УДК 343.533::004
371.3:004
DOI: https://doi.org/10.5937/bastina32-38103

Оригинални научни рад

*Радослав В. БАЛТЕЗАРЕВИЋ**
Мегатренд универзитет, Факултет за пословне студије, Београд, Република Србија

ДИГИТАЛНА ПИСМЕНОСТ КАО СРЕДСТВО ПРЕВЕНЦИЈЕ ПРОТИВ САЈБЕР КРИМИНАЛА**

Апстракт: Данас је тешко замислити како би човек функционисао у савременом друштву без употребе технологија заснованих на интернету. Свакодневне интеракције које се дешавају у дигиталном окружењу прожимају све сфере друштва, омогућавајући комуникацију, забаву али и пословање корисника. Међутим, недостатак технолошких вештина и дигиталне писмености код великог броја људи повећавају шансе да они постану жртве различитих видова, сајбер криминалних активности. Овакве активности често могу имати веома тешке физичке, материјалне и емоционалне последице по кориснике интернета и друштвених мрежа. Такође, није редак случај да интеракција са злонамерним сајбер криминалцем доведе и до трагичних последица. Овај проблем нарочито погађа најмлађу популацију, која свакодневно проводи време у виртуелном окружењу, често без потребних технолошких вештина и искустава, али и без надзора родитеља. Чињеница да је сваким даном на светском нивоу све већи број млађих корисника дигиталних технологија би морала да алармира стручњаке из ове области, али и владе свих земаља да се озбиљније посвете овој појави. Дигитална писменост се намеће као неоспорна полазна основа која може бити и најделотворније средство у сузбијању оваквих злонамерних сајбер активности.

Кључне речи: Интернет, Друштвене мреже, Дигитална писменост, Сајбер криминал, Виртуелно окружење

УВОДНЕ НАПОМЕНЕ

Дигитална писменост је способност приступа, управљања, разумевања, интеграције, комуникације, процене и креирања информација безбедно и на одговарајући начин путем дигиталних уређаја и умрежених технологија за учешће у економском и друштвеном животу. Укључује компетенције које се односе на компјутерску писменост, информационо-комуникациону технолошку писменост, информатичку писменост и медијску писменост (UNESCO 2018). Једна од подваријабли дигиталне писмености је стање приступа интернету и коришћење друштвених мрежа (Lopez 2013).

У модерном друштву које је вођено трансформативним технологијама, појавила се кључна потреба да грађани света свих узраста поседују одређени ниво

* Редовни професор, r.baltezarevic@gmail.com

** Овај рад је резултат пројекта Факултета за пословне студије, Мегатренд универзитета: Улога нових технологија у савременом друштву (ФПСНТС).

дигиталних вештина за живот, учење и рад. Дигитална писменост у великој мери постаје темељни оквир вештина сличних читању и писању. На глобалном нивоу, дигитална писменост и е-инклузија су све више препознате као инструментална средства за подстицање одрживог развоја и економског раста и смањење друштвених неједнакости (International Telecommunication Union 2018). Студија која је објављена 2021. године, показала је да у Републици Србији људи користе друштвене мреже како би првенствено комуницирали са породицом и пријатељима. Међу осталим мотивима коришћења друштвених мрежа налази се прикупљање информација о брендовима, забава, али и жеља за покретањем бизниса. Такође, како је показала студија, сајтови друштвених мрежа Инстаграм и Пинрест перципиране су као најбезбедније платформе (углавном од стране женских испитаника) (Kwiatek и др. 2021).

Према истраживању спроведеном у Републици Србији међу млађом популацијом, откривено је да скоро 90% испитаника користи интернет на свакодневном нивоу (98% њих са мобилног/паметног телефона), док је 16% испитаника тврдило да је доживело дигитално вршњачко насиље. Студија је такође показала да је све више млађих корисника интернета, који приступају виртуелном окружењу без одговарајућег надзора родитеља у њихове онлајн активности (Kuzmanović 2019).

