KIBERNOZIEGUMU RISKS PĀRVALDES INSTITŪCIJĀS

CYBERCRIME RISK IN THE INSTITUTIONS OF GOVERNMENT

Alise Gubene, Mg.sc.soc., alisegubene@inbox.lv
Laima Barisa, **Mg.sc.soc.,** Laima.Barisa@llu.lv

Abstract. The aim of the paper is to describe cybercrime risk in the institutions of government and to clarify views of the representatives of the institutions of government as well as views of the cybercrime experts about them. In the first part of the paper authors have studied the theoretical aspects of the cybercrime, such as: definition problems of the cybercrimes, views of the cybercrimes in the understanding of the concepts of the information security, specific features and types of the cybercrimes and also author has looked into the theories of the deviance. In the second part of the paper authors have gained an insight for the analysis while studying ideas of the risk concept in general ir the context of the cybercrime risk in the institutions of government and also has discussed sociologists Ulrich Beck's theory of the risk society. His theoretical ideas were supplemented with author's examples from cybercrime risk in the institutions of government. In the third part of the paper authors have focused on the governance system history, value in general and also gives an insight of the governance system and institutions, ruled in the Republic of Latvia. The qualitative research carried out by authors forms the research part of the thesis. To achieve the put forward aim of the research work, the author has used partially structured interview method. Hypothesis: the results of the research showed that cybercrime risk in the directed institutions of government was assessed as low, therefore author believes that the existing mechanism of the IT security matches the existing social reality.
Key words: cybercrimes, risk, institutions of government.

Ievads

Mūsdienu sabiedrībā aizvien lielāka ietekme ir dažāda veida tehnoloģijām. Divdesmit pirmo gadsimtu dēvē arī par informācijas laikmetu, taču būtiska nozīme ir tikai tai informācijai, kura tiek iegūta savlaicīgi. Ātrajam un dinamiskajam dzīves tempam ir raksturīga strauja informācijas nomaiņa. Lai informācijas aprite noritētu pēc iespējas ātrāk, tās nodošanas un saņemšanas procesā īpaši svarīgas ir jaunās informāciju tehnoloģijas (turpmāk tekstā IT).

Līdz ar IT attīstību par neatņemamu sociālās realitātes sastāvdaļu ir kļuvis internets. Virtuālā vide un komunikācija organizācijās tiek balstīta, veidojot noteiktas informāciju krātuves – datu bāzes, kas atvieglo darbu organizācijās, tāpat e-pasts ir kļuvis par neatņemamu sastāvdaļu, daudzām organizācijām ir izveidotas mājas lapas.

Internets paver daudz plašākas iespējas, kādas bijušas līdz šim. Ar internetā ievietoto informāciju vienlaicīgi spēj iepazīties dažādu valstu iedzīvotāji. Šai parādībai nav fizisku ierobežojumu kā laiks un telpa, tas ir globāls fenomens, kas vienā brīdī spēj ietekmēt dažādus procesus atšķirīgos kontinentos, kur mīt neskaitāmu kultūru pārstāvji.

Informācija ir šodienas pasaules atslēgas vārds. Kam ir pieeja šim resursam, tiem ir vara – zināma kontrole pār informācijas plūsmu, spēja noteikt, ko ar to darīt, kurus informēt, bet kurus atstāt „informatīvajā badā", nolemjot tos atpalicēju lomai vispārējās konkurences apstākļos.

Kā raksta Maija Kūle: *„Informācijas kontrole ir spēks, kas pieder varas pārstāvjiem, gluži kā kādreiz izrakteņi, zemes īpašumi un dārglietas"* (Kūle 2006:182).

Informācija, kas plūst pa esošā tehnoloģiskā progresa radītajiem komunikāciju kanāliem, ir tikai kaut kā atspoguļojums – faktu, datu, notikumu u.tml., taču šo līdzekli savu mērķu sasniegšanai var izmantot atšķirīgi, respektīvi, IT reversa puse ietver sevī noteiktu risku par to, kādam nolūkam iegūtā informācija tiks izmantota.

Funkcionāli raugoties, sabiedrība ir sastrukturēta sīkākās vienībās, izmantojot gan formālas, gan neformālas saites, tīklus, veidojot apvienības un dažāda tipa organizācijas. Respektīvi, organizāciju veidošana ir līdzeklis, lai nodrošinātu noteiktu kārtību, kādā pastāv un mijiedarbojas sabiedrības locekļi, turklāt, šādi līdzdarbojoties, kopā tiek maksimizētas iesaistīto indivīdu kvalitātes, radot sinerģijas efektu.

