https://doi.org/10.25143/SOCR.08.2017.2.25-43

Kriminalitātes izpausmes forma – kibernoziedzība: kriminoloģiskie aspekti

Dr. iur. ***Aldona Kipāne***

Rīgas Stradiņa universitāte, Juridiskā fakultāte, Latvija
aldonakipane@inbox.lv

Kopsavilkums

Mūsdienās stabilu vietu kopējā noziedzīgo nodarījumu skaitā ieņem kibernoziegumi jeb interneta vidē pastrādātie un vadītie noziedzīgie nodarījumi. Kibertelpa viegli ir izmantojama, lai nodarītu kaitējumu indivīdam, sabiedrības grupai vai valstij kopumā. Raksts sniedz ieskatu kibernoziedznieka kriminoloģiskajā raksturojumā, un īpaša uzmanība šajā publikācijā tiek veltīta kiberkrimināLo uzvedību skaidrojošo teoriju analīzei.

Pētījuma rezultāti liecina, ka:

1) kibernoziedznieka profila kriminoloģisko raksturojumu veido šādi pamatelementi: personīgās iezīmes, krimināLais profesionālisms, tehniskās zināšanas, sociālais raksturojums un motivācijas raksturojums;
2) kibernoziedzība ir komplicēta sociālā parādība ar tai raksturīgām determinantu īpatnībām;
3) kiberkriminalitāti var izskaidrot ar dažādu krimināLās uzvedības veidošanās teoriju palīdzību: telpu pārnešanas teoriju, ikdienas aktivitātes un oportūnistiskās uzvedības teorijām, sociālās iemācīšanas teoriju, lomu konflikta un racionālās izvēles teorijām, kā arī iespēju teoriju, sociālās kontroles un atturēšanas teorijām.

Atslēgvārdi: kriminalitāte, kibertelpa, kibernoziedzība, kibernoziedznieks.

Ievads

Mūsdienās cilvēks bieži dzīvo divās paralēlās pasaulēs – reālajā un virtuālajā (kibervidē), atsevišķos gadījumos nenošķirot vai pat neapzinoties abu pasauļu robežas. Pasaules lielākais informācijas apmaiņas tīkls internets ir starptautiska izplatības vieta, kurā valstis tiek savstarpēji saistītas. Kibertelpa kā interaktīva vide ietver lietotājus,

tīklus, skaitļošanas tehnoloģijas, programmatūru, procesus, pārsūtītas jeb uzglabātas informācijas kopumu, lietojumprogrammas, pakalpojumus un sistēmas, kas savienotas tieši vai netieši, izmantojot internetu, telekomunikācijas vai datortīklus, un kurā mijiedarbojas tās lietotāji [24]. Pēc Interneta asociācijas datiem 2016. gadā 80 % Latvijas iedzīvotāju bija sasniedzami internetā, 78 % internetu lietoja katru dienu (vidējais lietotāja vecums ir 25–44 gadi, 143 000 bija aktīvi interneta lietotāji, 800 000 internetu lietoja tālrunī, 400 000 lietoja internetu planšetē) [28]. Pētījums par mobilo ierīču (telefona un planšetes) lietošanas paradumiem mazu bērnu vidū apstiprina pieņēmumu par digitalizācijas radīto sociālo plaisu starp paaudzēm. Latvijā mobilās ierīces lieto lielākā daļa (72 %) bērnu vecumā līdz sešiem gadiem, taču īpaši zīmīgi, ka teju katrs otrais bērns (44 %) ierīces izmanto galvenokārt viens pats – bez pieaugušā klātbūtnes [2; 10].

Kibervide ietekmē sabiedrības, biznesa un indivīda dzīvi, radot jaunas iespējas un mainot saziņas, darba un studiju vidi [4, *154*]. Modernās tehnoloģijas rada cilvēcei labvēlīgus apstākļus darbam, studijām un saziņai, tās ietekmē cilvēku mijiedarbību. 2015. gadā 3,2 miljardi (43 %) pasaules iedzīvotāju lietoja internetu (2014. gadā – 2,9 miljardi). Cilvēki, izmantojot dažādas ierīces (datoru, viedtālruni, planšetdatoru u. tml.), no jebkuras pasaules daļas var iegūt informāciju, to radīt un ar to apmainīties (sazināties, izklaidēties un strādāt). Tomēr negatīvais aspekts globālajā tīmeklī un ar moderno tehnoloģiju saistītajā vidē ir iespējamā noziedzīgā rīcība – nodarīt kaitējumu, draudēt, vajāt, iebiedēt u. tml. [34, *505*], tādējādi radot sociāli negatīvu parādību – kibernoziedzību. Šajā aspektā var minēt itāļu kriminologa Enriko Ferri (*Enrico Ferri*) atziņas. Viņš strauju noziedzības attīstību skaidroja ar civilizācijas evolūcijas un noziedzības neizbēgamo saikni, jo gan sociālo, gan bioloģisko paradumu evolūcija nav saistīta tikai ar progresu. Jebkuram progresam vienā virzienā blakus pastāv arī regress [11, *51*].

Kibernoziedzība ir specifisks, sarežģīts nodarījumu kopums, kura, tāpat kā noziedzības fenomens, novērtējama ne tikai pēc tās veida, izdarīšanas paņēmieniem, kaitīguma, sociālās bīstamības, kaitīgajām sekām, bet arī pēc noziedznieka personības un kriminālās motivācijas raksturojuma, teorijām par šī noziedzības veida izcelšanos.

Darba mērķis: sniegt ieskatu kibernoziedznieka kriminoloģiskajā raksturojumā un kibernoziedzības cēloņu teorijās.

Materiāls un metodes: pētījumā izmantotas zinātniskās izziņas metodes – universālās, sevišķās un speciālās izziņas metodes. Galvenokārt tika izmantota analīzes un sintēzes metode, zinātniskās indukcijas un dedukcijas metode. Pētījuma bāze ir dažādu zinātnieku un speciālistu atziņas un viedokļi, kā arī izpētes secinājumi.

Kibernoziedzības izplatības tendences

Noziedzības attīstību un tendences ietekmē gan globalizācijas process, gan informācijas tehnoloģiju pilnveidošana. Visā pasaulē noziedzība, nekārtības un nemieri cilvēkos rada arvien lielāku satraukumu un bažas. Bailes no noziedzības un globālo draudu izplatīšanās sabiedrībā veicina pašpaļāvības trūkumu un nedrošības sajūtu. Šādai nedrošības sajūtai viens no reāliem pamatiem ir kibernoziedzība. Cilvēku ievainojamība un draudi virtuālajā vidē pieaug, iedzīvotājus satrauc drošība internetā. Noziedzīgs nodarījums ir daudzveidīgs, sarežģīts un komplekss fenomens, un daudzu tā aspektu izskaidrošana ir īsts izaicinājums [26, *34*]. Kibernozieguma daudzveidība ir sevišķi kaitīgs nodarījums, kas izpaužas dažādos sabiedrības dzīves segmentos un nopietni ietekmē sabiedrību vairākās formās – sociālajā dezorganizācijā, ekonomiskos zaudējumos un psiholoģiskos traucējumos. Kibernoziegums tiek pastrādāts, pastāvot kibernoziedznieka pārmērīgi palielinātai vajadzību izpausmei sabiedrībai nepieņemamā veidā. Kibernoziedznieks apstrīd tās vērtības, ko ir izstrādājusi sabiedrība. Turklāt jāņem vērā, ka dažādās situācijās kibernoziedzniekam ir vairāk vai mazāk iespēju pastrādāt noziedzīgu nodarījumu un ka pastāv apstākļi, kas rada augstu vai zemu riska pakāpi. Piemēram, konflikta teorijas modelī tiek uzsvērts, ka dažādām sociālajām grupām ir atšķirīgas vērtību sistēmas. Savukārt franču sociologa Emīla Dirkema (*Émile Durkheim*) ieskatā noziedzīgs nodarījums ir normāla sabiedrības pazīme, un tas ir nepieciešams. Noziedzība ir visur esoša, visās sabiedrībās un laikos. Teorija, ka noziedzība ir normāls sabiedrības aspekts, balstās uz pārliecību, ka noziedzīgs nodarījums pats par sevi ir kā sociāla funkcija.

