https://doi.org/10.25143/socr.23.2022.2.061-082

Algoritms kā būtiska kaitējuma noteikšanas metode noziedzīgos nodarījumos, kas saistīti ar automatizētu datu apstrādes sistēmu (ADAS)

Algorithm as a Method for Determining Substantial Harm in Crimes which are Related with Automated Data Processing System (ADAS)

Dr. iur. profesors ***Uldis Ķinis***
ORCID: 0000-0002-5573-9887
Rīgas Stradiņa universitāte, Latvija
uldis.kinis@rsu.lv

Mg. iur. ***Ņikita Sinkevičs***
ORCID: 0000-0001-5997-1379
Rīgas Stradiņa universitāte, Latvija
nikita.sinkevics@gmail.com

Abstract

The aim of the article is to analyse the problem of applying substantial harm in offenses against the security of information systems, in particular Paragraph one of Article 241 and the paragraph one and two of Article 243 of the Criminal Law. Although substantial harm is defined in Article 23 of the Law on the Procedures for the Coming into Force and Application of the Criminal Law, the wording of the current law and its application in the court practice of Latvia is still problematic. The authors have studied the European Union and regulations in Latvia on the network and information system, which provides security of services essential to society. The authors concluded that systems which provide essential service and significant impact of service must be recognised as the direct object of the offense of Article 241, Paragraph three and Article 243, Paragraph five of the Criminal Law. Furthermore, it is not necessary to prove existence of harmful effects in order to prosecute these offenses. The authors propose

to introduce a classification of information systems that would functionally cover all existing systems in the country. Therefore, the authors propose to simplify this process of determining significant damage and replace the current procedure with an algorithm. General methods of scientific research and methods of legal interpretation have been used in the research.

Keywords: algorithm, automated data processing system, substantial harm, security incident, non-material loss, criminal delinquency.

Ievads

1999. gada 1. aprīlī stājās spēkā Krimināllikums, un vienlaikus stājās spēkā arī likums "Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību" (turpmāk – Speciālais likums). Speciālā likuma 23. pantā tiek definēti trīs nosacījumi, kurus procesa virzītājam ir pienākums konstatēt, lai Krimināllikuma Sevišķajā daļā paredzētajam noziedzīgajam nodarījumam būtu iespējams konstatēt būtisku kaitējumu, un tie ir šādi:

1) mantiskam kaitējumam jāpārsniedz ne mazāk kā piecu minimālo mēnešalgu kopumu un ar nodarījumu tiek apdraudētas citas ar likumu aizsargātas intereses;
2) nodarīts mantiskais kaitējums, kas nav bijis mazāks par desmit minimālo mēnešalgu kopumu;
3) ievērojami ir apdraudētas citas ar likumu aizsargātās intereses.

2001. gada 21. novembrī Eiropas Padome pieņēma Kibernoziegumu konvenciju (turpmāk – konvencija), kurā paredzēta krimināltbildība par nodarījumiem, kas vērsti pret informācijas sistēmu drošību (turpmāk – ISD) – to pieejamību, integritāti un konfidencialitāti. Lai Latvija varētu pievienoties šai konvencijai, 2005. gada 28. aprīlī tika veikti attiecīgi grozījumi Krimināllikumā, iekļaujot tajā noziedzīgos nodarījumus, kas vērsti pret ISD, tostarp, Krimināllikuma 241. panta pirmo daļu, 243. panta pirmo un otro daļu, kas paredz kvalificējošo pazīmi – būtisku kaitējumu. Savukārt 2020. gadā Krimināllikums tika papildināts ar 145. pantu – šā panta pirmajā daļā par obligātu noziedzīga nodarījuma sastāva pazīmi ir noteikts būtisks kaitējums.

2019. gadā Eirobarometra ziņojumā Nr. 499 (Eiropas Komisija, 2022) teikts, ka 38 % Latvijas respondentu atzinuši, ka bažījas par personīgo datu ļaunprātīgu izmantošanu, 29 % – par tiešsaistes maksājumu drošību, 13 % respondentu bija kļuvuši par cietušajiem saistībā ar identitātes zādzību un sociālo tīklu vai e-pasta uzlaušanu, bērnu pornogrāfijas, naida informācijas izplatīšanu u. tml.

Saskaņā ar *Kantar* aptaujas *Latvia Digital* (*Kantar*, 2021) datiem 2020. gada pavasarī Latvijā vecumā no 16 līdz 74 gadiem internetu lietoja 1 miljons 444 tūkstoši iedzīvotāju, un lietotāju skaits pastāvīgi pieaug.

2018. gadā aprīlī Rīgas Stradiņa universitātes Juridiskās fakultātes zinātniskajā konferencē vairāki referenti uzsvēra, ka tieši būtiska kaitējuma identificēšana bieži kļūst par iemeslu, kāpēc arī uzsāktos kriminālprocesus par kibernoziegumiem nākas izbeigt, jo

nav iespējams pierādīt, ka ar attiecīgām darbībām cietušajiem nodarīts būtisks kaitējums. Savukārt Latvijas Kiberdrošības stratēģijā 2019.–2022. gadam (Aizsardzības ministrija, 2019) ir uzsvērts, ka kibernoziegumu skaits un intensitāte tikai pieaugs, un šā dokumenta 4.5.5. punktā akcentēts, ka jāveic Valsts policijas darbinieku, prokuroru, tiesnešu apmācības, lai efektīvi apkarotu kibernoziegumus.

Stratēģijā tiek izdalīti divu veidu kibernoziegumi:

1) noziegumi, kuriem ADAS ir noziegumu izdarīšanas līdzeklis un mērķis;
2) noziegumi, "kuru nodarījumu var palielināt", izmantojot ADAS.

Pārvēršot šeit teikto par kibernoziegumiem krimināltiesību terminoloģijā, varētu apgalvot, ka tie aptver visus noziedzīgos nodarījumus, kuros ADAS tiek izmantota kā nozieguma rīks, nozieguma priekšmets vai medijs nelikumīgas informācijas aprites nodrošināšanai. Tādējādi, lai efektivizētu kibernoziegumu apkarošanu, būtu vērts apsvērt jautājumu, vai esošais Speciālā likuma būtiska kaitējuma regulējums nebūtu jāpārskata un šī kritērija identificēšana tieši ar nodarījumiem, kas saistīti ar ADAS izmantošanu, vienkāršojama.

Tieši šādu virzienu savā politikā vēlas panākt Eiropas Savienība (turpmāk – ES), gan pieņemot Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un ISD visā ES (turpmāk – NIS1 Direktīva), gan izstrādājot NIS2 Direktīvas priekšlikumu (*The NIS2 Directive COM(2020)82*, 2021), kura mērķis ir stiprināt kiberdrošību ES. Direktīvas šim mērķim paredz radīt vienkāršu un pārskatāmu ADAS sistēmu klasifikāciju un to apdraudējuma pakāpes būtiskas ietekmes kritēriju noteikšanu. Savukārt šī apdraudējuma pakāpe noziedzīgos nodarījumos ir cieši saistīta ar kaitīgām sekām, ko šādi nodarījumi var radīt sabiedrībai. Līdz ar to minētais ir cieši saistīts ar noziedzīgo nodarījumu, kas saistīti ar ADAS, kaitīgo seku izvērtēšanu un identificēšanas vienkāršošanu.

Par būtiskā kaitējuma noteikšanas problēmām ir rakstījis profesors Uldis Krastiņš (2015), profesore Valentija Liholaja (2012) un docente Diāna Hamkova (2012), kā arī profesors Uldis Ķinis (2015), Džena Andersone (2018) u. c. Taču to, ka situācija būtiska kaitējuma noteikšanas jomā īpaši nav mainījusies, apliecina Valsts kontroles 2020. gada revīzijas ziņojumā "Noziedzīgu nodarījumu ekonomikas un finanšu jomā izmeklēšanu un iztiesāšanu kavējošo faktoru izvērtējums" (Valsts kontrole, 2020, 38) konstatētie fakti. Valsts kontrole ir secinājusi, ka kriminālprocesā pastāv problēmas ar "būtiska kaitējuma" izpratni un apstākļiem, kas nepieciešami tā pierādīšanā. Tas nozīmē, ka joprojām krimināltiesību praksē nav vienotas izpratnes par šiem jautājumiem. Būtiska kaitējuma problemātika ir ļoti plašs jautājums, tāpēc šeit tā tiks apskatīta vien tiktāl, cik tā saistīta ar noziedzīgiem nodarījumiem, kas vērsti pret ADAS. Raksta mērķis ir izvērtēt būtiska kaitējuma institūtu noziedzīgos nodarījumos, kas ir vērsti pret ISD, kā arī izstrādāt algoritmu būtiska kaitējuma noteikšanai šāda veida noziedzīgos nodarījumos.

Rakstā ir trīs nodaļas un nobeigums. Pirmajā nodaļā apskatīta būtiska kaitējuma legāldefinīcija un tās piemērošanas aktuālās problēmas, otrajā nodaļā – kiberapdraudējuma būtiskas ietekmes institūts ES un Latvijā, kā arī tiek veikts salīdzinājums ar būtiska kaitējuma noteikšanas kritērijiem Krimināllikumā. Trešajā nodaļā aplūkoti algoritma ieviešanas teorētiskie un praktiskie aspekti būtiska kaitējuma noteikšanā. Nobeigumā ir apkopoti secinājumi, kā arī sniegti priekšlikumi algoritma ieviešanai būtiska kaitējuma noteikšanai.

Raksta sagatavošanā izmantotas vispāratzītas zinātniskās pētniecības metodes un speciālās tiesību interpretācijas metodes.

1. Būtiskā kaitējuma regulējums Krimināllikumā un tā piemērošanas aktuālās problēmas

Terminu "būtisks" tiesību teorijā uzskata par atklāto juridisko terminu. Šis termins nevar pastāvēt pats par sevi, jo tam ir jābūt saistītam ar konkrētu saturu, piemēram, notikumu. Tiesību jomā tā saturu atklāj divi faktori:

1) tiesību joma, kurā termins ir piemērojams;
2) konkrētā tiesiskā attiecība, kas rada, groza vai izbeidz juridiskus faktus.

