ELEKTRONISKO PIERĀDĪJUMU IZPRATNE, TO IEGUVE UN NOSTIPRINĀŠANA KRIMINĀLPROCESĀ

UNDERSTANDING OF ELECTRONIC EVIDENCE, ITS ACQUISITION AND STRENGTHENING IN CRIMINAL PROCEEDINGS

Aleksandrs Brīvers
Rēzeknes Tehnoloģiju akadēmija, ab16288@edu.rta.lv, Rēzekne, Latvija
Zinātniskā vadītāja Dr.iur. ***Ilona Bulgakova***

Abstract. *Criminal investigations now face a new reality at the outset of criminal investigations. It involves the gathering of evidence, which has become more different than in previous decades. In line with the information and technology age, criminal investigations are increasingly finding that a large proportion of criminal offenses and criminal offenses are based on electronic evidence. The taking and consolidation of electronic evidence must take place in such a way that it can also be subject to existing general principles of law.*

Keywords*: acquisition, confirmation, criminal offense, electronic evidence.*

Ievads

Pasaules valstīs neviena sociālā sistēma nevar pilnvērtīgi pastāvēt bez informācijas aprites. Ar katru gadu pieaugošais informācijas daudzums, modernās tehnoloģijas, prasmes un iemaņas rīkoties ar tām, liek aizdomāties, cik lielā mērā ir izmainījušās daudzas sfēras, tāpēc arī juristi diskutē par to, kādām tiesībām ir jābūt informācijas sabiedrībā. Tāpēc jāizvērtē, kādas ir iespējas, riska faktori, priekšrocības un vājās puses informācijas tehnoloģiju izmantošanā tostarp tieslietās, kur par vienu no novitātēm ir kļuvuši *elektroniskie pierādījumi*. Cilvēku īpašība – ticēt tam, kas ir pilnībā pierādāms, ir iekļauta arī kriminālprocesuālajā lietvedībā. *Pierādījumi* un *pierādīšana* ir svarīga *noziedzīga nodarījuma* izmeklēšanā un atklāšanā. Elektroniskā pierādījuma ienākšana Eiropas Savienības normatīvajā regulējumā norāda uz šā juridiskā institūta nozīmīgumu. Arī tieslietu sistēmā darbiniekiem jārēķinās ar minētajām prasmēm.

Raksta **mērķis** – atklāt elektronisko pierādījumu ieguves un nostiprināšanas īpatnības kriminālprocesā.

Lai to realizētu, ar analīzes, salīdzinošo, dedukcijas un sintēzes metodēm rakstā tiks analizēti elektronisko pierādījumu veidi, elektronisko pierādījumu iegūšanas un nostiprināšanas gaita, kā arī raksturota elektronisko pierādījumu nostiprināšana.

Elektronisko pierādījumu izpratne kriminālprocesā

Attiecībā uz *elektroniskajiem pierādījumiem* kā pierādīšanas līdzekļiem, jākonstatē, ka elektronisko pierādījumu netiešu definīciju satur Kriminālprocesa likuma (turpmāk – KPL) 136. pants. Konkrēti, par pierādījumu kriminālprocesā var būt ziņas par faktiem elektroniskas informācijas formā, kas apstrādāta, uzglabāta vai pārraidīta ar automatizētas datu apstrādes ierīcēm vai sistēmām *(Kriminālprocesa likums, 2005)*.

2001.gada 23.novembra Eiropas Padomes Konvencijas par kibernoziegumiem (*Convention on cybercrimes*) normas par *elektronisko pierādījumu* procesuālo regulējumu tika iestrādātas jaunajā Kriminālprocesa likumā. Viens no pirmajiem jautājumiem, ko reglamentē Eiropas Padomes Konvencija par kibernoziegumiem, ir procesuālie jautājumi par *pierādījumu elektroniskā formā* meklēšanu, saglabāšanu, iegūšanu, vākšanu un pārtveršanu *(Konvencija par kibernoziegumiem, 2001)*

https://doi.org/10.17770/iss2021.6913

Atzīta nepieciešamība sadarboties starp valstīm un privātajiem uzņēmējiem, cīnoties pret kibernoziegumiem, aizsargājot informācijas tehnoloģiju lietošanas un attīstības likumīgās intereses. Skaidrs, ka efektīva cīņa pret kibernoziegumiem prasa pieaugošu, ātru un labi funkcionējošu starptautisko sadarbību kriminālliet̄as *(Konvencija par kibernoziegumiem, 2001)*.

