KRĀPŠANA E-VIDĒ
FRAUD ONLINE

Ksenija Gaide
Rēzeknes Tehnoloģiju akadēmija, Mg. sc. ing., ksenijaa@inbox.lv, Rēzekne, Latvija
Zinātniskā vadītāja Mg. iur. ***Aija Jermacāne***

Abstract. *E-fraud involves fraudulent online payments and e-commerce sites, soliciting personal data or cheating on virtual currency. In recent years, a new type of criminal e-transaction has been identified in Latvia - illegal access to bank accounts and fraud, which tends to Smart-ID users.*

Criminals are coming up with new ways to obtain money illegally. Often these crimes are transnational in nature, making it difficult for victims to return the money lost. Funds are transferred to payment systems such as cryptocurrencies, which makes it very difficult to track their progress.

Police statistics show that hundreds of Latvians suffer from various forms of Internet fraud every year. However, it must be acknowledged that this is largely due to people's credulity and the lack of cyber hygiene in society.

Keywords: *cybercrime, data security, fraud, suspicious transactions.*

Ievads

Vēl pavisam nesen, 20. gs. beigās, datornoziegumi visā pasaulē nebija liela problēma. Latvijā 1998. gadā bija reģistrēti tikai divi gadījumi, ko varētu nosaukt par datornoziegumiem *(Ķinis, 1999)*. Situācija kardināli mainījās jau pēc dažiem gadiem, kad informācijas tehnoloģiju izmantošana kļuva par ikdienišķu parādību lielam vairumam cilvēku.

Kibernoziedzības izplatīšanās ātrumu veicina trīs tendences:

- arvien vairāk cilvēku ikdienā izmanto internetu;
- arvien biežāk internetu lieto dažādās ierīcēs;
- arvien biežāk ierīces izmanto, lai veiktu tādus uzdevumus kā iepirkšanās un internetbankas pakalpojumi, kas rada risku, ka tiek nodota informācija par personas datiem un naudas *(Jarkina, 2019)*.

Kibernoziegumi ir kļuvuši par galvenajām rūpēm juridiskajā vidē, jo noziedznieki turpina izplatīt traucējošus vīrusus, piekļūt privātajai, biznesa / finanšu informācijai, veikt kiberspiegošanu, izplatīt dažādas ļaunprātīgas programmatūras variācijas, veikt īpašuma un identitātes zādzības, izplatīt ļaunprātīgu tiešsaistes saturu, iebrukt datorsistēmas procesos un tamlīdzīgi apdraudēt valsti vai tās pilsoņus *(Hirst, 2017)*.

Krāpšanas būtība palikusi tā pati – apmānīt, iegūt svešu mantu vai tiesības uz to, ļaunprātīgi izmantojot cilvēku uzticēšanos vai ar viltu, atšķirība ir tikai tā, ka e-noziegumi tiek izdarīti jaunos vides apstākļos. Pārceļoties no "dzīvās" vides uz virtuālo, datornoziegumam ir radušās vairākas priekšrocības tādas kā ģeogrāfisko robežu neesamība, izpildes ātrums un sarežģīta atklāšana.

Pētījuma mērķis ir izpētīt krāpšanas e-vidē tiesiskos aspektus.

Pētījuma objekts – kibernoziegumi.

Pētījuma priekšmets – krāpniecība e-vidē.

Pētījuma uzdevumi:

- noskaidrot datorkrāpšanas jēdziena būtību;
- izpētīt izplatītākās krāpniecības shēmas e-vidē un aktuālākās problēmas;
- izanalizēt noziedzīgus nodarījumus e-vides kontekstā, ņemot vērā Latvijas tiesu praksi.

Par **pētniecības bāzi** tika izmantotas ārvalstu un Latvijas vadošo pētnieku un ekspertu publikācijas, internetā pieejamā informācija un tiesu prakse.