Krimināltiesībās būtiskā kaitējuma institūts ir plaši izplatīts daudzviet pasaulē. Arī pirms Krimināllikuma pieņemšanas – toreizējā Latvijas PSR Krimināl kodeksā – vairākos pantos noziedzīgā nodarījuma obligāta pazīme bija būtisks kaitējums. Tāpēc ir pašsaprotami, ka Krimināllikuma eksperti, izstrādājot Krimināllikuma Sevišķo daļu, turpināja šo institūtu attīstīt un vairākos noziedzīgos nodarījumos iekļāva to kā objektīvās puses obligāto pazīmi, kas nošķir noziedzīgu nodarījumu, par kuru izdarīšanu paredzēta krimināl atbildība, no citiem pārkāpumu veidiem. Krimināllikumā iekļautie nodarījumi, kas saistīti ar ADAS nelikumīgu vai patvaļīgu izmantošanu, visi ir konstruēti tā, ka tieši būtisks kaitējums ir galvenais apstāklis, kas noteic, vai par konkrētām darbībām vainojamai personai ir nosakāms krimināl sods vai arī var piemērot citus ietekmēšanas līdzekļus.

Konvencija, definējot desmit ar ADAS saistītus noziedzīgus nodarījumus, speciāli neparedzēja kaitīgo seku apmēru kā pamatu darbību kriminalizēšanai. Taču konvencija elastīgi atstāja dalībvalstīm brīvas rokas lemt, vai atbildībai par patvaļīgu piekļuvi ADAS un tajā esošo datu traucēšanu ir nosakāmi papildu kritēriji. Piemēram, konvencijas 1. pants par tādu paredzēja "sistēmas drošības līdzekļu pārvarēšanu vai citu negodīgu nodomu". Savukārt saistībā ar datu un sistēmu traucēšanu konvencijas paskaidrojošā ziņojumā (*Council of Europe*, 2001, *8–12*) norādīts, ka krimināl atbildībai par šiem nodarījumiem kā kritēriju dalībvalstis var noteikt arī nopietnu (angļu val. *serious*) kaitējumu.

Latvijas Republikas Krimināllikuma 241. panta pirmajā daļā paredzēti alternatīvi papildu kritēriji: 1) sistēmas aizsardzības līdzekļu pārvarēšana un 2) situācija, kurā darbības izdarītas bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības,

kā arī jābūt trešajam kritērijam – 3) būtiskam kaitējumam, kuru procesa virzītājam obligāti ir jāpierāda, ja sekas iestājušās pirmajā vai otrajā kritērijā paredzēto darbību rezultātā. Līdzīgu konstrukciju likumdevējs ir izmantojis arī Krimināllikuma 243. panta pirmajā daļā, kurā paredzēta atbildība par nelikumīgu rīcību ar ADAS datiem, un otrajā daļā, kurā paredzēta atbildība par ADAS darbības nelikumīgu traucēšanu, kas iestājas tikai tad, ja ar šīm darbībām radīts būtisks kaitējums. Pēc būtības likumdevēja pieeja ir pragmatiska – ievērojot to, ka kiberapdraudējumu apjoms pasaulē dramatiski pieaug, nebūtu prātīgi uzlikt par pienākumu uzsākt kriminālvajāšanu par ikvienu patvaļīgas piekļuves, datu vai ADAS traucēšanas gadījumu, bet tā jāsāk tikai par tiem nodarījumiem, kuru rezultātā cietušajiem radies būtisks kaitējums.

Būtiskā kaitējuma kritēriji ir noteikti Speciālā likuma 23. pantā (Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību, 1998). Taču šeit sākas problēma, jo izrādās, ka cietušajiem (ADAS īpašniekiem vai arī tiesiskajiem valdītājiem) ar objektīviem pierādījumiem ir gandrīz neiespējami pierādīt, ka nodarīts būtisks kaitējums, jo, godīgi atzīsim, ne katrs cietušais spēj pierādīt, ka nodarījuma pret ISD rezultātā ir radies zaudējums, kas ir lielāks par piecām minimālajām mēnešalgām, un aizskartas ir arī citas ar likumu aizsargātās intereses. Teorētiski ikvienam procesa virzītājam būtu jāsaprot un jāspēj izskaidrot cietušajiem, kā būtu jāaprēķina būtiskais kaitējums. Diemžēl lielākā daļa procesa virzītāju nespēj to izdarīt, un iemesls – viņiem vienkārši trūkst nepieciešamo juridisko zināšanu, kā atklātos juridiskus jēdzienus vai vērtējamo jēdzienu piepildīt ar konkrētu saturu.

Šobrīd ir radusies absurda situācija, ka teorijā minētās atziņas, kā arī Augstākās tiesas secinājumi ne vienmēr ir piemērojami praksē. Piemēram, Augstākās tiesas apkopojumā "Tiesu prakse lietās, kurās noziedzīga nodarījuma sastāva pazīme ir būtisks kaitējums" (Hamkova, 2018, *62*) Secinājumu daļas 9. punktā Senāta Krimināllietu departaments ir atzinis: "Lai atzītu, ka ar nodarījumu ir radīts mantisks zaudējums, jāņem vērā, ka tam jābūt reālam, nevis varbūtējam." Tas nozīmē, ka, nosakot mantisko zaudējumu apmēru ADAS, netiek ņemta vērā neiegūtā peļņa, kuru dīkstāves dēļ nespēs saņemt cietušais. Savukārt tas daļēji ir pretrunā ar praksi, ko realizē absolūti lielākā daļa konvencijas dalībvalstu. Piemēram, Apvienotās Karalistes Prokuroru kodeksā ir uzsvērts, ka kaitējuma apmēra noteikšanā tiesas tulko šo terminu liberāli, iekļaujot šajā jēdziena arī tādu kaitējumu, kas var izrietēt no notikuma (*Crown Prosecution Service*, 2021).

1.1. Drošības incidenta rezultātā radīto ADAS zaudējumu tipoloģizācija

Drošības incidents krimināltiesību izpratnē ir tīšs nodarījums, kas vērsts pret ADAS integritāti, pieejamību vai konfidencialitāti (Informācijas tehnoloģiju drošības likums, 2010). Pasaulē ISD pētījumos tiek izmantotas dažādas sistēmu klasifikācijas metodes drošības incidenta rezultātā radīto risku izvērtēšanai, piemēram, pēc darbinieku skaita: 1–5, 5–25, 25–50, 50–100 utt.

Informācijas tehnoloģiju drošības likumā (turpmāk – ITDL) ir lietoti šādi termini: "*sistēmas, kas sniedz būtiskus pakalpojumus, pamatpakalpojumus, digitālos pakalpojumus, kuru sniegšana ir atkarīga no informācijas tehnoloģijām*". Taču ārpus šīs klasifikācijas paliek mazie e-komersanti, kas savas darbības nodrošināšanai izmanto ADAS; dažādas nevalstiskās organizācijas, kas digitālajā vidē sniedz informācijas pakalpojumus; kā arī personas, kas ADAS izmanto savām personiskajām vajadzībām vai arī sniedz sīkus pakalpojumus.

Saskaņā ar ES klasifikāciju mikrouzņēmumu kategorijā ietilpst uzņēmumi, kuros ir nodarbināti mazāk nekā 10 darbinieki un kuru gada apgrozījums un / vai gada bilances kopsumma nepārsniedz 2 miljonus eiro. Mazo uzņēmumu kategorijā ietilpst uzņēmumi, kuros ir nodarbināti mazāk nekā 50 darbinieki un gada apgrozījums un / vai gada bilances kopsumma nepārsniedz 10 miljonus eiro. Savukārt vidējo uzņēmumu kategorijā ietilpst uzņēmumi, kuros ir mazāk nekā 250 darbinieku un gada apgrozījums nepārsniedz 50 miljonus eiro un / vai gada bilances kopsumma nepārsniedz 43 miljonus eiro (Regula (ES) 651/2014, 2014).

Tādējādi var secināt, ka katrai valsts teritorijā esošajai ADAS ir sava sociālā funkcija. Tieši sociālā funkcija ir tā, kas nosaka ar likumu aizsargāto interešu būtiskumu. Tāpēc ir svarīgi saprast, kā veidojas kaitējums ADAS, jo neatkarīgi no sistēmu klasifikācijas metodes jebkuru nodarījumu pret ISD raksturo turpmāk minētā tipoloģija.

Marks Horonijs (*Horony,* 1999) uzskata, ka drošības incidenta rezultātā ADAS radušies zaudējumi ir iedalāmi taustāmos (angļu val. *tangible*) un netaustāmos (angļu val. *nontangible*) zaudējumos. Taustāmie zaudējumi ir tieši saistāmi ar incidenta rezultātā radītajām tiešajām izmaksām, ieskaitot pavadītās darba stundas sistēmas darbības atjaunošanai, darbinieku dīkstāves izmaksas, kas radušās sistēmas darbības pārtraukuma dēļ, jaunās programmatūras un tās instalēšanas izmaksas. Savukārt pie netaustāmiem zaudējumiem, pēc Horonija domām, pieder organizācijas vai komersanta reputācija, risks zaudēt klientus un saņemt juridiska rakstura pretenzijas, piemēram, apdrošināšanas kompānijas var celt apdrošināšanas likmes, zaudētās informācijas vērtība, peļņas zaudēšana, datu pārraides konfidencialitātes riski u. tml.

Nīderlandes pētnieki (*Michel, Bauer, & Tabatabaie*, 2009) zaudējumus iedala šādās kategorijās: tiešos un netiešos zaudējumos, un netiešie izdevumi vēl var būt iedalāmi nepārprotamos, piemēram, kā drošības sistēmas uzlabošanas izmaksas, un citos netiešajos izdevumos, uz kuriem varētu attiecināt reputācijas zaudēšanu, peļņas samazināšanos u. tml. Turklāt viņi uzsver, ka ir svarīgi, lai kaitējuma aprēķins būtu vispusīgs, taču vienlaikus tam ir jāizslēdz zaudējumu uzskaitījuma dublēšanās. Protams, kaitējuma apmēra noteikšanu nedrīkstētu saistīt tikai ar "tīru" cietušā ADAS īpašnieka vai tiesiskā valdītāja subjektīvo uztveri, kura saistīta ar kaitējuma noteikšanu, bet nav pamatota ar objektīviem pierādījumiem. Vienlaikus šo procesu nedrīkst padarīt par birokrātisku šķērsli, kura dēļ faktiski netiek sasniegts krimināltiesību galvenais uzdevums, t. i., aizsargāt savu iedzīvotāju pamattiesības un no tām izrietošās likumiskās intereses.

