Funded by the
Erasmus+ Programme
of the European Union

Kibernetinio saugumo įvadas

Ketvirtosios pramonės revoliucijos iššūkiai

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

Mokymo tikslai

- Supažindinti su kibernetinio saugumo sąvoka ir iššūkiais, su kuriais susiduria įmonės.
- Įvardinti kibernetinių atakų iššūkius, su kuriais asmenys ir įmonės susiduria ketvirtosios pramonės revoliucijos amžiuje.

CyberPhish
Safeguarding your digital future

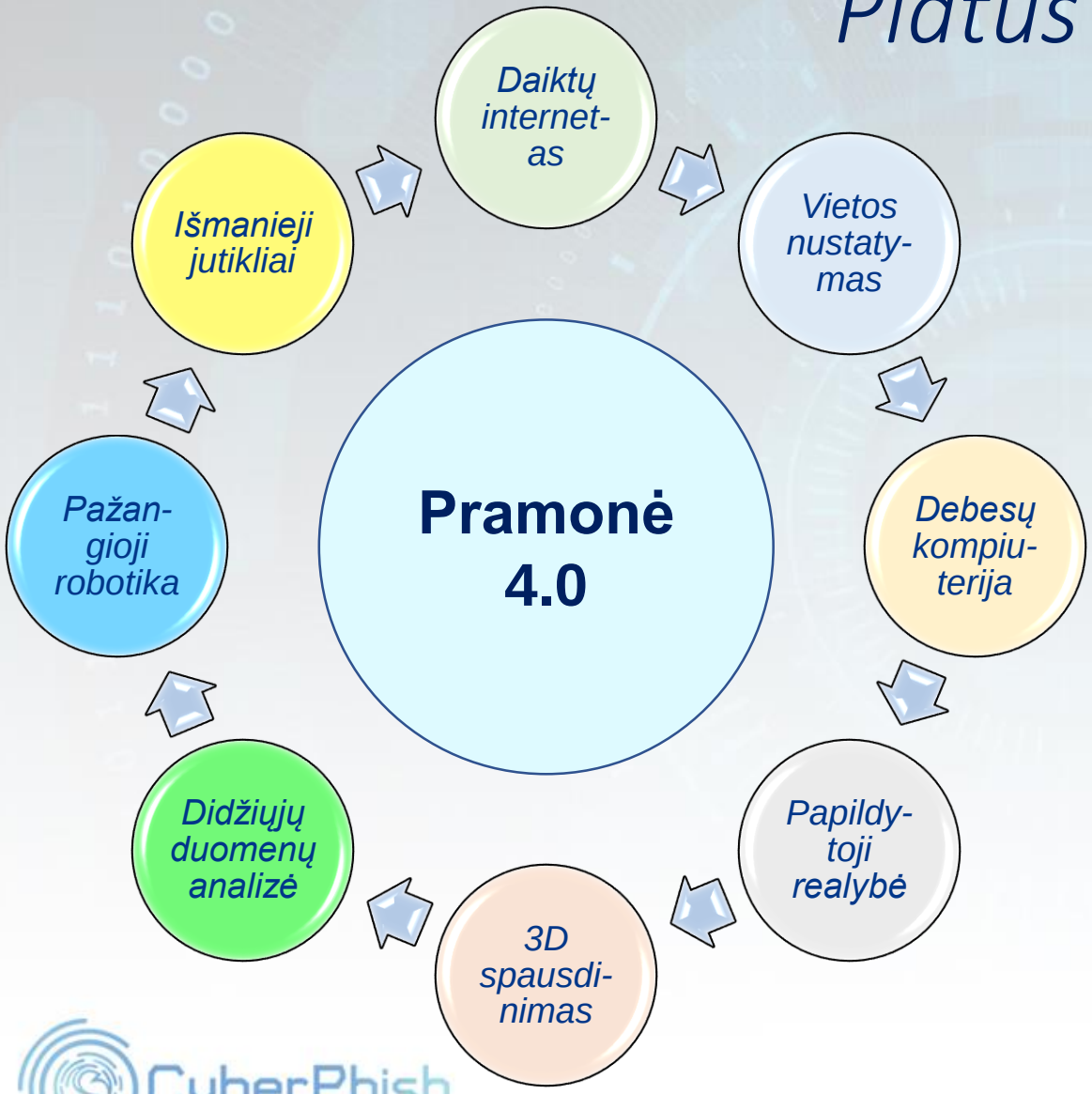
Funded by the Erasmus+ Programme of the European Union

Studento darbo krūvis

Paskaitos	1,5 val.
Garso ir vaizdo medžiaga	1,5 val.
Panaudojimo atvejai	1,5 val.
Papildomi skaitiniai	4 val.
Pasiruošimas atsiskaitymui	1,5 val.

Funded by the Erasmus+ Programme of the European Union

Platus technologijų naudojimas



Programinė įranga ir informacinės sistemos atlieka svarbų vaidmenį įvairiose žmogaus gyvenimo srityse.

Poreikis apsaugoti informaciją tampa ne galimybe, o būtinybe.

[Abiodun et al., 2021]

Apibrėžimas

Kibernetinis saugumas

Dar kitaip žinomas kaip,

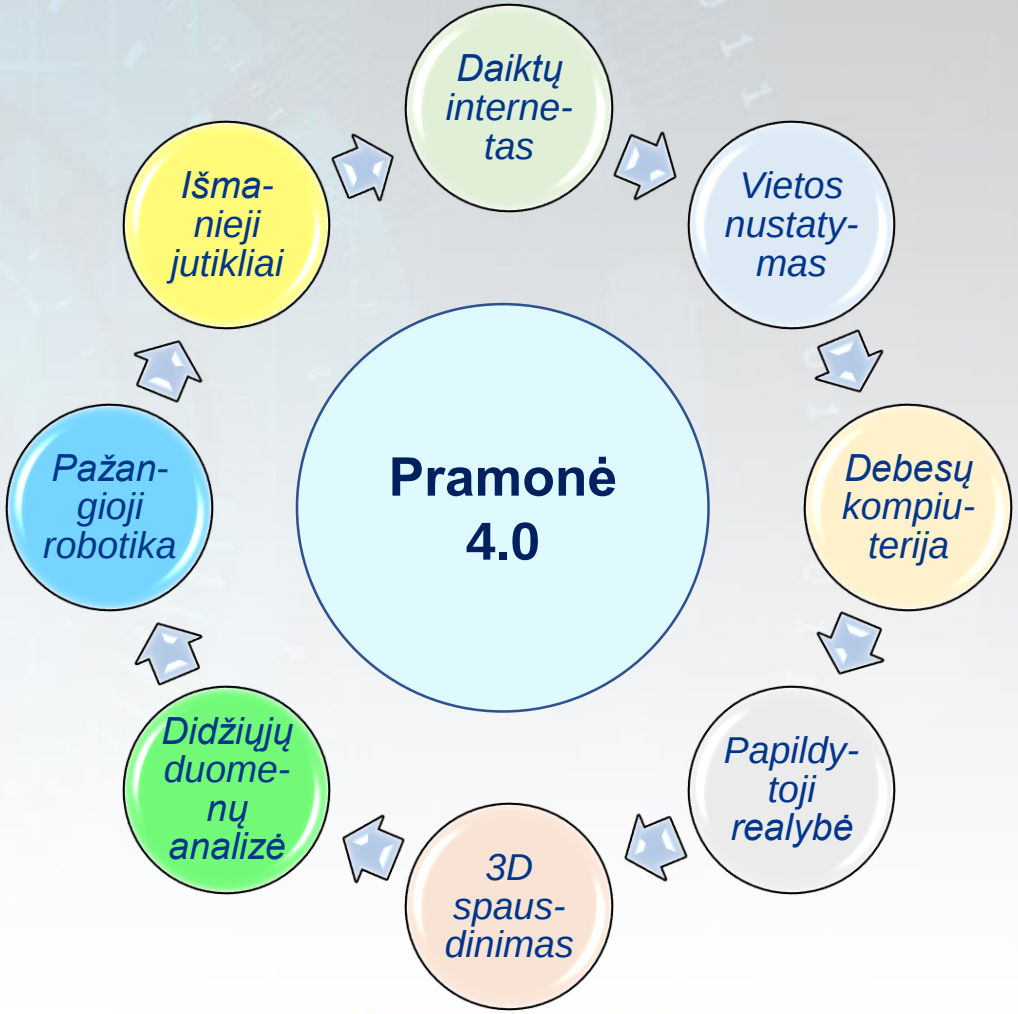
Kompiuterių saugumas, informacinių technologijų saugumas** arba **IT saugumas

Požiūris ir veiksmai, susiję su saugumo rizikos valdymo procesais, kurių laikosi organizacijos ir valstybės, siekdamos užtikrinti kibernetinėje erdvėje naudojamų duomenų ir turto konfidencialumą, vientisumą ir prieinamumą. Ši sąvoka apima gaires, politiką ir apsaugos priemonių, technologijų, priemonių ir mokymų rinkinius, siekiant užtikrinti geriausią kibernetinės aplinkos ir jos naudotojų būklės apsaugą.

