

Гордана ПЕТРОВИЋ
Филозофски факултет
Универзитет у Нишу

УДК 371.3:004
37.091.327.7
- оригинални научни рад-
DOI: 10.5937/gufv2202037P

РАЗВИЈЕНОСТ ДИГИТАЛНИХ КОМПЕТЕНЦИЈА УЧЕНИКА У ДОМЕНУ БЕЗБЕДНОСТИ

Сажетак: *Актуелна епидемијска ситуација допринела је да коришћење дигиталних технологија у свим аспектима живота и рада постане свакодневица. Тако се у први план истичу дигиталне компетенције које постају један од основних услова за сналажење и функционисање како у свакодневном животу, тако и у образовању. Како се акценат углавном ставља на испитивање оспособљености коришћења дигиталних технологија, у други план стављене су безбедност и заштита приватности дигиталних технологија, као и својих података на интернету. Због тога је важно сагледати да ли су и колико ученици оспособљени за очување своје безбедности кроз овај домен дигиталне компетенције. У раду се истражују дигиталне компетенције ученика средњих школа из домена безбедности. Циљ истраживања је утврдити нивое дигиталних компетенција ученика у домену безбедности. Настојали смо, такође, да утврдимо да ли постоје разлике у нивоима дигиталних компетенција ученика с обзиром на њихов школски успех, пол и разред. Резултати реализованог истраживања показују да је највећи број ученика овладао основним нивоом дигиталних компетенција из домена безбедности, али није занемарљив ни број ученика који су на самосталном и напредном нивоу из овог домена. Такође је утврђено да не постоје статистички значајне разлике у односу на пол, школски успех и разред ученика.*

Кључне речи: *дигиталне компетенције, ученици, безбедност, дигиталне технологије.*

Увод

Оспособљеност за коришћење дигиталних технологија у свакодневном животу од великог је значаја. Епидемиолошка ситуација допринела је подизању свести о значају дигиталних компетенција за све сфере живота и рада. Дигитални идентитет који имамо на интернету може врло лако бити злоупотребљен уколико нисмо оспособљени да се адекватно заштитимо. Од

* g.petrovic-17784@filfak.ni.ac.rs

великог значаја је указати ученицима какве опасности постоје на интернету и до каквих последица може довести несавесно коришћење дигиталних технологија и интернета. Потреба за образовањем младих о безбедности и приватности у дигиталном свету постаје све важнија. Влада Србије је 2016. године усвојила први системски акт из ове области – Уредбу о безбедности и заштити деце приликом коришћења информационо-комуникационих технологија. Желели смо да испитамо да ли су ученици оспособљени да заштите своје податке на интернету и своје уређаје којима њему приступају. У раду ће бити представљени резултати из домена безбедности, као део истраживања којим је обухваћено свих пет домена дигиталних компетенција (обрада информација, комуникација, стварање садржаја, безбедност и решавање проблема).

Неминовно је да млади не могу замислити живот без дигиталних технологија и интернета, али оно што је најбитније јесте њихово оспособљавање за адекватно коришћење и безбедност у том процесу. У раду ће бити представљен и значај развоја дигиталних компетенција из домена безбедности, као и досадашња истраживања из ове области. Потреба за образовањем о безбедности и приватности током коришћења дигиталних технологија постаје све већа. Развијање овог домена дигиталних компетенција подразумева најпре утврђивање нивоа знања и способности из ове области како би се приступило њиховом унапређивању.

Значај домена безбедности дигиталне компетенције

Број истраживања о дигиталној безбедности повећао се током последње деценије (нпр. Jones, Mitchell, & Finkelhor, 2013; Shin, 2015; Simandl & Vaníček, 2017; Chou & Peng, 2011; Napal, Peñalva-Vélez, & Mendióroz, 2018). Значајан део истраживања дигиталне компетенције углавном се фокусира углавном на процену дигиталне или информатичке писмености, док се знатно мањи број истраживања бави доменом безбедности приликом коришћења дигиталних технологија.

Концепт безбедности који се односи на коришћење информационо-комуникационе технологије заснива се на три основна принципа (Schneider, 1998): поверљивости, интегритету и доступности. Поверљивост се односи на спречавање злоупотребе, заштиту података и поштовање ауторских права. Интегритет осигурава заштиту информација, док доступност подразумева да информације треба да буду доступне кад год су потребне.

