm 570

Literārā redaktore Anitra Pārupe
Maketu un vāka dizainu veidojusi Ilze Reņģe

ISBN 9984-770-79-6

PRIEKŠVĀRDS

Šīs grāmatas galvenie adresāti ir pirmā līmeņa profesionālās augstākās izglītības programmu studenti, kuri vēlas iegūt ceturtā līmeņa profesionālo kvalifikāciju „programmētājs". Pašreiz šādas studiju programmas tiek īstenotas vairākās Latvijas augstākās izglītības iestādēs. Programmas balstās uz PHARE projekta „Profesionālā izglītība 2000" atziņām un tā ietvaros izstrādāto programmētāja profesijas standartu un studiju paraugprogrammu. Profesijas standarts prasa zināšanas sadaļā „IKT nozares tiesību pamati un standarti", bet studiju paraugprogramma paredz kursus „Nozares tiesību pamati un standarti" un „Darba aizsardzība un ergonomika".

Grāmatas trešais autors Juris Borzovs savulaik ir piedalījies minētajā PHARE projektā un izstrādājis attiecīgā kursa struktūru, bet kursa saturs fragmentāri jau agrāk ir lasīts LU un RTU bakalaurantūras un maģistrantūras kursos „Programmēšanas metodoloģija" un „Programmatūras kvalitāte", kā arī Rīgas Informācijas tehnoloģijas institūta t. s. elitārajos lekciju kursos „Lielu un svarīgu informācijas sistēmu projektu uzsākšana un attīstīšana". Grāmata ir izaugusi no pirmo divu autoru Darjas Šmites un Daiņa Dosberga maģistra darbiem, kuru izstrādi vadījis trešais autors. Juris Borzovs ir arī šīs grāmatas redaktors.

Darja Šmite ir uzrakstījusi I daļu "Nozares tiesības", bet Dainis Dosbergs – II daļu "Nozares standarti". Ļoti liela nozīme ir tam, ka abi autori kopš 2002. gada kopīgi docē attiecīgo kursu Latvijas Universitātē un Rīgas Tehniskajā universitātē.

Autori izsaka pateicību visiem, kuru darbu fragmenti, idejas, formulējumi un konsultācijas izmantoti šajā grāmatā, it īpaši – Uldim Ķinim.

Priekšvārda noslēgumā vēršam lasītāja uzmanību uz to, ka termini "informācijas tehnoloģija", "IT" un "informātika" ir lietoti kā sinonīmi, lai apzīmētu tautsaimniecības apakšnozari, kas pārsvarā ietver datorprogrammu un informācijas sistēmu izstrādi un uzturēšanu. IT, telekomunikācija jeb elektroniskie sakari un elektronika kopā veido nozari, ko pēdējos gados ierasts dēvēt par informācijas un komunikācijas tehnoloģijām jeb IKT.

SATURS

SAĪSINĀJUMI, TERMINI UN NOSAUKUMI

ANO	Apvienoto Nāciju Organizācija (UNO) United Nations Organization
BSA	*Business Software Alliance* organizācija, kas veicina drošas un legālas programmatūras izmantošanu
DVI	Datu valsts inspekcija
ECK	Eiropas Cilvēktiesību konvencija
EDA	elektroniskā datu apmaiņa *(EDI) Electronic Data Interchange*
EP	Eiropas Padome
ES	Eiropas Savienība
FPDAL	Fizisko personu datu aizsardzības likums
G-7	pasaules septiņu ekonomiski attīstītāko valstu apzīmējums
IKT	informācijas un komunikācijas tehnoloģijas
IPS	interneta pakalpojumu sniedzējs
IS	informācijas sistēma
ISO	*International Organization for Standardization* Starptautiskā standartu organizācija
IT	informācijas tehnoloģija
KL	Krimināllikums
LR	Latvijas Republika
KPS	kvalitātes pārvaldības sistēma
LU	Latvijas Universitāte
LVS	Latvijas Valsts standarts
MK	Ministru kabinets
PPA	programmatūras projektējuma apraksts
PPS	programmatūras prasību specifikācija
UN OECD	*United Nations Organisation for Economic Cooperation and Development* Apvienoto Nāciju Ekonomiskās sadarbības un attīstības organizācija
UNCITRAL	*United Nations Commission on International Trade Law* ANO Starptautiskā tirdzniecības komisija
VID	Valsts ieņēmumu dienests
VIĪO	Vispasaules Intelektuālā īpašuma organizācija *(WIPO) World Intellectual Property Organization*

NOZARES TIESĪBAS

1. IEVADS

Strauja informācijas tehnoloģiju attīstība ir ietekmējusi visas nozares. Līdz ar to ir mainījusies gan cilvēka loma dažādos procesos, gan arī paši procesi un tajos iesaistītie objekti. Visā pasaulē ir kļuvušas populāras dažāda veida elektroniskas darbības vai „attiecības", piemēram, e-pasta nosūtīšana, interneta mājaslapu izveidošana un publicēšana, pat enciklopēdijām, grāmatām un avīzēm parādījušās publiski pieejamas elektroniskas versijas.

Līdz ar jaunu tehnoloģiju ienākšanu mūsu dzīvē ir mainījusies arī tiesiskā regulēšana. Tā vairs nevarēja balstīties tikai uz agrākiem principiem. Jo kā gan var izvērtēt interneta mājaslapas uzlaušanu vai datu bāzes nelikumīgu kopēšanu un izplatīšanu? Līdz ar to aktuāli kļuvuši arī tālāk minētie tik šķietami vienkāršie jautājumi.

Kas ir dokumenta autors?

Kurš ir elektroniskā dokumenta oriģināls? Vai tas ir piesaistīts datoram, diskam, datnei?

Un, ja datne-dokuments ir pārnests ar disketes palīdzību, bet sākotnēji izveidotā datne izdzēsta, kas tad ir oriģināls?

Tās ir ikdienišķas „elektroniskas" attiecības. Bet pastāv arī vesela ražošanas sistēma, kas uztur un palīdz elektronisko attiecību progresam – tā ir datorprogrammatūras izstrāde un administrēšana, telesakaru tīklu izveidošana un uzturēšana, mājaslapu izstrāde un uzturēšana utt.

Programmētāji, testētāji, dokumentētāji, sistēmanalītiķi, projektētāji, projektu vadītāji, administratori un citi speciālisti, kas ir iesaistīti šajos procesos, savā ikdienas darbā saskaras ar likumdošanas nozari tiešā vai netiešā veidā. Tas nozīmē, ka programmatūras un datorsistēmu izstrādes un uzturēšanas procesi un produkti jeb nodevumi tiek pakļauti zināmiem standartiem un likumiem.

Tomēr ne jau vienmēr IKT speciālisti zina, kuras viņu darbības tiek regulētas un ar kādiem reglamentējošiem aktiem tas ir veikts. Nepieciešamās zināšanas viņi varēs gūt šai grāmatā.

Darja Šmite

2. TIESĪBU NOZARES PAMATI

Nodaļa izstrādāta, balstoties uz [1, 25.–37. lpp.].

Lai iedziļināties sarežģītos juridiski regulējamos jautājumos un procesos, ikvienam ir jāapgūst attiecīga terminoloģija un pamatjēdzieni. Tiesību nozarē, tāpat kā citās nozarēs, eksistē savs leksikons un specifisku jēdzienu apzīmējumi. To zināšana atvieglo juridiskās literatūras lasīšanu un saprašanu.

Dažas tiesību nozares pamatjēdzienu definīcijas ir apkopotas 1. tabulā.

1. tabula

Terminu skaidrojumi

Termins	Definīcija
Tiesību sistēma	Juridiski doktrināra kategorija, kas ietver tiesību normas, tās apvienojošos tiesību institūtus un tiesību nozares, kas regulē sabiedriskās attiecības valstī.
Tiesību nozare	Tiesību sistēmas sastāvdaļa. Katra nozare ir pa tiesību institūtiem sadalītu juridisku normu kopums, kas regulē īpašas, kvalitatīvi atšķirīgas sabiedriskās attiecības.
Tiesības	Izšķir konstitucionālās tiesības, cilvēktiesības, civiltiesības, administratīvās tiesības, krimināltiesības, civilprocesuālās un kriminālprocesuālās tiesības u. c.
Tiesību akts, normatīvs akts	Rakstīta tiesību norma, ko savas kompetences ietvaros izdevusi pilnvarota valsts vai pašvaldību institūcija. Pie tiesību aktiem pieder Satversme, konstitucionālie likumi, likumi, kodeksi, Ministru kabineta noteikumi, pašvaldību saistošie noteikumi.
Tiesību akta pieņemšanas datums	Tiesību akta apstiprināšanas datums. Tiesību akta pieņemšana nenozīmē to, ka pieņemtās normas sāk darboties.
Tiesību akta spēkā stāšanās datums	Datums, kad normatīvajā aktā noteiktas normas sāk darboties.
Tiesību aktu grozījumi	Tiesību aktu izmaiņas, kuras tiek pieņemtas atsevišķā redakcijā.
Likumprojekts	Likums sagatavošanas fāzē. Likumprojektus var iesniegt Saeimai Valsts prezidents, Ministru kabinets, Saeimas komisijas, ne mazāk kā pieci deputāti, kā arī viena desmitā daļa vēlētāju (Satversmē paredzētajā kārtībā).
Tiesas	Tiesa ir valsts institūcija, kas izšķir fizisko un juridisko personu strīdus un izskata krimināllietas. Latvijā ir rajona (pilsētas) tiesas, apgabaltiesas un Augstākā tiesa. Personai vai institūcijai, kas griezusies tiesā, ir tiesības uz tās lietas izskatīšanu.
Tiesnesis	Tiesnesis ir amatpersona, kas izskata lietas tiesā. Tiesneši ir neatkarīgi un vienīgi likumam pakļauti. Tiesnešus apstiprina Saeima, un viņi nav atceļami.

Direktīva	Direktīva ir obligāts rīkojums vai norādījums. ES direktīvās ir apvienotas visas tās normas, kuras ir jāīsteno ES dalībvalstīm likumdošanas jaunrades procesā, tomēr metodes mērķu sasniegšanai katra dalībvalsts var izvēlēties patstāvīgi.
Vadlīnija	Galvenais nozīmīgākais virziens, veids kādai darbībai, norisei. Starptautisko organizāciju izstrādātās vadlīnijas nosaka principus, ko valstis brīvprātīgi var piemērot tiesību aktu izstrādes procesā.
Valsts standarts	Valsts standarts nosaka prasības pret procesu vai produktu. Standarts ir obligāti ievērojams tikai tad, ja to pieprasa tiesību akts vai par to vienojušies līgumslēdzēji.

Attīstoties sabiedrībai, attīstās arī tiesību nozare, iekļaudama arvien jaunas tiesību nozares sastāvdaļas. Tieši tāpēc pēdējā laikā visā pasaulē attīstās jaunas informācijas un komunikāciju tiesības. Dažās valstīs tām ir paredzēta atsevišķa tiesību nozare, bet citur tā ir iekļauta kādā apakšnozarē, kādas tiesību nozares atzarā vai likumdošanas novirzienā kādas funkcionējošās tiesību nozares ietvaros.

2.1. TIESĪBU NOZARI REGLAMENTĒJOŠIE DOKUMENTI

Tiesību nozares reglamentējošie dokumenti ir visai dažādi, bet visi kopā veido tiesību avotus.

Tie, pirmkārt, ir tiesību akti – publiskās varas institūcijas tiesību normu jaunrades akti (Satversme, konstitucionālie likumi, likumi, kodeksi, Ministru kabineta noteikumi, pašvaldību saistošie noteikumi).

Otrkārt, tie ir priekšstati par IKT nozari un tās pamatprincipiem. Priekšstati nav nekādi reglamentējošie dokumenti, taču tie ir avoti, no kuriem juristi gūst informāciju, kas nepieciešama nozares, tās kultūras un tradīciju izzināšanai.

Treškārt, tās ir dažādu starptautisko organizāciju izstrādātās vadlīnijas, rekomendācijas un priekšlikumi. Šie dokumenti nosaka principus, ko valstis brīvprātīgi var piemērot tiesību jaunrades procesā. Tie ietver dažādu valstu tiesību aktu aprakstus, problēmu vērtējumu un risināšanas metodes. Centrālās starptautiskās vadlīnijas ir, piemēram, Apvienoto Nāciju Organizācijas (ANO) Ekonomiskās sadarbības un attīstības organizācijas (*UN OECD*) vadlīnijas par informācijas sistēmu drošību, kā arī rekomendācijas kriptogrāfijas politikā un ANO Starptautiskās tirdzniecības komisijas (*UNCITRAL – United Nations Commission on International Trade Law*) elektroniskās komercijas vadlīnijas.

Arī nozares standarti ir tiesību avots. Standarti ir vēl vairāk pakārtots jēdziens nekā principi un vadlīnijas, taču ir gadījumi, kad tiesību akti balstās uz kādu noteiktu standartu.

Iepriekš minētais liecina par to, ka tiesību sistēmas regulējumā tiek ietverti ne tikai likumi, bet tas balstās arī uz starptautisko pieredzi.

! *Latvijas tiesību akti sastāv no nodaļām (numurēti ar romiešu cipariem), kuras savukārt sastāv no pantiem (numurēti ar arābu cipariem). Tiesību aktu pirmā nodaļa ir vispārīgie noteikumi, kuri sākas ar aktā lietoto terminu skaidrojumu, tad seko aktā lietotie pamatprincipi un pēc tam tiek izdalītas tematiskas nodaļas ar pantiem.*

Autortiesību likums
I nodaļa
Vispārīgie noteikumi

1. pants. Likumā lietotie termini
Likumā ir lietoti šādi termini:
1) **autors** – fiziskā persona, kuras radošo spēju rezultātā radīts konkrētais darbs;
2) **darbs** – autora jaunrades rezultāts jebkādā materializētā formā, kā arī publiski izpildīta improvizācija tās izpildījuma brīdī;
3) **datu bāze** – neatkarīgu darbu, datu vai citu materiālu krājums, kas sakārtots sistemātiski vai metodiski un individuāli pieejams elektroniskā vai citādā veidā;
...
2. pants. Autortiesību principi
(1) Autortiesības pieder autoram, tiklīdz darbs ir radīts, neatkarīgi no tā, vai darbs ir pabeigts...

II nodaļa
Aizsargājamie un neaizsargājamie darbi
...
III nodaļa
Autors un autora tiesību pārņēmēji
...

1. att. Likuma teksta paraugs.

2.2. VISPĀRĪGIE PRINCIPI

Ar informācijas tehnoloģijas nozari saistītie principi ir vērsti galvenokārt uz informācijas lietošanas kvalitāti. Informācija šajā kontekstā ir visai dažāda – tā ir valsts pārvaldībā esoša informācija, personas dati, informācija, ko pauž vai iegūst ikviens internetā, informācija, ko rada kāda persona, u. tml. Arī informācijas lietošanai ir plaša nozīme – tā var būt datu elektroniskā apstrāde, pārsūtīšana, pieejamība, aizsardzība u. c.

- **Informācijas atklātības princips.** Visai valsts informācijai ir jābūt atklātai, izņemot likumā noteiktus ierobežojumus. Šis princips ir ietverts tādos tiesību aktos kā Informācijas atklātības likums, Civillikums, kā arī Satversme. Katram no mums ir jāzina, kādu informāciju mēs esam tiesīgi iegūt no valsts institūcijas un kādas informācijas izplatīšana, publicēšana un apstrāde ir nelikumīga.
- **Privātās dzīves aizsardzības princips.** Tas ir pilnīgi iekļauts Latvijas Republikas Satversmē, Fizisko personu datu aizsardzības likumā un Eiropas Cilvēktiesību konvencijas 8. pantā, kurā ir noteikts, ka nevienam nav tiesību iejaukties personas privātajā dzīvē.

- **Informācijas drošības princips.** Tas ietver informācijas autentiskumu, to, ka informācijai pārraides procesā ir jāatbilst oriģinālam, un integritāti, kas noteic, ka informāciju nevar mainīt. Šis princips ietver arī informācijas nenoliegšanas principu, to, ka nosūtītājam nav tiesību neatzīt savu nosūtīto informāciju, ja tā ir identificējama, un tādu informācijas aizsardzības līdzekli kā kriptogrāfija u. c.
- **Informācijas brīvas pārraides princips.** Tas nozīmē, ka nevienam nav tiesību ierobežot informācijas plūsmu, izņemot specifiskus, tieši likumā paredzētus gadījumus. Šis princips noteic, ka valstīm jāveicina brīva jauno tehnoloģiju attīstība.
- **Informācijas identifikācijas iespēja un tās kā pierādījuma izmantošana tiesas procesā.** Šis princips noteic, ka IKT aizsargā tikai identificējamu informāciju, un tai jābūt izmantojamai kā pierādījumam civilprocesā vai krimināprocesā. Šajā sakarā ir ārkārtīgi svarīga elektronisko dokumentu juridiska akceptēšana, kuras noteikumi ir iestrādāti 2002. gada 31. oktobrī pieņemtajā Elektronisko dokumentu likumā.
- **Personas aizsargāšana no negodīgas, nelikumīgas informācijas.** Šis princips ietver valsts uzdevumu sekmēt likumīgu informācijas tehnoloģiju izmantošanu un vienlaikus ar tiesiskām metodēm aizsargāt gan nepilngadīgo likumīgās intereses, gan arī iedzīvotāju godu, cieņu un veselību. Internets rada plašu viedokļu apmaiņas un paušanas arēnu, kuras robežas ir neaptveramas. Taču ir jāatceras, ka vārda un izteiksmes brīvība nevienam nedod neierobežotas tiesības uz informācijas izplatīšanu.
- **Atbildība par IKT tiesību pārkāpumiem.** Šis princips faktiski ir garants tam, ka dokumentēta informācija tiek aizsargāta un ka par katru pārkāpumu vainīgajai personai iestājas atbildība. Princips daļēji ir iestrādāts krimināllikumā. Patlaban likumdevējs nav paredzējis citus atbildības veidus par šāda rakstura pārkāpumiem.

2.3. LATVIJAS TIESĪBU AKTI IKT NOZARĒ

Informācijas atklātības likums [2]
Pieņemts 29.10.1998.
Kārtība, kādā valsts pārvaldes iestāžu un pašvaldību iestāžu rīcībā esošā informācija nododama atklātībai.

Fizisko personu datu aizsardzības likums [3]
Pieņemts 23.03.2000.
Kārtība, kādā ir uzglabājami un apstrādājami fizisko personu dati.
Eiropas Padomes 28.01.81. Konvencija par personu datu aizsardzību attiecībā uz personas datu automātisko apstrādi.

Autortiesību likums [4]
Pieņemts 06.04.2000.
Nosaka intelektuālā īpašuma autortiesības un to izmantošanas principus.

Likums par valsts noslēpumu [5]
Pieņemts 17.10.1996.
Likuma mērķis ir formulēt valsts noslēpuma jēdzienu, noteikt valsts noslēpuma glabāšanas un izmantošanas kārtību un tā aizsardzību.

Valsts informācijas sistēmu likums [6]
Pieņemts 02.05.2002.
Likuma mērķis ir nodrošināt valsts un pašvaldību institūciju sniedzamo informatīvo pakalpojumu pieejamību un kvalitāti valsts informācijas sistēmās.

Elektronisko dokumentu likums [7]
Pieņemts 31.10.2002.
Nosaka elektroniskā dokumenta un paraksta tiesisko statusu.

Elektroniskās komercijas likums
Tiek izstrādāts.
Ar MP 05.05.2000. rīkojumu Nr. 159 izveidota Ekonomikas ministrijas darba grupa.

MK noteikumi Nr. 106 – „Informācijas sistēmu drošības noteikumi" [8]
Pieņemti 21.03.2000.
Nav spēkā. Tiek pārstrādāti.
Saistībā ar Krimināllikumu.
Nosaka informācijas sistēmu drošības tiesiskās, tehniskās un organizatoriskās pamatprasības, kas jāievēro valsts īpašumā vai pārvaldībā esošo sistēmu uzturēšanā.

MK noteikumi Nr. 40 – „Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības" [9]
Pieņemti 30.01.2001.
Nosaka obligātās tehniskās un organizatoriskās prasības pret sistēmām, kuras glabā un apstrādā fizisko personu datus.
Saskaņā ar Fizisko personu datu aizsardzības likumu.

MK noteikumi Nr. 408 – „Datu valsts inspekcijas nolikums" [10]
Pieņemti 28.11.2000.
Nosaka fizisko personu datu aizsardzības likuma uzraudzības institūcijas nolikumu. Starp citiem datu valsts inspekcijas pienākumiem ir arī personas datu apstrādes sistēmu obligātā reģistrācija un pārbaude.
Saskaņā ar Fizisko personu datu aizsardzības likumu.

2.4. KONTROLJAUTĀJUMI

1. Kas ir tiesību sistēma, un no kā tā sastāv?
2. Kādi ir tiesību nozari reglamentējošie dokumenti?
3. Nosauciet vispārīgos nozares principus!

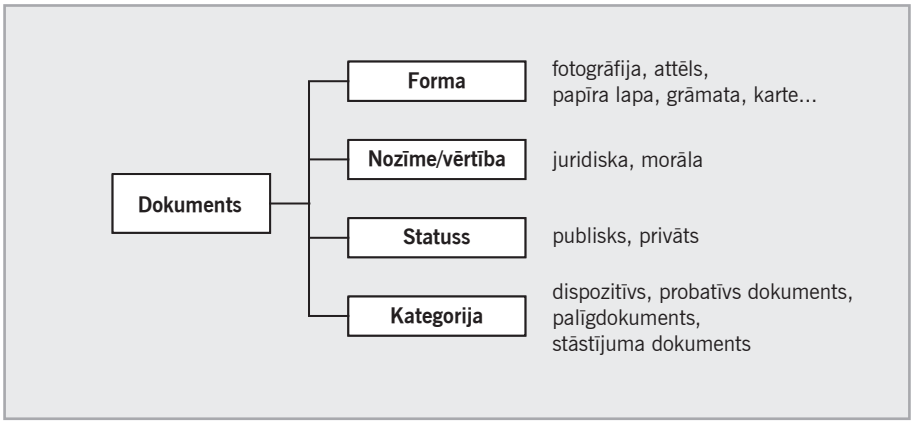
3. DOKUMENTI, TO VEIDI, ĪPAŠĪBAS UN DARBĪBAS AR TIEM

Nodaļa izstrādāta, izmantojot [1, 51.–76. lpp., 11].

3.1. KAS IR DOKUMENTS?

Viens no svarīgākiem likumdošanas objektiem ir dokuments. Dokuments ir elektroniskā veidā vai uz papīra publicētas vai nepublicētas informācijas vienība. Tas būtībā ir informācijas nesējs. Tam var būt dažāda forma – attēls, fotogrāfija, papīra lapa, grāmata, karte u. c. Dokumentiem ir atšķirīga nozīme. Juridiska nozīme ir tādiem dokumentiem kā dzimšanas apliecība, pase, zemesgrāmata, darba līgums, iesniegums par gāzes ievilkšanu, patents par izgudrojumu u. c. Dokumentiem var būt arī morāla vērtība, piemēram, kāda tuva radinieka fotogrāfija kā vienīgā atmiņa par viņu. Dokumentiem ir arī atšķirīgs statuss – vieni ir publiski, citi privāti. Piemēram, darba līgums ir publisks dokuments, kuru noslēdz juridiska persona un privātpersona, savukārt fotogrāfija vai e-pasta vēstule ir privāti dokumenti.

Dokumentus var iedalīt kategorijās. Dokumentu sadalījumu nosaka funkcijas, kurām tie kalpo, vai to rakstiskās formas sagatavošanas mērķis. Tie var būt dispozitīvie jeb rīkojuma dokumenti (rīkojums, līgums, testaments), kuri ierosina kādu darbību un kuriem piemīt juridisks spēks, probatīvie jeb pierādījuma dokumenti (statistiskie dati, saraksti, pirkumu čeki), kurus sastāda, lai dokumentētu kādu jau pirms tā sagatavošanas notikušu darbību un kuriem arī piemīt juridisks spēks, palīgdokumenti (konspektu pieraksti), kuri top iepriekšminēto dokumentu sagatavošanas procesā, kā arī stāstījuma jeb naratīvie dokumenti (informatīvas vēstules vai domu apmaiņa par kādu notikumu), kuri vēsta par darbības vai lēmuma pieņemšanas procesa gaitu, bet nav juridiski saistoši.



2. att. Dokumenta atribūti.

Ar dokumentu palīdzību ir organizēta visa mūsu dzīve. Ar dokumentiem cilvēki pierāda savas tiesības, un tieši šī iemesla dēļ dokumenti ir vieni no kriminālās pasaules iecienītākiem objektiem viltošanai un zagšanai.

3.2. DIPLOMĀTIKA

Tiesību sistēmā ir zinātne, kas nodarbojas ar jautājumu par dokumentiem, – tā ir diplomātika jeb zinātne par dokumentiem. Termins *diplomātika* ir latīņu izteiciena *res diplomatica* mūsdienu adaptācija.

Diplomātika kā zinātne ir radusies tādēļ, lai ar kritiskas analīzes palīdzību atšķirtu īstus dokumentus no viltojumiem. Dokumentu viltošana pastāv tik ilgi, cik ilgi pastāv dokumenti. Tomēr pirmie mēģinājumi izstrādāt paņēmienus viltojumu noteikšanai aizsākās tikai VI gadsimtā. Antīkajā pasaulē vispāratzīts bija juridisks princips, kas noteica, ka autentiskums (īstums, no grieķu *authentikos* – galvenais, īsts) nav dokumentam raksturīga pazīme. Priekšnoteikums autentiskuma radīšanai bija dokumenta glabāšana kaut kādā iepriekš noteiktā vietā – templī, valsts iestādē, mantnīcā vai arhīvā. Līdz ar to šo principu sāka bieži izmantot ļaunprātīgos nolūkos, viltotos dokumentus nododot glabāšanā speciālajās glabātavās, lai tādējādi "piešķirtu" tiem autentiskumu. Tāpēc Bizantijas imperatora Justiniāna radītajā civilkodeksā tika iekļautas normas, kas palīdzēja atšķirt viltotos dokumentus no īstajiem. XVIII gadsimtā diplomātiku sāka mācīt universitāšu juridiskajās fakultātēs. Tas veicināja strauju diplomātikas attīstību. Vācijā, Francijā, Anglijā, Spānijā un Itālijā publicēja lielu skaitu zinātnisku apcerējumu, kas veltīti dokumentu analīzes metodēm.

Līdz ar elektronisko dokumentu ienākšanu mūsu ikdienā diplomātikas apskatāmo jautājumu loks paplašinās. Arvien aktuālāks pasaulē kļūst jautājums par elektronisko dokumentu juridisko spēku.

3.3. DOKUMENTA AUTENTISKUMS UN UZTICAMĪBA

Iespēja izmantot dokumentus kā juridisku pierādījumu kādas darbības veikšanai, tiesību īstenošanai vai likumīgo interešu aizstāvībai ir atkarīga no to tiesiskā statusa. Dokumentiem ir jāpiemīt tādām īpašībām kā uzticamībai un autentiskumam.

Uzticamība attiecas uz dokumenta spēju būt par liecību vai pierādījumu (t. i., spēju simbolizēt faktu). Šo īpašību dokuments iegūst tikai tad, ja

- tas ir noformēts atbilstoši likumu un citu tiesību aktu prasībām,
- sastādīts saskaņā ar kontrolētu procedūru,
- to ir sastādījis uzticams autors.

Autentiskums nozīmē to, ka dokumentam var pierādīt tā īstumu vai apliecināt tā izcelsmi. Autentiskuma pilnīgs vai daļējs trūkums samazina vai pavisam likvidē dokumenta spēju būt par pierādījumu vai liecināt par darbību vai faktu.

Pastāv divas administratīvas un birokrātiskas sistēmas. Katra no tām jēdzienu "autentisks" interpretē dažādi.

Valstīs, kas bija izvēlējušās romiešu izstrādāto tiesību sistēmu, notikušas darbības un saistības atzina par tiesiskām jeb spēkā esošām, ja notārs vai valsts ierēdnis bija sagatavojis rakstisku aktu, kuru darbībā iesaistītās personas parakstīja ar vārdu, simbolu vai krustu un par kuru rakstītājs uzņēmās juridisko vai politisko atbildību.

Valstīs, kas bija izvēlējušās franku izstrādāto tiesību sistēmu, samierinājās arī ar mutisku vienošanos liecinieku klātbūtnē un izvēlētā objekta parādīšanu. Kad radās nepieciešamība pierādīt šīs darbības vai saistību esamību, tās dalībnieki vai to pēcteči otrreiz to pārskatīja karaļa tiesneša priekšā. Tiesnesis tiesas procesu pierakstīja un sagatavotajam dokumentam (rakstiskajam aktam) uzspieda zīmogu.

Abos minētajos gadījumos šo rakstisko aktu uzskatīja par uzticamu, tātad arī tiesisku dokumentu, jo personas (gan notārs, gan tiesnesis), kas to bija izdevušas, bija uzticamas. Dokumentu varēja arī laika gaitā uzskatīt par autentisku, jo tajā tika iekļauti elementi, ko grūti viltot (piemēram, zīmogi, speciālas zīmes utt.). Tomēr abos gadījumos tikai apzīmogošana un dokumentu glabāšana drošā vietā nevarēja garantēt, ka darbības un saistības, uz kurām attiecīgie dokumenti attiecas (kuras tie dokumentē), varētu uzskatīt par likumīgām arī nākotnē. Šie līdzekļi varēja garantēt dokumentu nākamajiem lietotājiem to autentiskumu, nevis to uzticamību.

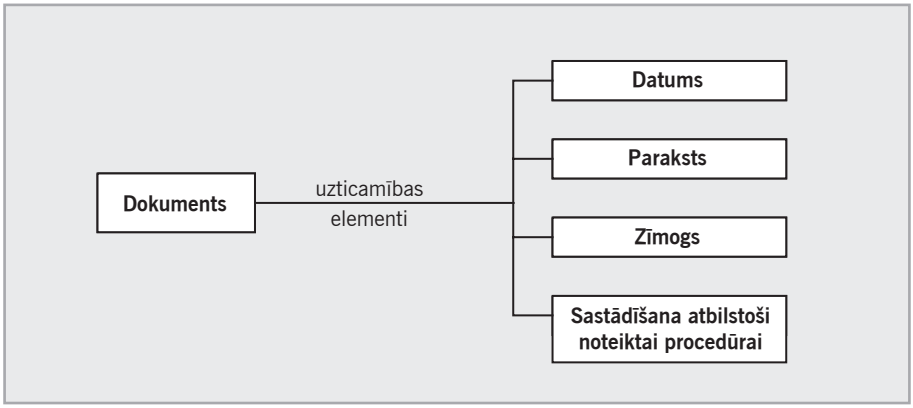
Dokuments nav nekas cits kā dokumentēta informācija, kas balstās uz faktiem vai darbībām. Dokuments ir šo faktu un darbību liecība. Šīs liecības nozīmīgums, juridiskais spēks, vērtība ir atkarīga no uzticamības. Tādējādi dokumentu jeb rakstisku aktu (tā to definē arī Civillikumā) uzskata par uzticības cienīgu tad, ja to var aplūkot kā faktu pašu par sevi, kā realitāti, kurai šis dokuments ir pierādījums. Piemēram, uzticams sertifikāts ir fakts, ka persona, kurai sertifikāts tiek izsniegts, ir persona, par kuru tā uzdodas, t. i., apstiprina tās identitāti.

Uzticamību dokumentam nodrošina tā fiziskā un intelektuālā forma vai atribūtu kopums, kuru nosaka attiecīgās valsts sociāli juridiskā sistēma. Otrs svarīgs faktors ir dokumentu sagatavošanas un noformēšanas procedūra. Latvijā dokumentu izstrādes procedūra ir aprakstīta Ministru kabineta izdotajos „Dokumentu izstrādāšanas un noformēšanas noteikumos" [12].

Dokumenta forma tātad ir visu tā raksturīgo pazīmju kopums, kuras var sadalīt, nosakot ar dokumentu saistītās vietas, personas un izskatāmos jautājumus. Dokuments ir pilnīgi noformēts, ja tajā ir iekļauti visi elementi, ko pieprasa attiecīgā laika sociāli juridiskā sistēma, jo dokumentu sastāda tādēļ, lai tas būtu spējīgs izraisīt tās konsekvences, ko atzīst šī sistēma.

Divi parasti visvairāk pieprasīti elementi ir datums un paraksts. Datuma funkcija ir sasaistīt savā starpā dokumenta autoru un informāciju, ko satur dokuments. Savukārt paraksts uzliek atbildību par dokumenta saturu šai personai. Citi nozīmīgie dokumentu uzticamības elementi ir apliecināšana, ko veic tā autors vai notārs, liecinieki, kā arī zīmogs, speciālas zīmes, spiedogi.

Dokumenta sagatavošanas procedūra ir noteikumu kopums, pēc kura ir jāizstrādā dokuments. Šie noteikumi reglamentē lietvedības procesu.



3. att. Dokumenta uzticamības elementi.

Tātad dokumenta uzticamību nosaka divi galvenie faktori:

- dokumenta sagatavošanas atbilstība likumu prasībām,
- procedūras kontroles pakāpe visā dokumenta dzīves ciklā.

! *Iestādes vadītājs, nosūtot elektroniskā pasta vēstuli savā pakļautībā esošajam darbiniekam, noformē nosūtīto informāciju arī uz iestādes veidlapas un pašrocīgi paraksta to. Lai gan abas vēstules ir oriģināli, tiem ir dažādas uzticamības pakāpes, jo to sagatavošanā tiek izmantotas dažādas procedūras un ir dažāds nepieciešamo atribūtu daudzums, lai tās atzītu par pilnīgi noformētām.*

3.4. ELEKTRONISKIE DOKUMENTI

Arvien vairāk dokumentu tiek sagatavoti un glabāti elektroniskajā veidā. Tomēr joprojām ir daudz cilvēku, kuri elektroniskos dokumentus vairāk uzskata par informācijas nesējiem, nevis par darbību un darījumu pierādījumu. Rodas jautājums arī par dokumentu oriģinalitāti – vai ar datora palīdzību izstrādātais vai uz papīra izdrukātais dokuments ir oriģināls? Kas ir datu bāze? Kas vispār ir elektronisks dokuments? Izmantojot mūsdienu tehnoloģijas, iespējams izdarīt tik daudzveidīgas manipulācijas ar elektroniskiem dokumentiem, ka rodas jautājums, vai elektroniskajam dokumentam vispār var būt juridisks spēks. Kā šādā gadījumā iegūt uzticamus un autentiskus dokumentus?

Kamēr tika formulēts, kas ir elektroniskais dokuments, ir pagājuši vairāki gadi. Elektroniskā dokumenta definīciju nedrīkst saistīt ne ar vienu no tehnoloģijām, piemēram, teksta formātu, kas ir atkarīgs no programmatūras izstrādātāja, kā arī tā definīcija nedrīkst būt pretrunīga vai neviennozīmīga.

! *Britu Kolumbijas universitātes projektā „Elektronisko dokumentu integritātes saglabāšana" elektronisko dokumentu definēja kā dokumentu, „kas radīts (tas ir, sagatavots vai saņemts un ielikts datnē tālākai darbībai vai uzziņām) elektroniskā formā". Taču tikpat labi sagatavotais fails var būt izpildes fails (.exe), datu bāze vai programma.*

Pēc ilgstošiem teorētiskiem strīdiem ASV Elektronisko dokumentu komiteja beidzot izstrādāja definīciju, kurā teikts: „Elektroniskais dokuments ir ierakstītas informācijas konkrēta vienība, kuru rada, vāc vai saņem kādas darbības izraisīšanai, vadīšanai vai izpildei un kuru veidojošās sastāvdaļas – saturs, konteksts un struktūra – ir tādas, lai darbību nodrošinātu ar pierādījumu."

Šī definīcija koncentrē uzmanību uz dokumenta saturu, struktūru un darbībām un aptver gan dokumentus, gan datus un datu bāzes, ja tie ir saistīti ar darbības veikšanu.

Savukārt Latvijā Elektronisko dokumentu likumā elektroniskais dokuments ir definēts šādi: elektroniskais dokuments ir jebkuri elektroniskā veidā radīti, uzglabāti, nosūtīti vai saņemti dati, ko veido saturs, struktūra un konteksts.

Dažādos noteikumos un likumos elektronisko dokumentu definīcijas ir dažādas – tiek lietots gan termins „elektroniskais dokuments", gan „elektronisks dokuments", tiek lietotas dažādas to veidojošo sastāvdaļu variācijas. Šis fakts kārtējo reizi pierāda nekonsekvenci tiesību dokumentu sagatavošanā.

3.4.1. ATŠĶIRĪBAS STARP ELEKTRONISKAJIEM UN PARASTAJIEM DOKUMENTIEM

Starp papīra un elektroniskajiem dokumentiem ir zināmas atšķirības. Tāpat kā papīra dokumentam, arī elektroniskajam dokumentam ir savas raksturīgas pazīmes, kuras atšķir to no cita veida dokumentiem. Tās ir šādas:

1) fiksācijas veids un simbolu izmantojums,
2) satura saistība ar vidi jeb informācijas nesēju,
3) fiziskā struktūra,
4) dokumentu identificēšana,
5) dokumentu saglabāšana.

Tradicionālo papīra dokumentu saturs ir fiksēts uz informācijas nesēja ar tādu simbolu (piemēram, burtu, ciparu, attēlu) palīdzību, kas dzīvai būtnei ir tieši pieejami un atpazīstami. Turpretī elektronisko dokumentu saturs ir ierakstīts uz magnētiskā vai optiskā nesēja kodētā veidā, kas cilvēkam nav tieši izlasāms, un to attēlo ar simboliem, kuri ir jāpārveido saprotamā formā.

Papīra dokumenta saturs ir fiksēts uz informācijas nesēja, kas ir informācijas uzglabāšanas ierīce jeb tā sauktais konteiners (piemēram, papīra lapa), un to nevar atdalīt no šī nesēja. Elektronisko dokumentu saturs arī ir ierakstīts uz informācijas nesēja, taču laiku pa laikam to atdala no oriģinālās uzglabāšanas iekārtas un pārsūta uz citu, bieži pavisam atšķirīgu nesēju.

Papīra dokumenta struktūra, kas ir tā neatņemama sastāvdaļa, ir skaidri saredzama tā lietotājam un ir viens no dokumenta autentiskuma noteikšanas pamatkritērijiem. Elektronisko dokumentu struktūra nav tieši acīm saredzama, tā var mainīties, dokumentu pārsūtot.

Elektronisko dokumentu nevar līdzīgi papīra dokumentam identificēt kā fizisku realitāti, tā vairāk ir loģiska realitāte, kas radusies kādas darbības vai darījuma gala rezultātā.

Šo elektroniskā dokumenta raksturīgo īpašību dēļ īpašu nozīmi iegūst tā uzticamības un autentiskuma nodrošināšana.

Taču ar elektroniskā dokumenta atzīšanu par līdzvērtīgu papīra dokumentam nepietiek, lai garantētu tā atzīšanu tiesvedībā. Elektroniskajam dokumentam nepieciešams piešķirt visas tās pašas īpašības, kādas ir tradicionālā veidā sastādītajam dokumentam:

- tas jāsastāda saskaņā ar likumu prasībām un pilnībā jānoformē;
- jānodrošina elektroniskā dokumenta izmantošanas, saglabāšanas iespējas un saprotamība, kā arī tā autentiskums.

To varēja panākt, tikai nodrošinot kontroli pār elektroniskajiem dokumentiem tādā pašā līmenī, kādā tā ir, strādājot ar papīra dokumentiem. Tādējādi tika izstrādāti jauni noteikumi elektroniskai lietvedībai, kas nodrošina dokumentu kontroli tā dzīves cikla laikā.

3.4.2. PARAKSTI ELEKTRONISKAJĀ VIDĒ

Paraksti elektroniskajā vidē var būt veidoti ļoti dažādos veidos. Diemžēl ne katrs paraksts ir pietiekams autentifikācijas līdzeklis.

Gan no tehniskā viedokļa, gan arī juridiski nekas neaizliedz jaunu elektroniska veida autentifikācijas līdzekļu ieviešanu. ASV tiesu prakse ir atzinusi dažādus simbolus dažādās vidēs par pietiekamiem, lai tos uzskatītu par parakstu, piemēram, vārdus uz teleksa vai ar rakstāmmašīnu uzdrukātus vārdus. Pat vēstules veidlapas ar nosūtītāja vārdu un rekvizītiem ir bijušas pietiekamas, lai uzskatītu, ka teksts, kas ar to nosūtīts, ir parakstīts. Arī ar faksu nosūtīti paraksti tiek atzīti par pietiekamiem. Pamatojoties uz šiem piemēriem, varētu arī uzskatīt, ka vārds, kas uzrakstīts e–pasta sūtījuma beigās, uzskatāms par parakstu, ja tas radīts ar atbilstīgu nodomu apliecināt sūtījuma autentiskumu. Likumdevēja rokās ir atzīt konkrēto parakstīšanas veidu par pietiekamu. Tomēr vairumam parakstīšanas veidu elektroniskā vidē nepiemīt ar roku radīta paraksta īpašības. Elektroniskajam parakstam jānodrošina ne tikai autentiskuma apliecināšanas spēja, bet arī drošība, īpašības, ko nodrošina ar roku rakstīta paraksta un papīra dokumentu fiziskā jeb materiālā daba.

! *Watson v. Tom Growney Equip. Inc., 721 p. 2d. 1302 (N.M. 1986) lietā uz pirkuma pasūtījuma formas uzdrukāts personas vārds un uzvārds tika atzīts par parakstu, jo parakstītājs bija labprātīgi aizpildījis pasūtījuma formas detaļas.*

! *Kohlmeyer & Co. v. Bowen, 192 S.E.2d 400 (Ga. Ct. App. 1972) lietā vērtspapīru brokeru firmas nosaukums, kas bija uzdrukāts uz apstiprinājuma veidlapas, kurā bija apstiprināta vērtspapīru pārdošana, tika atzīts par pietiekamu autentifikācijas līdzekli. Tiesa uzskatīja, ka firmas vārds nodrukāts ar nolūku apliecināt autentiskumu un tāpēc tas atbilst prasībai parakstīt apstiprinājumu.*

! *Beatty v. First Exploration Fund 1987 and Co. Limited partnership, 25 B.C.L.R.2d 377 (1988) lietā pa faksu nosūtīti paraksti uz pilnvarojuma dokumentiem tika atzīti par pietiekamiem, lai tos uzskatītu par pienācīgi parakstītiem saskaņā ar sabiedrības līgumu.*

Ja uz parakstu raugās kā uz vienkāršu simbolu, ar ko persona var apliecināt savu saistību ar dokumentu, tad iespējams identificēt vairākas elektroniskās parakstīšanas metodes. Pirmkārt, visvienkāršākais ir piestiprināt pašrocīga paraksta noskenētu attēlu, piemēram, *Word* programmā rakstītam dokumentam. Otrkārt, e–pastā "From" (latviešu valodā – "No") rindiņa sūtījuma sākumā parasti norāda, kurš ir vēstules sūtītājs. Šī rindiņa tiek piestiprināta vēstulei automātiski pēc tam, kad lietotājs ir atbilstīgi konfigurējis e–pasta programmu tā, lai tā parādītu vārdu. Šī metode ir visnedrošākā, jo ir diezgan vienkārši izmainīt konfigurāciju, norādot pavisam citu vārdu. Ir iespējams arī internetā radīt e–pasta pastkastīti ar pilnīgi izdomātiem personas datiem.

Treškārt, peles taustiņa nospiešana var nozīmēt līguma noteikumu pieņemšanu. Tādā interaktīvā vidē kā internets persona var noslēgt līgumu, nospiežot peles taustiņu uz norādītās ikonas. Lai precīzi norādītu, ka persona kļūst saistīta ar līguma noteikumiem, internetā parasti izmanto īpašas norādes. Piemēram, interneta lappusēs, kurās iespējams piekļūt ar autortiesībām aizsargātam materiālam, ir norādīts apmēram šāds teksts: "Ja jūs pieņemat šā licences līguma noteikumus, nospiediet šo taustiņu."

Ceturtkārt, e–pasta noslēgumu teksta formā var uzskatīt par parakstu. E–pasta sūtītājs var pabeigt savu sūtījumu ar nepārprotamu tekstu: "Paraksts: Agris Krūms" vai "Mans vārds šīs vēstules noslēgumā ir mans paraksts un norāda uz manu piekrišanu līguma noteikumiem. Agris Krūms". Šāds noslēgums noteikti ļautu izvairīties no pārpratumiem, vai teksts ir galīgs un nosūtītāju saistošs.

Piektkārt, elektronisku dokumentu var parakstīt, izmantojot biometrijas sasniegumus. Ar biometrijas izmantošanu elektroniska dokumenta parakstīšanā saprot kaut kā īpaši unikāla, personas darbībai vai uzvedībai raksturīga piestiprināšanu pie elektroniskā dokumenta. Viens no piemēriem ir zīmuļievades datoru *(pen–computer)* izmantošana. Šajos datoros var izmantot tehnoloģiju *PenOp*. Tā ir īpaša datorprogramma, ar kuras palīdzību tiek fiksēts personas paraksts un digitālā veidā piestiprināts dokumentam. Ar līdzīgu tehnoloģiju iespējams nodrošināt balss skaņu uztveršanu un piestiprināšanu digitālā veidā pie dokumenta. Biometrijas tehnoloģiju var izmantot acs tīklenes skenēšanai un pilnvarošanai.

Visbeidzot, elektronisko sūtījumu var parakstīt ar šifrēšanas līdzekļiem. Pamatoti tiek uzskatīts, ka šāda veida ciparparaksts ir funkcionāls ekvivalents ar roku rakstītajam parakstam.

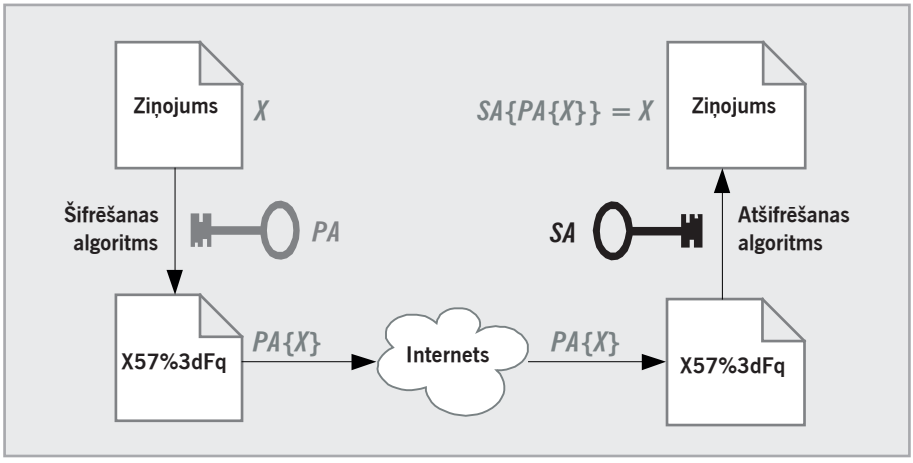
3.4.3. CIPARPARAKSTS

Lai izmantotu iespējas, ko sniedz internets un elektroniskā komunikācija, ir nepieciešama droša un uzticama komunikācijas vide. Elektroniskās komunikācijas drošības un uzticamības panākšanai izmanto vairākas metodes, kuru pamatā ir atšķirīgi šifrēšanas algoritmi. Ciparparaksti jeb digitālie paraksti palīdz pierādīt datu izcelsmi (datu autentiskums) un pārbaudīt, vai dati ir saņemti negrozītā veidā (datu integritāte). Šifrēšana nodrošina komunikācijas konfidencialitāti. Šo divu metožu tehnoloģija ir pamatā elektronisko dokumentu un elektronisko parakstu tiesiskajam regulējumam.

Ciparparaksts ir tehnoloģiski specifisks termins, kas apzīmē vienu elektronisko parakstu veidu, kurš izmanto publisko atslēgu kriptogrāfijas tehnoloģiju jeb *PKI (Public Key Infrastructure).* Publisko atslēgu kriptogrāfija izmanto algoritmu, kura pamatā ir divas atšķirīgas (asimetriskas), bet matemātiski saistītas šifra atslēgas. Viena atslēga tiek izmantota digitālā paraksta radīšanai vai datu pārvēršanai šifrētā sūtījumā, bet otru izmanto, lai pārbaudītu (verificētu) digitālo parakstu un atšifrētu sūtījumu tā oriģinālajā formā.

Publisko un privāto atslēgu infrastruktūras izmantošana var izpausties divējādi.

Pirmkārt, to izmanto ziņojumu šifrēšanai. Pieņemsim, ka PA ir lietotāja A privātā atslēga, bet SA – viņa publiskā atslēga. Lietotājs A grib sūtīt ziņojumu lietotājam B. Lai lietotājs B būtu drošs, ka ziņojumu ir sūtījis lietotājs A, lietotājs A to šifrē ar savu privāto atslēgu. Publiskā atslēga ir visiem pieejama. Tātad, kad ziņojums nonāk pie lietotāja B, viņš ar lietotāja A publisko atslēgu pārliecinās, ka to ir sūtījis tieši A. Un, tā kā privātā atslēga ir zināma tikai tās īpašniekam, mēs varam būt droši, ka neviens cits par viņu nevar uzdoties.

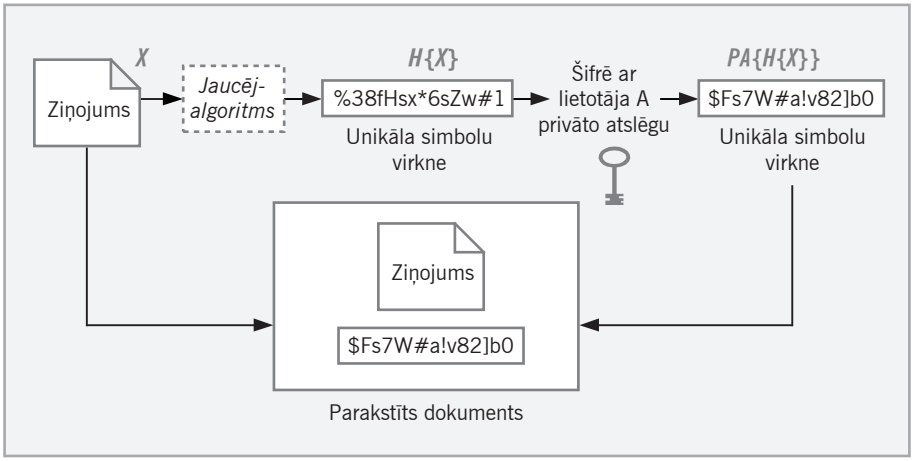


4. att. Šifrēto ziņojumu sūtīšana.

Savukārt, ja lietotājs A gribētu nevis identificēt sevi kā autoru, bet panākt to, lai viņa sūtījumu varētu izlasīt tikai un vienīgi lietotājs B, tad viņš šo ziņojumu šifrē ar lietotāja B publisko atslēgu. Tādējādi, kad ziņojums nonāks pie lietotāja B, to atšifrēt būs iespējams tikai viņam.

Otrkārt, *PKI* tiek izmantota elektronisko parakstu veidošanai, kuru pamatā ir šifrēšana ar asimetriskām atslēgām.

Dokumenta parakstīšanas process nav vienāds ar dokumenta šifrēšanas procesu. Dokumenta šifrēšanai ir pavisam cits mērķis (pamatā nodrošināt konfidencialitāti). Parakstīšanā lietotājs vēlas identificēt sevi, iespējams, nemaz nešifrējot dokumentu. Dokumenta šifrēšana ir ļoti laikietilpīgs process – jo lielāks dokuments, jo ilgāk notiek tā šifrēšana, un tādējādi ne vienmēr tas ir lietderīgi. Tāpēc, lai izveidotu parakstītu dokumentu, lietotājs A sākumā ar

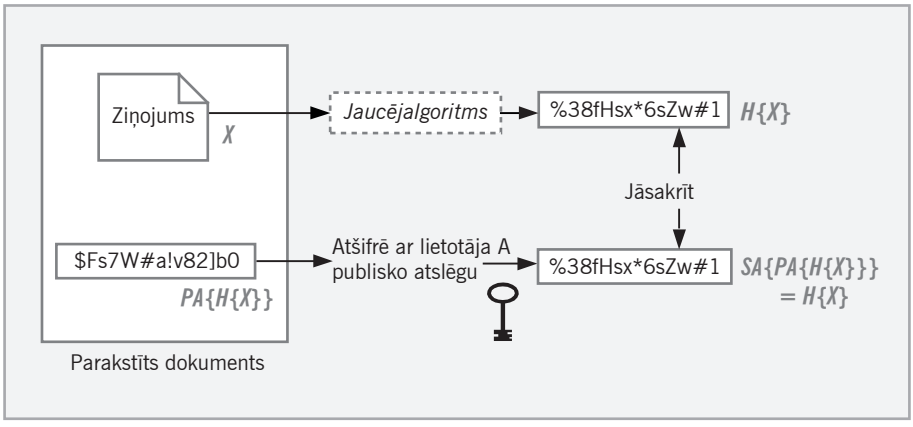


5. att. Ziņojumu parakstīšana.

speciālas jaucējfunkcijas *(hash function)* palīdzību iegūst unikālu simbolu virkni (H{X}), ko sauc par īssavilkumu *(digest)*, un šifrē to ar savu privāto atslēgu (PA{H{X}}). Iegūtais šifrētais īssavilkums tiek pievienots ziņojumam.

Kad lietotājs B, saņemot parakstītu ziņojumu, vēlas pārbaudīt, vai šo ziņojumu patiesi ir parakstījis lietotājs A, viņš atšifrē īssavilkumu ar pieejamo lietotāja A publisko atslēgu (SA{PA{H{X}}} = H{X}) un salīdzina iegūto ar īssavilkumu, ko iegūst, lietojot jaucējfunkciju saņemtajam ziņojumam (H{X}). Abiem īssavilkumiem ir jāsakrīt.

Personai, kas nav lietojusi elektronisko parakstu, šis process var likties visai sarežģīts. Tomēr dzīvē viss notiek daudz vienkāršāk. Elektroniskā paraksta veidošanas tehnoloģijas nodrošina visu iepriekš minēto algoritmu lietošanu tā, ka lietotājam nav pašam jāveido jaucējfunkcijas radītie īssavilkumi un nav pašam jāpārbauda, vai ziņojuma paraksts ir īstais. Dažas tehnoloģijas īssavilkumu pievieno dokumenta datnei, dažas veido to kā papildu datni, piemēram,



6. att. Parakstīto dokumentu atšifrēšana.

ar .sig paplašinājumu. Uzklikšķinot uz šīs datnes, lietotājs var pārliecināties, vai paraksts ir īsts, izlasīt paraksta sertifikāta datus un derīguma termiņu, kā arī pārliecināties, vai ir nodrošināta dokumenta integritāte, t. i., dokuments nav mainīts. Elektroniskā paraksta algoritmi ir starptautiski standartizēti, tāpēc dažādu tehnoloģiju veidotie paraksti ir lietojami dažādās sistēmās un platformās, piemēram, elektroniski parakstītā e-vēstule var būt atpazīta gan *Microsoft Outlook* e-pasta sistēmā, gan *Lotus Notes* e-pasta sistēmā.

Aplūkojot vēlreiz elektronisko dokumentu parakstīšanas procesu, rodas jautājums: ja mēs nepazīstam ziņojuma sūtītāju, kā lai mēs uzticamies viņa parakstam? Kurš veido šos parakstus? Runājot par kādu noteiktu organizāciju, šī problēma var tikt atrisināta vienkāršā veidā – katram organizācijas darbiniekam tiek izsniegti sertifikāti, un darbinieki savā starpā uzticas cits citam. Bet valsts līmenī vai pasaules līmenī – kā lai mēs zinām, kurš ir kurš?

Problēmas risinājumā ir paredzēta trešā puse – sertifikācijas pakalpojuma sniedzējs. Tā ir iestāde, kas pirms sertifikāta izsniegšanas pārbauda personas dokumentus (piemēram, pasi). Šo sertifikātu sertifikācijas iestāde paraksta ar savu privāto atslēgu, lai nodibinātu saikni ar atslēgas īpašnieku. Izmantojot sertifikācijas iestādes publisko atslēgu, ikviens var noskaidrot sertifikāta informāciju. Sertifikācijas pakalpojumu sniedzējs uztur sertifikātu lietotāju publiskās atslēgas un informāciju par nederīgiem sertifikātiem. Tomēr ir ļoti svarīgi, lai sertifikācijas iestāde būtu uzticama.

Sertifikāts var būt šāda informācija par publiskās atslēgas īpašnieku:

- parakstītāja vārds vai nosaukums;
- sertifikācijas iestādes nosaukums;
- parakstītāja publiskā atslēga;
- atslēgas veids;
- personas nodarbošanās;
- personas amats organizācijas iekšienē (piemēram, direktors, nodaļas vadītājs u. tml.);
- izsniegtās licences dažādām darbībām vai kvalifikācijas dokumenti (piem., ārsta licence);
- oficiālie apstiprinājumi (transporta vadītāja apliecība un dati par to);
- apdrošināšanas vai ar sertifikātu parakstāmo saistību apjoms naudas izteiksmē;
- sertifikāta darbības termiņš.

Saraksts nav izsmeļošs, un atkarībā no izmantojamās jomas sertifikātā vēl var iekļaut dažādu informāciju par paraksta īpašnieku.

Ciparparaksti var būt funkcionāli ekvivalenti ar roku rakstītiem parakstiem. Ciparparakstus var lietot šādos procesos:

- oficiālajā komunikācijā starp valsts pārvaldes iestādēm, kā arī starp valsts pārvaldes iestādēm un privātajām personām;
- līgumiskajās attiecībās, slēdzot līgumus starp privātajām personām;
- vienīgi identifikācijas un pilnvarošanas nolūkā, piemēram, lai pieslēgtos noteiktai datu bāzei un saņemtu noteiktu informāciju;
- slēgtās sistēmās, piemēram, korporatīvajā tīklā;
- personiskos nolūkos vienkāršā sarakstē starp dažādām personām.

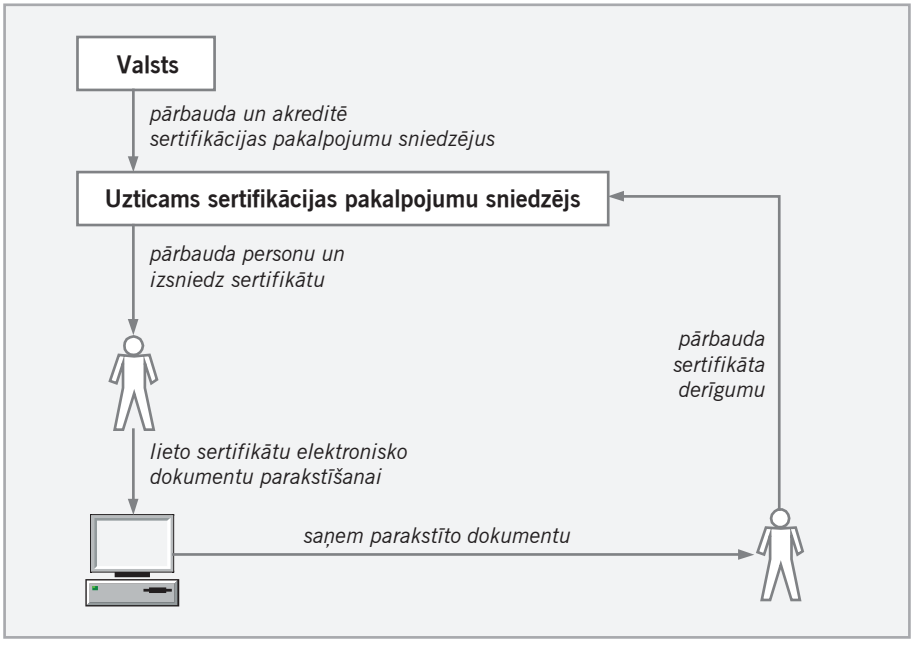
3.4.4. ELEKTRONISKO DOKUMENTU LIKUMS

Elektronisko dokumentu likums Latvijā tika pieņemts 2002. gada 31. oktobrī. Likums stājās spēkā 2003. gada 1. janvārī. Savukārt pārejas noteikumi nosaka, ka valsts institūcijām ir pienākums pieņemt elektroniskos dokumentus no fiziskām un juridiskām personām ne vēlāk kā 2004. gada 1. janvārī.

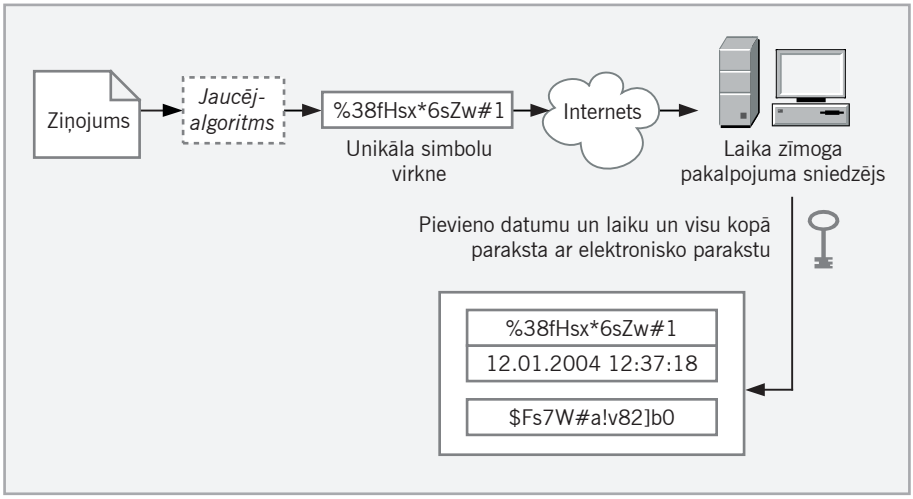
Elektronisko dokumentu likums sniedz ne tikai e-dokumentu definīciju, bet arī nosacījumus to juridiskai atzīšanai. Tas nosaka, kādā veidā Latvijas Republikā var tikt nodrošināta elektronisko dokumentu parakstīšana.

Likumā ir lietoti attiecīgi termini.

- Droši elektroniskā paraksta radīšanas līdzekļi – programmatūra, aparatūra un elektroniskā paraksta radīšanas dati, kas atbilst visām šādām prasībām:
  - tie var rasties tikai vienreiz, un ir nodrošināta to slepenība,
  - tos nevar atvasināt, un tie ir nodrošināti pret viltošanu,
  - tie ir droši aizsargāti pret nelikumīgu izmantošanu no trešo personu puses,
  - tie nemaina elektronisko dokumentu kā tādu un neliedz iepazīties ar to pirms parakstīšanas.
- Drošs elektroniskais paraksts – elektroniskais paraksts, kas atbilst visām šādām prasībām:
  - tas ir piesaistīts vienīgi parakstītājam,
  - tas nodrošina parakstītāja personas identifikāciju,
  - tas ir radīts ar drošiem elektroniskā paraksta radīšanas līdzekļiem, kurus var kontrolēt tikai parakstītājs,



7. att. Elektronisko sertifikātu nodrošināšana.



8. att. Laika zīmoga piestiprināšana.

- tas ir saistīts ar parakstīto elektronisko dokumentu tā, lai vēlākas izmaiņas elektroniskajā dokumentā būtu manāmas,
- tas ir apliecināts ar kvalificētu sertifikātu.

- Uzticams sertifikācijas pakalpojumu sniedzējs – fiziskā vai juridiskā persona, kas ir akreditēta sniegt sertifikācijas pakalpojumus.

Likums nosaka kārtību, kādā Latvijas Republikā var darboties sertifikācijas pakalpojumu sniedzēji (ar sertifikācijas pakalpojumu sniegšanu ir jāsaprot elektroniskā paraksta nodrošināšana), to darbības uzraudzības pasākumus, nosacījumus elektroniskiem parakstiem, kā arī paredz noteikumus starpvalstu elektronisko dokumentu parakstu atzīšanai.

Tiesību akti paredz, ka dokumentam juridiska spēka iegūšanai papildus citiem rekvizītiem nepieciešams arī zīmoga nospiedums. Šī prasība attiecībā uz elektronisko dokumentu ir izpildīta ar drošu elektronisko parakstu un laika zīmogu. Šeit laika zīmogs apzīmē parakstīšanas brīža datumu un laiku, kuriem ir jābūt uzticamiem, t. i., iegūtiem nevis no lietotāja datora, bet gan no uzticama laika zīmoga pakalpojumu sniedzēja (*Time Stamping Authority, TSA).*

Viens no laika zīmoga uzlikšanas paņēmieniem ir šāds: ja lietotājs vēlas uzlikt laika zīmogu uz sava dokumenta, viņš nosūta dokumenta īssavilkumu, kas iegūts ar jaucējfunkcijas palīdzību, laika zīmoga pakalpojumu sniedzējam (tas reizē var būt arī sertifikācijas pakalpojumu sniedzējs). Savukārt laika zīmoga pakalpojumu sniedzējs pievieno tam datumu un laiku un visu kopā paraksta ar elektronisko parakstu, t. i., šifrē ar savu privāto atslēgu. Tādējādi laika zīmoga pakalpojuma sniedzējs apstiprina to, ka dokuments ir eksistējis pirms laika zīmoga uzlikšanas.

Katram paraksta sertifikātam eksistē derīguma termiņš. Tādējādi var rasties problēma ar elektroniska dokumenta spēkā esamības pārbaudi. Tāpēc likums pieprasa, lai laika zīmogu būtu iespējams pārbaudīt arī pēc paraksta sertifikāta derīguma termiņa beigām, kā arī pēc iespējamās sertifikācijas vai

laika zīmoga pakalpojumu sniedzēja darbības pārtraukšanas. To var realizēt, publicējot visus izsniegtos sertifikātus un laika zīmogus kādā uzticamā izdevumā.

3.5. KONTROLJAUTĀJUMI

1. Nosauciet dokumenta atribūtus!
2. Kas ir diplomātika?
3. Kāds dokuments ir autentisks?
4. Nosauciet atšķirības starp elektroniskiem un parastiem dokumentiem!
5. Kas ir droši elektroniskā paraksta radīšanas līdzekļi?
6. Kas ir drošs elektroniskais paraksts?
7. Kas ir uzticams sertifikācijas pakalpojumu sniedzējs?

4. INFORMĀCIJA, TĀS ATKLĀTĪBA, TIESĪBAS IEGŪT UN IZPLATĪT INFORMĀCIJU

Nodaļa izstrādāta, izmantojot [1, 137.–146. lpp., 13].

4.1. KAS IR INFORMĀCIJA?

Jau pašā nosaukumā "informācijas un komunikācijas tehnoloģijas nozares" izskan vārds "informācija" – tā ir informācija par cilvēkiem, kura glabājas kādas organizācijas datu bāzē, tās ir avīžu slejas, kuras daudzi cilvēki lasa internetā, tās ir elektroniskas enciklopēdijas, tās ir vēstules, kas ceļo no viena pasaules gala uz otru, – tā ir bezgala dažāda informācija, kas glabājas vai tiek raidīta ar datora palīdzību.

Vēl viens plaši pazīstams termins, kas saistīts ar informāciju, ir dati. Dati ir informācija, kas tiek uzglabāta skaitļu, burtu un simbolu veidā [14]. Eiropas Padomes Kibernoziegumu konvencijā termins "dati" ir definēts kā „jebkurš faktu, informācijas vai satura attēlojums, kas derīgs datu pārraides procesam" [15]. Enciklopēdiskajā vārdnīcā jūs atradīsiet arī vispārīgu informācijas definīciju – „informācija ir cilvēkam izmantojamu ziņu, datu kopums (valodas vārdi, attēli, skaņas, matemātiski simboli), kas iekodēts kādā materiālā nesējā" [16]. Šajā grāmatā termini "dati' un "informācija" pārsvarā tiek lietoti kā sinonīmi.

Ar datiem ir saistīts arī termins "datu bāze". Liels daudzums datu tiek glabāti speciālās datu glabātavās – datu bāzēs, kuras ir pamatā gandrīz katram informācijas sistēmu risinājumam. Juristi īpaši izceļ šīs informācijas krātuves arī likumdošanā: tās tiek definētas kā „neatkarīgu darbu, datu vai citu materiālu krājums, kas sakārtots sistemātiski vai metodiski un individuāli pieejams elektroniskā vai citādā veidā" [17].

4.2. INFORMĀCIJAS REGULĒŠANA

Informācija pārtop par tiesību objektu tikai tad, ja tās lietošana rada, groza vai izbeidz noteiktas tiesiskās attiecības. Piemēram, ja informācija ir publicēta grāmatā, tad ar tās publicēšanu autoram rodas noteiktās tiesiskās attiecības, jo viņa vārdu un darbu aizsargā autortiesības. Lai informācija varētu radīt noteiktas tiesiskas sekas, tā ir jāatzīst par tiesību objektu.

! *Latvijā ļoti populāra kļuvusi kompromitējošas informācijas publicēšana, sevišķi pirmsvēlēšanu laikā. Šāda veida informācijas publicēšanai vienmēr ir negatīvas sekas, un tāpēc ir ļoti svarīgi, lai informācija būtu patiesa. No vienas puses, informācijai ir jābūt atklātai, un vēlētājam ir tiesības to iegūt. No otras puses, informācijas publicēšana šajā gadījumā var nodarīt nopietnus zaudējumus, un par tās patiesumu atbildība ir jāuzņemas informācijas izplatītājam.*

Darbības ar informāciju tiek regulētas ar vairākiem tiesību aktiem, kuros informācija, informācijas sistēmas, informācijas apstrādes uzraudzības institūcijas parādās kā galvenais objekts vai blakus objekts un ar kuriem tiek regulētas dažāda veida darbības ar informāciju – tās iegūšana, nodošana, izplatīšana, publicēšana, uzglabāšana, reģistrācija u. c.

4.3. INFORMĀCIJAS ATKLĀTĪBA

4.3.1. INFORMĀCIJAS TIESĪBAS UN CILVĒKTIESĪBAS

Cilvēktiesību kopums ir savstarpēji saistītu tiesību normas, kas pamatos nosaka indivīda stāvokli sabiedrībā un valstī. Cilvēktiesību kopuma "kodolā" ir politiski, filozofiski, reliģiski un juridiski pamatots priekšstats par cilvēku "kā visu lietu mēru", kam piemīt "dabiskā cieņa". Cilvēka cieņa vispirms nozīmē iekšējo domu un uzskatu brīvību. Savukārt domu brīvība prasa ārējo izteiksmes jeb vārda brīvību, jo cilvēkam ir jābūt iespējām dalīties domās un uzskatos ar citiem. Cilvēktiesības ietver arī katra tiesības piedalīties valsts darbā, ietekmēt valstiskos procesus. Lai to varētu darīt, indivīdam ir tiesības iegūt informāciju, kas ir valsts rīcībā. Tomēr informācijas iegūšanai un izplatīšanai var noteikt ierobežojumus, lai aizsargātu kādas atsevišķas personas vai pat visas valsts intereses. Tāpat ikvienam cilvēkam ir arī tiesības uz savas privātās dzīves aizsardzību, tiesības uz to, ka ne visa informācija, ko viņš valstij ir uzticējis vai ko valsts par viņu ir uzzinājusi no citiem avotiem, tiks nodota atklātībai.

4.3.2. INFORMĀCIJAS ATKLĀTĪBAS JĒDZIENS

Kā jau minēts iepriekš, viens no informācijas tiesību aspektiem, kas skar cilvēktiesības, ir saistīts ar uzskatu un domu brīvību, bet, lai domu un uzskatu brīvība nebūtu ierobežota, nepieciešama informācijas brīvība – tiesības iegūt un izplatīt informāciju.

Šī brīvība ir ietverta gandrīz vai visos starptautiskajos cilvēktiesību pamatdokumentos. Tā, piemēram, ANO "Vispārējās cilvēktiesību deklarācijas" 19. pants nosaka, ka „ikvienam ir tiesības uz pārliecības un izteiksmes brīvību; šīs tiesības ietver brīvību bez iejaukšanās palikt pie saviem uzskatiem un meklēt, saņemt un izplatīt informāciju un idejas ar jebkuriem informācijas līdzekļiem neatkarīgi no valstu robežām". Līdzīgi šīs tiesības noteiktas arī ANO "Starptautiskajā paktā par pilsoņu un politiskajām tiesībām", "Eiropas Cilvēka tiesību un pamatbrīvību aizsardzības konvencijā". Pat bērnam saskaņā ar ANO "Bērnu tiesību konvencijas" 13. pantu „ir tiesības uz izteiksmes brīvību; šajās tiesībās ietilpst brīvība, neievērojot robežas, meklēt, saņemt un izplatīt jebkuru informāciju un idejas kā mutvārdos, tā rakstveidā vai iespieddarbā, mākslas darba formā vai arī jebkurā citā formā pēc bērna izvēles".

Tomēr visos šajos dokumentos noteikts arī tas, ka informācijas iegūšanas un izplatīšanas tiesības nav absolūtas. Tās var ierobežot ar likumu, ja šāds ierobežojums nepieciešams, lai aizsargātu citu cilvēku cieņu, morāli vai citas valstij vai sabiedrībai nozīmīgas intereses.

Kaut arī saskaņā ar likumu informācijas tiesības var ierobežot, šāds ierobežojums – tāpat kā attiecībā uz citām cilvēktiesībām – ir attaisnojams tikai tad, ja pēc tā ir akūta nepieciešamība, proti, aizsargātajām interesēm jābūt nozīmīgākām nekā indivīda tiesību aizskārumam, kas rodas ar konkrēto ierobežojumu. Par to, vai informācijas tiesību ierobežojums patiešām bijis nepieciešams, ir diezgan daudz diskusiju un tiesas spriedumu, arī Eiropas Cilvēktiesību tiesas spriedumu.

Turklāt izteiksmes brīvība nereti var nonākt pretrunā ar kādu citu vispāratzītu cilvēktiesību. Visbiežāk tā var konfliktēt ar tiesībām uz privāto dzīvi. Arī tiesības uz privāto dzīvi ir garantētas visos iepriekš minētajos cilvēktiesību dokumentos.

Kā raksta Māris Ruķers [18], personas, kas apstrādā personas datus, nodarbojas ar citu personu privātās dzīves faktu apstrādi. Lai novērstu nelikumīgu iejaukšanos privātajā dzīvē attiecībā uz personisko informāciju, personai ir tiesības saņemt informāciju un kontrolēt informāciju par sevi. Tiesības saņemt informāciju par sevi balstās uz privātās dzīves aizsardzības tiesībām, bet tiesības saņemt un izplatīt informāciju vispār balstās uz informācijas brīvību. Informācijas brīvības likumi piešķir tiesības saņemt informāciju par valsti, sabiedrību un zināmā apjomā arī par citu personu privāto dzīvi.

Tādējādi informācijas tiesības no cilvēktiesību viedokļa var aplūkot divos aspektos:

- kā tiesības meklēt un iegūt informāciju,
- kā tiesības izplatīt informāciju.

4.4. TIESĪBAS IEGŪT INFORMĀCIJU

Informācijas pieejamība vai informācijas brīvība ir jebkuras tiesiskas un demokrātiskas valsts stūrakmens. Ir jāatzīst, ka tikai labi informēta sabiedrība spēj saprātīgi veidot valsts dzīvi un kontrolēt iestāžu darbību. Tas ir demokrātijas pamatelements. Valsts pārvaldes darbībai ir jābūt tādai, lai stiprinātu demokrātiju arī šādā veidā – nodrošinot informācijas pieejamību.

Informācijas iegūšana tieši veido arī pamatu personas vārda brīvībai – ja cilvēkam ir liegta iespēja saņemt informāciju, tad viņam nevar veidoties patiesībā sakņots viedoklis, kuru viņš varētu paust atklātībā.

Informācijas atklātība veicina demokrātijas attīstību un sabiedrības uzticību valsts un pārvaldes institūcijām, turpretī informācijas slepenība veicina sabiedrības neuzticību parlamentam, visu līmeņu valsts iestādēm un veido labvēlīgu augsni slēgtai sabiedrībai un korupcijai. Korupcijas uztveres indekss liecina, ka Skandināvijas valstu iedzīvotāji jūtas korupcijas vismazāk apdraudēti. Kā viens no būtiskākajiem argumentiem zemajam korupcijas izplatības līmenim šajās valstīs minēta valsts pretimnākošā attieksme, nodrošinot maksimāli brīvu pieeju tās rīcībā esošajiem dokumentiem. Padarot pieejamu informāciju par lēmumu pieņemšanas procesu un noslēgtajiem darījumiem, informācijas atklātība ierobežo ierēdņu iespējas iesaistīties negodīgos darījumos. Piekļūšana informācijai par dažādu labumu (pabalsti, sociālā palīdzība u. tml.) iegūšanu no valsts institūcijām vai par pārvaldes mehānisma darbību un politisko

lēmumu pieņemšanas procesu rada ievērojamus ierobežojumus augstākajām amatpersonām vienpersoniski pieņemt lēmumus, kuru sagatavošana nav bijusi pietiekami caurredzama. Padarot lēmumu pieņemšanas procesu caurskatāmāku, ir iespējams noteikt tās instances, kurās šis process norit bez pietiekami rūpīgas izstrādes vai arī ir klajā pretrunā ar lietpratēju ieteikumiem.

Nodrošinot iespēju iegūt personiski nepieciešamo informāciju un iepazīt valsts iestāžu darbību, tiek veicināta iedzīvotāju uzticēšanās valsts institūcijām un aktīva līdzdarbība valsts dzīvē. Jo atklātāk valsts pārvalde darbojas, jo lielāka ir iedzīvotāju uzticība šai pārvaldei. To īpaši svarīgi ir apzināties sabiedrībā, kurā vēsturisku iemeslu dēļ nav uzticības valstij vai tā ir minimāla. Tāpēc pienākums sniegt informāciju sabiedrībai Latvijā ir jo būtisks.

Vairumā demokrātisko valstu piekļūšana informācijai ir regulēta tiesību aktos, bet šis tiesību regulējums ļoti atšķiras pat Eiropas Savienības valstīs. Tā, piemēram, Zviedrija ir vienā no galējiem spektra punktiem, bet Apvienotā Karaliste – pretējā polā. Neatkarīgi no likumdošanas svarīgākais nosacījums ir tiesisko normu pareiza ieviešana un piemērošana. Sistēmai ir jādarbojas tādējādi, lai tā neapgrūtinātu piekļūšanu informācijai. Jebkuri ierobežojumi ir rūpīgi jāpārdomā un skaidri jāformulē, un tiem ir jābūt balstītiem uz pamatotiem apsvērumiem. Indivīdiem ir jāzina, kā viņi var iegūt informāciju, un viņiem nav jāpaskaidro pieprasījuma iemesli.