[Schatz et al. 2017]

Turinys

- Verslo iššūkiai
- Kibernetinio saugumo atakų augimas
- Technologijų naudojimas ir saugumo iššūkiai
  - Daiktų internetas
  - Debesų kompiuterija
  - Išmanioji infrastruktūra
  - Išmanieji namai
  - Blokų grandinės technologija
  - Didieji duomenys
- Didėjančių grėsmių iššūkis
- Nacionalinės valstybės grėsmės



Verslo iššūkiai

- Skaitmeninė transformacija
- Debesys
- Atitiktys
- Automatizacija
- Daiktų internetas
- Integracija ir atnaujinimai
- Dirbtinis intelektas ir mašininis mokymas

- Nuotolinio darbo pagalba
- Duomenų valdymas
- Dėmesys mobilumui
- Socialinė žiniasklaida
- Projektų valdymas
- Infrastruktūros pokyčiai
- Techninių mokymų trūkumas

CyberPhish
Safeguarding your digital future

[Perdomo, 2021]

Funded by the Erasmus+ Programme of the European Union

Verslo iššūkiai

- Skaitmeninė transformacija
- Debesys
- Atitiktys
- Automatizacija
- Daiktų interne
- Integracija ir at
- Dirbtinis intelek
  mašininis moky

- Nuotolinio darbo pagalba
- Duomenų valdymas
- esys mobilumui
- nė žiniasklaida
- jektų valdymas
- ktūros pokyčiai
- kymų trūkumas

Trečiųjų šalių rizika – rizika, kylanti dėl organizacijos ryšių su išorės šalimis, teikiančiomis su verslu susijusias prekes ar paslaugas.

- *Reguliavimo / atitikties rizika*
- *Finansinė rizika*
- *Veiklos rizika*
- *Reputacijos rizika*
- *Strateginė rizika*

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

[Perdomo, 2021]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Verslo iššūkiai

- Skaitmeninė transformacija
- Debesys
- Atitiktys
- Automatizacija
- Daiktų internetas
- Integracija ir atnaujinimai
- Dirbtinis intel
  mašininis mok

- Nuotolinio darbo pagalba
- Duomenų valdymas
- Dėmesys mobilumui
- Socialinė žiniasklaida
- Projektų valdymas
- Infrastruktūros pokyčiai
- rūkumas