Kibernoziedznieka profesionālās prasmes un iemaņas, par spīti nacionālās valsts un starptautisko organizāciju pretdarbībai, ļauj noziedzniekam nelikumīgi, ilgstoši un plaši darboties kibervidē – izveidot viltotas un ļaundabīgas interneta vietnes, viltot sociālos profilus, izveidot ļaundabīgu kodu saturošas aplikācijas, uzlauzt vai / un sabojāt mājaslapas u. tml. *Kaspersky Lab* pētījumā "Patērētāju drošības apdraudējuma aptauja 2016. Savienots, bet ne aizsargāts" (*Consumer Security Risks Survey 2016. Connected but not Protected*) apzināts, ka, pieaugot patērētāju finanšu tiešsaistes apdraudējumu daudzveidībai un sarežģītībai, krāpšanas, identitātes zādzību un ierīču uzlaušanas internetā radītie zaudējumi sasniedz daudzus miljardus gadā. Turklāt par daudziem gadījumiem netiek ziņots, tāpēc patiesās izmaksas varētu būt ievērojami lielākas [7].

Kiberkrimināla uzvedība ir sociāli postoša darbība, kas rada kaitējumu sabiedrībai kopumā, uzņēmumiem un indivīdam personiski. Piemēram, datorkrāpšana nodara ievērojamus zaudējumus kopienai, sabiedrībai un indivīdam. Potenciālās krāpšanas sekas var iespaidot organizācijas stratēģiskā, juridiskā, finanšu un operatīvā līmenī [40].

Starptautisko pētījumu rezultāti un kriminālās statistikas datu analīze liecina, ka kiberkriminalitātei kopējā noziedzības struktūrā ir visizteiktākais un krasākais pieaugums. Piemēram, Valsts policija arvien vairāk saņem iesniegumus par apkrāpšanu, iegādājoties dažādas preces interneta veikalos. Krāpšanas shēmas var darboties no

abām pusēm – no pārdevēja vai pircēja puses. Turklāt noziedzīgās aktivitātes kibervidē strauji palielinās, un attīstās to veidi, tie kļūst agresīvāki, uzbrūkošāki un tehniski prasmīgāki [8].

Kibernoziedzības fundamentālie cēloņi ir tiesiskie, ekonomiskie un sociālie cēloņi. Nepilngadīgu personu izdarītos kibernoziegumus veicina dažādi cēloņi un apstākļi – ģimenes sociāli ekonomiskais stāvoklis, vardarbība ģimenē, izpratnes trūkums par garīgajām, sociālajām vērtībām un normām, atkarības vielu lietošana, zems bērna pašnovērtējums, kā arī nelietderīga brīvā laika pavadīšana. *Kaspersky Lab* veiktā izpēte parāda, ka globālās tehnoloģijas arvien biežāk izmanto kibernoziedznieki, hakeri, kiberteroristi un bulinga īstenotāji [7]. Kibernoziedznieki var traucēt vai destabilizēt, kā arī sāpināt, meklēt iespēju iedzīvoties, censties iegūt datus vai identitāti, bet sociāli bīstamākie politisku mērķu vadīti var uzbrukt valsts infrastruktūrai (elektrības tīkliem u. tml.).

Ņemot vērā kibernoziedzības specifiskos parametrus, cīņā ar kibernoziegumiem tiek atzīti divi būtiski virzieni:

1) starptautisko un nacionālo tiesību aktu pilnveidošana;
2) institucionālās sistēmas struktūru, kas veic konkrētus pasākumus kibernoziegumu novēršanā un apkarošanā, attīstība [42, *198*].

Kibertelpā indivīds var tikt apdraudēts dažādos veidos. Publiskajā telpā ir nonākusi informācija par suicidālām sociālo tīklu spēlēm, piemēram, *Zilo vali*. Spēles Latvijā strauji izplatījušās jauniešu vidū (pārsvarā pusaudžu vecumā no deviņiem līdz piecpadsmit gadiem) – tajās tiek apgalvots, ka esot "stilīgi un varonīgi" nenobīties un spēt sagriezt sev rokas vai citādi nodarīt sev sāpes. Visa spēle ir orientēta uz sevis kropļošanu un iznīcināšanu. Spēlei ir 50 līmeņi, pēdējā līmenī tiek pieprasīts izdarīt pašnāvību. Pirmajās dienās bērni graiza rokas un, lai pierādītu uzdevuma izpildi, ievieto attēlus internetā. Gadījumos, kad bērns kādu uzdevumu atsakās pildīt, viņam tiek piedraudēts, ka cietīs viņa ģimene. Pusaudžu vecumā bērns ir uzņēmīgs un vēlas pamēģināt dažādas riskantas spēles, tāpēc, baidoties par savu ģimeni, "iet līdz galam" [33, *12*]. Visbiežāk, iespējams, spēlei pievēršas tie bērni, kuriem pietrūkst saskarsmes ģimenē vai skolā, vai abās vidēs. Spēles organizētāji, uzturētāji un pārziņi izmanto upura neaizsargātību un ievainojamību.

Pētījumi apliecina, ka spriedze ģimenē, skolā vai darbā var izraisīt stresu, tādējādi mazinot psiholoģisko un fizisko labklājību. Nenoliedzami, ka mūsdienu bērnu uzvedības traucējumu iemesli ir saistīti ar spriedzes sekām, lomu konfliktu, vecāku laika trūkumu veltīt uzmanību bērnam un divvirzienu saskarsmes saiknes nepilnību. Saskarsmes kvalitāte un attiecības, kas veidojas saskarsmes procesā, būtiski ietekmē cilvēku dzīvi, pašsajūtu un darbspējas. Konflikti, deformēta saskarsme traumē cilvēku psihi, izraisa spēcīgas negatīvas emocijas, aizvaino, cērt grūti dzīstošas brūces cilvēku dvēselēs. Tomēr cilvēks ir iekārtots tā, ka pat nelabvēlīga saskarsme viņam ir vēlamāka nekā pilnīga izolētība. Emocionālo saišu trūkums draud cilvēkam ar fatālu iznākumu [30, *10*], – psiholoģiski nenobrieduša un / vai depresīva pusaudža plānveidīga, sistēmiska, psiholoģiska, ļaunprātīga manipulācija pakļauj viņu iesaistei un uzraudzībai dažāda līmeņa aktivitātēs.

Spēles gala mērķis ir pamudināt pusaudzi rīkoties pret sevi galēji vardarbīgi (realizēt autoagresiju). Iespējams, ka šādā veidā tiek stimulētas un apmierinātas kādas personas slēptās vardarbīgās tieksmes (vērot citas personas savainošanos, pašsakropļošanos vai suicīda gadījumus). Pastāv liela iespējamība, ka šādas darbības ir saistītas ar organizēto noziedzību. Minētais fenomens rada jaunu izzināšanas kriminoloģijas virzienu – suicidālo kriminoloģiju.

Kibernoziedznieka pazīmes, raksturojums, motivācija

Kiberkriminalitātes augšupejošās dinamikas cēlonis ir ne tikai jauno tehnoloģiju straujā attīstība, bet arī iespēja iegūt lielus ienākumus un peļņu ar diezgan zemiem riskiem. Kibernoziegumu izplatību sekmē tas, ka tos var izdarīt no milzu attāluma, neizmantojot ievērojamus resursus un bez lieliem izdevumiem, saglabājot anonimitāti. Tajā pašā laikā kibernoziedznieki nepārtraukti meklē jaunus nodarījuma izdarīšanas veidus (kādā veidā apkrāpt, izmantot ļaunprogrammatūras, pikšķerēšanu u. c.). Tas parāda nākotnes kibernoziedzības prognozi, proti, kibernoziedzības turpmāku pieaugumu gandrīz visos aspektos (īpaši ekonomiskās noziedzības jomā). Izvērtējot moderno tehnoloģiju lietošanas paradumus un prasmes, var secināt, ka mainīsies kibernoziedznieka vidējais vecums, kibernoziedznieki būs arvien jaunāki.

Noziedzīgajā nodarījumā izpaužas indivīda antisociālā ievirze, atspoguļojot viņa negatīvās sociāli nozīmīgās vērtības, kas iedarbojas uz noziedzīga nodarījuma ārējiem apstākļiem un noziedzīgas darbības raksturu [20, *8*; 21; 22].