Informācijas pieejamības jautājumi ietverti arī Latvijas tiesību normās. Piekļuve informācijai, kas ir valsts iestāžu rīcībā, izriet jau no Satversmes 1. un 2. panta. Šie panti nosaka, ka Latvija ir demokrātiska republika un ka Latvijā valsts vara pieder tautai. Saeimas deputāti, tiesneši un valsts pārvaldes amatpersonas ir sabiedrības pārstāvji, kas tautas uzdevumā veic tiem uzticētos pienākumus. Iegūdama savu amatu valsts pārvaldē, valsts amatpersona nekļūst par *virscilvēku*, tai ir tikai tās tiesības, kas piešķirtas ar kādu tiesību aktu. Tāpat amatpersona nekļūst par īpašnieci informācijai, kuru tā apstrādā vai uzglabā kā amatpersona. Šī informācija pieder valstij, tātad ikvienam, jo demokrātiska valsts nav amatpersonu, bet gan iedzīvotāju kopums. No tā izriet, ka ar informāciju, kas ir valsts rīcībā, tiesības iepazīties ir ikvienam, ja vien likums nenosaka, ka informācija ir slepena vai ierobežota kāda likumīgi pamatota iemesla dēļ, piemēram, valsts noslēpuma aizsardzības, privātās dzīves vai komercnoslēpumu aizsardzības dēļ. Vispārīgais informācijas atklātības princips ir šāds: "Atklāts ir viss, kas nav aizliegts ar likumu."

Jāpiebilst, ka padomju laikā informācijas slēpšana bija reāla nepieciešamība. Valsts varas aparāts bija atdalīts no sabiedrības vairākuma, sabiedrības pārstāvji, pat parlamenta deputāti, faktiski nevarēja ietekmēt valsts norises. Kaut arī padomju konstitūcijās bija ierakstītas visas politiskās tiesības un brīvības, arī informācijas brīvība, reāli tās netika īstenotas. Ar parastiem likumiem, partijas lēmumiem, dažādām instrukcijām un pat atsevišķu funkcionāru norādījumiem konstitūcijas panti, kas garantēja cilvēktiesību ievērošanu, tika padarīti par nepiemērojamiem. Informācijas blokāde bija viena no padomju diktatoriskā režīma garantijām. Tāpēc atklātības principa ieviešana būtiski veicināja Padomju Savienības sabrukumu.

Arī patlaban informācijas apmaiņa sekmē demokrātijas attīstību visā pasaulē. Tālruņa, datora, satelīta, interneta un citas tehnikas attīstības dēļ kļūst

arvien grūtāk īstenot informācijas blokādi, kas raksturīga dažādiem diktatoriskiem režīmiem. Tādējādi informācijas tehnoloģijas attīstība kļūst arī par demokrātijas un tiesiskas valsts garantiju.

! *Ķīnā interneta lietotāju ir nedaudz mazāk par 9 miljoniem, taču šajā valstī globālais datoru tīkls attīstās straujā tempā. Ir gan viens "bet" – Ķīnas valdība ir sapratusi, ko tās autoritātei nozīmē neierobežota piekļuve informācijas resursiem. Ir jau bijuši precedenti – kāda ciema zemnieki ar interneta palīdzību izplatījuši informāciju par sava korumpētā kompartijas priekšsēdētāja patvaļu. Arī ārpus valsts izraidītie disidenti izmanto interneta iespējas, lai darītu zināmu patiesību par komunistu izdarībām valstī. Ķīnas varas iestāžu iecere cīnīties pret šo parādību ir drīzāk tuvredzīga nekā oriģināla. Šīs iestādes nolēmušas, ka valsts drošības orgāniem ir jāpārņem savā kontrolē visas aktivitātes, kas notiek Ķīnas internetā. Piemēram, ierēdņi lasīs valstī cirkulējošos e–pasta ziņojumus. Lai arī tīri tehniski šāda iespēja patiešām pastāv, eksperti uzskata, ka nezin vai būs iespējams visu izkontrolēt, ņemot vērā milzīgos attīstības tempus, kas vērojami Ķīnas datortīklā.*

Atgriežoties pie Latvijas konstitucionālajām tiesībām, jāņem vērā ka Satversmes 100. pantā ir noteikts, ka ikvienam ir tiesības uz vārda brīvību, kas ietver tiesības brīvi iegūt, paturēt un izplatīt informāciju. Savukārt Satversmes 104. pants nosaka ikviena tiesības vērsties valsts un pašvaldību iestādēs ar iesniegumiem un saņemt atbildi pēc būtības. Kārtību un termiņus atbildes sniegšanai uz iesniegumu nosaka likums "Iesniegumu, sūdzību un priekšlikumu izskatīšanas kārtība valsts un pašvaldību institūcijās". Attiecībā uz iesniegumiem par tās informācijas iegūšanu, kas tiesību aktos noteikto funkciju veikšanai ir valsts pārvaldes iestāžu un pašvaldību iestāžu rīcībā, 1998. gada 29. oktobrī Saeima pieņēma Informācijas atklātības likumu. Savukārt Ministru kabinets 1999. gada 3. augustā izdeva noteikumus Nr. 275 "Kārtība, kādā valsts pārvaldes iestāžu un pašvaldību iestāžu rīcībā esošā informācija nododama atklātībai". Šajos tiesību aktos atspoguļots iepriekš minētais atklātības princips (informācija ir pieejama sabiedrībai visos gadījumos, par kuriem likumā nav noteikts citādi), norādīti informācijas atklātības ierobežojumi, kā arī kārtība un termiņi informācijas sniegšanai.

Valsts informācijas pieejamību nosaka arī Satversmes 101. pants, kurā noteikts, ka ikvienam Latvijas pilsonim ir tiesības likumā paredzētajā veidā piedalīties valsts un pašvaldību darbā. Viens no šādiem likumiem ir likums "Par pašvaldībām". Tajā noteikts, ka pašvaldību domes vai padomes sēdes ir atklātas un tajās var būt klāt konkrētās pašvaldības iedzīvotāji; slēgtas sēdes var rīkot tikai izņēmuma gadījumos, kas norādīti likumā un pašvaldības nolikumā. Tāpat likumā noteikts, ka pilsētas domes un pagasta padomes lēmumiem, priekšsēdētāja rīkojumiem, revīzijas komisijas lēmumiem, kā arī pilsētas domes vai pagasta padomes atklāto sēžu protokoliem jābūt publiski pieejamiem, lai attiecīgās pašvaldības administratīvajā teritorijā dzīvojošās vai strādājošās personas, kā arī žurnālisti varētu bez maksas iepazīties ar šiem dokumentiem.

Daļēji pieejamību valsts informācijai nosaka arī Satversmes 115. pants, kurā minēts, ka valsts aizsargā ikviena tiesības dzīvot labvēlīgā vidē, sniedzot

ziņas par vides stāvokli. Šīs tiesības precizētas vairākos ar vides aizsardzību saistītos likumos, piemēram, likumā "Par vides aizsardzību", likumā "Par bīstamajiem atkritumiem", likumā "Par radiācijas drošību un kodoldrošību" un citos likumos, kā arī vairākos Ministru kabineta noteikumos. To, ka ziņas par dabas katastrofām un to sekām, kā arī vides stāvokli nevar būt valsts noslēpums, nosaka likums "Par valsts noslēpumu".

Attiecībā uz tiesībām iegūt informāciju jāmin arī Satversmes 90. pants, kurā noteikts, ka ikvienam ir tiesības zināt savas tiesības. Diemžēl šīs tiesības, turklāt daļēji, ir garantētas tikai 1994. gada 18. jūnija likumā "Par likumu un citu Saeimas, Valsts prezidenta un Ministru kabineta pieņemto aktu izsludināšanas, publicēšanas, spēkā stāšanās kārtību un spēkā esamību", kurā norādīts, ka visi tiesību akti ir publicējami oficiālajā preses izdevumā "Latvijas Vēstnesis". Diemžēl ne visiem Latvijas iedzīvotājiem bez maksas pieejamas datorizētās informācijas sistēmas vai citi sistematizēti tiesību aktu krājumi.

4.4.1. TIESĪBAS IEGŪT INFORMĀCIJU PAR APKĀRTĒJO VIDI

Saskaņā ar Eiropas cilvēktiesību tiesas praksi no Cilvēktiesību konvencijas 8. panta izriet arī tiesības iegūt informāciju par apkārtējās vides stāvokli un tās piesārņošanu. Tiesa ir noteikusi – ja ir radies vides piesārņošanas risks, personai, kura uzskata, ka viņu tas varētu ietekmēt, ir tiesības saņemt no atbilstošajām valsts institūcijām informāciju par šo risku. Tas saskaņā ar šīs tiesas viedokli izriet no tiesībām uz privātās dzīves neaizskaramību.

! *Itālijā kāda persona, kas dzīvoja netālu no ķīmiskās rūpnīcas, kura pārkāpa tehniskās prasības un kurā bija notikuši vairāki nopietni sprādzieni, sūdzējās, ka nevar iegūt informāciju par rūpnīcas radīto risku un pasākumiem, kas veikti pēc negadījuma. Pirmstiesas procesā komisija secināja, ka ir pārkāpts Konvencijas 10. pants (tiesības saņemt informāciju). Komisija arī noteica, ka informācijas pieejamība veselības un apkārtējās vides jautājumos ir ļoti svarīga un tāpēc valstij jāveic noteiktas darbības šīs informācijas nodrošināšanā. Tomēr tiesa, izskatot šo lietu, komisijas viedoklim nepiekrita, bet uzskatīja, ka Konvencijas 10. pants nerada valstij pienākumu ievākt un izplatīt konkrēto informāciju. Taču tiesa secināja, ka šajā lietā ir pārkāpts Konvencijas 8. pants – valsts, nenodrošinot attiecīgo personu ar būtisku informāciju par vides piesārņošanas risku un tā ietekmi, nav izpildījusi savu pienākumu nodrošināt personas privātās dzīves respektēšanu.*

4.4.2. PRESES BRĪVĪBA

Viens no informācijas brīvības aspektiem ir arī preses brīvība. Tas ir būtisks demokrātiskas politiskas iekārtas pamatelements. Politoloģijā reti var izveidot nepārprotamus "vienādojumus", bet viens no tādiem būtu šāds: ja pastāv preses brīvība, tad demokrātija ir iespējama; ja nepastāv preses brīvība, tad demokrātijas nav. Preses brīvībai demokrātiskā sabiedrībā ir divējāds raksturs. Tā ir gan institucionāla garantija, tāpat kā, piemēram, regulāras parlamenta vēlēšanas, politisko partiju brīvība, gan individuālas cilvēktiesības.

Lai preses brīvība varētu pastāvēt, žurnālistiem nepieciešama pieeja informācijai. Šo tiesību apjomu Latvijā nosaka "Preses likums" un likums "Par informācijas atklātību".

4.5. TIESĪBAS IZPLATĪT INFORMĀCIJU

Brīvība izteikt viedokļus, izjūtas un sniegt objektīvu informāciju ir priekšnosacījums pārējo cilvēka brīvību un tiesību īstenošanai. Tāpēc tiesības izteikt savu viedokli un tiesības izplatīt informāciju ir nostiprinātas visos cilvēktiesību dokumentos, kas skar politisko tiesību jomu.

Eiropas Cilvēktiesību tiesa ir noteikusi, ka tiesības paust savus uzskatus ir viens no demokrātiskas sabiedrības pamatelementiem, viens no šādas sabiedrības un katra cilvēka attīstības pamatnosacījumiem. Tiesības paust uzskatus attiecas ne tikai uz informāciju vai domām, kas ir labvēlīgas adresātam, bet arī uz tiem uzskatiem, kas aizskar, šokē vai uztrauc. Tas izriet no plurālisma un tolerances, bez kā demokrātiska sabiedrība nevar pastāvēt.

Par uzskatu paušanu dēvē gan politiskos izteikumus, gan dažādas mākslas izpausmes, gan ar uzņēmējdarbību saistītas informācijas izplatīšanu. Tā attiecas ne tikai uz vārdos ietvertu informāciju, bet arī uz gleznām, attēliem, skulptūrām, filmām, radio un televīzijas pārraidēm un citām informācijas izpausmēm.

Tomēr uzskatu paušanu var arī ierobežot, ja tā pārāk aizskar citu cilvēku tiesības vai sabiedrības intereses. Par uzskatu paušanu, pārkāpjot noteiktās robežas, valsts var pat noteikt civilās un arī krimināl ās sankcijas. Tomēr šādai atbildībai, it īpaši, ja paredzēta brīvības atņemšana vai ievērojams naudas sods, jābūt samērīgai ar nodarījumu, ņemot vērā, ka uzskatu paušanas tiesības ir demokrātijas stūrakmens un ierobežojamas tikai ļoti nopietnos gadījumos, kad tas patiešām ir nepieciešams.

Latvijā pēdējos gados ir uzbangojušas emocijas par to, cik kurš ir brīvs paust savu viedokli un kur ir robeža, aiz kuras sākas citu sabiedrības locekļu tiesību un brīvību aizskaršana. Šīs dilemmas risināšanā īpaša nozīme ir tiesu praksei – tai jālīdzsvaro indivīda tiesības uz vārda brīvību un sabiedrības tiesības uz informētību ar katra tiesībām uz goda un cieņas aizsardzību.

4.5.1. CIEŅAS UN GODA AIZSKARŠANA

Latvijā ir bijušas vairākas tiesas prāvas, kurās personas vērsušās ar sūdzībām par savas cieņas aizskārumu preses izdevumos un pieprasījušas kompensāciju no raksta autora un preses izdevuma, pamatojoties uz Civillikuma 2352.a pantu. Saskaņā ar Latvijas Republikas Augstākās tiesas 1993. gada 25. oktobra plēnuma lēmumu Nr. 9 prasītājam šādās lietās jāpierāda tikai godu un cieņu aizskarošu ziņu izplatīšanas fakts, taču tas, ka šis fakts atbilst patiesībai, jāpierāda tai personai, kas šīs ziņas izplatījusi. Nereti tiesa šīs prasības ir apmierinājusi.

! *Tiesa izskatīja pret laikrakstu "Diena" un tā komentētāju vērstu bijušā ekonomikas ministra prasību par goda un cieņas aizskaršanu. Bijušo ministru aizskāra "Dienā" publicētie komentētāja raksti, kuros tika pausts viedoklis,*

ka ministrs, cenzdamies panākt, lai kāds uzņēmums tiktu privatizēts par sertifikātiem, ir darbojies viena uzņēmuma interesēs un nodarījis valstij būtiskus zaudējumus. Ministrs neapstrīdēja, ka fakti ir patiesi, bet viņu aizskāris tonis, kādā žurnālists tos bija aprakstījis. Ministrs to dēvēja par apvainošanu, kas notikusi, „truli zākājoties un nemitīgi lietojot dažādas rupjības". Tiesa atzina, ka laikraksts ir aizskāris bijušā ministra godu un cieņu, un piedzina no tā kompensāciju.

Taču jāņem vērā, ka vārda brīvība aizsargā ne tikai viedokļa saturu, bet arī veidu, kādā tas tiek izklāstīts. Prese, paužot savu viedokli, var pieļaut pārspīlēšanu vai pat provocēšanu. Tomēr konkrēto apstākļu kontekstā vienmēr jāievēro proporcionalitāte starp preses tiesībām izteikties un nepieciešamību aizsargāt personas godu un cieņu. "Dienai" bija tiesības paust savus uzskatus par ministra darbību, un ministram bija tiesības apvainoties par kritiskajiem izteikumiem.

4.5.2. VALSTS NOSLĒPUMA UN KOMERCINFORMĀCIJAS AIZSARDZĪBA

Tāpat kā cieņu un godu aizsargā arī komercinformāciju un informāciju, kas satur valsts noslēpumu. Latvijas Krimināllikumā paredzēts krimināls sods par valsts noslēpuma izpaušanu (94. un 95. pants), neizpaužamu ziņu izpaušanu (329. un 330. pants), par ekonomisko, zinātniski tehnisko vai ar dienesta noslēpumu vai komercnoslēpumu saistītu neatļautu ziņu iegūšanu savai vai citas personas lietošanai vai izpaušanai, kā arī šādu ziņu neatļautu izpaušanu citai personai (200. pants) un sods par militāro ziņu izpaušanu (352. pants).

! *Informācijas izplatīšana, attīstoties tehnoloģijai, ir arī iespējama, izmantojot internetu, un tas var radīt un jau ir radījis nopietnus indivīda vai valsts interešu apdraudējumus. Tā kādā 1999. gada janvāra rītā tika uzlauzta Ministru kabineta oficiālā mājaslapa internetā (http://www.mk.gov.lv). Latvijas valsts ģerbonim pa virsu rēgojās uzraksts „hacked". Tālāk sekoja inteliģenti izsmējīgā "urķa" komentārs. Mājaslapu tas "greznoja" veselu stundu, atkārtojās vēl divas reizes, līdz mājaslapa tika izslēgta. Lielākoties visi komentāri pēc šā notikuma tika reducēti uz vienu – nekas īpašs nav noticis. Tomēr kāds komentārs bija tiešāks un nopietnāks: "Diemžēl neviena "atbildīgā persona" neiedomājās par to, cik nopietnas problēmas var radīt nevis kaut kādas mistiskas slepenas informācijas iegūšana, bet gan tādas savā būtībā oficiālas tribīnes kā Ministru kabineta tīmekļa lapas izmantošana, lai propagandētu rasu neiecietību vai pat fašisma ideoloģiju. Lappusi savos datoros var redzēt faktiski visa pasaule, tāpēc lokāls skandāls vienā mirklī var kļūt par starptautisku."*

Piemērā minētais komentārs ļoti labi ilustrē valsts interešu apdraudējumu, kādu var radīt ielaušanās tās informācijas sistēmā. Tādējādi šādos gadījumos būtu attaisnojama valsts iejaukšanās personas tiesībās paust savus uzskatus. Attaisnojama būtu gan atbildības paredzēšana, gan soda uzlikšana.

4.6. INTERNETS UN CENZŪRA

Sabiedrībai sasniedzot augstāku attīstības līmeni, pārstrukturējas arī noziedzība. Maldīgs ir uzskats, ka ekonomiski attīstītās valstīs noziedzība samazinās. Tieši šajās valstīs sākas kvalitatīvi jaunu noziegumu veidu attīstība. Lai cik tas būtu paradoksāli, taču patiesībā neviena valsts neiztiek bez cenzūras. Starpība ir tikai tā, ka vienā tā ir "caurspīdīga" un notiek stingrā sabiedrības kontrolē atbilstoši likumam, bet citā valstī tā ir dogmatiska.

Pasaulē ir zināmi daži mēģinājumi politiski reglamentēt un cenzēt interneta darbību. Ģeogrāfiski elektronu plūsmu norobežot nevar. Internetā ir apmēram 2 miljoni lapu ar pornogrāfiska rakstura informāciju. To skaits nevis samazinās, bet ar katru gadu, neskatoties uz preventīviem pasākumiem, palielinās.

ANO Starptautiskā pakta "Par pilsoniskajām un politiskajām tiesībām" 19. pantā ir teikts: "Katram cilvēkam ir tiesības netraucēti turēties pie saviem uzskatiem." Katram ir tiesības brīvi paust savus uzskatus. Šīs tiesības ietver brīvību meklēt, saņemt un izplatīt dažāda veida informāciju un idejas neatkarīgi no valstu robežām mutvārdos, rakstveidā, izmantojot presi vai mākslinieciskās izpausmes formas vai darot to citādā veidā pēc savas izvēles.

Šā panta 2. punktā paredzēto tiesību izmantošana uzliek īpašus pienākumus un īpašu atbildību. Tāpēc tā var būt saistīta ar zināmiem ierobežojumiem, taču tie jānoteic likumā, jo ir nepieciešami

- citu personu tiesību un reputācijas respektēšanai,
- valsts drošības, sabiedriskās kārtības, iedzīvotāju veselības un tikumības aizsardzībai.

4.6.1. CENZŪRAS ĪSS RAKSTUROJUMS

Vārds "cenzūra" ir cēlies no latīņu vārda *censura* (Senajā Romā amats, kuru pārstāvēja amatpersona – cenzors, kas sastādīja cenza sarakstus un pārraudzīja pilsoņu dzīvesveidu un viņu politisko uzticamību) un pēc būtības nav zaudējis savu nozīmi arī mūsdienās.

Plašākā nozīmē cenzūra nozīmē informācijas, ideju un mākslinieciskо izteiksmes līdzekļu aizliegšanu vai ierobežošanu, ko realizē valdības, baznīcas amatpersonas vai arī privātās cenzoru grupas. Šaurākā – juridiskā nozīmē jēdziens "cenzūra" apzīmē tikai darbību, ko veic oficiālas valsts amatpersonas, aizsargājot valstij svarīgas informācijas izplatīšanos plašsaziņas līdzekļos, kā arī ierobežojot un aizliedzot valstij un sabiedrībai kaitīgas informācijas izplatīšanos. Jebkuras valsts uzdevums ir radīt tādu sistēmu, kas, neierobežojot valsts pilsoņu tiesības uz vārda, runas un preses brīvību, aizsargā valsts noslēpumus, pilsoņu dzīvību, veselību, cieņu un godu. Eiropas Savienības Komisija savā ziņojumā Eiroparlamentam "Interneta izmantošanas nelegālais un kaitīgais saturs" [19] ir akcentējusi, ka ir ļoti svarīgi izstrādāt globālu preventīvu sistēmu, kas aizsargātu valstis un to pilsoņus no globālā datortīklā pārraidītās nelikumīgās un kaitīgās informācijas. Tas tika prezentēts ES Komisijā 1996. gada 27. septembrī, un līdz šim brīdim Eiropas Padomē un citās Eiropas Savienības institūcijās notiek pastāvīgas diskusijas par šo jautājumu.

Kas tad tā ir par informāciju, kura pieejama globālajā tīklā un kuras izplatīšanu un pieejamību būtu nepieciešams ierobežot? Cenzūras objektus internetā var iedalīt divās grupās:

- kaitīgajā informācijā un
- nelikumīgajā informācijā.

4.6.2. INTERNETA KAITĪGAIS SATURS

Speciālistus uztrauc interneta kaitīgā un nelikumīgā satura izplatība un iespējamās sekas. Visbīstamākais ir tas, ka internetam nav ģeogrāfisku robežu un tāpēc tikai vienā valstī pieņemtie pasākumi iedarbojas ļoti neefektīvi.

ES valstīs tiek diskutēts par dažādām prioritātēm, kas ir jāaizsargā valstij gan nacionālā, gan starpnacionālā līmenī. Šī aizsardzība ir jāsabalansē ar tiesībām uz brīvu informācijas plūsmu un garantētu publisko interešu aizstāvību. Tāpēc ir jāmēģina atbildēt uz jautājumiem – ko Eiroparlaments un ES eksperti uzskata par kaitīgu saturu, un vai jēdziens "kaitīgs" ir juridiska vai morāla kategorija?

Kā uzsvērts jau iepriekš pieminētajā ziņojumā, tad kaitīgums ir atkarīgs no tautu kultūras atšķirībām. Katrai valstij ir savas sabiedrībā akceptētas uzvedības normas, un iespējams, ka vienā valstī ir atļauts tas, kas ar likumu ir aizliegts citā. Vairākās valstīs par kaitīgu atzīst neonacistu informāciju, kā arī rasistu un homofobistu (neizprotamas bailes no cilvēka, nepatika pret homoseksuālismu un homoseksuāļu diskriminācija) sākumlapās ievietoto informāciju. Taču ne jau katrā valstī to precīzi aizliedz likums.

Kaitīgums ir sabiedriskās morāles jautājums, bet morāles norma ir "sociālo normu paveids, cilvēku uzvedības normu kopums, kas izsaka viņu savstarpējās attiecības un attieksmi pret sabiedrību. Morāles norma regulē cilvēka izturēšanos saskaņā ar vispārīgiem priekšstatiem un aizliegumiem, kas attiecināmi uz vienāda rakstura rīcību" [20].

4.6.3. INTERNETA NELIKUMĪGAIS SATURS

Nelikumīgs saturs nozīmē to, ka šādu informāciju aizliedz nacionālās vai starptautiskās tiesību normas. Tā, piemēram, nelicencētas programmatūras ievietotāji internetā kļūst par nelikumīga satura izplatītājiem, jo pārkāpj programmatūras izplatīšanas principus, kas noteikti autortiesību likumā.

Nelikumīgajā saturā ietilpst arī apmelošana, ķengāšanās, ielaušanās personas privātajā dzīvē un reputācijas aizskaršana vai pilsoņu tiesību ierobežošana ar uzmākšanos. Smagāko nelikumību saturu aizliedz krimināllikumi, bet aizliegumu var noteikt arī citas tiesību normas.

Eiropas Savienībā ir sagatavots dokuments "Par cilvēka goda aizsardzību audiovizuālajos un informatīvajos pakalpojumos", kurš iezīmē stingru pamatu ES politikā, lai nodrošinātu kvalitatīvu un efektīvu kontroli un arī stingri ievērotu cilvēka tiesības.

No vienas puses, dokumentā ir uzsvērta jauno komunikācijas tehnoloģiju attīstības nepieciešamība un nozīmīgums, bet, no otras puses, tas izvirza

prasības par jauno komunikācijas tehnoloģiju pakalpojumu izplatītāju un tīklu operatoru speciālo atbildību par cilvēka tiesību aizsardzību un demokrātisko vērtību nodrošināšanu. Tāpēc arī nacionālās valstis cenšas aizsargāties ar tehniskiem un likumdošanas līdzekļiem.

Internets pašreiz ir visu diskusiju stūrakmens, runājot par kriminālās informācijas izplatīšanu.

G-7 valstu Tieslietu un iekšlietu ministru komunikē uzsvērts: "Ar tradicionāliem iekšzemes līdzekļiem ir jāaizsargā mūsu pilsoņu drošība no starptautiskās organizētās noziedzības grupu darbības, ja viņi lieto globālās sakaru tehnoloģijas. Mūsu uzdevums ir ne tikai reaģēt uz starptautiskās noziedzības grupu aktivitātēm, bet arī paredzēt un novērst to pieaugumu."

To, ka ar Interneta starpniecību notiek noziedzīgas informācijas pārraidīšana un noziedzīgu kontaktu dibināšana starp starptautiskiem noziedzības sindikātiem, nevienam nav jāpierāda. Piemēram, minētās organizācijas vienojas par starptautisko sadarbību narkotiku kontrabandā.

Par krimināla rakstura informāciju, kuras plūsmu ir nepieciešams ierobežot, tiek uzskatīta informācija, kas saistīta ar terorismu, neķītru materiālu izplatīšanu, pornogrāfiju, naida kurināšanu.

TERORISMS

Neviena valsts pasaulē (vismaz oficiālajā valsts politiskajā doktrīnā) legāli neatbalsta terorismu. Taču terorisma draudi ar katru gadu kļūst aizvien nopietnāki. To pierāda terora akti Ziemeļīrijā, Kenijā, Tanzānijā un citās valstīs. Terorisms ir šaušalīgs noziegums, un nevar būt izņēmumu vainīgo personu saukšanai pie kriminālatbildības. G-7 dalībvalstis ir aicinājušas cīņu pret terorismu izvirzīt par absolūtu prioritāti visām pasaules valstīm, veikt profilaktiskus pasākumus pret terorismu, arī kavēt teroristu un to atbalstītāju aktivitātes, nepieļaut vardarbību un terorismu atbalstošu fondu veidošanu, kā arī informāciju par ieroču tirdzniecību. Patiesībā dalībvalstu līderi aicinājuši uz cenzūras izveidošanu nacionālo drošības interešu aizsardzības nolūkā. Datortiesību speciālisti pazīst "kiberterorismu", ko īsteno, izmantojot internetu.

! *Latvijā pazīstamākais "kibernoziegums" bija 1997. gadā atklātā bēdīgi slavenā "Viktora lieta", kur, izmantojot interneta elektronisko pastu, faktiski tika izdarīts terorisma mēģinājums, lai izspiestu naudu no Latvijas un Norvēģijas kopuzņēmuma "Varner Baltija".*

Izrādās, ka šādi terorisma akti notiek bieži – gan Eiropā, gan Amerikā. Šo valstu valdības līdz šim nav atradušas efektīvus pasākumus cīņai ar tiem.

Dažās interneta lapās ir sīki izklāstīts, kā izveidot vienkāršus masu iznīcināšanai paredzētus ieroču modeļus. Interneta lappusēs ikviens var atrast nepieciešamo informāciju, kā izgatavot vienkāršu, bet pietiekami jaudīgu spridzekli vai vēstuļu bumbu, kā ieprogrammēt vīrusu, tārpu vai citu ļaunprātīgu kodu, kas spēj pilnīgi vai daļēji sabojāt datorsistēmas un ne tikai tās.

Cenzūras pretinieki uzskata, ka šādu informāciju var iegūt arī bibliotēkās, un tās taču nevar aizliegt. Taču ir skaidrs, ka informācijas iegūšanā patērētais

laiks bibliotēkā ir nesamērojams ar to, kas ir jāpatērē, izmantojot internetu. Pietiek uzrakstīt frāzi „*How to make a bomb*", un jebkura meklēšanas programma izdod pāri par 100 mājaslapu adrešu, kur šī informācija ir brīvi pieejama. Bet cik grāmatu bibliotēkās būtu jāpārlasa, lai iegūtu šo pašu informāciju?

NEĶĪTRU MATERIĀLU IZPLATĪŠANA INTERNETĀ

1993. gadā krimināllietā "Kalifornijas štats pret Milleru" ASV Augstākā tiesa ieviesa aizlieguma standartus "neķītrībai" un "piedauzībai". Tiesa atzina, ka "neķītrības" attēlošanas aizliegums nevar tikt uzskatīts par ASV Konstitūcijas Pirmā labojuma pārkāpšanu. Tiesa noteica triju punktu testu neķītrības konstatēšanai:

- vidusmēra persona, kura atzīst mūsdienu sabiedrības standartus, uzskata, ka darbs kopumā aicina uz miesaskārību;
- darbs nepārprotami un skaidri attēlo vai nepatīkamā, uzmācīgā veidā apraksta seksuālu kontaktu;
- darbam kopumā trūkst nopietnas literāras, politiskas, zinātniskas, mākslinieciskas vērtības.

Kanādā publikācija ir atzīstama par "neķītru", ja tās saturā dominē nepiedienīga seksuāla izmantošana vai dzimumattiecības ir kombinētas ar noziegumiem, vardarbību, nežēlību, riebuma un pretīguma izraisīšanu.

PORNOGRĀFIJA

Pornogrāfija ir vulgāri naturālistisks, nepieklājīgs kailu cilvēku dzimumakta un to ģenitāliju attēlojums.

Latvijā dominē uzskats (to paudis arī bijušais Ministru prezidents Valdis Birkavs), ka pornogrāfija no erotikas atšķiras ar to, ka erotikai ir mākslinieciska vērtība un tajā netiek atklāti attēlotas seksuāli uzbudinātu vīriešu vai sieviešu ģenitālijas.

Gan Latvijas Krimināl kodeksa 209. pants, gan jaunā Krimināllikuma 166. pants, kas stājies spēkā 1999. gada 1. aprīlī, paredz atbildību par pornogrāfiska rakstura materiālu ievešanas, izgatavošanas vai izplatīšanas noteikumu pārkāpšanu. Tomēr Uldis Ķinis raksta, ka viņam tā arī nav izdevies sameklēt kaut vienu tiesas spriedumu par to, ka pēdējo gadu laikā kāda persona būtu notiesāta par šādu nodarījumu.

Bērnu pornogrāfija ir tas informācijas objekts, kuru nepieļauj nevienas valsts likumdošana. Visās valstīs par bērnu pornogrāfijas izplatīšanu ir paredzēta krimināl atbildība.

NAIDA KURINĀŠANAS LITERATŪRA

Neviens nav jāpārliecina par to, ka nacisms ir visekstrēmākais nacionālisma veids. Nacisma atdzimšanu visas valstis uzskata par nepieļaujamu. Īpaši stingri noteikumi šajā jomā ir Vācijā, un tāpēc tieši šajā valstī tiek izvērsta nesaudzīga cīņa ar labējiem ekstrēmistiem. Vācijas prokuratūra ne tikai ir bloķējusi *Compuserve* informācijas lapas, uzskatot, ka tās ietver informāciju, kas sēj rasu naidu un propagandē nacismu, bet arī citas norādes uz interneta lapām.

Rasisma propaganda ietver informāciju, kas kurina rasu naidu. Minētās mājaslapas propagandē dažādu tautu / rasu pārākumu un slavē rasismu visdažādākajās tā formās.

Homofobijas lapas kurina naidu pret homoseksuāļiem. Tajās ir sniegta nepatiesa informācija par šo parādību ar mērķi panākt sabiedrības nepatiku un noliegumu. Latvijā šī parādība nav izplatīta.

Par šādu literatūru varētu uzskatīt arī dažādu veselībai un dzīvībai kaitīgu reliģisku sektu darbības propagandu.

4.6.4. NEPILNGADĪGO INTEREŠU AIZSARDZĪBA

Interneta pieejamība Latvijas skolās arvien pieaug. Tas stimulē bērnus mācīties angļu valodu un iegūt ļoti daudz izziņas materiālu. Taču satrauc tas, ka skolās neviens tā pa īstam neuzrauga, ar ko bērni internetā nodarbojas.

Sarunā ar datorspeciālistiem, kas apkalpo skolu tīklus, ir dzirdētas sūdzības par to, ka ar pašreizējiem līdzekļiem faktiski nav iespējams izkontrolēt, ko nepilngadīgais dara interneta pieslēguma laikā. Tā kā nereti skolas datorā tiek ielādētas programmas no interneta bez jebkādas pārbaudes, no ierindas iziet arī skolu datoru tīkli.

Jebkurai sistēmai, kas aizsargā nepilngadīgo vajadzības, saprātīgā veidā ir jānodrošina, ka nepilngadīgajiem normālos apstākļos nav iespējama pieeja tādiem materiāliem, kas var traucēt viņu fizisko un garīgo attīstību.

Tā nav tikai Latvijas problēma. Ne jau velti gan Eiropas Padomē, gan Eiropas Savienībā, gan citās starptautiskajās institūcijās strādā speciālisti, lai pieņemtu attiecīgus dokumentus, kas nodrošinātu bērnu tiesību pilnvērtīgu aizsardzību. Latvijas likumdošana paredz, ka ir aizliegts bērnam demonstrēt, pārdot, dāvināt, izīrēt, propagandēt rotaļlietas, videoierakstus, laikrakstus, žurnālus un cita veida publikācijas, kurās propagandēta cietsirdīga uzvedība, vardarbība, erotika, pornogrāfija un kuras rada draudus bērna garīgajai attīstībai.

Tātad Latvija formāli ir ievērojusi ES un EP izstrādātās direktīvas bērnu tiesību aizsardzībā. Šī likuma izpildi sabiedrība var kontrolēt tikai publiskās vietās, t. i., kinoteātros, videozālēs, bibliotēkās un skolās. Tomēr, kā atzīmē arī eksperti, vienotas receptes visiem gadījumiem nav, jo katrai darbībai var piemērot pretdarbību.

4.7. KONTROLJAUTĀJUMI

1. Kas, jūsuprāt, ir informācija?
2. Kādi tiesību akti regulē tiesības iegūt un izplatīt informāciju?
3. Kādās kategorijās iedala informāciju, un kā tā tiek regulēta atkarībā no kategorijas?
4. Vai drīkst paust aizvainojošas ziņas par citiem cilvēkiem?
5. Kādas informācijas izplatīšana internetā ir aizliegta?

5. INTELEKTUĀLAIS ĪPAŠUMS

Nodaļa izstrādāta, izmantojot [1, 206.–241. lpp., 21, 22].

5.1. INTELEKTUĀLĀ ĪPAŠUMA JĒDZIENS

Juridiskajā literatūrā nav precīzas un universālas intelektuālā īpašuma definīcijas. Vispasaules Intelektuālā īpašuma organizācijas *(WIPO – World Intellectual Property Organization,* turpmāk tekstā – VIĪO) mājaslapā intelektuālais īpašums raksturots kā "*..īpašums, kas sevī apvieno: patenttiesības, autortiesības un blakustiesības, preču zīmes un ģeogrāfiskās izcelsmes norādes, dizaina paraugu tiesības, tehnoloģiju nodošanas kārtību utt.*". Vienkārši runājot, intelektuālais īpašums ir intelektuālā darba galaprodukts.

! *Tā kā intelektuālā īpašuma objekts ir intelektuālā darba galaprodukts, par to nevar kļūt, piemēram, galds. Galds ir fiziska darba rezultāts. Tomēr, ja runa būtu par pirmo galdu pasaulē, tad ideju izveidot objektu, kurš kalpotu kā darba virsma, var noteikti pieskaitīt pie intelektuālā īpašuma. Par intelektuālo īpašumu visbiežāk uzskata literāros darbus (grāmatas, rakstus u. tml.), vizuālās mākslas darbus (gleznas, fotogrāfijas, arī datorgrafikas attēlus u. tml.), muzikālus darbus un arī datorprogrammas.*

Kibertiesībās un citos ar informācijas tehnoloģijām saistītos jautājumos pasaulē nav vienotas izpratnes, izņēmums nav arī intelektuālā īpašuma joma. Jautājumā par intelektuālā īpašuma nodibināšanas faktu pasaulē ir atšķirīgas pieejas:

- par intelektuālo īpašumu ir jāuzskata tikai pabeigts darbs, kam pievienota intelektuāla vērtība;
- par intelektuālo īpašumu atzīstams arī intelektuālā darba process, kura rezultātā tiek radīts galaprodukts;
- par intelektuālo īpašumu ir atzīstamas arī idejas.

Patlaban par dominējošo viedokli pasaulē jāatzīst pirmā pieeja – par intelektuālā īpašuma objektu ir atzīstams darba rezultāts, bet netiek atzīts kā patstāvīgs intelektuālā īpašuma objekts tur ieguldītais darbs un idejas. Šādu viedokli atbalsta lielākā daļa tiesību speciālistu. VIĪO skaidro, ka par intelektuālā īpašuma objektu darbs atzīstams tikai no tā pabeigšanas brīža. Tomēr pasaulē diskusijas šajā jomā joprojām turpinās, un pamatu šīm diskusijām rada tieši intelektuālā īpašuma objektu izmantošanas problēmas kibertelpā.

Jāsecina, ka VIĪO apzināti nav devusi izsmeļošu intelektuālā īpašuma definīciju, jo tādā veidā ir iespējams izvairīties no kolīzijām, ko var radīt dažādu tiesību sistēmu doktrīnas intelektuālā īpašuma jautājumos. Tas, vai attiecīgais objekts ir intelektuālais īpašums, ir jāvērtē katrā konkrētā gadījumā tiesai vai citai tās statusam pielīdzinātai institūcijai. Tāpēc VIĪO min zināmās intelektuālā īpašuma nozares, atstājot iespēju jebkurā brīdī definīciju papildināt ar jaunu virzienu, kas varētu rasties intelektuālā īpašuma aizsardzības jomā.

Skaidrojumā ietverti šobrīd zināmie intelektuālā īpašuma veidi, bet tiek atstāta iespēja pievienot definīcijai jaunus veidus, kas rodas vai var rasties nākotnē. VIĪO faktiski ir devusi tikai intelektuālā īpašuma objektu uzskaitījumu un nav mēģinājusi precīzi definēt intelektuālā īpašuma saturu.

Intelektuālais īpašums ir personai zināmās informācijas apstrādes galarezultātā radītais produkts. Vārds "apstrāde" šajā gadījumā nozīmē ne tikai datu apstrādi, bet arī konkrētu priekšmetu vai lietu visdažādāko apstrādi. To raksturo informācijas radīšanā ieguldītais intelektuālais darbs un darba rezultātā radītais produkts.

5.2. INTELEKTUĀLĀ ĪPAŠUMA TIESISKĀ REGULĒŠANA

Tiesiskais regulējums intelektuālā īpašuma tiesībās pasaulē ir ļoti atšķirīgs. Viens no šo atšķirību cēloņiem ir dažādās valstu tiesību sistēmas.

Latvijā jautājumus, kas saistīti ar intelektuālā īpašuma autortiesību un blakus tiesību objektu aizsardzību, galvenokārt regulē Autortiesību likums un Patentu likums. Autortiesību likums aizsargājamo objektu lokā ir iekļāvis arī datorprogrammas un datu bāzes un noteicis to aizsardzības pasākumus.

Jautājumus, kas ir saistīti ar preču zīmēm, patentiem un ģeogrāfiskajām norādēm, koordinē un uzrauga Tieslietu ministrijas pārraudzībā esošā Patentu valde, savukārt lietas, kas saistītas ar autortiesībām un blakus tiesībām, ir Kultūras ministrijas atbildībā.

5.3. PATENTU LIKUMS

Latvijas Patentu likums [23] stājās spēkā 1993. gadā. Likums paredz izgudrojumu patentēšanas noteikumus un regulējumu. Atšķirībā no Autortiesību likuma Patentu likums aizsargā nevis intelektuālā īpašuma materiālo formu, bet gan tā ideju.

Katrā valstī eksistē patentu biroji, kuri nodarbojas ar izgudrojuma patenta pieteikumu izskatīšanu, patentu izsniegšanu un regulēšanu.

Patentu izsniedz uz izgudrojumu, kas atbilst 3 galvenajiem noteikumiem:

- tas ir jauns (t. i., nekur pasaulē agrāk nepublicēts),
- tas ir rūpnieciski izmantojams (t. i., rezultātā tiktu ražoti praktiski noderīgi produkti vai radīta šādu produktu ražošanas tehnoloģija),
- tam ir izgudrojuma līmenis (t. i., to nevarētu izdomāt jebkurš izglītots un pieredzējis inženieris).

Patenta pieteikuma novērtēšanai tiek sasaukta ekspertu komisija, kura pusgada laikā ekspertīzes rezultātā nosaka, vai pieteikums patiešām apraksta izgudrojumu. Pēc patenta saņemšanas izgudrojuma apraksts ir obligāti jāpublicē.

Patents darbojas noteiktā teritorijā, tā iegūšanai ir noteiktas izmaksas, kuras jāapmaksā patenta īpašniekam, un tam ir noteikts darbības termiņš. Patents parasti darbojas 17 gadus, un patenta īpašnieks ik gadu maksā patentu birojam maksu par tiesību aizsardzību.

Patents dod izgudrojuma autoram izņēmuma (monopola) tiesības uz izgudrojuma ražošanu, tiesības izdot izgatavošanas vai ražošanas atļaujas licenci trešajām personām, kā arī tiesības patentu pārdot citai ieinteresētai personai vai organizācijai. Taču patentu tiesības var tikt arī atņemtas, ja patenta īpašnieks neizplata vai neražo izgudrojumu, kā arī neļauj to darīt citām organizācijām.

Uz patentu var pretendēt arī datorprogrammas un algoritmi, ja tie atbilst visiem trim galvenajiem nosacījumiem. Piemēram, patents varētu būt izsniegts pirmajam teksta redaktoram vai pirmajai interneta pārlūkprogrammai. Tomēr Eiropas valstīs likums paredz aizliegumu patentēt datorprogrammas un algoritmus. Savukārt ASV ir izsniegti patenti vairāk nekā 10 000 datorprogrammām.

5.4. AUTORTIESĪBU LIKUMS

Latvijas Autortiesību likums [4] stājās spēkā 1993. gadā. Tas paredz autortiesību aizsardzību zinātniskiem, literāriem, mākslas un muzikāliem oriģināldarbiem, kā arī datorprogrammām un datu bāzēm neatkarīgi no izteiksmes veida un formas. Šādam darbam ir jābūt materializētam, t. i., tikai cilvēka iztēlē esoši tēli vai teksti nevar tikt aizsargāti. Oriģinalitāte likuma izpratnē nav saistāma ar kādu mākslinieciskuvai intelektuālu vērtīgumu, bet tikai ar to, ka attiecīgais intelektuālā darba produkts patiešām ir paša autora prāta radīts. Autortiesību aizsardzībai noteiktais termiņš ir 70 gadi no pēdējā līdzautora nāves. Tas nozīmē, ka, izbeidzoties aizsardzības termiņam, intelektuālā īpašuma objekts kļūst publiski pieejams pārpublicēšanai, reproducēšanai, kopēšanai un cita veida izplatīšanai.

Autortiesības pieder autoram no intelektuālā īpašuma radīšanas brīža, un viņam nekas nav jādara šo tiesību iegūšanai. Darbam nav jābūt pilnīgi pabeigtam, lai uz to attiektos autortiesības. Autortiesības uz darbu var apliecināt ar autortiesību aizsardzības zīmi, kas sastāv no šādiem elementiem:

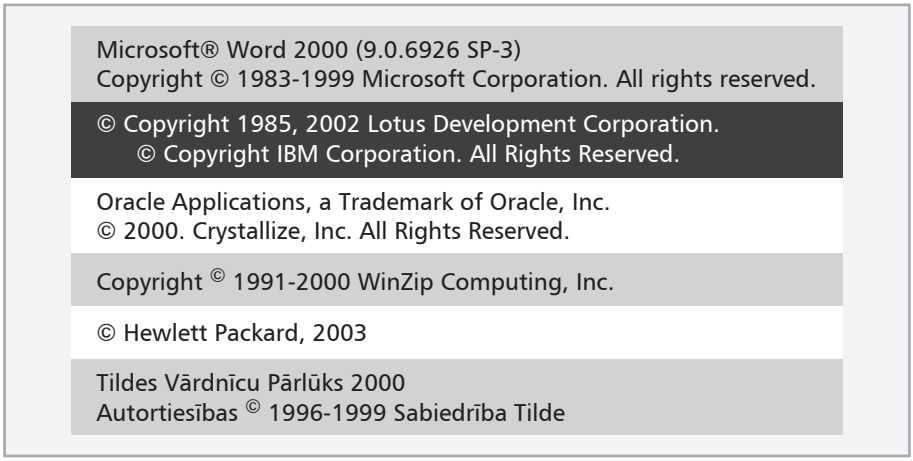
- burta „C” aplītī – ©,
- autortiesību īpašnieka vārda un uzvārda vai nosaukuma,
- darba pirmpublicējuma gada.

Autortiesību zīmes elementu secība dažreiz var atšķirties (sk. 9. attēlu).

Autortiesībām ir personisks un mantisks raksturs.

Personiskās jeb morālās autortiesības ietver tiesības uz autorību (tikt atzītam par autoru), uz izziņošanu, uz darba atsaukšanu, uz vārdu, tiesības atļaut vai aizliegt veikt jebkādus grozījumus, kā arī tiesības pretoties izkropļojumiem. Personiskās tiesības nedrīkst atsavināt, t. i., tās nevar uzdāvināt vai pārdot.

Mantiskās tiesības ietver reproducēšanas, izplatīšanas un kopēšanas tiesības, kā arī tiesības uz grozījumiem. Mantiskās tiesības ir atļauts atsavināt – tās var dāvināt vai pārdot, vai izīrēt. Uzmanīgāka likuma analīze ļauj secināt, ka personiskās un mantiskās tiesības daļēji pārklājas, radot iespēju juridiskiem strīdiem. Taču tā nav Latvijas likumdevēja vaina, jo šī pretruna ir ietverta jau Bernes konvencijā, uz kuru Latvijas likums balstās.



9. att. Autortiesību zīmes lietošana.

Autortiesību likuma 4. panta 1. punkts starp literāriem darbiem noteic arī datorprogrammu aizsardzību. To var saprast, jo datorprogrammu pamatā visbiežāk ir programmas kods jeb teksts. Lai salīdzinātu divas vai vairākas programmas, tām tiek veikta programmas koda salīdzināšana. Tas var būt gan pirmkods, gan objektkods, gan jebkurš cits programmu viennozīmīgi raksturojošs teksts.

Tomēr programmām izšķiramas arī sastāvdaļas, kuras atsevišķi var pretendēt uz autortiesību aizsardzību. Programma sastāv ne tikai no programmas koda. Piemēram, tai var būt lietotāja saskarne, kurai savukārt var būt oriģināls grafisks dizains.

Latvijā likums neparedz algoritmu autortiesību aizsardzību. Programmas lietotājs drīkst, novērojot tās darbību, izsecināt algoritmu, un viņam nevar liegt izstrādāt savu programmatūru pēc šī algoritma. Tāpat nevar aizsargāt kādu metodoloģiju, uz kuru var pamatoties (piemēram, programmatūras prasību specifikācijas noformēšanas metodoloģija vai risku novērtēšanas metodoloģija). Ja programmas algoritma realizācija (koda izteiksmē) nav nozagta, tad algoritma atdarināšana nevar tikt uzskatīta par autortiesību pārkāpumu.

5.4.1. REGULĒJOŠAS INSTITŪCIJAS

Par autortiesību praktisko aizsardzību iekšzemē ir atbildīga Iekšlietu ministrija (galvenokārt Ekonomikas policija). Arī Valsts policijas Tiesu ekspertīžu centrs ir iesaistīts praktiskās aizsardzības ieviešanas aktivitātēs – ir nozīmēts viens eksperts, kas veic ekspertīzes kontrafakto eksemplāru identificēšanu (par kontrafaktiem sauc autortiesību objektus, kuri radīti, pārkāpjot autortiesības). 1999. gada 1. septembrī VID Galvenās muitas pārvaldes Muitas noteikumu pārkāpumu novēršanas daļas sastāvā tika izveidota Intelektuālā īpašuma aizsardzības nodaļa. Nodaļas uzdevums ir koordinēt muitas iestāžu darbu visā Latvijas teritorijā saistībā ar intelektuālā īpašuma aizsardzību.

No 2001. gada 17. janvāra Latvijā darbojas sabiedriska organizācija, kas veic datorprogrammu pirātisma jeb autortiesību pārkāpšanas apkarošanu, – *Business Software Alliance* (*BSA*) Latvijas komiteja. Tā ir Latvijā reģistrēta sabiedriska organizācija, kuras galvenais uzdevums ir datorprogrammu autortiesību aizsardzība un cīņa pret datorprogrammu nelegālu lietošanu Latvijā. Organizācija, aizstāvot savu biedru intereses, nodarbojas ar dažāda veida kampaņu un izglītojošu pasākumu organizēšanu un vadīšanu, sabiedrības informēšanu par datorprogrammu nelegālas izmantošanas nodarīto ļaunumu, kā arī par tādu gadījumu atklāšanu un apkarošanu, kas saistīti ar datorprogrammu nelegālu lietošanu.

5.5. INTELEKTUĀLĀ ĪPAŠUMA OBJEKTI E–VIDĒ

5.5.1. DATU PUBLICĒŠANA INTERNETĀ

Informācijas pārraide e–vidē notiek, izmantojot tiešsaistes pieslēgumu. Darbība vai saruna tiešsaistes režīmā nozīmē darbu ar informāciju, reklāmu vai jebkuru citu izvēlēto materiālu laikā, kad lietotāja dators tieši sasaistās ar citu tīklā (*Internet, Ethernet* u. c.) pieslēgtu datu apstrādes procesa ierīci un veic informācijas apriti – ievadīšanu, uzkrāšanu, pārsūtīšanu utt. Internetā nosūtīto vai atstāto informāciju vai aizsargātos darbus var izmantot dažādi. No juridiskā viedokļa informāciju var izmantot gan labos nolūkos, gan ļaunprātīgi.

! *Iedomātais Autors internetā atrod noderīgu informāciju, kuru viņš var izmantot savas grāmatas tapšanas procesā. Viņš izmanto citātus no šīs informācijas un tos ietver savā darbā. Autors, izmantojot šo informāciju, ievēro tās autora personiskās tiesības, tas ir, izmanto informācijas citātu ar autora vārdu un informācijas nosaukumu. Līdz ar to autors nav šo informāciju piesavinājies, tātad nav piesavinājies internetā publicētās informācijas autora tiesības. Šajā piemērā autors e–vidē publicēto informāciju izmanto, labu nolūku vadīts.*

Informāciju var izmantot arī ļaunprātīgi, tas ir, iegūto informāciju izmantot kā savu un no šīs publicētās informācijas iegūt labumu. Ļaunprātība izpaužas tādējādi: informācijas lietotājam ir zināms, ka attiecīgā informācija nav viņa darbs un ka publikācijas autora tiesības aizsargā autortiesību likums, bet viņš to ignorē un šo informāciju izmanto negodīgos nolūkos.

! *Persona internetā atrod kādas N valsts universitātes profesora publicētu rakstu par autortiesību aizsardzību e–vidē. Šī persona apzināti, tīši pārkāpjot profesora autora tiesības, nokopē daļu raksta, to mazliet papildina, maina raksta struktūru un bez jebkādām atsaucēm savā vārdā publicē kādā zinātniskā žurnālā.*

Starptautiskajā praksē ir zināmi mēģinājumi interneta tiesisko bāzi sasaistīt ar tiesisko regulējumu, kas ir izveidots katrā valstī intelektuālā īpašuma

aizsardzības jautājumos, kā arī iespēju robežās piemērot starptautiskās konvencijas un līgumus, ja valstis ir tām pievienojušās. Tomēr šajos jautājumos pagaidām ASV, Vācijas un citu valstu speciālistu domas dalās. To pierāda ASV un dažu Eiropas valstu, piemēram, Dānijas nostāja mūzikas datņu elektroniskajā kopēšanā. Kaut arī Dānija ir ES dalībvalsts un tai ir saistoša ES Direktīva 2001/29/EC autortiesību jautājumos, Dānijas valdībā ir iesniegts likumprojekts, ar kuru Dānijā, iespējams, tiks legalizēta mūzikas kopēšana no interneta nekomerciālos nolūkos, par to tiešā veidā nemaksājot autoratlīdzību. Tā dara tāpēc, ka nav iespējams izkontrolēt šādu ierakstu gatavošanas procesus. E–vidē saistībā ar intelektuālo īpašuma objektu izmantošanu saduras divas intereses:

- autora mantiskās tiesības,
- informācijas brīvas apmaiņas princips.

No vienas puses, autoram ir tiesības saņemt autoratlīdzību. Tā ir viena no viņa neatņemamām tiesībām. Tomēr ir jāņem vērā tas, ka autoram vai viņa tiesību pārņēmējam jāveic nepieciešamie pasākumi, lai viņa darbs – intelektuālais īpašums – un tā izmantošana tiktu kontrolēta un nebūtu brīvi pieejama interneta lietotājiem. Praksē galvenokārt izmanto divus intelektuālā īpašuma aizsardzības paņēmienus:

- nodot uz līguma pamata savu intelektuālo īpašumu kādai personai un līgumā atrunāt visus noteikumus, kas jāievēro personai, izmantojot nodoto intelektuālo īpašumu;
- rīkoties pašam un ar dažādu drošības mehānismu starpniecību, konsultējoties ar datoru speciālistiem, noteikt sava intelektuālā īpašuma izmantošanas veidus internetā.

Taču, no otras puses, ir jāpastāv informācijas brīvai apmaiņai. Jebkuram ir tiesības brīvi saņemt informāciju un apmainīties ar to, ja tādā veidā netiek skartas informācijas īpašnieka vai valdītāja tiesības. Saņemot tiesības lietot intelektuālo īpašumu internetā, izmantotājam jāievēro noteikumi, ko nosaka tā īpašnieks. Ja persona vēlēsies izmantot šo intelektuālā īpašuma objektu, tad tam ir jāpiekrīt tā īpašnieka izvirzītajiem noteikumiem vai arī jāatsakās no objekta izmantošanas. Visas turpmākās darbības ar objektu bez atļaujas ir likuma pārkāpums.

Tādējādi saduras intelektuālā īpašuma objekta īpašnieka un izmantotāja intereses. LR likuma "Vispasaules Intelektuālā īpašuma organizācijas (VIĪO) līgums par autortiesībām" preambulas piektajā daļā teikts, ka "ir nepieciešams saglabāt līdzsvaru starp autora tiesībām un plašākas sabiedrības interesēm, īpaši izglītības un pētniecības jomā, kā arī attiecībā uz informācijas pieejamību, kā tas atspoguļots Bernes konvencijā". Galvenais priekšnoteikums ir intelektuālā īpašuma objektu atbilstība sabiedrības vajadzībām, kas arī nosaka to vērtību. Minētā likuma 8. pants noteic, ka, "..nepārkāpjot Bernes konvencijas 11(1)(ii), 11bis(1)(i) un (ii), 11ter(1)(ii), 14(1)(ii) un 14bis(1) panta noteikumus, literāro un mākslas darbu autoriem ir ekskluzīvas tiesības atļaut komunicēt ar publiku savus darbus pa vadiem vai ēterā, kā arī padarīt šos darbus pieejamus sabiedrībai tādā veidā, ka sabiedrības locekļi var tos izmantot jebkurā vietā un laikā pēc katra individuālās izvēles".

Internets dod vislielākās iespējas intelektuālā īpašuma tiesību īpašniekiem iepazīstināt citus ar savu radīto intelektuālā īpašuma objektu. Tas iespējams, publicējot, izplatot vai citādi padarot pieejamu savu darbu internetā.

! *Piemēram var minēt interneta veikalu – www.amazon.com. Sasaistoties ar datoru, kas uzglabā šī interneta veikala informāciju, ikviens var iepazīties ar veikalā piedāvāto produktu anotācijām, kā arī, ievērojot veikala izvirzītos elektroniski publicētos noteikumus, katrs var iegādāties izvēlēto, viņam nepieciešamo produktu.*

Cita situācija veidojas, ja strādā ar datoru publiskajās bibliotēkās. Te, iepazīstoties ar grāmatu saturu, ir iespējams datorā saņemt darbu fragmentus vai pat visus darbus. Kārtību, kādā bibliotēkā var iegūt nepieciešamo informāciju, nosaka bibliotēkas lietošanas noteikumi. Piemēram, Rīgas Juridiskās augstskolas bibliotēkas lasītājam ir tiesības pieslēgties ar bibliotēkas datoru *"Lexis – Nexis"* datu bāzei un par samaksu Ls 0,50 stundā iegūt tajā publicēto maksas informāciju, pārkopēt to uz disketi un pēc tam izmantot pēc vajadzības. Tas, protams, ir nesalīdzināmi lētāk nekā abonēt *"Lexis – Nexis"* datu bāzi. Tādā veidā bibliotēkas klients iegūst tiesības izmantot kādas citas personas intelektuālā īpašuma objektu.

Autortiesību likuma 4. panta 1. daļa noteic, ka ".. autortiesību objekts neatkarīgi no izcelsmes formas un veida ir ikviens literārs darbs". Šā paša likuma 15. pantā ir noteikts, ka ".. tikai autoram ir tiesības pieņemt lēmumu, kādā veidā viņa darbs tiks izmantots un kāda atlīdzība būs jāmaksā". Likums nosaka arī ierobežojumus autora tiesībām. Ierobežojumi ir saistīti ar atlīdzības saņemšanu par darbu izmantošanu individuālai lietošanai, zinātniskiem mērķiem, kā arī atlīdzības iekasēšanu par darbu reprogrāfisko reproducēšanu.

! *Datora lietotājs savā datorā savām vajadzībām saņem grāmatas pilnu tekstu. Viņš izlasa, vienu eksemplāru izdrukā, bet datorā tekstu izdzēš kā nevajadzīgu. Līdzīgi rīkojas daudz citu personu dažādās pasaules vietās. Vai šajā situācijā ir jāmaksā atlīdzība par autora tiesībām?*

Atbilde uz šo jautājumu nav tik vienkārša. Bernes konvencijas 9. panta 2. daļā šādas situācijas ir nosauktas par "īpašiem gadījumiem". Īpašie gadījumi ir norādīti arī Autortiesību likuma 19. pantā: "Autortiesības nav uzskatāmas par pārkāptām, ja bez autora piekrišanas un bez atlīdzības šajā likumā noteiktajā kārtībā:

- darbs tiek izmantots informatīviem mērķiem;
- darbs tiek izmantots izglītības un pētniecības mērķiem;
- darbs tiek reproducēts, lai to varētu izmantot redzes un dzirdes invalīdiem;
- darbs tiek reproducēts bibliotēku un arhīvu vajadzībām;
- darbs tiek reproducēts tiesvedības mērķiem;
- tiek izmantots publiski pieejams vai izstādīts darbs;
- muzikāls darbs tiek izmantots valstisku vai reliģisku ceremoniju laikā, kā arī izglītības iestādēs nepastarpinātā mācību procesā;
- darbu īslaicīgi izmanto raidorganizācija;

- darbs tiek reproducēts tehniskai izmantošanai raidorganizācijā;
- datorprogrammas tiek izmantotas reproducēšanai, translēšanai un citai pārveidošanai saskaņā ar šā likuma 29. pantu;
- tiek nodrošināta datorprogrammas sadarbspēja;
- darba atsavināšana citai personai notiek atkārtoti, izņemot likuma 17. panta pirmajā daļā noteiktos gadījumus. Autortiesības nav uzskatāmas par pārkāptām, ja bez autora piekrišanas, bet samaksājot viņam taisnīgu atlīdzību, publicēts darbs tiek izmantots publiskai patapināšanai."

! *Tomēr arī šos izņēmumus var interpretēt dažādi. Piemēram, ko nozīmē „izmantot informatīviem mērķiem"? Daudzi var uzskatīt, ka klausīties elektroniskā formāta mūzikas ierakstus „labos nolūkos", nevis komerciālos nolūkos (t. i., nodarboties ar elektroniskā formāta mūzikas tirdzniecību) nav autortiesību pārkāpums. Atbilde uz šo jautājumu meklējama nevis nolūkā, bet gan autora atlīdzībā. Ja persona ir iegādājusies licencēto mūzikas disku un pārveidojusi mūzikas ierakstus elektroniskā formātā personiskai lietošanai, tad to nevar uzskatīt par autortiesību pārkāpumu, jo autors ir saņēmis atlīdzību par nopirkto disku. Savukārt, ja persona ir iegādājusies disku dāvināšanai, bet, pirms to atdāvinājusi, pārveidojusi mūzikas ierakstus elektroniskā formātā savai lietošanai, autors saņems nosacīti divreiz mazāku autoratlīdzību, un tas būs autortiesību pārkāpums.*

Svarīgi arī noskaidrot, vai autors vai tiesību īpašnieks pats intelektuālā īpašuma objektu ir ievietojis internetā. Gadījumā, ja to ir izdarījis pats intelektuālā īpašuma objekta īpašnieks, neierobežojot darba izmantošanu vai nenorādot nekādus lietošanas ierobežojumus, lietotājam par darba lietošanu nav jāmaksā. Piemēram, grupas „Tumsa" mājaslapā albumu sadaļā iespējams noklausīties vairākas dziesmas, tātad šo mūzikas ierakstu izplatīšanu ir organizējis pats autors, neprasot par to atlīdzību. Vienīgā prasība pret darbu izmantošanu ir autora personisko tiesību ievērošana, t. i., izmantojot darbu, obligāti jānorāda darba autora vārds.

! *Autors publicē internetā savu darbu. Pēc kāda laika viņš atklāj, ka darbs ir mazliet mainīts, bet nav kļuvis sliktāks. Autors pret personu, kas bez viņa piekrišanas mainījusi darbu, pretenzijas nav cēlis. Pēc vairākiem gadiem pie autora vai firmas, kura izmanto autora darbu, ierodas persona, kas mainījusi viņa darbu, un pieprasa autora atlīdzību par pārveidoto intelektuālā īpašuma objektu, jo uzņēmējsabiedrība izmanto viņa izveidoto darbu un tas ir veicinājis tās virzību un attīstību. Ko darīt?*

Svarīgākais, kas šādās situācijās jāievēro, ir tas, ka tiesību pārkāpums uz konkrēto darbu ir ne tikai jāfiksē, bet nepieciešams arī reaģēt uz visām izmaiņām un fiksētajām pārmaiņām, kuras notikušas ar intelektuālā īpašuma objektu, neatkarīgi no tā, vai tas noticis pozitīvā vai arī negatīvā virzienā. Tātad ir jāreaģē uz visiem intelektuālā īpašuma tiesību aizskārumiem. Persona, kurai bija autora tiesības, ar konkrētām darbībām ir piekritusi darba mainīšanai tad, ja tā nav pieteikusi savas pretenzijas likumā vai līgumā paredzētajā kārtībā pret personu, kas mainījusi autora darbu. Ja autors nav veicis nepieciešamās

darbības, tad viņš klusējot ir piekritis darba izmainīšanai. Tādā gadījumā viņš nevar liegt citai personai, kas veikusi darba pārveidošanu, prasīt tai pienākošos atlīdzību. Patiesībā persona, kas sākotnēji radījusi produktu, ir atzinusi darba līdzautora tiesības. Protams, ja lieta nonāktu tiesā, tad darba autoram būtu jāceļ prasība tiesā par līdzautorības atzīšanu, jo Autortiesību likuma 8. pants nosaka kārtību autora tiesību atzīšanai.

Tie ir tikai daži piemēri, bet šādu un citādu situāciju var būt daudz, un katra no tām ir skatāma atsevišķi, ievērojot lietas apstākļus un katrā konkrētā gadījumā esošos pierādījumus.

Attīstoties IKT, interneta pakalpojumu ir iespējams saņemt gan pa kabeļiem, gan bezvadu tīkliem. Šis pakalpojums sevī ietver gan interneta, kabeļu televīzijas, telekomunikāciju, radio un citus pakalpojumus. Šis pakalpojumu veids rada vairākas tiesiskas problēmas, kas saistītas ar intelektuālā īpašuma izmantošanu e–vidē.

Saasinās intelektuālā īpašuma aizsardzības problēmas, kas saistītas ar

- intelektuālā īpašuma izmantošanu komerciālos nolūkos, gūstot peļņu,
- intelektuālā īpašuma izmantošanu reklāmās,
- intelektuālā īpašuma kopēšanu, kas varētu traucēt darba normālu izmantošanu.

Izplatot intelektuālā īpašuma objektus internetā peļņas nolūkos, to cena nereti ir nesamērīgi zema salīdzinājumā ar intelektuālā īpašuma īpašnieka prasīto.

! *Kāda persona internetā piedāvā nopirkt tulkošanas datorprogrammu – par ½ no tās cenas, par kuru datorprogrammu pārdod veikalā pie izplatītājiem. Nereti šī cenas starpība ir vēl lielāka.*

Intelektuālā īpašuma izmantošanas tiesiskās problēmas radīsies ar bibliotēku elektronisko tīklu izveidošanu – kā tīklā var kontrolēt klientu (lasītāju) darbību, kuri izmanto intelektuālā īpašuma objektus? Vēl aktuālākas šīs problēmas kļūs, ja netiks sakārtots jautājums par autoratlīdzības iekasēšanu un sadalīšanu. Problēma radīsies par tās informācijas izmantošanas kārtību komercstruktūrās, kuras statuss noteikts ar likumu. Kabeļu tīklu īpašnieki un valdītāji ir ieinteresēti šāda veida uzņēmējdarbības attīstībā.

5.5.2. DATORPROGRAMMAS

Datorprogrammu autortiesību aizsardzība Latvijā tiek nodrošināta ar Autortiesību likumu.

Autortiesību likums noteic, ka par datorprogrammas autoru tiek uzskatīts tās radītājs (cilvēks). Taču gadījumā, ja datorprogrammas radītāju saista līgumsaistības un tā ir radīta līgumdarba rezultātā, likums piešķir mantiskās tiesības uz izstrādāto programmu darba devējam, ja līgumā nav noteikts citādi.

Likuma 15. panta 2. punkts noteic īpašas datorprogrammas autora mantiskās tiesības

- reproducēt datorprogrammu (ciktāl datorprogrammas ielādēšana, demonstrēšana, lietošana, pārraidīšana vai glabāšana prasa to reproducēt, šādu darbību rakstveidā atļauj autors);

- izplatīt datorprogrammu;
- iznomāt datorprogrammu;
- translēt, adaptēt un jebkādi citādi pārveidot datorprogrammu un reproducēt šādi iegūtos rezultātus (ciktāl tas nav pretrunā ar tās personas tiesībām, kura pārveido datorprogrammu);
- padarīt datorprogrammu pieejamu publikai pa vadiem vai citādi individuāli izraudzītā vietā un individuāli izraudzītā laikā.

Datorprogrammu izmantošanas tiesības nosaka tālāk citētie Autortiesību likuma panti.

40. pants. Darba izmantošanas tiesības

(1) Lai iegūtu darba izmantošanas tiesības, darba izmantotājiem attiecībā uz katru darba izmantošanas veidu un katru darba izmantošanas reizi jāsaņem autortiesību subjekta atļauja.

(2) Autortiesību subjekta atļauja tiek izsniegta gan licences līguma, gan licences veidā.

(3) Darba izmantotājam pirms darba izmantošanas jānoslēdz licences līgums vai jāsaņem darba izmantošanas licence.

...

41. pants. Licences līgums

(1) Licences līgums ir līgums, ar kuru viena puse – autortiesību subjekts – dod atļauju otrai pusei – darba izmantotājam – izmantot darbu un nosaka darba izmantošanas veidu, vienojoties par izmantošanas noteikumiem, atlīdzības lielumu, tās izmaksāšanas kārtību un termiņu.

(2) Licences līgumā var paredzēt, ka licencē tiek piešķirtas tiesības darbu izmantot vienā vai vairākos norādītajos veidos, kā arī tiesības nodot licenci trešajām personām (sublicence). Attiecīgās tiesības var nodot pilnībā vai daļēji. Ja līgumā tādu norādījumu nav, darba izmantotāja tiesības tiek ierobežotas ar tām darbībām, kas izriet no līguma un ir nepieciešamas līguma mērķa sasniegšanai.

(3) Ja licences līgumā atlīdzības lielums nav konkretizēts, strīda gadījumā to nosaka tiesa pēc saviem ieskatiem.

42. pants. Licence un tās veidi

(1) Licence ir atļauja izmantot attiecīgo darbu tādā veidā un ar tādiem noteikumiem, kādi norādīti licencē. Ir vienkārša licence, izņēmuma licence un vispārēja licence.

(2) Vienkārša licence dod licences saņēmējam tiesības veikt tajā norādītās darbības vienlaikus ar autoru vai citām personām, kuras arī saņēmušas vai saņems attiecīgo licenci.

(3) Izņēmuma licence dod tiesības veikt tajā norādītās darbības vienīgi licences saņēmējam.

...

43. pants. Licences un licences līguma forma

(1) Jebkura licence izsniedzama rakstveidā.

(2) Licences līgumu var slēgt gan mutvārdos, gan rakstveidā.

...

44. pants. Licences līguma vai licences termiņš

(1) Laiks, uz kādu noslēgts licences līgums vai izsniegta licence, tiek noteikts, pusēm vienojoties.

(2) Ja noslēgtais licences līgums vai izsniegtā licence nav ierobežoti laika ziņā, autors vai cits autortiesību subjekts var izbeigt licences līgumu vai atsaukt licenci, sešus mēnešus iepriekš paziņojot uzteikumu.
(3) Licences līgumā vai licencē iekļautais noteikums par autora atteikšanos no šā panta otrajā daļā paredzētajām tiesībām nav spēkā.

45. pants. Teritorija, kurā ir spēkā licences līgums vai licence
(1) Licences līgumā vai licencē norādāma teritorija, kurā līgums vai licence ir spēkā.
(2) Ja licences līgumā vai licencē nav norādīta teritorija, kurā tie ir spēkā, tie attiecas uz valsti, kurā noslēgts licences līgums vai izsniegta licence.

Autortiesību likuma noteikumi par darba reproducēšanu bibliotēku un arhīvu vajadzībām, tiesvedības mērķiem, izglītības un pētniecības mērķiem uz datorprogrammām neattiecas.

5.5.3. DATU BĀZES

Īpaši Autortiesību likumā ir izceltas datu bāzes. Likuma 1. pantā datu bāze tiek definēta kā „neatkarīgu darbu, datu vai citu materiālu krājums, kas sakārtots sistemātiski vai metodiski un individuāli pieejams elektroniskā vai citādā veidā".

Autortiesību likums aizsargā datu bāzes divējādi. Ar autortiesībām aizsargā datu bāzes struktūras autora tiesības, kuras gan praksē reti izmanto, bet ar t. s. *sui generis* tiesībām aizsargā datu bāzes satura (parasti tie ir dažādi fakti) veidotāju tiesības, ja tās izveidošanai, iegūšanai, pārbaudei vai demonstrēšanai ir bijis nepieciešams būtisks kvalitatīvs vai kvantitatīvs ieguldījums – finanšu līdzekļi vai laika un enerģijas patēriņš. Veidotāji var būt gan fiziskas, gan juridiskas personas.

Datu bāzu aizsardzības termiņš ir noteikts 15 gadi no dienas, kad pabeigta datu bāzes izveide vai kopš datu bāze kļuvusi publiski pieejama. Ja datu bāzes saturā tiek izdarīti jebkādi būtiski kvalitatīvi vai kvantitatīvi novērtējami grozījumi, šādai datu bāzei ir tiesības uz savu aizsardzības termiņu; tas nozīmē, ka tai tiek piemērots jauns 15 gadu ilgs aizsardzības termiņš. No šī noteikuma loģiski var secināt, ka teorētiski ir iespējama beztermiņa datu bāzes veidotāju tiesību aizsardzība, kas atsevišķās valstīs, piemēram, ASV, netiek uzskatīta par pieļaujamu, jo tādējādi tiek radīts precedents, kad monopoltiesības ir neierobežotas laikā. Šī pretruna ir jau ilglaicīgs ASV un ES strīda objekts.

5.5.4. DOMĒNS

Internets ir vienots mehānisms, kas sastāv no neierobežota daudzuma neatkarīgu tīklojumu un ir veidots no vairākiem miljoniem atsevišķu datoru. Vispasaules tīklā – pasaules datu tīmeklī – pastāv noteikta lietotāju identifikācijas sistēma.

Domēns ir interneta adrešu sistēma, kas izteikta burtu, ciparu un citu grafisku simbolu veidā un kas tiek piesaistīta interneta vidē reģistrētu datoru IP adresēm. Attīstoties interneta izmantošanai komerciālos nolūkos, domēna vārdi ieguvuši

citu nozīmi, proti, tie sākuši apzīmēt tā turētājus (fiziskas vai juridiskas personas), preci vai pakalpojumu, tas ir, sākuši veikt līdzīgu funkciju kā preču zīmes.

Kā redzams no iepriekš minētā, tad uz domēna vārdu var tikt attiecināti dažādi juridiskie jēdzieni – īpašnieks, lietotājs, turētājs, nomnieks. Precīzi definēt domēna vārdu, lai tas būtu iedalāms kādā no iepriekšminētajām grupām, ne Civillikuma, ne arī intelektuālā īpašuma izpratnē nav iespējams. Tas saistīts ar vairākiem aspektiem. Domēna vārds nevar būt īpašumā, jo tam nepiemīt īpašumu raksturojoši lielumi Civillikuma (927.–1129. p) izpratnē. Tas nevar būt arī valdījumā, jo neatbilst Civillikuma (875.– 926. p.) izpratnei. Vistuvāk domēna vārdu lietošanai atbilstu nomas tiesības, jo domēna vārda lietotājs par šo vārdu maksā noteiktu maksu, taču par nomas tiesību objektu var būt tikai ķermeniskas lietas, kuras nav aizliegts atsavināt. Līdz ar to, lai noslēgtu nomas līgumu, ir jākonstatē, ka līguma priekšmetam piemīt taustāmas, kustamas lietas pazīmes.

Domēnam šādu pazīmju nav, tāpēc domēna līgumu varētu pielīdzināt pakalpojuma līgumam, jo uzņēmums, kurš ir pilnvarots reģistrēt domēna vārdus Latvijā vai citur pasaulē, to sniedz kā maksas pakalpojumu klientiem. Līdz ar to Latvijas teritorijā uz šo pakalpojumu veidu varētu attiecināt patērētāju tiesību aizsardzības likumus, piemēram, likumu "Par atbildību par preces un pakalpojuma trūkumiem" un "Preču un pakalpojuma drošības likumu". Tas, protams, nenozīmē, ka visu domēna vārda izmantošanas problēmu atrisinājums ir patērētāju tiesības. No tā izriet secinājums, ka patlaban pasaulē nav pieņemtas nevienas juridiski saistošas regulas, kas tieši būtu attiecināmas uz domēna vārda izmantošanas tiesisko problēmu risinājumu.

Jautājumus par domēna vārdu izmantošanas tiesisko aizsardzību, sadarbojoties ar dažādām starptautiskām sabiedriskām organizācijām, aktīvi risina Vispasaules Intelektuāla īpašuma organizācija (VIĪO). Šī organizācija izveidojusi speciālu Arbitrāžu, kuras uzdevums ir izskatīt dalībvalstu personu strīdus intelektuālā īpašuma izmantošanas jautājumos.

Pastāv arī zināmi ierobežojumi domēnu vārdu reģistrācijā. Visi augstākā līmeņa domēna vārdi tiek reģistrēti ar uzņēmējsabiedrību starpniecību, kuras pārstāv *ICANN* (*Internet Corporation for Assigned Names and Numbers*), ievērojot noteikto kārtību. Latvijā augstākā līmeņa domēna vārdus reģistrē *NIC* (*Network Information Center*), kas pārstāv *ICANN* Latvijā. Pirms vēlamā domēna vārda reģistrācijas ir jāņem vērā ierobežojumi, ko nosaka *Network Information Center for Latvia*. Domēna vārdu nevar reģistrēt šādos gadījumos:

- ja tas ir reģistrēta preču zīme, servisa zīme vai labi zināms nosaukums, kā arī to saīsinājumi, izņemot tās uzņēmējsabiedrības vai citas institūcijas, kam pieder preču zīmes vai šie nosaukumi;
- ja tas ir ģeogrāfiskas vietas nosaukums; izņēmums ir iekšējie ģeogrāfiskie nosaukumi, kurus var reģistrēt zināmas organizācijas, piemēram, Dobeles pilsētas dome drīkst reģistrēt domēnu *dobele.lv*;
- ja tas ir personas vārds;
- ja tas ir labi zināms vai publisks vārds;
- ja tas ir aizvainojošs;
- domēna nosaukumā nedrīkst būt ne mīkstinājuma zīmju, ne garumzīmju.

Tomēr, kā liecina 2001. gada 11. septembra notikumi, *ICANN* acīmredzot būs spiesta iepriekš minētos kritērijus pārvērtēt.