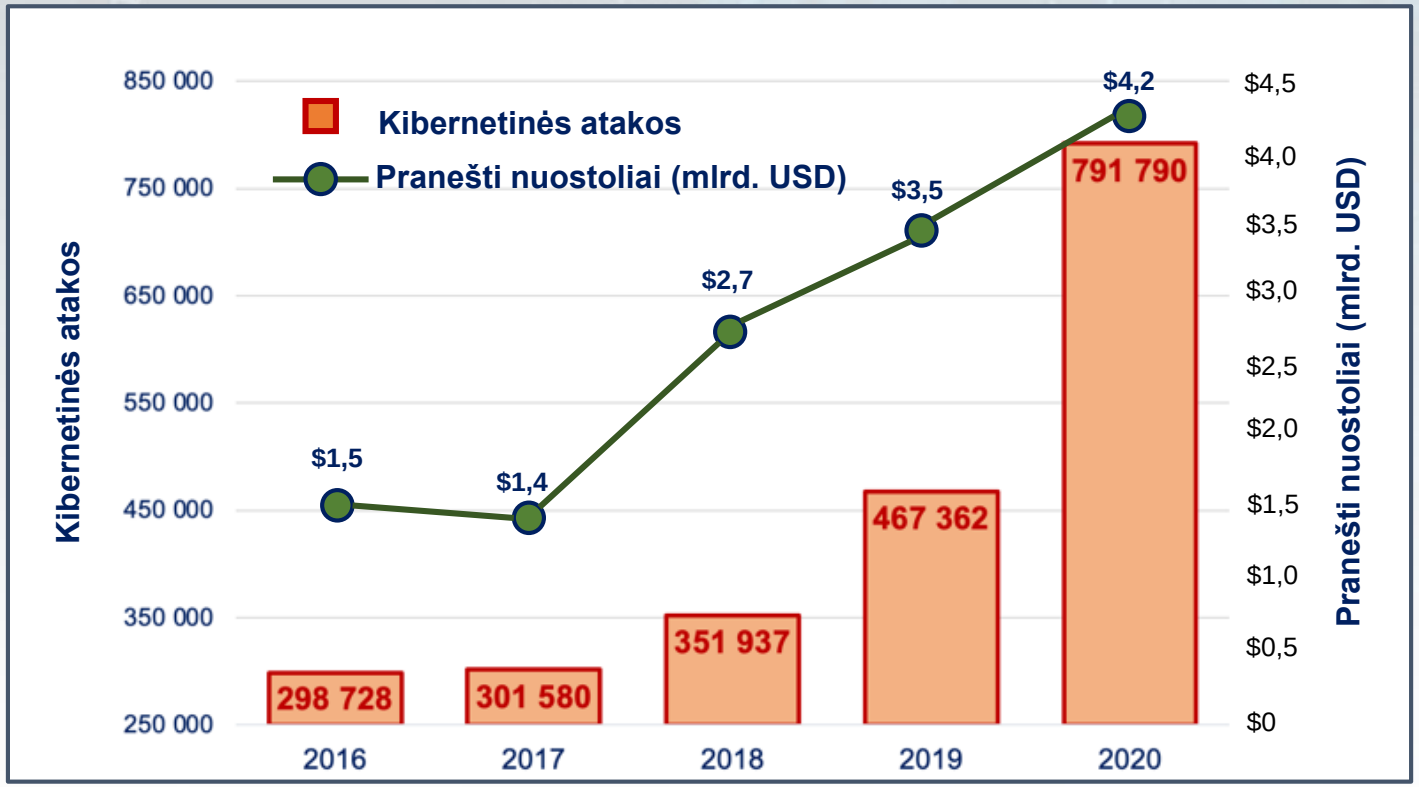
Informacijos saugumas

[Perdomo, 2021]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų augimas

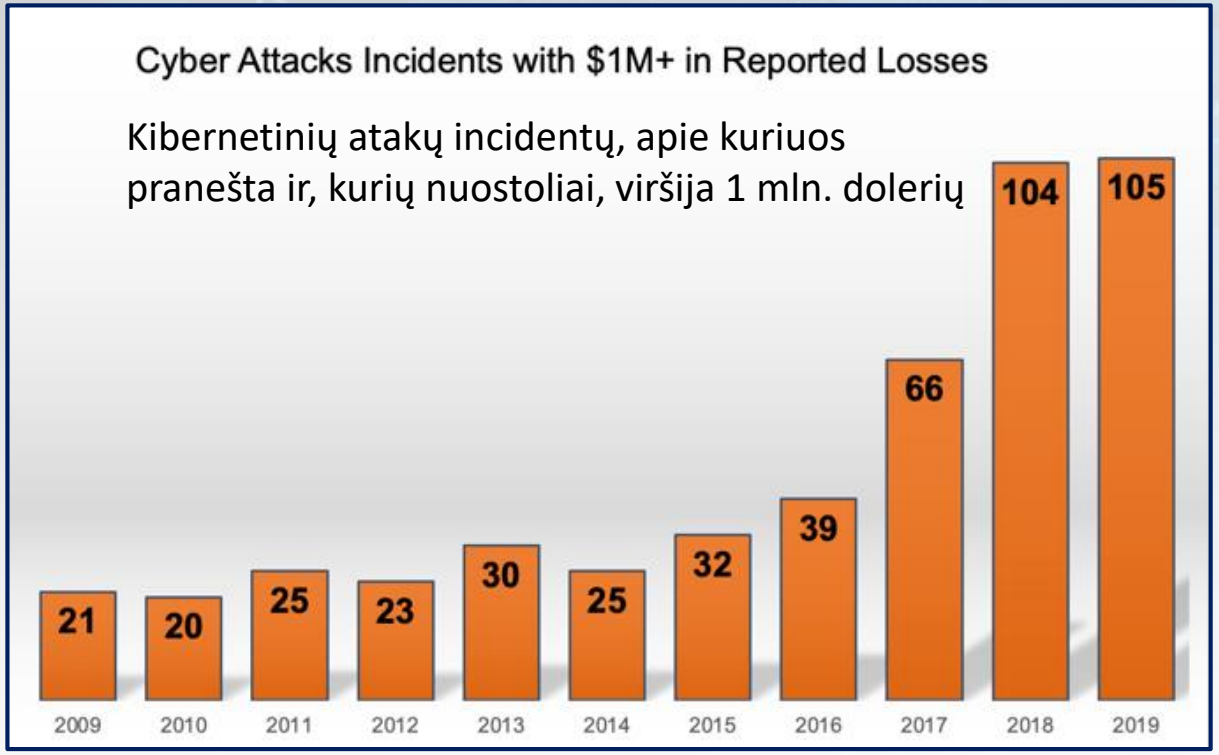


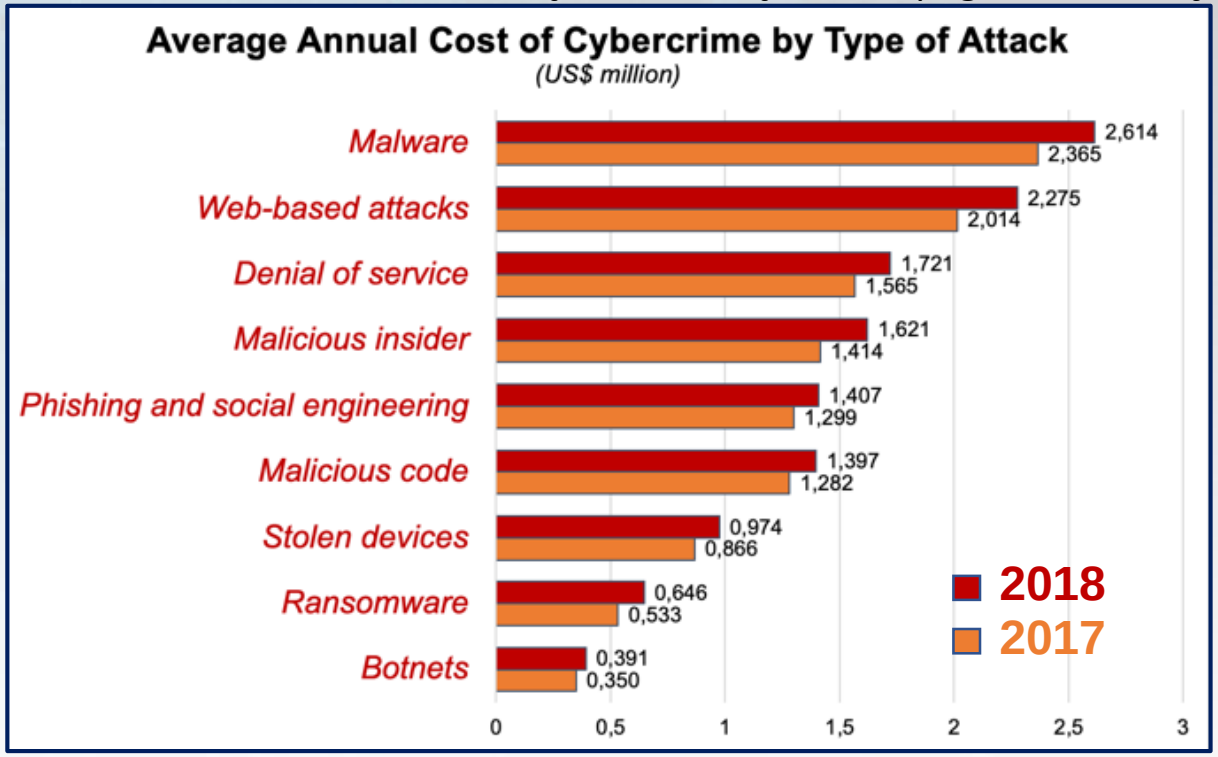
- *Taikomasi į žmones*
- *Atliekami namų darbai (pasiruošimas atakai)*
- *Tai yra skaičių žaidimas*
- *Sukčiai nuolat tobulėja*
- *Nusikaltėliai parduoda pavogtą informaciją*
- *Kantrybė ir atkaklumas atsiperka*
- *Nusikaltėliai gali veikti iš bet kurios vietos*

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

Kibernetinių atakų kaina

Vidutinės metinės kibernetinių nusikaltimų išlaidos pagal atakos rūšį





Per pastarąjį dešimtmetį – **490** reikšmingų kibernetinių incidentų

2018 viso = **13** mln. USD

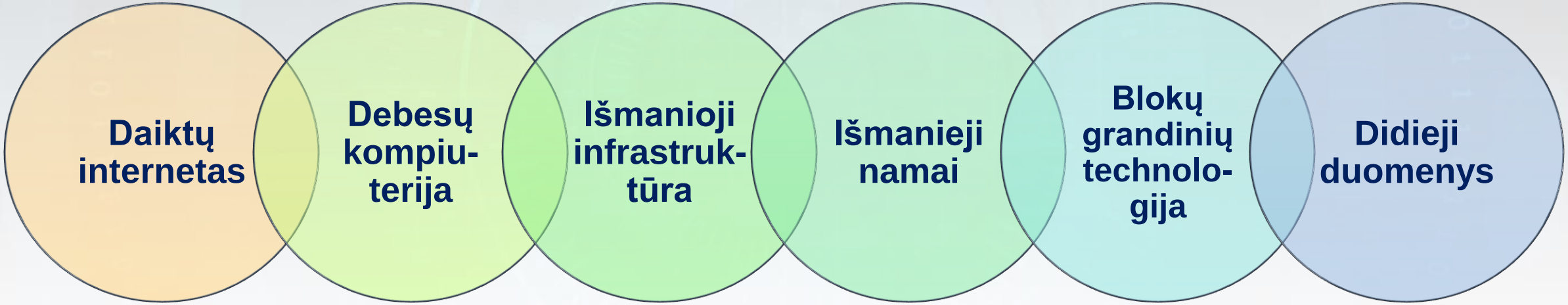
https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Platus mobiliųjų technologijų naudojimas



Daiktų internetas

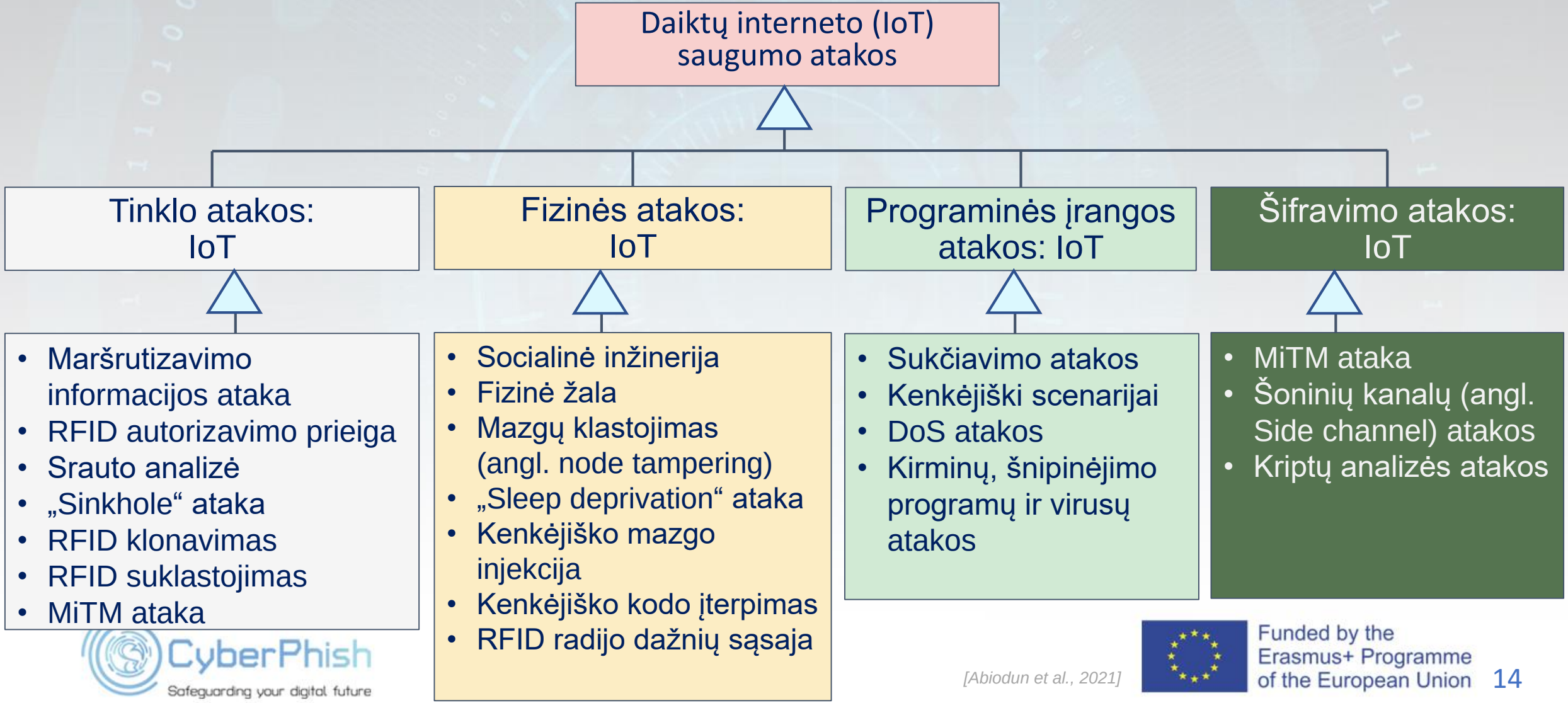
Daiktų internetas (IoT) apibūdina fizinių objektų, kuriuose įmontuoti jutikliai, programinė įranga ir kitos technologijos, tinklą, skirtą sujungti ir keistis duomenimis su kitais prietaisais ir sistemomis internetu

- *Daiktai, t. y. technologijos, prietaisai, objektai, gyvūnai ar žmonės.*
- *Ryšių tinklai, jungiantys įrenginį*
- *Kompiuterių tinklai per duomenų srautą iš interneto į įrenginį*

Metai	***Pasaulio gyventojų skaičius*** *(milijonais)*	***IoT prijungti įrenginiai*** *(milijardais)*	***Santykis***
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

[Abiodun et al., 2021]

