Izboljšanje ozaveščenosti na področju informacijske varnosti z uporabo metod igrifikacije

Alenka Brezavšček[1], Maja Minič[2]
[1]Univerza v Mariboru, Fakulteta za organizacijske vede, Kidričeva cesta 55 A, 4000 Kranj
[2]Ministrstvo za obrambo Republike Slovenije, Vojkova cesta 55, 1000 Ljubljana
alenka.brezavscek@um.si

Izvleček

V prispevku obravnavamo uporabo metod igrifikacije (tudi poigritev) za potrebe izobraževanja. Na kratko smo opisali elemente igrifikacije, predstavili ključne značilnosti teh metod ter zaznane pozitivne učinke na samo učinkovitost izobraževanja. Na podlagi izsledkov iz literature ter izkušenj iz prakse smo prikazali možnosti in načine uporabe teh metod pri ozaveščanju uporabnikov na področju informacijske (kibernetske) varnosti. Tako izkušnje iz literature kakor tudi empirične izkušnje dokazujejo, da je uporaba igrifikacije pri informacijsko varnostnem ozaveščanju povezana s pozitivno uporabniško izkušnjo, naklonjenostjo, kakor tudi z dejanskim dvigom ozaveščenosti.

Ključne besede: igrifikacija, informacijska varnost, kibernetska varnost, ozaveščanje, uporabnik.

Abstract

TThe paper deals with the use of gamification methods for educational purposes. We briefly described the elements of gamification, outlined the main features of these methods and the acknowledged positive effects on the effectiveness of education. Based on the findings from the literature and practical experience, we presented the possibilities and ways in which these methods can be used in awareness-raising activities in the field of information (cyber) security. Indeed, both literary and empirical experiences show that the use of gamification in information security awareness activities leads to a positive user experience, inclination and actual increase in awareness levels.

Keywords: Gamification, information security, cyber security, awareness, user.

1 UVOD

Zagotavljanje informacijske varnosti je danes ključnega pomena tako z vidika organizacij kot tudi posameznikov. Temelj zagotavljanja informacijske varnosti sicer res predstavlja implementacija ustreznih tehničnih rešitev, vendar empirične izkušnje dokazujejo, da ne glede na višino investicij v tehnične zaščite, doseženi nivo informacijske varnosti ne bo zadovoljiv, v kolikor v procese zagotavljanja informacijske varnosti ne vključimo najšibkejšega člena –človeka (Weishäupl et al., 2018). Tudi organizacija NIST (National Institute of Standards and Technology) poudarja pomen postopnega oblikovanja kompetenc na področju informacijske varnosti s ciljem spremembe vedenja v smeri varnostno ozaveščenega delovanja (NIST, 2003). Eno izmed ključnih aktivnostih pri tem zagotovo predstavlja kontinuirano in sistematično ozaveščanje zaposlenih. Če je program ozaveščanja in izobraževanja vsebinsko premišljen in učinkovito izveden, lahko bistveno pripomore k zmanjšanju verjetnosti za realizacijo varnostnega incidenta v organizaciji.

Številne sodobne študije razkrivajo, da lahko k učinkovitosti izobraževanja v splošnem precej pripomore uporaba metod igrifikacije (tudi poigritev; glej npr. Giang, 2013; Kapp, 2012). Rezultati raziskav dokazujejo mnoge pozitivne učinke uvedbe tovrstnih metod v izobraževanje. Nekateri avtorji med drugim navajajo, da le-te povečujejo sposobnost osvajanja novih znanj tudi za 40% (povzeto po Gabe Zichermann, citirano v Giang, 2013).

V prispevku se bomo osredotočili na uporabo metod igrifikacije pri izobraževanju in ozaveščanju uporabnikov na področju informacijske varnosti. Prispevek je organiziran na naslednji način: Najprej bomo podali nekaj osnov same igrifikacije, izpostavili ključne značilnosti ter podali definicije temeljnih pojmov. Osrednji del prispevka bo namenjen uporabi metod igrifikacije za potrebe ozaveščanja zaposlenih na področju informacijske (tudi kibernetske) varnosti. Na podlagi izsledkov iz literature kakor tudi empiričnih spoznanj bomo prikazali možnosti in načine uporabe tovrstnih metod pri reševanju vsakodnevnih izzivov, kot npr.: Kako uspešno usposabljati uporabnike, ki jih vsebina pravzaprav ne zanima? Kako preseči način delovanja – vem, vendar ne delam tako? Po naših izkušnjah se s tovrstnimi vprašanji vsakodnevno soočajo skrbniki za informacijsko varnost v sleherni organizaciji.

