Funded by the Erasmus+ Programme of the European Union

Ievads kiberdrošībā

Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izaicinājumi

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Apmācību mērķis

- Atgādināt par kiberdrošības koncepciju kopā ar parastajām problēmām, ar kurām saskaras uzņēmumi
- Uzskaitīt kiberuzbrukumu izaicinājumus, ar kuriem saskaras privātpersonas un uzņēmumi, sākoties 4. rūpniecības ērai

Kursantu darba slodze

Lekcija	1,5 st.
Audio un video materiāli	1,5 st.
Pētījumi	1,5 st.
Papildu lasīšana	4 st.
Sagatavošanās eksāmenam	1,5 st.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Plaša tehnoloģiju izmantošana

Programmatūrai un informācijas sistēmām ir liela nozīme dažādās cilvēka dzīves jomās

Nepieciešamība parūpēties par informācijas drošību kļūst par nepieciešamību, nevis izvēles iespēju

CyberPhish
Safeguarding your digital future

[Abjoduns [Abiodun] un citi, 2021. gads]

Funded by the Erasmus+ Programme of the European Union

Definīcija

Kiberdrošība

ko dēvē arī par

Datoru drošību, informācijas tehnoloģiju drošību** vai **IT drošību

Pieeja un darbības, kas saistītas ar drošības riska pārvaldības procesiem, ko ievēro organizācijas un valstis, lai aizsargātu kibertelpā izmantoto datu un līdzekļu konfidencialitāti, veselumu un pieejamību. Koncepcija ietver vadlīnijas, politikas un drošības pasākumu, tehnoloģiju, rīku un apmācību kopas, lai nodrošinātu vislabāko aizsardzību kibervides stāvoklim un tās lietotājiem.

[Šacs [Schatz] un citi, 2017. gads]

Satura rādītājs

- Uzņēmējdarbības izaicinājumi
- Kiberdrošības uzbrukumu pieaugums
- Tehnoloģiju izmantošana un drošības izaicinājumi
  - *"Lietu internets"*
  - *Skaitļošanas tehnika, izmantojot "mākoņa" pakalpojumus*
  - *Inteliģentā infrastruktūra*
  - *Viedās mājas*
  - *Blokķēdes tehnoloģija*
  - *Lielie dati*
- Pieaugošu draudu izaicinājums
- Nāciju valstu draudi

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Uzņēmējdarbības izaicinājumi

- Digitālā transformācija
- Mākoņpakalpojumi (*angl.* Cloud)
- Atbilstība noteikumiem, normām u. tml.
- Automatizācija
- "Lietu internets"
- Integrēšana, atjauninājumi
- Mākslīgais intelekts un mašīnmācīšanās

- Attālināta darba atbalsts
- Datu pārvaldīšana
- Koncentrēšanās uz mobilu darbību
- Sociālie mediji
- Projekta vadība
- Infrastruktūras izmaiņas
- Tehnisko apmācību trūkums

[Perdomo [Perdomo], 2021. gads] Nezināma autora fotoattēls, licencēts saskaņā ar CC BY-NC

Funded by the Erasmus+ Programme of the European Union

Uzņēmējdarbības izaicinājumi

- Digitālā transformācija
- Mākoņpakalpojumi (*angl.* Cloud)
- Atbilstība noteiku u. tml.
- Automatizācija
- "Lietu internets"
- Integrēšana, atj
- Mākslīgais intel un mašīnmāci
- Attālināta darba atbalsts
- Datu pārvaldīšana
- anās uz mobilu darbību
- Sociālie mediji
- Projekta vadība
- tūras izmaiņas
- nācību trūkums

Trešo pušu riski – riski, kas izriet no organizācijas sakariem ar ārējām pusēm, lai nodrošinātu ar uzņēmējdarbību saistītas piegādes vai pakalpojumus

- *Normatīvie/atbilstības*
- *Finanšu*
- *Darbības*
- *Reputācijas*
- *Stratēģiskie*

https://hyperproof.io/resource/author/hyperproof-team/

[Perdomo [Perdomo], 2021. gads] Nezināma autora fotoattēls, licencēts saskaņā ar CC BY-NC

Funded by the Erasmus+ Programme of the European Union

Uzņēmējdarbības izaicinājumi

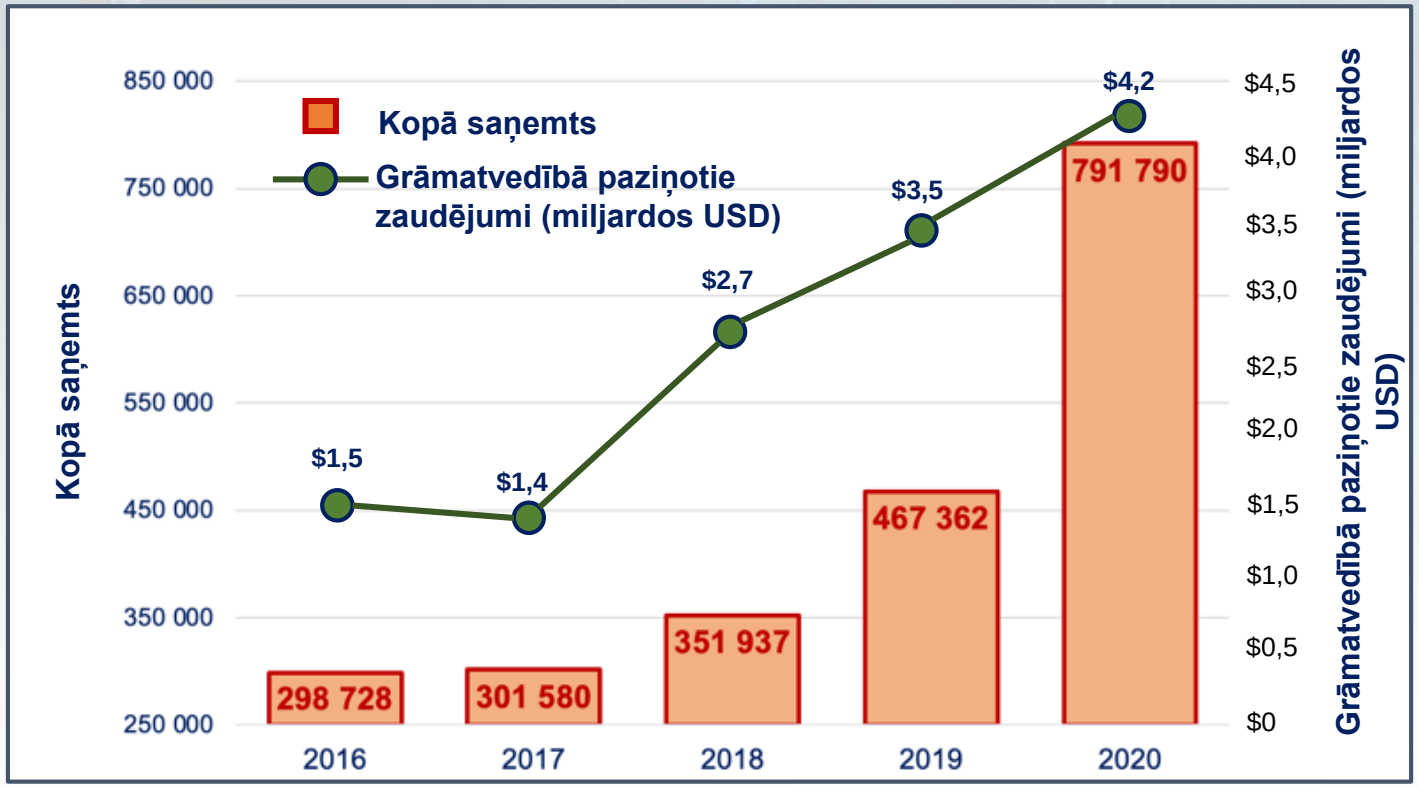
- Digitālā transformācija
- Mākoņpakalpojumi (*angl.* Cloud)
- Atbilstība noteikumiem, normām u. tml.
- Automatizācija
- "Lietu internets"
- Integrēšana, atjauninājumi
- Mākslīgais int
  un mašīnmācīšanās