Daiktų internetas



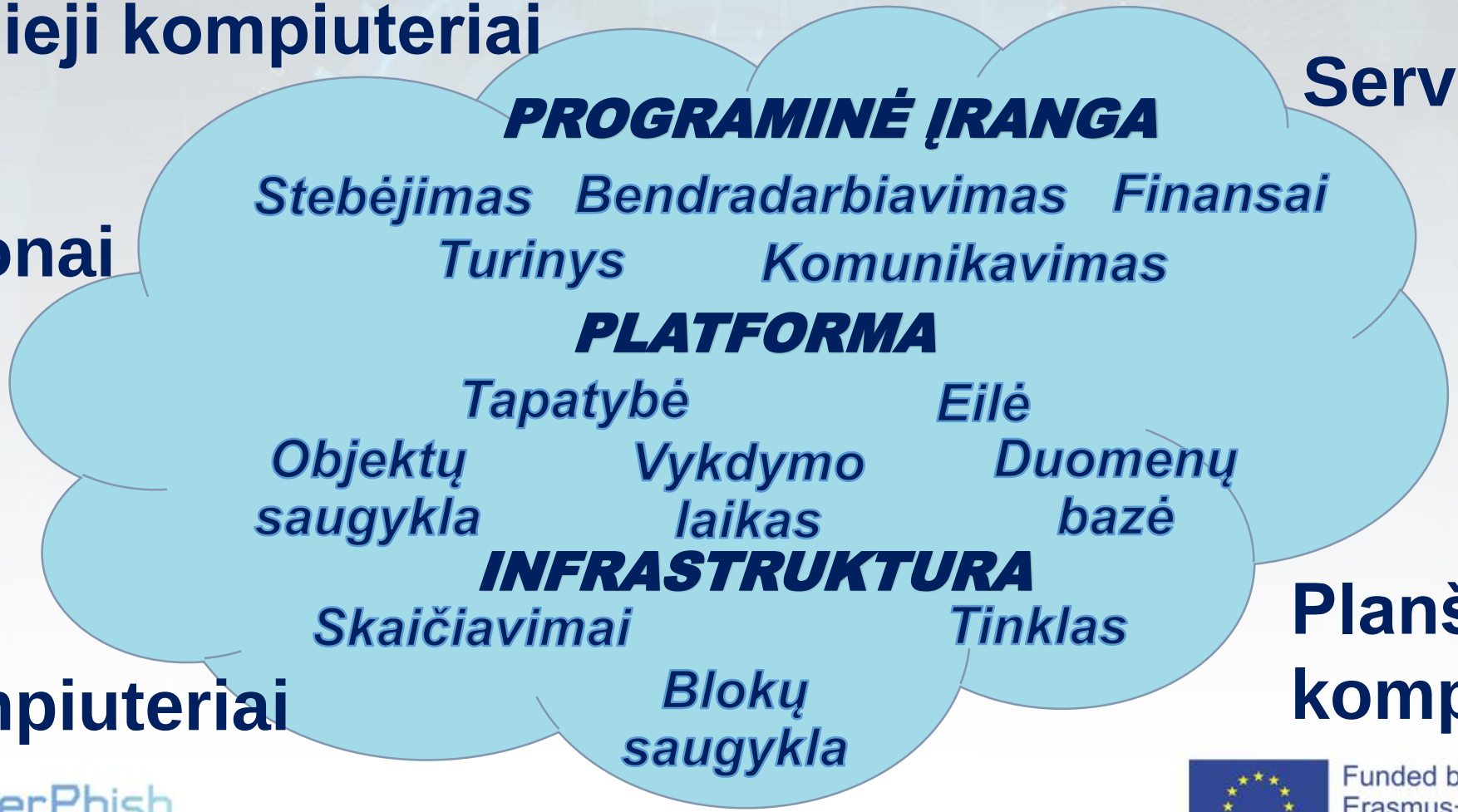
[Abiodun et al., 2021]

Debesų kompiuterija

Nešiojamieji kompiuteriai

Serveriai

Telefonai



Kompiuteriai

Planšetiniai kompiuteriai

[Tahirkheli at al., 2021]

Funded by the Erasmus+ Programme of the European Union

Debesų kompiuterija

Nešiojamieji kompiuteriai

Serveriai

Telefonai

Piktnaudžiavimas ir netinkamas naudojimasis debesų kompiuterija

Sąsajos ir nesaugi API

Vidinės grėsmės

Problemos, kylančios dėl bendrinamų technologijų

Informacijos praradimas arba nutekėjimas

Sesijos ar paslaugos užgrobimas

Rizika dėl žinių trūkumo

Planšetiniai kompiuteriai

Kompiuteriai

[Orantes-Jimenez and Aquirre, 2020]

Funded by the Erasmus+ Programme of the European Union

Išmaniosios sistemos

SUVOKIMO SLUOKSNIS

- Jutikliai
- Rega
- Padėties nustatymas
- Paleidimas / iniciavimas

TINKLO SLUOKSNIS

- Transporto priemonėje
- Transporto priemonė į transporto priemonę
- Transporto priemonė į infrastruktūrą

TAIKYMO SLUOKSNIS

- Kompiuterija / serveris
- Duomenų saugojimas
- Žmogus

[Affia at al., 2019]

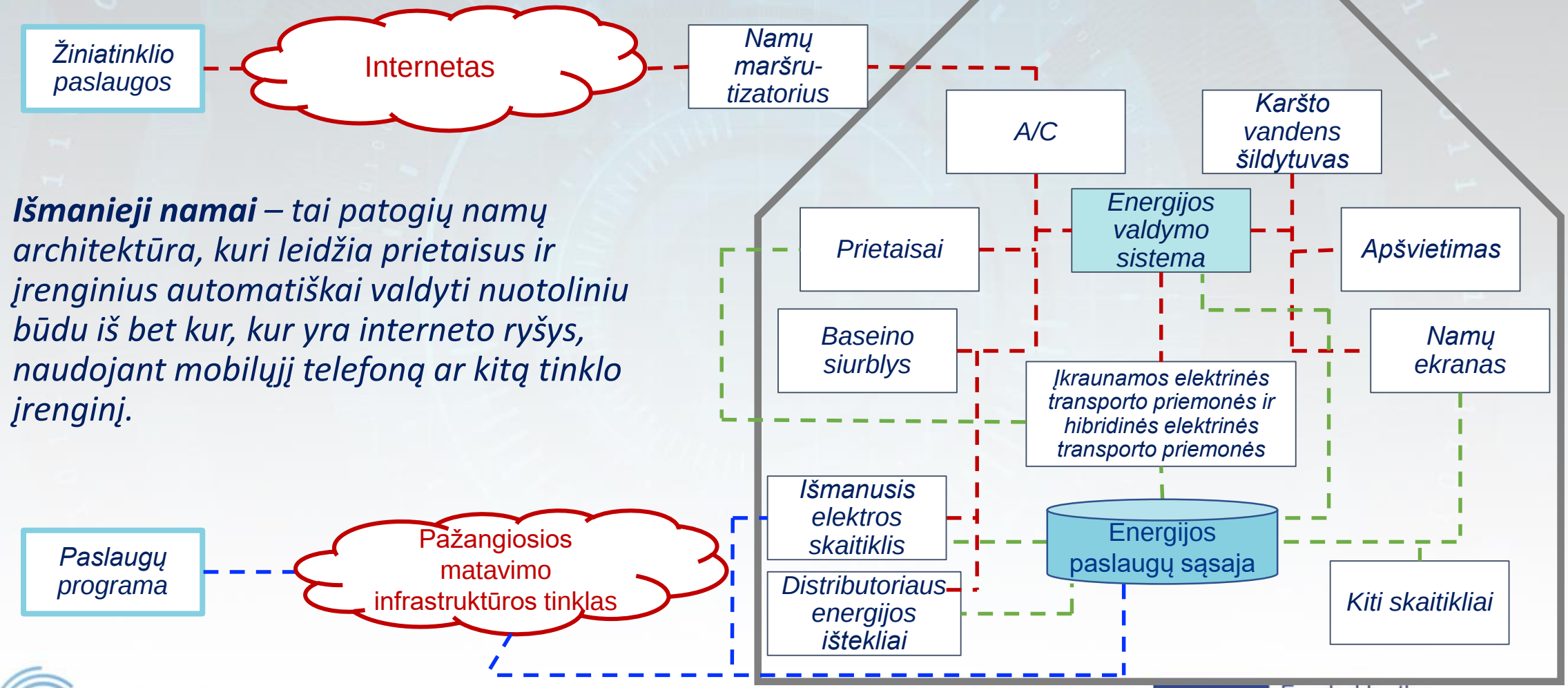
Funded by the Erasmus+ Programme of the European Union