У документу Стандарди општих међупредметних компетенција за крај средњег образовања из 2013. године, дигитална компетенција односи се на способност ученика да користи расположива средства из области информационо-комуникационих технологија (уређаје, софтверске производе, електронске комуникационе услуге и услуге које се користе путем електронских комуникација) на одговоран и критички начин ради ефикасног испуњавања постављених циљева и задатака у свакодневном животу, шко-

ловању и будућем послу. Ученик треба да познаје и основне карактеристике расположивих информационо-комуникационих технологија и могућности њихове примене у свакодневном животу, раду и образовању, односно њихов утицај на живот и рад појединца и заједница (*Стандарди опитних међупредметних компетенција за крај средњег образовања*, 2013).

Дигитално компетентан појединац из домена безбедности треба да буде свестан да постоје софтверски вируси, али и да зна колики је значај неопходности заштите личних података, као и заштите сопственог здравља и здравља других људи приликом употребе дигиталних технологија (Kluzer & Pujol Priego, 2018). Истраживања из области дигиталних компетенција интензивирани су у последњој деценији као одговор на све бржи развој дигиталних технологија. Домен безбедности односи се на заштиту личних података и дигиталних уређаја који се користе, на свест о онлајн ризицима, на знање и способности како се заштитити у дигиталном свету и свест о здравственим ризицима повезаним са коришћењем дигиталних технологија. Развијање свести о безбедности веома је важно не само у дигиталном свету, већ и у реалном животу. Системска подршка ученицима за стицање дигиталних вештина које омогућавају заштиту од потенцијалних ризика током коришћења дигиталних технологија од великог је значаја (Кузмановић и сар., 2019).

Неразвијеност свести о безбедности приликом коришћења дигиталних технологија потиче од неупућености у претње које њихово коришћење носи са собом. Грешке просечног корисника дигиталних технологија јесу грешка наивности и грешка поверења, а последице које настају – непредузимање мера заштите приватности (Путник, Бабић и Кордић, 2014).

Развијање дигиталне компетенције код ученика треба, између осталог, да доведе до јачања свести о мерама безбедности које ће заштити приватност корисника и обезбедити сигурност уређаја путем којих се приступа интернету и делује у дигиталном свету. Дигиталне компетенције су, према нивоима развијености код корисника, разврстане кроз пет области (домена) (Kluzer & Pujol Priego, 2018), а то су: обрада информација, комуникација у дигиталном окружењу, стварање дигиталног садржаја, безбедност у дигиталном окружењу и решавање проблема. С обзиром на то да се у овом раду бавимо доменом безбедности у дигиталном окружењу, табеларно ће бити представљен само овај домен дигиталне компетенције (Табела 1).

Табела 1. Самопроцена дигиталних компетенција из домена безбедности

ДОМЕН БЕЗБЕДНОСТИ	
Основна употреба (ниво)	Могу да предузем основне кораке за заштиту својих уређаја (нпр. да користим антивирус програме и лозинке). Знам да нису све информације на интернету поуздане. Знам да моји кориснички подаци (корисничко име и лозинка) могу бити украдени. Знам да не треба да откривам личне информације на интернету. Знам да превише коришћења дигиталних технологија може да нашкоди мом здрављу. Предузимам основне мере за уштеду енергије.
Самостална употреба (ниво)	На рачунару који користим за приступ интернету имам инсталиране програме за заштиту безбедности (антивирус, заштитни зид). Редовно користим и ажурирам ове програме. Користим различите лозинке за приступ опреми, уређајима и дигиталним услугама и периодично их мењам. Умем да препознам интернет странице или електронску пошту који могу бити употребљени за превару. Могу да препознам електронску пошту послату са намером да корисника завара да долази од познатог пошиљача. Умем да градим свој дигитални идентитет и да пратим какав дигитални отисак остављам. Разумем ризике по здравље које са собом носи коришћење дигиталних технологија (нпр. ергономија, ризик од зависности). Разумем позитивне и негативне утицаје технологије на животну средину.
Напредна употреба (ниво)	Редовно проверавам безбедносна подешавања и системе на својим уређајима и/или апликацијама које користим. Знам како да реагујем ако је мој рачунар заражен вирусом. Умем да подесим или изменим заштитни зид и безбедносна подешавања на својим дигиталним уређајима. Знам да шифрирам своју електронску пошту или датотеке. Могу да применим филтере на нежељену електронску пошту. Информационо-комуникационе технологије користим разумно како бих избегао/ла здравствене проблеме (физичке и психолошке). Мој став о томе какав утицај дигиталне технологије имају на свакодневни живот, потрошњу на интернету и животну средину утемељен је на информацијама.