- Attālināta darba atbalsts
- Datu pārvaldīšana
- Koncentrēšanās uz mobilu darbību
- Sociālie mediji
- Projekta vadība
- ūras izmaiņas
- Tehnisko apmācību trūkums

Informācijas drošība

[Perdomo [Perdomo], 2021. gads] Nezināma autora fotoattēls, licencēts saskaņā ar CC BY-NC

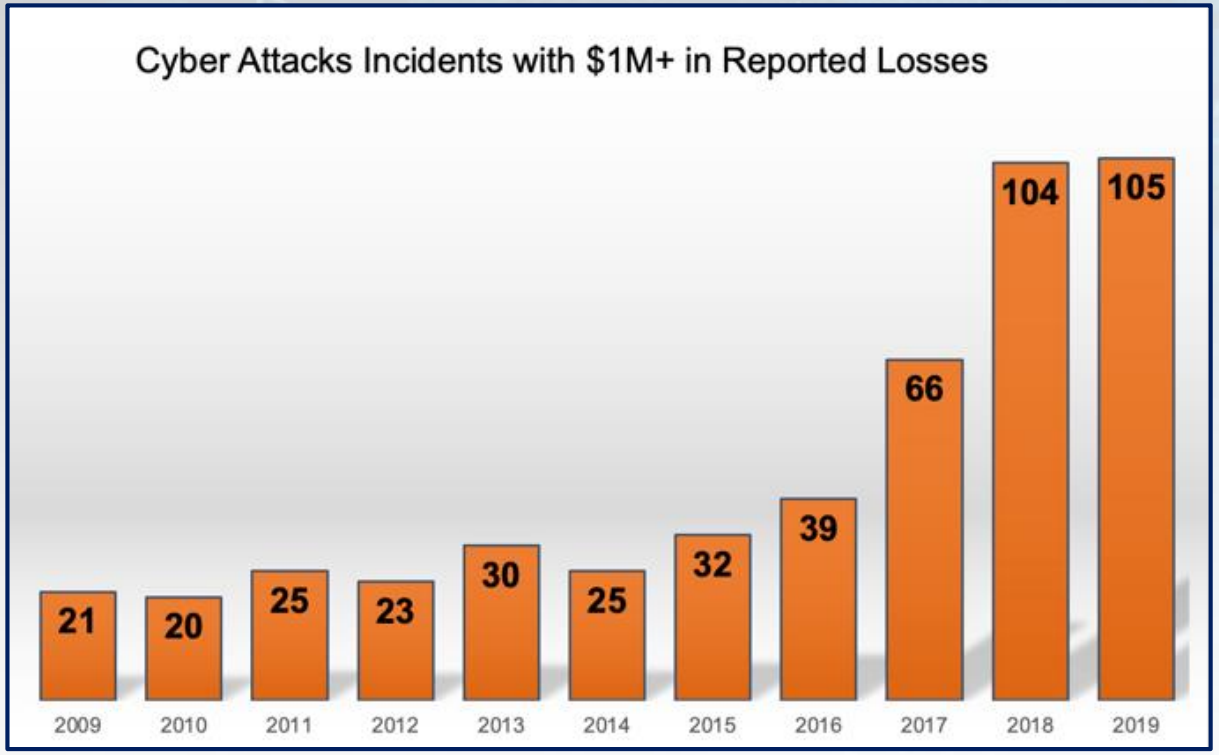
Kiberdrošības uzbrukumu pieaugums

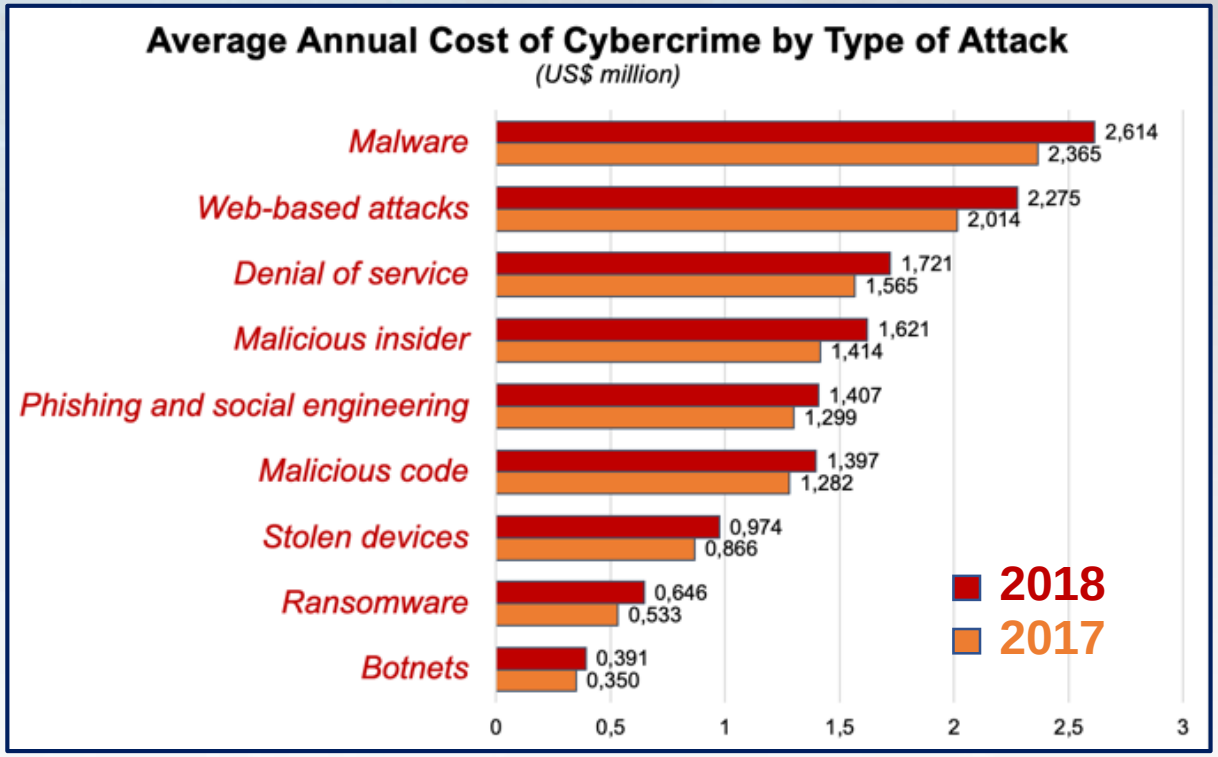


- *Mērķauditorijas atlase*
- *"Mājasdarba" pabeigšana*
- *Veiksmes un sakritības spēle*
- *Krāpniecības veidi turpina attīstīties*
- *Noziedznieki pārdod nozagto informāciju*
- *Pacietība un neatlaidība atmaksājas*
- *Noziedznieki var darboties no jebkuras vietas*

https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/?sh=17cfbc8c5fa2

Kiberdrošības uzbrukumu izmaksas





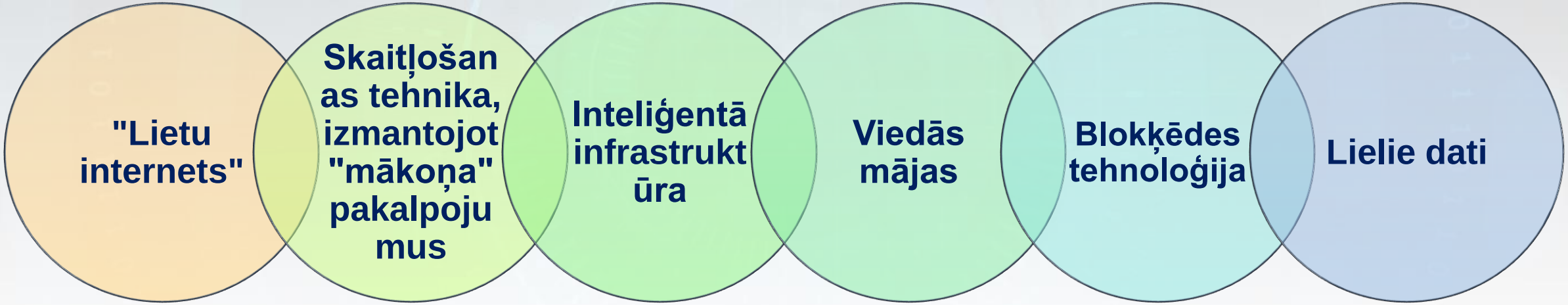
Pēdējās desmitgades laikā – **490** nozīmīgi kiberdrošības incidenti