Noziedznieks ir ne tikai cilvēks ar noteiktu statusu, kuram ir tiesības, pienākumi, atbildība, bet viņš ir arī indivīds kā sarežģīta sistēma ar:

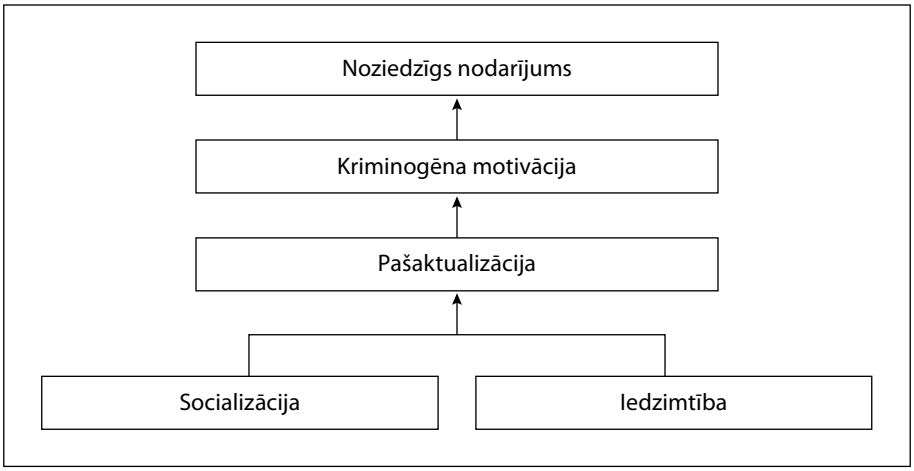
1) vajadzībām – interesēm – spējām;
2) emocijām – domāšanu – gribu;
3) temperamentu – raksturu – vērtīborientāciju.

Noziedzīga nodarījuma izdarīšanu var determinēt vajadzību sistēma, temperamenta un rakstura īpatnības, vērtīborientācijas pamatievirze un citi apstākļi. Personības iezīmēm ir būtiska loma personības uzvedības izpausmēs. Cilvēkam ir gan raksturīgās, gan tipiskās īpašības. Pēc Sāras Hempsonas (*Sarah E. Hampson*) uzskata, aplūkojot kriminālo uzvedību no personības psiholoģijas viedokļa, nevis situācijas vai apkārtējiem apstākļiem, tieši personību raksturojošajiem lielumiem ir noteicošā loma kriminālās uzvedības skaidrošanā [14, *3*]. Tiesu psiholoģijas eksperte Evija Strika secina, ka personības iezīmes ir relatīvi stabils personības raksturotājs. Tās ir kā vispārēja predispozīcija tam, kā personība reaģēs konkrētā situācijā. Personības uzvedība vienmēr ir tāda vai cita personības iezīmju konfigurācijas izpausme [29, *34*]. Noziedzniekiem ir saasinātas vairākas personības iezīmes: impulsivitāte, agresivitāte (augsts agresivitātes līmenis), grūtības prognozēt savas rīcības sekas, rigiditāte, melīgums, patmīlīgums, egocentriskums, afektīvi piesātināti pārdzīvojumi, savdabīga ievirze un spriedumi, grūti

prognozējama uzvedība, atrautība no sociālās realitātes, nespēja interiorizēt[1] morālās un likuma normas, naidīgums [1, *193–195*]. Šīs iezīmes nosaka viņu uzvedību, vājina sociālo adaptāciju un rada grūtības interpersonālajās attiecībās.

Noziedznieka personību tāpat kā jebkura indivīda personības veidošanos determinē trīs faktori:

1) iedzimtība – organisma īpašību pēctecība ar ģenētisko determināciju paaudžu maiņā. Bioloģiskā ietekme un ģenētiskie faktori ir pierādīti dažādos pētījumos, piemēram, ģenētikas daba apzināta metaanalizē par indivīda iezīmēm un īpašību pārmantojamību. Apkopojot datus par vairāk nekā 14 miljoniem dvīņu pāru 50 gadu periodā 39 pasaules valstīs, secināts, ka visas iezīmes ir pārmantojamas, nav īpašības ar mazāku ietekmes nozīmi [37];
2) socializācija – uzvedības normu apgūšana noteiktā sociālā vidē, kuru veido trīs apakšsistēmu vienība: mikrovide, makrovide un sociālā vide kopumā. Piemēram, noziedzīgas uzvedības attīstības daudzfaktoru pētījumu analīze rāda, ka garīgā veselība, ģimenes stabilitāte un apstākļi mājās ir izšķirošais kritērijs bērniem 8–10 gadu vecumā, lai piedzīvotu pilnvērtīgu pieaugušā dzīvi;
3) pašaktualizācija (raksturs, intelekts, dzīves vērtības) – personības veidojošo faktoru mijiedarbība (sk. 1. att.) koncentrējas pašaktualizācijā, kas tieši veido kriminogēnas motivācijas pamatu. Taču konkrēta noziedzīgā nodarījuma veicinošajiem apstākļiem šos faktorus sasaista tikai kriminogēnas motivācijas starpposms – noziedzīga nodarījuma cēlonis.



1. attēls. Personību veidojošo faktoru mijiedarbība (pēc Vedins, 2008)

[1] Interiorizēts (angļu val. *interiorise* < latīņu *interior*) – iekšā esošs.

Tradicionāli par kibernoziedzniekiem sauc noteikta profila speciālistus. Noziedzīgas darbības veicēji internetvidē tiek dēvēti par hakeriem, kiberkrāpniekiem, *WEB* noziedzniekiem u. tml. Kibernoziedzības pētījumā atzīts, ka vairāk nekā 10 % no noskaidrotajiem kibernoziedzniekiem bija pazīstami ar noziedzīgā nodarījuma upuriem, piemēram, kaimiņu, draugu, radinieku. Apmēram 5 % no noskaidroto noziedznieku skaita bija "neapmierinātie" darbinieki (angļu val. *disgruntled employee*) un datorkrampļauži (angļu val. *cracker*) – tehniski izglītoti cilvēki, kas spēj atklāt sistēmas neaizsargātās vietas [6]. Apjomīga ir nelegālā biznesa organizācijas darbība, kas organizētās noziedzības struktūrā piesaista informācijas tehnoloģijas speciālistus (hakerus, programmētājus, IT ekspertus, provaiderus, kasierus, kredītkašu kontu sagādniekus, līderus, "naudas mūļus" u. c.).

Kiberorganizēto kriminālo grupu struktūra ir kā savdabīga piramīda. Nav šaubu, ka mūsdienās virtuālā vide ieviesusi jaunu efektivitātes, saskarsmes un ražīguma līmeni biznesa struktūrās visā pasaulē. Speciālisti norāda, ka organizētās grupas dalībnieki darbojas pēc vislabākajiem uzņēmējdarbības organizatoriskajiem principiem – ar strikti noteiktiem biznesa procesiem, ar definētiem mērķiem, stratēģijām, dalībnieku lomu, atbildības plānu sadalījumiem. Turklāt organizētās noziedzības iesaiste un tās izdarītie kibernoziegumi ievērojami pieaug. Piemēram, pēc Apvienotās Karalistes organizētās noziedzības apkarošanas grupas datiem 2007. gadā internets ir ļāvis kriminālajām struktūrām vērienīgi palielināt viltoto preču un pirātiskās produkcijas realizācijas tirgu [30, *10*]. Savukārt pēc Ziemeļīrijas 2015. gada pārskata par organizēto noziedzību un draudu novērtējumu, organizētā noziedzība ir vairākus miljonus mārciņu gūstoša industrija [31]. Tās sfērā ir virkne noziedzīgu nodarījumu, to skaitā kibernoziegumu. Kibervide ir ļāvusi kriminālajām struktūrām vērienīgi palielināt ietekmi dažādās sfērās: degvielas aprites tirgū, narkotisko vielu izplatīšanas jomā, noziedzīgi iegūtu līdzekļu legalizēšanā ("naudas atmazgāšanas"), kontrabandas, krāpšanas un citu noziedzīgu nodarījumu jomā [32, *9*].