1.2. Būtiskais kaitējums – īss ieskats tik nesenajā vēsturē

Viens no šīs publikācijas autoriem – Uldis Ķinis – no 1981. līdz 2006. gadam strādāja par tiesnesi Kuldīgas rajona tiesā. Gatavojot šo rakstu, pārrunājot ar kolēģiem, pārlasot tā laika krimināltiesību komentārus, jāatzīst, ka nenāk atmiņā gadījumi, kad būtiska kaitējuma konstatēšana kriminālprocesā būtu radījusi kādas nopietnas diskusijas.

Var minēt divus piemērus. Pirmais saistīts ar huligānismu, un ļaunprātīga huligānisma pazīme bija būtiska sabiedrības interešu traucēšana. Praksē par ļaunprātīgu tas tika atzīts tad, ja ar huligāniskām darbībām bija traucēts uzņēmuma vai iestādes darbs vairāk par 30 minūtēm. Otrais gadījums – kādai sirmgalvei tika nozagti pieci rubļi, bet tiesa, ievērojot to, ka tie bija vienīgie viņas iztikas līdzekļi un līdz pensijai viņa bija atstāta vispār bez līdzekļiem, atzina, ka ar šo zādzību apsūdzētais nodarījis cietušajai būtisku kaitējumu. Tā bija visiem saprotama pieeja: tiesai bija kompetence izvērtēt, kas ir vai nav būtisks kaitējums. Turklāt šo būtisko kaitējumu varēja identificēt gandrīz ikviens tiesībaizsardzības iestāžu atbildīgais darbinieks.

1998. gadā tika pieņemts Krimināllikums un Speciālais likums, kurā definēts būtiskais kaitējums un noteikti tā piemērošanas kritēriji, kas ietver mantiskos un nemantiskos kritērijus. Tomēr šo kritēriju piemērošana rada problēmas. To atzīst arī Diāna Hamkova (Hamkova, 2018, *17*), rakstot, ka būtiskā kaitējuma konstatēšanā un pamatošanā ir daudz nekonkrētību. Šim viedoklim var piekrist, jo īpaši par gadījumiem, kuros noziedzīgs nodarījums ir vērsts pret ISD.

1.3. Speciālā likuma 23. pantā noteikto kritēriju būtiskā kaitējuma noteikšanai piemērošanas iespējas saistībā ar nodarījumiem, kas vērsti pret ISD

Iepriekš jau tika minēts, ka Speciālā likuma 23. panta pirmajā daļā paredzēti trīs kritēriji būtiskā kaitējuma noteikšanai. Pirmajā punktā noteiktais kritērijs satur divus kumulatīvus apakškritērijus, proti, materiālo zaudējumu minimālo slieksni un vērtējamo kritēriju – citas ar likumu aizsargātas intereses. Otrais punkts satur mantisko kritēriju – desmit minimālo mēnešalgu kopumu, un trešais kritērijs ietver to, pie kādiem apstākļiem var tikt konstatēts būtisks kaitējums, kas saistāms ar "ievērojamu citu ar likumu apdraudētu interešu aizskārumu. Var piekrist Jurijam Lomonovskim, ka vārdu kopa "citas intereses" norāda uz nemantiskajām interesēm, kas cietušajam radušās saistībā ar konkrēto nodarījumu.

Krimināllikumā grupas objektu "Informācijas sistēmu drošība" veido elementu triāde: **pieejamība, konfidencialitāte un integritāte**. Tāpēc procesa virzītājam ir precīzi jāidentificē tiešais nodarījuma objekts, proti, vai tas ir vērsts tikai pret vienu ISD pazīmi – pieejamību (Krimināllikums, 241. panta pirmā daļa) –, vai pret konfidencialitāti (Krimināllikums, 243. panta pirmā daļa), vai arī pret visām trim ISD pazīmēm (Krimināllikums, 243. panta otrā daļa). Savukārt, ja pārējās ISD triādes pazīmes

neietilpst konkrētā nodarījuma priekšmetā vai tiešajā apdraudējuma objektā, tad tās var izmantot par pamatu, lai no šiem elementiem atvasinātu un pamatotu aizskarto interesi.

Termins "interese" juridiskajā literatūrā ir skaidrots vairākkārt (Liholaja & Hamkova, 2012; Krastiņš, 2012), tomēr tiesību piemērotājiem tas joprojām sagādā nopietnas problēmas. Tiesību zinātnē termins "interese" ir vērtējamais kritērijs. Interese ir dzinulis, kas liek personai kaut ko darīt, tomēr dzinuļi var būt vērsti gan uz nelikumīgu, gan uz likumīgu darbību. To, vai interese ir aizsargājama vai gluži pretēji – nepieļaujama, nosaka tiesības. Herberts Laube (*Herbert David Laube*) norāda, ka "jebkurā kultūrā tikai leģitīmi aizsargātas intereses nosaka valstī pastāvošo tiesību jomu" (*Laube*, 1949). Taču nevajadzētu vārdus "interesei ir jābūt garantētai ar likumu" saprast tā, ka likumiska interese personai rodas tikai tad, ja joma ir speciāli regulēta. Tāpēc likumīgās intereses saturu nav iespējams definēt likumā, bet tas skaidrojams tiesību piemērošanas procesā. Cilvēkam jau dabiski piemīt vēlmes un intereses, kas nemitīgi dzen uz priekšu, ļauj radīt jaunus izgudrojumus un veikt atklājumus. Tieši dabiskā interese ir pamatā tam, kādu sabiedrība vēlas veidot tiesību sistēmu. Tā arī rodas aizsargājamās tiesības un no tām izrietošās intereses.

Tāpēc neizpratni rada Augstākās tiesas apkopojuma (Hamkova, 2018, *62*) Secinājumu daļas 11.1. punkts, kurā izvirzīto prasību norādīt "*konkrētu personu, kuras interesēm būtisks kaitējums radīts, tiesību aktu, kurā šīs intereses aizsardzība nostiprināta, kā arī aprakstīt, kā tieši kaitējums norādītajai interesei ir izpaudies*," citādāk kā par "birokrātiju" nosaukt diezin vai var, jo neizdevās atrast nevienu valsti, kur būtiskā kaitējuma pamatošanai tiktu izvirzītas tik striktas prasības. Būtiska kaitējuma jēdziens krimināltiesībās tiek piemērots daudzu Eiropas valstu krimināltiesībās, taču tur nodarījumiem, kas vērsti pret ISD, ir izveidojusies jau stabila prakse.

Latvijā ar stabilu tiesu praksi nodarījumos pret ISD lepoties nevar. Piemēram, baltkrievu krimināltiesību pētnieki (*Stuk, Turko* u. c., 2017) norāda, ka tiesu praksē lietās par ISD tiek lietoti šādi būtiskā kaitējuma pamatojumi: piekļuve ar mērķi izdarīt citu noziegumu, ierobežotas lietotāju līgumtiesiskās attiecības, nelikumīga likumisko īpašnieku identitātes piesavināšanās, lai piekļūtu citiem interneta resursiem u. tml. Līdzīgu argumentāciju izmanto arī Vācijas un Krievijas tiesas, kas būtisko kaitējumu ADAS pamato ar zaudējumu tipoloģijā uzskaitītajiem nemantisko zaudējumu kritērijiem. Katrs no šiem apstākļiem var būt par pamatu būtiska kaitējuma noteikšanai. Taču šie elementi ne vienmēr ir tieši likumā regulēti. Te nu ir skaidrs, ka pie esošās prakses nemantiskie zaudējumi vispār nevar tikt ņemti vērā, jo diezin vai katram reputācijas riskam, informācijas vērtības zudumam būtu iespējams piemeklēt konkrētu tiesību normu. Tāpēc jāpiekrīt Horonijam (*Horony,* 1999), ka visi iepriekš uzskaitītie faktori (mantiskie un nemantiskie) būtu vērtējami kā kaitējums, kas radies cietušajam kiberuzbrukuma gadījumā. Arī Krievijas Krimināl kodeksa komentārā par 274. pantu "ADAS ekspluatācijas vai tīkla noteikumu pārkāpšana" (*Verhovnyj Sud Rossijskoj Federacii*, 2008) ir uzsvērts, ka būtiskais kaitējums ir vērtējamais jēdziens,

kas ietver gan tiešos materiālos zaudējumus, gan arī citu kaitējumu, piemēram, morālo, kas nodarīts ADAS īpašniekam vai tiesiskajam valdītājam. Līdzīgi ir risināms jautājums par ievērojamu interešu apdraudējumu. Tā būtu pietiekami saprātīga pieeja. Taču, ja eksperti un likumdevējs šādu pieeju neatbalsta, tad ir nepieciešams būtiskā kaitējuma noteikšanai noziedzīgos nodarījumos, kas vērsti pret ISD, veidot speciālu pielikumu, kurā tiktu iekļauti skaidri un viegli identificējami kritēriji visām ADAS, grupējot tās pēc sociālā nozīmīguma un apdraudējuma pakāpes – sekām, kas var iestāties noziedzīga nodarījuma rezultātā.

2. Informācijas tehnoloģiju (ADAS) klasifikācija un drošības incidenta būtiskas ietekmes jēdziens

2021. gada janvārī Latvijā bija reģistrēti 1,67 miljoni interneta lietotāju, interneta izplatība valstī – 88,9 % (*Kemp*, 2021). Ja valstī ir vairāk nekā 1,6 miljoni interneta lietotāju, tad ir skaidrs, ka ADAS, kas tiek izmantotas šādas komunikācijas nodrošināšanai, gādā ne tikai par valstij būtisku informācijas pakalpojumu saņemšanu, bet tiek izmantotas arī dažādu citu sabiedrisko funkciju un privātpersonu likumisko interešu realizēšanai.