Иако постоји добра воља да се искорене или бар смање криминалне активности у дигиталном окружењу на глобалном нивоу, изгледа да се ипак овај проблем не решава довољно озбиљно. Штета коју је направио овај тип криминала је огромна у сваком смислу. Посебно забрињава чињеница да ова врста кривичног дела има предност у односу на традиционалне криминалне методе. Међународна стандардизација закона у овој области, едукација корисника у области дигиталне технологије, али и развој бољих рачунарских софтвера за рано откривање и спречавање таквих појава је неопходност (Baltezarević-Baltezarević 2021).

Много је примарних фактора одговорних за сајбер криминал, али и за сексуалну експлоатацију младих на мрежи и ван мреже. Поред родне неједнакости и сиромаштва, расизама, социјалне одвојености или усамљености, сексуалне оријентације, недостатка ефикасних законских оквира, политика и заштитних механизама, технолошка оспособљеност и дигитална неписменост издвајају се као кључни фактори који доприносе оваквим појавама. Све више се намеће потреба за дигиталном обуком младих, јер је дигитална писменост неопходност која ће обезбедити безбедно коришћење сајбер простора (Kumari 2021).

ДИГИТАЛНА ПИСМЕНОСТ

Дигитална писменост се дефинише као способност разумевања и коришћења информација у више формата са нагласком на критичко размишљање пре него на вештине информационих и комуникационих технологија (Gilster 1997). Људи данас имају нове врсте знања које су повезане са дигитално засићеним друштвеним праксама. Уобичајено је да људи користе кратке системе за размену порука друштвених мрежа као што су Фејсбук,

Твитер и Јутјуб којима комуницирају у дигиталном окружењу са осталим корисницима (Ibrahim и др. 2013). Међутим, нови дигитални видови комуникације захтевају и известан ниво дигиталне писмености, како би корисници остали безбедни. Може се рећи да је дигитално писмена особа она која је способна да идентификује, приступи, управља, интегрише, процени, анализира и синтетизује дигиталне ресурсе (Martin 2008). Разликује се неколико врста вештина дигиталне писмености, као што су: формалне оперативне вештине за навигацију интернетом, аналитичке и вештине проналажења информација, вештине креирања садржаја и вештине медијске писмености. Дигитална писменост у већини развијених земаља, укључује мултиписменост/мултимодалне димензије као што су техничке, социјално-емоционалне и когнитивне димензије (Brown, 2017). На основу резултата студије, коју је пре неколико година објавила Европска комисија може се видети да у просеку скоро 50% Европљана, узраста од 16 до 74 године, не поседује елементарне дигиталне вештине. У неким земљама, као што је на пример Бугарска, медијска „неписменост" износи алармантних 86%. Ово је забрињавајући податак, с обзиром да ова иста студија предвиђа да ће 90% послова у блиској будућности захтевати од запослених да поседују ове основне дигиталне вештине. Уколико се по овом питању нешто не промени, Европа би се могла суочити са дефицитом компетентних радника. Европска комисија је утврдила да већ данас око 40% компанија има потешкоћа да пронађе специјалисте из области информационо-комуникационих технологија. Сматра се да ће већ у наредних пар година Европска Унија бити у великом проблему услед немогућности да запосли пола милиона дигитално писмених радника, како би задовољила захтеве тржишта (Halachev 2017).

