LATVIJAS UNIVERSITĀTE
JURIDISKĀ FAKULTĀTE
KRIMINĀLTIESISKO ZINĀTŅU KATEDRA

Atbildības par izspiedējļaunatūras izmantošanu krimināltiesiskie aspekti

BAKALAURA DARBS

Anna Cimoška
stud. apl. nr. 16030
Darba vadītājs: prof., Dr.iur. Valentija Liholaja

Rīga 2019

Anotācija

Ņemot vērā straujo tehnoloģisko attīstību, arvien rodas jauni noziedzīgi nodarījumi, kas bieži vien ir kiber-analogs kādam tradicionālam noziegumam. Izspiedējļaunatūras izmantošana ir jauns noziedzīgs nodarījums, kas atbilst vairāku dažādu noziedzīgu nodarījumu sastāvu pazīmēm. Tas aptver gan tradicionālās izspiešanas pazīmes, gan kibernoziedzības aspektus.

Darbā analizēta izspiedējļaunatūras darbība un nodarījuma atbilstība esošajam Krimināllikuma normatīvajam regulējumam. Krimināllikuma normas salīdzinātas ar atbildības par kibernoziedzību normatīvo regulējumu ārvalstīs. Darbā ir secināts, ka noziegumu ir iespējams kvalificēt atbilstoši Krimināllikuma normām, bet personisku automatizētu datu apstrādes sistēmu aizsardzībai nepieciešams pazemināt būtiska kaitējuma slieksni un būtisku kaitējumu paredzēt kā kvalificējošu noziedzīga nodarījuma pazīmi.

Atslēgvārdi: kibernoziegumi, izspiedējļaunatūras izmantošana, krimināltiesiskā kvalifikācija, būtisks kaitējums.

Annotation

Considering the rapid development of technologies, new criminal offences emerge, often as a cyber-anologous of a traditional crime. The use of ransomware is a new criminal offence which corresponds to the characteristics of several different criminal offenses. It covers both the features of a traditional extortion and the aspects of cybercrime.

This thesis analyzes the functioning of ransomware and applicability of the Criminal Law of Latvia in ransomware cases. The norms of the Criminal Law have been compared with the regulatory framework of liability for cyber crime abroad. The thesis concludes that it is possible to qualify a crime according to the provisions of the Criminal Law, but for the protection of personal automated data processing systems it is necessary to lower the threshold of substantial damage and forsee substantial damage as a qualifying feature of a criminal offence.

Keywords: cybercrime, the use of ransomware, criminal qualification, substantial damage.

Satura rādītājs

Ievads

Pēdējās desmitgades visā pasaulē pagājušas informācijas tehnoloģiju attīstības zīmē. Līdz ar šo tehnoloģiju attīstību un izplatību, tādā pašā ātrumā attīstās un izplatās arī kibernoziedzība kā jauns noziedzības veids. Ņemot vērā mūsdienu sabiedrības vispārējo atkarību no informāciju tehnoloģijām, par kibernoziedzības upuri var kļūt ikviena persona. Sabiedrība ir kļuvusi par ‘’informācijas sabiedrību’’, kurā no informācijas tehnoloģijām atkarīgi ne tikai iedzīvotāji, bet arī valsts pārvalde, drošība un ekonomika.[1]

Kibernoziegumi tiek veikti tiešsaistes (*on-line*) slēguma režīmā izveidotajā kibertelpā, kuras lielākā un redzamākā izpausme ir internets.[2] Saskaņā ar Centrālās statistikas pārvaldes datiem, 2017. gadā Latvijā 78,5 % iedzīvotāju vecumā no 16-74 gadiem vismaz reizi nedēļā lietoja internetu, bet vecumā no 16-44 gadiem internetu regulāri lietoja 96% iedzīvotāju. E-pasta nosūtīšana vai saņemšana bija pats populārākais mērķis interneta izmantošanas mērķis, šo pakalpojumu izmantoja 85,5% aptaujāto.

Ar izspiedējļaunatūru inficēta e-pasta atvēršana ir visizplatītākais veids, kā inficēt datoru vai citu ierīci ar šo ļaunprātīgo programmatūru. Tas 2017. gadā bija inficēšanās veids 91% gadījumu. Pēc dažādām aplēsēm izspiedējļaunatūras 2017. gadā visā pasaulē ir radījušas zaudējumus vismaz 4,3 miljardu euro apmērā, salīdzinot ar 280 miljoniem euro 2015. gadā.[3] Tas liecina par augšupejošu tendenci, un tiek prognozēts, ka 2019. gadā zaudējumi būs lēšami 11 miljardu eiro apmērā. Kiberuzbrukuma upuri ir gan fiziskas, gan juridiskas personas. Jāatzīst, ka kibertelpu izspiešanas nolūkos plaši izmanto arī starptautiskas noziedzīgas oganizācijas.[4]

2017. gada maijā notika globāls kiberuzbrukums, inficējot ar izspiedējvīrusu vairāk nekā 200 tūkstošus datoru vismaz 150 valstīs, tostarp Latvijā.[5] Tās aktualizēja jautājumu par šāda nodarījuma krimināltiesisko kvalifikāciju. Ministru kabineta Latvijas kiberdrošības stratēģija

---

[1] Latvijas kiberdrošības stratēģija 2018-2022. Pieejams: http://www.mrcc.lv/~/media/AM/Ministrija/Sabiedribas_lidzdaliba/2018/11/AIMstrat_kiber_projekts_181022.ashx [aplūkots 20.04.2019.]

[2] Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas īpatnības. Rīga: Biznesa augstskola Turība, 2003, 45.lpp.

[3] Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019. Pieejams: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ [aplūkots 21.04.2019.]

[4] Ķinis U. Kibernoziegumi. Rīga: Biznesa augstskola Turība, 2007, 10. lpp.

[5] Par globālo izspiedējvīrusu Latvijā ziņojušas 20 personas. Pieejams: http://www.delfi.lv/news/national/politics/par-globalo-izspiedejvirusu-latvija-zinojusas-20-personas.d?id=48841773 [aplūkots 21.04.2019.]

2018.-2022. gadam paredz izvērtēt Krimināllikuma piemērošanas pamatu un pilnveidot to, lai nodrošinātu personu ar likumu aizsargāto interešu efektīvu krimināltiesisko aizsardzību kibertelpā un saistībā ar to.

Bakalaura darba mērķis ir noskaidrot, kā kvalificēt izspiedējļaunatūras izmantošanu, kādi ir kvalifikācijas problēmjautājumi un vai nav nepieciešami Krimināllikumā esošo normu grozījumi.

Darba mērķa sasniegšanai tika noteikti šādi uzdevumi:

1) iepazīties ar kibernoziedzības teorētiskajiem aspektiem un izspiedējļaunatūras darbības mehānismu;

2) analizēt tēmai nozīmīgās Krimināllikuma normas, un secināt, vai un kā tās piemērojamas attiecībā uz izspiedējvīrusu izmantošanu;

3) izpētīt ārvalstu regulējumu kibernoziedzības jomā un salīdzināt ar Latvijas normatīvo regulējumu;

4) kvalificēt klasiska izspiedējļaunatūras izmantošanas gadījumu un identificēt problēmjautājumus.

Lai sasniegtu darba mērķi un īstenotu darba uzdevumus, tika izmantotas šādas zinātniskās pētniecības metodes: 1) aprakstošā metode; 2) salīdzinošā metode; 3) deduktīvā metode un 4) analītiskā metode.

1. Kibernoziedzības teorētiskie aspekti

Pasaulē notiekošā straujā tehnoloģiju attīstība ir veicinājusi kibernoziedzības vērienu, radot jaunus noziedzīgus nodarījumus, kā arī izmantojot tehnoloģiskās iespējas tradicionālo noziegumu realizēšanai. Arvien vairāk noziedzīgo nodarījumu tiek veikti kibertelpā. Tiesiskas kibertelpas pamata princips ir ‘’Kas nelikumīgs fiziskajā vidē, tas nelikumīgs arī virtuālajā vidē’’, jeb tā dēvētais ekvivalences princips.[6] Šis princips paredz arī valsts pienākumu aizsargāt personas Satversmē noteiktās pamattiesības un brīvības un vispārīgo tiesību principu īstenošanu gan fiziskajā, gan virtuālajā vidē. Ekvivalences principa būtība krimināltiesības ir analizēt noziedzīgā nodarījuma raksturu un mērķi, proti, likumdevējam, izstrādājot noziedzīgā nodarījuma definīciju, jāizsver, vai ar kibertelpā veikto nodarījumu var sasniegt tādu pašu mērķi, kā ar tradicionālo noziedzīgo nodarījumu, un vai esošā nodarījuma definīcija pilnībā aptver arī kibertelpā pastrādāto noziedzīgo nodarījumu.[7]

1.1.Konvencija par kibernoziegumiem

Nozīmīgākais starptautisko tiesību akts kibernoziedzībā ir Eiropas Padomes Konvencija par kibernoziegumiem, saukta arī par Budapeštas konvenciju (turpmāk – Konvencija), kas pieņemta 2001. gadā un stājās spēkā 2004. gadā.[8] Konvencija ir starptautisks, daudzpusējs tiesību akts, kas jau sākotnēji bija iecerēts kā universāls tiesību akts, kura dalībnieces neaprobežojas ar Eiropas Padomes dalībvalstīm. Šobrīd Konvenciju ir ratificējušas 63 valstis, tostarp Latvija.[9]

Ņemot vērā kibernoziedzības globālo raksturu un efektīva tiesiskā regulējuma trūkumu, kā vispārpieņemts fakts atzīta nepieciešamība pēc zināma mēra harmonizācijas attiecīgajos tiesību jautājumos. Kaut gan ir tapuši un joprojām turpina tapt vairāki tiesību akti ar mērķi harmonizēt valstu tiesības kibernoziedzības jautājumos, Konvencija joprojām ir pirmais un vienīgais starptautiskais saistošais tiesību instruments, kas regulē kibernoziedzības jomu.

---

[6] Latvijas kiberdrošības stratēģija 2014-2018. Pieejams: https://www.unodc.org/res/cld/lessons-learned/lva/latvijas_kiberdrobas_stratija_html/Kiberdrosibas_strategija.pdf [aplūkots 20.04.2019.]

[7] Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija. Rīga: Apgāds ‘’Jumava’’, 2015, 80. lpp.

[8] Konvencija par kibernoziegumiem. Parakstīta Budapeštā 05.05.2004. [02.04.2019. red.]

[9] Chart of signatures and ratifications of Treaty 185. Pieejams: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=exhG7iJ7 [aplūkots 02.04.2019.]

Konvencija norāda uz pasākumiem, kas jāveic nacionālā līmenī. Tā, pirmkārt, ir definējusi dažādus noziedzīgus nodarījumus pret automatizētām datu apstrādes sistēmām, kā piemēram, patvaļīga piekļūšana, datu traucēšana, datorkrāpšana, un šīs definīcijas ir izmantotas vairāku valstu krimināl kodeksos.

Konvencija dalībvalstīm paredz pienākumu nacionālajā tiesību sistēmā veikt noteiktas darbības, lai definētos noziedzīgos nodarījumus iekļautu patstāvīgās krimināltiesību normās. Jāatzīmē, ka Konvencijas normas ir visai precīzi adaptētas Krimināllikumā, tomēr tām ir pievienots būtiska kaitējuma kritērijs, vairumu kibernoziegumu padarot par noziedzīgiem nodarījumiem ar materiālu sastāvu.

Otrkārt, Konvencija paredz ieviest procesuālu normatīvo regulējumu efektīvai kibernoziegumu izmeklēšanai, tostarp, tiesiskai pierādījumu iegūšanai.

Treškārt, Konvencija nosaka starptautiskās sadarbības principus kibernoziegumu izmeklēšanā.

Tomēr Konvencija nereti tiek kritizēta kā novecojusi un stagnējoša, un definīcijas, kas tajā formulētas diezgan plaši un neitrāli, uzskatāmas par pārāk šaurām mūsdienu tehnoloģiju tvērumam.[10] Problēmas sagādā arī straujā tehnoloģiju attīstība, kuras rezultātā pastāvīgi rodas jauni veidi, kā kibertelpā veikt kaitniecīgas darbības. Šo iemeslu dēļ, autore uzskata, ka likumdevējam jāspēj būt proaktīvam, t.i., jāspēj savlaicīgi reaģēt uz faktisko situāciju, radot konkrētus tiesību aizsardzības līdzekļus.

1.2. Automatizētās datu apstrādes sistēmas jēdziens

Automatizētās datu apstrādes sistēma (turpmāk – ADAS) ir jēdziens, kas iekļauts Krimināllikuma 78., 79.[1], 149.[1], 150., 177.[1], 241., 243. un 244. pantā. ADAS jēdziens 2005. gadā ar krimināllikuma grozījumiem aizvietoja automatizētas datorsistēmas jēdzienu. Šādi grozījumi likumprojekta anotācijā pamatoti ar ADAS jēdziena plašāko tvērumu, kura ieviešana bija nepieciešama, lai nodrošinātu Krimināllikumā paredzēto noziedzīgo nodarījumu sakritību ar Konvencijā par kibernoziegumiem paredzētajām prettiesiskajām darbībām.[11]

[10] Clough J. The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World. Criminal Law Forum, 2012, No.4, p. 367.-368.

[11] Likumprojekta ''Grozījumi Krimināllikumā'' anotācija. Pieejama: http://www.saeima.lv/bi8/lasa?dd=LP0894_0 [aplūkots 04.04.2019.]