Savukārt, piemēram, Krievijas Federācijas Kriminālprocesa kodeksā 74. pantā minēts pierādījumu definējums un uzskaitījums, kur termins *elektroniskais pierādījums* neeksistē *(Уголовно - процессуальный кодекс Российской Федерации, 2001)*. Saskaņā ar Krievijas Federācijas Kriminālprocesa kodeksa 88. pantu, elektroniskajiem dokumentiem kā *pierādījumiem* kriminālprocesā jāatbilst vairākām prasībām, t.sk. jābūt loģiskai saiknei starp ziņām, kas veido informācijas saturu, un apstākļiem, kas jāpierāda, pieņemamībai (procesuālās formas atbilstībai likuma prasībām) un ticamībai (atbilstībai faktiski pastāvošajiem faktiem) *(Воронин, 2019)*.

Savukārt Amerikas Savienoto Valstu (turpmāk – ASV) valdības Tieslietu ministrijas oficiālā vietnē (*National Institute of Justice - NIJ*) atrunāts, ka *digitālie pierādījumi* ir binārā formā glabāta vai pārsūtīta informācija, uz kuru var paļauties tiesā. Citu starpā to var saglabāt datora cietajā diskā, mobilajā tālrunī. Digitālie pierādījumi parasti ir saistīti ar elektronisko noziedzību jeb e-noziedzību, piemēram, bērnu pornogrāfiju vai krāpšanos ar kredītkartēm. Tomēr *digitālos pierādījumus* izmanto, lai sauktu pie atbildības par visu veidu noziegumiem, ne tikai par e-noziegumiem *(Ruddell, 2020)*.

Ņemot vērā iepriekš minēto, var redzēt, ka šobrīd pasaulē pastāv divi diametrāli pretēji viedokļi par to, kas ir *elektroniskie pierādījumi*. Vienviet tos uztver un saprot kā neatkarīgu pierādījumu veidu, citviet – neatzīst pilnībā, katrā valstī pamatojot šo viedokli ar saviem argumentiem.

Elektronisko pierādījumu veidi un to ieguve

Elektroniskie pierādījumi parasti tiek iegūti kratīšanā. Elektroniskā pierādījuma institūts kriminālprocesā Latvijas juridiskajā literatūrā analizēts nepietiekoši, 2001. gadā to raksturojis U. Ķinis savā publikācijā "Kibernoziegumi un kriminālprocess", minot, ka par elektronisko pierādījumu veidiem var kalpot:

1) abonenta jeb pakalpojuma pasūtītāja identifikācijas informācija (*subscriber information*);
2) datu plūsma jeb ar pārraidi saistīti dati (*traffic data*);
3) satura dati jeb abonenta/pasūtītāja elektroniskā korespondence (*content data*) – komunikācijas satura dati, kas pārraidīti ar datorsistēmas palīdzību. To paredz KPL 12. panta trešā daļa – tikai ar izmeklēšanas tiesneša piekrišanu *(Buko, 2020)*.

Pirmās instances tiesas spriedumā arhīvā lieta Nr. K33-0116-19/14 konstatēts, ka elektroniskais pierādījums ir neatliekamās medicīniskās palīdzības izsaukuma elektroniskā karte (*informācija,* kas tur glabājas). *(Latvijas Republikas Rīgas rajona tiesas spriedums, 2019, Nr. K33-0116-19/14)*. Savukārt Latvijas Republikas Augstākās tiesas Krimināllietu departamenta lēmuma lietā Nr. SKK-320/2017 minēts, ka Krimināllikuma 307.pantā paredzētā noziedzīgā nodarījuma (nelikumīgas darbības ar kriminālliet̄as materiāliem) priekšmets ir ne tikai procesuāls dokuments, bet arī *datu nesējā esoša informācija*. *(Latvijas Republikas Augstākās tiesas Krimināllietu departamenta spriedums, 2017, Nr. SKK-320/2017)*. No iepriekš minētajiem piemēriem redzams, ka elektroniskais pierādījums ir *informācija,* kas saglabāta datu nesējā.

