

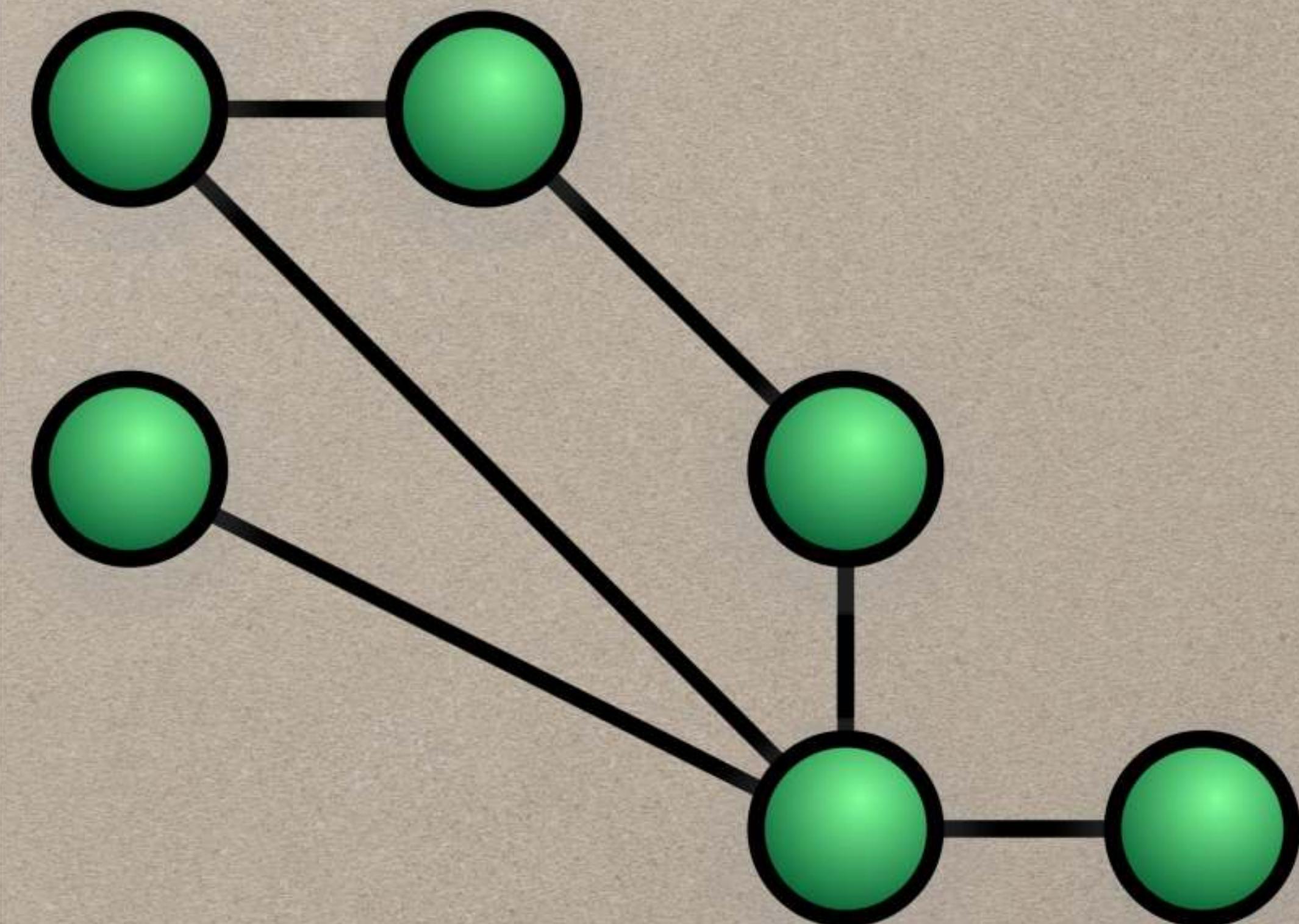
IT DROŠĪBAS PĒTNIECĪBAS VĒSTURE UN MŪSDIENU PROBLEMĀTIKA

KIRILS SOLOVJOVS

01.09.2016.