Darbā tika izmantotas teorētiskās izziņas un empīriskās pētniecības metodes.

https://doi.org/10.17770/iss2021.6915

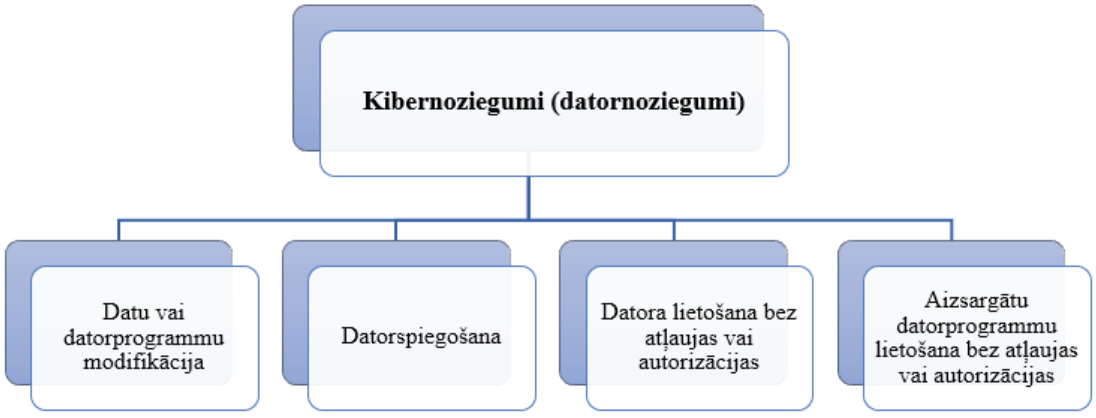
Datorkrāpšanas būtība un aktuālākās problēmas

Krāpšana ir svešas mantas vai tiesību uz tādu mantu iegūšana, ļaunprātīgi izmantojot uzticēšanos vai ar viltu. Pie krāpšanas veidiem var attiecināt ļaunprātīgi izmantošanu uzticēšanos: vainīgais, nolūkā iegūt svešu mantu vai tiesības uz mantu, izmanto līgumiskas vai citādas tiesiskas attiecības, kas pamatotas uz savstarpējo uzticēšanos, un tā rezultātā šo uzticēšanos izmanto pretēji cietušā interesēm; un krāpšanu ar viltu: vainīgais vai nu paziņo nepatiesas ziņas, vai arī noslēpj faktus, kurus viņam vajadzēja paziņot mantas īpašniekam vai tās valdītājam; ka arī būdams maldināts, cietušais mantu vai tiesības uz to atdod labprātīgi, uzskatot, ka tā vainīgajam pienākas. Ja nozieguma priekšmets iegūts no personas, kura nav spējīga saprast savu rīcību vai vadīt savu gribu, nodarījums kvalificējams kā zādzība *(Hamkova, Liholaja, 2009)*.

Tā kā pēc būtības datorkrāpšana ir viens no kibernozieguma veidiem, autore izpētīja vairākus avotus, tajā skaitā starptautiskas zinātniskās publikācijas, kurās tika konstatēta dažādu krāpšanas e-vidē aspektu definēšana, kas aptver tādus jēdzienus kā kibernoziegumi, datornoziegumi, interneta noziegumi, kiberdrošība utt. Izpētot Latvijas Republikas tiesību normas un doktrīnas, autore konstatēja, ka tajās nav atsevišķi definēts termins "kibernoziegums", līdz ar to nav arī vienota jēdziena "krāpšana e-vidē" skaidrojuma. Vairāki tiesību zinātnes eksperti ir mēģinājuši sniegt vispārinošu datornozieguma definīciju. Piemēram, Eiropas Padomes Kibernoziegumu komitejas eksperts U. Ķinis par datornoziegumu uzskata jebkuru ar likumu aizliegtu krimināli sodāmu darbību vai bezdarbību, kur dators vai datortehnoloģijas produkti (datori, skeneri, drukas iekārtas, datorprogrammas, komunikāciju līdzekļi u. c.) izmantoti kā nozieguma priekšmets vai nozieguma rīks ar mērķi ietekmēt datorsistēmu tehniskos un informācijas resursus *(Ķinis, 1999)*. Taču autorei visaptverošākā šķiet ekspertes V. Jarkinas definīcija, kur viņa kibernoziegumus raksturo kā noziedzīgus nodarījumus pret automatizētas datu apstrādes sistēmas drošību – pret konfidencialitāti, pieejamību un integritāti *(Jarkina, 2019)*.