Kopš 2020. gada drošības incidentu novēršanas institūcija CERT.LV uzskaita apdraudējumus pēc šādiem kritērijiem:

1) cik būtiskas sekas šis apdraudējums ir radījis vai radīs;
2) cik nozīmīgu iestādi, uzņēmumu vai cik plašu sabiedrības daļu apdraudējums ietekmē.

Atbilstoši šiem kritērijiem CERT.LV izmanto sešpakāpju (no C1 līdz C6) incidentu novērtēšanas sistēmu, kurā C6 ir ikdienas apdraudējumi, kas ietekmē atsevišķus IT pakalpojumu saņēmējus un kam nav nozīmīgas ietekmes uz uzņēmumiem vai valsts un pašvaldību iestādēm – tie ir 322 536 incidenti (98,7 % no visiem incidentiem); C5 – mēreni apdraudējumi, kam ir neliela ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm – 2770 incidenti (tas ir, 0,85 % no visiem incidentiem). Savukārt C4 un C3 incidenti jau ir vērtējami kā apdraudējumi ar būtisku ietekmi. Tā, piemēram, 2021. gadā CERT.LV reģistrēti 1252 (0,38 %) drošības incidenti ar būtisku ietekmi (C4 kategorija) un 118 (0,04 %) drošības incidenti, kas atbilst C3 kategorijai, kas klasificēti kā nozīmīgs apdraudējums ar plašu ietekmi uz komerciālo sektoru vai valsts un pašvaldību iestādēm (sk. 1. tab.). C3 apdraudējuma rezultātā skarta 471 persona, C4 apdraudējuma rezultātā – 1203 personas (sk. 2. tab.) (CERT.LV, 2022).

Tāpēc būtiskā kaitējuma noteikšanas algoritma veidošanā ir svarīgi veikt visu valstī esošo ADAS klasifikāciju. Vispirms visas ADAS var sadalīt sistēmās, kas sniedz sabiedrībai būtisku informācijas pakalpojumu, un sistēmās, kas sniedz pakalpojumus, bet nekvalificējas būtiska sabiedrības pakalpojuma statusam, un šai grupai pieder absolūtais ADAS vairākums.

1. tabula. Kopējais apdraudēto unikālo IP adrešu skaits sadalījumā pa apdraudējuma kategorijām (2021. gads)

C6	C5	C4	C3	C2	C1
322 536	2770	1252	118	—	—

Avots: CERT.LV, 2021.

2. tabula. Skarto iedzīvotāju, institūciju vai uzņēmumu kopējais skaits sadalījumā pa apdraudējuma kategorijām (2021. gads)

C6	C5	C4	C3	C2	C1
306 503	17 389	1203	471	582	528

Avots: CERT.LV, 2021.

2.1. Būtiskā informācijas pakalpojuma jēdziens

Atkarībā no tā, uz kuru tiesību nozari pakalpojums ir attiecināms, mainās arī pakalpojuma tiesiskās reglamentācijas pakāpe. Piemēram, ja informācijas pakalpojums saistīts ar komercdarbību, tad komersantu aizsargā Satversmes 105. pants, jo ierobežot komercdarbību valsts var tikai tad, ja pastāv Satversmes 116. pantā noteiktie leģitīmie mērķi. Jāpiebilst, ka par leģitīmo mērķi ir atzīta arī sabiedrības drošība un demokrātiskas valsts iekārtas aizsardzība. Valsts drošība ir viena no svarīgākajām valsts varas funkcijām, un kiberdrošība ir valsts drošības sastāvdaļa. Savukārt kiberdrošības mērķis ir "droša, atvērta, brīva un uzticama kibertelpa, kurā ir garantēta, valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta saņemšana un sniegšana, un indivīda cilvēktiesības tiek ievērotas kā fiziskajā, tā virtuālajā vidē" (Aizsardzības ministrija, 2019, *3*). Tādējādi var secināt, ka būtisks informācijas pakalpojums ir saistāms ar valsts varas funkciju un tas ir publisko tiesību regulēšanas objekts. Mūsdienās daudzas valsts funkcijas pilda arī privātais sektors un nevalstiskās organizācijas, piemēram, finanšu jomā – kredītiestādes u. tml. Tāpēc arī šādu ADAS sniegto pakalpojumu pārtraukšana vai ierobežošana var ietekmēt sabiedrisko kārtību, sabiedrības labklājību, nemaz nerunājot par sabiedrisko drošību un demokrātiskas valsts iekārtas apdraudējumu. Tas ir nostiprināts ITDL 2. pantā, kurā par subjektiem, kas var sniegt būtisku informācijas pakalpojumu, ir atzītas gan publiskās personas (valsts, pašvaldības), gan arī privāto tiesību juridiskās personas.

2.2. Informācijas pakalpojuma būtiskuma noteikšanas kritēriji

Iepriekšējā apakšnodaļā tika noskaidrots, ka sabiedrībai būtisks informācijas pakalpojums ir atkarīgs no diviem apstākļiem:

1) no tā, kam attiecīgā informācijas tehnoloģija pieder;
2) no jomas, kurā pakalpojums tiek sniegts, vai tā radītās sekas var tikt atzītas par tādām, kas apdraud demokrātiskas valsts būtisku funkciju izpildi.

Šīs informācijas tehnoloģijas nosacīti var iedalīt šādi:

1) kritiskā informācijas tehnoloģiju infrastruktūra, kas sniedz sabiedrībai būtisku informācijas pakalpojumu;
2) pamatpakalpojumi;
3) digitālo pakalpojumu sniedzēji;
4) valsts varas un pašvaldības institūcijas;
5) pakalpojumi, kuru iespējamo kaitīgo seku ietekmi uz sabiedrības drošību var atzīt pēc publiskās personas lūguma, ievērojot konkrētus faktiskos apstākļus.

Kritiskā informācijas tehnoloģiju infrastruktūra. Tā ir kritiskās infrastruktūras sastāvdaļa, jo ir nepieciešama, lai ADAS, kas veic datu apstrādi, nodrošinātu kritiskās infrastruktūras sniegto informācijas pakalpojumu nepārtrauktību gan reālā vidē, gan arī tiešsaistē. ITDL 3. pantā noteikts, ka kritisko informācijas tehnoloģiju infrastruktūru aizsargā, lai nodrošinātu valstij un sabiedrībai būtisku pamatfunkciju veikšanu. To atbilstoši Nacionālās drošības likumam reglamentē Ministru kabinets (turpmāk – MK) saskaņā ar 2011. gada 1. februāra MK noteikumiem Nr. 100 "Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība". Latvijā informācija par automatizētām datu apstrādes sistēmām, kas iekļautas kritiskajā informācijas tehnoloģiju infrastruktūrā, ir valsts noslēpums. Taču, izanalizējot dokumentu "Nacionālās drošības koncepcija", var secināt, ka šādā infrastruktūrā tiek iekļauti valsts reģistri, sistēmiskas banku informācijas tehnoloģijas, veselības aprūpes sistēma un citi sabiedrības drošībai svarīgi objekti.

Svarīgi ir uzsvērt, ka šo sistēmu klasifikācija balstās uz diviem kritērijiem:

1) sistēmu piederību (valstij, pašvaldībai vai komersantam, kas darbojas attiecīgā nozarē);
2) riska faktoru (būtisks un apgrūtinošs).

2018. gada 14. maijā visās ES dalībvalstīs stājās spēkā NIS1 Direktīva, kuras 14. panta ceturtajā daļā noteikts, ka, vērtējot apdraudējuma ietekmes būtiskumu, ir jāņem vērā vismaz trīs kritēriji: skarto **lietotāju skaits**, **ilgums** un **ģeogrāfiskā izplatība**. Turklāt NIS1 Direktīvas apsvērumu 53. pantā norādīts, ka prasībām ir jābūt samērīgām ar risku, ko rada attiecīgā tīklu vai informācijas sistēma. Tādējādi NIS1 Direktīva uzliek par pienākumu dalībvalstīm pamatpakalpojumu sniedzējus klasificēt daudz detalizētāk un precīzāk.

Jebkurš drošības incidents, kas vērsts pret kritiskajā informācijas tehnoloģiju infrastruktūrā iekļautu ADAS, satur Krimināllikuma 241. panta trešās daļas un 243. panta piektās daļas noziedzīga nodarījuma pazīmes, un atbilstoši jurisdikcijai šādu nodarījumu novērtēšana ir Valsts drošības dienesta kompetencē. Taču kritiskā informācijas tehnoloģiju infrastruktūra ir tikai neliela daļa no sistēmām, kas sniedz sabiedrībai būtiskus pakalpojumus.

Pamatpakalpojums. NIS1 Direktīvas 4. panta 4. punktā noteikts, ka pamatpakalpojumu sniedzējs ir tāda veida publiska vai privāta vienība, kā minēts 2. pielikumā, kas atbilst 5. panta 2. punktā noteiktajiem kritērijiem. NIS1 Direktīvas 5. panta pirmajā daļā noteikts, ka dalībvalstīm līdz 2018. gada 9. novembrim bija pienākums identificēt vienības, kas tiks uzskatītas par pamatpakalpojumu sniedzējiem.

NIS1 Direktīvas 5. panta otrajā daļā noteikti vienoti kritēriji, pēc kuriem identificējami pamatpakalpojumi. Tie ir šādi:

1) vienība sniedz pakalpojumu, kas ir būtisks īpaši svarīgu sabiedrisku un / vai ekonomisku darbību nodrošināšanai;
2) minētā pakalpojuma sniegšana ir atkarīga no tīklu un informācijas sistēmām;
3) incidentam būtu būtiska traucējoša ietekme uz minētā pakalpojuma sniegšanu.

NIS1 Direktīvas 6. pantā sniegts kritēriju minimums, kas dalībvalstīm jāņem vērā, vērtējot būtisko traucējošo ietekmi uz pakalpojuma sniegšanu, tostarp lietotāju skaitu, pakalpojuma sniedzēja tirgus daļu, ietekmi, kādu drošības incidents varētu nodarīt ekonomikai un sabiedriskām darbībām vai sabiedrības drošībai.