! *2001. gada 21. septembrī mājaslapā www.abc.news.com tika publicēta informācija par to, ka, izmeklējot teroristiskos uzbrukumus Ņujorkas Pasaules tirdzniecības centram un Pentagonam Vašingtonā, izmeklētāji ir atklājuši vairāk nekā 20 reģistrētus dīvainus domēna vārdus. Piemērā minētie domēna vārdi reģistrēti Afternic.com 15–18 mēnešus pirms liktenīgā uzbrukuma ar www.worldtowerattack.com, www.worldtradetowerstrike.com, www.pearlharborinmanhattan.com u. c. Minētais uzskatāmi liecina par to, ka, pastāvot līdzšinējiem domēnu reģistrācijas ierobežojumiem, jebkurš var reģistrēt pat domēnu, kas satur informāciju par noziedzīgu nodarījumu vai šāda nodarījuma organizēšanu, piemēram, www.autozaglis.com.lv, www.hakeris.edu.lv utt. Patlaban pārstāvis no Network Solutions organizācijas, kas uztur domēnu reģistrācijas bāzi, ir aizbildinājies ar to, ka kompānija nepublisko reģistrētāju vārdus tiem domēniem, kuru darbības laiks beidzies. Taču, ņemot vērā stingros pretterorisma pasākumus ASV un pasaulē, šī organizācija būs spiesta mainīt savu nostāju ne tikai publicitātes jautājumos, bet arī domēnu reģistrācijas kārtībā.*

ICANN domēna vārdu piešķir un reģistrē, ievērojot prioritātes principu. Tas nozīmē, ka priekšroka tiek dota tam pieteikumam, kurš ir iesniegts agrāk. Interneta lietotāji domēna vārdu pieprasa ne tikai tādēļ, lai nodrošinātu to atpazīstamību elektroniskā vidē, bet arī lai reklamētu savu piedāvāto pakalpojumu un ieņemtu zināmu elektroniskās tirdzniecības vai pakalpojumu sniegšanas vietu.

Kā minēts iepriekš, domēna vārda piešķiršana ir pakalpojums, kura juridisko saikni veido līgums starp klientu – potenciālo domēna lietotāju – un *ICANN* pilnvaroto reģistrācijas organizāciju. Te parādās vairākas juridiskas problēmas, piemēram, teorētiski tikai *NIC* ir tiesības reģistrēt domēnu .lv, bet praktiski piešķirt šo domēna vārdu var ikviena *ICANN* akreditēta reģistratora organizācija jebkur pasaulē.

! *1999. gadā kāda Latvijā reģistrēta organizācija vēlējās izveidot savu mājaslapu un reģistrēt domēna vārdu, kurā būtu organizācijas nosaukums, organizācijas atrašanās vieta un valsts. Meklējot informāciju, kur to izdarīt lētāk nekā Latvijā, organizācijai piedāvāja XOOM serveri. Sarakstoties ar servera administratoru, kuram bija arī tiesības reģistrēt domēna vārdus, organizācija saņēma laipnu atbildi, ka par 25 USD viņš reģistrēs organizācijas izvēlēto domēnu un piešķirs mājaslapas veidošanai bezmaksas apgabalu 10 MB. Līdz ar to tikai teorētiski var teikt, ka NIC ir ekskluzīvas tiesības piešķirt domēnu .lv, bet praktiski ir citādi – ja šādu domēna vārdu piešķirs kāds ASV, Kanādā, Jaunzēlandē, Austrālijā pilnvarots reģistrators, tad Network Solution nebūs nekāda iemesla, lai šādu domēnu nereģistrētu savā reģistrā. Līdzīgi tas ir arī ar vietvārdu reģistrāciju. Iespējams, ka Latvijā NIC nereģistrēs domēnu ar vietvārdu Rīga, Ogre, Vietalva, bet interesents to bez problēmām varēs izdarīt citā valstī, kur neviens nepārzina mūsu vietvārdus un ģeogrāfiskos nosaukumus. Tieši šis apstāklis padara šo tehnisko reģistrācijas problēmu par juridisku, jo ar šādu reģistrāciju tiek aizskartas Latvijas valsts iedzīvotāju un organizāciju, institūciju un iestāžu likumīgās tiesības un intereses.*

Lai arī liela daļa juristu, kas pēta elektroniskās vides tiesiskās problēmas, uzskata, ka domēna vārds ir preču zīme un tāpēc aizsargājams saskaņā ar preču zīmes aizsardzības principiem, tomēr tam pilnīgi nepiekrīt VIĪO. Piemēram, VIĪO 2001. gada 15. jūnijā publicētajā dokumentā par elektronisko vidi un domēna vārdu norādīts, ka domēna vārda nozīme ir plašāka par preču zīmes saturu, jo to izmanto ne tikai komercdarbībā, bet arī valsts, sabiedrisko organizāciju, pašvaldību un privātpersonu profesionālo un personisko interešu apmierināšanai. Domēna vārdu var izmantot gan kā pakalpojuma vai preču zīmi, ja to attiecīgi reģistrē, gan kā ģeogrāfiskas vietas apzīmējumu, gan kā fiziskas vai juridiskas personas nosaukumu apzīmējumu u. c. Domēna vārdu kā savu var reģistrēt un reģistrē arī privātpersonas. Tāpēc šis process saistās ne tikai ar personu ekonomisko interešu, bet arī ar personisko tiesību aizsardzību.

! *1999. gadā ASV viena no populārākajām grāmatām bija psiholoģes Katrinas Tarboksas grāmata "Katiet. com". Grāmatas izdevēja ASV kompānija Penguin Putman Inc tās virsrakstā kļūdījās, izlaižot vienu burtu, proti, paredzētā nosaukuma Katiet. com vietā grāmatu publicēja ar nosaukumu Katie. com, kas, izrādījās, bija kādas Anglijas privātpersonas K. Džonsas 1996. gadā reģistrēts domēna vārds. Pēc grāmatas publikācijas K. Džonsa saņēma lielu daudzumu korespondences, kas radīja nopietnus apgrūtinājumus. Tomēr šī Anglijas pilsone nevarēja vērsties ASV tiesā ar prasību pret izdevniecību par kaitējuma nodarīšanu, jo šādu kārtību neregulē ne ASV likumi, ne arī tiesu prakse.*

Šajā piemērā ir pārkāptas privātpersonas personiskās tiesības. Izdevniecība ir pieļāvusi uz citas personas vārda reģistrēta domēna vārda aizskārumu. Patlaban pasaulē nav izstrādāts tiesiskās aizsardzības mehānisms par tiesībām uz aizskāruma novēršanu.

5.6. PROGRAMMU IZSTRĀDE UN AUTORTIESĪBAS

5.6.1. KAS NOTIEK, JA NEVIENS NEKO ĪPAŠI NEDARA?

Likums nosaka, ka autoram vai līdzautoriem visas tiesības uz datorprogrammu pieder no tās radīšanas brīža un nekādas īpašas juridiskas darbības nav nepieciešamas. Atcerēsimies, ka autors vai līdzautori ir tikai fiziskas personas.

Vienīgi tādā gadījumā, ja datorprogramma izstrādāta darba devēja uzdevumā, tā sauktās mantiskās tiesības (piemēram, kopēt datorprogrammu, lietot to vai pārdot tās lietošanas tiesības) uzreiz pāriet darba devēja īpašumā. Taču autora īpašumā vienmēr paliek tā sauktās personiskās tiesības (piemēram, atļaut vai neatļaut jebkādas izmaiņas datorprogrammā vai tiesības saukt sevi par radītā darba autoru).

Pasūtītājs bez īpašu juridisku procedūru veikšanas (licences saņemšanas vai licences līguma noslēgšanas) nevar iegūt tiesības lietot datorprogrammu pat tad, ja ir nopircis, piemēram, disketi vai kompaktdisku, kurā ierakstīta

datorprogramma. Jāpiekrīt, ka zināmā mērā ir negaidīti, ka līdz ar vides (diskettes, CD u. tml.) īpašnieka maiņu tiesības lietot vides saturu ne vienmēr maina īpašnieku, tomēr tieši tā tas ir, un Latvijas likums šajā ziņā nav izņēmums.

5.6.2. KAS TIEK UN KAS NETIEK AIZSARGĀTS?

Aizsargāts tiek konkrētais datorprogrammas teksts, nevis tajā iemiesotais algoritms un tas, kā programma darbojas. Ir iespējams – un likums arī neaizliedz – ar oriģināla, atšķirīga datorprogrammas teksta palīdzību iemiesot kādas populāras datorprogrammas funkcionalitāti.

Aizsargāta tiek arī datu bāze un datorprogrammas saskarne, taču tikai tiktāl, cik tai ir unikāla struktūra vai dizains.

Autortiesību likums aizsargā arī datu bāzu veidotāju tiesības saņemt taisnīgu atlīdzību par bāzes radīšanā un uzturēšanā patērētiem resursiem.

5.6.3. PAR KO JĀRŪPĒJAS DARBA DEVĒJAM?

Darba devējam nozīmīgs ir autorlīgums ar ikvienu darbinieku, panākot vienošanos, ka autors nekad neizmantos vai uz ilgu laiku neaizdos neatsavināmās personiskās tiesības. Jāraugās, lai lietvedībā būtu dokumenti (piemēram, rīkojumi par projekta grupas sastāvu, darba līgumi), kas liecinātu par darbinieka piesaistīšanu konkrētu datorprogrammu izstrādē. Ja darba devējs nebūs noslēdzis autorlīgumu ar darbinieku, var izrādīties, ka nebūs iespējams nodot pasūtītājam līgumiski apsolītās tiesības uz programmatūras produkta lietošanu, un tas, protams, draud ar tiesas darbiem. Darbinieks varēs nepiekrist produkta grozījumiem (tā taču ir dabiska un vispārpieņemta prakse) vai vispār aiziet no darba un paziņot par savu mantisko tiesību atpakaļņemšanu 6 mēnešus pēc darba līguma izbeigšanās.

5.6.4. PAR KO JĀRŪPĒJAS AUTORAM VAI VIŅA TIESĪBU PĀRŅĒMĒJAM?

Kaut arī autortiesības rodas it kā pašas no sevis un uzreiz pieder autoram (vai algota darba uzdevuma izpildes gadījumā – pa daļai autoram, pa daļai darba devējam), grūtības var rasties, kādai trešajai personai iegūstot datorprogrammu un uzdodoties par tās autoru. Autortiesību likumā par šādu situāciju nekas nav teikts.

Ne vienā valstī vien autortiesību aizsardzības nodrošināšanai praksē izmanto autortiesību reģistrāciju, ko izdara, piemēram, autortiesību aizsardzības aģentūras. Autors iesniedz aģentūrai glabāšanai savas datorprogrammas tekstu, bet aģentūra pretī izdod reģistrācijas apliecību un apņemas konflikta gadījumā apliecināt teksta saņemšanas faktu un datumu, kā arī autora personību. No 1996. gada šāda reģistrācija notika arī Latvijā. Iesākumā to veica Latvijas Autortiesību aģentūra (LAA), bet vēlāk, apvienojoties aģentūrām, to turpināja AKKA/LAA.

Diemžēl 2000. gada maijā AKKA/LAA rakstiski paziņoja, ka no 2000. gada 1. janvāra tā vairs nereģistrēs datorprogrammu autortiesības, "jo Autortiesību likums tādu reģistrāciju neparedz".

5.7. PROGRAMMATŪRAS PIRĀTISMS

Termins „programmatūras pirātisms" attiecas uz dažādām darbībām: programmu nelegālu kopēšanu, programmatūras viltošanu un viltojumu pārdošanu, pat uz programmas aizņemšanos no drauga vai paziņas. Zināt dažādus datorpirātisma veidus ir svarīgi, ne tikai lai ievērotu likuma prasības, bet arī lai aizsargātos pret lielākām ekonomiskām problēmām – ieņēmumu samazināšanos vai darba zaudēšanu.

5.7.1. PROGRAMMATŪRAS PIRĀTISMA VEIDI

Pirātisma veidi jeb autortiesību pārkāpumi mēdz būt visai dažādi. Tos iedala atšķirīgās smaguma pakāpēs pēc nodarītā kaitējuma jeb zaudējumu apjoma.

Programmatūras pirātisma veidi ir vairāki.

- **Datorprogrammu viltošana**. Tā ir nelegāla datorprogrammu kopēšana, kas veikta ar nodomu pēc iespējas precīzi atdarināt datorprogrammas iepakojumu, drošības pazīmes, dokumentāciju u. tml.
- **Datorprogrammu gala lietotāju izdarītie pārkāpumi**. Tie tiek izdarīti tad, kad organizācijas, uzņēmumi, iestādes vai fiziskas personas veido datorprogrammu kopijas šādos veidos:
  - izmantojot vienu legāli iegādātu CD, lai instalētu konkrēto programmu uz vairākiem datoriem, ja licencē vai līgumā ir norādīts, ka programmu atļauts instalēt uz viena datora;
  - kopējot diskus programmas instalēšanai vai izplatīšanai;
  - iegādājoties un lietojot konkrētas programmas jauninājumus, ja pamatprogramma nav iegādāta legāli;
  - lejupielādējot nelegālas datorprogrammu kopijas no interneta;
  - ienesot darbavietā nelegālos diskus un instalējot programmatūru;
  - citādi pārkāpjot licences vai līguma noteikumus.
- **Nelegālu disku izgatavošana**. Nelikumīgi izgatavoti diski, kas satur datorprogrammu nelegālas kopijas, tiek saukti arī par "kompilācijām". Parasti tie ietver programmatūru vairāku tūkstošu dolāru vērtībā, taču to vērtība melnajā tirgū svārstās no diviem līdz pieciem latiem. Šo disku izplatītāji pat necenšas atdarināt ražotāja noteikto programmas iepakojumu un drošības pazīmes. Šādiem diskiem iepakojuma vai nu vispār nav, vai arī tas ļoti atšķiras no ražotāja noteiktā iepakojuma.
- **Datoru tirgotāju izdarītie pārkāpumi**. Lai veicinātu savas firmas tirgoto datoru noietu, tirgotāji jaunu vai lietotu datoru cietajā diskā instalē datorprogrammu nelegālas kopijas. Bieži vien šāda nelegālu kopiju izplatīšana tiek nosaukta par „speciālu piedāvājumu".
- **Uz serveriem lietotās programmatūras licences noteikumu pārkāpumi**. Jāievēro, ka programmatūra, kas instalēta uz serveriem, arī pakļaujas ražotāja noteikumiem par konkrētās programmas izmantošanu. Lai serverī instalētu programmatūru un to likumīgi varētu lietot vairāki lietotāji (fiksēts skaits), ir jāsaņem attiecīgas ražotāja izsniegtas licences (vai tam jābūt norādītam līgumā). Gadījumi, kad programmu lieto vairāk lietotāju, nekā norādīts licencē, uzskatāmi par pārkāpumiem.

- **Nelegālu datorprogrammu kopiju iegūšana internetā**. Tā kā interneta pieslēgums mūsdienīgā birojā jau ir kļuvis par standartu, tad nelegālu datorprogrammu kopiju iegūšana internetā ir ievērojami pieaugusi. Nelegālu programmu kopijas ļoti vienkārši var tikt lejupielādētas, gandrīz vienmēr anonīmi. Vairumā gadījumu tās tiek piedāvātas vai nu privātās mājaslapās, vai arī uz FTP serveriem. Šāda programmu iegūšana internetā ir uzskatāma par pārkāpumu.
- Te būtu jānošķir gadījumi, kad programmas tiek piedāvātas ražotāju oficiālajās mājaslapās. Šādos gadījumos pats ražotājs piedāvā programmu vai nu par brīvu, vai arī lietotājam tiek dota iespēja norēķināties internetā. Datorprogrammu iegūšana šādā veidā ir uzskatāma par likumīgu, jo šajos gadījumos tiek ievērota autora izteiktā griba.

Par datorprogrammu nelegālu lietošanu var iestāties LR likumdošanā paredzētā atbildība.

5.7.2. VĒL PAR PROGRAMMATŪRAS LICENCI

Programmatūras licence dod tiesības izmantot programmatūru. Saskaņā ar Autortiesību likumu licence ir "līgums, ar kuru viena puse – autortiesību subjekts – dod atļauju otrai pusei – darba izmantotājam – izmantot darbu un nosaka darba izmantošanas veidu, vienojoties par izmantošanas noteikumiem, atlīdzības lielumu, tās izmaksāšanas kārtību un termiņu".

Būtībā, nopērkot disku ar datorprogrammu vai datorspēli, pircējs nopērk nevis pašu programmu, bet gan tiesības to izmantot. Ja programmatūras pircējs ir programmatūru iegādājies no nelegāla tās izplatītāja, tad viņš nav tiesīgs šo programmatūru lietot, jo nav saņēmis programmatūras izstrādātāja atļauju to darīt, bet tas, ka programmatūras pircējam ir datu nesējs ar šo programmatūru, nekādas juridiska rakstura tiesības šim pircējam nerada.

Atbilstoši tiesību aktiem autoram ir piešķirtas tiesības noteikt veidu, kādā viņa darbs (arī datorprogramma) izmantojams, tādējādi licencēšanas noteikumus saskaņā ar Autortiesību likumu izstrādā katrs autors pats. Līdz ar to licencēšanas noteikumi un datorprogrammas komplektācijā iekļautā dokumentācija katram ražotājam ir atšķirīga.

Izstrādātājs licences var iestrādāt gan programmatūrā, gan izplatīt papīra veidā. Atšķirīga ir arī licenču aizsardzība. Piemēram, papīra licences var aizsargāt no kopēšanas ar hologrammu palīdzību. Bieži programmu aktivizēšanai tiek lietoti speciāli unikāli kodi. Vēl viens veids, kā programmatūras izstrādātājs var pasargāt savu produktu, ir reģistrēt visus programmatūras lietotājus. Sarakstu ar tiesīgiem lietotājiem var izmantot autortiesību aizsardzības uzraudzības institūcija, veicot pārbaudes. Šādā veidā izstrādātājs nodrošina sevi ar pierādījumiem strīdīgos gadījumos.

5.7.3. ATKLĀTĀ KODA PROGRAMMATŪRA UN LICENCES

Līdzās komerciālai programmatūras izstrādei un izplatīšanai pastāv arī bezmaksas programmatūra, kurai tomēr mēdz būt sava veida licences. Šāda veida programmatūru sauc par atvērtā koda programmatūru (*open source*

software). Nav vienkārši definēt atvērtā koda programmatūras jēdzienu divos vārdos, jo tai ir daudz kategoriju un variāciju. Pamatprincips, kas raksturo atvērta koda programmatūru, ir brīvība, kuru lietotāji var izmantot, lai

- lietotu programmatūru tā, kā viņi to vēlas, jebkādiem mērķiem, uz jebkuriem datoriem,
- pielāgotu programmatūru savām vajadzībām, ieskaitot kļūdu labošanu, funkcionalitātes uzlabošanu u. tml.,
- izplatītu uzlabotas programmatūras versijas citiem lietotājiem, kuri varētu to izmantot saviem mērķiem uz tādiem pašiem nosacījumiem; savus uzlabojumus izstrādātājs ir tiesīgs piedāvāt bez maksas vai par maksu.

Atvērta koda jeb bezmaksas programmatūras licences var atšķirties. Tajās pamatā ir noteikti šādi principi:

- **atvērtības aizsardzība**. Dažas licences nosaka, lai tālākā uzlabotās programmatūras izplatīšana būtu ar tādu pašu licenci kā iegūtā. Tādējādi visu autoru tiesības būtu vienādas neatkarīgi no tā, vai lietotājs iegūst šo programmu no autora vai starpnieka;
- **morālo tiesību aizsardzība**. Daudzās valstīs likumdošana aizsargā dažas morālas tiesības piemēram, autorības atzīšanu. Dažas licences īpaši pasvītro šo tiesību aizsardzību, nodrošinot to izpildi neatkarīgi no vietējās likumdošanas;
- **īpašumtiesību aizsardzība**. Dažos gadījumos „pirmajam autoram" (personai(-ām), kas sākotnēji izstrādājusi(-ušas) programmatūras pirmo versiju) pieder lielākas tiesības, kuras kaut kādā mērā var pielīdzināt „īpašumtiesībām";
- **saderība ar īpašuma licencēm**. Dažas licences ir izstrādātas tā, ka tās ir pilnīgi nesaderīgas ar īpašuma tiesībām uz programmatūru. Piemēram, tās var aizliegt tālāku programmas izplatīšanu;
- **saderība ar citām atvērtā koda licencēm**. Dažas licences nav saderīgas savā starpā, jo vienas licences noteikumi ir pretrunā ar citas licences noteikumiem. Šajā gadījumā vairākas programmas ar dažādā līmeņa licencēm nevar būt savienotas vienā programmatūrā.

Pasaulē eksistē vairākas plaši pazīstamas standartizētas atvērtā koda licences. Tās ir, piemēram, šādas:

- ***BSD*** *(Berkley Software Distribution). BSD* licence attiecas uz *Berkley Software Distribution* versijām, kā arī uz citu programmatūru. Tas ir labs paraugs „atļaujošai" licencei, kas neuzspiež gandrīz nekādus noteikumus, ieskaitot atļauju izplatīt klientiem programmatūru par maksu bez nepieciešamības iekļaut programmatūras kodu. Tādējādi tālākie izplatītāji var darīt ar programmatūru gandrīz visu, arī izmantot iegūto programmas kodu savā programmatūrā, iegūstot īpašuma tiesības uz to;
- ***GPL*** *(GNU General Public License).* Ar šo licenci tiek izplatītas *GNU* projekta programmas. Tomēr pašreiz var sastapt arī citu programmatūru, kas netiek izstrādāta *GNU* projekta ietvaros, bet ko izplata ar *GPL* licencēm (piemēram, *Linux* versijas). *GPL* licence tika izveidota ar mērķi veicināt bezmaksas atvērtā koda programmatūras izstrādi, un tāpēc tajā ir iekļauti noteikumi, kuri aizliedz *GPL* licencētas programmatūras

izplatīšanu par maksu, kā arī to programmas koda izmantošanu īpašuma programmatūrā. *GPL* licences ļauj tālāk izplatīt šo programmatūru tikai tad, ja programmas kods ir arī pieejams. Tās ļauj veikt izmaiņas un integrēt ar citu programmatūru, ja izveidotā programmatūra arī tiks aizsargāta ar *GPL* licenci. Eksistē arī *LGPL* (*GNU Lesser General Public License*), kuras ļauj integrāciju ar gandrīz visa veida programmām, ieskaitot īpašuma programmas;

- ***MPL** (Mozilla Public License).* Šo licenci izveidojusi *Netscape*, lai izplatītu *Mozilla* kodu un šīs pārlūkprogrammas jaunas versijas. Tā ļoti lielā mērā atgādina *GPL* licences, bet ir vairāk „uzņēmumu orientēta".

5.7.4. KĀ ATŠĶIRT NELICENCĒTU PROGRAMMATŪRU?

Programmatūras legalitātes pazīmes ir šādas:

- konkrētas programmas komplektācijā iekļautā dokumentācija – licence, lietotāja rokasgrāmata un oriģinālie datu nesēji;
- līgums (arī darba līgums) ar datorprogrammas izstrādātāju;
- dokuments, kas apliecina autora atļauju konkrētai personai izmantot viņa radīto datorprogrammu;
- rēķins un pavadzīme, bet tikai komplektācijā ar konkrētās datorprogrammas licenci vai līgumu ar ražotāju vai citiem legalitāti apliecinošiem atribūtiem;
- internetā iegādātas programmatūras legalitāti var apliecināt attiecīgā bankas konta vai kredītkartes izraksts, kurā redzams programmatūras iegādes fakts vai cits pirkuma faktu apliecinošs dokuments.

Ja datorprogramma ir iekļauta kādas iekārtas (piemēram, skenera vai printera dziņa u. tml.) komplektācijā, tad šīs programmatūras legalitāti apliecina rēķins par šīs iekārtas iegādi un tai pievienotā dokumentācija.

5.8. KONTROLJAUTĀJUMI

1. Kas ir intelektuālais īpašums?
2. Kāda starptautiska organizācija nodarbojas ar intelektuālā īpašuma strīdu tiesisko regulēšanu?
3. Nosauciet intelektuālā īpašuma objektus e-vidē un pastāstiet par to tiesisko regulējumu!
4. Kas ir autortiesības, kā tās iedala, un kādas tiesības tās dod izstrādātājam un darba devējam?
5. Kādā veidā autors var kontrolēt savas autortiesības?
6. Kas ir jāzina programmatūras izstrādātājam par autortiesībām?
7. Kāpēc tiek aizsargātas autortiesības?
8. Kas ir programmatūras licence? Kāpēc programmatūra ir jālicencē?

6. PROGRAMMATŪRAS IZSTRĀDES GALAPRODUKTS. PATĒRĒTĀJU AIZSARDZĪBAS JAUTĀJUMI

Nodaļa izstrādāta, izmantojot [24].

6.1. IEVADS

IKT nozares attīstība un tās ietekme uz mūsu dzīvi ir aplūkota no dažādām pusēm – no jaunu, kvalitatīvi atšķirīgu pakalpojumu puses, kā arī no informācijas, dokumentu un citu esošo objektu pārnešanas virtuālajā vidē. Taču visam pamatā ir programmprodukts, ko veido izstrādātāji un ko lieto patērētāji dažādās jomās.

Programmprodukts un tā pārdošanas, pirkšanas un tālākās attīstības un uzturēšanas principi zināmā mērā atšķiras no līdzīgām darbībām ar citiem produktiem, piemēram, mēbelēm, pārtikas, apģērbiem. Kādas tad ir atšķirības? Un kā šīs attiecības starp izstrādātāju un klientu tiek regulētas?

6.2. PROGRAMMPRODUKTS PATĒRĒTĀJU TIRGŪ

6.2.1. VAI PROGRAMMATŪRA VAR BŪT "NO TRŪKUMIEM BRĪVA"?

Viens no pašiem svarīgākajiem informācijas tehnoloģijas sfēras pamatprincipiem ir princips "kā ir" (*"as is"*). Tas nosaka, ka visa izstrādātā programmatūra klientam tiek piegādāta tādā stāvoklī, kādā tā ir attiecīgās piegādes brīdī, turklāt ar visām šīs programmatūras kļūdām, defektiem un citiem trūkumiem.

Neviens programmatūras izstrādātājs nekad nav apgalvojis un apzināti arī nekad neapgalvos, ka viņa izstrādātā programmatūra ir "no trūkumiem brīva" (*"defect free"*). Tas ir otrs ļoti svarīgs informācijas tehnoloģijas sfēras princips, kas papildina jau iepriekš minēto principu "kā ir". Šie abi principi ir tik svarīgi tāpēc, ka, izstrādājot programmatūru, neviens ražotājs principā nevar nodrošināt to, lai izstrādātā programmatūra būtu pilnīgi bez jebkādām kļūdām un citiem trūkumiem. No algoritmu teorijas pamatteorēmām izriet, ka nav iespējams konstatēt, vai programmā nav kļūdu. Tas, protams, nenozīmē, ka visās izstrādātajās programmās ir ļoti daudz trūkumu, jo dažās to var būt pavisam nedaudz vai arī tie var būt gandrīz nepamanāmi, taču lietas būtību tas nemaina.

Šeit varētu pieminēt, ka pat tādām iestādēm vai organizācijām, kuras strādā paaugstināta riska apstākļos vai kuru darbība ir saistīta ar sabiedrībai bīstamām lietām, piemēram, ķīmisko ieroču rūpnīcām, atomstacijām vai aviācijas un kosmosa lidojumu vadības centriem, netiek garantēts, ka izmantojamā

programmatūra būs pilnīgi bez jebkādiem trūkumiem. Protams, šādos gadījumos programmatūra papildus tiek daudzkārt un nopietni pārbaudīta, taču tas viss ļoti sadārdzina programmatūras izstrādes procesu, un pat tad nekādas garantijas dotas netiek.

Runājot par programmatūru, netiek domātas *„Hello world"* tipa programmas, kuras sastāv no 5–10 programmas koda rindiņām. Apjomīgas un sarežģītas programmas tiek uzskatītas par ļoti kvalitatīvām, ja uz 10 000 programmatūras koda rindiņām vidēji ir atrodamas 3 kļūdas.

Lai gan programmatūras ražotājs veic nopietnu testēšanu, ik pa laikam praksē sastopami gadījumi, kad programmatūras kļūdu dēļ tās lietotājiem rodas jūtami vai pat nopietni zaudējumi.

! *Ir bijuši gadījumi, kad banku sistēmas kļūdas dēļ no viena norēķinu konta pēkšņi pazūd lieli naudas līdzekļi vai, tieši otrādi, kāds pēkšņi kļūst par ļoti turīgu cilvēku. Vēl sliktāk ir tad, ja no šīs programmatūras ir atkarīga cilvēku dzīvība. Piemēram, lidmašīnas aparatūras programma paziņo aplamus datus pirms nosēšanās. Programmatūras drošības kļūdu dēļ var tikt apdraudētas valsts un sabiedrības intereses. Piemēram, ja kādā svarīgā informācijas sistēmā tiek atrasts drošības „caurums", konfidenciāla informācija kļūst pieejama un to var izmantot ļaunos nolūkos.*

Analizējot iepriekš aprakstītos principus, var secināt to, ka pircējs maksā ne tikai par pašu programmatūru, bet arī par tajā esošajām kļūdām un nepilnībām, jo ir šos programmatūras trūkumus iegādājies kopā ar pašu programmatūru.

Pārsvarā visu starptautisko kompāniju programmatūras licencēšanas noteikumos papildus jau iepriekš minētajiem principiem "kā ir" un "no trūkumiem brīva" ir iekļauts arī šāds punkts: "Mēs garantējam, ka programma pamatā darbosies atbilstoši konkrētajā programmas dokumentācijā aprakstītajam vienu gadu pēc tam, kad būsim jums tās piegādājuši" [25]. Vārds „pamatā" nozīmē to, ka izstrādātājs vēlreiz netieši uzsver, ka viņa izstrādātā programmatūra var arī nedarboties, kā tai ir paredzēts. Un šīs garantijas par programmas darbību atbilstoši dokumentācijai ir arī vienīgās garantijas, kuras izstrādātājs dod pircējam attiecībā uz iegādāto programmatūru.

6.2.2. ATBILDĪBA

Ja izstrādāto programmatūru pircējs iegādājas komplektā ar tajā esošajām kļūdām un nepilnībām, tad tas nozīmē, ka tikai un vienīgi pircējs pats ir atbildīgs par šīs programmatūras spēju darboties. Tāds ir arī visu programmatūras izstrādātāju uzskats. Tāpēc, pārdodot savu programmatūru, izstrādātāji nesniedz pircējam pilnīgi nekādas garantijas attiecībā uz šīs programmatūras spēju darboties.

Protams, šādai programmatūrai ir nepieciešami kļūdu labojumi. Tos programmatūras izstrādātājs piedāvā par atsevišķu samaksu.

Programmatūru var iegādāties divos dažādos veidos – pasūtot programmatūras izstrādi un noslēdzot sadarbības līgumu ar izstrādātāju vai arī nopērkot jau gatavu programmproduktu no ražotāja vai izplatītāja.

Pirmajā gadījumā kļūdu labošana parasti tiek noformēta ar atsevišķu līgumu, kuru sauc par „Tehniskā atbalsta pakalpojumu līgumu" vai „Programmatūras uzturēšanas līgumu" un kurā ir noteikta gada „abonēšanas" maksa. Izmaksas parasti tiek noteiktas 15–20% apjomā no iegādātās programmatūras tirgus vērtības.

Otrajā gadījumā izstrādātājs var noformēt kļūdu labošanu kārtējā programmprodukta versijā, piegādājot lietotājiem jauninājumu *(upgrade)* par atsevišķu samaksu.

Pircējs, protams, var šādus kļūdu novēršanas pakalpojumus nepasūtīt. Taču jāpiebilst, ka pats pircējs šīs kļūdas programmatūrā labot nav tiesīgs, jo programmatūru aizsargā autortiesības, kas nepieļauj darba pārveidošanu bez autora piekrišanas, un arī pats autors (mūsu gadījumā tas ir izstrādātājs) visbiežāk licencē vai līgumā atrunā savas tiesības, kategoriski aizliedzot iespēju pircējam pašam labot jebkādas programmatūrā atrastās kļūdas vai pasūtīt kļūdu labošanu pie cita programmatūras izstrādes pakalpojumu sniedzēja.

Pieminēšanas vērts ir arī fakts, ka gandrīz visi starptautiskie informācijas tehnoloģijas sfērā darbojošies uzņēmumi ir noteikuši, ka pircējam, sākotnēji iegādājoties programmatūru, obligāti ir jāpērk arī iepriekšminētais abonements par pirmo programmatūras lietošanas gadu. Sākot ar otro programmatūras lietošanas gadu, pircējs šos pakalpojumus var nepasūtīt, taču, ja šis pircējs vēlāk tomēr pārdomās un šos pakalpojumus pasūtīs, tad viņam būs jāmaksā pilna pakalpojumu maksa arī par visu šo pakalpojumu nepasūtīšanas laikposmu. Tas ir loģiski, jo pēdējā programmatūras versijā ir iekļauti visu šo gadu laikā atrasto kļūdu labojumi. Izstrādātājs nevar piegādāt 1. un 4. gada kļūdu labojumus. Tomēr juridiski šādu procesu varētu uzskatīt par netaisnīgu līguma noteikumu uzspiešanu.

6.2.3. MATERIĀLIE ZAUDĒJUMI

Ja izstrādātājs atzīst, ka programmatūrā var būt kļūdas, tad tas nozīmē, ka pastāv teorētiska iespēja, ka šo kļūdu rezultātā pircējam var tikt nodarīti materiālie zaudējumi. Taču arī šo jautājumu izstrādātājs praksē vienpusēji ir atrisinājis un ne jau par sliktu sev.

Izstrādātājs, pārdodot programmatūru, vienlaikus deklarē savu atsacīšanos no jebkādas atbildības par zaudējumiem, kas radušies vai varētu rasties šīs programmatūras lietošanas rezultātā, un viss risks par iespējamiem materiālajiem zaudējumiem tiek nodots pircējam. Tas ir viens no strīdīgākajiem jautājumiem, jo no atbildības neviens nevar tik vienkārši atteikties. Atbildība pēc savas būtības ir nevis programmatūras izstrādātāja tiesība, bet gan viņa pienākums.

Attiecībā uz iespējamiem zaudējumiem, kuri varētu rasties pircējam programmatūras izmantošanas rezultātā, visi programmatūras izstrādātāji no šādas atbildības jau iepriekš atsakās.

Papildus tam programmatūras izstrādātājs ir noteicis, ka programmatūras pircēja pienākumos ietilpst programmatūras datu rezerves kopēšana un arhivēšana. Tas ļauj programmatūras izstrādātājam ne tikai daļēji nodot

atbildību programmatūras pircējam, bet arī nodrošināt sevi: ja programmatūras pircējs nebūs veicis datu rezerves kopēšanu un arhivēšanu, tad par visiem zaudējumiem būs atbildīgs pats pircējs. Savukārt, ja programmatūras pircējs būs veicis visu nepieciešamo datu rezerves kopēšanu un arhivēšanu, tad iespējamie zaudējumi nevarētu būt nesamērīgi lieli.

6.2.4. STRĪDU IZSKATĪŠANA

No juridiskā aspekta visinteresantāko veidu, turklāt ar vairākiem līmeņiem, kā atteikties no atbildības, praktizē pasaulē otra lielākā programmatūras izstrādes kompānija *Oracle Corporation*. Šī kompānija savos programmatūras licencēšanas un izmantošanas noteikumos ir noteikusi, ka tā neuzņemas pilnīgi nekādu atbildību par pircējam nodarītiem zaudējumiem, kas tam radušies iegādātās programmatūras lietošanas rezultātā. Tā ir pirmā līmeņa atteikšanās no atbildības.

Otrā līmeņa atteikšanās no atbildības nosaka: ja tomēr jebkādu apstākļu dēļ pircējam izdodas pierādīt, ka programmatūras izstrādātājam ir jāatbild par pircējam radītajiem zaudējumiem, tad šī programmatūras izstrādātāja kopējais pieļaujamais atbildības apmērs tiek ierobežots un noteikts apjomā, kas ir vienāds ar pircēja iegādātās programmatūras tirgus vērtību.

Trešais līmenis nosaka, ka tad, ja pret pircēju kaut kādu apstākļu dēļ tomēr nevar izmantot otrajā līmenī noteikto atbildības apjoma ierobežojumu, kopējā programmatūras izstrādātāja atbildība tiek noteikta, piemēram, USD 500 000 apmērā.

Šādu dažādu atbildības līmeņu noteikšana jebkurā gadījumā apgrūtina pircējam iespēju saņemt atlīdzību par nodarītajiem zaudējumiem, kas tam radušies iegādātās programmatūras lietošanas rezultātā, jo pircējam tad ir pienākums tiesiskā veidā pārvarēt visus šos trīs programmatūras izstrādātāja noteiktos aizsardzības līmeņus un pierādīt, ka pircēja lietas ietvaros šie ierobežojumi nevar tikt piemēroti.

Vēl viens papildu aizsardzības pasākums pret to, lai programmatūras izstrādātāja noteikto programmatūras licencēšanas un lietošanas noteikumu piemērošanai nebūtu nekādu tiesisku šķēršļu nevienā valstī, ir tāds, ka programmatūras izstrādātājs pats jau ir norādījis valsti un likumus, pēc kuriem tiks apspriestas programmatūras pircēja un izstrādātāja savstarpējās attiecības. Pārsvarā visu civilizēto valstu likumdošanā ir paredzētas šādas kolīziju normas, kas atļauj piemērot citu valstu likumus attiecībām, kuras radušās privāto tiesību sfērā.

Šādā veidā programmatūras izstrādātājs ir panācis, ka tad, ja viņa izstrādātie programmatūras licencēšanas un lietošanas noteikumi atbilst, piemēram, ASV likumdošanai, programmatūras pircējam, lai piedzītu zaudējumus, kas tam radušies programmatūras lietošanas rezultātā, ar izstrādātāju būs jātiesājas ASV un saskaņā ar ASV spēkā esošajām tiesību normām.

Arī Latvijas Republikas Civillikumā ir paredzēta iepriekš pieminētā kolīziju norma, kas ļauj līgumslēdzēju pusēm brīvi izraudzīties likumus, pēc kuriem nākotnē tiks apspriestas viņu savstarpējās attiecības.

6.3. IKT UN PATĒRĒTĀJU AIZSARDZĪBA

6.3.1. PATĒRĒTĀJS UN PROGRAMMPRODUKTS

Latvijā patērētāju tiesības tiek aizsargātas ar LR Patērētāju tiesību aizsardzības likumu [26]. Tā 1. pants noteic, ka patērētājs ir ''fiziskā vai juridiskā persona, kas izsaka vēlēšanos iegādāties, iegādājas vai varētu iegādāties preci vai izmantot pakalpojumu nolūkam, kurš nav tieši saistīts ar tās uzņēmējdarbību''. Šāds likumā dots patērētāja skaidrojums nozīmē to, ka visi tie programmatūras pircēji, kuri šo programmatūru iegādājas nolūkā izmantot to savā uzņēmējdarbībā, par patērētājiem netiek uzskatīti un attiecībā uz šiem programmatūras pircējiem patērētāja tiesību aizsardzības normas nevar tikt piemērotas.

Jāsecina, ka pārsvarā par patērētājiem, protams, ar nelieliem izņēmumiem, likuma izpratnē tiek atzītas fiziskas personas, kuras attiecīgo programmatūru ir iegādājušās, lai lietotu to nekomerciāliem mērķiem jeb savām personiskajām vajadzībām.

Ja no tiem programmatūras pircējiem, uz kuriem var attiecināt patērētāja tiesību aizsardzības normas, vairums ir fiziskas personas, kuras šo programmatūru iegādājas specializētajos veikalos, tad būtu nevietā runāt par to, ka programmatūras izstrādātājam ar katru tās pircēju vajadzētu diskutēt un atsevišķi vienoties par katra programmatūras pārdošanas līguma noteikumiem. Šādā veidā izplatīto programmatūru vajadzētu uzskatīt par plaša patēriņa preci, kuru pārdodot ir lietderīgi izstrādāt un visiem piedāvāt standarta līguma noteikumus. Tas arī nav pretrunā ar likumdošanas prasībām, jo, nopērkot veikalā programmatūru, pircējs ar to ir devis savu *akceptu* (piekrišanu) programmatūras izstrādātāja *ofertei* (piedāvājumam) šo programmatūru iegādāties.

Pievērsīsimies tiem patērētāju aizsardzības principiem, kuru izpratne materiālajā pasaulē ir nostiprinājusies, bet attiecībā uz IKT sfēru var šķist pretrunīga.

Patērētāju tiesību aizsardzības likuma 3. pants noteic, ka ''Patērētāja tiesības ir pārkāptas, ja:

- iegādājoties preci vai saņemot pakalpojumu, nav ievērota patērētāja izvēles brīvība un viņa izteiktā griba;
- nav ievērots līgumslēdzēju pušu vienlīdzības princips un līguma noteikumi ir netaisnīgi; …''.

Tātad sākotnēji varam secināt, ka, lietojot tādus pakalpojumu sniegšanas nosacījumus, kādi ir informāciju tehnoloģijas sfērā (izstrādātāja atteikšanās no atbildības u. c.), ir pārkāptas vismaz divas ar likumu aizsargātas patērētāja tiesības.

Kā jau iepriekš minēts, programmatūras izstrādātājs ne tikai nesniedz programmatūras pircējam nekādas garantijas par programmatūras spēju darboties, bet vēl vairāk – pat tieši apgalvo, ka programmatūra nav bez kļūdām un ka programmatūra tikai pamatā darbosies atbilstoši tās dokumentācijai. Turklāt programmatūras izstrādātājs par savu kļūdu novēršanu pārdotajā programmatūrā no programmatūras pircēja prasa papildu samaksu.

Savukārt likumdevējs patērētāja tiesību aizsardzībai ir noteicis, ka „patērētājs ir tiesīgs pieteikt prasījumu ražotājam, pārdevējam vai pakalpojuma

sniedzējam attiecībā uz konstatētajiem preces vai pakalpojuma trūkumiem tūlīt pēc to atklāšanas, bet ne vēlāk kā gada laikā no preces iegādes vai pakalpojuma saņemšanas dienas".

Runājot par programmatūras kļūdām, jāizskata trīs Patērētāju aizsardzības likuma punkti.

''(1) Ražotājs, pārdevējs vai pakalpojuma sniedzējs ir tiesīgs piedāvāt un pārdot nepienācīgas kvalitātes preci vai sniegt šādu pakalpojumu tikai gadījumos, kad tas ir nodrošinājis preces vai pakalpojuma drošumu un nekaitīgumu, kā arī pirms līguma slēgšanas informējis patērētāju par nepienācīgu kvalitāti, norādot uz trūkumiem, un patērētājs ir piekritis iegādāties šādu preci vai saņemt šādu pakalpojumu.

(2) Uzskatāms, ka patērētājs ir piekritis iegādāties nepienācīgas kvalitātes preci vai saņemt šādu pakalpojumu, ja uz pirkumu vai pakalpojumu apliecinoša dokumenta ir pārdevēja izdarīta atzīme par nepienācīgu kvalitāti.

(3) Nepienācīgas kvalitātes preces pārdošanai jābūt norobežotai no pārējo (kvalitatīvo) preču pārdošanas, un tās pārdošanas vietā jābūt informācijai par nepienācīgu kvalitāti. Preces cenas pazemināšana (nocenošana, atlaides) vai preču izpārdošanas izsludināšana nav pielīdzināma informācijai par nepienācīgu kvalitāti.''

Iepazīstoties ar šiem likumā noteiktajiem izņēmumiem, jāsecina, ka programmatūras izstrādātāja rīcība, pārdodot savu programmatūru, neatbilst nevienam no iepriekš minētajiem izņēmumiem, jo izstrādātājs, pārdodot programmatūru, nevar konkrēti norādīt uz tās trūkumiem. Pirmkārt, programmatūras izstrādātājs apzinās, ka programmatūrā ir kļūdas, taču viņš nezina, tieši kādas, un tāpēc nav spējīgs šim programmatūras pircējam norādīt uz konkrētajiem preces trūkumiem. Otrkārt, pārdodot programmatūru, uz pirkuma rēķina nekad netiek norādīts, ka programmatūrai ir nepienācīga kvalitāte. Un treškārt, programmatūra nekad netiek tirgota speciāli norobežotā nekvalitatīvu preču stendā.

Šeit atkal jākonstatē pretrunas starp patērētāja tiesībām, no vienas puses, un informācijas tehnoloģijas sfērā lietotiem programmatūras pārdošanas principiem, no otras puses. Arī tas, ka programmatūras izstrādātājs garantē tikai to, ka programmatūra pamatā darbosies atbilstoši tās dokumentācijai, ir pretrunā ar likumu, kurš nosaka:

"(1) Prece uzskatāma par nepienācīgas kvalitātes preci, ja:

- tā neatbilst tiesību aktu vai normatīvtehnisko dokumentu prasībām un līguma noteikumiem; ...
- tā nav derīga mērķiem, kuriem patērētājs izvēlējies preci un par kuriem tas tieši vai netieši paziņojis pārdevējam, slēdzot līgumu, izņemot gadījumus, kad pārdevējs pārdošanas laikā nevarēja saprast šādus speciālus mērķus un patērētājam nebija pamatota iemesla paļauties uz pārdevēja kompetenci un spriedumu; …

(2) Pakalpojums uzskatāms par nepienācīgas kvalitātes pakalpojumu, ja:

- to sniedzot, nav ievērotas tiesību aktu vai normatīvtehnisko dokumentu prasības, nav ievēroti līguma noteikumi vai tam ir citi būtiski trūkumi…'', jo patērētājam ir tiesības preci iegādāties un pakalpojumus saņemt atbilstoši visām tām prasībām, par kurām puses (pircējs un pārdevējs) ir vienojušās.

Tādējādi, ja programmatūras pircējs, iepazīstoties ar programmatūras dokumentāciju, nolemj, ka viņam šāda programmatūra ir nepieciešama, bet, iegādājoties šo programmatūru, tā darbojas tikai pamatā atbilstoši dokumentācijai, pie tam vēl ar kļūdām, tad patērētāja likumīgās intereses var uzskatīt par aizskartām no programmatūras izstrādātāja puses. Līdz ar to, aplūkojot patērētāja tiesību aizsardzības tiesisko regulējumu, var secināt, ka, to nosakot, likumdevējs nav paredzējis un nav ņēmis vērā jaunās nozares – informācijas tehnoloģijas objektīvi pamatotās prasības. To vēl vairāk apliecina likumdevēja noteiktie patērētāja tiesību aizskārumu novēršanas pasākumi.

Piemēram, Patērētāju tiesību aizsardzības likuma 28. pants nosaka:
''(1) Patērētājs, kam pārdota vai nodota lietošanā nepienācīgas kvalitātes prece, ir tiesīgs pieprasīt, lai ražotājs vai pārdevējs veiktu vienu no šādām darbībām:

- attiecīgi samazinātu preces cenu;
- bez atlīdzības novērstu preces trūkumus vai atlīdzinātu patērētājam izdevumus par trūkumu novēršanu;
- apmainītu preci pret pienācīgas kvalitātes tādu pašu vai ekvivalentu preci;
- atceltu līgumu un atmaksātu patērētājam par preci samaksāto naudas summu...

(4) Šā panta pirmajā daļā minēto tiesību izmantošana neizslēdz patērētāja tiesības pieprasīt zaudējuma atlīdzību vai līgumsoda samaksu.''

No iepriekšminētā likuma panta izriet, ka programmatūras pircējs ir tiesīgs prasīt preces cenas samazināšanu, un tas nozīmē, ka programmatūras izstrādātājs ir pakļauts nepamatotam riskam, jo šādu cenu samazinājumu var pieprasīt pilnīgi visi programmatūras pircēji. Pat vēl vairāk, daži no iepriekšminētajā pantā noteiktajiem patērētāja tiesību aizsardzības mehānismiem ir ne tikai neloģiski pēc savas būtības, bet pat rada dažādu likumu kolīzijas.

! *Tā, piemēram, nosacījums, ka patērētājs drīkst prasīt, lai nekvalitatīvā prece tiktu apmainīta pret pienācīgas kvalitātes tādu pašu vai ekvivalentu preci, ir neloģisks. Apmainot programmatūru pret tādu pašu programmatūru, patērētājs iegūst identiski kvalitatīvu vai attiecīgi nekvalitatīvu preci, jo visas programmatūras kopijas ir vienādas un savā starpā pilnīgi ne ar ko neatšķiras. Savukārt tas, ka likumdevējs ir noteicis patērētājam tiesības pašam novērst preces (programmatūras) trūkumus, bet radušos izdevumus pieprasīt no programmatūras izstrādātāja, jau rada likumu kolīziju. Autortiesību likums nosaka, ka jebkādas izmaiņas programmatūrā var veikt tikai autors vai persona, kam pieder autora mantiskās tiesības. Mūsu gadījumā tas ir programmatūras izstrādātājs.*

6.3.2. PROBLĒMU RISINĀJUMS

Aplūkojot kopumā šīs dažādajos likuma pantos noteiktās patērētāja tiesības, sākotnēji var šķist, ka informācijas tehnoloģijas sfērā lietotie pakalpojumu sniegšanas principi ir lielā pretrunā ar likumu un patērētājam tiek nepārprotami uzspiesti netaisnīgi līguma noteikumi. Šo sākotnējo uzskatu vēl vairāk apstiprina tas, ka programmatūras pircējs ne tikai pirms programmatūras iegādes nekādā veidā nespēj šos noteikumus ietekmēt, bet arī tas, ka

pats programmatūras pircējs ar šiem noteikumiem var iepazīties tikai pēc programmatūras iegādes, jo visi programmatūras licencēšanas noteikumi atrodas kastītē, kurā glabājas šī programmatūra, un tā tiek attaisīta tikai pēc pašas programmatūras iegādes.

Taču visi šie būtiskie patērētāja tiesību pārkāpumi, ja šo jautājumu sāk analizēt, tik viennozīmīgi nemaz nevar tikt uzskatīti par patērētāja tiesību aizskārumiem.

Neņemot vērā visu iepriekš apskatīto, ir jānoskaidro, ko tad programmatūras pircējs, ieejot veikalā un nopērkot programmatūru, īsti ir iegādājies. Šeit seko interesanta atklāsme – programmatūras pircējs ir iegādājies nevis pašu programmatūru, bet gan tikai tiesības lietot šo programmatūru. Pat vēl vairāk, programmatūras pircējs šo kastīti ar programmatūras datu nesējiem ir saņēmis pilnīgi par velti, bet visa programmatūras pircēja samaksātā nauda ir ieguldīta par šīm iepriekšminētajām tiesībām šo programmatūru lietot.

No tā var secināt, ka kastīte ar programmatūras datu nesējiem šim programmatūras pircējam tiek nodota, lai programmatūras pircējs varētu savas iegūtās tiesības pienācīgi izmantot.

Jāpiebilst, ka nav pat svarīgi, vai programmatūras pircējs programmatūras kopiju ir iegādājies veikalā vai no kāda nelegāla šīs programmatūras izplatītāja, jo, lai šo programmatūru tas būtu tiesīgs lietot, iepriekš ir jāsaņem programmatūras izstrādātāja atļauja jeb licence.

Autortiesību likums nosaka: ''lai iegūtu darba izmantošanas tiesības, darba izmantotājiem attiecībā uz katru darba izmantošanas veidu un katru darba izmantošanas reizi jāsaņem autortiesību subjekta atļauja''. Tātad vienīgais un nepieciešamais priekšnosacījums legālai programmatūras izmantošanai ir programmatūras izstrādātāja sniegtā atļauja. Pērkot veikalā programmatūru, tās pircējam šī tiesiskā darījuma rezultātā tiek automātiski piešķirta licence šo programmatūru lietot, jo programmatūras izstrādātājs ir noteicis, ka pircējs ar to, ka iegādājas programmatūru, vienlaikus izsaka savu akceptu attiecībā uz programmatūras lietošanas noteikumiem jeb, juridiski izsakoties, veikalā tiek noslēgts licences līgums starp programmatūras pircēju un programmatūras izstrādātāju.

Savukārt, ja programmatūras pircējs ir programmatūru iegādājies no nelegāla tās izplatītāja, tad viņš nav tiesīgs šo programmatūru lietot, jo nav saņēmis programmatūras izstrādātāja atļauju to darīt, bet tas, ka programmatūras pircējam ir datu nesējs ar šo programmatūru, nekādas juridiska rakstura tiesības šim pircējam nerada.

Likumā ir konkrēti noteikts, ka ''autora tiesības nav saistītas ar īpašumtiesībām uz materiālo objektu, kurā darbs ir izteikts. Autora tiesības uz darbu, kas izteikts kādā materiālā objektā, šķiramas no šā objekta valdījuma. Materiālā objekta ... valdījuma pāreja pati par sevi nerada šā darba autora tiesību pāreju.''

Atgriežoties pie patērētāja tiesību aizsardzības normām, ar kurām likumdevējs aizsargā patērētāju pret nekvalitatīvas preces vai nekvalitatīvu pakalpojumu saņemšanu, jāsecina, ka par "tiesībām" likumdošanā nekas nav noteikts.

Un tas arī būtu saprotami, jo *tiesības* nevar būt nekvalitatīvas, tiesības kādam vai nu ir, vai arī šo tiesību kādam nav. Un, ja uz programmatūras licencēšanu lūkojas no pozīcijām, ka programmatūras pircējs iegādājas tikai tiesības lietot šo programmatūru, tad būtu jāatzīst, ka patērētāja tiesību aizsardzības regulējošās normas vispār nevar tikt piemērotas informācijas tehnoloģijas sfērā. Jo, pirmkārt, programmatūras izstrādātājs ar tiesību piešķiršanas brīdi programmatūras pircējam lietot kādu konkrētu programmatūru, par kuru tas, protams, iepriekš ir saņēmis noteiktu atlīdzību, būtu savas saistības pret programmatūras pircēju pilnībā izpildījis, otrkārt, kā jau iepriekš minēts, programmatūras pircējam piešķirtās lietošanas tiesības nekad nebūtu un arī nevarētu būt nekvalitatīvas.

No visa iepriekš rakstītā var secināt, ka likumdevējs, veidojot patērētāja aizsardzības tiesisko regulējumu, vienkārši nav iedomājies par šādu iepriekš aprakstīto un ar informācijas tehnoloģijas sfēru saistīto juridiski līdz galam neatrisināto jautājumu. Un, kamēr likumdevējs nebūs devis iepriekš aprakstītās problēmas tiesisko regulējumu, tikmēr vislielākais cietējs būs patērētājs, persona, kuras tiesības likumdevējs ir centies aizsargāt.

6.4. KONTROLJAUTĀJUMI

1. Vai programmatūra var būt bez kļūdām? Ko nozīmē jēdziens "brīva no trūkumiem"?
2. Ar kādām pretrunām saduras patērētāju aizsardzības likums, kad tas tiek lietots programmatūras pircēju aizsardzībai?
3. Ko iegūst pircējs, nopērkot programmatūru?
4. Kādā veidā var atrisināt pretrunas, kuras rodas, attiecinot Patērētāja tiesību aizsardzības likumu uz programmproduktiem?

7. FIZISKO PERSONU DATU AIZSARDZĪBA

Nodaļa izstrādāta, izmantojot [1, 154.–181., 27.–29. lpp.].

7.1. IEVADS

Straujas informācijas tehnoloģijas attīstības rezultātā liels daudzums no apstrādājamās informācijas attiecas tieši uz fiziskajām personām. Šo informāciju sauc par personas datiem un izmanto dažādās valsts un pašvaldību institūcijās, kā arī uzņēmējdarbībā. Personas datu aizsardzība ir jārisina kopumā gan kā tehniska rakstura problēma, gan arī kā juridiska problēma. Dažas no Eiropas valstīm jau kopš 1970. gada ir pieņēmušas tiesību aktus, kas aizsargā tās fundamentālās personu tiesības uz privātumu, kuras tiek apdraudētas, apstrādājot personas datus.

Personas datu aizsardzība ir aplūkojama kā viena no cilvēktiesībām, konkrēti – tiesībām uz privāto dzīvi jeb privātumu. Tās ir garantētas

- gan ANO 1948. gada "Vispārējā cilvēktiesību deklarācijā" (12. pants) [30],
- gan ANO 1966. gada "Starptautiskajā paktā par pilsoņu un politiskajām tiesībām" (17. pants).

Latvijā šīs tiesības nodrošina Latvijas Republikas Augstākās Padomes deklarācija "Par Latvijas Republikas pievienošanos starptautisko tiesību dokumentiem cilvēktiesību jautājumos".

Arī 1950. gada Eiropas Cilvēka tiesību un pamatbrīvību aizsardzības konvencijas [31] 8. pants paredz:

- ikvienam ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību,
- sabiedriskās institūcijas nedrīkst traucēt nevienam baudīt šīs tiesības, izņemot gadījumus, kas paredzēti likumā un ir nepieciešami demokrātiskā sabiedrībā, lai aizstāvētu valsts drošības, sabiedriskās kārtības vai valsts labklājības intereses, lai nepieļautu nekārtības un noziegumus, lai aizsargātu veselību un morāli vai lai aizstāvētu citu tiesības un brīvības.

Konvencijas 10. pants paredz informācijas, uzskatu paušanas brīvību. Personas datu aizsardzības pamatā ir šo divu pamattiesību – brīvu uzskatu paušanas un privātās dzīves neaizskaramības – sabalansēšana.

Personas datu aizsardzība tieši ir minēta vairākos vispārīga rakstura starptautiskos tiesību aktos. Tā, piemēram, Līgumā par Eiropas Savienību (Māstrihtas līgumā [32]), 286. pantā, un Amsterdamas līgumā [33], kas groza Līgumu par Eiropas Savienību, Eiropas Kopienu dibināšanas līgumus un dažus ar tiem saistītus aktus, 30. pantā, ir noteikts, ka, apstrādājot (glabājot, nododot utt.) personas datus, tiek ievēroti visi Eiropas Savienībā izstrādātie personas datu aizsardzību reglamentējošie tiesību akti.

Jauns attīstības posms personas datu aizsardzības jomā ir saistīts ar 1981. gadu, kad Eiropas Padome pieņem "Konvenciju par personu aizsardzību attiecībā

uz automātisko personas datu aizsardzību" (turpmāk – 108. konvenciju). 108. konvencija iedibina personu aizsardzības pamatprincipus, kas rodas, apstrādājot personas datus. Vairums Eiropas valstu ir to parakstījušas un ratificējušas. Latvija to ratificēja 2001. gada 5. aprīlī, un tā stājās spēkā 2001. gada 1. septembrī.

7.1.1. ELEKTRONISKI APSTRĀDĀTI PERSONAS DATI

Desmit gadus vēlāk ANO pieņēma vadlīnijas *(United Nations Guidelines concerning computerized personal data files)*, kas attiecas uz automātiski apstrādātu personas datu aizsardzību. Ekonomiskās sadarbības un attīstības organizācija (EDSO) pieņēma "Privātuma un personas datu pārrobežas plūsmas vadlīnijas" *(Guidelines on the protection of privacy and transborder flows of personal data)* un "Informācijas sistēmu drošības vadlīnijas" *(Guidelines for the Security in Informations Systems)*. Patlaban un arī tuvākajā laikā nav plānota Latvijas iestāšanās EDSO, un līdz ar to mums nav saistošas EDSO vadlīnijas. Tomēr tās ir jāņem vērā, lai Latvijā izveidotu starptautiskajām tiesību normām atbilstošu personas datu aizsardzības sistēmu.

Attiecībā uz personas datu aizsardzību 1995. gadā Eiropas Savienībā tika pieņemta Direktīva 95/46 [34], kurā jau daudz precīzāk definētas personas datu aizsardzības normas.

7.1.2. PERSONAS DATU AIZSARDZĪBA LATVIJĀ

Pēc neatkarības atgūšanas no 1991. gada 10. decembra Latvijā bija spēkā Konstitucionālais likums "Cilvēka un pilsoņa tiesības un pienākumi", kura 16., 17. un 30. pants reglamentēja personas privātuma aizsardzību un tiesības brīvi iegūt un izplatīt informāciju. Šis likums zaudēja spēku 1998. gada 6. novembrī, kad stājās spēkā Grozījumi Latvijas Republikas Satversmē (15.10.1998), papildinot to ar nodaļu par cilvēktiesību un brīvību aizsardzību. Satversmes 96. pants nosaka: "Ikvienam ir tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību."

Satversmes 100. pants ikvienam paredz tiesības uz vārda brīvību. Tās ietver gan tiesības iegūt, paturēt un izplatīt informāciju, gan tiesības brīvi paust savus uzskatus. Tā kā personas datu aizsardzības tiesību aktu mērķis ir sabalansēt šīs divas personas tiesības, tad par pamatu ir jāņem Satversmes 116. pants, kas paredz, ka attiecīgās tiesības var ierobežot tikai likumā paredzētajos gadījumos, lai aizsargātu citu cilvēku tiesības, demokrātisko valsts iekārtu, sabiedrības drošību, labklājību un tikumību.

2000. gada 23. martā tika pieņemts Fizisko personu datu aizsardzības likums [35] (turpmāk – FPDAL), kas stājās spēkā 2000. gada 20. aprīlī. Atsevišķas tā normas stājās spēkā ar 2001. gada 1. janvāri. Tās ir normas par personas datu apstrādes sistēmu reģistrāciju un personas datu uzraudzības, kontroles institūciju – Datu valsts inspekciju (DVI) [36]. Šis likums tika izstrādāts, pamatojoties uz ES Direktīvu 95/46 [34].

Fizisko personu datu aizsardzības likuma mērķis ir aizsargāt fizisko personu pamattiesības un brīvības, noteikt šādu datu saturošo reģistru tehniskos un organizatoriskos aizsardzības principus un apstrādes ierobežojumus, kā arī fizisko personu tiesības attiecībā uz saviem datiem.

7.2. PERSONAS DATI, TO VEIDI

Personas dati ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu (Likuma 2. panta 3. punkts). Definīcijā ir norāde uz laiku – norāde, ka persona var būt identificēta gan pagātnē, gan arī tikt identificēta nākotnē.

Svarīgi ir tas, kā tieši interpretējams vārds "identificēt". Latviešu valodā filoloģiskā nozīmē šis vārds nozīmē "uzskatīt, atzīt par identisku (kam), atzīt par īsto, atpazīt". Līdz ar to šo jēdzienu var piesaistīt jebkurai personu identificējošai pazīmei, īpaši tās neuzskaitot. Svarīgākā ir pati personas iespējamā identifikācija, tam par pamatu ņemot jebkāda veida informāciju.

! *Lekcijā pasniedzējs var uzrunāt studentu, piemēram, „students pēdējā solā" vai „studente sarkanā džemperī" – un tā būs pietiekama informācija, lai nepārprotami identificētu uzrunājamo studentu. Kaimiņš var runāt par kādu personu kā „vīrieti, kurš dzīvo otrajā stāvā". Citā vidē par pietiekamu informāciju identificēšanai var tikt uzskatīti vārds un uzvārds. Lai identificētu kādu personu, var tikt lietots tikai personas kods, kas kalpo par unikālu personas identifikatoru arī ārpus valsts robežām.*

Tātad pārnestā nozīmē personas dati ir jebkāda informācija, kuru var saistīt ar personu un ar kuru galarezultātā var identificēt fizisku personu. Personas datus parasti iedala sensitīvos un nesensitīvos personas datos.

Personas datu klasificēšana ir svarīga, lai sistēmu pārziņi varētu zināt un precīzi noteikt tos personas datus, kas uzskatāmi par sensitīviem datiem, jo tiem ir nepieciešama daudz stingrāka aizsardzība.

7.2.1. SENSITĪVIE DATI

Gan LR Fizisko personu datu aizsardzības likums, gan ES Direktīva 95/46 nosaka, ka sensitīvi personas dati ir dati, kas norāda personas rasi vai etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi. Prettiesiska sensitīvo personas datu izmantošana var nodarīt kaitējumu fiziskai personai.

7.2.2. DATU SUBJEKTS

Datu subjekts ir fiziska persona, kuru var tieši vai netieši identificēt, izmantojot personas datus. Pastāv diskusija par personas datu aizsardzības ilgumu (termiņu), tas ir, cik ilgi konkrētajiem personas datiem tiek piemērotas personas datu aizsardzības tiesību normas. Vairums speciālistu uzskata, ka personas datu aizsardzības noteikumi darbojas tikai datu subjekta dzīves laikā. Šis apgalvojums pamatojas uz to, ka personas datu aizsardzība ir viena no cilvēktiesībām un ir cieši saistīta ar pašu personu. Tomēr zināmā mērā pamatoti ir uzskati, ka personas datiem ir jābūt aizsargātiem arī pēc personas nāves. Šo uzskatu piekritēji pamatojas uz to, ka personas datiem ir jābūt

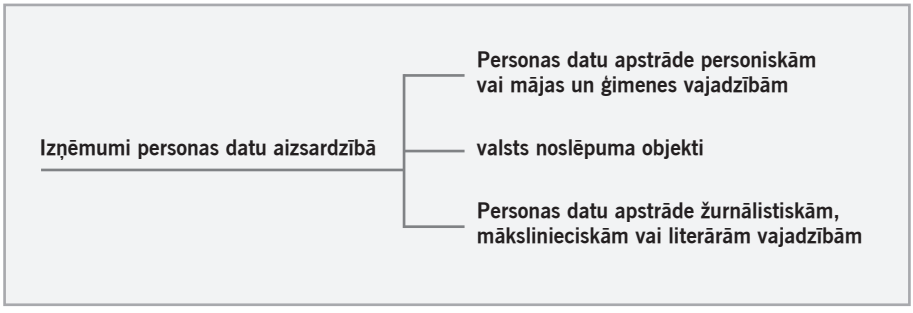
aizsargātiem neatkarīgi no iespējamiem kaitējumiem, ko var radīt konkrētai personai, un ka bieži vienas personas dati var netieši ietekmēt arī citas personas, piemēram, radiniekus.

7.3. IZŅĒMUMI PERSONAS DATU AIZSARDZĪBĀ

Fizisko personu datu aizsardzības vispārīgs princips ir tāds, ka personas datu aizsardzība attiecas uz visu veidu personas datu apstrādi un jebkuru juridisko vai fizisko personu, kas ir iesaistīta personas datu apstrādē. Tomēr pastāv atsevišķas jomas jeb datu kategorijas, kur vispārējo normu attiecināšana ir diskutējama.

Pirmā kategorija, uz kuru ne vienmēr tiek attiecinātas personas datu aizsardzības vispārējās normas, ir informācijas sistēmas, kurās personas datu apstrādi veic personiskām vai mājas un ģimenes vajadzībām un kurās savāktie personas dati netiek izpausti citām personām. Piemēram, tās ir tādas sistēmas, kur personas savos mājas datoros ir apkopojušas draugu, paziņu personas datus – vārdus, uzvārdus, telefona numurus utt. Šos personas datus nedrīkst izpaust trešajām personām. Šis izņēmums neattiecas uz visiem personas datiem, kas dažādu iemeslu dēļ var tikt apstrādāti kādas personas dzīvesvietā. Šinī gadījumā svarīgs ir personas datu apstrādes mērķis, un katrā ziņā tas nevar būt saistīts ar kādiem komerciāliem mērķiem.

Otra kategorija, uz kuru ne vienmēr tiek attiecinātas personas datu aizsardzības vispārējās normas, ir valsts noslēpuma objekti, un tos reglamentē 1996. gada likums "Par valsts noslēpumu". Minot valsts noslēpuma objektus, ir jāmin arī personas datu apstrāde, ko realizē operatīvās darbības subjekti, veicot operatīvo uzskaiti “Operatīvās darbības likumā” noteiktajā kārtībā. Tomēr tas nav vispārpieņemts izņēmums, jo dažās valstīs personas datu aizsardzības likumdošana attiecas arī uz tādiem personas datiem, kas ir atzīti par valsts noslēpumu, piemēram, Zviedrijā. Arguments ir tas, ka personas datu aizsardzības vispārējās normas ir attiecināmas uz visām informācijas sistēmām, bet var pastāvēt tikai izņēmumi no kopējiem personas datu apstrādes principiem, piemēram, izņēmums no datu subjekta tiesībām saņemt par viņu visu informāciju, kas glabājas attiecīgajā sistēmā.



10. att. Izņēmumi personas datu aizsardzībā.

Trešā izņēmumu kategorija attiecas uz personas datiem, kas ir apstrādāti žurnālistiskām, mākslinieciskām vai literārām vajadzībām.

Eiropas Savienības dalībvalstīm ir dotas tiesības izvēlēties izņēmumus no vispārējām personas datu aizsardzības normām. Tomēr, nosakot dažādus izņēmumus personas datu aizsardzības normu piemērošanā, nedrīkst deformēt personas datu aizsardzības kopējo sistēmu valstī. Attiecībā uz izņēmumiem ir jāizsver, vai atsevišķas tiesību normas, kas paredzētu personas datu aizsardzību atsevišķās nozarēs, nevarētu tikt iekļautas nozaru likumos. Piemēram, attiecībā uz valsts drošības un krimināltiesību jomu nevarētu tik pašsaprotami uzskatīt, ka šajās jomās vispār būtu iespējams ignorēt personas datu aizsardzību, jo šīm jomām varētu piemērot vispārīgos personas datu aizsardzības principus, paredzot tikai dažus izņēmumus personas datu apstrādes kārtībā.

7.4. PERSONAS DATU AIZSARDZĪBAS PRINCIPI

Personas datu aizsardzības principu ievērošana ir priekšnosacījums, lai sistēmas pārzinis varētu apstrādāt personas datus. Tātad personas datiem ir jābūt

1) godīgi un likumīgi apstrādātiem,
2) apstrādātiem noteiktiem (ierobežotiem) mērķiem un tikai saskaņā ar tiem,
3) adekvātiem, saistītiem un ne pārmērīgi izvērstiem,
4) pareiziem (precīziem),
5) apstrādātiem tik ilgā laikā, cik tas ir nepieciešams,
6) apstrādātiem saskaņā ar datu subjektu tiesībām,
7) drošiem,
8) adekvāti aizsargātiem, ja tiek nodoti citai valstij.

Šie principi ir ietverti gan FPDAL, gan Direktīvā 95/46/EC, un tie ir izveidojušies visā personas datu aizsardzības attīstības vēsturē.

Pirmais princips paredz, ka apstrādei jānotiek tikai saskaņā ar tiesību aktiem, kas reglamentē personas datu apstrādes kārtību. Tas ir gan pats FPDAL, gan arī citi tiesību akti, piemēram, tie, kas reglamentē datu drošību. Ir jāpiemin, ka ne jau visas personas datu normas ir iekļaujamas vienā likumā. Personas datu aizsardzība ir tik komplicēts process, ka ikvienai nozarei (piemēram, statistikai, medicīnai utt.) ir tikai tai specifiskas personas datu aizsardzības normas.

Otrais princips attiecas uz apstrādes mērķiem. Sistēmas pārzinim jau pirms datu apstrādes uzsākšanas ir precīzi jādefinē, kādiem mērķiem viņš apstrādās personas datus. Noteikto mērķi izmanto, lai strīdu gadījumos varētu izlemt, vai sistēmas pārzinis nav nepamatoti vācis kaut kādus personas datus, kas nav nepieciešami, lai viņš sasniegtu noteikto mērķi. Kad noteiktais mērķis ir sasniegts, tad personas datu apstrādi nedrīkst turpināt. Protams, personas datu apstrādē var pastāvēt mērķis, par kuru nav iespējams pateikt, kad uzskatīt to par sasniegtu.

Attiecībā uz trešo principu ir svarīgi pievērst uzmanību vārdiem "ne pārmērīgi izvērstiem". Tas nozīmē, ka sistēmas pārzinis nedrīkst vākt vairāk datu, nekā tas nepieciešams. Šis princips ir arī cieši saistīts ar personas datu apstrādes mērķi.

Ceturtais princips nosaka, ka datiem sistēmā ir jābūt precīziem. FPDAL 10. panta pirmās daļas 4. punkts noteic, ka sistēmas pārzinis nodrošina "personas datu pareizību un to savlaicīgu atjaunošanu, labošanu vai dzēšanu, ja personas dati ir nepilnīgi vai neprecīzi". Šo principu nodrošina gan sistēmas pārzinis, gan arī datu subjekts, kuram ir tiesības, atklājot neprecizitātes savos datos, sistēmas pārzinim pieprasīt tās novērst.

Piektais princips attiecas uz laika posmu, kurā sistēmas pārzinim ir tiesības apstrādāt personas datus. Viens no termiņa noteikšanas nosacījumiem varētu būt saistīts ar personas datu apstrādes mērķi.

Sestais princips nosaka, ka personas datu apstrādē ir jāievēro visas datu subjektam paredzētās tiesības. Šīs tiesības ir noteiktas FPDAL, piemēram, datu subjekta tiesības saņemt informāciju par sistēmā esošajiem datu subjekta personas datiem, kā arī par jebkuru trešo personu, kura saņēmusi personas datus.

Septīto principu var uzskatīt par vienu no svarīgākajiem. Personas datu drošība ir priekšnosacījums, lai šos datus aizsargātu pret nelikumīgu, neatļautu piekļuvi. Personas datu drošību panāk ar noteiktiem tehniskiem un organizatoriskiem pasākumiem. Latvijā tiesību aktos ir paredzēti gan vispārīgie informācijas sistēmu drošības noteikumi, gan tieši personas datiem paredzētās obligātās tehniskās un organizatoriskās prasības (2001. gada 30. janvāra Ministru kabineta noteikumi Nr. 40 "Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības" [9]).

Par astoto principu pēdējos gados ir ļoti daudz diskusiju. Gan ES Direktīvā, gan FPDAL ir noteikts: lai nodotu personas datus uz citu valsti, tajā ir jābūt adekvātam personas datu aizsardzības līmenim. Termins "adekvāts" tad arī ir daudzo diskusiju pamatā. Galvenā problēma ir personas datu nodošana valstij, kas nav Eiropas Savienības dalībvalsts, piemēram, ASV, jo tur pastāv pavisam atšķirīga un ļoti sadrumstalota personas datu aizsardzības sistēma.

7.5. PERSONAS DATU APSTRĀDE

Vārda "apstrāde" lietošana attiecībā uz personas datiem ir specifiska informācijas tehnoloģijas jomai. Apstrāde nozīmē – "programmā paredzēto instrukciju izpilde datora centrālajā procesorā, lai pēc noteiktiem kritērijiem pārveidotu, kārtotu un atlasītu datus vai izdarītu ar tiem matemātiskus aprēķinus".

Tomēr personas datu aizsardzības jomā ar vārdu "apstrāde" saprot "jebkuras ar personas datiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu", ko nosaka

likuma 2. panta 4. punkts. Tātad šī definīcija ietver pilnīgi visas darbības, kas ar personas datiem notiek informācijas sistēmā.

Apstrādājot personas datus, tie tiek apvienoti elektroniskās datu bāzēs, reģistros, kartotēkās un citās uzskaites sistēmās. Latvijā pastāv vairāki valsts nozīmes reģistri (Zemesgrāmata, Iedzīvotāju reģistrs, Uzņēmumu reģistrs u. c.), kā arī liels skaits personas datu apstrādes sistēmu, kas ir atsevišķu fizisku un juridisku personu rīcībā, sākot ar grāmatvedības un personāla uzskaites sistēmām un beidzot ar klientu datu bāzēm. Atkarībā no fizisko personu datu uzkrāšanas un apstrādes mērķiem tiek lietoti atšķirīgi to reģistrācijas nosacījumi (sk. 11. attēlu).

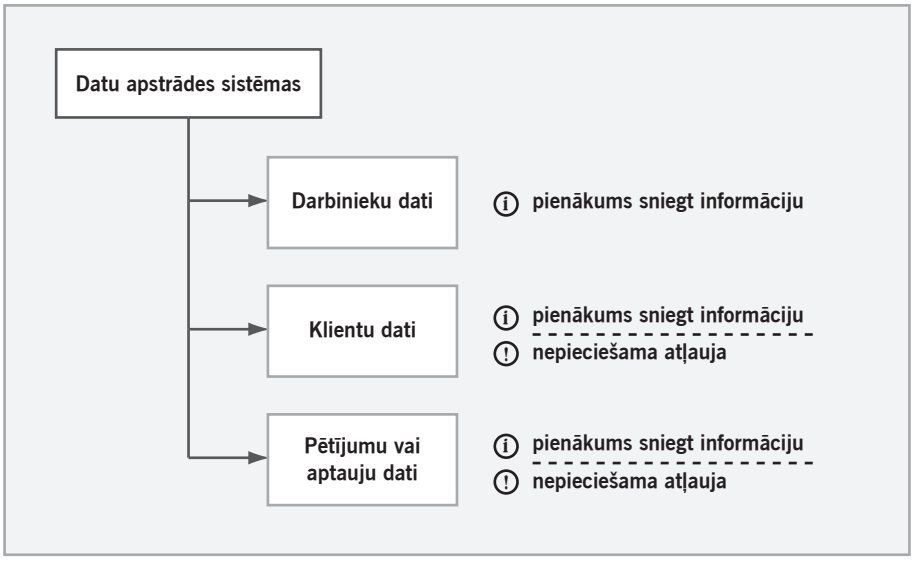
Pirms sistēmas pārzinis uzsāk personas datu apstrādi, viņam ir jāreģistrējas konkrētajā personas datu aizsardzības uzraudzības, kontroles institūcijā. Latvijā tā ir Datu valsts inspekcija.

Dažādās valstīs, pirms nosaka konkrētus kritērijus personas datu apstrādei, sistēmas tiek iedalītas pēc personas datu veidiem, institūcijām un personām, kas veic personas datu apstrādi.

! *Vācijā Federālajā personas datu aizsardzības aktā personas datu apstrāde tiek iedalīta pēc tā, vai apstrādi veic publisko tiesību subjekti vai privāto tiesību subjekti. Latvijā varētu uzskatīt, ka FPDAL veido personas datu apstrādes kārtību pēc personas datu apstrādes veidiem.*

Tātad, pirms sistēmas pārzinis sāk apstrādāt personas datus, jābūt konkrētiem nosacījumiem, lai viņš varētu to veikt, t. i., jābūt vienam no FPDAL minētajiem kritērijiem, kurus nosaka likuma 7. pants:

- ir datu subjekta piekrišana,
- datu apstrāde izriet no datu subjekta līgumsaistībām,



11. att. Datu apstrādes sistēmu reģistrācijas nosacījumi.

- datu apstrāde nepieciešama sistēmas pārzinim viņa likumīgo pienākumu veikšanai,
- datu apstrāde nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, arī dzīvību un veselību,
- datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ievērošanu vai realizētu publiskās varas uzdevumus, kuru veikšanai personas dati ir nodoti sistēmas pārzinim vai pārraidīti trešajai personai,
- datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu sistēmas pārziņa vai tās trešās personas likumiskās intereses, kurai personas dati atklāti.

Attiecībā uz sensitīviem personas datiem pastāv vispārīgs princips, ka šādu personas datu apstrāde ir aizliegta. Tomēr ir jāpastāv dažiem izņēmumiem, lai varētu nodrošināt atsevišķas svarīgas valsts, kā arī datu subjektu intereses:

- datu subjekts ir devis rakstveida piekrišanu savu sensitīvo datu apstrādei,
- speciāla personas datu apstrāde, neprasot datu subjekta piekrišanu, ir paredzēta tiesību aktos, kas regulē darba tiesiskās attiecības, un šie tiesību akti garantē personas datu aizsardzību,
- personas datu apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas personas dzīvību un veselību, un datu subjekts tiesiski vai fiziski nav spējīgs dot savu piekrišanu,
- personas datu apstrāde ir nepieciešama, lai sasniegtu likumīgus nekomerciālus sabiedrisko organizāciju un to apvienību mērķus, ja šī datu apstrāde ir saistīta tikai ar šo organizāciju vai to apvienību locekļiem un personas dati netiek nodoti trešajām personām,
- personas datu apstrāde ir nepieciešama ārstniecības vajadzībām, un to veic ārstniecības persona vai ārstniecības iestāde, nodrošinot atbilstīgu personas datu aizsardzību,
- apstrāde attiecas uz tādiem personas datiem, kuri ir nepieciešami fiziskās vai juridiskās personas likumīgo tiesību un interešu aizsardzībai tiesā.