Kibernoziegums (datornoziegums) kā jēdziens pirmo reizi tika minēts Ekonomiskās sadarbības un attīstības organizācijas (turpmāk - OECD) ziņojumā 1983. gadā, apzīmējot ar to ikvienu nelikumīgu, neētisku vai nesankcionētu uzvedību, kas saistīta ar automātisko datu procesu un/vai datu pārraidīšanu *(Schjølberg, Hubbard, 2005)*.

Visu kibernoziegumu pamatā ir krāpniecība vai ar to saistītas darbības (sk. 1. attēlu), jo, gan lietojot svešu datoru, gan modificējot datorprogrammas, gan nodarbojoties ar datorspiegošanu vai izsekošanu, notiek personas, organizācijas vai pat veselas valsts krāpšana.



1. attēls. **Ar datortehnoloģijām saistīto noziegumu klasifikācija** *(autores veidots)*

Piemēram, instalējot spiegu programmatūru datorā vai telefonā, var ierakstīt katru datorā nospiesto taustiņu. Tastatūras darbību spiegotājus bieži izmanto, lai vāktu tādus finanšu datus kā bankas kontu numurus, kredītkaršu rekvizītus, paroles vai PIN kodus. Zvanītājprogrammas tiek izmantotas, lai, lietotājiem nezinot, pārvirzītu iezvanpieslēgumus uz augsta tarifa tālsarunu numuriem. Ir arī tādas programmas, kas bez lietotāja ziņas aktivizē datora kameru un mikrofonu vai ļauj nesankcionēti pieslēgties citiem datoriem uzņēmuma tīklā no "ārpuses". Ar spiegu programmu palīdzību var tikt

savākta informācija par konkrētas datortehnikas lietotāju, kuru tālāk var pārdot kā datu bāzi.

Kibernoziegumu regulējums pirmo reizi starptautisko tiesību jomā parādījās 2001. gadā Eiropas Padomes Konvencijas par kibernoziegumiem ietvaros *(Konvencija par kibernoziegumiem, 2001)*. Taču Konvencijā nav sniegta jēdziena "kibernoziegums" definīcija, paredzot to noregulēt valstu nacionālajos tiesību aktos, tāpēc termins "kibernoziegums" ir uzskatāms par katras nacionālās krimināltiesību doktrīnas radītu jēdzienu.

2019. gada 17. aprīlī stājās spēkā Eiropas Parlamenta un Padomes direktīva (ES) 2019/713 par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem, kas aizstāja Padomes Pamatlēmumu 2001/413/TI. Ar šo direktīvu paredz minimālos noteikumus par noziedzīgu nodarījumu un sankciju definēšanu saistībā ar krāpšanu un viltošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem. Tā veicina šādu nodarījumu novēršanu un palīdzības un atbalsta cietušajiem sniegšanu *(Par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem un ar ko aizstāj Padomes Pamatlēmumu 2001/413/TI, 2019)*.

Krāpnieki vienmēr darbojas ar mērķi vai nu izkrāpt datus, vai finanšu līdzekļus. Biežākie interneta krāpšanas gadījumi ietver krāpšanos uzņēmējdarbībā, krāpšanos ar kredītkartēm, krāpšanos interneta izsolēs, investīciju shēmas, krāpšanos ar "Nigērijas" vēstulēm un preču nepiegādi *(Kavun, 2014)*. Piedāvājot nopelnīt fondu tirgos vai ieguldīt naudu kriptovalūtā, sākumā darījums notiek par nelielu summu, it kā ļauj nopelnīt, un cilvēks ir gatavs lielākam darījumam. Tā viņš ieiet azartā, un, kad summa sasniegusi iespaidīgus apmērus un grib to noņemt, viņam paskaidro, ka tas ir iespējams, samaksājot lielu komisijas naudu. Apkrāptais savā ekrānā redz savu kontu ar lielu summu, bet vieglas peļņas iespēja reizēm padara cilvēku aklu. Lieki piebilst, ka atgūt šo naudu ir pilnīgi bezcerīgi *(Seržants, 2020)*.