INTERNETA AIZMETŅI

ARPANET + TCP/IP =
INTERNET
(1983)

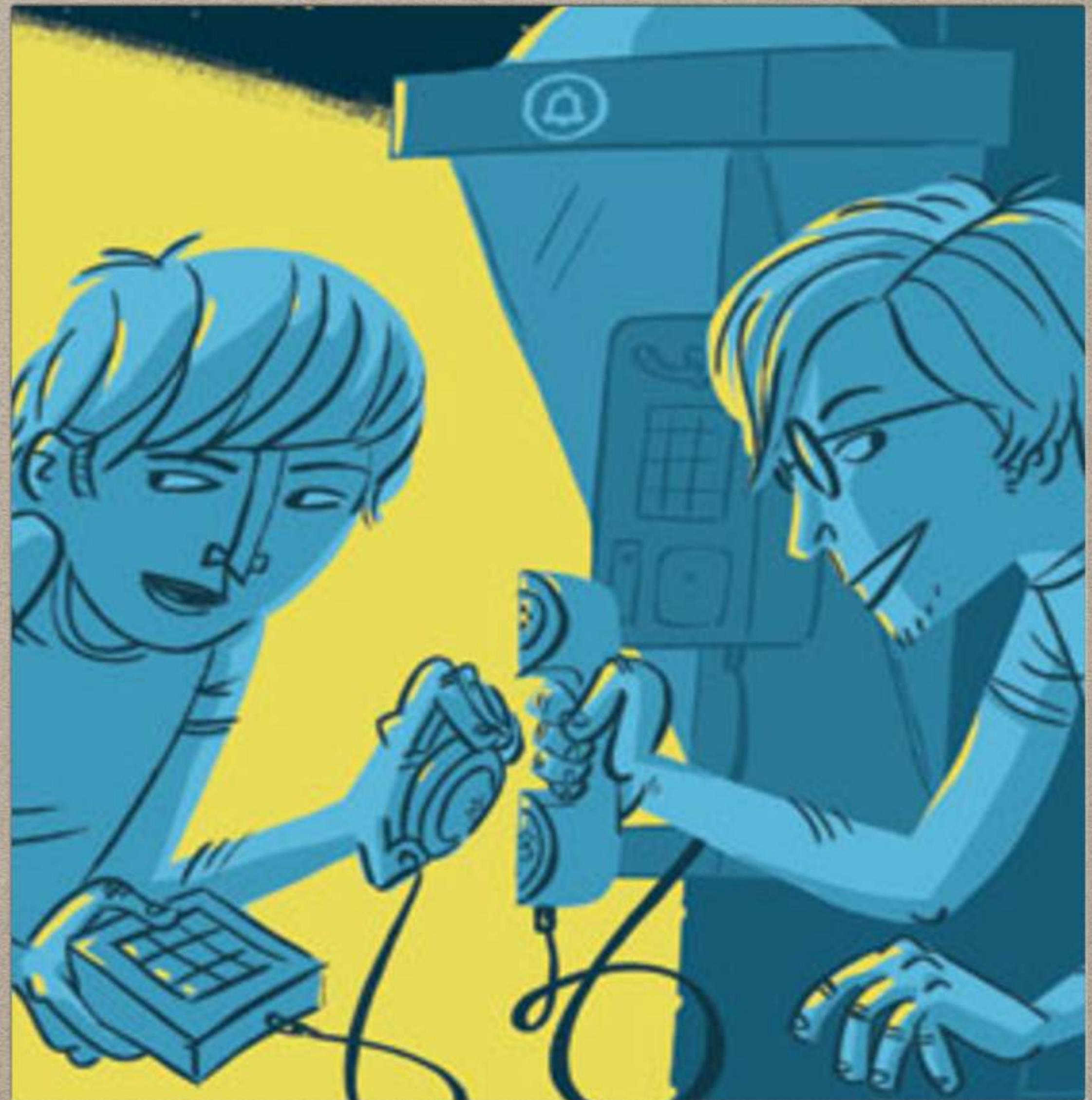


INTERNETA SĀKUMS

- Nav komerciālu interešu
- Nav īpašas vajadzības pēc drošības risinājumiem
- "Paralēlā pasaule"
- Uzlaušana - draudzīga, rotaļīga

TELEFONU CENTRĀLES UN KOMUNIKĀCIJU UZNĒMUMI

**TIKMĒR SASKARAS AR
LIELĀKO SATRAUKUMU**



KEVIN MITNICK

SOCIĀLAIS INŽENIERIS



INTERNETS KĀ KOMERCIJAS RĪKS

- Plaša interneta pieejamība piesaista komersantu uzmanību
- Sākotnēji kā informācijas kanāls
- Vēlāk piesardzīgi piedāvājot veikt pirkumus internetā
- Mūsdienās - standartizētas drošības procedūras, kas ļauj veikt maksājumus un justies droši

"CEPURES" (-HAT)

- Baltā
- Melnā
- Pelēkā



"BALTO CEPURU" MOTIVĀCIJA

- Aizsargāt valsti, pasauli, sevi
- Saņemt izaicinājumu, sarežģītu uzdevumu, puzli
- Iegūt atpazīstamību un prestižu
- Nopelnīt ar atlīdzību vai atalgojumu

UZBRUKUMI KĀ KIBERIEROCIS





IT DROŠĪBAS AIZMETŅI BALTIJAS VALSTĪS

BRONZAS KAREIVJA NEMIERI

IGAUNIJA, 2007



NEO UZLAUŽ VID

LATVIJA, 2009



???

LIETUVA,
2011 - 2013 - 2015 - ... ?