ADAS ir ierīce vai ierīču grupa, kas savienota ar elektroniskiem tīkliem un tās darbības mērķis ir automatizēta datu apstrāde.[12] Par ADAS nevar atzīt ierīces, kam piemīt automatizētas datu apstrādes funkcijas, bet tās ir paredzētas tādiem mērķiem, kas nav automatizēta datu apstrāde un informācijas aprite. ADAS fiziska ietekmēšana kvalificējama kā noziedzīgi nodarījumi pret īpašumu. ADAS tiek iedalītas pēc piederības, izveides mērķa un iespējamā apdraudējuma sociālā kaitīguma pakāpes. Par īpaši svarīgiem atzīstamas ADAS, kas apstrādā valsts ekonomiskajai, politiskajai un militārajai drošībai svarīgu informāciju, apstrādā fiziskas personas datus un ierobežotas pieejamības informāciju. Šādu ADAS ietekmēšanai ir augstāka kaitīguma pakāpe, un līdz ar to paaugstinās atbildība par nodarījumu.

1.3. Kibernoziegums, tā veidi

Ar tehnoloģijām saistītu noziegumu raksturošanai visbiežāk tiek lietots termins ‘’kibernoziegums’’. Kaut gan kibernoziedzības agrīnajos attīstības posmos tika izmantoti tādi jēdzieni kā *datornoziegums*, *interneta noziegum*s vai *digitāls, virtuāls, elektronisks noziegums*, katram no šiem jēdzieniem bija raksturīgs kāds trūkums.[13] Piemēram, *datornoziegums* uzskatāms par pārāk šauru jēdzienu, jo neaptver vienota datortīkla darbību. *Virtuāls noziegums* attiektos tikai uz internetu, bet *digitāls* un *elektronisks noziegums* ir pārāk plaši un nekonkrēti jēdzieni. Šie jēdzieni bieži tiek lietoti kā sinonīmi kibernozieguma jēdzienam, kas kļuvis par visbiežāk lietoto jēdzienu pateicoties tā izmantošanai Konvencijā.

Kibernoziegumi tiek veikti kibertelpā. Tā ir informācijas vide, kurā tiek radīti, uzglabāti un izplatīti digitalizēti dati.[14] Kibertelpa nav fiziska, tomēr arī ne pilnīgi virtuāla. Tā sastāv arī no fiziskām ADAS, kas apstrādā datus, kā arī no programmatūrām un infrastruktūrām, kas nodrošina datu apriti. Kibertelpu mēdz dēvēt par *quasi* telpu, jo tai iztrūkst ģeogrāfiskās robežas elements un vienota jurisdikcija.[15] Šī iemesla dēļ, kibertelpa ir uzskatāma par kriminogēnu vidi, kas piesaista gan uz noziedzīgiem nodarījumiem tendētus indivīdus, gan organizētas grupas. Noziedzīga darbība kibertelpā ir kļuvusi par ienesīgu nelegālās peļņas avotu, kam salīdzinājumā ar tradicionālajiem

[12] Ķinis U. Nodarījumi pret informācijas sistēmu drošību. Krimināllikuma piemērošanas problēmas. Jurista Vārds, 2011, Nr. 39, 6.-15. lpp.
[13] Clough J. Principles of cybercrime. New York: Cambridge University Press, 2010, p. 9.
[14] Singer P.W., Friedman A. Cybersecurity and cyberwar. New York: Oxford University Press, 2014, p. 13.
[15] Ķinis U. Jurisdikcija un kibernoziegumi. Rīga: Jumava, 2013, 14.-15. lpp.

noziegumiem ir raksturīgs zemāks vardarbības risks, bet noziedzīga nodarījuma izdarītājam ir mazāka iespēju tikt sauktam pie kriminālatbildības un tikt sodītam.[16]

Kibernoziegumi tiek uzskatīti par globāliem noziegumiem; tie pārvar ģeogrāfiskas robežas un var tikt izmantoti pret jebkuru personu un tehnoloģiju. Tā kā nav vienotas kibernoziegumu definīcijas, Š. Donaldsa (*C. Donalds*) un K. Osei-Braisons (*K. Osei-Bryson*) ir izveidojuši konceptuālu kibernozieguma modeli, kas tiek attēlots šādi:

Uzbrukuma notikums. Uzbrukuma notikums ir kibernoziegums vai kiberdarbība, kuru veic *uzbrucējs*.[17]

Ievainojamība. Ievainojamība ir ADAS trūkums vai vājais punkts, kuru izmanto uzbrucējs, lai sekmīgi veiktu uzbrukuma notikumu. Pastāv trīs veidu *ievainojamības*: darbības ievainojamība, dizaina ievainojamība un konfigurācijas ievainojamība, kas vienā vārdā apzīmējamas ar jēdzienu tehnoloģiskā ievainojamība. Atsevišķi iespējams nošķirt arī *ievainojamību*, kas izriet no drošības noteikumiem – tā izpaužas kā vāja ADAS aizsardzības plānošana un drošības noteikumu īstenošana.

Rīks vai tehnika. Rīks vai tehnika ir veids, kā uzbrucējs īsteno *uzbrukuma notikumu*.

Mērķuzdevums. Mērķuzdevums ir uzbrucēja galvenais nolūks, motīvs vai galarezultāts, ko tas vēlas panākt īstenojot *uzbrukuma notikumu*.

Nodarījums. Nodarījums ir prettiesiska kiberdarbība vai *uzbrukuma notikums*, ko ir izdarījis *uzbrucējs*, un kuru valsts ir atzinusi par sodāmu.

Cietušais. Cietušais ir vienība, kuru ir skāris *uzbrukuma notikums*. *Cietušais* var būt indivīds, grupa, organizācija, valsts. Ja *cietušais* ir mērķtiecīgi izvēlēts, *cietušā* jēdziens sakrīt ar *mērķa* jēdzienu. Tāpat ir iespējama situācija, kad, piemēram, *uzbrucējs* izplata datorvīrusu, kas nav mērķēts uz konkrētu vienību, bet *cietušais* par tādu kļūst gadījuma rakstura dēļ.

Mērķis. Mērķis ir vienība, pret kuru *uzbrukuma notikums* ir konkrēti un mērķtiecīgi vērsts. *Mērķis* var būt infrastruktūra, personiska ierīce, tīkla ierīce, indivīds, grupa, organizācija, valsts, programmatūra un interneta vietne.

Ietekme. Ietekme ir tiešās sekas, ko *uzbrukuma notikums* rada *cietušajam*. Iespējama ietekme uz darbību, informācijas apriti, kā arī uz ekonomiskiem, psiholoģiskiem un ģeopolitiskiem apstākļiem.

---

[16] Smith R., Cheung R., Yiu-Chang Lau L. Cybercrime risks and responses. Eastern and Western perspectives. Hampshire: Palgrave Macmillan, 2015, p. 16

[17] Donalds C., Osei-Bryson K.M. Toward a cybercrime classification ontology: A knowledge-based approach. Computers in Human Behavior, 2019, No. 92., p. 407.-409.

Uzbrucējs. Uzbrucējs ir vienība, kas īsteno *uzbrukuma notikumu,* lai sasniegtu *mērķuzdevumu*. *Uzbrucējs* var būt indivīds vai grupa, kas iespējama gan kā tradicionāls noziedzīgs grupējums, kura mērķis ir gūt peļņu ar noziedzīgu darbību, gan kibernoziedzinieku grupa, kas savu darbību izvērš tikai kiberteļpā, gan arī grupas ar ideoloģiski un politiski motivētiem indivīdiem.

Vairums tiesību zinātnieku kibernoziegumus mēdz iedalīt trīs kategorijās.[18] Izšķir noziedzīgus nodarījumus, kur uzbrukuma mērķis ir pats dators, proti, tā darbības traucēšana, informācijas iegūšana. Otra kategorija ir noziedzīgi nodarījumi, kuros dators tiek izmantots kā rīks nozieguma izdarīšanai. Trešā kategorija ir noziedzīgi nodarījumi, kuros datoram ir nejaušā loma nozieguma izdarīšanā. Dažkārt pirmais un otrais kibernoziegumu veids ir apvienots – dators ir gan nodarījuma izdarīšanas rīks, gan mērķis. Šī gadījuma klasiskākais piemērs ir datorvīrusa izplatīšana, ko izplata ar datoru, ar mērķi inficēt citus datorus.

Tiek atzīts arī tāds kibernoziegumu iedalīšanas veids, kurā pirmā kategorija ietver noziedzīgus nodarījumus, kurā dators tiek izmantots kā rīks tradicionāla nodarījuma izdarīšanai, piemēram, krāpšanai.[19] Otra kategorija ir satura noziegumi, kas lielākoties saistīti ar intelektuālo īpašumu un pornogrāfiju. Trešā kategorija ir noziedzīgie nodarījumi, kuru mērķis ir apdraudēt ADAS integritāti, piemēram, datorvīrusu izplatīšana.

Kibernoziegumus iedala arī šādās grupās: kiber-atkarīgie (*cyber dependent*) un kiber-iespējamie (*cyber enabled*) noziegumi.[20] Kiber-atkarīgie noziegumi ir izdarāmi vienīgi izmantojot datoru, datortīklu vai citu informācijas tehnoloģiju. Šai noziedzīgo nodarījumu grupai visbiežāk raksturīgi tādi nodarījumi kā ļaunatūru izplatīšana un patvaļīga piekļuve ADAS. Kiber-iespējamie noziegumi ir klasiskie noziedzīgie nodarījumi, kurus var paveikt bez informācijas tehnoloģijām, bet to izmantošana var palielināt nozieguma mērogu vai vienkārši būt ērtāks veids, kā to realizēt. Šo noziegumu grupu raksturo krāpšana, zādzības, izspiešana, pornogrāfijas izplatīšana un noziedzīgi iegūtu līdzekļu legalizācija.

---

[18] Brenner Susan W. Cybercrime. Criminal Threats from Cyberspace. California: Greenwood Publishing Group, 2010, p. 39

[19] Reed Chris, Angel John. Computer Law. Fifth Edition. New York: Oxford University Press, 2003, p. 295.-296.

[20] Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes.
Pieejams:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf [aplūkots 10.04.2019.]

1.4. Izspiedējļaunatūra

Latviešu valodā *ransomware* ļaunatūra (ļaunprātīga datorprogramma) tiek dēvēta par izspiedējvīrusu, kaut gan autores ieskatā šāds nosaukums būtu atbilstošs tikai atsevišķos gadījumos. Pastāv trīs ļaunatūru veidi, no kuriem trīs tiek izmantoti kiberizspiešanā – vīrusi, ‘’tārpi’’ un trojāni.[21] Vīrusi un ‘’tārpi’’ ir ļaunatūras, kas pašas sevi pavairo un traucē ADAS darbību, bojājot un dzēšot datnes. Trojāni ir visbiežāk izmantotā ļaunatūra kiberizspiešanas veikšanai. Ja ar vīrusiem un ‘’tārpiem’’ var inficēties nejauši, ADAS lietotājs trojānus parasti lejupielādē ar apzinātām darbībām, bet maldoties par lejupielādējamā faila saturu. Tā kā kiberizspiešana tiek veikta ar dažādām ļaunatūrām, šādas darbību apzīmēšanai būtu labāk izmantot vienojošu jēdzienu - izspiedējļaunatūru izmantošana. Jēdzieni izspiedējvīruss, izspiedējtārps, izspiedējtrojāns attiecināmi uz konkrētiem gadījumiem.

Izspiedējļaunatūra (*ransomware*) ir ļaunatūra, kuru vainīgais instalē datorā vai citās ierīcēs bez īpašnieka vai valdītāja piekrišanas.[22] ADAS inficējot ar izpiedējļaunatūru, tiek bloķēta piekļuve atsevišķiem vai visiem datiem. Ļaundari izmanto kriptogrāfiju, datus šifrējot un tādējādi padarot tos nepieejamus un praktiski neatgūstamus.[23] Datus iespējams atgūt, ievadot matemātisku dekriptācijas atslēgu, kas zināma vienīgi izspiedējļaunatūras izplatītājam. Par dekriptācijas atslēgas iegūšanu cietušajam tiek pieprasīta izpirkuma maksa, kas parasti jāveic kriptovalūtā. Kriptovalūta ir decentralizētā virtuāla nauda, kuras transakcijās izmanto blokķēdes tehnoloģiju (blockchain). Visas transakcijas, ko veic kriptovalūtā nonāk publiskā blokķēdēs blokā, tomēr katrs bloks ir šifrēts, līdz ar to anonīms trešajām personām.

Pastāv dažādas izpiedējvīrusu versijas. Vīrusa izplatītājs var maldināt ierīces īpašnieku vai valdītāju, uzdodoties par tiesībsargājošo iestādi, kas pieprasa soda naudu par datorā konstatētu pornogrāfiju vai nelikumīgi iegūtu programmatūru. Satopami arī tā dēvētās *leakware* vai *doxware* ļaunatūras, kas cietušajam piedraud ar ierīces cietajā diskā saglabāto sensitīvu datu publicēšanu, ja laikus netiks samaksāta pieprasītā nauda. Bet tā kā konkrētas informācijas meklēšana ierīcē ir laikietilpīga, un ne vienmēr efektīva, hakeri visbiežāk izvēlas veikt datu šifrēšanu.

Izspiedējļaunatūras izmantošana ir izspiešanas kā klasiska noziedzīga nodarījuma virtuālais analogs. Informācijas tehnoloģiju iesaiste palielina nozieguma mērogu un ir ērtāks veids,

---

[21] Jewked Y., Yar M. Internet crime handbook. New York: Willan Publishing, 2010, p. 184.-185.
[22] All about ransomware. Pieejams: https://www.malwarebytes.com/ransomware/ [aplūkots 13.04.2019.]
[23] Gercke M. Understanding cybercrime: phenomena, challenges and legal response. [b.v.]: ITU, 2012, 173. lpp.

kā to realizēt. Līdz ar to izspiedējļaunatūras izmantošanas klasificējama kā kiber-iespējams (cyber enabled) noziegums, kurā dators tiek izmantots kā rīks nozieguma izdarīšanai.