Sistēmas pārzinis var noslēgt vienošanos, datu apstrādi uzticot veikt personas datu operatoram. Tomēr sistēmas pārzinis ir atbildīgs kopumā par personas datu apstrādi.

7.5.1. DATU SUBJEKTA TIESĪBAS

Tā kā personas datu aizsardzība ir uzskatāma par nozīmīgu cilvēktiesību aspektu, tad tieši jautājumam par datu subjekta tiesībām ir jāpievērš liela uzmanība. Datu subjektam ir šādas tiesības:

- tiesības piekļūt saviem personas datiem,
- tiesības pieprasīt sistēmas pārzinim papildināt un labot personas datus,
- tiesības pieprasīt pārtraukt personas datu apstrādi, iznīcināt personas datus,
- tiesības pieprasīt pārtraukt personas datu apstrādi, ja tā notiek komerciāliem mērķiem,
- tiesības saņemt atbilstīgu atlīdzinājumu,
- tiesības saņemt informāciju par automatizētās apstrādes sistēmās izmantotajām apstrādes metodēm.

Datu subjekta tiesības piekļūt saviem personas datiem izpaužas tādā veidā, ka "datu subjektam ir tiesības iegūt visu informāciju, kas par viņu savākta jebkurā personas datu apstrādes sistēmā". Vienlaikus datu subjektam ir tiesības iegūt informāciju par personām, kas ir saņēmušas informāciju par viņu, kā arī informāciju par pašu sistēmas pārzini. Saskaņā ar FPDAL datu subjekts divas reizes gadā bez maksas saņem iepriekš minēto informāciju mēneša laikā no pieprasījuma iesniegšanas dienas. Ja datu subjekts vēlas saņemt šādu informāciju biežāk, tad sistēmas pārzinim ir tiesības noteikt maksu par šādas informācijas saņemšanu.

! *Austrijā sistēmas pārziņi, kas apstrādā personas datus tiešās tirgvedības mērķiem, gadījumos, ja personas datus sistēmā glabā ilgāk par trim mēnešiem, datu subjektiem paziņo rakstiski, ka attiecīgajā sistēmā tiek glabāti personas dati. Šo informāciju datu subjekti saņem bez maksas. Datu subjekts vispār var pieprasīt dzēst datus. Austrijas Industriālajā kodeksā datu subjektam ir paredzētas tiesības nesaņemt reklāmas materiālus. Šajā nolūkā Austrijas Reklāmas un tirgus komunikāciju asociācija veido to personu sarakstu, kas nevēlas saņemt reklāmas materiālus.*

Datu subjekta tiesības saņemt informāciju par automatizētās apstrādes sistēmās izmantotajām apstrādes metodēm piemēro tajos gadījumos, kad datu subjektam saistošus lēmumus pieņem, pamatojoties tikai uz automatizētiem lēmumiem.

! *Ja persona vēlas saņemt finanšu iestādē kredītu un informāciju par personas kredītspēju apstrādā automatizēta informācijas sistēma, tad datu subjektam pēc lēmuma saņemšanas no finanšu iestādes ir tiesības prasīt pamatojumu par šāda lēmuma pieņemšanu un uzzināt, tieši ar kādu metožu palīdzību tikusi noteikta viņa kredītspēja.*

7.6. DARBINIEKI, DATORI UN SPIEGOŠANA

Samērā nesen līdz ar globālo elektronizāciju mainījās arī darbinieku kontroles metodes. Uzņēmumos, kur darbā tiek izmantoti datori un internets, darba devējam ir plašas darbinieku kontroles un uzraudzības iespējas. Līdz ar to izvirzās divi savstarpēji saistīti jautājumi – cik liela drīkst būt darba devēja kontrole, un kādas ir darbinieku tiesības uz personiskās informācijas privātumu?

Datori, e-pasts un internets ir ļoti nepieciešami un tiek plaši izmantoti darbā. Taču darbinieki ir tikai cilvēki, un IT tiek izmantotas ne tikai darbam, bet arī personiskām vajadzībām un izklaidei. Loģiski, ka darba devējs par to nav sajūsmā un vēlas šādu problēmu novērst. Nereti tiek uzstādītas novērošanas programmas, ar kuru palīdzību var novērot pilnīgi visas ar datoriem saistītās darbinieku aktivitātes, tādējādi pavisam vienkārši atrisinot problēmu [37].

Ņemot vērā ne pārāk augstās novērošanas programmu cenas, to popularitāte strauji pieaug. Tā kā šādu programmu iespējas ir ļoti plašas, var kontrolēt visus uzņēmuma darbiniekus, nevienam to nepamanot. Tātad tiek iegūti visi dati par konkrēta darbinieka darbībām ar datoru, viņam pašam par to pat nezinot.

Ko saka likums par šāda veida fizisko personu privātuma pārkāpumiem? Pirmkārt, darba devējam ir jāinformē darbinieki, ka ir uzstādīta novērošanas programma, lai darbinieks zinātu, ka visas viņa darbības tiek novērotas, un nedarītu neko tādu, kas atklātu viņa personisko informāciju. Vismaz vajadzētu paziņot, ka darbs ar datoru tiek veikts novērošanas programmas uzraudzībā. Šāds paziņojums parādītos, ieslēdzot datoru. Otrkārt, darba devējam būtu darbiniekam jādara zināms, tieši kāda novērošanas programma tiek izmantota. Tas nav tik nebūtiski, jo ar vienu novērošanas programmu var iegūt statistisku informāciju par darbinieka izmantotajām programmām un laiku, bet ar otru – ierakstīt katru darbinieka nospiesto tastatūras taustiņu vai tiešsaistē vērot darbinieka datora monitora attēlu. Līdz ar to darbiniekam būtu tomēr jāzina, kādas ir izmantotās novērošanas programmas iespējas. Turklāt šādas prasības nav nekas pārmērīgs un būtu uzskatāmas par darbinieka elementārām tiesībām.

Bez darba devēja tiesībām iegūt informāciju par darbiniekiem, piemēram, izmantot novērošanas programmu, ir nepieciešams regulēt arī kontroli uzņēmuma iekšējos dokumentos.

Iekšējos darba kārtības noteikumos vai arī interneta un e-pasta izmantošanas noteikumos būtu precīzi jānosaka, kādi ir darbinieka pienākumi, strādājot ar datoru, un kādas ir darba devēja tiesības, it īpaši attiecībā uz e-pasta pārbaudīšanu, piemēram, tiesības īpašos gadījumos atvērt darbinieka e-pastu, ja tas ir pārpildīts vai saņemts sūtījums ar vīrusu. Taču nedrīkst aizmirst pamatprincipu, ka nav spēkā noteikumi, kas pasliktina darbinieka tiesisko stāvokli. Tas attiecas ne tikai uz darba līgumu, bet arī uz iekšējās darba kārtības noteikumiem un darba devēja rīkojumiem. Turklāt šādi noteikumi ne tikai nebūs spēkā, bet arī ļaus darbiniekam pierādīt, ka netiek ievērotas viņa tiesības uz privāto informāciju.

Interesanti ir tas, vai darbinieks var aizsargāties pret novērošanu. Lielākā daļa uzņēmumu, kas izstrādā novērošanas programmatūru, piedāvā arī pretēja rakstura programmas, tā ka darbinieks var arī iegādāties aizsardzības programmu, piemēram, pret tā saucamajiem "tastatūras ierakstītājiem" (*keyloggers*) [42]. Ja darba devējs nav to aizliedzis uzņēmuma iekšējos dokumentos un netiek izmantota nelicencēta programmatūra, tad pret to faktiski nevar iebilst.

Taču var būt arī tā, ka iepriekšminētos risinājumus nav iespējams izmantot, jo darba devējs nevienam nesniedz informāciju, ka kontrolē pilnīgi visas darbinieka darbības ar datoru. Kā rīkoties šādā gadījumā? Efektīvākā iespēja būtu vērsties tiesā, taču uzreiz jāuzsver kāda būtiska juridiska nianse – visi apgalvojumi ir jāpierāda. Tā kā viena no novērošanas programmu specifiskajām īpašībām ir to neatklājamība, tā var būt ļoti liela problēma. Taču arī

to var atrisināt, ja ir iespējams panākt, ka attiecīgs darbinieks, piemēram, sistēmas administrators, atzīst, ka tiek lietota novērošanas programma un iegūtie dati nodoti darba devējam.

7.7. PERSONAS DATU APSTRĀDES SISTĒMU DROŠĪBAS NOTEIKUMI

Nodrošinot attiecīgu personas datu aizsardzību, tiek panākta mazāka iespējamība, ka personas datu apstrādi var izmantot nelikumīgi. Direktīva 95/46 nosaka, ka pārraudzītājam ir jānodrošina "pienācīgi" tehniskie un organizatoriskie pasākumi, lai aizsargātu personas datus pret nejaušu vai nelikumīgu apstrādi. Pamatojoties uz to, FPDAL 26. pants paredz atbilstošu Ministru kabineta noteikumu pieņemšanu.

Dažādās valstīs pastāv dažādi viedokļi un modeļi, kas nosaka personas datu apstrādes sistēmu drošības prasības. Vairumā valstu šīs prasības nosaka nevis tiesību līmenī, bet gan paredz rekomendāciju veidā. Tiesību līmenī šīs drošības prasības ir noteiktas Norvēģijā un Itālijā. Galvenokārt ir jāpanāk situācija, ka konkrētās prasības var laikus mainīt, ņemot vērā informācijas tehnoloģiju straujo attīstību.

Ministru kabinets 2001. gada 30. janvārī pieņēma noteikumus Nr. 40 "Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības". Tie nosaka tikai pašas prasības, nenosakot konkrēti līdzekļus un metodes, kā sistēmas pārzinis to varētu panākt. Šo līdzekļu konkretizācijai sistēmas pārzinis izstrādā iekšējos sistēmas darbības noteikumus. Papildus tam sistēmas pārzinim katru gadu ir jāveic sistēmas audits un jāsagatavo pārskats par sistēmā veiktajiem pasākumiem informācijas drošības jomā. Apkopojot personas datu apstrādes sistēmu drošības prasības, var konstatēt, ka tās pēc savas būtības neatšķiras no vispārējiem starptautiskajā praksē pieņemtajiem sistēmu drošības noteikumiem.

7.8. PERSONAS DATU APSTRĀDES UZRAUDZĪBAS INSTITŪCIJA

Svarīgs jautājums, kas nesaraujami saistīts ar personas datu apstrādi, ir tādas institūcijas pastāvēšana, kas nodrošina personas datu uzraudzību, kontroli un aizsardzību valstī. Latvijā tā ir Datu valsts inspekcija, kas sāka darboties ar 2001. gada 1. janvāri un atrodas Tieslietu ministrijas pārraudzībā. Tās direktoru apstiprina Ministru kabinets. Direktīvā 95/46 par DVI statusu ir noteikts, ka tai jābūt neatkarīgai. Latvijā FPDAL izstrādāšanas laikā daudz diskutēja par šo jautājumu, jo Latvijā valsts pārvaldes sistēmā nepastāv institūcijas, kas būtu pilnīgi neatkarīgas no jebkuras citas institūcijas. Pilnīgi neatkarīgas institūcijas izveidošana varētu būt iespējama tikai pēc atbilstošiem grozījumiem Satversmē. Šajā gadījumā ir svarīgi arī atšķirt institucionālo un funkcionālo neatkarību. Latvijā saskaņā ar Satversmi nevar nodrošināt institucionālo neatkarību, bet ir nodrošināta funkcionālā neatkarība. Līdzīgi ir arī citās valstīs, piemēram, Zviedrijā.

Latvijā, kā jau minēts, par datu drošību rūpējas Datu valsts inspekcija, kuras pamatfunkcijas ir šādas:

- nodrošināt valstī personas datu apstrādes atbilstību FPDAL prasībām, tas ir, kontrolēt personas datu apstrādes sistēmu darbību atbilstoši likuma prasībām,
- pieņemt lēmumus un izskatīt sūdzības, kas saistītas ar personas datu aizsardzību,
- reģistrēt personas datu apstrādes sistēmas,
- pirms personas datu apstrādes sistēmas reģistrācijas veikt sistēmas personas datu apstrādes pārbaudi,
- dot rakstveida atļauju personas datu nodošanai citām valstīm.

Tomēr Latvijā ar laiku var rasties problēma, ja DVI nevarēs izdot sistēmu pārziņiem personas datu apstrādes sistēmām saistošus tiesību aktus. Visās Eiropas Savienības „vecajās" dalībvalstīs, kā arī Ungārijā un Igaunijā personas datu apstrādes uzraudzības institūcijas izdod vai nu saistošus, vai arī rekomendējoša rakstura noteikumus. Tie ir nepieciešami, jo pats apstrādes process ir cieši saistīts ar kopējo informācijas tehnoloģiju attīstību pasaulē. Lai būtu iespējams straujāk reaģēt uz attiecīgajām pārmaiņām, šīm institūcijām jābūt iespējai izdot šādus noteikumus.

Latvijā šīs institūcijas tiesības nosaka likuma 29. pants, un tās ir šādas:

- saņemt bez maksas no fiziskajām un juridiskajām personām nepieciešamo informāciju,
- veikt personas datu pirmsreģistrācijas pārbaudi,
- pieprasīt datu bloķēšanu personas datu apstrādes sistēmās, kļūdainu vai nelikumīgi iegūtu datu izdzēšanu vai iznīcināšanu, noteikt pastāvīgu vai pagaidu datu apstrādi,
- iesniegt tiesā prasības par personas datu apstrādes pārkāpumiem.

7.9. ATBILDĪBA PAR PĀRKĀPUMIEM FIZISKO PERSONU DATU JOMĀ

2003. gada 15. aprīlī Latvijas Administratīvo pārkāpumu kodeksā tika iestrādātas arī fizisko personu datu apstrādes pārkāpumu normas:

- 204.(7) pants – Fiziskās personas datu nelikumīga apstrāde;
- 204.(8) pants – Informācijas nesniegšana datu subjektam;
- 204.(9) pants – Datu apstrādes sistēmas darbība bez reģistrēšanas;
- 204.(10) pants – Informācijas nesniegšana Datu valsts inspekcijai;
- 204.(11) pants – Personu neakreditēšanās Datu valsts inspekcijā.

Kā redzams, par sodāmiem pārkāpumiem var uzskatīt datu subjekta tiesību ierobežošanu un fizisko personas datu reģistru pārziņu pienākumu nepildīšanu attiecībā uz Datu valsts inspekciju. Attiecībā uz fizisko personu datu nelikumīgu apstrādi bargāk tiek sodīta sensitīvo datu nelikumīga apstrāde. Sodi, kuri var būt piemēroti, ietver sevī brīdinājuma izteikumu, naudas sodu, kā arī pārkāpuma priekšmetu konfiscēšanu. Lietas, kas saistītas ar Administratīvo pārkāpumu kodeksa 204.(7), 204.(8), 204.(9), 204.(10) un 204.(11) pantu, izskata Datu valsts inspekcija.

7.10. KONTROLJAUTĀJUMI

1. Kas ir fizisko personu dati, un kādi ir to veidi?
2. Kādi ir personas datu apstrādes principi?
3. Kādi ir personas datu aizsardzības izņēmumi?
4. Kādos gadījumos IS, kas satur personas datus, nav jāreģistrē?
5. Kas ir datu subjekts, un kādas ir tā tiesības?
6. Kas regulē personas datu apstrādes sistēmu drošību?
7. Kas uzrauga fizisko personu datu aizsardzības likumdošanas ievērošanu?
8. Vai personas datu plūsma pāri robežām ir atklāta?

8. VALSTS INFORMĀCIJAS SISTĒMU LIKUMS

Valsts informācijas sistēmu likums pieņemts 2002. gadā un regulē valsts un pašvaldību informācijas sistēmas un to funkcijas. Likuma uzdevumi ir noteikt vienotu kārtību darbībām ar valsts informācijas sistēmām, regulēt valsts informācijas sistēmu pārziņus, kā arī noteikt to turētāju un subjektu tiesības.

Valsts informācijas sistēma tiek definēta kā strukturizēts informācijas tehnoloģiju un telekomunikāciju aprīkojuma un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas aprite – ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

Valsts informācijas sistēmu likumā ir definēti šādi termini:

- sistēmas pārzinis – valsts institūcija, kuras pārvaldībā atrodas informācijas sistēma;
- sistēmas turētājs – sistēmas pārzinis vai tā pilnvarota persona, kas uztur sistēmas darbību un tehnisko resursu nodrošinājumu;
- sistēmas lietotājs – juridiska vai fiziska persona, kas lieto sistēmu uz līguma vai pieprasījuma pamata;
- sistēmas datu subjekts – juridiska vai fiziska persona, kas sniedz datus par sevi;
- integrēta valsts informācijas sistēma – loģiska valsts informācijas sistēmu apvienība, kuras ietvaros tiek uzturēti dažādi valsts informācijas sistēmu dati;
- valsts informācijas sistēmu reģistrs – valsts reģistrs, kurā tiek reģistrētas visas valsts informācijas sistēmas un to funkcijas.

Valsts informācijas sistēmas tiek uzturētas par valsts budžeta līdzekļiem, un to datu bāzes ir valsts īpašums, savukārt tehniskais nodrošinājums var būt kā valstisks (valsts vai pašvaldību īpašums), tā arī privāts. IS vispārpieejamiem datiem ir jābūt pieejamiem internetā, citi dati var būt slēpti vai arī pieejami kā maksas informatīvs pakalpojums.

8.1. KONTROLJAUTĀJUMI

1. Kādi ir valsts informācijas sistēmu likuma uzdevumi?
2. Definējiet jēdzienus
   - sistēmas pārzinis,
   - sistēmas turētājs,
   - sistēmas datu subjekts!

9. ELEKTRONISKĀ KOMERCIJA

Nodaļa izstrādāta, izmantojot [1, 243.–277., 39.–41. lpp.].

Pēdējie desmit gadi uzņēmējdarbības un tehnoloģiju attīstības jomā ir uzskatāmi par ievadījumu jaunai ērai, kas aizsākusi revolūciju komunikāciju jomā un līdz ar to arī uzņēmējdarbībā. Šo ēru varētu nosaukt par "elektronisko ēru", ko raksturo tādu fenomenu rašanās kā, piemēram, atklāti elektroniskie tīkli un elektroniskā komercija. Ir pamats uzskatīt, ka informācijas gadsimtu, kas sagaida cilvēci, vadīs elektronika, datorizētas iekārtas, kurām arvien pieaugs spēja radīt, apstrādāt un izplatīt informāciju.

Interneta attīstība un agrāk neiedomājamas izmaiņas informācijas tehnoloģijās radījušas priekšnoteikumus globālās komunikācijas attīstībai. Ar šo attīstību vienlaikus rodas arī jaunas iespējas veikt darījumus atvērtajos tīklos. Arvien vairāk un vairāk uzņēmumu mēģina gūt labumu no jauniem uzņēmējdarbības veidiem. Ar interneta rašanos ir pavērusies iespēja darījumus noslēgt interaktīvā komunikācijā starp pusēm, kurām nav bijušas iepriekšējas darījumu attiecības.

9.1. KAS IR E-KOMERCIJA?

Lai pilnībā izprastu, kas ir e-komercija, jānoskaidro, ko šis termins nozīmē.

Ne starptautiskās tiesības, ne arī kāds no nacionālajiem tiesību aktiem tieši nedefinē e-komerciju. Vienīgais akts, kura nosaukumā ir minēta e-komercija, ir Apvienoto Nāciju Starptautisko tirdzniecības tiesību komisijas (UNCITRAL) izstrādātais Elektroniskās komercijas parauglikums *(Model Law on Electronic Commerce)* [42], kas 1996. gadā tika apstiprināts ANO Ģenerālajā Asamblejā. Tomēr Parauglikums nesniedz termina "e-komercija" skaidru definīciju. Parauglikums nav saistošs starptautisko tiesību instruments, bet gan lietojams kā paraugs valstīm, kas uz tā pamata var pieņemt atbilstīgus nacionālos likumus.

Parauglikuma 1. pantā ir noteikts, ka tas attiecas uz jebkuru informāciju, kas ir datu sūtījuma formā komercdarbības kontekstā. Minētā ANO Starptautisko tirdzniecības tiesību komisija uzskata, ka šim instrumentam vajadzētu attiekties arī uz tiem datu sūtījumiem, kas saistīti ar starptautisko komercdarbību. Terminam "komerciāls" būtu jāpiešķir pēc iespējas plašāks interpretējums, ar to aptverot tiesiskās attiecības, kam ir komerciāls raksturs neatkarīgi no tā, vai tās ir līgumattiecības vai nav. Komerciālās attiecības ietver šādus darījumus:

- jebkuru pirkuma–pārdevuma darījumu,
- izplatītāju līgumus,
- komerciālo pārstāvniecību,
- faktūrkreditēšanu,
- līzingu,
- konsultēšanu,
- licencēšanu,

- investīcijas,
- finansēšanu,
- apdrošināšanu,
- banku darbību,
- koncesiju līgumus,
- kopuzņēmumus,
- sauszemes, jūras vai gaisa preču un pasažieru pārvadājumus u. c.

Nav īstas skaidrības, ko nozīmē termins "elektronisks". Dažādu valstu nacionālie likumi nesniedz atbildi uz šo jautājumu. ASV Pavalstu unificēto likumu nacionālā konference *(National Conference of Comissioners on Uniform State Laws)* ir izstrādājusi Unificēto elektronisko darījumu likumu. Saskaņā ar šo aktu "elektronisks" nozīmē – tāds, kas attiecas vai izmanto tehnoloģiju, kurai piemīt elektriskas, digitālas, magnētiskas, bezkabeļu, optiskas, elektromagnētiskas vai līdzīgas īpašības. Šī definīcija ir "atvērta" dažādām jaunām tehnoloģijām, un līdz ar jaunu tehnoloģiju attīstību tas nodrošinās šā likuma piemērošanu plašākā nozīmē. Minētajā definīcijā dažas no nosauktajām īpašībām nav tehniskā nozīmē elektroniskas (piemēram, optisko kabeļu tehnoloģijas), tomēr šāda definīcija nodrošina vienotas izpratnes ieviešanu juridiskā nozīmē.

E-komercija attiecināma uz tirdzniecisko darbību ar elektronisko tehnoloģiju palīdzību, kur datoriem ir svarīga nozīme informācijas apmaiņā. E-komercija ir saistīta ar elektronisko datu sūtījumu apmaiņu, kuriem ir komerciāla nozīme. Abi šie definējumi ir diezgan plaši un ietver jebkādu komerciālo darbību. Tomēr šīs definīcijas nemin nozīmīgu faktu, kas ir būtisks e-komercijā, proti, ka tā notiek bez papīra starpniecības. Tajā nenotiek apmaiņa ar papīra dokumentiem. Protams, nav izslēgta papīra izdrukas radīšana, taču tas nav nepieciešams, lai darījums būtu spēkā. Ir pareizāk runāt par e-komercijas darījumu, kuru veikušas divas vai vairākas personas (vai divi vai vairāki datori, ko programmējušas personas), apmainoties sūtījumiem ar elektroniskas sistēmas palīdzību attiecībā uz darījuma noslēgšanu, un kura galarezultātā netiek radīts materializēts papīra dokuments.

E-komercijas definēšana ir grūts uzdevums. Ne vienmēr ir skaidrs, kādas darbības raksturo e-komerciju, ņemot vērā tās evolūciju un attīstības ātrumu. Nepārtraukti rodas arvien jauni darbības veidi, kuru rašanās ir tieši saistīta ar internetu. Turklāt jāņem vērā arī tas, ka vairums uzņēmumu vienlaikus veic tradicionālo komercdarbību un e-komerciju. Pasaulē pazīstami uzņēmumi izmanto internetu par papildu instrumentu savu pakalpojumu un preču realizācijai.

9.2. SATURA, FORMAS UN KATEGORIJU JAUTĀJUMS

E-komercija ir gan formas, gan satura jautājums. E-komercijai kā formas jautājumam ir divi aspekti. Viens no tiem atklāj dažādos veidus, kā izmantot tehnoloģijas, lai slēgtu darījumus. Otrs aspekts ir saistīts ar darījumu dematerializēšanos, t. i., darījumi, kas gadiem ilgi slēgti, fiksējot darījuma elementus uz papīra, pamazām transformējas dematerializētā elektroniskā formā.

E-komerciju var sadalīt vairākās kategorijās:

- uzņēmuma–uzņēmuma jeb B2B attiecības, kuru ietvaros notiek pirkšana vai pārdošana, kā arī jebkāda cita komerciāla komunikācija starp diviem vai vairākiem uzņēmumiem;
- uzņēmuma–patērētāja jeb B2C attiecības, kuru ietvaros notiek lielākā daļa darījumu internetā, uzņēmumam pārdodot savus pakalpojumus vai preces patērētājiem ar interneta kā komunikācijas vides starpniecību;
- uzņēmuma–valdības attiecības, kas aptver mijiedarbību starp uzņēmumiem un valdības institūcijām (piemēram, ASV internetā tiek izplatītas ziņas ar gaidāmo valdības lēmumu detaļām, un kompānijām ir iespēja uz tiem nekavējoties atsaukties elektroniski) un šobrīd ir tikai sākuma stadijā, bet varētu strauji paplašināties, jo valdības veic dažādas darbības, lai apzinātos e-komercijas nozīmi biznesā un veicinātu tās attīstību);
- patērētāja–valdības attiecības, kuru ietvaros valdība piedāvā pakalpojumus iedzīvotājiem, piemēram, sociālo maksājumu veikšanu, izmantojot interneta iespējas.

E-komercijai ir vairākas apakšgrupas, ko varētu nosacīti saukt par e-komercijas formām. Ir divas pamatformas. Pirmā pamatforma ir elektroniskā datu apmaiņa (*Electronic Data Interchange – EDI*), ko var raksturot kā elektronisku darījuma sūtījumu kustību no viena datora uz otru. Šo formu parasti izmanto uzņēmumu savstarpējo darījumu slēgšanai (B2B), lai pilnīgi automatizētā veidā pirktu un pārdotu preces. Šajā gadījumā komunikācija notiek slēgtā vai daļēji slēgtā tīklā, kuram nav iespējams piekļūt no ārpuses. Taču šo tehnoloģiju izmantošana pašlaik vēl ir dārga un gandrīz vai nepieejama mazajiem un vidējiem uzņēmumiem.

Otra pamatforma ir atvērtā elektroniskā komercija, ko raksturo interneta vidē balstīti darījumi bez iepriekš panāktas, tradicionālas divpusējas vienošanās starp tās dalībniekiem. Atvērtā e-komercija ir vai nu elektroniskais pasts, kur notiek sūtījumu apmaiņa no viena datora uz otru parasti cilvēkam izlasāmā veidā, vai arī "daudzi pret daudziem" komunikācija, kas padara masu informāciju interaktīvā veidā pieejamu lielā attālumā esošiem datoru lietotājiem. Šādā formā faktiski veidojas uzņēmuma un patērētāja attiecības.

Līdz ar pasaules tīmekļa (*Word Wide Web – WWW*) parādīšanos atvērtā e-komercija ir ieguvusi daudz lielāku nozīmi interneta komerciālā izmantošanā. Elektroniskās komercijas darījumi tīmekļa vidē arī notiek dažādās formās. Piemēram, viena no šādām formām ir atkārtoti darījumi internetā starp vienu un to pašu pircēju un pārdevēju. Šai formai līdzīgi būtu arī atkārtoti darījumi starp vienu pārdevēju un daudziem pircējiem. Visbeidzot, ir iespējami arī tā sauktie "svešinieku" darījumi internetā, kur puses līdz tam nav vispār komunicējušas jebkādā formā.

Elektroniskā komercija kā satura jautājums ietver ļoti plašu darbību spektru. Šīs darbības var būt ne tikai pirkšana vai pārdošana, bet arī reklāma, konsultācijas u. tml. Tādējādi elektroniskā komercija var aptvert ļoti plašu darbību spektru. Varētu pat teikt, ka elektroniskā komercija aptver jebkuru komerciālā rakstura komunikāciju vai darbību tiešsaistes režīmā vai nu interneta vidē, vai arī slēgtā informācijas sistēmā.

Ar elektronisko tehnoloģiju ekspansiju ir mainījies arī darījumu saturs. Piemēram, arvien biežāk pati informācija, nevis to saturošs priekšmets ("nesējs") ir darījumu priekšmets.

! *Internetā ir iespējams ne tikai pasūtīt un saņemt mūzikas kompaktdisku, bet arī iegādāties mūziku digitālā formā, kas tiek nosūtīta uz pircēja datoru. Tāpat arī eksistē elektroniskās bibliotēkas, kurās iespējams elektroniski veikt maksājumus par elektronisko grāmatu, žurnālu un citu literatūras darbu versiju abonēšanu.*

Dažādas informācijas formas, kurām, pēc agrākajiem uzskatiem, nepiemīt nekāda tirgus vērtība, tagad ir visai izplatīts darījumu priekšmets. Tas ir radījis pamatu izvirzīt domu par liettiesisko īpašību piešķiršanu informācijai kā vienībai.

9.3. ELEKTRONISKAIS PASTS UN ELEKTRONISKĀ DATU APMAIŅA

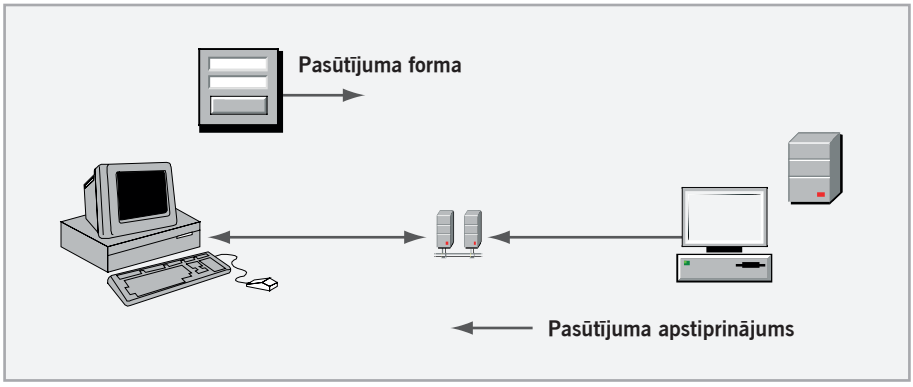
E-komercija ir saistīta ar elektronisko sūtījumu apmaiņu. Tajā izmantojamas dažādas formas, lai noslēgtu darījumus. Elektroniskais pasts un elektroniskā datu apmaiņa (EDA) ir divas formas, kādās var tikt noslēgts elektronisks līgums. Ir iespējams noslēgt līgumu arī interneta vidē, tikai uzklikšķinot uz ikonas "es piekrītu" *("I agree")* vai tamlīdzīgi – tas nozīmē, ka persona piekrīt piedāvātajiem līguma noteikumiem un apņemas tos izpildīt. *EDA* un e-pasts atšķiras no pārējiem attālinātās elektroniskās komunikācijas veidiem ar to, ka šīs tehnoloģijas sūta digitālus datus, kurus arī turpmāk var apstrādāt elektroniski.

E-pastu izmanto ikdienas darījumos, jo tas nodrošina gandrīz tūlītēju sūtījuma saņemšanu, neizmantojot papīra dokumentus. E-pasta priekšrocība ir tāda, ka šis pasts ir piemērots tūlītējai izlasīšanai, jo tajā izmanto cilvēkam saprotamas zīmes. Tomēr e-pasts nav piemērots automātiskai datu apstrādei, un tāpēc to nevar izmantot pilnīgi automātisku darījumu noslēgšanai, kur cilvēka iejaukšanās ir minimāla.

EDA komercdarījumu slēgšanā jau tiek izmantota gandrīz vai desmit gadus. EDA ir uz apstiprinātu standartu pamata strukturētu komercdatu automātiska apmaiņa starp dažādām datoru sistēmām elektroniskā veidā. Šis jēdziens ietver gan tādu sūtījumu apmaiņu, kuru galarezultātā tiek noslēgts līgums, gan arī tādu sūtījumu apmaiņu, kas nerada nekādas līgumsaistības (piemēram, sūtījumi informatīvos nolūkos). Taču vairumā gadījumu EDA izmanto starp pircējiem un pārdevējiem, un komunikācijas galarezultātā automātiski tiek radītas līgumattiecības. Tas ir iespējams, jo EDA ir ieprogrammēta datoram saprotamā formā tā, ka, saņemot atbilstīgu sūtījumu, automātiski sniedz pozitīvu vai negatīvu atbildi.

EDA var iedalīt divās apakšgrupās, proti, elektroniskajā līgumslēgšanā (*electronic contracting*) un elektroniskajā sūtījumu apmaiņā (*electronic messaging*). Šis dalījums ir nosacīts. Tam pamatā likts fakts, ka elektroniskajā līgumslēgšanā sūtījumu saturam un sūtītāja un saņēmēja darbībām ir juridiska nozīme. Tātad elektroniskā līgumslēgšana ietver elektroniskos piedāvājumus un elektroniskos apstiprinājumus.

EDA darījumā notiek tieša elektronisko dokumentu apmaiņa starp diviem datoriem. Saskaņā ar iepriekš ieprogrammētām darbībām dators veic arī noteiktas darbības. Piemēram, pircējs nosūta pirkuma pasūtījumu pārdevēja datorsistēmai. EDA ir standartforma, kas rada iespēju automātiski apstrādāt un izpildīt pasūtījumu. EDA varētu arī raksturot kā strukturētas komercinformācijas sūtījumus starp datoriem ar minimālu cilvēka iejaukšanās nepieciešamību.



12. att. Pasūtījumu apstiprinājums, izmantojot EDA.

Kā zināms, viens no saistību tiesību pamatprincipiem ir pieņēmums, ka līgumam, kuru noslēdz divas personas, ir jābūt pamatotam uz viņu gribas izteikumu. EDA gadījumā varētu šķist, ka datori pieņem lēmumu automātiski, piemēram, līdz ar apstiprinājuma nosūtīšanu tiek noslēgts līgums. Tomēr datori patstāvīgi nedomā. Ja tā būtu, tad varētu apšaubīt līguma spēkā esamību. Tomēr datori spēj darboties patstāvīgi, ja to darbības parametrus iepriekš nosaka un ieprogrammē. Cilvēciskais faktors nekad tā īsti nav apšaubīts EDA slēgtajos darījumos, jo faktiski tās ir personas, kas programmējušas datorus noteiktā veidā un vēlas, lai datori veiktu noteiktas darbības, pastāvot zināmiem priekšnoteikumiem. Tomēr šis izskaidrojums neatrisina svarīgas juridiskas problēmas, kas rodas EDA dēļ. Problēmas būtība ir jautājumā par to, ar kādiem nosacījumiem divu datoru darbības bez cilvēku iejaukšanās var radīt līgumu un kā šajos apstākļos darbojas citi saistību tiesību noteikumi, piemēram, par piedāvājuma atsaukšanu.

9.3.1. SLĒGTĀ ELEKTRONISKO DATU APMAIŅA

EDA no viena datora otram parasti tiek dēvēta par slēgto EDA, un tā notiek starp darījumu partneriem, kas viens otru zina vai ir pieslēgti slēgtam datortīklam. Viens no slēgtā EDA veidiem ir *SWIFT*, ko savā darbībā sekmīgi izmanto bankas, veicot elektroniskos norēķinus. Slēgtā EDA parasti tiek regulēta ar datu apmaiņas līgumiem, ko pirms konkrēto komercdarījumu slēgšanas savstarpēji noslēdz potenciālie darījumu partneri. Šajos līgumos puses vienojas par tehniskajiem un organizatoriskajiem darījumu priekšnoteikumiem.

Strīdu gadījumā šie līgumi ir svarīgs problēmu risināšanas instruments, jo vēl pagaidām daudzu valstu komerctiesības neregulē elektronisko līgumu slēgšanu un elektronisko dokumentu tiesisko atzīšanu.

9.3.2. ATVĒRTA ELEKTRONISKO DATU APMAIŅA

Iepretim slēgtajai EDA pastāv arī atvērtā EDA, kas nodrošina improvizētu *(ad hoc)* īstermiņa darījumu slēgšanas iespēju starp partneriem, kuriem nav bijušas iepriekšējas saskarsmes. Šajā gadījumā nav datu apmaiņas līgumu, kas regulētu komunikācijas pamatnoteikumus. Atvērtā EDA ir tikai attīstības sākumstadijā, taču daudzi prognozē, ka nākotnē tā var kļūt par nozīmīgu globālās infrastruktūras sastāvdaļu un veicināt elektroniskās komercijas uzplaukumu. Paredz, ka uzņēmumiem nākotnē būs iespēja komunicēt globālā līmenī ar atklātās EDA palīdzību un tā nodrošinās komunikāciju ar publiski pieejamu standartu palīdzību. Tādējādi atvērtā EDA tehniski radīs iespēju ikvienam nekavējoties sasniegt interesējošo potenciālo partneru datorsistēmas. Uzsver, ka tā būs galvenā atvērtās EDA priekšrocība, jo nevajadzēs iepriekš vienoties par dažādiem tehniskiem un organizatoriskiem jautājumiem datu apmaiņas līgumos pirms faktisko darījumu noslēgšanas. Nākotnē paredzams, ka internets darbosies kopā ar atvērto EDA, nodrošinot pieeju dažādām EDA sistēmām.

9.4. TIESISKĀS PROBLĒMAS

Starptautiskajā uzņēmējdarbībā jāsaskaras ar problēmām, ko izraisa līgumu noslēgšana ar elektroniskās komunikācijas palīdzību. E-komercija ir saistīta ar vairākām juridiska rakstura problēmām, piemēram, par to, kā parakstīt un pierādīt elektroniska līguma esamību. Darījuma dokumentu dematerializācija rada problēmas tradicionālajai komercdarbībai, jo elektroniskā komunikācija izslēdz papīra – tradicionālā informācijas fiksācijas veida izmantošanu. Šie jautājumi arvien vairāk norāda uz e-komercijas regulējuma nepieciešamību gan starptautiskajā, gan nacionālajā līmenī.

Attīstoties e-komercijai, nepieciešama skaidrība par noteikumiem, kas piemērojami elektroniskās komercijas dalībniekiem un to darījumiem. Daudzi uzņēmēji vēl neuzdrošinās uzsākt komercdarbību internetā, baidīdamies no neprognozējamības, kas izriet no neskaidrībām tiesību normās attiecībā uz elektroniskajā vidē veiktajiem darījumiem.

Daudzas problēmas balstās uz juridiskām koncepcijām un doktrīnām, kas radušās laikā, kad tik augsts informācijas tehnoloģiju līmenis nebija pat iedomājams. Jaunās tehnoloģijas, kas saistītas ar unikālās vides – interneta rašanos, izvirza jautājumu par to, kādas izmaiņas ir nepieciešamas tiesībās, lai IKT progresa sasniegumus veiksmīgi varētu izmantot komercijā. Galvenais likumdošanas izmaiņu mērķis ir piemērot pastāvošās komerctiesību koncepcijas darījumiem elektroniskajā vidē.

Viens no galvenajiem šķēršļiem pieaugošajai elektroniskās komunikācijas izmantošanai ir tiesiskajos aktos pieprasītā rakstiskās formas prasība un

nepieciešamība rakstisko dokumentu parakstīt. Prasība par dokumentu parakstīšanu ir arī Komerclikumā. Piemēram, 7. panta 2. daļa noteic, ka pēc saņēmēja pieprasījuma izraksta vai kopijas pareizība apliecināma ar komercreģistra iestādes amatpersonas parakstu un zīmogu, norādot izsniegšanas datumu.

Tomēr tradicionālā komunikācija, izmantojot papīru un uz tā uzrakstītu tekstu, strauji tiek aizstāta ar elektronisku komunikāciju ar interneta starpniecību. Vēl nesen vairums darījumu neprasīja neko vairāk kā vien papīru, pildspalvu un tiešu kontaktu starp darījuma slēdzējiem. Darījumi tika slēgti fiziskā vidē: tikšanās, rakstisks līgums, nobeigumā rokasspiediens. Ar interneta parādīšanos notikusi šo darījumu atribūtu dematerializēšanās, un komunikācijas elektroniskā vidē ir metušas izaicinājumu tradicionālajiem darījumu atribūtiem – rakstveida formai un parakstam.

9.4.1. KOMERCIĀLO FORMALITĀŠU DEMATERIALIZĒŠANĀS. RAKSTVEIDA FORMA

Lai pareizi piemērotu rakstveida formas prasības elektroniskajiem darījumiem, jānoskaidro, kādas tradicionālās funkcijas veic rakstisks dokuments materiālajā vidē. Viena no galvenajām rakstveida formas funkcijām ir tās pierādījuma funkcija. Pierādījuma funkcija nodrošina pierādījumus par darījumā iesaistītajām pusēm un par pašu noslēgto darījumu. Brīdināšanas funkcija aizsargā puses no neapdomāta un pārsteidzīga lēmuma pieņemšanas, jo dokumenta sagatavošana rakstveidā pusēm dod laiku apdomāties. Juridiskajā literatūrā tiek minēta rakstveida formas kanāla funkcija (*chanelling function*) un pieņemts, ka rakstveida formas prasība var ietekmēt pušu rīcību sabiedrības labā. Atbilstoši šim viedoklim sabiedrība ir ieinteresēta līgumu slēgšanā rakstiskā formā, jo tas veicina iespēju prognozēt pierādījumus tiesas procesā, kā arī pušu tiesību un pienākumu prognozējamību ārpus tiesas.

Nenoliedzami, pierādījuma funkcija ir galvenais rakstveida formas pamatojums. Lai saprastu formas prasību, tā jānošķir no pierādījuma aspekta. Lai gan formas prasība un rakstveida dokumenta pierādījuma aspekts ir savstarpēji cieši saistīti, tomēr starp tiem nevar likt vienādības zīmi. Profesore Kristīne Hultmarka Ramberga (*Christine Hultmark Ramberg)* šo atšķirību izceļ ar divu veidu argumentiem, ko varētu izvirzīt tiesā. Formas prasības pierādījuma aspektu labi demonstrē šāds izteikums: "Es neesmu parakstījis šo dokumentu. Uz dokumenta nav mans paraksts, tas ir uzrakstīts, lai radītu nepareizu priekšstatu, ka es esmu parakstījis šo dokumentu" vai "Dokumenta saturs nav tāds, kāds bija, kad es to nosūtīju. Tas ir mainīts". Šajā gadījumā tiesai ir jārisina pierādīšanas problēma. Tiesai jāizvērtē pierādījumi un jāspriež, vai dokumentu parakstījusi minētā persona vai kāds cits un vai dokumenta saturs ir mainīts.

Prasība attiecībā uz formas noteikumu ir šāda: "Es piekrītu, ka esmu nosūtījis šo dokumentu un mans vārds ir uz šī dokumenta, bet, tā kā tas nav parakstīts, tam nav juridiska spēka saskaņā ar likumu, un tāpēc man nav radies pienākums izpildīt saistību" vai "Es atzīstu, ka esmu nosūtījis šo dokumentu,

bet, tā kā tas ir digitālā formā, tas nav atzīstams par rakstisku dokumentu, un tāpēc tas nevar radīt saistību".

Jautājums tomēr joprojām ir neatbildēts: vai elektronisko darījumu var uzskatīt par rakstveida darījumu? Vai dematerializēts dokuments ir rakstisks? Kas ir jādara, lai komerciālo formalitāšu dematerializācija tiktu juridiski atzīta un nostiprināta? Tradicionāli zinām, ka "rakstveida forma" iekļauj sevī uz papīra uzrakstītu vai uzdrukātu tekstu. Tomēr, ja teksts ir iegrebts kokā vai akmenī, vai tas ir rakstveida dokuments? Kas ir ar krītu uzrakstīts teksts uz tāfeles? Atsevišķos gadījumos vārdu semantiskajai nozīmei tomēr var būt izšķirīga nozīme. Ja, piemēram, likuma teksts norādīs, ka apliecinājumam jābūt uzrakstītam uz papīra, tad gadījumā, ja tas būs ierakstīts pludmales smiltīs, acīmredzami likuma prasības nebūs izpildītas. Tomēr vairumā gadījumu ar gramatisko interpretēšanu ir par maz, īpaši, ja nav norādes uz formas vidi. Vai tas būs rakstisks teksts, kuru rada digitāli impulsi, kas parādās uz datora ekrāna tādu burtu veidā, kurus iespējams salasīt un izdrukāt?

Tas viss vedina domāt, ka ar vārdu "rakstveida" ir jāsaprot veids, kādā informācija ir nostiprināta vidē, nevis tas, kas saistīts ar pašas vides raksturu. Piemēram, ASV Vienotā komerclikuma komentārs skaidro vārdu "rakstisks" *(written* vai *writing),* ietverot mašīnrakstu, iespiešanu, kā arī jebkuru citu apzinātu informācijas izteikšanu uztveramā formā. Starptautiskajā praksē šī definīcija ir vēl vairāk paplašināta un iekļauj "telegrammas, faksa sūtījumus vai arī citus telekomunikācijas līdzekļus, kas nodrošina vienošanās ierakstu". Anglijas interpretācijas likums definē rakstisko formu kā "mašīnrakstā, iespiestā tekstā, litogrāfijā, fotogrāfijā, kā arī citos veidos reproducētus vārdus redzamā formā".

Tādējādi var saprast ka, visas minētās definīcijas ietver arī elektroniskos dokumentus. Varētu secināt, ka jebkurš raksts uz tāda materiāla (substances) vai virsmas, kas ļauj uztvert, fiksēt un saglabāt salasāmas zīmes, būtu jāuzskata par rakstisku. Pamatojoties uz šādu pieņēmumu, var izvirzīt argumentu, ka datorā uzglabāts ieraksts apmierina rakstveida formas prasību, jo gan magnētiskais disks, gan datora cietais disks ir spējīgs uztvert, fiksēt un saglabāt salasāmas zīmes. Protams, otra problēma, kas rodas ar šāda ieraksta atzīšanu par rakstisku, ir saistīta ar tā integritāti un parakstīšanas prasību, kas to nodrošina. Taču, ja paraugās uz rakstveida formas prasību, neņemot vērā parakstīšanas prasību, tad ir grūti atrast argumentu, kādēļ gan elektronisko ierakstu nevar uzskatīt par rakstisku.

Dažas valstis ir tieši mēģinājušas definēt vārdu "rakstveida" elektroniskās komunikācijas kontekstā. Piemēram, ASV Vienotais elektronisko darījumu likums 2.(7) pantā noteic, ka elektroniskais ieraksts ir "ieraksts, kas radīts, nosūtīts, novadīts, saņemts vai saglabāts ar elektroniskajiem līdzekļiem". Savukārt 7.(c) pantā minētais likums precizē: "Ja likums pieprasa ierakstam vai dokumentam rakstveida formu, elektronisks ieraksts apmierina šo likuma prasību." Mazliet atšķirīgāku pieeju ir izvēlējusies Kanāda savā Vienotajā elektronisko darījumu likumā, kura 7. pants nosaka: "Likuma prasība, ka informācijai jābūt rakstiskā formā, ir izpildīta, ja informācija, kas ir elektroniskā formā, ir pieejama izmantošanai turpmākai atsaucei uz to."

Ja tomēr likums tieši neparedz elektronisko ierakstu (dokumentu) atzīšanu, tad ir iespējams izmantot tā saukto funkcionālās ekvivalences interpretācijas metodi, lai atrisinātu elektroniskā ieraksta juridisko statusu. Šī metode ir nostiprināta UNCITRAL Elektroniskās komercijas parauglikumā. Saskaņā ar šo metodi tiesību interpretētājam ir jāveic divi analīzes posmi. Vispirms jāanalizē normas mērķis. Otrkārt, ir jānosaka, vai šo mērķi var sasniegt ar elektroniskās komunikācijas līdzekļiem salīdzinājumā ar tradicionālo, uz papīra balstīto komunikāciju. Šo interpretācijas metodi var izmantot arī tādu jēdzienu kā, piemēram, "ieraksts", "klātbūtne" un "dokuments" analīzē, to var izmantot arī vairumā citu tiesību nozaru, izņemot krimināltiesības un nodokļu tiesības. Tomēr vissvarīgāk ir šo metodi izmantot tieši IKT jomā, kur vecās tiesību normas jāpiemēro jaunai videi un tiesiskai realitātei.

Tomēr arvien vairāk valstu pieņem elektronisko dokumentu un parakstu likumus, kuri paredz elektronisko dokumentu tiesisko atzīšanu. Kā minēts iepriekš, paraksti elektroniskajā vidē mēdz būt ļoti dažādi. Savukārt juridiskais spēks piemīt tikai nedaudziem (digitālie sertifikāti).

9.4.2. PATĒRĒTĀJA TIESĪBU AIZSARDZĪBA

Elektroniskās komercijas attīstībā ļoti nozīmīga ir elektronisko pakalpojumu patērētāju uzticēšanās. Tāpēc likumdevējiem ir jāveicina uzvedības kodeksa ieviešana, jānodrošina alternatīvu strīdu pirmstiesas risināšanas metožu izmantošana, kā arī iespēja patērētājiem griezties tādā tiesā, kas ir spējīga reaģēt uz jebkuru kibernoziegumu. Lai Latvijā nodrošinātu e-komercijas strīdu izskatīšanu, tur paredzēto sankciju efektīvu, samērīgu un preventīvu darbību, ir nepieciešams sagatavot grozījumus Krimināllikumā, kas paredzētu kārtību e-pierādījumu iegūšanai, savākšanai, apstrādei un piemērošanai.

Jāatgādina, ka ASV par atsevišķiem kibernoziegumiem pret patērētājiem e-komercijas kontekstā jau tagad paredz kriminālsodu.

Latvijā e-komercijas patērētāju tiesību aizsardzību patlaban nodrošina šādi normatīvie akti:

- 1999. gada 18. marta Patērētāju tiesību aizsardzības likums,
- 1999. gada 18. maija MK noteikumi Nr. 178 "Kārtība, kāda norādāmas preču un pakalpojumu cenas",
- 1999. gada 13. jūlija MK noteikumi Nr. 257 "Noteikumi par patērētāja kreditēšanas līgumu",
- 1999. gada 7. septembra MK noteikumi Nr. 316 "Noteikumi par distances līgumu",
- 1999. gada 21. septembra MK noteikumi Nr. 325 "Noteikumi par līgumu par ēkas vai ēkas daļas (nekustamā īpašuma) lietošanas tiesību iegūšanu uz laiku",
- 1999. gada 20. decembra Reklāmas likums,
- 1998. gada 17. septembra Tūrisma likums un 2000. gada 5. maija MK noteikumi Nr. 163 "Noteikumi par kompleksiem tūrisma pakalpojumiem",
- 2000. gada 20. maija Preču un pakalpojuma drošuma likums,
- 2000. gada 20. maija likums "Par atbildību par preces un pakalpojuma trūkumiem",
- 1995. gada 31. oktobra MK noteikumi Nr. 317 "Noteikumi par zāļu reklāmu".

Internet veikals 24.LV
Birojs: Rīga, Bezdelīgu iela 12, LV 1007.
Tālrunis birojā: 7602566, 9566414 (Tele2), 9396223 (LMT)
Kurjerdienesta tālrunis: 9556422
Fakss: 7612060
E-pasts: info@24.lv
http://www.24.lv

Juridiskā informācija:
SIA L Grupa
Bezdelīgu iela 12, Rīga
PVN LV50003582221
Hansabanka, kods HABALV22
Konts LV19HABA0551001958590

13. att. Interneta veikala 24. LV informācija.

Patērētāju tiesību aizsardzības likums attiecībā uz interneta tirdzniecību noteic, ka "distances līgums ir vienošanās starp patērētāju un pārdevēju vai pakalpojuma sniedzēju, pamatojoties uz pakalpojuma sniedzēja vai pārdevēja piedāvājumu ar adresēta vai neadresēta iespieddarba, tipveida vēstules, interneta, elektroniskā pasta, televīzijas, radio un citu informācijas nosūtīšanas vai pārraidīšanas līdzekļu starpniecību". Likums nosaka vairākas prasības, kurām ir jādarbojas, arī slēdzot, piemēram, pirkuma līgumu elektroniskajā veikalā.

Slēdzot distances līgumu, vispirms jābūt identificējamam preces pārdevējam vai pakalpojuma sniedzējam. Jābūt zināmam komersanta nosaukumam, reģistrācijas numuram un tādos gadījumos, kad tiek prasīta priekšapmaksa, arī adresei. Vairākos interneta veikalos tomēr nav iespējams atrast informāciju par komersanta nosaukumu un reģistrācijas numuru, bet gan tikai uzzināt veikala nosaukumu, un tas ir uzskatāms par patērētāja tiesību pārkāpumu.

! *Piemēram, interneta veikala 24.LV (www.24.lv) klientiem ir pieejama 13. attēlā redzamā informācija.*

! *Savukārt, atverot lapu www.lulu.lv un ieejot sadaļā „Par LULU", tiek sniegta vēsturiska informācija par pakalpojumu attīstību. Vienīgi lapas apakšā ir atrodama 14. attēlā redzamā informācija.*

Distances līgumā jābūt norādītam preces vai pakalpojuma raksturojumam vismaz tādā apjomā, lai to varētu identificēt un nevarētu sajaukt ar citām līdzīgām precēm. Piemēram, distances līgumā par tādām precēm kā mājsaimniecības krāsnis, ledusskapji un saldētavas, veļas mazgājamās un žāvējamās mašīnas, trauku mazgājamās mašīnas un spuldzes ietverama īpaša informācija, kas attiecas uz preču marķēšanu, un to nosaka attiecīgi MK noteikumi.

(c) LuLu Pica, 2002, tālrunis: 800 5858 , 800 7422

14. att. Interneta veikala LULU Pica informācija.

! *Piemēram, krāsnīm ir jānorāda iekārtas veids, lietošanas tilpums, enerģijas patēriņš uzsilšanai līdz 200°C, enerģijas patēriņš stundā vienmērīgā 200°C temperatūrā, kopējais enerģijas patēriņš, tīrīšanas cikla enerģijas patēriņš un standarti, kas lietoti, nosakot attiecīgos raksturlielumus.*

Turklāt noteikumi paredz, ka ir aizliegts izplatīt preces, kas neatbilst iepriekšminētajām prasībām. Diemžēl interneta veikalos, kas tirgo sadzīves tehniku, bieži vien netiek ievēroti noteikumi attiecībā uz īpašo marķējumu.

Distances līgumā nosakāma preču un pakalpojumu cena, ieskaitot visus nodokļus, samaksas noteikumi (priekšapmaksa, pēcapmaksa, patērētāja kreditēšanas noteikumi), maksa par piegādi, ja tāda ir paredzēta, un laikposms, kurā cena vai piedāvājums ir spēkā.

Par līguma izpildes termiņiem puses savā starpā var vienoties. Tas ir saprotami, jo ir preces, kas jau atrodas pārdevēja noliktavā, un preces, kuras tiks izgatavotas pēc individuāla pasūtījuma. Taču, ja pušu starpā rodas domstarpības un vienošanās par līguma izpildes termiņu nav noteikta līgumā, likums nosaka, ka termiņš ir 30 dienas, skaitot no dienas, kad saņemts pasūtījums no patērētāja.

Akcentējot patērētāja aizsardzības tiesību aspekta nozīmīgumu e-komercijā, Eiropas Komisija pašlaik veic pasākumus, lai noteiktu līmeni, kādā jau esošajos patērētāju aizsardzības noteikumos konstatējama nepietiekama aizsardzība, paredzot vajadzības gadījumā sagatavot papildu priekšlikumus nepilnību novēršanai.

9.4.3. LĪGUMA IZPILDES NOTEIKUMI

Visos gadījumos, izņemot MK noteikumos Nr. 316 par distances līgumu uzskaitītajos, patērētājam ir tiesības 14 kalendāra dienu laikā vienpusēji atkāpties no līguma (atteikt pasūtījumu), nemaksājot līgumsodu, procentus un zaudējuma atlīdzību. Šo termiņu skaita no dienas, kad patērētājs ir saņēmis preci vai tās daļu, vai no līguma noslēgšanas dienas, ja tiek sniegti pakalpojumi vai par pirkumu maksā daļēji vai pilnībā, izmantojot patērētāju kreditēšanas līgumu.

Ja pārdevējs vai pakalpojuma sniedzējs nav sniedzis patērētājam visu iepriekš minēto informāciju par līguma priekšmetu un samaksu, kā arī informāciju par garantiju un apkalpošanu pēc pārdošanas, patērētājam atteikuma

Preču garantija
Visas internetveikalā izvietotās preces piegādā lielākie vairumtirgotāji Latvijā. Visām precēm ir ražotāja noteiktais garantijas laiks. Šajā laikā preces tiek labotas Ražotāja norādītajos autorizētajos servisa centros Latvijā. Ja prece ir brāķis, tā tiek bez papildu samaksas apmainīta. Ir iespējama arī naudas atdošana.

15. att. Interneta veikala 2x2 preču garantijas informācija.

tiesību izmantošanas termiņš ir 90 kalendāra dienas, taču, ja trūkstošā informācija patērētājam tiek sniegta, atteikuma tiesību termiņš saglabājas 14 kalendāra dienas no informācijas saņemšanas dienas. Līdz ar atteikuma tiesību realizēšanu patērētājam 7 dienu laikā no rakstveida atteikuma nosūtīšanas dienas ir pienākums preci atdot atpakaļ pārdevējam vai pakalpojuma sniedzējam.

! *Piemēram, interneta veikalā 2x2 (www.2x2.lv) klientiem tiek sniegta 15. attēlā ievietotā informācija.*

Līgumā, kas noslēgts ar interneta starpniecību, papildus jānorāda

- tehniskie posmi, kas jāievēro, lai noslēgtu līgumu;
- noslēgtā līguma glabāšanas noteikumi un līguma pieejamība patērētājam;
- tehniskie līdzekļi ievades kļūdu noteikšanai un labošanai pirms pasūtījuma izdarīšanas;
- līguma noslēgšanai piedāvātās valodas;
- uzvedības kodekss, kas tiek ievērots, un informācija par tā pieejamību.

Ja līgums tiek slēgts, izmantojot internetu, pārdevēja un pakalpojuma sniedzēja pienākums ir ar elektronisko saziņas līdzekļu starpniecību nekavējoties apliecināt pasūtījuma saņemšanu, nodrošināt patērētājam iespēju izlabot ievades kļūdas pirms pasūtījuma izdarīšanas, kā arī iespēju iepazīties ar līgumu un tā papildnoteikumiem, kā arī to saglabāt.

Attiecībā uz preču vai pakalpojumu garantiju nav spēkā noteikumi, kas pasliktina patērētāja tiesības. Līgumā nevar vienoties par sliktākiem noteikumiem attiecībā uz ražotāja dotās garantijas apjomu vai termiņu, kā arī noteikt īsāku garantijas termiņu, nekā to paredz normatīvie akti.

9.4.4. SPĒKĀ NEESOŠAS ATRUNAS

Interneta veikali mēdz norādīt īpašas atrunas, piemēram, par to, ka preces cenai ir tikai informatīvs raksturs, ka veikals negarantē pieejamās informācijas precizitāti vai ka sniegtā informācija nerada juridiskas saistības. Visas šīs atrunas nav spēkā, jo tās ir pretrunā ar Patērētāju tiesību aizsardzības likuma noteikumiem, kas noteic, ka patērētāja tiesības ir pārkāptas šādos gadījumos:

- nav ievērots līgumslēdzēju pušu vienlīdzības princips un līguma noteikumi ir netaisnīgi;
- nav nodrošināta iespēja saņemt vispusīgu un pilnīgu informāciju par preci vai pakalpojumu vai to cenu, tas ir, par pašu preci, norēķināšanās veidu, līguma izpildījumu un atbildību, ja līgumsaistības tiek pārkāptas;
- patērētājam pārdota bīstama vai līguma noteikumiem neatbilstoša prece.

Likums nosaka arī to, ka līgumos, kurus ražotājs, pārdevējs vai pakalpojuma sniedzējs slēdz ar patērētāju, jāievēro pušu tiesiskās vienlīdzības princips, proti, līgums nedrīkst samazināt ar likumu noteikto pušu atbildību, noteikt priekšrocības ražotājam, pārdevējam vai pakalpojuma sniedzējam un ierobežojumus patērētājam, noteikt, ka patērētājs atsakās no savām likumīgajām tiesībām, nostādot patērētāju neizdevīgā stāvoklī.

9.4.5. PERSONAS DATU AIZSARDZĪBA

Fiziskai personai, kas sniedz savus personas datus distances līguma noslēgšanai, ir tiesības neizpaust tādus personas datus, kas neattiecas uz konkrētā līguma noslēgšanu, un prasīt, lai dati netiktu izpausti trešajām personām. Tad, ja dati tiek apstrādāti, ir tiesības zināt, kādiem mērķiem tas tiek darīts. Vēl jo vairāk personai ir tiesības noteikt, ka tā neatļauj izmantot savus personas datus komerciālos nolūkos un nevēlas saņemt nekādas reklāmas.

Jāatceras, ka fizisko personu dati tiek glabāti noteiktiem mērķiem, piemēram, lai nogādātu preci. Tātad pēc tam, kad par preci ir samaksāts un tā ir nogādāta, faktiski interneta veikalam vairs nav pamata glabāt un apstrādāt pircēja datus.

! *Piemēram, interneta veikals Xnet.lv (www.xnet.lv) sniedz saviem klientiem 16. attēlā redzamo informāciju par personas datu drošību.*

9.4.6. NODOKĻI

Līdz ar jauno ekonomiku, ļoti iespējams, nodokļu iekasēšana valdībām kļūs sarežģītāka.

- Pērkot preces tiešsaistes režīmā, pircējam ir iespēja izvairīties no PVN maksāšanas, īpaši, ja prece tiek piegādāta digitālā formā.
- Internets palielina firmu un tīklā operējoša darbaspēka mobilitāti. Firmām ir tendence pārvietoties uz valstīm ar zemiem nodokļiem vai nodokļu "paradīzi". Saasinās valstu konkurence nodokļu sektorā.
- Internets daudzos gadījumos neprasa atsevišķu operāciju īstenošanā iesaistīt starpniekus (bankas, mazumtirgotājus), kas nodokļu iekasētājiem nodrošina derīgu informāciju un veicina nodokļu iekasēšanu.

Taču e-komercija paver arī jaunas iespējas nodokļu iekasētājiem, jo nodrošina daudz ātrāku komunikāciju ar nodokļu maksātājiem un operatīvāku pieeju tiem nepieciešamai informācijai. ASV prezidents 1998. gada 21. oktobrī parakstīja Aktu par nodokļu brīvību internetam (*Internet Tax Freedom Act*), kas tika sagatavots, balstoties uz principu, ka informācija nav jāapliek ar nodokļiem, paredzot 3 gadu moratoriju darbībām, kas tiek īstenotas, izmantojot internetu.

Tavu datu drošība
Mūsu datu bāzē tiek reģistrēti mūsu pircēju vārdi, personas kodi (kā arī reģistrācijas nr.), piegādes adrese, tālruņa numuri un e-pasta adreses. Šie dati nepieciešami, lai mēs varētu kvalitatīvi nodrošināt klientu servisu, novērtēt mūsu uzticīgos klientus un veikt kvalitatīvas preču piegādes. Informācija, kas tiek iesniegta līzinga noformēšanai, netiek saglabāta mūsu datu bāzē – tā tiek nosūtīta Hansa līzingam, kas to izmanto potenciālā līzinga ņēmēja datu analīzei.

Xnet nodrošina pilnīgu tavu datu slepenību, un tie netiek nodoti citām personām vai kompānijām.

16. att. Interneta veikala Xnet informācija par personas datu drošību.

ASV zaudējumi nodokļu neiekasēšanas dēļ esot mērāmi miljardos ASV dolāru. Tomēr valdība jau vairākos lasījumos nespēj pieņemt nodokļu iekasēšanas politiku attiecībā uz elektronisko komerciju. Attīstītās valstis aktīvi diskutē par nodokļu aspektiem e-komercijas kontekstā starptautiskās organizācijas *OECD* ietvaros.

Latvijā darbs pie šiem nodokļu jautājumiem ir tikai sācies. VID ir izstrādājis grozījumu projektu likumā "Par nodokļiem un nodevām", paredzot, ka nodokļu maksātājam ir tiesības iesniegt nodokļu administrācijai minētajā likumā paredzētās deklarācijas, pārskatus un nodokļu aprēķinus elektroniskā veidā. Diemžēl pagaidām tā ieviešanu kavē e-paraksta neesamība.

Finanšu ministrija nodokļu iekasēšanā ir izvirzījusi divas aktuālākās problēmas.

- **Tiešie nodokļi**. Tiešo nodokļu iekasēšanā problēmas rodas tikai tad, ja e-komercijā iesaistītais uzņēmums ir reģistrēts vienā valstī, bet veic savu darbību ārpus tā reģistrācijas valsts citā valstī. Kura valsts šajā gadījumā iekasē uzņēmuma ienākuma nodokli? Pašlaik ir svarīgi sekot līdzi *OECD* "Konvencijas par ienākuma un kapitāla nodokļu dubultās uzlikšanas un izvairīšanās no nodokļiem" modeļa komentāru izmaiņām attiecībā uz tiešo nodokļu piemērošanu e-komercijas darījumiem, jo šī konvencija varētu būt par pamatu nodokļu likumu grozījumiem.
- **Netiešie nodokļi**. Kā galvenā problēma šeit tiek minēta PVN iekasēšana. Jānosaka, vai Latvija vispār iekasēs PVN digitālo preču iegādes gadījumā, ja tās tiek piegādātas tiešsaistes režīmā (piemēram, mūzika elektroniskajā formātā, elektroniskas publikācijas, grāmatas u. tml.). Pasaules pašreizējā prakse liecina, ka pagaidām digitāli piegādātām precēm PVN un muitas nodokļus (tarifus) nepiemēro.

Ņemot vērā, ka vēl nav izstrādāts mehānisms, kā iekasēt tiešos un netiešos nodokļus no e-komercijas darījumiem, Finanšu ministrija ierosina uz neilgu laiku (līdz 3 gadiem) atteikties no to piemērošanas, tādējādi vienlaikus stimulējot e-komercijas sākotnējo attīstību Latvijā.

9.5. E-KOMERCIJA UN TĀS REGULĒŠANA ĀRVALSTĪS

9.5.1. E-KOMERCIJA ASV

ASV nenoliedzami ir pirmajā vietā gan jaunu tehnoloģiju jomā, gan arī atbilstoša tiesiskā regulējuma nodrošināšanā. Elektroniskās komercijas likumdošanas pioniere ir Jūtas pavalsts, kas, pamatojoties uz Amerikas advokātu asociācijas (*American Bar Association*) Digitālo parakstu vadlīnijām, 1995. gadā pieņēma Jūtas Digitālo parakstu likumu. Šis likums regulē tikai uz kriptogrāfiju balstītos digitālos parakstus. Drīz pēc tam arī vairākas citas ASV pavalstis pieņēma līdzīgus likumus. Otrā pavalsts, kas pieņēma šādu normatīvo aktu, bija Kalifornija. Taču drīz vien tā mainīja likumdošanas virzienu no tehnoloģiski specifiskas pieejas uz diezgan ierobežotu tehnoloģiski neitrālu pieeju, pieļaujot elektronisko parakstu lietošanu tikai darījumos ar atsevišķām

valsts iestādēm. Kalifornijai sekoja arī citas ASV pavalstis, nomainot savus tehnoloģiski specifiskos likumus, kuros uzmanība bija pievērsta tikai digitālajiem parakstiem, uz tehnoloģiski neitrāliem likumiem, kas pārsvarā attiecas uz dažāda veida elektroniskajiem parakstiem.

Patlaban vismaz 49 ASV pavalstīs ASV federālajā līmenī, kā arī vismaz 30 dažādās citās valstīs likumdevēji ir pieņēmuši vai domā pieņemt elektronisko parakstu un elektronisko komerciju regulējošus normatīvos aktus. Tikai ASV vien 1999. gada pirmajos divos mēnešos tika izstrādāti 57 elektroniskās komercijas un elektronisko parakstu normatīvo aktu projekti. ASV Pavalstu vienoto likumu nacionālā konference (*National Conference of Comissioners on Uniform State Laws*) ir izstrādājusi "Unificēto elektronisko darījumu likumu", kas uzskatāms par vienu no veiksmīgākajiem elektroniskās komercijas likumdošanas aktu paraugiem. Vairums pavalstu pēc šī parauga ir pieņēmušas atbilstīgus likumus pavalsts līmenī. ASV federālajā līmenī 2000. gada 30. jūnijā prezidents Bils Klintons parakstīja likumu par elektroniskajiem parakstiem globālajā un nacionālajā komercijā, kas stājās spēkā 2000. gada 1. oktobrī.

9.5.2. E-KOMERCIJA EIROPĀ

Eiropā viena no pirmajām valstīm, kas pieņēma elektroniskās komercijas likumu, bija Itālija (1997. g,). Patlaban gandrīz vai katra Eiropas valsts ir pieņēmusi vai gatavojas pieņemt elektronisko komerciju un elektroniskos parakstus regulējošus normatīvos aktus. Arī Eiropas Savienības līmenī šie jautājumi nav atstāti bez ievērības. Divi no nozīmīgākajiem likumdošanas aktiem ir Eiropas Savienības Elektroniskās komercijas direktīva un Direktīva par vienotu ietvaru elektroniskajiem parakstiem Eiropas Savienībā.

Apvienoto Nāciju Starptautiskās tirdzniecības tiesību komisijas (UNCITRAL) Elektroniskās komercijas darba grupa ir izstrādājusi vienu no ievērojamākajiem normatīvajiem aktiem starptautiskajā līmenī, proti, Elektroniskās komercijas parauglikumu. Tas 1996. gadā tika pieņemts ANO Ģenerālajā Asamblejā. Patlaban UNCITRAL strādā pie starptautiska akta, kas attiektos uz digitālajiem parakstiem un sertifikācijas iestādēm.

ANO *OECD* strādā arī pie juridisko jautājumu risināšanas attiecībā uz elektroniskajiem parakstiem. Vienlaikus līdzīgs darbs notiek dažādās publiskās un privātās organizācijās.

1997. gadā Eiropas Savienības Komisija publicēja paziņojumu par elektronisko komerciju. Tajā tika skaidri noteikts, ka līdz 2000. gadam Eiropā jāizveido saskaņota tiesiskā vide. Elektroniskās komercijas jautājumi ir tikai viena daļa no daudzajiem problemātiskajiem jautājumiem, kas skar personas datu aizsardzību, patērētāju aizsardzību attiecībā uz distances līgumiem, patērētāju aizsardzību attiecībā uz distances līgumiem finanšu un pakalpojumu jomā, elektroniskajiem parakstiem, autortiesībām un ar tām saistītām tiesībām un elektronisko naudu u. c.

Pašreiz pastāv liela neskaidrība jautājumos par to, kā pastāvošās tiesības varētu piemērot tiešsaistes režīmā sniegtajiem pakalpojumiem. Daudzās valstīs ir atšķirīgi regulējumi un atšķirīga tiesu prakse. Saskaņā ar Eiropas

Savienības Elektroniskās komercijas direktīvu arī Latvijā tuvākajā nākotnē šie jautājumi būtu jāregulē. Tie ir savstarpēji saistīti un nosaka galvenos tiesiskā regulējuma principus, kas veicina elektroniskās komercijas attīstību. Jautājumi ir šādi:

- informācijas sabiedrības pakalpojumu sniedzēju dibināšanas brīvība,
- komerciālā komunikācija (reklāma, tiešā tirgvedība utt.),
- līgumu slēgšana tiešsaistes režīmā,
- starpnieku atbildība.

Informācijas sabiedrības pakalpojumu sniedzēju veidošana ir balstīta uz brīvas dibināšanas tiesību principu. Saskaņā ar Elektroniskās komercijas direktīvas normām, kas regulē šo jautājumu, jāizslēdz sarežģītas atļauju sistēmas informācijas sabiedrības pakalpojumu sniegšanā. Faktiski ir jāiedibina brīvas izvēles princips pakalpojumu nodrošināšanā ar interneta starpniecību. To varētu nosaukt arī par tiesību uz savu vietu internetā – tiesību, kam jābūt katrai personai, kura nolemj izmantot internetu, lai sniegtu pakalpojumus. Otrs svarīgākais jautājums ir saistīts ar to, ka jānosaka precīzi informēšanas priekšraksti pakalpojumu sniedzējam, lai nodrošinātu tā pakalpojumu caurskatāmību un publicitāti. Šajā sakarībā direktīva noteic, ka Eiropas Savienības dalībvalstīm ir jāpieņem likumdošana, kas paredz, ka informācijas sabiedrības pakalpojumu sniedzējam jānodrošina patērētājiem un valsts kompetentajām iestādēm viegli pieejama minimāla informācija par to darbību:

- nosaukums,
- adrese,
- e-pasta adrese,
- reģistrācijas numurs,
- pievienotās vērtības nodokļa maksātāja reģistrācijas numurs,
- profesionālās pilnvaras vai dalība profesionālajās organizācijās, ja tāda ir.

Komerciālā komunikācija ir elektroniskās komercijas pakalpojumu būtiska sastāvdaļa, un tāpēc ir jānosaka pamatprincipi, lai veicinātu tās attīstību. Direktīva prasa, lai valstis noteiktu, kas ir komerciālā komunikācija un kādi ir noteikumi attiecībā uz tās skaidru funkcionēšanu. Tādējādi tiktu nodrošināta patērētāju uzticība un godīga konkurence. Piemēram, valstīm ir nepieciešams noteikt, ka komerciālajai komunikācijai ar e-pasta starpniecību jābūt identificējamai. Attiecībā uz nesankcionētu komerciālo komunikāciju ar e-pasta starpniecību ir paredzēts, ka valstīs ir jānodrošina tā saucamā izvairīšanās (*opt–out*) sistēma (7. panta 2. daļa). Šī sistēma paredz, ka valstī ir jābūt īpašam reģistram, kurā fiziskās personas var īpaši reģistrēties, norādot, ka tās nevēlas saņemt nesankcionētus komercpiedāvājumus un informāciju. Saskaņā ar direktīvu uzņēmumiem, kas regulāri piesūta dažādu komercinformāciju pa e-pastu, regulāri ir jāpārbauda, ka personas, kas reģistrējušas sevi šajā reģistrā, nesaņem nesankcionētus elektroniskos sūtījumus. Viena no valstīm, kurā darbojas šis princips, ir Ungārija.

Izvairīšanās sistēmai pretēja ir izvēlēšanās (*opt–in*) sistēma, kas paredz, ka personas, kas tieši vēlas saņemt šādu nesankcionētu komercinformāciju, īpaši reģistrējas līdzīgā reģistrā. Izvēlēšanās sistēmas uzņēmumiem nav tiesību sūtīt nesankcionētu komercinformāciju nevienam citam kā vien personām, kuras ir reģistrējušās šādā reģistrā.

Dažādiem tirgvedības veidiem, kuros tiek izmantotas veicināšanas dāvanas, prēmijas un citi tamlīdzīgi paņēmieni, ir nepieciešami detalizēti noteikumi, un tiem jābūt viegli pieejamiem. Tas pats attiecas uz dažādām veicināšanas spēlēm un sacensībām (piemēram, dažādu prēmijas punktu vākšana, iegādājoties noteiktu preci). Tāpat kā citām reglamentētajām profesijām (advokāti, revidenti, grāmatveži), arī pakalpojumu sniedzējiem būtu jānodrošina, ka komerciālā komunikācija atbilst noteiktiem profesionālās ētikas noteikumiem, ko izstrādājušas profesionālas asociācijas (organizācijas).

Līgumu slēgšana tiešsaistes režīmā ir e-komercijas stūrakmens. E-komercija nevar pilnvērtīgi attīstīties, ja elektronisko līgumu slēgšanu nepieļauj noteikti līgumu formas un dažādi citi formāli noteikumi, kuri nav piemēroti tiešsaistes videi. Normām, kas attiektos uz elektronisko līgumu slēgšanu, jāaptver ne tikai faktiskā līguma noslēgšana, bet arī dažādās līguma slēgšanas stadijas: uzaicinājums izteikt piedāvājumu, sarunas, piedāvājuma izteikšana, līguma noslēgšana, reģistrācija, līguma izbeigšana, līguma grozīšana, līgumu arhivēšana u. tml.

Lai šīs normas ieviestu, jāievēro vairāki apsvērumi.

1. Jāatceļ tās tiesību normas, kas tieši aizliedz elektronisko līgumu slēgšanu. Veiktie pētījumi liecina, ka Latvijā šādu normu nav.
2. Nedrīkstētu aizliegt noteiktu elektronisko sistēmu izmantošanu. Arī šādu aizliegumu Latvijā pagaidām nav.
3. Elektroniskajiem līgumiem nedrīkst piešķirt tikai sekundāru vai pakārtotu atzīšanu, jo tādā gadījumā priekšroka joprojām tiktu dota uz papīra rakstītiem līgumiem.
4. Jāadaptē pastāvošie līgumu formas noteikumi, kā arī dažādi citi formālie noteikumi, kuru interpretācija var izrādīties nepiemērojama elektroniskajiem līgumiem. Šādas formālas prasības attiecas
   - uz vidi, kas izmantota līguma slēgšanas nolūkos (piemēram, noteikums, ka līgumam jābūt "rakstiskam", apstiprinājuma vēstule "jānosūta", jāuzrāda "līguma oriģināls" u. tml.),
   - uz cilvēku klātbūtnes prasībām (piemēram, līgums jāparaksta, pusēm klātesot, vienošanās jāpanāk un līgums jāparaksta noteiktā vietā u. tml.),
   - uz trešo pušu piedalīšanās prasībām (līgums jāapliecina notāram; līgums jānoslēdz liecinieku klātbūtnē; līgums jāreģistrē un jāiesniedz kādai personai vai iestādei).

Elektroniskās komercijas direktīva nosaka īpašas prasības tiešsaistes līgumu slēgšanai patērētāju aizsardzības nolūkā. Līdz ar to patērētāji varētu izvairīties no tehniskām kļūdām. Tāpat patērētājiem jābūt pieejamai skaidri norādītai līguma slēgšanas procedūrai, informācijai par līguma valodu, kā arī iespējai reproducēt līguma noteikumus un saglabāt tos.

Starpnieku pakalpojumu sniedzēju atbildība ir plaši diskutēts jautājums. Lai nodrošinātu elektroniskās komercijas darbību, nepieciešams precizēt tiešsaistes pakalpojumu sniedzēju atbildību par trešo personu informācijas glabāšanu un nosūtīšanu (tas ir, gadījumos, kad pakalpojumu sniedzējs darbojas kā starpnieks). Elektroniskās komercijas direktīva mēģina sabalansēt dažādas intereses, lai veicinātu sadarbību starp dažādām pusēm un samazinātu nelikumīgu darbību risku.