У Извештају о дигиталној укључености у Републици Србији за период од 2014. до 2018. године истиче се да је Национална стратегија о информационој безбедности за период 2017. до 2020. године препознала безбедност деце, као посебно значајан аспект развоја информационе безбедности појединца (Ожеговић и сар., 2019). Министарство је од 2017. године успоставило Национални контакт центар за безбедност деце на интернету као место за пружање савета и пријем пријава које су у вези са безбедношћу деце на интернету.

Према аутору Фишеру (Fischer, 2005), када се говори о безбедности на интернету, то се односи на следеће три ствари: 1) скуп активности и других мера за заштиту компјутера, мрежа, хардвера, софтвера и података од напада; 2) стање или квалитет заштићености од таквих претњи и 3) поље деловања које се односи на истраживање и анализу у циљу спровођења и унапређивања тих активности и њиховог квалитета.

Безбедност и сигурност на интернету постану важни тек када се јави одређени проблем и дође до негативних последица приликом коришћења дигиталних технологија и приступања интернету. Тада се увиђа значај превенције из ове области како до таквих проблема не би дошло. Нико не може да гарантује потпуну сигурност на интернету, али она умногоме зависи од сопственог понашања. Треба радити на едукацији корисника о томе који су потенцијални ризици употребе дигиталних технологија и приступања интернету. Треба да постоји континуирана едукација која ће садржати мере заштите које треба предузимати како би се заштитили сопствени подаци и уређаји којима се приступа интернету.

Приказ резултата претходних истраживања

Истраживања која се односе на безбедност приликом коришћења дигиталних технологија нема у довољној мери у складу са њиховом неопходношћу. У Малезији је 2013. године у школама обављено испитивање ставова код 13945 ученика узраста од 7 до 19 година о сигурности, прикладном понашању на интернету и њиховој способности да се заштите на мрежи (DiGi, 2014). Резултати су показали да 80% ученика сматра да је сигурност на интернету важна, 40% њих не зна како да се заштити и 45% не осећа се сигурно на интернету (DiGi, 2014).

Постоји повезаност између различитих врста ризичних понашања на интернету и у свакодневном животу, док се емоционално стабилни и савесни појединци понашају опрезније на интернету (Karl, Peluchette & Schlaegel, 2010). Импулсивност, наивност и слабо развијене вештине за доношење одлука код деце доприносе да она буду најизложенија ризику и преварама на интернету (Kušić, 2010).

Ауторке Дејвис и Џејмс (Davis & James, 2013) у истраживању у коме је учествовало 42 ученика, интервјуисањем су желеле да испитају њихова размишљања о сигурности на интернету, приватности на друштвеним мрежама и њиховом начину ношења са тим изазовима. Резултати показују да ученици цене приватност и користе различите стратегије како би се заштитили, од којих је једна да не објављују своје личне податке. Иако је у питању мали узорак, ауторке су, пре свега, хтеле да укажу на важност спровођења сличних истраживања.

Истраживањем које је у Републици Хрватској спровела група аутора са циљем испитивања ризичног понашања 355 корисника компјутера у средњошколској популацији, дошло се до података којима би требало упозорити државне институције и наставнике у школама. Они истичу неопходност развијања ефикаснијих образовних програма и програма превенције који би имали за циљ повећање сигурног понашања када се ради о сигурности и заштити приватности на интернету (Velki i sar., 2017).

Аутор Ер и сарадници (Er et al., 2017) испитивали су свесност студената о питањима сигурности на интернету и њиховој способности да се заштите од ризика и установили су следеће: 1) студенти су се осећали при-

лично сигурно када су били на интернету; 2) имају добро разумевање шта представљају ризичне онлајн активности; 3) знају како да се заштите и 4) препознају важност учења о сигурности на интернету.

Позитивни предиктори поштовања сигурносних правила заштите личних података су савесност, прилагодљивост, емоционална стабилност и склоност преузимању ризика (McCormac et al., 2017). Корисници углавном не размишљају о заштити приватности и мерама које треба да предузму док им се не догоди негативно искуство. Поједина истраживања бавила су се и квалитетом и снагом лозинке корисника (Dell'Amico, Michiardi & Roudier, 2010; Kelley et al., 2012; Voyiatzis et al., 2011; Wanli et al., 2010).

Углавном у већини истраживања узорак су корисници млађег узраста док се приватности и сигурности старијих корисника не придаје велика важност. Разлог овоме може бити то што су деца подложнија ризицима на интернету и недовољно образована како да заштите своју приватност и обезбеде сигурност.

