Sara Rošeto, dr. Pucer Patrik, dr. Irena Trobec, dr. Boštjan Žvanut

Identifikacija in razvoj e-vsebin o informacijski varnosti v zdravstveni negi

Strokovni članek

UDK 004:614.253.5

KLJUČNE BESEDE: e-izobraževanje, zdravstvena nega, informacijska varnost, tveganje

POVZETEK - V vsakodnevni praksi zdravstvene nege je možno identificirati različna dejanja medicinskih sester, ki ogrožajo informacijsko varnost. Cilj pričujoče raziskave je bil identificirati najbolj problematična tovrstna dejanja v konkretni zdravstveni ustanovi in zanje razviti učne e-vsebine, ki bi medicinskem sestram na primeren način predstavile omenjeno problematiko. S pomočjo pregleda literature in s pomočjo intervjujev z dvema strokovnjakoma za zdravstveno informatiko so bila identificirana omenjena tvegana dejanja. Skladno s tem smo za pet identificiranih dejanj razvili e-vsebine, ki slikovito predstavljajo omenjena dejanja in njihove morebitne posledice. Za razvoj e-vsebin smo uporabili orodji Bitstrips in Courselab 2.4 ter sistem za e-izobraževanje Moodle. E-vsebine sta ocenila eden od intervjuvancev in visokošolski učitelj s področja informatike. Rezultati evalvacije kažejo, da so omenjene e-vsebine uporabne, privlačne, kakovostne in primerne za ciljno populacijo. Primanjkljaj znanja medicinskih sester o informacijski varnosti predstavlja nevarnost za zanesljivost in zaščito podatkov. Razvite e-vsebine bi lahko bistveno pripomogle k izboljšanju stanja na tem področju.

Professional paper

UDC 004:614.253.5

KEY WORDS: e-learning, nursing care, information security, risk

ABSTRACT - In everyday nursing practice it is possible to identify different threats to the violation of information security. The goal of this study was to identify some of the most problematic activities in the particular health institution and develop e-learning contents for nurses, which would present the problems of information security to this population in an appropriate way. The aforementioned threats were identified in the literature and with interviews, performed with two health informatics experts. According to five different identified threats, wedeveloped e-learning contents, which vividly present the aforementioned violations and potential consequences. For the development of e-contents the applications Bitstrip and Courselab 2.4 and the learning management system Moodle were used. E-contents were evaluated by one of the interviewee and a university lecturer expert in field of informatics. The results of the evaluation indicate that the developed e-contents are useful, on an adequate level of quality and appropriate for the target population. The lack of nurses' knowledge in the field of information security represents a threat for reliability and data protection. The developed e-contents could improve the situation in this field.

1 Uvod

Informacijskokomunikacijske tehnologije (IKT) so danes sestavni del vsakdanjika in imajo pomembno vlogo v zdravstvenem sistemu. Linden in sod. (2009) navajajo, da je za izvedbo kakovostnih zdravstvenih storitev ključnega pomena enostaven dostop do pacientovih podatkov v elektronski obliki.

Učinkovito dokumentiranje procesov zdravstvene nege je eden izmed ključnih problemov zdravstvene nege kot temeljne sestavine celovitega sistema zdravstvenega varstva (Rajkovič, 2010). Informacijski sistem nudi (oz. bi moral nuditi) medicinskim sestram podporo pri vsakodnevnem delu (Prijatelj, 2006). Slednje pa pogosto presega

področje zdravstvene nege. Medicinske sestre tako dostopajo do podatkov o pacientih, ki pa jih je treba skrbno varovati.

Številne države imajo natančno določene zakonske osnove in pravilnike za varovanje zaupnosti pacientovih podatkov (Leino-Kilpi et al., 2001). V Sloveniji so to npr. Zakon o zdravstvenem varstvu in zdravstvenem zavarovanju, Zakon o zdravstveni dejavnosti, Zakon o pacientovih pravicah, Zakon o zbirkah podatkov s področja zdravstvenega varstva, Pravila obveznega zdravstvenega zavarovanja, Zakon o varstvu osebnih podatkov, Zakon o elektronskem poslovanju in elektronskem podpisu, Kazenski zakonik. Kljub temu pa so v zdravstvenih institucijah kršitve zakonskih osnov zelo pogoste, saj zdravstveno osebje ključnih občutljivih podatkov pacientov ne varuje primerno (Marcelan and Bernik, 2012). Kršitve informacijske varnosti imajo lahko pogubne in pogosto neslutene posledice za pacientove podatke (Albarrak, 2012). Slednjim pa bi morali subjekti zdravstvenega sistema posvetiti še posebno pozornost, saj vsako kršenje informacijske varnosti ni podvrženo zgolj finančnim izgubam, temveč ima lahko ogroža tudi varnost pacientov oz. njihovo življenje. Tehnologija sama po sebi ne more zagotavljati predpisanega nivoja varnosti (Gobuty, 2003), zato je potrebna ustrezna organizacija in primerno usposobljeni ljudje. Večletne izkušnje pri poučevanju informatike v zdravstveni negi kažejo, da medicinske sestre niso ustrezno ozaveščene o informacijski varnosti. Slednje ugotavlja tudi Albarrak (2012), ki je na skupini medicinskih sester v Saudski Arabiji dokazal, da vsakdanja praksa medicinskih sester predstavlja nevarnost za zaupnost podatkov o pacientih. Omenjeni avtor ugotavlja, da obstaja veliko razhajanje med znanjem medicinskih sester na tem področju in njihovim dejanskim obnašanjem v praksi. Dvig nivoja zavedanja na področju informacijske varnosti pri omenjeni populaciji je torej nujen. Medicinske sestre namreč predstavljajo levji delež zaposlenih v zdravstvenem sistemu.