2. Atbildības par izspiedējļaunatūras izmantošanu tiesiskais regulējums Latvijā

2.1. Noziedzīga nodarījuma sastāvs

Atbilstoši Krimināllikuma (turpmāk – KL) 1. pantam persona saucama pie kriminālatbildības un sodāma tikai tad, ja tā ar nodomu (tīši) vai aiz neuzmanības izdarījusi šajā likumā paredzētu nodarījumu, kam ir visas noziedzīga nodarījuma sastāva pazīmes. [24] Kā norāda profesors U. Krastiņš, KL personas saukšanai kriminālatbildības paredz šādus priekšnoteikumus:

1) kaitīgs nodarījums (darbība vai bezdarbība);
2) nodarījums atbilst KL paredzēta noziedzīga nodarījuma pazīmēm;
3) darbībai vai bezdarbībai ir tāda kaitīguma pakāpe, kas nošķir noziedzīgu nodarījumu no citiem tiesībpārkāpumiem;
4) persona ir vainīga kaitīgajā nodarījumā;
5) KL par nodarījumu paredz krimināsodu.[25]

Kriminālatbildība ir fiziskai personai valsts vārdā uzlikts piespiedu pienākums atbildēt par izdarīto noziedzīgo nodarījumu atbilstoši KL un likumā paredzētajos gadījumos izciest sodu, kas saistīts ar personiskās brīvības, atsevišķu tiesību vai mantiska rakstura ierobežojumiem. [26]

Noziedzīgs nodarījums ir ar nodomu (tīši) vai aiz neuzmanības izdarīts kaitīgs nodarījums (darbība vai bezdarbība), kurš paredzēts KL un par kura izdarīšanu draud krimināsods. Pie kriminālatbildības iespējams saukt tikai fizisku personu. Tā kā personas par izdarīto noziedzīgo nodarījumu saucamas pie atbildības saskaņā ar likumu, lai nodarījumu atzītu par krimināli prettiesisku, jākonstatē pilnu noziedzīgā nodarījuma sastāvu.

Noziedzīgā nodarījuma sastāvu veidojošās pazīmes norādītas KL Sevišķās daļas panta dispozīcijā, kas satur pabeigtu noziedzīgu nodarījumu sastāvu pazīmes.[27] Izdala četras noziedzīga nodarījuma sastāva elementus – noziedzīgā nodarījuma objekts, objektīvā puse, subjekts un subjektīvā puse. [28]

---

[24] Krimināllikums. LV likums. Pieņemts: 17.06.1998. [08.04.2019. red.]

[25] Krastiņš U., Liholaja V., Niedre A. Kriminālatiesības. Vispārīgā daļa. Trešais papildinātais izd. Rīga: Tiesu namu aģentūra, 2008, 61. lpp.

[26] Krastiņš U., Liholaja V. Krimināllikuma komentāri. Pirmā daļa (I-VIII[1] nodaļa). Rīga: Tiesu namu aģentūra, 2015, 37. -39. lpp.

[27] Ibid. 41. lpp.

[28] Krastiņš U. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Rīga: Tiesu namu aģentūra, 2014, 30.-31. lpp.

Noziedzīgā nodarījuma objekts ir ar KL aizsargātas valsts sabiedrības, atsevišķu cilvēku grupu un indivīda intereses, kuras noziedzīgs nodarījums apdraud. Objekta noteikšana palīdz izdarīt nodarījuma sabiedriski politisko novērtējumu un noteikt nodarījuma kaitīguma smagumu.[29] Tiek izdalīti trīs objektu veidi – vispārējais, grupas un tiešais noziedzīga nodarījuma objekts. Profesors U. Krastiņš ir definējis, ka ''vispārējais objekts, kas kopīgs visiem noziedzīgajiem nodarījumiem, ir visu interešu kopums, ko aizsargā KL. Noziedzīgo nodarījumu grupas objekts ir tādas pašas vai viena veida un savstarpēji saistītas vairākas intereses, kuras apdraud noziedzīgo nodarījumu grupa. Noziedzīga nodarījuma tiešais objekts ir tās intereses, ko apdraud konkrēta veida noziedzīgs nodarījums.''

Noziedzīgā nodarījuma objektīvā puse atspoguļojas personas uzvedības ārējā izpausmē. Tā rada vai var radīt kaitīgas izmaiņas ārējā pasaulē.[30] Objektīvās puses pamatpazīmes ir prettiesiska darbība vai bezdarbība, kas ir personas ārējās gribas izpausme. Lai gan ir grūti nodalīt cilvēka uzvedības ārējās izpausmes no psihiskajiem procesiem personas apziņā, noziedzīgā nodarījuma objektīvā puse aptver tikai apzinātas, kaitīgas un prettiesiskas darbības vai bezdarbības realizācijas paņēmienus ārējā pasaulē. Pēc noziedzīga nodarījuma objektīvās puses pazīmēm izšķir formālus un materiālus nodarījumus. Ja KL Sevišķās daļas normas dispozīcijā kā objektīvās puses pazīme paredzētas kaitīgās sekas, kas iestājušās darbības vai bezdarbības rezultāta, nodarījuma sastāvs ir materiāls. Materiāla noziedzīga nodarījuma gadījumā obligāti jāpastāv cēloņsakarībai starp prettiesisko darbību vai bezdarbību un krimināltiesību normā paredzētajām sekām.

Noziedzīga nodarījuma subjekts ir prettiesisko darbību izdarījusī vai bezdarbību pieļāvusī fiziska un pieskaitāma persona, kas sasniegusi Krimināllikumā paredzētu vecumu, no kura iestājas krimināltatbildība, un līdz ar to viņu par izdarīto noziedzīgo nodarījumu var saukt pie krimināltatbildības.[31] Subjekta pamatpazīmes ir pieskaitāmība un sasniegts vecums, no kura iestājas krimināltatbildība. Par subjektu nevar būt juridiskas personas.

Noziedzīga nodarījuma subjektīvā puse ir nodarījuma subjekta psihiskā darbība, kas tieši saistīta ar viņas izdarīto (nodarījuma objektīvajām pazīmēm), un tā apvieno vienotā veselā

[29] Krastiņš U. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Rīga: Tiesu namu aģentūra, 2014, 55. -63. lpp.

[30] Ibid. 73.-80. lpp.

[31] Krastiņš U., Liholaja V. Krimināllikuma komentāri. Pirmā daļa (I-VIII[1] nodaļa). Rīga: Tiesu namu aģentūra, 2015, 76. lpp.

personas psihiskās darbības intelektuālos un gribas procesus.[32] Subjektīvās puses pazīmes ir:

- vaina - personas psihiskā attieksme pret viņa izdarīto prettiesisko darbību vai bezdarbību un ar to saistītajām kaitīgajām sekām. Pēc vainas formas izšķir noziedzīgus nodarījumus, kas izdarīti ar nodomu (tiešu vai netiešu), vai arī aiz neuzmanības (noziedzīga pašpaļāvība vai noziedzīga nevērība);
- motīvs – cilvēka iekšējais pamudinājums, kas virza vainīgā gribu uz noziedzīga nodarījuma izdarīšanu;
- mērķis – iecerētais rezultāts, ko persona ar noziedzīgu nodarījumu vēlas panākt.

Analizējot izspiedējļaunatūras izmantošanas darbības principus, secināms, ka darbības, kas nodrošina izspiedējļaunatūras izmantošanu, atbilst vairākiem Krimināllikumā ietvertiem noziedzīgu nodarījumu sastāviem. Tā kā izspiedējļaunatūras izmantošana ir paredzēta ADAS ietekmēšanai nolūkā izdarīt noziedzīgu nodarījumu (izspiešanu), šādas programmatūrās izgatavošana un izplatīšana ir atzīstama par kriminālī sodāmu saskaņā ar KL 244. pantu.

Inficējot ADAS ar izspiedējļaunatūru, hakeris veic patvaļīgu piekļuvi ADAS, tādējādi aizskarot sistēmas integritāti. Ja šādas darbības rezultātā tiek nodarīts būtisks kaitējums, personu var saukt pie krimināltatbildības saskaņā ar KL 241. pantu.

Kad ADAS ir inficēta ar izspiedējļaunatūru, tās kaitīgākā izpausme ir ADAS esošās informācijas šifrēšana jeb aizklāšana. Ja cietušais neveic hakera pieprasītās darbības, informācija tiek iznīcināta. Par ADAS darbības traucēšanu un nelikumīgu rīcību ar sistēmā iekļauto informāciju persona saucama pie krimināltatbildības saskaņā ar KL 243. pantu.

Izspiedējļaunatūras izmantošanas galvenais mērķis ir bez tiesiska pamata cietušajam pieprasīt samaksāt noteiktu summu kriptovalūtā, piedraudot iznīcināt šifrētos datus. Ja pieprasījums noteiktā laika posmā netiek izpildīts, šifrētie dati vairs nav atgūstami. Šāds nodarījums atbilst KL 183. panta noziedzīga nodarījuma sastāvam, kas paredz krimināltatbildību par izspiešanu.

2.2. Nelikumīgas darbības ar ADAS resursu ietekmēšanas līdzekļiem

Krimināllikuma 244. pants formulē, ka nelikumīgas darbības ar ADAS resursu ietekmēšanas līdzekļiem ir ierīces, datorprogrammas, datorparoles, pieejas koda vai līdzīgu datu neatļauta izgatavošana, pielāgošana izmantošanai, realizēšana, izplatīšana vai glabāšana, kurš paredzēts automatizētas datu apstrādes sistēmas resursu ietekmēšanai vai ar kura palīdzību var

[32]Krastiņš U. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Rīga: Tiesu namu aģentūra, 2014, 127.-128. lpp.

piekļūt automatizētas datu apstrādes sistēmai vai tās daļai nolūkā izdarīt noziedzīgu nodarījumu. Kā kvalificējoša pazīme panta otrajā daļā paredzētas šo darbību izraisītās smagās sekas. Kibernoziegumu konvencija nosaka, ka atbildība ir paredzama par tādu kaitīgu ierīču izmantošanu, kuru mērķis ir ļaunprātīgi ietekmēt ADAS.[33] Nosakot, vai tas ir kibernoziegums, uzsvars liekams uz mērķi, kam šī ierīce ir paredzēta, nevis izmantoto tehnoloģiju vai darbības metodi. Ierīcei ir jābūt speciāli veidotai, ar mērķi ietekmēt citu personu ADAS.

Krimināllikuma 244. pantā paredzētais noziedzīgais nodarījums pirmajā daļā ir mazāks smags noziegums, bet otrajā daļā – smags noziegums.

Noziedzīgā nodarījuma grupas objekts ir vispārējā drošība un sabiedriskā kārtība. Kaitīgās ierīces tiek speciāli veidotas un izplatītas, lai nelikumīgi ietekmētu citu personu ADAS. Ļaunprogrammatūra pārvar ADAS aizsardzības līdzekļus, aizskarot sistēmas integritāti. Piesavinoties, izmainot, aizklājot datus, tiek aizskarta konfidencialitāte un pieejamība. Noziedzīgā nodarījuma priekšmets ir ADAS sistēmas resursi vai to daļa.

Likumdevējs paredz kriminālatbildību par jebkuru darbību, kas saistīta ar kaitīgo rīku (ierīces, datorprogrammas, datorparoles, pieejas koda vai citu līdzīgo datu) apriti. Šīs darbības ir aktīvas - kaitīgā rīka neatļauta izgatavošana, pielāgošana līdz tā izmantošanai, realizēšana, izplatīšana vai glabāšana. Noziegums ir pabeigts ar brīdi, kad ir veikta jebkura no šīm darbībām.

Izgatavošana ir jebkādas darbības, kuru rezultātā rodas datu, komandu vai ierīču objektīvs kopums, kas paredzēts datorsistēmas vai datortīklu resursu ietekmēšanai.[34]

Pielāgošana izmantošanai ir darbības, kuru rezultātā tiek izmainītas ierīces īpašības, lai tās būtu izmantojamas datorsistēmas vai datortīklu ietekmēšanai.

Ar rīku realizēšanu saprotami tālāknodošanas paņēmieni, ar kuriem rīki nonāk citas personas īpašumā vai valdījumā. Pie rīku realizēšanas pieskaita pārdošanu, aizdošanu, uzdāvināšanu, parāda atdošanu un nodošanu personai bez citiem nosacījumiem.

Rīku izplatīšana izpaužas kā to ievadīšana datorvidē, padarot tos pieejamus citām personām. Tā var būt rīka nosūtīšana konkrētai vai nekonkrētai personai un personu lokam, vai kaitīgās programmas ievietošana publiskā datu pārraides tīklā. Izplatīšanas veidi ir saistīti ar

[33] Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija. Rīga: Apgāds ‘’Jumava’’, 2015, 147. lpp.

[34] Krastiņš U., Liholaja V., Hamkova D. Krimināllikuma komentāri. Trešā daļa (XVIII – XXV nodaļa). Rīga: Tiesu nama aģentūra, 2016, 342. lpp.

datorvides aktualitātēm.[35] Ja 20. gs. 90-os gados ļaunatūras tika izplatītas ar disketēm, vēlāk ar e-pastu pielikumiem, mūsdienās ar ļaunatūrām tiek inficētas sociālo tīklu un savstarpējo pakalpojumu (*peer-to-peer* jeb *P2P*) vietnes.

Glabāšana ir rīka atrašanās vainīgā valdījumā neatkarīgi no rīkā piederības. Vainīgajam nav jābūt rīka īpašniekam.