Методолошки оквир истраживања

Предмет овог истраживања био је ниво развијености дигиталних компетенција ученика из домена безбедности. Рад је имао за циљ утврђивање нивоа дигиталних компетенција из домена безбедност код ученика средњих школа. Из постављеног циља произашли су следећи задаци истраживања:

1. Утврдити ниво дигиталних компетенција ученика из домена безбедности.
2. Установити да ли постоји статистички значајна разлика у погледу нивоа дигиталних компетенција ученика из домена безбедности с обзиром на њихов пол.
3. Утврдити повезаност између нивоа дигиталних компетенција ученика из домена безбедности и њиховог школског успеха.
4. Установити да ли постоји статистички значајна разлика у погледу нивоа дигиталних компетенција ученика из домена безбедности с обзиром на њихов разред.

На основу циља и задатака истраживања, постављене су следеће хипотезе:

1. Претпоставља се да је већина ученика на нивоу основне употребе дигиталних компетенција из домена безбедности.
2. Претпоставља се да постоји статистички значајна разлика у погледу нивоа дигиталних компетенција ученика из домена безбедности с обзиром на њихов пол.
3. Претпоставља се да постоји повезаност између нивоа дигиталних компетенција ученика из домена безбедности и њиховог школског успеха.
4. Претпоставља се да постоји статистички значајна разлика у погледу нивоа дигиталних компетенција ученика из домена безбедности с обзиром на њихов разред.

У истраживању су коришћене дескриптивна метода и техника скалирање. На скали Ликертовог типа испитане су самопроцене ученика о нивоима дигиталних компетенција. Теоријско полазиште за израду овог инструмента налази се у класификацији дигиталних компетенција датој у ДигКом 1.0 (Оквир за развој и разумевање дигиталних компетенција у Европи), који је Европска комисија објавила 2013. године (Ferrari, 2013). Подаци који су добијени на основу одговора ученика на петостепеној скали обрађени су коришћењем SPSS 20 статистичког програма (фреквенција, t-тест, корелација, једнофакторска анализа варијансе).

Узорак истраживања чинила су 103 ученика средњих школа који живе у домовима ученика у Крушевцу, Трстенику и Александровцу. Варијабле у истраживању јесу: пол (две категорије), школски успех (четири категорије: одличан, врло добар, добар, довољан), разред средње школе (четири категорије: први, други, трећи и четврти). Као што можемо видети у Табели 2, од 103 ученика, 44 су мушког, а њих 59 женског је пола. Када је школски успех у питању, 57,3% ученика је са одличним успехом, 30,1% са врло добрим, 11,7% са добрим и 1,9% довољним успехом. Узорак је прилично уједначен у погледу ученика различитих разреда: 30,1% ученика похађа први разред, 20,4% други разред, 27,2% трећи разред и 22,3% ученика похађа четврти разред средње школе.

Табела 2. Структура узорка

Варијабле			
Пол	Мушки	f	44
	пол	%	42,7
	Женски	f	59
	пол	%	57,3
Школски успех	Одличан	f	59
		%	57,3
	Врло добар	f	31
		%	30,1
	Добар	f	12
		%	10,7
Разред средње школе	Довољан	f	1
		%	1,9
	Први	f	31
		%	30,1
	Други	f	21
		%	20,4
	Трећи	f	28
		%	27,2
	Четврти	f	23
		%	22,3

Анализа и интерпретација резултата истраживања

Све већа заступљеност дигиталних технологија у свакодневном животу подразумева и бољу оспособљеност за њено коришћење. Осим дигиталних вештина које омогућавају адекватно коришћење дигиталних технологија, неопходна су и знања како обезбедити сигурност свог идентитета и уређаја који се користе. У раду ће бити представљени резултати самопроце-на ученика у погледу нивоа дигиталних компетенција из домена безбедност.

Увидом у Табелу 3, где теоријски максимум износи 30, види се да је просечни скор из домена безбедности релативно висок.