Savukārt 2. pielikumā ir definētas jomas, kuru ietvaros pakalpojumu sniedzēji būtu atzīstami par pamatpakalpojuma sniedzējiem. Tā ir enerģētika, transports, banku nozare, finanšu tirgus infrastruktūras, veselības nozare, dzeramā ūdens piegāde un izplatīšana un digitālā infrastruktūra (interneta plūsmu apmaiņas punkts, domēnu nosaukumu sistēma, augstākā līmeņa domēnu nosaukuma reģistrs).

Atbilstoši NIS1 Direktīvai tika veikti grozījumi arī ITDL, papildinot to ar 3.[1] pantu "Pamatpakalpojuma sniedzējs, digitālā pakalpojuma sniedzējs un digitālā pakalpojuma pārstāvis".

Šā panta pirmajā daļā noteikts, ka pamatpakalpojuma sniedzējs ir valsts vai pašvaldības institūcija vai privātpersona, kas veic saimniecisko darbību Latvijā un sniedz:

1) finanšu pakalpojumus;
2) pakalpojumus, kas atkarīgi no informācijas tehnoloģijām;
3) pakalpojumus, kuru pārtraukšana informācijas tehnoloģiju incidenta rezultātā var radīt sabiedrībai būtisku traucējošu ietekmi.

Jāuzsver, ka "pamatpakalpojums" nav identisks termins "informācijas tehnoloģiju kritiskajai infrastruktūrai", jo pamatpakalpojumu statusu saskaņā ar MK noteikumu Nr. 43 9. punktu piešķir atbildīgā ministrija. Savukārt šo noteikumu 10. punktā norādīts, ka atbildīgā ministrija reizi divos gados izvērtē, vai šāds statuss ir saglabājams vai arī pakalpojums neatbilst ITDL 3.[1] pantā noteiktajiem kritērijiem. Turklāt lēmums par to, vai ir saglabājams vai maināms pamatpakalpojuma saturs, ir jāpieņem Administratīvā procesa likuma kārtībā un jāpaziņo arī pamatpakalpojuma sniedzējam. Līdz ar to šādu lēmumu pakalpojumu sniedzējs var apstrīdēt administratīvajā tiesā. No tā var secināt, ka jurisdikcija par nodarījumiem, kas saistīti ar patvaļīgu piekļuvi vai datu vai sistēmu darbības traucēšanu šajā ADAS kategorijā, ir Valsts policijas kompetence.

Digitālo pakalpojumu sniedzējs. ITDL 3.[1] panta otrajā daļā noteikts, ka digitālo pakalpojumu sniedzējs ir privāto tiesību juridiskā persona, kas:

1) veic saimniecisko darbību Latvijas Republikā un sniedz tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas vai mākoņdatošanas pakalpojumu kādā no Eiropas Savienības valstīm;
2) veic saimniecisko darbību ārpus Eiropas Savienības un digitālo pakalpojumu Latvijas Republikā sniedz ar pilnvarota pārstāvja palīdzību.

Savukārt šā panta trešajā daļā ir noteikts, ka par digitālā pakalpojuma sniedzēja pārstāvi var būt jebkura fiziska vai privāto tiesību juridiskā persona, kas veic saimniecisko darbību Latvijas Republikā.

Valsts pārvalde. Šajā sektorā iekļautas visas informācijas tehnoloģijas, kas tiek izmantotas, lai valsts un pašvaldību institūcijas, izpildot konkrētu valsts funkciju, spētu realizēt e-pārvaldes pakalpojumus sabiedrībai. Saskaņā ar NIS2 Direktīvas priekšlikuma 1. pielikumu šī infrastruktūra atzīstama par būtisku objektu. Turklāt šai kategorijai piederošās ADAS nav uzskatāmas par kritisko informācijas tehnoloģiju infrastruktūru.

Pakalpojumi, ko par būtiskiem var atzīt, ievērojot konkrētos faktiskos apstākļus un iespējamo kaitīgo seku ietekmi uz sabiedrības drošību. Pakalpojumu sniedzēja iekļaušana kritiskajā infrastruktūrā vai pamatpakalpojumā ir diezgan laikietilpīgs process. Taču var būt gadījumi, ka par šādu sabiedrībai būtisku informācijas pakalpojumu sabiedrības drošības un veselības interesēs ir nepieciešams atzīt infrastruktūru, kuras nepārtrauktu darbību ir nepieciešams nodrošināt nekavējoši. Gadījumos, kad ir noticis informācijas tehnoloģiju drošības incidents, izvērtējot konkrētos apstākļus, CERT vienojas ar drošības incidenta pieteicēju par atbalsta sniegšanu drošības incidenta novēršanā, un puses vadās no ITDL 6. panta trešajā un ceturtajā daļā paredzētās rīcības incidentu novēršanas gadījumā.

2.3. Drošības incidenta būtiskas traucējošas ietekmes jēdziens

NIS1 Direktīvā, kā jau iepriekš minēts, ir izvirzītas vairākas prasības dalībvalstīm informācijas tehnoloģiju drošības jomā – gan ADAS klasifikācijā, gan arī risku novērtēšanas sistēmas izveidošanā, ieviešot jaunu terminu "būtiska traucējoša ietekme". Direktīvas 6. pants satur kritēriju minimumu, kas dalībvalstīm jāņem vērā, vērtējot būtisku traucējošo ietekmi uz pakalpojuma sniegšanu, tostarp lietotāju skaitu, pakalpojuma sniedzēja tirgus daļu, ietekmi, ko drošības incidents varētu nodarīt ekonomikām un sabiedriskām darbībām vai sabiedrības drošībai.

Lai izpildītu NIS1 Direktīvas prasības, Latvijā 2019. gada 15. janvārī tika pieņemti MK noteikumi Nr. 43 "Par nosacījumiem drošības incidenta būtiski traucējošās ietekmes noteikšanai un kārtību kādā piešķir, pārskata un izbeidz pamatpakalpojuma sniedzēja un

pamatpakalpojuma statusu". Šo noteikumu 1. punktā ir norādīti nosacījumi informācijas tehnoloģiju drošības incidenta būtiski traucējošās ietekmes noteikšanai dažādās nozarēs, tostarp dzeramā ūdens piegādes un izplatīšanas, interneta plūsmas, domēnu nosaukumu, kā arī enerģētikas nozarē, transporta nozarē un veselības nozarē sniegtajiem pakalpojumiem. Turklāt noteikumi paredz arī kārtību, kā tiek pārskatīts šo pamatpakalpojumu sniedzēju statuss.

Savukārt MK 2019. gada 15. janvāra noteikumu Nr. 15 "Noteikumi par drošības incidenta būtiskuma kritērijiem, informēšanas kārtību un ziņojuma saturu" 2. punktā par būtisku ietekmi uz pakalpojuma nepārtrauktību tiek atzīti gadījumi, kas atbilst vismaz vienai no šīm pazīmēm:

1) ilgst vairāk nekā 24 stundas neatkarīgi no skarto lietotāju skaita;
2) skar no 1 līdz 10 % (ieskaitot) pamatpakalpojuma lietotāju un ilgst vismaz četras stundas;
3) skar no 10 līdz 15 % (ieskaitot) pamatpakalpojuma lietotāju un ilgst vismaz divas stundas;
4) skar vairāk nekā 15 % pamatpakalpojuma lietotāju un ilgst vismaz vienu stundu;
5) skar vismaz vienu pamatpakalpojuma lietotāju, kurš saskaņā ar Energoefektivitātes likuma 10. panta otro daļu ir iekļauts lielo uzņēmumu sarakstā;
6) skar pamatpakalpojuma lietotājus vismaz vēl vienā citā Eiropas Savienības dalībvalstī un ilgst vismaz divas stundas.

Savukārt šo noteikumu 3. punktā noteikts, ka drošības incidentam ir būtiska ietekme uz digitālā pakalpojuma sniegšanu, ja tas ilgst vairāk nekā divas stundas.

Šeit jau faktiski ir gatavs algoritms, kā būtu vērtējams būtiskais kaitējums nodarījumos pret ISD. To, ka šajā klasifikācijas shēmā iekļauto sistēmu loks nākotnē tikai paplašināsies, liecina arī Eiropas Komisijas 2020. gada 16. decembrī publicētais priekšlikums NIS2 Direktīvai "Eiropas Parlamenta un Padomes Direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148" (Eiropas Komisija, 2020).

NIS2 Direktīvas projekta 11. apsvērumā norādīts, ka pakalpojumi būtu jāiedala divās kategorijās atkarībā no nozares, kurā darbojas to sniedzēji, vai sniegto pakalpojumu veida. Šīs kategorijas apzīmētas kā būtiskas un svarīgas vienības. Turklāt, veicot to iedalīšanu kategorijās, būtu jāņem vērā nozares vai sniegto pakalpojumu veida svarīgums, kā arī atkarība no citām nozarēm vai pakalpojumu veidiem.

Šīs grupas ir uzskaitītas NIS2 Direktīvas priekšlikuma pielikumos. Pirmajā pielikumā uzskaitītas būtiskās vienības. Par būtisku pakalpojumu sektoru atzīta enerģētika, transports, banku pakalpojumi un finanšu tirgus infrastruktūra, veselības aprūpe, dzeramais ūdens, notekūdeņi, digitālā infrastruktūra, valsts pārvalde un kosmoss. Savukārt otrajā pielikumā ir reglamentētas svarīgo jomu vienības: pasts un kurjeru pakalpojumi, atkritumu pārvaldība, ķīmisko vielu izgatavošana, ražošana un izplatīšana, pārtikas ražošana, pārstrāde un izplatīšana, ražošana (medicīnisko ierīču un diagnostikas ierīču ražošana, datoru, elektronisko un optisko iekārtu ražošana, elektrisko iekārtu ražošana,

citur neklasificētu mehānismu un darba mašīnu ražošana, automobiļu, piekabju un puspiekabju ražošana, citu transportlīdzekļu ražošana), digitālos pakalpojumu sniegšana. Svarīgi uzsvērt, ka par šādām vienībām – objektiem – būtu jāatzīst visi vidēja lieluma un lielie uzņēmumi, kas darbojas "konkrētā kritiskā sektorā", kas ietverti 1. vai 2. pielikumā.