Студија која је 2019. године спроведена у Републици Србији, показала је да млади своје вештине дигиталне писмености процењују изнад просека. На скали од 1 до 10, просечна оцена испитаника креће се у распону од 6,7 до 8,6. Највиша просечна оцена у оквиру овог истраживања износила је 9,2 (социјалне вештине), док су испитаници сопствене вештине креирања садржаја у дигиталном формату оценили најнижом оценом 6,7. Скоро75% испитаника се донекле (или у потпуности) слаже са тврдњом да умеју да препознају и да знају како да провере истинитост информације коју су пронашли на интернету, док 68% испитаника тврди да без проблема могу закључити да ли могу веровати некој информацији (или извору информација) коју су пронашли на интернету (Kuzmanović 2019). Генерално, корисници интернет технологија и друштвених мрежа све више обраћају пажњу да ли се извори информација у виртуелном окружењу могу сматрати кредибилним, односно да ли могу имати поверења у смислу да им неће бити нанета било каква материјална или емоционална штета услед незаконитих сајбер активности (Baltezarević- Baltezarević 2021). Да би корисници друштвених мрежа могли веровати препорукама инфлуенсера на друштвеним мрежама, ти људи морају бити стручни у одређеној области, да поседују харизму и поштовање других корисника интернета (Kwiatek и др. 2021).

Међутим, данас су друштвене мреже претрпане инфлуенсерима, али и онима који се само тако представљају у покушају да изграде статус оних који се сматрају кредибилним извором информација, међутим невештим имитирањем веома често електронском комуникацијом од уста до уста (Ewom), само шире дезинформације и обмањују циљну публику. Иако микро инфлуенсери имају мањи број пратилаца од макро инфлуенсера (познатих личности), утисак је да остварују приснији и искренији однос са осталим корисницима друштвених мрежа, који им из тог разлога и више верују (Baltezarević-Baltezarević 2021).

Образовање и писменост могу помоћи у ефикаснијем спречавању сајбер криминала, нарочито едукација и обука о томе како се користе информациони системи и како избећи или се заштитити од криминалаца у сајбер простору (Herhalt, 2011). Робинсон тврди да као и свако друго друштвено понашање, на усвајање акција за спречавање сајбер криминалних активности утиче нечији положај у систему друштвене стратификације. Робинсон такође додаје да социо-демографске неједнакости утичу на усвајање технологије, као и на развој технолошких вештина и онлајн писмености (Robinson и др. 2015). Комуникација кроз неконтролисани канал, као што је интернет, може бити корисна, али често и веома штетна за потрошаче информација, пре свега што се интернет користи и за промоцију тероризма, порнографије, преваре и ширење порука мржње и дезинформација. Потреба за медијском, информацијском и дигиталном писменошћу намеће се као неопходност која ће довести до стабилности друштва и безбедног коришћења дигиталних платформи за приступање и размену информација (Abugu 2018).

ВРСТЕ САЈБЕР КРИМИНАЛА

Не постоји универзално прихваћена дефиниција појма „сајбер криминал". Често се овај термин користи да обухвати низ криминалних активности које користе информационо-комуникационе технологије. Међутим користе се и други замењиви термини, као што су „виртуелни криминал", „нет криминал", „хај-тек криминал" или „компјутерски криминал". Недостатак јасноће може бити збуњујући и узнемирујући и довести до тенденције да се свако кривично дело које укључује рачунар или његов део означава као сајбер криминал. Да би се ово превазишло, Валпредлаже да треба размотри како употреба информационо-комуникационих технологија трансформише злочин, а не сам чин (Wall 2004). Европска комисија се ослања на три категорије да би дефинисала сајбер криминал. Према Стратегији сајбер безбедности Европске Уније из 2013. године, сајбер криминал се обично односи на широк спектар различитих криминалних активности у којима су компјутери и информациони системи укључени или као примарни алат или као примарна мета. Сајбер криминал обухвата традиционална кривична дела (као што су превара, фалсификовање и крађа идентитета), кривична дела јединствена за рачунаре и информационе системе (као што су напади на информационе системе, ускраћивање услуге и малвер) и кривична дела у вези са садржајем (као што је онлајн дистрибуција

дечје порнографије или подстицање на расну мржњу) (European Commission 2013). У оперативном смислу, европска агенција за спровођење закона(Европол), сајбер криминал објашњава као сваки злочин који се може извршити само коришћењем рачунара, рачунарских мрежа или других облика информационо-комуникационе технологије. У суштини, без интернета, криминалци не би могли да почине ова кривична дела. То укључује активности као што су стварање и ширење злонамерног софтвера, хаковање ради крађе осетљивих личних или индустријских података и напади у циљу остваривања личне финансијске добити или побољшања репутације (Europol & Eurojust 2019).