Kibernoziedznieka profilu var raksturot, ietverot tādus pamatelementus kā:

1) personīgās iezīmes, kuras raksturīgas konkrētam cilvēkam un kuras predisponē indivīdu izdarīt kibernoziegumu. Personības raksturīgās iezīmes tiek definētas kā plaša individuāli psiholoģiskā dimensija, kas apraksta personas uzvedības, domu un izjūtu internālās, stabilās un vispārīgās individuālās atšķirības. Iezīmes parādās indivīda aktivitātēs dažādās situācijās un dažādos laika sprīžos [29, *33*];
2) kriminālais profesionālisms – ar to saprotot personības specifiskās iezīmes, kas sekmē droši un efektīvi izdarīt kibernoziegumu. Tas ietver četras obligātās pazīmes: specifiskās personiskās īpašības, zināšanas un iemaņas; bezbailību, drosmi un pārliecinātību par sevi; rīcības efektivitāti un dzīvotspēju; noziedzīga nodarījuma izdarīšanu un noteikta mērķa sasniegšanu [39, *94*], piemēram, finansiāli motivētiem kibernoziedzniekiem pārsvarā ir divi galvenie mērķi – ievades dati un lietotāja identitāte, lai ar iegūto identitāti varētu piekļūt finanšu datiem;

3) tehniskās zināšanas, kas saistītas ar speciālām zināšanām un tehniskām iemaņām darbā ar sarežģītām programmām un ierīcēm, kas ļauj izdarīt kibernoziegumus. Kibernoziedzības pētījumā secināts, ka tehniskā izpilde 65 % no visām pretlikumīgajām darbībām ir nosacīti vienkārša, 13 % – prasīja vidēja līmeņa tehniskās prasmes un iemaņas, bet 22 % gadījumu – sarežģītas tehniskās prasmes un iemaņas. Kibernoziegumu izdarījušās personas visbiežāk bija augstskolu studenti vai citu mācību iestāžu audzēkņi. Kopumā atzīts, ka izglītības līmenis starp kibernoziedzniekiem var būt augstāks nekā starp citu kategoriju noziedzniekiem [6]. Ja kibernoziedzniekam ir augstākā tehniskā izglītība, zināšanas un prasmes, kuras iespējams realizēt kibernoziegumā, tad nodarījuma sociālā bīstamība ne tikai paaugstinās, bet pieaug progresīvi. Šajā gadījumā kibernoziedznieka galvenais elements ir intelekts. Jāpiekrīt atziņai, ka personai ar kriminālajām prasmēm, kuru pamatā ir iegūtās zināšanas, prasmes un iemaņas, realizējot kriminālu uzvedību, gan ikdienas situācijās, gan arī izmainītās situācijās, tiek nodarīts lielāks kaitējums [39, *95*];
4) sociālais raksturojums – demogrāfiskās pazīmes, sociāli ekonomiskais statuss, sociāli psiholoģiskās un tikumiski morālās īpašības. Pamata elementi ir dzimums, vecums, nacionalitāte, sociāli ekonomiskais statuss, piemēram, tipiska krāpnieka raksturojums ir šāds: vidēja vecuma vīrietis ar augstāko izglītību un būtisku darba pieredzi savā uzņēmumā (gandrīz pusei bijusi sešu vai vairāku gadu pieredze, gandrīz trešdaļai – no trīs līdz piecu gadu pieredze). Pēc Tiesu informācijas sistēmas (TIS) datiem no 2007. līdz 2017. gadam par datorkrāpšanu notiesātas 72 personas (no tām 16 sievietes, ar iepriekšējo sodāmību – 23 personas, 32 notiesātās personas nodarījumu izdarījušas grupā, pēc vecuma grupām: 18–24 gadi – 29 personas, 25–29 gadi – 18, 30–49 gadi – 19, 50 un vairāk gadi – sešas personas) [38]);
5) motivācijas raksturojums – pētījumos apliecināts, ka cilvēka uzvedību vada vairāki motīvi – dažādi iekšējie un ārējie veicinošie apstākļi [23, *151*]. Motīvs ir darbības vadošā un veicinošā funkcija (iekšējs psihiskais mudinājums), kas, veidojot darbības priekšmetu, virza cilvēka aktivitāti. Atsevišķs motīvs vai motīvu kopa veido darbības motivāciju. Noteiktu motivāciju var veicināt dažādi darbības veidi un noteiktu darbības veidu var veicināt dažādi motīvi [41, *268*]. Profesors Uldis Skrastiņš norāda, ka motīvs ir cilvēka psihiskās darbības iekšējs pamudinājums, dziņa, tieksme, kas virza cilvēka gribu uz noziedzīga nodarījuma izdarīšanu. Mērķis (nolūks) ir vēlamais rezultāts, ko cilvēks, kas izdara noziedzīgu nodarījumu, vēlas sasniegt. Tieši vēlēšanās ir tas apstāklis, kas liecina, ka motīvs un mērķis ir vienīgi tādos nodarījumos, kurus izdara ar tiešu nodomu [18, *32*]. Noziedznieka motivācija ir cilvēka aktivitātes ievirzes sistēma, kas pamudina cilvēku rīkoties. Motivācija rosina uzvedību, vada un organizē to, dod tai personisku jēgu un nozīmību [44, *200*]. Attiecībā uz motīvu darbības stimuls pilda veicinoša apstākļa funkciju – ietekmē motivācijas vispārējo raksturu, stiprumu un stabilitāti. Stimuli pārveidojas motivācijā un pilda darbības tieša virzītājspēka funkciju.

Par atsevišķa kibernozieguma faktoru var uzskatīt cilvēka uzvedības kriminogēno motivāciju, kas izraisījusi noteiktas sociāli nelabvēlīgas sekas. Savukārt kriminogēna motivācija ir pamats noziedznieka vērtīborientācijas ievirzei, veidojot šādu sistēmu: **vērtīborientācijas ievirze → kriminogēna motivācija → kibernoziegums**. Tādējādi "ļoti svarīgi ir saprast individuālo kontekstu: cilvēka dzīves mērķi, kas nosaka jebkuras viņa rīcības un visu viņa tieksmju un nodomu virzienu. Dzīves mērķa izpratne sniedz iespēju uzzināt apslēpto jēgu, kas ir dažādu atsevišķu darbību pamatā, jo tā tās tiek aplūkotas, kā vienota veseluma daļas" [3, *67*]. Pietiekami lielai daļai noziedznieku piemīt spēcīgas destruktīvas, antisociālas un antikulturālas tendences. Kibernoziedzības straujā attīstība izmaina kibernoziedznieka motivāciju. Piemēram, ja kibernoziedzības pirmsākumos galvenais motīvs bija pašapliecināšanās vai apkārtējo cieņas iegūšana, tad šobrīd galvenais motīvs ir mantkārība.

Kriminoloģijas ietvaros var nodalīt vairākus kibernozieguma motīvus.

Mantkārības motīvs (nauda, finanšu līdzekļi). Pēc *Kaspersky Lab* datiem, interneta lietotāji uzbrukumā vidēji zaudē 476 ASV dolārus, un desmitdaļa aptaujāto sacīja, ka viņu zaudējumi pārsniedz 5000 ASV dolāru [7]. Pēc Lielbritānijā veiktā pētījuma datiem 67 % hakeru atzina, ka nauda ir galvenais noziedzīgas rīcības stimuls. Aprēķināts, ka viens kibernoziedznieks vidēji gadā nelikumīgi iegūst vairāk nekā 20 000 mārciņas, vidēji 8600 mārciņas katrā uzbrukumā [35].

Emocionālais motīvs. Bieži kibernoziegumu pamatā ir emocijas – dusmas, niknums, naids, atriebība, mīlestība vai izmisums, bezcerība. Krāpšanas motivācijas spektrs ir plašs – mantkārība, varas izpausme, atriebība, piedzīvojumu kāre, vēlme nobaudīt "aizliegto augli", gūt gandarījumu, pašapliecināties, iegūt cieņu, nodarīt zaudējumus, tā var būt arī neapmierināta darbinieka atriebība, pieslēdzoties darba devēja datorsistēmai.

Pašapliecināšanās vai pašcieņas motīvs. Jāņem vērā, ka kibernoziedznieka kā cilvēka aktivitāti nosaka viņa sadarbība ar apkārtējo vidi. Šis process notiek divos pamatveidos: pašīstenošanās (pašapliecināšanās) vajadzība un pašcieņas vajadzība. Kibernoziedzieka vajadzība pašīstenoties ir savu spēju, zināšanu, kā arī sava nozīmīguma un vajadzību apliecinājums, piemēram, vēlme gūt panākumus. Savukārt vajadzība pēc pašcieņas – tieksme iemantot citu (apkārtējo) personu atzinību, vērtējumu un atsauksmes. Tātad šādi izpaužas cenšanās gūt panākumus, atzinību, uzslavas, kas stiprina viņa pašcieņu.

Seksuālie impulsi un vēlmes. Seksuālā motivācija vai dzimumtieksme (libido) attīstās visu indivīda dzīves laiku.

Kibernoziegumu salīdzināmās izpētes [6, *150*] rezultāti parāda, ka:

1) ar bērnu pornogrāfijas materiāliem saistīto nodarījumu izdarītājs ir vecumā no 15 līdz 73 gadiem (vidējais vecums – 49 gadi);
2) 60 % noziedznieku ne tikai uzglabāja, bet arī izplatīja šos materiālus;
3) piektdaļa no šiem noziedzniekiem nestrādāja (bija pensionārs, bezdarbnieks vai saņēma pabalstu), pārējie strādāja vai studēja;
4) 42 % noziedznieku dzīvoja kopā ar partneri un / vai bērnu;

5) 4 % no vis iem noziedzniekiem bija garīgās veselības problēmas;
6) visi pētījumā apzinātie noziedznieki savas darbības rūpīgi slēpa no tuviniekiem;
7) reģistrētais noziedzīgo nodarījumu ilgums – no sešiem mēnešiem līdz 30 gadiem.