Tiesību aktiem ir jāierobežo tiešsaistes pakalpojumu nodrošinātāja atbildība horizontālā līmenī. Šīm normām jāattiecas uz jebkuru nelegālu darbības veidu, ko izdarījusi trešā persona (piemēram, autortiesību pirātisms, negodīga konkurence, viltus reklāma u. c.). Taču šīs normas nedrīkst ietekmēt tās dažādo tiesību nozaru materiālo tiesību normas, kas nosaka atbildību un regulē dažādus pārkāpumu veidus. Ja tiešsaistes pakalpojuma nodrošinātājs neatbilst atbildību ierobežojošiem kritērijiem, tad atsevišķā likumā ir jānosaka viņa atbildības raksturs un apjoms.

Elektroniskās komercijas direktīva starpniekus atbrīvo no atbildības gadījumos, kad tie darbojas tikai kā pasīvi informācijas "pārsūtītāji" no trešajām pusēm, un ierobežo pakalpojumu sniedzēju atbildību arī par citām "starpniecības" darbībām, piemēram, par informācijas glabāšanu. Direktīva lieto šādus terminus, aprakstot minētos starpniecības pakalpojumus: "tikai pārsūtīšana *(mere conduit)*", "kešēšana *(caching)*", "izviesošana *(hosting)*".

1. Tikai pārsūtīšana ir saistīta ar to, ka tiešsaistes pakalpojumu nodrošinātājs ir tikai pasīvs starpnieks, kas nosūta informāciju trešajai pusei.
2. Kešēšana ir īpaša informācijas glabāšanas forma, lai nodrošinātu digitālo tīklu ātrumu. Tajā ietilpst nevis informācijas izpēte, bet gan tikai informācijas replicēšana un uzglabāšana pakalpojuma sniedzēja sistēmā, lai nodrošinātu citiem patērētājiem pieeju tai pašai informācijai.
3. Izviesošana nozīmē pakalpojuma saņēmēja informācijas glabāšanu pēc viņa pieprasījuma (piemēram, servera vietas nodrošināšana uzņēmuma vai indivīda mājaslapai). Šajā gadījumā gan krimināltiesiskās, gan civiltiesiskās atbildības ierobežojums nevar attiekties uz pakalpojumu sniedzēju, ja viņš zina, ka viņa pakalpojuma izmantotājs veic nelikumīgas darbības (faktiskā zināšana) un nerīkojas, lai pārtrauktu nelikumīgās darbības (piemēram, nepārtrauc pieeju nelikumīgi iegūtajai informācijai).

Direktīva noteic, ka pakalpojumu nodrošinātājam nav tiešs pienākums veikt trešās puses darbību un informācijas pārbaudi, kā arī darbības pārraudzību. Taču šāds ierobežojums nedrīkst pilnībā izslēgt iespēju, piemēram, tiesībsargājošai iestādei (tiesai vai prokuratūrai) vai valsts drošības iestādei (piemēram, Latvijā Satversmes aizsardzības birojam) uz noteiktu laiku uzlikt par pienākumu veikt šādu pārraudzību, lai atklātu vai novērstu konkrētu nelikumīgu vai noziedzīgu rīcību.

ES Elektroniskās komercijas direktīva [43] risina tikai daļu no daudzajiem jautājumiem, kas ir saistīti ar e-komerciju. Neiedziļinoties direktīvas trūkumos un tās visai juceklīgajā jautājumu izkārtojumā, jāatzīst, ka tas ir ļoti svarīgs dokuments, kas nosaka vienotu regulācijas ietvaru svarīgākajiem ar e-komerciju saistītajiem jautājumiem. Papildus tam direktīvā ir mēģināts iekļaut mehānismu, kā ieviest direktīvu un nodrošināt tās izpildi ar sankciju palīdzību.

9.6. KONTROLJAUTĀJUMI

1. Kādu komerciālo darbību var veikt ar interneta palīdzību?
2. Kādās kategorijās var iedalīt e-komerciju?
3. Kas ir elektroniskā datu apmaiņa (EDA)?
4. Ar kādām tiesiskām problēmām saskaras e-komercija?

10. INFORMĀCIJAS SISTĒMU DROŠĪBA

Nodaļa izstrādāta, izmantojot [44].

10.1. MK "INFORMĀCIJAS SISTĒMU DROŠĪBAS NOTEIKUMI" NR.106

Pamatjēdziens informācijas sistēmu drošības noteikumos ir pati drošība, kuru definē šādi: „informācijas pieejamības (pēc informācijas sistēmas lietotāja pieprasījuma noteiktā laikposmā viņš var piekļūt informācijai), integritātes (pilnīgas un neizmainītas informācijas saglabāšana) un konfidencialitātes (informāciju saņem tikai tam pilnvarotas personas) nodrošināšana informācijas sistēmā". Latvijā 2000. gadā tika pieņemti MK "Informācijas sistēmu drošības noteikumi" Nr. 106, kuri nosaka obligātas dažādu (ne tikai valsts nozīmes) informācijas sistēmu drošības tiesiskās, tehniskās un organizatoriskās pamatprasības, kas jāievēro informācijas sistēmas organizācijai, tās vadītājam, informācijas sistēmas turētājam, tehnisko resursu turētājam, informācijas sistēmas lietotājam un citām personām, kuras ir atbildīgas par informācijas sistēmu drošību.

Diemžēl Valsts informācijas sistēmu likuma pārejas noteikumos tika paredzēts, ka šie drošības noteikumi ir spēkā ne ilgāk kā 6 mēnešus no Valsts informācijas sistēmu likuma spēkā stāšanās dienas. Tādējādi tie beidza darboties 2002. gada 5. decembrī. Šobrīd IS drošības noteikumi tiek pārstrādāti.

10.2. INFORMĀCIJAS DROŠĪBAS PAMATI

10.2.1. DROŠĪBAS PROBLĒMAS TAGAD UN NĀKOTNĒ

Analizējot pētījumu *2003 CSI/FBI Computer Crime Survey* par datoruzbrukumu veidiem, var secināt, ka galvenie drošības apdraudējumi joprojām ir vīrusi, ļaunprātīga datortehnikas izmantošana un tehnikas zādzības. No tiem pēdējos 12 mēnešos ir cietuši attiecīgi 82%, 80% un 59% aptaujāto uzņēmumu. Tāpat samērā daudz uzņēmumu ir cietuši no darbinieku nesankcionētas piekļuves (45%), pakalpojumu atteikumiem *(Denial of Service – DoS)* (42%) un ielaušanās datorsistēmās (36%).

Vērojot situācijas attīstību vēsturiski vairāku gadu garumā, var secināt, ka vīrusi, nesankcionēta piekļuve un zādzības saglabāsies arī nākotnē, un tātad ir vērts domāt par minēto drošības apdraudējumu seku samazināšanu un ieguldīt līdzekļus šai darbā.

Ievērojams drošības apdraudējums nākotnē ir nepieprasītās e-pasta vēstules jeb surogātpasts (*spam*), kas jau tagad sasniedz ap 60% no kopējās e-pasta plūsmas, turklāt ar tendenci pieaugt. Ko tas nozīmē? To, ka tikai četras no katrām 10 vēstulēm ir vajadzīgās, bet pārējās 6 lieki piesārņo pastkastes, noslogo tīklus un rada pakalpojumu atteikumu draudus.

Daudz ko liek pārdomāt arī prognoze par to, ka nākotnē tieši cilvēku (darbinieku, administratoru) kļūdas, nevis tehnoloģijas nepilnības būs galvenais drošības incidentu cēlonis. To var izskaidrot ar vienkāršu piemēru – uzņēmumu neglābs pat visdārgākais un drošākais ugunsmūris, ja nebūs attiecīgi kvalificēta administratora, kas spētu to konfigurēt atbilstoši uzņēmuma vajadzībām, un atbilstošas iekšējās kontroles sistēmas, kas reģistrētu un kontrolētu administratora darbības.

10.2.2. DROŠĪBAS TERMINU VĀRDNĪCA

Informācijas un informācijas sistēmas drošību raksturo šādi jēdzieni:

- drauds (*threat*) – iespējams notikums, kas var nelabvēlīgi ietekmēt organizāciju vai IT sistēmu un ko izraisa *draudu avota* ietekme uz *ievainojamību*,
- draudu avots *(threat resource)* –
  - tīšs *ievainojamības* izmantošanas nodoms,
  - netīša *ievainojamības* izmantošanas situācija,
- drošības incidents (*security incident*) – notikums, kas var izjaukt *informācijas sistēmas apstrādātās* informācijas vai *pašas informācijas sistēmas konfidencialitāti*, *integritāti* un/vai *pieejamību*, piem., sistēmas nepareiza darbība vai pārslodze, kļūdas datu ievadē, vīrusa uzbrukums, sistēmas uzlaušanas mēģinājums vai dabas katastrofa,
- drošības pārkāpums *(security breach) – informācijas sistēmas apstrādātās* informācijas vai *pašas informācijas sistēmas konfidencialitātes*, *integritātes* un/vai *pieejamības* zaudējums, kuru izraisa *drošības incidents*, piem., tas, ka IS nestrādā 10 stundas, sabojātas datnes,
- drošības pasākums *(security control)* – politika, metode, procedūra, iekārta vai programmas mehānisms, kas aizsargā *informācijas sistēmas apstrādātās* informācijas vai *pašas informācijas sistēmas konfidencialitāti*, *integritāti* un/vai *pieejamību* no *draudiem*. Drošības pasākumi var tikt paredzēti, lai
  - nepieļautu (*prevent*) drošības pārkāpumus,
  - atklātu (*detect*) notikušus drošības pārkāpumus,
  - atkoptu (*recover*) sistēmu pēc drošības pārkāpumiem,
- informācijas drošības mērķis – uzturēt darbībā to *drošības pasākumu* kopu, kuri kombinācijā notur *riskus* pieņemamā līmenī,
- ietekme *(impact)* – zaudējumu lielums, ko ciestu organizācija *drošības pārkāpuma darbības seku* rezultātā,
- ievainojamība (*vulnerability*) – potenciāla informācijas sistēmas "vājā vieta", kas rada iespēju *drošības pārkāpuma* realizēšanai,
- informācijas drošība (*information security*) – informācijas sistēmas apstrādātās informācijas vai pašas informācijas sistēmas konfidencialitātes, integritātes un pieejamības aizsardzība,
- informācijas integritāte *(information integrity)* – informācijas un tās apstrādes metožu precizitāte, pareizība un pilnīgums,
- informācijas konfidencialitāte *(information confidentiality)* – piekļuve informācijai tikai pilnvarotām personām,
- informācijas pieejamība *(information availability)* – iespēja pilnvarotām personām lietot informāciju noteiktā laikā un vietā,

- risku pārvaldīšana *(risk management)* – IS risku identificēšana, novērtēšana, samazināšana un kontrolēšana, kuras ietvaros tiek veikta IS risku mazināšana līdz organizācijai pieņemamam līmenim,
- risks (*risk*) – *drošības pārkāpumu* dēļ organizācijai nodarītu zaudējumu vai kaitējuma varbūtība. *Risks* ir funkcija no iespējamo zaudējumu vai kaitējuma lieluma (t. i., funkcija no *ietekmes*) un kaitējuma varbūtības,
- *iedzimtais* risks, kas saistīts ar *informācijas sistēmu*, – draudu īstenošanas varbūtība gadījumā, kad netiek izmantoti nekādi *drošības pasākumi,*
- *atlikušais* risks – risks, kas paliek, kad *drošības pasākumi* ir izmantoti.

10.2.3. INFORMĀCIJAS SISTĒMU AIZSARDZĪBA

Lai panāktu informācijas sistēmu drošību, katrā organizācijā jāīsteno informācijas sistēmu risku pārvaldība. Risku pārvaldība sastāv no vairākiem savstarpēji saistītiem procesiem, kuriem jānodrošina informācijas aizsardzība.

Informācijas sistēmu risku pārvaldības procesā ir izšķirami šādi galvenie posmi:

- informācijas sistēmas klasifikācija. Tiek analizēts IS glabājamās informācijas svarīgums, pēc kura tiek noteikts, vai sistēma ir kritiska, svarīga vai parasta. Kritiskām un svarīgām sistēmām risku pārvaldības process ir jāuzsāk nekavējoties,
- risku novērtēšanas process. Tajā jāveic 3 uzdevumi –
  - pirmkārt, jāidentificē visi tie draudi, kuri var apdraudēt aplūkojamo informācijas sistēmu (piemēram, elektrības padeves traucējumi, nesankcionēta piekļuve u. c.).,
  - otrkārt, identificētiem draudiem ir jānosaka to iestāšanās varbūtība un to iestāšanās ietekme uz organizāciju,
  - treškārt, no iegūtajiem datiem jāaprēķina riska varbūtība un ietekme,
- drošības pasākumu noteikšana. Iegūtie riski nosaka, cik drīz un kādā mērā ir jāievieš drošības pasākumi. Jo augstāks risku līmenis, jo lielāka IS aizsardzība ir nepieciešama. Drošības pasākumu noteikšanas aktivitātes ietver drošības pasākumu izvēli katram no riskiem un to ieviešanas plāna sastādīšanu. Protams, pieņemot lēmumu par drošības pasākumu ieviešanu,

2. tabula

Risku novērtēšana

Risks		Ietekme				
		Niecīga ietekme	Nebūtiska ietekme	Nozīmīgi zaudējumi	Nopietni zaudējumi	Apdraudēta darbība
Varbūtība	Neizbēgams	Ļoti zems	Zems	Vidējs	Augsts	Ļoti augsts
	Ļoti iespējams	Ļoti zems	Zems	Vidējs	Augsts	Augsts
	Iespējams	Ļoti zems	Zems	Vidējs	Vidējs	Vidējs
	Maz ticams	Ļoti zems	Zems	Zems	Zems	Zems
	Neiespējams	Ļoti zems	Ļoti zems	Ļoti zems	Ļoti zems	Ļoti zems

to izmaksām ir jābūt samērīgām ar iespējamiem zaudējumiem (organizācija var nevēlēties ieguldīt Ls 10 000 drošības pasākumos, kuri mazinās risku, kas var radīt Ls 200 zaudējumus). To var noskaidrot, veicot izmaksu un labumu analīzi,

- atkārtota risku analīze. Tā var tikt veikta pēc drošības pasākumu ieviešanas, lai noteiktu draudu iestāšanās varbūtību, jau ņemot vērā ieviestos drošības līdzekļus.

Informācijas sistēmu risku pārvaldība jāveic regulāri – tā jāatkārto IS paplašināšanas gadījumos vai arī, piemēram, tad, ja tiek arvien biežāk novēroti IS apdraudējumi. Procesā piedalās sistēmu turētāji, kā arī drošības speciālisti. Drošības pasākumu ieviešanas procesā var būt pieaicināti gan iekšējie tehniskie speciālisti, gan arī drošības speciālisti, kas darbojas ārpus organizācijas. Šī procesa veiksmi, protams, nosaka organizācijas vadības ieinteresētība un izpratne IS drošības jomā.

10.2.4. KAS ORGANIZĀCIJĀM JĀDARA DROŠĪBAS JOMĀ?

Pirmkārt, organizācijas augstākajai vadībai ir jāapzinās IS drošības vitālais svarīgums. Ļoti bieži var vērot izkropļotu situāciju, kad uzņēmuma vadība visu atbildību par informācijas sistēmām atstāj IT nodaļas ziņā, īpaši nepiepūloties ar stratēģisku lēmumu pieņemšanu un IT politikas definēšanu, vienīgi ar sakostiem zobiem un aizdomām parakstot kārtējos rēķinus. Kā pozitīvu piemēru Latvijā var minēt banku sektoru – gandrīz visās lielāko banku valdēs ir cilvēki, kas atbildīgi par informācijas sistēmām, un tādējādi tiek nodrošināts, ka banku lēmumi un darbības IS jomā ir izprastas un akceptētas visaugstākajā līmenī.

Otrkārt, ir nepieciešams kontrolēt, kā augstākās vadības akceptētā IS drošības politika un noteikumi tiek ievēroti un pildīti, kā arī noteikt cēloņus, kāpēc ir vērojamas dažādas atkāpes no tiem. Runa ir par informācijas sistēmu auditu. Pēc Eiropas Centrālās bankas ieteikumiem uz katriem 25 IT nodaļas darbiniekiem ir nepieciešams vismaz viens IS auditors.

Treškārt, nepavisam ne mazāk svarīgs ir izskaidrošanas darbs un uzņēmuma darbinieku regulāra apmācība IS drošības jautājumos. Šajā ziņā nenovērtējama loma ir IS drošības pārvaldniekam *(IS Security Officer)*.

Piemēram var minēt cīņu ar datorvīrusiem. Aizsardzība pret vīrusiem pēc būtības vienmēr nokavējas (to apliecina arī *2003 CSI/FBI Computer Crime Survey* rezultāti), jo pasaulē ik stundu, ik minūti tiek radīti jauni vīrusi un atjaunot vīrusu definīciju datnes tik ātri praktiski nav iespējams. Tāpēc ir nepieciešama ne tikai laba un laikus atjaunināta pretvīrusu programmatūra, bet arī izskaidrota un visu darbinieku akceptēta uzņēmuma iekšējā kārtība informācijas lejupielādei, surogātpasta apstrādei un rīcībai aizdomīgās situācijās.

10.3. KONTROLJAUTĀJUMI

1. Ko nosaka informāciju sistēmu drošības noteikumi?
2. Kas ir IS drošība?
3. Kādās kategorijās iedala sistēmās glabājamo informāciju?
4. Kā organizācija var pārvaldīt informācijas drošību?

11. KIBERNOZIEGUMI

Nodaļa izstrādāta, izmantojot [45, 46].

11.1. TIESISKĀ ATBILDĪBA

Atbildība informācijas un komunikāciju tiesībās ir viens no svarīgākajiem šīs nozares jautājumiem. Var izstrādāt ļoti labus likumus, kas regulēs e-pasaules tehniskās un organizatoriskās problēmas, bet, ja tie neregulēs IKT subjektu atbildību, tad šīs normas nefunkcionēs.

Pasaulē IKT atbildības jautājums ir regulēts ļoti neskaidri vai vispār nav regulēts. Daļēji ir atrisināti jautājumi par fizisku vai juridisku personu atbildību, ja to darbības IKT jomā ir radījušas fiziskai vai juridiskai personai mantisku vai nemantisku zaudējumu, bet praktiski nav atrisināts jautājums par atbildību, ja automatizētās datu apstrādes sistēma tās lietotājam ir nodarījusi kaitējumu. Tas arī saprotams, jo tradicionāli atbildības jēdziens ir cieši saistīts ar izpratni par cilvēka rīcības brīvību. Tomēr atkarībā no tā, kā termins „atbildība" tiek aplūkots – no filozofiskā, juridiskā vai cita skatpunkta, šim terminam definējums ir dažāds.

Sabiedrībā pastāv dažādi atbildības veidi, piemēram, morālā atbildība, politiskā atbildība un juridiskā atbildība. Lai piemērotu morālo vai politisko atbildību, nav nepieciešams valsts tiesiskais regulējums. Šie abi atbildības veidi netiek dibināti uz normatīva akta pamata. Varam darboties vienā "kiberkopienā", taču visas attiecības, kas radīsies "kiberkopienā", regulēs savstarpēja vienošanās starp kopienas dalībniekiem. Līdz ar to, ja kāds pārkāps kopienā pastāvošos noteikumus, vienīgais šāda subjekta ietekmes līdzeklis var būt viņa izslēgšana no kopienas. Ja "kibernauts" pēc viņa izslēgšanas no kopienas izplata kiberkopienas biedru informāciju, tad šādai rīcībai nevar iestāties tiesiskas sekas, izņemot gadījumus, ja tiek pārkāpts konfidencialitātes līgums vai ja iestājas sekas, kas tieši paredzētas likumā.

Patlaban nekur pasaulē nav tiesību normu, kas noteiktu šādu "kibernautu" tiesības, pienākumus un atbildību. Līdz ar to jāsecina, ka ne politiska, ne morāla, ne arī kāda cita veida atbildība, kas bāzēta uz savstarpējām attiecībām bez tiesiskā regulējuma elementa, nevar nodrošināt vienu no svarīgākiem atbildības uzdevumiem, tas ir, aizkavēt vai novērst indivīda vai juridiskas personas „nepareizo" darbību vai bezdarbību un to galarezultātā radītās negatīvās sekas, un nevar atjaunot stāvokli, kas pusēm bijušas pirms šādas „nepareizās" darbības. Politiskās un morālās atbildības pamats nav valsts sankcionēta darbība. Līdz ar to šādas nepareizas politiskas darbības vai bezdarbības dēļ nerodas juridiskas sekas. Ja politiķa darbības dēļ rodas juridiskas sekas, tad tās rodas ne jau tāpēc, ka viņš ir politiķis. Atbildība iestāsies tikai tad, ja politiķa – fiziskas personas darbības būs saistītas ar likumā paredzētu nosodījumu.

Personu atbildības tiesiskā izpausme vienmēr ir bijusi un paliks juridiskā atbildība par likumpārkāpumu. Juridiskā atbildība pamatojas tikai uz likumu vai likumpamatotu normatīvo aktu. Juridiskā atbildība ir īpaša jauna tiesiskā attiecība (saistība), kura rodas no likuma (tiesību normu) pārkāpuma, kas pārkāpējam

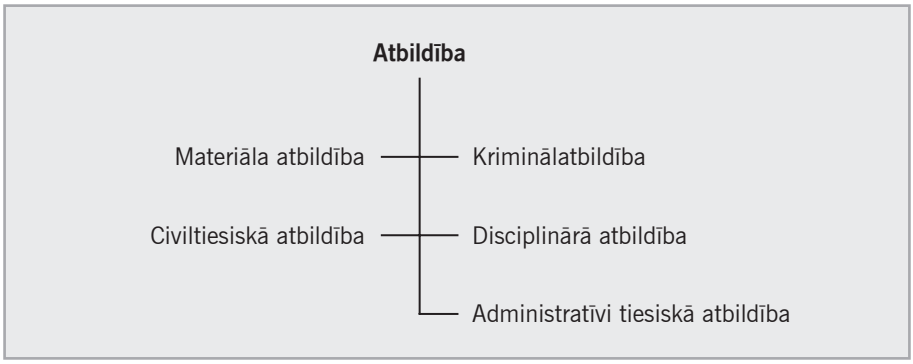
izpaužas soda, kompensācijas vai citādā personisko mantisko vai nemantisko ierobežojumu formā, un kuras piespiedu izpilde var tikt nodrošināta ar valsts piespiedu līdzekļiem. Juridisko atbildību no citiem atbildības veidiem nošķir divas pazīmes – tiesībpārkāpums un valsts piespiedu iedarbība uz tiesībpārkāpēju.

11.1.1. TIESĪBPĀRKĀPUMS

Tiesībpārkāpuma saturs ir atkarīgs no tās tiesību nozares, kuras regulētās sabiedriskās attiecības tiek pārkāptas. Civiltiesībās tās ir attiecības, kas saistītas ar civiltiesisko attiecību nodibināšanu, grozīšanu vai izbeigšanu un dažādiem tiesību un interešu aizskārumiem, nodibinot, grozot vai izbeidzot šīs tiesiskās attiecības. Darba tiesību pārkāpumu raksturo darba devēja vai darba ņēmēja tiesību pārkāpumi, kas var izpausties tiešā darba likumu kodeksa pārkāpšanā. Ja konkrēto sabiedrisko attiecību neaizsargā juridiska norma, tad nav arī juridiskās atbildības.

Praksē pazīstami vairāki juridiskās atbildības veidi (sk. 17. attēlu).

- Civiltiesiskā atbildība – saistības rodas, galvenokārt pārkāpjot normatīvos aktus civiltiesiskajā un uzņēmējdarbības jomā, piemēram, Civillikumu, uzņēmējdarbību regulējošos likumus, zemes un dabas resursu izmantošanas regulējošos normatīvos aktus, privatizāciju regulējošos normatīvos aktus.
- Materiālā atbildība – piemērojama likumā paredzētos gadījumos par dabai vai dabas videi, vai darba devējam nodarīto kaitējumu. Šo atbildības veidu piemēro papildus civiltiesiskajai atbildībai, un tās apjoms tiek noteikts ar likumu vai citu normatīvo aktu pēc noteiktas takses vai citas speciālas aprēķināšanas kārtības.
- Disciplinārā atbildība – saistīta ar darba likuma vai darba līguma pārkāpumu.
- Administratīvi tiesiskā atbildība – prettiesiska darbība vai bezdarbība, ko izdarījusi fiziska (pieskaitāma, 14 gadu vecumu sasniegusi) persona vai juridiska persona, ja likums paredz administratīvo atbildību par konkrēto nodarījumu.
- Krimināatbildība – vissmagākais juridiskās atbildības veids, ko var piemērot par fiziskas, (pieskaitāmas, 14 gadu vecumu sasniegušas) personas nodarījumu (darbību vai bezdarbību), ja likums par to paredz krimināatbildību.



17. att. Juridiskās atbildības veidi.

11.2. DATORNOZIEGUMI

11.2.1. DATORNOZIEGUMU VĒSTURE

ANO VIII kongresā, kas bija veltīts noziedzības apkarošanas problēmām, tika izstrādāts un pieņemts dokuments "Starptautiskās kriminālās politikas apskats – ANO rokasgrāmata ar datoriem saistītu noziegumu novēršanā un kontrolē" [47]. Tajā norādīts, ka pasaulē pirmais zināmais datornoziegums noticis 1801. gadā Francijā, kad Žozefs Žakārs savā tekstilrūpnīcā izgudroja un ieviesa perfokartes priekšteci, ar kuru varēja kopēt sērijveida ražošanā esošu audumu rakstu struktūru. Strādnieki, redzēdami, ka jaunais izgudrojums var apdraudēt viņu darbavietas, sabojāja šo ierīci. Šādā veidā veicot kaitniecības aktu pret izmantoto tehnoloģisko risinājumu, viņi izdarīja pasaulē pirmo datornoziegumu.

Kopš Havannas VIII ANO Noziedzības novēršanai un kriminālai tiesvedībai veltītā kongresa regulāri gan ANO, gan Eiropas Padomes un citu starptautisku organizāciju līmenī tiek pieņemtas dažādas rezolūcijas un pasākumu plāni, kuru uzdevums ir apkarot informācijas tehnoloģiju ļaunprātīgu izmantošanu noziedzīgos nolūkos.

Vārds "datornoziegums" cilvēkam, kas nav cieši saistīts ar datortehniku, nereti ir apvīts ar noslēpumu oreolu. Daži plašsaziņas līdzekļi urķus (*hackers*) uzskata gandrīz vai par nacionāliem ģēnijiem. Paradoksāli, bet pasaulē ir nodibinātas starptautiskas urķu organizācijas.

! *Kā norādīts Ukrainas Datornoziegumu pētniecības centra pētījumā, 2000. gada aprīlī notika Krievijas urķu forums "SPRYG-2K", bet 2000. gadā no 18. līdz 20. augustam Zaporožjē – starptautiskais urķu kongress. Informāciju par šo pasākumu varēja atrast http://www.hack-forum.org.ua. Viens no galvenajiem urķu sanāksmes organizētāju uzdevumiem bija saliedēt šo kustību visā pasaulē. Urķu forumā tika apspriesti jautājumi par tīmekļa serveru aizsardzības un uzlaušanas metodēm, Windows 98 un NT/2000 tālvadības trūkumiem un iespēju iedarboties uz sistēmu ar BO2K un NetBus vai cita veida programmām, par informācijas pārtveršanu, izmantojot TCP/IP protokolus, u. c.*

Šīs organizācijas ir pilnīgi oficiāli reģistrētas sabiedriskās organizācijas ar saviem preses izdevumiem, kas ir nopērkami arī Latvijas veikalos. Diemžēl tiesiski iedarboties uz šādu forumu norisi un šādu organizāciju izveidošanu nav iespējams ne Ukrainā, ne Krievijā, ne arī Latvijā, jo to pastāvēšanu pieļauj konstitucionālās tiesības.

11.2.2. KAS IR DATORNOZIEGUMS?

Datorspeciālistiem vārds "datornoziegums" nereti sagādā nopietnas galvassāpes, jo, kā jau iepriekš minēts, lielākā daļa datornoziegumu ir cieši saistīta ar informācijas sistēmu drošību. Jo vairāk IS īpašnieki vai turētāji var ieguldīt savu sistēmu drošībā, jo lielāka garantija, ka sistēmas resursi netiks pakļauti

apdraudējumiem. Vācijas informācijas sistēmu drošības rokasgrāmatā norādīts, ka cilvēks ar savu darbību tīši var ietekmēt informācijas un tehniskos resursus vairāk nekā 60 veidos, bet tikpat daudzos variantos iespējams pieļaut sistēmas apdraudējumus, rīkojoties neuzmanīgi. No iepriekš teiktā jāsecina, ka grūti ir atrast pasaulē tādu nozieguma sastāvu, kuru nevarētu izdarīt ar informācijas tehnoloģijas un komunikācijas palīdzību. Datornoziegumi var tikt iesaistīti tradicionālu reālā pasaulē pazīstamu noziegumu izdarīšanā, piemēram, krāpšanā, zādzībā, viltošanā, bojājumu nodarīšanā.

Neņemot vērā XIX gadsimta piemēru, oficiālā datornoziegumu vēsture sākās 1960. gadā, kad pasaulē parādījās pirmā zinātniskā informācija par jauna veida noziegumiem, ko speciālisti sauca gan par "datornoziegumiem" (*computer crimes),* gan arī par "datorsaistītiem noziegumiem" (*computer related crimes*). Šie noziegumi ietvēra sevī datormanipulācijas (*computer manipulation*), datorkaitniecību (*computer sabotage*), datorspiegošanu (*computer espionage*) un nelikumīgu datorsistēmu lietošanu (*illegal use of computer systems).*

20. gadsimta 70. gados arī Eiropā sākās pirmie zinātniskie pētījumi datornoziegumu jomā. Pētījuma avots bija dažas pierādītas datornoziegumu lietas, kā arī liels daudzums informācijas par latento datornoziedzību. Taču šie pētījumi vairāk balstījās uz jauno noziegumu veidu kriminoloģisko analīzi.

Eiropas Padomes vadībā datornoziegumu problēmas tika aplūkotas pirmo reizi XII Kriminoloģisko pētījumu institūtu direktoru konferencē, kas notika 1976. gadā, taču arī tad šo noziegumu kategoriju aplūkoja tikai kā ekonomisko noziegumu paveidu. Sabiedrības un zinātnes attieksme pret datornoziegumiem radikāli mainījās pēc 1980. gada, kad prese publicēja informāciju par pārsteidzošām urķu, vīrusu un "tārpu" lietām. Tas radīja nepieciešamību atrast piemērotu definīciju jaunajam fenomenam. Viens no ASV pazīstamākajiem datornoziegumu ekspertiem Dons Parkers (*Don Parker)* 1983. gadā datornoziegumu definēja kā "noziegumu, kura sekmīgai izdarīšanai ir nepieciešamas zināšanas datortehnikā". 1983. gadā ANO *OECD* ekspertu grupa definēja datornoziegumus kā "ikvienu nelikumīgu, neētisku vai nesankcionētu uzvedību, kas saistīta ar automātisko datu procesu un/ vai datu pārraidīšanu".

Viens no svarīgākajiem starptautisko tiesību dokumentiem datornoziegumu jomā ir Eiropas Padomes 1995. gada 11. septembrī pieņemtais dokuments "Par rekomendācijām procesuālajās tiesībās, kas saistītas ar informācijas tehnoloģijas izmantošanu" (95)13 (*Recommendation concerning problems of procedural law with information technology*). Minētais dokuments deva jaunu impulsu Eiropas valstu tiesiskās bāzes nostiprināšanā cīņai ar datornoziegumiem. Ja paraugāmies uz vēstures hronoloģiju, tad ir redzama ļoti skaidra tendence, kā tehnoloģiskais progress ietekmē noziedzību.

! *Tā, piemēram, Vācijā 1996. gadā policijā bija reģistrētas 32 128 lietas, ko apzīmēja ar terminu "datornoziegumi". No tām 26 802 lietas bija saistītas ar elektronisko naudas automātu manipulācijām, 3 588 – ar datorkrāpšanu, 198 – ar datu viltošanu, 282 – ar datorkaitniecību, bet 933 bija urķu lietas.*

! *Nīderlandē no 1981. līdz 1992. gadam bija reģistrētas apmēram 1 500 lietas, to skaitā apmēram 10% urķu lietu, 15% autortiesību pārkāpumu, 30% datorvīrusu. Turklāt katru gadu šis skaitlis pieaug.*

! *Japānā no 1971. gada līdz 1995. gadam bija 14 lietas, kas saistītas ar datora cietā diska sabojāšanu, 12 lietas par datu falsifikāciju, 7 lietas par nelegālu datora izmantošanu, 12 datu zādzības lietas. 1995. gadā parādījās jauna veida noziegumi, kas bija saistīti ar dažādām elektronisko karšu manipulācijām un netika ieskaitīti datornoziegumu statistikā.*

No datornoziegumu statistikas var izcelt divas tendences:
- nav bijusi vienota nostāja par to, ko uzskatīt par datornoziegumu;
- no 1970. līdz 1995. gadam ievērojami un uzskatāmi pieauga datornoziegumu izdarīšanas sarežģītības pakāpe, piemēram, no datu viltošanas parastajos veikala kases aparātos līdz sarežģītiem datu viltojumiem, ko var atklāt tikai ar dārgu un darbietilpīgu ekspertīžu palīdzību.

ASV ģenerālprokurora vietnieks E. Holders 2000. gada 12. janvārī Kibernoziegumu ekspertu sanāksmē norādīja, ka neviens patlaban nezina, cik lielas var būt augsto tehnoloģiju radītās problēmas. Var tikai aplēst ekonomiskos zaudējumus, kas nodarīti datornoziegumu dēļ. Zināms, ka rūpniecībai tie katru gadu rada miljardiem dolāru zaudējumu, bet neviens nevar pateikt, kādu sabiedrības dzīves jomu tie varēs ietekmēt nākotnē.

Latvijas policijas rīcībā ir neoficiāla informācija, ka 1997. gadā datornoziegumu nodarītie zaudējumi Latvijā varētu sasniegt 2–3 miļjonus dolāru. Taču jāpiebilst, ka šie skaitļi var būt arī pieņēmums, jo Iekšlietu ministrija līdz šim nav reģistrējusi datornoziegumus kā atsevišķu noziegumu veidu.

Iepriekš minētais izvirza ar datornoziegumiem saistītas krimināl ās likumdošanas harmonizācijas nepieciešamību. Lielu darbu šajā jomā veikusi Eiropas Padome (EP), kuras izveidotā ekspertu komiteja 1986. gadā apstiprinājavairākus ar datoriem saistītu pret privāto dzīvi vērstu noziegumu harmonizācijas principus.

- *Ultima ratio* princips.
  Privātās dzīves aizsardzība no apdraudējumiem, ko izraisa informācijas tehnoloģiju nelikumīga izmantošana.
  Šādi apdraudējumi galvenokārt ir jāapkaro ar administratīvām un civiltiesiskām metodēm, kriminālatbildību piemērojot tikai kā pēdējo līdzekli, ja iepriekšminētie pasākumi nevar tikt piemēroti.
- Krimināltiesību terminu precīzu formulējumu princips.
  Kriminālatbildības pamatam ir jābūt noteiktam precīzi, lai nebūtu divdomību iespējamības.
- Skaidrības princips.
  Krimināltiesību normai ir jābūt izteiktai skaidri un nepārprotami. Īpaši tas ir jāsaista ar nepieciešamību atturēties no tehnoloģisku terminu iekļaušanas tekstā.
- Dažādošanas princips.
  Nevar savienot vienā vispārējā pantā atbildību par dažāda rakstura privātās dzīves pārkāpumiem, kas izdarīti ar tehnoloģiju palīdzību. Tāpēc EP eksperti ierosina dažādot šo atbildību atkarībā no personas vainas, apdraudētām interesēm un nozieguma izdarīšanas motīviem.

- Nodoma princips.
  Privātuma pārkāpšanai saistībā ar datortehnoloģiju lietojumu ir jābūt sodāmai tikai tad, ja pārkāpums izdarīts ar nodomu. Ja šādi pārkāpumi izdarīti aiz neuzmanības, tad krimināatbildība piemērojama tikai izņēmuma gadījumos.
- Sūdzības princips.
  Ja pārkāpums uzskatāms par mazsvarīgu, pamatojoties uz EP Rekomendāciju R(87)17 "Par dalībvalstu justīcijas vienkāršošanu" 12.b (i) punktu, kas nosaka, ka "..būtu jāpalielina to lietu skaits, kurās tiesvedības ierosināšanai ir nepieciešama noteiktu nosacījumu izpildīšana, piemēram, tajos gadījumos, kur sabiedrības intereses nav tik svarīgas, par šādu nosacījumu tiesvedības ierosināšanai varētu būt cietušā lūgums vai piekrišana", tad tādas lietas ierosināmas tikai pēc cietušā sūdzības.

11.2.3. KIBERNOZIEGUMU KONVENCIJA

Kā jau iepriekš minēts, jau apmēram 20 gadus Eiropas Padome turpina darbu pie tādu starptautisko dokumentu izstrādes, kuru uzdevums būtu harmonizēt ar kibernoziegumiem saistītās krimināls un kriminālprocesuālās tiesību normas.

2001. gada 23. novembrī Budapeštā tika parakstīta EP Kibernoziegumu konvencija. Šīs Konvencijas uzdevums ir

- noteikt minimālo apjomu darbībām, par kuru izdarīšanu nepieciešams piemērot krimināatbildību;
- noteikt nepieciešamo kriminālprocesuālo darbību apjomu kibernoziegumu izmeklēšanai;
- noteikt kibernoziegumu jurisdikcijas principus;
- noteikt starptautiskās sadarbības principus kibernoziegumu atklāšanā un izmeklēšanā.

11.2.4. KIBERNOZIEGUMU KLASIFIKĀCIJA

Saskaņā ar Kibernoziegumu konvencijas izstrādāto klasifikāciju tiek izšķirti šādi kibernoziegumi:

- noziegumi pret datorsistēmu un datu drošību – konfidencialitāti, integritāti un pieejamību. Pie šiem noziegumiem pieder
  - nelikumīga piekļūšana,
  - nelikumīga noklausīšanās, pārtveršana,
  - datu traucēšana,
  - sistēmu traucēšana,
  - ierīču nelikumīga izmantošana;
- ar datoru saistīti noziegumi – krāpšana un viltošana;
- ar saturu saistīti noziegumi. Pie tiem pieder noziedzīgi nodarījumi, kur dators vai datorsistēma ir vide aizliegto materiālu nelikumīgai izgatavošanai vai izplatīšanai. Šie noziedzīgie nodarījumi ir vērsti pret konkrētās dalībvalsts kultūru un paražām. Dalībvalstis var pašas izlemt, kāda informācija internetā ir amorāla un nelikumīga. Konvencijā ir ietverts viens šāda rakstura noziegums – ar bērnu pornogrāfiju saistīts noziegums;

- ar autortiesībām saistīti noziegumi – autortiesību pārkāpumi, kas saistīti ar datu pārpublicēšanu, uzdošanos par autoru, nelikumīgu intelektuālo darbu izplatīšanu elektroniskajā veidā, arī pirātisms.

11.3. NOZIEDZĪGI NODARĪJUMI PRET DATORSISTĒMU DROŠĪBU

11.3.1. NELIKUMĪGA, PATVAĻĪGA, NESANKCIONĒTA PIEKĻŪŠANA DATORSISTĒMAI UN DATIEM

Daudzām pasaules valstīm pret ielaušanos datorsistēmās ir vāji tiesiskās aizsardzības mehānismi vai to vispār nav. Tas ir uzskatāms par nozīmīgāko trūkumu cīņā ar datornoziegumiem.

Terminu *computer hacking* tradicionāli tulko kā tādu ielaušanos datorsistēmās, kuras mērķis ir pārbaudīt informācijas sistēmu drošību, nevis izdarīt manipulācijas ar informāciju. Tomēr šī izpratne vairāk dominē starp tiem, kuri nav tieši saistīti ar informāciju sistēmu drošību vai tiesību aizsardzības iestādēm.

Datorsistēma ir līdzīga aizslēgtam dzīvoklim, un tāpēc ielaušanos datorsistēmā var pielīdzināt zādzībai, savukārt urķi – kramplauzim. Patvaļīga piekļūšana datorsistēmām ir kā stūrakmens citu ar datoriem saistītu noziegumu izdarīšanā.

! *Ir dzirdēts gadījums, kad darbinieces klātbūtnē urķis ielauzies datorsistēmā, atslēdzis visas sistēmas drošības funkcijas, pārbaudījis visu datorā esošo informāciju un sācis dzēst datnes. Šīs darbības varētas pārtraukt tikai ar datorsistēmas atvienošanu no elektrotīkla.*

Speciālisti uzskata, ka praksē šādas darbības sen jau ir pārkāpušas to robežu, ko varētu nosacīti dēvēt par "ziņkārību". Pēc ASV Federālā izmeklēšanas biroja 1999. gada datiem, biroja izmeklēšanas procesā ir vairāk nekā 8900 šādu noziegumu. 1997. gadā šis skaitlis nav pārsniedzis 200. Analoga situācija ir arī Eiropā, piemēram, 1991. gadā Nīderlandē katrs piektais kibernoziegums bijis piekļūšana datorsistēmai.

Īpaši šī problēma satrauc ASV Aizsardzības ministriju, jo urķi spēj iebrukt pat ļoti labi aizsargātās datorsistēmās, kas glabā militāra rakstura informāciju, un tādā veidā nodara ievērojamu kaitējumu. ASV Armijas Gaisa karaspēkā ir izstrādāts speciāls jautājumu bloks, kas palīdz atbildīgām amatpersonām kontrolēt situāciju datorsistēmas lietotāju vidū. Darbinieki tiek brīdināti, ka ik reizi, kad tiek ieslēgts dators vai mobilais telefons, viņi riskē iefiltrēt savā sistēmā kibertelpā noslēpušos, uzglūnošu urķi, kas gaida brīdi, kad kāds pieļaus kļūdu savas datorsistēmas aizsardzībā un pavērsies iespēja iegūt sensitīvu militāru informāciju. Periodiski darbiniekiem ir jāizpilda formulārs, kurā jāatbild uz vairākiem jautājumiem.

- Vai Jūs, saņemot datorā jaunu informāciju, pārbaudāt, no kurienes šī informācija nāk?
- Vai Jūs, saņemot e-pastu, varat identificēt sūtītāju? Vai šī e-vēstule ir sūtīta no interneta vai intraneta? Vai tās saturs ir pārbaudīts ugunsmūrī?

- Vai Jums pēdējās sanāksmes laikā bijis klāt digitālais palīgs *Palm Pilot*?
- Vai Jūs lietojat datoru, lai nosūtītu slepenotu vai neslepenotu informāciju?

Ja darbinieki uz kādu no jautājumiem atbild apstiprinoši, tad viņi uzskatāmi par potenciālajiem urķu apdraudējuma objektiem. Pamatojoties uz šiem jautājumiem, darbiniekiem tika izstrādāti ieteikumi, kuros ir izšķirti trīs riska avoti: pirmkārt, dators, otrkārt, interneta banka, treškārt, mobilais telefons.

Apdraudējumi var skart ne tikai datorsistēmu, bet arī mobilo telefonu, jo, attīstoties e-komercijas iespējām, pirkumus var izdarīt arī ar mobilo telefonu, tajā ievadot savas kredītkartes vai debetkartes numuru, kas savukārt ir urķu intereses objekts.

Visus ieteikumus var apkopot vienā teikumā, proti: neveiciet nepārdomātas darbības, neuzticieties svešiem, nesaistieties ar nezināmas izcelsmes informācijas avotiem, neglabājiet savas kredītkartes, debetkartes un citu tamlīdzīgu dokumentu numurus mobilajā telefonā vai datora atmiņā!

11.3.2. ATBILDĪBA PAR NOZIEGUMIEM PRET DATORSISTĒMU DROŠĪBU EIROPĀ

Eiropas valstu sodu likumos un krimināLkodeksos iekļautie noziedzīgie nodarījumi un to sastāvs, kas paredz atbildību par patvaļīgu piekļūšanu, dod iespēju izdarīt dažus secinājumus.

- Šiem nodarījumiem ir kopīgs tas, ka to objekts ir datorsistēma un tās resursi.
- Visas valstis paredz atbildību par nepilnvarotu jeb nesankcionētu (patvaļīgu) piekļūšanu datorsistēmas resursiem. Pilnvarošana neparedz, ka personai obligāti jābūt brīdinātai (rakstiski, mutiski) par neatļautām darbībām. Pat tad, ja konkrētais informācijas resurss ir publisks un visiem pieejams, mājaslapas autors, tajā ievietojot konkrētu informāciju, ir skaidri un nepārprotami klusējot izteicis savu gribu, proti, to, ka viņš nevēlas, lai kāda persona, bez viņa piekrišanas mājaslapu lietojot, mainītu tās saturu un vizuālo informāciju. Klusējošās gribas pārkāpums ir termina "nepilnvarota darbība" satura sastāvdaļa. Tāpēc tas var būt pamats personas saukšanai pie krimināLatbildības.
- Pieaugot tehnoloģiju iespējām, palielinās un paplašinās arī urķu iespējas, un prakse ir pierādījusi, ka tad, kad valsts sašaurina "nepilnvarotas piekļūšanas" definīciju, likumpārkāpējiem rodas iespējas izvairīties no atbildības.

Kā norādīts Kibernoziegumu konvenciju paskaidrojošā memorandā, Eiropas valstīm nodarījuma "nepilnvarota piekļūšana" satura formulējumā ir dažādas pieejas. Tā dažas valstis par nepilnvarotu pieslēgšanos atzīst pašu pieslēgšanās faktu neatkarīgi no tā, kādas sekas tas izraisa. Vairākas valstis ir iekļāvušas šā nozieguma aprakstā konkrētus kvalificējošos apstākļus, piemēram, sistēmas drošības pārkāpšanu, speciālu nodomu iegūt datus, citu personu negodīgu nolūku vai prasību, lai datorsistēma būtu saistīta ar citām datorsistēmām. Tāpēc Konvencija neatzīst par krimināli sodāmu nodarījumu gadījumus, kad persona fiziski ir iekļuvusi vientuļā, ar tīklu nesavienotā datorā. Par šo pieeju var strīdēties, jo saskaņā ar Konvencijas projekta 1. pantu

ikviens dators, kas ir savstarpēji saistīts ar vairākām ierīcēm, no kurām vienas vai vairāku ierīču darbības pamatā ir datorprogramma un iespēja veikt datu apstrādi, ir datorsistēma. Tomēr arī šis izskaidrojums ir dažādi vērtējams. Galvenais iemesls, kāpēc eksperti neatzīst par patvaļīgas piekļūšanas objektu vienu datoru, kas savienots ar drukas ierīci, monitoru, ir tas, ka šai sistēmai, ja tā nav saslēgta ar citiem datoriem vai tīkliem, nav "urķēšanas" *(hacking)* nozīmē paredzēto apdraudējuma faktoru, tas ir, nav iespējas piekļūt datorsistēmai no attāluma.

Konvencija neaizliedz dalībvalstīm savos krimināllikumos paredzēt arī papildu faktorus šādu darbību kriminalizēšanai, un tāpēc nevienai valstij nav aizliegts savā krimināl kodeksā vai sodu likumā paredzēt atbildību arī par piekļūšanu vienai nošķirtai datorsistēmai, kas nav savienota ar citām datorsistēmām.

11.3.3. ATBILDĪBA PAR NOZIEGUMIEM PRET DATORSISTĒMU DROŠĪBU LATVIJĀ

Latvijā Krimināllikuma (KL) [48] 241. panta 1. daļa par patvaļīgu piekļūšanu datorsistēmai atzīst darbību, „ja ar to nepiederīgai personai radīta iespēja iepazīties ar sistēmā esošo informāciju", bet otrā daļa paredz papildu nosacījumus, „ka darbībām jābūt saistītām ar datortehnikas programmatūras aizsardzības līdzekļu pārvarēšanu vai pieslēgšanos sakaru līnijām". Nodarījums paredz vairākas kvalificējošās pazīmes – iespēju trešajai personai iepazīties ar sistēmā ievietoto informāciju, to saistīšanu ar datortehnikas programmatūras aizsardzības līdzekļu pārvarēšanu vai ar pieslēgšanos sakaru līnijām.

KL 241. pantā paredzētais sods par patvaļīgu piekļūšanu datorsistēmai ir arests vai arī naudas sods līdz astoņdesmit minimālajām mēnešalgām. Par tādām pašām darbībām, ja tās saistītas ar datortehnikas programmatūras aizsardzības līdzekļu pārvarēšanu vai ar pieslēgšanos sakaru līnijām, soda ar brīvības atņemšanu uz laiku līdz vienam gadam vai ar naudas sodu līdz simt piecdesmit minimālajām mēnešalgām.

11.3.4. ATBILDĪBA PAR IS DROŠĪBAS NOTEIKUMU PĀRKĀPUMIEM

Krimināllikums paredz atbildību arī par organizācijas izstrādāto Informācijas sistēmu drošības noteikumu pārkāpumiem. Saskaņā ar KL 245. pantu par organizācijā „izstrādātu informācijas glabāšanas un apstrādes noteikumu vai citu informācijas datorsistēmas drošības noteikumu" pārkāpšanu, „ko izdarījusi persona, kura ir atbildīga par šo noteikumu ievērošanu, ja tas bijis par iemeslu informācijas nolaupīšanai, iznīcināšanai vai bojāšanai vai ar to radīts cits būtisks kaitējums, soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar piespiedu darbu, vai ar naudas sodu līdz četrdesmit minimālajām mēnešalgām".

Minētā panta speciālais nozieguma objekts ir informācijas sistēmu drošība, un atbildība par to var iestāties tikai tad, ja organizācijā ir izstrādāti IS drošības noteikumi un noteiktas atbildīgo personu tiesības un pienākumi, vai arī

gadījumos, ja organizācijai ir jāievēro MK noteikumos noteiktās minimālās drošības prasības.

! *Kāda rajona policijas pārvaldes ēkā notiek ugunsgrēks, un tā dēļ pilnīgi tiek sabojāta organizācijas datorsistēma. Līdz ar to sadeg visi informācijas resursi, arī datorsistēmā esošie operatīvās darbības izstrādes materiāli, izziņā esošās krimināllietas un citi svarīgi dokumenti, kuru atjaunošana praktiski nav iespējama. Ar šo dokumentu iznīcināšanu valstij ir nodarīts būtisks kaitējums. Kaut gan IS drošības noteikumi, kuri ir saistoši jebkurai valsts vai pašvaldības institūcijai, stājās spēkā jau 2000. gada 1. jūlijā, šajā policijas struktūrvienībā nebija izstrādāti savi IS drošības noteikumi un nebija norīkotas atbildīgās personas. Šajā gadījumā iestādes vadītājs, piemēram, rajona policijas priekšnieks, nebija izpildījis MK noteikumu prasības, proti, attiecībā uz pasākumiem, kas jāveic IS organizācijai pret ārkārtas apstākļiem, kā arī attiecībā uz informācijas resursu rezerves kopiju izgatavošanas un glabāšanas kārtību (MK IS drošības noteikumi nosaka, ka informācijas resursu kopijas ir glabājamas vismaz divās ģeogrāfiski dažādās vietās, kur nodrošināta to glabāšanas kārtība atbilstoši sistēmas organizācijai noteiktajai informācijas nesēju glabāšanas kārtībai). Šajā gadījumā konkrētā amatpersona ir saucama pie krimināltatbildības arī tad, ja šādi iekšējie IS drošības noteikumi nav izstrādāti.*

11.4. DATU UN SISTĒMU TRAUCĒŠANA

Iepriekš minētā nesankcionētā pieslēgšanās datorsistēmai it kā atver datorsistēmas, datortīklu vārtus iespējām izdarīt citus noziegumus. EP Kibernoziegumu konvencijā paredzēts kriminalizēt tādus samērā jauna veida nodarījumus kā datu un sistēmu darbības traucēšana.

Kibernoziegumu konvencijas 4. pants nosaka dalībvalstīm pienākumu paredzēt krimināltatbildību par tīšu, prettiesisku datu bojāšanu, iznīcināšanu, pasliktināšanu, grozīšanu vai apslāpēšanu, noklusēšanu, bet 5. pants paredz tādu pašu atbildību noteikt par sistēmu traucēšanu. Sistēmu traucēšana Konvencijas izpratnē ir tīša, prettiesiska nopietna datorsistēmas darbības funkciju traucēšana, kavēšana, ievadot, pārsūtot, bojājot, iznīcinot, pasliktinot, modificējot sistēmas datus.

Kā norādīts Konvenciju paskaidrojošā memorandā, šie abi iepriekš minētie panti tikuši iestrādāti tādēļ, lai datu vai datorsistēmas bojājuma gadījumā tiem nodrošinātu tādu pašu aizsardzību, kas paredzēta par tīšu zaudējumu nodarīšanu priekšmetiskām lietām. Aizsargātā juridiskā interese šeit ir pienācīga datorprogrammu un datu lietošana.

Datu un sistēmu traucēšanu var iedalīt vairākos veidos pēc lietotāju veiktajām darbībām.

- **Datu dzēšana**. Traucējumi datorsistēmā, kas radīti, dzēšot datus, var tikt pielīdzināti priekšmetiskas mantas bojāšanai; to apstiprina arī termina „izdzēšana" saturs. Proti, datu vai datorprogrammu datu dzēšana ir darbība,

kas izposta, sagrauj datus vai datorsistēmu resp. padara tos par neatpazīstamiem un nelietojamiem. Mantas bojāšana reālā pasaulē rada tādas pašas sekas.

- **Noklusēšana, apslāpēšana**. Tā nozīmē jebkuru darbību, kas beidz pieeju datorsistēmā vai vidē saglabātiem datiem. Šis termins ietver divas nozīmes:
  - dati ir nodzēsti, un tie vairs fiziski neeksistē;
  - dati ir padarīti nepieejami, tas ir, šiem datiem nevar piekļūt.
- **Datu pārveidošana**. Tā nozīmē jebkuru esošo datu modifikāciju, kas sevī ietver arī tādas darbības kā
  - datu viltošanu (*spoofing*), ko sauc arī par mānīšanos,
  - šifrēšanu, kas padara datus par neizlasāmiem.
- **Bojājumi, ko sistēmai nodara kaitīgas programmas**. Konvencijas izpratnē pie kaitīgām programmām pieskaita jebkuru datorprogrammu vai ierīci, kuras mērķis ir traucēt sistēmas datus vai resursus, piemēram, datorvīrusus, graujošas programmas – tārpus (*worm*) un datorindes (*computer contaminant*).
- **Surogātpasts** (*spamming*). Tas nozīmē liela apjoma nepieprasītus elektroniskā pasta sūtījumus, piemēram, ikdienā pienākošos reklāmas materiālus, kuri lietotājus neinteresē un no kuriem nav iespējams „atrakstīties". Surogātpasta problēmu juridiski mēģina ierobežot vairākas valstis, piemēram, ASV, Austrālija, Lielbritānija. Pēdējā paskaidrojošā memoranda variantā īpaši uzsvērts, ka krimināllatbildību par šīm darbībām var paredzēt tad, ja tās ir izraisījušās būtiskus sistēmas darbības traucējumus.

11.4.1. DATU PĀRVEIDOŠANA UN PROGRAMMATŪRAS BOJĀŠANA

LR Krimināllikuma 243. pants paredz atbildību par datortehnikas programmatūras bojāšanu. Tas ietver ne tikai „informācijas nesēju, datortehnikas programmatūras vai aizsardzības sistēmu apzinātu bojāšanu vai iznīcināšanu", bet arī sistēmas datu „neatļautu modifikāciju, grozīšanu, bojāšanu vai iznīcināšanu" un „apzināti nepatiesas informācijas ievadīšanu". Taču atbildība ir paredzēta tikai gadījumos, kad ar noziedzīgo darbību ir „radīts būtisks kaitējums". Par šāda veida noziegumu var sodīt ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar naudas sodu līdz simt piecdesmit minimālajām mēnešalgām.

Apzināti nepatiesas informācijas ievadīšana ir darbība, kuras mērķis ir ietekmēt datorsistēmas resursu funkcijas. Minētās darbības var ietvert arī vīrusveidīgu vai citu speciāli veidotu programmu iedarbību uz sistēmas tehniskajiem vai informācijas resursiem.

Jāatzīmē, ka datu pārveidošanu vai datortehnikas bojāšanu var veikt tīši vai netīši, likumīgie lietotāji vai lietotāji, kuri nelikumīgi ir ieguvuši piekļuvi sistēmai vai tās datiem. Minētais KL 243. pants izvirza pret noziegumu vēl vienu prasību, proti, iedarbībai uz sistēmas informācijas resursiem ir jābūt neatļautai. Šis jautājums ir cieši saistīts ar darbību tiesiskuma izvērtēšanu, jo diezgan nepārdomāti būtu interpretēt terminu "atļauts" vai "neatļauts", balstoties tikai uz aktīvā veidā paustu gribas izpausmi aizliegt kādu konkrētu

darbību. Tad tiesu prakse drīz vien nonāktu strupceļā, jo nav iespējams visu regulēt tikai ar rakstiskiem aizlieguma uzrakstiem. Šī neviennozīmīgā atruna ļauj daudzos gadījumos izvērtēt šī veida noziegumu par sliktu sistēmas pārzinim, kas, iespējams, acīmredzami neatļautas darbības nav īpaši izcēlis.

11.4.2. DATORVĪRUSU VĒSTURE

Modernā datora "tēvs" Džons fon Neimans jau no 1948. gada loloja ideju par pašreproducējošu datorprogrammas koda izstrādi. 1970. gadā notika pat speciālas apmācības datorvīrusu rakstīšanā. Šīs programmas nosauca par *Core wars*, un to uzdevums bija mākslīgi radītā vidē cīnīties vienai pret otru. Pašreplicējošās programmas ir kļuvušas par nopietnu draudu visām pasaules datorsistēmām. Vienīgi *Apple Macintosh* datorsistēmām līdz šim bijusi iespēja izvairīties no nopietniem apdraudējumiem.

Kaitīgo programmu veidi ir visai dažādi, tāpēc nebūtu pareizi likumdošanu saistīt tikai ar datorvīrusiem. Tā ir tikai maza daļa no kaitīgo ierīču un programmu klāsta, jo šajā kategorijā var iekļaut arī urķu instrumentus – jebkuru speciāli veidotu ierīci vai programmu, kas var piekļūt tīmekļa lapām tieši vai ar hipersaišu starpniecību, ieskaitot dziļās saites (*deep links*), kā arī sīkdatnes *(cookies)* un citas līdzīgas programmas, ar kuru starpniecību komunikācijās var noteikt informācijas atrašanās vietu un iegūt to. Šie instrumenti visbiežāk tiek izmantoti nelikumīgi ar mērķi nodarīt kaitējumu datorsistēmu vai tīklu resursiem. Tāpēc nereti speciālisti šīs kaitīgās ierīces un programmas kopā sauc arī par "kaitīgiem kodiem" (*harmful code)*. Šie instrumenti var būt pielāgoti vai tieši veidoti noziedzīga mērķa sasniegšanai.

Pamatojoties uz šo koncepciju, eksperti sākotnēji akcentēja ierīces nelikumīgo raksturu un nosauca attiecīgos noziegumus par tādiem, kas saistīti ar „nelikumīgām ierīcēm" (*illegal devices)*. Eksperti nebija ņēmuši vērā, ka šādas ierīces nereti tiek izmantotas, lai testētu informācijas sistēmu drošību. Tāpēc pēc Kibernoziegumu konvencijas projekta publicēšanas sabiedrību uztrauca tas, ka, definējot nelegālu ierīci, projekta autori ir tās saturā iekļāvuši ļoti plašu objektu loku, arī tos objektus, ko var izmantot likumīgiem mērķiem, bet tas savukārt var apdraudēt e-komercijas attīstību un samazināt cilvēktiesību garantijas.

! *Turcijas IPS kompānijas Super-online padomnieks rakstīja, ka arī nelikumīga ierīce var tikt izmantota likumīgiem mērķiem. Viņš norādīja vairākus gadījumus, kad sistēmas drošības stāvokļa pārbaudīšanai tika speciāli izveidota programma, kuras mērķi ir atklāt IS vājās vietas un tādējādi piekļūt tai un diagnosticēt tās drošības stāvokli. Tāpēc arī šis padomnieks norādīja: Konvencijā nepārprotami jāparedz, ka atbildība var iestāties tikai tad, ja nelikumīgā ierīce tiek izmantota noteikto noziegumu izdarīšanai, lai nevienam nerastos šaubas, ka atbildība nevar iestāties par likumīgu šādu programmu lietošanu. Viņš arī uzskata, ka, nosakot atbildību par šādas ierīces izgatavošanu, var ievērojami apgrūtināt darbu gan pie jaunu IS drošības instrumentu radīšanas, gan pie konkrēto problēmu zinātniskās izpētes.*

11.4.3. ATBILDĪBA PAR KAITĪGO PROGRAMMU IZPLATĪŠANU

Lielākā daļa Eiropas valstu atbalsta ideju par to, ka kaitīgo programmu vai kaitīgā koda izgatavošanai un izplatīšanai ir jābūt krimināli sodāmai darbībai. To īpaši mudina darīt jaunā veida kaitīgās programmas, ar kurām nav iespējams cīnīties vienas valsts robežās. Tāpēc īpaši svarīgi ir atrast to vidusceļu, kas būtu pieņemams visām valstīm.

Atbildība, kas var tikt piemērota par dažāda veida darbībām ar kaitīgām programmām, var būt iedalīta šādās grupās:

- atbildība par kaitīgās programmatūras izgatavošanu;
- atbildība par kaitīgās programmatūras izplatīšanu (jebkuras darbības, kas saistītas ar kaitīgo programmu realizēšanu, arī pavairošana, tirdzniecība, eksports, imports);
- atbildība par pieejamības nodrošināšanu citā veidā (piemēram, konkrētās kaitīgās programmas ievietošana tiešsaistē pieejamā resursā, lai to varētu izmantot citi lietotāji).

! *ASV datorspeciālists Moriss R. Tapans radīja tārpu (programmu, kas patstāvīgi vairojas) un izplatīja to internetā. Viņa mērķis bija pārbaudīt UNIX operētājsistēmas drošības vājās vietas. Pēkšņi tārps kļuva nevadāms. Tāpēc tas nodarīja ievērojamu kaitējumu svarīgākajām ASV datorsistēmām. Tiesa Tapanu atzina par vainīgu tāpēc, ka viņš, ieliekot programmā asprātīgus zinātniskus risinājumus, gribējis neatļauti iekļūt datorsistēmās, kaut arī nebojājot sistēmas aizsardzības līdzekļus.*

Šis piemērs uzskatāmi liecina, ka persona ir saucama pie atbildības nevis par jebkuras tādas ierīces izgatavošanu, kas var nodarīt arī kaitējumu datorsistēmai, bet par to, ka programma izveidota ar mērķi nelikumīgi iekļūt datorsistēmās.

! *Nesen pasaulē tika izplatīts vīruss ar nosaukumu "homepage", kurš atver lietotājam pieeju ar x atzīmētām mājaslapām, kas satur pornogrāfiju. Vīruss tiek ievadīts datorā ar e-pastam pievienoto datni, un tas izplatās, izmantojot e-pasta sistēmas adrešu grāmatiņu. Šis datorvīruss radīja nopietnus darbības traucējumus 7000 Zviedrijas tiesu administrācijas tīklam pievienotajiem datoriem.*

! *Beļģijas tiesa sodīja kādu 25 gadus vecu vīrieti ar naudas sodu ~ Ls 1500 apmērā par to, ka viņš, tīši atriebjoties kādai sievietei par interneta "tērzēšanas istabā" izteikto atraidījumu, nosūtīja tās datoram vīrusu, kas sabojāja šīs sievietes datorsistēmas informācijas resursus.*

Šie piemēri liecina, ka datorvīrusu var ievadīt internetā un tālāk šī programma pati, izmantojot dažādus tehniskos paņēmienus, izplatās pasaulē, bet ir arī gadījumi, kad datorvīrusu var nosūtīt konkrētai personai, lai atriebtos.

! *Kāds lietotājs ir izstrādājis datorvīrusa programmu un pārbaudījis tās darbības efektivitāti. Zinot, ka šī programma var nelikumīgi piekļūt datorsistēmas resursiem un nodarīt tiem kaitējumu, viņš apzināti ievietojis hipersaiti,*

kas dod pieeju šai kaitīgajai programmai, reklamējot to dažādos interneta meklētājos. Tātad šo personu var saukt pie atbildības gan par šādas programmas izgatavošanu, gan arī par to, ka tā padarīta pieejama citiem.

Arī Latvijā ir paredzēta atbildība par kaitīgo programmu izplatīšanu. Tā ir noteikta Krimināllikuma 244. pantā. KL datorvīrusu definē kā programmatūras līdzekli, kas izraisa datortehnikas programmatūras vai informācijas nesankcionētu iznīcināšanu vai grozīšanu vai kas sabojā datoru vai sagrauj aizsardzības sistēmu. Atbildība ir paredzēta par datorvīrusa apzinātu izplatīšanu vai „jauna veida vīrusa ievadīšanu datortehnikas programmatūras vidē". Vainīgo var sodīt „ar brīvības atņemšanu uz laiku līdz četriem gadiem vai ar naudas sodu līdz 200 minimālajām algām". Savukārt par tām pašām darbībām, kuras nodara būtisku kaitējumu, var sodīt ar „brīvības atņemšanu uz laiku līdz 10 gadiem".

Kā redzams no Krimināllikuma 244. panta dispozīcijas, Latvijas likumdevējs izvēlējies "šauro" kaitīgo programmu formulējumu. Ar šo dispozīciju var aptvert datorvīrusus. Taču jau iepriekš minēts, ka datorvīrusi ir tikai niecīga daļa no visu kaitīgo programmu vai ierīču apjoma.

11.4.4. SUROGĀTPASTS

Ikviens interneta lietotājs, kas izmanto e-pastu, kaut reizi ir saņēmis vēstuli, par kuras saturu vai saņēmēju neko nezina. Visbiežāk tie ir dažādi reklāmas materiāli, ko saņēmējs nekad nav lūdzis sūtīt, piedāvājumi iegādāties preces lētāk, kā arī daudzsološās ķēdes vēstules "Nosūtiet šo vēstuli 10 draugiem, un jūs šodien piedzīvosiet laimi", kuras visbiežāk mūsu e-pastu noslogo Ziemassvētku laikā un pirms Jaungada. Šāds ziņojums var ne tikai neatbilst saņēmēja interesēm, bet arī būt nevēlams, jo nekad nav bijis pasūtīts.

Viens no veidiem, kā surogātpasta sūtītāji iegūst savu upuru e-pasta adreses, ir to zagšana no ziņu grupām, kas visdažādāko iemeslu dēļ diemžēl nespēj aizsargāt savu klientu e-pasta adreses pret nokļūšanu ļaunprāšu rokās, kā arī to kompāniju izmantošana, kuras specializējušās e-pastu sarakstu izveidē un pārdošanā.

Ārzemēs surogātpasts jau ir apzināts kā nopietna problēma un uzsākta cīņa pret to, bet Latvijā, šķiet, šīs bezjēdzīgās vēstules tīklā vēl nav paspējušas interneta lietotājus nogurdināt, jo nav radījušas nopietnus draudus datoram. Amerikā, izvēloties savu interneta pakalpojumu sniedzēju (IPS), potenciālie klienti interesējas par iespēju nodrošināt datoram filtrus un sekošanu pēc reklāmas materiāliem. Arī paši IPS ir uzsākuši cīņu ar surogātpasta sūtītājiem, atslēdzot tos no tīkla. Pasaulē arvien vairāk tiek investēts cīņā pret surogātpastu. Vēlme pasargāt sevi no nelūgtām vēstulēm un aizsargāt savu datoru pret vīrusiem ir radījusi strauju investīciju pieaugumu dažādu programmatūru iegādē un filtru uzstādīšanā gan darba vidē, gan arī mājās. Piemēram, programma *Spam Killer* (darbojas 30 dienas pēc instalācijas datorā) piedāvā iespēju nosūtīt kļūdas paziņojumu, respektīvi, surogātpasta sūtītājs saņem vēstuli, kurā rakstīts *Subject: Returned mail: User unknown*, iespējams, aizdomājas par šādas adreses eksistenci, un tāpēc sistēma turpmāk šādus ziņojumus vairs nesūtīs.

Zinošākie lietotāji aktīvi izmanto arī e-pasta programmu piedāvātās aizsardzības iespējas. Piemēram, ja jums ir kāda no e-pasta programmām – *Outlook, Outlook Express, Eudora, Mozilla* utt., tās pašas piedāvā uzstādīt filtrus ienākošajam e-pastam (izdzēst, pārvietot citā mapē, automātiski atbildēt, taču šiem filtriem tomēr ir trūkumi – tie darbojas tikai tad, kad programma ir palaista). Svarīgi atzīmēt, ka filtrus vai aizsargprogrammas ir iespējams uzstādīt gan serverī, gan arī pašā datorā.

11.4.5. CĪŅA AR SUROGĀTPASTU ASV

Vissīvākā cīņa pret surogātpastu pašlaik norisinās ASV. Daudzi ierosinātie ASV federālie un pavalstu likumprojekti sola aizsargāt e-pasta lietotājus. Bet vai likumam tiešām ir pa spēkam apturēt surogātpasta plūdus?

Virdžīnijas pavalstī masveida e-pasta sūtīšana, uzrādot viltus atpakaļadresi, tiek atzīta par krāpšanu. Ja Vašingtona pavalstī tiek nosūtīts surogātpasts ar maldinošiem virsrakstiem (*Subject*), sūtītājiem var piespriest 500 dolāru lielu soda naudu par katru pārkāpumu. 14 ASV pavalstīs ir prasība, lai reklāmu e-pasta sūtītājiem temata ailē būtu apzīmējums ADV, bet Delaveras pavalstī ir aizliegti visi neaicināta komerciāla satura e-pasta veidi. Taču ikviens e-pasta lietotājs ir pārliecinājies, ka neviens no šiem likumiem, kā arī neviens no 15 citiem pret surogātpastu vērstiem likumdošanas aktiem nav apturējis nevēlamo masveida sūtījumu straumi.

Pret surogātpastu ir vērsti divi dažādi cīņas veidi: 1) likumdevēju pašreizējā cīņa par to, kā pasargāt saņēmēju e-pasta kastītes no „glumas" pornogrāfijas, augu valsts viagras un citas drazas, un 2) cīņa par to, kas notiks ar šīm pasta kastītēm tad, kad (ja vispār) iepriekšminētie pretīgie sūtījumi tiks iznīcināti. Lielākie reklāmdevēji – šīs pasaules varenie, piemēram, *Citibank*, *Ford*, *Microsoft,* – un lielie IPS, kas var labi nopelnīt, pārsūtot datus, vēlas gūt iespēju piesūtīt lietotājiem reklāmas, kamēr lietotāji paši no tām neatsakās (šī procedūra pazīstama ar nosaukumu *opt out* – izvēle atteikties).

Pretsurogāta aktīvisti (galvenokārt privātpersonas, kā arī mazi un vidēji IPS) vēlas tādu likumdošanu, kas prasītu katram reklāmdevējam – gan „glumajiem", gan pārējiem – vispirms iegūt saņēmēju atļauju, lai varētu sūtīt reklāmas, izmantojot *opt in* metodi – izvēli pieteikties. Pretējā gadījumā, viņuprāt, komerciālo e-pasta sūtījumu apjoms pieaugs līdz tādiem apmēriem, ka e-pasts kā saziņas līdzeklis zaudēs jēgu.

No šī strīda iznākuma ir atkarīga arī vienkāršo e-pasta lietotāju nākotne. Pagaidām gan uzvarai tuvāk ir reklāmdevēji.

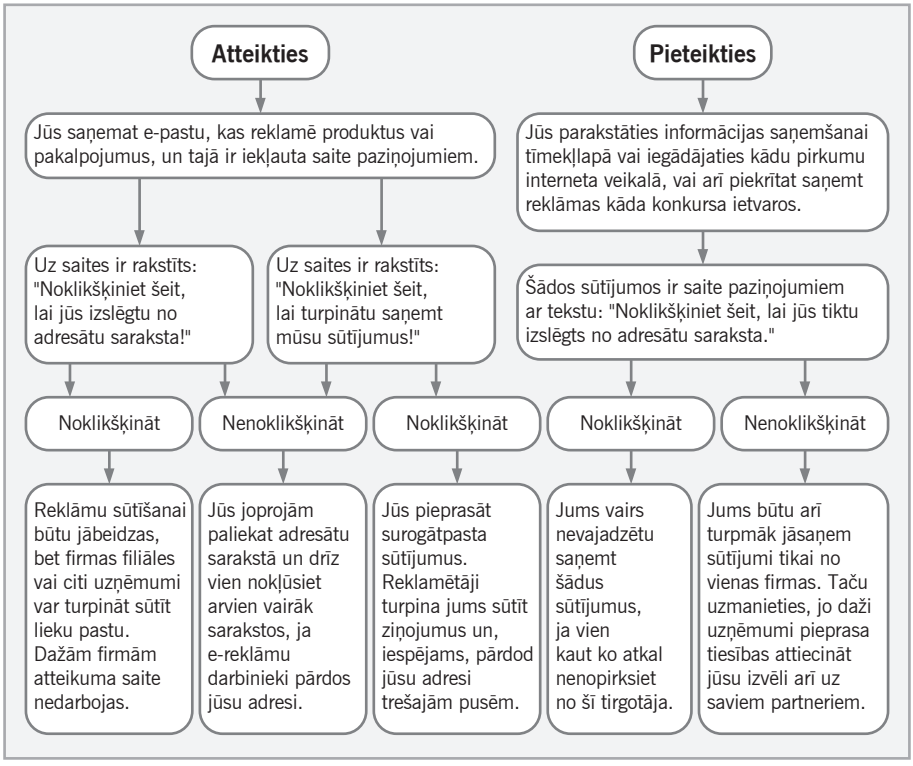
Pašlaik ASV visstingrākais pret surogātpastu vērstais likumdošanas akts nemaz neatrodas ASV Kongresā. 2003. gada maijā Kalifornijas Senāts apstiprināja Senāta likumprojektu Nr. 12 (SB 12), ko iesniedza senatore Debra Bouvena. Iesniegtajā SB 12 par pamatu izmantots 1991. gada federālais Likums par telefona lietotāju aizsardzību. Šis likums, kas plašāk pazīstams kā Surogātfaksu likums, izrādījās ļoti efektīvs cīņā pret neaicinātiem faksiem. SB 12 aizliedz sūtīt komerciāla satura e-pasta ziņojumus bez saņēmēja iepriekšējas piekrišanas un atļauj personām, kuras saņem neaicinātus komerciāla satura

e-pasta ziņojumus, iesūdzēt sūtītājus tiesā un saņemt 500–1500 dolārus par vienu pārkāpumu. Tātad, ja kāds cilvēks saņēmis no viena sūtītāja desmit surogātpasta ziņojumus, viņš var iesūdzēt vainīgo tiesā par 5 000–15 000 dolāru, ja tiesa atzīs, ka pārkāpums bijis tīšs.

„Vienīgais, ko surogātpasta sūtītāji sapratīs, ir peļņas zaudēšana," uzskata D. Bouvena, kas sarakstījusi Kalifornijā esošos noteikumus, kuri vērsti pret surogātpastu „izvēle "pieteikties". Tagad senatore ir pārliecināta, ka nepieciešami stingrāki likumi. „Tikai tie spēs apturēt šo lietu." (1997. gadā ar ASV Senāta likumprojektu tika mēģināts papildināt Surogātfaksu likumu, lai tas attiektos arī uz e-surogātpastu, bet tas tika „nogremdēts" komitejā.)

Protams, vajāt surogātpasta sūtītājus ne vienmēr ir viegli, jo viņi var iekārtot savu biroju ārzemēs un viņiem nav obligāti jāatklāj sava atrašanās vieta. Demokrātijas un tehnoloģiju centra pārstāvis A. Švarcs atzīst, ka Surogātfaksu likumu ir vieglāk īstenot nekā līdzīgas prasības attiecībā uz surogātpastu, jo faksa sūtītājs nevar viltot savu faksa numuru un faksu sūtīšana no ārzemēm pārmērīgi sadārdzina procesu. „Surogātpasta sūtītāji var pārvākties uz ārzonu," paskaidro Švarcs. „Drazu faksu sūtītāji to nevar."

Visu ASV likumprojektu pamatā ir shēma „izvēle atteikties": saņēmējam pašam ir aktīvi jārīkojas, lai neļautu reklāmdevējiem sūtīt liekus e-pasta paziņojumus.



18. att. Aizsardzība pret surogātpastu.

11.5. NELIKUMĪGA NOKLAUSĪŠANĀS

11.5.1. VĒSTURE

Kopš 1657. gada pasaulē ir pazīstams noziegums, ko dēvē par pasta sūtījumu nelikumīgu pārtveršanu. Lielbritānijā kopš 1663. gada atļauju pārtvert pasta sūtījumus drīkstēja dot tikai Valsts sekretārs. Līdzīga situācija bija arī citās valstīs – pārtvert pasta sūtījumus drīkstēja tikai ar noteiktas valsts amatpersonas rakstisku rīkojumu. Šāda prakse pastāv arī Latvijā.

No pasta karietes līdz mūsdienām sabiedrība ir nogājusi garu ceļu komunikācijas līdzekļu attīstībā. Tomēr visos laikos bijuši mēģinājumi nelikumīgi iegūt vērtīgu informāciju neatkarīgi no tās pārraides līdzekļiem. Sākotnēji nelikumīga pieslēgšanās un slepena sarunu noklausīšanās tika veikta, fiziski pieslēdzoties telefona līnijai, bet tagad, izmantojot jaunās tehnoloģijas, šo noklausīšanās/pārtveršanas procesu var veikt no attāluma, pārtverot elektromagnētiskos viļņus.