Latvijas tiesu pieredze e-krāpšanas kontekstā

Saskaņā ar Krimināllikuma (turpmāk - KL) 177. panta pirmo daļu krāpšana ir svešas mantas vai tiesību uz šādu mantu iegūšana, ļaunprātīgi izmantojot uzticēšanos vai ar viltu. Krāpšana kā viens no mantas nolaupīšanas izpausmes veidiem ietilpst KL 193. panta sastāvā. Savukārt datorkrāpšana saskaņā ar KL 177.[1] pantu ir ar datoriem saistīts noziegums jeb krāpšana automatizētā datu apstrādes sistēmā *(Krimināllikums, 1998)*.

Vēloties iedziļināties Latvijas tiesu praksē kibernoziegumu jomā, autorei diemžēl nācās saskarties ar ierobežotu statistiku un neapkopotiem datiem, jo par individuālo krāpniecību ir veikts maz akadēmisko un izvērtējošo pētījumu, un vadīties tikai no internetā publicētās informācijas. Taču tapa skaidrs, ka noziegumi e-vidē ir saistīti ar milzīgu tumšo statistiku, jo par lielu daļu gadījumu netiek ziņots. Upuri nezina, ka ir par tādiem kļuvuši, viņi notikušo neuztver pietiekami nopietni, viņiem nešķiet, ka ziņošana nesīs rezultātu, vai arī viņi gluži vienkārši nemaz nezina, kur būtu jāvēršas ar ziņojumu. Vienlaikus tādēļ, ka upuri paši aktīvi piedalās sevis apkrāpšanā, pašu vainas sajūta un kauns bieži vien viņus attur no runāšanas par krāpšanas gadījumu. Dažās krāpnieciskajās shēmās pat ir iestrādāti pretziņošanas mehānismi, liekot upuriem shēmas ietvaros veikt prettiesiskas darbības, tādējādi inkriminējot sevi. Ziņojot par krāpniecisko shēmu, cilvēks justos tā, it kā pats atzītos noziegumā *(Eiropas Noziedzības novēršanas tīkls, 2020)*.

Izpētot tiesu prakses lietas par krāpšanu 2008./2009. gadā, kad par krāpšanu internetā iedzīvotāji pat nedzirdēja, bija konstatēti 6 gadījumi, kad personas tika sodītas saskaņā ar KL 177.[1] pantu par krāpšanu automatizētās datu apstrādes sistēmās. Divas personas, kas veica nelikumīgas transakcijas internetbankās, tika sodītas par svešas naudas iegūšanu un mēģinājumu izmantot svešu naudu. Vainīgās personas, izmantojot bankas kontiem piesaistītās attālinātās norēķinu sistēmu lietotāja identitātes datus, t. i., lietotājvārdu, paroli un kodu no bankas izsniegtās kodu kartes, veica nelikumīgas naudas operācijas no citu personu kontiem internetbankā. Četras personas tika sodītas saskaņā ar Krimināllikuma 177.[1] pantu par krāpnieciskām darbībām ar Ungārijas forintu monētu izmantošanu Latvijas latu monētu vietā, lai nelikumīgi iegūtu laimestu spēļu automātos *(Latvijas Republikas Augstākā tiesa, 2008 / 2009)*.