KL 244. panta pirmajai daļai ir formāls sastāvs - noziegums ir pabeigts ar brīdi, kad izdarīta jebkura no augstākminētajām panta daļas dispozīcijā noteiktajām alternatīvajām darbībām. KL 244. panta otrā daļa ietver smagu seku pazīmi, tāpēc nodarījuma sastāvs ir materiāls. Saskaņā ar likuma ‘’Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību ‘’ (turpmāk – Īpašais likums) 24. panta pirmo daļu, par smagām sekām atzīstama noziedzīga nodarījuma rezultātā izraisīta cilvēka nāve, nodarīti smagi miesas bojājumi vismaz vienai personai, mazāk smagi miesas bojājumi vairākām personām, nodarīts mantisks zaudējums, kas nodarījuma izdarīšanas brīdī nav bijis mazāks par piecdesmit tai laikā Latvijas Republikā noteikto minimālo mēnešalgu kopsummu, vai radīts citāds smags kaitējums ar likumu aizsargātām interesēm.[36]

Noziedzīgā nodarījuma subjekts ir fiziska, pieskaitāma persona, kas sasniegusi 14 gadu vecumu.

Vērtējot noziedzīgā nodarījuma subjektīvo pusi, tas ir tīšs noziegums, tomēr atšķiras viedokļi, vai to var izdarīt ar netiešu nodomu. U. Ķinis pauž viedokli, ka šo nodarījumu var izdarīt gan ar tiešu, gan netiešu nodomu[37], kamēr V. Liholajas ieskatā to raksturo tikai tiešs nodoms.[38] Autore piekrīt viedoklim, ka KL 244. panta nodarījumu var izdarīt tikai ar tiešu nodomu, par ko liecina tas, ka objektīvās puses darbības tiek veiktas ar speciālu nolūku – izmantot kaitīgos rīkus, lai veiktu vēl kādu Krimināllikumā paredzēto noziedzīgo nodarījumu. Tātad vainīgais apzinās savas darbības kaitīgumu un to veic apzināti. Jāatzīmē, ka personas psihiskā attieksme pret savu prettiesisko darbību formāla sastāva nodarījumā var izpausties tikai ar tiešu nodomu, jo, kā

[35] Kirwan G., Power A. Cybercrime. The Psychology of Online Offenders. Cambridge: Cambridge University Press, 2013, p.87.
[36] Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību: LV likums. Pieņemts 15.10.1998. [12.04.2019. red.]
[37] Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija. Rīga: Apgāds ‘’Jumava’’, 2015, 149. lpp.
[38] Krastiņš U., Liholaja V., Hamkova D. Grām.: Krimināllikuma komentāri. Trešā daļa (XVIII – XXV nodaļa). Rīga: Tiesu nama aģentūra, 2016, 342. lpp.

pamatoti atzīmē U. Krastiņš, nav iespējams, ka persona apzināti veic kādu darbību, ko nevēlas darīt. [39]

2.3. Patvaļīga piekļuve ADAS

Krimināllikuma 241. pants formulē patvaļīgu piekļūšanu ADAS kā sistēmas aizsardzības līdzekļu pārvarēšanu, piekļuvi ADAS bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības, ja ar to radīts būtisks kaitējums. Tas klasificējams kā mazāk smags noziegums. Panta otrajā daļā minēta kvalificējoša pazīme – mantkārīgs nolūks, bet trešajā daļā – smagas sekas vai ja noziedzīgās darbības vērstas pret ADAS, kas apstrādā informāciju, kas saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību. Iestājoties kvalificējošām pazīmēm, noziegums atzīstams par smagu.

Noziedzīgā nodarījuma grupas objekts ir vispārējā drošība un sabiedriskā kārtība. Kā norāda U. Ķinis, nodarījuma tiešais objekts ir informācijas sistēmas drošību raksturojošās pazīmes – integritāte, konfidencialitāte un pieejamība.[40] No pieejamības izriet iespēja sistēmas lietotājam ietekmēt resursu integritāti un veselumu, tāpēc to var atzīt par galveno apdraudēto interesi. Panta trešās daļas objekts ir valsts drošības intereses. Nozieguma mērķis ir materiālas dabas.

Noziedzīgā nodarījuma priekšmets ir ADAS, kas veic automatizēto datu apstrādi, un panta trešajā daļā ADAS, kas apstrādā ar valsts drošību saistītu informāciju.

Noziedzīgā nodarījuma objektīvās puses pazīme ir patvaļīga piekļuve, kas ir aktīva darbība. Krimināatbildība iestājas par jebkuru no panta dispozīcijā noteiktajām alternatīvajām darbībām, ja tās radījušas būtisku kaitējumu. Attiecībā uz izspiedējļaunatūrām, galvenokārt aktuāla ir tāda patvaļīga piekļūšana ADAS, kas saistīta ar sistēmas aizsardzības līdzekļu pārvarēšanu. ADAS aizsardzības līdzekļi ir jebkura programma, kuras mērķis ir nodrošināt piekļuves kontroli ADAS resursiem. ADAS pārvarēšana ir darbība, kas mazina, apiet, neitralizē vai izmanto ADAS drošības caurumus, programmas nepilnības, tādējādi piekļūstot aizsargātiem sistēmas resursiem. Praktiski iespējams, bet ne bieži izplatīts veids, kā inficēt ADAS ar izspiedējļaunatūru, ir citai personai piederošu tiesību izmantošana vai likumīgajam lietotājām piešķirtā pilnvarojuma robežu pārkāpšana, lai apzināti inficētu ADAS ar konkrēto ļaunatūru.[41]

---

[39] Krastiņš U. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Rīga: Tiesu namu aģentūra, 2014, 149. lpp.

[40] Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija. Rīga: Apgāds ‘’Jumava’’, 2015, 130.-136. lpp.

[41] Branche P. Ransomware: An analysis of the current and future threat ransomware presents. Ann Arbour: ProQuest, 2017, p. 48

Ne visas izspiedējļaunatūras tiek izplatītas, patvaļīgi piekļūstot ADAS. Inficēt ADAS ar izspiedējļaunatūru var dažādos veidos – atverot surogātpasta vēstuli (spamu), iekļūstot interneta plūsmā, kas lietotāju novirza uz ļaunatūru saturošām interneta vietnēm, atverot ļaunatūru saturošu viltus reklāmu u.tml.[42] Autore uzskata, ka tādos gadījumos objektīvās puses pazīmes neiestājas. Lai inkriminētu šo pantu, jākonstatē, ka hakeris ir mērķtiecīgi noskaidrojis ADAS programmatūras ''vājos punktus'' un nepilnības, un tos ļaunprātīgi izmantojis, tādējādi pārvarot ADAS aizsardzību.

Tāpat hakeriem pastāv iespēja no ADAS iegūt privātu informāciju, kuras iespējamo publiskošanu izmantot kā cietušā ietekmēšanas līdzekli, pieprasot maksāt par to.

Lai iestātos krimināltbildība, obligāti jākonstatē būtisks kaitējums. Šis aspekts plašāk tiks izskatīts darba turpmākajā izklāstā.

Noziedzīgā nodarījuma subjects ir fiziska, pieskaitāma persona, kas sasniegusi 14 gadu vecumu.

241. pantā paredzētais noziedzīgais nodarījums ir tīšs nodarījums ar tiešu vai netiešu nodomu. Netiešu nodomu raksturo personas nevēlēšanās, lai iestājas kaitīgās sekas, tāpēc saistībā ar izspiedējļaunatūrām nodarījums var būt tikai ar tiešu nodomu – tas būtībā ir sagatavošanās posma process, kurā persona sameklē veidu, pielāgo apstākļus, lai veiktu noziedzīgo nodarījumu – inficētu ADAS ar izspiedējļaunatūru. Persona apzinās savu darbību kaitīgumu un rīkojas apzināti, vēlas kaitīgo seku iestāšanos. Patvaļīgas piekļuves primārais mērķis ir pārvarēt ADAS aizsardzības sistēmu, prettiesiski ietekmējot ADAS integritāti.[43]

2.4. ADAS darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju

Krimināllikuma 243. pants nosaka krimināltbildību par ADAS esošās informācijas neatļautu grozīšanu, bojāšanu, iznīcināšanu, pasliktināšanu, aizklāšanu vai apzināti nepatiesas informācijas ievadīšanu ADAS, ja ar to radīts būtisks kaitējums. Panta otrā daļa paredz atbildību par ADAS apzinātu traucēšanu, ievadot, pārnesot, bojājot, izdzēšot, pasliktinot, izmainot vai aizklājot informāciju, ja ar to tiek bojāta vai iznīcināta aizsardzības sistēma un radīts būtisks kaitējums. Trešās daļas kvalificējošā pazīme ir mantkārīgs nolūks, bet piektajā daļā – organizēta grupa, smagas sekas un darbības, kas vērstas pret ADAS, kas apstrādā informāciju, kas saistīta ar valsts drošību. KL 243. panta pirmajā un otrajā daļā paredzētie nodarījumi ir mazāk smagi

[42] A Closer Look at Ransomware Attacks: Why They Still Work. Pieejams: https://heimdalsecurity.com/blog/why-ransomware-attacks-still-work/ [aplūkots 15.04.2019.]
[43] Wall D.S. Cybercrime. The transformation of Crime in the Information Age. Cambridge: Polity Press, 2007, p. 53

noziegumi, bet trešajā un piektajā daļā – smagi noziegumi. Iespējamas panta piektās daļas kvalificējošās pazīmes.

Noziedzīgā nodarījuma grupas objekts ir vispārējā drošība un sabiedriskā kārtība. Noziedzīgā nodarījuma objekts ir ADAS resursu pieejamība, integritāte un konfidencialitāte. Izspiedējļaunatūru gadījumā tiešais objekts ir integritāte, jo ietekmējot informācijas resursu integritāti, automātiski tiek ietekmēta arī infrastruktūras un iekārtas integritāte.[44] ADAS ir sistēma, līdz ar to mainot vienu elementu, tiek izmainīta visa sistēma. KL 243. panta piektās daļas papildu tiešais objekts ir valsts drošības intereses.

KL 243. Pantā paredzētā noziedzīgā nodarījuma objektīvā puse ietver divas nelikumīgas darbības: 1) ADAS esošās informācijas nelikumīgu ietekmēšanu (panta pirmā daļa) un 2) ADAS darbības traucēšana (panta otrā daļa). Izspiedējļaunatūru darbība atbilst panta pirmajai daļai, jo neiestājas panta otrajā daļā paredzētās sekas - netiek bojāta vai iznīcināta ADAS aizsardzības sistēma. Izspiedējļaunatūra aizklāj ADAS datus, t.i., padara sākotnējo saturu neredzamu vai aizklāj ar cita rakstura informāciju, šifrējot ADAS datus.[45] Aizklāta informācija ir pirmās sekas. Ja cietušais hakerim noteiktā laikā nesamaksā pieprasīto maksu, informācija tiek iznīcināta – tā vairs nav izmantojama pēc nozīmes un to nav iespējams atgūt.

Nozieguma sastāvs ir materiāls. Krimināltiesību iestājas par iepriekš norādītajām objektīvās puses darbībām, ja no tām radies būtisks kaitējums.

Noziedzīgā nodarījuma subjekts ir fiziska, pieskaitāma persona, kas sasniegusi 14 gadu vecumu.

ADAS datu nelikumīga ietekmēšana ir tīšs nodarījums ar tiešu nodomu. Vainīgais apzinās savu darbību kaitīgumu, rīkojas apzināti un vēlas kaitīgo seku iestāšanos. Aktuāls ir jautājums, vai par informācijas aizklāšanu ar izspiedējļaunatūru var inkriminēt pazīmi - mantkārīgs nolūks. Šī panta kontekstā par mantkārīgu nolūku atzīstama personas vēlme konkrētā noziedzīga nodarījuma rezultātā iegūt jebkāda veida materiālu vai citāda rakstura labumu sev vai citai personai, vai atbrīvoties no materiālām saistībām.[46] Tomēr autores ieskatā, tikai ar šo noziedzīgo nodarījumu (informācijas aizklāšanu) ļaunatūras izplatītājs nevar sasniegt mērķi un gūt vēlamo labumu, jo vēl ir jāveic nelikumīgs pieprasījums izdarīt kādas mantiska rakstura darbības, piedraudot ar attiecīgu

[44] Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija. Rīga: Apgāds ''Jumava'', 2015, 139. lpp.
[45] Krastiņš U., Liholaja V., Hamkova D. Grām.: Krimināllikuma komentāri. Trešā daļa (XVIII – XXV nodaļa). Rīga: Tiesu nama aģentūra, 2016, 339. lpp.
[46] Ibid. 340. lpp.

kaitējumu. Līdz ar to mantkārīga nolūka pazīme pie izspiedējļaunatūras izmantošanas nav inkriminējama.

2.5. Izspiešana

Saskaņā ar Krimināllikuma 183. pantu, par izspiešanu paredzēta krimināltbildība. Izspiešana ir pieprasījums bez tiesiska pamata atdot mantu vai tiesības uz mantu vai izdarīt kādas mantiska rakstura darbības, cietušajam vai viņa tuviniekiem piedraudot ar vardarbību, piedraudot iznīcināt viņa mantu vai radīt citu būtisku kaitējumu. Tas ir smags noziegums. 183. panta otrā daļa paredz kvalificējošas pazīmes – personu grupa pēc iepriekšējas vienošanās vai izspiešana izdarīta, lietojot vardarbību, ieročus vai sprāgstošas vielas; tas ir sevišķi smags noziegums. KL 184. pants paredz krimināltbildību par izspiešanu organizētā grupa, kas ir sevišķi smags noziegums.

