# Ievads

Pēdējo gadu laikā ir notikusi ļoti strauja informācijas un komunikācijas tehnoloģiju (IKT) attīstība. Eiropas Savienībā (ES) no kopējās ekonomikas IKT izpētes un inovāciju sektoram atvēlēti 4,8% no Horizon 2020 programmā paredzētajiem finanšu resursiem, ar mērķi nodrošināt stabila digitālā vienotā tirgus izveidei (EC, 2019). IKT ražotāji ik dienas strādā pie jaunu ierīču un risinājumu izstrādes, cīnoties ar konkurentiem par tirgus daļu un cenšoties būt pirmie, kas piedāvā jaunākās inovācijas. Rezultātā pasaulē kopumā 10 gadu laikā IKT skaits un to izmantojums palielinājies vairāk kā divas reizes. Atbilstoši Starptautiskās telekomunikāciju savienības (*International Telecommunications Union* - ITU) Attīstības indeksa ietvaros aprēķinātajiem datiem, par valstīm ar straujākajiem IKT attīstības tempiem 2016. un 2017.gadā atzītas šādas: Islande (IKT attīstības indeksa vērtība 2017.g. – 8,98, 2016.g – 8,78), Dienvidkoreja (2017.g. – 8,85, 2016.g. – 8,8), Šveice (2017.g. – 8,74, 2016.g. – 8,66), Dānija (2017.g. – 8,71, 2016.g. – 8,68), Lielbritānija (2017.g. – 8,65, 2016.g. – 8,53), Ķīna / Honkonga (2017.g. – 8,61, 2016.g. – 8,47). Latvija atbilstoši šim rādītājam ierindota 35.vietā no 176 valstīm kopumā (2017.g. – 7,26, 2016.g. – 7,05) (ITU-b, 2017). Salīdzinot šos rādītājus ar valstu iedzīvotāju skaitu, tieša korelācija neveidojas, jo jāņem vērā, ka lielai daļai cilvēku īpašumā ir vairāk kā viena IKT ierīce, jo īpaši tas novērots attīstītās valstīs (ITU-a, 2017).

Straujā IKT attīstība un mainība novedusi pie tā, ka ne visi uzņēmumi spēj izsekot līdzi šīm izmaiņām, tās iegādāties un adaptēt savām vajadzībām (UNCSTAD, 2019). Tādēļ uzņēmumos nereti tiek izmantotas nevis jaunākās, bet gan jau dažus gadus vecas vai pat novecojušas IKT. IKT izmantojums tiešā veidā saistāms arī ar uzņēmuma darbības jomu. (Bajdor, 2015) Kūtrā IKT nomaiņa uzņēmumos skaidrojama ar jaunu IKT augstajām izmaksām un to vērtības strauju krišanos (Byrne & Corrado, 2017). Kā arī jāņem vērā, tas ka uzņēmuma darbības nodrošināšanai svarīgākais ir atbilstoša IKT, ar kuru darbinieks var veikt tam uzdotos darba pienākumus, nevis IKT ierīču modernums un trendīgums. Skatoties no otras puses, modernu un mūsdienīgu IKT izmantošana un integrācija ar visiem uzņēmuma biznesa procesiem viennozīmīgi paaugstina uzņēmuma darbības efektivitāti un konkurētspēju, kā arī samazina biznesa procesu izmaksas (Ács, 2018; de Wet *et.al.*, 2016).

Savukārt Eurostat statistikas pētījumā (2018) konstatēts, ka privātajā sektorā ar IKT ierīču izmantojumu ir teju vai gluži pretēji kā uzņēmumos – privātpersonām, jo īpaši gados jauniem cilvēkiem, ir svarīgi, lai to izmantotā IKT ierīce nebūtu vecāka par gadu vai diviem. Lai tā būtu ērta, vizuāli pievilcīga un moderna. Vienlaikus tās tehniskie parametri, papildus ierīces un aplikācijas atbilstu personīgajām vajadzībām un darba stilam. Attiecīgi, līdz ar jaunas ierastā un/vai interesējošā zīmola IKT ierīces izlaišanu tirgū privātpersonas izmantojumā esošas ierīces nereti nomaina uz jaunākām, neskatoties pat uz to, ka par jaunu ierīci un tās papildus funkcijām / uzstādījumiem var nākties maksāt dārgāk un /vai papildus.