2018. gadā kopā = US$ **13** miljoni

https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/

https://www.digitalmarketingcommunity.com/researches/ninth-annual-cost-of-cybercrime-research-2019/

Plašajā mobilo tehnoloģiju lietojumā



Lietu internetā

Lietu internets (IoT) apraksta fizisku objektu tīklu, kas ir iegults ar sensoriem, programmatūru un citām tehnoloģijām ar mērķi savienot iekārtas un aprīkojumu un apmainīties ar datiem ar citām ierīcēm un sistēmām internetā

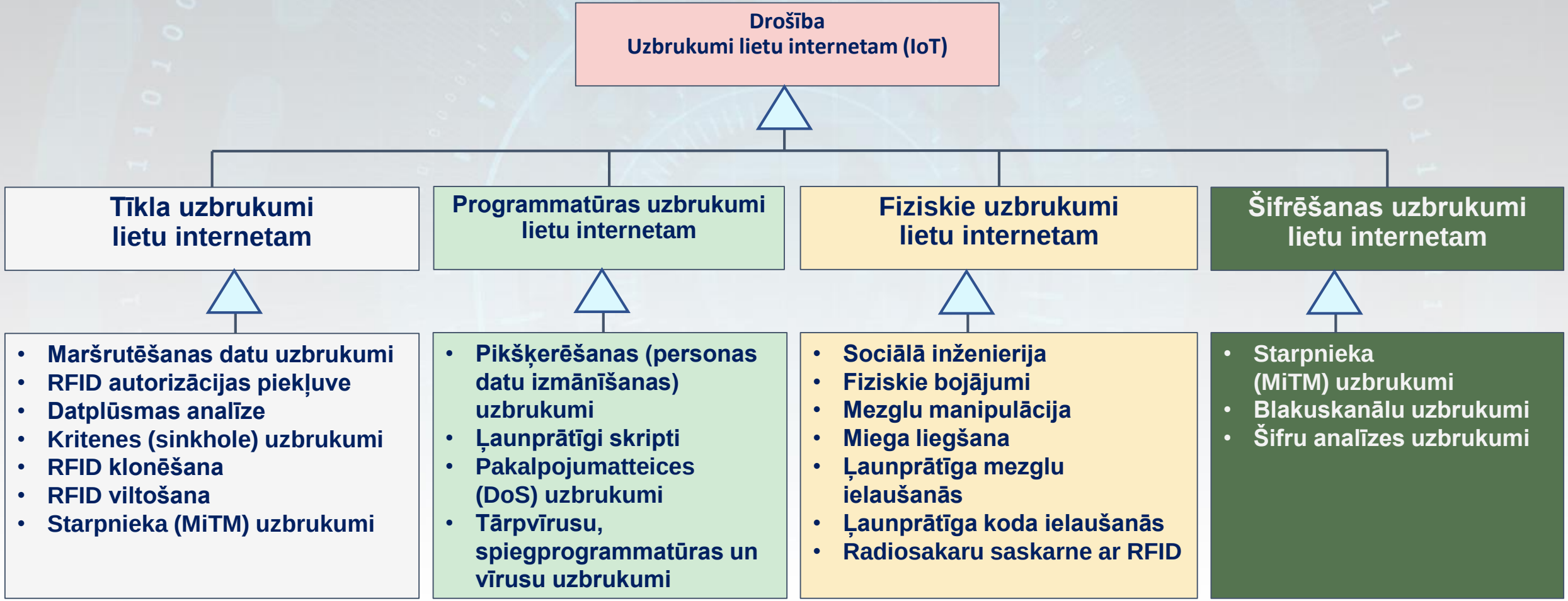
- *"Lietas" šajā gadījumā nozīmē tehnoloģijas, ierīces, priekšmetus, dzīvniekus vai cilvēkus*
- *Sakaru tīkli, kas savieno ierīci*
- *Datoru tīkli, izmantojot datu straumēšanu no interneta uz ierīci*

Gads	***Zemeslodes iedzīvotāji*** *(miljardos)*	***IoT pievienotās iekārtas*** *(miljardos)*	***Attiecība***
2003	6,3	0,5	0,08
2010	6,8	12,5	1,84
2015	7,2	25	3,47
2020	7,6	50	6,58

[Abjoduns [Abiodun] un citi, 2021. gads]

Drošības izaicinājumi

Lietu internetā



[Abjoduns [Abiodun] un citi, 2021. gads]

Funded by the Erasmus+ Programme of the European Union

Mākoņpakalpojumu datorsistēmās

CyberPhish
Safeguarding your digital future

[Tahirkeli [Tahirkheli] un citi, 2021. gads]

Funded by the Erasmus+ Programme of the European Union

Mākoņpakalpojumu datorsistēmās

Portatīvie datori

Serveri

Tālruņi

Mākoņdatošanas nepareiza un ļaunprātīga izmantošana

Saskarnes un nedrošas lietojumprogrammu saskarnes (API)

Iekšējie draudi

Problēmas, kas izriet no kopīgotām tehnoloģijām

Informācijas zudumi vai noplūdes

Sesijas vai pakalpojuma nolaupīšana

Riski zināšanu trūkuma dēļ

Planšetdatori

Datori

[Orantess – Himenezs [Orantes-Jimenez] un Akire [Aquirre], 2020]

Funded by the Erasmus+ Programme of the European Union

Inteliģentajās sistēmās

UZTVERES LĪMENIS

- Noteikšana
- Vīzija
- Pozicionēšana
- Aktivizācija

TĪKLA SLĀNIS

- Integrēts transportlīdzeklī
- Starp transportlīdzekļiem
- Starp transportlīdzekli un infrastruktūru

LIETOTŅU SLĀNIS

- Skaitļošana/serveri
- Datu uzglabāšana
- Cilvēks

[Afija [Affia] un citi, 2019. gads]