Табела 3. Приказ дескриптивних статистичких показатеља за домен безбедности дигиталне компетенције

Скала/тврдње	N	Min	Max	AC	СД
Безбедност	103	17	30	23,41	2,87

Први истраживачки задатак је био утврдити ниво дигиталних компетенција ученика из домена безбедности. Ученици највећи степен слагања (сумиране категорије *сагласан сам* и *у потпуности сам сагласан*) изражавају на две тврдње са основног нивоа, па тако 95% њих тврди да зна да њихови кориснички подаци могу бити украдени, док 85% сматра да може да предузме основне кораке за заштиту својих уређаја. Око 80% ученика уме да препозна интернет странице или електронску пошту које могу бити употребљене за превару, док 75% њих користи различите лозинке и периодично их мења – обе тврдње су са самосталног нивоа. Да редовно проверавају безбедносна подешавања и системе на својим уређајима и/или апликацијама које користе тврди око 70% ученика, док половина њих може да примени филтере на нежељену електронску пошту, око 30% је неодлучно по овом питању, а петина то не уме да уради. Када се сумирају сви одговори на тврдње о нивоима дигиталних компетенција из домена безбедности, може се закључити да се ученици налазе на основном нивоу употребе. Према томе, наша хипотеза да се већина ученика налази на основном нивоу употребе из домена безбедности потврђена је, јер се увидом у резултате истраживања може уочити да већина ученика изражава сагласност (сумиране категорије *сагласан сам* и *у потпуности сам сагласан*) са тврдњама које се односе на основни ниво компетенција. Такође, из резултата можемо видети да велики број ученика изражава сагласност и са тврдњама које се односе на самостални и напредни ниво употребе из домена безбедности дигиталне компетенције. Група аутора на узорку од 317 студената у Шпанији спровела је истраживање у коме је дошла до података да се 47% студената налази на средњем (самосталном) нивоу дигиталних компетенција из домена безбедности, као и да постоји спремност за безбедно понашање, али је не прате довољно знања и вештина које би то омогућиле (Gallego-Arrufat, Torres-Hernandez & Pessoa, 2019).

Како би се вештине и способности из области дигиталне безбедности унапредиле, неопходно је најпре утврдити ниво дигиталних компетенција из ове области, а затим осмислити програме превенције и образовања за безбедно и одговорно коришћење интернета (Chou & Peng, 2011; Fernandez-Montalvo, Penalva & Irazabal, 2015).

Тема насиља међу ученицима је увек актуелна, посебно његов облик – дигитално (електронско) насиље. Управо развијање дигиталних компетенција из домена безбедности може утицати на смањење учесталости дигиталног насиља код ученика.

Табела 4. Дистрибуција одговора испитаника на тврдње из домена безбедности

Тврдња	Уопште нисам сагласан	Нисам сагласан	Неодлучан сам	Сагласан сам	У потпуности сам сагласан
Предузимам основне кораке за заштиту својих уређаја (нпр. користим антивирус програме и лозинке).	0,0 %	1,9 %	13,6 %	55,3 %	29,1 %
Користим различите лозинке за приступ опреми, уређајима и дигиталним услугама и периодично их мењам.	3,9 %	13,6 %	7,8 %	53,4 %	21,4 %
Редовно проверавам безбедносна подешавања и системе на својим уређајима и/или апликацијама које користим.	1,9 %	12,6 %	12,6 %	49,5 %	23,3 %
Знам да моји кориснички подаци (корисничко име и лозинка) могу бити украдени.	0,0 %	1,9 %	2,9 %	56,3 %	38,8 %
Умем да препознам интернет странице или електронску пошту који могу бити употребљени за превару.	1,0 %	1,0 %	16,5 %	61,2 %	20,4 %
Могу да применим филтере на нежељену електронску пошту.	2,9 %	15,5 %	27,2 %	43,7 %	10,7 %

Добијени резултати указују нам на значај развијања дигиталних компетенција из домена безбедности, с обзиром на то да смо утврдили да се ученици налазе на основном нивоу употребе. Ово нам указује на потребу да се средњошколско образовање унапреди увођењем изборних предмета који би јачали дигиталне компетенције код ученика, а самим тим и домен безбедности, који је важан и у сегменту коришћења дигиталних технологија у слободном времену ученика. Дигиталне технологије све више прожимају све сфере друштва, а систем образовања је тај који треба да омогући адекватну оспособљеност грађана за њихово коришћење.

Наредним истраживачким задатаком желели смо установити да ли постоји статистички значајна разлика у погледу нивоа дигиталних компетенција ученика из домена безбедности с обзиром на њихов пол. Т-тестом независних узорака утврђено је да не постоје статистички значајне разлике између самопроцена ученика мушког и женског пола. Овим је наша хипотеза истраживања оповргнута. До сличних резултата дошло се у још неким истраживањима, која на основу добијених података указују да не постоји разлика између мушких и женских учесника у компаративним истраживањима дигиталних компетенција (Cabero-Almenara et al., 2021; Hatlevik & Hatlevik, 2018). Истраживања показују и да су просечни резултати жена виши од мушкараца (Guillen-Gamez et al., 2020; Krumsvik et al., 2016), као и да мушкарци имају виши ниво дигиталне и технолошке компетенције (Scherera et al., 2017).