Politiskie un reliģiskie motīvi. Visbiežāk politiski motivēta kaitniecības forma ir haktīvisms (angļu val. *hocktivism*) – kiberuzbrukumi politiska vai sociāla protesta izpausmes formā. Haktīvisti īpaši aktīvi kļūst politisku notikumu apstākļos.

"Joka pēc" (angļu val. *just for fun*) **motīvs** – parasti ir raksturīgs pusaudžiem vai bērniem [36]. Aptaujas "Mobilo telefonu un interneta izmantošanas paradumi bērnu un jauniešu vidū" apkopotie dati parāda, ka tikai 4 % vecāku zina, ka viņu bērns kādu emocionāli ir pazemojis, aizskāris, izmantojot mobilo tālruni, un 3 % zina, ka bērns kādam ir draudējis, izmantojot mobilo tālruni. Savukārt 12 % bērnu atzina, ka ir veikuši minētās darbības. Vecāki par savu bērnu šādu rīcību nezina: 23 % vecāku nezina par emocionālu pazemošanu, 18 % – par draudēšanu, izmantojot mobilo tālruni [2].

Kibernoziedznieki neveido homogēnu noziedznieku grupu. Kibernoziedznieks var būt gan sieviete, gan vīrietis, jebkura vecuma, ekonomiskā stāvokļa, rases, reliģijas vai nacionālās piederības cilvēks. Atšķirībā no lielākās sabiedrības daļas kibernoziedznieki nevar pienācīgi apgūt pieņemtās normas, jo viņu socializācijas procesā notikušas novirzes, vai viņi pieņem kriminālās vides "īpašās formas". To ietekmē dažādi faktori: iedzimtība, izglītība, kultūra, dzīvesveids un sociāli ekonomiskie apstākļi.

Apkopojot speciālās literatūras un pētījumu rezultātus, var nodalīt šādus kibernoziedznieku veidus:

1) hakeris (*hacker*) jeb urķis, datorkramplauzis – specializējas sistēmu uzlaušanā. Hakerus iedala baltajos jeb "labajos" hakeros (*white hat*) – atklāj sistēmu ievainojamību, paziņo īpašniekam; pelēkajos hakeros (*grey hat*) – atklāj ievainojamību (kļūdu) un paziņo, ka par noteiktu samaksu atklās ievainojamību sistēmā; melnajos hakeros (*black hat*) – atklāj ievainojamību un nozog vērtības; politiski motivētajos hakeros (*hacktivists*);
2) kiberterorists – izmanto kibertelpu, lai radītu nedrošību. Kibernoziedznieki individuālu iemeslu dēļ cīnās pret valsts iestādēm un valdībām, izmantojot visus pieejamos līdzekļus, lai sasniegtu mērķi [25];
3) kiberspiegs – veic gan rūpniecisko, gan citādu spiegošanu, piemēram, iekļūst valsts informācijas sistēmās, kur tiek glabāta klasificēta informācija, šī tiek saukta par kiberspiegošanu [15, *442*];
4) programmētāji (rada ļaundabīgus kodus), datorvīrusu izplatītāji;
5) sistēmas saimnieki un nodrošinātāji – nelikumīga satura vietņu un serveru saimnieki un nodrošinātāji;
6) kasieris (*cashier*) jeb banku, kredītkaršu kontu sagādnieks;
7) līderis (reālajai kriminālajai pasaulei pietuvinātie projektu, uzņēmumu vadītāji);
8) "naudas mūlis" (*money mule*) – persona, ar kuras starpniecību tiek veikti svešas naudas pārskaitījumi, tos legalizējot;

9) kiberkrāpnieks (*fraudster*) – izmanto krāpnieciskus paņēmienus, dažādas metodes;
10) personas identitātes zaglis;
11) virtuālais seksuālais noziedznieks;
12) kibervajātājs – kibernoziedznieks, kurš veic kiberuzmākšanos;
13) autortiesību un blakustiesību pārkāpējs;
14) kultveidīgās nāves grupas organizētājs, atbalstītājs un tīkla uzturētājs.

Savukārt pēc sociālās bīstamības pakāpes var nodalīt šādas kibernoziedznieku kategorijas:

1) īpaši bīstamie (organizētās noziedzības dalībnieki, kiberteroristi u. c.);
2) bīstamie (noziedzīgus nodarījumus pret personu, īpašumu veikušie u. c.);
3) nelielas bīstamības kibernoziedznieki.

Kriminoloģijā noziedzības pamatus parasti dēvē par noziedzības faktoriem jeb determinantiem [20, *198*; 21].

Pastāv divi cēlonības īstenošanas pamatlīmeņi:

1) atsevišķais cēlonis izraisa atsevišķas sekas, un tas balstās uz noteiktas situācijas īpatnībām, piemēram, apzinot noziedzīga nodarījuma cēloņus, jāņem vērā visu noteikto apstākļu dažādība un savdabība;
2) vispārīgais cēlonis izraisa vispārīgas sekas, un vispārīgo cēloņu līmenī var izdalīt apakšlīmeņus – sevišķo un universālo.

Kriminoloģijas literatūrā izšķir trīs noziedzības faktoru jeb determinantu līmeņus:

1) noziedzības vispārīgie faktori (universālais cēlonis). Noziedzības universālā cēloņa problēmas aspektā interesantu viedokli ir izteicis *Dr. habil. phil*., Latvijas Zinātņu akadēmijas korespondētājloceklis Ivans Vedins: "Droši vien pareizi būtu meklēt noziedzības vispārīgo cēloni ārpus tiesiskās realitātes sfēras. Tiesības ir tikai viena no sociālās realitātes apakšsistēmām, kas balstās uz sabiedrības tikumisko realitāti. Līdz ar to problēmas būtības universāla cēloņa līmenī izskaidrojamas vienkārši – noziedzības vispārīgais cēlonis ir cilvēka un cilvēces nepilnība" [41, *278*];
2) atsevišķu noziedzīgu nodarījumu grupu faktori (sevišķie cēloņi);
3) konkrēta noziedzīga nodarījuma faktors (atsevišķais cēlonis).

Kibernoziedzība ir komplicēta sociāla parādība ar tai raksturīgām determinantu īpatnībām, kas atklājas atsevišķo cēloņu līmenī. Konkrēta noziedzīga nodarījuma cēlonis atklājams noziedznieka personībā, un tas var norādīt, ka visu nosaka cilvēka brīva izvēle. Taču personība ir visai sarežģīta sistēma ar vairākām apakšsistēmām, tāpēc noziedzīga nodarījuma izdarīšanu var determinēt vajadzību sistēma, temperamenta un rakstura īpatnības, vērtīborientāciju pamatievirze un citi apstākļi [41, *279*].

Teorijas par kiberkrimināla uzvedību

Krimināls uzvedības izpēte vienmēr bijusi vairāku zinātņu (kriminoloģijas, psiholoģijas, medicīnas, socioloģijas u. c.) intereses objekts. Kriminoloģijas zinātne ir daudzveidīga un sistēmiski sakārtota, apvienojot dažādas teorētiskās nostādnes. Kriminoloģija kā multidisciplināra zinātne izmanto citu zinātņu zināšanas un pētnieciskās atziņas. Sociālās, kultūras un ētiskās normas nosaka uzvedības parametrus, bet teorijas palīdz izskaidrot novirzi no šiem parametriem. Teorētiskās atziņas var palīdzēt izprast indivīda antisociālo un kriminālā rakstura uzvedības motivāciju [9, *211*].

Kiberkrimināls uzvedību ietekmē mijiedarbība starp vairākiem faktoriem. Šāda uzvedība ir savstarpējās iedarbības rezultāts, kas aptver individuālos, sociālos, vides faktorus un starp indivīdu un sabiedrību pastāvošos konfliktus. Lai arī vairums kriminoloģijas teoriju tika izstrādātas, pētot fiziskajā pasaulē izdarītos noziedzīgos nodarījumus, tomēr arī kiberkriminalitātes skaidrošanai var izmantot analoģiskas teorijas, jo tās pamatu veido identiski faktori. Tāpat tās skaidrošanai var arī izstrādāt jaunas teorijas. Teorijas par noziedzīgu rīcību var skaidrot dažādos līmeņos: sabiedrības vai vietējā līmenī, sociālajā vai makrolīmenī (koncentrējas uz to izturēšanās modeļu izpēti, kas palīdz izprast sabiedrības būtību), individuālajā jeb mikrolīmenī (pēta cilvēka ikdienas dzīves norises, socializācijas ietekmi, interakciju un mijiedarbību, indivīda izturēšanos, motīvus u. c.) [26, *34*].