Noziedzīgā nodarījuma grupas objekts ir īpašuma intereses. Izspiešana ir vairākobjektu noziegums, kas apdraud ne tikai cietušā mantiskās intereses, bet atsevišķos gadījumos arī veselību, cieņu un godu.[47]

Izspiešana izpaužas kā aktīvas darbības, bez tiesiska pamata kategoriski pieprasot atdot svešu mantu, atdot tiesības uz šādu mantu vai izdarīt kādas mantiska rakstura darbības. Aktīvās darbības tiek veiktas, izmantojot Informācijas komunikāciju tehnoloģijas jeb ADAS mūsdienu izpratnē.[48] Izspiedējļaunatūras realizētājs pieprasa veikt samaksu noteiktā laika posmā. Pieprasījums tiek izteikts ar ADAS starpniecību, norādot, kā samaksāt pieprasīto summu. Lai nodrošinātu šo darbību izpildi, vainīgais piedraud cietušajam nodarīt kaitējumu – iznīcināt ADAS esošo informāciju, atsevišķos gadījumos piedraud izpaust apkaunojošas vai godu aizskarošas ziņas par cietušo vai viņa tuviniekiem, kas iegūtas, patvaļīgi piekļūstot ADAS.

Draudi tiek izteikti ar ADAS starpniecību. Izspiešanas draudi pastāv ar nosacījumu, ka tie tiks izpildīti, notekot noteiktajam laikam, ja cietušais neizpildīs prasības. Izspiedējļaunatūru izmantošanas gadījumā hakeris piedraud cietušajam, ka šifrētie dati vairs nebūs atšifrējami, t.i., būs neatgūstami un neizmantojami pēc savas nozīmes (iznīcināti), ja cietušais laikā nesamaksās noteikto summu.

Par būtiska kaitējuma piedraudējumu var uzskatīt jebkuru materiālu vai morālu kaitējumu, kas būtiski aizskar cietušā vai viņu tuvinieku intereses. Tas var izpausties datu iznīcināšana vai kā

[47]Krastiņš U., Liholaja V., Hamkova D. Grām.: Krimināllikuma komentāri. Trešā daļa (XVIII – XXV nodaļa). Rīga: Tiesu nama aģentūra, 2016, 63.-67. lpp.
[48] Ķinis U. Noziedzīgi nodarījumi datortīklos. Rīga: Tiesu namu aģentūra, 2000, 86.lpp.

ziņu atklāšana, ko cietušais vai viņa tuvinieki vēlas saglabāt slepenībā, piemēram, komercnoslēpuma atklāšana plašākai sabiedrībai, privātu attēlu publicēšana utml.

Nozieguma sastāvs ir nošķelts. Tas ir pabeigts ar brīdi, kad vainīgais bez tiesiska pamata pieprasa veikt mantiskās darbības, piedraudot ar kaitīgo seku iestāšanos. Ar šo brīdi noziegums ir pabeigts, pat ja pieprasītais labums netiek gūts. Nav iespējams izspiešanas mēģinājums.

Noziedzīgā nodarījuma subjekts ir fiziska, pieskaitāma persona, kas sasniegusi 14 gadu vecumu.

Izspiešanu var izdarīt tikai ar tiešu nodomu. Vainīgais apzinās savu darbību kaitīgumu, vēlas panākt konkrētu mērķi – lai cietušais viņa labā izdara mantiskas darbības, un veic apzinātas darbības (izsaka pieprasījumu bez tiesiska pamata, draud cietušajam), kas virzītas uz šā mērķa sasniegšanu.

Autores ieskatā šajā nodaļā analizētie noziedzīgie nodarījumi raksturo izspiedējļaunatūras izmantošanu. Pirmkārt, tiek veiktas nelikumīgas darbības ar ADAS resursu ietekmēšanas līdzekļiem. Otrkārt, hakeris atsevišķos gadījumos, kad mērķtiecīgi tiek noskaidrotas ADAS programmatūras nepilnības, patvaļīgi piekļūst automatizētai datu apstrādes sistēmai. Treškārt, tiek veikta automatizētā datu apstrādes sistēmā esošās informācijas neatļauta aizklāšana - šifrēšana. Ceturtkārt, tiek izteikts pieprasījums izdarīt kādas mantiska rakstura darbības, piedraudot izpaust apkaunojošas ziņas par cietušo vai viņa tuviniekiem, piedraudot iznīcināt viņu mantu vai radīt viņiem citu būtisku kaitējumu (izspiešana).

3. Atbildības par kibernoziedzību normatīvais regulējums ārvalstīs

3.1. Igaunijas Sodu kodeksa regulējums

Igaunijas Sodu kodeksa (turpmāk – Igaunijas SK) 206. pants paredz krimināltbildību par prettiesisku datorsistēmas datu ietekmēšanu, neatļauti grozot, iznīcinot, bojājot vai aizturot datorsistēmas datus.[49] Panta otrā daļa paredz šādas kvalificējošas pazīmes:

1) nodarījums veikts pret vairāku datorsistēmu datiem un tā veikšanai izmantotas ierīces vai datorprogrammas, kuru realizēšana, izgatavošana, glabāšana un izplatīšana ir kriminalizēta ar Igaunijas SK 216.[1] pantu;

2) to ir izdarījusi grupa;

3) nodarījums vērsts pret datiem, kas atrodas nozīmīgas nozares datorsistēmā;

4) nodarījums ir radījis būtisku kaitējumu.

Panta trešā daļa kā kvalificējošu pazīmi paredz juridisku personu kā noziedzīgā nodarījuma izdarītāju.

Igaunijas SK 207. panta pirmā daļa paredz krimināltbildību par prettiesisku datorsistēmas darbības ietekmēšanu vai traucēšanu, augšupielādējot, pārraidot, iznīcinot, bojājot vai aizturot datus.[50] Kaut gan pantā ietvertā noziedzīgā nodarījuma objektīvās puses pazīmes ir līdzīgas Igaunijas SK 206. panta pazīmēm, 207. panta sastāvs paredz tādu datu ietekmēšanu vai traucēšanu, kas nodrošina datorsistēmas darbību. Panta otrā un trešā daļa paredz tādas pašas kvalificējošas pazīmes, kā 206. pantā.

Igaunijas SK 206. un 207. pants ir līdzīgi KL 243. pantā ietvertā noziedzīgā nodarījuma sastāvam, bet KL vienā pantā apvieno divas objektīvās puses pazīmes – ADAS darbības traucēšanu un nelikumīgu rīcību ar šajā sistēmā iekļauto informāciju. Atšķirībā no KL regulējuma, Igaunijas SK paredz, ka šo noziedzīgo nodarījumu sastāvs ir formāls.

Igaunijas SK 216.[1] pants paredz krimināltbildību par sagatavošanos kibernoziegumam, realizējot, izgatavojot, glabājot vai izplatot ierīci vai datorprogrammu, kas ir izgatavota vai pielāgota noziedzīga nodarījuma veikšanai. Noziedzīgā nodarījuma mērķis ir sagatavoties Igaunijas SK 206., 207., 213., 217. panta nodarījumiem, turpretī KL nepieprasa nolūku veikt konkrētu, normatīvi regulētu noziedzīgo nodarījumu. Latvijas pieeja autores ieskatā ir pozitīvi

[49] Karistusseadustik [Igaunijas Sodu kodekss]. Pieejams: https://www.riigiteataja.ee/en/eli/522012015002/consolide [aplūkots 30.03.2019.]

[50] Krastiņš U., Liholaja V. Salīdzināmās Krimināltiesības. Igaunija, Latvija, Lietuva. Rīga: Tiesu namu aģentūra, 2004, 160.lpp.

vērtējama, ņemot vērā straujo kibernoziedzības attīstību un normatīvā regulējuma nespēju tikt līdzi šai attīstībai.

Igaunijas SK 217. pants paredz kriminālatbildību par prettiesiskas piekļuves datorsistēmai iegūšanu, kas izpaužas kā datorsistēmas aizsardzības līdzekļu iznīcināšana vai izvairīšanās no tiem. Panta otrā daļa papildus nosaka tādas kvalificējošas pazīmes kā būtisks kaitējums, prettiesiska piekļuve iegūta tādai datorsistēmai, kas satur informāciju par valsts noslēpumu, klasificētu ārvalstu informāciju vai valsts iestāžu ierobežotas aprites informāciju, vai piekļuve iegūta nozīmīgas nozares datorsistēmai. Šis pants ir līdzīgs KL 241. pantam par patvaļīgu piekļuvi ADAS, bet galvenā atšķirība ir nozieguma sastāvu veidos pēc to sastāva konstruktīvajām īpatnībām– Igaunijas regulējums tā pamatsastāvu paredz kā formālu, bet Latvijas regulējums kā materiālu noziedzīgu nodarījumu.

Kopumā Igaunijas SK un KL regulējumi kibernoziedzības jautājumos ir līdzīgi, tomēr ir atzīmējamas dažas ievērojamas atšķirības. Pirmkārt, redzamākā atšķirība ir būtiska kaitējuma loma regulējumos. KL 241. un 243. pants ir ar materiālu sastāvu un kaitīgās sekas ir obligāts priekšnoteikums noziedzīgā nodarījuma esībai, turklāt kā kaitējuma latiņa ir uzstādīts būtisks kaitējums. KL regulējums ir detalizētāks un paredz augstāku slieksni nodarījuma atzīšanai par prettiesisku, kā priekšnoteikumus paredzot ne tikai būtisku kaitējumu, bet tam papildus arī tādas kvalificējošās pazīmes kā ‘’smagas sekas’’, ‘’vērsts pret valsts drošību’’, ‘’organizēta grupa’’ Turpretī Igaunijas SK visi ar kibernoziedzību saistītie panti kriminālatbildību par noziedzīgā nodarījuma pamatsastāvu paredz kā formālu noziedzīgu nodarījumu. Būtisks kaitējums un citas pazīmes kā kvalificējošas objektīvās puses pazīmes tiek paredzētas pantu turpmākajās daļās.

Otrkārt, KL regulējums paredz ADAS jēdzienu, kas ir daudz plašāks par Igaunijas SK norādīto datorsistēmu jēdzienu, un precīzāk atbilst kibernoziegumu definīciju veidošanā svarīgajam tehnoloģiskās neitralitātes principam, kas noziedzīgā nodarījuma dispozīcijā prasa atturēties no konkrētas tehnoloģijas apzīmējošiem vārdiem.

Atšķiras arī noziedzīgo nodarījumu grupas objekts. KL attiecīgās normas iekļauj nodaļā par noziedzīgiem nodarījumiem pret sabiedrisko kārtību, turpretī Igaunijas regulējums tos klasificē pie nodarījumiem pret īpašumu.

3.2. Vācijas Krimināl kodeksa regulējums

Vācijas Federatīvās Republikas Krimināl kodekss (turpmāk – Vācijas KK) 202.§ paredz krimināl atbildību par korespondences noslēpuma pārkāpšanu, prettiesiski iegūstot datus, kas īpaši tikuši aizsargāti pret neatļautu piekļuvi.[51]

Vācijas KK, tāpat kā Igaunijas SK, datu bojāšanu atzīst par noziedzīgu nodarījumu pret īpašumu, un 303.a§ paredz krimināl atbildību par datu prettiesisku dzēšanu, padarīšanu par nederīgu vai izmainīšanu. Salīdzinājumā ar KL un Igaunijas SK regulējumu, Vācijas KK atzīstams par stingrāku, jo panta otrā daļā paredz krimināl atbildību par datu bojāšanas mēģinājumu.

Smagākiem gadījumiem Vācijas KK 303.b§ paredz atbildību par datorsabotāžu jeb būtisku nozīmes datu apstrādes traucēšanu, ja ar to tiek traucēta tādu datu apstrāde, kuriem ir būtiska nozīme svešam uzņēmumam, firmai vai valsts institūcijai.[52] Atšķirībā no KL 243. panta pamatsastāva, nodarījums ir formāls. Panta dispozīcija paredz alternatīvās darbības:

1) prettiesiska datu dzēšana, padarīšana par nederīgu vai izmainīšana;
2) datu ievadīšana vai pārtveršana ar nolūku nodarīt kaitējumu;
3) datu apstrādes sistēmas vai datu nesēja iznīcināšana, bojāšana, padarīšana par neizmantojamu, izņemšana vai izmainīšana.

Kā kvalificējoša pazīme ir paredzēta datu apstrādes traucēšana uzņēmumam vai valsts insitūcijai.

Pants īpaši nopietniem gadījumiem papildus paredz šādas kvalificējošās pazīmes:

1) radīti būtiski zaudējumi;
2) nodarījumam ir komerciāls pamats vai arī to veic banda ar mērķi gūt peļņu ar datorsabotāžu;
3) nodarījums apdraud sabiedrības apgādi ar svarīgām precēm vai pakalpojumiem, vai arī apdraud Vācijas Federatīvās Republikas drošību.

Kopumā Vācijas regulējums ir mazāk detalizēts un plašāks nekā Latvijas KL regulējums, tādēļ atzīstams par plašāk interpretējamu. Vācijas regulējums jēdzienus ‘’dators’’ un ‘’automatizēta datu apstrādes sistēma’’ lieto kā sinonīmus.

Salīdzinot Latvijas regulējumu ar Igaunijas SK un Vācijas KK, pozitīvi vērtējams KL jēdziens ‘’automatizētā datu apstrādes sistēma’’, kas šajos trīs regulējumos ir bijis tehnoloģiski visneitrālākais jēdziens.

---

[51] Strafgesetzbuch [Vācijas Federatīvās Republikas Krimināl kodekss] Pieejams: //www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html [aplūkots 07.04.2019.]

[52] Krastiņš U., Liholaja V. Salīdzināmās Krimināltesības.Latvija, Austrija, Šveice, Vācija. Rīga: Tiesu namu aģentūra, 2006, 177.lpp.