2 TEORETIČNE OSNOVE S PODROČJA IGRIFIKACIJE

Osnovni koncepti igrifikacije temeljijo na lastnostih iger, ki so ena izmed najstarejših oblik socialne interakcije posameznika (Voorhies, 2012). Dandanes se z igrami srečujemo zelo pogosto tako v fizičnem kot virtualnem okolju. Čeprav je primarni namen iger sicer zabava, mnoge raziskave dokazujejo, da predstavljajo metode in principi, na katerih temeljijo igre, pomembno sodobno orodje, ki je uporabno na marsikaterem področju, od razvoja novih produktov, prilagajanja delovnih mest, marketinga ali oblikovanja življenjskega sloga (glej npr. Kim, 2013; Kim, 2013a). Tako se v zadnjem obdobju tako v teoriji kot v praksi vse bolj uveljavlja področje, znano pod imenom *igrifikacija* (ang. gamification).

Sam pojem *igrifikacija* lahko definiramo kot uporabo lastnosti iger in igralne mehanike v neigralnem okolju (Kapp, 2012). Osnovni namen metod igrifikacije je motiviranje udeležencev za njihovo aktivno vključevanje v določen proces, kar se izkaže kot uporabno na marsikaterem področju (Kim, 2013a). Zaradi široke aplikativnosti in dokazanih pozitivnih učinkov je problematika igrifikacije v zadnjem obdobju bogato zastopana tako v strokovni kot v znanstveni literaturi. Sistematičen pregled najdemo npr. v Hamari et al. (2014) ali Koivisto & Hamari (2019). V nadaljevanju bomo predstavili nekaj temeljnih pojmov in konceptov igrifikacije.

Igralno mehaniko (ang. game mechanics) predstavljajo elementi in pravila, ki narekujejo, kako igra poteka. Po svoj naravi so lahko taka pravila različna, skupno vsem pa je, da v sami igri igrajo pomembno vlogo. Igro lahko naredijo zahtevno, zabavno, tekmovalno, potek igre pa vztrajno usmerjajo k njenemu glavnemu cilju (Seppo, n.d.). Primeri elementov igralne mehanike so: točke (ang. points), značke (ang. badges), uvrstitev na lestvici (ang. leaderboard), nivoji (ang. levels), ipd. Primarni namen elementov igralne mehanike je zadovoljevanje določenih želja igralca. Povezavo med elementi igralne mehanike in igralčevimi željami ponazarja tabela 1.

Podoben koncept kot igralna mehanika predstavlja *igralna dinamika* (ang. game dynamics). Razlika je v tem, da ima igralna dinamika nekoliko bolj motivacijski vzgib. S kombinacijo igralne dinamike in igralne mehanike skušajo avtorji igre pri igralcu vzbuditi njegove naravne potrebe po dokazovanju, kot npr. tekmovalnost, junaštvo, samopotrjevanje ali altruizem. Osnovni cilj je pri igralcu vzbuditi zanimanje in motivacijo za neko konkretno dejanje (Seppo, n.d.).

		Igralčeva potreba					
		Nagrada	Status	Dosežek	Samopotrditev	Tekma	Altruizem
Igralna mehanika	Točke	●	◐	◐		◐	◐
	Nivoji		●	◐		◐	
	Izzivi	◐	◐	●	◐	◐	◐
	Virtualne dobrine	◐	◐	◐	●	◐	
	Lestvica		◐	◐		●	◐
	Dobrodelnost		◐	◐		◐	

Tabela 1: **Povezava med elementi igralne mehanike in željami igralca (Kim, 2013a).**

Najvišji cilj je igralca pripeljati v t.i. *stanje toka* (ang. flow state), ki predstavlja stanje duha, ko je igralec visoko motiviran in zelo osredotočen na doseganje trenutnega cilja tako, da je sposoben iz samega procesa eliminirati vse ostale zunanje dejavnike (Seppo, n.d.). Namen je vzbuditi t.i. *notranjo motivacijo* (ang. intrinsic motivation), ki predstavlja človekovo notranjo željo nekaj narediti zaradi naloge same in ne zaradi zunanje nagrade za opravljeno nalogo. Notranja motivacija predstavlja temeljni pojem znane motivacijske teorije samodoločenosti (ang. selfdetermination theory) (Ryan & Deci, 2000).