Табела 5. Статистичка значајност разлика у одговорима испитаника с обзиром на пол

Скала/домен	Пол	N	AS	SD	t	p
Безбедност	мушки	44	23,48	2,62	0,211	0,833
	женски	59	23,36	3,06		

Напомена: N – број испитаника, AS – аритметичка средина, SD – стандардна девијација, t – статистик, p – статистичка значајност

Поређењем ученика у погледу нивоа дигиталне компетенције из домена безбедности у односу на разред дошло се до податка да не постоје статистички значајне разлике у њиховим одговорима на основу резултата приказаних у Табели 6. Ова хипотеза истраживања није потврђена, јер се у истраживању пошло од претпоставке да постоје статистички значајне разлике у одговорима ученика с обзиром на њихов разред.

Табела 6. Поређење просечних вредности дигиталних компетенција из домена безбедности у односу на разред

Скала/домен	Сума квадрата	df	Просечан квадрат	F	P
Безбедност	Између група	36,711	3	12,237	1,510 0,217
	Унутар група	802,163	99	8,103	
	Укупно	838,874	102		

Напомена: df – степени слободе, F – статистик, p – статистичка значајност

Повезаност школског успеха и нивоа дигиталних компетенција ученика из домена безбедности није доказана корелационом анализом. Резултати показују да не постоји повезаност између школског успеха и нивоа дигиталне компетенције ученика из домена безбедности ($r=0.050$, $p=0.619$). То значи да нема статистички значајних разлика у погледу нивоа дигиталних компетенција ученика из домена безбедности с обзиром на њихов школски успех.

Табела 7. *Статистичка значајност разлика у одговорима испитаника
с обзиром на школски успех испитаника*

Школски успех	Безбедност	
	Pearson Correlation	0,050
	Sig.	0,619
	N	103

Напомена: Spearman's rho – статистик, Sig. – статистичка значајност, N – број испитаника

Закључак

Дигиталне технологије и интернет постали су доступни скоро свима, али нажалост, поставља се питање да ли сви који имају приступ њима знају да предузму мере којима би заштитили своју приватност и омогућили безбедност приликом коришћења. Све већа доступност дигиталних технологија доводи до повећања корисника, што условљава и неопходност развоја њихових дигиталних компетенција за ефикасно функционисање у дигиталној ери у којој се налазимо. Свесни смо да дигитализација друштва у коме живимо и радимо још увек представља неоткривену област за многе. Они који сматрају да добро владају дигиталним технологијама нису освестили своје слабости и недостатке у том процесу. Безбедност у области коришћења дигиталних технологија је веома значајна и треба радити на системском оспособљавању свих корисника у том процесу. Добијени резултати у овом истраживању указују нам да се ученици налазе на основном нивоу употребе из домена безбедности дигиталних компетенција, што значи да треба радити на њиховом унапређивању и развијању како би се достигао виши ниво. Само учествовање ученика у истраживањима о безбедности на интернету може допринети освешћивању значаја адекватне заштите у дигиталном простору.

Дигиталну компетенцију, као једну од кључних компетенција целоживотног учења, треба континуирано развијати у складу са напретком дигиталне технологије. Домен безбедности у оквиру дигиталне компетенције постаје све важнији јер сигурност и заштићеност ученика приликом коришћења дигиталних технологија треба да буде на првом месту. Упознавање ученика и њихових родитеља са потенцијалним ризицима, као и начинима како да се заштите, представља основу развијања дигиталних компетенција из домена безбедности.

Ова област дигиталних компетенција све више ће добијати на значају са бржим развојем дигиталних технологија и представљаће изазов у образовању у смислу начина њеног развијања код ученика. Веома је битно разграничавање шта је то што би школа требало да пружи ученицима и на који начин би требало пратити развој ове компетенције код њих од најранијег узраста. Системски приступ у проучавању и развијању дигиталних компетенција код ученика је неопходан како би се на тај начин проналазиле области које треба унапређивати.