! *Kāds autovadītājs piebrauc pie sava biroja, ar centrālo atslēgu aizslēdz savu automašīnu un nospiež signalizācijas pulti. Pretējā ielas pusē stāv automašīna, kurā sēž cilvēks ar klēpja datoru un mazu kompaktu ierīci. Ar šīs ierīces palīdzību viņš uztver automašīnas datorsistēmas pārraidīto signālu uz signalizācijas pulti un ar speciālas datorprogrammas palīdzību signāls tiek atkodēts. Rezultātā automašīna tiek nozagta. Šī operācija no signalizācijas ieslēgšanas līdz automašīnas nozagšanai ilgst tikai dažas minūtes.*

11.5.2. ATBILDĪBA PAR KORESPONDENCES PRIVĀTUMA PĀRKĀPUMIEM

Atbildība un pamatnostādnes nelikumīgas informācijas pārtveršanas jautājumā ir noteiktas Kibernoziegumu konvencijas 3. pantā. Tas nosaka, ka „dalībvalstīm ir jāparedz tādi tiesiski un citi pasākumi, kas nepieciešami, lai nacionālo valstu krimināllikumos paredzētu atbildību par nelikumīgu pārtveršanu, ja tā izdarīta tīši privāto datordatu pārraides laikā uz datorsistēmu, no tās vai tās iekšienē, izmantojot tehniskos līdzekļus, arī elektromagnētiskos izstarojumus no datorsistēmas, kas satur šādus datus". Dalībvalstis var paredzēt papildu nosacījumus, piemēram, "negodīgā nolūkā", vai arī attiecināt atbildību tikai uz tīklā savienotām, nevis patstāvīgām datorsistēmām.

Izstrādājot šā panta redakciju, eksperti vienojās par vairākiem kopīgiem nosacījumiem, kas varētu palīdzēt potenciālajām Konvencijas dalībvalstīm sakārtot savu kriminālo likumdošanu atbilstīgi Konvencijas prasībām. Pants paredz, ka šāda veida noziegums attiecas ne tikai uz tradicionālo telefona sarunu noklausīšanos un ierakstīšanu, bet uz visiem datu pārraides veidiem, arī uz telefona, faksimila, e-pasta un datņu pārsūtīšanas procesu.

Konvencija paredz atbildību par nelikumīgu pārtveršanu, ja tā izdarīta, izmantojot tehniskas ierīces. Līdz ar to Konvencija norobežojas no gadījumiem,

kad persona ir ieguvusi informāciju tieši no datorsistēmas, tas ir, lietojot datoru, jo to nevar atzīt par noklausīšanos vai pārtveršanu. Konvencijas izpratnē par noziegumu tiek uzskatītas tādas darbības kā komunikāciju satura noklausīšanās, pārraudzīšana un ierakstīšana, vai nu tieši piekļūstot un izmantojot datorsistēmu, vai arī netieši izmantojot speciālas elektroniskas pieslēgšanās un ierakstīšanas ierīces.

Konvencija atzīst par nelikumīgu un paredz atbildību par privātās (nevis publiskās) komunikācijas noklausīšanos, arī darbinieku personiskās sarunas darbavietā.

! *Halfordas kundze strādāja Lielbritānijā par Meiseidas galvenā policista palīdzi. Kaut viņa bija nostrādājusi policijā 20 gadu, tomēr nevarēja panākt paaugstinājumu. Tāpēc 1990. gadā viņa iesniedza augstāka līmeņa policijas iestādē sūdzību par dzimuma diskrimināciju. Tika nodibināta speciāla komisija, kas vadītu izmeklēšanu šajā lietā. Meiseidas policijas amatpersonas uzsāka Halfordas kundzes telefona sarunu noklausīšanos un ierosināja disciplinārlietu pret viņu. Tās dēļ 1990. gada 12. decembrī kundzi atlaida no darba, saglabājot pilnu darba algu. Halfordas kundze šo lēmumu pārsūdzēja un norādīja, ka pirms galvenā tribunāla sēdes darbavietā regulāri notiek viņas telefona sarunu noklausīšanās, jo viņa darba telefonu izmantoja privātajām un darba sarunām. Policijas iecirknī nebija izstrādāti telefona iekšējie lietošanas noteikumi un darbinieki nebija brīdināti par iespējamu sarunu pārtveršanu. Policija aizbildinājās ar to, ka sūdzētāja bieži lietojusi darba telefonu personiskām sarunām ar piederīgajiem savā dzīvesvietā, kuru telefons bija saistīts ar publisko telekomunikācijas tīklu, tātad izmantojusi publisko sakaru pārraides tīklu, un tāpēc policijas rīcība nav uzskatāma par noklausīšanos. Eiropas Cilvēktiesību tiesa, izskatot šo sūdzību, atzina, ka telefona sarunas, ko veikusi sūdzētāja no sava darba telefona, ietilpst privātās dzīves un korespondences jēdzienā un tāpēc pret Halfordas kundzi ir pieļauts Eiropas Cilvēktiesību Konvencijas (ECK) 13. panta tiesībaizskārums. Tiesa vienbalsīgi atzina, ka ECK Konvencijas 8. pantā noteiktā aizsardzība attiecas gan uz darba, gan personiskajām sarunām.*

Tas ir ļoti svarīgs secinājums, jo arī Latvijā ir bijuši gadījumi, kad administrācija iepazīstas ar darbinieka personisko e-pasta saraksti viņa darba datorā, motivēdama savu darbību ar to, ka šī sarakste ietver darbavietu kompromitējošu informāciju. Cietušie nav sūdzējušies, un šī problēma noklususi, bet patiesībā tas ir ECK 8. panta pārkāpums. Tāpēc, lai izvairītos no līdzīgām problēmām, Kibernoziegumu konvencijā dalībvalstīm ieteikts izstrādāt tiesisku pamatu darbinieku korespondences pārtveršanai, tas ir, noteikt precīzi likumā gadījumus, kad šāda darbinieku "privātā saruna" un "korespondence" ir pārtverama.

Latvijā šī problēma patlaban ir daļēji atrisināta, pieņemot 2000. gada 21. martā MK Noteikumus Nr. 106 "Informācijas sistēmu drošības noteikumi". Patlaban tie gan ir zaudējuši spēku un tiek pārstrādāti. Jebkurā gadījumā problēma ir atrisināta tikai daļēji, jo šādas administrācijas tiesības izdarīt darbinieku personiskās korespondences likumīgu pārraudzību ar likumu nav noteiktas, un šādu tiesību nenosaka arī iepriekš minētie noteikumi. Informācijas

sistēmu drošības noteikumi nosaka pamatprincipus, kādi IS organizācijām jāievēro, izstrādājot iekšējos informāciju sistēmu drošības noteikumus, bet nenosaka saistošas prasības darbiniekiem.

Kā jau minēts iepriekš, tad, lai personu sauktu pie atbildības par nelikumīgu pārtveršanu, šai darbībai ir jābūt nelikumīgai un tīšai. Te atkal no jauna saskaramies ar pretrunām nelikumīgo darbību novērtējumā. Darbība ir attaisnojama tad, ja personai ir tiesības to darīt, piemēram, ja persona paraksta pilnvarojuma līgumu vai ir pārraides dalībnieks, vai likumīgi veic uzraudzību par nacionālo drošības interešu ievērošanu vai arī valsts amatpersona veic likumā paredzētas darbības noziegumu atklāšanai. Par nelikumīgām darbībām nevar atzīt arī vispārēju komerciālu praksi, piemēram, sīkdatnes (*cookies*) izmantošanu komerciālos nolūkos, izņemot gadījumus, ja šī programma tiek izmantota speciāli nepilnvarotai piekļūšanai.

Pārtveršanas metodes ir dažādas.

- Vissenākā pārtveršanas metode, kas tradicionāli tiek lietota fiksētajos telefona tīklos, ir noklausīšanās.
- Atrašanās vietas noteikšana ar noklausīšanās ierīci, kas tiek izmantota, lai noskaidrotu, kur indivīds atrodas.
- Spiegošana ietver pārraudzīšanu *(monitoring)*, ierakstīšanu un elektromagnētiskās emisijas izmantošanu.
- Datorsistēmu elektromagnētiskā starojuma skenēšana.

Atbildību par šāda veida pārkāpumiem Latvijā nosaka KL 144. pants "Korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšana". KL īpaši atzīst par nelikumīgu elektronisko datu apstrādi, kas saistīta ar informācijas noslēpuma tīšu pārkāpšanu, nosakot sodu – "piespiedu darbs vai naudas sods līdz 5 minimālajām mēnešalgām. Par tām pašām darbībām, ja tās izdarītas mantkārīgā nolūkā, soda ar brīvības atņemšanu uz laiku līdz trīs gadiem vai ar arestu, vai ar piespiedu darbu, vai ar naudas sodu līdz sešdesmit minimālajām algām, atņemot tiesības uz zināmu nodarbošanos uz laiku līdz pieciem gadiem vai bez tā".

Kā redzams no KL 144. panta, tad tas pilnīgi atbilst Kibernoziegumu konvencijas projektā paustajām nostādnēm, proti, tā priekšmets ir jebkāda veida informācija, arī elektroniskie dati, kas tiek pārraidīti telekomunikāciju tīklos, datorsistēmās un datortīklos. Likumdevējs speciāli nav ierobežojis informācijas noslēpuma pārkāpšanas metodes, līdz ar to par tādām ir atzīstamas gan noklausīšanās, gan pārtveršana, gan uzraudzība u. c.

11.6. AR DATORIEM SAISTĪTI NOZIEDZĪGI NODARĪJUMI

Ar datoriem saistītiem noziedzīgiem nodarījumiem *(computer related crimes)* ir divi veidi – viltošana un krāpšana.

11.6.1. VILTOŠANA

ANO sagatavotajā dokumentā „Datornoziegumu rokasgrāmata" *(Computer Crime: The U.N. Manual adapted by Editor M.J. O'Brien) [49]* ar datoriem

saistīta viltošana definēta kā darbība, kurā „datu sagrozīšana ir saistīta ar datorizētā formā saglabātu dokumentu".

! *Kādas valsts pilsoņi, veikdami nelikumīgas darbības, bija uzkrājuši naudu Šveices bankā. Tā kā mītnes zemē šie pilsoņi tika vajāti, tad viņi nevarēja šo naudu izmantot. Lai varētu iegūt šo naudu, viņi nosprieda, ka vajadzētu iegūt kaut kādas iedomātas valsts personas dokumentu – pasi. Šādu informāciju viņi atrada internetā, kur viņiem par attiecīgu samaksu tika piedāvāts pakalpojums iegūt neesošas Āfrikas valsts pasi. Viņi nosūtīja uz konkrēto bankas kontu naudu un pēc kāda laika saņēma pasaulē neesošas valsts pases. Lai īstenotu savu nodomu, viņi aizbrauca uz kādu no Austrumeiropas valstīm un, uzrādīdami šīs pases, vairākās bankās atvēra kontus. Viņi bija pārliecināti, ka Austrumeiropas valstīs šī viltojuma piemērošana ir iespējama, jo šo valstu banku darbinieki vēl nepazīst pasaules valstu personības dokumentus. Bankas ierēdnis uz šī viltotā dokumenta pamata atvēra kontus, un viņam neradās šaubas par pasu autentiskumu. Uz šiem kontiem blēži pārskaitīja ievērojamas naudas summas. Tomēr brīdī, kad viņi mēģināja izņemt skaidrā naudā lielas naudas summas, policijas darbinieki viņus aizturēja.*

No šī piemēra redzams, ka viltojums ne vienmēr ir jāsaista ar kāda dokumenta oriģināla mainīšanu. Minētajā piemērā šāda oriģināla vispār nav.

Eiropas Parlamenta Rekomendācija 89(9) ietver norādi, ka par datorviltojumu nepieciešams paredzēt krimināltiesību tāpat kā par tradicionālā dokumenta viltojumu. Savukārt Kibernoziegumu konvencijas 7. pants „Ar datoru saistīta viltošana" nosaka, ka šai noziegumā ietilpst „tīšas, nelikumīgas darbības, kuras saistītas ar datordatu ievadīšanu, grozīšanu, dzēšanu vai apslāpēšanu, noklusēšanu un kuru dēļ tie kļūst neautentiski, ar nodomu, lai tie tiktu uzskatīti vai lietoti likumīgiem mērķiem kā autentiski neatkarīgi no tā, vai dati ir tieši lasāmi un saprotami". Tādējādi šis pants paredz atbildību ne tikai par acīm redzama un salasāma rakstiska dokumenta viltošanu, bet arī par datordatu viltošanu, kā arī tādām darbībām kā viltus datu ievadīšana datorsistēmā, datu pārveidošana, dzēšana vai noklusēšana jeb slēpšana.

Krimināllikuma 275. pants „Dokumenta, zīmoga un spiedoga viltošana un viltota dokumenta zīmoga un spiedoga realizēšana un izmantošana" paredz atbildību par dokumentu vai to atribūtu viltošanu. Ir skaidrs, ka dators var būt izmantots kā rīks viltošanai, kuras rezultātā tiek viltotas naudas zīmes vai dokumenta atribūti u. c. Savukārt jautājums par to, vai minēto KL pantu par viltošanu var piemērot datordatu viltošanas gadījumā, paliek atklāts. Speciālu atbildību par viltošanu, kas saistīta ar datoriem, KL neparedz.

11.6.2. KRĀPŠANA

Tradicionāli krāpšana ir tīša, apzināta, mērķtiecīga darbība, kas tiek veikta pret personu, lai ar viltu iegūtu sev vai citai personai zināmas tiesības, privilēģijas vai ekonomisku labumu. Krāpšanai ir vairākas specifiskas pazīmes, kas to nošķir no citiem noziedzīgu nodarījumu veidiem.

- Atšķirībā no zādzības un pārējiem mantas nolaupīšanas veidiem, kur nodarījuma priekšmets ir tikai manta, krāpšana var būt saistīta ne tikai ar nolūku iegūt kustamu vai nekustamu mantu, bet arī ar nolūku iegūt tiesības uz mantu vai jebkuru citu mantisku labumu.
- Reālajā pasaulē krāpšana ir saistīta ar tīšu psihisku iedarbību uz fizisku personu. Šī psihiskā vai psiholoģiskā iedarbība tiek veikta, vai nu izmantojot viltus ziņas, vai arī iegūstot cietušā uzticību.
- Šo noziedzīgo nodarījumu persona var izdarīt tikai mantkārīgu motīvu vadīta.

Kibernoziegumu konvencijas 8. pants paredz atbildību par datorkrāpšanu. Tā tiek saistīta ar „tīšām, nelikumīgām darbībām, kas var būt par iemeslu citas personas īpašuma zaudēšanai, ja darbības izdarītas

- ar jebkuru datordatu ievadīšanu, grozīšanu, dzēšanu, noklusēšanu,
- ar jebkuru datora vai sistēmas funkciju ietekmēšanu, kas izdarīta krāpnieciskā vai negodīgā nolūkā nelikumīgi iegūt sev vai citai personai ekonomisku labumu".

Šī panta mērķis ir paredzēt kriminālatbildību par jebkuru nelikumīgu datu apstrādes procesa manipulāciju, kas izdarīta ar nodomu nelikumīgi pārvietot īpašumu. Eksperti, izstrādājot šo normu, ir ņēmuši vērā pastāvošās realitātes, ko cilvēcei uzspiež straujā informācijas tehnoloģiju attīstība. Elektroniskās izsoles, elektroniskās biržas, elektroniskās bankas un veikali paver jaunas krāpnieciskas iespējas nelikumīgā vērtību iegūšanā. Eksperti uzskata, ka krāpnieciskās darbības datu apstrādes procesā ir kriminalizējamas tad, ja to galarezultātā ir radīts tiešs ekonomisks vai mantisks zaudējums citas personas īpašumam un ja tās izdarītas tīši ar nodomu iegūt nelikumīgu ekonomisku labumu sev vai citai personai.

Krimināllikuma 177. pants paredz atbildību par „svešas mantas vai tiesību uz šādu mantu iegūšanu, ļaunprātīgi izmantojot uzticēšanos vai ar viltu (krāpšana)". Pretstatā dažām krimināllikumos ierakstītām Rietumu tiesību doktrīnām, kur krāpšana ir kādas personas nelikumīga tīša darbība, kas vērsta pret citu personu, KL formulējumā šāds teksts nav iekļauts. Nav saprotams arī tas, kāpēc likumdevējs apdraudējuma objektu skaitā ir norādījis tikai mantu vai tiesību uz mantu un nav norādījis citas intereses.

No Eiropas un ASV krimināllikumu apskata ir redzams, ka neviens kodekss neparedz šauru apdraudējuma interesi. Patiesībā gandrīz visi Eiropas valstu krimināllikumi, arī tādi, kuros nav iestrādāta speciāla norma par datorkrāpšanu, paredz, ka krāpšana ir tāda darbība, ar kuru likumpārkāpējs, nodarīdams zaudējumus trešajai personai, viltus ceļā ir ieguvis nelikumīgu ekonomisku labumu, kas ir neapšaubāmi plašāks jēdziens nekā manta vai tiesības uz mantu.

11.6.3. KRĀPŠANA TELEKOMUNIKĀCIJAS JOMĀ

Krāpšana telekomunikācijas jomā ir atzīta par atsevišķu nozieguma veidu tikai Lielbritānijā un Austrālijā, kur ir pieņemti speciāli likumi, kuros par galvenajām telekomunikācijas krāpšanas metodēm atzītas dažāda veida nelikumīgas ielaušanās telekomunikācijas sistēmā, arī automātiskās telefona

centrālēs, ar nodomu iegūt bez samaksas telekomunikācijas pakalpojumus, kā arī ļaunprātīga telekaršu izmantošana, mobilo telefonu un radiotelefonu nelikumīga izmantošana, telebanku, teletirgvedības pakalpojumu izkrāpšana u. c. Krāpšana telekomunikācijas jomā Latvijā patlaban ir izvērsusies ļoti plaši, un tas ir iespējams tāpēc, ka spēkā esošās KL normas nav piemērojamas krāpšanai datorsistēmās.

! *Kādā pilsētā četri nepilngadīgie, pārgriezdami Lattelekom kabeli un lietojot speciāli pielāgotu telefona klausuli, pieslēdzās šim kabelim. Izmantojot dažādus kabeļa vadus, kas veido attiecīgo vadu pāri, viņi varēja uzdoties par konkrētas telefona līnijas reģistrētu lietotāju. Tādā veidā nepilngadīgie pusgadu regulāri zvanīja uz 909. sērijas numuriem, izmantoja "intīmpakalpojumus pa telefonu" un arī tālsarunas. Šo darbību dēļ daudziem rajona iedzīvotājiem tika sūtīti rēķini par nenotikušām sarunām. Abonentu iesniegto sūdzību dēļ Lattelekom drošības speciālisti veica attiecīgas pārbaudes un konstatēja, ka šī rajona centrā ir pārgriezts Lattelekom kabelis, kas nodrošina telefona sakarus lielai daļai rajona iedzīvotāju un ka noticis nelikumīgs pieslēgums. Lattelekom anulēja klientiem iepriekš piesūtītos rēķinus un uzņēmās segt šos zaudējumus. Kopīgais zaudējumu apmērs šajā gadījumā pārsniedza Ls 7000.*

Šis piemērs uzskatāmi liecina, ka ielaušanās telekomunikācijas sistēmā, lai nelikumīgi iegūtu tiesības bez maksas izmantot telekomunikācijas pakalpojumus, ir tīša darbība. Tā ir izdarīta ar mērķi iegūt sev vai citai personai mantisku labumu (šajā gadījumā mantiskais labums izpaužas nesamaksātā naudas summā, kas personai būtu jāsamaksā tad, ja tā šo pakalpojumu būtu izmantojusi likumīgi). Darbība ir nesaraujami saistīta ar mantisku zaudējumu nodarīšanu citai personai, šajā gadījumā *Lattelekom* vai citai fiziskai vai juridiskai personai, kuras rēķinam tiek pievienota samaksa par konkrēto pakalpojumu. Visā pasaulē, arī Latvijā, līdzīgi gadījumi nav retums un, ļaundariem izmantojot jaunākos IKT sasniegumus, kļūst aizvien izsmalcinātāki. Tāpēc kibernoziegumu eksperti komitejā vienprātīgi atzinuši, ka krāpšana telekomunikācijas jomā ir ar datoriem saistītas krāpšanas veids un to nav nepieciešams nodalīt kā atsevišķu nozieguma sastāvu, jo attiecīgās darbības pilnībā aptver Konvencijas 8. pants par datorsaistītu krāpšanu.

11.7. SATURSAISTĪTI NOZIEGUMI

Viena no izplatītākajām darbībām internetā ir informācijas izplatīšana, iegūšana, apmaiņa, un ir ļoti svarīgi katram zināt, kāda informācija ir likumīga un kāda ir nelikumīga, kāda informācija ir kaitīga un kāda nav.

11.7.1. NELIKUMĪGAS INFORMĀCIJAS RAKSTUROJUMS

Nelikumīga informācija ir tāda, kuras izplatīšanu aizliedz nacionālās vai starptautiskās tiesību normas. Nelikumīgas informācijas piemēri ir

1) terorisms – ir informācija par to, kā veikt teroristiskus aktus, sagatavot diversijas, veidot kaitējumu IT programmām utt.,

2) neķītru materiālu izplatīšana internetā. Šo informāciju Latvijā atzīst par nelikumīgu tad, ja tā tiek izplatīta publiski,
3) bērnu pornogrāfija – tas ir informācijas objekts, kura izplatīšanu nepieļauj neviena pasaules valsts, arī Latvija,
4) informācija, kas kurina rasu naidu un propagandē nacionālās nesaskaņas (rasisma propaganda, kreisais, labējais ekstrēmisms u. c.),
5) ikviens aicinājums izdarīt noziegumu.

11.7.2. KAITĪGAS INFORMĀCIJAS RAKSTUROJUMS

Par kaitīgo informāciju sauc dažāda veida informāciju, kas var apdraudēt citu personu vērtības un jūtas saistībā ar to politisko, reliģijas, dzimuma, tautības, seksuālo interešu un cita veida piederību. Tās apjomu nosaka katras nacionālās valsts tiesību akti un kultūras tradīcijas. Latvijā pie šādas informācijas var pieskaitīt

1) pornogrāfiska satura informācijas izplatīšanu nepilngadīgajiem,
2) pieaugušiem domātu informāciju, kas var ietekmēt nepilngadīgo izpratni par sabiedrības attīstības procesiem,
3) informāciju, kas propagandē brutalitāti, asiņainu vardarbību,
4) informāciju, kas var aizskart godu un cieņu, profesionālo reputāciju.

11.7.3. TIEŠSAISTES KONTROLES METODES

Informācijas kontrole ir sarežģīts uzdevums. Tā ir jāveic gan katram cilvēkam individuāli, gan valsts līmenī, lai informācija par pārkāpumiem kļūtu pieejama plašākam sabiedrības lokam. Jāsniedz arī atbalsts no likumdošanas puses. Informācijas kontrole ir jāuzņemas arī katram interneta pakalpojumu sniedzējam un informācijas sistēmu turētājam.

Pie kontroles funkcijām var pieskaitīt šādas darbības:

- nepiemēroto materiālu identifikācija un klasifikācija ar elektronisko programmu gidu palīdzību;
- lietotāju vecuma pārbaudes identifikatori (personas kodi, maksāšanas līdzekļi u. c.);
- sistemātiska materiālu filtrēšana pēc attēliem un atslēgvārdiem;
- navigācijas atmiņas uzglabāšana tīklā (saglabājas informācija, kura norāda, ko lietotājs darījis, kur ceļojis, ar ko sarakstījies u. c.);
- sākumlapu izlases bloķēšana (pēc noteiktām pazīmēm);
- elektronisko viedkaršu lietošana lietotāja darbību identifikācijai u. c.

11.7.4. BĒRNU PORNOGRĀFIJA

Bērnu pornogrāfijas izplatīšana ir kļuvusi par vienu no smagākajām XXI gadsimta problēmām. Par sevišķi bīstamu noziegumu tā izvērsusies tieši informācijas tehnoloģiju attīstības apstākļos, noziedzniekiem spējot izmantot jaunos sasniegumus savu noziedzīgo mērķu īstenošanai.

Kā jau iepriekš minēts, vairākas valstis ir pieņēmušas jaunas krimināllikuma normas, kas pastiprina atbildību par bērnu pornogrāfijas izplatīšanu,

paredz atbildību par ceļošanu internetā ar nolūku iegūt bērnu pornogrāfiju saturošu informāciju, kā arī atbildību par bērnu pornogrāfijas saturu, atzīstot virtuālos kustīgos tēlus par bērnu pornogrāfiju saturošu informāciju, kuras izgatavošana vai glabāšana ir krimināli sodāma, un veikušas citus pasākumus. Gan ANO, gan ES līmenī tiek izstrādāti vairāki pasākumu plāni un pieņemti svarīgi dokumenti, kas atvieglotu cīņu ar bērnu pornogrāfijas izplatīšanu. Tāpēc EP Kibernoziegumu komitejas eksperti jau sākotnēji paredzējuši iekļaut kibernoziegumu skaitā bērnu pornogrāfiju. EP iepriekš ir veikusi dalībvalstu aptauju, un uz iegūto galarezultātu pamata ir izstrādāta Konvencijas 9. panta redakcija.

11.7.5. ATBILDĪBA PAR BĒRNU PORNOGRĀFIJU

Kibernoziegumu konvencijas 9. pants paredz krimināatbildību par šādām tīšām nelikumīgām darbībām:

- bērnu pornogrāfijas izgatavošanu ar mērķi to izplatīt ar datorsistēmām;
- bērnu pornogrāfijas piedāvāšanu vai pārvēršanu par pieejamu ar datorsistēmām;
- bērnu pornogrāfijas izplatīšanu vai pārraidīšanu datorsistēmās;
- bērnu pornogrāfijas sagādāšanu ar datorsistēmas palīdzību sev vai citai personai;
- bērnu pornogrāfijas glabāšanu datorsistēmā vai datorsistēmas atmiņā.

Arī LR Krimināllikums paredz atbildību par bērnu pornogrāfiju. Tā ir iekļauta KL 166. pantā „Bērnu pornogrāfijas vai erotisku materiālu izgatavošana, publiska demonstrēšana, reklamēšana vai citāda izplatīšana".

Likums šobrīd paredz atbildību tikai par bērnu pornogrāfijas izgatavošanu, izplatīšanu un reklamēšanu. Šie nosacījumi ir ievērojami šaurāki, nekā to paredz Kibernoziegumu konvencija.

! *Teksasas pavalsts Karnes apgabala administrācija bija pārsteigta, kad saņēma no iedzīvotājiem sūdzības par to, ka, atverot iestādes mājaslapu, viņiem tiek piedāvāta pornogrāfija. Komentējot šo notikumu, speciālisti atzina, ka nav nekāds retums gadījumi, kad pornogrāfijas izplatītāji izmanto labi pazīstamu mājaslapu, arī oficiālu valsts institūciju lapu adreses, lai popularizētu savu produkciju. Šāda situācija bija radusies arī ar ASV Baltā nama mājaslapu, kuras adrese ir www.whitehouse.gov. Lai izmantotu lietotāju neuzmanību, pornogrāfiju saturoša mājaslapa tika piereģistrēta ar adresi, kas atšķīrās tikai ar to, ka .gov vietā bija .com.*

Ja jau ASV Baltais nams nav pasargāts no šādām kļūmēm, tad kāda ir garantija, ka ar speciāli izveidotas datorprogrammas palīdzību šāda kompromitējoša informācija netiek ievadīta datorsistēmā arī atsevišķām personām? Piemēram, šāda informācija apzināti, mērķtiecīgi tiek ievadīta kādam pazīstamam politiķim vai valsts amatpersonai piederošā vai lietojumā esošā datorsistēmā ar mērķi šantažēt vai diskreditēt šo personu. Tāpēc, pastiprinot cīņu ar bērnu pornogrāfiju, tomēr ir jāizstrādā arī garantiju un nosacījumu mehānisms, lai netiktu pārkāptas arī citas cilvēka tiesības.

11.8. NOZIEDZĪGI NODARĪJUMI INTELEKTUĀLĀ ĪPAŠUMA JOMĀ

Informācijas tehnoloģijas tiesībās intelektuālā īpašuma aizsardzībai ir īpaši liela nozīme. Uzsākot darbu pie Kibernoziegumu konvencijas projekta, eksperti vienojās, ka galvenā uzmanība ir jāvelta trīsdimensiju topogrāfijas, datorprogrammu, datu bāzu, mikroshēmu un citu ar datortehnoloģiju saistītu objektu aizsardzības jautājumiem. Informācijas tehnoloģijai attīstoties, ir iespējams ar datortīklu palīdzību pārraidīt gan skaņu, gan fotogrāfiju, gan videodatnes. Šī jauno tehnoloģiju augšupeja un popularitāte dod ne tikai iespēju plašam lokam legāli izmantot šos intelektuālā īpašuma objektus, bet arī pastiprina tās tendences, kas saistītas ar šādu darbu nelikumīgu izmantošanu.

Kaut arī pasaulē tiek veikti aizsardzības pasākumi, intelektuālā īpašuma nelikumīga izmantošana kļūst par vienu no svarīgākajām XXI gadsimta problēmām. Tāpēc arī EP Kibernoziegumu komitejas eksperti veltījuši lielas pūles, lai visām dalībvalstīm pieņemamā veidā iekļautu šo normu Konvencijas projektā.

11.8.1. ATBILDĪBA PAR PĀRKĀPUMIEM INTELEKTUĀLĀ ĪPAŠUMA JOMĀ

Kibernoziegumu konvencijas 10. pantā ir ietverta norma "Noziegumi, kas saistīti ar pārkāpumiem autortiesību un blakustiesību jomā". Šī norma paredz krimināatbildību par tīšiem autortiesību pārkāpumiem, ja tie izdarīti ar datorsistēmu līdzekļiem komerciālos nolūkos. Galvenais šā panta uzdevums ir noteikt starptautiskās atbildības režīmu tiem autortiesību un blakustiesību pārkāpumiem, kas izdarīti, izmantojot datorsistēmu resursus, arī autortiesību un blakustiesību aizsardzību internetā. Minētā panta teksts nav ierobežots ar konkrētu autortiesību vai blakustiesību objektu loku. Šo objektu lokā var ietvert jebkuru autora darbu, ja tā tiesības aizsargā konvencijā uzskaitītie starptautiskie tiesību akti vai nacionālo tiesību normas.

Pēc ilgām diskusijām eksperti ir vienojušies, ka par autortiesību un blakustiesību pārkāpumu šīs konvencijas izpratnē ir uzskatāma komerciāla rakstura darbība, speciāli tekstā iestarpinot vārdus „vismaz komerciālos nolūkos". Tomēr tas neliedz dalībvalstīm paplašināti tulkot terminu "komerciāli nolūki" un paredzēt krimināatbildību arī par citiem pārkāpumiem bez šāda nolūka.

LR Autortiesību likums noteic, ka par autortiesību un blakustiesību pārkāpumu uzskatāma darbība, ar kuru aizskartas autortiesību vai blakustiesību subjekta personiskās vai mantiskās tiesības, arī aizsargājamo objektu fiksācija, to publicēšana, publiskošana, reproducēšana, izplatīšana jebkurā veidā bez tiesību subjekta piekrišanas.

Latvijā krimināatbildība par intelektuālā īpašuma tiesību pārkāpumiem ir iekļauta četros Krimināllikuma pantos.

- **KL 147. pantā** "Izgudrojuma tiesību pārkāpšana" paredzēta šāda atbildība: (1) par izgudrojuma tīšu izpaušanu bez izgudrojuma tiesību īpašnieka

piekrišanas pirms izgudrojuma pieteikuma, kā arī par izgudrojuma autorības piesavināšanos vai līdzautorības uzspiešanu – soda ar
- brīvības atņemšanu uz laiku līdz 3 gadiem
- vai arestu,
- vai naudas sodu līdz 50 minimālajām mēnešalgām;

(2) par piespiešanu ar vardarbību vai tās draudiem vai ar šantāžu atteikties no izgudrojuma vai par tā līdzautorības uzspiešanu – soda ar
- brīvības atņemšanu uz laiku līdz 5 gadiem
- vai arestu,
- vai naudas sodu līdz 100 minimālajām mēnešalgām.

- **KL 148. pantā** "Autortiesību un blakustiesību pārkāpšana" paredzēta šāda atbildība:

(1) par autortiesību vai blakustiesību tīšu pārkāpšanu, ja tā izdarīta, pārkāpjot autoru tiesības uz darba publicēšanu vai izziņošanu un izmantošanu, kā arī pārkāpjot blakustiesību īpašnieku tiesības, – soda ar
- piespiedu darbu
- vai naudas sodu līdz 60 minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas;

(2) par tādām pašām darbībām, ja tās izdarītas atkārtoti vai ja tās izdarījusi personu grupa pēc iepriekšējas vienošanās, – soda ar
- brīvības atņemšanu uz laiku līdz 3 gadiem
- vai arestu,
- vai naudas sodu līdz 100 minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas;

(3) par autortiesību piesavināšanos, piespiešanu ar vardarbību vai tās draudiem vai ar šantāžu atteikties no autorības vai par līdzautorības uzspiešanu – soda ar
- brīvības atņemšanu uz laiku līdz 5 gadiem,
- vai naudas sodu līdz 160 minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas.

- **KL 149. pantā** "Nelikumīgas darbības ar autortiesību un blakustiesību objektiem" paredzēta šāda atbildība:

(1) par autortiesību vai blakustiesību objektu nelikumīgu realizāciju, kā arī citādu materiāla labuma gūšanu, izmantojot šos objektus, kuri publicēti, izziņoti, izpildīti publiski vai kā citādi izmantoti, pārkāpjot autortiesības vai blakustiesības, – soda ar
- brīvības atņemšanu uz laiku līdz 2 gadiem
- vai arestu,
- vai naudas sodu līdz 80 minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas;

(2) par tādām pašām darbībām, ja tās izdarītas atkārtoti vai ja tās izdarījusi personu grupa pēc iepriekšējas vienošanās, vai ja tās izdarītas lielā apmērā, – soda ar
- brīvības atņemšanu uz laiku līdz 5 gadiem
- vai arestu,
- vai naudas sodu līdz 150 minimālajām mēnešalgām, konfiscējot mantu;

(3) par šā panta pirmajā daļā norādīto objektu iegūšanu realizācijai, uzglabāšanu vai slēpšanu – soda ar
   - piespiedu darbu
   - vai naudas sodu līdz 40 minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas.

Apdraudētā interese šajā pantā ir autoru, izpildītāju, producentu, raidorganizāciju nemantiskās tiesības, kas saistītas gan ar darba izmantošanas kārtību, vārdu, izpildījuma kvalitāti, gan mantiskās tiesības, kas saistītas ar tiesībām uz atlīdzību. Šo noziedzīgo nodarījumu visā pasaulē sauc par d a t o r p i r ā t i s m u . Speciālisti datorpirātismu iedala vieglajā un smagajā datorpirātismā. Tas izriet no tā, vai persona, kas tīši pārkāpj autortiesības, šo darbību saista ar peļņu vai tas ir bezpeļņas pasākums. Pat Eiropā joprojām nav skaidra un vienota attieksme pret datorpirātismu. Tā, piemēram, Dānijā valdība plāno legalizēt mūzikas ielādēšanu datoros no interneta. To, kā zināms, *Napster* lietā aizliedza ASV tiesa.

- Arī **KL 206. pantā** "Preču zīmes un citas atšķirības zīmes neatļauta izmantošana vai viltošana" ir paredzēta noteikta krimināltatbildība par intelektuālā īpašuma tiesību pārkāpumiem.

Kaut gan ekspertu vidū notikušas nopietnas diskusijas par nepieciešamību iekļaut kibernoziegumu skaitā plašāku intelektuālā īpašuma objektu loku, piemēram, tādu pārkāpuma veidu kā *cybersquatting* (pārkāpumi, kas saistīti ar domēna vārdu piesavināšanos), tomēr Konvencijas projektā nav īpaši izdalīti jautājumi par patenta, preču zīmes, domēna vārda, ģeogrāfisko norāžu un citu intelektuālā īpašuma objektu tiesisko aizsardzību, jo, kā jau minēts iepriekš, šie jautājumi ir Pasaules Intelektuālā īpašuma organizācijas kompetence.

Svarīgi atzīmēt apstākļus, kuri padara autortiesību un patentu tiesību pārkāpumus smagākus, – to atkārtotu veikšanu, kā arī vardarbību un citu personu piespiešanu pārkāpumu nodarīšanā. Sodi, ko var piespriest par autortiesību pārkāpumiem, protams, var šķist nesamērīgi lieli – vislielākais sods, ko var piespriest, ir 5 gadu cietumsods, – taču intelektuālā īpašuma pārkāpumi var radīt ārkārtīgi lielus zaudējumus. Izmantojot jaunas tehnoloģijas, nelikumīgo intelektuālā īpašuma objektu izplatīšana ir kļuvusi vieglāka nekā ierastā tirdzniecība. Savukārt atlīdzība par šāda veida piedāvājumiem ir nesamērīgi maza salīdzinājumā ar licencētām produktu versijām. Šie faktori palielina nelicencētas programmatūras, videodarbu, mūzikas darbu u. c. popularitāti intelektuālā īpašuma tirgū.

11.9. KONTROLJAUTĀJUMI

1. Nosauciet kibernoziegumu veidus!
2. Kādā veidā tiek tiesiski regulēti kibernoziegumi Eiropas Savienībā?
3. Kādas informācijas izplatīšana internetā ir aizliegta?
4. Kādu kibernoziegumu apkarošana, jūsuprāt, ir aktuāla Latvijā?

12. DARBA TIESĪBAS, DARBA DROŠĪBA UN ERGONOMIKA

Nodaļa izstrādāta, izmantojot [50].

12.1. DARBA TIESĪBAS

Darba tiesību zināšanas dod iespēju jauniem cilvēkiem adekvāti novērtēt piedāvājamo darbu, kā arī aizstāvēt savas tiesības darba devēju priekšā, ja tas ir nepieciešams. Nereti jauni cilvēki tiek izmantoti ne tikai kā lēts darbaspēks, bet arī kā nepretenciozi darbinieki, kuri neprotestē un neuzstāj uz darbavietas izvēli. Darba tiesību normu nezināšanas dēļ cilvēks kļūst neaizsargāts.

Šajā nodaļā ir izklāstīti darba tiesību punkti, ar kuriem visbiežāk jāsaskaras ikdienas dzīvē un kuru zināšana ir ļoti svarīga.

12.1.1. DARBA TIESĪBU REGULĒŠANA

Darba tiesības Latvijā ir regulētas ar vairāku normatīvo aktu palīdzību. Tie ir Darba likums un Darba aizsardzības likums, kā arī vairāki citi normatīvie akti, kuri ietver specifisku darbu regulēšanas nosacījumus:

- Bezdarbnieku un darba meklētāju atbalsta likums,
- Darba devēju organizāciju un to apvienību likums,
- Par darba aizsardzību,
- Par apdrošināšanu bezdarba gadījumam,
- Par darbinieku aizsardzību darba devēju maksātnespējas gadījumā,
- Par nodarbinātību,
- Valsts darba inspekcijas likums,
- Streiku likums
- u. c.

Darba likums noteic, ka darba tiesiskās attiecības regulē Latvijas Republikas Satversme, Latvijai saistošās starptautisko tiesību normas, Darba likums un citi normatīvie akti, kā arī darba koplīgums un darba kārtības noteikumi.

12.1.2. DARBA INTERVIJA

Gandrīz jebkuram darbiniekam pirms stāšanās darbā tiek speciāli organizēta darba intervija. Darba intervija ir darba devēja sagatavota mutvārdu vai rakstveida aptauja pretendenta piemērotības novērtēšanai. Jebkuram ir jāzina, ka darba intervijā nav pieļaujami tādi darba devēja jautājumi, kas neattiecas uz paredzētā darba veikšanu vai nav saistīti ar pretendenta piemērotību šim darbam, kā arī jautājumi, kas ir tieši vai netieši diskriminējoši, it īpaši jautājumi par

- grūtniecību, izņemot gadījumu, kad paredzēto darbu vai nodarbošanos nevar veikt grūtniecības laikā,
- ģimenes vai laulības stāvokli,

- iepriekšēju sodāmību, izņemot gadījumu, kad tai attiecībā uz veicamo darbu varētu būt būtiska nozīme,
- reliģisko pārliecību vai piederību pie kādas reliģiskās konfesijas,
- piederību pie kādas politiskās partijas, darbinieku arodbiedrības vai citas sabiedriskas organizācijas,
- nacionālo vai etnisko izcelsmi.

Pretendentam ir ne tikai tiesības, bet arī pienākumi
- sniegt patiesu informāciju,
- informēt darba devēju par savu veselības stāvokli un savu profesionālo sagatavotību, ciktāl tam ir būtiska nozīme darba līguma slēgšanā un paredzētā darba veikšanā.

Darba devējs var pieprasīt, lai pretendents veic veselības pārbaudi, kas ļautu pārliecināties par viņa piemērotību paredzētā darba veikšanai.

12.1.3. DARBA LĪGUMS

Stājoties darba attiecībās, tām ir jābūt noformētām darba līgumā. Ja darbiniekam nepiedāvā parakstīt darba līgumu, pušu atbildība, pienākumi un tiesības netiek reglamentētas un tas strīdu gadījumā var radīt sarežģījumus abām pusēm.

Darba līgums ir rakstveida vienošanās starp darba devēju un darbinieku. Saskaņā ar to darbinieks apņemas veikt noteiktu darbu, pakļaujoties iekšējai darba kārtībai vai darba devēja rīkojumiem, bet darba devējs apņemas nodrošināt darba samaksu un darba apstākļus, kas paredzēti likumdošanas aktos, darba koplīgumā un noteikti, pusēm vienojoties.

Darba līgumā norāda
- darbinieka vārdu, uzvārdu, personas kodu, dzīvesvietu, darba devēja vārdu, uzvārdu (nosaukumu), reģistrācijas numuru un adresi,
- darba tiesisko attiecību sākuma datumu,
- darba tiesisko attiecību paredzamo ilgumu (ja darba līgums noslēgts uz noteiktu laiku),
- darba vietu (ja darba pienākumu veikšana nav paredzēta kādā noteiktā darba vietā, to, ka darbinieku var nodarbināt dažādās vietās),
- darbinieka profesiju (arodu, amatu) un vispārīgu nolīgtā darba raksturojumu,
- darba samaksas apmēru un izmaksas laiku,
- nolīgto dienas vai nedēļas darba laiku,
- ikgadējā apmaksātā atvaļinājuma ilgumu,
- darba līguma uzteikuma termiņu,
- atsauci uz darba koplīgumu, darba kārtības noteikumiem, kas piemērojami darba tiesiskajām attiecībām.

Līgumā mēdz atrunāt, vai darbinieks var stāties darba attiecībās ar citiem darba devējiem. Darba likums nosaka, ka " Darbiniekam ir tiesības slēgt darba līgumu ar vairākiem darba devējiem, ja darba līgumā vai darba koplīgumā nav noteikts citādi". Tas nozīmē, ka līgums var arī aizliegt pildīt vairākus darba līgumus.

Darba līgums var būt noslēgts
- uz noteiktu laiku (darba līgums ar beigu termiņu),
- uz nenoteiktu laiku,
- uz noteikta darba izpildīšanas laiku jeb "gabaldarbu" (darba līguma pamatā ir noteikts darbs, pēc kura izpildīšanas līgums tiek izbeigts).

Darba līgumu sastāda 2 eksemplāros, no kuriem viens glabājas pie darba devēja, otrs – pie darbinieka.

Darba līgums paredz arī dažus ierobežojumus attiecībā uz valsts un pašvaldību institūcijām – vienā valsts vai pašvaldību uzņēmumā, iestādē vai organizācijā nedrīkst strādāt kopā radinieki, ja viņi ir pakļauti viens otram vai tieši kontrolē viens otru. Darba kodeksā par radiniekiem ir uzskatītas personas, kas savā starpā ir tuvi radinieki vai arī laulātā radinieki (vecāki, laulātais, brāļi, māsas, dēli, meitas, kā arī laulātā brāļi, māsas, vecāki un bērni). Šī noteikuma izņēmumus var noteikt Ministru kabinets.

Viens no svarīgiem darba aspektiem ir darbinieka tiesības nepildīt darbus, kas nav paredzēti darba līgumā. Darba devējam nav tiesību prasīt, lai darbinieks izpildītu darba līgumā neparedzētu darbu.

Darba līguma izbeigšanas pamats var būt
- pušu vienošanās,
- termiņa izbeigšanās, izņemot gadījumus, kad darba attiecības faktiski turpinās un neviena puse nav pieprasījusi tās izbeigt,
- darbinieka iesaukšana obligātajā valsts dienestā, iekšlietu iestāžu dienestā, Nacionālajos bruņotajos spēkos vai iestāšanās civildienestā,
- darba līguma laušana pēc darbinieka uzteikuma, pēc darba devēja iniciatīvas vai pēc tādu institūciju pieprasījuma, kuras nav darba līguma puses,
- darbinieka pārcelšana uz citu uzņēmumu, iestādi vai organizāciju ar viņa piekrišanu vai pāriešana vēlētā amatā,
- darbinieka atteikšanās no pārcelšanas citā darbā uz citu apvidu kopā ar darba devēju, atteikšanās turpināt darbu sakarā ar būtiskiem līguma nosacījumu grozījumiem vai neievēlēšana amatā uz jaunu termiņu,
- spēkā stājies tiesas spriedums, ar kuru darbinieks notiesāts ar brīvības atņemšanu vai citu sodu, kas izslēdz iespēju turpināt attiecīgo darbu,
- LR likumu pārkāpumi, noslēdzot darba līgumu, vai darba līguma neatbilstība likumu prasībām,
- darbinieka nāve.

Darbinieks ir tiesīgs lauzt darba līgumu, vienu mēnesi iepriekš rakstveidā brīdinot par to darba devēju.

12.1.4. DARBA LAIKS

Darba laiks var būt
- normālais darba laiks – tas nedrīkst pārsniegt 40 stundas nedēļā,
- nepilns darba laiks – īsāks par normālo dienas vai nedēļas darba laiku,
- darbiniekiem, kuri strādā kaitīgos vai smagos darba apstākļos, – ne vairāk par 35 stundām nedēļā,
- sievietēm, kurām ir bērni līdz 3 gadu vecumam, – 35 stundas nedēļā.

Darba nedēļa var sastāvēt no 5 vai 6 darba dienām, taču kopējais nostrādātais laiks nedrīkst pārsniegt normālo nedēļas darba laiku.

Pirms svētku dienas darbadienu saīsina par vienu stundu, ja darba līgumā nav iekļauta vienošanās par īsāku darbadienu.

Darbinieks var būt pieņemts arī uz nepilnu darba laiku, tā saucamo pusslodzi vai citu slodzes dalījumu. Šajā gadījumā alga ir aprēķināma proporcionāli nostrādātajam laikam vai arī ir atkarīga no darba rezultātiem, bet tas nevar būt pamats darba tiesību ierobežojumam – ikgadējā atvaļinājuma ilguma saīsināšanai, darba stāža aprēķināšanai u. tml.

Darbadienas grafiku nosaka iekšējie uzņēmuma darba kārtības noteikumi.

12.1.5. VIRSSTUNDAS

Virsstundu darbs ir darbs, ko veic virs noteiktā darba laika. Tas ir pieļaujams tikai tad, ja ir darbinieka rakstveida piekrišana darba devēja rīkojumam. Piespiest strādāt virsstundas nedrīkst. Izņēmuma gadījumi, kad atļauts virsstundu darbs, no LR Darba likuma ir izslēgti. Virsstundu darba ilgums katram darbiniekam nedrīkst pārsniegt 4 stundas 2 dienās pēc kārtas un 120 stundas gadā. Darba devējam ir pienākums precīzi uzskaitīt katra darbinieka nostrādātās virsstundas.

12.1.6. ATPŪTAS LAIKS

Darbiniekam atpūtai un ēšanai dod pārtraukumu. Tas nav ilgāks par 2 stundām, un to neieskaita darba laikā. Pārtraukumu laika grafiku nosaka iekšējie noteikumi. Šajā laikā darbiniekam ir tiesības atstāt darba vietu. Ja darba pārtraukumus ražošanas apstākļu dēļ noteikt nevar, darbiniekam ir jādod iespēja ēst darba laikā.

12.1.7. BRĪVDIENAS

Darba likums nosaka, ka uzņēmumos ar 5 darba dienu nedēļu ir 2 brīvdienas, savukārt uzņēmumos, kuros darba nedēļu veido 6 darbadienas, – 1 brīvdiena.

Darbinieku piesaistīt darbam brīvdienās drīkst ar arodorganizācijas atļauju vai izņēmuma gadījumos:

- lai novērstu vai likvidētu dabas katastrofas, avārijas ražošanā vai lai nekavējoties likvidētu to sekas;
- lai novērstu nelaimes gadījumus, mantas bojājumus vai bojāeju;
- lai veiktu neatliekamus, iepriekš neparedzētus darbus, no kuru steidzamas izpildes turpmāk atkarīgs visa uzņēmuma, iestādes vai organizācijas vai arī atsevišķu to apakšvienību normāls darbs;
- lai veiktu neatliekamus iekraušanas un izkraušanas darbus, kā arī ar tiem saistītus transporta darbus, tādējādi novēršot vai likvidējot transporta līdzekļu dīkstāvi un kravas uzkrāšanos nosūtīšanas punktos un galapunktos.

Atsevišķus darbiniekus brīvdienās darbā iesaista ar darba devēja rakstisku rīkojumu. Darbu brīvdienā var kompensēt, pēc pušu vienošanās piešķirot vienu atpūtas dienu vai samaksājot divkāršā apmērā.

12.1.8. ATVAĻINĀJUMS

Ikgadējo atvaļinājumu piešķir katru gadu un to grafiku nosaka darba devējs. Darba likums aizliedz atvaļinājumu kompensēt naudā, izņemot gadījumus, kad darbinieks tiek atlaists. Darbiniekam pienākas ne mazāk kā 4 kalendāra nedēļu atvaļinājums, neieskaitot svētku dienas.

Jauni darbinieki var pieprasīt atvaļinājumu ne agrāk kā pēc 6 mēnešu nostrādāšanas ar šādiem izņēmumiem:

- sievietēm pirms grūtniecības un dzemdību atvaļinājuma vai tieši pēc tā,
- sievietēm, kurām ir bērni līdz 12 gadu vecumam,
- darbiniekiem, kuri jaunāki par 18 gadiem,
- personām, kas ir nepamatoti politiski represētas,
- un citos likumā paredzētajos gadījumos.

Ikgadējie papildatvaļinājumi jāpiešķir

- darbiniekiem, kuri strādā kaitīgos vai smagos darba apstākļos, – saskaņā ar likumdošanu un darba koplīgumiem,
- sievietēm, kurām ir trīs vai vairāk nekā trīs bērni vecumā līdz sešpadsmit gadiem vai bērns invalīds, – trīs darbadienas.

Ikgadējos papildatvaļinājumus var piešķirt darbiniekiem, kuri ilgstoši strādā pie darba devēja, darbiniekiem ar nenormētu darbadienu, darbiniekiem, kuri strādā nakts laikā, maiņās, kā arī citos gadījumos. Šo papildatvaļinājumu ilgumu un piešķiršanas kārtību nosaka darba koplīgums.

12.1.9. ATVIEGLOJUMI DARBINIEKIEM, KAS DARBU SAVIENO AR MĀCĪBĀM

Darba likums paredz īpašus atvieglojumus darbiniekiem, kas darbu savieno ar mācībām. Darba devēja pienākums ir radīt nepieciešamos apstākļus, kas jāparedz darba koplīgumā, lai darbinieki, kas, nepārtraucot darbu, iesaistījušies arodapmācībā vai mācās mācību iestādēs, varētu savienot darbu ar mācībām.

Teorētiskās nodarbības un praktisko apmācību, ja sagatavo darbiniekus tieši ražošanā, organizē darba laikā vai ārpus darba laika saskaņā ar likumdošanas aktiem, darba koplīgumu vai darba līguma pušu vienošanos.

Darba likuma izņēmumi, kas saistīti ar studijām, profesionālo un vispārizglītojošo skolu apmeklēšanu ir šādi:

- darba devēji *var* piešķirt mācību atvaļinājumu ar darba algas saglabāšanu vai bez tās darbiniekiem, kas, nepārtraucot darbu, sekmīgi mācās;
- valsts eksāmenu kārtošanai vai diplomdarba sagatavošanai un aizstāvēšanai jāpiešķir mācību atvaļinājums – ne mazāks par 20 kalendāra dienām, saglabājot valsts noteikto minimālo darba samaksu.

12.1.10. SIEVIEŠU DARBS

Aizliegts sievietes nodarbināt smagos darbos un darbos ar kaitīgiem darba apstākļiem. Sarakstus par smagiem darbiem un darbiem ar kaitīgiem darba apstākļiem, kuros aizliegts nodarbināt sievietes, apstiprina Latvijas Republikas Ministru kabinets, saskaņojot tos ar darbinieku arodorganizācijām.

Aizliegts likt sievietēm pārnēsāt un pārvietot smagumus, kas pārsniedz likumdošanas aktos viņām noteiktās maksimālās normas.

Sieviešu iesaistīšana nakts darbā nav atļauta, izņemot darbu veidus, kur tas ir sevišķi nepieciešams, piemēram, slimnīcā.

LR Darba likums neatļauj iesaistīt nakts darbā, virsstundu darbā, darbā brīvdienās, svētku dienās un sūtīt komandējumos grūtnieces, kā arī sievietes, kurām ir bērns līdz triju gadu vecumam.

Sievietes, kurām ir bērns līdz 14 gadu vecumam (bērns invalīds līdz 16 gadu vecumam), nedrīkst iesaistīt virsstundu darbā vai sūtīt komandējumā bez viņu piekrišanas. Grūtnieces un sievietes, kurām ir bērns līdz 14 gadu vecumam (bērns invalīds līdz 16 gadu vecumam), nedrīkst iesaistīt dežūrās pēc darbadienas beigām, naktī, brīvdienās un svētku dienās.

Grūtniecēm saskaņā ar medicīnisko atzinumu samazina darba normas vai pārceļ viņas citā, vieglākā un nelabvēlīgu faktoru ietekmi izslēdzošā darbā, saglabājot agrākā darba vidējo izpeļņu. Sievietes, kurām ir bērns līdz 3 gadu vecumam, ja viņas nespēj veikt līdzšinējo darbu, pārceļ citā darbā, saglabājot agrākā darba vidējo izpeļņu, līdz bērns sasniedz 3 gadu vecumu.

Sievietēm, kurām ir bērns līdz 3 gadu vecumam un kuras ik dienas strādā saīsinātu darba laiku, darba algu izmaksā tādā pašā apmērā kā attiecīgo kategoriju darbiniekiem, kuri ik dienas strādā normālu darba laiku. Darbiniecēm, kam ir bērni līdz 3 gadu vecumam un kas strādā gabaldarbu, par darbu samaksā pēc gabaldarba izcenojumiem tāpat kā pārējiem darbiniekiem ar piemaksu pēc tarifa likmes par to laiku, par kādu viņu darba laiks ik dienas ir īsāks nekā pārējo darbinieku darba laiks.

Grūtniecības atvaļinājumu 56 kalendārās dienas un dzemdību atvaļinājumu 56 kalendārās dienas aprēķina kopā un piešķir 112 kalendārās dienas neatkarīgi no grūtniecības atvaļinājuma dienu skaita, kas izmantots līdz dzemdībām. Sievietēm, kurām sakarā ar grūtniecību medicīniskā aprūpe uzsākta ārstnieciski profilaktiskajā iestādē līdz divpadsmitajai grūtniecības nedēļai un turpināta visu grūtniecības laiku, piešķir 14 kalendāro dienu ilgu papildu grūtniecības atvaļinājumu, pievienojot to grūtniecības atvaļinājumam un aprēķinot kopā 70 kalendārās dienas. Grūtniecības, dzemdību vai pēcdzemdību sarežģījumu dēļ, kā arī tad, ja dzimuši divi vai vairāki bērni, sievietei piešķir 14 kalendāro dienu ilgu papildu dzemdību atvaļinājumu, pievienojot to dzemdību atvaļinājumam un aprēķinot kopā 70 kalendārās dienas. Sievietēm pēc viņu vēlēšanās piešķir atvaļinājumu bērna kopšanai līdz 3 gadu vecumam, izmaksājot par šo periodu valsts sociālās apdrošināšanas pabalstu. Laiku bērna kopšanai līdz 3 gadu vecumam ieskaita kopējā un nepārtrauktajā darba stāžā.

Pirms grūtniecības un dzemdību atvaļinājuma vai tieši pēc tā sievietei pēc viņas iesnieguma piešķir ikgadējo atvaļinājumu neatkarīgi no darba stāža pie attiecīgā darba devēja. Sievietēm, kurām ir bērns līdz 14 gadu vecumam (bērns invalīds līdz 16 gadu vecumam), ikgadējo atvaļinājumu piešķir vasarā vai – pēc sievietes iesnieguma – citā viņai izdevīgā laikā.

Aizliegts pazemināt sievietēm darba samaksu sakarā ar grūtniecību vai bērna kopšanu. Nav atļauts pēc darba devēja iniciatīvas atlaist grūtnieces un sievietes, kurām ir bērns līdz 3 gadu vecumam. Atlaišana atļauta tajos gadījumos, kad pilnīgi likvidē uzņēmumu, iestādi vai organizāciju.

12.2. DROŠĪBAS NOTEIKUMI DARBAM AR DATORU

Darba drošība ir viens no svarīgākiem faktoriem darba attiecībās. Eiropas Savienības valstīs darba drošības un arodveselības regulēšanas jautājumiem tiek pievērsta ārkārtīgi liela uzmanība. Nostiprinot uzskatu par to, ka vesels un aizsargāts darbinieks spēj ātri un efektīvi veikt savu darbu, uzņēmēji tiek pārliecināti ievērot darba likumdošanu un attīstīt darba drošību savās organizācijās. Jāpiebilst, ka ļoti liela nozīme ir Eiropas Savienības sodu sistēmai, kas motivē uzņēmējus nodrošināt normatīviem atbilstošu darba vidi, nevis maksāt sodus.

Latvijā darba drošības un arodveselības prasības ir noteiktas 1993. gada 4. maija likumā "Par darba aizsardzību" un tam pakārtotajos Ministru kabineta noteikumos. Saskaņā ar likumu "Par darba aizsardzību" darba devējam ir jānodrošina darbinieku veselībai nekaitīgi un droši darba apstākļi. Taču noteikumu neievērošana diemžēl netiek sodīta ar pietiekami lielu sodu, kas motivētu darba devējus noteikumus ievērot. Turklāt bezdarba līmenis Latvijā ir tāds, ka darbinieki bieži vien neuzdrošinās aizstāvēt savas tiesības darba devēju priekšā, jo viņi baidās zaudēt darbu.

Iestāšanās Eiropas Savienībā ietekmē arī Latvijas likumdošanas aktu izstrādi. Pašlaik notiek strauja darba aizsardzības normatīvo aktu saskaņošana ar ES prasībām. Tiek izstrādāts jauns Darba aizsardzības likuma projekts atbilstoši ES jumta direktīvai 89/391 EEC, kas nosaka vispārējās darba drošības un veselības aizsardzības prasības darba vietās. Par šo prasību ievērošanu ir atbildīgs darba devējs. Gaidāmā likuma galvenā atšķirība no vecā likuma ir tā, ka darba devējam būs jāveic riska novērtēšana darba vietās un nepieciešamie pasākumi, lai šo risku novērstu vai pēc iespējas vairāk samazinātu. Likuma projektā kā viens no darba aizsardzības pamatprincipiem ir minēts tas, ka darbs indivīdam jāpiemēro galvenokārt darba vietas iekārtojuma, darba aprīkojuma, kā arī darba un ražošanas metožu izvēles ziņā. Īpaša uzmanība pievēršama vienmuļa darba atvieglošanai, mazinot tā negatīvo ietekmi uz veselību.

12.2.1. DARBA DROŠĪBAS UN VESELĪBAS AIZSARDZĪBAS NOTEIKUMI, STRĀDĀJOT AR DISPLEJU UN IEKĀRTOJOT DARBSTACIJU

Darba devējam ir jānodrošina visas tālāk minētās prasības.

Darbstacija ir iekārtota tā, lai tās lietošana neapdraudētu nodarbinātā drošību un veselību.

DISPLEJS:

- rakstu zīmes uz ekrāna ir skaidrā formā, atbilstošā lielumā un ar atbilstošām atstarpēm starp rakstu zīmēm un rindām;
- attēls uz ekrāna ir stabils, bez mirgošanas vai cita veida nestabilitātes;
- gaišums un kontrasts starp rakstu zīmēm un fonu ir tāds, lai nodarbinātais to varētu viegli regulēt un viegli pielāgot apkārtējiem apstākļiem;

- ekrāns ir viegli pagriežams un noliecams atbilstoši nodarbinātā vajadzībām;
- var izmantot atsevišķu pamatni vai pielāgojamu galdu;
- uz ekrāna nav spīduma un atstarojuma, kas var radīt neērtības nodarbinātajam.

TASTATŪRA:

- tastatūra ir pagriežama un atdalīta no ekrāna, lai nodarbinātais varētu atrast ērtu darba stāvokli, novēršot roku vai plaukstu nogurumu;
- tastatūras virsma ir matēta un novērš atspīdumu;
- tastatūras izkārtojums un taustiņi ir viegli lietojami;
- simboli uz taustiņiem ir pietiekami kontrastaini un salasāmi paredzētajā darba pozīcijā.

DARBA GALDS:

- darba galda virsma maz atstaro gaismu;
- darba galds ir pietiekami liels, lai nodarbinātais varētu uz tā atbalstīt plaukstas un rokas, mainīt darba vietā esošo ierīču un priekšmetu izvietojumu, kā arī atrast sev ērtu darba stāvokli;
- platība tastatūras priekšā ir pietiekama, lai nodrošinātu atbalstu nodarbinātā rokām un plaukstām;
- dokumentu turētājs ir stabils, pielāgojams un novietots tā, lai līdz minimumam samazinātu neērtas nodarbinātā galvas un acu kustības.

DARBA KRĒSLS:

- darba krēsls ir stabils un nodrošina nodarbinātajam iespēju brīvi kustēties un ieņemt ērtu stāvokli;
- darba krēsla augstums ir regulējams;
- darba krēsla atzveltnes augstums un slīpums ir regulējams;
- katram nodarbinātajam ir kāju atbalsts, ja viņš to vēlas.

DARBA TELPAS:

- darbstacijas izmēri un plānojums nodrošina nodarbinātajam pietiekami daudz vietas ķermeņa stāvokļa mainīšanai un kustību brīvībai;
- telpas un darba vietas apgaismojums ir pietiekams un nodrošina kontrastu starp ekrānu un fonu veidojošo vidi atbilstoši darba veidam un nodarbinātā redzes prasībām;
- iespējamais traucējošais spīdums un atstarojums uz displeja vai cita aprīkojuma ir novērsts, saskaņojot darbstacijas izkārtojumu ar mākslīgo gaismas avotu izvietojumu un tehnisko raksturojumu;
- darbstacijas gaismas avoti, logi, caurredzamas vai caurspīdīgas sienas un spilgtas krāsas konstrukcijas vai sienas nerada tiešu spīdumu un, ciktāl iespējams, nerada atstarojumu uz displeja;
- logi ir aprīkoti ar atbilstoši pielāgojamu aizsegu sistēmu, lai samazinātu dienasgaismu, kas krīt uz darbstaciju;
- troksnis, ko rada darbstacijas aprīkojums, netraucē darba telpā normāli sarunāties un koncentrēties darba pienākumu izpildei;

- darbstacijas aprīkojums neizplata papildu siltumu, kas varētu radīt neērtības nodarbinātajam;
- viss starojums ir samazināts līdz līmenim, kas neapdraud nodarbinātā veselību;
- darba telpā tiek uzturēts piemērots gaisa mitruma līmenis.

Izstrādājot, izvēloties, pasūtot un modificējot programmatūru, kā arī nosakot uzdevumus saistībā ar darbstacijas iekārtu lietošanu, tiek ņemti vērā šādi principi:

- programmatūra ir piemērota nodarbinātā darba uzdevumu veikšanai, kā arī pēc iespējas atbilst nodarbinātā pieredzei un zināšanu līmenim;
- aizliegts izmantot datorprogrammas, kas kontrolē nodarbinātā darba kvalitāti vai kvantitāti, iepriekš par to nebrīdinot nodarbināto;
- programmatūra nodrošina nodarbinātā informētību par datorprogrammas darba gaitu un darba rezultātu;
- informācija uz displeja parādās nodarbinātajam pieņemamā formātā un ātrumā;
- ir ievēroti ergonomikas principi, īpaši, ja datu apstrādē piedalās nodarbinātais.

12.2.2. JAUNI NOTEIKUMI

Pašlaik darba aizsardzības jomā ir izstrādāti un pieņemti vairāki MK noteikumi saskaņā ar ES jumta direktīvas 89/391 EEC un tai pakārtoto direktīvu pamatprasībām, piemēram, 2001. gada 3. aprīļa MK noteikumi Nr. 153 "Darba drošības un veselības aizsardzības noteikumi, strādājot ar displeju un iekārtojot darbstaciju", kas ir izstrādāti saskaņā ar ES direktīvas 90/270/EEC prasībām.

Šajos noteikumos ietvertās darba drošības un veselības aizsardzības prasības attiecas uz darbiniekiem, kas, veicot savu darbu, katru darba dienu pie displeja strādā vismaz divas stundas. Par noteikumu prasību ievērošanu ir atbildīgs darba devējs. Noteikumu kontroles un uzraudzības funkcijas veic Valsts darba inspekcija.

Noteikumi stājās spēkā ar 2001. gada 1. jūniju, līdz ar to darba devējam, iekārtojot jaunas darba vietas pie datora pēc 2001. gada 1. jūnija, ir jāievēro šo noteikumu prasības. Zināms pārejas periods ir dots tiem darba devējiem, kuru uzņēmumos jau ir izveidotas darba vietas ar datoru līdz 2001. gada 1. jūnijam. Šīs darba vietas ir jāiekārto atbilstoši noteikumu prasībām līdz 2004. gada 31. decembrim.

Saskaņā ar šo noteikumu prasībām darba devēja pienākums ir

- veikt datorizētas darba vietas riska faktoru novērtējumu, kā arī nepieciešamos pasākumus, lai novērstu vai samazinātu konstatētos riska faktorus,
- informēt darbiniekus par visiem veiktajiem darba drošības un veselības aizsardzības pasākumiem,
- pirms darba uzsākšanas, kā arī tad, ja būtiski tiek mainīta datorizētas darba vietas organizācija, apmācīt darbiniekus, kā samazināt kaitīgo faktoru iedarbību uz veselību,
- radīt iespēju darbiniekiem ikdienas darbā izmantot periodiskas atpūtas pauzes vai mainīt darba raksturu,

- iesaistīt darbiniekus visos ar darba aizsardzību saistītajos jautājumos,
- nodrošināt darbiniekiem obligātās veselības pārbaudes normatīvajos aktos noteiktajā kārtībā, ieskaitot redzes pārbaudi (kārtību, kādā veicamas obligātās veselības pārbaudes, nosaka 1997. gada 4. marta MK noteikumi Nr. 86 "Noteikumi par obligāto veselības pārbaudi un apmācību pirmās palīdzības sniegšanā" un 1998. gada 12. janvāra LM rīkojums Nr. 8 "Par obligāto veselības pārbaužu veikšanas kārtību"),
- ja darbiniekam veikta obligātā veselības pārbaude un tajā konstatēts, ka darbā ar datoru viņam ir nepieciešama redzes korekcija, darba devējam darbinieks jānodrošina ar redzi koriģējošām brillēm,
- nodrošināt darba vietu pie datora, ievērojot minimālās darba drošības un veselības aizsardzības prasības.

Šais noteikumos paredzētas minimālās prasības, kas ievērojamas attiecībā uz displeju, tastatūru, darba galdu, darba krēslu, darba telpas iekārtojumu, ieskaitot darba vidi (apgaismojumu, tiešos atspīdumus un atspulgus displejā, troksni, mikroklimatu), kā arī uz programmatūru un pareizu darba organizāciju.

Lai nodrošinātu noteikumu prasību izpildi, darba devējam ir ieteicams ņemt vērā Latvijas valsts standartu – LVS EN ISO 9241 "Ergonomikas prasības darbam ar displejiem", taču darba devējs var izmantot arī citu valstu izstrādātās metodikas vai standartus, jo svarīga ir attiecīgo noteikumu prasību ievērošana, nevis veids, kāds izvēlēts, lai iekārtotu ergonomiski pareizu darba vietu pie datora.

Starptautiskais standarts EN ISO 9241 "Ergonomikas prasības darbam ar displejiem" 2000. gadā tika adaptēts ar titullapas metodi kā Latvijas standarts, un tam ir piešķirts nacionālā standarta statuss. Diemžēl šobrīd standarts ir pieejams tikai angļu valodā, taču ir uzsākta tā tulkošana.

LVS EN ISO 9241 standarta 1., 2., 10. un 11. daļa nosaka vispārīgas ergonomikas prasības, 3., 4., 7., 8. un 9. daļa – ergonomikas prasības aparatūrai, 5. un 6. daļa – ergonomikas prasības darba videi, bet 12., 13., 14., 15., 16. un 17. daļa – programmatūrai.

Izpildot prasības, kas noteiktas 2001. gada 3. aprīļa MK noteikumos Nr. 153 "Darba drošības un veselības aizsardzības noteikumi, strādājot ar displeju un iekārtojot darbstaciju", darba devējam īpaši saistoša ir standarta 5. un 6. daļa.

Standartā ir ietverti šādi noteikumi:

- LVS EN ISO 9241-1: 1997 – 1. daļa. Vispārīgs ievads,
- LVS EN ISO 9241- 2: 1993 – 2. daļa. Prasības darba uzdevumiem,
- LVS EN ISO 9241-3: 1992 – 3. daļa. Prasības displejam,
- LVS EN ISO 9241-4:1998 – 4. daļa. Prasības tastatūrai,
- LVS EN ISO 9241-5:1998 – 5. daļa. Darbstacijas izkārtojums un prasības darba pozām,
- LVS EN ISO 9241-6:1999 – 6. daļa. Ieteikumi darba videi,
- LVS EN ISO 9241-7:1998 – 7. daļa. Prasības atstarojošiem displejiem,
- LVS EN ISO 9241-8:1997 – 8. daļa. Prasības attēla krāsām,
- LVS EN ISO 9241-9:2000 – 9. daļa. Prasības ievadierīcēm bez tastatūras,
- LVS EN ISO 9241-10:1996 – 10. daļa. Dialogu principi,

- LVS EN ISO 9241-11:1998 – 11. daļa. Lietojamības vadlīnijas,
- LVS EN ISO 9241-12:1998 – 12. daļa. Informācijas pasniegšana,
- LVS EN ISO 9241-13:1998 – 13. daļa. Lietotāju vadīšana,
- LVS EN ISO 9241-14:1999 – 14. daļa. Izvēļņu dialogi,
- LVS EN ISO 9241-15:1998 – 15. daļa. Komandu dialogi,
- LVS EN ISO 9241-16:1999 – 16. daļa. Tiešās manipulācijas dialogi,
- LVS EN ISO 9241-17:1998 – 7. daļa. Ekrānformu dialogi.

12.2.3. DATORU LIETOTĀJU SŪDZĪBAS UN TO CĒLOŅI

Datora lietotāju skaits aug ar katru dienu. Pasaulē ir veikti daudzi pētījumi par datora ietekmi uz cilvēka veselību. Īpaša uzmanība pievērsta redzes traucējumiem, atsevišķu balsta un kustību aparāta daļu pārslodzei un dažādām psiholoģiska rakstura problēmām. Pētījumu rezultāti liecina, ka pirmās sūdzības par veselības traucējumiem var rasties jau dažus mēnešus pēc tam, kad cilvēks ir sācis strādāt ar datoru; nopietnas slimības, ieskaitot arodslimības, parasti konstatē pēc pieciem gadiem vai ilgāka laikposma.

3. tabulā attēloti iespējamo veselības traucējumu cēloņi cilvēkam, kas strādā ar datoru.

3. tabula

Datoru lietotāju sūdzības un to cēloņi

Sūdzības	Iespējamie cēloņi
Redzes diskomforts: • sausās acs sindroms • asarošana • graušana • svešķermeņa sajūta acīs • pārejošas redzes asuma izmaiņas • acu nogurums vai apsārtums • u. c.	• Nekvalitatīvs attēls uz monitora ekrāna (netīrs, putekļains monitors vai tā filtrs, nepietiekami vai pārmērīgi kontrastains attēls, pārāk mazs zīmju izmērs, sarežģīta burtu forma) • Nepiemērots apgaismojums (pārāk spilgts vai nepietiekams) • Atspīdumi un apžilbinājumi (nepareizi novietots vai pārāk vājš ekrāns vai gaismas ķermenis) • Nekoriģēta redze (nepārbaudīta redze vai nepareizi izvēlētas brilles) • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks • Nepareizi izvēlēts attālums no acīm līdz ekrānam, dokumentu turētājam un tastatūrai • Intensīvas datu ievadīšanas laikā netiek izmantots dokumentu turētājs • Zems gaisa mitrums telpā • Putekļaina telpa (nepietiekami uzkopta telpa)
Sāpes sprandā	• Monitors novietots par augstu • Krēsls novietots pārāk tuvu vai pārāk zemu attiecībā pret monitoru • Intensīvas datu ievadīšanas laikā netiek izmantots dokumentu turētājs • Monitors vai dokumentu turētājs novietots pārāk tālu un/vai neatrodas tieši pretī strādājošajam • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks • Nekoriģēta redze (nepārbaudīta redze vai nepareizi izvēlētas brilles) • Nepiemērots apgaismojums (pārāk spilgts vai pārāk vājš)

Sāpes plecos	• Pārāk augsta darba virsma ar tastatūru un peli • Pele novietota par tālu (sānis) no tastatūras • Roku balsti novietoti par augstu, par tālu vai par tuvu • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks
Sāpes jostasvietā un krustu rajonā	• Nav muguras atbalsta, vai tas ir nepietiekams • Pārāk augsts darba krēsls • Pārāk zema darba virsma • Nepietiekama telpa kājām zem darba virsmas • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks • Atspīdumi monitorā, kuru dēļ darba poza ir nepareiza
Sāpes plaukstu pamatlocītavās	• Vienveidīgas plaukstu pamata un pirkstu locītavu kustības (darbs ar tastatūru un peli) • Pārāk liels leņķis starp darba virsmu un tastatūru (veidojas fizioloģiski nepareizs plaukstu pamata stāvoklis) • Nepietiekams plaukstu pamata atbalsts • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks
Sāpes elkoņu locītavās	• Pārāk augsta darba virsma • Pele novietota par tālu (sānis) no tastatūras • Netiek izmantoti roku balsti • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks
Sāpes apakšdelmos	• Pārāk augsta darba virsma • Asas darba virsmas malas • Apakšdelmu atbalsts nav pietiekams • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks
Diskomforts apakšstilbos (sāpes, tirpšanas sajūta, nogurums u. c.)	• Ilgstoša sēdēšana • Pārāk zema darba virsma • Pārāk dziļš sēdeklis • Sēdekļa priekšējā mala nav noapaļota • Pārāk augsts sēdeklis un netiek izmantots kāju paliktnis • Sēdēšana ar sakrustotām kājām • Nepietiekama telpa kājām zem darba virsmas • Nepietiekami atpūtas brīži • Pārāk ilgs darba laiks

NOZARES STANDARTI

13. IEVADS

Pēdējos gadu desmitos programmatūras izstrādes process ir mainījies. Vidēju un lielu projektu izstrādē veiksmīga rezultāta sasniegšanai ir nepieciešams ievērot noteiktus programmatūras izstrādes „likumus" – standartus. Ievērojot standartu prasības programmatūras projektu izstrādē, uzņēmumā tiek organizēti visi programmatūras izstrādes procesi, kā arī izvirzītas vienotas formas prasības pret visiem programmatūras izstrādes procesa rezultātiem – dokumentiem, programmatūras moduļu „kodiem" utt.

Standartu lietošana projektā izvirza savas prasības un papildu darbības, un līdz ar to palielinās programmatūras projekta izstrādei patērētais laiks. Standartu lietošanu programmatūras projektu izstrādē var uzskatīt par sava veida nodrošinājumu pret dažāda veida problēmām programmatūras izstrādes laikā un pēc tā – programmatūras izstrādātājam veicot programmatūras uzturēšanu. Tomēr nelielos projektos, kad projekta izstrādē nodarbināti viens vai divi darbinieki un projekts nav darbietilpīgs, dažu standartu prasību apzināta neievērošana var tikt pieļauta.

Nozares standarti obligāti ir jāzina darbā ar programmatūras izstrādes projektiem nozares uzņēmumos. Tas ir nepieciešams ne tikai tiem projektos iesaistītajiem darbiniekiem, kuri nodarbojas ar dažādu dokumentu izstrādi un projektu plānošanu, bet arī visiem pārējiem projektos iesaistītajiem darbiniekiem.

Dainis Dosbergs

14. STANDARTI

Standarts ir oficiāls dokuments, kas nosaka prasības attiecībā pret dažāda veida objektiem un tehnoloģiskiem procesiem. Datu apstrādes un pārraides sistēmās ar šo terminu parasti saprot Starptautiskās standartizācijas organizācijas (*International Organization for Standardization – ISO*) standartus vai Starptautiskās telefonijas un telegrāfijas konsultatīvās komitejas rekomendācijas. Tomēr ar standartu izstrādāšanu nodarbojas arī daudzas citas nacionālās un starptautiskās organizācijas [51].

Latvijā bieži tiek lietoti LVS standarti, kuri ir latviešu valodā. LVS standarti ir izstrādāti, par pamatu ņemot attiecīgos ANSI/IEEE standartus. Tas darīts galvenokārt divu iemeslu dēļ: 1) esošu standartu adaptēšana latviešu valodai ir mazāk darbietilpīga nekā standartu izstrādāšana „no nulles", 2) esošajos standartos ir ietverta labākā nozares prakse, un tie ir vairāku gadu (pat gadu desmitu) laikā pietiekami labi „noslīpēti". Lai arī nozares ANSI/IEEE standarti pēdējā laikā ir mainījušies, izmaiņas atbilstošajos LVS standartos nav ieviestas. Tas saistīts ar procesa darbietilpību, kā arī ar nozares specifiku – nozares speciālistiem nesagādā problēmas izmantot ANSI/IEEE standartus angļu valodā. Tāpēc precīzas informācijas iegūšanai tos ieteicams izmantot.

Nozares standartus pēc to izmantošanas veida nosacīti ir iespējams iedalīt divās grupās:

- standarti, kuri izvirza prasības pret programmatūras projekta izstrādes rezultātiem, piemēram, standarti, kas izvirza prasības pret izstrādājamo dokumentu saturu;
- standarti, kuri izvirza prasības pret programmatūras izstrādes procesu.

Nevienam standartam nav likuma spēka. Standarta ievērošanu padarīt obligātu var, paredzot šādu prasību līgumā vai arī kādā normatīvā aktā, piemēram, likumā, Ministru kabineta noteikumos, firmas prezidenta rīkojumā u. tml., taču tas, ka standarti nav obligāti ievērojami, nepavisam nenozīmē, ka tie būtu bez apdomas jāignorē. Parasti standartos ir apkopota plaša pieredze un tie balansē starp to, ko vēlamies panākt, un to, ko praktiski var sasniegt. Šādas pieredzes ignorēšana reti kad dod ko labu [52].