Pri pregledu literature nismo zasledili, da bi v Sloveniji obstajale e-vsebine ali druga digitalna gradiva, ki bi jih medicinske sestre in drugi zdravstveni delavci lahko uporabljali in si z njimi izboljšali in bogatili nivo znanja na področju informacijske varnosti. Zato je bil cilj pričujoče raziskave identificirati najbolj pereča dejanja ki ogrožajo informacijsko varnost v konkretni zdravstveni ustanovi in zanje razviti učne e-vsebine, ki bi medicinskim sestram na primeren način predstavile omenjeno problematiko.

2 Metode dela

Raziskava je zajemala tri ključne faze: (1) identifikacija perečih dejanj medicinskih sester, ki ogrožajo informacijsko varnost; (2) razvoj e-vsebin za pet omenjenih dejanj; in (3) evalvacija razvitih e-vsebin. Dovoljenje za izvedbo raziskave smo pridobili od vseh sodelujočih. Vsak posameznik, ki je sodeloval v raziskavi, je imel pravico kadarkoli odstopiti od raziskave in pravico ne odgovoriti, če bi s tem razkril zaupne podatke.

Prvo fazo smo izvedli v oktobru 2012, ko smo po temeljitem pregledu literature izvedli še intervjuje s strokovnjaki iz prakse. Iz teh intervjujev smo identificirali in zapisali omenjena dejanja ter jih primerjali s tistimi v literaturi. Na željo intervjuvancev

intervjuji niso bili posneti. Potekali so približno eno uro, ravno toliko, da smo identificirali in zapisali omenjena dejanja. V omenjeni fazi sta sodelovala dva strokovnjaka za zdravstveno informatiko, ki vsakodnevno delata z medicinskim sestrami in dobro poznata te probleme in sta bila pripravljena sodelovati v raziskavi.

V drugi fazi smo e-vsebine razvili s pomočjo aplikacij Bitstrips in CourseLab 2.4. Bitstrips je enostavno spletno orodje, ki omogoča oblikovanje avatarjev in njihovo vključevanje v različna okolja. Na voljo je veliko že izdelanih objektov (npr. ozadij, oseb, oblačkov), ki jih lahko uporabnik vključi v končni strip (Spletna stran Bitstrips, n. d.). Izdelane stripe smo vključili v končno e-vsebino s pomočjo brezplačnega orodja CourseLab 2.4. Gre za napredno programsko orodje, namenjeno predvsem oblikovanju interaktivnih e-vsebin, primernih za objavo na svetovnem spletu, zgoščenkah ali v sistemih za upravljanje z učnimi vsebinami (Zakrajšek, 2013). CourseLab 2.4 podpira standard SCORM, kar razvitim e-vsebinam (vsaj načeloma) zagotavlja delovanje v različnih sistemih za upravljanje z učnimi vsebinami, ki podpirajo standard SCORM. Ključne značilnosti programa CourseLab so (WebSoft Ltd., Russia, n. d.): deluje na principu »What you see is what you get«, kar pomeni da oblika in vsebina ostajata isti od postavitve do končnega produkta; za izdelovanje e-vsebin ne potrebuje internetne povezave; podpira najrazličnejše multimedijske elemente v različnih formatih (besedilo, zvok, slike, animacije Macromedia Flash, Java in Shockwave vsebine ter različne video formate ipd.); omogoča sprotno pregledovanje, dopolnjevanje in testiranje vgrajenih elementov; animacijo objektov; omogoča izdelavo navigacije znotraj e-vsebine; povezava med več zahtevnimi objekti je omogočena z enim samim klikom na miško; za predvajanje e-vsebin ni potrebna namestitev programskega jezika Java; omogoča izdelavo zahtevnih e-vsebin.

Tretjo fazo raziskave, tj. evalvacijo razvitih e-vsebin, smo izvedli s pomočjo enega od zgoraj omenjenih strokovnjakov in vključili dodatnega visokošolskega učitelja, ki se ukvarja s področjem informacijsko-komunikacijskih tehnologij in ni sodeloval v prvi fazi raziskave. E-vsebine smo postavili na spletni strežnik, da so bile na vpogled evalvatorjema. V evalvacijo e-vsebine sta bila vključena dva strokovnjaka iz različnih delovnih okolij, ki pa sta se že srečala s področjem e-izobraževanja, saj je bil cilj pridobiti čim bolj neodvisno in objektivno oceno izdelanih e-vsebin. Skladno s tem omenjenima strokovnjakoma nismo vsiljevali nobenih kriterijev ocenjevanja e-vsebin. Evalvatorja sta prošnjo za evalvacijo izdelanih e-vsebin prejela po elektronski pošti in sta se strinjala s sodelovanjem.