Viena no būtiskām problēmām elektronisku pierādījumu ieguvē ir to ieguve no ārzemēm, jo pastāv atšķirības dažādu valstu tiesiskajā regulējumā. Problēma ir tā, ka Latvijas Republikas un, piemēram, Amerikas Savienoto Valstu likumi atšķiras un, ja Latvijā izplatīta nepatiesa informācija par personu kvalificējama pēc Krimināllikuma 157.panta, tad, iespējams, Amerikas Savienotajās Valstīs atsevišķos štatos tas vispār varētu nebūt kriminālpārkāpums vai izplatītā informācija varētu būt vērtētā kā rīcība, kas būtu aizsargāta ar vārda brīvību.

Elektronisko pierādījumu procesuālā nostiprināšana

ASV eksperti D. B. Gerijs (*Garrie)* un J. D. Morisijs (*Morrissy)* min procedūru, kas raksturo elektronisko pierādījumu apkopošanas pārbaudes mehānismu. Sākotnēji ir jāpievērš uzmanība

pierādījumu ieguves veidam. Būtu jānosaka, vai sākotnējie pierādījumi ir iegūti ar kopiju no cietā diska, vai tieši. Kopēšana parasti ir uzticamāka nekā tieša iegūšana, jo tas samazina kļūdu iespējas. Attēlu formātam ir jāizmanto *Guidance Systems* programmatūra *Encase*, kas ir vispopulārākā programmatūra spoguļkopijai. Vajadzētu detalizēti aprakstīt visus veiktos soļus, lai neatkarīgai trešajai personai tie nebūtu pārprotami. ASV lietā *Nucor Corp v. Bell, 2008, WL 4442571* (D.S.C., 2008. gada 11. janvārī) eksperts apgalvoja, ka pretējā puse, lai notīrītu pierādījumus no klēpjdatora, izmantoja speciālu datu dzēšanas programmu. Pamatā bija cietā diska pārbaude *(Garrie, Morrissy, 2014)*. Tiesa noraidīja ierosinājumu izslēgt eksperta liecību, secinot, ka eksperta izmantotā metode pietiekami sasaista datus ar secinājumiem. Tiesa atzīmēja, ka eksperts ir pārbaudījis hipotēzi par to, kā nulles bloki parādījušies diskā, un atkārtojis nulles modeli.

Tiesa arī pieņēma pierādījumus, kas iegūti testēšanas rezultātā, jo eksperts katru testa soli bija kārtīgi dokumentējis, lai pārliecinātos, ka dati cietajā diskā ir ierakstīti paredzētajā veidā. Parasti, ja kriminālistikas dati nav pieejami digitāli, kriminālistikas ziņojums ir mazāk uzticams, jo nevar novērtēt tā precizitāti vai metodoloģijas ticamību. Ziņojumi ar secinājumiem, kurus nevar reproducēt, izmantojot kriminālistikas attēlu kopijas un līdzīgu analīzes programmatūru, ir maz ticami. Kriminālistikas ziņojuma izklāsts:

1) īss informācijas kopsavilkums;
2) izmeklēšanas procesā izmantotie rīki, tostarp to mērķis un visi citi pamatā esošie pieņēmumi, kas saistīti ar rīku;
3) pierādījumu vienums Nr. 1 (piemēram: A darbinieka darba dators);
   a) pierādījumu kopsavilkums, kas atrasts A darbinieka darba datorā,
   b) A darbinieka darba datora attiecīgo daļu analīze,
   c) e-pasta vēsture,
   d) interneta meklēšanas vēsture,
   e) USB reģistra analīze,
   f) iepriekš minēto darbību atkārtošana citiem pierādījumu elementiem (kas var ietvert citus datorus un mobilās ierīces utt.);
4) ieteikumi un turpmākās darbības, lai turpinātu vai izbeigtu izmeklēšanu, pamatojoties uz ziņojumā konstatēto.

Digitālajai kriminālistikai attīstoties, informācijai par elektronisko pierādījumu iegūšanas metodiku vajadzētu būt pieejamākai. Zināmi daudzi gadījumi, kas prasījuši datorzinātņu ekspertu iesaisti, bieži vien izmantojot arī novatoriskas pieejas *(Garrie, Morrissy, 2014)*. Var apgalvot, ka tieši ASV tiesu praksē e-pierādījumi ir kļuvuši par stabilu, noregulētu bāzi, kas nevienam vairs neizraisa nekādas šaubas.