Par primāri svarīgiem tiek uzskatīti tādi formāli veidojumi, kas ir atvasināti no pašas sabiedrības locekļu vidus, veidojot valsts pārvaldes sistēmu, nosakot likumiskās normas, izveidojot noteiktas procedūras, tādējādi radot kopēju sistēmu.

Kibernoziegumu risks ir globāla parādība un autore saprot, ka draudus, ko tie sevī ietver, nav iespējams kaut kādā mērā ierobežot laikā un telpā, taču izpētes fokuss ir vērsts uz valsts pārvaldes institūcijām, jo valsts pārvaldes esamība un pastāvēšana lielā mērā ietekmē sabiedrības pilnvērtīgu funkcionēšanu. Nesankcionētas darbības var radīt neatgriezeniskas sekas, kuras var ietekmēt visus sabiedrībā dzīvojošos indivīdus.

Piemēram, 1998. gadā Latvijas valsts iestādēm tika nodarīti zaudējumi, kas radās CIH „Černobiļa" datorvīrusa rezultātā. Precīzs zaudējuma apmērs netika noteikts, taču pēc šī precedenta tika pieņemts lēmums izstrādāt informācijas sistēmu drošības politiku. (Ķinis 2007:44)

Minētais piemērs liecina, ka sākotnēji netika izprasts pastāvošais risks, ko sevī ietver IT un interneta izmantošana. Jaunas tehnoloģiskas izmaiņas ir radījušas tādas deviantās parādības kā mājas lapu „uzlaušanu", dažādu datorvīrusu programmu izstrādāšanu utt. Uzskaitītās deviantās aktivitātes jau ir klasificējamas kā noziegums, šajā gadījumā ir runa par īpašu noziegumu veidu – kibernoziegumiem.

Likumu un dažādu noteikumu izstrāde un ieviešana determinē konkrētu uzvedības veidu, kas sabiedrībai ir pieņemams, cenšoties izslēgt novirzes no normas, lai integrētu indivīdu un padarītu par daļu no sociāli strukturēta veseluma. Tehniskais progress rada izmaiņas esošajā sociālajā realitātē un ne vien nodrošina jaunas iespējas, bet vienlīdz satur sevī risku, kas ne vienmēr būt redzams, bet gluži pretēji – latents.

Kibernoziegumu risks ir saistīts ar virtuālo vidi un, lai arī valsts pārvaldes institūcijām IT ir kā atbalsta funkcija, tā tiek izmantota pamatfunkciju nodrošināšanai – sociāli strukturēta veseluma pastāvēšanai un kārtības nodrošināšanai. Gadsimtā, kad IT ir līdzeklis, kā to izdarīt un sasniegt, risks, kas varētu rasties apdraudot šīs funkcijas veikšanu, zināmā mērā apdraud arī esošās kārtības pastāvēšanu.

Sabiedrībai attīstoties arvien diferencētāks kļūst sabiedrības pārvaldīšanas mehānisms un ar to arī valsts pārvaldes sistēma kopumā. Ja sistēmu apdraud izmantoto līdzekļu kopums, ar to domājot IT, ir nepieciešams pētīt, kādā veidā tas ietekmē sabiedrības pārvaldes mehānismu. Mēģinājumi izvairīties no riska un deviantām personām, kas draudus varētu īstenot, iespējams liktu veidot līdz šim neaprobētus aizsardzības mehānismus, kas gala rezultātā pat varētu radīt izmaiņas visā sociālajā struktūrā. Līdz ar to ir nepieciešams pētīt kibernoziegumu risku valsts tiešās pārvaldes institūcijās, lai sasniegtu **pētījuma mērķi –** raksturot kibernoziegumu risku tiešās valsts pārvaldes institūcijās un noskaidrot tiešās valsts pārvaldes institūciju pārstāvju, kā arī ekspertu viedokli par tiem, autore **izvirza šādus pētnieciskos jautājumus:**

1) Kāds ir tiešo valsts pārvaldes institūciju pārstāvju un ekspertu viedoklis par to, kāda ir kibernoziegumu riska izpratne tiešajās valsts pārvaldes institūcijās?
2) Kāds ir tiešo valsts pārvaldes institūciju pārstāvju un ekspertu viedoklis par risku (augsts/zems/vidējs) saistībā ar kibernoziegumiem?
3) Kāds ir tiešo valsts pārvaldes institūciju pārstāvju un ekspertu vērtējums par to, vai un kādus preventīvus pasākumus ir iespējams veikt, lai izvairītos no kibernozieguma riska?