Teorētiski par visiem C4 un C3 kategorijas incidentiem, ja tiktu konstatēts nodarījums, būtu jāuzsāk kriminālprocesi. Anonimizētu tiesu nolēmumu datubāzē šīs publikācijas autori neatrada nevienu publiski pieejamu tiesas nolēmumu pēc Krimināllikuma 241., 243., 244., 244.[1] vai 245. panta. Visticamāk, šādus spriedumus tiesas nav pieņēmušas.

Jautājums – kāpēc tika izdarīti grozījumi Krimināllikuma 241. panta trešajā un 243. panta piektajā daļā?

Atbile – lai nepieļautu situācijas, ka personām, kuras nelikumīgi piekļūst šādām sistēmām, izdotos izvairīties no kriminālatbildības, jo nav iespējams pierādīt būtisko kaitējumu. Tādēļ likumdevējs noteica, ka atbildība par abiem nodarījumiem iestājas jau par pašu drošības incidentu – darbībām, kas vērstas pret ADAS, kas iekļautas iepriekš minētajās būtisko pakalpojumu sniedzēju kategorijās. Tāpēc uz šīm sistēmām attiecas Krimināllikuma 241. panta trešā daļa, proti, to apdraudējuma gadījumā būtu automātiski uzsākams kriminālprocess, jo minēto nodarījumu sastāvs ir pabeigts ar brīdi, kad persona ir izdarījusi Krimināllikuma 241. panta pirmajā daļā paredzētās darbības.

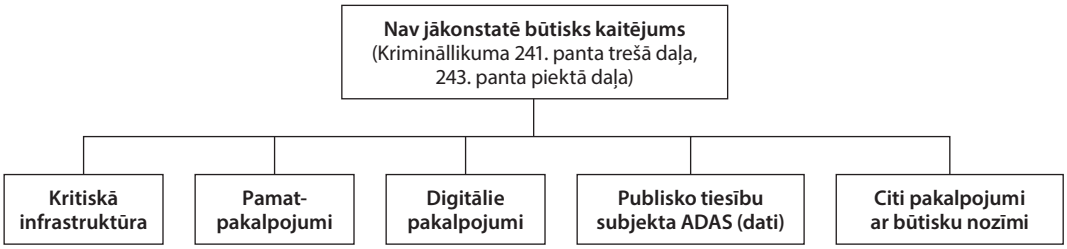
Līdzīgi būtu jārīkojas, ja iepriekš minēto grupu sistēmās tiktu veikta nelikumīga rīcība ar sistēmā esošo informāciju (Krimināllikuma 243. panta pirmā daļa) vai arī ADAS apzināta darbības traucēšana, ja ar to tiek bojāta vai iznīcināta aizsardzības sistēma (Krimināllikuma 243. panta otrā daļa). Respektīvi, šādos gadījumos būtu jāuzsāk kriminālprocess pēc Krimināllikuma 243. panta piektās daļas. Turklāt, ja ADAS vai ar tās palīdzību apstrādājamie dati tiek saistīti ar valsts deleģētas funkcijas pildīšanu vai arī ADAS darbība tiek finansēta no valsts budžeta, neatkarīgi no jau iepriekš minētās CERT.LV klasifikācijas, par jebkuru apdraudējumu šādām ADAS vai datiem ir uzsākams kriminālprocess.

3. Būtiska kaitējuma noteikšanas algoritmiskā metode pret ISD vērstos noziedzīgos nodarījumos

No iepriekš minētā var secināt, ka ADAS, kas ir saistītas ar kritisko infrastruktūru, kā arī ar pamatpakalpojumu, digitālpakalpojumu un citu būtiskas nozīmes pakalpojumu sniegšanu, nevar būt par apdraudējuma priekšmetu noziedzīgos nodarījumos, par kuriem kriminālatbildība ir paredzēta Krimināllikuma 241. panta pirmajā daļā, 243. panta pirmajā un otrajā daļā. Šāda veida ADAS krimināltiesiskā aizsardzība ir paredzēta speciālajās normās, tas ir, Krimināllikuma 241. panta trešajā daļā un 243. panta piektajā daļā. Tas nozīmē, ka būtisko kaitējumu nav nepieciešams konstatēt, ja noziedzīgs nodarījums ir vērsts pret šāda veida ADAS.

3.1. Krimināllikuma 241. panta trešās daļas un 243. panta piektās daļas piemērošanas problēmas

Krimināllikuma 241. panta trešajā daļā un 243. panta piektajā daļā paredzētie noziedzīgie nodarījumi ir vērsti pret ADAS, kas apstrādā ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību saistītu informāciju. Taču svarīgi ir precīzi noteikt ADAS un tajā apstrādājamo datu funkcionālo nozīmi (sk. 1. att.).



1. attēls. ADAS un tajā apstrādājamo datu funkcionālās nozīmes noteikšana

Praksē ir bijuši gadījumi, ka šo normu piemērotajiem radušās grūtības pierādīt, ka konkrēta ADAS patiešām apstrādā šāda veida informāciju. Kā jau minēts iepriekš, gan nacionālajos, gan starptautiskajos normatīvajos aktos ir noteikts, ka ADAS ar būtisku nozīmi jau pati par sevi ir krimināltiesiski aizsargājams objekts, tādējādi jebkura ADAS ar šādu nozīmi ir saistīta ar minētājos Krimināllikuma pantos norādītajām drošības jomām. Līdz ar to kriminālatbildība iestājas jau ar kaitīgo darbību izdarīšanu (formāls sastāvs), proti, par patvaļīgu piekļūšanu šāda veida ADAS, pārvarot attiecīgus drošības līdzekļus vai izmantojot citai personai piešķirtas tiesības, vai arī par šāda veida ADAS esošās informācijas (datu) neatļautu grozīšanu, bojāšanu, iznīcināšanu, pasliktināšanu vai aizklāšanu, vai apzināti nepatiesas informācijas ievadīšanu.

3.2. Krimināllikuma 241. panta pirmajā daļā, 243. panta pirmajā un otrajā daļā ietvertais "būtiskais kaitējums"

Krimināllikuma 241. panta pirmajā daļā, 243. panta pirmajā un otrajā daļā paredzētie noziedzīgie nodarījumi, kuros ir jānoteic būtisks kaitējums, ir vērsti tieši pret ADAS (un datiem), kas ir piederīgas galvenokārt privāto tiesību jomai un nepilda publisko tiesību funkcijas.

Līdzīgi Horonija (*Horony,* 1999) paustajam, arī Liholaja norāda, ka šāda veida noziedzīgajos nodarījumos būtisks kaitējums ir saistīts ar vairākiem faktoriem: ADAS darbības traucēšanas ilgumu, zaudējumiem, kas saistīti ar ADAS dīkstāvi, izdevumiem par bojātās informācijas atjaunošanu vai tās aizstāšanu, jaunu programmisku resursu instalēšanu, sistēmas lietotāju piekļuves tiesību korekciju, neiegūtu peļņu, kā arī citiem izdevumiem (Liholaja, 2019).

Papildinot šos kritērijus, ir jānorāda, ka būtisks kaitējums pats par sevi iestājas tad, ja ADAS apstrādājamā informācija ir ar likumu aizsargājama, piemēram, sensitīvie dati, komercnoslēpums u. tml. Tāpat tas ir tad, ja ADAS ir noteikta sabiedriska funkcija, piemēram, ADAS ir piederīga kādai biedrībai, partijai, fondam u. tml.

Savukārt, ja ADAS neapstrādā ar likumu aizsargājamos datus vai arī tai nav noteikta sabiedriska funkcija, tad **būtiskā kaitējuma izvērtēšanā jāpiemēro turpmāk minētie kritēriji**.

Laika kritērijs. Kā jau iepriekš tika minēts, MK 2019. gada 15. janvāra noteikumos Nr. 15 "Noteikumi par drošības incidenta būtiskuma kritērijiem, informēšanas kārtību un ziņojuma saturu" noteikti nosacījumi, kuru iestāšanās gadījumā drošības incidents ir atzīstams par būtisku. Šie kritēriji ir saistīti, pirmkārt, ar pakalpojuma nepārtrauktību noteiktā laika griezumā; otrkārt, ar skarto lietotāju skaitu. Tādējādi šajos noteikumos norādītie nosacījumi būtu piemērojami kaitējuma izvērtēšanā.

Mantisko zaudējumu kritērijs. ADAS apdraudējuma gadījumā var rasties kā faktiski zaudējumi, kurus var izteikt naudas izteiksmē, jeb mantiskie zaudējumi, tā arī zaudējumi, kas nav novērtējami naudas izteiksmē, jeb nemantiskie zaudējumi.

Speciālā likuma 23. panta pirmās daļas 1. punktā noteikts, ka būtisko kaitējumu veido mantiskie zaudējumi vismaz piecu minimālo mēnešalgu apmērā un vēl citu ar likumu aizsargāto interešu apdraudējums, savukārt no šīs daļas 2. punkta izriet, ka būtisko kaitējumu veido arī zaudējumi, kas paši par sevi jau ir vismaz 10 minimālo mēnešalgu apmērā. Uz mantiskiem zaudējumiem attiecināmi arī izdevumi, ko veido tehnisku manipulāciju izmaksas, kas vērstas uz radīto seku novēršanu, piemēram, programmēšanas, datu atjaunošanas / aizstāšanas izmaksas u. c. Turklāt mantisko zaudējumu var veidot arī neiegūta peļņa un dīkstāves izmaksas darbiniekiem ADAS traucējumu dēļ.

Nemantisko zaudējumu un sociālā nozīmīguma kritērijs. Nemantisko zaudējumu izvērtēšana ir saistāma ar ADAS sociālā nozīmīguma kritēriju. Šis kritērijs vienmēr būs vērtējams kopā ar bīstamību – risku, ko nodarījums var radīt sabiedrībai. Lai šis kritērijs izpildītos, ir jākonstatē acīmredzams, nepārprotams sabiedrisks kaitējums, kas kādai sabiedrības grupai radījis leģitīmo interešu aizskārumu. Ja ar noziedzīgo nodarījumu ir apdraudēts uzņēmums, tad šī kritērija izvērtēšanā ņemams vērā arī uzņēmuma lielums, proti, vai uzņēmums ir mikrouzņēmums vai vidēja lieluma uzņēmums. Ja uzņēmums ir atzīstams par lielu, tad būtisks kaitējums iestājas pats par sevi.