Mūsdienu izplatītākie datu nesēji, kuros iespējams savākt elektroniskos pierādījumus, ir USB zibatmiņas, ārējie cietie diski, visu veidu datoru cietajiem diskiem, ieskaitot HDD un SSD diski, atmiņas kartes u. c.

Tāpat kā izņemta faila identitāti un patiesumu nosaka *HASHSUM* vai kriptogrāfiskā kontrolsumma, fiksēta izmēra atskaites aprēķins, elektroniskais "pirkstu nospiedums", datnes (faila) integritāte tiek pārbaudīta, aprēķinot un vēlāk salīdzinot kontrolsummu *(Buko, 2020)*.

Krimināprocesa likumā komentāros par Krimināprocesa likuma 160. pantu minēts, ka šobrīd likumdevējs ir noteicis vienu gadījumu, kad apskatāmais objekts parasti nevar tikt apskatīts uz vietas. Tas attiecināts uz automatizētās datu apstrādes sistēmu vai tas daļu šādā situācijā, ja vien tiešam nav iespējams kvalitatīvi to izdarīt uz vietas, šo sistēmu vai tas daļu izņem, nodrošinot datu veseluma saglabāšanu neizmainītā stāvoklī. Objekta apskati veic vēlāk kā atsevišķu apskati vai arī dara to ekspertīzes gaitā *(Strada-Rozenberga, 2019)*.

Ņemot vērā iepriekš teikto, praktiski nav iespējams kvalitatīvi nodrošināt apstākļus, tehniku un programatūru nozieguma notikuma vietā, lai uzreiz veiktu izņemtā objekta (piemēram, cietajā diskā, citā datu nesējā utt.) un tajā saglabātā satura apskati. Elektronisko pierādījumu nostiprināšana krimināprocesā ir svarīga un atbildīga procesuāla darbība, kura prasa tās veicējam speciālas iemaņas IT sfērā.

Tomēr pēc pieredzes var apgalvot, ka nevar izņemt datoru un pietiek tikai uztaisīt datu kopiju. Datu kopija nepieciešam tikai, lai veiktu apskati un konstatētu, vai uz izņemtā oriģināla ir meklējamais elektroniskais pierādījums vai nē, bet pats izņemtais objekts - izņemtais dators un it īpaši uz tā glabātā informācija būs elektroniskais pierādījums.

Šinī gadījumā rodas jautājums, vai glabātā informācija *cietajā diskā* arī ir attiecināmā uz likumā definētajām *sistēmām* (*tās daļām*)? Vai saglabātā informācija cietajā diskā jādefinē atsevišķi kā, piemēram, automatizētās datu apstrādes sistēmas saglabāta *saturiska informācija*? Interesēt var informācija, kas tika saglabāta iepriekšminētajā portatīvajā datorā, tieši tur būtu meklējami un atrodami elektroniskie pierādījumi.

Pastāv tāds modelis kā elektroniskā pierādījuma informācijas satura apskate. Zināms, ka galvenais elektroniskajā pierādījumā ir *datu veseluma saglabāšanas neizmainīta stāvoklī*. Tātad, lai apskatītu elektroniskā pierādījuma saturu, nedrīkst veikt jebkādas manipulācijas (atvērt failu, labot failu utt.) ar to saturu, jo pretējā gadījumā elektroniskajā pierādījumā būs mainīta *HASHSUM* (izņemta faila identitāte un patiesums), un elektroniskais pierādījums tiks atzīts par nederīgu. Lai šāda situācija nerastos, tad ieteicams no cietajā diskā glabātās informācijas satura izveidot *spoguļkopiju*, kuras saturu varēs apskatīt un konstatēt elektronisku pierādījumu (video failu, fotoattēla failu utt.)

No raksturotajiem apstākļiem izriet jautājums, vai *spoguļkopijas* izveidošana attiecināma uz *apskati,* vai tā ir *ekspertīze,* un pēc tam tikai seko *apskate*, kurā ietver sevī *spoguļkopijas apskati*? Kriminālprocesa likuma 194.panta kontekstā jāsaprot, ka, ja procesa virzītajam nav speciālu zināšanu (atbilstošas izglītības IT sfērā), viņš nevar izveidot informācijas satura *spoguļkopiju* no cietā diska un, ņemot vērā, ka *spoguļkopijas* izveidošanai nepieciešams tehniskais aprīkojums, speciāla programatūra, iemaņas ar to strādāt un speciālas IT iemaņas, viennozīmīgi var uzskatīt, ka *spoguļkopijas* izveide attiecināma uz *ekspertīzi* un nekādā gadījumā iepriekšminētā darbība nevar būt uzskatīta par apskates daļu.