Pētījuma priekšmets:
Kibernoziegumu risks tiešās valsts pārvaldes institūcijās.
Pētījuma objekts:
Tiešo valsts pārvaldes institūciju pārstāvji, ar kibernoziegumiem saistīti eksperti.
Iepriekš nospraustā **mērķa sasniegšanai izvirzīti uzdevumi:**

1. Kibernoziegumu specifikas izpēte un analīze;
2. Kibernoziegumu juridiski reglamentējošās bāzes apskats un analīze;
3. Kibernoziegumu izpēte deviances teoriju kontekstā;

4. Kibernoziegumu analīze riska teorijas kontekstā;
5. Pārvaldes institūciju raksturojums (valsts pārvaldes mehānisma nozīme un LR pārvaldes sistēmas apskats);
6. Tiešās valsts pārvaldes institūciju pārstāvju, kā arī ekspertu viedokļu noskaidrošana par kibernoziegumu risku tiešajās valsts pārvaldes institūcijās, izmantojot kvalitatīvās pētniecības metodi – daļēji strukturētās intervijas.

Andris Rubenis, runājot par tehnikas ciešo sasaisti ar kultūru, uzsver: *„Giljotīnu var izmantot augļu sagriešanai, un tas, ka praksē to šim nolūkam nelieto, nozīmē, ka tehniku nevar izraut no sociālā konteksta."* (Rubenis 2004:364).

Citātā minētais apgalvojums it kā liekas pašsaprotams, taču runājot par „tehnoloģiju kaitīgumu", ir svarīgi atcerēties, ka indivīds ir tas, kurš tās rada, lai arī pastāv mijiedarbība starp radīto produktu un indivīdu, kas to ir radījis. Šajā gadījumā par tehnoloģiju radīto ietekmi atbildība ir jāuzņemas indivīdam un sabiedrībai kopumā.

Pētījuma metodoloģija

Savā pētījumā autore informācijas iegūšanai izmanto daļēji strukturētās intervijas, ko nosaka vairāki aspekti. Pirmais aspekts ir tas, ka formālā intervijā jautājumu loks ir jau iepriekš stingri noslēgts, bez būtisku pārmaiņu ieviešanas tajā. Citiem vārdiem sakot, pētījuma saturs un izvirzītais mērķis noteica konkrētās metodes pielietošanu, jo gan kibernoziegumu eksperti, gan valsts pārvaldes institūciju pārstāvji darbojas katrs savā jomā. No tā izriet, ka jautājumiem ir jābūt pietiekami elastīgiem, lai tos spētu piemērot atbilstoši katrai intervijai.

Otrais aspekts ir saistīts ar to, ka pētāmā joma ir attiecināma uz mikrosocioloģiju lai spētu atklāt cilvēka izpratni par sociālo realitāti, tās uzbūves un konstrukcijas principiem, ir nepieciešams veikt daļēji strukturētās intervijas. (Ядов 2003:388)

Daļēji strukturētās intervijas metode ir ērta arī pašam pētniekam, jo pieļauj radošu aktivitāšu veikšanu, piemēram, mainot jautājumu secību, ievirzīt sarunu vajadzīgajā gultnē, ja informants novirzās no tēmas, ir mazrunīgs vai pārlieku detalizēti atbild uz jautājumiem. Intervējamais arī jūtas brīvāk, tādējādi iegūtajai informācijai ir lielāka ticamības pakāpe un analizējamais materiāls tiek iegūts pilnīgāks, objektīvāks. (Silverman 2008:114)

Tika izvēlēta mērķtiecīgā izlase, jo pētījuma dalībniekiem ir jābūt personīgai pieredzei attiecībā uz pētījuma tēmu un viņiem ir jāspēj paust viedokli par to, tādējādi tiek atlasīta visproduktīvākā izlase (Cimdiņa 2011:107).

Autore, balstoties uz Nacionālās drošības likumu, ar kuru kritiskā infrastruktūra tiek aizsargāta, lai tādējādi valstij un sabiedrībai nodrošinātu būtisku pamatfunkciju veikšanu, izvirzīja pazīmes, pēc kurām atlasītas ministrijas un to pakļautībās esošās institūcijas, kas realizē konkrētu pamatfunkciju veikšanu valstī.