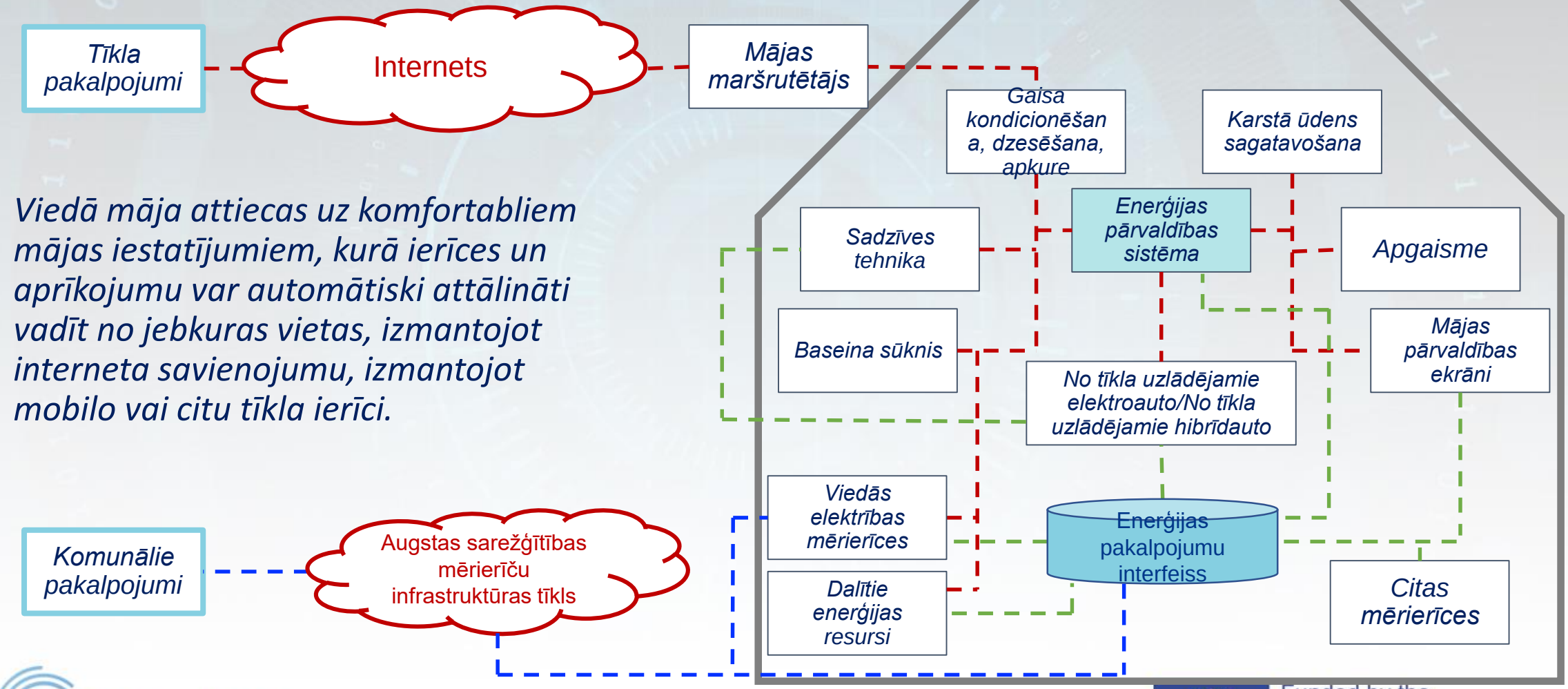
Funded by the Erasmus+ Programme of the European Union

	DROŠĪBAS DRAUDI					
Sistēmas aktīvi	*Viltošana*	*Falsifikācija*	*Dalības noliegums*	*Informācijas paušana*	*Pakalpojuma noliegums*	*Privilēģiju paaugstināšana*
Noteikšanas, pocizionēšanas un vīzijas metodes	Viltošana, mezglu identitātes uzdošanās, ilūzija, atkārtota atskaņošana, maldinošu ziņojumu sūtīšana, maskēšanās	Datu viltošana, datu manipulācija, falsifikācija, lasījumu falsifikācija, ziņojumu iepludināšana	Viltus ziņojumi	Uzglabātie uzbrukumi, noklausīšanās	Ziņojumu piesātināšana, nosprostošana, pakalpojuma atteikums (DoS), sistēmas traucējumu izraisīšana	Aizmugures durvju izmantošana, neautorizēta piekļuve, privilēģiju paaugstināšana, elektronisko vadības bloku (ECU) attālinātā atjaunināšana
Transportlīdzeklī integrētais tīkls, starp transportlīdzekļiem (V2V) un starp transportlīdzekli un infrastruktūru (V2I)	Sibilas uzbrukumi (Sybil), viltošana, atkārtota atskaņošana, maskēšanās, pirkstu nospiedumu uzbrukumi, tārpejas, kamuflāžas uzbrukumi, identitātes uzdošanās	Laika uzbrukumi, iepludināšana, manipulācija, maršrutēšanas manipulācija, falsifikācija, datu viltošana, ļaunprātīga atjaunināšana	Viltus ziņojumi, negodīgs dalības noliegums, notikumu izsekojamības zudums	Noklausīšanās, starpnieka uzbrukumi (MiTM), ID atklāšana, lokācijas izsekošana, ziņojumu pārtveršana, informācijas atklāšana	DoS/DDoS, mēstules, nosprostošana, pārpludināšana, ziņojumu apspiešana, kanālu interfeiss, melnā cauruma uzbrukumi	Ļaunprātīga programmatūra, brutāla spēka uzbrukumi, kontroles pārņemšanas uzbrukumi, sociālā inženierija, loģikas uzbrukumi, neautorizēta piekļuve, sesijas nolaupīšana
Lietotņu serveri, nomales datu centrs, cilvēciskie faktori	Viltošana, Sibilas uzbrukumi (Sybil), ilūzijas uzbrukumi	Ļaunprātīgi atjauninājumi	--	Noklausīšanās, lokācijas izsekošana, privātuma noplūdes	Pakalpojuma noliegšana	Operētājsistēmu uzlaušana, sociālā inženierija, negodīgi datu centri, ļaundabīga programmatūra

Drošības izaicinājumi

Viedo māju sistēmās

Viedā māja attiecas uz komfortabliem mājas iestatījumiem, kurā ierīces un aprīkojumu var automātiski attālināti vadīt no jebkuras vietas, izmantojot interneta savienojumu, izmantojot mobilo vai citu tīkla ierīci.



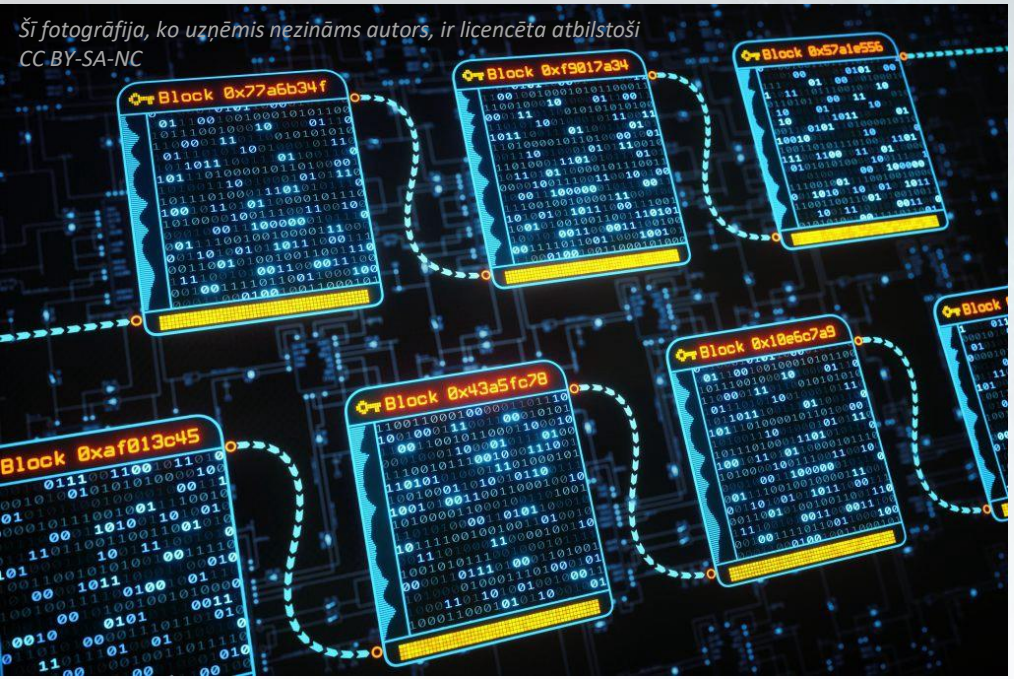
[Kominoss [Komninos] un citi, 2014. gads]

CyberPhish
Safeguarding your digital future
Funded by the Erasmus+ Programme of the European Union