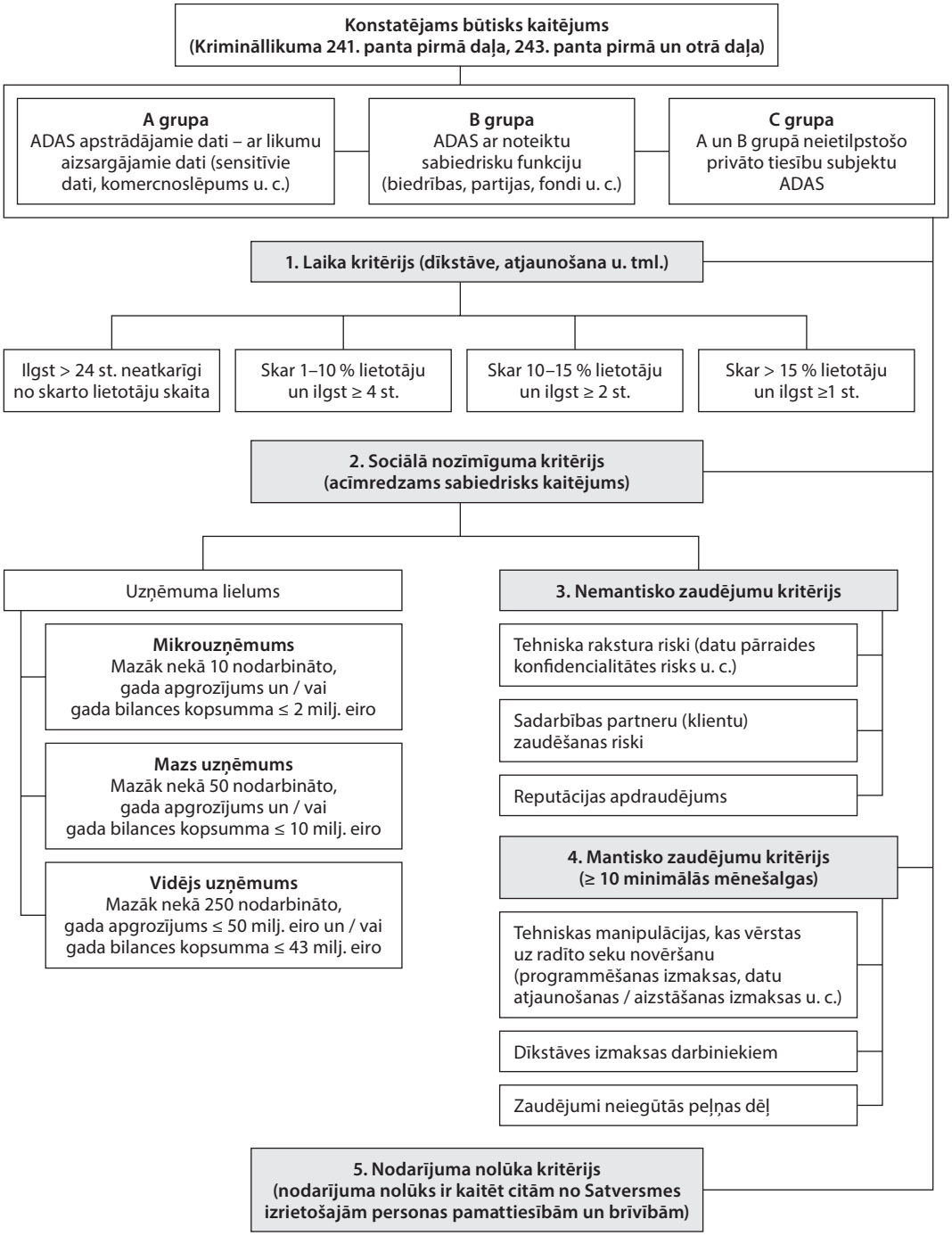
Savukārt nemantiskie zaudējumi veido arī tehniska rakstura riskus, sadarbības partneru (klientu) zaudēšanas riskus, reputācijas apdraudējuma, kā arī citus nemantiskus riskus. Ņemot vērā to, ka noziedzīgos nodarījumos, kas vērsti pret ADAS, būtisks kaitējums jau iestājas ar jebkuru citu leģitīmo interešu aizskārumu, kuram var būt arī nemantisks raksturs, nav nepieciešams nemantisko zaudējumu tiešā veidā saistīt ar mantisko kaitējumu, jo aizskarto interesi pēc būtības var veidot jebkurš no uzskaitītajiem nemantisko zaudējumu veidiem. Turklāt to saraksts noteikti nedrīkst būt

izsmeļošs, jo, vērtējot sociālā nozīmīguma kritēriju, jāņem vērā arī cietušās personas subjektīvais viedoklis. Tādējādi šā panta pirmās daļas 1. punkta jēga zūd attiecībā uz būtiskā kaitējuma noteikšanu noziedzīgos nodarījumus, kas vērsti pret ADAS. Līdz ar to būtiska kaitējuma noteikšanā būtu piemērojams Speciālā likuma 23. panta pirmās daļas 2. un 3. punkts.

Nodarījuma nolūka kritērijs. Ar šā kritērija palīdzību tiek izvērtēts, vai nodarījuma mērķis ir bijis kaitēt citām leģitīmām interesēm. Tas nozīmē, ka īpaši ir jāvērtē, vai nodarījuma mērķis nav saistāms ar citu Satversmē noteikto pamattiesību, kas nav saistītas ar noziedzīgā nodarījuma objektu (priekšmetu), ierobežošanu. Piemēram, nesankcionēti piekļūstot ADAS, vainīgais bija plānojis šajā sistēmā apstrādājamos datus iegūt savā prettiesiskajā rīcībā un pēc tam tos nelikumīgi izplatīt nolūkā apdraudēt personas reputāciju, kas nepieciešama konkrētas komercdarbības veikšanai.

Jāuzsver, ka minētie kritēriji nav izsmeļoši, taču tie veido minimumu, kas būtu obligāti jāizvērtē, lai konstatētu būtiska kaitējuma esamību konkrētajā noziedzīgajā nodarījumā, kas ir vērsts pret ISD. Turklāt nebūtu pareizi, ja šos kritērijus uzskatītu par kumulatīviem. Šo kritēriju izvērtēšanā jābūt kopsakarībai, kas tieši izriet no konkrētā noziedzīgā nodarījuma faktiskajiem apstākļiem. Piemēram, ļaunprātīgu darbību rezultātā kāda tīmekļvietnes darbība tikusi traucēta vairāk nekā 24 stundas. Pēc laika kritērija, kas izriet no jau iepriekš minētājiem MK noteikumiem Nr. 15, šāds traucējums jau pats par sevi ir uzskatāms par būtisku drošības incidentu. Taču var būt arī tā, ka šādu tīmekļvietni apmeklē vien pāris lietotāju dienā un tajā nav publicēta kāda patiešām nozīmīga informācija, kura kādai personai varēja būt vitāli nepieciešama tieši traucējumu brīdī. Šajā gadījumā, izvērtējot apstākļus kopsakarībā atbilstoši minētajiem kritērijiem, nebūtu konstatējams, ka ļaunprātīgu darbību rezultātā kādai personai būtu radīts tieši būtisks kaitējums.

Turklāt nedrīkst aizmirst, ka būtiska kaitējuma jēdziens ir jāpiepilda ar saturu, līdz ar to tieši likuma piemērotājam ir nepieciešams vispusīgi, izmantojot minētos kritērijus, izvērtēt būtiska kaitējuma esamību. Ņemot vērā visu iepriekš minēto, ar mērķi sistematizēt būtiska kaitējuma noteikšanas kritērijus noziedzīgajos nodarījumos, kas vērsti pret ISD, autori ir izstrādājuši būtiskā kaitējuma noteikšanas algoritmu šāda veida noziedzīgajos nodarījumos (sk. 2. att.). Jāuzsver, ka šis algoritms, tāpat kā paši izvērtēšanas kritēriji, nekādā gadījumā neaprobežo attiecīgo likuma piemērotāju būtiska kaitējuma tvērumu izskatīt vēl plašāk.



2. attēls. Algoritms būtiska kaitējuma noteikšanai noziedzīgos nodarījumos, kas vērsti pret ISD

Nobeigums

Ar pašreizējo Speciālā likuma 23. panta pirmo daļu, kurā noteikti būtiska kaitējuma kritēriji, netiek sasniegts Krimināllikuma 241. panta pirmās daļas un 243. panta pirmās un otrās daļas mērķis – nodrošināt krimināltiesisko aizsardzību ADAS un tās datiem, ja nodarījuma rezultātā ir nodarīts būtisks kaitējumus. Tas ir saistīts ar to, ka, galvenokārt, izmeklēšanas iestādēm vai arī pašiem cietušajiem rodas grūtības pierādīt būtiska kaitējuma iestāšanos, jo īpaši tad, ja radītais kaitējums ir saistīts ar nemantiskiem zaudējumiem.

ITDL 3. un 3.[1] pantā ir norādīti kritēriji, pēc kuriem ADAS atzīstamas par sistēmām, kas sniedz būtisku pakalpojumu. Minētās sistēmas kopumā veido Krimināllikuma 241. panta trešās daļas un 243. panta piektās daļas apdraudējuma objektu, jo jebkura būtiska pakalpojumu sniegšana ir saistīta ar Krimināllikuma attiecīgajos pantos definētajām drošības jomām. Ja ADAS vai ar tās palīdzību apstrādājamie dati pilda valsts deleģētu funkciju vai arī ADAS darbība tiek finansēta no valsts budžeta, tad par jebkuru apdraudējumu ir jāuzsāk kriminālprocess pēc Krimināllikuma 241. panta trešās daļas vai 243. panta piektās daļas. Turklāt tikai ITDL 3. pantā definētā informācijas tehnoloģiju kritiskā infrastruktūra ir Valsts drošības dienesta jurisdikcijā, savukārt pārējie pakalpojumu veidi, kas noteikti 3.[1] pantā, ir vispārējās jurisdikcijas pārraudzībā. Krimināllikuma 241. panta pirmās daļas un 243. panta pirmās un otrās daļas apdraudējuma objekts ir ADAS, kas nesniedz būtisku pakalpojumu, piemēram, darbojas privāto tiesību jomā un apstrādā ar likumu aizsargājamu informāciju. Šajos noziedzīgajos nodarījumos būtisks kaitējums ir izvērtējams sistematizēti, pēc noteiktiem vispārpieņemtiem kritērijiem.