Pētījumam izvēlēti tādi ar kibernozieguma jomu saistīti eksperti, kā: informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (CERT.LV) vadītāja Baiba Kaškina, Uldis Ķinis (piedalījies gan starptautiskās konferencēs par kibernoziegumu jautājumiem, gan arī bijis Eiropas Padomes Kibernoziegumu ekspertu komisijā), Aleksandrs Buko (Valsts policijas Kibernoziegumu apkarošanas nodaļas priekšnieks), kā arī Liene Kreicberga (IT drošības konsultante – auditore).

Autore vēlas **noskaidrot šādus aspektus saistībā ar kibernoziegumu risku pārvaldes institūcijās**:

- Kibernoziegumu riska izpratne/uztvere pārvaldes institūcijās;
- Kibernoziegumu riska likumiskais ietvars pārvaldes institūcijās;
- Kibernoziegumu riska īstenošanās pārvaldes institūcijās;
- Kibernoziegumu riska reducēšana pārvaldes institūcijās.

Informanti, kas piedalījās pētījumā, tika iepriekš informēti par intervijas laikā iegūto datu izmantošanu, atbilstoši maģistra darbā uzstādītajiem mērķiem un uzdevumiem, kur šo iegūto informāciju paredzēts apkopot un izmantot konkrētu citātu veidā, atsaucoties uz

intervijās pausto viedokli. Daļēji strukturētās intervijas tikai veiktas, izmantojot diktofonu, par ko intervējamie iepriekš tika brīdināti.

Runājot par anonimitāti, daļa intervēto indivīdu (eksperti) ir publiskas personas, daļa ir valsts pārvaldes institūciju pārstāvji. Sakarā ar pētījuma specifiku – kibernozieguma riska atklāšanu un to pastāvēšanu pārvaldes institūcijās, autore vienojās ar pārvaldes iestāžu pārstāvjiem, ka maģistra darba izstrādes ietvaros nenotiks viņu vārda un uzvārda publiskošana, ne arī konkrētās tiešās valsts pārvaldes institūcijas nosaukuma atklāšana.

Pētījums tika veikts 2013. gadā laika posmā no marta vidus līdz aprīļa vidum. Ar informantiem sākotnēji notika virtuāla saziņa, izmantojot interneta sniegtās iespējas, kas nodrošināja iespēju abām pusēm apmainīties ar kontaktinformāciju, lai varētu vienoties par intervijas norises laiku un vietu. Vienas intervijas ilgums bija no 45 minūtēm līdz 1,5 h. Kopumā tika aptaujātas desmit personas: četri eksperti un seši pārvaldes iestāžu pārstāvji.

Pētījuma rezultāti

Pirmā jautājumu bloka mērķis ir noskaidrot kibernoziegumu riska izpratni/uztveri pārvaldes institūcijās, tāpēc jautājumu loks, kas iekļauti šajā blokā, ir vērsti uz to, lai uzzinātu, kāds ir konkrētās tiešās valsts pārvaldes institūcijas viedoklis par jautājumiem, kas saistīti ar riska kategorizēšanu, mēģinot identificēt un noteikt, kas ir svarīgs un būtisks, lai pēc tam ieviestu noteiktus principus, kā šo informāciju sargāt. Viņiem tiek jautāts, kā viņi to dara, cik lielu uzmanību pievērš jautājumiem, kas saistīti ar risku. Tas tiek skatīts kontekstā gan ar esošo finansējumu un tā nodrošinājumu, gan jautājumiem, kas skar darbinieku izglītošanu un instruēšanu konkrētajā institūcijā, kā arī ar pašu IT darbiniekiem, kas strādā un nodrošina institūcijas funkcionēšanu, vēlmi izglītoties un attīstīt savas prasmes. Informantiem tiek jautāts par nākotnes tendencēm, kas varētu mainīties un attīstīties šajā jomā, kā arī aplūkota riska varbūtības iestāšanās pakāpe privātajā un publiskajā sektora, mēģinot rast atbildi uz jautājumu, cik liels ir potenciālais risks, par kādu var runāt, attiecinot to uz tiešās valsts pārvaldes institūcijām. Pirmā un otrā bloka jautājumi ir veidoti ar mērķi, lai atbildētu uz to, kāda izpratne tiešās valsts pārvaldes institūcijām ir saistībā ar kibernoziegumu potenciālo risku.