Сајбер криминалци се на веома креативне начине довијају како би заобишли сигурносне системе и преварили своје жртве. Данас постоји читав дијапазон оваквих сајбер превара и оне временом еволуирају и постају све сложеније и делотворније. У наредном тексту биће поменуте најупечатљивије врсте оваквих активности:

• Нежељена пошта

Један од најчешћих облика сајбер криминала је нежељена пошта или спем. Представља дистрибуцију масовне е-поште која рекламира услуге, производе, или инвестиционе шеме, за које се често покаже да су лажне. Основна сврха овакве нежељене поште је да превари клијенте и натера их да верују да ће добити прави производ или услугу, обично по сниженој цени. Међутим, у следећем кораку пошиљалац нежељене поште тражи од потенцијалне жртве новац или безбедносне податке (попут броја кредитне картице) пре него што дође до коначног договора. Након што купац открије своје безбедносне податке, престаје било каква даља комуникација, када прималац нежељене поште схвата да је уствари преварен (Kaspersky 2012).

• Фишинг (лажно представљање)

Фишинг (Phishing) подразумева покушај преваре клијената у циљу добијања/откривања њихових личних безбедносних података, бројева кредитних картица, података о банковном рачуну или других осетљивих података. Сајбер криминалци путем поруке или е-поште могу затражити од прималаца да потврде/ажурирају информације о свом налогу. Овом методом настоји се да се украде идентитет компаније, који се затим користи да се од потрошача украду њихови кредитни идентитети. Фишинг је прилично једноставан за извођење и није потребна директна комуникација између хакера и жртве, односно хакер не мора да оствари директну комуникацију са потенцијалном жртвом претварајући се да је на пример особље за техничку подршку. Слање масовне поште хиљадама потенцијалних жртава повећава шансе да ова криминална активност буде успешна (Anti-Phishing Working Group (APWG) 2013).

• Хаковање

Хаковање је један од облика сајбер криминала који се често анализира и о коме се дискутује као о криминалној активности која је у средишту забринутости јавности због претњи коју представља за друштво. Хаковање се може описати као неовлашћен приступ и накнадна употреба рачунарских система других људи. Напади се углавном одвијају у неколико корака, почињу прикупљањем информација

или извиђањем, скенирањем и завршавају коначним уласком у циљни систем. Хаковање се спроводи на сличан начин на који се врши традиционална врста пљачке. Криминалац ће прво сазнати све податке о месту или особи коју жели да опљачка. Друштвени инжењеринг је једна од метода коју нападач користи за добијање информација. Постоје две главне категорије у које се могу класификовати сви покушаји друштвеног инжењеринга: обмана заснована на рачунару или технологији и обмана заснована на људима. Први, заснован на технологији, представља обмањивање корисника да верује да је у интеракцији са правим рачунарским системом и наводи корисника да пружи поверљиве информације. Други, људски приступ се постиже такође обманом и искоришћавањем жртвиног незнања и лаковерности (Yar 2006).

• Превара са платним или кредитним картицама

Ова врста преваре представља неовлашћену употребу платних или кредитних картица или крађу броја платне картице ради прибављања новца или имовине. Учињена штета на годишњем нивоу оваквим активностима у Великој Британији износи скоро 350 милиона фунти (Financial fraud action UK 2012). Превара са платним картицама обухвата све преваре које укључују плаћање путем интернета, паметног телефона или поште. Проблем у сузбијању овакве преваре лежи у чињеници да ни картица ни њен власник нису присутни на физичком месту. Преваранти као и у другим случајевима сајбер криминала, користе лажно представљање, хаковање базе података компанија или/и слање нежељене е-поште (Akhgar и др. 2014).