	SAUGUMO GRĖSMĖS					
Sistemų turtas	*Apsimetinėjimas kitu* ***S****poofing*	*Klastojimas* ***T****ampering*	*Išsižadėjimas* ***R****epudiation*	*Informacijos atskleidimas* ***I****nformation disclosure*	*Paslaugos ribojimas* ***D****enial of service*	*Privilegijų suteikimas* ***E****levation of privileges*
Jutimo, padėties nustatymo, regos technologijos	Apsimetinėjimas kitu, Mazgo apsimetinėjimas, Iliuzija, Pakartojimas, Apgaulingų pranešimų siuntimas, Maskavimas	Klastotės, Manipuliavimas duomenimis, Klastojimas, Rodmenų klastojimas, Žinutės injekcija	Apgaulingas pranešimas	Išsaugotos atakos, Slaptas duomenų stebėjimas	pranešimų prisotinimas, Slopinimas, Paslaugų ribojimas (DoS), Sistemos sutrikdymas	„Užpakalinės durys“, Neteisėta prieiga, Privilegijos suteikimas, Nuotolinis ECU atnaujinimas
Transporto priemonėje esantis tinklas, Transporto priemonė - transporto priemonei (V2V), Transporto priemonė - infrastruktūrai (V2I)	„Sybil“, Apsimetinėjimas kitu, Pakartojimo ataka, Maskavimas, Pirštų atspaudai, „Wormhole“, Maskuojamoji ataka, Apsimetimo ataka	Laiko atakos, Injekcijos, Manipuliavimas, Maršrutizavimo manipuliacijos, Klastojimas, Padirbinėjimas, Kenkėjiškas atnaujinimas	Apgaulingi pranešimai, Nesąžiningas atmetimas, Įvykių atsekamumo praradimas	Informacijos atskleidimas, MiTM, ID atskleidimas, Buvimo vietos sekimas, Žinučių perėmimas, Informacijos atskleidimas	DoS/DDoS, šlamštas, Trukdymas, Dirbtinis srauto sudarymas, Pranešimų slopinimas, Kanalo trukdžiai, „Black hole“	Kenkėjiška programinė įranga, „Brute Force“, Kontrolės gavimas, Socialinė inžinerija, Loginės atakos, Netesėta prieiga, Sesijos užgrobimas
Taikomųjų programų serveris, Kraštinis duomenų centras, Žmogus	Apsimetinėjimas kitu, „Sybil“, Iliuzijos ataka	Kenkėjiškas atnaujinimas	--	Buvimo vietos sekimas, Slaptas duomenų stebėjimas, Privačių duomenų nutekėjimas	Paslaugos ribojimas	„Jail-breaking OS“, Socialinė inžinerija, „Roque data-center“, Kenkėjiška programinė įranga

Saugumo iššūkiai

Išmaniojo namo sistemos

Išmanieji namai *– tai patogių namų architektūra, kuri leidžia prietaisus ir įrenginius automatiškai valdyti nuotoliniu būdu iš bet kur, kur yra interneto ryšys, naudojant mobilųjį telefoną ar kitą tinklo įrenginį.*



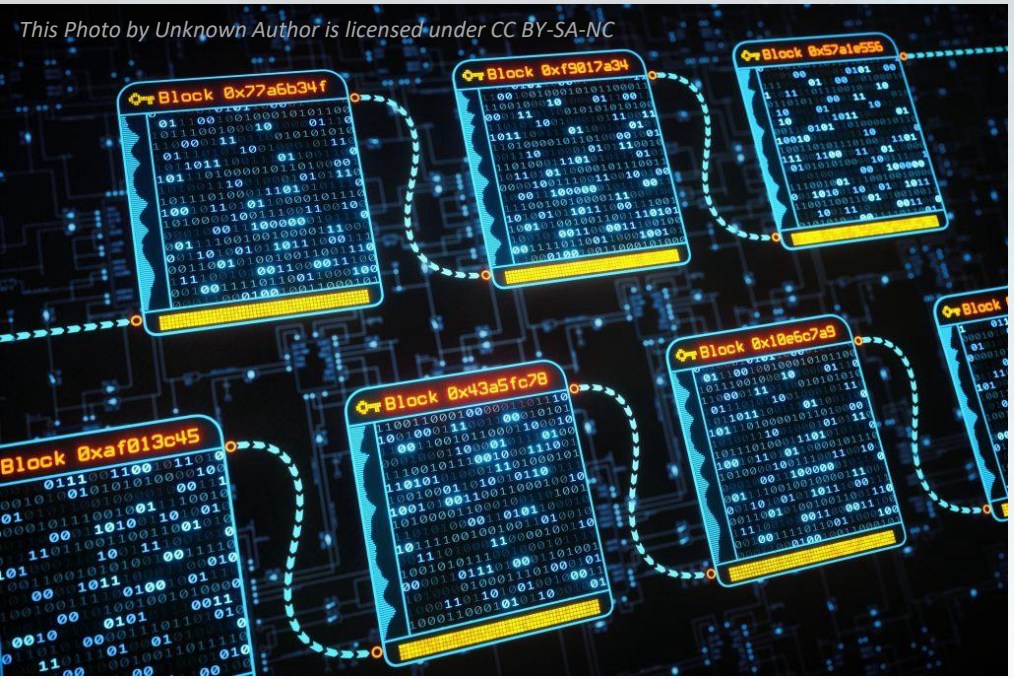
[Komninos et al., 2014]

Saugumo iššūkiai

Išmaniojo namo sistemos

Scenarijus	**Galima grėsmė** (N – tinklo sritis, SH – išmaniųjų namų konceptas)	**Pažeistas saugumo kriterijus**
AS1: Atakos, keliančios grėsmę sėkmingam prietaiso energijos suvartojimo ataskaitų teikimui	Pasiklausymas (N), Duomenų srauto analizė (N), Pranešimų keitimas (N), Pakartotinė ataka (N), Apsimetimas energijos valdymo sistema (SH)	Konfidencialumas, vientisumas, autentiškumas
AS2: Atakos, nukreiptos į energijos importo/eksporto signalus, į energijos paslaugų sąsają arba namų tinklą	Išsižadėjimas (N), Pranešimo pakeitimas (N), Pakartotinė ataka (N)	Neišsižadėjimas, vientisumas, autentiškumas
AS3: Fizinis poveikis skaitikliui, rodmenų atsukimas arba pašalinimas	Apskaitos prietaiso falsifikavimas/atsukimas, skaitiklio pašalinimas (SH), neteisėtas programinės įrangos keitimas/atnaujinimas (SH)	Autentiškumo nustatymas, vientisumas
AS4: Atakos, nukreiptos į nuotolinį namų stebėjimą ir valdymą	Apsimetimas klientu (N), Apsimetimas įrenginiu (SH), Pranešimų keitimas (N), Pakartotinė ataka (N), Atkūrimas (N), Išsižadėjimas (N)	Vientisumas, neišsižadėjimas, autentiškumas
AS5: Atakos, nukreiptos į energijos vartojimo duomenų užklausas	Apsimetimas klientu (N), Duomenų stebėjimas (N), Perėmimas (N), Pranešimų keitimas (N)	Konfidencialumas, vientisumas, prieinamumas

Blokų grandinių technologija



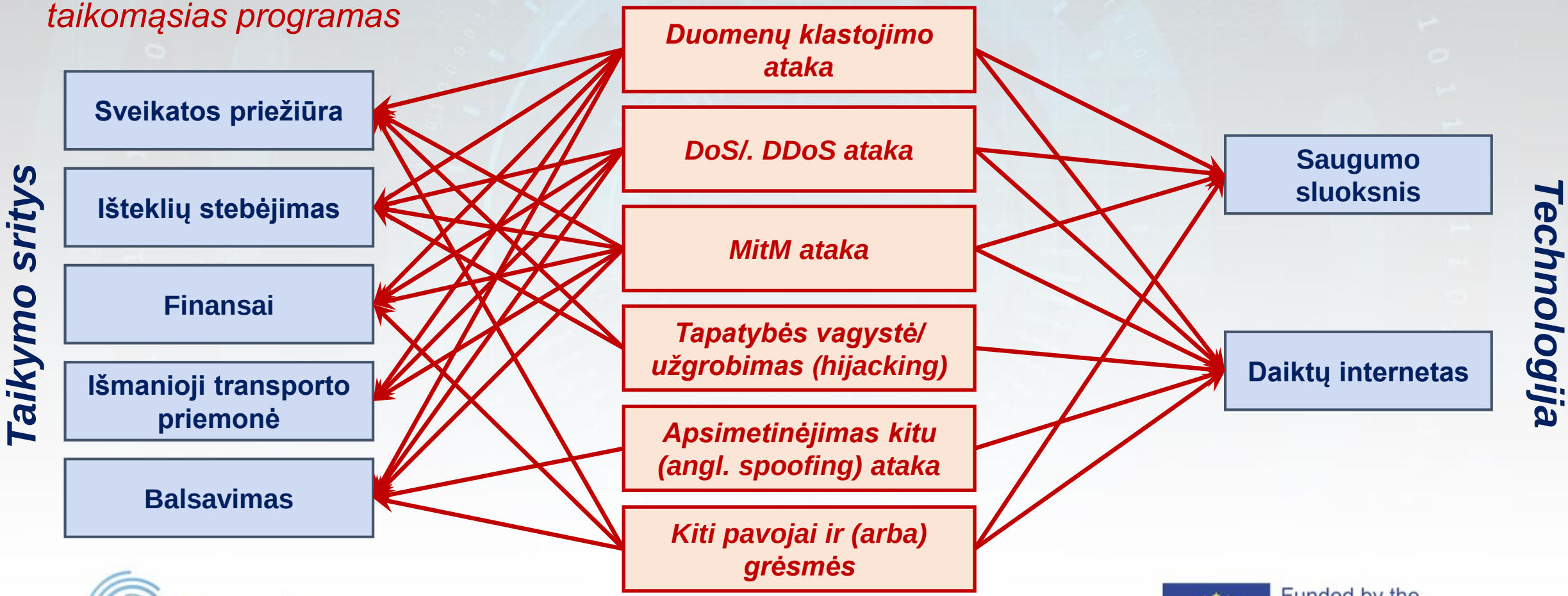
Blokų grandinė – tai paskirstyta nekintamos apskaitos knygos technologija, suteikianti galimybę saugoti aktualią apskaitos knygos versiją, kuri atnaujinama kiekvieną kartą patvirtinus naują sandorį.