Tādējādi rezultātā privātpersonas izmanto jaunākas un tehnoloģiski attīstītākas IKT ierīces (viedtālruņus, planšetdatorus un portatīvos datorus), nekā to dara biznesa sektors. Līdz ar to rodas jautājums: “Kādēļ gan neizmantot privātās IKT ierīces darba vajadzībām ?”.

Tirgus izpētes uzņēmums “Gartner” ik gadus veic pētījumus par IKT izmantošanu. Pēdējos 10 gados veikti arī pētījumi par privātpersonu personīgo ierīču izmantošanu darba vajadzībām. Atsaucoties uz “Gartner” sniegto informāciju (2018), personīgo ierīču izmantošana darba vajadzībām ir kļuvusi par ļoti aktuālu jautājumu lielai daļai uzņēmumu visā pasaulē.

Veiktajos pētījumos konstatēts (Bullock, 2019; Cooper, 2019; Eslahi *et.al.*, 2014; French *et.al.*, 2014), ka pasaulē 2022. gadā darba pienākumu veikšanai 367 biljoni darbinieku izmantos savas personīgās IKT ierīces. Salīdzinoši 2014. gadā šādu ierīču izmantojums bija tikai 30 biljoni. Tādējādi prognozēts, ka faktiski nepilnu 10 gadu laikā personīgo IKT izmantojums būs pieaudzis vairāk kā 10 reizes. Turklāt jau šobrīd līdz pat 85% darbinieku (atkarībā no valsts) darba vajadzībām izmanto savus viedtālruņus. 42% no tiem norādījuši uz izmantojuma pozitīvo ietekmi - tas veicina viņu laika izmantojuma efektivitāti un darba produktivitāti. Šī tendence kļūst arvien populārāka arī Latvijā, kur 74% uzņēmumos un 62% valsts pārvaldes institūcijās strādājošo darba vajadzībām izmanto personīgos viedtālruņus (CERT.LV, 2014).

Privātās IKT ierīces darba vajadzībām tiek izmantotas, jo darbiniekam tā nenoliedzami ir daudz ērtāk. Var strādāt sev patīkamā un pierastā veidā un vidē. Nav līdzi jānēsā dubultīgs IKT ierīču skaits, jānodrošina to pieejamība un jāatceras to paroles. Tas atvieglo arī darba pienākumu veikšanu atrodoties ārpus uzņēmuma darba telpām vai strādājot attālināti no mājām. Turklāt pēdējos gados viedtālrunis ieņem aizvien būtiskāku lomu autentifikācijas procesā. Savukārt Bullock (2019), konstatējusi, ka tā tiek ieekonomēts līdz pat 58 minūtēm laika darba dienā, kas citādi tiktu izmantots IKT ierīces ieslēgšanai, konkrēto programmu un dokumentu atvēršanai u.tml. Tieši šo darbību veikšana nereti darbiniekiem liekas bezjēdzīga, laiku velti tērējoša un rada tajos papildus nevajadzīgu stresu. Privāto IKT ierīču izmantojums darba vajadzībām nenoliedzami arī saistāms ar indivīdu psiholoģiskajiem aspektiem un uzvedības iezīmēm.

Turklāt iespēja savienot darba aktivitātes ar privāto dzīvi ir viena no personīgo IKT ierīču izmantošanas priekšrocībām. To nepārtrauktā klātesamība ļauj būt sasniedzamiem jebkurā laikā, kā arī veikt ātru privāto jautājumu kārtošanu darba laikā.