Indijas kriminologs profesors Karupanans Džaišankars (*Karuppannan Jaishankar*), lai izskaidrotu noziedzīgu nodarījumu cēloņsakarību kibertelpā, izstrādāja **telpu pārnešanas teoriju** (angļu val. *space transition theory*). Šī teorija izskaidro personas pretiesiskās uzvedības pārnešanu no fiziskās telpas uz kibertelpu. Telpas pārnešana ietver personas kustību no vienas telpas uz otru, tas ir, no fiziskās telpas uz kibertelpu un otrādi. Telpas pārnešanas teorija pierāda, ka indivīds uzvedas citādāk, kad viņš pārvietojas no vienas telpas uz citu.

Telpas pārnešanas teorijas ietvaros tiek pieņemts, ka:

1) personām, kuras apspiež krimināla rakstura uzvedību fiziskajā telpā, ir tieksme izdarīt noziedzīgus nodarījumus kibertelpā, kuru viņas fiziskajā telpā neizdarītu sociālā statusa dēļ;
2) personības fleksibilitāte[2], norobežošanās anonimitāte un atturēšanas faktora trūkums kibervidē sniedz noziedzniekam iespēju izdarīt noziedzīgu nodarījumu;
3) noziedznieks noziedzīgu uzvedību no kibertelpas var pārnest uz fizisko telpu un no fiziskās telpas var eksportēt arī uz kibertelpu;
4) noziedznieka intermitējoša (periodiska vai atkārtota) darbība kibertelpā un kibervides dinamiskums telpā un laikā sniedz iespēju noziedzniekam nozust:
   a) kibertelpā pastāv iespēja apvienoties svešiniekiem, lai izdarītu noziedzīgu nodarījumu fiziskajā pasaulē;
   b) apvienojot partnerus fiziskajā telpā, iespējams paveikt noziegumu kibertelpā;

[2] Fleksibilitāte (angļu val. *flexibility*) – elastīgums, pielāgošanās spēja, mainīgums.

5) noziedzīgus nodarījumus kibertelpā noslēgtas sabiedrības locekļi izdara biežāk nekā atvērtas sabiedrības locekļi;
6) normu un vērtību konflikts fiziskajā vidē ar normām un vērtībām kibervidē var radīt noziedzīgu nodarījumu kibervidē [16, *7–10*].

Ikdienas aktivitāšu teorijas (angļu val. *routine activities theory*) atziņa: tiek apgalvots, ka nodarījums notiek tad, kad iespējamais noziedznieks un piemērotais mērķis satiekas laikā un vietā un kad mērķis netiek pietiekami aizsargāts. Līdz ar to tiek apstiprināta iespējamā noziedznieka faktiskā pastāvēšana, jo cilvēka alkatība un savtība ir pietiekams skaidrojums noziedzīgas rīcības motivācijai [17, *27*]. Noziedzīgs nodarījums tiek izdarīts, ja eksistē šādi apstākļi: piemērots mērķis, "aizskartā" indivīda ievainojamības un neaizsargātības stāvoklis, noziedznieka motivācija. Attiecinot minēto uz kibernoziegumiem, Garijs Gordona (*Gary R. Gordon*), Česters Hosmers (*Chester D. Hosmer*), Kristīne Siedsma (*Christine Siedsma*) un Dons Rebovičs (*Don Rebovich*) apgalvo, ka kibernoziegums ir noziedznieka darbības rezultāts, lai sasniegtu noziedzīgu mērķi. Noziedznieks pamana iespēju patvaļīgi un nelikumīgi piekļūt datorsistēmai vai datoru izmanto kā noziedzīga nodarījuma priekšmetu, turklāt šajā gadījumā aizskartajam nav nepieciešamo līdzekļu vai zināšanu, lai novērstu vai atklātu noziedzīgo rīcību [13]. Šajā kontekstā jānorāda, ka viktimizācijas pētījumi liecina par dzīvesveida faktoru korelēšanu ar viktimizāciju un sociālās aktivitātes ietekmi uz viktimizāciju kibervidē. Tiek norādīts uz četriem kibervides riskiem (angļu val. *the "4C`s" of child risk*), kurus sastop bērni, – kibernozieguma (*cybercrime*), saskarsmes (*contact*), uzvedības (*conduct*) un satura (*content*) risku [6]. Drošību kibervidē nepieciešams pastāvīgi uzmanīt, īpaši to attiecinot uz bērniem. Tātad jāvērš plašumā iedzīvotāju informēšanas kampaņas un jāveicina kiberdrošības kultūra iedzīvotāju vidū.

Klasiskās kriminoloģijas skolas pārstāvji noziedzīgu nodarījumu aplūko kā pavisam racionālu kategoriju, noziedznieka garīgajam stāvoklim vai sociālās vides ietekmei nepiešķirot nozīmi. Noziedzīgs nodarījums (arī kibernoziegums) ir cilvēka izvēle, un pastāv tikai divi nosacījumi: rīkoties saskaņā ar tiesisko regulējumu vai riskēt, pārkāpjot likumu, un ar šādu uzvedību sasniegt kādu personisku labumu vai iegūt materiālu labumu, peļņu.

Racionālās izvēles teorijas (angļu val. *rational choice theories*) ietvaros tiek uzskatīts, ka noziedznieks vienmēr tiecas gūt labumu no noziedzīgiem nodarījumiem. Pieņemts uzskatīt, ka noziedznieki, izdarot noziedzīgus nodarījumus, meklē ieguvumus, kas viņam ir pietiekami lietderīgi un pamatoti, piemēram, datorkrāpšanas gadījumā meklē materiālu labumu. Mantiskās intereses ietver mantu, tiesības uz mantu vai citu mantisku labumu, piemēram, dažādu maksas pakalpojumu apmaksu [19, *48*].

Oportūnistiskās uzvedības teorijas ietvaros kibernoziegumu var skatīt kā oportūnistiskās uzvedības paveidu, centienus sasniegt personīgās intereses ar viltību. Šāds uzvedības tips iekļauj tādas maldināšanas formas kā nepilnīgas vai sagrozītas informācijas iesniegšanu, īpašus centienus maldināt, izkropļot, padarīt neskaidru, citādi sajaukt melojot, zogot un krāpjot.

Iespēju teorijas (angļu val. *crime opportunity theories*) ietvaros tiek apgalvots, ka noziedznieks veic izvēli un izvēlas mērķi, kas piedāvā lielu atdevi ar minimālu piepūli un risku. Piemērots mērķis – cilvēks, objekts, vieta. Noziedznieks novērtē iegūstamo vērtību, darbību inerci (aktivitāšu daudzumu) un pārskatāmību, kā arī piekļuves iespējas vieglumu (*value*, *inertia*, *visibility*, *access*). Kibernoziedznieks var izveidot sarežģītus uzbrukumus ar mazāku ieguldījumu, piemēram, izmantot bezmaksas vai tiešsaistes ļaunprogrammatūras [34].

Sociālās kontroles teorija (angļu val. *social control theory*) pieļauj, ka cilvēki var saskatīt noziedzības priekšrocības un spēj izdomāt, un realizēt dažādas noziedzīgas darbības, nevilcinoties jeb momentā – bez īpaša stimula vai iepriekšējas apmācības. Tādējādi tiek pieļauts, ka rezultātā primārais ir potenciālais ieguvums no noziedzīga nodarījuma.

Atturēšanas teorijā (angļu val. *deterrence theory*) soda piedraudējums tiek izmantots, lai indivīdu atturētu no likumpārkāpuma izdarīšanas.

Atturēšanas teorijā ir divi galvenie pieņēmumi:

1) konkrēti sodi, kas piemēroti pārkāpējam, to attur no noziedzīga nodarījuma izdarīšanas vai novērš jaunu nodarījumu izdarīšanu;
2) bailes no soda neļaus citiem indivīdiem izdarīt nodarījumus [45].