Viedo māju sistēmās

Scenārijs	**Iespējami draudi** (N – tīkla zona, SH – viedās mājas koncepcija)	**Pārvarētais drošības kritērijs**
AS1: Uzbrukumi, kas apdraud sekmīgu ierīču enerģijas un patēriņa pārskatu sagatavošanu	Noklausīšanās (N), datu plūsmas analīze (N), ziņojumu modifikācija (N), atkārtotas atskaņošanas uzbrukumi (N), enerģijas pārvaldības sistēmu identitātes piesavināšanās (SH)	Konfidencialitāte, sistēmas veselums (integritāte), autentifikācija
AS2: Uzbrukumi, kuru mērķis ir enerģijas importa/eksporta signāli enerģijas pakalpojuma saskarnei vai mājas tīklam	Dalības noliegums (N), ziņojumu modifikācija (N), atkārtotas atskaņošanas uzbrukumi (N)	Dalības nolieguma neiespējamība, sistēmas veselums (integritāte), autentifikācija
AS3: Fiziska manipulācija ar mērierīcēm, to reversēšana vai noņemšana	Manipulācija, reversēšana, mērierīču noņemšana (SH), nelegālas programmatūras modifikācijas/atjaunināšanas (SH)	Autentifikācija, sistēmas veselums (integritāte)
AS4: Uzbrukumi attālinātai mājas uzraudzībai un kontrolei	Klientu identitātes piesavināšanās (N), ierīču identitātes piesavināšanās (SH), ziņojumu modifikācija (N), atkārtotas atskaņošanas uzbrukumi (N), dalības noliegums (N)	Sistēmas veselums (integritāte), dalības nolieguma neiespējamība, autentifikācija
AS5: Uzbrukumi, kuru mērķis ir enerģijas patēriņa datu pieprasījumi	Klientu identitātes piesavināšanās (N), noklausīšanās (N), pārtveršana (N), ziņojumu modifikācija (N)	Konfidencialitāte, sistēmas veselums (integritāte), pieejamība

Blokķēžu tehnoloģijās



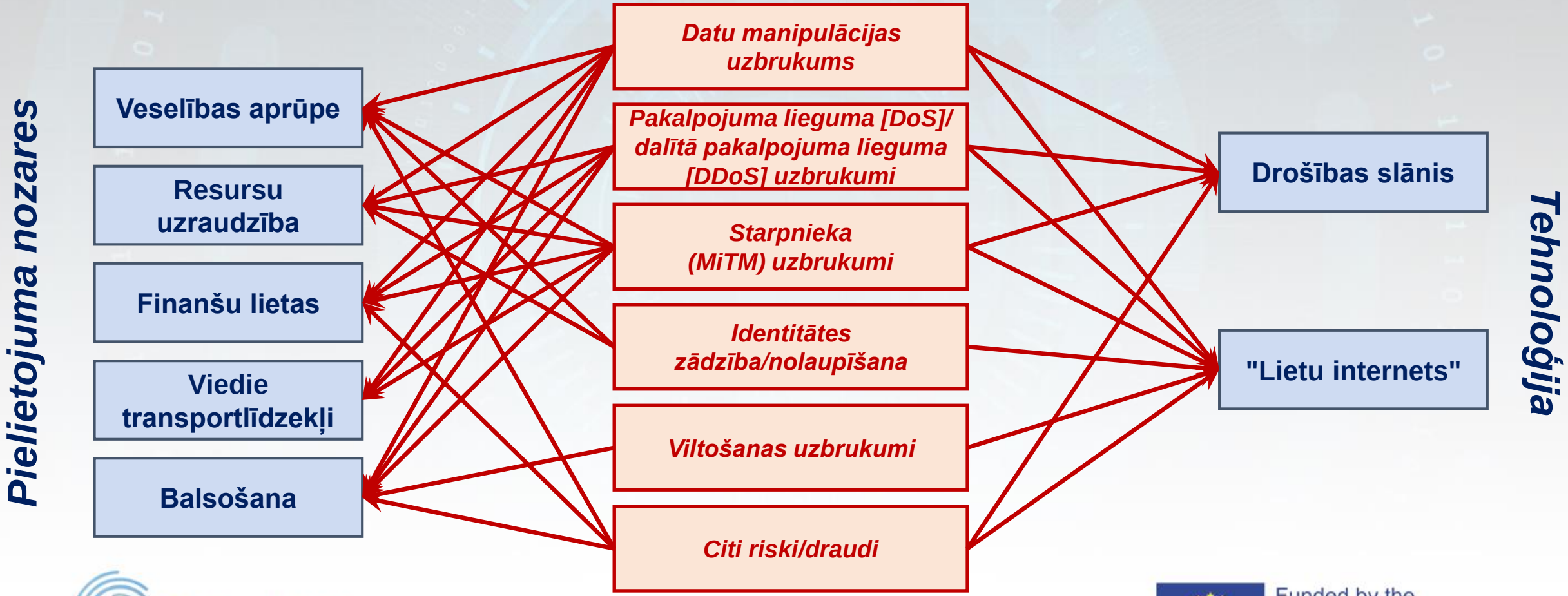
Šī fotogrāfija, ko uzņēmis nezināms autors, ir licencēta atbilstoši CC BY-SA-NC

Blokķēdes (blockchain) ir izplatīta nemainīga koplietotu reģistru (žurnālu) tehnoloģija, kas sniedz dalībniekiem iespēju koplietot reģistru, izmantojot vienādranga replikāciju un atjauninot katru reizi, kad notiek darījums.

[Lūiss [Lewis], 2015; Sato [Sato] un Himura [Himura], 2018. gads]

Blokķēžu tehnoloģijās

Drošības riski dažādās lietojumprogrammu jomās tiek mazināti, izmantojot blokķēžu lietojumprogrammas



CyberPhish
Safeguarding your digital future

[Ikbals [Iqbal] un Matulevičiuss [Matulevičius], 2019. gads]

Funded by the Erasmus+ Programme of the European Union

Drošības izaicinājumi

Blokķēžu tehnoloģijās

Drošības riski blokķēžu lietotnēm

Pielietojuma nozares

- Veselības aprūpe
- Resursu uzraudzība
- Finanšu lietas
- Viedie transportlīdzekļi
- Balsošana

- ***Sibilas uzbrukumi (Sybil)***
- ***Dubulttēriņu uzbrukumi***
- ***51% uzbrukums***
- ***Deanonimizācijas uzbrukumi***
- ***Atkārtotas atskaņošanas uzbrukumi***
- ***Kvantu skaitļošanas uzbrukumi***
- ***Egoistiskā maininga uzbrukumi***
- ***Viedā līguma atkārtotas ielaušanās uzbrukumi***
- ***Citi riski/draudi***

- Drošības slānis
- "Lietu internets"

Tehnoloģija

[Ikbals [Iqbal] un Matulevičiuss [Matulevičius], 2019. gads]

Lielo datu ekosistēmās

	IZAICINĀJUMI
CILVĒCISKIE FAKTORI *Uzņēmējdarbība, informācija, sociālie un profesionālie aspekti*	Piekrišanas neesamība, Sociālā zināšanu ļaunprātīga izmantošana, neautorizēta piekļuve, datu plūdi, neatbilstošas analīzes, pieejamība, precizitāte
TEHNOLOĢIJAS *Lietotnes, platformas, datu infrastruktūra*	Vairāki datu lietojumi, tehnoloģiju nepilnības, saskaņots datu lietojums, dati, savlaicīgums, datu izcelsme, ierīču neviendabīgums, pieejamība, datu vākšanas pārvaldība un pārsūtīšana, datu veidi un formāti, nepilnīgi un nekonsekventi dati
OBJEKTI *Telpiskie; apkures, ventilācijas un gaisa kondic palīgobjekti*	Uzglabāšana un apstrāde Dažādi datu avoti, pieejamība
VIDE *Politiskā, apkārtējās vides, sociālā vide, tehnoloģiskā, juridiskā vide*	Pārvaldības trūkums, politika, likumi, organizatoriskā pretestība, uz datiem balstītas kultūras izveide

CyberPhish
Safeguarding your digital future

[Anvars [Anwar] un citi, 2021. gads]