Arī darba devēji (uzņēmumi) situācijā, kad darba vajadzībām tiek izmantotas darbinieku personīgās IKT ierīces, ir ieguvēji, jo darba pienākumu veikšanai tiek izmantotas jaunākās tehnoloģijas. Kā arī uzņēmums var ietaupīt finanšu resursus (līdz par 350 USD gadā par darbinieku), kas citādi tiktu izmantoti IKT iegādei un infrastruktūras uzturēšanai (Bullock, 2019).

Līdz ar to faktiski var apgalvot, ka personīgo IKT ierīču izmantošana ir abpusēji izdevīga (gan uzņēmumam, gan darbiniekam). Tādēļ nav brīnums, ka šādam IKT izmantojuma veidam ir tik straujš pieauguma temps un tas uzņēmumos sastopams aizvien biežāk.

Tā laika gaitā pamazām attīstoties personīgo IKT ierīču izmantojumam darba vajadzībām, aptuveni 2004. gadā radies jēdziens ‘privāto ierīču izmantošana darbā’ (*Bring your own device* - BYOD) (Cooper, 2019), ar ko apzīmē situāciju, kad uzņēmuma politika pieļauj darbinieku personīgo IKT ierīču izmantošanu darba vajadzībām, tādējādi ar personīgajām IKT ierīcēm piekļūstot uzņēmuma resursiem (informācijai, informācijas sistēmām un tīklam u.c.). Vienlaikus jānorāda, ka jēdziena latviskais tulkojums nav nostiprināts un dažādu autoru avotos joprojām mēdz atšķirties.

Jāatzīst, ka BYOD izmantošanā ir ne tikai pozitīvie, bet arī negatīvie aspekti, jo īpaši tie, kas saistīti ar uzņēmuma IKT drošības nodrošināšanu. Galvenais jautājums, kas rodas saistībā ar BYOD, parasti ir šāds: “Kā pasargāt uzņēmuma resursus no BYOD radītajiem apdraudējumiem ?”. Jo īpaši satraucošs tas ir, ņemot vērā, ka darbiniekiem nereti nav vispusīgas zināšanas, lai pietiekošā drošības līmenī pārvaldītu personīgās IKT ierīces. Tie nereti neizmanto antivīrusu programmatūras, ļauj arī citām personām lietot tām piederošas IKT (piemēram, mājas apstākļos bērniem), nenodrošina pietiekošu paroles stiprību un drošu autorizāciju. Attiecīgi BYOD ir IKT drošības jautājumiem un to uzvedību.

Tendence, ka BYOD tik lielā skaitā aizvien vairāk tiek izmantotas darba vajadzībām, radījusi jaunas problēmas uzņēmumiem. Tiem jāmeklē veidi kā risināt IKT ierīču aizsardzības un vienotas pārvaldības jautājumus. Līdz ar to, strauji pieaugusi uzņēmumu interese par BYOD drošības politiku, izmantošanas kontroli, finanšu un juridisko saistību pārvaldību, savlaicīgu risku identificēšanu un novērtēšanu, preventīvo darbību veikšanu.

Vēl pavisam nesen lielā daļā uzņēmumu informācijas aizsardzība, pārvaldība un BYOD atbalsts nebija ieguldījuma vērts. Uzņēmumos ar stingru drošības politiku BYOD lietošana vispār netika pieļauta. Ņemot vērā, ka pēdējos gados BYOD skaits pieaug ar katru dienu, BYOD drošības pārvaldības jautājumi ir grūti ignorēt.

Būtiskākais jautājums šobrīd BYOD drošības pārvaldībā ir: “Kā panākt uzņēmuma resursu, informācijas drošības un personas privātuma kompromisu starp uzņēmumu un darbinieku ?”. Jo būtiski un aizsargājami ir abi. Nesankcionēta piekļuve uzņēmuma resursiem vai tā informācijai, drošības incidenti, ko izraisījušas BYOD, var pasliktināt uzņēmuma reputāciju, radīt neuzticamību uzņēmumam klientu acīs, ietekmēt uzņēmuma finanšu rādītājus, kā arī novest uzņēmumu līdz bankrotam. Savukārt ES personas privātumu apstrādi aizsargā *Vispārējā datu aizsardzības regula*. Tā rada ierobežojumus uzņēmumiem veikt personas datu apstrādi.