3 Rezultati

3.1 Predstavitev razvitih e-vsebin

Razvitih je bilo pet e-vsebin z različnimi tematikami s področja informacijske varnosti, in sicer: »Zloraba osebnih podatkov«, »Zloraba gesla«, »Zloraba podatkov preko telefona«, »Brskanje po spletu na službenih računalnikih« in »Okužen USB ključ«. E-vsebine so različno dolge, najkrajša ima 8 strani, najdaljša pa 11. Vse se

začnejo z uvodno stranjo, nadaljujejo z različnimi animacijami, oblački, ki e-vsebino popestrijo in naredijo bolj privlačno za uporabnike. Pri prehajanju med eno in drugo stranjo so spodaj prikazani kvadratki, ki predstavljajo kazalo in kažejo, na kateri strani se uporabnik nahaja. Vsak klik omogoča prikaz novega besedila, oblačkov, prehajanja strani in animacij. Vsaka e-vsebina se zaključi na isti način, in sicer tako, da se prikaže zadnja stran z napisom konec. V nadaljevanju sta na kratko opisani dve e-vsebini. Vse razvite e-vsebine si lahko ogledate v celoti na povezavi: http://inoedu.info/evsebine/roseto/, kjer so prosto dostopne. Priporočljiva je uporaba spletnega brskalnika Firefox ali Chrome.

Vsako od omenjenih e-vsebin se lahko ponazori z diagramom prehajanja stanj, ki predstavlja neke vrste scenarij razvite e-vsebine. Vsak diagram je opremljen s pripadajočo preglednico, kjer je vsako stanje podrobneje opisano. Vsako stanje je dejansko stran razvite e-vsebine. Primer diagrama prehajanja stanj za e-vsebino »Zloraba gesla« je prikazan na sliki 1, podroben opis stanj pa v tabeli 1. Podobni diagrami s pripadajočo tabelo so bili narejeni tudi za ostale e-vsebine.

Slika 1: Diagram prehajanja stanja e-vsebine »Zloraba gesla«

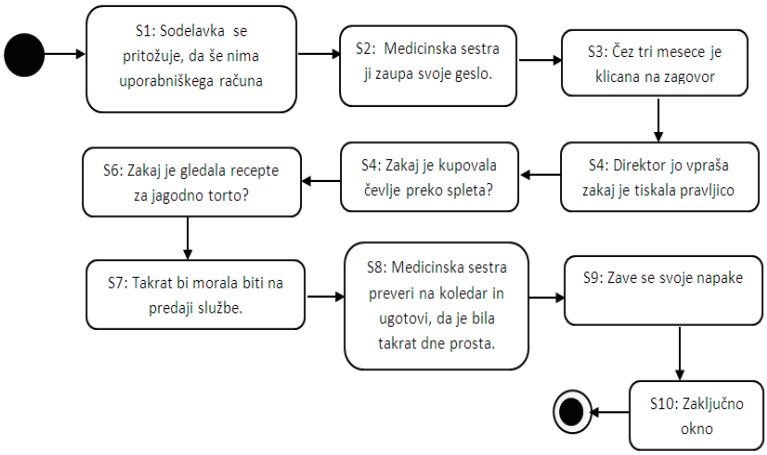


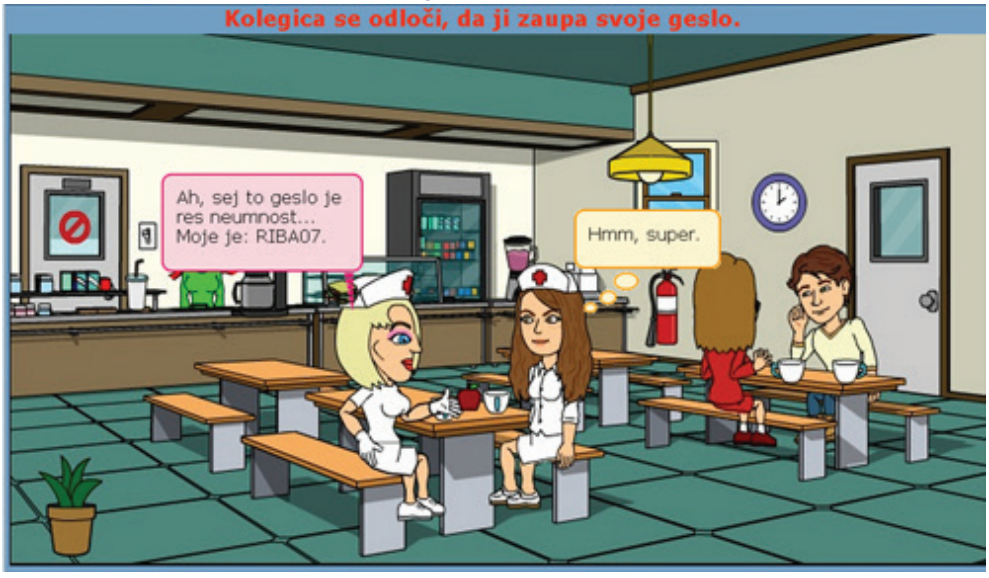
Tabela 1: Opis diagrama prehajanja stanja

Stanje	*Opis*
S1: Sodelavka se pritožuje, da še nima uporabniškega računa	Pri malici med osebnim pogovorom sodelavka potoži medicinski sestri, da še vedno nima svojega uporabniškega računa, kar ji onemogoča delo.
S2: Medicinska sestra ji zaupa svoje geslo.	Medicinski sestri se zdijo gesla nepomembna, zato se odloči, da ji zaupa kar svojega.
S3: Čez tri mesece je klicana na zagovor.	Medicinska sestra je čez tri mesece med opravljanjem svojega dela klicana na zagovor.
S4: Direktor jo vpraša, zakaj je tiskala pravljico.	Med zagovorom ji direktor postavi vprašanja, o katerih ona prav nič ne ve. Vpraša jo, zakaj je 6. 5. 2013 ob 18:30 tiskala pravljico o Pepelki?