Lithuanian Presidency
of the Council of the
European Union 2013



IT DROŠĪBAS EKSPERTĪZE - PIEPRASĪTAS PRASMES

IT DROŠĪBAS EKSPERTI ATROD SAVU VIETU

1. Nacionālās drošības intereses
2. Komercnoslēpuma saglabāšana
3. Klientu datu aizsardzība
4. Pētniecība

IT DROŠĪBAS PĒTNIECĪBA LATVIJĀ

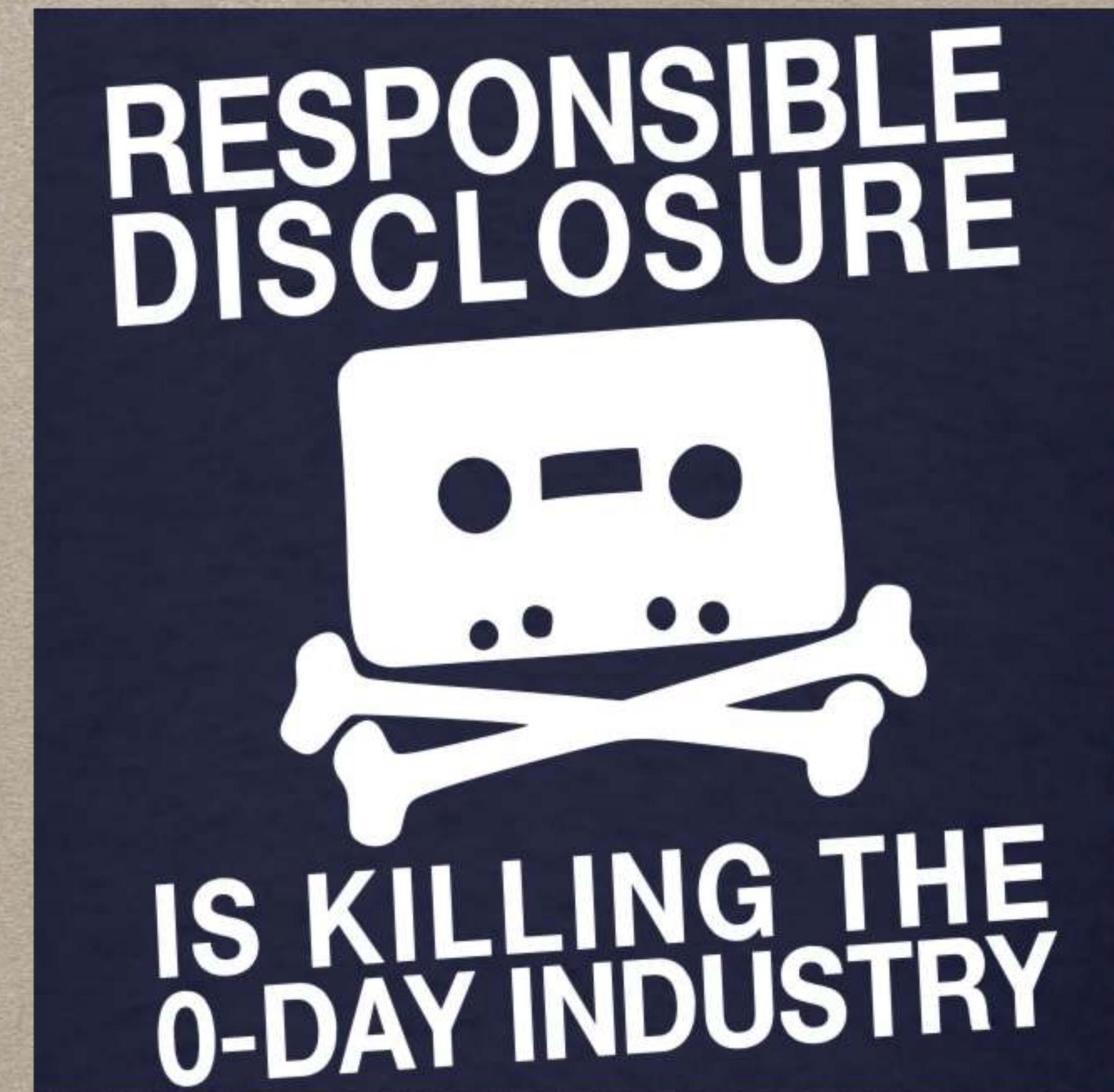
- Pirmais Dr.sc.comp. IT drošības virzienā - 13.11.2015. (Ilze Murāne)
- Ne katrs var būt zinātnieks,
 - "Zinātnieks ir fiziskā persona, kura veic zinātnisko darbību un kura šajā likumā noteiktajā kārtībā ieguvusi zinātnisko kvalifikāciju."
- bet jebkurš var nodarboties ar zinātni.
 - "Tiesības veikt zinātnisko darbību ir jebkurai personai [...]"