Pētījuma ietvaros izstrādāta būtiska algoritmiskā metode kaitējuma noteikšanai noziedzīgos nodarījumos, kas vērsti pret ISD, un tā būtu izmantojama būtiska kaitējuma pierādīšanā.

Priekšlikumi

Speciālo likumu nepieciešams papildināt ar speciālu pielikumu par būtiska kaitējuma noteikšanu noziedzīgos nodarījumos, kas vērsti pret ISD, ietverot tajā šā pētījuma autoru izstrādāto būtiska kaitējuma noteikšanas algoritmu, kas pamatojas uz vispārpieņemtajiem būtiska kaitējuma izvērtēšanas kritērijiem.

Nepieciešams veidot visu valstī esošo ADAS vienotu klasifikāciju, kas aptvertu sistēmas, kuras nav minētas ITDL 3.[1] pantā, ieskaitot tās, kurām netiek atzīta būtiski traucējošā ietekme, tostarp maziem un vidējiem e-komersantiem, nevalstiskām organizācijām, kā arī citām privātpersonām piederošām ADAS. Tas radītu vienotu pieeju ADAS (un datu) funkcionālās nozīmes noteikšanā, tādējādi arī mazinātu pret ISD vērsto nodarījumu kvalifikācijas noteikšanas un būtiska kaitējuma pierādīšanas problemātiku.

Nepieciešams Krimināllikuma 241. panta trešo daļu un 243. panta piekto daļu grozīt, precizējot, ka šajos pantos norādīto nodarījumu apdraudējuma objekts ir tieši ADAS, kas apstrādā informāciju, kura ir saistīta ar būtiska informācijas pakalpojuma sniegšanu, atsevišķi neminot konkrētas drošības jomas, ar kurām šīs ADAS ir saistītas.

Tas ir nepieciešams, lai šo normu dispozīcijās ietvertais teksts neradītu šaubas likuma piemērotājiem attiecībā uz ADAS (un datu) saistību ar šajās normās norādītajām drošības jomām, lai šo normu mērķis būtu nepārprotams.

Avoti un literatūra

1. Aizsardzības ministrija. (2019). *Latvijas kiberdrošības stratēģija 2019.–2022. gadam*. Informatīvais ziņojums. Iegūts no: https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
2. Andersone, Dž. (2018). *Personas datu aizsardzības krimināltiesiskie aspekti* (promocijas darbs). Rīga: Latvijas Universitāte. Iegūts no: https://dspace.lu.lv/dspace/bitstream/handle/7/48862/298-72144-Andersone_Dzena_da15039.pdf?sequence=1&isAllowed=y
3. CERT.LV. (2022). *Pieejama statistika par 2021. gadu*. Iegūts no: https://cert.lv/lv/2022/01/pieejama-statistika-par-2021-gadu
4. Council of Europe. (2001). *Explanatory report Cybercrime Convention*. Iegūts no: https://rm.coe.int/16800cce5b
5. Crown Prosecution Service. (2021). *Criminal Damage*. Iegūts no: https://www.cps.gov.uk/legal-guidance/criminal-damage
6. Eiropas Komisija. (2022). *Directorate-General for Communication* (Special Eurobarometer 499: Europeans' attitudes towards cyber security (cybercrime). Iegūts no: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en
7. Eiropas Komisija. (2020). *Priekšlikums: Eiropas Parlamenta un Padomes Direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148*. COM(2020) 823 final. Iegūts no: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0823&from=LV
8. *Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148* (2016. gada 6. jūlijs) *par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā*. Eiropas Savienības Oficiālais Vēstnesis, L194/1, 19.07.2016.
9. European Parliament. (2021). *The NIS 2 Directive A high common level of cybersecurity in the EU*. COM(2020), 823, 16.12.2021. Iegūts no: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
10. Hamkova, D. (2018). *Latvijas Republikas Augstākā tiesa: Tiesu prakse lietās, kurās noziedzīga nodarījuma sastāva pazīme ir būtisks kaitējums*. Iegūts no: https://www.at.gov.lv/files/uploads/files/6_Judikatura/Tiesu_prakses_apkopojumi/2018/Apkopojums_butisks%20kaitejums_15_03_2018.docx
11. Horony, M. D. (1999). *Information system incidents: the development of a model damage assessment model*. Indianapolis University.
12. *Informācijas tehnoloģiju drošības likums*: Latvijas Republikas likums. Latvijas Vēstnesis, 178, 10.11.2010.
13. *Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība*: Latvijas republikas Ministru kabineta 15.02.2011. noteikumi Nr. 100. Latvijas Vēstnesis, 25, 01.02.2011.
14. Kantar. (2021). *Šī gada pavasarī interneta lietotāju skaits aizvien turpina pieaugt*. Iegūts no: https://www.kantar.lv/si-gada-pavasari-interneta-lietotaju-skaits-aizvien-turpina-pieaugt/

15. Kemp, S. (2021). Digital 2021: Latvia. *DataReportal*. Iegūts no: https://datareportal.com/reports/digital-2021-latvia
16. *Komisijas Regula (ES) Nr. 651/2014* (2014. gada 17. jūnijs), *ar ko noteiktas atbalsta kategorijas atzīst par saderīgām ar iekšējo tirgu, piemērojot Līguma 107. un 108. pantu*. Dokuments attiecas uz EEZ. Eiropas Savienības Oficiālais Vēstnesis, L187/1, 26.06.2014.
17. *Konvencija par kibernoziegumiem*: starptautisks dokuments. Latvijas Vēstnesis, 171, 26.10.2006.
18. Krastiņš, U. (2015). *Krimināltiesību teorija un prakse. Viedokļi, problēmas, risinājumi (2009–2014)*. Rīga: Latvijas Vēstnesis.
19. Krastiņš, U. (2012). Vērtējuma jēdzieni Krimināllikuma normās. *Jurista Vārds*, 24(723), 12.06.2012.
20. *Krimināllikums*: Latvijas Republikas likums. Latvijas Vēstnesis, 199/200, 08.07.1998.
21. Ķinis, U. (2015). *Kibernoziedzība, kibernoziegumi un jurisdikcija*. Rīga: Jumava.
22. *Latvijas Republikas Satversme*. Latvijas Vēstnesis, 43, 01.07.1993.
23. Laube, H. D. (1949). The Jurisprudence of interests. *Cornell Law Review*. 34(3), 291. Iegūts no: http://scholarship.law.cornell.edu/clr/vol34/iss3/1
24. Liholaja, V. (2019). 241. pants. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai. No *Krimināllikuma komentāri*. Trešā daļa. Otrais papildinātais izdevums, autoru kolektīvs U. Krastiņš, V. Liholaja, D. Hamkova. Rīga: Tiesu nama aģentūra.
25. Liholaja V., D. Hamkova (2012). Būtiska kaitējuma izpratne: likums, teorija, prakse. *Jurista Vārds*, 2(701). Iegūts no: https://juristavards.lv/doc/242455-butiska-kaitejuma-izpratne-likums-teorija-prakse/
26. Lomonovskis, J. (2018). Ievērojams citu interešu apdraudējums kā būtiska kaitējuma kritērijs krimināltiesībās. *Administratīvā un Krimināla Justīcija*, 4/2018. http://journals.rta.lv/index.php/ACJ/article/download/3673/3994
27. *Noteikumi par drošības incidenta būtiskuma kritērijiem, informēšanas kārtību un ziņojuma saturu*: Latvijas Republikas Ministru kabineta 15.01.2019. noteikumi Nr. 15. Latvijas Vēstnesis, 12, 17.01.2019.
28. *Noteikumi par nosacījumiem drošības incidenta būtiski traucējošās ietekmes noteikšanai un kārtību, kādā piešķir, pārskata un izbeidz pamatpakalpojuma sniedzēja un pamatpakalpojuma statusu:* Latvijas Republikas Ministru kabineta 15.01.2019. noteikumi Nr. 43. Latvijas Vēstnesis, 13, 18.01.2019.
29. Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību: Latvijas Republikas likums. Latvijas Vēstnesis, 331/332, 04.11.1998.
30. Stuk A. K., & Turko V. L. i dr. (eds.). (2017). *Praktika prokurorskogo nadzora*. Podderzhanie gosudarstvennogo obvinenija i nadzor za zakonnost'ju sudebnyh reshenij po ugolovnym delam (izvlechenie): posobie. Minsk: Konsul'tantPljus.
31. Valsts Kontrole (2020). *Lietderības revīzija. Noziedzīgu nodarījumu ekonomikas un finanšu jomā izmeklēšanu iztiesāšanu kavējošu faktoru izvērtējums*. Iegūts no: https://www.lrvk.gov.lv/lv/getrevisionfile/29451-9N0xF5QxFfikjVCe1yEvqXHRvSShChAF.pdf
32. Van Eeten, M., Bauer, J. M., & Shirin Tabatabaie (eds). (2009). *Damages from internet security incidents. A framework and toolkit for assessing the economic costs of security breaches*. Iegūts no: https://www.acm.nl/sites/default/files/old_publication/publicaties/9923_TU%20Delft%20-%20OPTA%20-%20Damage%20of%20Security%20Incidents.pdf [sk. 13.02.2022].
33. Verhovnyj Sud Rossijskoj Federacii (2008). *Kommentarij k Ugolovnomu zakonu Rossijskoj Federacii*. Pod red. Radchenko V. D., s vnesennymi izmenenijami. 2-e dopolnennoe izdanie. Moskva: Prospekt, 2008.