Igre in igrifikacija vključujejo različne metode in tehnike, ki so se izkazale za učinkovite pri spodbujanju ključnih elementov notranje motivacije igralca (glej sliko 1). Zanimivo študijo podaja Karimi (2017), kjer analizira metode igrifikacije z vidika motivacijske teorije.

Slika 1: **Ključni elementi motivacije, ki jih metode igrifikacije spodbujajo (Seppo, n.d.).**

Strokovnjaki s področja igrifikacije se precej ukvarjajo tudi s proučevanjem psiholoških lastnosti samih igralcev, pri čemer igralce razvrščajo v različne kategorije. Znan je Bartlejev model (citirano v Kim, 2013), ki v osnovi opredeljuje štiri različne tipe igralcev (glej sliko 2): ubijalec (ang. killer), dosežkar (achiever), socialnež (ang. socializer) in raziskovalec (ang. explorer).

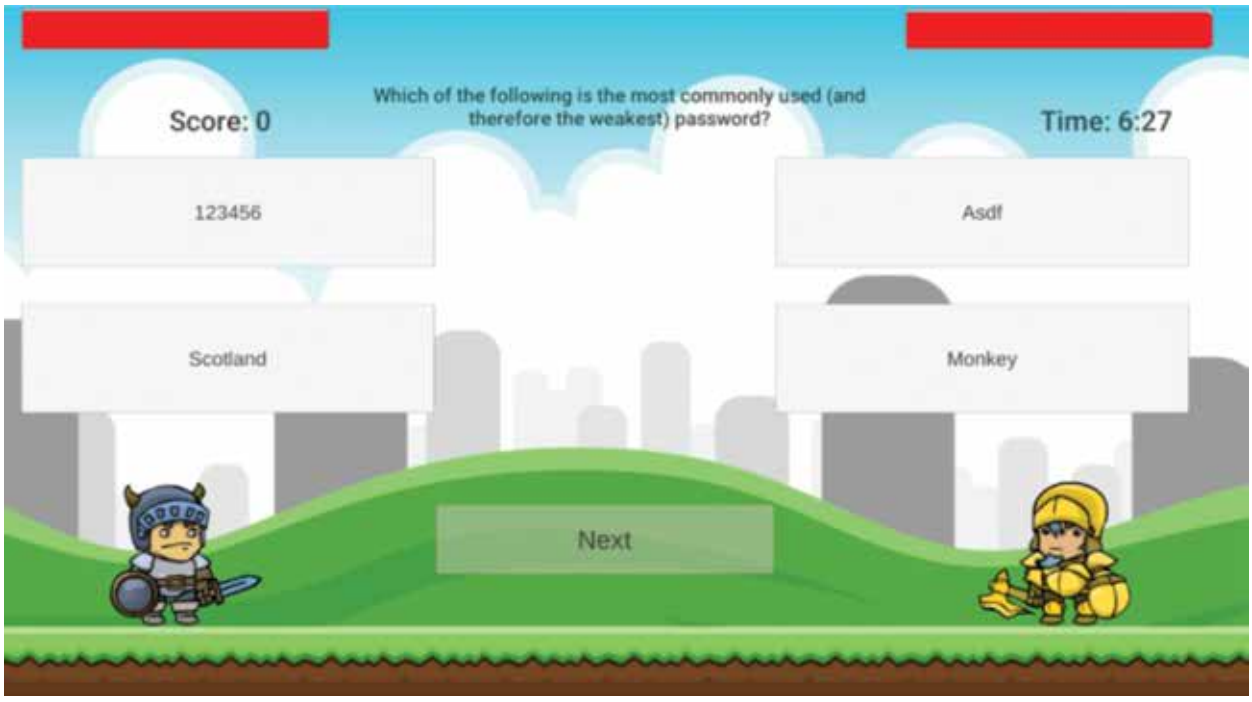
Slika 2: **Bartlejev model kategorizacije igralcev (prirejeno po Kumar et al., 2019).**