Funded by the Erasmus+ Programme of the European Union

Lielo datu ekosistēmās

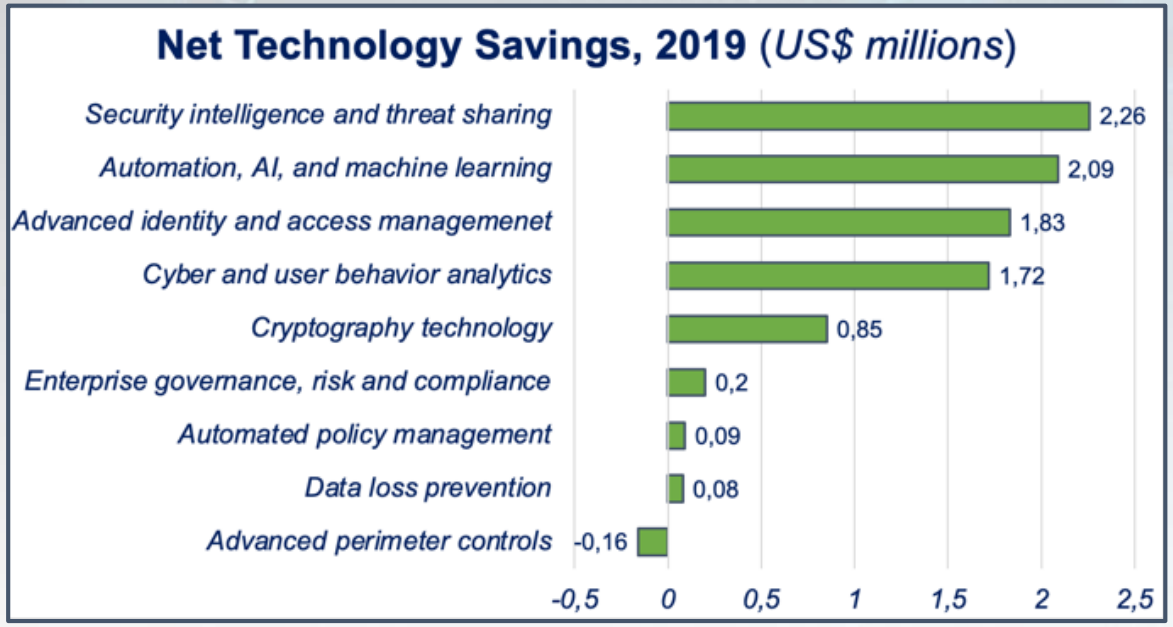
	SOLUTIONS
CILVĒCISKIE FAKTORI *Uzņēmējdarbība, informācija, sociālie un profesionālie aspekti*	Lietotāju apstiprināšana, prasmes, piekļuves kontrole, lietotāju izglītība, audits, sakaru drošība, draudu modelēšana, riska novērtējums, datu klasifikācija, uz datiem balstīta privātuma saglabāšana, privātums sociālajos tīklos
TEHNOLOĢIJAS *Lietotnes, platformas, datu infrastruktūra*	Gala punkta validācija un šifrēšana, droši vaicājumi, diferenciālā konfidencialitāte, latento datu konfidencialitāte, droša datu ievākšana, Uzglabāšana un transformācija, mašīnmācīšanās algoritmi, ielaušanās atpazīšana, datu anonimizācija
OBJEKTI *Telpiskie; apkures, ventilācijas un gaisa kond palīgobjekti*	Izplatīti datu avoti, dublēšana un atkopšana, šifrētas galvenes informācijas glabāšana
VIDE *Politiskā, apkārtējās vides, sociālā vide, tehnoloģiskā, juridiskā vide*	Pārvaldība un tiesiskais atbalsts

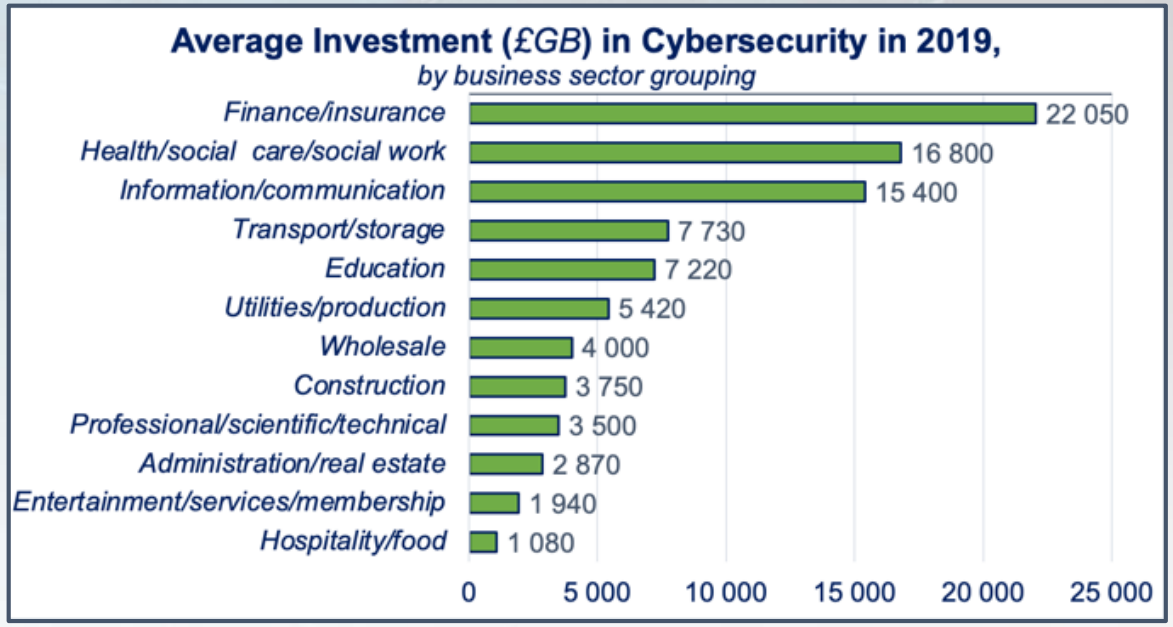
CyberPhish
Safeguarding your digital future

[Anvars [Anwar] un citi, 2021. gads]

Funded by the Erasmus+ Programme of the European Union

Investīcijas drošībai





Drošības izlūkošana un draudu kopīgošana *tiek ierindotas kā visbiežāk izmantotās drošības tehnoloģijas*

https://www.digitalmarketingcommunity.com/indicators/security-technologies-cost-saving-2019/

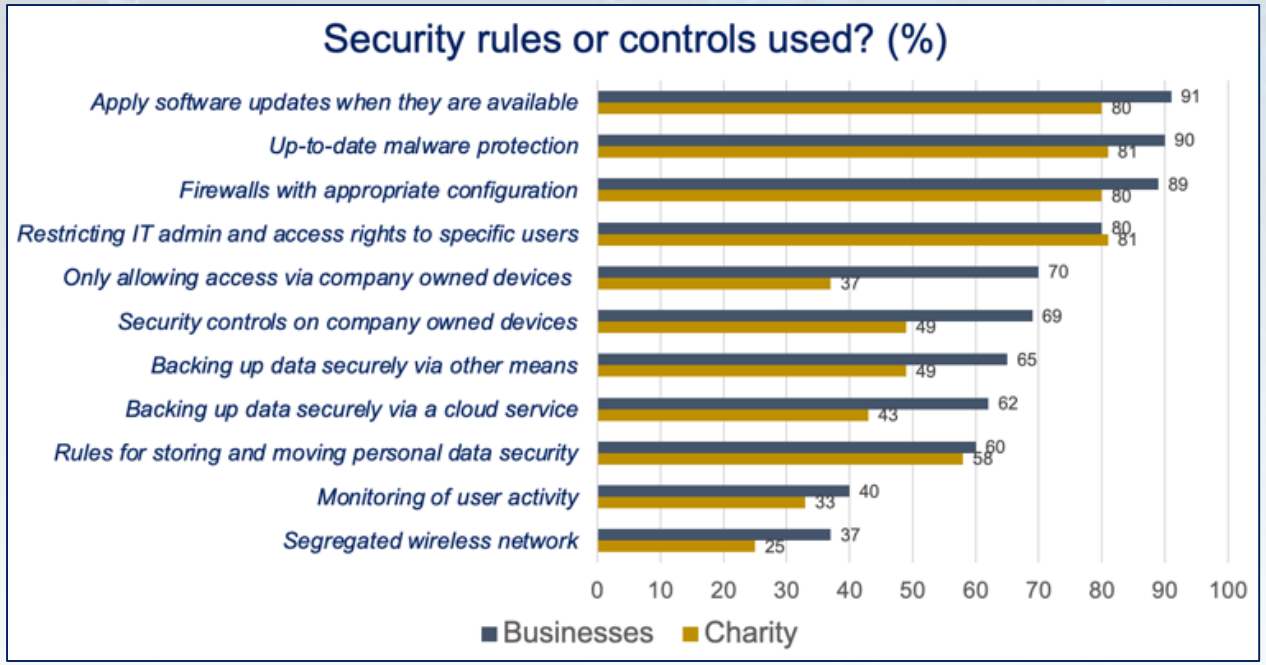
Finanses un apdrošināšana *tiek ierindotas kā galvenās uzņēmējdarbības nozares, kas investē kiberdrošībā*