Protams, sabiedrības lielākā daļa ievēro likumus. Taču jārēķinās, ka ir cilvēki, kuriem piemīt spēcīgas destruktīvas, antisociālas un nekulturālas tendences, kas nosaka šo personu uzvedību. Vislielāko problēmu rada tieši indivīda atturēšana no kibernoziegguma izdarīšanas. Soda efektivitātes aspektā var minēt Vācijas tiesību speciālista Paula Johana Anselma fon Feierbaha (*Paul Johann Anselm Ritter von Feuerbach*) atziņas: vēlme izdarīt noziedzīgu nodarījumu var beigties tikai tad, ja sekas par nodarījumu jeb sods būs lielāks nekā neapmierinātā vajadzība, kas ir noziedzīga nodarījuma pamatā. Sodus viņš iedala divās grupās: pirmkārt, paredzētajam jeb draudošajam sodam ir preventīva nozīme, lai atturētu indivīdus no nodarījuma izdarīšanas iespējamās soda realizācijas nākotnē dēļ; otrkārt, realizējamais sods – soda nozīme saistīta ar to, ka sods tiks realizēts, un vainīgā persona tiks sodīta atbilstoši krimināltiesiskajām normām [42, *73*]. Lai sods pildītu atturēšanas funkciju, soda piemērošanai jābūt ātrai, noteiktai un stingrai (iespējami ātri pēc nodarījuma izdarīšanas, atbilstošs soda veids un termiņš).

Sociālās iemācīšanas teorija (angļu val. *social learning theory*) izskaidro cilvēka rīcību mijiedarbībā ar izziņas procesa, uzvedības un vides ietekmi. Psihologs Alberts Bandura norāda, ka noziedzīga uzvedība ir iemācīta, tā nav iedzimta vai predisponēta, vienīgi iemācīta. Cilvēki mācās, vērojot citus – uzvedību, attieksmi, izturēšanos un rezultātu. Šī informācija kalpo kā ceļvedis darbībai nākotnē. Iemācīšana notiek grupā: ģimenē, darbā un draugu vidē [5, *40–41*]. Savukārt medijiem ir maza loma. Šis process aptver tehnoloģijas, motīvus, attieksmes un internalizāciju (procesu, kurā iekšējie iespaidi un uztvērumi, kas saistīti ar kādu cilvēku, kļūst par subjektīvu tēlu).

Amsterdamas Universitātes pētnieks Bovens Paulle (*Bowen Paulle*) pauž viedokli, ka "visiem bērniem ir nepieciešama veselīga vide, kur attīstīties – vienalga, vai bērni ir vietējie, migranti, vairākums, minoritāte, bagāti vai nabadzīgi. Jebkurš bērns, kuram liegta strukturāla pieeja drošai, paredzamai, siltai un disciplinētai videi, izaugs emocionāli nestabils. Ja atstāsim neaizsargātākus jauniešus skolās, kuras raksturo galvenokārt augsts nabadzības līmenis, mums ir milzīgas izredzes, ka šie jaunieši nekad neattīstīsies par informētiem un kritiskiem (un līdzjūtīgiem un pietiekoši emocionāli stabiliem) pieaugušajiem, kādi vajadzīgi demokrātijai [12].

Lomu konflikts – ar divām vai vairāk lomām saistītu cerību sadursme, kurā atbilstība vienas lomas prasībām apgrūtina citu lomu izvirzīto prasību pienācīgu izpildi. No katra cilvēka statusa sabiedrība sagaida noteiktu darbību, piemēram, skolotāji māca, skolēni mācās, vecāki rūpējas un audzina, bērni klausa un ciena. Tiek nodalīts iekšējais lomu konflikts un starplomu konflikts. Skolas–ģimenes un darba–ģimenes konfliktiem ir nopietnas sekas, kas ietekmē gan indivīda labsajūtu, gan vides kvalitāti. Tādējādi tie nerada pietiekamu pozitīvu mijiedarbību (skola, darba vide, ģimene negūst labumu). Bieži lomu konflikti ir saistīti ar adikciju[3] vai personīgajiem iekšējiem konfliktiem, kas nosaka iekšējo psiholoģisko diskomfortu. Pēc Krievijas Behtereva Zinātniski pētnieciskā institūta datiem 85 % gadījumu tiem ir sociāls pamats, bet 15 % šādu konfliktu ir seksuāls pamats, [43, *125*].

Kibernoziedzības izskaidrošanai var lietot arī kompensācijas jeb aizvietošanas teoriju un izplatīšanās teoriju.

Kompensācijas jeb aizvietošanas teorija – reālās dzīves vides (ģimenes, skolas, darba vides) pozitīvās ietekmes un mijiedarbības neesamība. Indivīds, nesaņemot atgriezenisko saikni (indivīds un sabiedrība, indivīds un ģimene, indivīds un skola, indivīds un darbs), trūkstošo posmu (ieinteresētību, aprūpi, atbalstu) aizstāj ar kibervides iespējām, meklējot sev radnieciskas interešu grupas, kurās sociālajai funkcionēšanai (vēlmēm, vērtībām un mērķiem) ir labvēlīgi un personas vajadzībām atbilstoši apstākļi.

Raksturojot interneta kā sociālo attiecību "aizvietotāja" izmantošanas un interaktīvās komunikācijas popularitātes iemeslus, tiek izdalīti šādi cēloņi:

1) nepietiekami piesātināta saskarsme reālajos kontaktos;
2) iespējas realizēt personiskās īpašības, tēlot lomas, pārdzīvot emocijas, kuras nav reālas vai iespējamas ikdienas dzīvē;
3) neapmierinātība ar reālo sociālo identitāti un tieksme to pārveidot [27, *265*].

Īpaši tas asi izpaužas ekstrēmās kiberdarbībās – teroristiskā rīcībā, suicidālās spēlēs, suicidālu darbību organizēšanā un realizācijā.

---

[3] Adikcija (angļu val. *addiction*) – atkarība. Ķīmisku vielu, piemēram, alkohola, kokaīna un nikotīna lietošana vai darbību, piemēram, azartspēļu, seksa, iepirkšanās u. tml., veikšana, kas varētu būt patīkamas, bet var kļūt nepārvaramas un traucēt ikdienas pienākumus un rūpes, piemēram, darba attiecības vai veselību.

Izplatīšanas teorija – stress skolā, darbā un / vai ģimenē noved pie frustrācijas[4]. "Frustrācijas–agresijas" teorijas autori pieņem, ka agresija personības uzvedībā vienmēr paredz frustrācijas esamību un otrādi. Manuprāt, darbā, skolā vai ģimenē izraisītas spriedzes dēļ cilvēks nav spējīgs atbrīvoties no pārdzīvojumiem. Būtībā starp cilvēka dzīves vidēm un jomām nav skaidru robežu, piemēram, profesionālās vai mājas stresa izraisītas problēmas tiek reducētas kibervidē.

Secinājumi

Kibernoziedzības apdraudējums ir visaptverošs un globāls, tomēr Latvijā nav pietiekami izzināts kibernoziedzības fenomens:

1) nav pieejami visaptveroši un pilnīgi dati par tā stāvokli, tendencēm un dinamiku;
2) trūkst datu par kibernoziedzniekiem un viņu kriminoloģiskā raksturojuma – nenotiek noziedzības, tai skaitā kibernoziedzības, attīstības tendenču prognozēšana.

Latvijā jāveido prakse sistemātiski veikt kriminoloģiska rakstura pētījumus. Šādas izpētes iespējas jāveicina praktizējošo darbinieku un zinātnieku vidū, kā arī starp augstskolu studentiem.

Cyber Crime as Form of Criminality: Criminological Aspect

Abstract

Nowadays, cybercrime or crime that has been done or led through the Internet has taken a steady place among the multitude of criminal offences committed. Cyberspaces is easily applied to harm the individual, community group or country as a whole. The article provides overview of the criminological characteristics of cyber offender and cyber criminal behavioural interpretive theories.

The results of the research demonstrate that

1) criminologic characterisation of cyber offender profile consists of such key elements as: technical know-how; criminal professionalism; personal traits; social characteristics; motivating factors [4];
2) the specific purpose of criminological theory is to help us understand why individuals commit cybercrime. cyber criminal behaviour can be explained by using various theories of criminal behaviour.

Keywords: criminality, cyberspace, cybercrime, cyber criminal.

[4] Frustrācija (angļu val. *frustration*) – neveiksme, vilšanās. Psihisks stāvoklis, kas var izveidoties, ja cilvēkam ceļā uz nozīmīgu mērķi rodas reāli vai šķietami šķēršļi. Tam raksturīgs nepatīkams iekšējs spriegums, bezizejas sajūta u. tml.