Poleg številnih aplikacij na različna področja so se metode igrifikacije izkazale za zelo učinkovite ravno na področju izobraževanja (Majuri et al, 2018). Cilj igrifikacije je narediti proces učenja zabaven z namenom vzbuditi interes za obravnavano tematiko. Tako tovrstne metode pozitivno vplivajo na motivacijo pri učenju ter posledično na učinkovitost samega učenja in učne rezultate (Damsa & Fromann, 2016). Poleg tega metode igrifikacije pomagajo razumeti povezave med abstraktnimi koncepti in vsakdanjim življenjem (Seppo, n.d.), kar »učencem« pomaga pri boljšem razumevanju proučevane tematike, kar se zopet kaže v boljših učnih rezultatih.

3 UPORABA IGRIFIKACIJE PRI OZAVEŠČANJU ZA IFORMACIJSKO VARNOST

3.1 Izkušnje iz literature

Da je uporaba metod igrifikacije za potrebe informacijsko varnostnega ozaveščanja aktualna tema, dokazuje število z obravnavano tematiko povezanih prispevkov, ki je v zadnjih letih precej naraslo. Avtorji poudarjajo pomen ozaveščanja na področju informacijske (kibernetske) varnosti, kakor tudi izpostavljajo prednosti, ki jih prinašajo metode igrifikacije v primerjavi s klasičnimi izobraževalnimi metodami. Nekateri avtorji so mnenja, da na področju informacijsko varnostnega ozaveščanja klasični pristopi izobraževanja ne zadoščajo več. Sklicujejo se na psihološke raziskave, ki priporočajo vpeljavo, sodobnih, sistemskih pristopov, kakršnega nudi tudi učenje, podprto z igrifikacijo (Scholl, 2018). Splošni vtis po pregledu literature je, da so se metode igrifikacije na področju



Slika 2: **Bartlejev model kategorizacije igralcev (prirejeno po Kumar et al., 2019).**

informacijsko varnostnega ozaveščanja izkazale kot uporabne, med uporabniki priljubljene, kakor tudi učinkovite, saj dejansko lahko pripomorejo k višjemu nivoju ozaveščenosti (Rieff, 2018).

Nekateri avtorji podajajo rezultate konkretnih empiričnih študij uvajanja metod igrifikacije pri informacijsko varnostnem ozaveščanju. Scholefield in Shepard (2019) na primer delita svoje izkušnje pri ozaveščanju uporabnikov za varno uporabo gesel. Le-to se izvaja z namensko Android aplikacijo (slika 3), ki temelji na kvizu z igranjem vlog. Rezultati dokazujejo pozitivno uporabniško izkušnjo, dejanski dvig ozaveščenosti med uporabniki, kakor tudi naklonjenost uvajanju metod igrifikacije. Podobnega mnenja so tudi avtorji raziskave Gjertsen et al. (2017), ki so uporabniško izkušnjo proučevali s pomočjo namenske prototipne interaktivne aplikacije, ki so jo testirali med zaposlenimi v dveh različnih organizacijah.