S5: Zakaj je kupovala čevlje preko spleta?	Zakaj je isti dan ob 18:42 kupovala čevlje preko spleta?
S6: Zakaj je gledala recepte za jagodno torto?	In zakaj je ob 19:00 gledala recepte za jagodno torto?
S7: Takrat bi morala biti na predaji službe.	Direktor je preveril in ob tistem času bi morala medicinska sestra biti na sestanku, oz. predaji službe. Žalostna in začudena ne da nobenega odgovora.
S8: Medicinska sestra preveri na koledarju in ugotovi, da je bila takrat prosta.	Ne da ji miru, zato pogleda na svoj koledar in ugotovi, da je bila tistega dne na dopustu.
S9: Zave se svoje napake	V trenutku se medicinska sestra zave, da je svoje računalniško geslo zaupala drugim, kar je privedlo do zlorabe. Odločila se je, da tega ne bo nikoli več storila.
S10: Zaključno okno	Prikaže se zadnja stran e-vsebine, ki pokaže, da se zgodba konča.

Na sliki 2 je prikazan primer druge e-vsebine, in sicer »Zloraba gesla«. V omenjeni e-vsebini je medicinska sestra v menzi zaupala sodelavki svoje uporabniško ime in geslo za dostop do zdravstvenega informacijskega sistema. Prikazana je realna neformalna situacija, kjer se sodelavki pogovarjata in mimogrede ena drugi posredujeta zaupno informacijo. Omenjena e-vsebina v nadaljevanju prikaže, kako je nekdo uporabniški račun zlorabil, zaradi česar se je medicinska sestra znašla pri nadrejenem na zagovoru.

Slika 2: Izsek iz e-vsebine »Zloraba gesla«



Na sliki 3 je prikazan primer e-vsebine »Okužen USB ključ«. Medicinska sestra med delom posluša glasbo s svojega USB ključa. Slednje pa ne bi bilo nič narobe, če ne bi bil okužen. V nadaljevanju omenjene e-vsebine je prikazan možen varnostni incident, o katerem so poročali tudi intervjuvanci. V preteklosti so namreč zabeležili

dogodek, kako je nezaželeni računalniški program zasedel vse prenosne kapacitete v pošiljanju in sprejemanju podatkov in s tem vsem uporabnikom informacijskega sistema onemogočil delo.

Slika 3: Izsek iz e-vsebine »Zloraba gesla«

3.2 Evalvacija razvitih e-vsebin

V nadaljevanju je predstavljeno strokovno mnenje obeh evalvatorjev, pripombe in pohvale. Ker sta oba strokovnjaka na svojem področju, jima je bila prepuščena prosta pot pri ocenjevanju.

Odgovor evalvatorja A

Razvite e-vsebine niso klasične e-vsebine, ki ponavadi vsebujejo večinoma elemente za pridobivanje, ponavljanje ali preverjanje znanja. Razvite e-vsebine vsebujejo elemente za dodatne učne dejavnosti, saj uporabnikom preko različnih učnih pripomočkov uspešno predstavljajo resnične situacije s področja informacijske varnosti in omogočajo doživljanje navideznih negativnih posledic, do katerih lahko pride pri vsakdanjem delu zdravstvenih delavcev.

S tehnično-uporabniškega vidika menim, da so e-vsebine dobro zasnovane. So kompatibilne in večinoma delujejo v glavnih spletnih brskalnikih Firefox, Chrome in Internet Explorer. Zaradi končne standardizirane oblike SCORM je njihova kompatibilnost zagotovljena tudi v različnih sistemih za upravljanje e-vsebin (npr. Moodle, ECHO, WebCT), kar omogoča hitro namestitev in pripravo za uporabo. Vse razvite e-vsebine, teh je pet, imajo skupno celostno grafično podobo in so zapakirane v paketu SCORM, kar olajša navigacijo in njihovo pregledovanje. Poleg tega se vsaka e-vsebina ob odprtju pojavi v svojem oknu, ki je velikosti oz. ima zaslonsko ločljivost ustrezno večini današnjih osebnih računalnikov.

Konkretne situacije s področja informacijske varnosti posameznih e-vsebin so predstavljene z različnimi stanji v obliki animiranih stripov, sestavljenih iz kakovostnih slikovnih gradiv z dobro ločljivostjo, ki omogočajo uporabniku dober pogled in razumevanje opisane situacije oz. stanja. Poleg izvirnega slikovnega gradiva je tu pozicija oblačkov, ki sledi klasični stripovski filozofiji, in evolucija pri uporabi barv in kontrastov za ozadja oblačkov. Določena barva ozadja oblačka je namreč vezana na določeno osebo, ki nastopa, v takem stanju, da je popolnoma jasno, kdo kaj pove ali razmišlja. Stopnja interaktivnosti je nizka (enosmerna komunikacija), saj e-vsebine omogočajo uporabnikom le kontroliranje poteka scenarija (naprej na naslednje stanje scenarija, nazaj, ponovni ogled trenutnega stanja, skakanje med stanji), ni drugega vpliva, zank ali razvejanj.