Kopumā ņemot, kibernozieguma riska izpratni tiešās valsts pārvaldes institūcijās veido, galvenokārt, pieredze, no tās izriet IT drošības sistēmas izveide, koncepcijas veidošana, risku pārvaldīšana, izmantojot riska matricas, riska analīzes u.c. paņēmienus. Tehnoloģijas attīstās ātrāk par sabiedrības locekļu spēju reaģēt un pielāgoties jaunajiem riskiem, ar kuriem nākas saskarties līdz ar IT parādīšanos, tāpēc joprojām aizsardzības mehānismi tiek bāzēti tradicionālajā izpratnē, veidojot normatīvos aktus un likumus.

Otrā jautājumu bloka mērķis ir vērsts uz normatīvo aktu un likuma bāzi, jo tie ir instrumenti, ar kuriem sabiedrība ir deleģējusi valdībai tiesības to pārvaldīt. Jautājumi ir orientēti uz izpratni par noteiktu principu un noteikumu reālo devumu kontekstā ar viņu ikdienas darbībām, lai tādējādi izvairītos no potenciālā riska. Autore vēlējās noskaidrot, vai viņi orientējās prasībās un pārzina noteikumus, vai izstrādātie normatīvie akti un likumi ir efektīvi un tajos nav nepieciešami uzlabojumi un cik savietojami tie ir ar esošos sociālo realitāti. Likumiskais ietvars tiek skatīts ar mērķi, lai atbildētu uz to, kāda izpratne tiešās valsts pārvaldes institūcijām ir saistībā ar kibernoziegumu potenciālo risku.

Rezumējot autore uzskata, ka pilnīgi pārliecinoši atbildēt uz jautājumu, cik lielā mērā konkrētu prasību ievērošana ir samērojama ar centralizācijas un decentralizācijas tendencēm, konkrētās tiešās valsts pārvaldes iestādes darbības profilu un iekšējās vides tradīcijām, kultūru, lai sekmētu efektīvāko veidu kā adekvāti nodrošināt stabilu un atbilstoši ārējās vides prasībām pielāgoties spējīgu modeli ar pēc iespējas mazākiem finanšu izdevumiem un maksimāliem ieguvumiem, nav iespējams sniegt vienu noteiktu atbildi. Tam ir jābūt atvērtam dialogam, kurā ir iespējams dažādot un savietot atšķirīgus uzskatus, pieejas un metodes, tanī pat laikā atceroties, ka kibernoziegumu risks pārvaldes institūcijās pastāv un lielā mērā no

iestādē strādājošo izpratnes dziļuma ir atkarīga proporcija starp kibernoziegumu riska īstenošanos un tā reducēšanu pārvaldes iestādēs.

Trešā jautājumu bloka mērķis ir noskaidrot atbildi uz otru izvirzīto pētniecisko jautājumu, respektīvi, kāds ir tiešo valsts pārvaldes institūciju pārstāvju un ekspertu viedoklis par risku (augsts/zems/vidējs) saistībā ar kibernoziegumiem. Šajā blokā ir ietverti jautājumi, kas saistīti jau ar reāliem drošības incidentiem, ar ko ir saskārušās pētījumā iekļautajām iestādēm. Tiek jautāts par reakciju, kāda tā bijusi, saskaroties ar šādu situāciju, ja tāda ir bijusi. Tāpat autore turpina analizēt teorētiskā un praktiskā modeļa saderību un to, vai ir kādas pretrunas un potenciālas problēmas aizsardzības mehānismā, lai nodrošinātos pret potenciālajiem kibernoziegumu riska draudiem. Bez tā, ka tiek apskatīts, kāda saskare tiešās valsts pārvaldes institūcijām bijusi ar riska draudiem, autore aplūko arī viņu viedokli kontekstā ar preventīvu pasākumu veikšanu, iespēju objektīvi noteikt riska lielumu, analizēt potenciālās sekas, īstenoties riska draudiem.

Skatot U. Beka nākotnes attīstības skatījumu, un, sakot, ka progress ietver sevī ne vien to, ka notiek sabiedrības locekļu attīstība, gan pilnveidojot esošos pārvaldes mehānismus, pārskatot normas un radot jaunas, bet notiek arī risku attīstība. Cenšoties riskus ierobežot, var nonākt otrā galējībā, kad viss pārvēršas par risku un šādam uzstādījumam kļūstot par dominējošo, kad apdraudējums ir sociālās realitātes sastāvdaļa, nākamos solis ir, ka riski tiek uztverti kā tirgus iespēja, nevis kā „iespēju tumšā puse". Attīstoties tehnoloģiskajai infrastruktūrai, kļūstot tai par daļu no īstenības, esošajā realitātē paliekošu vietu ieņem, piemēram, bezpilota lidmašīnas u.tml. ir jāsecina, ka neesam nemaz tik tālu no iespējamības, kad notiks tirgošanās ar riskiem.