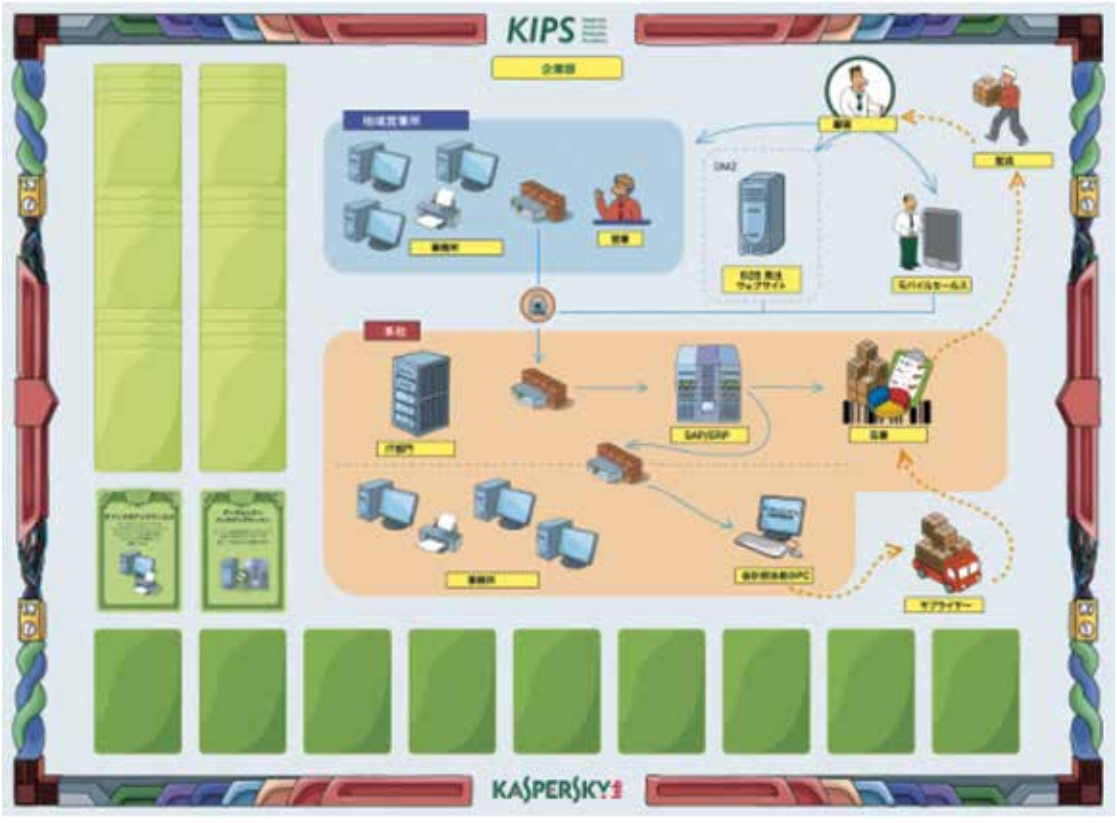
Nekateri avtorji proučujejo učinek t.i. *resnih iger*[1] (ang. serious games) in želijo raziskati, ali so tovrstne igre lahko učinkovito orodje pri ozaveščanju. Hendrix et al. (2016) in Alotaibi et al. (2016) podajajo izčrpen pregled literature in samih iger, uporabnih za namene informacijsko (kibernetsko) varnostnega ozaveščanja. Avtorji ugotavljajo, da so prvi učinki uporabe dejansko povečini pozitivni, vendar opozarjajo, da je za relevantnost rezultatov potrebno daljše obdobje opazovanja. Opozarjajo tudi na vrzel na tržišču, saj je večina tovrstnih izdelkov namenjenih povprečnim uporabnikom (splošni javnosti), pogrešajo pa igre, namenjene IT strokovnjakom.

To vrzel najbrž vsaj deloma zapolnjuje produkt Kaspersky Interactive Protection Simulation (KIPS)[2], ki omogoča skrbnikom informacijske varnosti in odločevalcem v organizacijah, da se preko simulacij različnih poslovnih okolij spopadejo z vrsto nepričakovanih kibernetskih groženj, jih skušajo obvladovati, hkrati pa povečevati dobiček in ohranjati zaupanje. Primer simulacije poslovnega okolja v sistemu KIPS prikazuje slika 4.

Rezultati eksperimentalne študije Yonemura et al. (2018) dokazujejo, da sočasno igranje več uporabnikov (ang. multiple playing) pozitivno vpliva tako na izobraževalne učinke kot na prenos veščin med uporabniki.

Antonaci et al. (2017) in Fuhrman et al. (2016) se

[1] Resne igre so igre, katerih primarni namen je širši kot zgolj zabava.
[2] https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf



Slika 4: **Primer simulacije poslovnega okolja v sistemu Kaspersky Interactive Protection Simulation (Yonemura Set al., 2018).**

ukvarjajo z uporabo igrifikacje za potrebe informacijsko varnostnega ozaveščanja mladostnikov (najstnikov in študentov). Poudarjajo, da se mladi pogosto ne zavedajo tveganj, povezanih z deljenjem zasebnih informacij v internet (npr. preko socialnih omrežij). Hkrati pa poudarjajo pomen ozaveščenosti mladih kot bodočih zaposlenih tudi z vidika organizacij in poslovnih okolij. Avtorji raziskave Antonaci et al. (2017) menijo, da igrajo ključno vlogo pri ozaveščenosti mladih njihovi učitelji, zato so razvili interaktivni spletni portal za izobraževanje učiteljev. Kot atraktiven, uporaben in učinkovit pristop za učenje mladih pa avtorji Li & Kulkarni (2016) navajajo tudi dogodke CTF (Capture-the-Flag).