Atšķirībā no Krimināllikuma, kas kibernoziegumus paredz kā noziedzīgus nodarījumus pret vispārējo drošību un sabiedrības kārtību, Igaunijas un Vācijas regulējums kibernoziegumus paredz kā noziedzīgus nodarījumus pret īpašumu. Autores ieskatā, šāds grupas objekts precīzāk raksturo ar kibernoziegumu aizskartās intereses, jo kibernoziegums būtībā aizskar ADAS īpašnieku valdījuma vai lietojuma tiesības uz savu ierīci.

Paredzot kibernoziegumu pamatsastāvus kā formālus noziedzīgus nodarījumus, Igaunijas SK un Vācijas KK ir precizāk adaptētas Konvencijas normas, kas kibernoziegumus formulē kā formālus noziedzīgus nodarījumus. Šāda pieeja neparedz noteiktu kaitīguma slieksni, kas atvieglo interešu un tiesību aizstāvību personām, kas automatizētās datu apstrādes sistēmas lieto personiskām vajadzībām.

4. Izspiedējļaunatūras izmantošanas kvalifikācija

4.1. Kvalifikācijas problēmjautājumi

4.1.1. Virtuālā valūta kā manta

Kā jau autore secinājusi, KL 241., 243. un 244. panta objekta un objektīvās puses pazīmes neaptver būtiskāko izspiedējļaunatūras darbības pazīmi – prettiesisko pieprasījumu atdot mantu (naudas summu, kas jākonvertē virtuālās valūtas formā).

Ar jēdzienu ‘’manta’’ apzīmē gan lietu kopumu, gan individuālas lietas. P. Mincs pauž ideju, ka manta ir cilvēka valdīšanas priekšmets, viņa ekonomiskās kundzības objekts.[53] Prettiesiski izņemot lietu no cietušās personas valdījuma, tiek pārkāptas cietušās personas īpašuma tiesības un personas manta kā lietu kopums samazinās par tādu vērtību, cik vērta ir nolaupītā lieta. [54]

Virtuālā valūta, kas tiek pieprasīta cietušajam, nav atzīstama par elektronisko naudu. Vadoties no Maksājumu pakalpojumu un elektroniskās naudas likuma un Eiropas Padomes Direktīvas 2000/46/EK[55], virtuālajai valūtai trūkst viens kritērijs, lai to atzītu par elektronisko naudu, proti, tās segums ir nevis īsta nauda, bet matemātisks algoritms interneta vidē.[56] Saskaņā ar Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likumu, virtuālā valūta ir vērtības digitālais atspoguļojums, kas var būt digitāli nosūtīts, glabāts vai tirgots un funkcionēt kā apmaiņas līdzeklis, bet nav atzīts par likumīgu maksāšanas līdzekli, nav uzskatāms par banknoti un monētu, bezskaidru naudu un elektronisko naudu, kā arī nav monetārā vērtība, kura uzkrāta maksājuma instrumentā, kas tiek izmantots Maksājumu pakalpojumu un elektroniskās naudas likuma 3. panta 10. un 11. punktā minētajos gadījumos.[57] Līdz ar to secināms, ka virtuālā valūta pēc būtības ir maiņas prece, kas digitāli atspoguļo kādu noteiktu vērtību. Jāatzīmē, ka tiesību radītāji ir diezgan atturīgi un nesteidzas noteikti definēt virtuālās valūtas statusu, ieņemot nogaidošas pozīcijas.

---

[53] P. Mincs Krimināltiesības. Sevišķā daļa. Ar V. Liholajas komentāriem. Rīga: Tiesu namu aģentūra, 2005, 315.lpp.
[54] Mežulis D. īpašuma krimināltiesiskā aizsardzība. Rīga: Biznesa augstskola Turība, 2006, 91.-92. lpp.
[55] Eiropas Parlamenta un Padomes Direktīva 2000/46/EK par elektroniskās naudas iestāžu darbības sākšanu, veikšanu un konsultatīvu uzraudzību. Pieņemta 18.09.2000. [12.04.2019. red.]
[56] Kalniņa I. Elektroniskās naudas definīcija un veidi. Jurista vārds, 2017, Nr.40, 13.-14. lpp.
[57] Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likums: LV likums. Pieņemts 17.07.2008. [18.04.2019. red.]

Autores ieskatā, virtuālā valūta atzīstama par mantu krimināltiesiskā izpratnē, jo virtuālās valūtas ieguve, neatkarīgi no iegūšanas veida, prasa finansiālus līdzekļus, un iegūtajai valūtai ir noteikta ekonomiska vērtība. Ja personai jāiegādājas virtuālā valūta no virtuālās valūtas pakalpojumu sniedzēja, iegāde tiks veikta, izmantojot likumīgos maksāšanas līdzekļus, samazinot cietušā mantas apjomu.

P. Mincs ir paudis viedokli, ka nodarījuma kriminālraksturojumam ir būtiski noteikt, vai cietušajam ar nodarījumu noteikts tikai kaitējums vai zaudējums, kā arī, vai tas saistīts ar vainīgā, vai citas personas likumīgu labumu iegūšanu.[58] Tādējādi ir iespējams noteikt atšķirību starp mantkārīgu un tikai kaitīgu uzbrukumu. Analizējot izspiedējļaunatūru izmantošanu, secināms, ka ļaunatūra netiek izplatīta tikai kaitniecības nolūkos. Primārais nodarījuma mērķis ir likumīgu labumu (virtuālās valūtas) gūšana, kas liecina par mantkārīgu nodarījumu.

4.1.2. Būtiska kaitējuma jēdziens kibernoziedzības kontekstā

Krimināllikumā noteikts priekšnoteikums vairāku kibernoziegumu konstatēšanai un pareizai kvalifikācijai ir būtisks kaitējums. Prettiesiska darbība vai bezdarbība var radīt dažādas sekas, bet krimināltiesībās sekas ir tas kaitējums, kas rada ar Krimināllikumu aizsargāto interešu izmaiņas.[59] Būtisks kaitējums ir apzīmējums, ko lieto likumdevējs, lai novērtētu no noziedzīgā nodarījuma radušos kaitīgo seku pakāpi.[60] Ja kaitīgās sekas ir noteiktas noziedzīgā nodarījuma objektīvās puses pazīmju skaitā, tās ietekmē kvalifikāciju, bet ja kaitīgās sekas nav objektīvās puses pazīme, tās palīdz novērtēt nodarījuma kaitīgumu un raksturu, ko ņem vērā pie soda noteikšanas. Būtiska kaitējuma kritēriji ir noteikti Īpašā likuma 23. pantā, un tie ir šādi:

1) nodarīts mantisks zaudējums, kas noziedzīga nodarījuma izdarīšanas brīdī nav bijis mazāks par piecu tai laikā Latvijas Republikā noteikto minimālo mēnešalgu kopsummu, un apdraudētas vēl citas ar likumu aizsargātās intereses;

2) nodarīts mantisks zaudējums, kas noziedzīga nodarījuma izdarīšanas brīdī nav bijis mazāks par desmit tai laikā Latvijas Republikā noteikto minimālo mēnešalgu kopsummu;

3) ievērojami apdraudētas citas ar likumu aizsargātās intereses.

---

[58] P. Mincs Krimināltiesības. Sevišķā daļa. Ar V. Liholajas komentāriem. Rīga: Tiesu namu aģentūra, 2005, 316.lpp.

[59] Krastiņš U. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Rīga: Tiesu namu aģentūra, 2014, 89. lpp.

[60] Liholaja V., Hamkova D. Būtiska kaitējuma izpratne: likums, teorija, prakse. Jurista Vārds, 2012, nr. 2, 6.-12. lpp.

Pirmajā gadījumā ir jākonstatē gan mantisks zaudējums, gan apdraudējums citām ar likumu aizsargātām interesēm; šim apdraudējumam nav jābūt ievērojamam.[61] Trešajā gadījumā jākonstatē ievērojams apdraudējums citām ar likumu aizsargātām interesēm un tiesībām, kas nav saistītas ar mantiska zaudējuma nodarīšanu. Šis kritērijs attiecas uz gadījumiem, kad radīto kaitējumu nav pieņemts vērtēt naudas izteiksmē. U. Krastiņš kā piemēru šādam kaitējumam min ievērojamu kaitējumu valsts institūcijas prestižam, vai tiesisku, fizisku vai morālu kaitējumu kādai personai.

Likumā nav tieši izklāstīti kritēriji ar likumu aizsargāto interešu un tiesību apdraudējuma izvērtēšanai automatizētas datu apstrādes sistēmas darbības apzinātas traucēšanas gadījumā. Līdz ar to, kvalificējot šo noziedzīgo nodarījumu, jābalstās uz Īpašajā likumā noteiktajiem būtiska kaitējuma pamatkritērijiem, kas jāizvērtē un jāpiemēro konkrētais situācijai, izmantojot krimināltiesību teorijā un praksē nostiprinātās atziņas, un, ja nepieciešams, ņemot vērā attiecīgo speciālistu viedokli.[62]

U. Ķinis ir formulējis materiālo un sociālo kritēriju, lai konstatētu ‘’būtisku kaitējumu’’ nodarījumos pret informācijas sistēmu drošību. [63] Lai konstatētu materiālo kritēriju, mantiskajos zaudējumos var ieskaitīt:

1) zaudējumus, kas saistīti ar sistēmas dīkstāvi;

2) izdevumus, kas saistīti ar bojātās informācijas atjaunošanu vai aizstāšanu;

3) izdevumus, kas saistīti ar jaunu programmatisku resursu instalēšanu, kas paredzēti sistēmas drošības funkciju atjaunošanai;

4) izdevumus, kas saistīti ar sistēmas lietotāju piekļuves tiesību korekciju.

Autore uzskata, ka materiālais kritērijs var būt arī zaudējumi, kas traucētas datu apstrādes dēļ nodarīti un atlīdzināmi trešajām personām.

Bieži vien kibernoziegumā cietušās personas nav cietušas Īpašā likuma 23. pantā norādīto zaudējumu piecu minimālo mēnešalgu apmērā vai arī to ir grūti pierādīt. Šī iemesla dēļ jāvērtē arī sociālais kritērijs, kas izriet no citām ar likumu aizsargātām personas interesēm. Personas pamattiesības garantē Satversme, normatīvie akti un līgumi, kas personai piešķir tiesības dibināt,

---

[61] Krastiņš U. Par vērtējuma jēdzieniem krimināltiesību normās. Grām.: Krastiņš U. Krimināltiesību teorija un prakse: viedokļi, problēmas, risinājumi 1998 – 2008. Rīga: Latvijas Vēstnesis, 2009, 52. lpp.

[62] Liholaja V., Hamkova D. Būtiska kaitējuma izpratne: likums, teorija, prakse. Jurista Vārds, 2012, nr. 2, 6.-12. lpp.

[63] Ķinis U. Nodarījumi pret informācijas sistēmu drošību. Krimināllikuma piemērošanas problēmas. Jurista Vārds, 2011, nr. 39, 6.-15. lpp.

grozīt vai izbeigt tiesiskas attiecības. Ar jēdzienu ‘’intereses’’ saprotams labums, ko persona var gūt vai zaudēt. Vērtējot aizskartās ‘’intereses’’, nosaka gan nodarījuma objektu, gan nodarītā kaitējuma apmēru, vērtējot visu sociālā labuma kopumu, ko cietušā persona iegūtu, ja šāds nodarījums nebūtu noticis. Lai par nodarījumu iestātos krimināltbildība, šim interešu aizskārumam jābūt krimināli prettiesiskam. Ar likumu aizsargāta interese ir tieši noteikta tiesību normās vai nav pretrunā ar tām; tas ir mantisks vai nemantisks labums, kuru personai ir tiesība iegūt, īstenojot savas tiesības. Likumīgās intereses aizsardzība ir valsts pozitīvais pienākums. Jāuzsver, ka tas, ka personas ‘’labums’’ ir virtuāls, nenozīmē, ka tas nepastāv.[64]

U. Ķiņa ieskatā, lai noteiktu interešu un tiesību aizskāruma smaguma pakāpi un atzītu to par ievērojamu, jāizvērtē ADAS sociālā nozīmība un veicamo funkciju nozīmība, piemēram, kādu informācijas apriti ADAS nodrošina, kādas sekas iestātos, ja ADAS darbība tiktu traucēta vai apturēta. Sociālās nozīmības izvērtēšanā būtu jāņem vērā šādi kritēriji: vai ADAS tiek izmantots personīgām vajadzībām, vai ADAS apstrādā sensitīvu informāciju, vai tiek ierobežota iespēja apmainīties un saņemt informāciju. Prasībām apdraudējuma pierādīšanai jābūt zemākām, ja apdraudētais objekts ir ar augstu sociālo nozīmību, un augstākām, ja objekta sociālā nozīmība ir zemāka. Interešu aizskārumam jābūt reālām, kā arī jābūt augstākam par vidējo aizskārumu sabiedrības izpratnē. Līdz ar to cietušajam jāspēj pierādīt, ka aizskārums nav ar ikdienišķu raksturu un viegli novēršams.

Attiecībā uz izspiedējļaunatūru izmantošanu, autores ieskatā, cietušajam nav īpaši jāpierāda, ka izspiedējļaunatūras radītais kaitējums ir augstāks par sabiedrībā pieņemto vidējo interešu aizskārumu un nav ar ikdienišķu raksturu, jo datu aizklāšana notiek gandrīz vienlaicīgi ar prettiesiskā pieprasījuma izteikšanu. Noziedzīgais nodarījums rada tādu apgrūtinājumu, kāds nav viegli novēršams parastā situācijā, aizklājot failus, bez iespējas tos atgūt tiesiskā ceļā. Cietušajam noziedzīgā nodarījuma rezultātā ir jāizdara izvēle starp neatgriezenisku informācijas zaudēšanu un mantisko zaudējumu. Pie tam zaudējumi nereti izceļas abos gadījumos.