Kar se tiče berljivosti besedil, je slednja otežena zaradi uporabe temnejše barve besedila. Glede na temnejše ozadje bi bilo bolj ustrezno uporabiti svetlejšo barvo besedila. Večina besedil je strokovno ustreznih in dosledno organiziranih, ampak je nekaj izjem, kjer se uporabnik rahlo zmede. Omenjene pomanjkljivosti so bile tudi v nadaljevanju odpravljene.

Omenjeni evalvator si je pomagal s kriteriji za vrednotenje e-vsebin, ki jih predvideva razvojna skupina za vzpostavitev ocenjevalnega sistema elektronskih učnih vsebin na Zavodu Republike Slovenije za šolstvo (Liljana Kač et al., 2011).

Odgovor evalvatorja B:

Čeprav nisem strokovnjak s področja pedagogike, menim, da je sporočilo, ki ga želite posredovati, precej jasno. Poskušal bom komentirati vsako vsebino posebej:

Pri e-vsebini »Zloraba osebnih podatkov« je razvidno, da medicinska sestra g. Novaka ni ustrezno identificirala, kar je povzročilo resen problem. Pogrešam sicer, da animacija ne nauči učečega, kaj pomeni ustrezna identifikacija (npr. osebni dokument, kartica ZZZS), in ali mora sestra karkoli iz kartice vnesti ali zapisati, da bo kasneje lahko dokazovala, da je preverila pristnost dokumenta.

»E-vsebina« zloraba gesla ima zelo jasno sporočilo. Čeprav nadrejeni očita medicinski sestri stvari, za katere po zakonu ne sme voditi evidence (npr. dostopanje do spletnih vsebin posameznika), pa kot informatik menim, da bi se lahko zgodila tudi hujša kršitev, ki je ne omenjate, tj. uporaba elektronske pošte v imenu drugega ali vpogled v osebne podatke določene v javnosti izpostavljene osebe.

E-vsebina »Zloraba podatkov preko telefona« prikazuje problem identifikacije, ki je po telefonu težko izvedljiva. Na zaključku e-vsebine pogrešam poduk učečemu o omenjeni problematiki, ki bi bolje zaokrožil omenjeno tematiko.

Prav tako ima e-vsebina »Brskanje po spletu na službenih računalnikih« zelo jasno sporočilo. Dejstvo je, da je dovolj že samo brskanje po okuženih spletnih straneh, kar lahko povzroči varnostni incident. Morda je za učečega zavajajoče to, da je medicinska sestra povzročila okužbo šele s prenosom vsebine na svoj računalnik in ne že z njenim vpogledom.

S primerom e-vsebine »Okužen USB ključ« smo se srečali v praksi in menim, da je omenjena e-vsebina lahko zelo koristna konkretno v naši in ostalih organizacijah, ne samo zdravstvenih. Morda je zavajajoče v e-vsebini prikazano dejstvo, da se lahko okužba pojavi šele, če je USB ključ dalj časa v računalniku. Virusi se navadno aplicirajo takoj po vstavitvi oz. v trenutku, ko dobijo ustrezne pravice s strani uporabnika.

Kar se tiče ocene tehnične izvedbe, menim, da so e-vsebine implementirane kot spletna vsebina. Dostopne so od koderkoli in komurkoli, ki ima na voljo povezavo do njih. Če bi se e-vsebine uporabilo kot obvezno izobraževanje za določeno skupino ljudi, pa bi bilo treba izdelati modul, ki za posameznega uporabnika evidentira, ali je e-vsebino pregledal.

Kar se tiče kakovosti izdelave e-vsebine, lahko rečem, da so tako grafika kot besedila zelo primerni za doseganje cilja. Vse, kar je potrebno, da učeči se opazi in prebere, je jasno prikazano. Manjša kritika bi morda šla v smeri dolgega nalaganja slik (slednje je bilo odpravljeno z optimizacijo slik). Prav tako lahko rečem, da je uporabniški vmesnik preprost in jasen. Učeči se lahko e-vsebino upravlja zgolj s premikanjem med vsebinami v trenutkih, ko so »besedilni oblaki« v celoti naloženi z dinamiko, ki jo krmili avtomatizem. Morda bi bilo bolje, če bi pojav »besedilnega oblačka« lahko pospešili s klikom na levi miškin gumb, a to je zgolj predlog.

4 Razprava

E-vsebine torej niso običajna pedagoška gradiva, saj omogočajo vpogled v resnične situacije s področja informacijske varnosti in prikazujejo možne negativne posledice, do katerih lahko pride pri vsakdanjem delu medicinskih sester in zdravstvenih delavcev. Ne glede na to, da so bile razvite v sodelovanju z informatiki iz konkretne zdravstvene ustanove, lahko glede na nevarnosti, identificirane v pregledu literature, sklepamo, da bi bile zanimive tudi za ostale institucije. Glede na evalvacijo so razvite e-vsebine uporabne in kakovostno izdelane, kljub temu pa so rezultati evalvacije pokazali določene pomanjkljivosti. Nekatere od njih so že odpravljene: npr. vseh pet pripomb evalvatorja A. Popravljene so bile tudi slovnične napake, besedila, vizualna neskladja, neustrezne barve pa so bile spremenjene. Pripombe evalvatorja B glede ocene uporabniškega vmesnika pri uporabi e-vsebin pa niso bile odpravljene zaradi omejenosti programa za razvoj e-vsebin. Njihova odprava bi zahtevala razvoj dodatnih multimedijskih elementov. Tudi težava predolgega nalaganja je sedaj odpravljena.