3.2 Izkušnje iz prakse

Na podlagali dolgoletnih izkušenj na področju informacijsko-varnostnega ozaveščanja uporabnikov ugotavljamo naslednje: če želimo nivo ozaveščenosti uporabnikov dvigniti na želeno raven, to raven ohranjati in nenazadnje nadgrajevati, je potrebno izobraževanja izvajati sistematično in kontinuirano. Menimo, da je v večjih sistemih z velikim številom uporabnikov dobrodošel pripomoček za doseganje želenega cilja uporaba e-izobraževanja. Pri tem pa se postavlja vprašanje, na kakšen način podati izobraževalna gradiva, da bodo le-ta ne samo pritegnila uporabnika, temveč tudi zadržala njegovo pozornost skozi celoten proces učenja. Na podlagi dosedanje prakse ugotavljamo, da je eden od ključnih faktorjev, ki nam pri tem nedvomno pomaga, interaktivnost samih izobraževalnih gradiv, kar pa lahko učinkovito dosežemo z vključevanjem elementov igrifikacije.

Po našem mnenju se na področju informacijsko-varnostnega ozaveščanja uporabnikov v slovenskih poslovnih okoljih igrifikacija v pravem pomenu besede (z vsemi, v poglavju 2 predstavljenimi, elementi) v danem trenutku le redko uporablja. Najpogosteje manjka ravno element tekmovanja, vendar pa je viden porast implementacije simulacijskih iger. V takih primerih je uporabnik postavljen pred nek izziv, vsak naslednji korak pa je posledica njegove odločitve. Na tak način se posameznik sreča s problemom (npr. napad socialnega inženirja) v virtualnem okolju. Ne

Slika 5: **Šola internetne samoobrambe kot dober primer uporabe igrifikacije pri varnostnem ozaveščanju3.**

glede na to, ali je njegova posamezna izbira pravilna ali ne, se preko virtualnih izobraževalnih elementov nauči pravilnega odziva, ki ga v prihodnje lahko uporabi v realnem okolju. Uporaba igrifikacijskih metod tako preseže samo (pogosto suhoparno) teoretično učenje in uporabnika postavi bodisi v vlogo žrtve bodisi napadalca. Ključnega pomena je namreč vzpostavitev povezave med varnostnimi napadi in njihovimi potencialnimi vplivi na ljudi in podjetja. Z uporabo igrifikacije so uporabniki ves čas aktivno vključeni v usposabljanje, kar po mnenju nekaterih strokovnjakov poveča vztrajnost za učenje tudi za 75 odstotkov (Sedova, 2018). Z namenom ohranjanja pozornosti in koncentracije uporabnika je po naših izkušnjah priporočljivo tematiko razdeliti na krajše segmente, pri čemer priporočamo, da posamični segment ni daljši od 20 minut.

Odličen primer uporabe igrifikacije za ozaveščanje na področju informacijske varnosti v Sloveniji je primer izobraževanja za otroke, imenovano Šola internetne samoobrambe[3] (slika 5), pri razvoju katerega smo tudi aktivno sodelovali. Gre za interaktivni spletni portal, ki vključuje večino elementov igrifikacije, od simulacijskih iger, socialne interakcije, pa vse do pridobivanja točk (v tem primeru so otroci ob pridobivanju znanj pridobivali virtualne karateistične pasove). Rezultati omenjenega izobraževanja so bili spodbudni, saj so otroci na vseh področjih dosegli izboljšanje rezultatov pri preverjanju znanja na področju varne rabe interneta.