Secināms, ka iepriekš raksturotās situācijas aspektā pieņemamais modelis varētu būt sekojošs:

- darbu sāk ar automatizētās datu apstrādes sistēmas (tās daļas) izņemšanu (attiecināmu pie apskates);
- tam seko ekspertīze, lai noskaidrotu, piemēram, vai cietajā diskā glabājas kaut kāda saturiska informācija un, ja tāda ir, tad šai informācijai izveido spoguļkopiju;
- tam seko spoguļkopijas satura apskate un interesējošas informācijas konstatēšana un nostiprināšana apskates protokolā.

Līdzīgs modelis ir aprobēts un aprakstīts D. B. Garrie un J. D. Morrissy rakstā, kas min ASV tiesu prakses piemēru *(Garrie, Morrissy, 2014)*.

Multimediju datu izmantošana, piemēram, video pierādījumi, īpaši no novērošanas kamerām, var būt tikpat apjomīgi kā mobilo ierīču dati, un ir pieejami ierobežoti izmeklēšanas rīki, lai droši analizētu video. Lai efektīvi operētu šķirošanu un optimizētu ierobežoto resursu izmantošanu, ir nepieciešama sistemātiska darba kārtības prioritāšu noteikšanas metode *(Goodison et al., 2021)* Minēto problēmu kontekstā 2020. gada 24. novembrī valsts administrācijas skola, sadarbībā ar ASV Tieslietu departamenta Prokuratūras attīstības, palīdzības un mācību biroju ārvalstīs (DOJ-OPDAT), citām ASV institūcijām, Latvijas, Lietuvas un Igaunijas tiesību aizsardzības un prokuratūras iestādēm īstenoja starptautisku semināru "Baltijas reģionālais elektronisko pierādījumu vebinārs prokuroriem un izmeklētājiem" *(Valsts administrācijas skola, 2020)* Latvijas, Lietuvas un Igaunijas tiesībaizsardzības un prokuratūras iestāžu 60 pārstāvji iepazīstināja klātesošos ar situāciju elektronisko pierādījumu jomā, uzsverot galvenos jautājumus, ar kuriem saskaras viņu pārstāvētas institūcijas.

Secinājumi un priekšlikumi

1. Elektroniskie pierādījumi ir pierādījumi kriminālprocesā. Tādejādi elektroniskajiem pierādījumiem jāatbilst pierādījumu pazīmēm jeb īpašībām, t.i., attiecināmībai, pieļaujamībai un ticamībai. Savukārt, ja netiek ievērotas Kriminālprocesa likuma prasības un pamatprincipi, iegūtie pierādījumi atzīstami par nepieļaujamiem un pierādīšanā neizmantojamiem.