Ceturtā un noslēdzošā jautājumu bloka mērķis ir rast atbildi uz trešo nosprausto pētniecisko jautājumu, proti, kāds ir tiešo valsts pārvaldes institūciju pārstāvju un ekspertu vērtējums par to, vai un kādus preventīvus pasākumus ir iespējams veikt, lai izvairītos no kibernozieguma riska. Šajā blokā iekļautais jautājumu loks ir vērsts uz to, lai noskaidrotu, kas tiek darīts, lai tiešās valsts pārvaldes institūcijā risks tiktu samazināts līdz tādam drošības līmenim, ko varētu uzskatīt par atbilstošu un pietiekamu, ņemot vērā iestādes darbības profilu. Cik efektīvs ir drošības pasākumu komplekss, kurā ietilps gan auditoru piesaiste objektīvākam reālās situācijas novērtējumam, vai IT drošības noteikumu izveide palīdz mazināt iekšējās vides draudus? Tāpat autore izjautā informantus par viņu domām saistībā ar Latvijas IT drošības stratēģiju, par to, cik skaidri definētas ir atbildības jomas attiecībā uz kibernoziegumu riska reaģēšanu, atbildīgajām personām pašā iestādē un institūcijām, skatot to valsts mērogā.

Skatoties kopumā par kibernoziegumu risku tiešās valsts pārvaldes institūcijās, tad izpratne par potenciālo apdraudējumu veidojas pakāpeniski, gan ņemot vērā iestādē strādājošo speciālistu pieredzi un arī pašas organizācijas kultūru un tradīcijas, kas veicina vai tieši pretēji – nerada labvēlīgus apstākļus izpratnes veicināšanai un nostiprināšanai. Situācijā, kad kibernozieguma riska draudi netiek vērtēti kā augsti, kaut gan nākotnē tiek prognozēts, ka IT apdraudējums palielināsies, tāpat arī uzbrukumi virtuālajā vidē, izmantotie līdzekļi un instrumenti, kas nodrošina risku reducēšanu tiešajās valsts pārvaldes institūcijās, tiek izmantoti atbilstoši izpratnes līmenim un sociālajai realitātei.

Autore prognozē, ka sabiedrības locekļiem pieejamo un izmantojamo e – pakalpojumu, ko piedāvā valsts iestādes, klāsts paplašināšanās (iespējams iekļaujot arī e – balsošanu) un notiks pārēja uz aizvien sarežģītākām un progresīvākām tehnoloģijām un automatizētajām sistēmām, kā rezultātā radīsies nepieciešamība izstrādāt jaunus aizsardzības mehānismus pret risku iestāšanos. Jau tagad tiek realizēta ideja par kiberaizsardzības vienības izveidi, kas būtu uzskatāms kā pirmais solis jaunu risinājumu meklēšanā uz maksimāli iespējamās drošības garantēšanu.