TIKMĒR PĒTNIECĪBAS IZAUGSME TURPINĀS

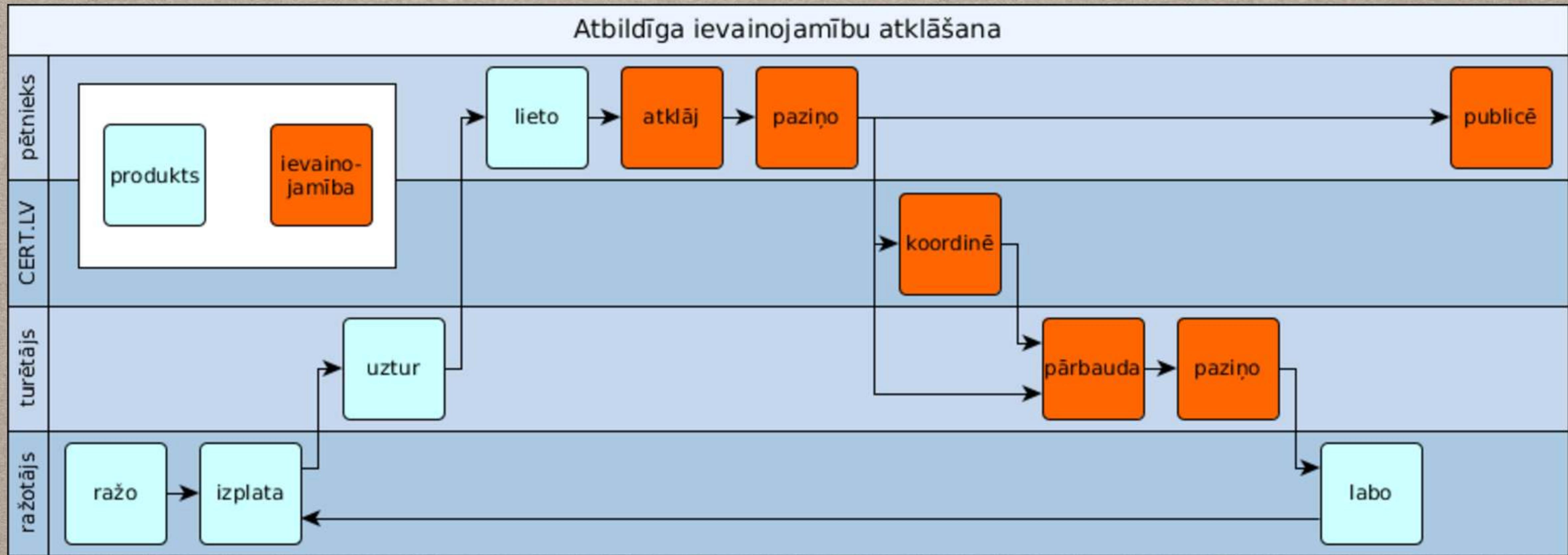
- Swedbank mobilā aplikācija
- Banklink uzbrukumi
- Rīgas Kartes "e-maks.lv"
- Rīgas Satiksmes "e-talons"
- Vairāki gadījumi valsts iestādēs

ATBILDĪGAS IEVAINOJAMĪBU ATKLĀŠANAS POLITIKA (RDP)

- viens no veidiem, kā risināt ievainojamības programmatūrā
- parasti procesu uzsākt pētnieks
- nepieciešama abpusēja uzticēšanās
- atļauj ražotājam novērst ievainojamību saprātīgā laika periodā
- noslēgumā ievainojamība tiek izziņota publiski



Atbildīga ievainojamību atklāšana



RDP IEVIESĒJU PIEMĒRI

- Nīderlande
- ASV Pentagons
- Swedbank grupa
- Dažādas "kļūdu atlīdzību" (bug bounties) apvienības:
 - HackerOne, BugCrowd u.c.

RDP VĀJĀS PUSES UN IZAICINĀJUMI

- Turētāja kapacitāte reaģēt uz ziņojumiem
- Iesaistīto pušu pienākums ievērot noteikumus
- Steoreotipi par "uzlaušanu"



RDP IEGUVUMI

- Mazina esošo ievainojamību
jaunprātīgu izmantošanu
- Taupa cilvēkresursus
- Veicina izpratni par kiberdrošību



NOSLĒGUMĀ: PAR LATVIJU

- Aizsardzības ministrija sagatavojuusi grozījumus, kas paredz ar likuma spēku nostiprināt RDP attiecībā uz valstij nozīmīgām informācijas sistēmām.
- VSS-448 (19.05.2016.)
- Saskaņošanas procesā
- Iespējams, pirmais šāda veida regulējums pasaule

Pateicos par uzmanību!