4 SKLEP

Metode igrifikacije kot sodobne metode izobraževanja prinašajo številne pozitivne učinke na samo učinkovitost izobraževanja in na učne rezultate. S pričujočim prispevkom smo skušali prikazati, kako lahko tovrstne metode izkoristimo tudi na področju informacijsko varnostnega ozaveščanja uporabnikov. Ker slednje predstavlja dokaj nov in v slovenskem prostoru še neraziskan koncept, menimo, da so izsledki prispevka koristni za vso strokovno javnost, predvsem pa za skrbnike informacijske varnosti v or-

[3] Šola internetne samoobrambe. https://otroci.e-ucenje.com/show.aspx?xid=WBT:X:Start.

ganizacijah, ki si vsakodnevno prizadevajo, da bi njihovi uporabniki ne le pridobili, temveč tudi ohranjali in nadgrajevali zanimanje in znanje na področju informacijske varnosti ter posledično prispevali k vse višjemu nivoju informacijske varnosti v organizaciji.

LITERATURA

[1] Alotaibi, F., Furnell, S., Stengel, I. & Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness. *International Journal for Information Security Research*, 6(2), 660-666. Pridobljeno iz: https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf

[2] Antonaci, A., Klemke, R., Stracke, C. & Specht, M. (2017, April). Gamification in MOOCs to enhance users' goal achievement. In *Proceedings of 2017 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1654-1662, IEEE Xplore. Pridobljeno iz: https://ieeexplore.ieee.org/document/7943070

[3] Damsa, A. & Fromann, R. (2016). Gamification and Gameful Approaches in Education, Business, and IT. *Informatika*, 8(1), 28-33. Pridobljeno iz: https://www.semanticscholar.org/paper/GAMIFICATION-AND-GAMEFUL-APPROACHES-IN-EDUCATION-%2C-Damsa-Fromann/fa6d5ab15a43dbd706c5d44dffa6b4e47c8bc08d

[4] Fuhrmann, F., Scholl, M., Ehrlich, E.P., Edich, D., Leiner, B. & Scholl, L. (2016, November). Raising Awareness for Information Security in a Playful Way. In *Proceedings of the London International Conference on Education (LICE)*, pp. 190-191, London: Infonomics Society. Pridobljeno iz: https://publister.bib.th-wildau.de/publister/public/publication/2119

[5] Giang, V. (2013). Gamification Techniques Increase Your Employees' Ability To Learn By 40%, *Business Insider.* Pridobljeno iz: https://www.businessinsider.com/gamification-techniques-increase-your-employees-ability-to-learn-by-40-2013-9

[6] Gjertsen, E., Gjære, E. A., & Bartnes, M. & Flores, W. (2017, February). Gamification of Information Security Awareness and Training. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pp. 59-70. SciTePress. Pridobljeno iz: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006128500590070

[7] Hamari, J., Koivisto, J. & Sarsa, H. (2014, January). Does Gamification Work? — A Literature Review of Empirical Studies on Gamification. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 3025-3034, IEEE. Pridobljeno iz: https://ieeexplore.ieee.org/document/6758978

[8] Hendrix, M., Al-Sherbaz, A. & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training?. *International Journal of Serious Games*, 3(1), 53-61. Pridobljeno iz: https://www.semanticscholar.org/paper/Game-Based-Cyber-Security-Training%3A-are-Serious-for-Hendrix-Al-Sherbaz/b5a5182a975504051ee241cff1e02caec04a1082

[9] Karimi, K. (2017). Gamification from the viewpoint of motivational theory. *Italian Journal of Science & Engineering, 2017*, 1, 34-42. Pridobljeno iz: https://ijournalse.org/index.php/ESJ/article/view/19/4

[10] Kapp, K. M. (2012). *The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education*, Pfeiffer, San Francisco, 2012.

[11] Kim, S. (2013). Fundamental Strategic Approach for Gamification : How to Start a Gamification in Your Organization. *International Journal of Digital Content Technology and its Applications*, 7(12). 48-55. Pridobljeno iz: https://www.researchgate.net/publication/310465839_Fundamental_Strategic_Approach_for_Gamification_How_to_Start_a_Gamification_in_Your_Organization

[12] Kim, S. (2013a). Recent Advances in Gamification Application. *Advances in information Sciences and Service Sciences,* 5(13), 93-99. Pridobljeno iz: https://www.researchgate.net/publication/310465687_Recent_Advances_in_Gamification_Application

[13] Koivisto, J. & Hamari, J. (2019). The rise of motivational information systems: A review of gamification research. *International Journal of Information Management*, 45, 191-210. Pridobljeno iz: https://www.sciencedirect.com/science/article/pii/S0268401217305169

[14] Kumar, J., Herger, M. & Dam, R. F. (2019). Bartle's Player Types for Gamification. *The Interaction Design Foundation.* Pridobljeno iz: https://www.interaction-design.org/literature/article/bartle-s-player-types-for-gamification.