[Lewis , 2015; Sato and Himura, 2018]

Funded by the Erasmus+ Programme of the European Union

Blokų grandinių technologija

Saugumo rizikos įvairiose taikomųjų programų srityse mažinamos naudojant blokų grandinės taikomąsias programas

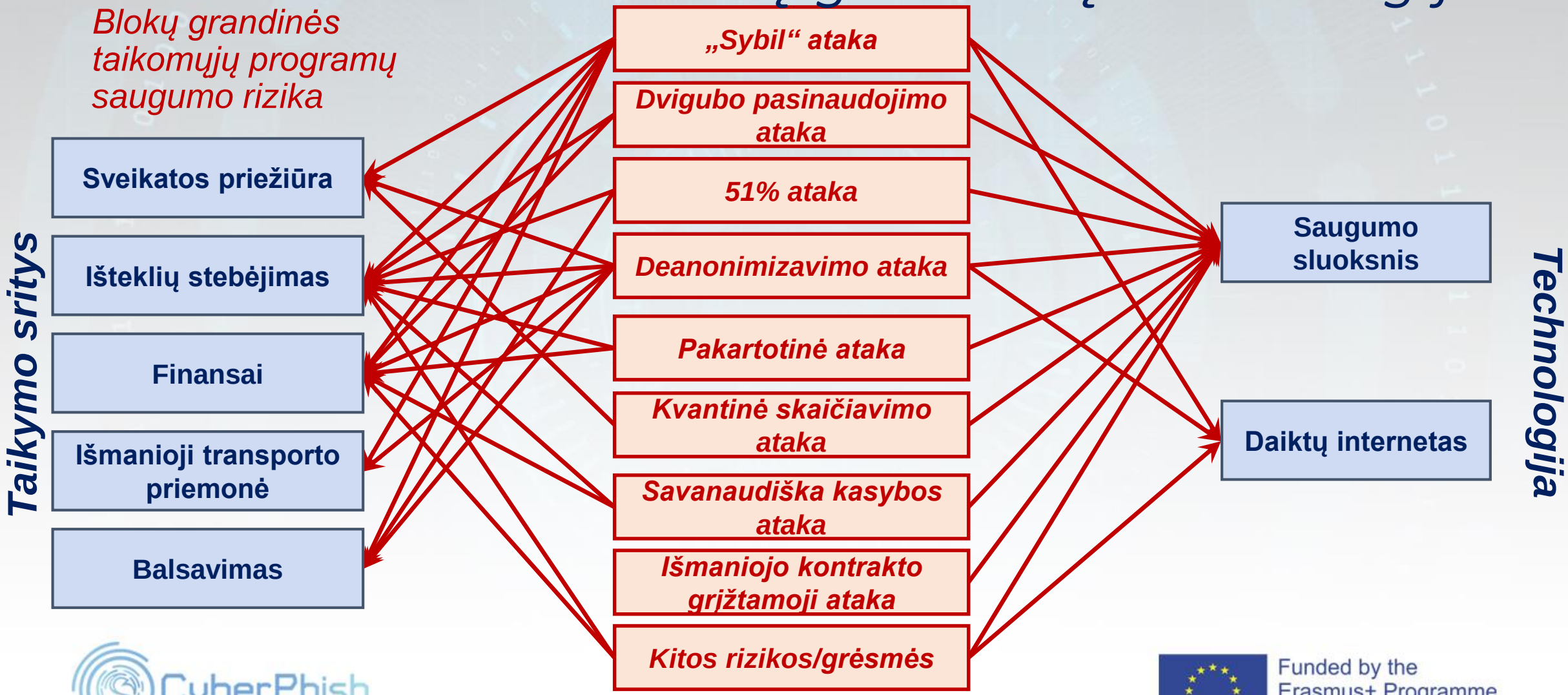


[Iqbal and Matulevičius, 2019]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Blokų grandinių technologija



[Iqbal and Matulevičius, 2019]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Didžiųjų duomenų ekosistema

	IŠŠŪKIAI
ŽMOGUS *Verslas, informacija, socialiniai ir profesiniai reikalai*	Sutikimo nebuvimas, socialinis piktnaudžiavimas žiniomis, neteisėta prieiga, duomenų perkrova, netinkama analizė, prieinamumas, tikslumas
TECHNOLOGIJA ***Programa, platforma, duomenų infrastruktūra***	Daugkartinis duomenų naudojimas, technologinės spragos, suderintas duomenų naudojimas, duomenys, savalaikiškumas, duomenų kilmė, įrenginių heterogeniškumas, prieinamumas, duomenų rinkimo valdymas ir perdavimas, duomenų tipai ir formatai, neišsamūs ir nenuoseklūs duomenys
ĮRANGA ***Erdvinė, HVAC, Energijos, Pagalbinė***	Saugojimas ir apdorojimas Skirtingi duomenų šaltiniai, prieinamumas
APLINKA ***Politinė, aplinkosauginė, socialinė, technologinė, teisinė***	Valdymo, politikos, įstatymų trūkumas, organizacinis pasipriešinimas, duomenimis grindžiamos kultūros kūrimas

[Anwar et al., 2021]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Didžiųjų duomenų ekosistema

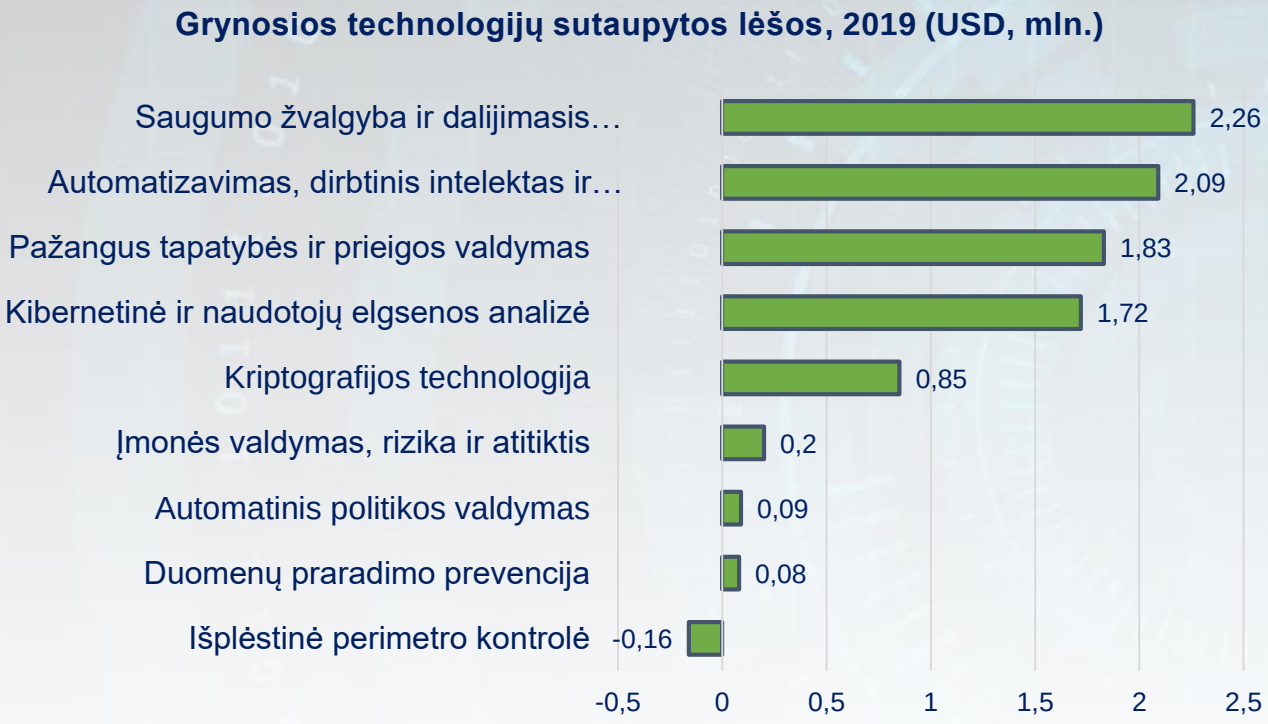
	SPRENDIMAI
ŽMOGUS *Verslas, informacija, socialiniai ir profesiniai reikalai*	Naudotojo patvirtinimas, įgūdžiai, prieigos kontrolė, naudotojų mokymas, auditas, ryšių saugumas, grėsmių modeliavimas, rizikos vertinimas, duomenų klasifikavimas, duomenų privatumo išsaugojimas, privatumas socialiniuose tinkluose
TECHNOLOGIJA ***Programa, platforma, duomenų infrastruktūra***	Galutinio taško patvirtinimas ir šifravimas, saugios užklausos, diferencinis privatumas, įterptųjų duomenų privatumas, saugus duomenų rinkimas, saugojimas ir transformavimas, mašininio mokymosi algoritmai, įsilaužimo atpažinimas, duomenų anonimizavimas
ĮRANGA ***Erdvinė, HVAC, Energijos, Pagalbinė***	Atsarginių duomenų kopijų kūrimo ir atkūrimo paskirstytieji šaltiniai Užšifruotos antraštės informacijos saugojimas
APLINKA ***Politinė, aplinkosauginė, socialinė, technologinė, teisinė***	Valdymo ir teisinė parama