2. Spriedums tiesas procesā ir tiesībaizsardzības procesa noslēgums, kas sākās ar likuma pārkāpumu un beidzas ar likuma izpildi. Iebildumi pret digitāliem pierādījumiem reti tiek atbalstīti tiesā daudzās pasaules valstīs, ja vien pierādījumi atbilst *Daubert* standartam.
3. Dažādās krimināltiesību sistēmas jomās joprojām pastāv atšķirības, iepazīstot digitālos pierādījumus (piemēram, darbinieku zināšanu trūkums par digitālajiem pierādījumiem var sarežģīt atbilstošu izmantošanu tiesā) vai, piemēram, augstākā vadība var nekavējoties atzīt digitālo pierādījumu iespēju priekšrocības. Tomēr vienprātību ir vieglāk atrast, ja veiksmīga digitālo pierādījumu apstrāde tieši noved pie vairāku gadījumu atrisināšanas un sekmīgākas kriminālvajāšanas, pamatojoties uz šiem pierādījumiem.
4. Lai e-pierādījums būtu definējams kā pierādīšanas līdzeklis kriminālprocesā, tas būtu iegūstams un procesuāli nostiprināms KPL paredzētajā kārtībā, gan izpildot attiecīga pierādīšanas līdzekļa nostiprināšanas priekšnosacījumu (attiecīgas darbības atļaujas/piekrišanas, izvēles atbilstība KPL prasībām), gan KPL paredzētas procedūras ievērošanas. Tas skar arī elektronisko pierādījumus.
5. Darbam ar elektroniskajiem pierādījumiem kriminālprocesā palīdz digitālā kriminālistika, kas turpina attīstīties, lai nodrošinātu metodikas un stratēģijas, kas nepieciešamas elektronisko pierādījumu ieguvē, lai integrētu digitālās kriminālistikas iespējas, lai garantētu digitālo pierādījumu pieļaujamību. Daudzās grāmatās digitālajiem pierādījumiem galvenā uzmanība tiek pievērsta tehniskajos, programmatūras un izmeklēšanas elementos, bet tas, ko mēdz aizmirst, ir organizāciju cilvēki un procesa elementi.
6. Šobrīd pasaulē pastāv divi diametrāli pretēji viedokļi par to, kas ir elektroniskie pierādījumi. Vienviet tos uztver un saprot kā neatkarīgu pierādījumu veidu, citviet – neatzīst pilnībā, katrā valstī pamatojot šo viedokli ar saviem argumentiem.
7. Pastāv būtiski šķēršļi, lai kriminālprocesa izmeklēšanas laikā iegūtu elektroniskus pierādījumus no ārzemēm. Viena no būtiskām problēmām elektronisku pierādījumu iegūšanai no ārzemēm ir valstu likumu atšķirība.
8. Tāpat kā izņemta faila identitāti un patiesumu nosaka *HASHSUM* vai kriptogrāfiskā kontrolsumma, fiksēta izmēra atskaites aprēķins, elektroniskais "pirkstu nospiedums", galvenais elektroniskajā pierādījumā ir *datu veseluma saglabāšanas neizmainīta stāvoklī.*
9. Ne jau pats dators vai datu nesējs kā fiziska vienība ir pierādījums nozieguma veikšanai, bet gan tikai konkrētie informācijas dati tajā.
10. No raksturotajiem apstākļiem izriet jautājums, vai *spoguļkopijas* izveidošana attiecināma pie *apskates* vai tā ir *ekspertīze*. Šajā sakarā autors izvirza priekšlikumu: Papildināt Kriminālprocesa likuma 160.panta sesto daļu kur būtu atrunāts, ka tādas darbības kā automatizētas sistēmas vai tās daļas saglabāta uz tas informācijas satura apskate veicama iepriekš ja nepieciešams ekspertīzes ceļā izveidojot izņemta priekšmetā informācijas satura *spoguļkopiju*. Konkrēti, 160.panta sestās daļas norma nosakāma šādā redakcijā: *"Automatizētās datu apstrādes sistēmas (tās daļas) apskati parasti uz vietas neveic, bet šo sistēmu (tās daļu) izņem, nodrošinot datu veseluma saglabāšanu neizmainītā stāvoklī. Ja elektronisko pierādījumu apskatei nepieciešamas specialas zināšanas vai nepieciešams izmantot tehniku, tad nozīmē ekspertīzi, un datu nesēja satura spoguļkopijas izveidošana attiecināma uz ekspertīzi".*
11. Kriminālprocesa likuma 160.panta ietvaros var ieviest tādu terminu kā "uz elektroniska datu nesēja saglabātas informācijas satura apskate" vai "saturiska apskate".
12. Mūsdienās elektroniskais pierādījums un tā nozīme ir sevi apliecinājusi kriminālprocesā, tomēr Kriminālprocesa likuma normas krietni atpaliek elektronisko pierādījumu ieguvē un nostiprināšanā, kā arī kopumā elektroniskās vides regulēšanas jautājumā.

Izmantotie avoti un literatūra

1. *Konvencija par kibernoziegumiem* (23.11.2001). Eiropas Padomes valstis, red. uz 14.04.2007. https://likumi.lv/ta/lv/starptautiskie-ligumi/id/1460-konvencija-par-kibernoziegumiem, sk. 14.10.2020.
2. *Kriminālprocesa likums* (21.04.2005). LR likums, red. uz 06.07.2020. https://likumi.lv/ta/id/107820-kriminalprocesa-likums, sk. 14.10.2020.