IKT, t.sk. BYOD drošības reglamentācija ir uzņēmumu pašu atbildība, kas netiek centralizēti reglamentēta valsts, ES vai starptautiskā mērogā. Līdz ar to nenoliedzami saprotams, ka drošības prasību nosacījumu kvalitāti tieši ietekmē uzņēmuma normatīvus izstrādājošo darbinieku kompetence IKT drošības jautājumos. Un līdz ar skaidriem nosacījumiem vien nepietiek, tie arī jāievēro. Attiecīgi, lai būtu pārliecība par to ievērošanu jāveic darbības, kas sevī ietver monitoringu un uzraudzību. Tomēr šīs darbības būs vairāk vērstas uz incidentu identifikāciju un to novēršanu, nevis preventīviem risinājumiem, lai incidentu notikšanu nemaz nepieļautu.

Preventīvo risinājumu efektīva īstenošana, nodrošinātu, ka incidentu skaits uzņēmumā samazinātos un palielinātos uzņēmuma IKT drošības līmenis. Viens no veidiem kā risināt BYOD drošības jautājumus preventīvi ir regulāri veikt uzņēmuma IKT, t.sk. BYOD, risku novērtēšanu. Tas sevī ietvertu risku identificēšanu, iespējamo seku apzināšanu, risku novērtēšanu, risku tolerances un apetītes noteikšanu, kā preventīvo darbību noteikšanu, lai mazinātu vai likvidētu riskus.

Tomēr veicot risku analīzi reizi gadā, ievērojot konkrētu metodoloģiju, konstatēts, ka tā nav efektīva, rada slogu iesaistītajiem darbiniekiem un nebūt neidentificē visus faktiski esošos riskus. Turklāt veicot risku analīzi, balstoties tikai uz iesaistīto darbinieku teikto, nav pārliecības, ka atsevišķi riski nemaz netiek apzināti vai pat tiek apzināti slēpti. Ņemot vērā to, identificēts, ka nepieciešams universāls risinājums visu šo jautājumu kopējam, vienotam risinājumam.

Temats par BYOD drošību ir salīdzinoši jauns un aktuāls pētījuma lauks, kas vienlaikus cieši saistāms ar IKT drošību. **Novitāti** apstiprina fakts, ka tā līdz šim vēl nav plaši pētīta, atrodami tikai atsevišķi pētījumi par šo tēmu - Latvijā (Bušs, 2013; Dziļuma, 2015; Plisko, 2014; Zariņš, 2015) un ārzemēs (Arregui, 2015; Bais, 2016). Tomēr neviens no tiem nav orientēts uz preventīvo pasākumu veikšanu, ar mērķi paaugstināt BYOD izmantošanas drošību.

Lai objektīvi novērtētu BYOD riskus, jāizveido atbilstoša lēmumu pieņemšanas sistēma, ar ko šādu novērtējumu veikt. Līdz šim risku novērtēšana veikta balstoties uz vispārpieņemtiem teorijas principiem par risku novērtēšanu, kas neaptver visas iesaistītās puses, rada tām administratīvo slogu un nav efektīva.

No iepriekš minētā identificēta **problēma** – BYOD izmantošana uzņēmumā samazina tā IKT drošības līmeni.

Pētījuma **objekts**: Risku novērtēšanas metožu analīze, lēmumu atbalsta sistēmas projektēšana un izstrāde uz risku novērtējumu balstītu preventīvo darbību noteikšanai jautājumos par BYOD.

Maģistra darba **mērķis** ir izstrādāt risinājumu uz BYOD risku novērtējumu balstītu preventīvu darbību veikšanai.