Ne glede na to, da orodje CourseLab 2.4 (WebSoft Ltd., Russia, n. d.) deluje na principu »What you see is what you get«, pa so se vseeno pojavila določena odstopanja med e-vsebino, prikazano z orodjem CourseLab 2.4, in tisto, ki je bila prenesena na spletni strežnik. Zaradi navedenega so se pojavile številne pomanjkljivosti, povezane z estetiko e-vsebine, ki pa smo jih skušali odpraviti ali zaobiti (angl. »workaround«). Vseeno pa omenjeno orodje priporočamo, saj omogoča enostavno izdelavo kakovostnih e-vsebin in je tudi zastonj.

Po mnenju evalvatorjev so razvite e-vsebine primerne za pridobivanje znanja na področju informacijske varnosti. V praksi pa lahko medicinske sestre dajejo vodstvu in strokovnjakom s področja informacijske varnosti vtis, da omenjeno področje razmeroma dobro poznajo. Problematika rizičnega vedenja na področju informacijske varnosti, o kateri govori Albarrak (2012), pa predstavlja tempirano bombo za nemoteno delovanje zdravstvene organizacije in varstvo pacientovih pravic. V tem duhu so bile omenjene e-vsebine tudi razvite. Naš cilj je razviti e-vsebine, v katerih se medicinske sestre prepoznajo. Trček in sod. (2007) menijo, da je človek najpomembnejši dejavnik pri zagotavljanju informacijske varnosti. Ali ogled omenjenih e-vsebin tudi dejansko vpliva na samo vedenje, pa, žal, zaenkrat ne moremo odgovoriti. Z omenjenimi e-vsebinami bi bilo treba izvesti t. i. akcijsko raziskovanje v obliki kvazi-eksperimenta, kjer bi dejansko spremljali število za informacijsko varnost rizičnih dogodkov pred in po ogledu e-vsebin. Pričujoči članek prikazuje zgolj prvi del omenjene raziskave, sledi še uporaba e-vsebin in ugotavljanje učinka le-teh. Pojavlja pa se tudi vprašanje, kako opazovati in ugotoviti rizična dejanja med medicinskimi sestrami, saj že s samim opazovanjem oz. s samo seznanitvijo, da so opazovane, lahko vplivamo na njihovo obnašanje. Odgovori na ta vprašanja so ključnega pomena, saj vplivajo na načrt nadaljnje raziskave in seveda tudi na pridobivanje etičnih dovoljenj.

Skladno s smernicami Ministrstva za zdravje Republike Slovenije bo slovenski zdravstveni sistem slej ali prej dobil težko pričakovani elektronski zdravstveni zapis. Green in Rubin (2011) pa eksplicitno opozarjata na probleme informacijske varnosti pri njegovi uvedbi v prakso. Skladno s tem menimo, da je treba tako medicinske sestre kot ostale zdravstvene delavce pravočasno opozoriti na omenjeno problematiko. Informacijska varnost je proces, ki se v določeni instituciji razvija samo postopoma (IT Governance Institute, 2007) in je tesno povezan z organizacijsko kulturo. Po uvedbi tega pomembnega elementa informatizacije slovenskega zdravstvenega sistema ne bo več časa za pridobivanje omenjenega znanja.

5 Zaključek

IKT nudi veliko možnosti, ena izmed teh je e-izobraževanje. Tovrsten način izobraževanja se vedno bolj uveljavlja tudi v Sloveniji. Uporabnike IKT, v tem primeru medicinske sestre, je treba motivirati, da sprejmejo ta način učenja in se mu ne izogibajo, saj s tem kvečjemu pripomorejo k izvajanju kvalitetne zdravstvene nege. Tehnologija jim nudi podporo pri vsakdanjem delu in zato je na tem področju treba narediti spremembo.

Primanjkljaj znanja na področju informacijske varnosti predstavlja pri medicinskih sestrah nevarnost za zdravstvo. Na žalost se vse morebitnih posledic sploh ne zavedajo, zato omenjene e-vsebine lahko veliko pripomorejo k izboljšanju stanja. Glede na to, da je prva avtorica prispevka razvila e-vsebine kot del svoje diplomske naloge na dodiplomskem študiju zdravstvene nege, menimo, da je pričujoči prispevek lahko dokaz, da lahko tudi zdravstveni delavci razvijemo kakovostne e-vsebine na področju

zdravstva. Žal pa je v Sloveniji tovrstnih e-vsebin premalo in mogoče bo pričujoči prispevek spodbudil širšo javnost k njihovemu razvoju in ponudbi za širše občinstvo. Glede na številne dobre primere uporabe razvitih e-vsebin v zdravstvu, ki jih navaja literatura, bi lahko medicinske sestre na učinkovit in zabaven način pridobile potrebno znanje in kompetence. Orodje, ki smo ga uporabili za razvoj e-vsebin, omogoča enostavno izdelavo in posodobitev le-teh. Za izdelavo kakovostnih in kompleksnih e-vsebin pa je potrebno nekoliko več znanja, ki ga lahko pridobimo z izkušnjami na tem področju in ob sodelovanju s strokovnjaki, ki se ukvarjajo z razvojem e-vsebin.