Visgrūtāk jebkādu būtisku kaitējumu pierādīt ir ADAS īpašniekiem, kas to izmanto personiskai lietošanai. Šajā gadījumā būtu jāņem vērā, kāds raksturs ir zaudētajiem datiem un informācijai. Jāvadās no fakta, ka ar likumu aizsargāta interese ir tieši noteikta tiesību normās. Kaut arī dati un informācija digitālajā vidē pamatā nav uzskatāmi par īpašumu, Satversmes 105. pants aizsargā ne vien īpašuma tiesības civiltiesiskajā izpratnē, bet jēdzienā ‘’īpašums’’ ietver arī

[64] Ķinis U. Jurisdikcija un kibernoziegumi. Rīga: Apgāds ‘’Jumava’’, 2013, 136.lpp.

citas tiesības un nemateriālus labumus, tai skaitā autortiesības. [65] Autortiesību objekts var būt cietušā veidotas datu bāzes, literārie darbi, fotoattēli un citi autora radošās darbības rezultāti[66], kas var būt neatgūstamas, neatkārtojamas vērtības ar privātu raksturu. Kā norādījis Augstākās tiesas Senāta Civillietu departaments, autortiesību objekta pastāvēšana apstiprina radošu darbību darba tapšanā, autoram iegūstot personiskās un mantiskās tiesības, kuras aizsargā Autortiesību likums. [67] Ja persona zaudē autortiesību objektu izspiedējļaunatūras dēļ, jāizvērtē viss sociālā labuma kopums, ko cietušā persona iegūtu, ja šāds nodarījums nebūtu noticis. Līdz ar to secināms, ka arī privātpersonai pastāv iespēja pierādīt būtisko kaitējumu.

Lai personu sauktu pie krimināatbildības, nodarījumam jāsasniedz noteikta kaitīguma pakāpe, kas to atšķir no citiem likumpārkāpumiem.[68] Tomēr jāatzīmē, ka Latvijas likumdevējs neparedz administratīvo atbildību par kibernoziegumiem, bet lai personu varētu saukt pie krimināatbildības, jāpamato būtisks kaitējums. Autore uzskata, ka šī KL pantu dispozīcijā uzstādītā kaitējuma pakāpe ir pārāk augsta, jo praktiski līdz minimumam samazina iespēju aizsargāt savas aizskartās intereses tiem ADAS īpašniekiem, kas to lieto personiskām vajadzībām. Ņemot vērā, ka būtisku kaitējumu nevar pamatot ar vairāku ‘’ne ievērojami’’ apdraudētu interešu kopumu,[69] varētu veidoties arī tāda absurda situācija, kad saskaņā ar KL 241. un 243. pantu pie krimināatbildības nebūtu saucami izspiedējļaunatūras izplatītāji, kas ļaunatūru masveidā izplatītu pa personiskām automatizētām datu apstrādes sistēmām. Šāda veida nodarījumi viennozīmīgi būt atzīstami par prettiesiskiem Kibernoziedzības konvencijas izpratnē, tomēr tie nebūtu sodāmi (ne administratīvi, ne krimināltiesiski) Latvijas tiesību sistēmā. Šajā aspektā autore uzskata par veiksmīgākiem Igaunijas un Vācijas krimināltiesību normatīvos regulējumus, kas kibernoziegumu pamatsastāvus paredz kā formālus noziedzīgus nodarījumus, būtisku kaitējumu paredzot kā kvalificējošu pazīmi.

---

[65] Balodis K. Komentārs Satversmes 105. pantam. Grām.: LR Satversmes komentāri. VIII nodaļa. Cilvēka pamattiesības. Aut. kol. Prof.R.Baloža zinātniskā vadībā. Rīga:Latvijas Vēstnesis, 2011, 466. lpp.

[66] Autortiesību likums. LV likums. Pieņemts 06.04.2000. [20.04.2019. red.]

[67] Augstākās tiesas 19.04.2006. spriedums lietā SKC-266. Pieejams: http://at.gov.lv/lv/judikatura/judikaturas-nolemumu-arhivs?nr=skc-266&date_from=&date_to=&case_nr=&ecli_nr=&dep=&ruling=&name=&action=filter [aplūkots 20.04.2019.]

[68] Hamkova D. Tiesu prakse lietās, kurās noziedzīga nodarījuma sastāva pazīme ir būtisks kaitējums. Rīga, 2018, 40. lpp. Pieejams: http://at.gov.lv/lv/judikatura/tiesu-prakses-apkopojumi/kriminaltiesibas [aplūkots 20.04.2019.]

4.2. Kvalifikācija

Kaut arī izspiedējļaunatūru izmantošanas apmēri aug, Latvijā par šo jautājumu nav tiesu prakse. Šāda situācija pamatojama ar dažādiem iemesliem. Sabiedrības līdzdalība un ziņošana tiesībsargājošām iestādēm par savu tiesību aizskārumu ir atkarīga no sabiedrības izpratnes par kiberdrošību un kibernoziegumiem.[70] Līdz ar to tiesu prakses neesamība saistībā ar izspiedējļaunatūru izmantošanu, un minimālais lietu skaits par kibernoziegumiem vispār, var būt indikātors par kopējo sabiedrības zināšanu līmeni. Jāņem vērā arī fakts, ka kibernoziegumu izmeklēšana prasa speciālas zināšanas informāciju tehnoloģiju jomā, bet Latvijas tiesībsargājošās iestādes raksturo kapacitātes trūkums kibernoziegumu izmeklēšanā.[71] Autores ieskatā, pirmais solis uz tiesu prakses izveidi ir sabiedrības informēšana par izspiedējļaunatūru darbību un to prettiesiskumu, aicinot cietušos vērsties tiesībsargājošās iestādēs.

Tomēr Valsts policija saņem iesniegumus par izspiedējļaunatūru izmantošanu un ir uzsākusi kriminālprocesus, pamatojoties uz KL 243. panta trešo daļu. [72] Autore jau ir pamatojusi, kādēļ šādu kvalifikāciju atzīst par nepareizu. Kaut arī nepastāv tiesu prakse un tiesībsargājošās iestādes saskaras ar grūtībām kibernoziegumu izmeklēšanā, situācijā, kad pastāv gan atbilstošas krimināltiesību normas, gan faktiski tiek izdarīti krimināltiesību normās paredzētie noziedzīgie nodarījumi, ir nepieciešama diskusija par izspiedējvīrusu izmantošanas krimināltiesisko kvalifikāciju.

Analizējot izspiedējļaunatūras darbību un tā radītās sekas, autore ir secinājusi, ka, kvalificējot šo nodarījumu, jāveido ideālā kopība. Vainīgais ar savstarpēji saistītām darbībām vienā šo darbību realizēšanas procesā izdara vairākus patstāvīgus noziedzīgus nodarījumus. Vainīgās personas mērķis ir no cietušā bez tiesiska pamata pieprasīt un iegūt mantiskus līdzekļus, un, lai realizētu šo mērķi, tiek izdarīti citi patstāvīgi noziegumi – nelikumīgas darbības ar ADAS resursu ietekmēšanas līdzekļiem, patvaļīga piekļuve ADAS, un ADAS darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju.

---

[70] Latvijas kiberdrošības stratēģija 2018-2022. Pieejams: http://www.mrcc.lv/~/media/AM/Ministrija/Sabiedribas_lidzdaliba/2018/11/AIMstrat_kiber_projekts_181022.ashx [aplūkots 20.04.2019.]

[71] Trūkst kapacitātes kibernoziegumu izmeklēšanā. Pieejams: https://juristavards.lv/doc/258905-trukst-kapacitates-kibernoziegumu-izmeklesana/ [aplūkots 10.05.2019.]

[72] Par datoru inficēšanu ar izspiedējvīrusu sāk kriminālprocesu. Pieejams: https://www.delfi.lv/news/national/criminal/par-datoru-inficesanu-ar-izspiedejvirusu-sak-kriminalprocesu.d?id=45645004 [aplūkots 10.05.2019.]

Autore piemērā kvalificēs tikai klasiskās izspiedējļaunatūras izmantošanas gadījumu, kurā noziedzīgās darbības nav izraisījušas smagas sekas, tās nav vērstas pret ADAS, kas apstrādā informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību, kā arī noziedzīgo nodarījumu nav izdarījusi organizēta grupa. Šajos gadījumos jāpiemēro attiecīgā panta daļa.

Piemērs: uzņēmuma X īpašnieks, atverot e-pasta pielikumu, kas maskēts kā neapmaksāts rēķins, inficēja uzņēmuma datoru ar izspiedējļaunatūru. Tā rezultātā izspiedējļaunatūra šifrēja ADAS esošo datus, norādot, ka datus iespējams atgūt, samaksājot atlīdzību 0.1 BitCoin kriptovalūtas jeb 738 eiro vērtībā. Ņemot vērā izdevumus par datu atjaunošanu un sistēmas dīkstāves dēļ, uzņēmumam nodarīts zaudējums 2500 eiro apmērā.

Izspiedējļaunatūras izmantošana kvalificējama saskaņā ar KL 244. panta pirmo daļu kā nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm, KL 243. panta pirmo daļu kā automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju, un KL 183. panta pirmo daļu kā izspiešana. Autore kvalifikācijā neiekļaus KL 241. pantu par patvaļīgu piekļuvi ADAS, jo, kā jau iepriekš secināts, inficējot ADAS ar surogātpasta satrpniecību, vainīgais neīsteno patvaļīgu piekļuvi.

4.2.1. Objekts

KL 244. un 243. pantā ietvertā noziedzīgā nodarījuma grupas objekts ir vispārējā drošība un sabiedriskā kārtība, galvenais tiešais objekts – ADAS integritāte, bet papildus tiešais objekts – ADAS konfidencialitāte un pieejamība

KL 183. pantā ietvertā noziedzīgā nodarījuma grupas objekts ir īpašuma aizsardzības intereses, bet tiešais objekts – ADAS valdītāja vai īpašnieka mantiskās intereses

4.2.2. Objektīvā puse

Saskaņā ar KL 244. panta pirmo daļu, pirmais noziedzīgais nodarījums ir aktīvas darbības, kas vērstas uz izspiedējļaunatūras kā ļaunprātīgas datorprogrammas, kura paredzēta ADAS ietekmēšanai, izplatīšanu nolūkā izdarīt noziedzīgu nodarījumu. Izspiedējļaunatūras izplatīšana izpaužas kā tā ievadīšana datorvidē, padarot to pieejamu citām personām. Izspiedējļaunatūru nosūta konkrētai vai nekonkrētai personai un personu lokam, vai to ievieto publiskā datu pārraides tīklā. Konkrētajā piemērā izspiedējļaunatūra ir nosūtīta ar surogātpasta (spama) starpniecību.

Kvalifikācijā norādāma vēl vismaz viena KL 244. panta pirmās daļas dispozīcijā noteiktā alternatīvā darbība, kas raksturo izspiedējļaunatūras iegūšanas veidu – izgatavošana, pielāgošana līdz tā izmantošanai, realizācija.

Noziedzīgā nodarījuma sastāvs ir formāls, līdz ar to nodarījums ir pabeigts ar brīdi, kad izdarīta jebkura no alternatīvajām darbībām.

Otrais noziedzīgais nodarījums ir KL 243. panta pirmajā daļā noteiktās aktīvās darbības, kas izpaužas kā apzināta ADAS ietekmēšana, aizklājot ADAS datus, t.i., padara sākotnējo saturu neredzamu vai aizklāj ar cita rakstura informāciju, šifrējot ADAS datus. Cietušajam laikus nesamaksājot pieprasīto naudas summu, dati tiek iznīcināti.

Nozieguma sastāvs ir materiāls, jo obligāta tā pazīme ir kaitīgas sekas – būtisks kaitējums. Lai konstatētu mantisko kaitējumu, izmantojami 4.1.2 nodaļā norādītie kritēriji zaudējumu noteikšanai. Nemantisko kaitējumu noteikt ir grūtāk. Tiesību piemērotājam jāizvērtē ADAS sociālā nozīmība, kādas sekas rada informācijas aizklāšana – vai tā skars ne tikai ADAS valdītāja un īpašnieka intereses, bet arī trešo personu intereses. Trešais noziedzīgais nodarījums ir tas, ar kuru vainīgais tieši cenšas panākt savu mērķi. Autore uzskata, ka KL 244. panta pirmās daļas un KL 243. panta pirmās daļas noziedzīgie nodarījumi ietilpst sagatavošanās procesā KL 183. panta nodarījumam. Sagatavošanās ir rīka (izspiedējļaunatūras) sameklēšana vai pielāgošana, un cita labvēlīgu apstākļu radīšana noziegumam, kas izpaužas kā datu aizklāšana, kas cietušajam rada pārliecību par to, ka vainīgais pēc pieprasījuma izteikšanas var realizēt draudus un datus iznīcināt.

Saskaņā ar KL 183. pantu, izspiešanas ar izspiedējļaunatūru objektīvās puses pazīmes ir aktīvas darbības, bez tiesiska pamata pieprasot veikt samaksu virtuālajā valūtā noteiktā laika posmā, piedraudot ar ADAS datu iznīcināšanu. Draudi tiek izteikti ar ADAS starpniecību. Cietušajam jāspēj pierādīt, ka ADAS iznīcināšana radītu būtisku kaitējumu.

Nozieguma sastāvs ir nošķelts. Tas ir pabeigts ar brīdi, kad vainīgais bez tiesiska pamata pieprasa veikt mantiskās darbības, piedraudot ar kaitīgo seku iestāšanos. Ar šo brīdi noziegums ir pabeigts, pat ja pieprasītais labums netiek gūts.

4.2.3. Subjekts

244. panta pirmās daļas, 243. panta pirmās daļas un 183. panta pirmās daļas noziedzīgo nodarījumu subjekts ir fiziska, pieskaitāma persona, kas sasniegusi četrpadsmit gadu vecumu.