Šobrīd e-krāpšana visā pasaulē attīstās ļoti strauji un apjomīgi. Atsaucoties uz *Swedbank* publiski sniegto informāciju, jāsecina, ka divas trešdaļas jeb 64 % Latvijas iedzīvotāju ir personiski saskārušies ar krāpniecības mēģinājumiem e-pastā, telefoniski vai sociālajos tīklos. 20 % krāpnieku noskatīto upuru

ir arī iekrituši viņu tīklos, piedzīvojot finansiālus zaudējumus *(Multinews.lv, 2019)*.

Iepazīstoties ar vairākiem LR tiesu spriedumiem, autore konstatēja, ka sods par krāpšanos e-vidē lielākoties ir piespiedu darbs, īslaicīga brīvības atņemšana (sākot no 45 dienām), attiecīgas kompensācijas par mantisko zaudējumu, valsts procesuālie izdevumi un stāšanās Valsts probācijas dienesta uzraudzībā. Turklāt vairāki spriedumi, kur vainīgā persona tika sodīta ar brīvības atņemšanu, reāli bija nosacīta soda pasludināšana. Vislielākais sods – 14 gadi – tika piespriests 2017. gadā Latvijas valstspiederīgajam Ruslanam Bondaram par hakeru testēšanas pakalpojumu sniegšanu ASV.

Izpētot Latvijas tiesu praksi un vairāku ekspertu viedokļus, autore pievērsa uzmanību vēl vienai problēmai, proti, Krimināllikuma 193. panta otrās daļas izpratnē maksāšanas līdzekļa izmantošana aptver jebkuru rīcību ar maksājuma kartei piesaistītajā kontā esošajiem naudas līdzekļiem, tāpēc nepatiesu datu ievadīšana automatizētā datu apstrādes sistēmā, lai ietekmētu tās resursus un tādā veidā iegūtu svešu mantu, nav jākvalificē arī pēc Krimināllikuma 177.[1] panta. Par to liecina arī Latvijas Republikas Augstākās tiesas Krimināllietu departamenta 2016. gada 19. septembra lēmums lietā Nr. 11130078713 SKK-496/2016 *(Latvijas Republikas Augstākā tiesas lēmums, 2016, Nr.* SKK-496/2016*)*.

Saistībā ar KL 193. pantu nereti novēroti vairāki kvalifikācijas problēmjautājumi, proti, līdzīgos apstākļos tiesas atšķirīgi vērtē nodarījumus, kas attiecas uz kredīta izkrāpšanu, izmantojot svešu maksāšanas līdzekli – internetbankas palīdzību, tādējādi analizējamā panta vietā piemērojot KL 177., 177.[1] vai 193.[1] pantu. Situācijas, kurās uz vienu faktisko sastāvu var attiecināt vairākas tiesību normas, nav retums, tāpēc bieži vien nepieciešams noskaidrot, vai nepastāv tiesību normu konkurence *(Fogele, 2018)*.

Jāatzīmē, ka šobrīd Latvijā top jauni grozījumi Krimināllikumā, ar kuru pieņemšanu Latvijā tiks pastiprināta aizsardzība pret noziedzīgiem nodarījumiem, kas saistīti ar bezskaidras naudas maksāšanas līdzekļu krāpšanu un viltošanu (kredītkartēm, tiešsaistes iepirkšanos utt.). Grozījumi izstrādāti, lai ieviestu Eiropas Parlamenta un Padomes 2019. gada 17. aprīļa direktīvu (ES) 2019/713 par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem un ar ko aizstāj Padomes pamatlēmumu Nr. 2001/413/TI *(Latvijas Republikas Ministru kabinets, 2021)*.