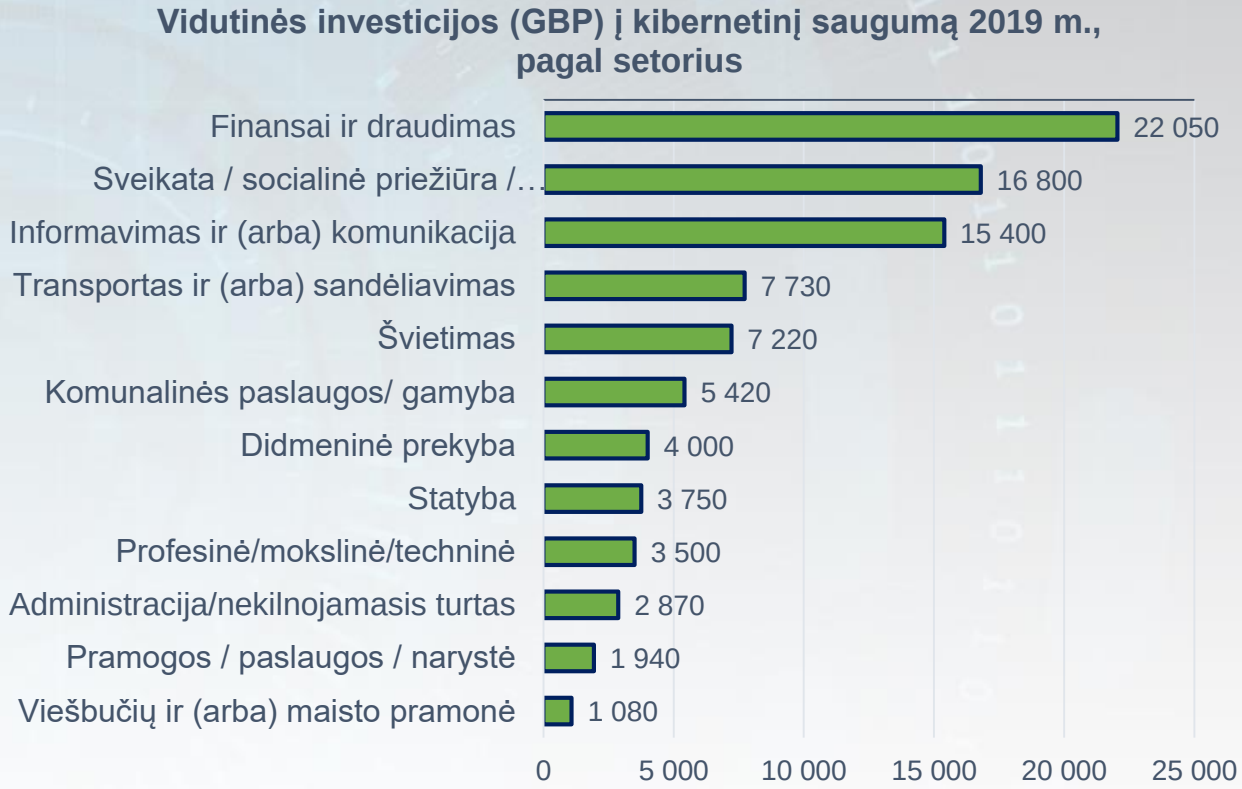
[Anwar et al., 2021]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Investicijos į saugumą





Saugumo žvalgyba ir dalijimasis grėsmėmis – dažniausiai naudojamos saugumo technologijos

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

Finansai ir draudimas – pagrindiniai verslo sektoriai, investavę į kibernetinį saugumą

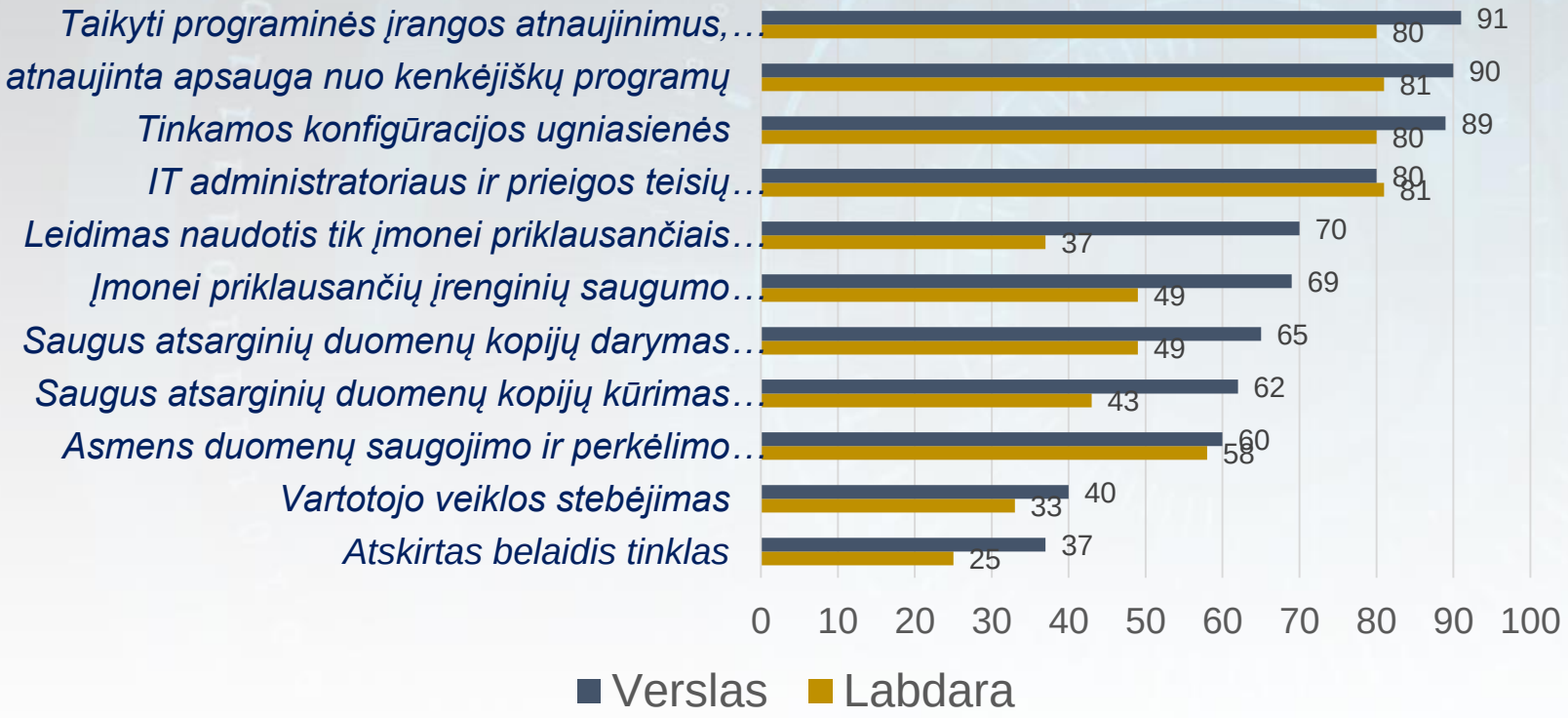
https://www.digitalmarketingcommunity.com/indicators/cyber-security-investment-2019/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Didėjančių grėsmių iššūkis

Naudojamos saugumo taisyklės ar kontrolės priemonės? (%)



- Neneigti, kad grėsmė egzistuoja, nes neigimo pasekmė bus nesėkmė
- Tikėtis, kad atsitiktiniai informacijos įsilaužimai bus labiau tikėtini nei piktavališkos atakos
- Imtis veiksmų nelaukiant, kol būsite užpulti arba kol nutekės informacija
- Nuosekliai taikyti politiką
- Spręsti kultūrinius klausimus įvairiais lygmenimis
- Subalansuoti investicijas į apsaugą nuo išorinių ir vidinių grėsmių
- Laikytis principo „mokymas, mokymas, mokymas“!

[Colwill, 2009]

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Nacionalinės valstybės grėsmės

- Kibernetinio šnipinėjimo taikiniai
  - *pramonės sektoriai*
  - *ypatingos svarbos ir strateginė infrastruktūra*
  - *vyriausybiniai subjektai*
  - *geležinkeliai*
  - *telekomunikacijų paslaugų teikėjai*
  - *energetikos įmonės*
  - *ligoninės*
  - *bankai*

Kibernetinio šnipinėjimo motyvuoti duomenų pažeidimai
20%

Kenkėjiški veikėjai, susiję su nacionalinėmis valstybėmis
38%

Kibernetinio šnipinėjimo motyvuoti incidentai
11,2%

Kibernetinio šnipinėjimo incidentai, susiję su sukčiavimu
63%

CyberPhish
Safeguarding your digital future

ENISA Threat Landscape Report 2018, 2020

Funded by the Erasmus+ Programme of the European Union

Nacionalinės valstybės grėsmės

- Kibernetinis šnipinėjimas orientuotas į
  - *geopolitikos valdymą*
  - *valstybės ir komercinių paslapčių vagystes*
  - *intelektinės nuosavybės teisės vagystes*
  - *nuosavybės teise priklausančios informacijos strateginėse srityse vagystes*

- 2019 metais
  padaugėjo prieš ekonomiką nukreiptų kibernetinių atakų, kurias finansuoja nacionalinės valstybės, ir tikėtina, kad taip bus ir toliau.
- Vis dažniau pasitaiko valstybių remiamų atakų prieš pramoninį daiktų internetą (IIoT) šiuose sektoriuose
  - *komunalinės paslaugos*
  - *nafta ir gamtinės dujos*
  - *gamyba*

Nacionalinės valstybės grėsmės

- Kibernetinis šnipinėjimas orientuotas į
  - geopolitikos valdymą
  - valstybės ir k
  - intelektinės n
  - nuosavybės
    informacijos
- 2019 metais
  padaugėjo prieš ekonomiką nukreiptų
  nansuoja
  ėtina, kad
  bių remiamų
  ų internetą
  gos
  jos

Nustatyti svarbiausius organizacijos vaidmenis ir įvertinti šnipinėjimo riziką.