4.2.4. Subjektīvā puse

244. panta pirmās daļas nodarījumu var izdarīt tikai ar tiešu nodomu. Vainīgais apzinās izspiedējļaunatūras izplatīšanas kaitīgumu, paredz, kādas kaitīgās sekas izspiedējļaunatūra izraisīs, un vēlas šo seku iestāšanos. Konstatējams īpašs nolūks - izmantot izspiedējļaunatūru, lai veiktu vēl kādu Krimināllikumā paredzēto noziedzīgo nodarījumu.

243. panta pirmās daļas nodarījums ir tīšs nodarījums, kuru raksturo tiešs nodoms. Vainīgais apzinās savu darbību nepieļaujamību, paredz, ka datu aizklāšana radīs kaitīgas sekas, un vēlas kaitīgo seku iestāšanos. Par tiešu nodomu liecina tas, ka šis nodarījums ievada nākamo noziedzīgo nodarījumu – izspiešanu.

183. panta pirmās daļas nodarījums ir tīšs nodarījums, kuru raksturo tiešs nodoms. Vainīgais apzinās savu darbību kaitīgumu, vēlas panākt konkrētu mērķi – lai cietušais viņa labā izdara mantiskas darbības, un veic apzinātas darbības (izsaka pieprasījumu bez tiesiska pamata, draud cietušajam), kas virzītas uz šā mērķa sasniegšanu.

Kopsavilkums

Pētījuma rezultātā autore izvirza aizstāvēšanai šādas tēzes:

1. *Ransomware* ļaunatūras līdz šim ir tikušas dēvētas par ''izspiedējvīrusiem'', bet šāds jēdziens ir pārāk šaurs, attiecināms uz atsevišķiem gadījumiem un neatbilst tehnoloģiskās neitralitātes principam. Lai jēdziens aptvertu visu veidu ļaunatūru izmantošanu kiberizpiešanā, par atbilstošāku atzīstams jēdziens ''izspiedējļaunatūra''.
2. Izspiedējļaunatūras izmantošana ir izspiešanas kā klasiska noziedzīga nodarījuma kiber- analogs. Informācijas tehnoloģiju iesaiste palielina nozieguma mērogu un ir ērtāks veids, kā to realizēt. Līdz ar to izspiedējļaunatūras izmantošanas klasificējama kā kiber-iespējams (*cyber enabled*) noziegums, kurā dators tiek izmantots kā rīks nozieguma izdarīšanai.
3. Izspiedējļaunatūras izmantošana ir noziedzīgs nodarījums, kas atbilst vairāku dažādu savstarpēji saistītu noziedzīgu nodarījumu sastāvu pazīmēm. Vainīgās personas mērķis ir no cietušā bez tiesiska pamata pieprasīt un iegūt mantiskus līdzekļus, veicot izspiešanu, bet lai sasniegtu šo mērķi, tiek izdarīti tādi noziedzīgi nodarījumi kā nelikumīgas darbības ar ADAS resursu ietekmēšanas līdzekļiem, patvaļīga piekļuve ADAS, un ADAS darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju.
4. Klasisks izspiedējļaunatūras izmantošana gadījums kvalificējams saskaņā ar KL 244. panta pirmo daļu kā nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm, KL 243. panta pirmo daļu kā automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju, un KL 183. panta pirmo daļu kā izspiešana.
5. Kaut gan virtuālā valūta, kas cietušajam tiek prettiesiski pieprasīta, nav atzīstama par elektronisko naudu, tā ir uzskatāma par mantu krimināltiesiskā izpratnē, jo virtuālo valūtu raksturo noteikta ekonomiska vērtība.
6. Latvijas likumdošana neparedz administratīvo atbildību par kibernoziegumiem, bet Krimināllikums personas saukšanai pie kriminālatbildības paredz būtisku kaitējumu kā nepieciešamo minimālo kaitīguma pakāpi. Tik augstas minimālā kaitīguma pakāpes noteikšana būtiski ierobežo personisko ADAS lietotāju iespējas aizsargāt savas aizskartās intereses, kā arī neatbilst Konvencijas par kibernoziegumiem mērķim.

7. Lai nodrošinātu Krimināllikuma atbilstību Konvencijai par kibernoziegumiem un nodrošinātu personisko ADAS lietotāju interešu aizsardzību, nepieciešams veikt grozījumus Krimināllikumā, no kibernoziegumu pamatsastāva izslēdzot pazīmi ‘’būtisks kaitējums’’. Būtisks kaitējums saglabājams kā kvalificējoša kibernozieguma pazīme.
8. Atšķirībā no Krimināllikuma, kas kibernoziegumus paredz kā noziedzīgus nodarījumus pret vispārējo drošību un sabiedrības kārtību, Igaunijas un Vācijas regulējums kibernoziegumus paredz kā noziedzīgus nodarījumus pret īpašumu. Šāds grupas objekts precīzāk raksturo ar kibernoziegumu aizskartās intereses, jo kibernoziegums aizskar ADAS īpašnieku valdījuma vai lietojuma tiesības uz savu ierīci.
9. Latvijā nepastāv tiesu prakse par izspiedējļaunatūru izmantošanu, kas raksturo sabiedrības zināšanu līmenī informāciju tehnoloģiju jomā un tiesībsargājošo iestāžu ierobežoto kapacitāti kibenoziegumu izmeklēšanā. Tiesu prakses rašanos varētu veicināt sabiedrības informēšana par izspiedējļaunatūru prettiesiskumu un iespēju vērsties tiesībsargājošās iestādēs.
10. Likumdevējam jāspēj būt proaktīvam, jāseko līdzi tehnoloģiskajai attīstībai un nepieciešamības gadījumā laikus jāveic normatīvo tiesību aktu grozījumi atbilstoši tehnoloģiskā progresa tendencēm.

Izmantotās literatūras un avotu saraksts

Literatūras avoti:

1. Balodis K. Komentārs Satversmes 105. pantam. Grām.: LR Satversmes komentāri. VIII nodaļa. Cilvēka pamattiesības. Aut. kol. Prof.R.Baloža zinātniskā vadībā. Rīga:Latvijas Vēstnesis, 2011
2. Kalniņa I. Elektroniskās naudas definīcija un veidi. Jurista vārds, 2017, Nr.4
3. Krastiņš U., Liholaja V., Niedre A. Krimināltiesības. Vispārīgā daļa. Trešais papildinātais izd. Rīga: Tiesu namu aģentūra, 2008
4. Krastiņš U., Liholaja V. Krimināllikuma komentāri. Pirmā daļa (I-VIII[1] nodaļa). Rīga: Tiesu namu aģentūra, 2015
5. Krastiņš U. Noziedzīga nodarījuma sastāvs un nodarījuma kvalifikācija. Teorētiskie aspekti. Rīga: Tiesu namu aģentūra, 2014
6. Krastiņš U., Liholaja V. Salīdzināmās Krimināltiesības. Igaunija, Latvija, Lietuva. Rīga: Tiesu namu aģentūra, 2004
7. Krastiņš U., Liholaja V. Salīdzināmās Kriminăltesības.Latvija, Austrija, Šveice, Vācija. Rīga: Tiesu namu aģentūra, 2006
8. Ķinis U. Jurisdikcija un kibernoziegumi. Rīga: Jumava, 2013
9. Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija. Rīga: Apgāds ‘’Jumava’’, 2015
10. Ķinis U. Kibernoziegumi. Rīga: Biznesa augstskola Turība, 2007
11. Ķinis U. Nodarījumi pret informācijas sistēmu drošību. Krimināllikuma piemērošanas problēmas. Jurista Vārds, 2011, Nr. 39
12. Ķinis U. Noziedzīgi nodarījumi datortīklos. Rīga: Tiesu namu aģentūra, 2000
13. Latvijas kiberdrošības stratēģija 2014-2018. Pieejams: https://www.unodc.org/res/cld/lessons-learned/lva/latvijas_kiberdrobas_stratija_html/Kiberdrosibas_strategija.pdf [aplūkots 20.04.2019.]
14. Latvijas kiberdrošības stratēģija 2018-2022. Pieejams: http://www.mrcc.lv/~/media/AM/Ministrija/Sabiedribas_lidzdaliba/2018/11/AIMstrat_kiber_projekts_181022.ashx [aplūkots 20.04.2019.]
15. Liholaja V., Hamkova D. Būtiska kaitējuma izpratne: likums, teorija, prakse. Jurista Vārds, 2012, Nr. 2
16. Mežulis D. īpašuma krimināltiesiskā aizsardzība. Rīga: Biznesa augstskola Turība, 2006

17. Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas īpatnības. Rīga: Biznesa augstskola Turība, 2003
18. Mincs P. Krimināltiesības. Sevišķā daļa. Ar V. Liholajas komentāriem. Rīga: Tiesu namu aģentūra, 2005
19. Par datoru inficēšanu ar izspiedējvīrusu sāk kriminālprocesu. Pieejams: https://www.delfi.lv/news/national/criminal/par-datoru-inficesanu-ar-izspiedejvirusu-sak-kriminalprocesu.d?id=45645004 [aplūkots 10.05.2019.]
20. Par globālo izspiedējvīrusu Latvijā ziņojušas 20 personas. Pieejams: http://www.delfi.lv/news/national/politics/par-globalo-izspiedejvirusu-latvija-zinojusas-20-personas.d?id=48841773 [aplūkots 21.04.2019.]
21. Rozenfelds J. Intelektuālais īpašums. Rīga: Zvaigzne ABC
22. Trūkst kapacitātes kibernoziegumu izmeklēšanā. Pieejams: https://juristavards.lv/doc/258905-trukst-kapacitates-kibernoziegumu-izmeklesana/ [aplūkots 10.05.2019.]
23. All about ransomware. Pieejams: https://www.malwarebytes.com/ransomware/ [aplūkots 13.04.2019.]
24. A closer Look at Ransomware Attacks: Why They Still Work. Pieejams: https://heimdalsecurity.com/blog/why-ransomware-attacks-still-work/ [aplūkots 15.04.2019.]
25. Branche P. Ransomware: An analysis of the current and future threat ransomware presents. Ann Arbour: ProQuest, 2017
26. Brenner Susan W. Cybercrime. Criminal Threats from Cyberspace. California: Greenwood Publishing Group, 2010
27. Chart of signatures and ratifications of Treaty 185. Pieejams: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=exhG7iJ7 [aplūkots 02.04.2019.]
28. Clough J. The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World. Criminal Law Forum, 2012, No.4
29. Clough J. Principles of cybercrime. New York: Cambridge University Press, 2010, p. 9.
30. Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes. Pieejams:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf [aplūkots 10.04.2019.]

31. Donalds C., Osei-Bryson K.M. Toward a cybercrime classification ontology: A knowledge-based approach. Computers in Human Behavior, 2019, No. 92.
32. Gercke M. Understanding cybercrime: phenomena, challenges and legal response. [b.v.]: ITU, 2012
33. Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019. Pieejams: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ [aplūkots 21.04.2019.]
34. Jewked Y., Yar M. Internet crime handbook. New York: Willan Publishing, 2010
35. Kirwan G., Power A. Cybercrime. The Psychology of Online Offenders. Cambridge: Cambridge University Press, 2013
36. Reed Chris, Angel John. Computer Law. Fifth Edition. New York: Oxford University Press, 2003
37. Singer P.W., Friedman A. Cybersecurity and cyberwar. New York: Oxford University Press, 2014
38. Smith R., Cheung R., Yiu-Chang Lau L. Cybercrime risks and responses. Eastern and Western perspectives. Hampshire: Palgrave Macmillan, 2015
39. Wall D.S. Cybercrime. The transformation of Crime in the Information Age. Cambridge: Polity Press, 2007

Normatīvie akti:

40. Konvencija par kibernoziegumiem. Parakstīta Budapeštā 05.05.2004. [02.04.2019. red.]
41. Eiropas Parlamenta un Padomes Direktīva 2000/46/EK par elektroniskās naudas iestāžu darbības sākšanu, veikšanu un konsultatīvu uzraudzību. Pieņemta 18.09.2000. [12.04.2019. red.]
42. Krimināllikums. LV likums. Pieņemts: 17.06.1998. [08.04.2019. red.]
43. Autortiesību likums. LV likums. Pieņemts 06.04.2000. [20.04.2019. red.]
44. Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likums: LV likums. Pieņemts 17.07.2008. [18.04.2019. red.]
45. Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību: LV likums. Pieņemts 15.10.1998. [12.04.2019. red.]

46. Likumprojekta ‘’Grozījumi Krimināllikumā’’ anotācija. Pieejama: http://www.saeima.lv/bi8/lasa?dd=LP0894_0 [aplūkots 04.04.2019.]
47. Karistusseadustik [Igaunijas Sodu kodekss]. Pieejams: https://www.riigiteataja.ee/en/eli/522012015002/consolide [aplūkots 30.03.2019.]
48. Strafgesetzbuch [Vācijas Federatīvās Republikas Krimināl kodekss] Pieejams: //www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html [aplūkots 07.04.2019.]

Juridiskās prakses materiāli:

49. Augstākās tiesas 19.04.2006. spriedums lietā SKC-266. Pieejams: http://at.gov.lv/lv/judikatura/judikaturas-nolemumu-arhivs?nr=skc-266&date_from=&date_to=&case_nr=&ecli_nr=&dep=&ruling=&name=&action=filter [aplūkots 20.04.2019.]
50. Hamkova D. Tiesu prakse lietās, kurās noziedzīga nodarījuma sastāva pazīme ir būtisks kaitējums. Rīga, 2018, 40. lpp. Pieejams: http://at.gov.lv/lv/judikatura/tiesu-prakses-apkopojumi/kriminaltiesibas / [aplūkots 20.04.2019.]