• Сајбер узнемиравање (застрашивање)

Сајбер узнемиравање или застрашивање представља употребу електронских информационих и комуникационих уређаја, као што су е-пошта, тренутне поруке, мобилни телефони, текстуалне поруке, блогови и многе веб локације за узнемиравање групе или појединца путем личних напада или других начина узнемиравања. Овакав вид сајбер узнемиравања се не разликује по много чему од узнемиравања (малтретирања) у физичком простору, барем на основу емоционалне штете која се наноси жртвама. Сајбер малтретирање, подсмевање, увреде и узнемиравање путем интернета или текстуалних порука послатих од стране злонамерних сајбер нападача, данас су постале веома распрострањеније међу младима широм света, на жалост овакве активности неретко имају и трагичне последице. Верује се да је сајбер малтретирање постало толико распрострањено на друштвеним мрежама, као што су Фејсбук, Твитер или Инстаграм да је погодило сваку школу у свакој заједници (StopCyberbullying 2013).

• Крађа идентитета у онлајн окружењу

Крађа идентитета је једна од најбрже растућих врста превара у Европи. Представља криминалну радњу прибављања осетљивих информација о другој особи без њеног знања, и даље коришћење ових података за извршење крађе или преваре. Интернет је дао сајбер криминалцима прилику да добију такве информације из базе података угрожених компанија. Понекад поприма облик апликације

за (лажно) оглашавање посла на интернету. Према једном истраживању, превара са идентитетом је велики проблем због ескалирајућих метода добијања и коришћења личних података и очекује се да ће се у наредним годинама додатно повећати (CIFAS 2012).

ЗАКЉУЧАК

Студије које су претходних година спроведене у области дигиталне писмености и њеног утицаја на препознавање и превенцију од активности сајбер криминала недвосмислено су показале да су корисници дигиталних технологија недовољно информисани и технолошки невешти и самим тим незаштићени од оваквих напада. Ситуација по овом питању у Републици Србији није сјајна, али ни земље Европске Уније се не могу похвалити значајним успесима у овој области. Иако се коришћење информационо-комуникационих технологија све више имплементира у свакодневни живот модерног човека, велики проблем је тај што већина корисника не поседује потребне дигиталне вештине како би своје потребе за комуникацијом, пословањем или забавом у виртуелном окружењу обављала на безбедан начин. Посебно је битно напоменути да је тренд у последњим годинама да деца све више постају корисници дигиталних технологија у најранијем добу, међутим без адекватног дигиталног искуства и мониторинга родитеља (или старатеља) постају лаке мете злонамерних сајбер криминалаца.

Анализом стручне литературе из ове области, може се лако закључити да још увек не постоји консензус око дефинисања основних појмова сајбер криминала, нити су још увек јасне границе у квалификацији традиционалног и сајбер криминала. Ова чињеница имплицира да су самим тим и законодавство, међународна законодавна усклађеност и сарадња у области сајбер криминала на самом почетку једног дугог пута. Повећање броја дигитално писмених становника, које укључује компетенције које се односе на компјутерску, медијску, информатичку и информационо-комуникациону технолошку писменост се намеће као стратегија која би требала свим државама да буде приоритетна и која би имплементирањем у друштвени систем била можда и најјаче оружје којим би се овакве криминалне активности смањиле или барем биле под контролом.

ЛИТЕРАТУРА

Abugu 2018: Jude Chukwunonso Abugu. "The imperative of media, information and digital literacy in the era of internet-driven global communication." https://en.unesco.org/sites/default/files/gmw2018_jude_abugu.pdf (Приступљено: 02.01.2022.)

Anti-Phishing Working Group (APWG) 2013: "Global Phishing Survey: Trends and Domain Name Use in 1H2013". http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf (Приступљено: 29.12.2021).