Secinājumi un priekšlikumi

1. Kibernoziedznieki izdomā arvien jaunus veidus, kā nelikumīgi iegūt finanšu līdzekļus. Šiem noziegumiem ir starptautisks raksturs, kas apgrūtina zaudētās naudas atgriešanu cietušajiem. Naudas līdzekļi tiek ieskaitīti tādās maksāšanas sistēmās kā kriptovalūtas, kā rezultātā to tālākās virzības izsekošana ir ļoti sarežģīta. Tikpat sarežģīti ir atklāt un likvidēt t. s. ļauno programmatūru, piemēram, spiegu programmas, kas mūsdienās spēj veikt sarežģītas krāpnieciskas darbības.
2. Saskaņā ar KL 177. panta pirmo daļu krāpšana ir svešas mantas vai tiesības uz šādu mantu iegūšana, ļaunprātīgi izmantojot uzticēšanos vai ar viltu. Krāpšana kā viens no mantas nolaupīšanas izpausmes veidiem ietilpst KL 193. panta sastāvā. Savukārt datorkrāpšana saskaņā ar KL 177.[1] pantu ir ar datoriem saistīts noziegums jeb krāpšana automatizētā datu apstrādes sistēmā.
3. Analizējot Latvijas tiesu praksi e-krāpšanas kontekstā, autore konstatēja, ka pastāv problēmas noziedzīga nodarījuma satura noteikšanā, tāpēc ir svarīgi nošķirt KL 193. pantu no KL 177. un 177.[1] Autoresprāt, ja pretlikumīgu darbību rezultātā tiek iegūti tādi dati, kas ļauj izmantot svešas personas finanšu instrumentus vai maksāšanas līdzekļus, noziedzīgais nodarījums ir kvalificējams pēc KL 193. panta. Savukārt KL 177. pants ir pielietojams tajos gadījumos, kad datu iegūšana nenotiek, piemēram, tad, kad pati persona labprātīgi (bet krāpšanas iespaidā) ievada savus datus.
4. Tā kā šo noziegumu izmeklēšana ir ļoti sarežģīta, autore uzskata, ka milzīga nozīme ir prevencijas darbam sabiedrības izglītošanā, lai tā prastu atpazīt krāpniekus un neļautos turpmākajām mahinācijām. Lai sevi pasargātu no krāpšanas, iedzīvotājiem jābūt piesardzīgiem un nebūt pārlieku uzticīgiem, komunicējot ar nepazīstamiem cilvēkiem.
5. Tā kā mūsdienās krāpšana e-vidē strauji izplatās un ir grūti novēršama, nepietiek ar likuma grozījumiem atsevišķas valsts ietvaros, ir jāmeklē risinājumi starptautiskā līmenī, piemēram, izveidojot Starptautisko kibernoziegumu apkarošanas biroju, kas operatīvi reaģētu uz plaša mēroga e-krāpniecības shēmām un koordinētu citu valstu attiecīgos dienestus.