Secinājumi

1. Kibernoziegumu salīdzinoši nesenā parādīšanās un arvien jaunu šo noziegumu paveidu un izpausmju dēļ nepastāv vienota kibernoziegumu definīcija. Tāpat netiek lietots viens un tas pats jēdziens, lai apzīmēto šo parādību.
2. Likumiskais ietvars, kas vērsts uz jauno tehnoloģiju radīto potenciālo riska apdraudējumu, vērtējams kā atbilstošs. Pozitīva ir šo regulējošo dokumentu savstarpējā sasaite, kā arī tas, ka ir izveidoti Latvijas MK noteikumi, kuri precīzāk paskaidro izstrādātos likumus to realizācijai praksē.
3. Ar kibernoziegumiem saistītajā reglamentējošajā likumdošanā pastāv arī savas nepilnības, kas apgrūtina likumu ievērošanu vai potenciālā soda mēra piespriešanu sakarā ar skaidri nenodefinētiem terminiem.
4. T. Hiršī delinkvences/kontroles teorijas skaidrojums kibernoziegumu kontekstā ir cieši saistīts ar racionalitāti. Indivīds, apzinoties savas rīcības iespējamās sekas, izvēlas pārkāpt noteiktās normas, ja, tās pārkāpjot, potenciālais ieguvums ir lielāks par varbūtējiem zaudējumiem.
5. Sabiedrības dzinējspēks ir dažāda veida apdraudējumi, kas indivīdiem liek organizēties, lai spētu pastāvēt, tādējādi notiek dažādu institūciju izveide, morāles un likumīgo normu noteikšana.
6. Sabiedrības attīstības rezultātā rodas arvien jauni riski, līdz ar to tiek determinētas arvien jaunas funkcijas un aizsardzības mehānismi. Apdraudējums veidojas līdz ar kopienas progresu kā negatīvo blakus parādību apkopojums.
7. Risks parasti tiek izprasts kā racionāla kalkulācija, mēģinot izvairīties no iespējamās nedrošības un briesmām, ar ko nāktos saskarties. Ulrihs Beks riskus uztver gan kā reālus, gan sirreālus pieņēmumus par nenotikušo, tādējādi risks vienlaicīgi ir gan reāls, gan sociāli konstruēts.
8. Jebkura darbība dabiski satur arī riska elementu (-us), kā rezultātā sabiedrība ir spiesta dzīvot bailēs par nākotni, kaut tā vēl nemaz neeksistē. Taču esošā sociālā realitāte nespēj nodrošināt stingru attiecību dalījumu laika kategorijās starp pagātni un tagadni, un tagadni un nākotni, tas noved pie „baiļu kultūras" izveidošanās, kas „online" režīmā gaida iespējamā riska seku īstenošanos.
9. Viens no kibertelpas apdraudējumiem ir ļaunprātīgi „savi cilvēki" (*malicious insiders*), tāpēc institūcijai ir nepieciešams domāt, kā novērst šādas situācijas iestāšanos, gan izstrādājot IT drošības noteikumus, gan nodrošinoties pret biežu personāla maiņu, skaidri sadalot atbildības līmeni, un, veicinot darbinieku lojalitāti pret konkrēto iestādi, lai tādējādi veidotu izpratni par kibernoziegumu risku tiešajās valsts pārvaldes iestādēs.
10. Izpratnes veidošana ir pasākumu komplekss, process, kurš ir jāpilnveido un jāattīsta, jo tehnoloģijas attīstās nepārtraukti un pieredze par to, kādus iespējamos riskus un potenciālos draudus ietver inovatīvās tehnoloģijas, neveidojas proporcionāli ātrumam, ar kādu jaunās tehnoloģijas mainās un ienāk sociālajā realitātē, līdz ar to indivīdu apziņā nav pietiekoši aprobētas esošās, kad jau jāsatopas ar jaunām.
11. Kibernozieguma riska izpratni tiešajās valsts pārvaldes institūcijās veido galvenokārt pieredze, no tās izriet IT drošības sistēmas izveide, koncepcijas veidošana, risku pārvaldīšana, izmantojot riska matricas, riska analīzes u.c. paņēmienus.
12. IT novēršanas institūcijas – CERT.LV darbības mērķis nav vērsts tikai uz valsts pārvaldes institūcijām (primāri tās ir būtiskākas par citām sabiedrībā pastāvošajiem elementiem), jo tiek rīkoti izglītojošie pasākumi arī skolās, neizpaliek sadarbība arī ar privātā sektora pārstāvjiem, tādējādi atklājas riska sabiedrības viena no būtiskākajām iezīmēm, proti, izzūd risku robežas, jo riskam vairs nav pakļautas konkrētas grupas vai kategorijas.