Akhgar-Staniforth-Bosco 2014: Babak Akhgar, Andrew Staniforth, Francesca Bosco. "Cyber Crime and Cyber Terrorism Investigator's Handbook". Syngress

Baltezarević–Baltezarević 2021: Ivana Baltezarević & Radoslav Baltezarević. „Sajber bezbednost: izgradnja digitalnog poverenja." *Megatrend Revija*, Vol. 18 (4). pp. 269-280 UDK 343.533::004 DOI: 10.5937/MegRev2104269B

Baltezarević–Baltezarević 2021: Radoslav Baltezarevic & Ivana Baltezarevic. „Uloga instagrama u poslovanju mladih.“ *Megatrend Revija. Vol. 18, № 2, 2021: 23-38* • DOI: 10.5937/MegRev2102023B

Baltezarevic-Baltezarevic 2021: Radoslav Baltezarevic &Ivana Baltezarevic. “The Dangers and Threats that Digital Users Face in Cyberspace”. *IPSI Transactions on Internet Research*, Vol. 17, No. 1, January 2021, pp. 46-52.

Brown 2017: Mark Brown. “A critical review of frameworks for digital literacy: Beyond the flashy, flimsy and fad- dish.” ASCILITE Technology Enhanced Learning Blog. https://blog.ascilite.org/a-critical-review-of-frameworks-for-digital-literacy-beyond-the-flashy-flimsy-and-faddish-part-1 (Приступљено: 28.12.2022.)

CIFAS 2012: “The UK’s Fraud Prevention Service”. http://www.cifas.org.uk/ (Приступљено: 29.12.2021).

Europol & Eurojust 2019: “Common challenges in com bating cybercrime, As identified by Eurojust and Europol.” JOINT REPORT, Europol and Eurojust Publi Information https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf (Приступљено: 03.01.2022.)

European Commission 2013: “Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.” Brussels JOIN(2013) 1 final.

Financial fraud action UK 2012: “Fraud: The Facts 2012. The definitive overview of payment industry fraud and measures to prevent it.” http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf (Приступљено: 30.12.2021).

Gilster 1997: Paul Gilster. “Digital literacy”. New York: John Wiley & Sons Halachev 2017: Rumen Halachev. “Nearly half of Europeans don’t have basic digital skills.” https://epale.ec.europa.eu/en/content/nearly-half-europeans-dont-have-basic-digital-kills (Приступљено: 03.01.2022.)

Herhalt 2011: John Herhalt. “Cyber-crime-A growing challenge for governments.” KPMG Issues Monitor, 8: 1-24, https://kpmg-inst.adobecqms.net/content/dam/institutes/en/government/pdfs/2011/cyber-crime-growing-challenge.pdf (Приступљено: 01.01.2022).

Ibrahim- Shariman- Woods 2013: Nazerin Ibrahim, Tenku Norishah Tenku Shariman & P. Woods. “The Concept of Digital Literacy from the Perspective of the Creative Multimedia Industry.” 2013 International Conference (pp. 259-264): IEEE.

International Telecommunication Union (ITU) 2018: “Digital Skills Toolkit.” Geneva, Switzerland: ITU. https://www.itu.int/en/ITUD/DigitalInclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf (Приступљено: 29.12.2022.)

Kaspersky 2012: “Spam in April 2012: Junk Mail Gathers Pace in the US.” https://www.kaspersky.com/about/press-releases/2012_spam-in-april-2012-junk-mail-gathers-pace-in-the-us (Приступљено: 29.12.2021).

Kumari 2021: Madhu Kumari. “Cyber Crime and Children in Digital Era.” International Journal of Scientific Research in Science and Technology. Vol.8, Issue 1, pp. 151-160 doi : https://doi.org/10.32628/IJSRST218124

Kuzmanović-Pavlović-Popadić-Milošević 2019: Dobrinka Kuzmanović, Zoran Pavlović, Dragan Popadić i Tijana Milošević. „Korišćenje interneta i digitalne tehnologije kod dece i mladih u Srbiji - Rezultati istraživanja Deca Evrope na internetu“ http://dobrinkakuzmanovic.weebly.com/uploads/2/6/4/8/26488972/koriscenje_interneta_kod_dece_i_mladih_u_srbiji_v1-1.pdf (Приступљено: 03.01.2022.)