Izmantotie avoti un literatūra

1. *Konvencija par kibernoziegumiem* (23.11.2001). Eiropas Savienība. https://likumi.lv/ta/lv/starptautiskie-ligumi/id/1460, sk. 15.03.2021.
2. *Krimināllikums* (17.06.1998). Latvijas Republikas likums. https://likumi.lv/doc.php?id=88966, sk. 10.02.2021.
3. *Par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem un ar ko aizstāj Padomes Pamatlēmumu 2001/413/TI* (17.04.2019). Eiropas Parlamenta un Padomes Direktīva (ES), 2019/713. https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32019L0713, sk.10.02.2021.
4. Eiropas Noziedzības novēršanas tīkls (2020). *Individuālās krāpniecības novēršana.* EUCPN rīkkopu sērija Nr. 13. https://eucpn.org/sites/default/files/document/files/samenvatting%20BG_LV.pdf, sk. 15.04.2021.
5. Fogele, I. (26.06.2018). Krimināllikuma 193. pantā paredzētā noziedzīgā nodarījuma kvalifikācijas problēmjautājumi. *Jurista Vārds,* 26 (1032). https://juristavards.lv/doc/272978-kriminallikuma-193panta-paredzeta-noziedziga-nodarijuma-kvalifikacijas-problemjautajumi/, sk. 29.04.2021.
6. Hamkova, D., Liholaja, V. (2009). *Krimināltiesības. Sevišķā daļa.* http://home.lu.lv/~lilze/PLK/bakalauri_2/kriminaltiesibas_seviska_dala/KT_SEV_Dala_2009_pavasaris_.pdf, sk. 28.04.2021
7. Hirst, V. (2017). *Cybercrime Laws: What Internet Fraud Victims Need to Know*. Retrieved 25.03.2021 from https://www.tripwire.com/state-of-security/security-awareness/cybercrime-laws-what-internet-fraud-victims-need-to-know/
8. Jarkina, V. (2019). *Kibernoziegumi Latvijā*. https://itiesibas.lv/raksti/komercdarbiba/datu-aizsardziba/ kibernoziegumi-latvija/12443, sk. 25.03.2021.
9. Jarkina, V. (25.03.2019). *Kibernoziedzības uzvaras gājiens*. https://itiesibas.lv/public/contents/article_ print/14748, sk. 10.04.2021.
10. Kavun, S., Golubev, V., Trydid, O., Revak, I. (2014). Statistical Analysis of Critical Infrastructure Protection. *Proceedings of the International Conference on Application of Information and Communication Technology and Statistics in Economy and Education ICAICTSEE-2014*, 100, 190-203. Retrieved 10.02.2021 from https://www.proquest.com/openview/bd43b9d0c9e7c04b360e4ccecefaf0c6/1.pdf?pq-origsite=gscholar&cbl =2032294
11. Ķinis, U. (1999). Latvijas Krimināllikums un datornoziegumi. *Jurista Vārds*, 15 (122).
12. Latvijas Republikas Augstākā tiesa (2008 / 2009). *Tiesu prakse lietās par krāpšanu*. https://www.at.gov.lv/files/uploads/files/docs/summaries/2009/tp_krapsana.doc, sk. 15.04.2021.
13. Latvijas Republikas Augstākās tiesas Krimināllietu departamenta 2016. gada 19. septembra lēmums lietā Nr. 11130078713 SKK-496/2016. http://www.at.gov.lv/downloadlawfile/3622, sk. 15.04.2021.
14. Latvijas Republikas Ministru kabinets (04.03.2021). *Likumprojekts "Grozījumi Krimināllikumā"* Tiesību aktu projekti. http://tap.mk.gov.lv/lv/mk/tap/?pid=40496927&mode=mk&date=2021-03-04, sk.25.04.2021
15. Multinews.lv (31.07.2019). *64% iedzīvotāju saskārušies ar krāpšanas mēģinājumiem internetā un telefoniski*. https://multinews.lv/64-iedzivotaju-saskarusies-ar-krapsanas-meginajumiem-interneta-un-telefoniski/, sk. 15.04.2021.
16. Schjølberg, J. S., Hubbard, A. M. (10.06.2005). *Harmonizing National Legal Approaches on Cybercrime.* Retrieved 10.04.2021 from https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf
17. Seržants, K. (2020). *Lamatas internetā: krāpnieki sākuši izmantot jaunas shēmas.* https://jauns.lv/ raksts/zinas/382446-lamatas-interneta-krapnieki-sakusi-izmantot-jaunas-shemas, sk. 15.04.2021.

Summary

Cybercrime has become a major concern in the legal environment today. Criminals are coming up with new ways and schemes to spread disruptive viruses, access private, business / financial information, spy, spread various malware variations, commit property and identity theft, distribute malicious online content, invade computer systems, and threaten any country in the world or its citizens.

All cybercrime is based on fraud or related activities. Moving from a "living" to a virtual environment, cybercrime has several advantages, such as the absence of geographical boundaries, speed of execution and difficult detection. Therefore, the author believes that prevention work in educating the public is important here, so that it can recognize fraudsters and prevent further machinations, moreover, it is not enough to amend the law within a country, solutions should be sought at international level, such as the International Cybercrime large -scale e-fraud schemes and coordinate relevant services in other countries.

Wanting to delve into the Latvian court practice in the field of cybercrime, the author unfortunately had to deal with limited statistics and non-aggregated data, because there have been few academic and evaluative studies on individual fraud and only guided by information published on the Internet. However, it became clear that cybercrime is associated with huge dark statistics, as a large proportion of cases are not reported.