Kam vajadzīgi standarti, ja to ievērošana nav obligāta? Informācijas tehnoloģija un it īpaši programmēšana ir ļoti pateicīgs piemērs atbildei uz šo jautājumu [52].

Akadēmiski izglītotiem datorprogrammu izstrādātājiem ir labi zināms (teorēmās ir pierādīts), ka nav nekādas iespējas noskaidrot, vai datorprogramma dara to, kas paredzēts, un nedara neko tādu, kas nav paredzēts. Mēs varam padarbināt programmu vienreiz ar vieniem datiem, otrreiz – ar otriem, trešoreiz ar citiem utt. un katru reizi konstatēt, ka notiek tiešām tas, ko mēs esam gribējuši sagaidīt. Taču vēl ir tūkstošā, miljonā un vēl citas reizes, kad būs citi dati. Kas būs tad, uzzināsim tikai tad, kad šī reize pienāks. Tā mēs varam testēt programmu līdz pasaules galam, bet kādreiz taču tā arī „jālaiž darbā". Tātad datorprogrammas pasūtītājs un lietotājs vienmēr varēs gribēt un prasīt, lai programma būtu labāk izveidota un vairāk pārbaudīta un atbrīvota no kļūdām. Bet vai viņi var arī sagaidīt „pasaules galu" un apmaksāt šo

teorētiski nebeidzamo darbu? No juridiskā viedokļa programmētājam faktiski nevar pārmest kļūdas programmā jau minēto apsvērumu dēļ. Tomēr gluži bezatbildīgu programmētāja rīcību arī nedrīkst pieļaut, jo zaudējumi programmas nepareizas darbības dēļ var būt katastrofāli. Ko darīt? [52.]

Ja nu lietotājs, cietis zaudējumus, iesūdzētu programmētāju tiesā, kas būtu jādara tiesnesim (kas vairumā gadījumu nav programmēšanas speciālists un kam tādam arī nav jābūt)? Tiesnesis jautās ekspertiem, vai programmētājs ir varējis garantēti nepieļaut kļūdu un zaudējumu rašanos. Eksperti godprātīgi atbildēs, ka tas ir teorētiski neiespējami. Tad tiesnesis jautās, vai programmētājs ir darījis visu saprātīgi nepieciešamo, lai nepieļautu zaudējumus. Kas ir saprātīgi nepieciešamais? Tas ir standarts! Standarts(-i) ir pašreizējā tehnoloģijas attīstības līmenī nepieciešamais, kompromiss starp gribēto un praktiski iespējamo, vienošanās starp pasūtītāju un izpildītāju, balstoties uz pasaulē uzkrāto pieredzi. Ja programmētājs būs disciplinēti izpildījis visas norunāto standartu prasības, tiesnesis būs spiests viņu attaisnot un zaudējumus atzīt par stihisku nelaimi. Toties līgumā norunāto standartu neievērošanas gadījumā pilnīgi pamatoti tiktu notiesāts izstrādātājs [52].

14.1. KONTROLJAUTĀJUMI

1. Kas ir standarts?
2. Kāpēc standartus nepieciešams lietot?
3. Kāpēc topošajiem nozares speciālistiem ir nepieciešams pārzināt standartus?

15. KVALITĀTES PĀRVALDĪBAS SISTĒMA. KVALITĀTES ROKASGRĀMATA. ISO UN CMM STANDARTI

15.1. IEVADS

Pirms aplūkojam jēdzienus „kvalitātes pārvaldības sistēma”[1] un „kvalitātes rokasgrāmata”, ir nepieciešams apzināt jēdziena „kvalitāte” nozīmi. Kvalitāte ir plašs un diskutējams jēdziens. Runājot par kvalitāti, cilvēki parasti iedomājas produkta vai procesa atbilstību tam, kas no šī produkta/procesa tiek sagaidīts, tas ir, apskatāmā produkta atbilstību patērētāja prasībām. Aplūkojot šo jēdzienu attiecībā uz konkrētiem produktiem, nav tik vienkārši noteikt produkta kvalitāti. Lai to veiktu, ir nepieciešams zināt konkrētus vērtēšanas kritērijus. Tāpat kā kvalitāte, arī kvalitātes nodrošināšana ir ļoti plašs jēdziens. Parasti ar kvalitātes nodrošināšanu tiek saprasta procesu kopa līdz ar dažādu kvalitātes atribūtu ievērošanu [53].

Kvalitātes atribūti ir vērtēšanas kritēriji, pēc kuriem konkrētu programmatūras produktu var novērtēt. Kvalitātes atribūti varētu būt šādi [54]:

- pareizība[2] (*Correctness*) – pakāpe, kādā programmatūra, dokumentācija vai citi izmantojamie objekti atbilst specificētajām prasībām;
- pārnesamība *(Portability)* – iespēja izmantot programmatūru un datus dažādās sistēmās;
- lietojamība *(Usability)* – sistēmas īpašība, kas raksturo, cik viegli lietotājs var apgūt tās izmantošanu, sagatavot tai ieejas datus un interpretēt tās izejas datus;
- atkallietojamība *(Reusability)* – programmatūras moduļu īpašība, kas nodrošina to izmantošanas iespējas vairākās datoru programmatūrās vai programmu sistēmās;
- uzturamība *(Maintainability)* – programmatūras vai tās komponentu īpašība, kas nodrošina iespēju tos modificēt, lai labotu kļūdas, uzlabotu veiktspēju un citus raksturojumus, kā arī adaptētu tos funkcionēšanas videi;
- testējamība *(Testability)* – īpašība, kas raksturo sistēmas vai tās komponenta piemērotību testēšanas procedūru izpildei;
- uzticamība *(Reliability)* – datora aparatūras vai programmas spēja izpildīt lietotāja prasības bez kļūmēm vai funkcionēšanas traucējumiem;
- efektivitāte *(Efficiency)* – pakāpe, kādā sistēma vai tās komponents izpilda savas funkcijas ar minimālo resursu patēriņu;
- integritāte *(Integrity)* – datora atmiņā uzglabāto datu pilnīguma un korektuma saglabāšana pēc to modificēšanas
- un citi.

---

[1] ISO 9001 standarta oficiālajā latviskojumā – kvalitātes vadības sistēma.

[2] Kā sinonīms tiek lietots arī „korektums”.

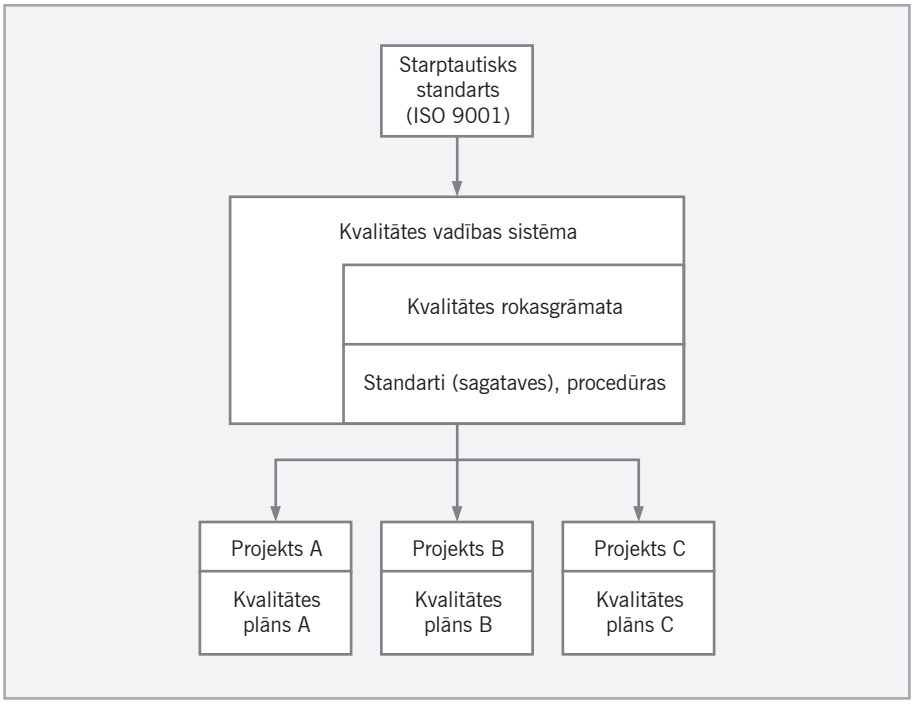
15.2. KVALITĀTES PĀRVALDĪBAS SISTĒMA

Uzņēmumam sasniedzot noteiktu skaitu darbinieku vai projektu, kļūst sarežģīti kontrolēt un organizēt visus programmatūras izstrādes procesus. Tās ir situācijas, kad viens vai vairāki uzņēmuma vadītāji vairs nespēj kvalitatīvi pārvaldīt uzņēmuma darbību. Tad ir nepieciešams izstrādāt sistēmu, kas precīzi aprakstītu uzņēmumā notiekošos procesus. Uzņēmuma vadībai jānodrošina personāla apmācība un kontrole, lai panāktu darbinieku vienādu un pilnvērtīgu rīcību uzdoto uzdevumu izpildē. Viens no risinājumiem darbības organizēšanas uzlabošanā ir programmatūras izstrādes procesa sakārtošana un šī procesa aprakstīšana kvalitātes pārvaldības sistēmā.

Ierasti ar darbībām kvalitātes pārvaldības sistēmas ieviešanā tiek saistītas šādas aktivitātes:

- dažādu apskates procedūru izmantošana, lai pārliecinātos par kvalitātes prasību ievērošanu,
- procesus aprakstošas procedūras izstrādāšana, nozares standartu lietošana, vadlīniju noteikšana,
- kvalitātes pārvaldības sistēmas pārskatīšana un pastāvīga pilnveidošana.

Lai vārds „kvalitāte" nebūtu tikai termins kvalitātes pārvaldības sistēmā, nepieciešams to atbilstoši „pastiprināt". Viens no ierastajiem standartiem kvalitātes pārvaldības sistēmu sertificēšanā ir ISO standarts (pašlaik nozares uzņēmumos izplatīts ir ISO 9001:2000).



19. att. Standartu, kvalitātes pārvaldības sistēmas un projektu saistība [53].

Veids, kādā ir veidota kvalitātes vadības sistēmas un starptautiskā standarta saikne ar izstrādājamo produktu, apskatāms 19. attēlā.

19. attēlā redzams, ka kvalitātes pārvaldības sistēma tiek izstrādāta, balstoties uz kādu standartu. Vēlams, lai šis standarts būtu kāds no pasaulē plaši lietotajiem standartiem, piemēram, ISO 9001:2000. Kvalitātes pārvaldības sistēmu ierasti veido kvalitātes rokasgrāmata, procedūras un dokumenti (iekšējie dokumenti un projekta dokumentu sagataves).

Kvalitātes rokasgrāmata ir primārais dokuments, kurā tiek aprakstīta uzņēmuma kvalitātes pārvaldības sistēma. Kvalitātes rokasgrāmatā ievieto atsauces uz kvalitātes pārvaldības sistēmā lietotajiem dokumentiem, projektos izstrādājamo dokumentu sagatavēm, uzņēmuma procesu aprakstiem – procedūrām un citiem dokumentiem. Kvalitātes rokasgrāmata ir dokuments, kas palīdz darbiniekam saprast, kā tam izpildīt uzdotos pienākumus atbilstoši kvalitātes pārvaldības sistēmas prasībām.

Dokumentu sagataves (standarti) ir izstrādāti noteikumi, kuros aprakstīta dokumenta izstrādes organizēšana un dokumentā iekļautās informācijas pasniegšanas forma.

Procedūrā ir ietverts to darbību kopums, kuras darbiniekam nepieciešams veikt, pildot kādus uzdevumus programmatūras projekta izstrādes ietvaros, piemēram, izstrādājot programmatūras prasību specifikāciju. Procedūra apraksta veicamos uzdevumus, to izpildes secību un nosaka atbildīgos.

Balstoties uz kvalitātes pārvaldības sistēmas prasībām un projektā izvēlēto dokumentu kopu, tiek izstrādāts katra atsevišķa projekta kvalitātes nodrošināšanas plāns – dokuments, kurā aprakstīts, kā konkrētā projekta ietvaros tiks nodrošināta kvalitāte.

15.3. PRASĪBAS PRET KVALITĀTES PĀRVALDĪBAS SISTĒMU

Kvalitātes pārvaldības sistēmu (KPS) iespējams apstiprināt atbilstoši standarta prasībām, ja uzņēmumā, ieviešot kvalitātes pārvaldības sistēmu, ir ievērotas visas standarta prasības.

ISO 9001:2000 standartā ir 5 nodaļas [55].

- Kvalitātes pārvaldības sistēma.
- Pārvaldības atbildība.
- Resursu pārvaldība.
- Produkta ražošana.
- Mērīšana, analīzes un uzlabošana.

15.3.1. KVALITĀTES PĀRVALDĪBAS SISTĒMA

Kvalitātes pārvaldības sistēmas izstrāde, dokumentēšana un ieviešana uzņēmumā jāveic saskaņā ar šī standarta prasībām. Kvalitātes pārvaldības sistēmas dokumentācijai ir jāietver dokumentēti kvalitātes politikas un mērķu paziņojumi, kvalitātes rokasgrāmata, dokumentētas procedūras u. c.

15.3.2. PĀRVALDĪBAS ATBILDĪBA

Augstākajai pārvaldībai (administrācijai) jāapliecina savas saistības kvalitātes pārvaldības sistēmas izstrādāšanā un uzlabošanā, izstrādājot kvalitātes politiku, nodrošinot kvalitātes mērķu noteikšanu un veicot pārvaldības apskates.

Augstākajai pārvaldībai ir jārūpējas par klientu prasību noteikšanu un nodrošināšanu, lai klienti būtu apmierināti.

Augstākajai pārvaldībai ir jānodrošina kvalitātes politikas atbilstība organizācijas mērķiem, tās izskaidrošana un izpratne organizācijā.

15.3.3. RESURSU PĀRVALDĪBA

Organizācijai ir nepieciešams nodrošināt resursus kvalitātes pārvaldības sistēmas ieviešanai un uzturēšanai, klientu apmierinātības veicināšanai.

Organizācijai ir jānosaka personāla kompetence, jānodrošina personāla apmācība, jāpieprasa personāla izglītību, apmācību, pieredzi un kvalifikāciju apstiprinoši dokumenti.

Organizācijai ir jānodrošina infrastruktūra – darba telpas, procesu iekārtas.

Organizācijai ir jānosaka un jāpārvalda darba vide, lai nodrošinātu projektu atbilstību kvalitātes pārvaldības sistēmas prasībām.

15.3.4. PRODUKTU RAŽOŠANA VAI PAKALPOJUMU SNIEGŠANA

Šajā standarta nodaļā ir izvirzītas prasības pret produkta ražošanas procesu. Programmatūras izstrādes projektos par šo procesu var uzskatīt visu programmatūras izstrādes dzīves ciklu no ieceres un prasību apkopošanas fāzes līdz uzturēšanas un nobeigšanas fāzei. Tiek aprakstīta produkta ražošanas plānošana, klienta prasību apzināšana un apkopošana, projektēšana un izstrāde, projektēšanas un izstrādes apskates, verificēšana un validēšana, sagāde (uzstādīšana) un glabāšana (uzturēšana).

15.3.5. MĒRĪŠANA, ANALĪZES UN UZLABOŠANA

Organizācijai jāplāno un jāievieš pārraudzība, mērīšana, analīzes un uzlabošana, lai uzskatāmi parādītu produkta atbilstību un nodrošinātu kvalitātes sistēmas pārvaldības efektivitāti.

Organizācijai nepieciešams veikt aktivitātes klientu apmierinātības izvērtēšanai.

Organizācijai ir jāveic iekšējie auditi ar mērķi noteikt, vai kvalitātes pārvaldības sistēma ir efektīvi ieviesta un tiek uzturēta atbilstoši standarta prasībām.

Organizācijai ir jāvērtē klientu apmierinātības, piegādātāju u. c. datu analīzes.

Lai uzlabotu organizācijas kvalitātes pārvaldības sistēmas efektivitāti, organizācijai jāveic korektīvās darbības (neatbilstības cēloņu likvidēšana, novēršot to atkārtošanās iespēju) un preventīvās darbības (potenciālu neatbilstības cēloņu likvidēšana, nepieļaujot to rašanos).

15.4. CMM STANDARTS

CMM – *Capability Maturity Model* ir starptautisks standarts, kas atšķirībā no ISO (kuru var lietot praktiski jebkurā ražošanas un pakalpojumu nozarē) ir izmantojams tieši programmatūras izstrādē.

CMM apraksta efektīva programmatūras izstrādes procesa pamatelementus. Tas ir palīgs kompāniju centienos gūt kontroli pār programmatūras izstrādes un uzturēšanas procesiem un attīstīt programmatūras izstrādes kultūru.

15.5. CMM ATTĪSTĪBAS VĒSTURE

1984. gadā ASV Kongress nodibināja *Software Engineering Institute (SEI)* uz *Carnegie Mellon University* bāzes.

1985. gadā SEI uzsāka darbu pie procesu brieduma ietvara *(Process Maturity Framework),* lai dotu iespēju novērtēt kompāniju iespējas izstrādāt programmatūru. Procesu brieduma ietvars attīstījās par spēju brieduma modeli *(Capability Maturity Model).*

1991. gadā tika izlaista pirmā CMM versija – CMM 1.0.

Pēc CMM versijas 1.0 adaptācijas tika izstrādāti CMM citām disciplīnām – programminženierijai (*System Engineering*), programmatūras iegādei (*Software Acquisition*) u. c. Lai gan daudzas kompānijas šo modeli uzskatīja par lielisku, tomēr vajadzēja cīnīties ar pārklāšanās, pretrunības un integrācijas problēmām. Daudzas kompānijas saskārās ar pretrunām starp esošo modeli un ISO 9001. Lai apvienotu vairākus dažādus CMM procesus, tika izstrādāts CMMI (*Capability Maturity Model Integration*). Atšķirībā no CMM, kurš ir vairāk orientēts uz izstrādi, kas balstīta uz ūdenskrituma (*Waterfall*) modeli, CMMI modelis ir vairāk saistīts ar iteratīvajām metodēm [56].

15.6. CMM LATVIJĀ

Atšķirībā no ISO 9001 standarta, pēc kura prasībām ir sertificēta lielākā daļa vadošo nozares uzņēmumu kvalitātes pārvaldības sistēmu, CMM ieviešana Latvijas IT nozares uzņēmumos praktiski nenotiek. Vienīgais no uzņēmumiem, kurā ir ieviests CMM, ir „Exigen Latvia". Lai arī CMM attiecībā pret ISO ir priekšrocības, jo tas ir izveidots tieši programmatūras izstrādes procesiem, tomēr ne Eiropas, ne arī Latvijas pasūtītāji nepārzina CMM standartu tādā līmenī, kā pārzina ISO standartu, tāpēc ne pašlaik, ne arī tuvākajā nākotnē nav plānojama CMM parādīšanās kā prasība pasūtītāju sludinātos konkursos, aizstājot tur esošo prasību attiecībā uz ISO standartu.

Uzņēmumā „Exigen Latvia" CMM standarts ir ieviests, lai spētu veiksmīgi konkurēt ASV tirgū, kur CMM tiek lietots plašāk. CMM modelim ir vairāki „procesu brieduma" līmeņi (kopumā pieci), pēc kuriem tiek novērtēts uzņēmums. „Exigen Latvia" ir novērtēts atbilstoši 4. līmeņa prasībām. Tas ir liels sasniegums, ņemot vērā, ka pasaulē 2003. gada beigās bija tikai 108 CMM 4. līmeņa un 98 CMM 5. līmeņa organizācijas [57].

15.7. KONTROLJAUTĀJUMI

1. Kas ir kvalitāte?
2. Kas ir kvalitātes pārvaldības sistēma?
3. Kas ir kvalitātes rokasgrāmata?
4. Kas ir ISO standarts? Kādas pamatprasības tajā ir ietvertas?
5. Kas ir CMM standarts?
6. Kādas ir būtiskākās ISO un CMM atšķirības?

16. PROGRAMMINŽENIERIJAS STANDARTU SISTĒMA

Nodaļa izstrādāta, balstoties uz [58].

Standartus, kas nepieciešami, izstrādājot programmatūru, atbilstoši to lietošanas veidam iespējams iedalīt četrās grupās.

1. Valsts standarti, kas nosaka programmatūras dokumentēšanu dažādās tās attīstības stadijās.
   - Informācijas tehnoloģija. Programmatūras lietotāja dokumentācija (LVS 66:1996).
   - Informācijas tehnoloģija. Programmatūras prasību specifikācijas (PPS) ceļvedis (LVS 68:1996).
   - Informācijas tehnoloģija. Programmatūras testēšanas dokumentācija (LVS 70:1996).
   - Informācijas tehnoloģija. Ieteicamā prakse programmatūras projektējuma aprakstīšanai (LVS 72:1996).
   - Informācijas tehnoloģija. Sistēmas darbības koncepcijas apraksts (LVS 75:1996).
2. Valsts standarti, kas nosaka programmatūras izstrādes procesa dokumentēšanu dažādās tās attīstības stadijās.[1]
   - Informācijas tehnoloģija. Programmatūras projekta pārvaldības plāns (LVS 67:1996).
   - Informācijas tehnoloģija. Programmatūras konfigurācijas pārvaldības plāns (LVS 69:1996).
3. Valsts standarti, kas nosaka programmatūras kvalitātes nodrošināšanas pasākumu veikšanu.
   - Informācijas tehnoloģija. Programmatūras kvalitātes nodrošināšanas plāns (LVS 65:1996).
   - Informācijas tehnoloģija. Programmatūras vienībtestēšana (LVS 73:1996).
   - Informācijas tehnoloģija. Programmatūras apskate un auditēšana (LVS 74:1996).
4. Citi ar nozari saistītie standarti.
   - Latviešu valoda datoriem (LVS 24:1993).
   - *Standard for Information Technology, Software Life Cycle Processes, Software Development. Acquirer-Supplier Agreement* (IEEE/EIA Std J-STD-016).
   - Ergonomikas prasības biroja darbam ar datoriem (LVS EN ISO 9241:2000).

[1] Pie šās grupas piederīgs ir arī standarts Programmatūras verifikācijas un validācijas plāns (LVS 71:1996), kas gan tiek lietots ļoti reti.

16.1. STANDARTU APRAKSTS

16.1.1. PROGRAMMATŪRAS KVALITĀTES NODROŠINĀŠANAS PLĀNS

Šī standarta mērķis ir aprakstīt minimālās prasības programmatūras kvalitātes nodrošināšanas plāna (PKNP) izstrādāšanai un tā saturam.

Standarts ir obligāta prasība kritisku programmu izstrādē un uzturēšanā, t. i., tādās programmās, kurās radušās kļūmes varētu ietekmēt drošību, veselību vai radīt lielus finansiālus vai sociālus zaudējumus. Standarts ir lietojams, lai palielinātu attiecīgās programmatūras uzticamību, un tāpēc to vai tā daļas varētu izmantot arī nekritiskās programmatūrās.

Kas ir kritiska programmatūra? Kritiska programmatūra (*critical software*) atbilstoši standarta definīcijai ir tāda programmatūra, kuras kļūme dotu triecienu drošībai vai varētu būt cēlonis lieliem finansiāliem vai sociāliem zaudējumiem.

! *Runājot par kritisku programmatūru, noteikti var minēt visas valsts nozīmes reģistrus pārvaldošās sistēmas, dažādu nodokļu administrēšanas sistēmas, kā arī sistēmas, kurās esošā informācija tiek izmantota dažādu nozīmīgu dokumentu izsniegšanā (pases, laulības reģistrācijas apliecības, miršanas apliecības u. tml.).*

Standarta nosaukumā minētais jēdziens „kvalitātes nodrošināšana" (*quality assurance*) ir saistīts ar plānotu un sistemātisku darbību shēmu, kas nepieciešama, lai panāktu adekvātu uzticību tam, ka lieta vai produkts atbilst izvirzītajām tehniskajām prasībām.

Tātad mēs, izmantojot šo standartu, varam sastādīt programmatūras kvalitātes nodrošināšanas plānu un panākt to, lai šajā plānā minētās operācijas tiktu lietotas, izstrādājot projektu.

16.1.2. PROGRAMMATŪRAS PROJEKTA PĀRVALDĪBAS PLĀNS

Standarta mērķis ir aprakstīt projekta pārvaldības plāna formātu un saturu. Standartu izmanto projekta pārvaldnieki vai citas personas, kuras sagatavo programmatūras projekta pārvaldības plānu. Standarts identificē minimālo elementu komplektu, kuram jāparādās visos programmatūras projekta pārvaldības plānos.

Kas tad ir programmatūras projekta pārvaldība, un kas ir programmatūras projekta pārvaldības plāns?

Programmatūras projekta pārvaldība *(software project management)* ir programmatūras projekta plānošanas, organizēšanas, personāla komplektēšanas, pārraudzības un vadības process.

Programmatūras projekta pārvaldības plāns *(software project management plan)* ir pamatdokuments programmatūras projekta pārvaldē. Programmatūras

projekta pārvaldības plānā jānosaka tehniskās un pārvaldošās projekta funkcijas, aktivitātes un uzdevumi, kas nepieciešami projekta līgumā noteikto programmatūras projekta prasību apmierināšanai.

16.1.3. PROGRAMMATŪRAS KONFIGURĀCIJAS PĀRVALDĪBAS PLĀNS

Standarts nosaka minimālo konfigurācijas pārvaldības plāna saturu.

Kas ir konfigurācijas pārvaldība? Par konfigurācijas pārvaldību tiek uzskatīta sava veida vadība, kas izmanto administratīvus un tehniskus rīkojumus un uzraudzību, lai identificētu un dokumentētu konfigurācijas elementu funkcionālās un fiziskās raksturiezīmes, vadītu izmaiņas šajās raksturiezīmēs, reģistrētu izmaiņu apstrādes un implementēšanas stāvokļus un formētu pārskatus par tiem, kā arī verificētu atbilstību specificētajām prasībām.

Konfigurācijas pārvaldes galvenie uzdevumi ir konfigurācijas identificēšana, konfigurācijas vadība, stāvokļu uzskaite, auditēšana un apskates, kā arī produkta izlaides organizēšana.

16.1.4. PROGRAMMATŪRAS VERIFIKĀCIJAS UN VALIDĀCIJAS PLĀNS

Standarts nosaka programmatūras verifikācijas un validācijas plāna (PVVP) formātu un minimālās prasības. Standartu var izmantot kā kritiskām, tā nekritiskām programmatūrām.

Kas ir verifikācija? Verifikācija ir process, kurā tiek noteikts, vai produkts attiecīgajā izstrādes fāzē atbilst iepriekšējā fāzē noteiktajām prasībām, t. i., vai pāreja no fāzes uz fāzi ir notikusi korekti.

Kas ir validācija? Validācija ir process, kas tiek veikts izstrādes fāzes beigās, lai pārliecinātos, vai izstrādātais produkts atbilst visām tām prasībām, kuras ir specificētas sākumā.

16.1.5. PROGRAMMATŪRAS APSKATE UN AUDITĒŠANA

Standarts skaidro apskates un auditācijas procedūras būtību, pamatojumu un šo procedūru attiecības ar citiem standartiem.

Standarts definē apskates un auditēšanas procesus, kas izmantojami kritiskai un nekritiskai programmatūrai, kā arī specifiskās procedūras, kuras nepieciešamas apskates un auditēšanas izpildei.

Standarts nesniedz novērtējumu individuālā darba ieguldījumam produkta izstrādāšanā. Tikai tad, ja apskate un auditēšana tiek veikta, lietojot standarta definētās procedūras, drīkst apgalvot, ka pastāv atbilstība šim standartam.

Standarts lietojams visās tipisku programmatūras dzīves ciklu fāzēs un ir uzlūkojams par etalonu, pēc kura var tikt gatavoti un novērtēti apskates un auditēšanas plāni.

16.1.6. LATVIEŠU VALODA DATORIEM

Standarts apraksta vispārīgās ziņas par latviešu valodu un dažādu datu standartpierakstu latviešu valodā.

Standartā tiek aprakstīti dažādie valsts un valodas kodi un tos reglamentējošie starptautiskie ISO standarti. Lai nodrošinātu valsts un valodas kodu unikalitāti starptautiskā līmenī, kodus piešķir starptautiskās standartizācijas organizācijas ISO izvēlēts reģistrācijas orgāns.

Standartā tiek aprakstīts latviešu alfabēts, skaitļu un ciparu pieraksts un teksta telpiskā organizācija. Teksta telpiskā organizācija nosaka, kādā veidā teksts tiek organizēts, t. i., no kreisās uz labo pusi, rindas kārtojot no augšas uz leju. Standartā minēts lietojamo pieturzīmju saraksts ar paskaidrojumiem. Standartā aprakstīti arī skaitļu, naudas summu, datumu un laiku pieraksta veidi.

Viena standarta nodaļa ir veltīta datu kārtošanas un meklēšanas likumu aprakstīšanai.

16.1.7. PROGRAMMATŪRAS LIETOTĀJA DOKUMENTĀCIJA

Standarta mērķis ir aprakstīt minimālās prasības lietotāja dokumentācijas izstrādāšanai un informācijas saturam. Šis standarts attiecas tikai uz tradicionālo lietotāju dokumentāciju drukātā veidā un nav attiecināms uz informācijas sistēmās esošajām palīgfunkcijām lietotājiem, piemēram, uz palīdzību (*Help*), jo šāda veida informācija krasi atšķiras no drukātās informācijas.

Standarts nosaka galvenos principus lietotāju dokumentācijā, taču katrā kompānijā var būt izstrādātas savas sagataves lietotāju dokumentācijas rakstīšanā.

Standarts tiek attiecināts uz trim lietotāju dokumentācijas veidiem.

- Lietotāja ceļvedis programmatūras instalēšanā.
- Lietotāja ceļvedis programmatūras darbināšanā.
- Lietotāja ceļvedis programmatūras pārvaldīšanā.

16.1.8. PROGRAMMATŪRAS PRASĪBU SPECIFIKĀCIJAS (PPS) CEĻVEDIS

Standarts ir ceļvedis lietotāja prasību aprakstīšanā. Tas iepazīstina ar PPS nepieciešamo saturu, raksturiezīmēm un ieskicē PPS struktūru. Standarts lietojams jaunradāmas programmatūras prasību aprakstīšanai, taču tas ne visai ērti un efektīvi ir lietojams tad, ja projekts tiek izstrādāts ar ātro prototipēšanu. Izmantojot standartu par palīgu, var izstrādāt pilnīgu un noteiktu PPS.

Kas tad ir ātrā prototipēšana? Ātrā prototipēšana ir programmatūras izstrādes modelis, ar kura palīdzību tiek ātrāk izstrādāti programmatūras prototipi, kurus lietotāji var sākt izmantot. Realizējot projektu pēc ūdenskrituma modeļa, nepieciešami arvien detalizētāki plāni, un tikai tad var notikt sistēmas izstrāde, savukārt ātrās prototipēšanas metodes pamatideja ir radīt sistēmu un pēc tam noteikt, ko nepieciešams pārplānot [59].

16.1.9. PROGRAMMATŪRAS TESTĒŠANAS DOKUMENTĀCIJA

Standarts apraksta testēšanas pamatdokumentus, kas ir saistīti ar programmatūras testēšanas dinamisko aspektu, t. i., procedūru un kodu izpildīšanu. Lai gan aprakstītie dokumenti ir veltīti dinamiskajai testēšanai, daži no tiem var tikt lietoti arī citās testēšanas darbībās, piemēram, projekta apskatēs.

Standarts paredzēts gan sākotnējās testēšanas dokumentācijai, gan arī turpmāku programmas laidienu dokumentācijai. Attiecībā uz konkrētu programmas laidienu standartu var lietot visām testēšanas fāzēm – no moduļa testēšanas līdz lietotāja akceptēšanai.

Standarts nepieprasa specifisku testēšanas metodoloģiju, pieeju, rīkus un nespecificē to lietošanas dokumentāciju. Standarts arī nenorāda un neprasa specifisku metodoloģiju dokumentu vadībai, konfigurācijas pārvaldībai vai kvalitātes nodrošināšanai.

16.1.10. IETEICAMĀ PRAKSE PROGRAMMATŪRAS PROJEKTĒJUMA APRAKSTĪŠANAI

Standartā tiek aplūkota ieteicamā prakse programmatūras projektējuma aprakstīšanai. Standarts specificē nepieciešamo informācijas saturu, iesaka programmatūras projektējuma organizatorisko formu, kā arī ietver norādījumus, kā savākt, organizēt un pasniegt projektējuma informāciju. Šie ieteikumi ir izmantojami neatkarīgi no izvēlētās programmatūras darbības sfēras un projektēšanas procesā izmantotajiem līdzekļiem. Standarts paredzēts visiem, kuri izstrādā un lieto programmatūras projektējuma aprakstu.

Programmatūras projektējuma apraksts – PPA (*software design description*) ir programmatūras sistēmas attēlojums, kas tiek radīts, lai atvieglotu analīzi, plānošanu, implementēšanu un lēmumu pieņemšanu. Tas ir programmatūras sistēmas uzmetums vai modelis. PPA tiek lietots kā sākotnējā vide, kuru izmanto, lai izplatītu programmatūras projektējuma informāciju.

16.1.11. PROGRAMMATŪRAS VIENĪBTESTĒŠANA

Standarts definē integrētu pieeju sistemātiskai un dokumentētai vienībtestēšanai. Tas apraksta testēšanas procesu, ko veido fāzu, darbību un uzdevumu hierarhija, un definē minimālo uzdevumu kopu katrai darbībai. Lai gan standarts identificē atteiču analīzes informācijas un programmatūras defektu labošanas vajadzību, tas nespecificē programmatūras atkļūdošanas procesu. Šo standartu var lietot jaunizstrādātu un modificētu vienību testēšanai.

Programmatūras vienībtestēšana ir process, kas ietver testēšanas plānošanu, testu kopas iegūšanu un testējamās programmatūras vienības mērīšanu, salīdzinot testējamo vienību ar tai noteiktajām prasībām. Mērīšana nozīmē datu paraugu izmantošanu, lai izpildītu vienību un salīdzinātu vienības faktisko uzvešanos ar to uzvedību, kas specificēta vienības prasību dokumentācijā.

16.1.12. SISTĒMAS DARBĪBAS KONCEPCIJAS APRAKSTS

Standarts nosaka dokumenta apraksta saturu un galvenos tā sastādīšanas principus. Sistēmas darbības koncepcijas apraksts ir pirmais dokuments, ar kuru sākas produkta izstrādāšana vai eksistējoša programmatūras produkta modificēšana. Tā uzdevums ir formulēt problēmu, veikt sākotnējās situācijas analīzi un aprakstīt sistēmas darbību saistībā ar tās funkcionēšanas vidi. Pēc šī dokumenta var pārliecināties, vai izpildītājam ir pareizs priekšstats par problēmu, tās aptuveno risinājumu un programmatūras un aparatūras izmaksām. Tas arī dod pasūtītājam iespēju pārbaudīt, vai ir formulētas visas viņa vēlmes.

Standarta galvenie lietotāji ir darbinieki, kas sagatavo sistēmas darbības koncepcijas aprakstu, kā arī veic tā verificēšanu.

16.1.13. *STANDARD FOR INFORMATION TECHNOLOGY, SOFTWARE LIFE CYCLE PROCESSES, SOFTWARE DEVELOPMENT ASQUIRER–SUPPLIER AGREEMENT*

Tas ir standartu standarts, jo apraksta visus procesus programmatūras izstrādē, iespējamās aktivitātes, nepieciešamos dokumentus.

16.1.14. ERGONOMIKAS PRASĪBAS PAR BIROJA DARBU AR DATORIEM

Standarts nosaka prasības, kas ievērojamas, organizējot darbu pie datora. Standarta nodaļās tiek apskatītas gan prasības par darba vidi (darba vietu, datora parametriem), gan arī par saskarni ar lietojumprogrammām. Tā, piemēram, standartā tiek aprakstīti ieteikumi, kā sniegt informāciju lietotājam, kā veidot dialogu ar lietotāju.

16.2. KONTROLJAUTĀJUMI

1. Kādi ir programminženierijā visbiežāk lietotie standarti?
2. Aprakstiet katru standartu!

17. PROGRAMMATŪRAS DOKUMENTĀCIJAS KOPAS IZVĒLE

Nodaļa izstrādāta, balstoties uz [58].

4. tabulā ir dots programmatūras lietošanai un uzturēšanai nepieciešamo dokumentu saraksts.

4. tabula

Programmatūras lietošanai un uzturēšanai nepieciešamā dokumentācija

Nr.	Dokumenta nosaukums	Komplekts			Rekomendējošie materiāli dokumenta izstrādei
		Min.	Ieteic.	Pilns	
1.Programmatūras lietošanai nepieciešamā dokumentācija					
1.1.	Programmatūras produkta apraksts		✓	✓	ISO/IEC 12119; IEEE/EIA J-STD-016 (I.2.1.)
1.2.	Programmatūras versijas apraksts		✓	✓	IEEE/EIA J-STD-016 (I.2.2.)
1.3.	Programmatūras lietotāja dokumentācija	✓	✓	✓	LVS 66:1996; ISO/IEC 12119; IEEE/EIA J-STD-016
1.3.1.	Programmatūras instalēšanas apraksts	✓	✓	✓	IEEE/EIA J-STD-016 (E.2.3.)
1.4.	Programmatūras izpildkodi	✓	✓	✓	IEEE/EIA J-STD-016 (I.2.1.)
2. Programmatūras uzturēšanai papildus nepieciešamā dokumentācija					
2.1.	Programmatūras darbības koncepcijas apraksts		✓	✓	LVS 75:1996; IEEE/EIA J-STD-016 (F.2.1.)
2.2.	Programmatūras prasību specifikācija	✓	✓	✓	LVS 68:1996;IEEE/EIA J-STD-016 (F.2.2., F.2.3., F.2.4.)
2.3.	Programmatūras projektējuma apraksts		✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (G.2.1., G.2.2., G.2.4.)
2.3.1.	Datu bāzu projektējuma apraksts	✓	✓	✓	IEEE/EIA J-STD-016 (G.2.3.)
2.4.	Programmatūras pirmkodi	✓	✓	✓	IEEE/EIA J-STD-016 (G.2.1.)
2.5.	Programmatūras uzturēšanas rokasgrāmatas			✓	IEEE/EIA J-STD-016 (5.13.8.)
2.5.1.	Programmatūras uzturēšanas plāns			✓	ISO/IEC 12007
2.5.2.	Programmatūras uzturēšanas procedūra			✓	ISO/IEC 12007

Minimālais komplekts ietver tos dokumentus, bez kuriem nav iespējama ne programmatūras lietošana, ne uzturēšana, t. i., dokumentus, bez kuriem programmatūra nav uzskatāma par pabeigtu un nevar tikt pieņemta.

Ieteicamajā komplektā iekļauti tie dokumenti, kuri nodrošina normālu programmatūras lietošanu un neliela apjoma pārveidojumu (pārprogrammēšanas) veikšanu tās uzturēšanas laikā. Protams, t. s. ieteicamais komplekts nav vienīgais iespējamais un konkrētā gadījumā, ja to prasa projekta īpatnības, no tā var nedaudz atkāpties uz vienu vai otru pusi.

Pilnajā komplektā norādītie dokumenti atspoguļo pilnu informāciju, kas ir izstrādātāja rīcībā par programmatūras produktu un kas ir nepieciešama gan pašam izstrādātājam jaunu produkta versiju attīstīšanai, gan arī personālam, kurš veic programmatūras būtisku mainīšanu un pilnveidošanu tās uzturēšanas laikā.

Tabulā nav atspoguļots, kura no minētām dokumentācijām tiek nodota pasūtītājam un kura paliek tikai programmatūras izstrādātāju rīcībā. Nododamās dokumentācijas komplekts ir atkarīgs pirmām kārtām no tā, kas veiks programmatūras uzturēšanu. Šo darbu sadali vēlams īpaši atrunāt līgumā vai arī slēgt atsevišķu līgumu par programmatūras uzturēšanu. Jāņem vērā, ka veicamā darba apjoms un līdz ar to programmatūras uzturēšanai nepieciešamais personāls un izmaksas ir aptuveni vienādas gan tad, ja programmatūras uzturēšanu veic lietotājs, gan tad, ja to dara programmatūras izstrādātājs. Lietotāja gadījumā izmaksas un darbietilpība būs lielāka vēl par tik, cik vajadzīgs, lai apgūtu programmatūras darbību un pirmkodus līdz tādam līmenim, ka ir iespējams veikt to modificēšanu. Par nododamās dokumentācijas (nodevumi – *deliverables*) komplektu pasūtītājam un izstrādātājam jāvienojas atsevišķi, rakstiski dokumentējot šo vienošanos (piemēram, līguma pielikumā). Jāņem vērā, ka dokumentu sagatavošana, īpaši, ja tie tiek gatavoti nodošanai lietotājam, ir darbietilpīga un līdz ar to arī dārga. Turklāt nepavisam programmatūras uzturamība nepieaug proporcionāli tās dokumentācijas apjomam. Pārāk liels dokumentācijas apjoms izraisa pretēju efektu – tā sagatavošana un apgūšana ir ļoti darbietilpīga, un to var būt grūti lietot. Turklāt pieaug bīstamība, ka nav pilnībā izsekotas un atspoguļotas visas izmaiņas, kas tiek izdarītas programmatūras dzīves jebkurā posmā. Tas ir sevišķi bīstami, jo padara dokumentāciju pretrunīgu.

5. tabulā ir dots pilns programmatūras projekta dokumentācijas saraksts.

5. tabula

Pilna programmatūras projekta dokumentācija

Nr.	Dokumenta nosaukums	Komplekts			Rekomendējošie materiāli dokumenta izstrādei
		Min.	Ieteic.	Pilns	
1	2	3	4	5	6
1. Projekta sagatavošanas un uzturēšanas dokumenti					
1.1.	Sākotnējie projekta priekšlikumi *(Preliminary Design Proposal)*		✓	✓	

1.2.	Līgums ar pasūtītāju	✓	✓	✓	
1.2.1.	Līguma izpildes kalendārais plāns	✓	✓	✓	
1.3.	Projekta dienasgrāmata		✓	✓	
1.4.	Programmatūras izstrādes datne		✓	✓	IEEE/EIA J-STD-016
2. Projekta plānošanas dokumenti					
2.1.	Programmatūras (sistēmas) izstrādes plāns			✓	IEEE/EIA J-STD-016
2.2.	Projekta pārvaldības plāns			✓	LVS 67:1996; IEEE 1058.1
2.2.1.	Programmatūras konfigurācijas pārvaldības plāns		✓	✓	LVS 69:1996; IEEE 1042, IEEE 828
2.2.2.	Projekta iekšējo pārbaužu plāns		✓	✓	
2.2.3.	Kvalitātes nodrošināšanas plāns (*Software Quality Assurance Plan*)		✓	✓	LVS 65:1996; IEEE 730.1
2.3.	Programmatūras verifikācijas un validācijas plāns			✓	LVS 71:1996; IEEE 1012
2.4.	Programmatūras (kvalifikācijas) testēšanas plāns	✓	✓	✓	LVS 70:1996; IEEE/EIA J-STD-016, IEEE 829
2.5.	Programmatūras pārcelšanas (*transition*) plāns			✓	IEEE/EIA J-STD-016
2.6.	Programmatūras instalēšanas plāns	✓	✓	✓	IEEE/EIA J-STD-016 (E.2.3.)
3. Projekta specifikācijas					
3.1.	Darbības koncepcijas apraksts (*Operational Concept Description*)		✓	✓	LVS 75:1996; IEEE/EIA J-STD-016 (F.2.1.)
3.2.	Sistēmas/apakšsistēmas (kopā ar aparatūru) prasību specifikācija	✓	✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (F.2.2.)
3.3.	Programmatūras prasību specifikācija *(Software Requirements Specification*)	✓	✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (F.2.4.)
3.4.	Saskarņu prasību specifikācija	✓	✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (F.2.3.)
3.5.	Programmatūras produkta specifikācija		✓	✓	ISO/IEC 12119; IEEE/EIA J-STD-016 (I.2.1.)
3.6.	Programmatūras versijas apraksts		✓	✓	IEEE/EIA J-STD-016 (I.2.2.)
4. Projektējumu dokumentācija					
4.1.	Sistēmas/apakšsistēmas (kopā ar aparatūru) projektējuma apraksts		✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (G.2.1.) IEEE 1016

4.2.	Programmatūras projektējuma apraksts		✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (G.2.4.) IEEE 1016
4.3.	Saskarņu projektējuma apraksts		✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (G.2.2.) IEEE 1016
4.4.	Datu bāzu projektējuma apraksts	✓	✓	✓	LVS 72:1996; IEEE/EIA J-STD-016 (G.2.3.) IEEE 1016
5. Implementēšanas dokumentācija					
5.1.	Programmatūras pirmkodi	✓	✓	✓	IEEE/EIA J-STD-016 (G.2.1.)
5.2.	Programmatūras izpildkodi	✓	✓	✓	IEEE/EIA J-STD-016 (I.2.1.)
6. Lietotāja dokumentācija					
6.1.	Lietotāja rokasgrāmata	✓	✓	✓	LVS 66:1996; ISO/IEC 12119; IEEE/EIA J-STD-016 (J.2.1.)
6.2.	Datora programmēšanas rokasgrāmata			✓	IEEE/EIA J-STD-016 (I.2.3.)
6.3.	Programmaparatūras atbalsta rokasgrāmata			✓	IEEE/EIA J-STD-016 (I.2.4.)
6.4.	Programmatūras uzturēšanas rokasgrāmatas			✓	IEEE/EIA J-STD-016 (5.13.8.)
6.4.1.	Programmatūras ievad-izvades rokasgrāmata			✓	IEEE/EIA J-STD-016 (J.2.2.)
6.4.2.	Datora darbināšanas rokasgrāmata			✓	IEEE/EIA J-STD-016 (J.2.4.)
7. Testēšanas dokumentācija					
7.1.	Programmatūras testēšanas apraksts	✓	✓	✓	LVS 70:1996; LVS 73:1996; IEEE/EIA J-STD-016 (G.2.3.); IEEE 1008; IEEE 829
7.2.	Testu projektējuma specifikācija		✓	✓	LVS 70:1996; IEEE 829
7.3.	Testpiemēru specifikācija		✓	✓	LVS 70:1996; IEEE 829
7.4.	Testēšanas procedūras specifikācija		✓	✓	LVS 70:1996; IEEE 829
7.5.	Testēšanas žurnāls	✓	✓	✓	LVS 70:1996; IEEE 829
7.6.	Problēmu ziņojumi		✓	✓	LVS 70:1996; IEEE 829; firmas problēmu reģistrācijas rīks
7.7.	Testēšanas (kopsavilkuma) pārskats	✓	✓	✓	LVS 70:1996; IEEE 829
8. Projekta iekšējo pārbaužu pārskatu dokumentācija					
8.1.	Programmatūras izstrādes plāna apskates pārskats			✓	LVS 74:1996
8.2.	Programmatūras testēšanas plāna apskates pārskats	✓	✓	✓	LVS 74:1996

8.3.	Programmatūras instalēšanas plāna apskates pārskats	✓	✓	✓	LVS 74:1996
8.4.	Programmatūras pārcelšanas (*transition*) plāna apskates pārskats			✓	LVS 74:1996
8.5.	Programmatūras projekta pārvaldības plāna apskates pārskats			✓	LVS 74:1996
8.6.	Programmatūras verifikācijas un validācijas plāna apskates pārskats			✓	LVS 74:1996
8.7.	Programmatūras konfigurāciju pārvaldības plāna apskates pārskats		✓	✓	LVS 74:1996
8.8.	Programmatūras kvalitātes nodrošināšanas plāna apskates pārskats		✓	✓	LVS 74:1996
8.9.	Datorsistēmas darbības koncepcijas apskates pārskats		✓	✓	LVS 74:1996
8.10.	Programmatūras prasību apskates pārskats	✓	✓	✓	LVS 74:1996
8.11.	Programmatūras projektējuma apskates pārskats		✓	✓	LVS 74:1996
8.12.	Testēšanas gatavības apskates pārskats			✓	LVS 74:1996
8.13.	Testēšanas rezultātu apskates pārskats		✓	✓	LVS 74:1996
8.14.	Programmatūras lietojamības apskates pārskats			✓	LVS 74:1996
8.15.	Programmatūras uzturamības apskates pārskats			✓	LVS 74:1996
8.16.	Kritisku prasību apskates pārskats		✓	✓	LVS 74:1996

17.1. DOKUMENTU ĪSS RAKSTUROJUMS

- *Apskates pārskats* ir projekta iekšējo pārbaužu dokumentēšanas forma. Tā nosaukumu parasti papildina, norādot, kāda dokumenta, kāda notikuma vai procesa apskates rezultātus tas ietver (piemēram, Programmatūras izstrādes plāna apskates pārskats).
- *Datora darbināšanas rokasgrāmatai* jānodrošina informācija, kas nepieciešama, lai darbinātu konkrēto datoru un tā perifēriskās ierīces. Šāds dokuments parasti tiek izstrādāts jauna veida datoriem, speciāla nolūka datoriem vai citiem datoriem, kuriem nav pieejamas komerciālas darbināšanas rokasgrāmatas.

- *Datora programmēšanas rokasgrāmatai* jānodrošina informācija, kas nepieciešama programmētājam, lai veiktu programmēšanu konkrētajam datoram.
- *Datu bāzu projektējuma aprakstam* jāietver informācija par datu bāzu struktūru, datu bāzes elementu funkcionālo saturu, saistīto programmatūru, informācija par prasībām, kas noteiktas datu bāzei un tās elementiem, piemēram, drošībai, integritātei, kā arī jebkura cita veida informācija, kas nepieciešama datu pārbaudei, modificēšanai u. tml.
- *Kvalitātes nodrošināšanas plānā* jāapraksta visu plānoto un sistemātisko darbību shēma, ko paredzēts veikt projekta attīstības gaitā, lai radītu pārliecību, ka programmatūras produkts atbilst iepriekš noteiktajām prasībām.
- *Lietotāja dokumentācijai* jāietver visa informācija, kas ir nepieciešama, lai produktu varētu lietot. Lietotāja dokumentācijai ir jāatbilst konkrētās programmatūras īpatnībām, tajā jābūt aprakstītam, kā tieši izpildāmas visas tās funkcijas, kuras minētas produkta aprakstā, turklāt jādod informācija par ievaddatu sagatavošanu, formātu, pieļaujamajām vērtībām, jāapraksta visas izvaddatu formas, visi ierobežojumi programmatūras darbībā u. tml. Turklāt šai dokumentācijai jābūt orientētai tieši uz lietotāju, jābūt skaidrai, viegli saprotamai un nepretrunīgai, tajā nav vēlams izmantot specifiskus programmēšanas terminus utt. Lietotāja dokumentācija ir jāsagatavo jebkurai programmatūrai un vienmēr jānodod lietotājam, t. i., tā nav vienīgais dokuments, kurš jāsagatavo un jānodod lietotājam, bet ir dokuments, kurš jāsagatavo un jānodod lietotājam vienmēr.
- *Problēmu ziņojumos* ir jādokumentē jebkurš notikums, kas gadījies testēšanas laikā, ja tam nepieciešama izpēte.
- *Programmaparatūras atbalsta rokasgrāmatai* jānodrošina informācija, kas nepieciešama, lai programmētu un pārprogrammētu sistēmas programmaparatūras (*firmware*) ierīces.
- *Programmatūras (sistēmas) izstrādes plāns* ir dokuments, kurā jādod kopskats par izstrādājamo produktu, projekta galvenajiem uzdevumiem un produkta izstrādāšanas procesu. Šajā plānā var tikt ietverti (vai arī uz tiem tiek dotas atsauces kā uz atsevišķiem dokumentiem) galveno programmatūras attīstīšanas pasākumu plāni (piemēram, konfigurācijas pārvaldības plāns, kvalitātes pārvaldības plāns).
- *Programmatūras darbības koncepcijas apraksts* ir dokuments, kurā aprakstīts esošās sistēmas mērķis, darbības principi un iespējas, dots pamatojums sistēmas modificēšanai vai jaunas sistēmas izstrādāšanai un norādīti jaunās (izstrādājamās) sistēmas darbības pamatprincipi. Šajā dokumentā jādod arī piedāvātās sistēmas novērtējums salīdzinājumā ar citiem iespējamiem risinājumiem, kā arī jānovērtē, kādu ietekmi šādas sistēmas izstrādāšana atstās uz tās organizācijas un personāla darbību, kurā paredzēts sistēmu lietot.
- *Darbības koncepcijas apraksts* ir pirmais dokuments, uz kura pamata pasūtītājs un izstrādātājs vienojas par pamatprasībām, kurām izstrādājamai sistēmai jāatbilst. Šī dokumenta izstrādāšanā ir aktīvi jāpiedalās pasūtītājam. Turpmākā izstrādes gaitā detalizētās prasības tiek vērtētas pēc atbilstības šai koncepcijai. Ja darbības koncepcijas aprakstu izstrādā kā atsevišķu dokumentu, pēc abu pušu vienošanās tas var būt projekta iekšējais dokuments vai arī tikt nodots pasūtītājam.

- *Programmatūras ievadizvades rokasgrāmata* informē lietotāju par to, kā veikt datu ievadīšanu, kādus izvaddatus iespējams saņemt un kā tie interpretējami. Parasti šādas rokasgrāmatas jāizstrādā programmatūrai, kas paredzēta darbināšanai centralizētos datorcentros (datoru operatoru vajadzībām).
- *Programmatūras instalēšanas apraksts* jāsagatavo gadījumos, kad programmatūras pirmreizējo vai atkārtoto instalēšanu veic programmatūras lietotājs. Aprakstā jāietver konkrētās produkta versijas instalēšanas instrukcijas, nepieciešamā vide (*environment*), personāla apmācīšana, kā arī jebkura cita informācija, kas nepieciešama, lai programmatūru sagatavotu darbināšanai.
- *Programmatūras instalēšanas plānā* jāparedz aparatūras un programmatūras sagatavošana, lietotāja apmācīšana, kā arī visi citi pasākumi, kuri nepieciešami, lai lietotājs varētu sākt darbināt programmatūru tai paredzētajā vietā.
- *Programmatūras izstrādes datne* ir krātuve, kurā glabājas visi materiāli, kuri ir saistīti ar programmatūras izstrādi (piemēram, apsvērumi un ierobežojumi attiecībā uz prasību definēšanu, testu informācija, plānu un stāvokļa informācija utt.).
- *Programmatūras konfigurācijas pārvaldības plānā* jāapraksta, kādi programmatūras konfigurācijas pārvaldības (PKP) pasākumi jāveic projekta izstrādāšanas laikā, kā tie jāveic, kas ir atbildīgs par konkrēto pasākumu veikšanu, kad tiem jānotiek un kādi resursi ir nepieciešami. Ar konfigurācijas pārvaldību saprot disciplīnu, kas izmanto tehniskus un administratīvus rīkojumus un uzraudzību, lai veiktu projekta un izstrādājamā produkta elementu identificēšanu, šo elementu izmaiņu vadību, stāvokļa uzskaiti, kā arī konfigurācijas auditēšanu un apskati.
- Programmatūras pārcelšanas *(transition)* plānā jāparedz programmatūras lietošanas vietā nepieciešamā aparatūra un programmatūra, kā arī jāapraksta procedūra, kā programmatūra tiek nodota lietošanai.
- *Programmatūras pirmkodi* ir programmu teksti, kas izpildīti izvēlētās realizācijas apkārtnes noteiktā veidā (piemēram, konkrētā programmēšanas valodā).
- *Programmatūras prasību specifikācijā* tiek aprakstītas detalizētas prasības katram programmatūras vienumam. Tas ir galvenais dokuments, kuram atbilstoši turpmākajā izstrādes gaitā tiek veikta programmatūras testēšana. Prasību specifikācija tiek sagatavota jebkura programmatūras projekta izstrādes gaitā, ja vien nav citi īpaši līguma noteikumi. Parasti tas ir projekta iekšējais dokuments, taču pēc abu pušu vienošanās tas var tikt arī nodots pasūtītājam.
- *Programmatūras produkta apraksta* galvenais uzdevums ir sniegt lietotājam (vai potenciālam lietotājam) precīzu informāciju par produkta piegādātāju (vai izstrādātāju) un koncentrētu priekšstatu par produktu, tā galvenajām iespējām (bez dziļas funkcionālas detalizācijas), kā arī par prasībām, kas tiek izvirzītas programmatūras funkcionēšanas videi. Tajā ir jādod arī īsa informācija par to, kādus atbalsta vai uzturēšanas pasākumus piedāvā produkta piegādātājs (vai izstrādātājs) un kādā veidā tiek sniegta informācija par produkta attīstību.

Lietotājs var izmantot produkta aprakstu, lai novērtētu produkta piemērotību savām prasībām. Produkta aprakstu var izmantot arī produkta testēšanā, lai pārbaudītu, vai produkta īpašības atbilst visiem šajā aprakstā minētajiem apgalvojumiem. Ja produkta apraksts tiek sagatavots, tas vienmēr ir nododamais dokuments.

- *Programmatūras projektējuma apraksta* forma un apjoms ir atkarīgs no izstrādājamās programmatūras rakstura un līguma noteikumiem. Projektējumu var izstrādāt vairākos posmos (vairākos līmeņos), īpaši var tikt veikta datu bāzu vai saskarnes *(interface)* projektēšana u. tml. Projektējumu pārbauda atbilstoši prasību specifikācijai. Parasti tas ir projekta iekšējais dokuments, taču pēc abu pušu vienošanās to var arī nodot pasūtītājam.
- *Programmatūras testēšanas aprakstā* jāapskata testu sagatavošana, testpiemēri un testēšanas procedūras, kas nosaka, kā veikt programmatūras elementa, sistēmas vai apakšsistēmas testēšanu.
- *Programmatūras testēšanas plānā* jāietver projekta izstrādes laikā veicamo testēšanas pasākumu kalendārais plāns, kā arī jāapraksta šo pasākumu darbības sfēra, izvēlētā pieeja, resursi u. c. Jāidentificē testējamie vienumi, raksturiezīmes, kuras jātestē, testēšanas uzdevumi, kas jāizpilda, personāls, kurš ir atbildīgs par katru uzdevumu, un risks, kas ir saistīts ar plānu.
- *Programmatūras uzturēšanas rokasgrāmatai* ir jānodrošina tā programmatūras uzturēšanai nepieciešamā informācija, kas nav atrodama programmatūras (sistēmas) projektējuma aprakstā, programmatūras produkta aprakstā vai kādā citā projekta gaitā izstrādātā dokumentā. Katrai konkrētai programmatūrai jānosaka tās uzturēšanai nepieciešamās rokasgrāmatas un jāsagatavo tikai tās. Uzturēšanas rokasgrāmatas sagatavo to darbinieku vajadzībām, kuri atbilstoši līguma noteikumiem veic programmatūras uzturēšanu.
- *Programmatūras verifikācijas un validācijas plāns* apraksta visus plānotos verifikācijas un validācijas pasākumus, kurus paredzēts veikt projekta attīstības gaitā. Verifikācija ir process, kurā nosaka, vai produkts attiecīgajā izstrādes fāzē atbilst iepriekšējās fāzes izvirzītajām prasībām, t. i., vai pāreja no fāzes uz fāzi notikusi korekti. Validācija ir process izstrādes beigu fāzē. Tā gaitā var pārliecināties, vai galaprodukts atbilst visām tam uzstādītajām prasībām, t. i., vai radīts tas, kas vajadzīgs.
- *Programmatūras versijas apraksta* galvenais uzdevums ir sniegt lietotājam (vai potenciālam lietotājam) precīzu informāciju par konkrēto produkta versiju, kas ir izstrādāta kārtējo izmaiņu rezultātā, atbilstoši konkrētai produkta lietošanas vietai (piemēram, organizācijas katras filiāles vajadzībām) u. tml. Versijas aprakstā ir precīzi jāuzskaita visi elementi, kuri ietilpst šīs versijas sastāvā (dokumenti, programmas utt.), norādot katra elementa identifikatoru, laidienu un cita veida informāciju. Tajā jāapraksta šīs versijas būtiskās atšķirības no iepriekšējās versijas un datu īpatnības, kā arī jāsniedz visa cita šai versijai unikālā informācija.
- *Projekta dienasgrāmata* ir veidlapu, tabulu un citu formu apkopojums. Tas izmantojams par palīglīdzekli, lai uzkrātu pilnīgu un vienotu kopējo informāciju par projekta stāvokli un attīstību visa tā dzīves cikla laikā. Dienasgrāmatā jāatspoguļo projekta dinamika, vispārīgās ziņas par projekta

izpildes pamatnoteikumiem un līgumslēdzēja pusēm, jāfiksē visas būtiskās izmaiņas, kā arī jebkura cita informācija, kas projekta attīstības gaitā var interesēt kā projekta vadību, tā arī pasūtītāju.

- *Projekta iekšējo pārbaužu plānā* jāapraksta projekta attīstīšanas laikā paredzētās iekšējās pārbaudes (apskates un auditēšanas), to īstenošanas procesi, kā arī specifiskās procedūras, kas nepieciešamas apskates un auditēšanas izpildei.
- *Projekta pārvaldības plānā* (standarts LVS 67:1996) jānosaka projekta tehniskās un pārvaldības funkcijas, pasākumi un uzdevumi, kas nepieciešami, lai apmierinātu projekta līgumā noteiktās prasības.
- *Sākotnējie projekta priekšlikumi* ir dokuments, kuru sagatavo pirms līguma noslēgšanas. Tā uzdevums ir potenciālajam pasūtītājam radīt priekšstatu par izpildītāja spēju apmierināt līguma prasības, par viņa iepriekšējo pieredzi, personāla kvalifikāciju, kā arī dot iespēju pārliecināties, vai izpildītājam ir pareizs priekšstats par risināmo problēmu, tās aptuveno risinājumu un programmatūras un aparatūras izmaksām.
- *Saskarņu prasību specifikācijā* jāapraksta prasības, kas tiek izvirzītas sistēmai, apakšsistēmām, aparatūrai, programmatūrai, lietotāja veiktajām darbībām vai citām sistēmas komponentēm, lai īstenotu prasīto sadarbību starp tām.
- *Saskarņu projektējuma aprakstā* jāapskata sistēmu, apakšsistēmu, aparatūras, programmatūras, lietotāja iedarbība un citu sistēmas komponentu savstarpējā sadarbība.
- *Sistēmas un/vai apakšsistēmas prasību specifikācijā* (kopā ar aparatūru) jāapraksta prasības, kas tiek izvirzītas sistēmai vai apakšsistēmai, kā arī metodes, kā pārliecināties, ka šīs prasības ir apmierinātas.
- *Sistēmas/apakšsistēmas projektējuma apraksts* (kopā ar aparatūru) atspoguļo sistēmas vai apakšsistēmas projektējumu un arhitektūru.
- *Testēšanas (kopsavilkuma) pārskatā* jāapraksta visu plānoto un izpildīto testēšanas darbību rezultātu kopsavilkums, kā arī jādod novērtējums, balstoties uz minētiem rezultātiem.
- *Testēšanas procedūras specifikācijas* uzdevums ir aprakstīt testpiemēru izpildīšanas soļus, kas nodrošina testēšanas uzdevuma izpildi (t. i., testēšanas darbību izpildes secību).
- *Testēšanas žurnālā* jāietver būtisko testa izpildīšanas detaļu hronoloģiski pieraksti.
- *Testpiemēru specifikācijā* jāapraksta katrs testpiemērs, kas definēts testu projektējuma specifikācijā.
- *Testu projektējuma specifikācijā* jāapraksta programmatūras pazīmju vai to kombināciju testēšanas pieejas detaļas un jāidentificē atbilstošie testi.

17.2. KONTROLJAUTĀJUMI

1. Kādi dokumenti ir nepieciešami programmatūras lietošanai un uzturēšanai?
2. Kādi standarti reglamentē dokumentu izstrādi?

18. PROGRAMMATŪRAS PRASĪBU SPECIFIKĀCIJA

18.1. PROGRAMMATŪRAS PRASĪBU SPECIFIKĀCIJAS IZSTRĀDE

Nodaļa izstrādāta, balstoties uz [60].

Pirms tiek uzsākta programmatūras projekta izstrāde, nepieciešams apzināt visas tās prasības, kuras pasūtītājs izvirza izstrādājamai programmatūrai. Prasību apzināšana ir jāveic ļoti nopietni, jo apkopotās prasības būs pamatā ar programmatūru saistīto prasību specifikācijas izstrādāšanai un pēc šās specifikācijas savukārt tiks izstrādāta programmatūra. Pareizi apzinātas prasības var nākotnē novērst lietotāju izvirzītas pretenzijas pret izstrādājamo sistēmu.

Programmatūras prasību specifikācija ir dokuments, kas tiek izstrādāts, iesaistoties abām pusēm – programmatūras pasūtītājam un izpildītājam. Tas nepieciešams tāpēc, ka programmatūras izstrādātājs parasti nav kompetents pasūtītāja darba procesā, bet pasūtītāja pārstāvjiem nav pieredzes programmatūras izstrādē un tāpēc tie nezina, kam jāpievērš uzmanība, izstrādājot programmatūras prasību specifikāciju.

Izstrādājot programmatūras prasību specifikāciju, ir nepieciešams ievērot standartos izvirzītās prasības. Prasību specifikāciju izstrādē visbiežāk tiek ņemtas vērā prasības, kas noteiktas vienā vai otrā standartā:

- ANSI/IEEE Std. 830-1998, IEEE Recommended Practice for Software Requirements Specification;
- LVS 68:1996, Programmatūras prasību specifikācijas ceļvedis.

Minētie standarti var tikt lietoti kā ceļveži programmatūras prasību specifikācijas izstrādē. Lietojot standartu, dokumenta izstrādātājs var nodrošināt viennozīmīgu un pilnīgu programmatūras prasību specifikāciju.

Standartā ir iekļauta programmatūras izstrādāšanas pamatprasība, kas jau iepriekš minēta šajā nodaļā, – programmatūras prasību specifikācijā ir jābūt visam konkrēti pateiktam, t. i., visām prasībām jābūt specificētām pilnīgi, jo tikai tad programmatūras prasību specifikāciju iespējams izmantot tā, kā tas iecerēts.

Izstrādājot programmatūras prasību specifikāciju, ir nepieciešams zināt tās raksturīgākās iezīmes.

- V i e n n o z ī m ī g a – katrai aprakstītajai prasībai ir tikai viena nepārprotama interpretācija.
- P a b e i g t a – ir aprakstītas visas prasības, kas saistītas ar sistēmas funkcionālajām iespējām, veiktspēju, projektēšanas ierobežojumiem, atribūtiem un ārējām saskarnēm, kā arī visas sistēmas reakcijas uz ievaddatiem (kā pareiziem, tā nepareiziem). Ir noformēts dokuments: ieliktas atsauces un apzīmējumi, sniegtas visas mērvienību un terminu definīcijas. Panākta dokumenta atbilstība PPS standartam. Aprakstītas prasības, kuras tiks precizētas laika gaitā, minēts iemesls un laiks, kad šīs prasības tiks aprakstītas.

- Verificējama – visas minētās prasības ir pārbaudāmas. Dokumentā nedrīkst būt iekļautas tādas prasības, kuras nav iespējams pārbaudīt un par kuru izpildi nevar pārliecināties.
- Nepretrunīga – dokumentā nav prasību, kuras savā starpā konfliktētu. Piemēram var minēt pretrunību datu objektā: vienā prasībā, aprakstot šo datu objektu, tiek lietotas vienas mērvienības un kritēriji, savukārt citā prasībā, veicot citas darbības ar šo pašu datu objektu, jau parādās citas mērvienības.
- Modificējama – izmaiņu ieviešana dokumenta struktūrā vai prasībās ir viegli, pilnīgi un nepretrunīgi izdarāma. Lai to panāktu, izstrādātajai dokumenta struktūrai jābūt viegli saprotamai. Dokumentā nepieciešams arī satura rādītājs un savstarpējas atsauces. Lai dokumentu būtu iespējams modificēt, jāizvairās no prasību dublēšanās. Ja dublēšanos novērst nav iespējams, tad nepieciešams nodrošināt dublētās prasības ar savstarpējām atsaucēm.
- Trasējama – ir skaidra katras prasības izcelsme un izdalīti divi trasējamības veidi: atpakaļejošā un turpejošā trasējamība.
- Lietojama darbināšanas un uzturēšanas fāzes laikā – programmatūras prasību specifikācija ir modificējama, un tajā ir iekļauti visi specifiskie apsvērumi, kuri attiecas uz atsevišķiem komponentiem.

Pastāv vairāki risinājumi, kā izstrādāt programmatūras prasību specifikāciju. Ja izstrādājamā sistēma ir apjomīga, projektējuma izstrādāšanā vienlaikus piedalās vairāki darbinieki. Prasību par vairāku darbinieku piedalīšanos var izvirzīt arī pasūtītājs kontraktā. PPS izstrādāšanai iespējams lietot īpaši izveidotus automatizācijas rīkus. Tomēr visbiežāk tiek lietoti ierastie dokumentu sagatavošanas rīki, ar kuriem iespējams nodrošināt automātisku satura, atsauču un paragrāfu veidošanu un līdz ar to izstrādāt lasāmu un pārskatāmu PPS.

Aprakstot prasības, papildus var tikt lietotas citas – netekstuālās prasību izvirzīšanas metodes. Funkcijas, kuras tiek izvirzītas prasībās, dažreiz ir efektīvāk aprakstīt, izmantojot grafiskas shēmas, matemātiskus modeļus vai piemēru kopas.

Lai izstrādātā specifikācija būtu labāka lasīšanai, iespējams dokumentā minētās prasības komentēt – aprakstīt katras prasības svarīgumu un nozīmi projektā. Komentāru klātbūtne dažreiz var palīdzēt pašiem dokumenta izstrādātājiem: neizlaižot kādu svarīgu niansi, iespējams nodrošināt viennozīmīgu un pilnu programmatūras prasību specifikāciju.

Izstrādājot programmatūras prasību specifikāciju, jāatceras, ka specifikācija nav projektējums, t. i., specifikācijā nav jāparādās sistēmas moduļu projektējumam, datu struktūras aprakstam. Specifikācija parāda tikai to, kam jābūt izstrādājamā sistēmā, nevis veidu, kā tas tiks realizēts.

18.2. PPS SATURS

Apskatīsim vienu no iespējamiem programmatūras prasību specifikācijas noformēšanas veidiem. Dokumenta izstrādātājs pēc savas izvēles var organizēt dokumentā minētās konkrētās prasības.

1. Ievads
    1.1. Nolūks
    1.2. Darbības sfēra
    1.3. Definīcijas, akronīmi un saīsinājumi
    1.4. Saistība ar citiem dokumentiem
    1.5. Pārskats
2. Vispārējais apraksts
    2.1. Produkta perspektīva
    2.2. Produkta funkcijas
    2.3. Lietotāja raksturiezīmes
    2.4. Vispārējie ierobežojumi
    2.5. Pieņēmumi un atkarības
3. Konkrētās prasības
    3.1. Funkcionālās prasības
        3.1.1. Funkcionālā prasība 1
            3.1.1.1. Ievads
            3.1.1.2. Ievade
            3.1.1.3. Apstrāde
            3.1.1.4. Izvade
        3.1.2. Funkcionālā prasība 2
        .....
        3.1.n. Funkcionālā prasība n
    3.2. Ārējās saskarnes prasības
        3.2.1. Lietotāja saskarne
        3.2.2. Aparatūras saskarne
        3.2.3. Programmatūras saskarne
        3.2.4. Sakaru saskarne
    3.3. Veiktspējas prasības
    3.4. Projekta ierobežojumi
        3.4.1. Atbilstība standartiem
        3.4.2. Aparatūras ierobežojumi
        .....
    3.5. Atribūti
        3.5.1. Drošība
        3.5.2. Uzturamība
        .....
    3.6. Citas prasības
        3.6.1. Datu bāze
        3.6.2. Operācijas
        3.6.3. Vietas adaptācija
Atsauces
Pielikumi
Indekss

18.3. KONTROLJAUTĀJUMI

1. Kas ir programmatūras prasību specifikācija?
2. Kā notiek programmatūras prasību specifikācijas izstrāde?

19. PROGRAMMATŪRAS PROJEKTĒJUMA APRAKSTS

19.1. PROGRAMMATŪRAS PROJEKTĒJUMA APRAKSTA IZSTRĀDE

Nodaļa izstrādāta, balstoties uz [61].

Programmatūras projektējuma apraksts pēc standarta definīcijas ir programmatūras sistēmas attēlojums, kas tiek radīts, lai atvieglotu analīzi, plānošanu, implementēšanu un lēmumu pieņemšanu. Tas ir sistēmas uzmetums vai modelis. Programmatūras projektējuma apraksts (PPA) tiek lietots kā sākotnējā vide programmatūras projektējuma informācijas izplatīšanai.

Pēc tam kad ir izstrādāta programmatūras prasību specifikācija (PPS) un tā ir atbilstoši abu iesaistīto pušu apstiprināta, tajā aprakstītās prasības nepieciešams pārnest programmatūras projektējuma aprakstā. Kā jau definīcijā teikts, specifikācijā minētās prasības aprakstā tiek attēlotas atbilstoši sistēmas izstrādes videi.

Izstrādājot PPA, nekas no jauna nav jāizgudro, jo projektējot tiek izmantotas tās prasības, kuras parādās programmas prasību specifikācijā. Projektējot tiek pieņemti lēmumi par to, kādā veidā konkrētās prasības tiks realizētas izstrādājamā sistēmā.

Projektēšanas rezultāta – programmatūras projektējuma apraksta izstrādi nosaka vairāki standarti. Latvijā biežāk tiek lietoti divi standarti:

- ANSI/IEEE Std. 1016-1998, IEEE Recommended Practice for Sowftware Design Description;
- LVS 72:1996, Ieteicamā prakse programmatūras projektējuma aprakstīšanai.

Šie standarti apraksta ieteicamo praksi programmatūras projektējuma izstrādāšanai. Tie specificē nepieciešamo informācijas saturu, iesaka programmatūras projektējuma organizatorisko formu, kā arī ietver norādījumus, kā savākt, organizēt un pasniegt projekta informāciju. Šie ieteikumi ir ievērojami neatkarīgi no projektējamās programmatūras darbības sfēras un projekta īstenošanā izmantotajiem līdzekļiem.

Viens no svarīgākajiem uzdevumiem, izstrādājot programmatūras projektējuma aprakstu, ir raudzīties, lai projektējumā būtu iekļautas visas tās prasības, kuras aprakstītas programmatūras prasību specifikācijā. Protams, projektējot sistēmu, ir sarežģīti nodrošināt visu prasību izpildi projektējumā, piemēram, prasību par datu apstrādes ātrumu tad, kad noteikts procents operāciju veikšanai konstantā laika posmā.

Programmatūras projektējuma apraksta izstrādāšanu ietekmē arī tas, cik pilnīga un viennozīmīga ir PPS. Ja PPS neatbildīs prasībām, tad arī PPA nebūs iespējams kvalitatīvi izstrādāt.

Izstrādājot projektējumu, nepieciešams aprakstīt visus veidojamās sistēmas moduļus, definēt, kādas būs moduļu saskarnes, moduļu atkarības.

Tāpat kā tiek aprakstīts moduļu projektējums, nepieciešams izstrādāt arī projektējumu datu objektiem – kādi būs sistēmas uzkrātie datu objekti, datu objektu datu tipi, datu objektu atkarības.

Programmatūras projektējuma apraksts, tāpat kā PPS, ir viens no pieprasītajiem dokumentiem programmatūras izstrādē. Programmatūras projektēšanā un implementēšanā, kā arī programmatūras uzturēšanā projektējuma apraksts tiek lietots, lai nodrošinātu sistēmas vadīšanas prasības.

Programmatūras projektējuma apraksts ir attēlojums, kā programmatūras prasību specifikācijā uzskaitītās prasības tiks translētas konkrētajā sistēmas izstrādes vidē. Pēc tam kad programmatūras projektējums ir pabeigts, dokumentā jābūt izpildītam nosacījumam – katrai PPS prasībai jābūt trasējamai uz vienu vai vairākām projektējuma entītijām. Katrai projektējuma entītijai nepieciešams aprakstīt tās svarīgākās īpašības, kā arī norādīt attiecības starp entītijām. Katras entītijas īpašības un attiecības programmatūras projektējuma apraksta vienkāršošanai tiek aprakstītas ar tipveida atribūtu kopu.

Programmatūras projektējuma aprakstu var uzskatīt par pabeigtu, ja visām aprakstā iekļautajām entītijām ir aprakstīti atribūti. Projektējuma entītijas rodas programmatūras sistēmas prasību dekompozīcijas rezultātā, kad sistēma tiek sadalīta komponentos, no kuriem katru atsevišķi var implementēt, mainīt un testēt, minimāli ietekmējot citas projektējuma entītijas. Projektējuma entītijas var būt sistēmas, apakšsistēmas, datu krājumi, moduļi, procesi un programmas. Izstrādājot entītijas, nepieciešams ievērot kopīgās entītiju raksturiezīmes: nosaukumu, nolūku un funkciju. Ja projektējuma entītijas savā starpā ir saistītas vai arī izmanto vienus datu objektus, tad šīs kopējās raksturiezīmes tiek aprakstītas, izmantojot projektējuma entītiju atribūtus. Programmatūras entītijas atribūts ir projektējuma entītijas raksturiezīme, kurai ir piešķirts nosaukums un kura konstatē kādu faktu par entītiju. Katrai projektējuma entītijai ir vairāki atribūti. Veidojot projektējumu, ir nepieciešams iekļaut visus atribūtus. Ja entītijai kāda atribūta aprakstīšana nav nepieciešama, tad atribūtam norāda vērtību – *nav*. Entītijai iespējami vairāki atribūti.

- Identificējums – entītijas projektējuma ietvaros izvēlēts nosaukums. Entītijas nosaukumu ieteicams veidot tā, lai no nosaukuma intuitīvi būtu nosakāma entītijas daba.
- Tips – entītijas veids. Tas var būt modulis, programma, datu objekts u. tml.
- Nolūks – entītijas eksistences iemesls. Atribūtā tiek aprakstīts, kāpēc attiecīgā entītija ir nepieciešama, un norādītas entītijas funkcionālās un veiktspējas prasības.
- Funkcija – tas, ko entītija dara. Tiek aprakstīts, ko entītija dara ar ievaddatiem, lai tos pārvērstu par izvaddatiem. Datu entītijas gadījumā atribūtā jāapraksta entītijas uzkrātās vai pārsūtītās informācijas tips.
- Pakļautība – visu to entītiju uzskaitījums, kuras tiek izmantotas attiecīgās entītijas izveidošanā *(sastāv no)*.
- Atkarības – attiecīgās entītijas un citu entītiju attiecību apraksts. Bieži šīs attiecības attēlo grafiski. Atribūtam jāapraksta entītiju mijiedarbības daba.