Literatūra

1. Andrews, D. A., Bonta, J. *The Psychology of Criminal Conduct*. New York: Matthew Bender & Company, Inc., 1998, 193–195.
2. Aptauja "Mobilo telefonu un interneta izmantošanas paradumi bērnu un jauniešu vidū". No: *Drošs internets*. 2012. Iegūts no: http://www.drossinternets.lv/upload/materiali/petijumi/mob-tel_interneta_izmantosana_2012.pdf [sk. 26.02.2017.].
3. Ādlers, A. Māksla dzīvot. *Psiholoģija Ģimenei un Skolai*. 2015, 67.
4. Baer, M. Cyberstalking and the internet landscape we have constructed. *Virginia Journal of Law & Technology*. 2010, 15(2).
5. Bandura, A. *Social Learning Theory*. New York: General Learning Press, 1971.
6. *Comprehensive Study on Cybercrime*. New York: United Nations, 2013. Iegūts no: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [sk.12.03.2017.].
7. Consumer Security Risks Survey 2016. Connected but not protected. No: *Kaspersky Lab*. 2016. Iegūts no: https://press.kaspersky.com/files/2016/11/B2C_survey_2016_report_.pdf [sk. 17.04.2017.].
8. Cyber Crime Assessment 2016. No: *National Crime Agency*. 2016. Iegūts no: http://www.national-crimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file [sk. 17.04.2017.].
9. Dobbert, D. L., Mackey, T. X. *Deviance: Theories on behaviors that defy social norm*. California: Praeger, 2015.
10. Dziļuma, D. Pētījums par mobilo ierīču (telefonu un planšetu) lietošanas paradumiem mazu bērnu vidū. No: *Centrs Dardedze*. 2016. Iegūts no: http://www.centrsdardedze.lv/lv/uzzinai/petijumi [sk. 17.04.2017.].
11. Ferri, E. *Criminal Sociology*. Charlottesville, Va.: University of Virginia Library, 1996.
12. Golubeva, M. Pāris vienkāršas patiesības. No: *Providus.lv* [Sabiedriskās politikas portāls]. 2006. Iegūts no: http://www.politika.lv/index.php?id=10152 [sk. 20.03.2017.].
13. Gordon, G. R., Hosmer, C. D., Siedsma, C., Rebovich D. Assessing technology, methods, and information for committing and combating cyber crime. No: *Nacional Criminal Justice Reference Service*. Iegūts no: https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf [sk. 14.03.2017.].
14. Hampson, S. E. *The Construction of Personality: An Introduction*. London: Routledge, 1988, 3.
15. Hoisington, M. Cyberwarfare and the use of force giving rise to the right of self-defense. *Boston College International and Comparative Law Review*. 2009, 32(2).
16. Jaishankar, K. Establishing a theory of cyber crimes. *International Journal of Cyber Criminology*. 2007, 1(2).
17. Klarks, R. V., Eks, Dž. E. Noziedzības analīze 60 soļos. Rīga: Valsts policija, 2011.
18. Krastiņš, U. *Tieša nodoma tvērums krimināltiesībās. Krimināllikuma 9. panta otrās daļas paplašināts komentārs ar teorētiskām nostādnēm*. Rīga: Tiesu nama aģentūra, 2017.
19. Krastiņš, U., Liholaja, V., Hamkova, D. *Krimināllikuma komentāri*. Trešā daļa, XVIII–XXV nodaļa. Rīga: Tiesu nama aģentūra, 2016.
20. *Kriminologiia*. Pod red. V. D. Malkova. Moskva: Iustucinform, 2006. (Криминология. Под редакцией В. Д. Малкова. Москва: Юстицинформ, 2006.)
21. *Kriminologiia. Uchebnik dlia vuzov*. Pod obshchei redakciei professora A. I. Dolgovoi. Moskva: Izdatelstvo NORMA, 2001. (*Криминология. Учебник для вузов*. Под общей редакцией профессора А. И. Долговой. Москва: Издательство НОРМА, 2001.).
22. *Kriminoloģija*. Mācību grāmata. Zin. red. K. Ķipēna, A. Vilks. Rīga: Nordik, 2004.

23. Ksheti, N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. New York: Springer, 2010.
24. Latvijas kiberdrošības stratēģija 2014.–2018. gadam (apstiprināta ar Ministru kabineta 2014. gada 21. janvāra rīkojumu Nr. 40 "Par pamatnostādnēm "Latvijas kiberdrošības stratēģija 2014.–2018. gadam""). *Latvijas Vēstnesis*. 16(5075), 23.01.2014.
25. Lemos, R. What are the real risk of cyberterrorism? August 26, 2002. No: *ZDNet*. Iegūts no: http://www.zdnet.com/article/what-are-the-real-risks-of-cyberterrorism/ [sk. 18.04.2017.].
26. Lilly, R. J., Cullen, F. T., Ball, R. A. *Criminological Theory. Context and Consequences*. Sage Publication, Inc., 2015.
27. Mihailovs, I. J. Interneta ietekme uz sabiedrības tiesisko kultūru. *Rīgas Stradiņa universitātes Zinātniskie raksti, 2009. gada sociālo zinātņu pētnieciskā darba publikācijas*. Rīga: RSU, 2010.
28. Nozare ciparos, 2016. No: *Latvijas Interneta asociācija*. Iegūts no: www.lia.lv [sk. 24.04.2017.].
29. Omārova, S. *Cilvēks runā ar cilvēku*. Rīga: Kamene, 2002.
30. Organised Crime Task Force. Annual Report & Threat Assessment, 2007. *United Kingdom, National Crime Agency*. 2008. No: *Organised Crime Task Force*. Iegūts no: www.soca.gov.uk. [sk. 17.04.2017.].
31. Organised Crime Task a Force. Annual Report & Threat Assessment, 2015. No: *Organised Crime Task Force*. Iegūts no: http://www.octf.gov.uk/OCTF/media/OCTF/documents/publications/OCTF-REPORT-2015-1.pdf?ext=.pdf [sk. 17.04.2017.].
32. Polderman, T. J., Benyamin, B., de Leeuw, C. A., Sullivan, P. F., van Bochoven, A., Visscher, P. M., Posthuma, D. Meta-analysis of the heritability of human traits based on fifty years of twin studies. *Nature Genetics.* 2015, 47(7)
33. Pusaudžu nāves spēle pārņem Latviju. *Kas Jauns*. 2017, 9(209).
34. Recupero, P. R. Forensic evaluation of problematic internet use. *Journal of the American Academy of Psychiatry Law.* 2008, 36.
35. Simkin, S., Ponemon, L. *Flipping the Economics of Attacks.* No: *Ponemon Institute*. 2016. Iegūts no: http://www.polyscope.ch/site/assets/files/42688/06_16_53.pdf [sk. 26.03.2017.].
36. Shinder, D. Profiling and categorizing cybercriminals. No: *TechRepublic*. 2010. Iegūts no: http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/ [sk. 15.03.2017.].
37. Strika, E. *Tiesu psihiatriskajā vai kompleksajā tiesu psiholoģiskajā un psihiatriskajā ekspertīzē nonākušo likumpārkāpēju personības raksturojums*. Promocijas darbs. Rīga: Latvijas Universitāte, 2009.
38. Tiesu informācijas sistēmas TIS statistika. Krimināllietu statistikas pārskati. No: *Tiesu informācijas sistēma*. Iegūts no: https://tis.ta.gov.lv/tisreal?Form=TIS_STAT_O&topmenuid=0&groupid=tisstat [sk. 19.02.2017.].
39. Tulegenov, V. V. Kiberprestupnost kak forma virazheniia kriminalnogo professionalizma. *Kriminologiia: vchera, segodnia, zavtra*. 2014, 2(33) (Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма. *Криминология: вчера, сегодня, завтра*, № 2 (33), 2014.).
40. Vasiu, L., Warren M. and Mackay, D. Defining fraud: Issues for organizations from an information systems perspective. No*: Association for Information Systems*. 2003. Iegūts no: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1065&context=pacis2003 [23.01.2017.].
41. Vedins, I. *Zinātne un patiesība*. Rīga: Avots, 2008.

42. Vilks, A. *Krimināltiesiskā politika: diskursa analīze un attīstības perspektīvas*. Rīga: Drukātava, 2013.
43. Vishniakova, N. F. Kreativnaia psihologia: psihologia tvorcheskogo obucheniia. Moskva: Rotaprint NIO, 1995 (Вишнякова, Н. Ф. Креативная психология: психология творческого обучения. Москва: Ротапринт НИО,1995.)
44. Vorobjovs, A. *Sociālā psiholoģija. Teorētiskie pamati*. Rīga: SIA "Jumi", 2002.
45. Wright, V. Deterrence in criminal justice evaluating certainty *vs*. severity of punishment. No: *The sentencing project*. 2010. Iegūts no: http://www.sentencingproject.org/wp-content/uploads/2016/01/Deterrence-in-Criminal-Justice.pdf [sk. 17.04.2017.].