https://www.digitalmarketingcommunity.com/indicators/cyber-security-investment-2019/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pieaugošu draudu izaicinājums



https://www.digitalmarketingcommunity.com/indicators/preventing-minimizing-cyber-security-2019/

- Nenoliedziet draudu pastāvēšanu – tas novedīs pie lielākām problēmām
- Prognozējiet, ka nejauši informācijas pārkāpumi būs biežāki nekā ļaunprātīgi uzbrukumi
- Negaidiet, lai veiktu darbības, līdz jums ir uzbrukts vai tiek nopludināta informācija
- Veiciet vadlīniju un politiku ieviešanu pastāvīgi
- Pievērsiet uzmanību kultūras jautājumiem dažādos līmeņos
- Sabalansējiet ieguldījumus starp ārējiem un iekšējiem draudiem
- Akceptējiet teicienu *"mācīties, mācīties, mācīties"!*

[Kolvils [Colwill], 2009. gads]

Nāciju valstu draudi

- Kiberspiegošanas mērķi
  - *Rūpniecības nozares*
  - *Kritiskās un stratēģiskās infrastruktūras*
  - *Valdības struktūras*
  - *Dzelzceļi*
  - *Telekomunikāciju pakalpojumu sniedzēji*
  - *Enerģētikas uzņēmumi*
  - *Slimnīcas*
  - *Bankas*

Datu pārkāpumi, kurus motivē kiberspiegošana

20%

Ļaunprātīgi aktīvisti, kas saistīti ar specifiskām nāciju valstīm

38%

Incidenti, kurus motivē kiberspiegošana

11,2%

Kiberspiegošanas incidenti, kas saistīti ar pikšķerēšanu

63%

ENISA Apdraudējumu reljefa pārskats 2018., 2020. gads

Nāciju valstu draudi

- Kiberspiegošana koncentrējas uz sekojošo:
  - *ģeopolitisko aspektu veicināšanu noteiktos virzienos;*
  - *valsts un komercnoslēpumu zagšanu;*
  - *intelektuālajām īpašumtiesībām;*
  - *patentētu informāciju stratēģiskās jomās.*

- 2019. gadā *palielinājās nāciju valstu atbalstīto kiberuzbrukumu skaits, kas vērsti pret ekonomiku, un tas, visticamāk, turpināsies*

- Pieaug nāciju valstu sponsorēti uzbrukumi rūpnieciskajam lietu internetam (IIoT) sekojošās nozarēs:
  - *komunālie pakalpojumi;*
  - *naftas un dabasgāzes ieguvē un pārstrādē;*
  - *ražošanas industrijā.*

Nezināma autora fotoattēls, licencēts saskaņā ar CC BY-NC

Nāciju valstu draudi

- Kiberspiegošana koncentrējas uz sekojošo:
  - *ģeopolitis*
    veicināša
  - *valsts un*
    zagšanu;
  - *intelektuā*
  - *patentētu*
    stratēģ
- 2019. gadā
  palielinājās nāciju valstu atbalstīto
  vērsti pret
  āk,
  rēti
  ietu
  nozarēs:
  umi;
  es ieguvē
  uzņēmumus industrijā.

Nosakiet svarīgākās lomas organizācijā un novērtējiet to pakļautību spiegošanas riskiem

Izveidojiet drošības politikas un vadlīnijas

Izveidojiet korporatīvo praksi, lai komunicētu un apmācītu darbiniekus

Izstrādājiet novērtēšanas kritērijus (KPI), lai veiktu darbības salīdzinošo novērtēšanu

Izveidojiet svarīgu lietojumprogrammu un pakalpojumu "balto" (atļauto) sarakstu

Novērtējiet ievainojamības un regulāri labojiet un atjauniniet programmatūru

Ieviesiet piekļuves tiesību noteikšanas principu saskaņā ar attiecīgās personas nepieciešamību iegūt attiecīgo informāciju

Izveidojiet satura filtrēšanu visiem ienākošajiem un izejošajiem kanāliem

Nezināma autora fotoattēls, licencēts saskaņā ar CC BY-NC

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kopsavilkums

- Uzņēmējdarbības izaicinājumi
- Kiberdrošības uzbrukumu pieaugums
- Tehnoloģiju izmantošana un drošības izaicinājumi
- Pieaugošu draudu izaicinājums
- Nāciju valstu draudi

Funded by the Erasmus+ Programme of the European Union

Uzdevumi

Pārrunājiet, kāds ir otrs lielākais biznesa izaicinājums (*protams, pēc informācijas drošības*)

Kas, jūsuprāt, ir visbīstamākais drošības apdraudējums/uzbrukums?

Vai savā ikdienā izmantojat kādu (mobilo) tehnoloģiju? Kuru? Vai tā ir droša?

Vai zināt vai esat lasījis par nāciju valsts draudiem? Vai varat pastāstīt par to un paskaidrot, kā tas notiek?

Funded by the Erasmus+ Programme of the European Union

Papildu lasīšana

Šīs lekcijas sagatavošanā izmantotie materiāli

- **Abjoduns O. I. A.** *[Abiodun O. I. A.]*, **Abjoduns E. O.** *[Abiodun E. O.]*, **Alavida M.** *[Alawida M.]*, **Alkavaldess R. S.** *[Alkhawaldeh R. S.]*, **Aršads H.** *[Arshad H.]*, (2021). Lietu interneta drošības apsvērumu pārskats: Izaicinājumi un risinājumi. *Bezvadu personīgā komunikācija 119:2603–2637 https://doi.org/10.1007/s11277-021-08348-9*

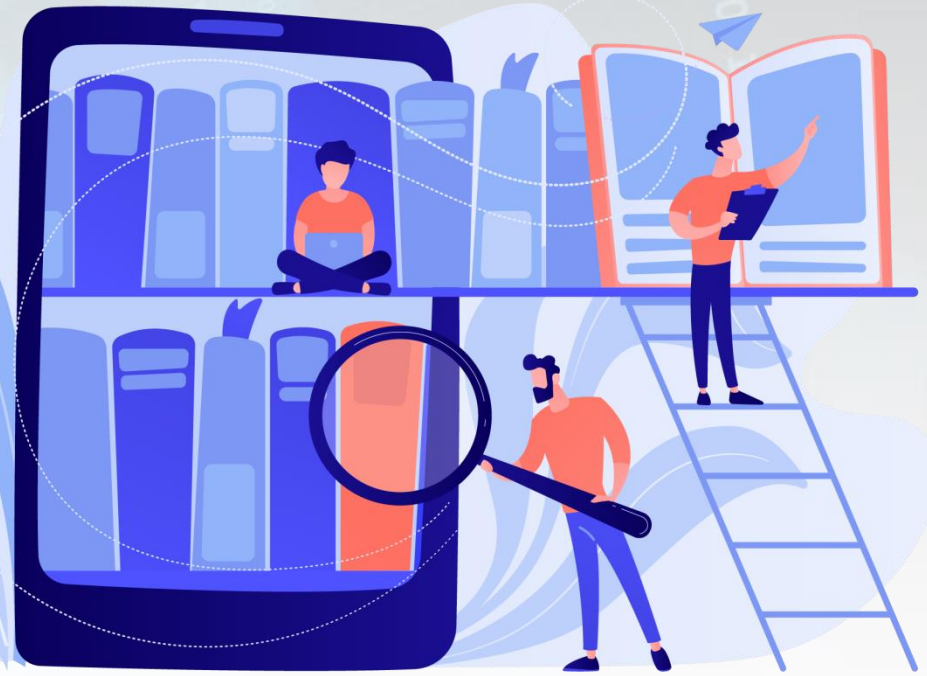
- **Afija A. A. O.** *[Affia A-A. O.]*, **Matulevičius R., Nolte A.** *[Nolte A.]* **(2019. gads)**: Drošības risku pārvaldība kooperatīvās inteliģentās transporta sistēmās: Sistemātisks literatūras apskats. *Paneto H.[Panetto H.] un citi (redakcija), LNCS 11877, CoopIS 2019, Springer*