Sara Rošeto, Pucer Patrik, PhD, Irena Trobec, PhD, Boštjan Žvanut, PhD

Identification and Development of E-Contents about Information Security in Nursing

Nowadays, information communication technologies are an important part of people's life and have a considerable role in healthcare systems. The quality of healthcare services depends also on the accessibility of patient data, which, in this era, should be available digitally.

Effective documentation of nursing processes is one of the key problems of healthcare. The information system provides support to nurses in their everyday work. Nurses also access patient data, which according to the legislation, should be carefully protected. Many countries have well-defined legislation and policies to protect the confidentiality of patient information. For example, in Slovenia the following acts regulate this field: Healthcare and Health Insurance Act, Health Services Act, Patients' Rights Act, Healthcare Databases Act, Rules on Compulsory Health Insurance, Personal Data Protection Act, Electronic Commerce and Eelectronic Signature Act, Criminal Code of the Republic of Slovenia. However, in everyday nursing practice it is possible to identify different threats to the violation of information security. According to many studies, leaking of confidential information and unauthorised information access are not an exception and the technology alone does not ensure that the aforementioned regulations will be respected. A study performed by Albarrak (2012) on a group of nurses in Saudi Arabia shows that there is a gap between the knowledge and actual behaviour of nurses in this field. It is important to increase the level of awareness of this population in the field of information security, as they represent approximately half of the employees in healthcare services. Hence, the healthcare organisations should implement the required information security processes and train all their employees, which have access to the healthcare information system. The violations of information security can have serious consequences which cannot be expressed in financial terms only. Such violations can have a serious impact even on patient safety and thus endanger patients' lives. In practice, nurses can give the impression that they have a good knowledge of the field of information security to the management and to the experts in the field of information security. However, the issue of risky behaviour

in the field of information security, which is highlited by Albarrak (2012), represents a time bomb for healthcare organizations, entire healthcare systems, and the protection of patients' rights.

According to the results found in the literature and in other relevant resources, we realised that there are no available e-contents or digital materials in Slovenian language for the acquisition of knowledge in the field of information security appropriate for nurses and other healthcare staff. The goal of this study was to identify different threats to the violation of information security in a particular health institution and develop e-learning contents for nurses, which will present the problems of information security in an appropriate way.

Our study consisted of three phases: (1) identification of threats to the violation of information security; (2) development of e-contents; and (3) evaluation of the developed e-contents. The threats were identified with a literature review and interviews. The interviews were performed in October 2012 with health informatics experts in the mentioned healthcare institution. Both interviewees have considerable experiences in health informatics and they work with nurses on a daily basis. According to five different identified threats, wedeveloped e-learning contents, which vividly present the aforementioned violations and potential consequences. Different real clinical situations are presented with comics, which were designed with the web application Bitstrip. For the development of e-contents the freeware application CourseLab 2.4 was used. Some key features of CourseLab 2.4 are: "What you see is what you get" environment for creating and managing high-quality interactive e-learning content, where no special programming skills are required; no internet connection is required in the development phase; allows the use and test of multimedia elements in different formats (text, sound, images, animations, videos); allows the implementation of simple or complex navigation through e-content in a trivial manner; no Java or other supporting program installation is required. CourseLab 2.4 supports the Sharable Content Object Reference Model (SCORM) standard, which provides the interoperability of the created e-contents and thus their use on different learning management systems.

In phase 2, the following e-contents were developed: Violation of personal data privacy, Password abuse, Violation of data privacy on the telephone, Web browsing on a ward computer, and Infected USB stick. Our goal was to develop e-contents where nurses can recognize themselves and their potential violations to information security. The developed e-contents are of different lengths, the shortest consists of 8 presentation slides, the longest of 11. All contents are introduced by the introduction page, followed by different animations, where comic balloons, different images, etc. make the e-contents interesting and attractive for the target population. The transition between slides is implemented through different navigation elements, where squares indicate the exact position in the e-content. The e-contents were deployed on Moodle learning management system. In order to be available to a broader interested public the e-contents are available also on the following web site: http://inoedu.info/evsebine/roseto/ (the use of web browser Google Chrome or Firefox is recommended). Each of the contents is represented with a state transition diagram, which in fact represents

the scenario of the developed e-content. A detailed description of each state in the diagram, represented by the square, is described in detail in the corresponding table. In fact, each state is transformed in one slide of the developed e-content.

Finally in phase 3, the e-contents were evaluated by one of the interviewees and a university lecturer, expert in the field of information and communication technology. The results of the evaluation indicate that the developed e-contents are useful, attractive, on an adequate level of quality, and appropriate for the target population. The deficiencies identified by the experts were removed, for example: lack of explanation of what does adequate identification actually mean in the e-content Violation of personal data privacy, grammatical errors, unclear texts, visual inconsistencies, excessive loading time, and inadequate colouring. However, some of the deficiencies were not possible to remove due to technical limitations of the tools used in the development phase and lack of financial resources, which will be required for the development of new multimedia components. Despite the fact that the e-contents were developed in collaboration with information system experts of one healthcare institution, we believe that the developed e-contents would be of interest to other institutions as the presented violations were also identified in the literature. Both evaluators concluded that the developed e-contents are appropriate for the acquisition of knowledge in the field of information security for the population under consideration.