Sukurti saugumo politiką

Nustatyti įmonės praktiką, kaip bendrauti su darbuotojais ir juos mokyti

Sukurti vertinimo kriterijus (KPI), kad būtų galima palyginti veiklą

Sukurti svarbiausių taikomųjų programų paslaugų „baltąjį sąrašą“

Įvertinti pažeidžiamumą ir reguliariai atnaujinti programinę įrangą

Įgyvendinkite principą „būtina žinoti“, norint apibrėžti prieigos teises

Nustatyti turinio filtravimą visiems įeinantiems ir išeinantiems kanalams

Santrauka

- Verslo iššūkiai
- Kibernetinio saugumo atakų augimas
- Technologijų naudojimas ir saugumo iššūkiai
- Didėjančių grėsmių iššūkis
- Nacionalinės valstybės keliamos grėsmės

Funded by the Erasmus+ Programme of the European Union

Užduotys

Aptarkite, koks yra antras pagal dydį verslo iššūkis (žinoma, po informacijos saugumo).

Kokia, jūsų nuomone, yra pavojingiausia saugumo grėsmė / ataka?

Ar kasdieniame gyvenime naudojate kokias nors (mobiliąsias) technologijas? Kokias? Ar jos yra apsaugotos?

Ar žinote arba esate skaitę apie kokią nors grėsmę, susijusią su nacionalinėmis valstybėmis?
Ar galėtumėte apie ją papasakoti ir paaiškinti, kas tai yra?

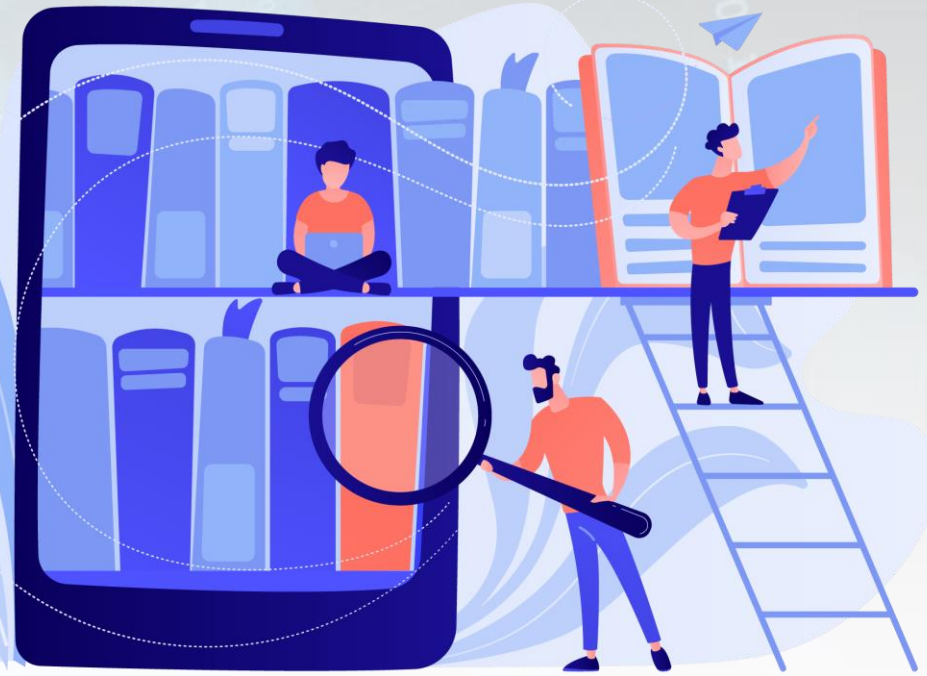
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Papildomi skaitiniai

Medžiaga, naudota rengiant šią pateiktį

- **Abiodun O. I. A., Abiodun E. O., Alawida M., Alkhawaldeh R. S., Arshad H.,** (2021). A Review on the Security of the Internet of Things: Challenges and Solutions. *Wireless Personal Communications 119:2603–2637 https://doi.org/10.1007/s11277-021-08348-9*
- **Affia A-a. O., Matulevičius R., Nolte A.** (2019): Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review. *Panetto H. et al. (eds.), LNCS 11877, CoopIS 2019, Springer*
- **Anwar M. J. Gill A. Q., Hussain F. K., Imran M.** (2021), Secure big data ecosystem architecture: challenges and solutions. *J Wireless Com Network 2021:130 https://doi.org/10.1186/s13638-021-01996-2*
- **Colwill C.** (2009) Human factors in information security: The insider threat e Who can you trust these days? *Information Security Technical Report 14,186-196*
- **Iqbal, M., Matulevičius, R.** (2019) Blockchain-Based Application Security Risks: A Systematic Literature Review, *Proceedings of CAiSE 2019 International Workshops, 2019 Workshop, LNBIP 349, 176-188*
- **Komninos N., Philippou E., Pitsillides A.** (2014). Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures, *IEEE Communication Surveys & Tutorials, 16(4)*



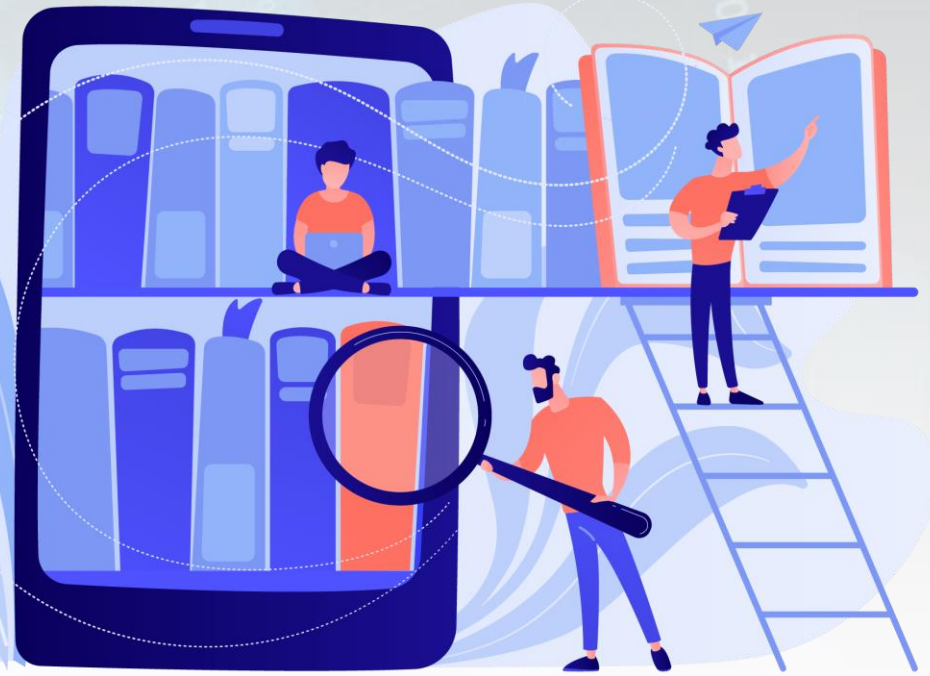
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Papildomi skaitiniai

Medžiaga, naudota rengiant šią pateiktį

- **Lewis, A.** (2015): Blockchain technology explained (2015). *http://www.blockchaintechnologies.com/blockchain-definition*
- **Orantes-Jimenez A.D., Aquirre E.** (2020): A Survey on Information Security in Cloud Computing, *Computacion y Sistemas 24(2)*
- **Perdomo R.** (2021): 15 Technology Challenges Business May Face in 2021, URL: *https://blog.systems- x.com/author/rubens-perdomo*
- **Sato, T., Himura, Y.** (2018): Smart-contract based system operations for permissioned blockchain. *NTMS 2018, vol., 1–6*
- **Schatz, D., Bashroush, R., Wall, J.** (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law. 12 (2).*
- **Tahirkheli, A.I.; Shiraz,M.; Hayat, B.; Idrees, M.; Sajid, A.; Ullah, R.; Ayub, N.; Kim, K.-I. A.** (2021). Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics 2021,10,1811. https:// doi.org/10.3390/electronics10151811*



Trumpi vaizdo įrašai

- Verslo technologijų tendencijos (EN)
  https://youtu.be/DOAnYtqhXBU
- Daiktų interneto saugumas (EN)
  https://youtu.be/IQkRscixagM
- Debesų kibernetinis saugumas (EN)
  https://youtu.be/k2684fuzHLs
- Įsilaužimas į jūsų namus (EN)
  https://youtu.be/iRQPfISsG9k
- Įvadas į blokų grandinės saugumą (EN)
  https://youtu.be/dl8Hl91siM8
- Didžiųjų duomenų apsaugos iššūkiai (EN)
  https://youtu.be/3xIuIcPzMVs
- Kokios yra dabartinės grėsmės duomenų saugumui? (EN)
  https://youtu.be/WugGZaT2oHE
- Top 7: nacionalinių valstybių remiami įsilaužėliai (EN)
  https://youtu.be/S_IPgHbondk

Dėkojame!