13. Būtiskākās problēmas, domājot par likumisko ietvaru, skatāmas kontekstā ar precīza un skaidra definējuma trūkumu, likumos un normatīvajos aktos nepieciešams ieviest vienotu terminoloģiju, iestrādāt arī precīzākus skaidrojumus.
14. IT tehniskie parametri jāsasaista ar juridiskās izpratnes tradīcijām, kā arī jāievieš noteikta gradācijas sistēma, pēc kuras būtu iespējams noteikt, cik svarīgs ir konkrētais risks, ņemot vērā vispārējus sabiedrības funkcionēšanas un sociāli ekonomiskās labklājības pamatprincipus, lai saprastu, kāds ir pārkāpuma apjoms, vērtējot izdarīto pēc konkrētām sekām, kas ir iestājušās.
15. IT drošības incidenti pastāv un tiešās valsts pārvaldes iestāžu līmenī ir izplatīti, taču lielākoties definējami kā zemas prioritātes gadījumi. Šādos apstākļos jāatzīst, ka kibernoziegumu risks tiešās valsts pārvaldes institūcijās vairāk tiek uztverts kā teorētiski pastāvoša perspektīva, ar nelielu varbūtību, ka šāda situācija reāli varētu iestāties, tādējādi ietekmējot iestādes darbību un arī apgrūtinot sabiedrības funkcionēšanu.
16. U. Beks rakstījis, ka arvien jaunu draudu parādīšanās veicina nedrošības intensitāti izplatību, taču realitātē lielākā daļa institūcijās strādājošo tieši nesaskaras ar potenciālajiem kibernoziegumu riska draudiem, līdz ar to uz institūciju kopumā un viņu darbu redzamu ietekmi tas neatstāj, kaut gan pēc būtības par drošību ir atbildīgi visi institūcijā strādājošie, jautājums, vai viņi to vienmēr apzinās.
17. Informanti piekrīt U. Beka izteiktajai tēzei par to, ka sabiedrību rada draudi un jo attīstītāka sabiedrība kļūst, jo ar nopietnākiem riskiem nākas saskarties. Vistuvākais no globālā veida apdraudējumiem, kuri būtu saistāmi ar kibernoziegumu fenomenu, tiek nosaukts variants par masu iznīcināšanas līdzekli, taču tas tiek saprasts diezgan futūristiskā skatījumā.
18. Riska sabiedrības teorijā izvirzītā ideja par to, ka riska sabiedrībā dzīvojošajiem kontrolēt riskus, nosakot gan preventīvu kompleksu kopumu attiecībā uz risku pārvaldīšanas paņēmieniem, gan to, kādā veidā izmērīt un prognozēt sekas, kas saistītas ar riska varbūtības īstenošanos, ir samērā sarežģīti un tas rada papildus grūtības, informanti neapstiprināja.
19. Lai tiešās valsts pārvaldes institūcija būtu spējīga nodrošināties pret potenciālajiem kibernoziegumu risku apdraudējumiem, svarīga ir speciālistu sagatavotība un prasmju līmenis. Situāciju uzlabotu īpaši šajā virzienā vērstu augstskolu programmu izveide, jo nereti pieredze ir reālais balsts, kas nodrošina darboties spējīgas drošības koncepcijas izveidi un pastāvēšanu.
20. Būtisks jautājums ir atalgojuma nodrošinājums un institūcijās strādājošo indivīdu iniciatīvas, jo ne vienmēr ir nepieciešamas nodrošināties ar īpaši dārgām, vai tehniski sarežģītām aizsardzības sistēmām, lai izvairītos no potenciālā riska.
21. Apstākļos, kad pagaidām kibernoziegumu risks tiek vērtēts kā zems, pastāvošais drošības mehānisms un tā principu realizēšana tiešās valsts pārvaldes institūcijās IT drošības jautājumos ir atbilstoša.
22. Sasaistot U. Beka ideju par jauna veida aizsardzības mehānismiem, kas varētu palīdzēt novērst potenciālos riska draudus, jāmin kiberaizsardzības vienības izveides projekts, lai gan realitātē, lielākoties, aizsardzības mehānismi tiek bāzēti tradicionālajā izpratnē, veidojot normatīvos aktus un likumus.
23. Informanti norādīja, ka valstiskā mērogā IT drošības modelis ir izveidots atbilstoši sociālās realitātes prasībām.
24. Balstoties uz intervijās iegūtajiem datiem, **izvirzīta hipotēze**:
    Kibernoziegumu riska draudu īstenošanās tiešajās valsts institūcijās vērtējama kā zema, līdz ar to izveidotais IT drošības aizsardzības mehānisms ir atbilstošs sociālās realitātes prasībām.

Izmantoto literatūras avotu saraksts

1. Cimdiņa R. (red.) (2011) Ievads pētniecībā: stratēģijas, dizaini, metodes, Rīga: Raka, 284 lpp
2. Kūle M. (2006) Eirodzīve. Gulbene: Vītola izdevniecība, 435l lpp.
3. Ķinis U. (2007) Kibernoziegumi. Rīga: Turība, 413 lpp
4. Rubenis A. (2004) 20. gadsimta kultūra Eiropā. Rīga: Zvaigzne ABC, 456 lpp..
5. Silverman D. (2008) Interpreting qualitative data. London: Sage publication 428 p.
6. Ядов В. А. (2003) Стратегия социологического исследования. Москва: „Добросвет” 595 с.