According to the directives of Ministry of Health, Republic of Slovenia, the Slovenian health system will sooner or later introduce the electronic health record. Healthcare workers should be properly informed about the potential threats of its use in practice. Information security is a process, which can be developed only gradually as it is tightly connected with the organisation's culture. When the electronic health record will be implemented in practice, there will be no time left for the acquisition of the required knowledge in the field of information security. The lack of nurses' knowledge in the field of information security represents a threat for the reliability and data protection. The developed e-contents could improve the situation in this field. Unfortunately, in Slovenia there is a lack of e-contents and we hope that this article will encourage experts to design and develop similar e-contents and to make them available to the broader public.

With this study it is not possible to confirm, if the developed e-contents have actually an effect on nurses' information security related behaviour. To confirm this, further studies should be performed. For example, a combination of action research with a quasi-experiment, where potential threats to information security will be monitored before and after visiting the e-contents. Another interesting question is how to monitor nurses' behaviour and how to identify the security threats among nurses, since the sole information about being observed can substantially modify their behaviour. However, according to the experts opinion, the developed e-contents are properly designed and implemented and there is no argument not to test them in the real environment.

The first author of the article was a nursing student (BSc) and developed these contents as a part of her diploma thesis with the help of other authors. Hence, we believe that also other nurses can actively participate in the development of similar

e-contents in their field of expertise. This will facilitate the dissemination of their knowledge in practice and not only in the field of information security. The tools used in this study allow the development of trivial, but still effective multimedia e-contents. A short training is required for nurses to be able to design and develop these contents. However, the development of complex e-contents on a certain level of quality requires expert knowledge, which can be achieved through their past experience and interdisciplinary work with experts in the field of e-learning.

LITERATURA

1. Albarrak, A. (2012). Information security behavior among nurses in an academic hospital. HealthMED, št. 6, str. 2349–2354.
2. Gobuty, D. E. (2003). Organizing security and privacy enforcement in medical imaging technology. Int. Congr. Ser., CARS 2003. Computer Assisted Radiology and Surgery. Proceedings of the 17th International Congress and Exhibition 1256, str. 319–329.
3. Green, M. D. and Rubin, A. D. (2011). A research roadmap for healthcare IT security inspired by the PCAST health information technology report, in: Proceedings of the 2nd USENIX Conference on Health Security and Privacy. USENIX Association, San Francisco, CA, str. 5.
4. IT Governance Institute (2007). COBIT. IT Governance Institute, Rolling Meadows, IL.
5. Kač, L., Kreuh, N. in Mohorčič, G. (2011). Izhodišča za izdelavo e-učbenikov - elektronski vir, 2. izd. Ljubljana: Zavod Republike Slovenije za šolstvo.
6. Leino-Kilpi, H., Välimäki, M., Dassen, T., Gasull, M., Lemonidou, C., Scott, A. and Arndt, M. (2001). Privacy: a review of the literature. International Journal of Nursing Studies, št. 38, str. 663–671.
7. Linden, H. van der, Kalra, D., Hasman, A. and Talmon, J. (2009). Inter-organizational future proof EHR systems. A review of the security and privacy related issues. International Journal of Medical Informatics, št. 78, str. 141–160.
8. Marcelan, N. in Bernik, I. (2012). Varnost in zagotavljanje zasebnosti bolnišničnih podatkov o pacientih. V: Bernik, I. in Meško, G. (ur.), Zbornik prispevkov/ Konferenca Informacijska varnost: odgovori na sodobne izzive, Ljubljana, 20. 1. 2012. Pridobljeno dne 27. 5. 2014 s svetovnega spleta: http://www.fvv.uni-mb.si/konferencaIV/zbornik.html.
9. Prijatelj, V. (2006). Opportunities and obstacles in electronic data collection in nursing. Studies in health technology and informatics, št. 122, str. 329–332.
10. Rajkovič, U. (2010). Sistemski pristop k oblikovanju e-dokumentacije zdravstvene nege.
11. Spletna stran Bitstrips, n. d. Bitstrips - Comics starring YOU and your Friends. Pridobljeno dne 27. 5. 2014 s svetovnega spleta: http://www.bitstrips.com/.
12. Trček, D., Trobec, R., Pavešić, N. and Tasič, J. F. (2007). Information systems security and human behaviour. Behav. Information Technology, št. 26, str. 113–118.

Sara Rošeto, diplomantka na Fakulteti za vede o zdravju Univerze na Primorskem.
E-naslov: sarica712@gmail.com

Dr. Pucer Patrik, predavatelj na Fakulteti za vede o zdravju Univerze na Primorskem.
E-naslov: patrik.pucer@fvz.upr.si

Dr. Irena Trobec, docentka na Fakulteti za vede o zdravju Univerze na Primorskem.
E-naslov: irena.trobec@fvz.upr.si

Dr. Boštjan Žvanut, docent na Fakulteti za vede o zdravju Univerze na Primorskem.
E-naslov: bostjan.zvanut@fvz.upr.si