Истраживање самопроцена ученика о нивоима дигиталних компетенција из домена безбедности има својих ограничења. Ова ограничења огледају се у питању да ли ученици на прави начин процењују своје дигиталне компетенције. Да би дигиталне компетенције из домена безбедности успешно биле испитане, неопходно је ставити ученике у проблемске ситуације и на тај начин утврдити колико су они оспособљени да се заштите у дигиталном окружењу. Правци будућих истраживања из ове области треба да буду усмерени на откривање домена дигиталних компетенција које треба развијати како би успешност коришћења дигиталних технологија од стране ученика била у складу са њиховим убрзаним развојем и потребама образовања.

Литература

1. Chou, C. & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education*, 14(1), 44-53. <https://doi.org/10.1016/j.iheduc.2010.03.006>
2. Davis, K. & James, C. (2013). Tweens' conceptions of privacy online: implications for educators. *Learning, Media and Technology*, 38(1), 4-25. <https://doi.org/10.1080/17439884.2012.658404>
3. Dell'Amico, M., Michiardi, P. & Roudier, Y. (2010). Password strength: An empirical analysis. In *Proceedings IEEE INFOCOM* (1-9).
4. DiGi. (2014). *Safety net: Capacity building among Malaysian school children on staying safe online*. A national survey report. Preuzeto sa: https://safeinternet.my/wp-content/uploads/2021/02/CyberSAFE_Survey_Report_2014.pdf
5. Er, P. H., Cheah, P. K., Moses, P., Chong, C. K. & Ang, B. H. (2017). Awareness of Safe and Responsible Use of ICT Among Students in a Malaysian University. In *Empowering 21st Century Learners Through Holistic and Enterprising Learning* (41-48). Springer, Singapore.
6. Ferrari, A. (2013). DIGCOMP: A Framework for Developing and Understanding Digital Competence. *JRC Science and Policy Reports*. Luxembourg: Publications Office of the European Union.
7. Fernández-Montalvo, J., Peñalva, A. & Irazabal, I. (2015). Hábitos de uso y conductas de riesgo en Internet en la preadolescencia.[Internet use habits and risk behaviours in preadolescence]. *Comunicar*, 44, 113–121. <https://doi.org/10.3916/C44-2015-12>
8. Fischer, E. A. (2009). *Creating a National Framework for Cybersecurity: an Analysis of Issues and Options*, New York, Nova Science Publisher, Inc. <https://apps.dtic.mil/sti/pdfs/ADA463076.pdf>
9. Gallego-Arrufat, M., Torres-Hernández, N. & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar. Media Education Research Journal*, 27(2). DOI <https://doi.org/10.3916/C61-2019-05>
10. Guillén-Gámez, F. D., Mayorga-Fernández, M. J., Bravo-Agapito, J. & Escribano-Ortiz, D. (2020). Analysis of teachers' pedagogical digital competence: Identification of factors predicting their acquisition. *Tech Know Learn*, 26, 481–498. <https://doi.org/10.1007/s10758-019-09432-7>

11. Jones, L.M., Mitchell, K.J. & Finkelhor, D. (2013). Online harassment in context: Trends from three youth internet safety surveys. *Psychology of Violence*, 3(1), p. 53-69. <https://doi.org/10.1037/a0030309>
12. Kaleli, Y. S. (2020). The effect of computer-assisted instruction on piano education: An experimental study with pre-service music teachers. *International Journal of Technology in Education and Science*, 4(3), 235-246. <https://doi.org/10.46328/ijtes.v4i3.115>
13. Karl, K., Peluchette, J. & Schlaegel, C. (2010). Who's posting Facebook faux-pas? A crosscultural examination of personality differences. *International Journal of Selection and Assessment*, 18(2), 174-186
14. Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L. & Lopez, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *IEEE symposium on security and privacy* (523-537).
15. Kluzer S. & Pujol Priego L. (2018). DigComp into Action – Get inspired, make it happen. S. Carretero, Y. Punie, R. Vuorikari, M. Cabrera, and O'Keefe, W. (Eds.). *JRC Science for Policy Report, EUR 29115 EN*, Publications Office of the European Union, Luxembourg, 2018.
16. Krumsvik, R., Jones, L., Øfstegaard, M. & Eikeland, O. (2016). Upper secondary school teachers' digital competence: Analysed by demographic, personal and professional characteristics. *Nordic Journal of Digital Literacy*, 11(3), 143–164. <https://doi.org/10.18261/issn.1891-943x-2016-03-02>
17. Kuzmanović, D., Pavlović, Z., Popadić, D. i Milošević, T. (2019). *Korišćenje interneta i digitalne tehnologije kod dece i mladih u Srbiji: rezultati istraživanja Dece Evrope na internetu*. Beograd: Institut za psihologiju Filozofskog fakulteta u Beogradu.
18. Kušić, S. (2010). Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: navike Facebook generacije. *Život i škola*, 24(2), 103–125.
19. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computer in Human Behavior*, 69(3), 151–156.
20. Napal, M., Peñalva-Vélez, A. & Mendióroz, A. (2018). Development of digital competence in secondary education teachers' training. *Education Sciences*, 8, 104. <https://doi.org/10.3390/educsci8030104>
21. Ожеговић, Ј., Перков, Б., Мишић, Ј., Винкић, Д. М., Кузманов, Ј. и Јовановић, Д. (2019). Извештај о дигиталној укључености у Републици Србији за период од 2014. до 2018. године. *Тим за социјално укључивање и смањење сиромаштва Владе Републике Србије*.
22. Putnik, N., Babić, L. i Kordić, B. (2014). Socio-psihološki i bezbednosni rizici narušavanja privatnosti na društvenim mrežama. *Sinteza - Impact of the Internet on Business Activities in Serbia and Worldwide*. doi:10.15308/sinteza-2014-683-686
23. Schneier, B., (1998). Cryptographic design vulnerabilities. *Computer (Long Beach Calif)* 31, 29–33. <https://doi.org/10.1109/2.708447>
24. Scherera R., Tondeurb, J., & Siddiq, F. (2017). On the quest for validity: Testing the factor structure and measurement invariance of the technology - dimensions in the Technological, Pedagogical, and Content Knowledge (TPACK) model. *Computers & Education*, 112, 1-17. <https://doi.org/10.1016/j.compedu.2017.04.012>

