# Kibernoziegumu vispārīgs raksturojums

# IT sfēras attīstība

- Priekšnosacījumi jaunu tiesisko attiecību veidošanai
- Cilvēces eksistences vides izmaiņas – cilvēces atkarība no kibertelpas, no informācijas tehnoloģiju resursiem
- Katrs jaunieviesums – jaunas iespējas noziedzībā
- Latvijas nacionālo tiesību būtiskās izmaiņas

# Kibernoziegumu jēdziens un definēšanas problemātika

- Kibernoziegumi, datornoziegumi, augsto tehnoloģiju noziegumi, digitālie noziegumi, IT noziegumi, noziegumi kibertelpā, e-noziegumi ...
- 1983.gadā OECD definēja datornoziegumu kā - ikvienu nelikumīgu, neētisku vai nesankcionētu uzvedību, kas saistīta ar automātisko datu procesu un/vai datu pārraidīšanu

2001.gada 23.novembrī Budapeštā tika pieņemta Eiropas Padomes Konvencija par kibernoziegumiem (*Convention on cybercrimes*), kas šādas darbības klasificē 5 grupās:

- ar nodomu izdarīti noziedzīgi nodarījumi pret datu un datorsistēmu konfidencialitāti, integritāti un pieejamību (patvaļīga piekļūšana, informācijas sistēmas darbības traucēšana, kaitīgas programmas izplatīšana utt.)
- Ar datoru saistītie noziedzīgie nodarījumi (ar datoriem saistīta viltošana, datorkrāpšana utt.)
- Ar saturu saistītie noziedzīgie nodarījumi (bērnu seksuālās izmantošanas materiālu izplatīšana)
- Ar autortiesību un blakustiesību pārkāpšanu saistītie noziedzīgie nodarījumi
- noziedzīgi nodarījumi, kas saistīti ar rasismu, ksenofobiju un genocīdu propagandējošu materiālu izplatīšanu automatizētās datu apstrādes sistēmās

# IT noziegumi (U.Miķelsons)

- Informācijas tehnoloģiju resursi (aparatūra, programmatūra, elektroniskā informācija, IS pakalpojumi) var būt noziedzīgā nodarījuma apdraudējuma priekšmets.
- Informācijas tehnoloģiju resursi var būt izmantoti kā būtisks līdzeklis (nozieguma rīks) noziedzīgā nodarījuma īstenošanai, bez to izmantošanas šo nodarījumu atbilstošā veidā nav iespējams veikt.
- Informācijas tehnoloģiju resursi var būt izmantoti kā līdzeklis noziedzīgā nodarījuma sagatavošanai un / vai īstenošanai, taču šādu nodarījumu iespējams veikt arī bez IT resursu izmantošanas. Tādēļ vairāk uzmanību pievērš tieši tāda IT resursu izmantošanas īpatnība nodarījuma sagatavošanai un / vai īstenošanai, ka IT resursi veido un saglabā noteiktas, specifiskas šī nozieguma pēdas.

# U.Ķiņa piedāvātā kibernozieguma definīcija

- jebkura tīša nelikumīga, krimināli sodāma darbība, kur informācijas tehnoloģijas (automātiskās datu apstrādes sistēmas, komunikācijas līdzekļi, tajā skaitā, datu pārraides vai telekomunikāciju tīkli utt.) izmantotas kā nozieguma priekšmets vai nozieguma rīks ar mērķi ietekmēt informācijas sistēmu tehniskos un informācijas resursus vai arī kā medijs nelikumīgas informācijas aprites procesā

# Kibernoziegumi LR izpratnē

- Kibernoziegumi – LR speciālistu skatījumā (šaura definēšana) – ir noziedzīgi nodarījumi pret automatizētas datu apstrādes sistēmas (turpmāk – ADAS) drošību – pret konfidencialitāti, pieejamību un integritāti/veselumu

# ADAS drošība

- informācijas **pieejamības** (pēc informācijas sistēmas lietotāja pieprasījuma noteiktā laikposmā viņš var piekļūt informācijai), **integritātes** (pilnīgas un neizmainītas informācijas saglabāšana) un **konfidencialitātes** (informāciju saņem tikai tam pilnvarotas personas) nodrošināšana automatizētas datu apstrādes sistēmā

# Krimināllikums

(no 01.06.2005, kad stājās spēkā būtiskie KL grozījumi nolūkā harmonizēt LR likumdošanu ar EP konvencijas pamatnostādnēm)

- 144.pants. Korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšana – piemēram, e-pasta korespondences grozīšana
- 177.[1] pants. Krāpšana automatizētā datu apstrādes sistēmā, apzināti ievadot nepatiesus datus - krāpšanas „mērķis” ir datorsistēma, nevis cilvēks kā tradicionālai krāpšanai;
- 193.[1] pants. Datu, programmatūras un iekārtu iegūšana, izgatavošana, izplatīšana, izmantošana un glabāšana nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem – piemēram, “phishing” gadījumi

# Krimināllikums

*(spēkā esošs no 01.04.1999)*

- 241.pants – patvaļīga piekļūšana automatizētai datu apstrādes sistēmai – būtiskākais – ir nepieciešamas sekas („būtisks kaitējums”) materiālajam sastāvam
- 243.pants – automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju – būtiskākais –LR ir kriminālizēta traucēšana, kas var izpausties, piemēram, kā „DDos” uzbrukums, nodarot zaudējumus lielā apmērā
- 244.pants – nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm – būtiskākais – tiek paplašināts kaitīgas programmas jēdziens, nomainot „datorvīrusa” šauro saturu
- 245.pants – informācijas sistēmas drošības noteikumu pārkāpšana – būtiskākais – ir blankēta dispozīcija, MK not.Nr.106. no 2000.03.21 noteikumi vairs nav spēkā, jo bija saistoši praktiski visam juridiskajām personām. Taču neizslēdz atbildīgās personas atbildību iekšējo noteikumu esamības gadījumā

# Paldies par uzmanību!