- **Anvars M. Dž.** ***[Anwar M. J.]*****; Džils A. K.** ***[Gill A. Q.]*****; Huseins F. K.** ***[Hussain F. K.]*****; Imrans M.** ***[Imran M.]*** **(2021. gads),** Droša lielo datu ekosistēmas arhitektūra: izaicinājumi un risinājumi. *J Bezvadu sakaru tīkls 2021:130 https://doi.org/10.1186/s13638-021-01996-2*

- **Kolvils C.** *[Colwill C.]* (2009. gads) Cilvēciskie faktori informācijas drošībā: Iekšējie draudi. Kam mūsdienās var uzticēties? *Informācijas drošības tehniskais ziņojums 14,186-196*

- **Ikbals** *[Iqbal]* **un Matulevičiuss** *[Matulevičius]*, **2019. gads** Uz blokķēdes tehnoloģijām balstīts lietotņu drošības risks: Sistemātisks literatūras apskats, CAiSE 2019 dokumenti. Starptautiskās darbnīcas, 2019. gada sesija, LNBIP 349, 176-188

- **Kominoss N.** *[Komninos N.]*, **Filipū E.** *[Philippou E.]*, **Pitsilidess A.** *[Pitsillides A.]* (2014. gads) Aptauja par viedajiem tīkliem un viedo māju drošību: Problēmas, izaicinājumi un pretpasākumi, IEEE saziņas aptaujas un apmācības, 16(4)



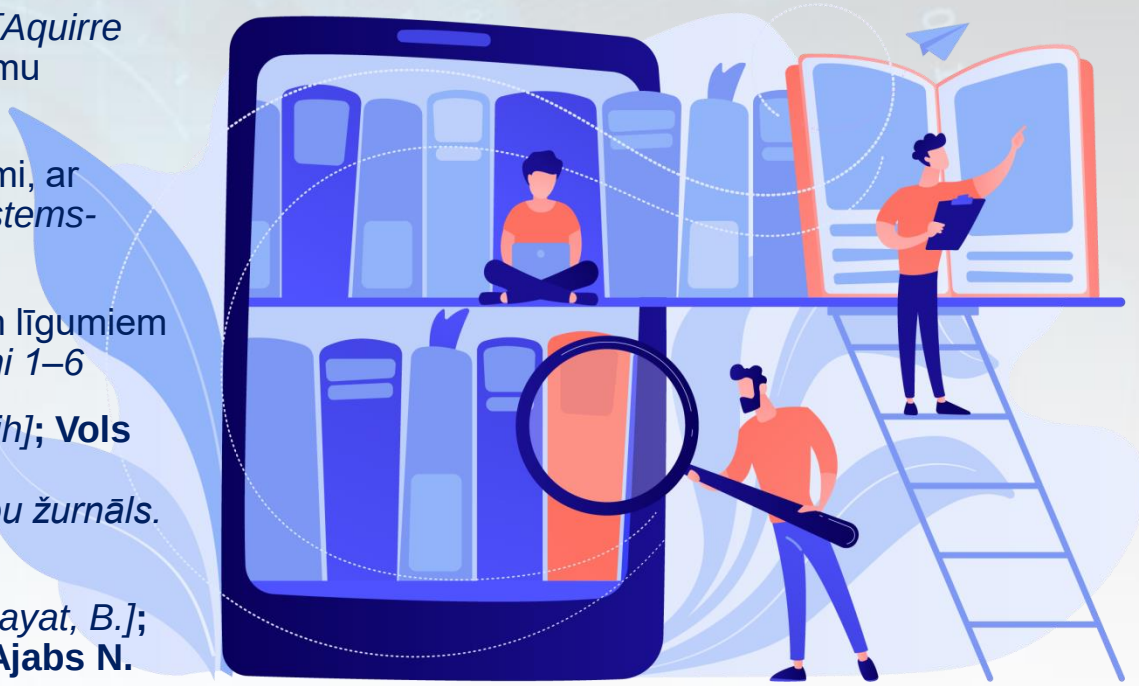
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Papildu lasīšana

Šīs lekcijas sagatavošanā izmantotie materiāli

- **Lūiss A.** *[Lewis, A.]* **(2015. gads)**: Blokķēdes tehnoloģijas skaidrojums (2015. gads). *http://www.blockchaintechnologies.com/blockchain-definition*
- **Orantess – Himenezs A. D.** *[Orantes-Jimenez A. D.]* un **Akire E.** *[Aquirre E.]*, 2020. gads: Aptauja par informācijas drošību mākoņpakalpojumu sistēmās, *Computacion y Sistemas* 24(2)
- **R. Perdomo** *[R. Perdomo]* (2021. gads): 15 Tehnoloģiju izaicinājumi, ar kuriem uzņēmumi var saskarties 2021. gadā, saite: *https://blog.systems-x.com/author/rubens-perdomo*
- **Sato T.** *[Sato, T.]***, Himura J.** *[Himura, Y.]* **(2018. gads)**: Uz viediem līgumiem balstītas sistēmas atļautas darbības blokķēdei. *NTMS 2018, sējumi 1–6*
- **Šacs** *[Schatz]***, Daniels Bešrušs** *[Daniel; Bashroush]***, Rabai** *[Rabih]***; Vols** *[Wall]***, Džūlijs** *[Julie]* **(2017).** Ceļā uz lielākā mērā reprezentatīvu kiberdrošības definīciju. *Digitālās kriminālistikas, drošības un tiesību žurnāls. 12 (2).*
- **Tahirkeli A. I.** *[Tahirkheli, A.I.]***; Širazs M.** *[Shiraz M.]***; Hajats B.** *[Hayat, B.]***; Idrīss M.** *[Idrees, M.]***; Sadžīds A.** *[Sajid, A.]***; Ullas R.** *[Ullah, R.]***; Ajabs N.** *[Ayub, N.]***; Kims K. I. A.** *[Kim, K.-I. A.]* (2021). Aptauja par mūsdienu mākoņdatošanas drošību viedajos pilsētu tīklos: Draudi, ievainojamības, sekas, pretpasākumi un izaicinājumi. *Elektronika 2021,10,1811. https://doi.org/10.3390/electronics10151811*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Īsi video

- Biznesa tehnoloģiju tendences
  https://youtu.be/DOAnYtqhXBU
- Lietu interneta drošība
  https://youtu.be/IQkRscixagM
- Mākoņpakalpojumu kiberdrošība
  https://youtu.be/k2684fuzHLs
- Jūsu mājas informācijas sistēmu uzlaušana
  https://youtu.be/iRQPfISsG9k
- Ievads blokķēdes drošībā
  https://youtu.be/dl8Hl91siM8
- Lielo datu drošības problēmas
  https://youtu.be/3xIuIcPzMVs
- Kādi ir pašreizējie datu drošības draudi?
  https://youtu.be/WugGZaT2oHE
- 7 populārākie elites nāciju valstu hakeri
  https://youtu.be/S_IPgHbondk

Pateicamies!