[15] Li, C. & Kulkarni, R. (2016, June). Cybersecurity Education through Gamification – the CTF Approach. In *Proceedings of 2016 ASEE Annual Conference & Exposition*, American Society for Engineering Education. Pridobljeno iz: https://www.asee.org/public/conferences/64/papers/16728/view

[16] Majuri, J., Koivisto, J., & Hamari, J. (2018, May). Gamification of education and learning: A review of empirical literature. In *Proceedings of the 2nd International GamiFIN conference*, pp. 11-19, At Pori, Finland. Pridobljeno iz: http://ceur-ws.org/Vol-2186/paper2.pdf

[17] NIST (2003). *NIST. SP 800-50: Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology. Pridobljeno iz: https://csrc.nist.gov/publications/detail/sp/800-50/final

[18] Rieff, I. (2018). *Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach*, Master thesis, Faculty of TPM, Delft University of Technology, 2018. Pridobljeno iz: https://repository.tudelft.nl/islandora/object/uuid:bf832ca0-91d9-4be1-9a25-fe284c23d115/datastream/OBJ1/download

[19] Ryan. R. M. & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55(1), 68–78. Pridobljeno iz: https://selfdeterminationtheory.org/SDT/documents/2000_RyanDeci_SDT.pdf

[20] Scholefield, S. & Shepherd, L. (2019). Gamification techniques for raising cyber security awareness. In A. Moallem (Ed.), *HCI for cybersecurity,privacy and trust: HCII 2019*, 191-201. (Lecture Notes in Computer Science, 2019, Vol. 11594. Springer. Pridobljeno iz: https://www.researchgate.net/publication/331916014_Gamification_Techniques_for_Raising_Cyber_Security_Awareness

[21] Scholl, M. (2018). Play the Game! Analogue Gamification for Raising Information Security Awareness. *Systemics, Cybernetics and Informatics*, 16(3), 32-35. Pridobljeno iz: https://www.semanticscholar.org/paper/Play-the-Game-!-Analogue-Gamification-for-Raising-Scholl/6e23340c5ce46cfd1ae36e6f2bdddb84f02a3991

[22] Sedova, M. (2018). How Gamification Is Changing the Way Employees Engage in Security Training, *Elevate Security*. Pridobljeno iz: https://elevatesecurity.com/blog/how-gamification-is-changing-the-way-employees-engage-in-security-training/

[23] Seppo (n.d.). *Motivation Through Gamification*, Seppo.IO. Pridobljeno iz: https://seppo.io/site/assets/files/2292/motivation-through-gamification-corporate.pdf
[24] Voorhies, B. (2012). Games ancient people played. *Archaeology*, 65(3), 48-51. Pridobljeno iz: https://archive.archaeology.org/1205/features/tlacuachero_chiapas_patolli_hualapai.html
[25] Weishäupl, E., Yasasin, E. & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, 77, 807-823. Pridobljeno iz: https://www.sciencedirect.com/science/article/pii/S0167404818300555
[26] Yonemura, K. et al. (2018). Effect of security education using KIPS and gamification theory at KOSEN. In *Proceedings of 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, pp. 255-258. Pridobljeno iz: https://ieeexplore.ieee.org/document/8405480

▪

Alenka Brezavšček je izredni profesor na Fakulteti za organizacijske vede Univerze v Mariboru. Njeno habilitacijsko področje so kvantitativne metode v organizacijskih vedah. Ukvarja se z raziskavami na področju stohastičnih procesov, zanesljivosti in razpoložljivosti tehničnih sistemov ter varnosti informacijskih sistemov.

▪

Maja Minič je zaposlena na Ministrstvu za obrambo Republike Slovenije. Ima vrsto let izkušenj na področju analize in razvoja informacijskih sistemov, implementacije in razvoja e-izobraževanja, ter ozaveščanja na področju informacijske varnosti.