- S a s k a r n e – citu entītiju mijiedarbība ar attiecīgo entītiju. Atribūts apraksta metodes un likumus, kas nosaka šo mijiedarbību. Jābūt detalizēti aprakstītām mijiedarbības metodēm un līdz ar to jānorāda ievades diapazons, ievades un izvades nozīme, katrs ievades un izvades tips, formāta un izvades kļūdas.
- R e s u r s i – projektējuma ārējie elementi, kurus lieto entītija. Šis atribūts nodrošina informāciju par tādām entītijām kā fiziskās ierīces (drukātāji, diska ierīces, atmiņas bloki), programmatūras pakalpojumi (matemātiskās bibliotēkas, operētājsistēmas) un apstrādājošie resursi (centrālā procesora cikli, atmiņas iedalījums, buferi).
- A p s t r ā d e – darbības likumi, ko lieto entītija, lai veiktu funkcijas. Apstrādes atribūts apraksta darbības algoritmu, iekļaujot arī neparedzētās situācijas.
- D a t i – entītijas iekšējo datu elementi. Datu informācijai jāapraksta viss, kas attiecas uz entītijas datu lietošanu vai iekšējo datu struktūru. Tajā jāietver datu specifikācijas, piemēram, formāti, elementu skaits un sākotnējās vērtības, kā arī struktūras, kas jālieto datu attēlošanai, piemēram, datņu struktūras, masīvi, steki, rindas un atmiņas apgabali.

Nepieciešamības gadījumā entītijām var tikt papildus pievienoti arī citi atribūti.

Projektējuma informācijas sniegšana tiek organizēta, izmantojot projektējuma skatus. Projektējuma skats ir projektējuma entītijas atribūtu informācijas apakškopa, kas ir speciāli pielāgota konkrēta programmatūras projektēšanas pasākuma vajadzībām.

19.2. PPA SATURS

Standarts piedāvā programmatūras projektējuma apraksta satura rādītāju.

19.3. KONTROLJAUTĀJUMI

1. Kas ir programmatūras projektējuma apraksts?
2. Kā notiek programmatūras projektējuma apraksta izstrāde?

20. DATORPROGRAMMAS KODA NOFORMĒŠANA

Veicot programmēšanu, nepieciešams nodrošināt izstrādātā programmas koda vieglu lasāmību, kas ļauj vieglāk uztvert programmas kodā veiktās darbības, kā arī vieglāk konstatēt kļūdas šajā kodā. Ja mēs panākam, ka programmas kods ir vieglāk lasāms, tad mēs atvieglojam šī koda uzturamību, t. i., darbības, kas saistītas ar programmas koda izmaiņām. Tāpēc nepieciešams ievērot vairākus kritērijus.

Nodaļa izstrādāta, balstoties uz [53].

20.1. BIROKRĀTISKIE KOMENTĀRI

Katram no izstrādātajiem moduļiem programmas kodā ir nepieciešams ietvert t. s. birokrātisko minimumu, t. i., katrā modulī nepieciešams norādīt izstrādātāja vārdu, kontaktinformāciju, kādā veidā iespējams ar izstrādātāju kontaktēties (nepieciešams lielās kompānijās, kurās programmētāji cits citu nepazīst), moduļa beigšanas datumu, versijas numuru, kā arī to izmaiņu datumu sarakstu, kuros ir notikušas izmaiņas modulī, moduļa funkcijas aprakstu. Ja moduļa saskarnē tiek izmantoti mainīgie (moduļa izsaukšanas parametri), tad nepieciešams aprakstīt arī tos. Labs stils ir aprakstīt globālos mainīgos, kurus attiecīgais modulis izmanto, kā arī uzskaitīt citus moduļus, kurus attiecīgais modulis izsauc savas darbības laikā (taču tas nav obligāts nosacījums, jo moduļu savstarpējā saskarne jau tiek aprakstīta programmatūras projektējuma aprakstā). Programmētājiem nepieciešams arī saprāta robežās komentēt programmas kodu, lai uzlabotu šī koda lasāmību.

20.2. NEDROŠĀS PROGRAMMAS KONSTRUKCIJAS

Pirmām kārtām par šādām konstrukcijām tiek uzskatītas *goto* konstrukcijas. Kaut gan dažās programmēšanas valodās to funkcionalitāte tiek realizēta, tieši pateicoties šai konstrukcijai, programmētājiem ir ieteikts izvairīties no šīm konstrukcijām. Iespējams, ka eksistē arī citas nevēlamas programmas konstrukcijas, kuras samazina koda lasāmību un no kuru lietošanas ieteicams izvairīties.

20.3. VIENOŠANĀS PAR IZSKATU

Nepieciešams panākt vienošanos par to, kādā veidā programmas kods tiks organizēts, t. i., kā tiks izmantotas atstarpes no kreisās malas, kādas mainīgo inicializācijas būs jāveic pirms ciklu izpildes, kādā veidā tiks saukti mainīgie, kādā – moduļi. Lai organizācijā nebūtu pretenziju, programmas koda formēšanu nepieciešams aprakstīt atsevišķā dokumentā. Panākot šāda veida vienošanos programmētāju starpā, programmētājiem nebūs problēmu ar cita kolēģa

programmas kodu lasīšanu un līdz ar to vajadzības gadījumā tiks nodrošināta laba uzturamība.

20.4. NOSACĪJUMU LIMITI

Nepieciešams definēt limitu Būla *(boolean)* izteiksmju apvienošanai vienā nosacījumā, lai novērstu nepārskatāmu izteiksmju veidošanu. Nav ieteicams veidot sarežģītas loģiskās konstrukcijas, kurās bez detalizētas iedziļināšanās nav iespējams saprast šo izteiksmju vērtības.

20.5. FUNKCIONALITĀTES LIMITS MODUĻOS

Nepieciešams noteikt to funkciju limitu, kas var tikt apvienotas vienā modulī. Veidojot programmatūras projektu, ieteicams katrai programmatūras funkcijai veidot savu moduli. Šāda pieeja projekta organizēšanā ļauj vieglāk uzturēt programmatūras projektu.

20.6. GLOBĀLO MAINĪGO SKAITA LIMITS

Nepieciešams noteikt globālo mainīgo skaita limitu. Programmētājiem būtu jāierobežo globālo mainīgo nolasīšanas un mainīšanas funkcijas. Ja attiecīgajā programmatūrā ir izmantots daudz globālo mainīgo, tad prasību izmaiņu gadījumā programmētājam jāvelta liels darbs, lai caurskatītu visu kodu un ieviestu jaunās izmaiņas globālajos mainīgajos.

20.7. KONTROLJAUTĀJUMI

1. Aprakstiet prasības programmas koda noformēšanā!
2. Kādi ir ieteikumi programmēšanas procesa organizēšanai, strādājot vairākiem programmētājiem komandā?

21. TESTĒŠANA UN TESTĒŠANAS DOKUMENTĀCIJA

21.1. TESTĒŠANAS PROCESA SADALĪJUMS

Testēšanas mērķis ir atklāt programmā kļūdas. Par kļūdām programmā tiek uzskatītas ne tikai programmas izpildes kļūdas, kad programma nav spējīga dažādu iemeslu dēļ apstrādāt ieejas datus un izdod kļūdas paziņojumu. Par kļūdu var arī uzskatīt izstrādātās programmatūras neatbilstību programmatūras prasību specifikācijā aprakstītajām prasībām.

Eksistē vairāki veidi, kā tiek iedalīts testēšanas process. Viens no veidiem ir šo procesu iedalīt 4[1] dažādās testēšanas fāzēs [53]:

- vienībtestēšanā *(Unit testing)*;
- integrācijas testēšanā *(Integration testing)*;
- sistēmas testēšanā *(System testing)*;
- akcepttestēšanā *(Acceptance testing)*.

Visas iepriekš minētās testēšanas fāzes veic programmatūras izstrādātājs. Izņēmums ir vienīgi akcepttestēšana, kuru parasti veic pasūtītājs (dažreiz izpildītāja klātbūtnē).

Viens no ieteikumiem, kuru vēlams ievērot, plānojot testēšanu, ir pēc iespējas agrāka kļūdas atklāšana. Tā samazina resursu patēriņu šīs kļūdas novēršanā. Tā, piemēram, ja programmatūras izstrādes laikā ieviesusies kļūda nav pamanīta programmatūras testēšanas laikā, bet atklāta pēc programmatūras iedarbināšanas pie pasūtītāja, tās novēršana var izmaksāt daudz dārgāk nekā tad, ja tā tiktu izlabota uzreiz izstrādes laikā.

21.1.1. VIENĪBTESTĒŠANA

Vienībtestēšana (*Unit testing*) ir testēšana, kuras laikā izstrādātājs (parasti programmas koda rakstītājs) pārliecinās par to, ka programmas modulis (vienums) izpilda izvirzītās prasības [62].

Programmatūras vienībtestēšanu apraksta:

- LVS 73:1996, Programmatūras vienībtestēšana;
- *ANSI/IEEE std* 1008-1987, *IEEE Standard for Software Unit Testing*.

21.1.2. INTEGRĀCIJAS TESTĒŠANA

Integrācijas testēšana ir testēšanas fāze, kuras laikā programmatūras un/vai aparatūras sastāvdaļas tiek kombinētas un testētas, lai pārliecinātos par to savstarpējo sadarbību atbilstoši izvirzītajām prasībām. Integrācijas testēšana var turpināties, līdz visa sistēma pilnībā ir integrēta [62].

---

[1] Literatūrā tiek minēts piektais veids – pakotnes testēšana. Nav dzirdēts, ka praksē šo veidu lietotu.

21.1.3. SISTĒMAS TESTĒŠANA

Sistēmas testēšana (jeb programmatūras testēšana) ir testēšanas fāze, kuras laikā tiek pārbaudīts, vai visi programmatūras moduļi izpilda darbības, kā ir aprakstīts specifikācijā, un vai sistēma kopumā adekvāti strādā platformā, kurai tā ir izstrādāta. Sistēmas testēšanu jāveic testētājiem, kuri ir apmācīti testu sastādīšanā un izpildīšanā. Testētājiem jābūt lietas kursā par sistēmas darbības scenārijiem, kuri sistēmas gala lietotājiem var būt nezināmi, piemēram, testējot ar neaizpildītām vai pretrunīgām vērtībām. Testētājam jābūt spējīgam atkārtot soļus, kas noveduši pie programmatūras kļūdas izpaušanās [62].

21.1.4. AKCEPTTESTĒŠANA

Akcepttestēšana ir testēšanas fāze, kas tiek veikta, lai pārliecinātos, ka sistēma apmierina tās akceptēšanas kritērijus un ka pasūtītājs var akceptēt sistēmu [62].

21.2. TESTĒŠANAS DOKUMENTI

Nodaļa izstrādāta, izmantojot standartā [63] aprakstītās prasības.

Testēšanas dokuments ir testēšanas procesa laikā izstrādāts dokuments. Testēšanas laikā tiek izstrādāti dažādi dokumenti. Lielākā daļa no tiem ir savstarpēji saistīti.

- Testēšanas plāns.
- Testu projektējuma specifikācija.
- Testpiemēra specifikācija.
- Testēšanas procedūras specifikācija.
- Testējamā vienuma pavadzīme.
- Testēšanas žurnāls.
- Testa problēmas ziņojums.
- Testēšanas kopsavilkuma pārskats.

21.2.1. TESTĒŠANAS PLĀNS

Dokumenta nolūks ir noteikt darbības sfēru, pieeju, resursus un testēšanas pasākumu kalendāro plānu. Dokumentā nepieciešams identificēt testējamos vienumus, testējamās raksturiezīmes, izpildāmos testēšanas uzdevumus un noteikt atbildīgo personālu.

Dokumenta struktūra:

- testēšanas plāna identifikators,
- ievads,
- testējamie vienumi,
- testējamās raksturiezīmes,
- netestējamās raksturiezīmes,
- pieeja,
- testējamā vienuma novērtēšanas kritēriji,

- atlikšanas kritēriji un atsākšanas prasības,
- testēšanas nodevumi,
- testēšanas uzdevumi,
- vides vajadzības,
- atbildība,
- personāla komplektēšanas un apmācības vajadzības,
- kalendārais plāns,
- risks un neveiksmju sekas,
- apstiprinājumi.

Minētajiem nodalījumiem jābūt sakārtotiem norādītajā secībā. Ir arī iespējams kādus no tiem ietvert atsevišķā dokumentā, un tādā gadījumā testēšanas plānam attiecīgajā nodaļā tiek pievienota atsauce uz šo dokumentu.

Turpinājumā dokumenta struktūras daļas izklāstītas detalizētāk.

Testēšanas plāna identifikators. Nodaļā tiek specificēti unikāli testēšanas plāna identifikatori.

Ievads. Nepieciešams sastādīt testējamo programmatūras vienumu un raksturiezīmju kopsavilkumu. Augstākā līmeņa testēšanas plānā jāievieto šādas norādes: projekta pilnvarojums, projekta plāns, kvalitātes nodrošināšanas plāns, konfigurācijas pārvaldības plāns, būtiskā politika, būtiskie standarti.

Testējamie vienumi. Nepieciešams norādīt vienumus, kuri tiek testēti. Nedrīkst aizmirst norādīt testējamo vienumu versijas. Tāpat jānorāda prasības attiecībā uz testējamās programmatūras darbināšanas vidi. Šajā nodaļā tiek liktas atsauces uz testēšanā izmantotajiem dokumentiem: programmatūras prasību specifikāciju, projektējuma specifikāciju, lietotāja ceļvedi, programmatūras darbināšanas ceļvedi, instalācijas ceļvedi. Šajā nodaļā var tikt arī identificēti tie vienumi, kuri netiek testēti.

Testējamās raksturiezīmes. Šeit tiek identificētas visas programmas raksturiezīmes, kuras nepieciešams testēt. Jāidentificē testēšanas projekta specifikācija, kas ir saistīta ar katru raksturiezīmi un raksturiezīmju kombināciju.

! *Piemērs testējamām raksturiezīmēm varētu būt šāds: datu ievades laukos tiek ievadīta informācija, kas pārsniedz ievadāmās vērtības garumu (skaitļiem tās varētu būt datu tipu vērtību robežas, datumiem – dažādi ievades formāti) un neatbilst ievadāmās vērtības datu tipam (mēģinot skaitļu ievades laukos ievadīt burtus, vairākus decimālatdalītājus).*

Netestējamās raksturiezīmes. Šeit tiek aprakstītas visas netestējamās raksturiezīmes, kā arī to netestēšanas iemesli.

Pieeja. Nepieciešams precīzi aprakstīt testēšanas pieeju, lai garantētu to, ka konkrētās raksturiezīmes tiks pietiekami testētas. Pēc iespējas precīzāk aprakstīta pieeja spēj identificēt galvenos testēšanas uzdevumus, ļaujot precīzāk noteikt testēšanai neieciešamos termiņus. Nepieciešams aprakstīt testēšanas apjomu, kā arī noteikt, kā iespējams novērtēt testēšanas pilnību.

Testējama vienuma novērtēšanas kritēriji. Nepieciešams specificēt kritērijus, uz kuriem balstoties iespējams noteikt, vai testējamais vienums izturējis testēšanu vai ne.

Atlikšanas kritēriji un atsākšanas prasības. Nepieciešams aprakstīt kritērijus, kas nosaka, kādos gadījumos testēšana ir jāpārtrauc. Jāapraksta testēšanas darbības, kuras atkārtoti jāveic, testēšanu atsākot.

Testēšanas nodevumi. Nepieciešams norādīt nododamos dokumentus. Tie varētu būt šādi: testēšanas plāns, testu projektējuma specifikācija, testpiemēru specifikācijas, testēšanas procedūras specifikācija, testējamā vienuma pavadzīmes, testēšanas žurnāli, testa problēmu ziņojumi, testēšanas kopsavilkumu pārskati, testa ievaddati un izvaddati. Papildus var tikt izveidots un nodots dokuments, kurā būtu norādes uz izmantotajiem testēšanas rīkiem.

Testēšanas uzdevumi. Nepieciešams aprakstīt uzdevumus testēšanas sagatavošanā un testēšanas veikšanā. Jāapraksta testēšanas uzdevumu savstarpējās atkarības. Ja uzdevumu veikšanai ir nepieciešama papildu prasme, tad arī to ir nepieciešams aprakstīt.

Vides vajadzības. Nepieciešams aprakstīt prasības par testēšanas vidi, t. i., prasības par aparatūru, sakaru sistēmām, lietošanas režīmiem. Nepieciešams norādīt vajadzīgos speciālos testēšanas rīkus.

Atbildība. Nepieciešams norādīt personu grupas, kuras atbildīgas par pārvaldīšanu, projektēšanu, sagatavošanu, izpildīšanu, apliecinājumu, kontrolēšanu un izlemšanu. Tāpat nepieciešams norādīt grupas, kuras atbildīgas par testējamo vienumu nodrošināšanu, un grupas, kuras atbildīgas par vides prasību nodrošināšanu.

Personāla komplektēšanas un apmācīšanas vajadzība. Nepieciešams aprakstīt vajadzīgo personāla prasmju līmeni, kā arī norādīt iespējamos apmācības variantus, kas jāveic, lai personālam būtu nepieciešamais prasmju līmenis.

Kalendārais plāns. Jānorāda laiks, kas nepieciešams katra testēšanas uzdevuma izpildīšanai. Katram testēšanas uzdevumam jāidentificē resursa darbības periods.

Risks un neveiksmju sekas. Nepieciešams aprakstīt testēšanas plāna riska pakāpi, kā arī noteikt neveiksmju novēršanas veidus.

Apstiprināšana. Dokumenta beigās jānorāda personas, kuras šo plānu apstiprina.

21.2.2. TESTU PROJEKTĒJUMA SPECIFIKĀCIJA

Nolūks. Dokumenta nolūks ir aprakstīt detalizētas testēšanas pieejas un identificēt testējamās raksturiezīmes.

Dokumenta struktūra. Testu projektējuma specifikācijas struktūra ir šāda:

- testu projektējuma specifikācijas identifikators,
- testējamās raksturiezīmes,
- pieejas detalizēšana,

- testu identifikācija,
- raksturiezīmes novērtēšanas kritēriji.

Nodalījumi dokumentā uzdodami noteiktā secībā. Ja kāds nodalījums ir pārnests atsevišķā dokumentā, tad attiecīgajā vietā liekama atsauce uz šo dokumentu. Turpinājumā tiek sniegts nodalījumu sīkāks apraksts.

Testu projektējuma specifikācijas identifikators. Katrai testu projektējuma specifikācijai tiek piešķirts unikāls identifikators. Gadījumos, kad tas nepieciešams, tiek piešķirtas atsauces uz saistīto testēšanas plānu.

Testējamās raksturiezīmes. Nepieciešams aprakstīt visas raksturiezīmes un testējamos vienumus. Katrai raksturiezīmei jāiekļauj atsauce uz vienuma prasību specifikāciju.

Pieejas detalizēšana. Nepieciešams sniegt testēšanas plānā aprakstītās pieejas detalizāciju. Jāiekļauj lietojamās specifiskās testēšanas metodes, jāidentificē testa rezultātu analizēšanas metode. Jāapraksta jebkuras analīzes rezultāti, kas nodrošina racionālu testpiemēru atlasi. Jādod testpiemēru kopīgo atribūtu kopsavilkums. Tajā var tikt iekļauti ievades ierobežojumi, kuriem jābūt spēkā attiecībā uz katru testa piemēru kopu.

Testa identifikācija. Jāuzrāda testa identifikators un īsi jāapraksta katrs testpiemērs.

Raksturiezīmes novērtēšanas kritēriji. Nepieciešams norādīt kritērijus, uz kuriem balstoties iespējams noteikt, vai raksturiezīme ir izturējusi vai nav izturējusi pārbaudi.

21.2.3. TESTPIEMĒRA SPECIFIKĀCIJA

Nolūks. Dokumenta nolūks ir definēt testpiemērus, kuri identificēti testu projektējuma specifikācijā.

Struktūra:

- testpiemēra specifikācijas identifikators,
- testējamie vienumi,
- ievades specifikācijas,
- izvades specifikācijas,
- vides vajadzības,
- speciālās procedurālās prasības,
- starppiemēru atkarības.

Nodalījumiem jābūt sakārtotiem norādītajā secībā. Ja kāds nodalījums ir pārnests atsevišķā dokumentā, tad attiecīgajā nodalījumā liekama atsauce uz šo dokumentu. Turpinājumā sniegti visu satura detaļu paskaidrojumi.

Testpiemēru specifikācijas identifikators. Tiek piešķirts unikāls identifikators visām testpiemēru specifikācijām.

Testējamie vienumi. Tiek identificēti un aprakstīti vienumi un raksturiezīmes, kas attiecīgajā testpiemērā tiek pārbaudītas. Katram vienumam jādod atsauces uz šādiem dokumentiem: programmatūras prasību specifikāciju, projektējuma specifikāciju, lietotāju ceļvedi, darbināšanas ceļvedi, instalācijas ceļvedi.

Ievades specifikācijas. Jāapraksta visi datu ievades stāvokļi, kas nepieciešami, lai izpildītu attiecīgo testa piemēru, – datu vērtības, datu bāzes stāvoklis u. c.

Izvades specifikācijas. Jāapraksta visas izvades un raksturiezīmes, kas tiek prasītas testa vienumiem. Katrai izvadei jādod precīza rezultāta vērtība.

Vides prasības. Jāapraksta aparatūras un tās konfigurācijas prasības, kā arī programmatūra, kas nepieciešama testpiemēru veikšanai. Turklāt var tikt norādītas papildus izvirzītās prasības, piemēram, prasības par specifiskām personāla zināšanām.

Speciālās procedurālās prasības. Jāidentificē speciālās prasības testēšanas procedūrām, piemēram, speciālu testējamo vienumu uzstādīšana.

Atkarība starp piemēriem. Jāsastāda saraksts ar testpiemēriem, kuri izpildāmi pirms konkrētā testpiemēra. Jāapraksta atkarība starp testpiemēriem.

21.2.4. TESTĒŠANAS PROCEDŪRAS SPECIFIKĀCIJA

Nolūks. Dokumenta nolūks ir specificēt vienumu analīzes soļus (testpiemēru kopas izpildīšanas soļus), lai novērtētu raksturiezīmju kopu.

Struktūra:

- testēšanas procedūras specifikācijas identifikators,
- nolūks,
- speciālās prasības,
- procedūras soļi.

Nodalījumiem jābūt sakārtotiem norādītajā secībā. Ja kāds nodalījums ir pārnests atsevišķā dokumentā, tad attiecīgajā nodalījumā liekama atsauce uz šo dokumentu. Turpinājumā sniegti visu satura detaļu paskaidrojumi.

Testēšanas procedūras specifikācijas identifikators. Katrai testēšanas procedūras specifikācijai tiek piešķirts unikāls identifikators.

Nolūks. Jāapraksta procedūras nolūks. Ja šī procedūra paredzēta testpiemēru izpildīšanai, tad jānorāda uz tiem. Papildus jānodrošina norādes uz būtiskām testējamo vienumu dokumentācijas sastāvdaļām, piemēram, norāde uz lietošanas procedūrām.

Speciālās prasības. Jāapraksta speciālās prasības, kuras ir nepieciešamas procedūras izpildīšanai. Šeit var tikt pievienotas prasības par personālu vai darbināšanas vidi.

Procedūras soļi. Ir iekļaujami šādi soļi: reģistrācija – jāapraksta visas speciālās metodes vai formāti, kas tiek lietoti novērojumu un problēmu reģistrācijā; uzstādīšana – jāapraksta darbību secība, kas nepieciešama procedūras izpildei; startēšana – jāapraksta procedūras uzsākšanas darbības; turpināšana – jāapraksta darbības, kuras nepieciešamas procedūras izpildes laikā; mērīšana – jāapraksta mērīšanas veidi; apturēšana – jāapraksta darbības, kuras nepieciešams izpildīt testu apturēšanai; restartēšana – jāapraksta procedūras atsākšanas darbības, lai atsāktu darbības no jebkura pārtraukšanas punkta;

beigšana – jāapraksta darbības veiksmīgām darba beigām; atjaunošana – jāapraksta darbības vides atjaunošanai; neveiksmju seku novēršana – jāapraksta darbības, kuras nepieciešams izpildīt negaidītu notikumu sākšanās laikā.

21.2.5. TESTĒJAMĀ VIENUMA PAVADZĪME

Nolūks. Dokumenta nolūks ir identificēt testēšanai nosūtītos vienumus. Tiek uzrādīta informācija par atbildīgajiem, vienumu atrašanās vietu un statusu.

Struktūra:

- pavadzīmes identifikators,
- nosūtītie vienumi,
- atrašanās vieta,
- statuss,
- apstiprinājumi.

Nodalījumiem jābūt sakārtotiem norādītajā secībā. Ja kāds nodalījums ir pārnests atsevišķā dokumentā, tad attiecīgajā nodalījumā liekama atsauce uz šo dokumentu. Turpinājumā sniegti visu satura detaļu paskaidrojumi.

Pavadzīmes identifikatori. Tiek piešķirts unikāls vienuma pavadzīmes identifikators.

Nosūtītie vienumi. Tiek uzskaitīti testējamie vienumi, kuri pašlaik nosūtīti, iekļaujot to versijas un izlaides informāciju. Nepieciešams nodrošināt atsauces uz vienumu dokumentāciju un testēšanas plānu attiecībā uz nosūtītajiem vienumiem. Jāuzrāda atbildīgais personāls.

Atrašanās vieta. Jāidentificē nosūtīto vienumu atrašanās vieta.

Statuss. Jāapraksta nosūtīto testējamo vienumu statuss. Jāiekļauj novirzes no testējamo vienumu dokumentācijas, no iepriekšējā šo vienumu nosūtījuma. Jāuzrāda to problēmu ziņojumi, kuras būtu jāatrisina nosūtītajiem vienumiem.

Apstiprinājumi. Jānorāda personas, kuras apstiprinās šo dokumentu, jānodrošina vieta parakstiem un datumiem.

21.2.6. TESTĒŠANAS ŽURNĀLS

Nolūks. Žurnāla nolūks ir nodrošināt būtisko testa izpildīšanas detaļu hronoloģisko secību.

Struktūra:

- testēšanas žurnāla identifikators,
- apraksts,
- darbību un notikumu pieraksts.

Nodalījumiem jābūt sakārtotiem norādītajā secībā. Ja kāds nodalījums ir pārnests atsevišķā dokumentā, tad attiecīgajā nodalījumā liekama atsauce uz šo dokumentu. Turpinājumā doti visu satura detaļu paskaidrojumi.

Testēšanas žurnāla identifikators. Katram testēšanas žurnālam tiek piešķirts unikāls identifikators.

Apraksts. Jāidentificē testēšanas vienumi, jānorāda atsauce uz vienuma pavadzīmi, ja tāda eksistē. Jānorāda visi atribūti, kas ietekmē testēšanu (reģionālie iestatījumi, operatīvās atmiņas apjoms, izmantotās programmatūras versijas u. tml.).

Darbības un notikumu pieraksti. Katram notikumam norāda datumu, autoru. Nepieciešamības gadījumā var aprakstīt testa izpildīšanas procesu. Jāapraksta procedūras izpildes rezultāti un dažādi paziņojumi. Jāapraksta vides nosacījumi, kā arī anomālu notikumu gadījumā jāapraksta darbības pirms šiem notikumiem un pēc tiem. Katram problēmu ziņojumam jāpievieno tā identifikators.

21.2.7. TESTA PROBLĒMAS ZIŅOJUMS

Nolūks. Dokumenta nolūks ir uzskaitīt jebkurus testēšanas gaitā konstatētos notikumus, kuri prasa papildu izpēti.

Struktūra:
- testa problēmas ziņojuma identifikators,
- kopsavilkums,
- problēmas apraksts,
- iespaids.

Nodalījumiem jābūt sakārtotiem norādītajā secībā. Ja kāds nodalījums ir pārnests atsevišķā dokumentā, tad attiecīgajā nodalījumā liekama atsauce uz šo dokumentu. Turpinājumā sniegti visu satura detaļu paskaidrojumi.

Testa problēmas ziņojuma identifikators. Katram testa problēmas ziņojumam tiek piešķirts unikāls identifikators.

Kopsavilkums. Tiek noformēts problēmas kopsavilkums, kurā tiek identificēti testējamie vienumi, norādīta to versijas informācija. Ieteicams pievienot norādes uz attiecīgo testēšanas procedūras specifikāciju, testpiemēra specifikāciju un testēšanas žurnālu.

Problēmas apraksts. Katrai problēmai tiek pievienots apraksts, kurā varētu būt šādi vienumi: ievade, gaidāmie rezultāti, faktiskie rezultāti, anomālijas, datums un laiks, procedūras soļi, vide, mēģinājumi atkārtot, testētāji, novērotāji. Katrā ziņā šajā nodalījumā ir jācenšas sniegt pēc iespējas plašāku informāciju, lai spētu problēmu novērst.

Iespaids. Ja ir zināms, tad jānorāda, kā šī problēma ietekmē testēšanas plānu, testu projektējuma specifikācijas vai testpiemēru specifikācijas.

21.2.8. TESTĒŠANAS KOPSAVILKUMA PĀRSKATS

Nolūks. Jāveido plānoto testēšanas darbību rezultātu kopsavilkums un jānodrošina novērtējums, bāzējoties uz minētajiem rezultātiem.

Struktūra:
- testēšanas kopsavilkuma pārskata identifikators,
- kopsavilkums,
- novirzes,

- aptvēruma novērtējums,
- rezultātu kopsavilkums,
- novērtējums,
- darbību kopsavilkums,
- apstiprinājumi.

Nodalījumiem jābūt sakārtotiem norādītajā secībā. Ja kāds nodalījums ir pārnests atsevišķā dokumentā, tad attiecīgajā nodalījumā liekama atsauce uz šo dokumentu. Turpinājumā sniegti visu satura detaļu paskaidrojumi.

Testēšanas kopsavilkuma pārskata identifikators. Katram testēšanas pārskatam tiek piešķirts unikāls identifikators.

Kopsavilkums. Jādod testējamo vienumu novērtējuma kopsavilkums. Jāidentificē testētie vienumi, norādot versijas informāciju. Jāuzrāda vide, kurā veiktas testēšanas darbības. Katrs testēšanas vienums jānodrošina ar atsaucēm uz šādiem dokumentiem: testēšanas plānu, testu projektējuma specifikāciju, testēšanas procedūras specifikācijām, testējamo vienumu pavadzīmēm, testēšanas žurnāliem un testa problēmu ziņojumiem.

Novirzes. Jāziņo par katru testējamā vienuma novirzi no tā projektējuma specifikācijas. Jāparāda novirze no testēšanas plāna, testu projektējuma vai testēšanas procedūrām. Jānorāda novirzes cēloņi.

Aptvēruma novērtējums. Jānovērtē testēšanas procesa aptvērums salīdzinājumā ar testēšanas plānā specificētajiem aptvēruma kritērijiem.

Rezultātu kopsavilkums. Jāidentificē visas atrisinātās problēmas un jādod to atrisinājumu kopsavilkums, jāuzskaita neatrisinātās problēmas.

Novērtējums. Jānodrošina katra testējamā vienuma novērtējums, iekļaujot tā ierobežojumus. Novērtējumam jābalstās uz testa rezultātiem un testa vienumu novērtēšanas kritērijiem.

Darbības kopsavilkums. Jādod kopsavilkums svarīgākajiem testēšanas kritērijiem un darbībām. Jādod kopsavilkums par izmantotajiem resursiem.

Apstiprinājums. Jānorāda personas, kuras apstiprina šo pārskatu, kā arī jānodrošina parakstu un datumu vietas.

21.3. KONTROLJAUTĀJUMI

1. Nosauciet standartus, kuri nosaka testēšanas procesu vai tā rezultātus!
2. Nosauciet iespējamos testēšanas dokumentus!
3. Aprakstiet katra testēšanas dokumenta nolūku un struktūru!

22. LIETOTĀJA DOKUMENTĀCIJA

Nodaļa izstrādāta, balstoties uz [64].

Lietotāja dokumentācija ir palīgs lietotājam darbā ar sistēmu. Dokumentācijai jāsatur visa tā informācija, kas ir nepieciešama, lai produktu varētu lietot. Lietotāja dokumentācijai ir jāatbilst konkrētās programmatūras īpatnībām, tajā jābūt aprakstītam, kā tieši izpildīt visas tās funkcijas, kuras minētas produkta aprakstā, jādod arī informācija par ievaddatu sagatavošanu, formātu, pieļaujamām vērtībām, jāapraksta visas izvaddatu formas, visi ierobežojumi programmatūras darbībā u. tml. Turklāt šai dokumentācijai jābūt orientētai tieši uz lietotāju, jābūt skaidrai, viegli saprotamai un nepretrunīgai, tajā nav vēlams izmantot specifiskus programmēšanas terminus utt. Lietotāja dokumentācija ir jāsagatavo jebkurai programmatūrai un vienmēr jānodod lietotājam, t. i., tā nav vienīgais dokuments, kas jāsagatavo un jānodod lietotājam, bet ir dokuments, kas jāsagatavo un jānodod lietotājam vienmēr.

Prasības lietotāja dokumentācijas izstrādāšanā izvirza šādi standarti:

- LVS 66:1996, Programmatūras lietotāja dokumentācija;
- ANSI/IEEE std. 1063-2001, *IEEE Standard for Software User Documentation.*

Nodaļas turpinājumā apskatītas LVS standarta izvirzītās prasības par dokumenta saturu un formu.

Standarts tiek attiecināts tikai uz tādu dokumentāciju, kas palīdz sistēmas lietošanā, uzstādīšanā, pārvaldīšanā. Standarts neattiecas uz dokumentiem, kuri saistīti ar programmatūras pirmkodu modificēšanu.

Pirms uzsāk lietotāja dokumentācijas izstrādāšanu, ir vērts vienoties par standartā minētajiem apzīmējumiem, kurus ir nepieciešams pareizi lietot, izstrādājot dokumentāciju. Tā standartā dokumenta hierarhiski pakārtotas teksta sastāvdaļas apzīmē šādi:

- Nodalījums (1. līmenis);
- Nodaļa (2. līmenis);
- Sadaļa (3. līmenis);
- Paragrāfs (4. līmenis);
- Punkts (5. līmenis);
- Apakšpunkts (6. līmenis).

Lai noteiktu, kādi dokumenti ir nepieciešami, jāapraksta programmatūras produkta lietotāji, dokumentu lietošanas veids (instrukcijas vai izziņas veids) un jānosaka dokumentu komplekts. Dokumenta lietošanas veids norāda uz informācijas organizēšanu lietotāja dokumentācijā. Instruējoši dokumenti tiek orientēti uz informāciju vai uz uzdevumu (klasisks piemērs ir darbību apraksts, lai sasniegtu kaut kādu mērķi). Turpretī informatīvi dokumenti tiek orientēti informācijas ātras ieguves nodrošināšanai (piemēram, informatīvs dokuments varētu būt kļūdu ziņojumu rokasgrāmata, kurā katram kļūdas ziņojumam ir pievienots apraksts un ar kuru lietotājs strādā, meklējot aprakstu pēc kļūdas ziņojuma identifikatora).

22.1. LIETOTĀJA DOKUMENTĀCIJAS SATURS

Lietotāja dokumentācijā obligāti ir jāiekļauj šādi komponenti (izņemot gadījumus, kad informācija nav piemērojama):

- titullapa – dokumenta nosaukums, versija un datums, aprakstāmās programmatūras nosaukums, versija, izdevējorganizācijas dati,
- ierobežojumi – jāapraksta noteiktie ierobežojumi attiecībā uz dokumenta kopēšanu,
- garantijas – jāuzrāda garantijas vai līgumsaistības, vai arī atteikšanās no tām,
- satura rādītājs,
- ilustrāciju saraksts,
- ievads – ievadā tiek sniegts auditorijas raksturojums, lietojamība, dokumenta nolūks, dokumenta lietošanas apraksts (tas, kas katrā dokumenta nodaļā tiek aprakstīts). Nepieciešams norādīt saistītos dokumentus, kuri ir lietojami kopā ar lietotāja dokumentāciju. Ir nepieciešams detalizēti aprakstīt pieņemtos apzīmējumus un stilistiskās norunas, jo tās ir pāreja no datoru terminoloģijas uz lietotājam saprotamu valodu. Jāsniedz informācija par sistēmā konstatēto problēmu ziņošanu,
- dokumenta pamatteksts – dokumenta pamatteksta noformēšana tiek sniegta tālāk,
- kļūdu situācijas – jāapraksta kļūdu ziņojumi, kādās situācijās tie notiek, kādā veidā iespējams no kļūdu situācijām izkļūt,
- atsauces – nepieciešams norādīt visas tekstā minētās publikācijas,
- skaidrojošā vārdnīca – jādod visu tekstā lietoto terminu, akronīmu un saīsinājumu paskaidrojums,
- alfabētiskais priekšmetu skaidrojums – jādod uz atslēgvārdiem vai jēdzieniem bāzēts priekšmetu rādītājs.

9. tabulā norādīts, kuri dokumentu komponenti ir obligāti iekļaujami lietotāja dokumentācijā atkarībā no dokumenta lappušu skaita un noformējuma vienā vai vairākos sējumos.

22.2. LIETOTĀJA DOKUMENTĀCIJAS PAMATTEKSTS

Dokumenta pamatteksta formu nosaka dokumenta veids – instrukcijas vai izziņas veids.

Instrukcijas veida lietotāja dokumentācija jāorganizē šādi:

- jāapraksta, kāda informācija lietotājam ir nepieciešama, lai veiktu darbu ar sistēmu, – paroles, ievades rokasgrāmatas u. tml.,
- jāapraksta sagatavošanās darbības pirms sistēmas lietošanas uzsākšanas, piemēram, kā reģistrēt sistēmas lietotāju, kā nodrošināt piekļuvi datu bāzei u. tml.,
- jāapraksta vispārējos pabrīdinājumus un brīdinājumus, kuri attiecas uz konkrēto uzdevumu,
- jāapraksta uzdevuma veikšanai nepieciešamās darbības – kā uzsākt darbību, kā noteikt, vai darbība beigusies veiksmīgi, kāds ir sagaidāmais rezultāts un kā uzdevuma veikšanas laikā izvairīties no kļūdām.

9. tabula

Lietotāja dokumentācijas komponentu iekļaušanas prasības

Komponents	Viensējuma dokuments		Vairāksējumu dokuments	
	<=8 lpp.	>=9 lpp.	1. sējums	Pārējie sējumi
Titullapa	O	O	O	O
Ierobežojumi	O	O	O	O
Garantijas	R	R	R	R
Satura rādītājs	N	O	O	O
Ilustrāciju saraksts	N	N	N	N
Ievads				
Auditorijas raksturojums	R	O	O	R
Lietojamība	O	O	O	O
Dokumenta nolūks	R	O	O	R
Dokumenta lietošanas apraksts	R	O	O	R
Saistītie dokumenti	R	R	R*	R
Pieņemtie apzīmējumi un vienošanās	O	O	O	R
Problēmu ziņošana	R	O	O	R
Dokumenta pamatteksts:				
instrukcijas veida teksts,	1	1	1	1
izziņas veida teksts	1	1	1	1
Kļūdu situācijas	R	R	R	R
Pielikumi	N	N	N	N
Atsauces	O	O	O**	O**
Skaidrojošā vārdnīca	O	O	O**	O**
Alfabētiskais priekšmetu rādītājs	2	2	O**	O**

O – obligāti jāiekļauj, ja informācija eksistē.
N – nav obligāti.
R – reference jeb atsauce: informācija tieši iekļaujama atsevišķā nodalījumā vai arī norādāma vieta, kur dokumentu komplektā tā būtu atrodama.
* – jānorāda saistība ar citiem sējumiem.
** – obligāti jābūt vismaz kādā no sējumiem, kur norādīts arī uz citos sējumos ietverto informāciju.
1 – ikvienā dokumentā ir pamatteksts; katrā dokumentu komplektā jābūt auditorijai nepieciešamajiem instrukcijas veida un izziņas veida dokumentiem.
2 – priekšmetu rādītājs ir obligāts dokumentiem ar apjomu 40 lpp. un vairāk.

Izziņas veida lietotāja dokumentēšana jāorganizē šādi:

- izziņas veida dokuments jānoformē tā, lai lietotājs varētu atrast viņam nepieciešamās funkcijas aprakstu, piemēram, izmantojot funkciju alfabētisko kārtojumu vai arī kārtojumu pa funkciju grupām,
- jāapraksta, kāda informācija lietotājam ir nepieciešama, lai veiktu darbu ar sistēmu, – paroles, ievades rokasgrāmatas u. tml.,

- jāapraksta sagatavošanās darbības pirms sistēmas lietošanas uzsākšanas, piemēram, sistēmas lietotāja reģistrēšana, piekļuves datu bāzei nodrošināšana u. tml.,
- jāapraksta ievaddati funkcijas korektai darbināšanai,
- jāapraksta vispārējie pabrīdinājumi un brīdinājumi, kuri attiecas uz konkrēto uzdevumu,
- jāapraksta funkcijas izsaukšana, norādot obligātos parametrus, noklusētās parametru vērtības, funkciju izsaukšanas kārtību un sintaksi,
- jāapraksta lietotāja iespējas apturēt funkcijas darbību un vajadzības gadījumā darbības atjaunošanu,
- jāapraksta uzdevuma veikšanai nepieciešamās darbības – kā uzsākt darbību, kā noteikt, vai darbība beigusies veiksmīgi, kāds ir sagaidāmais rezultāts un kā uzdevuma veikšanas laikā izvairīties no kļūdām,
- jāapraksta funkcijas izpildes izvaddati – ekrāna formas, izmaiņas datnēs vai datos. Nepieciešams aprakstīt visus iespējamos beigu rezultātus. Ja iespējami vairāki beigu rezultāti, jāapraksta to rašanās cēloņi.

22.3. KONTROLJAUTĀJUMI

1. Aprakstiet lietotāja dokumentācijas izstrādāšanā ievērojamās prasības!
2. Aprakstiet iespējamos lietotāja dokumentācijas veidus un atšķirības starp tiem!

23. PRASĪBAS PRET SASKARNI

Nodaļa izstrādāta, balstoties uz [65].

Projektējot informācijas sistēmu saskarni (*interface*), ir nepieciešams ievērot dažādas ergonomiskas prasības. Daļa no šādām prasībām ir apkopota starptautiskajā standartā *ISO 9241 – Ergonomic requirements for office work with visual display terminals*. Šis standarts ir iedalīts vairākās daļās. Dažas no šīm nodaļām veltītas ergonomikai attiecībā uz to, kā mēs šo vārdu saprotam, t. i., darbam ar datoru, datoru izvietojumam telpā utt. Taču standartā tiek aplūkotas arī citas prasības – prasības pret lietotāja saskarni, jautājumi par to, kā projektējama lietotāja saskarne, kā veidojams dialogs ar sistēmas lietotāju.

Turpinājumā pievērsīsimies tieši tām standarta nodaļām, kurās aplūkota informācijas sistēmu saskarne ar lietotājiem. Tās ir šādas:
- 10. nodaļa. Dialogu principi;
- 12. nodaļa. Informācijas pasniegšana;
- 13. nodaļa. Lietotāju vadība.

23.1. 10. NODAĻA. DIALOGU PRINCIPI

Šī standarta nodaļa apraksta informācijas sistēmu saskarnes izstrādi, kur tiktu ievēroti ergonomikas principi, un vispārējos ergonomikas principus, kuri ir atkarīgi no katra specifiska dialogu veida.

Šajā standartā aprakstītie principi var tik lietoti kā vadlīnijas, projektējot informācijas sistēmu saskarni.

Lietotāju saskarnes izstrādāšanā svarīgākie ir šādi atribūti:
- piemērotība uzdevumam (*suitability for the task*);
- pašaprakstāmība (*self-descriptiveness*);
- vadāmība (*controllability*);
- atbilstība lietotāja gaidītajam (*conformity with user expectations*);
- iecietība pret kļūdām (*error tolerance*);
- piemērotība individualizācijai (*suitability for individualization*);
- mācīšanās piemērotība (*suitability for learning*).

23.1.1. PIEMĒROTĪBA UZDEVUMAM

Lietotāja saskarne ir piemērota uzdevumam, ja tā atbalsta lietotāju uzdevuma efektīvā un racionālā izpildē.

Lietotāja saskarnei ir jāiekļauj tikai tā informācija, kas nepieciešama konkrētā uzdevuma izpildīšanai.

Palīdzības informācijai (*help information*) ir jāattiecas uz konkrēto uzdevumu.

Darbības, kuras var notikt automātiski, ir jāizpilda bez lietotāja iejaukšanās.

! *Datu ievades formā kursors, atverot formu, tiek novietots pirmajā teksta ievades laukā.*

Ievaddatu un izvaddatu formātam jābūt atbilstošam izpildāmajam uzdevumam un lietotāja prasībām.

Sistēmai ir jāatbalsta lietotājs, atkārtoti izpildot uzdevumus.

! *Pēc vienas datu ievades operācijas pabeigšanas nepieciešams ievades formu sagatavot nākamajai datu ievadei.*

Uzdevuma izpildē jāpaaugstina veiktspēja datu ievadē.

! *Ja konkrētā datu ievades laukā eksistē kāda noklusētā vērtība, tad jāparedz iespēja ātri šo noklusēto vērtību ievadīt. Tāpat jāparedz iespēja šo noklusēto vērtību vajadzības gadījumā aizstāt ar citu vērtību.*

Veicot ievaddatu maiņu, nepieciešams iepriekšējos datus saglabāt atmiņā, lai vajadzības gadījumā tos varētu atjaunot.

! *Lietotājs uzsāk datu izmaiņas, t. i., nomaina datu ievades laukos esošās vērtības pret citām. Ja uzreiz pēc ievaddatu nomaiņas lietotājam ir nepieciešams atgriezt bijušās vērtības, piemēram, nospiežot tastatūras taustiņu [Esc], tad jāatjauno iepriekšējās datu ievades lauku vērtības.*

23.1.2. PAŠAPRAKSTĀMĪBA

Lietotāja saskarne ir pašaprakstoša, ja katrs saskarnes solis ir saprotams sistēmas reakcijas dēļ vai arī uz to lietotājam ir iespējas saņemt paskaidrojumu.

Pēc katras lietotāja darbības sistēmai ir jāizdod paziņojums.

! *Pēc lietotāja veiktās datu saglabāšanas sistēmai jāizdod paziņojums par datu saglabāšanu. Ja datu dzēšanas process ir neatgriezenisks, tad pirms darbības izpildes lietotājam nepieciešams izdot paziņojumu par to, ka darbība ir neatgriezeniska.*

Sistēmas paziņojumos jālieto terminoloģija, kas ir analoģiska sistēmas formās lietotajai terminoloģijai.

! *Ja formā personas koda ievades lauka iezīme (label) tiek nosaukta par „personas kodu", tad arī sistēmas paziņojumos jālieto atbilstošs apzīmējums „personas kods".*

Sistēmas paziņojumiem jāsniedz papildu informācija par sistēmas darbību.

! *Sistēmai veicot datu saglabāšanu datu bāzē, procedūru lietotājam tiek paziņots „Dati tiek saglabāti ... Lūdzu, uzgaidiet".*

Lietotājam ir nepieciešams radīt iespēju saņemt dažāda līmeņa paziņojumus.

! *Izsaucot sistēmas palīdzību un nospiežot tastatūras taustiņu vienreiz, lietotājs saņem īsu palīdzību par konkrēto saskarni, savukārt, nospiežot tastatūras taustiņu divreiz, lietotājam tiek piedāvāta pilna palīdzība par konkrēto saskarni.*

Sistēmas paziņojumiem ir jābūt pēc iespējas vairāk paskaidrojošiem – tiem jāspēj identificēt konkrētās problēmas apgabals, mazinot lietotājam nepieciešamību izmantot lietotāja rokasgrāmatu konkrētās problēmas novēršanai.

Ja eksistē noklusētās vērtības ievadīšanas iespējas, tad lietotājam par tām ir jāzina.

Ja ir nepieciešams ievadīt kādas vērtības pirms uzdevuma tālākas izpildes, lietotājs par to ir jāinformē. Lietotāju nepieciešams informēt arī gadījumos, kad lietotājs ir ievadījis nepareizu vērtību. Šādos gadījumos lietotājam jāpaskaidro, kā ievadīt pareizu vērtību.

! *Lietotājs mēģina ievadīt sistēmā datumu, bet tas neatbilst sistēmas datuma formātam. Šādā gadījumā lietotājs jāinformē par to, kādā formātā nepieciešams datumu ievadīt.*

23.1.3. VADĀMĪBA

Saskarne ir vadāma, ja lietotājs ir spējīgs noteikt un vadīt saskarnes norādījumus un gaitu tik ilgi, kamēr tiek sasniegts rezultāts.

Saskarnes reakcijas ātrumam jābūt ierobežojamam atkarībā no lietotāja spējām.

Lietotājam ir jābūt iespējām noteikt, kā turpināt konkrēto darbību.

! *Datu ievades formās pēc viena datu ievades lauka aizpildīšanas kursors tiek pārvietots uz nākamo datu ievades lauku, tomēr lietotājam tiek saglabāta iespēja pārvietot kursoru uz citu datu ievades lauku.*

Pazūdot saskarnei ar sistēmu, ir jāparedz iespēja pēc saskarnes atjaunošanas lietotājam turpināt iesākto procesu.

! *Lietotājs veic ievadīto datu saglabāšanu datu bāzē. Saglabāšanas laikā tiek konstatēts, ka pieslēgums datu bāzei pārtrūcis. Pēc paziņojuma sistēma mēģina pieslēgties datu bāzei, un izdošanās gadījumā lietotājs var pabeigt uzsākto saglabāšanas procedūru.*

Ja darbības ir atgriezeniskas, lietotājam jābūt iespējai veikt pēdējās(-o) darbības(-u) atcelšanu.

! *Pēc datu dzēšanas lietotājam vajadzības gadījumā ir iespējams atjaunot dzēstos datus.*

Lietotājam ir iespējams mainīt ievaddatu un izvaddatu attēlošanas veidu.

! *Lietotājam ir iespējams mainīt pārskata kolonnas vietām, pielikt vai noņemt kādas kolonnas.*

Ja ir iespējams, lietotājam nepieciešams sniegt iespēju vadīt apstrādājamo datu apjomu.

! *Lietotājs ir veicis datu pieprasījumu. Ja tā izpildes laikā lietotājs konstatē, ka tālāk šo pieprasījumu izpildīt nav nepieciešams, lietotājs var apturēt tā izpildi.*

Ja eksistē alternatīvas ievadierīces un izvadierīces, lietotājam jārada iespēja izvēlēties, kuru ierīci lietot.

! *Lietotājam ir iespējas izvēlēties lietot tastatūru vai peli. Veicot datu drukāšanu, lietotājam ir iespējams izvēlēties drukas iekārtu.*

23.1.4. ATBILSTĪBA LIETOTĀJA GAIDĪTAJAM

Saskarņu uzvedībai un parādīšanās formai jābūt saskanīgai.

! *Visiem sistēmas kļūdu paziņojumiem jābūt vienādā formā. Piemēram, lai aizvērtu konkrēto formu, tiek lietota komandpoga ar vienmēr vienādu komandpogas nosaukumu.*

Darbībām sistēmas stāvokļu izmaiņai jābūt saskanīgām.

! *Tastatūras taustiņš [F1] vienmēr tiek lietots palīdzības izsaukšanai.*

Saskarnē nepieciešams lietot apzīmējumus atbilstoši tiem apzīmējumiem, kurus lietotājs izmanto uzdevumu izpildē ārpus informācijas sistēmas.

Saskarnei, lietotājam veicot līdzīgus uzdevumus, jābūt līdzīgai.

! *Lai datuma ievades laukā ievadītu noklusēto vērtību, lietotājam jānospiež tastatūras taustiņš [F12]. Lai saskarne būtu līdzīga, veicot noklusētās vērtības ievadi arī citos datu ievades laukos, jālieto tas pats tastatūras taustiņš.*

Kursoru nepieciešams novietot tajā datu ievades laukā, kurā ir nepieciešams ievadīt nākamo vērtību.

Ja sistēmas reakcijas laiks uz lietotāja veikto darbību ir ilgstošs, lietotāju par to nepieciešams informēt.

! *Ilgstošu procesu laikā lietotāju nepieciešams informēt par procesa izpildi, piemēram, peles rādītāju nomainot ar „strādā" vai arī attēlojot procesa izpildi procesa joslā (progress bar).*

23.1.5. IECIETĪBA PRET KĻŪDĀM

Saskarne ir iecietīga pret kļūdām, ja, par spīti nepārprotamām kļūdām datu ievadē, iecerētais rezultāts var tikt saņemts bez minimālām lietotāja korektīvām darbībām vai ar tām.

Sistēmai jāpalīdz lietotājam identificēt kļūdas lietotāja datu ievadē. Sistēmas saskarnei jāaizsargājas pret jebkuru lietotāja ievadi, kas varētu izraisīt kļūdu vai sistēmas darbības pārtraukšanu.

! *Sistēma kļūdainu ievaddatu gadījumā izdod paziņojumu par kļūdainiem ievaddatiem un norāda uz formātu, kādā jāievada ievaddati. Piemēram, ja ir nepieciešams ievadīt skaitli, tad saskarnei ir jābūt tādai, lai lietotājs simbolus, kas neveido skaitli, nevarētu ievadīt.*

Kļūdu paziņojumiem jābūt paskaidrojošiem, lai lietotājs varētu kļūdas novērst.

Atkarībā no sistēmas iespējām var tikt izmantota kļūdaino ievaddatu analīze.

! *Lietotājam tiek paziņots par to, kurā vietā ievaddatos ir iespējamā kļūda.*

Ja informācijas sistēma ir spējīga kļūdu novērst automātiski, ir nepieciešams par to informēt lietotāju, radot iespēju lietotājam izmantot sistēmas piedāvāto kļūdas novēršanu.

! *Teksta redaktoros plaši tiek izmantota pareizrakstības pārbaude. Gadījumos, ja vārds ievadīts kļūdaini, sistēma par to paziņo lietotājam, kā arī lietotājam ir iespējams izlabot šo kļūdu atbilstoši kādam no sistēmas piedāvātajiem pareizajiem vārdiem.*

Situācijās, kad ir pieļaujama sistēmas darbība ar kļūdām ievaddatos, ir nepieciešams radīt iespēju lietotājam šīs kļūdas novērst.

! *Lietotājam ir iespējams teksta redaktorā turpināt rakstīt dokumentu ar kļūdām, bet vajadzības gadījumā lietotājs var pa vienai kļūdai veikt dokumentā esošo kļūdu labošanu.*

23.1.6. PIEMĒROTĪBA INDIVIDUALIZĀCIJAI

Saskarne ir individualizējama, ja to var modificēt atbilstoši uzdevuma vajadzībām, individuāliem iestatījumiem vai lietotāja prasmēm.

Sistēmai jābūt izveidotai tā, lai ļautu saskarni adaptēt lietotāja valodai, kultūras prasībām, individuālām zināšanām vai pieredzei.

! *Lietotājam ir iespējams uzstādīt tādu decimāldaļas atdalītāju un datuma formātu, kāds tiek attiecīgajā reģionā lietots.*

Lietotājam ir iespējams sistēmā izveidot savu terminu vārdnīcu, kuru piekārtot sistēmā lietotajiem terminiem, tādējādi adaptējot sistēmu lietotājam ērtiem terminiem. Lietotājam ir iespējams mainīt sistēmas piedāvātos komandtaustiņus pret viņam ērtiem komandtaustiņiem.

23.1.7. MĀCĪŠANĀS PIEMĒROTĪBA

Saskarne atbalsta mācīšanos, ja tā atbalsta lietotāju un palīdz lietotājam apgūt sistēmas lietošanu.

Var tikt lietotas dažādas mācīšanās stratēģijas (mācīšanās darot, mācīšanās, izmantojot piemērus, veicinot izpratni).

! *Lietotājam neatkarīgi no procesa stāvokļa, kurā viņš atrodas, ir iespējams pārvietoties no palīdzības loga uz veicamo uzdevumu un atpakaļ. Metode „mācīšanās darot" var tikt lietota, dodot iespēju lietotājam veikt eksperimentus ar uzdevumiem.*

23.2. 12. NODAĻA. INFORMĀCIJAS PASNIEGŠANA

Šī standarta nodaļa apraksta ieteikumus, kas saistīti ar ergonomiku informācijas pasniegšanā, un specifiskas īpašības, attēlojot informāciju teksta vai grafiskā veidā. Tā sniedz rekomendācijas vizuālas informācijas pasniegšanā. Šie ieteikumi var tik lietoti projektēšanas laikā (piemēram, kā vadlīnijas saskarnes projektēšanā).

23.2.1. SNIEGTĀS INFORMĀCIJAS RAKSTURLIELUMI

Vizuālās informācijas pasniegšanai jāļauj lietotājam veikt uzdevumus, kam nepieciešama jutekliskā uztvere, jeb perceptuālus uzdevumus (piemēram, meklēt informāciju ekrānā) efektīvāk, racionālāk un ar patiku. Lai to panāktu, ir svarīgi ievērot vairākus raksturlielumus, attēlojot vizuālo informāciju. Tie ir šādi:

- skaidrība (*clarity*);
- spēja nodalīt (*discriminability*);
- koncentrētība (*conciseness*);
- nepretrunība (*consistency*);
- uztveramība (*detectability*);
- lasāmība (*legibility*);
- saprotamība (*comprehensibility*).

23.2.2. INFORMĀCIJAS ORGANIZĒŠANA

Informācijas atrašanās vieta. Informāciju nepieciešams organizēt tā, lai tā atbilstu uzdevuma nosacījumiem un lietotāju gaidītajai vietai.

Logu atbilstība. Logu lietošanas dažādība ir daudz lielāka, nekā tas uzskaitīts pie uzdevumu prasībām vai sistēmas spējām. Logus nav ieteicams lietot situācijās, ja tas var kavēt lietotāja dialogu ar sistēmu.

Uzdevumu prasības:

- lietotājs aplūko vai piekļūst vairāk nekā vienai sistēmai, lietotnei vai procesam vienlaikus;

- lietotājs apstrādā, salīdzina vai rīkojas ar informāciju no dažādiem informācijas avotiem;
- lietotājs bieži pārvietojas starp uzdevumiem, lietotnēm, skatiem vai datnēm.

Sistēmas spējas.

- Attēla lielums un izšķirtspēja: ar ekrāna izmēru saistīta izšķirtspēja ļauj lietotājam aplūkot saprātīgu daudzumu informācijas dažādos logos bez daudzkārtējas pārvietošanās starp logiem.
- Sistēmas reakcija: notiek logu izmaiņas atbilstoši pieprasītajam grafikas līmenim, lai ievērojami nesamazinātu ekrāna parametrus.

Ieteikumi logiem.

Informācijas attēlošanu vai apstrādi vairākos logos vai vienā logā ar vairākiem ievades un izvades apgabaliem ir nepieciešams saskaņot.

Katram logam ir jāveido savs unikāls loga identifikators.

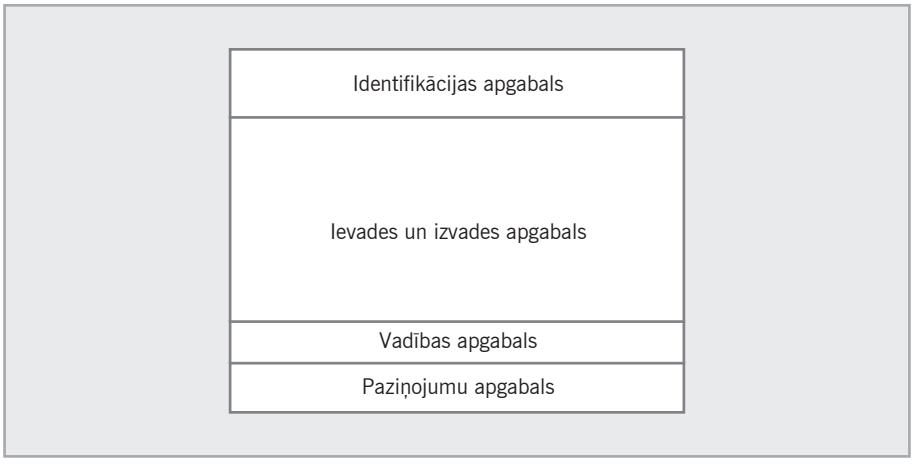
! *Par loga identifikatoru lieliski kalpo loga nosaukums. Identificējot logus, ir ieteicams identificēt arī uzdevuma soli, kurā atrodas lietotājs, piemēram, jauna datu ievade.*

Katram logam nepieciešams radīt noklusētos loga izmērus un atrašanās vietu ekrānā, lai mazinātu lietotāja operāciju skaitu, kas lietotājam ir jāizdara uzdevuma veikšanai.

Lietotnes ietvaros ir nepieciešams logus veidot tā, lai to āriene būtu saskanīga.

Logu vadības elementiem, kuri veic dažādas funkcijas, ir jāatšķiras savā starpā. Lietojot šos elementus dažādās formās, tie ir jāizvieto vienmēr vienā un tajā pašā formā.

! *Piemēram, loga aizvēršanas, maksimizēšanas un minimizēšanas pogas vienmēr atrodas loga labajā augšējā stūrī.*



20. att. Iespējamais dažādu apgabalu izvietojums logā.

Saskarnē lietotiem apgabaliem jābūt atbilstoši novietotiem (identifikācijas apgabalu ieteicams novietot virs ievades un izvades apgabala, vadības apgabalu – aiz ievades un izvades apgabala).

Attēlotās informācijas biezībai jābūt tādai, ka tā nerada traucējumus lietotājam informācijas uztverē (daudzās tekstuāla rakstura saskarnēs tiek minēts limits 40% – procentuāli ar rakstzīmēm aizpildītais laukums logā).

Ievades un izvades apgabals.

Ja ir iespējams, visa nepieciešamā informācija jāizvieto ievades un izvades apgabalā. Ja to nav iespējams veikt, tad 1) informāciju nepieciešams organizēt pa apakškopām, bet strukturējot pēc uzdevumu veikšanas secības; 2) jāatceras, ka informācijas sadalīšanas dēļ uzdevumu izpilde var būt sliktāka.

Ja informācijas apjoms pārsniedz ievades un izvades apgabalā pieejamo vietu, ir jārada apstākļi lietotājam (piemēram, horizontālā vai vertikālā ritināšana (*scrolling*)), lai viņš varētu aplūkot to informāciju, kas pašlaik nav redzama.

Lietotāju ir nepieciešams informēt par to, ka visa informācija ievades un izvades apgabalā nav attēlota, bet lietotājs to var attēlot, veicot kādas darbības. Par šādiem informatoriem kalpo ritjoslas, slīdjoslas (*sliders*) vai norādījumi „lapa X no Y".

Grupas.

Rekomendācijas ietver vadlīnijas informācijas apkopošanai grupās. Informācijas grupēšana palīdz lietotājam uztvert, atrast un interpretēt informāciju daudz vieglāk.

Grupas elementiem ir jābūt skaidri sakārtotiem. Ja nepieciešams, var tikt lietoti papildu līdzekļi grupas nodalīšanai, piemēram, ietvars (*frame*).

Ja uzdevumam ir noteikta izpildes secība, tad, veidojot grupas, ir jāievēro šī uzdevuma izpildes secība.

Ja uzdevums neizvirza izpildes secību, informāciju ieteicams organizēt semantiski saistītās grupās.

Ja uzdevuma specifika prasa veikt informācijas vizuālo meklēšanu, grupu skaitam jābūt pēc iespējas mazākam un grupu atrašanās vietām – pēc iespējas tuvākām, tā, lai attālums starp grupām nebūtu lielāks par 5° no vizuālā leņķa. Nav ieteicams veikt attēlojamās informācijas izmēra samazināšanu tikai tādēļ, lai varētu attēlot pēc iespējas vairāk informācijas.

Saraksti.

Saraksti tiek lietoti, lai organizētu attēlojamo informāciju. Ieteikumi sarakstu veidošanā ietver kārtošanas, numerācijas un informācijas izveidošanas likumus, kā arī virsrakstu lietošanu un informācijas attēlošanu, ja attēlojamā informācija pārsniedz ievades un izvades apgabala izmērus.

Sarakstus ir nepieciešams kārtot loģiskā vai dabiskā veidā. Ja nav izvirzītas prasības par saraksta kārtošanu, vēlams veikt kārtošanu atbilstoši alfabētam.

Alfabētiskas informācijas attēlošana jāveic atbilstoši konkrētās valodas teksta telpiskai organizācijai.

Skaitliskas informācijas attēlošana ir atkarīga no pašas attēlojamās informācijas.

! *Attēlojot veselos skaitļus, tie tiek labēji taisnoti (right justified). Attēlojot skaitļus ar decimāldaļas atdalītājiem, tos nepieciešams kārtot virknē pēc decimāldaļas atdalītāja.*

Attēlojot skaitlisku informāciju, jālieto fiksēts fontu izmērs un atstarpes.

Sarakstu numerācijai jāsākas ar 1 un nevis ar 0, ja vien tas nav specifiski prasīts.

Ja informācijas apjoms pārsniedz ievades un izvades apgabala robežas, tad, pārvietojoties informācijā uz priekšu, numerācijai jāturpinās uz priekšu.

Tabulas.

Tabulas tiek lietotas, lai piešķirtu attēlojamai informācijai sadalījumu apakškopās.

Attēlojot informāciju tabulā, kolonnas nepieciešams izvietot tā, lai kreisajā kolonnā attēlotā informācija būtu vissvarīgākā, pēc tam sekotu mazāksvarīgas informācijas kolonna utt. līdz vismazāk svarīgākas informācijas kolonnai.

Ja attēlotā informācija logos ir analoģiska papīra formā esošajai informācijai, tad tabula jāveido atbilstoši uz papīra esošajai tabulai, lai starp šīm tabulām nebūtu atšķirības.

Ja tabulas kolonnām vai rindām tiek piekārtoti virsraksti, tad situācijās, kad tabulas informācija neiekļaujas ievades un izvades apgabalā, veicot pārējo datu aplūkošanu, jāraugās, lai tabulas kolonnu vai rindu virsraksti vienmēr būtu redzami.

Ja nepieciešams atvieglot informācijas pārlūkošanu vai meklēšanu, var tikt lietotas papildu iezīmes.

! *Attēlojot informāciju tabulā, ik pa piecām rindām tiek ievietota tukša rinda, tādējādi atvieglojot informācijas pārlūkošanu.*

Kolonnas tabulā nepieciešams atdalīt.

! *Ir dažādi veidi, kā atdalīt kolonnas, piemēram, lietot atdalošo vertikālo svītru vai pāris atstarpju.*

Iezīmes *(labels).*

Iezīmes tiek lietotas, lai aprakstītu informācijas vienumus.

Logu elementus (datu ievades laukus, attēlus u. tml.) ir nepieciešams aprakstīt, ja vien šo elementu nozīmi lietotājs nevar skaidri identificēt bez apraksta.

Ja iezīmju pielikšanu nav iespējams veikt vai to esamība kādā veidā traucē, ir iespējams lietot alternatīvus risinājumus elementu paskaidrošanai, piemēram, rīku paskaidrojumu (*tool-tip).*

Iezīmes nepieciešams izvietot blakus informācijas vienumam, ko tās paskaidro.

! *Lietotnes formās visas iezīmes tiek novietotas informācijas vienumu kreisajā pusē.*

Iezīmes un informācijas vienumi, ko tās paskaidro, ir jāformatē un jācentrē, lai tie atrastos pēc iespējas tuvāk.

! *Ja iezīmes tiek novietotas informācijas vienumu kreisajā pusē, tad ieteicama iezīmju labās puses taisnošana (right justified).*

Ja nepieciešams iezīmēs norādīt informācijas vienumos attēlotās informācijas mērvienības, iespējams lietot divus risinājuma variantus (sk. piemēru).

1. variants	Distance (km):	15.6
2. variants	Distance:	15.6 (km)

Lauki *(fields).*

Datu ievades laukiem un lasāmajiem laukiem (*read-only*) ir jābūt vizuāli atšķirīgiem.

! *Ierasti datu ievades laukiem tiek lietota balta fona krāsa, savukārt lasāmajiem laukiem – pelēka fona krāsa. Teksta krāsa datu ievades laukos var būt melna, bet lasāmajos datu laukos – pelēki melna.*

Lielas informācijas attēlošanai datu laukos var izmantot informācijas papildu formatēšanu.

! *Attēlojot summas, var tikt lietoti tūkstošdaļas atdalītāji, tādējādi palielinot informācijas lasāmību.*

Datu ievades laukos, kuros informācija ir ievadāma atbilstoši kādām specifiskām prasībām, ieteicams datu ievades laukus noformēt tā, lai palīdzētu lietotājam saprast, kādā formā informācija ievadāma.

! Personas kods: _ _ _ _ _ _ - _ _ _ _ _

23.3. 13. NODAĻA. LIETOTĀJU VADĪBA

Šajā standarta nodaļā ir aprakstīti ieteikumi lietotāju vadības organizēšanai programmatūras saskarnē.

Ieteikumi lietotāju vadības organizēšanai.

Paziņojumos lietotāja veicamā darbība jāapraksta vispirms un pēc tam jānorāda, kādā veidā šo darbību veikt.

! *Lai attīrītu ekrānu, nospiediet komandpogu **Attīrīt** (pareizi).*
*Nospiediet komandpogu **Attīrīt**, lai attīrītu ekrānu (nepareizi).*

Paziņojumiem jābūt virzītiem uz lietotāja izpratnes palielināšanu, nevis uz sistēmas veikto darbību.

! *Lai saglabātu Jūsu veiktās izmaiņas, nospiediet komandpogu **Saglabāt** (pareizi).*

*Sistēma saglabās Jūsu veiktās izmaiņas datu bāzē, ja nospiedīsiet komandpogu **Saglabāt** (nepareizi).*

Paziņojumi jāveido tā, lai tie atbildētu uz jautājumu „kas ir jādara" un nevis „no kā nepieciešams izvairīties".

Paziņojumos, minot vairākus uzdevumus, nepieciešams lietot vienādu sintaksi.

! *Pieejamas šādas sistēmas opcijas: atvērt datni, drukāt datni, dzēst datni (pareizi).*

Pieejamas šādas sistēmas opcijas: atvērt datni, datnes izdrukāšana, izdzēst doto datni (nepareizi).

Paziņojumus, ja tas iespējams, jāraksta vienkāršos nepaplašinātos teikumos.

Paziņojumos jālieto sistēmas lietotājam pazīstama terminoloģija.

Kļūdu apstrādē, ja ir iespējams pirms operācijas izpildes noteikt, ka tā būs nesekmīga, vēlams par to lietotāju informēt.

Lietotāju nepieciešams informēt par to, ka viena vai otra operācija ir neatgriezeniska, t. i., ka pēc operācijas izpildes nav iespējams atgriezt agrāko stāvokli.

23.4. KONTROLJAUTĀJUMI

1. Aprakstiet standarta ieteikumus lietojumprogrammas dialogu veidošanā!
2. Kādas pamatprasības informācijas pasniegšanā ir izvirzītas lietojumprogrammas lietotājiem!

IZMANTOTĀ LITERATŪRA

NOZARES TIESĪBAS

1. *Informācijas un komunikāciju tiesības*. I sējums /Aut. kol. Ķinis U. u. c. – Rīga: Biznesa augstskola Turība, 2002
2. *Latvijas Vēstnesis*, 06.11.1998. Sk. arī http://www.likumi.lv/doc.php?id=50601, 2004
3. *Latvijas Vēstnesis*, 06.04.2000. Sk. arī http://www.likumi.lv/doc.php?id=4042, 2004
4. *Latvijas Vēstnesis*, 27.04.2000. Sk. arī http://www.likumi.lv/doc.php?id=4042, 2004
5. *Latvijas Vēstnesis*, 29.10.1996. Sk. arī http://www.likumi.lv/doc.php?id=41058, 2004
6. *Latvijas Vēstnesis*, 22.05.2002. Sk. arī http://www.likumi.lv/doc.php?id=62324, 2004
7. *Latvijas Vēstnesis*, 20.11.2002. Sk. arī http://www.likumi.lv/doc.php?id=68521, 2004
8. *Latvijas Vēstnesis*, 24.03.2000. Sk. arī http://www.likumi.lv/doc.php?id=3339, 2004
9. *Latvijas Vēstnesis*, 02.02.2001. Sk. arī http://www.likumi.lv/doc.php?id=2697, 2004
10. *Latvijas Vēstnesis*, 01.12.2000. Sk. arī http://www.likumi.lv/doc.php?id=13216, 2004
11. Kase J. Elektroniskie paraksti un dokumentu drošība //*DatorPasaule* – Nr. 3, 2003
12. *Latvijas Vēstnesis*, 30.04.1996. Sk. arī http://www.likumi.lv/doc.php?id=52392, 2004
13. Ķinis U. Internets un cenzūra (jurista skatījumā) //*DatorPasaule* – Nr. 2, 1999
14. *Angļu-latviešu skaidrojošā datorvārdnīca*. – Rīga: Jumava, 1998. 111 lpp.
15. Draft Convention on (cyber crime) PC-CY (1999)12
16. *Enciklopēdiskā vārdnīca*. – Rīga: Latvijas Enciklopēdiju redakcija, 1991. – 2. sēj., 256. lpp.
17. Autortiesību likums //*Latvijas Vēstnesis,* 27.04.2000. 1. pants. Sk. arī http://www.likumi.lv/doc.php?id=5138, 2004
18. Ruķers M. *Personas datu tiesiskā aizsardzība*. – Rīga: Biznesa augstskola Turība, 2000
19. Working party on illegal and harmful content on the Internet report PC-CY (97) 29
20. Krastiņš I. *Tiesību teorijas kategorijas un termini*. – Rīga: LU Juridiskā fakultāte, 1997, 13. lpp.
21. Borzovs J. Uzmanību! Programmu izstrāde un autortiesības //*E-pasaule* – Nr. 2, 2001
22. Pirātisms. Jūsu drošība/ Baltic Software Aliance. http://www.bsa.lv, 2004
23. *Latvijas Vēstnesis*, 19.04.1995. Sk. arī http://www.likumi.lv/doc.php?id=34734, 2004
24. Kiršteins K. *Likumu piemērošanas īpatnības informācijas tehnoloģiju sfērā*. Diplomdarbs
25. Oracle AG. Oracle license agreement – 2000

26. *Latvijas Vēstnesis*, 01.04.1999. Sk. arī http://www.likumi.lv/doc.php?id=23309, 2004
27. IT tiesības un risinājumi / Juridisko pakalpojumu firma „E-sabiedrības risinājumi". Sk. http://www.e-risinajumi.lv, 2004
28. Ruķers M. *Uzstāšanās par Interneta pakalpojumu sniedzējiem un klientu datu aizsardzību*. Sk. http://www.lia.lv/doc/IPSdatuaizsardziba.doc, 2004
29. Zoldners J. Darbinieku privātā informācija //*E-pasaule* – Nr. 12, 2002
30. http://www.humanrights.lv/doc/vispaar/vispcd.htm, 2004
31. Sk. http://www.humanrights.lv/doc/regional/eck.htm, 2004
32. Sk. http://www.ttc.lv/New/primarie/11992M.doc, 2004
33. Sk. http://www.ttc.lv/New/primarie/11997D.doc, 2004
34. Sk. http://europa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html, 2004
35. *Latvijas Vēstnesis*, 06.04.2000. Sk. arī http://www.likumi.lv/doc.php?id=4042
36. http://www.dvi.gov.lv/
37. Darbinieku novērošanas programmu piedāvājums. Sk. http://www.employee-monitoring.com, 2004
38. Personīgās informācijas aizsardzība. Sk. http://www.spycops.com, 2004
39. Mazure L. E-komercijas juridiskie aspekti //*E-pasaule*, 2003
40. Koncepcija par elektronisko komerciju. Ekonomikas ministrija. Sk. http://www.em.gov.lv/em/images/modules/items/item_file_737_koncepcija%20par%20e-komerciju.doc
41. Suļskis A. Drošība elektronisko darījumu veikšanā //*E-pasaule* – Nr. 1, 2001
42. http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm, 2004
43. http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf 2004
44. Ziediņš J. Nedroša informācijas sistēmu drošība //*E-pasaule.*
45. *Informācijas un komunikāciju tiesības*. II sējums /Aut. kol. Ķinis U. u. c. – Rīga: Biznesa augstskola Turība, 2002
46. Tynan D. ASV valdības cīņa pret surogātpastu //*E-pasaule* – Nr. 11, 2003
47. http://www.uncjin.org/Documents/EighthCongress.html#congress, 2004
48. *Latvijas Vēstnesis*, 08.07.1998. Sk. arī http://www.likumi.lv/doc.php?id=88966, 2004
49. O'Brien M. J. u. c. Computer Crime: The U.N. Sk. http://www.mobrien.com/computer_crime.shtml, 2004
50. Jēkabsone J. Aktuālākais darba drošībā un veselības aizsardzībā, strādājot ar datoru //*E-pasaule* – Nr. 6, 2001

NOZARES STANDARTI

51. *Datorstandartu informācija. Tildes Datorbibliotēka*. – Rīga: sabiedrība Tilde, 2002. gada aprīlis
52. Borzovs J. Standartizācijas vadlīnijas //*EU Phare Projekts „Ģeogrāfisko datu standartizācija"*, 1998. gada marts
53. Ince D. *Software Quality Assurance*. – England: McGraw-Hill Publishing Company, 1995

54. *Lielā terminu vārdnīca. Datortermini*. Sk. www.termini.lv, 2004
55. Kvalitātes vadības sistēmas. Prasības, LVS EN ISO 9001:2000
56. http://www-106.ibm.com/developerworks/rational/library/content/RationalEdge/feb02/ConventionalToModernFeb02.pdf, 2004
57. http://www.exigen.lv/zinas/jaunumi/index.php?id=14, 2004
58. *Ieteikumi programmatūras dokumentācijas komplektam* /Aut. kol. Borzovs J., Viļums Ē., Čevere R. , Plūme J. – Rīga: RITI, 1997
59. Vītoliņš V. IT Projektu pārvaldība //*E-pasaule* – Nr. 9' 2001
60. Programmatūras prasību specifikācijas ceļvedis, LVS 68:1996, Latvijas Valsts standarts
61. Ieteicamā prakse programmatūras projektējuma aprakstīšanai, LVS 72:1996, Latvijas Valsts standarts
62. http://www.webster-dictionary.org/definition, 2004 vai http://www.realdictionary.com/computer, 2004
63. Programmatūras testēšanas dokumentācija, LVS 70:1996, Latvijas Valsts standarts
64. Programmatūras lietotāja dokumentācija, LVS 66:1996, Latvijas Valsts standarts
65. Ergonomic requirements for office work with visual display terminals, ISO 9241, starptautisks standarts