**Pētījuma jautājums**: Kāda lēmumu atbalsta sistēma sekmīgi realizētu atbalstu lēmumu pieņemšanai BYOD riskiem un BYOD drošībai ?

Lai sasniegtu maģistra darba mērķi un rastu atbildi uz izvirzīto pētījuma jautājumu, jārisina šādi **uzdevumi**:

1. Izpētīt risku novērtēšanas metodes BYOD jomā un izstrādāt teorētisko modeli uz risku novērtējumu balstītai lēmumu pieņemšanai par BYOD.

2. Izvērtēt metodes un rīkus lēmumu atbalsta sistēmas projektēšanai.

3. Adaptēt kritērijus lēmumu realizācijas novērtēšanai.

4. Izstrādāt lēmumu atbalsta sistēmas prototipu sekmīgi realizētu lēmumu pieņemšanai.

5. Veikt prototipa verifikāciju un validāciju, novērtēt tā ietekmi uz lēmumu pieņemšanu BYOD jomā.

Maģistra darbā izmantotās **metodes**:

1. Teorētiskās metodes:

- teorētiskās literatūras analīze par risku novērtēšanas metodēm BYOD jomā, par kritērijiem lēmumu realizācijas novērtēšanai un metodēm lēmumu atbalsta sistēmas projektēšanai;

- tehniskās dokumentācijas un mēdiju analīze par pieejamajiem rīkiem lēmumu atbalsta sistēmas prototipa izstrādei un to iespējām;

2. Datu ieguves metodes:

- netiešie novērojumi (ekspertu metode, testēšana) par risku novērtēšanas metožu izmantojumu lēmumu pieņemšanā BYOD drošības nodrošināšanai;

- risku novērtēšanas un uzņēmumu drošības auditu dokumentācijas analīze;

3. Datu apstrādes metodes:

- kārtošana;

- ranžēšana;

- faktoranalīze;

- klāsteranalīze;

4. Datu analīzes metodes:

- aprakstošās analīzes metodes (kontentanalīze, grafiskā analīze, abstrakti loģiskā metode, dedukcija);

- statistiskās analīzes metodes (faktoru un korelāciju analīze, regresija, dinamikas statistiskā izpēte);

5. Rezultātu novērtēšanas metodes:

- verifikācija;

- validācija.

Maģistra darba **nosaukums**: BYOD drošības pilnveides risinājums

Darba rezultātā izstrādāts … prototips BYOD jomā ar kritērijiem lēmumu realizācijas novērtēšanai un metodēm lēmumu atbalsta sistēmas projektēšanai.

Pētījuma bāze ir xxx datu avoti laika periodā xxxx

Pētījuma posmi:

1. Teorētiskā modeļa izstrāde xxxxxxxx
2. Prototipa izstrāde un novērtēšana xxxxxxx
3. Rekomendāciju izstrāde xxxxxxxx

Maģistra darbs sastāv no xxx daļām. Pirmajā daļā ir …

# Izmantotā literatūra

1. Ács, Z.J., Szerb, L. & Lloyd, A. (2018). *Global entrepreneurship index 2018*. USA: Washington. The Global Entrepreneurship and Development Institute. 89 p. Avots: <https://thegedi.org/wp-content/uploads/dlm_uploads/2017/11/GEI-2018-1.pdf>
2. Arregui, D.A. (2015). *Mitigating BYOD Information Security Risks*. Research project. University of Melbourne.
3. Bajdor, P. (2015). *The Use of Information and Communication Technologies in Polish Companies in Comparison to Companies from European Union*. 22nd International Economic Conference – IECS 2015 “Economic Prospects in the Context of Growing Global and Regional Interdependencies” (IECS 2015). Procedia Economics and Finance. Vol.27. 702 – 712 p. doi: <https://doi.org/10.1016/S2212-5671(15)01051-5> Avots: ScienceDirect datubāze.
4. Bais, A. (2016). *Security risks associated with BYOD*. Master Thesis. ICTE Aalborg University Copenhagen.
5. Bullock, L. (2019) *The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future*. Journal Forbes. Avots: <https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#5918ca0c1f30>
6. Bušs, R. (2013). *Mobilo ierīču pārvaldības programmatūras un risinājumu analīze*. Bakalaura darbs. Rīgas Tehniskā universitāte.
7. Byrne, D. & Corrado, C. (2017). *ICT Services and Their Prices: What Do They Tell Us About Productivity and Technology ?* International Productivity monitor. No.33. 150 – 181 p. Avots: <http://www.csls.ca/ipm/33/Byrne_Corrado.pdf>
8. Cooper, S. (2019) *The Ultimate Guide to BYOD in 2019*. Avots: <https://www.comparitech.com/net-admin/ultimate-guide-to-byod/>
9. de Wet, W., Koekemoer, E. & Nel, J.A. (2016). *Exploring the impact of information and communication technology on employees' work and personal lives*. SA Journal of Industrial Psychology. Vol.42, No.1. doi: <https://doi.org/10.4102/sajip.v42i1.1330>
10. Dziļuma, A. (2015). *Personīgo tehnisko ierīču izmantošana uzņēmumos Latvijā un līdzekļi datu konfidencialitātes nodrošināšanai*. Bakalaura darbs. Latvijas Universitāte.
11. Eslahi, M., Var Naseri, M., Hashim, H., Tahir, N.M., Hisham Mat Saad, E. (2014) *BYOD: Current State and Security Challenges*. The Conference “ IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE 2014)” Proceedings DOI: 10.1109/ISCAIE.2014.7010235 Avots: <https://www.researchgate.net/publication/261871646_BYODCurrent_State_and_Security_Challenges>
12. European Commision (EC) (2019). *ICT Research & Innovation*. Horizon 2020. Avots: <https://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation>
13. Eurostat (2017). *Being young in Europe today*. ISSN 2443-8219 Avots: <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Being_young_in_Europe_today>
14. French, A.M., Guo, Ch., Shim, J.P. (2014) *Current Status, Issues, and Future of Bring Your Own Device (BYOD)*. Communications of the Association for Information Systems, Vol. 35(10). DOI: 10.17705/1CAIS.03510 Avots: <https://www.researchgate.net/publication/268445822_Current_Status_Issues_and_Future_of_Bring_Your_Own_Device_BYOD>
15. Gartner (2018). *Why Gartner declared BYOD a money saver*. Avots: <https://hobi.com/gartner-declared-byod-money-saver/gartner-declared-byod-money-saver/>
16. Information and Communication Technology (ITU-a) (2017). *Global E-waste Monitor 2017*. Chapter 3 Information and Communication Technology (ICT) and EEE Consumption Trends. 6 p. Avots: <https://www.itu.int/en/ITU-D/Climate-Change/Pages/Global-E-waste-Monitor-2017.aspx>
17. Information and Communication Technology (ITU-b) (2017). *ICT Development index 2017*. Measuring the Information Society Report. Avots: <https://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017rank-tab>
18. Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) (2014) *Ieteikumi drošai mobilo ierīču lietošanai*. Avots: <https://cert.lv/lv/2014/11/ieteikumi-drosai-mobilo-iericu-lietosanai>
19. Plisko, A. (2014). *BYOD politikas izmantošana uzņēmumos*. Bakalaura darbs. Latvijas Universitāte.
20. United Nations Commission on Science and Technology for Development (UNCSTAD) (2019). *Issues Paper on the impact on rapid technological change on sustainable development*. Inter-sessional Panel 2018-2019. Austria: Vienna. 46 p. Avots: <https://unctad.org/meetings/en/SessionalDocuments/CSTD2019_Issues01_RapidTechChange_en.pdf>
21. Zariņš, A. (2015). *Personisko mobilo iekārtu izmantošana darba vajadzībām koncepta izstrāde un ieviešana Rīgas Domē*. Maģistra darbs. Rīgas Tehniskā universitāte.