3. *Уголовно - процессуальный кодекс Российской Федерации* (2001). Закон Российской Федерации, № 174-ФЗ. Получено 05.04.2021 из http://pravo.gov.ru/proxy/ips/?docbody=&nd=102073942
4. Buko, A. (2020). *Pierādījumu saglabāšanas principi IT vidē notikušos noziegumos.* https://cert.lv/uploads/pasakumi/Aleksandrs_Buko_elektroniskie_pieradijumi_updated.pdf, sk. 14.10.2020.
5. Garrie, D.,B., Morrissy, J.D. (2014). Digital Forensic Evidence in the Courtroom: Understanding Content and Quality. *Northwestern Journal of Technology and Intellectual Property*, 12 (2), 121-128. Retrieved 26.04.2021 from https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article= 1218&context=njtip
6. Goodison, S. E., Davis, R. C., Jackson, B. A. (2021). *Understanding digital evidence*. Retrieved 05.04.2021 from https://www.iacpcybercenter.org/investigators/digital-evidence/understanding-digital-evidence/
7. Latvijas Republikas Augstākās tiesas Krimināllietu departamenta 2017.gada 30.novembra spriedums lietā Nr. SKK-320/2017. http://at.gov.lv/lv/tiesu-prakse/judikaturas-nolemumu-arhivs/kriminallietu-departaments/hronologiska-seciba?year=2017, sk. 30.04.2021.
8. Latvijas Republikas Rīgas rajona tiesas 2019.gada 28.augustā spriedums lietā Nr. K33-0116-19/14. https://manas.tiesas.lv/eTiesasMvc/lv/nolemumi, sk. 30.04.2021.
9. Ruddell, M. (2020). *Just Science Podcast: Just Digital Evidence 101.* Retrieved 05.04.2021 from https://www.ojp.gov/ncjrs/virtual-library/abstracts/just-science-podcast-just-digital-evidence-101
10. Strada-Rozenberga, K. (red)., (2019). *Kriminālprocesa likuma komentāri. A daļa*. Rīga: Latvijas Vēstnesis.
11. Valsts administrācijas skola (2020). *Baltijas reģionālais vebinārs par elektroniskiem pierādījumiem*. https://www.vas.gov.lv/lv/jaunums/baltijas-regionalais-vebinars-par-elektroniskiem-pieradijumiem, sk. 20.04.2021.
12. Воронин, М. (2019). Электронные доказательства в УПК: быть или не быть? *Науки Криминального Цикла,* 7, 74-84. Получено 05.04.2021 из https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-v-upk-byt-ili-ne-byt

Summary

With the ever-increasing amount of information, modern technology raises questions about the extent to which many areas have changed, so lawyers are debating what rights should be in the information society. The opportunities, risks, advantages and disadvantages of using information technology need to be assessed, including in law, where electronic evidence has become a novelty. The aim of the article is to reveal the peculiarities of the process of obtaining and consolidating electronic evidence in criminal proceedings. In order to achieve this, the types of electronic evidence, the process of obtaining and strengthening electronic evidence, as well as the strengthening of electronic evidence will be analysed in the article with the methods of analysis, comparison, deduction and shipment. There are currently two diametrically opposed views in the world about what electronic evidence is. In one place they are perceived and understood as an independent form of evidence, in other places they are not fully recognized in each country, basing this view on their own arguments. A major problem in obtaining electronic evidence is obtaining it from abroad, as there are differences in national laws. The digital forensic report should describe all the steps taken in sufficient detail so that they are not unambiguous to an independent third party. It can be argued that it is in US jurisprudence that e-evidence has become a stable, regulated base that no longer raises any doubts. Strengthening electronic evidence in criminal proceedings is an important and responsible procedural activity that requires its performer to have special skills in the field of IT. The question arises as to whether the information stored on the hard disk is also applicable to the systems (parts thereof) defined by law. Should the information stored on the hard disk be defined separately as, for example, content information stored by an automated data-processing system? It is known that the key to electronic proof is to keep the integrity of the data intact. It is recommended that you make a mirror copy of the contents of the information stored on your hard disk so that the contents can be viewed and electronic evidence (video file, photo file, etc.) can be identified. The question arises as to whether the creation of a mirror is attributable to an examination, is it an examination, and is it only followed by an examination which includes an examination of the mirror. Digital evidence must conform to the Daubert standard. A proposal may be put forward - to supplement Section 160, Paragraph six of the Criminal Procedure Law where it would be stipulated that such activities as inspection of the information content of an automated system shall be performed by creating a mirror copy of the information content in the removed subject.