25. Shin, S.K. (2015). Teaching critical, ethical, and safe use of ICT in pre-service teacher education. *Language Learning & Technology*, 19(1), p. 181-197. <https://doi.org/10125/44408>
26. Simandl, V. & Vaníek, J. (2017). Influences on ICT teachers' knowledge and routines in a technical e-safety context. *Telematics and Informatics*, 34(8), 1488-1502. <https://doi.org/10.1016/j.tele.2017.06.012>
27. Tang, T. & Austin, J. (2009). Students' perceptions of teaching technologies, application of technologies, and academic performance. *Computers and Education*, 53(4), 1241–1255. <https://doi.org/10.1016/j.compedu.2009.06.007>
28. Velki, T., Šolić, K., Gorjanac, V. i Nenadić, K. (2017). Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings*, 1496-1500. DOI: 10.23919/MIPRO.2017.7973620
29. Voyiatzis, A. G., Fidas, C. A., Serpanos, D. N. & Avouris, N. M. (2011). An Empirical Study on the Web Password Strength in Greece. *15th Panhellenic Conference on Informatics*, 212-216.
30. *Standardi opštih međupredmetnih kompetencija za kraj srednjeg obrazovanja* (2013). Beograd: Zavod za vrednovanje kvaliteta obrazovanja i vaspitanja. Dostupno na: https://ceo.edu.rs/wpcontent/uploads/obrazovni_standardi/Opsti_standardi_postignuca/MEDJUPREDMETNE%20KOMPETENCIJE.pdf (Pristupljeno 25. 03. 2022).
31. Wanli, M., Campbell, J., Tran, D. & Kleeman, D. (2010). Password Entropy and Password Quality. *4th International Conference on Network and System Security*, 583-587.

DEVELOPMENT OF DIGITAL COMPETENCES OF STUDENTS IN THE SECURITY DOMAIN

Summary: *The current epidemiological situation has contributed to the use of digital technologies in all aspects of life and work becoming everyday. Thus, digital competences stand out in the foreground, becoming one of the basic conditions for coping and functioning both in everyday life and in education. As the emphasis is mainly on testing the ability to use digital technologies, security and privacy protection of digital technologies as well as one's data on the Internet is placed in the background. That is why it is important to see if and to what extent students are trained to preserve their safety through this domain of digital competence. The paper investigates the digital competences of high school students in the field of security. The aim of the research is to determine the levels of students' digital competences in the domain of security. We also tried to determine whether there are differences in the levels of students' digital competences with regard to their school performance, gender and grade. The results of the conducted research show that the largest number of students have mastered the basic level of digital competences in the domain of security, but the number of students who are at an independent and advanced level in this domain is also not negligible. It was also determined that there are no statistically significant differences in relation to gender, school performance and class of students.*

Key words: *digital competences, students, security, digital technologies.*