Kwiatek- Baltezarević- Papakonstantinidis 2021: Piotr Kwiatek, Radoslav Baltezarević, Stavros Papakonstantinidis. “The impact of credibility of influencers recommendations on social media on consumers behavior towards brands.” *Informatologia.Vol. 54 No. 3-4,* 181-196

Kwiatek-Papakonstantinidis-Baltezarevic 2021: Piotr Kwiatek, Stavros Papakonstantinidis, Radoslav Baltezarevic. “Digital Natives’ Entrepreneurial Mindset: a Comparative Study in Emerging Markets.” In S. Rezaei, L. Jizhen, S. Ashourizadeh, V. Ramadani, & S.e Gërguri-Rashiti (Eds.), *The Emerald Handbook of Women and Entrepreneurship in Developing Economies,* Chapter 15. (295-316). Emerald Publishing Limited

Lopez 2013: Islas Lopez. "Digital literacy and academic success in online education for underprivileged communities : the prep@net case." Ph.D. Dissertation, University of Texas, Austin.
Martin 2008: Allan Martin."Digital Literacy and the "Digital Society". In C. Lankshear & M. Knobel (Eds.), Digital Literacies: Concepts, Policies and Practices (pp. 151-176). New York: Peter Lang.
Robinson- Cotton- Ono- Quan-Haase- Mesch- Chen- Shulz- Hale- Stern 2015: Laura Robinson, Sheila Cotten, Hiroshi Ono, Anabel Quan-Haase, GustavoMesch, Wenhong Chen, Jeremy Shulz, Timothy Hale, Michael Stern. "Digital inequalities and why they matter." *Information, Communication & Society*, *18*(5), 569–582. doi: 10.1080/1369118X.2015.1012532
StopCyberbullying 2013: StopCyberBullying Youth Summit http://stopcyberbullying.org/index2.html (Приступљено: 29.12.2021).
UNESCO 2018:"Global framework of reference on digital literacy skills for indicator 4.4.2: Percentage of youth/adults who have achieved at least a minimum level of proficiency in digital literacy skill (Draft Report)." Paris: UNESCO. http://uis.unesco.org/sites/default/files/documents/draft-report-global-framework-reference-digital-literacy-skills-indicator-4.4.2.pdf (Приступљено: 28.12.2022.)
Wall 2004: David Wall. "What are Cybercrimes?" Criminal Justice Matters. 58(1), 20-21
Yar 2006: Majid Yar. "Cybercrime and Society". Sage Publication Ltd, London.

Radoslav V. BALTEZAREVIĆ

DIGITAL LITERACY AS A MEANS OF PREVENTING CYBERCRIME

Summary

It is difficult today to imagine how a person would function in modern society without the use of Internet-based technologies. Everyday interactions that take place in the digital environment permeate all spheres of society, enabling communication, entertainment and business of users. However, the lack of technological skills and digital literacy in a large number of people increases the chances of them becoming victims of various types of cybercrime activities. Such activities can often have very severe physical, material and emotional consequences for Internet and social networks users. Also, it is not uncommon for the victim's interaction with a malicious cybercriminal to lead to tragic consequences. This problem especially affects the youngest population, who spend time every day in a virtual environment, often without the necessary technological skills and experience, but also without parental supervision. The fact that the number of young users of digital technologies is increasing every day on the world level should alert experts in this field, but also the governments of all countries to take this phenomenon more seriously. Digital literacy is emerging as an indisputable starting point that can be the most effective means of combating such malicious cyber activities.

Keywords: Internet, Social Networks, Digital Literacy, Cybercrime, Virtual Environment

Рад је предат 6. фебруара 2022. године, а након мишљења рецензената, одлуком одговорног уредника *Баштине*, одобрен за штампу.